Bitdefender®

INTERNET SECURITY 2018

PODRĘCZNIK UŻYTKOWNIKA

Bitdefender Internet Security 2018
Podręcznik użytkownika

Data publikacji 07/05/2017

Uwagi prawne

Bitdefender

Spis treści

INSTALACJA

1. PRZYGOTOWANIE DO INSTALACJI

Zanim zainstalujesz Bitdefender Internet Security 2018, wykonaj odpowiednie przygotowania, aby instalacja przebiegała płynnie i bez problemów:

- Upewnij się, że komputer, na którym chcesz zainstalować produkt Bitdefender, spełnia minimalne wymagania systemowe. Jeśli komputer nie spełnia minimalnych wymagań systemowych, Bitdefender nie zostanie zainstalowany lub zainstaluje się, lecz nie będzie działał poprawnie, w znacznym stopniu spowalniając pracę systemu i czyniąc go niestabilnym. Aby zobaczyć pełną listę wymagań systemowych, przejdź do *„Wymagania systemowe"* (p. 3).
- Zaloguj się do systemu korzystając z konta administratora.
- Usuń z komputera wszelkie oprogramowanie antywirusowe. Jeśli coś zostanie wykryte w procesie instalacji Bitdefender, będziesz powiadomiony aby to odinstalować. Jednoczesne korzystanie z dwóch programów antywirusowych może wpłynąć negatywnie na ich działanie i powodować problemy z systemem. Podczas instalacji zostanie wyłączony program Windows Defender.
- Zablokuj lub usuń oprogramowanie zapory sieciowej, które może być uruchomione na tym komputerze. Korzystanie z dwóch zapór sieciowych naraz może wpłynąć negatywnie na ich działanie i spowodować problemy z systemem. Podczas instalacji Zapora sieciowa systemu Windows zostanie wyłączona.
- Zaleca się, aby w czasie instalacji komputer był podłączony do internetu, nawet jeśli instalacja prowadzona jest z płyty CD/DVD. Jeśli nowsze wersje plików aplikacji zawartych w pakiecie instalacyjnym będą dostępne, Bitdefender może je pobrać i zainstalować.

2. WYMAGANIA SYSTEMOWE

Możesz zainstalować Bitdefender Internet Security 2018 tylko na komputerach z następującymi systemami operacyjnymi:

- Windows 7 z dodatkiem Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Przed instalacją upewnij się, że Twój komputer spełnia minimalne wymagania systemowe.

Notatka

Aby poznać szczegóły systemu Windows zainstalowanego na komputerze oraz informacje o konfiguracji sprzętowej, wykonaj następujące czynności:

- W systemie **Windows 7** należy kliknąć prawym na ikonę **Mój Komputer** i następnie wybrać **Właściwości** z menu kontekstowego
- Na ekranie menu Start systemu **Windows 8** zlokalizuj **Komputer** (przykładowo, możesz zacząć pisać "Komputer" bezpośrednio na ekranie menu Start) a następnie kliknąć na jego ikonę. W systemie **Windows 8.1**, zlokalizuj **Ten Komputer**.

  Wybierz **Właściwości** w dolnym menu. Zajrzyj do obszaru **Informacje o systemie** , aby znaleźć informacje o rodzaju systemu.
- Na **Windows 10** , kliknij ikonę wyszukiwania na pasku i wpisz **Informacje o systemie** Zajrzyj do obszaru **Informacje o systemie** , aby znaleźć informacje o rodzaju systemu.

2.1. Minimalne wymagania systemowe

- 1.5 GB wolnej przestrzeni na dysku twardym
- Dual core procesor 1.6 GHz
- 1 GB pamięci (RAM)

2.2. Zalecane wymagania systemowe

- 2 GB wolnego miejsca na dysku twardym (przynajmniej 800 MB na dysku systemowym)
- Intel CORE Duo (2 GHz) lub procesor o podobnej wydajności
- 2 GB pamięci (RAM)

2.3. Wymagania programowe

Aby móc używać Bitdefender i wszystkich jego funkcji, komputer musi spełniać następujące wymagania programowe:

- Microsoft Edge 40 lub wyższa
- Internet Explorer 10 lub nowszy
- Mozilla Firefox 51 lub wyższa
- Google Chrome 34 i wyższa
- Skype 6.3 lub nowszy
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 lub nowsza

3. INSTALOWANIE PRODUKTU BITDEFENDER

Możesz zainstalować Bitdefender z dysku instalacyjnego lub korzystając z instalatora internetowego pobranego na komputer z Bitdefender Central.

Jeśli Twój zakup obejmuje więcej niż jeden komputer (np. kupiłeś Bitdefender Internet Security 2018 na 3 stanowiska), powtórz proces instalacji i aktywuj swój produkt, korzystając z tego samego konta na każdym komputerze. Konto, które powinieneś użyć, to to, które zawiera Twoją aktywną subskrypcję Bitdefender.

3.1. Zainstaluj z Bitdefender Central

Z konta Bitdefender Central możesz pobrać pakiet instalacyjny odpowiadający zakupionej subskrypcji. Po zakończeniu instalacji, Bitdefender Internet Security 2018 jest aktywny.

Aby pobrać Bitdefender Internet Security 2018 z Bitdefender Central:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. W oknie **MOJE URZĄDZENIA**, kliknij **ZAINSTALUJ Bitdefender**.
4. Wybierz jedną z dwóch dostępnych opcji:
   - **POBIERANIE**

     Kliknij przycisk i zapisz plik instalacyjny.
   - **Na innym urządzeniu**

     Zaznacz **Windows**, aby pobrać swój produkt Bitdefender, a następnie kliknij **KONTYNUUJ**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ**.
5. Poczekaj na zakończenie pobierania, a następnie uruchomm instalator.

Sprawdzanie poprawności instalacji

Bitdefender sprawdzi najpierw Twój system, aby zatwierdzić poprawność instalacji.

Jeśli system nie spełnia minimalnych wymagań do zainstalowania Bitdefender, zostaniesz poinformowany o obszarach, które należy poprawić, zanim przejdziesz dalej.

W przypadku wykrycia starszej wersji Bitdefender lub jakiegokolwiek niekompatybilnego programu antywirusowego, zostaniesz poproszony o jego usunięcie z systemu. Postępuj według wskazówek, aby usunąć oprogramowanie z systemu i dzięki temu uniknąć problemów w przyszłości. W celu zakończenia usuwania wykrytych programów antywirusowych niezbędne może być ponowne uruchomienie komputera.

Pakiet instalacyjny Bitdefender Internet Security 2018 jest stale uaktualniany.

Notatka

Pobieranie plików instalacyjnych może zająć chwilę, zwłaszcza w przypadku wolnego łącza internetowego.

Po sprawdzeniu poprawności instalacji wyświetlony zostanie kreator konfiguracji. Aby zainstalować Bitdefender Internet Security 2018, wykonaj poniższe kroki.

Krok 1 - instalacja Bitdefender

W oknie procesu instalacji Bitdefender, kliknij przycisk **Instaluj** aby uruchomić proces instalacji produktu Bitdefender

Trzy dodatkowe zadania mogą być wykonane w tym kroku:

- Przed rozpoczęciem instalacji zapoznaj się z Umową Subskrypcji. Umowa Subskrypcji precyzuje warunki, zgodnie z którymi możesz korzystać z Bitdefender Internet Security 2018.

  Jeśli nie wyrażasz zgody na te warunki, zamknij to okno. Proces instalacji zostanie przerwany, a praca instalatora zakończy się.

- Zachowaj opcję **Wyślij anonimowe raporty użycia** włączoną. Dopuszczając tę opcję, na serwery Bitdefender wysyłane są raporty wyszczególniające sposób użytkowania produktu. Te informacje są kluczowe dla ulepszenia produktu i pomogą nam zapewnić wygodniejszą obsługę produktu w przyszłości. Proszę mieć na uwadze, iż raporty nie zawierają żadnych prywatnych danych, takich jak Twoja nazwa użytkownika, czy adres IP. Dodatkowo, raporty nigdy nie zostaną wykorzystane do celów komercyjnych.

- Wybierz język, w którym chcesz zainstalować produkt.

Krok 2 - Instalacja w toku

Zaczekaj, aż instalacja zostanie zakończona. Wyświetlane są szczegółowe informacje o postępie.

Ważne obszary systemu skanowane są pod kątem obecności wirusów, pobierane i instalowane są najnowsze wersje plików aplikacji, uruchamiane są główne usługi Bitdefender. Ten krok może zająć kilka minut.

Krok 3 - Ukończenie instalacji

Twój produkt Bitdefender został pomyślnie zainstalowany.

Wyświetlane jest podsumowanie instalacji. Jeśli w czasie instalacji zostanie wykryte i usunięte jakiekolwiek aktywne złośliwe oprogramowanie, konieczne może być ponowne uruchomienie systemu. Kliknij **ZACZNIJ UŻYWAĆ Bitdefender**, aby kontynuować.

Krok 4 - Rozpocznij

W oknie **Rozpocznij** możesz sprawdzić informacje na temat swojej aktywnej subskrypcji.

Kliknij **Zakończ**, aby uzyskać dostęp do interfejsu Bitdefender Internet Security 2018.

3.2. Zainstaluj z płyty instalacyjnej

Aby zainstalować Bitdefender z dysku instalacyjnego, włóż dysk do napędu optycznego.

Za chwilę powinien wyświetlić się ekran instalacyjny. Aby rozpocząć instalację, postępuj według instrukcji.

Jeżeli ekran instalacyjny się nie pojawi, użyj Windows Eksplorer, aby dotrzeć do katalogu głównego napędu i dwukrotnie kliknij na plik autorun.exe.

Jeśli łącze internetowe jest powolne lub system nie jest podłączony do Internetu, kliknij przycisk **Zainstaluj z CD/DVD**. W tym przypadku, produkt Bitdefender dostępne na dysku zostanie zainstalowany i nowsza wersja zostanie pobrana z serwerów Bitdefender poprzez aktualizację produktu.

Sprawdzanie poprawności instalacji

Bitdefender sprawdzi najpierw Twój system, aby zatwierdzić poprawność instalacji.

Jeśli system nie spełnia minimalnych wymagań do zainstalowania Bitdefender, zostaniesz poinformowany o obszarach, które należy poprawić, zanim przejdziesz dalej.

W przypadku wykrycia starszej wersji Bitdefender lub jakiegokolwiek niekompatybilnego programu antywirusowego, zostaniesz poproszony o jego usunięcie z systemu. Postępuj według wskazówek, aby usunąć oprogramowanie z systemu i dzięki temu uniknąć problemów w przyszłości. W celu zakończenia usuwania wykrytych programów antywirusowych niezbędne może być ponowne uruchomienie komputera.

Notatka

Pobieranie plików instalacyjnych może zająć chwilę, zwłaszcza w przypadku wolnego łącza internetowego.

Po sprawdzeniu poprawności instalacji wyświetlony zostanie kreator konfiguracji. Aby zainstalować Bitdefender Internet Security 2018, wykonaj poniższe kroki.

Krok 1 - Instalacja Bitdefender

W oknie procesu instalacji Bitdefender, kliknij przycisk **Instaluj** aby uruchomić proces instalacji produktu Bitdefender

Trzy dodatkowe zadania mogą być wykonane w tym kroku:

- Przed rozpoczęciem instalacji zapoznaj się z Umową Subskrypcji. Umowa Subskrypcji precyzuje warunki, zgodnie z którymi możesz korzystać z Bitdefender Internet Security 2018.

  Jeśli nie wyrażasz zgody na te warunki, zamknij to okno. Proces instalacji zostanie przerwany, a praca instalatora zakończy się.

- Zachowaj opcję **Wyślij anonimowe raporty użycia** włączoną. Dopuszczając tę opcję, na serwery Bitdefender wysyłane są raporty wyszczególniające sposób użytkowania produktu. Te informacje są kluczowe dla ulepszenia produktu i pomogą nam zapewnić wygodniejszą obsługę produktu w przyszłości. Miej na uwadze, iż raporty nie zawierają żadnych prywatnych

danych, takich jak Twoja nazwa użytkownika, czy adres IP. Dodatkowo, raporty nigdy nie zostaną wykorzystane do celów komercyjnych.

- Wybierz język, w którym chcesz zainstalować produkt.

Krok 2 - Instalacja w toku

Zaczekaj, aż instalacja zostanie zakończona. Wyświetlane są szczegółowe informacje o postępie.

Kluczowe obszary Twojego systemu są skanowane w poszukiwaniu wirusów, następnie startują usługi Bitdefender Ten krok może zająć kilka minut.

Krok 3 - Ukończenie instalacji

Wyświetlane jest podsumowanie instalacji. Jeśli w czasie instalacji zostanie wykryte i usunięte jakiekolwiek aktywne złośliwe oprogramowanie, konieczne może być ponowne uruchomienie systemu. Kliknij **ZACZNIJ UŻYWAĆ Bitdefender**, aby kontynuować.

Krok 4 - konto Bitdefendera

Po zakończeniu wstępnej konfiguracji, pojawi się okno konta Bitdefender. Konto Bitdefender jest wymagane w celu aktywacji produktu i wykorzystania jego możliwości online. Aby uzyskać więcej informacji, odwołaj się do *„Bitdefender Central”* (p. 37).

Postępuj zgodnie z zaistniałą sytuacją.

Chcę utworzyć konto Bitdefender

Wpisz wymagane informacje w odpowiednie pola, a następnie kliknij przycisk **UTWÓRZ KONTO**.

Wprowadzone dane pozostaną poufne.

Hasło musi mieć co najmniej 8 znaków i zawierać cyfrę.

Przeczytaj warunki usług Bitdefender przed dalszymi krokami

Notatka

Po utworzeniu konta możesz użyć podanego adresu e-mail oraz hasła, aby zalogować się na swoje konto pod adresem https://central.bitdefender.com.

Już posiadam konto Bitdefender

Kliknij **Zapisz się**, następnie wprowadź adres e-mail oraz hasło do Twojego konta Bitdefender.

Kliknij **Zapisz się**, aby kontynuować.

Jeśli zapomniałeś hasła do swojego konta lub po prostu chcesz zresetować to, które już ustawiłeś, kliknij link **Zapomniałem hasła**. Wpisz swój adres e-mail, a następnie kliknij przycisk **ZAPOMNIAŁEM HASŁA**. Sprawdź swoje konto e-mail i wykonaj podane instrukcje, aby ustawić nowe hasło dla swojego konta Bitdefender.

Notatka

Jeśli masz już konto MyBitdefender, możesz je użyć do zalogowania się do konta Bitdefender. Jeśli zapomniałeś swojego hasła, to najpierw musisz iść do https://my.bitdefender.com, aby je zresetować. Następnie, użyj zaktualizowanych poświadczeń, aby zalogować się do swojego konta Bitdefender.

Chcę się zalogować przy użyciu konta Microsoft, Facebook lub Google (opcja aktualnie niedostępna)

Aby zalogować się przy użyciu konta Microsoft, Facebook lub Google:

1. Wskaż usługę, której chcesz użyć. Zostaniesz przekierowany na stronę logowania tej usługi.
2. Postępuj zgodnie ze wskazówkami wyświetlanymi przez wybraną usługę, aby połączyć Twoje konto z produktem Bitdefender.

Notatka

Bitdefender nie ma dostępu do żadnych poufnych informacji, takich jak hasło, którego używasz do logowania, czy osobiste informacje o Twoich znajomych i kontaktach.

Krok 5 - Aktywuj swój produkt

Notatka

Krok ten pojawia się, jeśli wybrałeś, aby utworzyć nowe konto Bitdefender podczas poprzedniego etapu lub jeśli zalogowałeś się za pomocą konta z wygasłą subskrypcją.

Aktywne połączenie internetowe jest wymagane do ukończenia aktywacji produktu.

Postępuj zgodnie ze swoją sytuacją:

- Mam kod aktywacyjny

  W takim przypadku, aktywuj produkt, wykonując następujące czynności:

  1. Wisz kod aktywacyjny w polu **Mam kod aktywacyjny**, a następnie kliknij **KONTYNUUJ**.

     Notatka
     Możesz znaleźć swój kod aktywacyjny:
     - na etykiecie płyty CD/DVD.
     - na karcie rejestracyjnej produktu.
     - w wiadomości e-mail potwierdzającej zakup.

  2. **Chcę przetestować Bitdefender**

     W takim przypadku możesz korzystać z produktu przez 30 dni. Aby zacząć okres próbny, wybierz **Nie mam subskrypcji, chcę wypróbować produkt za darmo**, następnie kliknij **KONTYNUUJ**.

Krok 6 - Rozpocznij

W oknie **Rozpocznij** możesz sprawdzić informacje na temat swojej aktywnej subskrypcji.

Kliknij **Zakończ**, aby uzyskać dostęp do interfejsu Bitdefender Internet Security 2018.

ROZPOCZNIJ

4. PODSTAWY

Po zainstalowaniu Bitdefender Internet Security 2018 Twój komputer jest chroniony przed wszystkimi rodzajami złośliwego oprogramowania (tzn. wirusami, oprogramowaniem szpiegującym, ransomware, exploitami, botnetami i trojanami) i zagrożeń internetowych (hakerami, phishingiem i spamem).

Aplikacja korzysta z technologii Photon, aby zwiększyć szybkość i wydajność procesu skanowania w poszukiwaniu zagrożeń. Działa poprzez poznanie sposobów korzystania z aplikacji systemowych, aby wiedzieć, co i kiedy skanować i jak minimalizować wpływ na wydajność systemu.

Możesz zarządzać swoimi hasłami i kontami online poprzez przechowywanie ich w *„Ochrona Manager Haseł dla Twoich poświadczeń”* (p. 146) w portfelu. Z jednym głównym hasłem możesz chronić swoją prywatność przed intruzami, którzy mogą próbować pozbawić cię pieniędzy.

„Ochrona kamery internetowej” (p. 140)trzymaj niezaufane aplikacje z dala od Twojej kamery internetowej, unikając w ten sposób prób włamania się. W zależności od wyborów użytkowników Bitdefender dostęp do popularnych aplikacji w Twojej kamerze będzie dozwolony lub zablokowany.

Aby chronić cię przed potencjalnym podsłuchanie i szpiegowaniem, kiedy twoje urządzenie jest podłączone do niezabezpieczonej sieci, Bitdefender analizuje poziom ochrony, i jeśli to konieczne, podpowiada jak zwiększyć ochronę przy twoich aktywnościach online. W poszukiwaniu instrukcji jak zachować swoje osobiste dane chronione, proszę sprawdzić *„Doradca Ochrony Wi-Fi ”* (p. 136).

Twoje osobiste pliki przechowywane lokalnie takie jak dokumenty, fotografie lub filmy oraz te pliki przechowywane w chmurze, mogą zostać zabezpieczone przed dzisiejszym najgorszym cybernetycznym zagrożeniem: ransomware. Po informacje jak chronić prywatne pliki, proszę odnieś się do *„Bezpieczne pliki”* (p. 143).

Podczas gdy Ty pracujesz, grasz lub oglądasz filmy, Bitdefender może wstrzymać lub przesunąć zadania konserwacyjne, eliminując przerwy i dostosowując efekty wizualne systemu. Możesz korzystać z tego wszystkiego aktywując i konfigurując *„Tryby”* (p. 177).

Bitdefender podejmie za Ciebie większość decyzji związanych z ochroną, a powiadomienia będą wyświetlane niezwykle rzadko. Szczegóły podjętych

działań oraz informacje o działaniu programu są dostępne w oknie "Powiadomienia". Aby uzyskać więcej informacji, odwołaj się do *„Powiadomienia"* (p. 17).

Od czasu do czasu należy otworzyć Bitdefender i rozwiązać wszelkie istniejące problemy. Być może będziesz musiał skonfigurować niektóre komponenty Bitdefender lub podjąć akcje prewencyjne, aby skutecznie chronić komputer i swoje dane.

Aby korzystać z funkcji internetowych Bitdefender Internet Security 2018 i zarządzać swoimi subskrypcjami i urządzeniami, wejdź do swojego konta Bitdefender. Aby uzyskać więcej informacji, odwołaj się do *„Bitdefender Central"* (p. 37).

W sekcji „Jak to zrobić?" (p. 48) znajdziesz instrukcje krok po kroku dotyczące wykonywania typowych zadań. W przypadku wystąpienia problemów podczas korzystania z Bitdefender, sprawdź sekcję *„Rozwiązywanie typowych problemów"* (p. 185) w poszukiwaniu rozwiązań najczęstszych problemów.

4.1. Otwieranie okna Bitdefender

Aby uzyskać dostęp do głównego interfejsu Bitdefender Internet Security 2018, wykonaj poniższe czynności:

- W systemie **Windows 7**:
  1. Kliknij **Start** i przejdź do **Wszystkie programy**.
  2. Kliknij **Bitdefender 2018**.
  3. Kliknij **Bitdefender Internet Security 2018** lub, w szybszy sposób, dwukrotnie kliknij ikonę Bitdefender B w zasobniku systemowym.
- W systemach **Windows 8 i Windows 8.1**:

  Na ekranie menu Start systemu Windows zlokalizuj Bitdefender Internet Security 2018 (przykładowo, możesz zacząć pisać "Bitdefender" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę. Alternatywnie, otwórz aplikację Pulpit, a następnie kliknij dwukrotnie ikonę Bitdefender B w zasobniku systemowym.
- W systemie **Windows 10**:

  Wpisz "Bitdefender" w polu wyszukiwania z paska zadań, a następnie kliknij jego ikonę. Alternatywnie, kliknij dwa razy ikonę Bitdefender B w zasobniku systemowym.

Więcej informacji o oknie programu i ikonie Bitdefender w zasobniku systemowym znajdziesz w *„Interfejs produktu Bitdefender"* (p. 22).

4.2. Rozwiązywanie problemów

Bitdefender używa systemu śledzenia problemów, aby wykryć i poinformować Cię o zagadnieniach mogących mieć negatywny wpływ na bezpieczeństwo komputera i Twoich danych. Domyślnie, monitorowane są tylko grupy zagadnień uważanych za najważniejsze. Możesz także skonfigurować, wedle potrzeb, wyświetlanie powiadomień dotyczących tylko konkretnych zagadnień.

Wykryte problemy mogą dotyczyć ważnych ustawień ochrony, które są wyłączone oraz innych czynników, które mogą stwarzać zagrożenia bezpieczeństwa. Są one podzielone na dwie kategorie:

- **Problemy krytyczne** - uniemożliwiają Bitdefender ochronę przed złośliwym oprogramowaniem lub niosą ze sobą duże zagrożenie bezpieczeństwa.
- **Problemy o mniejszej wadze** - mogą w przyszłości wpływać na poziom ochrony.

Ikona produktu Bitdefender w zasobniku systemowym pokazuje aktualne problemy, zmieniając kolory na następujące:

Problemy krytyczne bezpośrednio wpływają na bezpieczeństwo systemu. Wymagają natychmiastowej uwagi i muszą być naprawione tak szybko, jak jest to możliwe.
Niekrytyczne problemy dotyczące pośrednio bezpieczeństwa systemu. Należy zająć się tymi problemami, gdy tylko będzie taka sposobność.

Dodatkowo, jeśli przesuniesz wskaźnik myszy nad ikonę, wyświetlone zostanie okienko z potwierdzeniem istnienia oczekujących zagadnień.

Po otwarciu interfejs Bitdefender pole stanu ochrony w górnym pasku narzędziowym pokaże typ zagadnień zagrażających bezpieczeństwu systemu.

4.2.1. Instruktor postępowania z problemami ochrony

Aby naprawić wykryte problemy, postępuj zgodnie z instrukcjami kreatora **naprawiania wszystkich problemów**.

1. Aby uruchomić kreator, wykonaj którąś z następujących czynności:

- Kliknij prawym przyciskiem myszy na ikonie Bitdefender w zasobniku systemowym i wybierz **Wyświetl problemy bezpieczeństwa**.
- Otwórz okno interfejsu Bitdefender i kliknij gdziekolwiek na obszarze Statusu ochrony na górnym pasku narzędziowym.

2. Możesz zobaczyć problemy wpływające na bezpieczeństwo Twojego komputera i danych. Wszystkie aktualne problemy zostały wybrane do naprawienia.

   Jeśli nie chcesz zajmować się konkretnym problemem od razu, odznacz odpowiadające mu pole wyboru. Zostaniesz poproszony o określenie, na jak długo chcesz odłożyć naprawę problemu. Wybierz z menu żądaną opcję i kliknij **OK**. Aby przestać monitorować konkretną kategorię zagadnień, wybierz **Trwale**.

   Stan problemu zmieni się na **Odroczony** i nie zostanie podjęta żadna akcja, aby go naprawić.

3. Aby naprawić wybrane zagadnienia, kliknij **Napraw**. Niektóre zagadnienia są naprawiane natychmiast. Inne problemy wymagają użycia kreatora.

Zagadnienia, które wymagają pomocy kreatora, zostały podzielone na kilka głównych kategorii:

- **Wyłączone ustawienia zabezpieczeń.** Takie problemy są rozwiązywane natychmiast, poprzez włączenie odpowiednich ustawień ochrony.
- **Zapobiegawcze zadania bezpieczeństwa, które należy wykonać.** Podczas naprawiania zagadnień tego typu, kreator pomaga wykonać każde z zadań.

4.2.2. Konfigurowanie powiadomień

Bitdefender może poinformować Cię, gdy wykrywane są problemy z funkcjonowaniem następujących komponentów programu:

- Ochrona antywirusowa
- Zapora Sieciowa
- Aktualizacja
- Ochrona przeglądarki internetowej

System powiadomień można skonfigurować tak, aby najlepiej służył zapewnieniu ochrony, poprzez wybranie zagadnień, o których chcesz być informowany. Wykonaj następujące kroki:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.

2. Wybierz zakładkę **Zaawansowane**.
3. Kliknij **Konfiguruj powiadomienia**.
4. Kliknij przyciski, aby włączyć lub wyłączyć powiadamianie według własnego uznania.

4.3. Powiadomienia

Bitdefender zapisuje szczegółowy dziennik zdarzeń mających miejsce na Twoim komputerze. Ilekroć wydarzy się coś ważnego dla bezpieczeństwa systemu lub danych, dodawana jest nowa wiadomość do obszaru Zdarzeń Bitdefender, oprócz tego w skrzynce mailowej też pojawi się informacja.

Powiadomienia są ważnym narzędziem w monitorowaniu i zarządzaniu ochroną Bitdefender Przykładowo, możesz łatwo sprawdzić czy aktualizacja została zakończona sukcesem,oraz czy na komputerze znaleziono wirusa, słabe zabezpieczenie itp. Ponadto, możesz podjąć dalsze działania lub zmienić działania podejmowane przez produkt Bitdefender.

Aby wejść do loga z powiadomieniami, kliknij ikonę po lewej stronie Interfejsu Bitdefender Za każdym razem kiedy dojdzie do krytycznego zdarzenia pojawi się ikona z odliczaniem .

Zależnie od typu i istotności, powiadomienia są pogrupowane w:

- **Zdarzenia krytyczne** powiadamiają o ważnych problemach. Powinieneś od razu je sprawdzić.
- **Ostrzeżenia** powiadamiają o mniej istotnych problemach. Należy zająć się tymi problemami, gdy tylko będzie taka sposobność.
- **Informacje** powiadamiają o operacjach zakończonych sukcesem.

Kliknij każdą z kolei zakładkę aby znaleźć detale dotyczące generowanych zdarzeń. Zwięzły opis jest wyświetlony po pojedynczym kliknięciu na tytuł zdarzenia: krótki opis działań jakie podjął Bitdefender, data oraz czas kiedy zaszło wydarzenie Jeśli wymagane będą dalsze działania, zostaną wyświetlone odpowiednie opcje.

Aby ułatwić zarządzanie zdarzeniami zapisanymi w dzienniku, w każdej sekcji powiadomień możesz usunąć lub oznaczyć każde zdarzenie jako wykonane.

4.4. Autopilot

Dla wszystkich użytkowników, którzy chcą, aby ich program zabezpieczający ochraniał komputer i nie przeszkadzał w wykonywaniu pracy, Bitdefender Internet Security 2018 został wyposażony w tryb Autopilota.

Kiedy włączona jest funkcja Autopilota, Bitdefender stosuje optymalną konfigurację ochrony i podejmuje wszystkie decyzje związane z ochroną za Ciebie. To oznacza, że nie będą pojawiać się wyskakujące okienka i powiadomienia, a także nie będziesz musiał konfigurować żadnych ustawień.

W trybie Autopilota Bitdefender automatycznie naprawia krytyczne błędy, dyskretnie zarządza i włącza:

- Ochrona antywirusowa zapewniona przez skanowanie w czasie rzeczywistym oraz skanowanie ciągłe.
- Ochrona zapewniana przez Zaporą sieciową.
- Ochrona sieciowa.
- Automatyczne aktualizacje.

Aby włączyć lub wyłączyć Autopilota kliknij przycisk **Autopilot** na górnym pasku narzędzi Interfejs Bitdefender.

Dopóki Autopilot jest włączony, ikona Bitdefender w zasobniku systemowym będzie zmieniona na .

WAŻNE
Jeśli Autopilot jest włączony, modyfikacja jakichkolwiek ustawień przez niego kontrolowanych spowoduje jego wyłączenie.

Aby zobaczyć historie akcji wykonanych przez Bitdefender kiedy Autopilot jest włączony, otwórz okno Zdarzenia .

4.5. Tryby

Niektóre aplikacje, takie jak gry online lub prezentacje wideo, wymagają zwiększonej reakcji systemu, wysokiej wydajności i braku przerw. Kiedy Twój laptop pracuje na zasilaniu z baterii, najlepiej jest przesunąć dodatkowe operacje, które zwiększają zużycie prądu, na później, kiedy znowu zostanie podłączony do zasilania A/C.

Tryby Bitdefender przypisują więcej zasobów systemowych do uruchomionych aplikacji poprzez czasową modyfikację ustawień ochrony i

dostosowanie konfiguracji systemu. W konsekwencji, wpływ na aktywność systemu jest ograniczony do minimum.

Aby dostosować się do różnych działań, Bitdefender dostarczany jest z następującymi trybami:

Tryb Pracy
: Optymalizuje wydajność pracy poprzez określenie i dostosowanie ustawień produktu i systemu.

Tryb Filmu
: Wzmacnia efekty wizualne i eliminuje przerwy podczas oglądania filmów.

Profil Gry
: Wzmacnia efekty wizualne i eliminuje przerwy podczas grania w gry.

Profil Publiczne Wi-Fi
: Stosuje ustawienia produktu, aby korzystać z pełnej ochrony przy jednoczesnym podłączeniu do niezabezpieczonej sieci bezprzewodowej.

Profil Tryb Pracy na Baterii
: Stosuje ustawienia produktu i obniża aktywność w tle w celu oszczędzania baterii.

4.5.1. Konfiguruj automatyczną aktywację profili

Dla wygodniejszego korzystania z Bitdefender możesz skonfigurować profile W tym przypadku Bitdefender automatycznie wykrywa aktywność użytkownika i wprowadza optymalne ustawienia dla systemu.

Aby pozwolić Bitdefender aktywować profile:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Użyj następującego przełącznika aby włączyć **Aktywuj profile automatycznie**.

Jeśli nie chcesz, by Profile były automatycznie aktywowane, wyłącz przełącznik.

Aby ręcznie aktywować profil, kliknij odpowiedni przełącznik ON/OFF. Tylko jeden profil może być ręcznie aktywowany na raz.

Aby uzyskać więcej informacji na temat profili, odwołaj się do„*Tryby*" (p. 177)

4.6. Ustawienia ochrony hasłem Bitdefender

Jeżeli nie jesteś jedynym użytkownikiem danego komputera z prawami administratora, zaleca się, żebyś chronił ustawienia Bitdefender hasłem.

Aby skonfigurować ochronę hasłem dla ustawień Bitdefender:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. W oknie **OGÓLNE**, włącz **Ochronę hasłem** przez kliknięcie odpowiedniego przycisku.
3. Wpisz hasło w oba pola i kliknij **OK**. Hasło musi posiadać minimum 8 znaków.

Po ustawieniu hasła każdy, kto spróbuje zmienić ustawienia produktu Bitdefender, będzie musiał najpierw podać hasło.

WAŻNE

Koniecznie zapamiętaj swoje hasło lub zapisz je w bezpiecznym miejscu. Jeśli zapomnisz hasła, będziesz musiał ponownie zainstalować program lub skontaktować się z Bitdefender, w celu uzyskania pomocy.

Aby usunąć ochronę hasłem:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. W oknie **OGÓLNE**, wyłącz ochronę hasłem przez kliknięcie odpowiedniego przycisku.
3. Wprowadź hasło i kliknij **OK**.

Notatka

Aby zmodyfikować hasło dla produktu, kliknij odnośnik "**Zmień hasło**". Wpisz swoje obecne hasło i kliknij *OK*. W nowym oknie, które się pojawi, wpisz hasło, które chcesz używać od teraz aby ograniczyć dostęp do ustawień Bitdefender.

4.7. Anonimowe raporty użycia

Domyślnie Bitdefender wysyła informacje o sposobie użytkowania do serwera Bitdefender. Informacje te są konieczne do ulepszenia produktu. Pomogą nam zapewnić Ci wygodniejszą jego obsługę w przyszłości. Raporty nie będą zawierały żadnych prywatnych danych, takich jak Twoja nazwa, adres IP itp., oraz nie będą wykorzystywane do celów komercyjnych.

W przypadku, gdy chcesz zaprzestać wysyłania Anonimowych raportów wykorzystania:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Zaawansowane**.
3. Kliknij odpowiedni przełącznik WŁĄCZ/WYŁĄCZ.

4.8. Powiadomienia o ofertach specjalnych

Kiedy oferty promocyjne będą dostępne, Bitdefender powiadomi Cię o nich za pomocą wyskakujących okienek. Daje Ci to dostęp do korzystnych cen i ochrony urządzenia przez długi okres czasu.

Aby wyłączyć specjalne oferty oraz powiadomienia o produkcie:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. W oknie **OGÓLNE** kliknij odpowiedni przycisk WŁĄCZ/WYŁĄCZ.

Powiadomienia o specjalnych ofertach są domyślnie włączone.

5. INTERFEJS PRODUKTU BITDEFENDER

Bitdefender Internet Security 2018 spełnia wymagania zarówno zaawansowanych użytkowników, jak i użytkowników początkujących. Graficzny interfejs użytkownika jest tak zaprojektowany, aby mogli z niego korzystać wszyscy użytkownicy.

Aby przejść przez interfejs Bitdefender, wprowadzenie zawierające szczegóły o tym jak pracować z produktem i jak konfigurować go, jest wyświetlony w na górze po lewej stronie. Wybierz **DALEJ** aby kontynuować samouczek, lub **Pomiń instruktaż** aby go zamknąć.

Aby zobaczyć stan produktu i wykonać niezbędne zadania, możesz zawsze kliknąć na ikonę produktu Bitdefender w zasobniku systemowym.

Główne okno pozwala zarządzać zachowaniem produktu korzystanie z Autopilota, pozwala na dostęp do ważnych informacji o produkcie i pozwala na wykonywanie regularnych zadań. Z lewego paska interfejsu, możesz wejść do konto Bitdefender oraz Sekcji Bitdefender do szczegółowej konfiguracji i zaawansowanych zadań administracyjnych.

Jeśli chcesz mieć oko na istotne informacje bezpieczeństwa i mieć szybki dostęp do najważniejszych ustawień, wyświetl Gadżet bezpieczeństwa na pulpicie.

5.1. Ikona zasobnika systemowego

Aby sprawniej zarządzać całym programem, możesz skorzystać z ikony Bitdefender B w zasobniku systemowym.

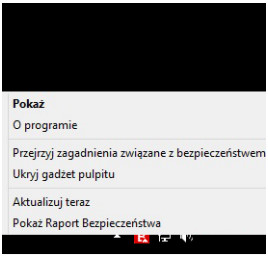
Notatka

Ikona Bitdefender może nie być widoczna przez cały czas. Aby ikona pojawiała się na stałe:

- W systemach **Windows 7, Windows 8 i Windows 8.1**:
  1. Kliknij strzałkę ▲ w prawym dolnym rogu ekranu.
  2. Kliknij **Dostosuj...**, aby otworzyć okno ikony obszaru powiadomień.
  3. Zaznacz opcję **Pokaż ikony i powiadomienia** dla ikony **Agenta Bitdefender**.
- W systemie **Windows 10**:
  1. Prawym przyciskiem myszy kliknij pasek zadań i wybierz **Właściwości**.
  2. Kliknij **Dostosuj** w oknie Paska Zadań.

3. Kliknij link **Wybierz które ikony są wyświetlane na pasku zadań** okno **Powiadomienia & akcji**.
4. Włącz przełącznik obok **Agenta Bitdefender**.

Jeżeli klikniesz dwukrotnie na tę ikonę, otwarte zostanie okno Bitdefender. Ponadto kliknięcie prawym przyciskiem myszy w menu kontekstowym pozwala na szybkie konfigurowanie produktu Bitdefender.



Ikona paska

- "**Pokaż**" - otwiera główne okno Bitdefender.
- "**O programie**" - otwiera okno, w którym możesz przeczytać informacje o produkcie Bitdefender, oraz gdzie szukać pomocy, jeśli zdarzy się coś niespodziewanego.
- "**Wyświetl zagadnienia bezpieczeństwa**" - pomaga rozwiązać bieżące problemy z bezpieczeństwem. Jeśli ta opcja jest niedostępna, nie ma żadnych problemów, które należałoby naprawić. Aby uzyskać więcej informacji, odwołaj się do *„Rozwiązywanie problemów"* (p. 15).
- "**Pokaż / Ukryj Gadżet pulpitu** " - włącza / wyłącza Gadżet bezpieczeństwa.
- "**Aktualizuj teraz**" - uruchamia aktualizację. Możesz śledzić stan aktualizacji w panelu Aktualizacji, w głównym oknie Bitdefender.
- "**Pokaż Raport bezpieczeństwa**" - otwiera okno, w którym można zapoznać się z tygodniowym podsumowaniem stanu bezpieczeństwa i z rekomendacjami dla systemu użytkownika. Możesz zastosować się do zaleceń, aby poprawić bezpieczeństwo systemu.

Ikona Bitdefender w zasobniku systemowym informuje użytkownika, kiedy pojawiają się nowe zagadnienia dotyczące bezpieczeństwa, oraz jak działa program, wyświetlając odpowiedni symbol:

Krytyczne zagadnienia wpływające na bezpieczeństwo systemu. Wymagają błyskawicznego sprawdzenia oraz jak bezzwłocznej naprawy.
Niekrytyczne problemy dotyczące pośrednio bezpieczeństwa systemu. Należy zająć się tymi problemami, gdy tylko będzie taka sposobność.
Autopilot Bitdefender jest włączony.

Jeśli Bitdefender działa, ikona w zasobniku systemowym pojawia się na szarym tle: . Zazwyczaj dzieje się tak, kiedy subskrypcja wygasa. Może to

także wystąpić, gdy usługi Bitdefender nie odpowiadają lub inne błędy zakłócają normalną pracę Bitdefender.

5.2. Główne okno

Główne okno Bitdefender pozwala uruchamiać najczęściej wykonywane zadania, szybko usuwać problemy z bezpieczeństwem, przeglądać informacje o zdarzeniach związanych z działaniem produktu oraz pozwala uzyskać dostęp do paneli, z których możesz skonfigurować ustawienia produktu. Wystarczy kilka kliknięć.

Okno dzieli się na cztery główne strefy:

Obszar stanu
: Tutaj możesz sprawdzić status ochrony Twojego komputera, uruchomić aktualizacje i skonfigurować Autopilota .

Lewa strona
: To menu pozwala na dostęp i zarządzanie Twoim kontem Bitdefender razem z innymi funkcjami online produktu, lub zmianę między trzema głównymi sekcjami produktu. Stąd, możesz też mieć dostęp do Powiadomień, tygodniowe Raport bezpieczeństwa, Główne opcje i obszary Pomoc & Wsparcie.

Przyciski akcji i dostęp do obszaru funkcji
: To jest miejsce, gdzie możesz uruchamiać różne zadania, aby chronić swój system. Możesz również wejść do funkcji Bitdefender, aby skonfigurować produkt samodzielnie.

Dolna belka
: W tym miejscu można łatwo zainstalować Bitdefender na innych urządzeniach, pod warunkiem że Twoja subskrypcja ma wystarczająco dużo wolnych slotów.

5.2.1. Obszar stanu

Obszar status zawiera następujące elementy:

- **Status ochrony** po lewej stronie interfejsu informuje czy są jakieś problemy z ochroną Twojego komputera, oraz pomaga Ci jest naprawić.

  Kolor stanu strefy ochronnej oraz wyświetlane powiadomienia zmieniają się w zależności od rodzaju wykrytego problemu:

- **Ta sekcja ma kolor zielony.** Brak problemów do naprawy. Twój komputer i dane są chronione.
- **Ta sekcja ma kolor żółty.** Niekrytyczne problemy dotyczące pośrednio bezpieczeństwa systemu. Należy zająć się tymi problemami, gdy tylko będzie taka sposobność.
- **Ta sekcja ma kolor czerwony.** Problemy krytyczne bezpośrednio wpływają na bezpieczeństwo systemu. Powinieneś natychmiast zająć się tymi problemami.

Po kliknięciu gdziekolwiek na obszarze stanu ochrony, możesz skorzystać z pomocy asystenta, który umożliwi Ci łatwe usunięcie wszelkich zagrożeń z komputera. Aby uzyskać więcej informacji, odwołaj się do *„Rozwiązywanie problemów"* (p. 15).

- **AUTOPILOT** pozwala na ustawienie optymalnej ochrony i rozkoszować się całkowicie niewidoczną ochroną. Aby uzyskać więcej informacji, odwołaj się do *„Autopilot"* (p. 18).
- **AKTUALIZUJ TERAZ** pozwala aktualizować program, kiedy tylko chcesz aby mieć pewność, że masz najnowsze sygnatury wirusów. Aby uzyskać więcej informacji, odwołaj się do *„Dbanie o aktualizacje Bitdefender"* (p. 43).
- **Aktywny Profil** wyświetla profil aktualnie włączony w Twoim produkcie Bitdefender. Aby uzyskać więcej informacji, odwołaj się do *„Tryby"* (p. 177).

5.2.2. Lewa strona

Obrazowe ikony są dostępne na lewym pasku, dając Ci dostęp do konta Bitdefender, sekcji produktów, raportu aktywności, powiadomień, głównych ustawień i wsparcia.

Nazwy ikon są widoczne po kliknięciu na ikonę ≡, po kolei:

- **Ochrona**. Przyciski akcji **Skan szybki** i **Skanowanie luk** są widoczne w lewym-dolnym rogu interfejsu Bitdefender Jeszcze, informacje o zablokowanych aplikacjach, wykrytych zagrożeniach i atakach stają się widoczne. Kliknij link **WYŚWIETL FUNKCJE** aby wejść do obszaru ich konfiguracji.
- **Prywatność**. Przyciski akcji **Bezpieczne płatności** i **Asystent Rodzica** stają się widoczne w lewym-dolnym rogu interfejsu Bitdefender Jeszcze, informacje o wykrytych portfelach i sejfach plików są wyświetlone. Kliknij link **WYŚWIETL FUNKCJE** aby wejść do obszaru ich konfiguracji.

- **Aktywność**. Stąd, możesz zobaczyć aktywność produktów w ciągu ostatnich 30 dni i uzyskać dostęp do raportu bezpieczeństwa, który jest generowany co siedem dni.
- **Powiadomienia**. Z tego miejsca, masz dostęp do generowanych powiadomień.
- **Konto**. Dostępne są szczegółowe informacje na temat konta Bitdefender oraz używania subskrypcji. Uzyskaj dostęp do swojego konta Bitdefender, aby zweryfikowć swoje subskrypcje i przeprowadzić zadania związane z bezpieczeństwem zarządzanych urządzeń.
- **Ustawienia**. Stąd masz dostęp do ustawień ogólnych.
- **Wsparcie**. Z tego miejsca, kiedy potrzebujesz pomocy w rozwiązaniu sytuacji z Twoim Bitdefender Internet Security 2018, możesz skontaktować się z Wsparciem Technicznym Bitdefender

5.2.3. Przyciski akcji i dostęp do obszaru funkcji

Korzystając z przycisków akcji, możesz szybko uruchomić ważne zadania. Przyciski akcji są widoczne w lewej dolnej części interfejsu Bitdefender, po zaznaczeniu wybranej sekcji spośród dwóch:**Ochrona** i **Prywatność** z paska po lewej.

Zależnie od wybranej sekcji, będą widoczne dane przyciski akcji:

- **Szybkie skanowanie**. Uruchom skanowanie szybkie aby upewnić się, że Twój komputer nie jest zainfekowany złośliwym oprogramowaniem.
- **Skanowanie luk**. Skanowanie komputera w poszukiwaniu luk, aby upewnić się, że wszystkie zainstalowane aplikacje, wraz z Systemem Operacyjnym, są aktualizowane i prawidłowo funkcjonują.
- **Bezpieczne płatności**. Otwórz Bitdefender Safepay™, aby chronić poufne dane podczas przeprowadzania transakcji online.
- **Asystent Rodzica**. Wejdź w Asystenta Rodzica Bitdefender aby być informowanym na temat aktywności "dziecka"

5.2.4. Dolna belka

Aby rozpocząć ochronę dodatkowych urządzeń:

1. Kliknij link **ZAINSTALUJ NA INNYM URZĄDZENIU**.

Jesteś przekierowany do strony konta Bitdefender. Upewnij się, że jesteś zalogowany przy użyciu swoich poświadczeń.

2. W wyświetlonym oknie wybierz żądany system operacyjny, a następnie kliknij **KONTYNUUJ**.
3. Wpisz adres e-mail, na który należy wysłać link do pobrania instalatora aplikacji na wybraną platformę.

W zależności od Twojego wyboru, produkt Bitdefender zostanie zainstalowany:

- Bitdefender Internet Security 2018 na urządzeniach opartych na systemie Windows.
- Bitdefender Antivirus dla Mac dla urządzeń opartych na macOS.
- Bitdefender Mobile Security & Antywirus na urządzeniach opartych na Androidzie.
- Bitdefender Mobile Security na urządzeniach opartych na iOS-ie.
- Bitdefender Doradca Rodzica na macOS, iOS i urządzeniach z systemem Android.

5.3. Sekcje Bitdefender

Produkt Bitdefender jest wyposażony w przydatne moduły, podzielone na trzy sekcje, które pomogą Ci pozostać chronionym podczas pracy, surfowania po Internecie, grania w gry, lub gdy chcesz dokonać płatności online.

Kiedy chcesz wejść w specyficzne sekcje funkcjonalności, lub skonfigurować swój produkt, możesz to zrobić klikając ikony na lewym pasku interfejsu Bitdefender:

- Ochrona
- Prywatność

5.3.1. **Ochrona**

W zakładce Ochrona możesz konfigurować swój poziom ochrony, zarządzać przyjaciółmi i spamerami, zobaczyć i edytować ustawienia połączeń sieciowych, ustawić Bezpieczne Pliki i Ochronę Sieci, sprawdzić i naprawić potencjalne luki w systemie oraz wejść w ustawienia ochrony sieci bezprzewodowej, do której jesteś podłączony.

Funkcjonalności, którymi możesz zarządzać w sekcji Ochrona są:

ANTYWIRUS

Ochrona antywirusowa stanowi podstawę Twojego bezpieczeństwa. Bitdefender chroni Cię w czasie rzeczywistym i na żądanie przed wszelkimi rodzajami szkodliwego oprogramowania, czyli wirusami, trojanami, adware, programami szpiegowskimi itd.

Z funkcjonalności Antywirus możesz w łatwy sposób uzyskać dostęp do następujących zadań skanowania:

- Szybkie skanowanie
- Skanowanie systemu
- Zarządzanie skanowaniem
- Tryb Ratunkowy (Środowisko Ratunkowe w Windows 10)

Więcej informacji o zadaniach skanowania antywirusowego oraz sposobach konfiguracji ochrony antywirusowej znajdziesz w *„Ochrona antywirusowa"* (p. 87).

OCHRONA SIECIOWA

Internetowa ochrona pomoże Ci bronić się przed atakami phishingu, próbami oszustw i wyciekiem prywatnych danych podczas przeglądania internetu.

Więcej informacji o tym, jak skonfigurować Bitdefender, żeby lepiej chronił Twoją aktywność w sieci, znajduje się tutaj *„Ochrona sieciowa"* (p. 113).

ZAPORA SIECIOWA

Zapora sieciowa zapewnia ochronę, kiedy jesteś podłączony do internetu lub sieci lokalnej, filtrując wszelkie próby połączenia.

Więcej informacji o konfiguracji zapory sieciowej znajduje się tutaj: *„Zapora Sieciowa"* (p. 126).

AKTYWNA KONTROLA ZAGROŻEŃ

Aktywna Kontrola Zagrożeń chroni system przed malware takim jak ransomware, spyware i trojanami analizując zachowanie wszystkich zainstalowanych aplikacji. Podejrzane procesy są identyfikowane i, jeśli jest to konieczne, blokowane.

Aby uzyskać więcej informacji o tym, jak uchronić swój system przed złośliwym oprogramowaniem, przejdź do *„Aktywna Kontrola Zagrożeń"* (p. 110).

ANTYSPAM

Moduł antyspamowy Bitdefender chroni Twoją skrzynkę odbiorczą przed spamem, filtrując ruch pocztowy POP3.

Aby uzyskać więcej informacji na temat ochrony antyspamowej, proszę odnieść się do *„Antyspam”* (p. 116).

LUKA

Moduł Skanowania luk, pomaga utrzymać Twój system oraz aplikacje, z których regularnie korzystasz zaktualizowane, a także identyfikuje połączone niezabezpieczone sieci bezprzewodowe.

Kliknij **Skanowanie luk** w module wykrywania luk, aby rozpocząć identyfikację krytycznych aktualizacji systemu Windows, aktualizacji aplikacji, słabych haseł należących do kont Windows i sieci bezprzewodowych, które nie są bezpieczne.

Kliknij **Doradca Wi-fi** aby zobaczyć listę wykrytych sieci bezprzewodowych razem z ich reputacją i możliwymi do podjęcia krokami w celu ich zabezpieczenia.

Więcej informacji o konfiguracji ochrony przed lukami znajdziesz w sekcji *„Luki”* (p. 132).

Bezpieczne Pliki

Funkcja Bezpieczne Pliki gwarantuje, że Twoje pliki osobiste będą chronione przed atakami ransomware.

Aby uzyskać więcej informacji dotyczących sposobu konfigurowania Bezpiecznych Plików, aby chronić Twoje prywatne pliki przed atakami ransomware, zapoznaj się z *„Bezpieczne pliki”* (p. 143).

5.3.2. Prywatność

W zakładce Prywatność możesz szyfrować swoje prywatne dane, chronić transakcje online, dostęp do swojej kamery,informacje o przeglądanych stronach, a także chronić swoje dzieci przeglądając i ograniczając ich aktywność online.

Funkcje, którymi możesz zarządzać w sekcji Prywatność to:

OCHRONA KAMERY INTERNETOWEJ

Ochrona Kamery Internetowej Bitdefender uniemożliwia włamanie się do kamery przez zablokowanie dostępu do niezaufanych aplikacji.

Aby uzyskać więcej informacji o tym, zapobiec niepowołanemu dostępowi do kamery internetowej, przejdź do *„Ochrona kamery internetowej"* (p. 140).

PORTFEL

Manager Haseł Bitdefender pomaga Ci mieć pod kontrolą Twoje hasła, chroni Twoją prywatność i zapewnia bezpieczeństwo przy korzystaniu z Internetu.

Więcej informacji o konfiguracji Managera Haseł znajduje się tutaj: *„Ochrona Manager Haseł dla Twoich poświadczeń"* (p. 146).

SAFEPAY

Bezpieczna przeglądarka (moduł Bitdefender Safepay) zapewnia prywatność i bezpieczeństwo bankowości internetowej, dostępu do e-sklepów, oraz innych rodzajów transakcji online.

Kliknij przycisk akcji**Safepay** z intefejsu Bitdefender, aby dokonywać transakcji online w bezpiecznym środowisku.

Więcej informacji na temat modułu Bitdefender Safepay zawiera sekcja *„Bezpieczne płatności online"* (p. 154).

Asystent Rodzica

Asystent Rodzica Bitdefender pozwala Ci na monitorowanie tego, co Twoje dziecko robi na komputerze. W przypadku nieodpowiednich treści można zdecydować, aby ograniczyć jego dostęp do internetu lub do konkretnych aplikacji.

Kliknij przycisk **Konfiguruj** w module Asystent Rodzica, aby rozpocząć konfigurację urządzeń Twojego dziecka i monitoruj jego aktywność gdziekolwiek jesteś.

Więcej informacji o konfiguracji Asystenta Rodzica znajduje się tutaj *„Asystent Rodzica"* (p. 162).

OCHRONA DANYCH

Funkcja Ochrony Danych pozwala Ci usunąć pliki na stałe.
Kliknij **Niszczarka Plików** w module Ochrona Danych, aby uruchomić kreator, który trwale usunie pliki z systemu.

Więcej informacji o konfiguracji ochrony danych znajdziesz tutaj: *„Ochrona danych"* (p. 160)

5.4. Gadżet bezpieczeństwa

Gadżet bezpieczeństwa jest szybkim i łatwym sposobem monitorowania i kontroli produktu Bitdefender Internet Security 2018. Dodanie tego małego i nieprzeszkadzającego gadżetu do Twojego pulpitu pozwala Ci zawsze widzieć krytyczne informacje i wykonać kluczowe zadania:

- otworzyć główne okno Bitdefender.
- monitorować aktywność skanowania w czasie rzeczywistym.
- monitorować stan bezpieczeństwa systemu i naprawiać istniejące problemy.
- widzieć, gdy aktualizacja jest w toku.
- oglądać powiadomienia i uzyskiwać dostęp do najnowszych zdarzeń zgłoszonych przez Bitdefender.
- skanować pliki i foldery po przeciągnięciu i upuszczeniu jednego lub wielu elementów na obszar gadżetu.

Gadżet bezpieczeństwa

Ogólny stan ochrony Twojego komputera jest wyświetlany **w centralnej części** gadżetu. Stan jest sygnalizowany przez kolor i kształt ikon wyświetlanych w tym obszarze.


Problemy krytyczne bezpośrednio wpływają na bezpieczeństwo systemu. Wymagają natychmiastowej uwagi i muszą być naprawione tak szybko, jak jest to możliwe. Kliknij ikonę stanu, aby rozpocząć naprawianie zgłoszonych problemów.


Niekrytyczne problemy dotyczące pośrednio bezpieczeństwa systemu. Należy zająć się tymi problemami, gdy tylko będzie taka sposobność. Kliknij ikonę stanu, aby rozpocząć naprawianie zgłoszonych problemów.


Twój system jest chroniony.

Gdy zadanie skanowania na żądanie jest w toku, wyświetlana jest animowana ikona.

Gdy zgłaszane są problemy, kliknij na ikonę stanu, aby uruchomić kreator naprawy problemów.

Na dole gadżetu wyświetlana jest lista nieprzeczytanych komunikatów (ilość pozostających do przeczytania komunikatów raportowanych przez Bitdefender, jeśli takie są). Kliknij licznik zdarzeń, na przykład 1 dla jednego nieprzeczytanego powiadomienia, aby otworzyć okno Powiadomień. Aby uzyskać więcej informacji, odwołaj się do *„Powiadomienia"* (p. 17).

5.4.1. Skanowanie plików i folderów

Możesz użyć Gadżetu bezpieczeństwa, żeby szybko przeskanować pliki lub foldery. Przeciągnij plik lub folder, który chcesz przeskanować i upuść go na obszarze **Gadżetu bezpieczeństwa**.

Wyświetlony zostanie Kreator skanowania antywirusowego, który przeprowadzi Cię przez proces skanowania. Opcje skanowania są wcześniej skonfigurowane tak, aby zapewnić najlepszą wykrywalność i nie mogą być zmienione. Jeśli wszystkie zainfekowane pliki zostaną wykryte, Bitdefender spróbuje je wyleczyć (usunąć z nich szkodliwy kod). Jeśli to zawiedzie, kreator skanowania antywirusowego pozwoli na wybranie innych akcji, które zostaną wykonane na zainfekowanych plikach.

5.4.2. Ukryj / Pokaż Gadżet pulpitu

Kiedy nie chcesz, aby gadżet pozostawał widoczny, kliknij ⊗.

Aby przywrócić Gadżet bezpieczeństwa, użyj jednej z poniższych metod:

- Z zasobnika systemowego:
  1. Kliknij prawym przyciskiem myszy na ikonie Bitdefender w zasobniku systemowym.
  2. Kliknij **Pokaż Gadżet pulpitu** w menu kontekstowym, które się pojawi.
- Z interfejsu Bitdefender:
  1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
  2. Wybierz zakładkę **Ogólne**.

3. Włącz opcję **Wyświetl Gadżet pulpitu** klikając na odpowiednim przełączniku.

Widżet Ochrony Bitdefender jest domyślnie wyłączony.

5.5. Aktywność

Okno Aktywność wyświetla informacje na temat podjętych przez Bitdefender akcji na Twoim urządzeniu w ciągu ostatnich 30 dni. Tutaj możesz sprawdzić, jakie aplikacje, zagrożenia i ataki zostały zablokowane w tym okresie i czy podjęto jakieś próby ransomware.

Raport Bezpieczeństwa, który zapewnia cotygodniowy status dla Twojego produktu i różne wskazówki, które poprawią ochronę systemu, można go również uzyskać klikając odpowiednie łącze. Te wskazówki są ważne z punktu widzenia zarządzania całkowitym bezpieczeństwem systemu i łatwego dostępu do możliwych do wykonania działań.

Raport jest generowany raz w tygodniu i podsumowuje informacje związane ze stanem działania produktu, dając użytkownikowi przegląd zdarzeń, które ostatnio miały miejsce w systemie.

Informacje dostarczane przez Raport bezpieczeństwa zostały podzielone na dwie kategorie:

- Obszar **Ochrona** - wyświetla informacje związane z ochroną systemu.
  - **Przeskanowane pliki**

    Pozwala na wyświetlenie informacji o plikach skanowanych przez Bitdefender w ciągu tygodnia. Można zobaczyć szczegóły, takie jak liczba przeskanowanych plików i liczba plików wyleczonych przez Bitdefender.

    Aby uzyskać więcej informacji na temat ochrony antywirusowej, proszę odnieść się do *„Ochrona antywirusowa”* (p. 87).
  - **Przeskanowane strony internetowe**

    Pozwala sprawdzić liczbę stron WWW przeskanowanych i zablokowanych przez Bitdefender. Aby zabezpieczyć Cię przed wyciekiem poufnych informacji podczas przeglądania stron WWW, Bitdefender chroni ruch sieciowy.

    Aby uzyskać więcej informacji na temat ochrony stron, sięgnij do *„Ochrona sieciowa”* (p. 113).

- **Luki**

  Umożliwia łatwe identyfikowanie i naprawianie luk systemowych, w celu zapewnienia lepszej ochrony przed szkodliwym oprogramowaniem i hakerami.

  Aby uzyskać więcej informacji na temat skanowania w poszukiwaniu luk, prosimy odnieść się do *„Luki”* (p. 132).

- **Oś czasu zdarzeń**

  Pozwala na uzyskanie ogólnego obrazu wszystkich procesów i zagadnień skanowania naprawionych przez Bitdefender w ciągu tygodnia. Zdarzenia są podzielone na dni.

  Aby uzyskać więcej informacji na temat szczegółowych logów zdarzeń dotyczących aktywności na komputerze, zobacz *„Powiadomienia”* (p. 17).

- Obszar **Optymalizacja** - pokazuje informacje związane z wyczyszczonym miejscem, zoptymalizowanymi aplikacjami i ilością baterii, która została zaoszczędzona przy użyciu Profilu Tryb Pracy na baterii.

  - **Oszczędność baterii**

    Pozwala zobaczyć, ile baterii udało się zaoszczędzić, gdy system jest uruchomiony w profilu Tryb Pracy na baterii.

    Aby dowiedzieć się więcej na temat profilu Tryb Pracy na baterii, sięgnij do *„Profil Tryb Pracy na Baterii”* (p. 182).

  - **Aplikacje zoptymalizowane**

    Pozwala zobaczyć, ile aplikacji jest używanych w poszczególnych Profilach.

    Aby uzyskać więcej informacji na temat Profili, odwołaj się do *„Tryby”* (p. 177).

5.5.1. Sprawdzanie Raportu bezpieczeństwa

Raport bezpieczeństwa używa systemu śledzenia problemów, aby wykryć i poinformować Cię o zdarzeniach mogących mieć negatywny wpływ na bezpieczeństwo komputera i Twoich danych. Wykryte problemy mogą dotyczyć ważnych ustawień ochrony, które są wyłączone oraz innych czynników, które mogą stwarzać zagrożenia bezpieczeństwa. Używając raportu można skonfigurować poszczególne składniki Bitdefender lub podjąć

działania prewencyjne mające na celu poprawę bezpieczeństwa komputera i danych użytkownika.

Aby sprawdzić Raport Bezpieczeństwa:

1. Dostęp do raportu:

   - Kliknij ikonę po lewej stronie interfejsu Bitdefender.

     Kliknij link zlokalizowany **Raport Bezpieczeństwa** w prawym dolnym rogu okna Raport Aktywności.
   - Kliknij prawym przyciskiem myszy na ikonie Bitdefender w zasobniku systemowym i wybierz opcję **Pokaż Raport bezpieczeństwa**.
   - Kiedy raport zostanie utworzony, wyświetlone zostanie wyskakujące powiadomienie. Kliknij **Pokaż**, aby uzyskać dostęp do raportu aktywności.

     Twoja przeglądarka wyświetli stronę, na której zamieszczony będzie wygenerowany raport.
2. W górnej części okna znajduje się informacja o stanie bezpieczeństwa.
3. Sprawdź nasze rekomendacje wyświetlone na środku strony.

Kolor stanu strefy ochronnej oraz wyświetlane powiadomienia zmieniają się w zależności od rodzaju wykrytego problemu:

- **Obszar jest koloru żółtego.** Nie ma problemów do naprawienia. Twój komputer i dane są chronione.
- **Obszar jest koloru pomarańczowego.** W Twoim systemie występują problemy, nie są one jednak krytyczne. Należy zająć się tymi problemami, gdy tylko będzie taka sposobność.
- **Obszar jest koloru czerwonego.** W Twoim systemie występują krytyczne problemy. Powinieneś natychmiast zająć się tymi problemami.

5.5.2. Włączanie lub wyłączanie powiadomień o Raporcie bezpieczeństwa.

Aby włączyć lub wyłączyć powiadomienie Raportu Bezpieczeństwa:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. W oknie **OGÓLNE** kliknij odpowiedni przycisk WŁĄCZ/WYŁĄCZ.

Powiadamianie o Raporcie bezpieczeństwa jest domyślnie włączone.

6. BITDEFENDER CENTRAL

Bitdefender Central jest platformą webową, gdzie masz dostęp do online'owych funkcji produktu i usług i możesz zdalnie przeprowadzić ważne zadania na urządzeniach, na których jest zainstalowany Bitdefender. Możesz się zalogować do swojego konta Bitdefender z jakiegokolwiek komputera lub urządzenia mobilnego połączonego z Internetem przechodząc do https://central.bitdefender.com. Gdy jesteś zalogowany, możesz rozpocząć w następujący sposób:

- Pobierz i zainstaluj Bitdefender na systemach operacyjnych Windows, macOS, iOS i Android. Produkty dostępne do pobrania są:
  - Bitdefender Internet Security 2018
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security & Antywirus na systemy Android
  - Bitdefender Mobile Security na systemy iOS
  - Bitdefender Asystent Rodzica
- Zarządzaj i odnów swoją subskrypcję Bitdefender.
- Dodaj nowe urządzenia do sieci i zarządzaj nimi, gdziekolwiek jesteś.
- Konfiguruj ustawienia Asystenta Rodzica dla urządzeń swoich dzieci i monitoruj ich aktywność gdziekolwiek są.

6.1. Uzyskiwanie dostępu do Bitdefender Central

Jest wiele sposobów na uzyskanie dostępu do Bitdefender Central. W zależności od zadania, które chcesz wykonać, możesz użyć jednej z następujących możliwości:

- Z głównego interfejsu Bitdefender:
  1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  2. Wybierz link **Przejdź do Bitdefender Central**.
  3. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
- Z Twojej przeglądarki internetowej:

1. Otwórz przeglądarkę internetową na jakimkolwiek urządzeniu z dostępem do Internetu.
2. Idź do: https://central.bitdefender.com.
3. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.

6.2. Moje Subskrypcje

Platforma Bitdefender Central daje Tobie możliwość łatwego zarządzania subskrypcjmi, które posiadasz dla wszystkich swoich urządzeń.

6.2.1. Sprawdź dostępne subskrypcje

Aby sprawdzić swoje dostępne subskrypcje:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Subskrypcje**.

Tutaj masz informacje na temat dostepności subskrypcji, którą posiadasz i liczby urządzeń korzystających z niej.

Możesz dodać nowe urządzenie do subskrypcji lub odnowić ją wybierając kartę subskrypcji.

Notatka
Możesz mieć jedną lub więcej subskrypcji na swoim koncie pod warunkiem, że są one dla różnych platform (Windows, macOS, iOS lub Android).

6.2.2. Dodaj nowe urządzenie

Jeśli Twoja subskrypcja obejmuje więcej niż jedno urządzenie, możesz dodać nowe urządzenie i na nim zainstalować swój Bitdefender Internet Security 2018 jak poniżej:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. W oknie **MOJE URZĄDZENIA**, kliknij **ZAINSTALUJ Bitdefender**.
4. Wybierz jedną z dwóch dostępnych opcji:
   - **POBIERANIE**

     Kliknij przycisk i zapisz plik instalacyjny.

- **Na innym urządzeniu**

  Zaznacz **Windows**, aby pobrać swój produkt Bitdefender, a następnie kliknij **KONTYNUUJ**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ**.

5. Poczekaj na zakończenie pobierania, a następnie uruchomm instalator.

6.2.3. Odnów Subskrypcję

Jeśli nie zdecydowałeś się na automatyczne odnowienie subskrypcji Bitdefender, możesz go ręcznie odnowić, wykonując następujące kroki:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Subskrypcje**.
3. Wybierz pożądaną subskrypcję karty.
4. Kliknij **ODNÓW**, aby kontynuować.

Strona otwiera się w Twojej przegladarce internetowej, gdzie możesz odnowić swoją subskrypcję Bitdefender.

6.2.4. Aktywuj subskrypcje

Subskrypcja może być aktywowana podczas procesu instalacji przy użyciu Twojego konta Bitdefender. Wraz z procesem aktywacji, jego ważność rozpoczyna odliczanie w dół.

Jeśli zakupiłeś kod aktywacyjny od jednego z naszych sprzedawców lub otrzymałeś go w prezencie, możesz dodać jego dostępność do jakiejkolwiek istniejacej subskrypcji Bitdefender dostępnej na koncie, pod warunkiem, że są one dla tego samego produktu.

Aby aktywować subskrypcję przy użyciu kodu aktywacyjnego:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Subskrypcje**.
3. Kliknij przycisk **KOD AKTYWACYJNY**, a następnie wpisz kod w odpowiednie pole.
4. Kliknij **KOD AKTYWACYJNY** aby kontynuować.

Subskrypcja jest teraz aktywna. Idź do panelu **Moje Urządzenia** i wybierz **ZAINSTALUJ Bitdefender**, aby zainstalować produkt na jednym ze swoich urządzeń.

6.3. Moje urządzenia

Obszar **Moje urządzenie** w Bitdefender Central pozwala na instalację, zarządzanie oraz wykonywanie zdalnych zadań na Twoim Bitdefender na jakimkolwiek urządzeniu, ważne aby było włączone i połączone z Internetem. Karty urządzeń wyświetlają nazwę urządzenia, stan ochrony i pozostałą dostępność w Twojej subskrypcji.

Aby łatwo zidentyfikować swoje urządzenie, możesz dostosować nazwę urządzenia:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. Kliknij ikonę ⋮ na pożądanej karcie urządzenia, a następnie wybierz **Ustawienia**.
4. Zmień nazwę urządzenia w odpowiednim polu, a następnie wybierz **Zapisz**.

W przypadku, gdy Autopilot jest wyłączony, możesz go włączyć klikając przycisk. Naciśnij **Zapisz** aby zastosować ustawienia.

Możesz tworzyć i przypisywac właściciela swoich urządzeń dla lepszego zarządzania:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. Kliknij ikonę ⋮ na pożądanej karcie urządzenia, a następnie wybierz **Profil**.
4. Kliknij **Dodaj właściciela**, a następnie wypełnij odpowiednie pola, ustaw datę urodzenia, a nawet dodaj zdjęcie profilowe.
5. Kliknij **DODAJ**, aby zapisać profil.
6. Wybierz pożądanego właściciela z listy **Własciciel urządzenia**, a następnie kliknij **PRZYPISZ**.

Aby zdalnie zaktualizować Bitdefender na urządzeniu:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.

3. Kliknij ikonę ⋮ na pożądanej karcie urządzenia, a następnie wybierz **Aktualizuj**.

Dla większej ilości zdalnych działań i informacji dotyczących Twojego produktu Bitdefender na konkretnym urządzeniu, kliknij żądaną kartę urządzenia.

Po kliknięciu na kartę urządzenia, dostępne są następujące zakładki:

- **Panel nawigacyjny**. W tym oknie możesz sprawdzić stan ochrony produktów Bitdefender oraz liczbę pozostałych dni subskrypcji. Stan ochrony może być zielony, gdy nie ma żadnego problemu wpływającego na Twój produkt, lub czerwony, gdy urządzenie jest w niebezpieczeństwie. Gdy występują problemy wpływające na Twój produkt, kliknij **Zobacz problemy**, aby poznać szczegóły. Stąd można ręcznie naprawić problemy, które wpływają na bezpieczeństwo Twoich urządzeń.
- **Ochrona**. Z tego okna możesz zdalnie uruchomić Szybkie Skanowanie lub Skanowanie Systemu na Twoim urządzeniu. Kliknij przycisk **SKANUJ**, aby rozpocząć proces. Możesz również sprawdzić, kiedy zostało przeprowadzone ostatnio skanowanie na urządzeniu, dostępny jest też raport z ostatniego skanowania z najważniejszymi informacjami.Aby uzyskać więcej informacji na temat tych dwóch procesów skanowania, przejdź do *„Uruchamianie Skanowania systemu"* (p. 95) oraz do *„Uruchamianie szybkiego skanowania"* (p. 94).
- **Luka**. Aby sprawdzić urządzenie w poszukiwaniu jakichkolwiek luk takich jak brakujących aktualizacji systemu Windows, przestarzałych aplikacji lub słabych haseł kliknij przycisk **SKANUJ** w zakładce Luki. Luki nie mogą być zdalnie naprawione. W przypadku wykrycia jakichkolwiek luk, trzeba uruchomić nowe skanowanie na urządzeniu, a następnie podjąć zalecane działania. Kliknij **Więcej szczegółów**, aby uzyskać dostęp do szczegółowego raportu na temat znalezionych problemów. Aby uzyskać więcej szczegółów na temat tej funkcji, należy zapoznać się z *„Luki"* (p. 132).

6.4. Moje Konto

W obszarze **Moje Konto** masz możliwość aby spersonalizować swój profil, zmienić hasło przypisane do konta, zarządzać sesją logowania oraz wiadomościami pomocy w Bitdefender Central.

Kiedy klikniesz ikonę 👤 u góry po prawej stronie ekranu, a następnie wybierzesz **Moje Konto**, ukażą się następujące zakładki:

- **Profil** - tu możesz dodać i edytować informacje o koncie.
- **Zmień hasło** - z tego miejsca możesz zmienić hasło powiązane z kontem.
- **Zarządzanie sesją** - tu możesz zobaczyć i zarządzać ostatnie aktywne i nieaktywne sesje logowania uruchomione na urządzeniach powiązanych z kontem.
- **Ustawienia** - tu możesz włączyć lub wyłączyć wiadomości pomocy Bitdefender Central oraz zdecydować czy chcesz otrzymać powiadomienia i zdjęcia zrobione na twoim urządzeniu.

6.5. Powiadomienia

Aby pomóc ci zostać na bieżąco z tym co się dzieje na urządzeniach powiązanych z twoim kontem, następujące ikony 🔔 się przydadzą. Po kliknięciu masz ogólny obraz informacji o aktywności produktów Bitdefendera zainstalowanych na twoich urządzeniach.

7. DBANIE O AKTUALIZACJE BITDEFENDER

Nowe złośliwe oprogramowanie jest znajdowane i identyfikowane każdego dnia. Dlatego bardzo ważnym jest, aby na bieżąco aktualizować Bitdefender najnowszymi sygnaturami.

Jeśli jesteś podłączony do internetu za pomocą łącza szerokopasmowego lub DSL, Bitdefender zadba o to sam. Domyślnie aktualizacje sprawdzane są w trakcie włączania komputera i potem **co godzinę**. Jeśli aktualizacja będzie dostępna, zostanie ona automatycznie pobrana i zainstalowana na Twoim komputerze.

Proces aktualizacji wykonywany jest na bieżąco, co oznacza że pliki będą aktualizowane na bieżąco. Dzięki temu proces aktualizacji nie wpływa na działanie produktu i jednocześnie eliminuje wszelkie luki.

WAŻNE
Aby chronić się przed najnowszymi zagrożeniami, aktualizacje automatyczne powinny być zawsze włączone.

W niektórych sytuacjach będzie potrzebny Twój udział, żeby ochrona produktu Bitdefender była aktualna:

- Jeśli Twój komputer łączy się z internetem przez proxy, to należy skonfigurować ustawienia proxy, jak opisano w *„Jak skonfigurować Bitdefender, aby używał połączenia z internetem przez serwer proxy?"* (p. 80).
- Podczas pobierania aktualizacji przez powolne łącze internetowe mogą wystąpić błędy. Informacje o tym, jak pozbyć się takich błędów, znajdują się tutaj: *„Jak zaktualizować produkt Bitdefender przy użyciu wolnego połączenia internetowego?"* (p. 195).
- Jeśli łączysz się z internetem za pomocą modemu, zalecane jest regularne aktualizowanie Bitdefender na żądanie. Aby uzyskać więcej informacji, odwołaj się do *„Przeprowadzanie aktualizacji"* (p. 44).

7.1. Sprawdzanie aktualności produktu Bitdefender

Aby sprawdzić czas ostatniej aktualizacji swojego Bitdefender, spójrz na **Stan Bezpieczeństwa**, po lewej stronie paska narzędzi.

Aby uzyskać szczegółowe informacje o ostatnich aktualizacjach, sprawdź zdarzenia aktualizacji:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. W zakładce **Wszystko** zaznacz powiadomienia dotyczące ostatniej aktualizacji

Możesz dowiedzieć się, kiedy zaczęto aktualizację, oraz zapoznać się ze szczegółami (czy aktualizacje były udane czy nie, czy wymagają ponownego uruchomienia sytemu, aby dokończyć instalację). Jeśli to konieczne, uruchom komputer ponownie w wybranym przez Ciebie momencie.

7.2. Przeprowadzanie aktualizacji

Aby zaktualizować, potrzebne będzie połączenie z internetem.

Aby uruchomić proces aktualizacji, wykonaj którąkolwiek z poniższych czynności:

- Otwórz Interfejs Bitdefender i kliknij link **AKTUALIZUJ TERAZ** znajdujący się pod statusem Twojego programu.
- Kliknij prawym przyciskiem myszki ikonę produktu Bitdefender w zasobniku systemowym i wybierz **Aktualizuj teraz**.

Moduł aktualizacji sprawdzi dostępne aktualizacje na serwerze Bitdefender. Jeśli aktualizacja będzie dostępna, w zależności od ustawień aktualizacji zostaniesz poproszony o jej potwierdzenie lub zostanie ona automatycznie pobrana i zainstalowana na Twoim komputerze.

WAŻNE
Może okazać się, że będziesz musiał ponownie uruchomić komputer po zakończeniu aktualizacji. Zalecamy zrobić to jak najszybciej.

Możesz też wykonać zdalnie aktualizacje na swoich urządzeniach, pod warunkiem, że są one włączone i podłączone do Internetu.

Aby zdalnie zaktualizować Bitdefender na urządzeniu:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. Kliknij ikonę na pożądanej karcie urządzenia, a następnie wybierz **Aktualizuj**.

7.3. Włączanie i wyłączanie aktualizacji automatycznych

Aby włączyć lub wyłączyć automatyczne aktualizacje:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Aktualizacja**.
3. Kliknij odpowiedni przełącznik WŁĄCZ/WYŁĄCZ.
4. Pojawia się okno ostrzegawcze. Musisz potwierdzić swój wybór, określając w menu czas, w którym automatyczna aktualizacja ma być wyłączona. Możesz wyłączyć automatyczną aktualizację na 5, 15 lub 30 minut, na godzinę, całkowicie albo aż do restartu systemu.

Ostrzeżenie

To jest krytyczne zagadnienie bezpieczeństwa. Zalecamy wyłączenie automatycznej aktualizacji na tak krótko jak to możliwe. Jeśli Bitdefender nie będzie aktualizowany regularnie nie będzie w stanie chronić Cię przed najnowszymi zagrożeniami.

7.4. Dostosowanie ustawień aktualizacji

Aktualizacje mogą być przeprowadzone z lokalnej sieci, bezpośrednio przez internet albo przez serwer proxy. Domyślnie, Bitdefender sprawdzi co godzinę czy są aktualizacje w internecie, i zainstaluje je bez powiadamiania Cię.

Domyślne ustawienia aktualizacji są dopasowane do potrzeb większości użytkowników i zwykle nie musisz ich zmieniać.

Aby dostosować ustawienia aktualizacji:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Aktualizacja** i dostosuj ustawienia zgodnie z własnymi preferencjami.

Częstotliwość aktualizacji

Bitdefender jest skonfigurowany, aby sprawdzać dostępność aktualizacji co godzinę. Aby zmienić częstotliwość aktualizacji, przeciągnij suwak wzdłuż skali, aby ustawić pożądany okres czasu, gdy aktualizacja powinna się pojawić.

Lokalizacja aktualizacji

Bitdefender jest skonfigurowany w taki sposób, aby pobierał przez internet aktualizacje z serwerów firmy Bitdefender. Lokalizacją aktualizacji jest ogólny adres internetowy, który jest automatycznie przekierowywany do najbliższego serwera aktualizacji Bitdefender w Twoim regionie.

Nie zmieniaj lokalizacji aktualizacji, jeśli nie było to zalecane przez przedstawiciela Bitdefender lub przez administratora Twojej sieci (jeśli jesteś połączony z siecią biurową).

Możesz powrócić do domyślnej internetowej lokalizacji aktualizacji, klikając opcję "**Domyślny**".

Reguły przetwarzania aktualizacji

Możesz wybrać jeden z trzech sposobów na pobranie i zainstalowanie aktualizacji:

- **Cicha aktualizacja** - Bitdefender automatycznie pobiera i implementuje aktualizacje.
- **Pytaj przed pobraniem** - jeśli aktualizacja jest dostępna, każdorazowo zostaniesz zapytany o jej pobranie.
- **Pytaj przed zainstalowaniem** - za każdym razem, kiedy zostanie pobrana aktualizacja, zostaniesz poproszony o jej zainstalowanie.

Aby ukończyć instalację niektórych aktualizacji, będziesz musiał ponownie uruchomić komputer. Domyślnie, jeśli aktualizacja wymaga ponownego włączenia systemu, Bitdefender będzie pracował ze starymi plikami, dopóki użytkownik sam nie zrestartuje komputera. Uniemożliwi to procesowi aktualizacji Bitdefender przeszkadzanie w pracy użytkownika.

Jeśli chcesz, by program pytał w momencie, kiedy aktualizacja wymaga ponownego uruchomienia, włącz opcję "**Odrocz ponowne uruchomienie**", klikając odpowiedni przycisk.

7.5. Ciągłe aktualizacje

Aby mieć pewność, że używasz najnowszej wersji, Twój Bitdefender automatycznie będzie wyszukiwał aktualizacji produktu. Te aktualizacje mogą wprowadzać nowe funkcje i ulepszenia, rozwiązać problemy z produktem lub automatycznie uaktualnić go do nowej wersji. Gdy nowa wersja Bitdefender jest dostarczana przez aktualizację, ustawienia

niestandardowe są zapisywane, a procedura odinstalowywania i ponownej instalacji jest pomijana.

Te aktualizacje wymagają ponownego uruchomienia systemu, aby rozpocząć instalację nowych plików. Po zakończeniu aktualizacji produktów, okno pop-up poinformuje Cię, o ponownym uruchomieniu komputera. Jeśli pominiesz to powiadomienie, możesz kliknąć **ZRESETUJ TERAZ** w oknie Powiadomienia, gdzie wymieniona jest ostatnia aktualizacja lub ręcznie zresetować system.

Notatka

Aktualizacje zawierające nowe funkcje i ulepszenia zostaną dostarczone tylko użytkownikom, którzy mają zainstalowany Bitdefender 2017.

JAK TO ZROBIĆ?

8. INSTALACJA

8.1. Jak zainstalować Bitdefender na drugim komputerze?

Jeśli subskrypcja, którą kupiłeś obejmuje więcej niż jeden komputer, możesz użyć swojego konta Bitdefender, aby aktywować drugi komputer.

Aby zainstalować Bitdefender na drugim komputerze:

1. Kliknij link **ZAINSTALUJ NA INNYM URZĄDZENIU** w prawym dolnym rogu interfejsu Bitdefender.

   Jesteś przekierowany do strony konta Bitdefender. Upewnij się, że jesteś zalogowany przy użyciu swoich poświadczeń.

2. W wyświetlonym oknie wybierz żądany system operacyjny, a następnie kliknij **KONTYNUUJ**.

3. Wpisz adres e-mail, na który należy wysłać link do pobrania instalatora aplikacji na wybraną platformę.

4. Uruchom produkt Bitdefender, który pobrałeś. Poczekaj, aż proces instalacji będzie ukończony, a następnie zamknij okno.

Nowe urządzenie, na którym zainstalowaałeś produkt Bitdefender pojawi się w panelu nawigacyjnym Bitdefender Central.

8.2. Jak mogę odinstalować Bitdefender?

Typowe sytuacje, w których konieczne będzie ponowne zainstalowanie produktu Bitdefender to:

- Przeinstalowałeś system operacyjny.
- Napraw błędy, które mogą powodować spowolnienia lub awarie.
- Twój Bitdefender nie uruchamia się lub nie działa prawidłowo.

Jeśli wystąpiła jedna z wymienionych sytuacji, wykonaj następujące kroki:

- W systemie **Windows 7**:

  1. Kliknij **Start** i przejdź do **Wszystkie programy**.
  2. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
  3. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.

4. Musisz zrestartować komputer, aby zakończyć proces.

- W systemach **Windows 8 i Windows 8.1**:

1. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
2. Kliknij **Odinstaluj program** lub **Programy i funkcje**.
3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
5. Musisz zrestartować komputer, aby zakończyć proces.

- W systemie **Windows 10**:

1. Kliknij **Start**, a następnie kliknij Ustawienia.
2. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Funkcje aplikacji &**.
3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.
5. Kliknij **PRZEINSTALUJ**.
6. Musisz zrestartować komputer, aby zakończyć proces.

Notatka
Postępując zgodnie z procedurą ponownej instalacji, ustawienia dostosowane są zapisywane i dostępne w nowym zainstalowanym produkcie. Inne ustawienia mogą zostać przywrócone do domyślnej konfiguracji.

8.3. Skąd mogę pobrać produkt Bitdefender?

Możesz zainstalować Bitdefender z dysku instalacyjnego lub korzystając z instalatora internetowego, który możesz pobrać na komputer z platformy Bitdefender Central.

Notatka
Przed uruchomieniem pakietu zalecane jest usunięcie wszelkich rozwiązań antywirusowych zainstalowanych w systemie. Gdy na jednym komputerze uruchomione jest więcej niż jedno rozwiązanie bezpieczeństwa, system staje się niestabilny.

Aby zainstalować Bitdefender z Bitdefender Central:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. W oknie **MOJE URZĄDZENIA**, kliknij **ZAINSTALUJ Bitdefender**.
4. Wybierz jedną z dwóch dostępnych opcji:
   - **POBIERANIE**

     Kliknij przycisk i zapisz plik instalacyjny.
   - **Na innym urządzeniu**

     Zaznacz **Windows**, aby pobrać swój produkt Bitdefender, a następnie kliknij **KONTYNUUJ**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ**.
5. Uruchom produkt Bitdefender, który pobrałeś.

8.4. Jak mogę zmienić język mojego produktu Bitdefender?

Jeśli chcesz użyć Bitdefender w innym języku, będziesz musiał ponownie zainstalować produkt we właściwym języku.

Aby użyć Bitdefender w innym języku:

1. Usuń Bitdefender w następujący sposób:
   - W systemie **Windows 7**:

     a. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.

     b. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

     c. Kliknij **USUŃ** w oknie, które się pojawi.

     d. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
   - W systemach **Windows 8 i Windows 8.1**:

     a. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania"

bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.

b. Kliknij **Odinstaluj program** lub **Programy i funkcje**.

c. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

d. Kliknij **USUŃ** w oknie, które się pojawi.

e. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

- W systemie **Windows 10**:

a. Kliknij **Start**, a następnie kliknij Ustawienia.

b. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.

c. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

d. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.

e. Kliknij **USUŃ** w oknie, które się pojawi.

f. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

2. Zmień język Bitdefender Central:

a. Uzyskaj dostęp do Bitdefender Central.

b. Kliknij ikonę w prawym górnym rogu ekranu.

c. Kliknij **Moje Konto** w menu slajdów.

d. Wybierz zakładkę **Profil**.

e. Wybierz język z rozwijanej listy **Język**, a następnie kliknij **ZAPISZ**.

3. Pobierz plik instalacyjny:

a. Wybierz panel **Moje Urządzenia**.

b. W oknie **MOJE URZĄDZENIA**, kliknij **ZAINSTALUJ Bitdefender**.

c. Wybierz jedną z dwóch dostępnych opcji:

- **POBIERANIE**

  Kliknij przycisk i zapisz plik instalacyjny.

- **Na innym urządzeniu**

  Zaznacz **Windows**, aby pobrać swój produkt Bitdefender, a następnie kliknij **KONTYNUUJ**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ**.

4. Uruchom produkt Bitdefender, który pobrałeś.

Notatka
Ta procedura ponownej instalacji spowoduje trwałe usunięcie dostosowanych ustawień.

8.5. W jaki sposób korzystać z subskrypcji Bitdefender po zmianie wersji systemu Windows?

Taka sytuacja ma miejsce kiedy zmienisz wersję systemu Windows i chcesz kontynuować używanie subskrypcji Bitdefender.

Jeżeli używasz wcześniejszej wersji Bitdefender, możesz ją za darmo ulepszyć do najnowszej wersji Bitdefender w następujący sposób:

- Uaktualnienie Bitdefender Antywirus do najnowszej wersji Bitdefender Antywirus jest dostępne.
- Uaktualnienie Bitdefender Internet Security do najnowszej wersji Bitdefender Internet Security jest dostępne.
- Uaktualnienie Bitdefender Total Security do najnowszej wersji Bitdefender Total Security jest dostępne.

Mogą wystąpić dwa przypadki:

- Uaktualniłeś system operacyjny za pomocą usługi Windows Update i zauważyłeś wstrzymanie pracy Bitdefender.

  W takim przypadku zainstaluj ponownie produkt, wykonując następujące czynności:

  - W systemie **Windows 7**:

    1. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
    2. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
    3. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.

4. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

   Otwórz interfejs nowego zainstalowanego produktu Bitdefender, aby uzyskać dostęp do jego funkcji.

- W systemach **Windows 8 i Windows 8.1**:

1. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
2. Kliknij **Odinstaluj program** lub **Programy i funkcje**.
3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
5. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

   Otwórz interfejs nowego zainstalowanego produktu Bitdefender, aby uzyskać dostęp do jego funkcji.

- W systemie **Windows 10**:

1. Kliknij **Start**, a następnie kliknij Ustawienia.
2. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.
3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.
5. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
6. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

   Otwórz interfejs nowego zainstalowanego produktu Bitdefender, aby uzyskać dostęp do jego funkcji.

Notatka

Postępując zgodnie z procedurą ponownej instalacji, ustawienia dostosowane są zapisywane i dostępne w nowym zainstalowanym

produkcie. Inne ustawienia mogą zostać przywrócone do domyślnej konfiguracji.

- Zmieniłeś system operacyjny i nadal chcesz korzystać z ochrony oferowanej przez Bitdefender. W takim przypadku należy ponownie zainstalować produkt, korzystając z najnowszej wersji.

  Aby rozwiązać tę sytuację:

  1. Pobierz plik instalacyjny:
     a. Uzyskaj dostęp do Bitdefender Central.
     b. Wybierz panel **Moje Urządzenia**.
     c. W oknie **MOJE URZĄDZENIA**, kliknij **ZAINSTALUJ Bitdefender**.
     d. Wybierz jedną z dwóch dostępnych opcji:
        - **POBIERANIE**

          Kliknij przycisk i zapisz plik instalacyjny.
        - **Na innym urządzeniu**

          Zaznacz **Windows**, aby pobrać swój produkt Bitdefender, a następnie kliknij **KONTYNUUJ**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ**.
  2. Uruchom produkt Bitdefender, który pobrałeś.

  Aby uzyskać więcej informacji o procesie instalacji Bitdefender, prosimy odnieść się do *„Instalowanie produktu Bitdefender”* (p. 5).

8.6. Jak mogę zaktualizować do najnowszej wersji Bitdefender?

Począwszy od Bitdefender 2018 uaktualnienie do najnowszej wersji jest możliwe bez konieczności ręcznej procedury odinstalowania i ponownej instalacji. Dokładniej - nowy produkt, zawierający nowy funkcje i ulepszenia, jest dostarczany za pomocą aktualizacji produktu, a jeśli masz już aktywną subskrypcję Bitdefender, produkt zostanie automatycznie aktywowany.

Jeśli korzystasz z wersji 2017, możesz uaktualnić do najnowszej wersji, wykonując następujące kroki:

1. Kliknij **ZRESETUJ TERAZ** w powiadomieniu, które otrzymałeś wraz z informacją o aktualizacji. Jeśli je przegapiłeś, przejdź do okna

Powiadomienia, otwórz najnowsze i kliknij przycisk **URUCHOM PONOWNIE TERAZ**. Zaczekaj na ponowne uruchomienie komputera.

Pojawia się okno **Co nowego** z informacjami o ulepszonych i nowych funkcjach.

2. Kliknij link **Czytaj więcej**, aby przejść do naszej dedykowanej strony ze szczegółami i pomocnymi artykułami.
3. Zamknij okno **Co nowego**, aby uzyskać dostęp do interfejsu nowo zainstalowanej wersji.

Użytkownicy, którzy chcą uaktualnić bezpłatnie z Bitdefender 2016 lub niższej wersji do najnowszej wersji Bitdefender, muszą usunąć bieżącą wersję z Panelu sterowania, a następnie pobrać najnowszy plik instalacyjny ze strony internetowej Bitdefender, pod następującym adresem: http://bitdefender.pl/dom-mala-firma/uzyteczne-linki/span-classns9pobierz-wersje-homespan. Aktywacja jest możliwa tylko z ważną subskrypcją.

9. SUBSKRYPCJE

9.1. Jak aktywować subskrypcję Bitdefender przy użyciu klucza licencyjnego?

Jeśli masz ważny klucz licencyjny i chcesz go użyć, aby aktywować subskrypcję dla Bitdefender Internet Security 2018, możliwe są dwa przypadki:

- Zaktualizowałeś z poprzedniej wersji Bitdefender do nowej:
  1. Po zakończeniu aktualizacji do Bitdefender Internet Security 2018, zostaniesz poproszony o zalogowanie się do swojego konta Bitdefender.
  2. Kliknij **Zapisz się**, następnie wprowadź adres e-mail oraz hasło do Twojego konta Bitdefender.
  3. Kliknij **Zapisz się**, aby kontynuować.
  4. Na ekranie konta pojawi się powiadomienie informujące, że subskrypcja została utworzona. Utworzona subskrypcja będzie ważna przez pozostałe dni na kluczu licencyjnym i dla tej samej liczby użytkowników.

     Urządzenia, które korzystają z poprzednich wersji Bitdefender i są zarejestrowane z kluczem licencyjnym, który przekonwertowałeś na subskrypcję muszą aktywować produkt przy użyciu tego samego konta Bitdefender.
- Bitdefender nie był dotychczas zainstalowany na systemie:
  1. Gdy tylko proces instalacji zostanie zakończony, użytkownik zostanie poproszony o zalogowanie się do swojego konta Bitdefender.
  2. Kliknij **Zapisz się**, następnie wprowadź adres e-mail oraz hasło do Twojego konta Bitdefender.
  3. Kliknij **ZALOGUJ SIĘ**, aby kontynuować, a następnie przycisk **ZAKOŃCZ**, aby uzyskać dostęp do interfejsu Bitdefender Internet Security 2018.
  4. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  5. Kliknij link **Kod Aktywacyjny**.

     Pojawi się nowe okno.
  6. Kliknij link **Otrzymaj swój DARMOWY upgrade teraz!**.

7. Wpisz swój klucz licencyjny w odpowiednim polu i naciśnij **AKTUALIZUJ MÓJ PRODUKT**. Subskrypcja z tą samą dostępnością i liczbą użytkowników klucza licencyjnego wiąże się z Twoim kontem.

10. BITDEFENDER CENTRAL

10.1. W jaki sposób zalogować się do Bitdefender Central używając innego konta?

Utworzono nowe konto Bitdefender i można już z niego korzystać.

Aby z powodzeniem użyć innego konta:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij przycisk **PRZEŁĄCZ KONTO**, aby zmienić konto połączone z komputerem.
3. W odpowiednich polach wprowadź adres e-mail i hasło do Twojego konta, a następnie kliknij **ZALOGUJ SIĘ**.

Notatka
Produkt Bitdefender z Twojego urządzenia zmienia sie automatycznie w zależności od subskrypcji związanej z nowym kontem Bitdefender.
Jeśli nie ma dostępnych subskrypcji związanych z nowym kontem Bitdefender, lub chcesz przenieść ją z poprzedniego konta, możesz skontaktować się z Bitdefender, aby uzyskać pomoc tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

10.2. Jak wyłączyć wiadomości pomocnicze Bitdefender Central?

Aby pomóc Ci zrozumieć każdą opcję w Bitdefender Central możesz skorzystać z informacji pomocniczych w panelu.

Jeżeli nie chcesz widzieć tego typy wiadomości:

1. Uzyskaj dostęp do Bitdefender Central.
2. Kliknij ikonę w prawym górnym rogu ekranu.
3. Kliknij **Moje Konto** w menu slajdów.
4. Wybierz zakładkę **Ustawienia**.
5. Wyłącz informacje pomocnicze **Włącz/Wyłącz wiadomości pomocy**

10.3. Jak mogę przestać widzieć zdjęcia snap zrobione na moich urządzeniach?

Aby zatrzymać widoczność zrobionych zdjęć zrobione na Twoim urządzeniu:

1. Uzyskaj dostęp do Bitdefender Central.
2. Kliknij ikonę w prawym górnym rogu ekranu.
3. Kliknij **Moje Konto** w menu slajdów.
4. Wybierz zakładkę **Ustawienia**.
5. Wyłącz opcje **Pokaż/nie pokazuj zdjęć wykonanych na Twoim urządzeniu** .

10.4. Zapomniałem hasła, które ustawiłem dla mojego konta Bitdefender. Jak to zresetować?

Są dwie możliwości aby ustawić hasło do konta Bitdefendera :

- Z interfejsu Bitdefender:
  1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  2. Kliknij przycisk **PRZEŁĄCZ KONTO**.

     Pojawi się nowe okno.
  3. Kliknij odnośnik **Zapomniałem hasła**.
  4. Wprowadź adres e-mail użyty do stworzenia konta Bitdefender, a następnie kliknij przycisk **ZAPOMNIAŁEM HASŁĄ**.
  5. Sprawdź skrzynkę e-mail i kliknij dostarczony przycisk.

     Otworzy się okno ZRESETUJ HASŁO Bitdefender.
  6. Wprowadź adres e-mail i nowe hasło w odpowiednich polach. Hasło musi mieć co najmniej 8 znaków i zawierać liczby.
  7. Kliknij przycisk **RESETUJ HASŁO**.
- Z Twojej przeglądarki internetowej:
  1. Idź do: https://central.bitdefender.com.
  2. Kliknij odnośnik **Zapomniałem hasła**.

3. Wpisz swój adres e-mail, a następnie kliknij przycisk **ZAPOMNIAŁEM HASŁA**.
4. Sprawdź swoje konto e-mail i wykonaj podane instrukcje, aby ustawić nowe hasło dla swojego konta Bitdefender.

Aby uzyskać dostęp do konta Bitdefender od teraz, wprowadź swój adres e-mail i nowo utworzone hasło.

10.5. Jak mogę zarządzać sesjami logowania powiązanymi z kontem Bitdefendera?

Na twoim koncieBitdefender masz możliwość zobaczyć ostatnie aktywne i nieaktywne sesje logowania na urządzeniach związanych z kontem. Oprócz tego, możesz wylogować się zdalnie postępując według kroków:

1. Uzyskaj dostęp do Bitdefender Central.
2. Kliknij ikonę w prawym górnym rogu ekranu.
3. Kliknij **Moje Konto** w menu slajdów.
4. Wybierz zakładkę **Zarządzanie sesją**.
5. W zakładce **Aktywne sesje** wybierz opcję **WYLOGUJ się** obok urządzenia jeśli chcesz zakończyć sesje.

11. SKANOWANIE PRZY POMOCY BITDEFENDER

11.1. Jak można skanować plik lub folder?

Najprostszym sposobem na przeskanowanie pliku lub folderu jest kliknięcie prawym przyciskiem myszy na wybranym obiekcie, wskazanie Bitdefender i wybór **Skanuj za pomocą Bitdefender**.

Aby zakończyć skanowanie, postępuj zgodnie z poleceniami kreatora skanowania antywirusowego. Bitdefender automatycznie podejmie zalecane działania względem wykrytych plików.

Jeśli pozostaną nierozwiązane zagrożenia, zostaniesz poproszony o wybranie działań, jakie względem nich zostaną podjęte.

Typowe sytuacje, kiedy należałoby użyć tej metody skanowania to:

- Podejrzewasz, że konkretny plik lub folder może być zainfekowany.
- Kiedykolwiek ściągasz pliki z internetu i podejrzewasz że mogą być niebezpieczne.
- Skanujesz współdzielone zasoby sieciowe przed skopiowaniem ich na Twój komputer.

11.2. Jak mogę przeskanować swój system?

Aby wykonać kompletne skanowanie na systemie:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYWIRUS** wybierz **Skanowanie Systemu**.
4. Podążaj według zaleceń kreatora Skanowania Systemu, aby przeprowadzić skanowanie. Bitdefender automatycznie podejmie zalecane działania względem wykrytych plików.

   Jeśli pozostaną nierozwiązane zagrożenia, zostaniesz poproszony o wybranie działań, jakie względem nich zostaną podjęte. Aby uzyskać więcej informacji, odwołaj się do „*Kreator skanowania antywirusowego*" (p. 98).

11.3. Jak zaplanować skanowanie?

Możesz ustawić produkt Bitdefender, aby rozpocząć skanowanie ważnych lokalizacji systemu, gdy nie siedzisz przy komputerze.

Aby zaplanować skanowanie:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYWIRUS**, wybierz **Zarządzanie Skanowaniem**.
4. Wybierz typ skanowania, który chcesz zaplanować, Pełne Skanowanie Systemu lub Szybkie Skanowanie, a następnie kliknij **Opcje Skanowania**.

   Alternatywnie, możesz utworzyć typ skanowania, aby dostosować go do własnych potrzeb klikając **Nowe zadanie niestandardowe**.
5. Włącz przełącznik **Harmonogram**.

   Wybierz jedną z odpowiednich opcji, aby ustalić harmonogram:

   - Przy uruchomieniu systemu
   - Raz
   - Okresowo

W oknie **Cele skanowania** możesz wybrać lokalizacje, które chcesz by były skanowane.

11.4. Jak utworzyć niestandardowe zadanie skanowania?

Jeśli chcesz przeskanować konkretną lokalizację lub skonfigurować opcje skanowania, ustaw i uruchom niestandardowe zadanie skanowania.

Aby utworzyć niestandardowe zadanie skanowania, wykonaj następujące czynności:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYWIRUS**, wybierz **Zarządzanie Skanowaniem**.

4. Naciśnij **Nowe zadanie niestandardowe**. W zakładce **Podstawowe** wprowadź nazwę skanowania i wybierz obiekty, które mają być przeskanowane.
5. Jeśli chcesz skonfigurować szczegółowe opcje skanowania, wybierz zakładkę **Zaawansowane**.

   Opcje skanowania można z łatwością konfigurować poprzez dostosowanie poziomu skanowania. Aby ustawić wybrany poziom skanowania, przeciągnij suwak wzdłuż skali.

   W przypadku braku zagrożeń możesz również zadecydować o wyłączeniu komputera po zakończeniu skanowania. Pamiętaj, że będzie to domyślna akcja, każdorazowo, gdy uruchomisz to zadanie.
6. Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.
7. Użyj odpowiedniego przełącznika, jeśli chcesz ustawić harmonogram dla zadania skanowania.
8. Kliknij **Uruchom skanowanie** i użyj Kreatora skanowania, aby ukończyć skanowanie. Na koniec skanowania zostaniesz poproszony o wybranie działania, które zostanie wykonane względem wykrytych plików, jeśli takowe wystąpią.
9. Jeśli chcesz, możesz szybko ponownie uruchomić poprzednie własne skanowanie poprzez kliknięcie odpowiedniego wpisu na dostępnej liście.

11.5. Jak wykluczyć folder ze skanowania?

Bitdefender pozwala na wykluczanie ze skanowania konkretnych plików, folderów i rozszerzeń plików.

Wyjątki powinny być używane przez użytkowników posiadających zaawansowaną wiedzę komputerową i tylko w następujących przypadkach:

- Na komputerze znajduje się duży folder, w którym trzymasz filmy i muzykę.
- Na komputerze znajduje się duże archiwum, w którym trzymasz różne dane.
- Stwórz folder, gdzie będziesz instalował różne programy w celu ich testowania. Skanowanie folderu może się zakończyć utratą części danych.

Aby dodać folder do listy Wykluczeń:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.

2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę ⚙ w prawym dolnym rogu panelu **ANTYWIRUS**.
4. Kliknij zakładkę **WYKLUCZENIA**.
5. Kliknij w **Lista plików i folderów wykluczonych ze skanowania** w rozwijanym menu, a następnie przycisk **DODAJ**.
6. Kliknij **Wyszukaj**, wybierz folder, który chcesz wykluczyć ze skanowania, a następnie wybierz typ skanowania, z którego folder ma zostać wykluczony.
7. Kliknij **Dodaj**, aby zapisać zmiany i zamknąć okno.

11.6. Co zrobić, kiedy Bitdefender rozpoznał niezarażony plik jako zarażony?

Zdarza się, że Bitdefender błędnie uznaje dozwolony plik za zagrożenie (i zgłasza fałszywy alarm). Aby naprawić ten błąd, dodaj dany plik do obszaru wykluczeń Bitdefender:

1. Wyłącz ochronę antywirusową w czasie rzeczywistym Bitdefender:
   a. Kliknij ikonę Ⓑ po lewej stronie interfejsu Bitdefender.
   b. Kliknij link **POKAŻ FUNKCJE**.
   c. Wybierz ikonę ⚙ w prawym dolnym rogu panelu **ANTYWIRUS**.
   d. W oknie **OCHRONA** kliknij przełącznik WŁĄCZ/WYŁĄCZ.

      Pojawia się okno ostrzegawcze. Musisz potwierdzić swój wybór, określając w menu czas, w którym ochrona w czasie rzeczywistym ma być wyłączona. Możesz wyłączyć ochronę w czasie rzeczywistym na 5, 15 lub 30 minut, na godzinę, na stałe lub do czasu następnego uruchomienia systemu.
2. Wyświetl ukryte obiekty w systemie Windows. Informacje, jak należy to zrobić, znajdują się w *„Jak wyświetlić ukryte obiekty w systemie Windows?”* (p. 82).
3. Odzyskaj plik z sektora kwarantanny:
   a. Kliknij ikonę Ⓑ po lewej stronie interfejsu Bitdefender.
   b. Kliknij link **POKAŻ FUNKCJE**.

c. Wybierz ikonę ⚙ w prawym dolnym rogu panelu **ANTYWIRUS**.

d. Wybierz zakładkę **Kwarantanna**.

e. Zaznacz plik, a następnie kliknij **PRZYWRÓĆ**.

4. Dodaj plik do listy wykluczeń. Informacje, jak należy to zrobić, znajdują się w *„Jak wykluczyć folder ze skanowania?"* (p. 64).
5. Włącz ochronę antywirusową w czasie rzeczywistym Bitdefender.
6. Skontaktuj się z przedstawicielem pomocy technicznej, by móc usunąć sygnaturę. Informacje, jak należy to zrobić, znajdują się w *„Prośba o pomoc"* (p. 219).

11.7. Jak mogę sprawdzić, jakie wirusy wykrył Bitdefender?

Za każdym razem, gdy wykonywane jest skanowanie, tworzony jest dziennik skanowania, a Bitdefender rejestruje wykryte problemy.

Dziennik skanowania zawiera szczegółowe informacje o procesie skanowania, takie jak opcje skanowania, cel skanowania, zagrożenia znalezione i działania wykonane na tych zagrożeniach.

Po zakończeniu skanowania dziennik skanowania można otworzyć bezpośrednio z poziomu kreatora skanowania. Aby to zrobić, kliknij opcję **Pokaż dziennik**.

Aby sprawdzić logi skanowania lub wykrytych infekcji później:

1. Kliknij ikonę 🔔 po lewej stronie interfejsu Bitdefender.
2. W zakładce **Wszystko**, zaznacz powiadomienia dotyczące ostatniego skanowania

   Tutaj znajdziesz wszystkie zdarzenia skanowania w poszukiwaniu obecności szkodliwego oprogramowania, włącznie z zagrożeniami wykrytymi przez skanowanie w czasie rzeczywistym, skanowanie zainicjowane przez użytkownika oraz zmiany stanu skanowania automatycznego.
3. Na liście powiadomień, możesz sprawdzić jakie skanowanie zostało ostatnio wykonane. Kliknij powiadomienie, aby dowiedzieć się więcej na jego temat.

4. Aby otworzyć dziennik skanowania, kliknij **Pokaż dziennik**.

12. ASYSTENT RODZICA

12.1. Jak mam chronić moje dzieci przed zagrożeniami z internetu?

Asystent Rodzica Bitdefender zezwala na ograniczenie dostępu do Internetu oraz konkretnych aplikacji, chroniąc Twoje dziecko przed oglądaniem niedozwolonych treści, kiedy nie ma Cię w pobliżu.

Aby skonfigurować Asystenta Rodzica:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij przycisk akcji **Asystent Rodzica**.

   Jesteś przekierowany do strony konta Bitdefender. Upewnij się, że jesteś zalogowany przy użyciu swoich poświadczeń.
3. Otwiera panel Asystenta rodzica. Tu można sprawdzić i skonfigurować ustawienia Asystenta Rodzica.
4. Kliknij **DODAJ PROFIL** po prawej stronie okna **Moje Dzieci**.
5. Ustaw konkretne informacje w odpowiednich polach, takie jak: imię i data urodzenia. Aby dodać zdjęcie profilowe kliknij link **Wybierz plik**. Kliknij **NASTĘPNY KROK** aby kontynuować.

   W oparciu o normy rozwoju dzieci, ustawiając datę narodzin dziecka automatycznie ładują się ustawienia uważane za właściwe dla jego kategorii wiekowej.
6. Jeśli urządzenie Twojego dziecka ma już zainstalowany Bitdefender Internet Security 2018, wybierz jego urządzenie z dostępnej listy, wybierz konto, które chcesz monitorować. Kliknij **ZAPISZ**.

   Jeśli dziecko używa urządzenia z Androidem lub iOS i Asystent Rodzica Bitdefender nie jest zainstalowany, kliknij **DODAJ URZĄDZENIE**. Jeśli dziecko używa urządzenia Mac, a Antywirus dla Mac Bitdefender nie jest zainstalowany, kliknij ten sam przycisk. Wybierz system operacyjny, którego applikację chcesz zainstalować, a następnie kliknij **NASTĘPNY KROK** aby kontynuować.
7. Wpisz adres e-mail, na który mamy wysłać link do pobrania instalatora aplikacji Bitdefender , a następnie kliknij **WYŚLIJ LINK INSTALACYJNY**.

Sprawdź aktywność Twojego dziecka i zmień ustawienia Asystenta Rodzica korzystając z konta Bitdefender z jakiegokolwiek komputera lub urządzenia mobilnego podłączonego do Internetu.

WAŻNE

Na urządzeniach z systemem Windows, Bitdefender Internet Security 2018 zawarty w Twojej subskrypcji trzeba pobrać i zainstalować.
W urządzeniach z systemem macOS należy pobrać i zainstalować Antywirus Bitdefender dla produktów Mac.
Na urządzeniach z systemem Android aplikacja Asystenta Rodzica Bitdefender musi zostać pobrana i zainstalowana.

12.2. Jak zablokować mojemu dziecku dostęp do strony internetowej?

Asystent Rodzica Bitdefender pozwala Ci kontrolować treści, które przegląda Twoje dziecko podczas korzystania ze swojego urządzenia i pozwala Ci na zablokowanie dostępu do strony internetowej.

Aby zablokować dostęp do strony internetowej, należy dodać ją do listy Wykluczeń, w następujący sposób:

1. Idź do: https://central.bitdefender.com.
2. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
3. Kliknij opcję **Asystent Rodzica**, żeby wyświetlić pulpit.
4. Wybierz profil Twojego dziecka z okna **Moje Dzieci**.
5. Wybierz zakładkę **Strony Internetowe**.
6. Kliknij przycisk **ZARZĄDZAJ**.
7. Wpisz w odpowiednim polu stronę internetową, którą chcesz zablokować.
8. Wybierz **Zezwól** lub **Zablokuj**.
9. Kliknij **ZAKOŃCZ**, aby zapisać zmiany.

Notatka

Ograniczenia można ustawiać tylko dla urządzeń z systemem Android i Windows.

12.3. W jaki sposób zapobiec graniu w gry przez moje dziecko?

Asystent Rodzica Bitdefender pozwala na kontrolowanie treści przeglądanej przez Twoje dziecko podczas używania komputera.

Aby zablokować dostęp do gry:

1. Idź do: https://central.bitdefender.com.
2. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
3. Kliknij opcję **Asystent Rodzica**, żeby wyświetlić pulpit.
4. Wybierz profil Twojego dziecka z okna **Moje Dzieci**.
5. Wybierz zakładkę **Aplikacje**.

   Została wyświetlona lista z kartami. Karty przedstawiają aplikacje, z których korzysta Twoje dziecko.
6. Wybierz kartę z aplikacją, którą chcesz, aby Twoje dziecko przestało używać.

   Symbol znacznika wyboru, który się pojawia wskazuje, że Twoje dziecko nie będzie mogło korzystać z aplikacji.

12.4. Jak mogę zapobiec, by moje dziecko nie kontaktowało się z osobami niezaufanymi?

Asystent Rodzica Bitdefender daje Ci możliwość blokowania połaczeń od nieznanych numerów telefonów lub od znajomych z listy telefonów dziecka.

Aby zablokować konkretny kontakt na urządzeniu z Adroidem, które ma zainstalowaną aplikacje Asystenta Rodzica Bitdefender:

1. Idź do: https://central.bitdefender.com.
2. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
3. Kliknij opcję **Asystent Rodzica**, żeby wyświetlić pulpit.
4. Wybierz profil dziecka, któremu chcesz ustawić ograniczenia.
5. Wybierz zakładkę**Kontakty Telefoniczne**.

Została wyświetlona lista z kartami. Karty stanowią kontakty z telefonu Twojego dziecka.

6. Wybierz kartę z numerem telefonu, który chcesz zablokować.

   Symbol znacznika wyboru, który się pojawia, wskazuje, że wybrany numer telefonu nie połączy się z Twoim dzieckiem.

Aby zablokować konkretny kontakt na urządzeniu z Adroidem, które nie posiada zainstalowanej aplikacji Asystenta Rodzica Bitdefender:

1. Idź do: https://central.bitdefender.com.
2. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
3. Kliknij opcję **Asystent Rodzica**, żeby wyświetlić pulpit.
4. Wybierz profil dziecka, któremu chcesz ustawić ograniczenia.
5. Kliknij link **Instaluj Asystenta Rodzica** w wybranej karcie.
6. Kliknij **DODAJ URZĄDZENIE** na oknie które się pojawi.
7. Opcja **Bitdefender Asystent Rodzica na Androida** jest zaznaczona domyślnie. Kliknij **NASTĘPNY KROK** aby kontynuować oraz instalować aplikacje na wybranym urządzeniu.
8. Wybierz zakładkę**Kontakty Telefoniczne**.

   Została wyświetlona lista z kartami. Karty stanowią kontakty z telefonu Android Twojego dziecka.

9. Wybierz kartę z numerem telefonu, który chcesz zablokować.

   Symbol znacznika wyboru, który się pojawia, wskazuje, że wybrany numer telefonu nie połączy się z Twoim dzieckiem.

Aby zablokować nieznane numery telefonów, włącz przycisk **Blokuj połączenia bez numeru ID**.

Notatka

Ograniczenia połączeń telefonicznych można ustawić tylko dla urządzeń z Androidem dodanych do profilu Twojego dziecka.

12.5. W jaki sposób można ustawić lokalizację jako bezpieczną lub ograniczoną dla mojego dziecka?

Asystent Rodzica Bitdefender pozwala Ci ustawić lokalizację jako bezpieczną lub ograniczoną dla Twojego dziecka.

Aby ustawić lokalizację:

1. Idź do: https://central.bitdefender.com.
2. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
3. Kliknij opcję **Asystent Rodzica**, żeby wyświetlić pulpit.
4. Wybierz profil Twojego dziecka z okna **Moje Dzieci**.
5. Wybierz zakładkę **Lokalizacja Dziecka**.
6. Kliknij **Urządzenia** w ramce, którą masz w oknie **Lokalizacja Dziecka**.
7. Kliknij **WYBIERZ URZĄDZENIA**, a następnie wybierz urządzenie, które chcesz konfigurować.
8. W oknie **Obszar**, kliknij przycisk **DODAJ OBSZAR**.
9. Wybierz typ lokalizacji, **BEZPIECZNA** lub **OGRANICZONA**.
10. Wpisz poprawną nazwę dla obszaru, gdzie dziecko ma pozwolenie, aby iść lub nie.
11. Ustaw zakres, który powinien być stosowany do monitorowania używając suwaka **Promień**.
12. Kliknij **DODAJ OBSZAR**, aby zapisać swoje ustawienia.

Gdy chcesz ustawić ograniczoną lokalizację jako bezpieczną lub bezpieczne miejsce jako ograniczone, kliknij je, a następnie wybierz przycisk **EDYTUJ OBSZAR**. W zależności od zmiany, którą chcesz wprowadzić, wybierz opcję **BEZPIECZNY** lub **OGRANICZONY**, a następnie kliknij **AKTUALIZUJ OBSZAR**.

12.6. Jak zablokować dostęp dziecku w trakcie dni szkolnych do przypisanego urządzenia?

Asystent Rodzica Bitdefender pozwala na ograniczenie dostępu dla dziecku do przypisanego urządzenia w trakcie dni szkolnych i kiedy praca domowa powinna być wykonana.

Aby ustawić ograniczenia:

1. Uzyskaj dostęp do panelu Asystent Rodzica z Bitdefender Central.
2. Z okna **MOJE DZIECI**, wybierz profil dziecka dla którego chcesz ustawić ograniczenia.
3. Wybierz zakładkę **Harmonogram**.
4. W obszarze **LIMITY DZIENNE** kliknij**DOKŁADNY**.
5. Wybierz pole wyboru **Limity Czasu Dni Szkolnych**.
6. Wybierz z siatki przedziały czasowe, w których dostęp ma być zablokowany.

Notatka
Ograniczenia można ustawiać tylko dla urządzeń z systemem Android i Windows.

12.7. Jak zablokować dostęp dziecku w trakcie nocy szkolnych do przypisanego urządzenia?

Asystent Rodzica Bitdefender pozwala na ograniczenie dostępu dla dziecku do przypisanego urządzenia w trakcie nocy przed szkołą.

Aby ustawić ograniczenia:

1. Uzyskaj dostęp do panelu Asystent Rodzica z Bitdefender Central.
2. Z okna **MOJE DZIECI**, wybierz profil dziecka dla którego chcesz ustawić ograniczenia.
3. Wybierz zakładkę **Harmonogram**.
4. O obszarze **CZAS SNU**wybierz pole wyboru**Noc Szkolna**.
5. Użyj strzałek góra i dół z wybranych pól aby zablokować dostęp w ustalonych interwałach czasu.

Notatka
Ograniczenia można ustawiać tylko dla urządzeń z systemem Android i Windows.

12.8. Jak zablokować dostęp dziecku w trakcie weekendów do przypisanego urządzenia?

Asystent Rodzica Bitdefender pozwala na ograniczenie dostępu dla dziecku do przypisanego urządzenia w trakcie weekendu i w nocy.

Aby ustawić ograniczenia:

1. Uzyskaj dostęp do panelu Asystent Rodzica z Bitdefender Central.
2. Z okna **MOJE DZIECI**, wybierz profil dziecka dla którego chcesz ustawić ograniczenia.
3. Wybierz zakładkę **Harmonogram**.
4. O obszarze **CZAS SNU**wybierz pole wyboru**Noc Weekendowa**.
5. Użyj strzałek góra i dół z wybranych pól aby zablokować dostęp w ustalonych interwałach czasu.
6. W obszarze **LIMITY DZIENNE** masz następujące opcje:
   - **NARASTAJĄCY**
     a. Wybierz pole wyboru **Weekendowe Limity Czasu**.
     b. Przeciągnij suwak aby ustawić czas dostępu do urządzenia.
   - **DOKŁADNY**
     a. Wybierz pole wyboru **Weekendowe Limity Czasu**.
     b. Wybierz z siatki przedziały czasowe, w których dostęp ma być zablokowany.

   Zauważ, że ustawienia **NARASTAJĄCY** oraz **DOKŁADNY** nie są zaprojektowane aby pracować jednocześnie.

Notatka
Ograniczenia można ustawiać tylko dla urządzeń z systemem Android i Windows.

12.9. W jaki sposób usunąć profil dziecka?

Jeśli chcesz usunąć istniejący profil dziecka:

1. Idź do: https://central.bitdefender.com.

2. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
3. Kliknij opcję **Asystent Rodzica**, żeby wyświetlić pulpit.
4. Kliknij ikonę ⋮ z profilu dziecka, która chcesz usunąć, a nastepnie wybierz **Usuń**.

13. KONTROLA PRYWATNOŚCI

13.1. Co mogę zrobić, aby moje transakcje online były bezpieczne?

Aby upewnić się, że Twoje operacje online pozostaną prywatne, można używać przeglądarki dostarczonej przez produkt Bitdefender do ochrony transakcji online i aplikacji bankowych.

Moduł Bitdefender Safepay jest bezpieczną przeglądarką, która ma na celu ochronę danych karty kredytowej, numerów konta lub innych poufnych danych podczas korzystania z różnych internetowych lokalizacji.

Aby utrzymać swoją aktywność online prywatną i bezpieczną:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij przycisk akcji **Safepay**.
3. Kliknij przycisk , aby uzyskać dostęp do **klawiatury wirtualnej**.

   Użyj **klawiatury wirtualnej** podczas wpisywania poufnych informacji, takich jak hasła.

13.2. Jak przy pomocy Bitdefender usunąć plik na stałe?

Jeśli chcesz usunąć plik na stałe z systemu, trzeba fizycznie usunąć dane z dysku twardego.

Niszczarka plików Bitdefender pomoże Ci szybko zniszczyć pliki i foldery, korzystając z menu kontekstowego Windows, wykonując następujące kroki:

1. Kliknij prawym przyciskiem myszy plik lub katalog, który chcesz trwale usunąć, wskaż Bitdefender i wybierz **Niszczarka plików**.
2. Pojawia się okno potwierdzające. Kliknij "**Tak, USUŃ**", aby uruchomić kreator Niszczarki plików.

   Poczekaj, aż Bitdefender zakończy niszczenie plików.
3. Wyniki są wyświetlane. Kliknij "**Zakończ**", aby wyjść z kreatora.

13.3. Jak zabezpieczyć moją kamerę przed włamaniem?

Możesz ustawić produkt Bitdefender aby zezwolić lub odmówić dostępu zainstalowanych aplikacji to twojej kamery, przez postępowanie według kroków:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W panelu **OCHRONA KAMERY**, kliknij **Dopuszczone Kamery**.

   Lista z aplikacjami, które prosiły o dostęp to twojej kamery jest wyświetlona.
4. Wskaż aplikacje, której chcesz pozwolić na dostęp lub go odebrać i kliknij odpowiedni przełącznik.

   Aby sprawdzić, co inni użytkownicy Bitdefender, zdecydowali się zrobić z wybraną aplikacją, kliknij ikonę . Będziesz powiadamiany za każdym razem, kiedy jedna z wylistowanych aplikacji jest zablokowana przez użytkowników Bitdefender, nieważnie od statusu Autopilota.

Aby ręcznie dodać aplikacje do tej listy, kliknij link **Dodaj aplikacje do listy**.

Notatka

Kiedy aplikacje Windows Store uruchamiają się jako pojedynczy proces, za każdym razem kiedy dostęp aplikacji jest ustawiony na Zezwól lub Zablokuj, reguła będzie przypisana do całego systemu. Internet Explorer i Microsoft Edge to dwa przykłady takich aplikacji.

14. PRZYDATNE INFORMACJE

14.1. W jaki sposób mogę przetestować mój program antywirusowy?

Aby upewnić się, że produkt Bitdefender funkcjonuje poprawnie, zalecamy przeprowadzenie testu EICAR.

Test EICAR pozwala na sprawdzenie ochrony antywirusowej z wykorzystaniem bezpiecznego pliku, stworzonego specjalnie do takich zadań.

Aby przetestować Twoje rozwiązanie antywirusowe:

1. Pobierz plik testowy z oficjalnej strony organizacji EICAR http://www.eicar.org/.
2. Kliknij zakładkę **Antywirusowy plik testowy**.
3. Kliknij **Pobierz** w menu po lewej stronie.
4. Z obszaru **pobierania z wykorzystaniem standardowego protokołu http** wybierz plik testowy **eicar.com**.
5. Zostaniesz poinformowany, że strona, którą próbujesz otworzyć, zawiera wirusa testowego EICAR-Test-File.

   Kiedy klikniesz **Rozumiem ryzyko, mimo to otwórz stronę**, rozpocznie się pobieranie pliku testowego, a okno wyskakujące produktu Bitdefender wyświetli komunikat informujący o wykryciu wirusa.

   Kliknij **Szczegóły**, aby dowiedzieć się więcej o tym działaniu.

Jeżeli Bitdefender nie wyświetla żadnych powiadomień, radzimy skontaktować się z działem pomocy technicznej Bitdefender, tak jak opisane zostało to w sekcji *„Prośba o pomoc”* (p. 219).

14.2. W jaki sposób usunąć Bitdefender?

Jeśli chcesz usunąć swój Bitdefender Internet Security 2018:

- W systemie **Windows 7**:
  1. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
  2. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

3. Kliknij **USUŃ** w oknie, które się pojawi.
4. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

- W systemach **Windows 8 i Windows 8.1**:

1. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
2. Kliknij **Odinstaluj program** lub **Programy i funkcje**.
3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **USUŃ** w oknie, które się pojawi.
5. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

- W systemie **Windows 10**:

1. Kliknij **Start**, a następnie kliknij Ustawienia.
2. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.
3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.
5. Kliknij **USUŃ** w oknie, które się pojawi.
6. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

Notatka
Ta procedura ponownej instalacji spowoduje trwałe usunięcie dostosowanych ustawień.

14.3. Jak automatycznie wyłączyć komputer po zakończeniu skanowania?

Bitdefender oferuje wiele zadań skanowania, które można wykorzystać, aby upewnić się czy system nie jest zainfekowany złośliwym oprogramowaniem. Skanowanie całego komputera może zająć dłuższy czas, w zależności od konfiguracji sprzętowej i oprogramowania.

Z tego powodu Bitdefender umożliwia taka konfigurację Bitdefender, która pozwoli automatycznie wyłączyć komputer po zakończeniu skanowania.

Rozważmy następujący przykład: kończysz pracę na komputerze i chcesz iść spać. Chcesz sprawdzić programem Bitdefender cały system w poszukiwaniu złośliwego oprogramowania.

Oto w jaki sposób można ustawić Bitdefender, aby wyłączyć system po zakończeniu skanowania:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYWIRUS**, wybierz **Zarządzanie Skanowaniem**.
4. W oknie **Zarządzaj Zadaniami Skanowania**, kliknij **Nowe zadanie niestandardowe**, aby wprowadzić nazwę dla skanowania i wybierz lokalizacje, które mają być skanowane.
5. Jeśli chcesz skonfigurować szczegółowe opcje skanowania, wybierz zakładkę **Zaawansowane**.
6. Wybierz opcję wyłączenia komputera po zakończeniu skanowania, jeśli nie znaleziono zagrożeń.
7. Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.
8. Kliknij przycisk **Rozpocznij Skanowanie**, aby przeskanować swój system.

Jeśli zagrożenia nie zostaną odnalezione, komputer zostanie wyłączony.

Jeśli pozostaną nierozwiązane zagrożenia, zostaniesz poproszony o wybranie działań, jakie względem nich zostaną podjęte. Aby uzyskać więcej informacji, odwołaj się do *„Kreator skanowania antywirusowego"* (p. 98).

14.4. Jak skonfigurować Bitdefender, aby używał połączenia z internetem przez serwer proxy?

Jeśli Twój komputer łączy się z internetem przez serwer proxy, musisz skonfigurować ustawienia proxy dla produktu Bitdefender. Zwykle Bitdefender automatycznie wykrywa i importuje z systemu ustawienia proxy.

WAŻNE

Domowe połączenia internetowe nie używają zwykle serwera proxy. Z zasady musisz sprawdzać i konfigurować ustawienia połączeń proxy Twojego

programu Bitdefender, jeśli aktualizacje nie działają. Jeśli Bitdefender jest w stanie przeprowadzić aktualizację, oznacza to, że jest on poprawnie skonfigurowany, żeby łączyć się z internetem.

Aby zarządzać ustawieniami proxy:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Zaawansowane**.
3. Włącz korzystanie z serwera proxy, klikając odpowiedni przełącznik.
4. Kliknij link "**Zarządzaj proxy**".
5. Są dwa sposoby na zmianę ustawień proxy:
   - **Importuj ustawienia proxy z domyślnej przeglądarki** - ustawienia proxy dla obecnego użytkownika pobrane z domyślnej przeglądarki internetowej. Jeśli serwer proxy wymaga nazwy użytkownika i hasła, musisz podać je w odpowiednich polach.

     Notatka
     Bitdefender może zaimportować ustawienia proxy z większości popularnych przeglądarek, włączając najnowsze wersje przeglądarek Microsoft Edge, Internet Explorer, Mozilla Firefox oraz Google Chrome.

   - "**Własne ustawienia proxy**" - ustawienia proxy, które możesz skonfigurować sam. Następujące ustawienia muszą zostać podane:
     - **Adres** - wpisz adres IP serwera proxy.
     - **Port** - wpisz port, którego Bitdefender używa do łączenia się z serwerem proxy.
     - **Nazwa użytkownika** - wpisz nazwę użytkownika rozpoznawanego przez proxy.
     - **Hasło proxy** - wpisz poprawne hasło dla wcześniej podanego użytkownika.
6. Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.

Bitdefender będzie korzystać z dostępnych ustawień proxy, dopóki nie uzyska połączenia z internetem.

14.5. Mój system Windows jest w wersji 32- czy 64-bitowej?

Aby sprawdzić czy masz 32 lub 64 bitowy system operacyjny:

- W systemie **Windows 7**:
  1. Kliknij **Start**.
  2. W menu **Start** znajdź **Komputer**.
  3. Kliknij prawym przyciskiem myszy na **Komputer** i wybierz **Właściwości**.
  4. W polu **System** sprawdź informacje na temat systemu.
- W systemie **Windows 8**:
  1. Na ekranie menu Start systemu Windows zlokalizuj **Komputer** (przykładowo, możesz zacząć pisać "Komputer" bezpośrednio na ekranie menu Start), a następnie kliknij jego ikonę.

     W systemie **Windows 8.1**, zlokalizuj **Ten Komputer**.
  2. Wybierz **Właściwości** w dolnym menu.
  3. Zajrzyj do obszaru Systemu, aby zobaczyć swój typ systemu.
- W systemie **Windows 10**:
  1. Wpisz "System" w polu wyszukiwania z paska zadań, a następnie kliknij jego ikonę.
  2. Zajrzyj do obszaru Systemu, aby znaleźć informacje o rodzaju systemu.

14.6. Jak wyświetlić ukryte obiekty w systemie Windows?

Kroki te są przydatne w tych przypadkach, gdy ma się do czynienia ze złośliwym oprogramowaniem i trzeba odnaleźć i usunąć zainfekowane pliki, które mogą być ukryte.

Aby pokazać obiekty ukryte w systemie Windows, wykonaj następujące kroki:

1. Kliknij **Start** i przejdź do **Panelu sterowania**.

   W systemie **Windows 8 i Windows 8.1**: na ekranie Start zlokalizuj **Panel sterowania** (przykładowo, zacznij wpisywać "Panel sterowania" bezpośrednio na ekranie Start), a następnie kliknij na jego ikonie.

2. Wybierz **Opcje folderów**.
3. Przejdź do zakładki **Widok**.
4. Wybierz **Pokaż ukryte pliki i foldery**.
5. Usuń zaznaczenie z pola **Ukryj rozszerzenia znanych typów plików**.
6. Usuń **Ukryj chronione pliki systemu operacyjnego**.
7. Kliknij **Zastosuj**, a następnie kliknij **OK**.

W systemie **Windows 10**:

1. Wpisz "Pokaż ukryte pliki i foldery" w polu wyszukiwania z paska zadań, a następnie kliknij jego ikonę.
2. Wybierz **Pokaż ukryte pliki, foldery i dyski**.
3. Usuń zaznaczenie z pola **Ukryj rozszerzenia znanych typów plików**.
4. Usuń **Ukryj chronione pliki systemu operacyjnego**.
5. Kliknij **Zastosuj**, a następnie kliknij **OK**.

14.7. Jak usunąć inne rozwiązania bezpieczeństwa?

Głównym powodem używania rozwiązań bezpieczeństwa jest możliwość zapewnienia ochrony i bezpieczeństwa danym. Co dzieje się, gdy w systemie znajduje się więcej niż jeden produkt zabezpieczający?

Gdy na jednym komputerze uruchomione jest więcej niż jedno rozwiązanie bezpieczeństwa, system staje się niestabilny. Instalator Bitdefender Internet Security 2018 automatycznie wykrywa inne programy zabezpieczające i oferuje możliwość ich deinstalacji.

Jeśli podczas instalacji nie usuniesz innych rozwiązań bezpieczeństwa,

- W systemie **Windows 7**:
  1. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
  2. Poczekaj chwilę, aż wyświetlona zostanie lista zainstalowanych programów.
  3. Znajdź nazwę programu, który chcesz usunąć i wybierz **Odinstaluj**.
  4. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

- W systemach **Windows 8 i Windows 8.1**:
  1. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
  2. Kliknij **Odinstaluj program** lub **Programy i funkcje**.
  3. Poczekaj chwilę, aż wyświetlona zostanie lista zainstalowanych programów.
  4. Znajdź nazwę programu, który chcesz usunąć i wybierz **Odinstaluj**.
  5. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
- W systemie **Windows 10**:
  1. Kliknij **Start**, a następnie kliknij Ustawienia.
  2. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.
  3. Znajdź nazwę programu, który chcesz usunąć i wybierz **Odinstaluj**.
  4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.
  5. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

Jeśli nie usuniesz z systemu innego rozwiązania bezpieczeństwa, pobierz narzędzie deinstalacji z witryny sieciowej swojego sprzedawcy lub skontaktuj się z nim bezpośrednio, w celu uzyskania informacji na ten temat.

14.8. Jak uruchomić ponownie komputer w Trybie awaryjnym?

Tryb awaryjny to tryb działania diagnostycznego używany głównie do rozwiązywania problemów, które mają wpływ na normalną pracę systemu Windows. Tego rodzaju problemy mogą być wywołane przez problemy ze sterownikami lub wirusy blokujące normalne uruchamianie systemu Windows. W Trybie awaryjnym działa tylko kilka aplikacji, a system Windows wczytuje jedynie podstawowe sterowniki i minimalną liczbę składników systemu operacyjnego. Oto dlaczego w Trybie awaryjnym większość wirusów nie jest aktywna i może być łatwo usunięta.

Uruchamianie systemu Windows w Trybie awaryjnym:

- W systemie **Windows 7**:
  1. Uruchom ponownie komputer.
  2. Aby przejść do menu uruchamiania, naciśnij kilka razy klawisz **F8** przed załadowaniem systemu Windows.
  3. Wybierz "**Tryb awaryjny**" z menu uruchamiania lub "**Tryb awaryjny z obsługą sieci**", jeśli potrzebujesz dostępu do sieci.
  4. Naciśnij klawisz **Enter** i poczekaj, aż system Windows uruchomi się w Trybie awaryjnym.
  5. Proces ten kończy się wiadomością potwierdzającą. Kliknij **OK**, aby potwierdzić.
  6. Aby uruchomić system Windows normalnie, po prostu uruchom system ponownie.
- W systemach **Windows 8, Windows 8.1 i Windows 10**:
  1. Uruchom **Konfiguracje Systemu** w Windowsie przez naciśniecie **Windows+R** jednocześnie na klawiaturze.
  2. Wpisz **msconfig** w oknie dialogowym **Otwórz** a następnie naciśnij **OK**
  3. Wybierz zakładkę **Start systemu**.
  4. W obszarze **Opcje rozruchu**, wybierz **Bezpieczne uruchomienie**
  5. Kliknij **Sieć**, a następnie **OK**.
  6. Kliknij **OK** w oknie **Konfiguracji Systemu**, które informuje, że system musi zostać uruchomiony ponownie, aby wprowadzić nowe ustawienia.

     Twój system uruchomia się ponownie w trybie awaryjnym z obsługą sieci.

  Aby przywrócić komputer do normalnego trybu, wyłącz poprzednie ustawienia poprzez uruchomienie **Konfiguracji Systemu** oraz odznaczenie opcji **Rozruch bezpieczny** Kliknij **OK**, a następnie **Restartuj**. Czekaj aż nowe ustawienia zostaną zastosowane.

ZARZĄDZANIE BEZPIECZEŃSTWEM

15. OCHRONA ANTYWIRUSOWA

Bitdefender chroni Twój komputer przed wszystkimi rodzajami zagrożeń (wirusy, trojany, spyware, rootkity itd.). Ochrona Bitdefender jest podzielona na dwie kategorie:

- Skanowanie dostępowe - nie dopuszcza, aby nowe szkodliwe oprogramowanie dostało się do Twojego systemu. Na przykład Bitdefender przeskanuje dokument Word, kiedy go otworzysz, oraz wiadomość e-mail, kiedy ją otrzymasz.

  Skanowanie w czasie rzeczywistym zapewnia ochronę przed szkodliwym oprogramowaniem w czasie rzeczywistym, stanowiąc podstawowy komponent każdego programu chroniącego komputer.

  WAŻNE
  Aby uniemożliwić wirusom zainfekowanie Twojego komputera, opcja **skanowanie w czasie rzeczywistym** powinna być aktywna.

- Skanowanie na żądanie - pozwala wykrywać i usuwać złośliwe oprogramowanie znajdujące się już w systemie. Jest to klasyczne skanowanie wirusów zainicjowane przez użytkownika – wybierasz jaki dysk, folder lub plik Bitdefender ma skanować, a Bitdefender skanuje go na żądanie.

Bitdefender automatycznie skanuje wszelkie wymienne nośniki danych podłączone do komputera, aby można było bezpiecznie ich używać. Aby uzyskać więcej informacji, odwołaj się do *„Automatyczne skanowanie wymiennych nośników danych"* (p. 102).

Zaawansowani użytkownicy mogą skonfigurować wyjątki, aby pominąć określone pliki lub typy plików podczas skanowania. Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie wyjątków skanowania"* (p. 105).

W przypadku wykrycia wirusa lub innego złośliwego oprogramowania, Bitdefender dokona automatycznej próby usunięcia kodu złośliwego oprogramowania z zainfekowanego pliku i odtworzenia oryginalnego pliku. Ta operacja określana jest mianem oczyszczania. Pliki, których nie można wyleczyć, są poddawane kwarantannie, aby powstrzymać infekcję. Aby uzyskać więcej informacji, odwołaj się do *„Zarządzanie plikami w kwarantannie"* (p. 108).

Jeśli komputer został zainfekowany złośliwym oprogramowaniem, zapoznaj się z informacjami w *„Usuwanie szkodliwego oprogramowania z systemu"* (p. 208). Aby pomóc Ci w pozbyciu się szkodliwego oprogramowania, które nie może zostać usunięte z uruchomionego systemu Windows, Bitdefender posiada funkcję*„Bitdefender Tryb Ratunkowy (Środowisko Ratunkowe w Windows 10)"* (p. 208). To zaufane środowisko, zaprojektowane specjalnie w celu usuwania szkodliwego oprogramowania, umożliwia uruchomienie komputera bez uruchamiania systemu Windows. Kiedy komputer działa w Trybie ratunkowym (Środowisko Ratunkowe w Windows 10), szkodliwe oprogramowanie nie jest aktywne, więc łatwo je usunąć.

15.1. Skanowanie dostępowe (ochrona w czasie rzeczywistym)

Bitdefender zapewnia ciągłą ochronę w czasie rzeczywistym przed szerokim zakresem zagrożeń, poprzez skanowanie wszystkich plików oraz wiadomości e-mail.

15.1.1. Włączanie lub wyłączanie ochrony w czasie rzeczywistym

Aby włączyć lub wyłączyć ochronę w czasie rzeczywistym przeciwko malware:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. W oknie **OCHRONA** kliknij przełącznik WŁĄCZ/WYŁĄCZ.
5. Jeśli chcesz wyłączyć ochronę w czasie rzeczywistym, pojawia się okno ostrzegawcze. Musisz potwierdzić swój wybór, określając w menu czas, w którym ochrona w czasie rzeczywistym ma być wyłączona. Możesz wyłączyć ochronę w czasie rzeczywistym na 5, 15 lub 30 minut, na godzinę, na stałe lub do czasu następnego uruchomienia systemu. Ochrona w czasie rzeczywistym zostanie włączona automatycznie po upływie zdefiniowanego czasu.

Ostrzeżenie
To jest krytyczne zagadnienie bezpieczeństwa. Zalecamy wyłączanie ochrony w czasie rzeczywistym na tak krótko, jak to tylko możliwe. Jeśli ochrona w czasie rzeczywistym jest wyłączona, nie będziesz chroniony przed zagrożeniami.

15.1.2. Konfigurowanie zaawansowanych ustawień ochrony w czasie rzeczywistym

Profesjonalni użytkownicy mogą chcieć skorzystać z ustawień skanowania, które oferuje Bitdefender. Możesz szczegółowo skonfigurować ochronę w czasie rzeczywistym poprzez utworzenie własnego poziomu ochrony.

Aby skonfigurować zaawansowane ustawienia ochrony w czasie rzeczywistym:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. W oknie **OCHRONA**, kliknij w menu **POKAŻ ZAAWANSOWANE USTAWIENIA**.

   Wyświetlane jest okno.
5. Zjedź niżej, aby skonfigurować ustawienia skanowania, jeśli to potrzebne.

Informacje o opcjach skanowania

Ta informacja może być przydatna:

- Jeśli nie znasz pewnych określeń, sprawdź je w słowniczku. Możesz także uzyskać więcej informacji przeszukując internet.
- **Opcje skanowania dla otwartych plików.** Możesz ustawić Bitdefender tak, aby skanował wyłącznie pliki i aplikacje (pliki programowe), z których korzystasz. Najlepszą ochronę zapewnia skanowanie wszystkich użytych plików, natomiast lepszą wydajność zapewnia skanowanie tylko aplikacji.

  Domyślnie foldery lokalne i udziały sieciowe podlegają skanowaniu w czasie rzeczywistym. Dla lepszej wydajności systemu można wykluczyć lokalizacje sieciowe ze skanowania w czasie rzeczywistym.

Aplikacje (lub pliki programów) są bardziej narażone na ataki złośliwego oprogramowania od plików innego typu. Ta kategoria obejmuje następujące rozszerzenia plików:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Skanowanie wewnątrz archiwów.** Skanowanie wewnątrz archiwów to powolny i zasobożerny proces, który z tego powodu nie jest zalecany do użycia w ochronie w czasie rzeczywistym. Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym.

  Jeśli zdecydujesz się używać tej opcji, włącz ją, a następnie przeciągnij suwak wzdłuż skali, aby ustawić maksymalny dopuszczalny rozmiar (w MB) archiwów skanowanych dostępowo w czasie rzeczywistym.

- **Skanowanie wiadomości e-mail.** Aby uniemożliwić pobieranie złośliwego oprogramowania na Twój komputer, Bitdefender automatycznie skanuje przychodzące i wychodzące wiadomości e-mail.

  Choć nie jest to zalecane, możesz wyłączyć skanowanie antywirusowe poczty e-mail, aby zwiększyć wydajność systemu. Jeśli wyłączysz odpowiednie opcje skanowania, wiadomości e-mail oraz pliki otrzymane lub pobrane z internetu nie będą skanowane. Zainfekowane pliki będą mogły wówczas zostać zapisane na komputerze. Nie jest to poważne zagrożenie, ponieważ ochrona w czasie rzeczywistym blokuje złośliwe oprogramowanie, gdy zainfekowane pliki są otwierane, przenoszone, kopiowane lub uruchamiane.

- **Skanowanie sektorów startowych.** Możesz ustawić Bitdefender tak, aby skanował sektory rozruchowe dysku twardego. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu rozruchu. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
- **Skanowanie tylko nowych i zmienionych plików.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Skanuj w poszukiwaniu keyloggerów.** Wybierz tę opcję, aby skanować system w poszukiwaniu aplikacji typu keylogger. Keyloggery zapisują to, co wpiszesz na klawiaturze i wysyłają raporty przez internet do hakera. Haker może poznać ważne informacje z ukradzionych danych, takie jak numer i hasło do konta bankowego i użyć ich na własną korzyść.
- **Skanowanie podczas startu systemu.** Wybierz opcje **skan przy rozruchu** aby skanować system przy starcie jak tylko załaduję się wszystkie kluczowe usługi. Zadaniem tej funkcji jest poprawa wykrywania wirusów przy starcie systemu i czasu uruchamiania systemu.

Działania podjęte wobec wykrytego szkodliwego oprogramowania

Można skonfigurować działania podejmowane przez ochronę w czasie rzeczywistym, postępując według następujących kroków:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. W oknie **OCHRONA**, kliknij w menu **POKAŻ ZAAWANSOWANE USTAWIENIA**.

   Wyświetlane jest okno.
5. Zjedź niżej aż zobaczysz opcję **Działania po zakończeniu skanowania**.
6. Skonfiguruj ustawienia skanowania według uznania.

Następujące działania mogą być podjęte przez ochronę w czasie rzeczywistym w Bitdefender:

Podejmij odpowiednie działania

Bitdefender podejmie zalecane działania w zależności od typu wykrytego pliku:

- **Pliki zainfekowane.** Pliki, w których wykryto infekcje, są zgodne z sygnaturami w Bazie Danych Sygnatur Złośliwego Oprogramowania Bitdefender. Bitdefender podejmie automatyczną próbę usunięcia złośliwego kodu z zainfekowanego pliku i przywrócenia pierwotnego pliku. Ta operacja określana jest mianem oczyszczania.

  Pliki, których nie można wyleczyć, są poddawane kwarantannie, aby powstrzymać infekcję. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Aby uzyskać więcej informacji, odwołaj się do *„Zarządzanie plikami w kwarantannie"* (p. 108).

  WAŻNE

  W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

- **Podejrzane pliki.** Pliki są wykrywane jako podejrzane przez analizę heurystyczną. Podejrzanych plików nie można leczyć, ponieważ brak jest służących do tego procedur. Zostaną one przeniesione do kwarantanny, aby zapobiec potencjalnej infekcji.

  Pliki poddane kwarantannie są domyślnie wysyłane do laboratoriów firmy Bitdefender w celu analizy szkodliwego oprogramowania dokonywanej przez analityków Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

- **Archiwa zawierające zainfekowane pliki.**
  - Archiwa zawierające jedynie zainfekowane pliki są usuwane automatycznie.
  - Jeśli archiwum zawiera zarówno pliki zainfekowane, jak i czyste, to Bitdefender podejmie próbę usunięcia plików zainfekowanych pod warunkiem, że będzie mógł odtworzyć archiwum z czystymi plikami. Jeśli przywrócenie archiwum jest niemożliwe, zostaniesz poinformowany o braku możliwości podjęcia jakiegokolwiek działania z uwagi na ryzyko utraty czystych plików.

Przenieś pliki do kwarantanny

Przenosi pliki wykryte jako zainfekowane do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Aby uzyskać więcej informacji, odwołaj się do *„Zarządzanie plikami w kwarantannie”* (p. 108).

Blokuj dostęp

W przypadku wykrycia zainfekowanego pliku dostęp do niego zostanie zablokowany.

15.1.3. Przywracanie ustawień domyślnych

Domyślne ustawienia ochrony w czasie rzeczywistym zapewniają dobrą ochronę przed złośliwym oprogramowaniem, a jednocześnie wywierają tylko niewielki wpływ na wydajność systemu.

Przywracanie domyślnych ustawień ochrony w czasie rzeczywistym:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. W oknie **OCHRONA**, kliknij w menu **POKAŻ ZAAWANSOWANE USTAWIENIA**.

   Wyświetlane jest okno.
5. Zjedź niżej, aż zobaczysz opcję **Resetuj ustawienia**. Zaznacz tę opcję, aby zresetować ustawienia antywirusa do ustawień domyślnych.

15.2. Skanowanie na żądanie

Głównym zadaniem Bitdefender jest zabezpieczenie Twojego komputera przed wirusami. Wykonuje się to przez powstrzymywanie nowych wirusów przed wniknięciem do komputera oraz dzięki skanowaniu wiadomości e-mail i wszystkich nowych plików pobranych lub skopiowanych do systemu.

Istnieje ryzyko, że wirus już umiejscowił się w systemie, zanim zainstalowałeś Bitdefender. Dlatego też ważne jest przeskanowanie Twojego komputera po zainstalowaniu Bitdefender w poszukiwaniu rezydentnych wirusów. Ponadto zdecydowanie ważne również jest regularne skanowanie komputera na obecność wirusów.

Skanowanie na żądanie oparte jest na zadaniach skanowania. Zadania skanowania określają opcje skanowania i elementy do przeskanowania. Komputer przeskanować można w dowolnej chwili, uruchamiając zadania domyślne albo niestandardowe (zadania zdefiniowane przez użytkownika). Jeśli chcesz przeskanować konkretną lokalizację lub skonfigurować opcje skanowania, ustaw i uruchom własne skanowanie.

15.2.1. Skanowanie pliku lub folderu w poszukiwaniu szkodliwego oprogramowania

Pliki i foldery należy skanować zawsze, gdy istnieje podejrzenie, że są zainfekowane. Kliknij prawym przyciskiem myszy plik lub folder, który ma być przeskanowany, wskaż **Bitdefender** i wybierz opcję **Skanuj z Bitdefender**. Wyświetlony zostanie Kreator skanowania antywirusowego, który przeprowadzi Cię przez proces skanowania. Na koniec skanowania zostaniesz poproszony o wybranie działania, które zostanie wykonane względem wykrytych plików, jeśli takowe wystąpią.

15.2.2. Uruchamianie szybkiego skanowania

Do wykrywania w systemie złośliwego oprogramowania zadanie szybkiego skanowania wykorzystuje skanowanie w chmurze. Wykonanie szybkiego skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.

Aby uruchomić Szybkie Skanowanie:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYWIRUS**, wybierz **Szybkie Skanowanie**.
4. Kliknij "Kreator skanowania antywirusowego", aby ukończyć skanowanie. Bitdefender automatycznie podejmie zalecane działania względem wykrytych plików. Jeśli pozostaną nierozwiązane zagrożenia, zostaniesz poproszony o wybranie działań, jakie względem nich zostaną podjęte.

Lub szybciej, kliknij ikonę na lewym paskuInterfejsu Bitdefender, następnie kliknij przycisk **Szybkiego Skanowania**

15.2.3. Uruchamianie Skanowania systemu

Zadanie Skanowania systemu skanuje cały komputer w poszukiwaniu wszystkich rodzajów złośliwego oprogramowania zagrażającego bezpieczeństwu użytkownika, takich jak wirusy, oprogramowanie typu spyware i adware, rootkity i inne.

Notatka

Ponieważ **Skanowanie systemu** wykonuje dokładne skanowanie całego systemu, zadanie skanowania może chwilę potrwać. Zatem zaleca się uruchamianie tego zadania, kiedy nie używasz komputera.

Zanim uruchomisz Skanowanie systemu, zalecane jest:

- Upewnij się, że produkt Bitdefender jest zaktualizowany wraz z jego sygnaturami szkodliwego oprogramowania. Skanowanie komputera w momencie posiadania nieaktualnych sygnatur wirusów może spowodować niewykrycie przez Bitdefender nowego szkodliwego oprogramowania, które mogło się pojawić od czasu ostatniej aktualizacji. Aby uzyskać więcej informacji, odwołaj się do *„Dbanie o aktualizacje Bitdefender"* (p. 43).
- Zamknij wszystkie otwarte programy.

Jeśli chcesz przeskanować konkretną lokalizację lub skonfigurować opcje skanowania, ustaw i uruchom skanowanie niestandardowe. Aby uzyskać więcej informacji, odwołaj się do *„Konfiguracja skanowania niestandardowego"* (p. 95).

Aby uruchomić Skanowanie Systemu:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYWIRUS** wybierz **Skanowanie Systemu**.
4. Kliknij "Kreator skanowania antywirusowego", aby ukończyć skanowanie. Bitdefender automatycznie podejmie zalecane działania względem wykrytych plików. Jeśli pozostaną nierozwiązane zagrożenia, zostaniesz poproszony o wybranie działań, jakie względem nich zostaną podjęte.

15.2.4. Konfiguracja skanowania niestandardowego

Aby skonfigurować szczegóły niestandardowego skanowania i je uruchomić:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYWIRUS**, wybierz **Zarządzanie Skanowaniem**.
4. Kliknij przycisk **Nowe zadanie niestandardowe**. W zakładce **Podstawowe** wprowadź nazwę skanowania i wybierz obiekty, które mają być przeskanowane.
5. Jeśli chcesz skonfigurować szczegółowe opcje skanowania, wybierz zakładkę **Zaawansowane**. Pojawi się nowe okno. Wykonaj następujące kroki:

   a. Opcje skanowania można z łatwością konfigurować poprzez dostosowanie poziomu skanowania. Aby ustawić wybrany poziom skanowania, przeciągnij suwak wzdłuż skali. Użyj opisów po prawej stronie skali, aby określić poziom skanowania najlepiej spełniający Twoje wymagania.

   Profesjonalni użytkownicy mogą chcieć skorzystać z ustawień skanowania, które oferuje Bitdefender. Aby skonfigurować szczegóły opcji skanowania, kliknij **Niestandardowe**. Więcej informacji na ich temat znajduje się pod koniec tej sekcji.

   b. Skonfigurować można także następujące opcje ogólne:

   - **Uruchom zadanie z niskim priorytetem. .** Obniża priorytet procesu skanowania. Umożliwisz innym programom szybszą pracę i zwiększysz czas potrzebny na zakończenie skanowania.
   - **Minimalizuj kreator skanowania do zasobnika systemowego. .** Minimalizuje okno skanowania do zasobnika systemowego. Kliknij dwukrotnie ikonę Bitdefender, aby otworzyć okno skanowania.
   - Określ działanie, które zostanie podjęte w przypadku nieznalezienia zagrożenia.

   c. Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.

6. Jeśli chcesz ustawić harmonogram dla zadania skanowania, użyj przełącznika **Harmonogram** w oknie **Podstawowym**. Wybierz jedną z odpowiednich opcji, aby ustalić harmonogram:

   - Przy uruchomieniu systemu
   - Raz

- Okresowo

7. Kliknij "**Uruchom skanowanie**" i użyj "Kreatora skanowania antywirusowego", aby ukończyć skanowanie. W zależności od lokalizacji do przeskanowania, czynność może zająć więcej czasu. Na koniec skanowania zostaniesz poproszony o wybranie działania, które zostanie wykonane względem wykrytych plików, jeśli takowe wystąpią.
8. Jeśli chcesz, możesz szybko ponownie uruchomić poprzednie własne skanowanie poprzez kliknięcie odpowiedniego wpisu na dostępnej liście.

Informacje o opcjach skanowania

Ta informacja może być przydatna:

- Jeśli nie znasz pewnych określeń, sprawdź je w słowniczku. Możesz także uzyskać więcej informacji przeszukując internet.
- **Skanowanie plików.** Możesz ustawić Bitdefender tak, aby skanował wszystkie rodzaje plików lub jedynie aplikacje (pliki programów). Najlepszą ochronę zapewnia skanowanie wszystkich plików, natomiast skanowanie jedynie aplikacji jest szybsze.

  Aplikacje (lub pliki programów) są bardziej narażone na ataki złośliwego oprogramowania od plików innego typu. Ta kategoria obejmuje następujące rozszerzenia plików: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Opcje skanowania archiwów.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym. Zaleca się użycie tej opcji, w celu wykrycia

i usunięcia wszelkich potencjalnych zagrożeń, nawet jeśli nie jest to zagrożenie bezpośrednie.

Notatka
Skanowanie zarchiwizowanych plików wydłuża ogólny czas skanowania i wymaga więcej zasobów systemowych.

- **Skanowanie sektorów startowych.** Możesz ustawić Bitdefender tak, aby skanował sektory rozruchowe dysku twardego. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu rozruchu. Po zainfekowaniu sektora rozruchowego przez wirusa, możesz utracić dostęp do napędu, przez co uruchomienie systemu i uzyskanie dostępu do danych stanie się niemożliwe.
- **Skanowanie pamięci.** Wybierz tę opcję, aby przeskanować programy działające w pamięci Twojego systemu.
- **Skanowanie rejestru.** Włącz tę opcję, aby skanować klucze rejestru. Rejestr systemu Windows jest bazą danych przechowującą ustawienia konfiguracji i opcje dla komponentów systemu operacyjnego Windows oraz dla zainstalowanych aplikacji.
- **Skanowanie ciasteczek.** Wybierz tę opcję, aby przeskanować ciasteczka zapisane w Twojej przeglądarce.
- **Skanowanie tylko nowych i zmienionych plików.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Ignoruj komercyjne keyloggery.** Wybierz tę opcję, jeżeli na komputerze masz zainstalowane komercyjne keyloggery, z których korzystasz. Komercyjne keyloggery to legalne oprogramowanie komputerowe, którego głównym zadaniem jest monitorowanie tego, co pisane jest na klawiaturze.
- **Skanowanie w poszukiwaniu rootkitów.** Zaznacz tę opcję, aby skanować w poszukiwaniu rootkitów i ukrytych obiektów, które korzystają z tego rodzaju oprogramowania.

15.2.5. Kreator skanowania antywirusowego

Gdy w dowolnym momencie rozpoczniesz skanowanie na żądanie (np. klikniesz prawym przyciskiem myszy na folder, wskażesz Bitdefender i

wybierzesz **Skanuj z Bitdefender**), pojawi się Kreator skanowania antywirusowego Bitdefender. Użyj kreatora, aby ukończyć skanowanie.

Notatka

Jeśli kreator nie pojawi się, może to oznaczać że został skonfigurowany tak, aby skanować w tle. Szukaj ikony z postępem skanowania w zasobniku systemowym. Możesz kliknąć tą ikonę, aby otworzyć okno skanowania i zobaczyć jego postępy.

Krok 1 - Rozpocznij skanowanie

Bitdefender rozpocznie skanowanie zaznaczonych elementów. Możesz widzieć informacje podawane w czasie rzeczywistym, dotyczące stanu skanowania i statystyk (w tym czasu, który upłynął, szacowanego pozostałego czasu oraz liczby wykrytych zagrożeń).

Zaczekaj, aż Bitdefender zakończy skanowanie. Proces skanowania może chwilę potrwać, w zależności od złożoności skanowania.

Przerywanie lub zatrzymywanie skanowania. Możesz przerwać skanowanie w każdej chwili poprzez naciśnięcie przycisku **Stop**. Przejdziesz bezpośrednio do ostatniego kroku kreatora. Aby tymczasowo wstrzymać proces skanowania, kliknij **Wstrzymaj**. Będziesz musiał kliknąć **Wznów**, aby wznowić skanowanie.

Archiwa chronione hasłem. W przypadku wykrycia archiwum chronionego hasłem, w zależności od ustawień skanowania możesz otrzymać monit o podanie hasła. Archiwa chronione hasłem nie mogą być skanowane, chyba że podasz hasło. Dostępne są następujące opcje:

- **Hasło.** Jeśli chcesz, aby Bitdefender przeskanował archiwum, wybierz tę opcję i podaj hasło. Jeśli nie znasz hasła, wybierz jedną z pozostałych opcji.
- **Nie pytaj o hasło i pomiń ten obiekt podczas skanowania.** Wybierz tę opcję, aby pominąć skanowanie tego archiwum.
- **Pomiń skanowanie wszystkich obiektów chronionych hasłem.** Wybierz tę opcję, jeśli nie chcesz być pytany o archiwa zabezpieczone hasłem. Bitdefender nie będzie w stanie ich skanować, ale informacja na ich temat zostanie zostanie zapisana w dzienniku skanera.

Wybierz daną opcję i kliknij "**OK**", aby kontynuować skanowanie.

Krok 2 - Wybierz działania

Na koniec skanowania zostaniesz poproszony o wybranie działania, które zostanie wykonane względem wykrytych plików, jeśli takowe wystąpią.

Notatka

Gdy przeprowadzasz szybkie skanowanie lub pełne skanowanie systemu,Bitdefender automatycznie podejmie zalecane działania względem plików wykrytych podczas skanowania. Jeśli pozostaną nierozwiązane zagrożenia, zostaniesz poproszony o wybranie działań, jakie względem nich zostaną podjęte.

Zainfekowane elementy wyświetlane są w grupach, w zależności od rodzaju infekcji. Kliknij link dotyczący zagrożenia, aby dowiedzieć się więcej na jego temat.

Możesz wybrać ogólne działanie dla wszystkich zagadnień lub wybrać oddzielne działanie dla każdej grupy. Jedna z kilku następujących opcji może pojawić się w menu:

Podejmij odpowiednie działania

Bitdefender podejmie zalecane działania w zależności od typu wykrytego pliku:

- **Pliki zainfekowane.** Pliki, w których wykryto infekcje, są zgodne z sygnaturami w Bazie Danych Sygnatur Złośliwego Oprogramowania Bitdefender. Bitdefender podejmie automatyczną próbę usunięcia złośliwego kodu z zainfekowanego pliku i przywrócenia pierwotnego pliku. Ta operacja określana jest mianem oczyszczania.

  Pliki, których nie można wyleczyć, są poddawane kwarantannie, aby powstrzymać infekcję. Pliki w kwarantannie nie mogą być uruchomione ani otwarte - teoretycznie, ryzyko zainfekowania nimi znika. Aby uzyskać więcej informacji, odwołaj się do *„Zarządzanie plikami w kwarantannie”* (p. 108).

  ### WAŻNE

  W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

- **Podejrzane pliki.** Pliki są wykrywane jako podejrzane przez analizę heurystyczną. Podejrzanych plików nie można leczyć, ponieważ brak

jest służących do tego procedur. Zostaną one przeniesione do kwarantanny, aby zapobiec potencjalnej infekcji.

Pliki poddane kwarantannie są domyślnie wysyłane do laboratoriów firmy Bitdefender w celu analizy szkodliwego oprogramowania dokonywanej przez analityków Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

- **Archiwa zawierające zainfekowane pliki.**
  - Archiwa zawierające jedynie zainfekowane pliki są usuwane automatycznie.
  - Jeśli archiwum zawiera zarówno pliki zainfekowane, jak i czyste, to Bitdefender podejmie próbę usunięcia plików zainfekowanych pod warunkiem, że będzie mógł odtworzyć archiwum z czystymi plikami. Jeśli przywrócenie archiwum jest niemożliwe, zostaniesz poinformowany o braku możliwości podjęcia jakiegokolwiek działania z uwagi na ryzyko utraty czystych plików.

Usuń

Usuwa wykryte pliki z dysku.

Jeśli pliki zainfekowane są zapisane w archiwum wraz z czystymi plikami,Bitdefender podejmie próbę usunięcia plików zainfekowanych i odtworzenia archiwum z czystymi plikami. Jeśli przywrócenie archiwum jest niemożliwe, zostaniesz poinformowany o braku możliwości podjęcia jakiegokolwiek działania z uwagi na ryzyko utraty czystych plików.

Nie podejmuj żadnych działań

Żadne działanie nie zostanie podjęte na wykrytych plikach. Po zakończeniu skanowania, możesz otworzyć dziennik skanowania i zobaczyć informacje o tych plikach.

Kliknij **Kontynuuj**, aby zastosować wybrane działanie.

Krok 3 - Podsumowanie

Kiedy Bitdefender zakończy naprawianie zagadnień, w nowym oknie pojawi się rezultat skanowania. Jeśli chcesz uzyskać kompleksowe informacje o procesie skanowania, kliknij **Pokaż dziennik**, aby zobaczyć dziennik skanowania. Dziennik jest dostarczany w formie .xml i może zostać lokalnie zapisany, poprzez kliknięcie przycisku **Zapisz Dziennik**, a następnie wybranie lokacji.

WAŻNE

W większości wypadków Bitdefender leczy zarażone pliki lub izoluje je. Istnieją jednak zagadnienia, których nie można rozwiązać automatycznie. Jeśli będzie to wymagane, proszę zrestartować system, aby zakończyć proces czyszczenia. Więcej informacji na temat ręcznego usuwania złośliwego oprogramowania zawiera *„Usuwanie szkodliwego oprogramowania z systemu"* (p. 208).

15.2.6. Sprawdzanie dzienników skanowania

Za każdym razem, gdy wykonywane jest skanowanie, tworzony jest dziennik skanowania, a Bitdefender rejestruje wykryte problemy w oknie widoku sekcji "Antywirus". Dziennik skanowania zawiera szczegółowe informacje o procesie skanowania, takie jak opcje skanowania, cel skanowania, zagrożenia znalezione i działania wykonane na tych zagrożeniach.

Po zakończeniu skanowania dziennik skanowania można otworzyć bezpośrednio z poziomu kreatora skanowania. Aby to zrobić, kliknij opcję **Pokaż dziennik**.

Aby sprawdzić logi skanowania lub wykrytych infekcji później:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. W zakładce **Wszystko**, zaznacz powiadomienia dotyczące ostatniego skanowania

   Tutaj znajdziesz wszystkie zdarzenia skanowania w poszukiwaniu obecności szkodliwego oprogramowania, włącznie z zagrożeniami wykrytymi przez skanowanie w czasie rzeczywistym, skanowanie zainicjowane przez użytkownika oraz zmiany stanu skanowania automatycznego.
3. Na liście powiadomień, możesz sprawdzić jakie skanowanie zostało ostatnio wykonane. Kliknij powiadomienie, aby dowiedzieć się więcej na jego temat.
4. Aby otworzyć plik dziennika skanowania, kliknij "**Pokaż dziennik**".

15.3. Automatyczne skanowanie wymiennych nośników danych

Bitdefender automatycznie wykrywa podłączenie wymiennego nośnika danych do komputera i skanuje go w tle, gdy opcja Automatycznego

Skanowania jest włączona. Jest to zalecane ze względu na możliwość zainfekowania komputera złośliwym oprogramowaniem.

Wykryte urządzenia są przyporządkowywane do jednej z tych kategorii:

- CD/DVD
- Urządzenia pamięci masowej USB, takie jak flash i zewnętrzne dyski twarde
- mapowane (zdalne) dyski sieciowe

Możesz skonfigurować automatyczne skanowanie oddzielnie dla każdej kategorii urządzenia magazynującego. Automatyczne skanowanie mapowanych dysków sieciowych jest domyślnie wyłączone.

15.3.1. Jak to działa?

Kiedy Bitdefender wykryje przenośne urządzenie magazynujące, zaczyna w tle skanować je pod kątem złośliwego oprogramowania (skanowanie automatyczne jest wyłączone dla takich urządzeń). Ikona skanowania Bitdefender będzie widoczna w zasobniku systemowym. Możesz kliknąć tą ikonę, aby otworzyć okno skanowania i zobaczyć jego postępy.

Jeśli aktywna jest funkcja Autopilota, skanowanie przebiegnie bez Twojego udziału. Skanowanie zostanie zapisane w dzienniku, a informacje o nim dostępne będą w oknie "Powiadomienia".

Jeśli funkcja Autopilota jest wyłączona:

1. Wyskakujące okienko powiadomi Cię, że nowe urządzenia zostały wykryte i są skanowane.
2. Z reguły Bitdefender automatycznie usuwa wykryte szkodliwe oprogramowanie lub izoluje zainfekowane pliki poprzez przeniesienie ich do kwarantanny. Jeśli po skanowaniu pozostały nierozwiązane zagrożenia, zostaniesz poproszony o wybranie czynności, które zostaną na nich przeprowadzone.

Notatka

Zwróć uwagę, że na zainfekowanych lub podejrzanych plikach na nośnikach CD i DVD nie można wykonać żadnych operacji. Analogicznie, bez odpowiednich uprawnień nie można również wykonać żadnych operacji na zainfekowanych lub podejrzanych plikach wykrytych na dyskach sieciowych.

3. Po ukończeniu skanowania pojawia się okno z jego rezultatami i informacją, czy pliki na wymiennych nośnikach danych są bezpieczne.

Te informacje mogą Ci się przydać:

- Zachowaj ostrożność używając nośników CD/DVD zainfekowanych złośliwym oprogramowaniem, ponieważ nie można usunąć z nich złośliwego oprogramowania (są to nośniki tylko do odczytu). Upewnij się, że ochrona w czasie rzeczywistym jest włączona, aby ochraniać Twój system przed atakiem szkodliwego oprogramowania. Zaleca się skopiowanie ważnych danych z płyty na komputer, a następnie zniszczenie płyty.
- W niektórych przypadkach Bitdefender może nie być w stanie usunąć szkodliwego oprogramowania z pewnych plików z powodu ograniczeń prawnych lub technicznych. Są to np. archiwa plików utworzone przy użyciu zastrzeżonej technologii (dzieje się tak dlatego, że te archiwa nie mogą być poprawnie odtworzone).

  Informacje o tym, jak pozbyć się szkodliwego oprogramowania, znajdują się tutaj: *„Usuwanie szkodliwego oprogramowania z systemu"* (p. 208).

15.3.2. Zarządzanie skanowaniem wymiennych nośników danych

Aby automatycznie zarządzać skanowaniem wymiennych nośników danych:

Dla najlepszej ochrony zalecane jest włączenie **Automatycznego Skanowania** wszystkich rodzajów wymiennych nośników danych.

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. Wybierz zakładkę **Napędy i Urządzenia**.

Opcje skanowania są skonfigurowane wcześniej tak, aby zapewnić najlepszą wykrywalność. Jeśli zostaną wykryte zainfekowane pliki, Bitdefender spróbuje je wyleczyć (usunąć szkodliwy kod) lub przenieść do kwarantanny. Jeśli żadne z tych działań nie przyniesie skutku, kreator skanowania antywirusowego zaoferuje Ci wybór innych działań, które mogą być wykonane na zainfekowanych plikach. Opcje skanowania są standardowe i nie możesz ich zmienić.

15.4. Skanuj plik hostów

Pliki hostów instalowane domyślnie wraz z system operacyjnym i wykorzystane do mapowania nazw hostów do adresów IP, za każdym razem kiedy wchodzisz na nową stronę, łączysz się z serwerem FTP lub innym serwerem internetowym. Jest to zwykły plik tekstowy i złośliwe programy mogą go zmodyfikować. Zaawansowani użytkownicy wiedzą jak tego użyć, aby zablokować irytujące reklamy, bannery, ciasteczka lub hijackers.

Aby skonfigurować plik skanu hostów:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Zaawansowane**.
3. Kliknij odpowiedni przełącznik WŁĄCZ/WYŁĄCZ.

15.5. Konfigurowanie wyjątków skanowania

Bitdefender pozwala na wykluczanie ze skanowania konkretnych plików, folderów i rozszerzeń plików. Funkcja ta ma na celu uniknięcie wpływu na Twoją pracę, a ponadto może poprawić wydajność systemu. Wyjątki powinny być używane przez użytkowników posiadających zaawansowaną wiedzę komputerową lub według wskazówek przedstawiciela firmy Bitdefender.

Możesz tak skonfigurować wykluczenia, żeby były stosowane tylko dla skanowania w czasie rzeczywistym lub skanowania na żądanie, bądź też dla obu tych rodzajów. Obiekty wykluczone ze skanowania w czasie rzeczywistym nie zostaną przeskanowane, nieważne czy zostały otwarte przez Ciebie, czy przez aplikację.

Notatka

W skanowaniu kontekstowym i systemie NIE są stosowane wykluczenia. System posiada skanowanie na żądanie, co umożliwia analizowanie całego systemu w celu wykrycia złośliwego oprogramowania, które zagrażają bezpieczeństwu Twoich danych. Skanowanie kontekstowe jest typem skanowania na żądanie: klikasz prawym przyciskiem myszy na folder, który chcesz skanować i wybierasz **Skanuj z Bitdefender**.

15.5.1. Wykluczanie plików i folderów ze skanowania

Aby wykluczyć określone pliki i foldery ze skanowania:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. Wybierz zakładkę **Wykluczenia**.
5. Wybierz opcje **lista plików i folderów wykluczonych ze skanowania** aby ją zdefiniować Pojawi się okno, w którym możesz zarządzać plikami i folderami wykluczonymi ze skanowania.
6. Aby dodać wyjątek, należy postępować w następujący sposób:
   a. Kliknij przycisk **DODAJ**.
   b. Kliknij **Przeglądaj**, zaznacz plik lub folder, który ma być wykluczony ze skanowania, a następnie kliknij **OK**. Możesz również wpisać (lub skopiować i wkleić) ścieżkę pliku lub folderu w polu edycji.
   c. Domyślnie wybrany plik lub folder będzie wykluczony zarówno ze skanowania w czasie rzeczywistym, jak i skanowania na żądanie. Aby wybrać, kiedy zastosować wykluczenie, wybierz jedną z opcji.
   d. Kliknij **Dodaj**.

15.5.2. Wykluczanie rozszerzeń plików ze skanowania

Jeśli wykluczysz ze skanowania jakieś rozszerzenie pliku, Bitdefender nie będzie skanował plików o tym rozszerzeniu, niezależnie od tego, gdzie się znajdują. Wykluczenie dotyczy również nośników wymiennych, takich jak płyty CD, DVD, urządzenia magazynujące USB lub dyski sieciowe.

WAŻNE
Zachowaj ostrożność przy wykluczaniu określonych rozszerzeń, bo Twój komputer może zostać narażony na działanie szkodliwego oprogramowania.

Wykluczanie rozszerzeń plików ze skanowania:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. Wybierz zakładkę **Wykluczenia**.

5. Wybierz opcje **lista rozszerzeń wykluczonych ze skanowania** aby ją zdefiniować W wyskakującym oknie możesz zarządzać określonymi rozszerzeniami plików, wkluczonymi ze skanowania.
6. Aby dodać wyjątek, należy postępować w następujący sposób:
   a. Kliknij przycisk **DODAJ**.
   b. Wprowadź rozszerzenia, które mają być wykluczone ze skanowania, oddzielając je średnikami (;). Oto przykład:

      txt;avi;jpg

   c. Domyślnie wszystkie pliki o określonych rozszerzeniach będą wykluczone zarówno ze skanowania w czasie rzeczywistym, jak i ze skanowania na żądanie. Aby wybrać, kiedy zastosować wykluczenie, wybierz jedną z opcji.
   d. Kliknij **Dodaj**.

15.5.3. Zarządzanie wyjątkami ze skanowania

Jeśli skonfigurowane wyjątki skanowania nie są już potrzebne, zaleca się ich usunięcie lub wyłączenie.

Zarządzanie wyjątkami skanowania:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. Wybierz zakładkę **Wykluczenia**.
5. Użyj opcji **Lista plików i folderów wykluczonych ze skanowania** aby zarządzać wyjątkami
6. Aby usunąć lub edytować wyjątki skanowania, kliknij jeden z dostępnych linków. Wykonaj następujące kroki:
   - Aby usunąć wpis z listy, zaznacz go i kliknij przycisk "**USUŃ**".
   - Aby edytować wpis w tabeli, dwukrotnie go kliknij (lub zaznacz wpis i kliknij przycisk "**Edytuj**"). Pojawia się nowe okno, w którym możesz zmienić rozszerzenia lub ścieżki dostępowe do wykluczenia i typ skanowania, które chcesz wykluczyć, w zależności od potrzeb. Dokonaj zmian, a następnie kliknij "**Zmodyfikuj**".

15.6. Zarządzanie plikami w kwarantannie

Bitdefender izoluje pliki zainfekowane szkodliwym oprogramowaniem, których nie może wyleczyć, oraz inne podejrzane pliki w bezpiecznym obszarze, zwanym kwarantanną. Kiedy wirus znajduje się w kwarantannie nie może uczynić żadnej szkody ponieważ nie może być uruchomiony lub otwierany.

Pliki poddane kwarantannie są domyślnie wysyłane do laboratoriów firmy Bitdefender w celu analizy szkodliwego oprogramowania dokonywanej przez analityków Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

Dodatkowo, po każdej aktualizacji sygnatur wirusów, Bitdefender skanuje wszystkie pliki objęte kwarantanną. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji.

Aby sprawdzać i zarządzać plikami poddanymi kwarantannie:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
4. Wybierz zakładkę **Kwarantanna**.
5. Pliki poddane kwarantannie są automatycznie zarządzane przez Bitdefender zgodnie z domyślnymi ustawieniami kwarantanny. Choć nie jest to zalecane, możesz dostosować ustawienia kwarantanny według swoich preferencji.

   Przeskanuj ponownie kwarantannę po aktualizacji baz sygnatur wirusów
   Opcja powinna być aktywna, aby automatycznie skanować pliki objęte kwarantanną natychmiast po aktualizacji definicji wirusów. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji.

   Prześlij podejrzane pliki z kwarantanny do dalszej analizy
   Opcja powinna być aktywna, aby automatycznie odsyłać pliki objęte kwarantanną do laboratoriów Bitdefender. Przykładowe pliki będą przeanalizowane przez badaczy szkodliwego oprogramowania firmy Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.

Usuń zawartość starszą niż {30} dni

Domyślnie wszystkie pliki objęte kwarantanną dłużej niż 30 dni są automatycznie usuwane. Jeśli chcesz zmienić odstęp czasu, wprowadź nową wartość w odpowiednie pole. Aby wyłączyć automatyczne usuwanie starych plików w kwarantannie, wpisz 0.

6. Aby usunąć plik z kwarantanny, zaznacz go i kliknij przycisk **Usuń**. Jeśli chcesz przywrócić plik poddany kwarantannie w jego oryginalnym miejscu, zaznacz go i kliknij **Przywróć**.

16. AKTYWNA KONTROLA ZAGROŻEŃ

Aktywna Kontrola Zagrożeń Bitdefender to innowacyjna, proaktywna technologia detekcji, która do wykrywania w czasie rzeczywistym ransomware i nowych, potencjalnych zagrożeń korzysta z zaawansowanych metod heurystycznych.

Moduł Aktywnej Kontroli Zagrożeń nieustannie monitoruje aplikacje działające na komputerze w poszukiwaniu aktywności charakterystycznej dla złośliwego oprogramowania. Każde z tych działań jest oceniane, a dla każdego procesu obliczana jest ocena ogólna.

Jako środek bezpieczeństwa zostaniesz powiadomiony za każdym razem, gdy atak ransomware zostanie wykryty i zablokowany, nawet jeśli zostanie włączona funkcja Autopilot.

16.1. Włączanie i wyłączanie Aktywnej Kontroli Zagrożeń

Aby włączyć i wyłączyć Aktywną Kontrolę Zagrożeń:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **AKTYWNA KONTROLA ZAGROŻEŃ**, kliknij przycisk WŁĄCZ/WYŁĄCZ.

Notatka

Aby chronić system przed ransomware i innymi atakami typu malware, zaleca się wyłączenie funkcji Advanced Threat Defense w jak najrzadziej.

16.2. Sprawdzanie wykrytych ataków ransomware

Aby sprawdzić atak ransomware wykryty przez Aktywną Kontrolę Zagrożeń:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **AKTYWNA KONTROLA ZAGROŻEŃ**, kliknij **Ochrona przed Ransomware**.

4. W oknie z opisem funkcji Aktywna Kontrola Zagrożeń kliknij **OK, ZROZUMIAŁEM**.

   Ataki wykryte w ciągu ostatnich 90 dni są wyświetlane. Aby uzyskać szczegółowe informacje na temat rodzaju wykrytego ransomware, ścieżki złośliwego procesu lub czy oczyszczanie zakończyło się pomyślnie, wystarczy kliknąć.

16.3. Sprawdzanie wykrytych podejrzanych aplikacji

Aby sprawdzić podejrzane aplikacje wykryte przez Aktywną Kontrolę Zagrożeń:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **AKTYWNA KONTROLA ZAGROŻEŃ**, kliknij **Kontrola Zagrożeń**.
4. W oknie z opisem funkcji Aktywna Kontrola Zagrożeń kliknij **OK, ZROZUMIAŁEM**.

   Aplikacje wykryte jako zagrożenie i zablokowane w ciągu ostatnich 90 dni są wyświetlane. Aby uzyskać szczegółowe informacje na temat aplikacji, ścieżki złośliwego procesu lub czy oczyszczanie zakończyło się pomyślnie, wystarczy kliknąć.

16.4. Dodawanie wyjątków procesów

Możesz skonfigurować zasady dotyczące wykluczenia dla zaufanych aplikacji w taki sposób, że Aktywna Kontrola Zagrożeń nie będzie ich blokować, jeśli będą wykonywać działania charakterystyczne dla złośliwego oprogramowania. Aktywna Kontrola Zagrożeń będzie stale monitorować wykluczone aplikacje.

Aby zacząć dodawać procesy do listy wykluczeń Aktywnej Kontroli Zagrożeń:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Kliknij ikonę w prawym dolnym rogu modułu **AKTYWNA KONTROLA ZAGROŻEŃ**.
4. W oknie **BIAŁA LISTA**, kliknij **Dodaj aplikacje do białej listy**.

5. Znajdź i wybierz aplikację, która ma być wykluczona, a następnie kliknij **OK**.

   Aby usunąć wpis z listy, kliknij przycisk **Usuń**.

17. OCHRONA SIECIOWA

Ochrona sieciowa Bitdefender zapewnia bezpieczne przeglądanie, informując o potencjalnych stronach ze złośliwym oprogramowaniem.

Bitdefender zapewnia ochronę w czasie rzeczywistym dla:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Aby konfigurować ustawienia Ochrony Webowej:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu modułu **OCHRONA SIECIOWA**.

Kliknij przyciski, aby włączyć lub wyłączyć:

- Skanowanie ruchu Internetowego blokuje malware pochodzące z Internetu, w tym przypadkowe pobieranie.
- Asystent wyszukiwania jest składnikiem, który ocenia i oznacza wyniki Twoich wyszukiwarek i linki zamieszczone na portalach społecznościowych poprzez umieszczenie ikony obok każdego wyniku:

  Nie powinieneś wchodzić na tę stronę.

  Ta strona może zawierać niebezpieczną treść. Należy zachować ostrożność, jeśli zdecydujesz się ją odwiedzić.

  Ta strona jest bezpieczna.

  Asystent wyszukiwania ocenia wyniki wyszukiwania z następujących wyszukiwarek internetowych:
  - Google
  - Yahoo!
  - Bing
  - Baidu

Asystent wyszukiwania ocenia linki zamieszczone na następujących portalach społecznościowych:
- Facebook
- Twitter

- Skanowanie SSL.

  Bardziej zaawansowany atak może używać zabezpieczonego ruchu sieciowego w celu zmylenia ofiary. Zaleca się włączenie skanowania SSL.

- Ochrona przed oszustwem.
- Ochrona przed phishingiem.

Stwórz listę stron, które nie będą skanowane przez silniki Bitdefender: antywirusowy, antyphishingowy i antywyłudzeniowy. Na tej liście powinny znajdować się tylko w pełni zaufane strony. Przykładowo, dodaj stronę WWW, na której aktualnie robisz zakupy online.

Aby skonfigurować i zarządzać stronami internetowymi za pomocą ochrony sieci dostarczanej przez Bitdefender:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W panelu **OCHRONA SIECI**, kliknij **Biała lista**.
4. W oknie tekstowym **Dodaj URL** wpisz nazwę strony, którą chcesz dodać do Białej Listy, a następnie kliknij **Dodaj**.

   Aby usunąć stronę internetową z listy, wybierz stronę i kliknij odpowiadający jej link **Usuń**.

   Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

17.1. Alarmy produktu Bitdefender w przeglądarce

Za każdym razem, kiedy próbujesz odwiedzić stronę internetową zaklasyfikowaną jako niebezpieczna, jest ona blokowana i wyświetlana jest strona ostrzegawcza.

Strona zawiera informacje, takie jak adres URL strony i wykryte zagrożenie.

Musisz podjąć decyzję co do działania. Dostępne są następujące opcje:

- Wyjdź ze strony klikając **Wróćmy w bezpieczne miejsce**.

- Jeśli mimo ostrzeżenia chcesz odwiedzić stronę, kliknij "**Rozumiem ryzyko, mimo wszystko pozwól mi wejść**".

18. ANTYSPAM

Spam to termin określający niechcianą pocztę. Spam jest narastającym problemem zarówno dla użytkowników indywidualnych jak i organizacji. Nieprzyjemny dla oka, a dzieci zdecydowanie nie powinny tego oglądać, dodatkowo może doprowadzić do utraty Twojej pracy (marnowanie czasu, lub otrzymywanie materiałów pornograficznych), nie można powstrzymać ludzi przed jego rozsyłaniem. Najlepiej byłoby, oczywiście, nie otrzymywać go wcale. Niestety spam przychodzi w wielu formach oraz rozmiarach i jest go bardzo dużo.

Moduł antyspamowy Bitdefender zawiera wiele innowacyjnych technologii i oferuje najwyższe standardy filtrów antyspamowych, aby wykryć spam zanim dotrze on do Twojej skrzynki odbiorczej. Aby uzyskać więcej informacji, odwołaj się do *„Przegląd funkcji modułu antyspamowego"* (p. 117).

Ochrona przed spamem Bitdefender jest dostępna tylko dla klientów poczty e-mail skonfigurowanych na odbieranie wiadomości przez protokół POP3. POP3 jest najbardziej popularnym protokołem używanym do pobierania wiadomości e-mail z serwera poczty.

Notatka
Bitdefender nie zapewnia ochrony antyspamowej kont pocztowych, do których dostęp zapewniają internetowe usługi pocztowe.

Wiadomości spamowe wykryte przez Bitdefender są w temacie oznakowane przedrostkiem [SPAM]. Bitdefender automatycznie przenosi informacje oznaczone jako spam do specjalnego katalogu:

- W Microsoft Outlook, wiadomości te przenoszone są do folderu **Spam**, zlokalizowanego w folderze **Usunięte**. Folder **Spam** jest tworzony kiedy email jest oznaczony jako spam.
- W Mozilla Thunderbird, wiadomości są przenoszone do folderu **Spam**, zlokalizowanego w folderze **Kosz**. Folder **Spam** jest tworzony kiedy email jest oznaczony jako spam.

Jeśli korzystasz z innych klientów pocztowych, ustaw reguły tak, aby przekierowywały wiadomości oznaczone przez Bitdefender jako [SPAM] do odpowiedniego katalogu kwarantanny. Jeśli wykryte elementy lub folder Śmieci jest usunięty, folder Span też zostanie usunięty. Jednakże, nowy folder Spam zostanie utworzony jak tylko email zostanie oznaczony jako spam.

18.1. Przegląd funkcji modułu antyspamowego

18.1.1. Filtry antyspamowe

Silnik antyspamowy Bitdefender opiera się na technologii ochrony w chmurze i kilku innych filtrach, takich jak Lista przyjaciół, Lista spamerów i Filtr ciągu znaków, które zapewniają Twojej skrzynce odbiorczej ochronę przed spamem..

Lista przyjaciół / Lista spamerów

Większość ludzi komunikuje się regularnie lub otrzymuje wiadomości z firm lub organizacji w tej samej domenie. Używając **listy przyjaciół lub listy spamerów** możesz łatwo określić, od kogo chcesz otrzymywać e-maile (przyjaciele) bez względu na ich zawartość lub od których nadawców nie chcesz otrzymywać żadnych informacji (spamerzy).

Notatka
Zalecamy dodawanie nazwisk i adresów e-mail osób z Twojej listy przyjaciół do **Listy przyjaciół**. Bitdefender nie zablokuje żadnej wiadomości od przyjaciół z listy - dodanie ich do listy przyjaciół zapewnia więc, że legalne wiadomości nie są oznaczane jako spam.

Filtr językowy

Wiele wiadomości spamowych jest napisanych cyrylicą i/lub azjatycką czcionką. Skonfiguruj ten filtr, jeżeli chcesz odrzucać wszystkie wiadomości e-mail napisane w ten sposób.

18.1.2. Działanie antyspamowe

Silnik antyspamowy Bitdefender korzysta z połączonych wszystkich typów filtrów antyspamowych, aby określić, czy poczta przychodząca powinna się znaleźć w folderze **Odebrane**, czy też nie.

Każdy e-mail, który przychodzi jest najpierw sprawdzany w przez filtr Lista przyjaciół / Lista spamerów. Jeżeli adres nadawcy jest znaleziony na liście Przyjaciele e-mail bezpośrednio jest przenoszony do **Skrzynki odbiorczej**.

W przeciwnym razie filtr Spamerzy przejmie wiadomość e-mail, aby sprawdzić czy adres nadawcy znajduje się na tej liście. Jeśli tak, wiadomość zostanie potraktowana jako SPAM i przeniesiona do folderu **Spam**.

W przeciwnym razie, Filtr językowy sprawdzi czy e-mail jest napisany cyrylicą lub czcionką azjatycką. Jeżeli tak, e-mail będzie potraktowany jako SPAM i przeniesiony do folderu **Spam**.

Notatka
Jeżeli e-mail jest oznaczony jako SEKSUALNY w linii tematu, Bitdefender potraktuje go jako SPAM.

18.1.3. Obsługiwane klienty poczty i protokoły

Ochrona antyspamowa jest zapewniona dla wszystkich klientów e-mail POP3/SMTP. Jednakże pasek narzędzi antyspamowych Bitdefender jest zintegrowany tylko z:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 lub nowsza

18.2. Włączanie lub wyłączanie ochrony antyspamowej

Ochrona przed spamem jest domyślnie włączona.

Aby wyłączyć moduł Antyspam:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYSPAM** kliknij przełącznik WŁĄCZ/WYŁĄCZ.

18.3. Używanie paska narzędzi antyspamowych w oknie Twojego klienta poczty

W górnej części okna Twojego klienta e-mail powinieneś zobaczyć pasek antyspamowy. Pasek antyspamowy pomaga Ci zarządzać zabezpieczeniem antyspamowym bezpośrednio z poziomu klienta poczty. Możesz poprawić Bitdefender, jeśli błędnie zakwalifikował wiadomości e-mail jako spam.

WAŻNE
Bitdefender jest zintegrowany z najbardziej popularnymi klientami poczty dzięki wykorzystaniu łatwego w użyciu antyspamowego paska narzędziowego. W celu uzyskania kompletnej listy obsługiwanych klientów poczty e-mail, odwołaj się do *„Obsługiwane klienty poczty i protokoły”* (p. 118).

Każdy przycisk antyspamowego paska Bitdefender jest wyjaśniony poniżej:

Ustawienia - otwiera okno, w którym możesz konfigurować filtry antyspamowe i ustawienia paska narzędzi.
To jest Spam - oznacza to, że wybrany e-mail to spam. Wiadomość zostanie automatycznie przeniesiona do folderu **SPAM**. Jeśli usługa chmury antyspamowej jest włączona, wysyłana jest wiadomość do chmury produktu Bitdefender w celu dalszej analizy.
To nie jest Spam - powiadamia, że wybrany e-mail nie jest spamem i Bitdefender nie powinien był go oznaczyć. Wiadomość zostanie przeniesiona z folderu **SPAM** do folderu **Skrzynka odbiorcza**. Jeśli usługa chmury antyspamowej jest włączona, wysyłana jest wiadomość do chmury produktu Bitdefender w celu dalszej analizy.

WAŻNE
Klawisz **To nie jest Spam** staje się aktywny, kiedy wybierzesz wiadomość oznaczoną jako Spam przez Bitdefender (zazwyczaj te wiadomości znajdują się w folderze **Spam**).

Dodaj Spamera - dodaje nadawcę wybranej wiadomości e-mail do listy Spamerów. Możesz zostać zapytany o potwierdzenie, klikając "**OK**". Wiadomości e-mail pochodzące od adresów zawartych w liście Spamerów są automatycznie oznaczane jako [spam].
Dodaj Przyjaciela - dodaje nadawcę wybranej wiadomości e-mail do listy Przyjaciół. Możesz zostać zapytany o potwierdzenie, klikając "**OK**". Będziesz zawsze otrzymywał wiadomości e-mail z tego adresu bez względu na zawartość wiadomości.
Spamerzy - otwiera **Listę spamerów**, która zawiera wszystkie adresy e-mail, z których nie chcesz otrzymywać wiadomości bez względu na ich zawartość. Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Listy spamerów"* (p. 122).
Przyjaciele - otwiera **Listę przyjaciół**, która zawiera wszystkie adresy e-mail, z których zawsze chcesz odbierać wiadomości bez względu na ich zawartość. Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Listy przyjaciół"* (p. 121).

18.3.1. Powiadamianie o wykrytych błędach

Jeśli używasz wspieranego klienta poczty, możesz z łatwością ulepszyć filtr antyspamowy (poprzez zaznaczenie, które wiadomości e-mail nie powinny

być oznaczone jako [spam]). Ta czynność poprawi skuteczność filtrów antyspamowych. Wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu śmieci, gdzie zostały przeniesione wiadomości spamowe.
3. Wybierz dozwoloną wiadomość nieprawidłowo oznaczoną przez Bitdefender jako [spam].
4. Kliknij przycisk **Dodaj przyjaciela** znajdujący się na antyspamowym pasku narzędziowym Bitdefender, aby dodać nadawcę do listy Przyjaciół. Możesz zostać zapytany o potwierdzenie, klikając "**OK**". Będziesz zawsze otrzymywał wiadomości e-mail z tego adresu bez względu na zawartość wiadomości.
5. Kliknij przycisk **To nie jest Spam** na antyspamowym pasku narzędzi produktu Bitdefender (zwykle zlokalizowanym w górnej części okna klienta pocztowego). Wiadomości e-mail będą przenoszone do folderu „Skrzynka odbiorcza".

18.3.2. Powiadamianie o niewykrytym spamie

Jeśli używasz wspieranego klienta poczty, możesz łatwo wskazać, które z wiadomości mają być traktowane jako spam. Ta czynność poprawi skuteczność filtrów antyspamowych. Wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu Skrzynki odbiorczej.
3. Wybierz niewykryte wiadomości spamowe.
4. Kliknij przycisk **To jest Spam** w pasku narzędziowym produktu Bitdefender (zwykle zlokalizowanym w górnej części okna klienta pocztowego). Są one natychmiast oznaczane jako [spam] i przenoszone do folderu śmieci.

18.3.3. Konfiguracja ustawień paska narzędzi

Aby skonfigurować ustawienia paska narzędzi antyspamowych dla Twojego klienta poczty elektronicznej, kliknij przycisk **Ustawienia** na pasku, a następnie zakładkę **Ustawienia paska narzędzi**.

Oto dostępne możliwości:

- **Oznacz spam jako przeczytane** - po odebraniu wiadomości automatycznie oznacza spam jako wiadomości przeczytane, aby nie przeszkadzały w pracy.
- Możesz zdecydować, czy wyświetlać, czy nie wyświetlać okna z potwierdzeniem, kiedy klikasz przyciski **Dodaj spamera** i **Dodaj przyjaciela** na pasku narzędzi antyspamowych.

  Potwierdzenia mogą zapobiec przypadkowemu dodaniu nadawców wiadomości e-mail do listy Przyjaciół / Spamerów.

18.4. Konfigurowanie Listy przyjaciół

Lista przyjaciół jest listą wszystkich adresów e-mail, z których chcesz zawsze otrzymywać wiadomości, bez względu na ich zawartość. Wiadomości od Twoich przyjaciół nie są oznaczane jako Spam nawet wtedy, gdy ich zawartość przypomina Spam.

Notatka

Każdy przychodzący mail z **Listy przyjaciół**, będzie automatycznie dostarczany do Twojej skrzynki "Przychodzące", bez dalszego przetwarzania.

Konfigurowanie i zarządzanie Listą przyjaciół:

- Jeśli używasz programu Microsoft Outlook lub Thunderbird, kliknij przycisk **Przyjaciele** znajdujący się na antyspamowym pasku narzędziowym Bitdefender.
- Alternatywnie:
  1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  2. Kliknij link **POKAŻ FUNKCJE**.
  3. W module **ANTYSPAM** wybierz **Zarządzaj Przyjaciółmi**.

Aby dodać adres e-mail, zaznacz opcję **Adres e-mail**, wprowadź adres, a następnie kliknij **Dodaj**. Składnia: nazwa@domena.com.

Aby dodać wszystkie adresy e-mail konkretnej domeny, wybierz opcję **Nazwa domeny**, wejdź w domenę, a następnie kliknij **Dodaj**. Składnia:

- @domena.com, *domena.com i domena.com - wszystkie przychodzące maile z domena.com dostaną się do folderu **Skrzynka odbiorcza** Twojej poczty bez względu na ich zawartość;

- *domena* - wszystkie przychodzące maile z domena (bez względu na przyrostki domeny) dostaną się do **Skrzynki odbiorczej** Twojej poczty bez względu na ich zawartość;
- *com - wszystkie maile posiadające przyrostek domeny com dostaną się do **Skrzynki odbiorczej** Twojej poczty bez względu na ich zawartość;

Zaleca się unikać dodawania całych domen, aczkolwiek w niektórych sytuacjach jest to przydatne. Możesz na przykład dodać domenę e-mail firmy, dla której pracujesz lub domeny zaufanych partnerów.

Aby usunąć element z listy, kliknij "**Usuń**" obok tego elementu. Aby usunąć wszystkie wpisy z listy, kliknij przycisk "**Wyczyść listę**".

Możesz zapisać listę przyjaciół do pliku, aby móc skorzystać z niej na innym komputerze lub po reinstalacji oprogramowania. Aby zapisać listę przyjaciół, kliknij przycisk "**Zapisz**" i zapisz ją do wybranej lokalizacji. Plik będzie miał rozszerzenie .bwl.

Aby załadować poprzednio zapisaną listę przyjaciół, kliknij przycisk "**Załaduj**" i otwórz odpowiedni plik .bwl. Aby wyczyścić dotychczasową zawartość listy podczas wczytywania poprzednio zapisanej, zaznacz "**Nadpisz obecną listę**".

Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.

18.5. Konfigurowanie Listy spamerów

Lista spamerów jest listą wszystkich adresów e-mail, z których nie chcesz otrzymywać wiadomości bez względu na ich zawartość. Każdy przychodzący mail z adresu z **Listy spamerów** będzie automatycznie oznaczony jako Spam, bez dalszego przetwarzania.

Konfigurowanie i zarządzanie Listą spamerów:

- Jeśli używasz programu Microsoft Outlook lub Thunderbird, kliknij przycisk **Spamerzy**, znajdujący się na zintegrowanym z klientem poczty antyspamowym pasku narzędziowym Bitdefender.
- Alternatywnie:
  1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  2. Kliknij link **POKAŻ FUNKCJE**.
  3. W module **ANTYSPAM**, wybierz **Zarządzaj Spamerami**.

Aby dodać adres e-mail, zaznacz opcję **Adres e-mail**, wprowadź adres, a następnie kliknij **Dodaj**. Składnia: nazwa@domena.com.

Aby dodać wszystkie adresy e-mail konkretnej domeny, wybierz opcję **Nazwa domeny**, wejdź w domenę, a następnie kliknij **Dodaj**. Składnia:

- @domena.com, *domena.com i domena.com - wszystkie maile z domena.com będą oznaczone jako SPAM;
- *domena* - wszystkie maile z domena (bez względu na przyrostki domeny) będą oznaczone jako SPAM;
- *com - wszystkie maile posiadające przyrostek domeny com będą oznaczone jako SPAM.

Zaleca się unikać dodawania całych domen, aczkolwiek w niektórych sytuacjach jest to przydatne.

Ostrzeżenie

Nie dodawaj do Listy spamerów domen pochodzących ze znanych serwisów (takich jak Onet, WP, Interia, Gmail, Hotmail i innych). Każda wiadomość od użytkowników zarejestrowanych w takiej usłudze zostałaby oznaczona jako SPAM. Jeśli np. dodasz yahoo.com do Listy spamerów, wszystkie wiadomości przychodzące z adresów yahoo.com będą oznaczone jako [spam].

Aby usunąć element z listy, kliknij "**Usuń**" obok tego elementu. Aby usunąć wszystkie wpisy z listy, kliknij przycisk "**Wyczyść listę**".

Możesz zapisać Listę spamerów do pliku, aby móc skorzystać z niej na innym komputerze lub po reinstalacji oprogramowania. Aby zapisać Listę spamerów, kliknij na przycisk "**Zapisz**" i zapisz ją do wybranej lokalizacji. Plik będzie miał rozszerzenie .bwl.

Aby załadować poprzednio zapisaną Listę spamerów, kliknij na przycisk "**Wczytaj**" i otwórz odpowiedni plik .bwl. Aby wyczyścić dotychczasową zawartość listy podczas wczytywania poprzednio zapisanej, zaznacz "**Nadpisz obecną listę**".

Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.

18.6. Konfigurowanie lokalnych filtrów antyspamowych

Zgodnie z tym, co opisano w *„Przegląd funkcji modułu antyspamowego"* (p. 117), do identyfikowania spamu Bitdefender używa kombinacji różnych filtrów antyspamowych. Filtry antyspamowe są wstępnie skonfigurowane, aby zapewnić skuteczną ochronę.

WAŻNE

W zależności od tego, czy otrzymujesz dozwolone wiadomości pisane w językach azjatyckich lub cyrylicą, wyłącz lub włącz ustawienie, które automatycznie blokuje takie wiadomości e-mail. Odpowiednie ustawienie jest wyłączone w zlokalizowanych wersjach programu, korzystających z takich właśnie zestawów znaków (na przykład w wersji rosyjskiej lub chińskiej).

Aby skonfigurować lokalne filtry antyspamowe:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu modułu **ANTYSPAM**.
4. Kliknij odpowiedni przełącznik WŁĄCZ/WYŁĄCZ.

Jeśli korzystasz z Microsoft Outlook lub Thunderbird, możesz skonfigurować lokalne filtry antyspamowe bezpośrednio z konta klienta poczty. Kliknij przycisk **Ustawienia** na antyspamowym pasku narzędzi Bitdefender (z reguły znajdującym się w górnej części okna klienta poczty), a następnie zakładkę **Filtry antyspamowe**.

18.7. Konfigurowanie ustawień chmury

Wykrywanie w chmurze zapewnia skuteczną i zawsze aktualną ochronę przed spamem dzięki usługom w chmurze Bitdefender.

Ochrona oparta o chmurę działa tak długo, jak włączony jest moduł antyspamowy Bitdefender.

Próbki prawidłowych e-maili lub spamu mogą zostać wysłane do chmury produktu Bitdefender, jeśli wystąpią błędy w wykrywaniu lub spam nie zostanie w ogóle wykryty. Pozwala to na ulepszenie wykrywania spamu produktu Bitdefender.

Skonfiguruj wysyłanie próbek wiadomości e-mail do chmury Bitdefender zaznaczając wymagane opcje, po wykonaniu tych kroków:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu modułu **ANTYSPAM**.
4. W oknie **USTAWIENIA**, zaznacz wybrane opcje.

Jeśli korzystasz z Microsoft Outlook lub Thunderbird, możesz skonfigurować wykrywanie cloud bezpośrednio z konta klienta poczty. Kliknij przycisk ⚙ **Ustawienia** na antyspamowym pasku narzędzi Bitdefender (z reguły znajdującym się w górnej części okna klienta poczty), a następnie przycisk **Ustawienia chmury**.

19. ZAPORA SIECIOWA

Zapora sieciowa chroni Twój komputer przed nieautoryzowanymi próbami połączeń przychodzących i wychodzących, zarówno w sieci lokalnej, jak i w internecie. Przypomina to strażnika przy bramie - monitoruje próby połączenia i decyduje, na które zezwolić, a które zablokować.

Zapora sieciowa Bitdefender kieruje się zasadami, aby filtrować dane przesyłane do i z Twojego komputera.

W normalnych warunkach Bitdefender automatycznie tworzy regułę za każdym razem, kiedy aplikacja próbuje połączyć się z internetem. Możesz również ręcznie dodać lub edytować reguły aplikacji.

Ze względów bezpieczeństwa otrzymasz powiadomienie za każdym razem, gdy potencjalnie szkodliwa aplikacja zostanie zablokowana przed dostępem do internetu, nawet jeśli jest włączona funkcja Autopilot.

Bitdefender automatycznie przydzieli typ sieci każdemu wykrytemu połączeniu sieciowemu. W zależności od rodzaju sieci, ochrona Zaporą sieciową jest ustawiona na odpowiednim poziomie dla każdego połączenia.

Aby dowiedzieć się więcej o ustawieniach Zapory sieciowej dla każdego typu sieci, oraz jak można edytować ustawienia sieci, zapoznaj się z *„Zarządzanie ustawieniami połączeń”* (p. 130).

19.1. Włączanie lub wyłączanie Zapory sieciowej

Aby włączyć lub wyłączyć ochronę firewall:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **ZAPORA SIECIOWA** kliknij przełącznik WŁĄCZ/WYŁĄCZ.

Ostrzeżenie

Zapora sieciowa powinna być wyłączona na krótko, gdyż takie działanie grozi próbą nieautoryzowanego połączenia. Jak najszybciej ponownie włącz Zaporę sieciową.

19.2. Zarządzanie regułami aplikacji

Aby przeglądać i zarządzać regułami Zapory sieciowej kontrolującymi dostęp aplikacji do zasobów sieciowych i Internetu:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **ZAPORA SIECIOWA** kliknij **Dostęp do aplikacji** .
4. W oknie z opisem funkcji Zapory Sieciowej kliknij **OK, ZROZUMIAŁEM**.

Możesz zobaczyć 15 najnowszych programów (procesów), które przeszły przez zaporę Bitdefender i sieć internetową, do której jesteś podłączony. Aby zobaczyć reguły utworzone dla określonej aplikacji, po prostu kliknij ją, a następnie kliknij link **Wyświetl reguły aplikacji** Okno **REGUŁY** otwiera się.

Dla każdej reguły wyświetlana jest następująca informacja:

- **SIEĆ** - proces i typy kart sieciowych (Dom /Biuro, Publiczne lub Wszystkie), do których ma zastosowanie reguła. Reguły tworzone automatycznie, tak aby filtrować dostęp do sieci i internetu przez dowolne urządzenie. Domyślnie, reguły stosuje się do każdej sieci. Możesz ręcznie dodać regułę lub edytować już istniejące reguły aby filtrować dostęp aplikacji do sieci lub internetu przez wybrane urządzenie (przykładowo, kartę sieci bezprzewodowej).
- **PROTOKÓŁ** - protokół IP do którego stosowana jest reguła. Domyślnie, reguły stosuje się do każdego protokołu.
- **RUCH SIECIOWY** - reguła obowiązuje w obu kierunkach, przychodzących i wychodzących.
- **PORTY** - Protokół PORT, do którego stosowana jest reguła. Domyślnie, reguły stosuje się do każdego portu.
- **IP** - Protokół internetowy (IP), do którego stosowana jest reguła. Domyślnie, reguły stosuje się do każdego adresu IP.
- **DOSTĘP** - zezwolenie lub odmowa dostępu do sieci lub internetu, określone pewnymi warunkami.

Aby edytować lub usunąć reguły dla wybranych aplikacji, kliknij ikonę .

- **Edytuj regułę** - otwiera okno, w którym możesz edytować bieżącą regułę.
- **Usuń regułę** - możesz usunąć bieżący zestaw reguł dla danej aplikacji.

Dodawanie reguł aplikacji

Aby dodać regułę aplikacji:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu okienka **ZAPORA SIECIOWA**.
4. Wybierz link **Dodaj regułę** na górze okna **REGUŁY**.

W oknie **USTAWIENIA** możesz zastosować następujące zmiany:

- **Zastosuj tą regułę do wszystkich aplikacji.** Włącz ten przełącznik, aby zastosować regułę do wszystkich aplikacji.
- **Ścieżka programu.** Kliknij "**Przeglądaj**" i wybierz aplikację, do której ma być zastosowana reguła.
- **Zezwolenie.** Wybierz jedno z dostępnych uprawnień:

Zezwolenie	Opis
Zezwól	Podana aplikacja dostanie zezwolenie na dostęp do sieci / internetu pod pewnymi warunkami.
Zabroń	Podana aplikacja nie dostanie dostępu do sieci / internetu pod pewnymi warunkami.

- **Typ sieci.** Wybierz typ sieci, do której stosuje się ta reguła. Aby zmienić typ, otwórz listę wyboru "**Typ sieci**" i wybierz jeden z dostępnych typów z listy.

Typ sieci	Opis
Dowolna sieć	Zezwalaj na wszelki ruch pomiędzy Twoim komputerem i innymi komputerami bez względu na rodzaj sieci.
Dom / Biuro	Zezwala na wszelki ruch pomiędzy Twoim komputerem i komputerami w sieci lokalnej.
Publiczna	Cały ruch jest filtrowany.

- **Protokół.** Wybierz z menu protokół IP, dla którego ma być stosowana reguła.
  - Jeśli chcesz aby reguła była stosowana dla wszystkich protokołów, zaznacz "**Dowolne**".
  - Jeśli chcesz zastosować tą regułę do protokołu TCP, wybierz **TCP**.
  - Jeśli chcesz zastosować tę regułę do protokołu UDP, wybierz **UDP**.
  - Jeśli chcesz zastosować tą regułę do protokołu ICMP, wybierz **ICMP**.
  - Jeśli chcesz zastosować tą regułę do protokołu IGMP, wybierz **IGMP**.
  - Jeśli chcesz, aby reguła była stosowana do określonego protokołu, wpisz numer przypisany do protokołu, który chcesz filtrować w pustym polu edycyjnym.

  Notatka

  Numery protokołów IP są przypisane przez organizację Internet Assigned Numbers Authority (IANA). Kompletną listę protokołów IP możesz znaleźć tutaj: http://www.iana.org/assignments/protocol-numbers.

- **Kierunek.** Wybierz z menu kierunek ruchu, do którego ma być stosowana reguła.

Kierunek	Opis
Wysyłane	Reguła będzie dotyczyła tylko ruchu wychodzącego.
Odbierane	Reguła będzie dotyczyła tylko ruchu przychodzącego.
Oba	Reguła będzie dotyczyła obu kierunków.

W zakładce **ZAAWANSOWANE** możesz dostosować następujące ustawienia:

- **Niestandardowy adres lokalny.** Określ lokalny adres IP oraz port, do którego odnosi się dana reguła.
- **Niestandardowy adres zdalny.** Określ zdalny adres IP oraz port, do którego odnosi się dana reguła.

Aby usunąć bieżący zestaw reguł i przywrócić ustawienia domyślne, kliknij link **Resetuj reguły** u góry okna **ZASADY**.

19.3. Zarządzanie ustawieniami połączeń

Niezależnie od tego, czy łączysz się z Internetem za pomocą adaptera sieciowego Wi-Fi czy Ethernet, możesz skonfigurować to, jakie ustawienia powinny być zastosowane do bezpiecznej nawigacji. Możesz wybrać z opcji:

- **Dynamiczna** - typ sieci zostanie automatycznie ustawiony w oparciu o profil podłączonej sieci, Dom/Biuro lub Publiczna. W takim przypadku, będą miały zastosowanie tylko reguły Zapory Sieciowej dla określonego typu sieci lub te, które mają zastosowanie do wszystkich typów sieci.
- **Dom/Biuro** - typem sieci będzie zawsze Dom/Biuro, niezależnie od profilu podłączonej sieci. W takim przypadku, będą miały zastosowanie tylko reguły Zapory Sieciowej dla sieci Dom/Biuro lub te, które mają zastosowanie do wszystkich typów sieci.
- **Publiczna** - typem sieci będzie zawsze Publiczna, niezależnie od profilu podłączonej sieci. W takim przypadku, będą miały zastosowanie tylko reguły Zapory Sieciowej dla sieci Publicznej lub te, które mają zastosowanie do wszystkich typów sieci.

Aby skonfigurować swoje adaptery sieciowe:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu okienka **ZAPORA SIECIOWA**.
4. Wybierz kartę **TY SIECI**.
5. Wybierz ustawienia, które chcesz zastosować podczas łączenia z następującymi adapterami:
   - Wi-Fi
   - Ethernet

19.4. Konfigurowanie ustawień zaawansowanych

Aby skonfigurować zaawansowane ustawienia zapory sieciowej:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu okienka **ZAPORA SIECIOWA**.

4. Wybierz zakładkę **Ustawienia**.

Można skonfigurować następujące funkcje:

- **Wykrywanie skanowania portów** - wykrywa i blokuje próby sprawdzenia, które porty są otwarte.

  Operacja skanowania portów jest często wykorzystywana przez hakerów w celu znalezienia otwartych portów na komputerze. Napastnicy mogą włamać się do komputera, jeśli znajdą słabo zabezpieczony lub podatny port.

- **Tryb paranoiczny** - alerty wyświetlane są za każdym razem, gdy aplikacja próbuje nawiązać połączenie z internetem Wybierz **Zezwól** lub **Zablokuj**. Kiedy włączony jest Tryb Paranoiczny, Autopilot i Profile są automatycznie wyłączane. Tryb paranoiczny może być używany jednocześnie z **Trybem Baterii**.

- **Tryb ukryty** - Nie będziesz wykrywany przez inne komputery w sieci. Kliknij **Edytuj ukryte połączenia** aby wybrać kiedy urządzenie powinno lub nie powinno być widoczne dla innych komputerów.

- **Domyślne zachowanie aplikacji** - zezwól Bitdefender na zastosowanie automatycznych ustawień dla aplikacji bez zdefiniowanych reguł. Wybierz opcję **Skonfiguruj aplikacje**, aby zdecydować, czy powinny być stosowane automatyczne ustawienia.

  - Automatyczny - dostęp do aplikacji będzie dozwolony lub zabroniony na podstawie automatycznych reguł Zapory Sieciowej i użytkowników.
  - Zezwól - aplikacje, które nie mają zdefiniowanych reguł Zapory Sieciowej będą automatycznie dozwolone.
  - Blokuj - aplikacje, które nie mają zdefiniowanych reguł Zapory Sieciowej będą automatycznie blokowane.

20. LUKI

Ważnym krokiem w ochronie Twojego komputera przed szkodliwymi akcjami i aplikacjami jest aktualizowanie systemu oraz aplikacji z których często korzystasz. Co więcej, aby zapobiec nieautoryzowanemu dostępowi fizycznemu do Twojego komputera, silne hasła(takie, których nie można zgadnąć) muszą być skonfigurowane dla każdego konta Windows oraz sieci bezprzewodowej do której się łączysz.

Bitdefender automatycznie sprawdza system w poszukiwaniu podatności na zagrożenia i alarmuje o nich. Skanuje pod kątem:

- nieaktualne oprogramowanie zainstalowane na Twoim komputerze.
- brakujące aktualizacje Windows.
- słabe hasła do kont użytkowników Windows.
- nie zabezpieczone bezprzewodowe sieci oraz routery

Bitdefender oferuje dwa sposoby poradzenia sobie z zagrożeniami dla Twojego systemu:

- Możesz skanować swój system w poszukiwaniu luk i naprawić je, używając opcji: **Skaner luk**.
- Korzystając z automatycznego monitorowania luk, możesz sprawdzić i naprawić wykryte słabe punkty w oknie Powiadomienia.

Powinieneś sprawdzać i naprawiać zagrożenia systemowe co tydzień lub co dwa tygodnie.

20.1. Skanowanie Twojego komputera w poszukiwaniu luk

Aby naprawić luki systemowe, korzystając z opcji Skanera luk, należy:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij przycisk **Skanowanie Luk** .
3. Poczekaj, aż Bitdefender zakończy sprawdzanie systemu pod kątem podatności. Żeby zatrzymać proces skanowania, naciśnij "**Pomiń**" na górze okna.

   - **Krytyczne aktualizacje Windows**

Naciśnij "**Zobacz szczegóły**", żeby zobaczyć listę krytycznych aktualizacji Windows, które aktualnie nie są zainstalowane na Twoim komputerze.

Aby rozpocząć instalację wybranych aktualizacji, kliknij **Zainstaluj aktualizacje**. Zainstalowanie aktualizacji może zająć trochę czasu, a ukończenie niektórych z nich może wymagać ponownego uruchomienia systemu. Jeśli to konieczne, uruchom komputer ponownie w wybranym przez Ciebie momencie.

- **Aktualizacje aplikacji**

  Jeśli aplikacja jest nieaktualna, kliknij link **Pobierz nową wersję**, aby pobrać najnowszą wersję.

  Naciśnij "**Pokaż szczegóły**", żeby zobaczyć więcej informacji o aplikacji, którą chcesz zaktualizować.

- **Słabe hasła kont Windows**

  Możesz zobaczyć listę użytkowników kont Windows skonfigurowanych na Twoim komputerze i poziom ochrony, jaki te hasła zapewniają.

  Kliknij **Zmiana hasła przy logowaniu**, aby ustawić nowe hasło dla swojego systemu.

  Kliknij "**Zobacz szczegóły**", aby zmodyfikować słabe hasła. Możesz wybrać między poproszeniem użytkownika o zmianę hasła przy następnym logowaniu lub samemu zmienić hasło natychmiast. Aby hasło było silne, użyj kombinacji dużych i małych liter, cyfr oraz znaków specjalnych (takich jak: #, $ lub @).

- **Słabe sieci Wi-Fi**

  Kliknij **Pokaż szczegóły** aby dowiedzieć się więcej na temat sieci bezprzewodową do której jesteś połączony. Jeśli jest rekomendowane ustawienie silniejszego hasła dla Twojej domowej sieci, kliknij odpowiedni link.

  Kiedy zalecenia są dostępne, kieruj się dostępnymi instrukcjami, aby upewnić się, że Twoja sieć domowa pozostaje bezpieczna

W prawym górnym rogu okna, można filtrować wyniki według własnych preferencji.

20.2. Korzystanie z automatycznego monitorowania luk

Bitdefender regularnie skanuje Twój komputer w tle w poszukiwaniu zagrożeń i zapisuje wykryte programy w oknie "Powiadomienia".

Aby sprawdzić i naprawić wykryte problemy:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. W zakładce **Wszystko**, zaznacz powiadomienia dotyczące ostatniego skanowania Luk
3. Możesz zobaczyć dokładne informacje o wykrytych zagrożeniach dla systemu. W zależności od zagadnienia, naprawienie określonej luki wygląda następująco:
   - Jeśli aktualizacje Windows są dostępne, kliknij **INSTALUJ**.
   - Jeśli automatyczna aktualizacja systemu Windows jest wyłączona, kliknij **WŁĄCZ**.
   - Jeśli aplikacja jest nieaktualna, kliknij "**Aktualizuj teraz**", aby otrzymać link do strony, skąd możesz pobrać i zainstalować najnowszą wersję aplikacji.
   - Jeśli konto użytkownika Windows zabezpieczone jest słabym hasłem, kliknij "**Zmień hasło**", aby zmusić użytkownika do zmiany hasła przy następnym logowaniu lub zmień je samodzielnie. Aby hasło było silne, użyj kombinacji dużych i małych liter, cyfr oraz znaków specjalnych (takich jak: #, $ lub @).
   - Jeśli funkcja autouruchamiania w systemie Windows jest włączona, kliknij **Napraw**, aby ją wyłączyć.
   - Jeśli router, który posiadasz ma słabe hasło, kliknij **ZMIEŃ HASŁO**, aby wejść w jego interfejs i ustawić silniejsze.
   - Jeśli ustawienia sieci, do której jesteś podłączony posiada luki, które mogą wystawić Twój system na ryzyko, kliknij **Zmień ustawienia WI-FI**

Aby skonfigurować ustawienia monitora luk:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.

3. W module **LUKI** kliknij przełącznik WŁĄCZ/WYŁĄCZ.

WAŻNE
Aby być automatycznie powiadamianym o lukach systemowych i aplikacji, **Automatyczne skanowanie luk** powinno być zawsze włączone.

4. Przy użyciu odpowiednich przełączników wybierz luki systemu, które chcesz regularnie sprawdzać.

Krytyczne aktualizacje Windows
Sprawdź, czy Twój system Windows posiada ostatnie krytyczne aktualizacje zabezpieczeń Microsoft.

Aktualizacje aplikacji
Sprawdź, czy aplikacje zainstalowane w Twoim systemie są aktualne. Nieaktualne aplikacje mogą być podatne na atak złośliwego oprogramowania i narazić Twój komputer na ataki z zewnątrz.

Słabe hasła
Sprawdź, czy hasła kont Windows i routerów skonfigurowane na tym systemie są łatwe do odgadnięcia. Utworzenie haseł trudnych do zgadnięcia (silne hasła) utrudnia hakerom włamanie się do Twojego systemu. Silne hasło składa się z wielkich i małych liter, cyfr oraz znaków specjalnych (np. #, $ lub @).

Autouruchamianie nośników danych
Sprawdź stan funkcji autoodtwarzania systemu Windows. Ta opcja pozwala na automatyczne uruchamianie aplikacji z płyt CD i DVD, dysków USB lub innych wymiennych nośników danych.

Niektóre rodzaje szkodliwego oprogramowania używają funkcji autoodtwarzania, aby automatycznie rozprzestrzeniać się z wymiennych nośników danych na komputer. Dlatego zaleca się wyłączenie tej opcji systemu Windows.

Powiadomienia Doradcy Ochrony Wi-Fi
Sprawdź czy domowa sieć bezprzewodowa, do której jesteś podłączony jest zabezpieczona oraz czy ma jakieś luki. Należy także sprawdzić, czy hasło routera domowego jest wystarczająco silne, i jak możesz uczynić je bezpieczniejszym.

Większość niechronionych sieci bezprzewodowych nie jest zabezpieczona, to pozwala "wścibskim oczom" hakerów mieć dostęp do Twoich prywatnych działań.

Notatka
Jeśli wyłączysz monitorowanie wybranych luk, związane z nimi problemy nie będą już zapisane w oknie powiadomień.

20.3. Doradca Ochrony Wi-Fi

Będąc w trasie, pracując na terenie kawiarni, czekając na lotnisku, łączęnie się do publicznych sieci bezprzewodowych, aby sprawdzić maile, konta mediów społecznościowych, wykonać przelewy może być najszybszym rozwiązaniem. Ale wścibskie oczy próbujące przejąć Twoje dane osobowe mogą tam być, obserwując w jaki sposób informacje przeciekają do sieci.

Dane osobiste to hasła i loginy, z których korzystasz przy dostępie do kont internetowych, jak adresy email, konta bankowe, konta mediów społecznościowych, oraz wysłane wiadomości.

Przeważnie, publiczne sieci bezprzewodowe są raczej niezabezpieczone gdyż nie wymagają hasła do zalogowania, jeśli tak, to jest to hasło dostępne dla każdego kto chcę się połączyć. Co więcej, może to być złośliwy program lub sieć typu honeypot, prezentując cel dla cyberprzestępców.

Aby uchronić Cię przed niebezpieczeństwem, nieszyfrowanych i niezabezpieczonych publicznych bezprzewodowych hotspotów. Doradca Wi-Fi Bitdefender analizuje jak chroniona jest sieć, i jeśli to potrzebne zaleca skorzystanie z modułu Bitdefender Safepay™ z zaznaczoną opcją ochrony hotspotu.

Doradca Wi-Fi Bitdefender daje Ci informacje na temat:

- Domowe sieci Wi-Fi
- Publiczne sieci Wi-Fi

20.3.1. Włączanie lub wyłączanie powiadomień Doradcy Ochrony Wi-Fi

Aby włączyć lub wyłączyć powiadomienia Doradcy Ochrony Wi-Fi:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu modułu **LUKI**.

4. W oknie **USTAWIENIA** kliknij odpowiedni przycisk WŁĄCZ/WYŁĄCZ.

20.3.2. Konfigurowanie Domowej sieci Wi-Fi

Aby rozpocząć konfigurowanie Twojej sieci domowej:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **Luki** kliknij **Doradca Ochrony Wi-Fi**.
4. W zakładce **Domowe Wi-Fi**, kliknij przycisk **WYBIERZ DOMOWE WI-FI**.

   Lista sieci bezprzewodowych, do których łączyłeś się do teraz jest wyświetlana.
5. Wskaż swoją sieć domową, a następnie kliknij **WYBIERZ**.

Jeżeli sieć macierzysta jest uważana za niezabezpieczoną lub niebezpieczną, wyświetlane są porady konfiguracyjnych, aby poprawić jej bezpieczeństwo.

Aby usunąć sieć bezprzewodową, którą ustawiłeś jako sieć domową, kliknij przycisk **USUŃ**.

20.3.3. Publiczne Wi-Fi

Podczas połączenia z niezabezpieczoną lub niebezpieczną siecią bezprzewodową, profil publiczny Wi-Fi jest włączony. Kiedy pracując na tym profilu Bitdefender Internet Security 2018 automatycznie stosuje następujące ustawienia:

- Zaawansowana Ochrona Przed Zagrożeniami jest włączona
- Firewall Bitdefender jest włączony i następujące ustawienia są zastosowane dla Twojego bezprzewodowego adaptera:
  - Tryb ukrycia - WŁACZONY
  - Typ sieci - Publiczny
- Następujące ustawienia z Ochrony Webowej są włączone:
  - Skanuj SSL
  - Ochrona przed oszustwami
  - Ochrona przed phishingiem

- Przycisk, który otwiera Bitdefender Safepay™ jest dostępny. W tym przypadku, Ochrona Hotspotu dla niechronionych sieci jest domyślnie włączona.

20.3.4. Sprawdzanie informacji na temat sieci Wi-Fi

Aby sprawdzić informacje o sieciach bezprzewodowych, do których na ogół się łączysz:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **Luki** kliknij **Doradca Ochrony Wi-Fi**.
4. W zależności od informacji, które potrzebujesz, wybierz jedną z dwóch zakładek, **Domowe Wi-Fi** lub **Publiczne Wi-Fi**.
5. Kliknij **Zobacz szczegóły** obok sieci, na której temat chcesz znaleźć więcej informacji.

Istnieją trzy typy sieci bezprzewodowych filtrowanych ze względu na poziom istotności, każdy typ oznaczony jest odpowiednią ikoną:

Wi-Fi jest niebezpieczne - wskazuje, że poziom bezpieczeństwa w sieci jest niski. To oznacza, że jest wysokie ryzyko przy korzystaniu, i nie zalecane aby wykonywać transakcje i sprawdzać konto bez dodatkowej ochrony. W takiej sytuacji, zalecamy aby użyć Bitdefender Safepay™ z włączoną ochroną hotspotu dla niezabezpieczonych sieci.

Wi-Fi jest niebezpieczne - wskazuje, że poziom bezpieczeństwa w sieci jest umiarkowany. To oznacza, że posiada luki w ochronie, i niezalecane jest wykonywanie opłat i sprawdzanie konta bankowego bez dodatkowej ochrony. W takiej sytuacji, zalecamy aby użyć Bitdefender Safepay™ z włączoną ochroną hotspotu dla niezabezpieczonych sieci.

Wi-fi jest bezpieczna - wskazuje, że sieć, której używasz jest bezpieczna. W tym przypadku możesz użyć wrażliwych danych do dokonywania operacji internetowych.

Klikając link w obszarze sieci **Zobacz szczegóły**, następujące szczegóły są wyświetlone:

- **Zabezpieczona** - tu możesz zobaczyć czy wybrane sieci są bezpieczne lub nie. Niezaszyfrowane sieci mogą pozostawić używane dane odsłonięte.
- **Typ szyfrowania** - tutaj możesz zobaczyć typ szyfrowania użyty przez wybraną sieć. Niektóre rodzaje szyfrowania mogą nie być bezpieczne. W

związku z tym, zalecamy sprawdzić informacje o typu szyfrowania, aby upewnić się, że jesteś chroniony w trakcie surfowania po sieci.

- **Kanał/Częstotliwość**- tu możesz zobaczyć częstotliwość kanału z której korzysta wybrana sieć.
- **Siła hasła** - tutaj możesz zobaczyć, jak silne jest hasło. Zapamiętaj, że sieć ze słabym hasłem, może być celem dla cyberprzestępców.
- **Wpisz lub zapisz się** - tu możesz zobaczyć czy wybrana sieć jest chroniona hasłem lub nie. Jest wysoce rekomendowane, aby łączyć się tylko do sieci, które mają ustawione silne hasła.
- **Typ uwierzytelniania** - tu możesz zobaczyć typ uwierzytelniania wybranej sieci.

Miej włączoną opcje **Powiadamiaj** aby otrzymywać powiadomienia za każdym razem gdy Twój system łączy się do sieci.

21. OCHRONA KAMERY INTERNETOWEJ

Hakerzy mogą przejąć kontrolę nad twoją kamerą aby cię szpiegować, to nie jest nowość, oraz rozwiązań do ochrony przed tym, takie jak odebranie uprawnień aplikacji, wyłączenie wbudowanej kamery, lub przykrycie jej nie jest zbyt praktyczne. Aby zablokować dalsze próby uzyskania dostępu do twojej prywatności Ochrona Kamery Bitdefender stale sprawdza aplikacje, które próbują uzyskać dostęp do kamery i zablokować te, które nie są uznane za zaufane.

Jako środek bezpieczeństwa będziesz zawsze powiadamiany jeśli niezaufana aplikacja spróbuje uzyskać dostęp do twojej kamery, jeśli nawet funkcjonalność Autopilota jest włączona.

21.1. Włączanie lub wyłączanie Ochrony Kamery

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W panelu **OCHRONA KAMERY**, kliknij przełącznik ON/OFF.

21.2. Konfigurowanie Ochrony Kamery

Możesz skonfigurować reguły, które mają być stosowane, gdy aplikacja próbuje uzyskać dostęp do aparatu, wykonując następujące czynności:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Kliknij ikonę w prawym dolnym rogu modułu **OCHRONA KAMERY INTERNETOWEJ**.

Zasady blokowania aplikacji

- **Zablokuj całkowicie dostęp do kamery internetowej** - żadna aplikacja nie będzie miała dostępu do kamery internetowej.
- **Zablokuj przeglądarkom dostęp do kamery** - żadna przeglądarka internetowa, z wyjątkiem programu Internet Explorer i Microsoft Edge, nie będzie miała dostępu do kamery internetowej. Ze względu na procedurę aplikacji Windows Store w jednym procesie Internet Explorer i Microsoft

Edge nie mogą zostać wykryte przez Bitdefender jako przeglądarki internetowe, dlatego są wykluczone z tego ustawienia.

- **Ustaw dostęp do kamery internetowej aplikacji na podstawie wyboru użytkowników Bitdefender** - jeśli większość użytkowników Bitdefender uzna, że popularna aplikacja jest nieszkodliwa, jej dostęp do kamery internetowej zostanie automatycznie ustawiony na Zezwalaj. Jeśli popularna aplikacja jest często uznawana za niebezpieczną, to jej dostęp automatycznie będzie blokowany.

  Będziesz informowany za każdym razem, gdy jedna z zainstalowanych aplikacji zostanie wyświetlona jako zablokowana przez większość użytkowników Bitdefender, nawet jeśli jest włączona funkcja Autopilot.

Powiadomienia

- **Powiadom, kiedy dozwolone aplikacje łączą się z kamerą internetową** - otrzymasz powiadomienie za każdym razem, gdy dozwolona aplikacja uzyska dostęp do kamery internetowej, nawet jeśli została włączona funkcja Autopilot.

21.3. Dodawanie aplikacji do listy Ochrony Kamery Internetowej

Aplikacje, które próbują się połączyć do twojej kamery są automatycznie wykrywane oraz opierając się na ich zachowaniu oraz wyborze społeczności, ich dostęp jest dopuszczony lub zablokowany. Jednakże, możesz samodzielnie zacząć konfigurować jakie akcje powinny być podjęte poprzez wykonane tych kroków:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W panelu **OCHRONA KAMERY**, kliknij **Dopuszczone Kamery**.
4. W oknie z opisem funkcji Ochrony Kamery Internetowej, kliknij link **Zacznij dodawać aplikacje do listy dopuszczonych do kamery internetowej**.
5. Znajdź plik .exe, który chcesz dodać do listy i kliknij **OK**.
6. Kliknij przełącznik Dostęp dopuszczony/Dostęp zablokowany.

   Aby sprawdzić, co użytkownicy Bitdefender, zdecydowali się zrobić z wybraną aplikacją, kliknij ikonę .

Aby dodać dodatkowe aplikacje, kliknij link **Dodaj nową aplikacje do listy**.

Aplikacje, które poproszę o dostęp do kamery wraz z czasem ostatniej aktywności pojawi się w tym oknie.

Będziesz powiadamiany za każdym razem, kiedy jedna z dopuszczonych aplikacji jest zablokowana przez użytkowników Bitdefender, nieważnie od statusu Autopilota.

Notatka

Kiedy aplikacje Windows Store uruchamiają się jako pojedynczy proces, za każdym razem kiedy dostęp aplikacji jest ustawiony na Zezwól lub Zablokuj, reguła będzie przypisana do całego systemu. Internet Explorer i Microsoft Edge to dwa przykłady takich aplikacji.

22. BEZPIECZNE PLIKI

Ransomware to złośliwe oprogramowanie, które atakuje podatne systemy blokując je, i prosi o pieniądze, aby użytkownik mógł odzyskać kontrolę nad swoim systemem. To złośliwe oprogramowanie działa inteligentnie wyświetlając fałszywe wiadomości, aby sprawić, że użytkownik spanikuje i dokona płatności, o którą go poproszono.

Infekcja może rozprzestrzeniać się za pośrednictwem spamu, przez pobieranie załączników, lub odwiedzając zainfekowane strony internetowe i instalację złośliwych aplikacji, nie pozwalając użytkownikowi wiedzieć, co dzieje się w jego systemie.

Ransomware może mieć jeden z następujących zachowań uniemożliwiających użytkownikowi dostęp do jego systemu:

- Szyfrowanie poufnych i osobistych plików, nie dając możliwości deszyfrowania dopóki okup nie zostanie wpłacony przez ofiarę.
- Blokuje ekran komputera i wyświetla wiadomość z prośbą o pieniądze. W tym przypadku, żaden plik nie jest zaszyfrowany, tylko użytkownik jest zmuszony do dokonania płatności.
- Blokuje aplikacje, aby się nie uruchamiały.

Dzięki Bezpiecznym Plikom Bitdefender możesz chronić przed ransomware pliki osobiste, takie jak dokumenty, zdjęcia czy filmy.

Notatka

Aktywna Kontrola Zagrożeń i Bezpieczne Pliki są dwiema warstwami ochrony przed ransomware. Aktywna Kontrola Zagrożeń to funkcja, która blokuje ataki ransomware na najważniejsze obszarów Twojego systemu, a Bezpieczne Pliki chronią ważne pliki na Twoim komputerze przed szyfrowaniem.

22.1. Włączanie i wyłączanie Bezpiecznych Plików.

Aby włączyć lub wyłączyć opcje Bezpiecznych Plików:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **BEZPIECZNE PLIKI** kliknij przełącznik WŁĄCZ/WYŁĄCZ.

Za każdym razem, gdy aplikacja będzie próbowała uzyskać dostęp do chronionego pliku, pojawi się wyskakujące okienko Bitdefender. Możesz zezwolić lub odmówić dostępu.

Notatka
Funkcja Bezpieczne pliki jest domyślnie włączona.

22.2. Chroń prywatne pliki przed atakami ransomware

Jeśli chcesz umiejscowić osobiste pliki w bezpiecznym miejscu:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **BEZPIECZNE PLIKI** kliknij **Chronione Foldery**.
4. W oknie z opisem funkcji Bezpieczne Pliki, kliknij **CHROŃ WIĘCEJ FOLDERÓW**.
5. Wybierz folder, który chcesz chronić i kliknij **OK**.

   Ab dodać foldery, kliknij link **Chroń więcej folderów**. Lub przeciągnij foldery do tego okna.

Domyślnie, foldery Obrazki, Filmy, Muzyka, Pulpit i Pobrane są chronione przed atakami zagrożeń. Dane osobowe przechowywane w hostingowych serwisach plików online, takich jak Box, Dropbox, Google Drive i OneDrive również zaliczają się do chronionego środowiska, pod warunkiem, że ich aplikacje są zainstalowane w systemie.

Aby uniknąć spowolnienia systemu, zaleca się dodanie maksymalnie 30 folderów lub zapisanie wielu plików w jednym folderze.

Notatka
Foldery niestandardowe mogą być chronione tylko dla obecnych użytkowników. Pliki systemowe i aplikacji nie mogą być dodane do wyjątków.

22.3. Konfigurowanie dostępu do aplikacji

Te aplikacje, które próbują zmienić lub usunąć chronione pliki, mogą zostać oznaczone jako potencjalnie niebezpieczne oraz dodane do listy zablokowanych aplikacji. Jeśli dana aplikacja jest blokowana, ale jesteś pewien, że działa normalnie, możesz dodać ją do wyjątków w następujących krokach:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **BEZPIECZNE PLIKI** kliknij **Dostęp do aplikacji**.
4. Aplikacje, które usiłowały zmienić pliki w chronionych folderach są wypisane. Kliknij przycisk Zezwól obok aplikacji, którą uważasz za bezpieczną.

W tym samym oknie można wyłączyć ochronę ransomware dla konkretnych aplikacji, klikając przycisk Blokuj.

Jeśli chcesz dodać do listy nowe aplikacje, kliknij link **Dodaj nowe aplikacje**.

22.4. Ochrona przy starcie systemu

Wiadomo, że wiele złośliwych aplikacji jest ustawionych, aby uruchamiały się przy starcie systemu, jest to fakt, który może poważnie uszkodzić maszynę. Ochrona Bitdefender podczas rozruchu skanuje wszystkie obszary krytyczne systemów zanim wszystkie pliki zostaną załadowane, z zerowym wpływem na system.

Aby wyłączyć ochronę przy rozruchu:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę prawym dolnym rogu **BEZPIECZNE PLIKI**.
4. Kliknij przełącznik WŁĄCZ/WYŁĄCZ.

Notatka

Aplikacje dodane do wykluczeń będą również skanowane i odpowiednio traktowane.

23. OCHRONA MANAGER HASEŁ DLA TWOICH POŚWIADCZEŃ

Wykorzystujemy komputery do robienia zakupów online lub płacenia rachunków, łączymy się z sieciami społecznościowymi lub logujemy do komunikatorów internetowych.

Każdy użytkownik zdaje sobie sprawę, że pamiętanie wielu haseł może być nie lada problemem!

Jeśli jednak niezbyt ostrożnie przeglądamy internet, nasze prywatne informacje, takie jak nasz adres e-mail, nasz identyfikator w komunikatorze lub dane karty kredytowej mogą być zagrożone.

Trzymanie swoich haseł lub danych osobistych na kartce papieru albo w komputerze może być niebezpieczne ponieważ mogą się do nich dostać osoby zamierzające je ukraść i wykorzystać. Pamiętanie każdego hasła swoich kont online lub do wielu ulubionych stron nie jest łatwym zadaniem.

Zatem, czy jest sposób, żeby mieć pewność, że znajdziemy swoje hasła gdy ich potrzebujemy? I czy możemy spać spokojnie myśląc, że nasze tajne hasła są zawsze bezpieczne?

Manager Haseł pomaga Ci mieć pod kontrolą Twoje hasła, chroni Twoją prywatność i zapewnia bezpieczeństwo przy korzystaniu z Internetu.

Używając jednego głównego hasła dostępu do danych logowania, Manager Haseł sprawia, że łatwo można przechowywać swoje hasła bezpieczne w Portfelu.

Aby zapewnić najlepszą ochronę aktywności online, Manager Haseł został zintegrowany z modułem Bitdefender Safepay™, tworząc w ten sposób ujednolicone rozwiązanie, zapobiegające wielu metodom kradzieży poufnych danych.

Manager Haseł chroni następujące poufne informacje:

- Dane osobowe, takie jak adres e-mail, czy numer telefonu
- Dane logowania na stronach internetowych
- Informacje o koncie bankowym i numery kart kredytowych
- Dane dostępowe do kont pocztowych
- Hasła do aplikacji

- Hasła do sieci Wi-Fi

23.1. Stwórz nową bazę danych Portfela

Portfel Bitdefender jest miejscem, w którym możesz przechowywać swoje dane osobowe. Dla łatwiejszego przeglądania stron, musisz utworzyć bazę danych Portfela jak poniżej:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W panelu **PORTFEL** kliknij **Stwórz nowy Portfel**.
4. Kliknij przycisk **Utwórz nowy**.
5. W odpowiednich polach wprowadź wymagane informacje.
   - Etykieta Portfela - wpisz unikalną nazwę dla bazy danych Portfela.
   - Hasło Główne - wpisz hasło dla swojego Portfela.
   - Wpisz ponownie Hasło - wpisz ponownie hasło, które ustawiłeś.
   - Podpowiedź - wpisz wskazówkę, aby zapamiętać hasło.
6. Kliknij "**Kontynuuj**".
7. Na tym etapie możesz wybrać przechowywanie swoich danych w chmurze. Jeśli wybierzesz Tak, informacje bankowe zostaną zapisane lokalnie na urządzeniu. Wybierz pożądaną opcję, a następnie kliknij **Kontynuuj**.
8. Wybierz przeglądarkę internetową, z której chcesz zaimportować poświadczenia.
9. Kliknij "**Zakończ**".

23.2. Importuj istniejącą bazę danych

Aby zaimportować bazę danych portfela przechowywaną lokalnie:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W panelu **PORTFEL** kliknij **Stwórz nowy Portfel**.
4. Kliknij przycisk **Od Celu**.
5. Znajdź lokacje twojej bazy danych portfela i wybierz (plik .db)

6. Kliknij "**Otwórz**".
7. Nadaj nazwę dla swojego Portfela i wpisz hasło przypisane przy jego tworzeniu.
8. Kliknij opcję **Importuj**.
9. Wybierz programy, w których chcesz importować poświadczenia przez Portfel, następnie kliknij przycisk **Zakończ**.

23.3. Eksportuj bazę danych Portfela

Aby wyeksportować bazę danych Portfela:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Na panelu **Portfel** kliknij **Moje Portfele**.
4. Kliknij ikonę na wybranym Portfelu, a następnie wybierz **Exportuj**.
5. Znajdź lokacje twojej bazy danych portfela i wybierz (plik .db)
6. Kliknij **Zapisz**.

Notatka

Portfel musi być otwarty, aby opcja **Eksportuj** była dostępna.
Jeśli portfel, który chcesz eksportować jest zamknięty, kliknij przycisk **AKTYWUJ PORTFEL** następnie wpisz hasło, które jest do niego przypisane od początku.

23.4. Synchronizuj swoje portfele w chmurze

Aby włączyć lub wyłączyć synchronizację portfeli w chmurze:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Na panelu **Portfel** kliknij **Moje Portfele**.
4. Kliknij ikonę na wybranym Portfelu, a następnie wybierz **Ustawienia**.
5. Wybierz pożądaną opcję w oknie, które się pojawi, a następnie kliknij **Zapisz**.

Notatka
Portfel musi być otwarty, aby opcja **Eksportuj** była dostępna.
Jeśli portfel, który chcesz synchronizować jest zamknięty, kliknij przycisk **AKTYWUJ PORTFEL** następnie wpisz hasło, które jest do niego przypisane od początku.

23.5. Zarządzaj danymi logowania Portfela

Aby zarządzać swoimi hasłami:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Na panelu **Portfel** kliknij **Moje Portfele**.
4. Wybierz pożądaną bazę danych Portfela z sekcji **MOJE PORTFELE**, a następnie kliknij przycisk **AKTYWUJ PORTFEL**.
5. Wpisz hasło główne, a następnie kliknij **OK**.

Pojawi się nowe okno. W górnej części okna wybierz wymaganą kategorię:

- Tożsamość
- Strony WWW
- Bankowość elektroniczna
- E-maile
- Aplikacje
- Sieci Wi-Fi

Dodawanie/ edytowanie poświadczeń

- Aby dodać nowe hasło, w górnej części okna wybierz żądaną kategorię, kliknij **+ Dodaj element**, wprowadź informacje w odpowiednich polach i kliknij przycisk Zapisz.
- Aby edytować element z tabeli, zaznacz go i kliknij przycisk **Edytuj**.
- Aby usunąć wpis, zaznacz go i kliknij przycisk **Usuń**.

23.6. Włączanie lub wyłączanie ochrony Managera Haseł

Aby włączyć lub wyłączyć ochronę Managera Haseł:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **Portfel** kliknij przełącznik WŁĄCZ/WYŁĄCZ.

23.7. Zarządzanie ustawieniami Manager Haseł

Aby skonfigurować szczegółowo hasło główne:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu modułu **PORTFEL**.
4. Wybierz zakładkę **Ustawienia Bezpieczeństwa**.

Dostępne są następujące opcje:

- **Pytaj o moje główne hasło, kiedy zaloguję się na komputerze** - przy próbie dostępu do komputera zostanie wyświetlona prośba o podanie głównego hasła.
- **Pytaj o moje główne hasło, kiedy uruchamiam przeglądarki lub aplikacje** - prośba o podanie głównego hasła zostanie wyświetlona przy próbie dostępu do przeglądarki lub aplikacji.
- **Automatycznie blokuj Portfel, kiedy jestem z dala od komputera** - prośba o podanie głównego hasła zostanie wyświetlona po 15-minutowej bezczynności komputera.

WAŻNE

Upewnij się, że nie zapomnisz głównego hasła, a najlepiej zapisz je i przechowuj w bezpiecznym miejscu. Jeżeli hasło zostanie zapomniane, należy ponownie zainstalować produkt, lub skontaktować się z działem wsparcia Bitdefender.

Zwiększanie funkcjonalności

Aby wybrać przeglądarki lub aplikacje, które chcesz, by zintegrowały się z Managerem Haseł:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu modułu **PORTFEL**.
4. Wybierz zakładkę **Wtyczki**.

   Sprawdź aplikację, która będzie korzystała z Managera Haseł, aby ulepszyć funkcjonalność:

   - Microsoft Edge
   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Konfiguracja automatycznego uzupełniania

Funkcja automatycznego wpisywania ułatwia otwieranie ulubionych stron lub logowanie do kont online. Podczas pierwszego wprowadzenia danych logowania i danych osobowych w swojej przeglądarce internetowej, są one automatycznie zabezpieczone w Portfelu.

Aby skonfigurować ustawienia **Autouzupełniania**:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu modułu **PORTFEL**.
4. Wybierz zakładkę **Ustawienia autouzupełniania**.
5. Skonfiguruj następujące opcje:
   - **Skonfiguruj, jak Portfel ma chronić Twoje dane logowania**:
     - **Automatycznie zapisz poświadczenia w Portfelu** - poświadczenia logowania i inne informacje identyfikujące, takie jak dane osobiste i

dane karty kredytowej są automatycznie zapisywane i aktualizowane w Portfelu.

- **Pytaj za każdym razem** - będziesz pytany za każdym razem, gdy zechcesz dodać swoje hasło do Portfela.
- **Nie zachowuj, zaktualizuję te informacje samodzielnie** - hasło może być dodane do Portfela jedynie własnoręcznie.

- **Automatycznie uzupełniaj dane logowania**:
  - **Automatycznie wypełniaj hasła za każdym razem** - hasła będą automatycznie wpisywane do przeglądarki.
- **Automatycznie uzupełniaj formularze**:
  - **Pytaj o opcje uzupełniania, gdy odwiedzam stronę z formularzami** - okienko z opcjami uzupełniania pojawi się za każdym razem, gdy Bitdefender wykryje, że chcesz wykonać płatności online lub chcesz się zarejestrować lub zalogować.

Zarządzanie informacjami Managera Haseł z przeglądarki

Możesz łatwo zarządzać szczegółami Managera Haseł bezpośrednio z przeglądarki, aby wszystkie ważne dane mieć na wyciągnięcie ręki. Dodatek "Portfel" Bitdefender jest obsługiwany przez następujące przeglądarki: Google Chrome, Internet Explorer i Mozilla Firefox, jest również zintegrowany z modułem Safepay.

Aby uzyskać dostęp do rozszerzenia Portfela Bitdefender, otwórz przeglądarkę internetową, pozwól na zainstalowanie dodatku i kliknij ikonę na pasku narzędziowym.

Rozszerzenie Portfela Bitdefender zawiera następujące opcje:

- Otwórz Portfel - otwiera Portfel.
- Blokuj Portfel - blokuje Portfel.
- Strony www - otwiera podmenu z wszystkimi logowaniami do stron internetowych zapisanych w Portfelu. Kliknij **Dodaj stronę**, aby dodać nową stronę do listy.
- Wypełnij formularze - otwiera podmenu zawierające informację, którą dodano dla określonej kategorii. Stąd możesz dodać nowe dane do swojego Portfela.

- Generator Haseł - Pozwala na generowanie losowych haseł, które możesz użyć dla nowych lub istniejących kont. Kliknij **Pokaż zaawansowane ustawienia**, aby dostosować złożoność hasła.
- Ustawienia - otwiera okno ustawień Managera Haseł.
- Zgłoś problem - zgłaszaj każdy problem, który napotkasz z Managerem Haseł Bitdefender.

24. BEZPIECZNE PŁATNOŚCI ONLINE

Komputer szybko staje się głównym narzędziem do robienia zakupów i przeprowadzania transakcji bankowych. Płacenie rachunków, przelewy, kupowanie prawie wszystkiego, co można sobie wyobrazić nigdy nie było szybsze i łatwiejsze.

Obejmuje to wysyłanie informacji osobistych, kont i danych kart kredytowych, haseł i innych rodzajów informacji prywatnych przez internet, czyli dokładnie taki rodzaj informacji, którym cyberprzestępcy są bardzo zainteresowani. Hakerzy są nieustępliwi w dążeniu do kradzieży takich informacji, więc nigdy nie można być zbyt ostrożnym, zabezpieczając transakcje online.

Moduł Bitdefender Safepay jest przede wszystkim bezpieczną przeglądarką - odizolowanym środowiskiem, które zostało zaprojektowane do utrzymania poufności wszelkich danych dotyczących przelewów, płatności i transakcji w internecie.

Dla zachowania najlepszej ochrony prywatności, Manager Haseł Bitdefender został zintegrowany z Bitdefender Safepay™, aby zabezpieczać dane logowania podczas dostępu do prywatnych zasobów online. Aby uzyskać więcej informacji, odwołaj się do *„Ochrona Manager Haseł dla Twoich poświadczeń”* (p. 146).

Moduł Bitdefender Safepay oferuje następujące funkcje:

- Blokuje dostęp do Twojego pulpitu i każdej próby wykonania zrzutu ekranu.
- Chroni Twoje tajne hasła, podczas przeglądania stron internetowych z Managerem Haseł.
- Wyposażony jest w wirtualną klawiaturę, która uniemożliwia hakerom odczytywanie używanych klawiszy.
- Jest to narzędzie całkowicie niezależne od innych przeglądarek.
- Wyposażone jest w zintegrowaną ochronę hotspotów używaną wtedy, gdy Twój komputer jest podłączony do niezabezpieczonych sieci Wi-Fi.
- Obsługuje zakładki i pozwala na poruszanie się pomiędzy ulubionymi stronami banków i sklepów.
- Nie ogranicza się jednak tylko do bankowości i e-sklepów. Każda strona może zostać otwarta w module Bitdefender Safepay.

24.1. Używanie modułu Bitdefender Safepay

Domyślnie, Bitdefender wykrywa, kiedy przechodzisz do witryny internetowej banku lub sklepu internetowego w każdej przeglądarce na Twoim komputerze i wyświetla monit, aby uruchomić taka witrynę w oknie modułu Bitdefender Safepay.

Aby uzyskać dostęp do głównego interfejsu modułu Bitdefender Safepay, skorzystaj z jednej z następujących metod:

- Z interfejsu Bitdefender:
  1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  2. Kliknij przycisk akcji **Safepay**.
- Z systemu Windows:
  - W systemie **Windows 7**:
    1. Kliknij **Start** i przejdź do **Wszystkie programy**.
    2. Kliknij **Bitdefender**.
    3. Kliknij **Bitdefender Safepay™**.
  - W systemach **Windows 8 i Windows 8.1**:

    Zlokalizuj moduł Bitdefender Safepay na ekranie Windows Start (dla przykładu, możesz zacząć wpisywać "Bitdefender Safepay" bezpośrednio na ekranie Start), a następnie kliknij jego ikonę.
  - W systemie **Windows 10**:

    Wpisz "Bitdefender Safepay™" w polu wyszukiwania z paska zadań, a następnie kliknij jego ikonę.

Notatka

Jeżeli wtyczka Adobe Flash Player nie jest zainstalowana lub jest nieaktualna, Bitdefender wyświetli odpowiedni komunikat. Aby kontynuować, kliknij odpowiedni przycisk.
Po zakończeniu instalacji, należy ponownie ręcznie otworzyć przeglądarkę Bitdefender Safepay, aby kontynuować swoją pracę.

Jeśli jesteś przyzwyczajony do przeglądarek internetowych, nie będziesz miał problemów z używaniem modułu Bitdefender Safepay - wygląda i zachowuje się jak zwykła przeglądarka:

- W pasku adresu wpisz adres URL, do którego chcesz przejść.
- dodawaj zakładki do odwiedzenia wielu stron internetowych w oknie Bitdefender Safepay klikając .
- nawiguj w przód i wstecz, odświeżaj strony używając odpowiednio .
- uzyskaj dostęp do ustawień Bitdefender Safepay™ klikając i wybierając **Ustawienia**.
- chroń swoje hasła za pomocą Managera Haseł klikając .
- zarządzaj swoimi zakładkami, klikając obok paska adresu.
- otwórz wirtualną klawiaturę klikając .
- zwiększ lub zmniejsz rozmiar przeglądarki naciskając jednocześnie klawisze **Ctrl** i **+/-** na klawiaturze numerycznej.
- wyświetl informacje o swoim produkcie Bitdefender klikając i wybierając **O nas**.
- wydrukuj ważne informacje klikając .

Notatka
Aby przełączać się między pulpitem Windows i Bitdefender Safepay™ naciśnij kombinacje klawiszy **Alt+Tab**, lub kliknij przycisk **Minimalizuj**.

24.2. Konfigurowanie ustawień

Kliknij i wybierz **Ustawienia**, aby skonfigurować Bitdefender Safepay™:

- W **Ustawieniach Ogólnych** możesz ustawić następujące:

Zachowanie Bitdefender Safepay™
Wybierz co się stanie, gdy wejdziesz na stronę sklepu internetowego lub banku w swojej zwykłej przeglądarce internetowej:
- Automatycznie otwiera strony w module Safepay.
- Zalecaj mi użycie modułu Bezpiecznych płatności.
- Nie proponuj mi używania modułu Safepay.

Lista domen
Wybierz sposób, w jaki Bitdefender Safepay będzie się zachowywać podczas odwiedzania witryn z poszczególnych domen w

przeglądarkach WWW, dodając je do listy domen i wybierając zachowanie dla każdej z nich:

- Otwórz automatycznie w module Bitdefender Safepay.
- Niech Bitdefender zapyta o działanie za każdym razem.
- Nigdy nie używaj modułu Bitdefender Safepay podczas odwiedzania strony z domeny w zwykłej przeglądarce.

Blokowanie wyskakujących okienek

Możesz wybrać, aby zablokować wyskakujące okienka, klikając odpowiedni przycisk.

Możesz także utworzyć listę stron internetowych, dla których zezwolisz na wyskakujące okienka. Na tej liście powinny znajdować się tylko w pełni zaufane strony.

Aby dodać stronę do listy, wprowadź jej adres w odpowiednie pole i kliknij "**Dodaj domenę**".

Aby usunąć stronę z listy, naciśnij X przy wybranym wpisie.

Włączona ochrona Hotspot

Możesz włączyć dodatkową warstwę ochrony w przypadku podłączania do niezabezpieczonych sieci Wi-Fi, włączając tę funkcję.

Wejdź *„Ochrona hotspotów dla niezabezpieczonych sieci"* (p. 158), aby uzyskać więcej informacji.

- W polu **Zaawansowane Ustawienia**, są dostępne następujące opcje:

Zarządzaj wtyczkami

Możesz wybrać czy chcesz włączyć lub wyłączyć wybrane wtyczki w Bitdefender Safepay™.

Zarządzaj certyfikatami

Możesz zaimportować certyfikaty ze swojego systemu do magazynu certyfikatów.

Wybierz **Importuj certyfikaty** i postępuj zgodnie z kreatorem aby korzystać z nich w Bitdefender Safepay™.

Automatycznie uruchamiaj Klawiaturę wirtualną w polach haseł

Klawiatura wirtualna pojawi się automatycznie gdy wybierzesz pole z hasłem.

Użyj odpowiedniego przełącznika, aby włączyć lub wyłączyć funkcję.

Zapytaj o potwierdzenie przed drukowaniem
Włącz tą opcje jeśli chcesz potwierdzać przed rozpoczęciem procesu drukowania.

24.3. Zarządzanie zakładkami

Jeśli wyłączyłeś automatyczne wykrywanie niektórych lub wszystkich stron, lub Bitdefender po prostu nie wykrywa niektórych stron internetowych, możesz dodać zakładki do modułu Bitdefender Safepay, dzięki czemu możesz z łatwością uruchomić ulubione strony internetowe w przyszłości.

Wykonaj następujące kroki, aby dodać adres URL do zakładek modułu Bitdefender Safepay:

1. Kliknij ikonę obok paska adresu, aby otworzyć stronę Zakładki.

   Notatka
   Strona zakładek otwierana jest domyślnie po uruchomieniu modułu Bitdefender Safepay.

2. Kliknij przycisk **+**, aby dodać nową zakładkę.
3. Wpisz adres URL i tytuł zakładki i kliknij **Utwórz**. Sprawdź opcję **Automatycznie otwórz w Safepay** jeśli chcesz, aby wybrana strona była otwierana w Bitdefender Safepay™ za każdym razem, gdy uzyskujesz do niej dostęp. Adres URL jest również dodany do listy domen na stronie "Ustawienia".

24.4. Ochrona hotspotów dla niezabezpieczonych sieci

Podczas korzystania z modułu Bitdefender Safepay podczas połączenia z niezabezpieczonymi sieciami Wi-Fi (na przykład publiczne hotspoty) dodatkową warstwą zabezpieczeń jest funkcja ochrony hotspotów. Usługa ta szyfruje komunikację internetową na niezabezpieczonych połączeniach, pomaga utrzymać prywatność niezależnie od tego do jakiej sieci jesteś podłączony.

Ochrona Hotspot działa tylko wtedy, gdy Twój komputer jest podłączony do niezabezpieczonej sieci.

Zainicjowane będzie bezpieczne połączenie i zostanie wyświetlona wiadomość w oknie modułu Bitdefender Safepay, gdy nawiążesz połączenie.

Symbol pojawia się przed adresem URL w pasku adresu, aby pomóc Ci łatwo zidentyfikować bezpieczne połączenia.

Możliwe, że musisz potwierdzić akcję.

25. OCHRONA DANYCH

25.1. Trwałe usuwanie plików

Gdy skasujesz plik, nie może on być otwarty w normalny sposób. Jednakże plik nadal jest przechowywany na dysku, aż zostanie nadpisany przy kopiowaniu nowych plików.

Niszczarka plików Bitdefender umożliwia trwałe usunięcie danych przez fizyczne usunięcie ich z dysku twardego.

Możesz szybko zniszczyć pliki lub foldery, korzystając z kontekstowego menu Windows, wykonując następujące czynności:

1. Kliknij prawym przyciskiem myszy plik lub folder, który chcesz trwale usunąć.
2. Wybierz **Bitdefender** > **Niszczarka plików** z menu kontekstowego, które się pojawi.
3. Pojawia się okno potwierdzające. Kliknij "**Tak, USUŃ**", aby uruchomić kreator Niszczarki plików. Poczekaj, aż Bitdefender zakończy niszczenie plików.
4. Wyniki są wyświetlane. Kliknij "**Zakończ**", aby wyjść z kreatora.

Alternatywnie, możesz zniszczyć pliki z poziomu interfejsu produktu Bitdefender jak niżej:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **OCHRONY DANYCH**, wybierz **Niszczarkę plików**.
4. Postępuj z godnie z instrukcjami Kreatora Niszczarki plików:
   a. Kliknij przycisk **DODAJ FOLDERY**, aby dodać pliki lub foldery, które chcesz permanentnie usunąć.

      Alternatywnie, przeciągnij te pliki lub foldery do tego okna.

   b. Kliknij **TRWALE USUŃ PLIKI**, a następnie potwierdź, że chcesz kontynuować proces.

      Poczekaj, aż Bitdefender zakończy niszczenie plików.

   c. **Podsumowanie wyników**

Wyniki są wyświetlane. Kliknij "**Zakończ**", aby wyjść z kreatora.

26. ASYSTENT RODZICA

Funkcja Asystenta Rodzica pozwala na kontrolowanie dostępu do Internetu i określonych aplikacji dla każdego urządzenia, na którym jest zainstalowana ta funkcja. Po skonfigurowaniu Asystenta Rodzica, można łatwo dowiedzieć się, co Twoje dziecko robi na używanych urządzeniach i gdzie było w ciągu ostatnich 24 godzin. Ponadto, aby pomóc Ci się więcej dowiedzieć, co robi Twoje dziecko, aplikacja daje Ci statystyki dotyczące jego działalności i zainteresowań.

Potrzebujesz jedynie komputera z dostępem do internetu i przeglądarką internetową.

Możesz skonfigurować Asystenta Rodzica, aby blokował:

- nieodpowiednie strony internetowe.
- aplikacje, takie jak: gry, komunikatory internetowe, programy do udostępniania plików i wiele innych.
- konkretne kontakty, które nie mogą wejść w kontakt telefoniczny z Twoim dzieckiem.

Sprawdź aktywność Twojego dziecka i zmień ustawienia Asystenta Rodzica korzystając z konta Bitdefender z jakiegokolwiek komputera lub urządzenia mobilnego podłączonego do Internetu.

26.1. Uzyskiwanie dostępu do Asystenta Rodzica - MOJE DZIECI

Po uzyskaniu dostępu do sekcji Asystent Rodzica, okno **MOJE DZIECI** jest dostępne. Tutaj możesz wyświetlać i edytować wszystkie profile, które utworzyłeś dla swojego dziecka. Profile są wyświetlane jako karty profilowe, co pozwala szybko nimi zarządzać i sprawdzać ich statusy w mgnieniu oka.

Jak tylko utworzysz profil, możesz rozpocząć dostosowywanie bardziej szczegółowych ustawień do monitorowania i kontrolowania dostępu do Internetu i określonych aplikacji dla swoich dzieci.

Możesz uzyskać dostęp do ustawień Asystenta Rodzica z Bitdefender Central na dowolnym komputerze lub urządzeniu mobilnym podłączonym do Internetu.

Uzyskaj dostęp do swojego konta Bitdefender:

- na dowolnym urządzeniu z dostępem do internetu:
  1. Uzyskaj dostęp do Bitdefender Central.
  2. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
  3. Wybierz moduł **Asystent Rodzica**.
  4. W oknie **MOJE DZIECI**, które się pojawia, możesz zarządzać i konfigurować profile Asystenta Rodzica dla każdego urządzenia.
- Z interfejsu Twojego produktu Bitdefender:
  1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  2. Kliknij link **POKAŻ FUNKCJE**.
  3. W module **Asystent Rodzica** wybierz **Konfiguruj**.

     Jesteś przekierowany do strony konta Bitdefender. Upewnij się, że jesteś zalogowany przy użyciu swoich poświadczeń.
  4. Wybierz moduł **Asystent Rodzica**.
  5. W oknie **MOJE DZIECI**, które się pojawia, możesz zarządzać i konfigurować profile Asystenta Rodzica dla każdego urządzenia.

Notatka
Upewnij się, że jesteś zalogowany na komputerze z kontem administratora. Tylko użytkownicy z prawami administracyjnymi (administratorzy systemu) mają dostęp do Asystenta Rodzica.

26.2. Dodawanie profilu Twojego dziecka

Aby rozpocząć monitorowanie aktywności swojego dziecka, musisz skonfigurować profil i zainstalować Agenta Asystent Rodzica Bitdefender na urządzeniach, z których korzysta.

Aby dodać profil Twojego dziecka do Asystenta Rodzica:

1. Uzyskaj dostęp do panelu Asystent Rodzica z Bitdefender Central.
2. Kliknij **DODAJ PROFIL** po prawej stronie okna **Moje Dzieci**.
3. Ustaw konkretne informacje w odpowiednich polach, takie jak: imię i data urodzenia. Aby dodać zdjęcie profilowe kliknij link **Wybierz plik**. Kliknij **NASTĘPNY KROK** aby kontynuować.

W oparciu o normy rozwoju dzieci, ustawiając datę narodzin dziecka automatycznie ładują się ustawienia uważane za właściwe dla jego kategorii wiekowej.

4. Jeśli urządzenie Twojego dziecka ma już zainstalowany Bitdefender Internet Security 2018, wybierz jego urządzenie z dostępnej listy, wybierz konto, które chcesz monitorować. Kliknij **ZAPISZ**.

   Jeśli dziecko używa urządzenia z Androidem lub iOS i Asystent Rodzica Bitdefender nie jest zainstalowany, kliknij **DODAJ URZĄDZENIE**. Jeśli dziecko używa urządzenia Mac, a Antywirus dla Mac Bitdefender nie jest zainstalowany, kliknij ten sam przycisk. Wybierz system operacyjny, którego applikację chcesz zainstalować, a następnie kliknij **NASTĘPNY KROK** aby kontynuować.

5. Wpisz adres e-mail, na który mamy wysłać link do pobrania instalatora aplikacji Bitdefender , a następnie kliknij **WYŚLIJ LINK INSTALACYJNY**.

WAŻNE

Na urządzeniach z systemem Windows, Bitdefender Internet Security 2018 zawarty w Twojej subskrypcji trzeba pobrać i zainstalować.
W urządzeniach z systemem macOS należy pobrać i zainstalować Antywirus Bitdefender dla produktów Mac.
Na urządzeniach z systemem Android aplikacja Asystenta Rodzica Bitdefender musi zostać pobrana i zainstalowana.

26.2.1. Przypisywanie wielu urządzeń do tego samego profilu

Możesz przypisać wiele urządzeń do tego samego profilu, aby zastosować te same ograniczenia:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz moduł Asystent Rodzica.
3. Kliknij ikonę ⋮ na pożądanej karcie profilu, a następnie wybierz **Urządzenia**.
4. Wybierz z listy dostępnych urządzeń, które pragniesz przypisać do profilu.

   Jeśli dziecko używa urządzenia z Androidem lub iOS i Asystent Rodzica Bitdefender nie jest zainstalowany, kliknij **DODAJ URZĄDZENIE**. Jeśli dziecko używa urządzenia Mac, a Antywirus dla Mac Bitdefender nie jest

zainstalowany, kliknij ten sam przycisk. Wybierz system operacyjny, którego applikację chcesz zainstalować, a następnie kliknij **NASTĘPNY KROK** aby kontynuować.

Wpisz adres e-mail, na który mamy wysłać link do pobrania instalatora aplikacji Bitdefender , a następnie kliknij **WYŚLIJ LINK INSTALACYJNY**.

5. Po zakończeniu procesu instalacji na nowym urządzeniu, wybierz go z listy, aby zastosować profil.
6. Zaznacz **ZAPISZ**.

26.2.2. Podlinkowywanie Asystenta Rodzica do Bitdefender Central

Aby monitorować aktywność online swojego dziecka na Androidzie i iOS, musisz zalogować się na swoje konto Bitdefender z poziomu aplikacji, aby powiązać jego urządzenie ze swoim kontem.

Aby powiązać urządzenie z Twoim kontem Bitdefender:

- Dla systemu **Android**:
  1. Wybierz przycisk, który pojawi się w wiadomości e-mail wysłanej przez nasz serwer. Zostałeś przekierowany do aplikacji Google Play.

     Jeśli nie wybrałeś opcji wysłania linku do ściągnięcia aplikacji na adres e-mail Twojego dziecka na koncie Bitdefender, przejdź do Google Play i wyszukaj aplikację Bitdefender Doradca Rodzica.
  2. Stuknij **Zainstaluj** w oknie Doradca Rodzica Bitdefender, a następnie stuknij **AKCEPTUJ**, jeśli pojawi się prośba o zezwolenie. Bitdefender wymaga uprawnień do informowania Cię o aktywności Twojego dziecka, i jeśli nie one zostaną zaakceptowane, aplikacja nie zostanie zainstalowana.
  3. Otwórz aplikację Asystent Rodzica.
  4. Przeczytaj **Umowę Subskrypcji**, a następnie kliknij **KONTYNUUJ**.
  5. Zaloguj się do swojego istniejącego konta Bitdefender.

     Jeśli nie masz konta, wybierz tworzenie nowego konta za pomocą odpowiedniej opcji.
  6. Stuknij **Włącz dostęp do użytkowania** i wybierz odpowiednią opcję.
  7. Stuknij **Włącz Dostępność** i wybierz odpowiednią opcję.

8. Aktywuj prawa administratora urządzenia dla aplikacji naciskając **AKTYWUJ**.

   Pozwoli to zapobiec odinstalowaniu przez Twoje dziecko Agenta Asystenta Rodzica.

9. Stuknij **ZAKOŃCZ** aby zakończyć instalację.

Notatka

Aby móc śledzić wiadomości SMS Twojego dziecka, na Androidzie 4.4 i nowszych wersjach, Bitdefender potrzebuje zmian w ustawieniach aplikacji Android Messages. Zalecamy Ci wybrać **Tak** w oknie dialogowym wyskakującym po kliknięciu przycisku **ZAKOŃCZ**.

- Na **iOS**:

1. Wybierz przycisk, który pojawi się w wiadomości e-mail wysłanej przez nasz serwer, a następnie zainstaluj aplikację.
2. Otwórz aplikację Asystent Rodzica.
3. Zostanie wyświetlony kreator wprowadzania zawierający szczegóły dotyczące funkcji produktu. Kliknij **Dalej** aby kontynuować.
4. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
5. Zezwól na dostęp do lokalizacji urządzenia, aby Bitdefender mógł go zlokalizować.
6. Zezwól aplikacji na wysyłanie powiadomień.
7. Przypisz urządzenie do profilu Twojego dziecka.

26.2.3. Monitorowanie aktywności dziecka

Bitdefender pomaga Ci na bieżąco śledzić to, co Twoje dzieci robią online.

W ten sposób możesz zawsze dowiedzieć się, jakie strony odwiedziło Twoje dziecko, jakich aplikacji używało i jakie rodzaje aktywności zostały zablokowane przez Asystenta Rodzica.

W zależności od ustawień, które sprawiają, że raporty mogą zawierać szczegółowe informacje na temat każdego wydarzenia, takie jak:

- Stan danego zdarzenia.
- Nasilenie powiadomień.

- Nazwa urządzenia.
- Data i godzina wystąpienia zdarzenia.

Aby monitorować ruch internetowy, uruchamiane aplikacje lub aktywność Twojego dziecka na Facebooku, wykonaj następujące kroki:

1. Uzyskaj dostęp do panelu Asystent Rodzica z Bitdefender Central.
2. Wybierz pożądaną kartę urządzenia.

   W oknie **Aktywność** możesz zobaczyć informacje, którymi się interesujesz. Alternatywnie, wybierz link **Zobacz dzisiejszą aktywność** na karicie monitorowanego urządzenia aby zostać przekierowanym do okna **Aktywność**.

26.2.4. Konfigurowanie Ustawień ogólnych

Domyślnie, gdy Asystent Rodzica jest włączony, działania Twojego dziecka są rejestrowane.

Aby otrzymywać powiadomienia e-mail:

1. Uzyskaj dostęp do panelu Asystent Rodzica z Bitdefender Central.
2. Wybierz zakładkę **Ustawienia** w prawym górnym rogu.
3. Włącz odpowiednią opcję, aby otrzymywać raporty aktywności.
4. Wpisz adres email gdzie powiadomienia email mają być wysyłane.
5. Otrzymuj powiadomienia e-mail odnośnie:
   - Zablokowanych stron WWW
   - Zablokowanych aplikacji
   - Zastrzeżone obszary
   - Przychodzące połączenie lub SMS od zablokowanego numeru telefonu
   - Usunięcie aplikacji Asystent Rodzica na Facebooku
6. Kliknij **ZAPISZ**.

26.2.5. Edytowanie profilu

Aby edytować istniejący profil:

1. Uzyskaj dostęp do Bitdefender Central.

2. Wybierz panel **Asystent Rodzica**.
3. Kliknij ikonę ⋮ na pożądanej karcie profilu, a następnie wybierz **Edytuj**.
4. Po dostosowaniu pożądanych ustawień, wybierz **ZAPISZ**.

26.2.6. Usuwanie profilu

Aby usunąć istniejący profil:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Asystent Rodzica**.
3. Kliknij ikonę ⋮ na pożądanej karcie profilu, a następnie wybierz **Usuń**.
4. Potwierdź swój wybór.

26.3. Konfigurowanie profili Asystenta Rodzica

Aby rozpocząć monitorowanie swojego dziecka, profil musi być przypisany do urządzenia, na którym zainstalowano Agenta Asystenta Rodzica Bitdefender.

Po dodaniu profilu dla Twojego dziecka, możesz dostosować bardziej szczegółowe ustawienia monitorowania i kontroli dostępu do Internetu oraz do określonych aplikacji.

Aby rozpocząć konfigurowanie profilu, wybierz żądaną kartę profilu z okna **MOJE DZIECI**.

Kliknij zakładkę, aby skonfigurować odpowiednią funkcję Asystenta Rodzica dla danego urządzenia:

- Aktywność - wyświetla wszystkie działania, zainteresowania, lokalizacje i kontakty z przyjaciółmi, z bieżącego dnia.
- Aplikacje - pozwala zablokować dostęp do niektórych aplikacji, takich jak gry, komunikatory, filmy, itp.
- Strony Internetowe - pozwala na filtrowanie nawigacji stron internetowych.
- Kontakty Telefoniczne - tutaj możesz określić, które kontakty z listy Twojego dziecka mogą się z nim skontaktować przez telefon.
- Lokalizacja Dziecka - tutaj możesz ustawić lokalizacje, które są bezpieczne lub nie dla Twojego dziecka.

- Społeczne - pozwala Tobie na zablokowanie dostępu do portali społecznościowych.
- Harmonogram - pozwala na blokowanie dostępu do urządzeń, które określiłeś w profilu dziecka.

26.3.1. Aktywność

Okno Aktywności podaje ci szczegółowe informacje o aktywności twojego dziecka z ostatnich 24 godzin, w i poza domem. Aby zobaczyć aktywność z poprzedniego dnia, kliknij ikonę kalendarza z lewego rogu okna.

W zależności od aktywności, to okno zawiera informacje o:

- **Lokalizacje** - tutaj możesz zobaczyć lokalizacje, w których Twoje dziecko było w ciągu dnia.
- **Zainteresowania** - tutaj możesz zobaczyć informacje na temat kategorii stron internetowych, które odwiedziło Twoje dziecko. Kliknij link **Recenzja nieodpowiednich treści**, aby umożliwić lub zablokować dostęp do określonych zainteresowań.
- **Interakcje społeczne** - tutaj możesz przeglądać kontakty, które komunikują się z dzieckiem. Kliknij link **Zarządzaj kontaktami**, aby wybrać kontakty, z którymi Twoje dziecko powinno pozostać w kontakcie lub też nie.
- **Aplikacje** - tutaj możesz zobaczyć aplikacje używane przez Twoje dziecko. Kliknij link **Przejrzyj uprawnienia aplikacji** aby blokować lub zezwolić na dostęp wybranym aplikacjom.
- **Dzienna aktywność** - tutaj możesz zobaczyć czas spędzony online na wszystkich urządzeniach przypisanych do Twojego dziecka, oraz miejsca, gdzie był aktywny. Zgromadzone informacje są z bieżącego dnia.

26.3.2. Aplikacje

Okno Aplikacji pomaga blokować uruchomienie aplikacji. Gry, media i komunikatory, jak również inne kategorie oprogramowania mogą zostać zablokowane w ten sposób.

Moduł może być włączony lub wyłączony za pomocą odpowiedniego przełącznika.

Konfigurowanie Kontroli Aplikacji dla określonego konta użytkownika:

1. Została wyświetlona lista z kartami. Karty przedstawiają aplikacje, z których korzysta Twoje dziecko.
2. Wybierz kartę z aplikacją, którą chcesz, aby Twoje dziecko przestało używać.

   Symbol znacznika wyboru, który się pojawia wskazuje, że Twoje dziecko nie będzie mogło korzystać z aplikacji.

26.3.3. Strony WWW

Okno Stron Internetowych pomaga Ci zablokować strony internetowe z nieodpowiednimi treściami. Strony internetowe, które hostują filmy, gry, oprogramowanie typu komunikatory, a także inne kategorie negatywnych treści mogą być zablokowane w ten sposób.

Moduł może być włączony lub wyłączony za pomocą odpowiedniego przełącznika.

W zależności od wieku, który ustawisz dla swojego dziecka, lista Zainteresowań jest domyślna z włączonym wyborem kategorii. Aby umożliwić lub zablokować dostęp do określonej kategorii, kliknij ją.

Symbol znacznika wyboru, który się pojawia wskazuje, że Twoje dziecko nie będzie w stanie uzyskać dostępu do treści związanych z daną kategorią.

Otwieranie lub blokowanie strony internetowej

Aby zezwolić lub ograniczyć dostęp do niektórych stron internetowych, musisz dodać je do listy Wykluczeń w następujący sposób:

1. Kliknij przycisk **ZARZĄDZAJ**.
2. Wpisz stronę internetową, którą chcesz dopuścić lub zablokować w odpowiednim polu.
3. Wybierz **Zezwól** lub **Zablokuj**.
4. Kliknij **ZAKOŃCZ**, aby zapisać zmiany.

Notatka

Ograniczenia dostępu do witryn internetowych można ustawiać tylko dla urządzeń z systemem Windows, Android i macOS dodanym do profilu Twojego dziecka.

26.3.4. Kontakty Telefoniczne

Okno Kontaktów Telefonicznych daje ci możliwość wybrania z którą listą znajomych, twoje dziecko może się kontaktować poprzez telefon.

Aby ograniczyć konkretny numer telefonu lub kontakt, pierw musisz dodać profil dziecka i jego urządzenie mobilne Android, poprzez następujące kroki:

1. Wybierz zakładkę **Asystent Rodzica** w Bitdefender Central.
2. Kliknij link **Instaluj Asystenta Rodzica** w wybranej karcie.
3. Kliknij **DODAJ URZĄDZENIE** na oknie które się pojawi.
4. Opcja **Bitdefender Asystent Rodzica na Androida** jest zaznaczona domyślnie. Kliknij **NASTĘPNY KROK** aby kontynuować.
5. Wybierz profil dziecka, któremu chcesz ustawić ograniczenia.
6. Wybierz zakładkę**Kontakty Telefoniczne**.

   Została wyświetlona lista z kartami. Karty stanowią kontakty z telefonu Android Twojego dziecka.
7. Wybierz kartę z numerem telefonu, który chcesz zablokować.

   Symbol znacznika wyboru, który się pojawia, wskazuje, że wybrany numer telefonu nie połączy się z Twoim dzieckiem.

Aby zablokować nieznane numery telefonów, włącz przycisk **Blokuj połączenia bez numeru ID**.

Notatka
Ograniczenia połączeń telefonicznych można ustawić tylko dla urządzeń z Androidem dodanych do profilu Twojego dziecka.

26.3.5. Lokalizacja dziecka

Zobacz bieżące położenie tego urządzenia na Google Maps. Lokalizacja jest odświeżana co 5 sekund, więc możesz śledzić urządzenie, nawet jeśli jest przenoszone.

Dokładność lokalizacji zależy od tego, jak Bitdefender jest w stanie ją ustalić:

- Jeśli funkcja GPS jest włączona na tym urządzeniu, jego lokalizacja może być określona z dokładnością do kilku metrów, tak długo, jak pozostaje ono w zasięgu satelitów GPS (tj. poza budynkiem).

- Jeśli urządzenie znajduje się w jakimś budynku, jego lokalizacja może być ustalona z dokładnością do kilkudziesięciu metrów, jeżeli sieć Wi-Fi jest włączona i w zasięgu tego urządzenia są otwarte sieci bezprzewodowe.
- W przeciwnym wypadku lokalizacja będzie określona tylko przy użyciu sieci operatora komórkowego, co oznacza dokładność nie lepszą niż w zakresie kilkuset metrów.

Konfigurowanie lokalizacji & Bezpieczne meldowanie

Aby mieć pewność, że Twoje dziecko chodzi do pewnych miejsc, możesz zrobić listę bezpiecznych i niebezpiecznych miejsc. Za każdym razem, gdy wejdzie samo na określony obszar, w aplikacji Doradca Rodzica pojawi się powiadomienie, aby potwierdzić, że jest bezpieczny. Stukając **DOTARŁEM BEZPIECZNIE** jesteś informowany poprzez powiadomienie na twoim koncie Bitdefender, że dziecko dotarło do miejsca docelowego.

Jeśli dziecko nie wyśle potwierdzenia, i tak możesz zobaczyć jego dzienną historię lokalizacji, sprawdzając jego profil na swoim koncie Bitdefender.

Aby skonfigurować lokalizację:

1. Kliknij **Urządzenia** w ramce, którą masz w oknie **Lokalizacja Dziecka**.
2. Kliknij **WYBIERZ URZĄDZENIA**, a następnie wybierz urządzenie, które chcesz konfigurować.
3. W oknie **Obszar**, kliknij przycisk **DODAJ OBSZAR**.
4. Wybierz typ lokalizacji, **BEZPIECZNA** lub **OGRANICZONA**.
5. Wpisz poprawną nazwę dla obszaru, gdzie dziecko ma pozwolenie, aby iść lub nie.
6. Ustaw zakres, który powinien być stosowany do monitorowania używając suwaka **Promień**.
7. Kliknij **DODAJ OBSZAR**, aby zapisać swoje ustawienia. Jesteś pytany czy Twoje dziecko będzie podróżowało samo czy nie. Potwierdź zaznaczając Tak lub Nie.

Notatka

Tropiciel lokalizacji może być używany do monitorowania urządzeń z Androidem i iOS, które zainstalowały aplikację doradca Rodzica Bitdefender.

26.3.6. Społecznościowy

Asystent Rodzica monitoruje konto Twojego dziecka na Facebooku i raportuje najważniejsze rodzaje podejmowanej aktywności.

Ta aktywność internetowa jest weryfikowana i jesteś ostrzegany, jeśli okaże się być zagrożeniem dla prywatności Twojego dziecka.

Monitorowane elementy konta online obejmują:

- Informacje o koncie
- Strony z like'ami
- załadowane zdjęcia

Aby skonfigurować ochronę Facebooka dla wybranego konta, wpisz adres email monitorowanego konta dziecka i kliknij **WYŚLIJ**.

Poinformuj swoje dziecko o swoich zamiarach, i poproś, by kliknęło w link aktywacyjny **Chroń to konto**, który otrzymało od nas na swój adres e-mail.

Aby uzyskać dostęp do monitorowanego konta Facebook, kliknij link **Pokaż na Facebook'u**.

Aby przestać monitorować to konto, użyj przycisku **Odłącz konto** w górnej części.

Aby dostać powiadomienie poprzez e-mail, kiedy Twoje dziecko usunie aplikacje Parental Advisor z urządzenia, wybierz odpowiedni checkbox.

26.3.7. Harmonogram czasowy

Okno Harmonogramu pozwala ograniczyć dostęp do urządzenia ustalony w profilu dziecka. Ograniczenia można skonfigurować o dowolnej godzinie podczas tygodnia szkolnego i w weekendy tylko dla urządzeń z systemem Android i Windows.

Aby rozpocząć konfiguracje ograniczeń w ciągu nocy:

1. W obszarze **CZAS SNU**, wybierz pola wyboru **NOC SZKOLNA** i **NOC WEEKENDOWA**.
2. Kliknij ikonę ⊗ w odpowiedniego pola, i użyj strzałek góra/dół aby ustawić interwały czasowe w których dostęp powinien być zablokowany.

Aby rozpocząć konfiguracje ograniczeń w ciągu dnia:

1. W obszarze **LIMITY DZIENNE** masz następujące opcje:

- **NARASTAJĄCY**
  a. Wybierz pola wyboru **Limity Czasu Dni Szkolnych** oraz **Weekendowe Limity Czasu**.
  b. Przeciągnij suwak aby ustawić czas dostępu do urządzenia.
- **DOKŁADNY**
  a. Wybierz pola wyboru **Limity Czasu Dni Szkolnych** oraz **Weekendowe Limity Czasu**.
  b. Wybierz z siatki przedziały czasowe, w których dostęp ma być zablokowany.

Notatka
Ustawienia **narastające** i **specyficzne** są zaprojektowane do pracy niezależnie od siebie.

27. USB IMMUNIZER

Funkcja automatycznego uruchamiania wbudowana w systemach operacyjnych Windows jest bardzo przydatnym narzędziem, które pozwala komputerom na automatyczne uruchamianie plików z mediów do niego podłączonych. Na przykład instalowanie oprogramowania może być uruchomione automatycznie po włożeniu płyty CD do napędu optycznego.

Niestety, funkcja ta może być również wykorzystywana przez złośliwe oprogramowanie do automatycznego uruchamiania i infiltracji komputera z nośników wielokrotnego zapisu, takich jak dyski flash USB i karty pamięci podłączone przez czytniki kart. W ostatnich latach stworzono wiele ataków opartych o autoodtwarzanie.

Dzięki funkcji "Zabezpieczania nośników USB" możesz zapobiec wykonywaniu się złośliwego kodu z przenośnych dysków USB sformatowanych w systemach NTFS, FAT i FAT32. Kiedy urządzenie USB jest zabezpieczone, złośliwe oprogramowanie nie może go skonfigurować, aby uruchomić szkodliwą aplikację, gdy urządzenie jest podłączone do komputera z systemem Windows.

Aby uodpornić urządzenie USB:

1. Podłącz dysk flash do swojego komputera.
2. Przeglądaj komputer w celu zlokalizowania wymiennego urządzenia pamięci masowej i kliknij prawym przyciskiem myszy jego ikonę.
3. W menu kontekstowym, wskaż **Bitdefender** i wybierz **Zabezpiecz ten dysk**.

> **Notatka**
> Jeśli dysk został już uodporniony, pojawi się wiadomość **Urządzenie USB jest chronione przed złośliwym oprogramowaniem opartym o autoodtwarzanie**.

Aby uniknąć uruchomienia złośliwego oprogramowania na Twoim komputerze z urządzeń USB, które nie są zabezpieczone, wyłącz funkcję autoodtwarzania mediów zewnętrznych. Aby uzyskać więcej informacji, odwołaj się do *„Korzystanie z automatycznego monitorowania luk”* (p. 134).

OPTYMALIZACJA SYSTEMU

28. TRYBY

Codzienne czynności, oglądanie filmów lub granie w gry może spowodować spowolnienie systemu, zwłaszcza jeśli są one uruchomione jednocześnie z procesami Windows Update i zadaniami konserwacyjnymi. Dzięki Bitdefender możesz teraz wybrać i stosować preferowany profil, który sprawia, że system dostosowuje się do zwiększonej wydajności poszczególnych zainstalowanych aplikacji.

Bitdefender udostępnia następujące profile:

- Tryb Pracy
- Tryb Filmu
- Profil Gry
- Profil Publiczne Wi-Fi
- Profil Tryb Pracy na Baterii

Jeśli nie zdecydujesz się na używanie **Profili**, domyślny profil o nazwie **Standardowy** będzie włączony, ale nie wnosi on żadnych optymalizacji do systemu.

W zależności od Twojej aktywności, następujące ustawienia produktu są stosowane, gdy profile Praca, Film lub Gra są aktywne:

- Wszystkie alarmy i wyskakujące okienka Bitdefender są zablokowane.
- Automatyczna aktualizacja jest przełożona.
- Zaplanowane zadania skanowania są przełożone.
- Asystent wyszukiwania jest wyłączony.
- Powiadomienia o ofertach specjalnych są wyłączone.

W zależności od Twojej aktywności, następujące ustawienia systemu są stosowane, gdy profile Praca, Film lub Gra są aktywne:

- Automatyczne aktualizacje Windows są przełożone.
- Wszystkie alarmy i wyskakujące okienka są wyłączone.
- Niepotrzebne programy działające w tle są zawieszone.
- Efekty wizualne zostały dostosowane dla uzyskania najlepszej wydajności.
- Zadania konserwacyjne zostały przełożone.

- Ustawienia planu zasilania zostały dostosowane.

Podczas pracy na tym profilu Publiczne Wi-Fi, Bitdefender Internet Security 2018 automatycznie stosuje następujące ustawienia:

- Zaawansowana Ochrona Przed Zagrożeniami jest włączona
- Firewall Bitdefender jest włączony i następujące ustawienia są zastosowane dla Twojego bezprzewodowego adaptera:
  - Tryb ukrycia - WŁACZONY
  - Typ sieci - Publiczny
- Następujące ustawienia z Ochrony Webowej są włączone:
  - Skanuj SSL
  - Ochrona przed oszustwami
  - Ochrona przed phishingiem

28.1. Tryb Pracy

Uruchamiania wielu zadań w miejscu pracy, takich jak wysyłanie e- maili, konferencje wideo z kolegami lub praca z aplikacjami do projektowania, może mieć wpływ na wydajność systemu. Profil "Praca" został zaprojektowany, aby pomóc Ci poprawić wydajność pracy, poprzez wyłączenie niektórych usług w tle i prac konserwacyjnych.

Konfigurowanie profilu "Praca"

Aby skonfigurować działania, które należy podjąć w Profilu Praca:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Modułu Praca.
4. Wybierz dostosowania systemowe, które chcesz zastosować, zaznaczając następujące opcje:
   - Zwiększ wydajność w aplikacjach do pracy
   - Optymalizuj ustawienia produktu dla Trybu pracy
   - Odłóż na później zadania programów w tle i konserwację

- Przełóż automatyczne aktualizacje Windows

5. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

Ręczne dodawanie aplikacji do listy profilu "Praca"

Jeśli Bitdefender nie przechodzi automatycznie do profilu "Praca" podczas uruchamiania określonej aplikacji, możesz ręcznie dodać aplikację do **Listy aplikacji**.

Aby ręcznie dodać aplikacje do listy aplikacji w profilu "Praca":

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Modułu Praca.
4. W oknie **PROFIL PRACY** kliknij link **Lista aplikacji**.
5. Kliknij "**Dodaj**", aby dodać nową aplikację do **Listy aplikacji**.

   Pojawi się nowe okno. Przejdź do pliku wykonywalnego aplikacji, zaznacz go i kliknij "**OK**", aby dodać go do listy.

28.2. Tryb Filmu

Wyświetlanie wysokiej jakości treści wideo, takich jak filmy w wysokiej rozdzielczości, wymaga znacznych zasobów systemowych. Profil "Film" dostosowuje ustawienia systemu i produktu, dzięki czemu możesz nieprzerwanie i bezproblemowo cieszyć się z filmu.

Konfigurowanie profilu "Film"

Aby skonfigurować działania, które należy podjąć w profilu "Film":

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Modułu Film.
4. Wybierz dostosowania systemowe, które chcesz zastosować, zaznaczając następujące opcje:
   - Zwiększ wydajność odtwarzaczy wideo
   - Optymalizuj ustawienia produktu dla Trybu Filmowego

- Odłóż na później zadania programów w tle i konserwację
- Przełóż automatyczne aktualizacje Windows
- Dostosuj ustawienia planu zasilania do filmów

5. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

Ręczne dodawanie odtwarzaczy wideo do listy profilu "Film"

Jeśli Bitdefender nie przechodzi automatycznie do profilu "Film" podczas uruchamiania pewnej aplikacji odtwarzacza wideo, możesz ręcznie dodać aplikację do **Listy odtwarzaczy**.

Aby ręcznie dodać odtwarzacze wideo do listy odtwarzaczy w profilu "Film":

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Modułu Film.
4. W oknie **Profil filmu** kliknij link **Lista odtwarzaczy**.
5. Kliknij "**Dodaj**", aby dodać nową aplikację do **Listy odtwarzaczy**.

   Pojawi się nowe okno. Przejdź do pliku wykonywalnego aplikacji, zaznacz go i kliknij "**OK**", aby dodać go do listy.

28.3. Profil Gry

Możesz się cieszyć z nieprzerywanego grania, dzięki zredukowaniu obciążenia systemu i zmniejszeniu spowolnień. Za pomocą heurystyki behawioralnej wraz z listą znanych gier, Bitdefender może automatycznie wykryć uruchomioną grę i optymalizuje zasoby systemowe, dzięki czemu możesz cieszyć się swoją przerwą na grę.

Konfigurowanie Profilu gracza

Aby skonfigurować działania, które wykonujesz będąc w Profilu Gra:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Profilu Gra.

4. Wybierz dostosowania systemowe, które chcesz zastosować, zaznaczając następujące opcje:
   - Zwiększ wydajność w grach
   - Optymalizuj ustawienia produktu dla Trybu gracza
   - Odłóż na później zadania programów w tle i konserwację
   - Przełóż automatyczne aktualizacje Windows
   - Dostosuj ustawienia planu zasilania do gier
5. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

Ręczne dodawanie gier do listy gier

Jeśli Bitdefender nie przechodzi automatycznie do Profilu gracza podczas uruchamiania określonej gry lub aplikacji, możesz ręcznie dodać aplikację do **Listy gier**.

Aby ręcznie dodać gry do listy gier w Profilu gracza:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Profilu Gra.
4. W oknie **Profil Gra** kliknij link **Lista gier**.
5. Kliknij "**Dodaj**", aby dodać nową grę do **Listy gier**.

   Pojawi się nowe okno. Przejdź do pliku wykonywalnego gry, zaznacz go i kliknij "**OK**", aby dodać go do listy.

28.4. Profil Publiczne Wi-Fi

Wysyłając wiadomości e-mail, wpisując wrażliwe poświadczenia lub dokonując zakupów online, podczas gdy jesteś podłączony do niebezpiecznej sieci bezprzewodowej może narazić Twoje dane osobowe na ryzyko. Profil Publiczne Wi-Fi dostosowuje ustawienia urządzenia, aby dać Ci możliwość dokonywania płatności online i korzystania z poufnych informacji w chronionym środowisku.

Profil Konfiguracji Publicznego Wi-Fi

Aby skonfigurować Bitdefender, by zastosował ustawienia urządzenia podczas połączenia z niebezpieczną siecią bezprzewodową:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Profilu Publiczne Wi-Fi.
4. Pozostaw pole wyboru **Dostosowuje ustawienia urządzenia w celu zwiększenia ochrony, gdy jest podłączone do niebezpiecznej publicznej sieci Wi-Fi** włączona.
5. Kliknij **Zapisz**.

28.5. Profil Tryb Pracy na Baterii

Profil Tryb Pracy na baterii został specjalnie zaprojektowany dla użytkowników laptopów i tabletów. Jego celem jest zminimalizowanie wpływu zarówno systemu, jak i Bitdefender, na zużycie energii, gdy poziom naładowania akumulatora jest niższy od domyślnego lub tego, który wybrałeś.

Konfigurowanie Profilu Moduł Pracy na baterii

Aby skonfigurować profil Trybu Baterii:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Profilu Moduł pracy na baterii.
4. Wybierz ustawienia systemowe, które mają być zastosowane, zaznaczając następujące opcje:
   - Optymalizuj ustawienia produktu dla Trybu Baterii.
   - Odłóż na później zadania programów w tle i konserwację.
   - Przełóż automatyczne aktualizacje systemu Windows.
   - Dostosuj ustawienia zasilania do Trybu Baterii.
   - Wyłącz urządzenia zewnętrzne i porty sieciowe.
5. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

Wpisz odpowiednią wartość w polu lub wybierz ją korzystając ze strzałek góra i dół, aby sprecyzować, kiedy system powinien zacząć pracować w trybie bateryjnym. Domyślnie, Tryb ten jest aktywowany, gdy poziom baterii spadnie poniżej 30%.

Następujące ustawienia są stosowane, gdy Bitdefender pracuje w profilu Tryb Pracy na baterii:

- Automatyczna aktualizacja Bitdefender jest przełożona.
- Zaplanowane zadania skanowania są przełożone.
- Gadżet bezpieczeństwa jest wyłączony.

Bitdefender wykrywa, kiedy laptop został przełączony na zasilanie bateryjne i na podstawie poziomu naładowania baterii automatycznie przechodzi w Tryb pracy na baterii. Podobnie Bitdefender automatycznie wyłącza Tryb pracy na baterii, gdy wykryje, że laptop został podłączony do zasilania.

28.6. Optymalizacja w czasie rzeczywistym

Optymalizacja w czasie rzeczywistym Bitdefender, to wtyczka, która poprawia wydajność systemu w tle, upewniając się, że Ci nie przeszkadza, gdy jesteś w trybie profilu. W zależności od obciążenia procesora, wtyczka monitoruje wszystkie procesy, koncentrując się na tych, które stanowią wyższe obciążenia, aby dostosować je do Twoich potrzeb.

Aby włączyć lub wyłączyć Optymalizacje w czasie rzeczywistym:

1. Kliknij ikonę ⚙ po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Profile**.
3. Przewiń w dół, aż zobaczysz opcję optymalizacji czasu rzeczywistego, a następnie użyj odpowiedniego przełącznika, aby ją włączyć lub wyłączyć.

ROZWIĄZYWANIE PROBLEMÓW

29. ROZWIĄZYWANIE TYPOWYCH PROBLEMÓW

Ten rozdział przedstawia niektóre problemy, na jakie można się natknąć w trakcie użytkowania Bitdefender, oraz ich potencjalne rozwiązania. Większość tych problemów można rozwiązać poprzez odpowiednie skonfigurowanie ustawień produktu.

Jeśli nie możesz w tym miejscu znaleźć pomocy dla swojego problemu lub przedstawione rozwiązania nie pomagają, możesz skontaktować się z przedstawicielem pomocy technicznej Bitdefender, korzystając z metody przedstawionej w rozdziale *„Prośba o pomoc"* (p. 219).

29.1. Mój system działa wolno

Po zainstalowaniu nowego oprogramowania zabezpieczającego może występować niewielkie spowolnienie pracy systemu. Do pewnego poziomu jest to sytuacja normalna.

Jeśli zauważysz znaczące spowolnienie pracy systemu, może to być spowodowane przez:

- **Bitdefender nie jest jedynym programem zapewniającym ochronę zainstalowanym w systemie.**

  Choć Bitdefender wyszukuje i usuwa inne, zapewniające ochronę programy znalezione w czasie instalacji, przed rozpoczęciem instalacji Bitdefender zaleca się usunięcie wszelkich programów chroniących przed złośliwym oprogramowaniem. Aby uzyskać więcej informacji, odwołaj się do *„Jak usunąć inne rozwiązania bezpieczeństwa?"* (p. 83).

- **Minimalne wymagania systemowe dla produktu Bitdefender nie zostały spełnione.**

  Jeśli Twój komputer nie spełnia minimalnych wymagań systemowych, może on działać wolno, zwłaszcza przy kilku aplikacjach uruchomionych jednocześnie. Aby uzyskać więcej informacji, odwołaj się do *„Minimalne wymagania systemowe"* (p. 3).

- **Zainstalowane zostały aplikacje, które nie są używane**.

  Na każdym komputerze znajdują się programy i aplikacje, które nie są używane. W tle często działa wiele niechcianych programów, które zużywają przestrzeń dyskową i pamięć. Jeśli nie używasz danego programu, odinstaluj go. To dotyczy także każdego innego oprogramowania lub wersji demonstracyjnej, którą zapomnisz usunąć.

  WAŻNE
  Jeśli wydaje Ci się, że dany program czy aplikacja są ważną częścią Twojego systemu operacyjnego, nie usuwaj ich i skontaktuj się z Obsługą klienta Bitdefender, aby uzyskać pomoc.

- **Twój system może być zainfekowany**.

  Szkodliwe oprogramowanie może wpłynąć na szybkość działania Twojego systemu oraz jego ogólne zachowanie. Oprogramowanie szpiegujące, wirusy, trojany i adware - wszystkie one mają wpływ na wydajność Twojego komputera. Skanuj swój system regularnie, przynajmniej raz w tygodniu. Zalecane jest skanowanie systemu przez Bitdefender, ze względu na konieczność wykrycia wszelkiego złośliwego oprogramowania, zagrażającego bezpieczeństwu Twojego systemu.

  Aby rozpocząć Skanowanie Systemu:

  1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
  2. Kliknij link **POKAŻ FUNKCJE**.

3. W module **ANTYWIRUS** wybierz **Skanowanie Systemu**.
4. Postępuj zgodnie z poleceniami kreatora.

29.2. Skanowanie się nie rozpoczyna

Ten rodzaj problemu może mieć dwie główne przyczyny:

- **Wcześniejsza instalacja Bitdefender, która nie została całkowicie usunięta lub Bitdefender został nieprawidłowo zainstalowany**.

  W takim wypadku przeinstaluj Bitdefender:

  - W systemie **Windows 7**:
    1. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
    2. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
    3. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
    4. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
  - W systemach **Windows 8 i Windows 8.1**:
    1. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
    2. Kliknij **Odinstaluj program** lub **Programy i funkcje**.
    3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
    4. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
    5. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
  - W systemie **Windows 10**:
    1. Kliknij **Start**, a następnie kliknij Ustawienia.
    2. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.

3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.
5. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
6. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

Notatka

Postępując zgodnie z procedurą ponownej instalacji, ustawienia dostosowane są zapisywane i dostępne w nowym zainstalowanym produkcie. Inne ustawienia mogą zostać przywrócone do domyślnej konfiguracji.

- **Bitdefender nie jest jedynym rozwiązaniem bezpieczeństwa zainstalowanym w systemie**.

W tym przypadku:

1. Usuń inne rozwiązanie bezpieczeństwa. Aby uzyskać więcej informacji, odwołaj się do *„Jak usunąć inne rozwiązania bezpieczeństwa?"* (p. 83).
2. Przeinstaluj Bitdefender:
   - W systemie **Windows 7**:
     a. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
     b. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
     c. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
     d. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
   - W systemach **Windows 8 i Windows 8.1**:
     a. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
     b. Kliknij **Odinstaluj program** lub **Programy i funkcje**.

c. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

d. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.

e. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

- W systemie **Windows 10**:

a. Kliknij **Start**, a następnie kliknij Ustawienia.

b. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.

c. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

d. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.

e. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.

f. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

Notatka
Postępując zgodnie z procedurą ponownej instalacji, ustawienia dostosowane są zapisywane i dostępne w nowym zainstalowanym produkcie. Inne ustawienia mogą zostać przywrócone do domyślnej konfiguracji.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

29.3. Nie mogę dłużej używać aplikacji

Problem ten zachodzi, gdy próbujesz użyć programu, który działał normalnie przed zainstalowaniem Bitdefender.

Po zainstalowaniu Bitdefender możesz napotkać jedną z tych sytuacji:

- Możesz otrzymać od Bitdefender wiadomość, że program próbuje zmodyfikować system.
- Program, który próbujesz uruchomić, może wyświetlić komunikat o błędzie.

Sytuacja tego typu występuje wtedy, gdy moduł Aktywnej Kontroli Zagrożeń błędnie rozpoznaje niektóre aplikacje jako złośliwe.

Aktywna Kontrola Zagrożeń to moduł Bitdefender, który nieustannie monitoruje aplikacje działające w systemie i informuje o tych, które zachowują się jak oprogramowanie potencjalnie złośliwe. Ponieważ funkcja ta bazuje na analizie heurystycznej, mogą występować przypadki, gdy dozwolone aplikacje są raportowane przez moduł Aktywnej Kontroli Zagrożeń jako złośliwe.

Gdy wystąpi taka sytuacja, można wyłączyć monitorowanie danej aplikacji przez moduł Aktywnej Kontroli Zagrożeń.

Aby dodać program do listy wyjątków:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Kliknij ikonę w prawym dolnym rogu modułu **AKTYWNA KONTROLA ZAGROŻEŃ**.
4. W oknie **BIAŁA LISTA**, kliknij **Dodaj aplikacje do białej listy**.
5. Znajdź i wybierz aplikację, która ma być wykluczona, a następnie kliknij **OK**.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

29.4. Co robić, gdy Bitdefender blokuje bezpieczne strony lub aplikacje online

Bitdefender oferuje bezpieczne przeglądanie internetu poprzez filtrowanie całego ruchu w sieci i blokowanie szkodliwych treści. Jednak możliwe jest, że Bitdefender uważa bezpieczną stronę internetową lub aplikację online jako niebezpieczne, co spowoduje ich nieprawidłowe blokowanie przez skanowanie ruchu HTTP Bitdefender.

Jeśli ta sama strona lub aplikacja są wielokrotnie zablokowane, możesz je dodać do białej listy, tak że nie będą one skanowane przez silniki Bitdefender, zapewniając w ten sposób płynne przeglądanie stron internetowych.

Aby dodać stronę do **Białej listy**:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.

3. W panelu **OCHRONA SIECI**, kliknij **Biała lista**.
4. Podaj adres zablokowanej strony internetowej lub aplikacji online w odpowiednim polu i kliknij **Dodaj**.
5. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

Tylko strony internetowe i aplikacje, którym w pełni ufasz, powinny być dodawane do tej listy. Zostaną one wyłączone ze skanowania przez następujące silniki: antywirusowy, antyphishingowy i antywyłudzeniowy.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

29.5. Co zrobić jeśli Bitdefender wykrywa bezpieczną aplikację jako ransomware

Ransomware to złośliwy program, który stara się zarobić pieniądze na użytkownikach poprzez zablokowanie ich wrażliwych systemów. Aby utrzymać Twój system bezpieczny od niefortunnych sytuacji, Bitdefender daje Ci możliwość zabezpieczenia osobistych plików.

Kiedy aplikacja próbuje zmienić lub usunąć jeden z twoich chronionych plików, zostanie uznana za niebezpieczną i Bitdefender zablokuje jej funkcjonowanie.

W przypadku, kiedy taka aplikacja jest dodana do listy niezaufanych aplikacji, lecz jesteś pewien, że można bezpiecznie z niej korzystać, wykonaj następujące kroki:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **BEZPIECZNE PLIKI** kliknij **Dostęp do aplikacji**.
4. Aplikacje, które usiłowały zmienić pliki w chronionych folderach są wypisane. Kliknij przycisk Zezwól obok aplikacji, którą uważasz za bezpieczną.

29.6. Nie mogę połączyć się z internetem

Może się zdarzyć, że program lub przeglądarka nie będą mogły się połączyć z internetem lub korzystać z usług sieciowych po zainstalowaniu Bitdefender.

W takim przypadku najlepiej będzie skonfigurować produkt Bitdefender tak, aby automatycznie zezwalał na połączenia nawiązywane przez konkretne aplikacje:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu okienka **ZAPORA SIECIOWA**.
4. Wybierz zakładkę **Reguły**.
5. Aby dodać regułę aplikacji, kliknij link **Dodaj regułę**.
6. Pojawiło się nowe okno, w którym możesz dodać szczegóły. Upewnij się, że wybierasz wszystkie dostępne typy sieci i w sekcji **Pozwolenie** wybierz **Zezwól**.

Zamknij Bitdefender, otwórz aplikację i spróbuj ponownie połączyć się z internetem.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc”* (p. 219).

29.7. Nie mogę uzyskać dostępu do urządzenia w mojej sieci

W zależności od sieci, do której jesteś podłączony, Zapora sieciowa produktu Bitdefender może zablokować połączenie pomiędzy Twoim systemem, a innym urządzeniem (np. innym komputerem lub drukarką). W wyniku tego możesz nie mieć możliwości udostępniania i drukowania dokumentów.

W takim wypadku najlepszym rozwiązaniem jest skonfigurowanie produktu Bitdefender tak, aby automatycznie zezwalał na obustronne łączenie się poszczególnych urządzeń z komputerem w następujący sposób:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. Wybierz ikonę w prawym dolnym rogu okienka **ZAPORA SIECIOWA**.
4. Wybierz link **Dodaj regułę** na górze okna **REGUŁY**.
5. W oknie **USTAWIENIA** włącz opcję **Zastosuj tę regułę do wszystkich aplikacji**

6. Wybierz zakładkę **ZAAWANSOWANE**.
7. W polu **Niestandardowy adres zdalny** wpisz adres IP komputera lub drukarki, do którego chcesz mieć nieograniczony dostęp.

Jeśli nadal nie możesz połączyć się z urządzeniem, przyczyną problemu prawdopodobnie nie jest Bitdefender.

Sprawdź inne potencjalne przyczyny, takie jak:

- Udostępnianie plików i drukarki Twojemu komputerowi może być blokowane przez Zaporę sieciową innego komputera.
  - Jeśli używana jest Zapora sieciowa systemu Windows, można ją skonfigurować, aby zezwalała na współdzielenie plików i drukarek w następujący sposób:
    - W systemie **Windows 7**:
      1. Kliknij **Start**, przejdź na **Panel sterowania** i wybierz **System i zabezpieczenia**.
      2. Przejdź do **Zapora sieciowa Windows**, a następnie kliknij **Zezwalaj programowi lub funkcji na dostęp przez Zaporę systemu Windows**.
      3. Wskaż pole wyboru **Udostępnianie plików i drukarek**.
    - W systemach **Windows 8 i Windows 8.1**:
      1. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
      2. Kliknij **System i bezpieczeństwo**, przejdź do **Zapora sieciowa Windows** i wybierz **Zezwalaj programowi lub funkcji na dostęp przez Zaporę systemu Windows**.
      3. Zaznacz pole wyboru **Udostępnianie plików i drukarek**, a następnie kliknij **OK**.
    - W systemie **Windows 10**:
      1. Wpisz "Pozwala aplikacji przez Windows Firewall" w polu wyszukiwania z paska zadań, a następnie kliknij jego ikonę.
      2. Kliknij **Zmień ustawiania**.
      3. Z listy **Dozwolone aplikacje i funkcje** wybierz **Udostępnianie Pliku i Drukarki**, a następnie kliknij pole wyboru **OK**.

- Jeśli komputer posiada inną Zaporę sieciową, odwołaj się do jej dokumentacji lub pliku pomocy.

- Główne warunki, które mogą przeszkodzić w używaniu lub podłączaniu udostępnionej drukarki to:
  - Aby korzystać z udostępnionej drukarki w sieci, może być wymagane zalogowanie się na konto Administratora.
  - Dla każdej współdzielonej drukarki ustawiane są uprawnienia dostępu dla konkretnego komputera i użytkownika. Jeśli już współdzielisz drukarkę, sprawdź jak ustawione są uprawnienia, aby dowiedzieć się, czy użytkownik innego komputera posiada do niej dostęp. Jeśli próbujesz podłączyć się do udostępnionej drukarki, sprawdź czy użytkownik drugiego komputera przydzielił prawa dostępu do drukarki.
  - Drukarka podłączona do Twojego lub innego komputera nie jest udostępniona.
  - Udostępniona drukarka nie została dodana do komputera.

  Notatka
  Aby nauczyć się zarządzać udostępnianiem drukarek w sieci (współdzielenie drukarki, dodawanie lub usuwanie praw dostępu do drukarki, łączenie się z drukarką sieciową), przejdź do Centrum pomocy i wsparcia Windows (w menu Start kliknij **Pomoc i obsługa techniczna**).

- Dostęp do drukarki sieciowej może być ograniczony tylko do określonych komputerów i użytkowników. Powinieneś zapytać administratora sieci, czy masz uprawnienia do połączenia się z tą drukarką.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

29.8. Moje łącze internetowe jest powolne

Sytuacja ta może zaistnieć po zainstalowaniu Bitdefender. Problem ten może być wywołany przez błędy w konfiguracji Zapory sieciowej Bitdefender.

Aby rozwiązać ten problem:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.

3. W okienku **ZAPORA SIECIOWA**, kliknij przełącznik WŁĄCZ/WYŁĄCZ, aby wyłączyć tę funkcję.
4. Sprawdź, czy wyłączenie Zapory sieciowej Bitdefender wpłynęło na jakość połączenia internetowego.
   - Jeśli połączenie internetowe jest nadal wolne, przyczyną problemów prawdopodobnie nie jest Bitdefender. Należy skontaktować się z dostawcą usług internetowych, aby sprawdzić, czy nie ma problemów z połączeniem po jego stronie.

     Jeśli otrzymasz potwierdzenie od swojego dostawcy usług internetowych, że połączenie jest sprawne po jego stronie, a problem mimo to nadal występuje, skontaktuj się z działem obsługi klienta Bitdefender w sposób opisany w *„Prośba o pomoc"* (p. 219).
   - Jeśli połączenie z internetem polepszyło się po wyłączeniu Zapory sieciowej Bitdefender:

     a. Kliknij ikonę po lewej stronie interfejsu Bitdefender.

     b. Kliknij link **POKAŻ FUNKCJE**.

     c. Wybierz ikonę w prawym dolnym rogu okienka **ZAPORA SIECIOWA**.

     d. Przejdź do zakładki **ADAPTERY SIECIOWE** i ustaw połączenie internetowe na **Dom/Biuro**.

     e. W zakładce **USTAWIENIA ZAAWANSOWANE**, kliknij przełącznik, aby wyłączyć **Blokuj skanowanie portów w sieci**.

     W polu **Tryb Ukryty**, kliknij **Edytuj ukryte połączenia**. Włącz Tryb Ukryty dla adaptera sieciowego, do którego jesteś podłączony.

     f. Wyłącz Bitdefender, uruchom ponownie system i sprawdź szybkość połączenia internetowego.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

29.9. Jak zaktualizować produkt Bitdefender przy użyciu wolnego połączenia internetowego?

Jeśli masz wolne połączenie z internetem (takie jak połączenie telefoniczne), w trakcie procesu aktualizacji mogą występować błędy.

Aby utrzymać Twój Bitdefender zaktualizowany o najnowsze sygnatury złośliwego oprogramowania:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Wybierz zakładkę **Aktualizacja**.
3. Obok opcji **Reguły przetwarzania aktualizacji** wybierz **Pytaj przed pobraniem** z rozwijanego menu.
4. Wróć do głównego okna i kliknij przycisk akcji **Aktualizacja** z interfejsu Bitdefender.
5. Wybierz tylko **Aktualizacje sygnatur**, a następnie kliknij **OK**.
6. Bitdefender pobierze i zainstaluje jedynie aktualizacje sygnatur złośliwego oprogramowania.

29.10. Usługi produktu Bitdefender nie odpowiadają

Ten artykuł pozwala na rozwiązanie problemów z **nieodpowiadającymi usługami Bitdefender**. Możesz napotkać na ten błąd w przypadku, gdy:

- Ikona produktu Bitdefender w zasobniku systemowym jest szara i pojawia się informacja, że usługi Bitdefender nie odpowiadają.
- Okno Bitdefender wskazuje na nieodpowiadające usługi Bitdefender.

Ten błąd może pojawić się w następujących okolicznościach:

- Tymczasowe błędy w komunikacji pomiędzy usługami Bitdefender.
- Niektóre z usług Bitdefender są zatrzymane.
- Oprócz Bitdefender, inne oprogramowanie zabezpieczające jest uruchomione na Twoim komputerze.

Aby naprawić ten błąd, spróbuj poniższych rozwiązań:

1. Poczekaj kilka chwil i sprawdź, czy coś się zmieniło. Ten błąd może być tymczasowy.
2. Uruchom komputer ponownie i odczekaj chwilę, aż Bitdefender się uruchomi. Uruchom program Bitdefender i sprawdź, czy błąd nadal występuje. Ponowne uruchomienie komputera zazwyczaj rozwiązuje ten problem.
3. Sprawdź, czy masz zainstalowane inne oprogramowanie zabezpieczające, gdyż może ono zakłócić normalną pracę programu Bitdefender. Jeśli tak,

zalecamy usunięcie wszystkich programów tego typu przed rozpoczęciem instalacji programu Bitdefender.

Aby uzyskać więcej informacji, odwołaj się do *„Jak usunąć inne rozwiązania bezpieczeństwa?”* (p. 83).

Jeśli błąd się powtarza, skontaktuj się z naszym przedstawicielem, tak jak opisano w sekcji *„Prośba o pomoc”* (p. 219).

29.11. Filtr antyspamowy nie działa poprawnie

Ten artykuł pomaga rozwiązać problemy, które mogą się pojawić w przypadku korzystania z filtra antyspamowego Bitdefender:

- Liczba prawidłowych wiadomości e-mail oznaczonych jako [spam].
- Wiele wiadomości zawierających spam nie zostało poprawnie oznaczonych przez filtr antyspamowy.
- Filtr antyspamowy nie wykrywa żadnych wiadomości spamowych.

29.11.1. Prawidłowe wiadomości oznaczone są jako [spam]

Prawidłowe wiadomości są oznaczane jako [spam], ponieważ wyglądają jak spam dla filtra antyspamowego Bitdefender. Możesz rozwiązać te problemy przez właściwą konfigurację filtra antyspamowego.

Bitdefender automatycznie dodaje odbiorców Twoich wiadomości e-mail do listy Przyjaciół. Wiadomości e-mail odebrane od kontaktów z listy Przyjaciół są traktowane jako wiarygodne. Nie są weryfikowane przez filtr antyspamowy i, w związku z tym, nigdy nie są oznaczane jako [spam].

Automatyczna konfiguracja listy Przyjaciół nie zapobiega błędom wykrywania, które mogą wystąpić w następujących sytuacjach:

- Otrzymywanie wielu komercyjnych wiadomości e-mail z powodu subskrybowania wielu różnych stron. W tym przypadku rozwiązaniem jest dodanie adresów e-mail osób, od których otrzymujesz te wiadomości do listy Przyjaciół.
- Duża część prawidłowej poczty pochodzi od ludzi, z którymi nigdy nie kontaktowano się drogą e-mailową, np. klientami, potencjalnymi partnerami biznesowymi itd. W tym przypadku wymagane są inne rozwiązania.

  Jeśli używasz jednego z klientów pocztowych zintegrowanych z Bitdefender, spróbuj wyświetlić błędy wykrywania.

Notatka

Bitdefender jest zintegrowany z najbardziej popularnymi klientami poczty dzięki wykorzystaniu łatwego w użyciu antyspamowego paska narzędziowego. W celu uzyskania kompletnej listy obsługiwanych klientów poczty e-mail, odwołaj się do *„Obsługiwane klienty poczty i protokoły"* (p. 118).

Dodaj kontakty do listy Przyjaciół

Jeśli używasz obsługiwanego klienta poczty, możesz łatwo dodawać uprawnionych nadawców do listy Przyjaciół. Wykonaj następujące kroki:

1. W programie klienta poczty zaznacz wiadomość e-mail od nadawcy, którego chcesz dodać do listy Przyjaciół.
2. Kliknij przycisk **Dodaj przyjaciela** na pasku narzędziowym modułu antyspamowego Bitdefender.
3. Możesz zostać poproszony o potwierdzenie adresów dodanych do listy Przyjaciół. Wybierz **Nie pokazuj tego komunikatu ponownie** i kliknij **OK**.

Będziesz zawsze otrzymywał wiadomości e-mail z tego adresu bez względu na zawartość wiadomości.

Jeśli używasz innego klienta poczty, możesz dodać kontakty do listy Przyjaciół, korzystając z interfejsu Bitdefender. Wykonaj następujące kroki:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYSPAM** wybierz **Zarządzaj Przyjaciółmi**.

   Pojawia się okno konfiguracji.
4. Wpisz adres skrzynki e-mail, z której zawsze chcesz otrzymywać wiadomości, a następnie kliknij "**Dodaj**". Możesz dodać dowolną liczbę adresów poczty elektronicznej.
5. Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.

Wyświetl błędy wykrywania

Jeśli używasz wspieranego klienta poczty, możesz z łatwością ulepszyć filtr antyspamowy (poprzez zaznaczenie, które wiadomości e-mail nie powinny być oznaczone jako [spam]). Ta czynność poprawi skuteczność filtrów antyspamowych. Wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu śmieci, gdzie zostały przeniesione wiadomości spamowe.
3. Wybierz dozwoloną wiadomość nieprawidłowo oznaczoną przez Bitdefender jako [spam].
4. Kliknij przycisk **Dodaj przyjaciela** znajdujący się na antyspamowym pasku narzędziowym Bitdefender, aby dodać nadawcę do listy Przyjaciół. Możesz zostać zapytany o potwierdzenie, klikając "**OK**". Będziesz zawsze otrzymywał wiadomości e-mail z tego adresu bez względu na zawartość wiadomości.
5. Kliknij przycisk **To nie jest Spam** na antyspamowym pasku narzędzi produktu Bitdefender (zwykle zlokalizowanym w górnej części okna klienta pocztowego). Wiadomości e-mail będą przenoszone do folderu „Skrzynka odbiorcza".

29.11.2. Spam nie jest odpowiednio wykrywany

Jeśli odbierasz dużo wiadomości spamowych, które nie są oznaczane jako [spam], musisz skonfigurować filtr antyspamowy Bitdefender tak, aby zwiększyć jego wydajność.

Spróbuj następujących rozwiązań:

1. Jeśli używasz jednego z klientów pocztowych zintegrowanych z Bitdefender, spróbuj wyświetlić niewykryte wiadomości spamowe.

   Notatka

   Bitdefender jest zintegrowany z najbardziej popularnymi klientami poczty dzięki wykorzystaniu łatwego w użyciu antyspamowego paska narzędziowego. W celu uzyskania kompletnej listy obsługiwanych klientów poczty e-mail, odwołaj się do *„Obsługiwane klienty poczty i protokoły"* (p. 118).

2. Dodaj spamerów do listy Spamerów. Wiadomości e-mail pochodzące od adresów zawartych w liście Spamerów są automatycznie oznaczane jako [spam].

Wyświetl niewykryte wiadomości spamowe

Jeśli używasz wspieranego klienta poczty, możesz łatwo wskazać, które z wiadomości mają być traktowane jako spam. Ta czynność poprawi skuteczność filtrów antyspamowych. Wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu Skrzynki odbiorczej.
3. Wybierz niewykryte wiadomości spamowe.
4. Kliknij przycisk **To jest Spam** w pasku narzędziowym produktu Bitdefender (zwykle zlokalizowanym w górnej części okna klienta pocztowego). Są one natychmiast oznaczane jako [spam] i przenoszone do folderu śmieci.

Dodaj spamerów do listy Spamerów.

Jeśli używasz obsługiwanego klienta pocztowego, możesz łatwo dodawać nadawców wiadomości zawierających spam do listy Spamerów. Wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu śmieci, gdzie zostały przeniesione wiadomości spamowe.
3. Wybierz wiadomości oznaczone przez Bitdefender jako[spam].
4. Kliknij przycisk **Dodaj spamera** na pasku narzędziowym modułu antyspamowego Bitdefender.
5. Możesz zostać poproszony o potwierdzenie adresów dodanych do listy Spamerów. Wybierz **Nie pokazuj tego komunikatu ponownie** i kliknij **OK**.

Jeśli używasz innego klienta pocztowego, możesz ręcznie dodać spamerów do listy Spamerów z poziomu interfejsu Bitdefender. Najlepiej zrobić to tylko wtedy, gdy otrzymano już kilka wiadomości spamowych z tego adresu. Wykonaj następujące kroki:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W module **ANTYSPAM**, wybierz **Zarządzaj Spamerami**.

   Pojawia się okno konfiguracji.

4. Wprowadź adres e-mail spamera i kliknij "**Dodaj**". Możesz dodać dowolną liczbę adresów poczty elektronicznej.
5. Kliknij "**OK**", aby zapisać zmiany i zamknąć okno.

29.11.3. Filtr antyspamowy nie wykrył żadnej wiadomości spamowej

Jeśli żadna wiadomość nie jest oznaczana jako [spam], problem może dotyczyć filtra antyspamowego Bitdefender. Przed próbą rozwiązania tego problemu sprawdź, czy nie jest on powodowany przez jeden z poniższych czynników:

- Ochrona antyspamowa może nie być włączona. Aby zweryfikować status antyspamu, kliknij ikony po lewej stronie interfejsu Bitdefender i wybierz link **Zobacz funkjonalności**. Kliknij "zębatkę" z panelu **ANTISPAM**, następnie sprawdź górną stronę okna i sprawdź czy funkcjonalność jest włączona.

  Jeśli moduł antyspamowy jest wyłączony, może to być przyczyną problemu. Kliknij przełącznik, aby włączyć ochronę antyspamową.

- Ochrona przed spamem Bitdefender jest dostępna tylko dla klientów poczty e-mail skonfigurowanych na odbieranie wiadomości przez protokół POP3. To oznacza poniższe:

  - Wiadomości e-mail odbierane przez usługi oparte na stronach WWW (takie jak Yahoo, Gmail, Hotmail i inne) nie będą filtrowane przez Bitdefender pod kątem spamu.
  - Jeśli Twój klient pocztowy jest skonfigurowany, aby odbierać wiadomości poprzez protokoły inne niż POP3 (takie jak np. IMAP4), Bitdefender nie będzie filtrował spamu.

  Notatka

  POP3 jest najbardziej popularnym protokołem używanym do pobierania wiadomości e-mail z serwera poczty. Jeśli nie znasz protokołu, z którego korzysta Twój klient pocztowy, spytaj osobę, która go konfigurowała.

- Bitdefender Internet Security 2018 nie skanuje ruchu POP3 programu Lotus Notes.

Jednym z możliwych rozwiązań jest naprawa lub reinstalacja oprogramowania. Można jednak również skontaktować się z Bitdefender,

korzystając z metody przedstawionej w sekcji *„Prośba o pomoc”* (p. 219), aby uzyskać pomoc techniczną.

29.12. Nie działa u mnie automatyczne uzupełnianie danych przez Portfel

Zapisałeś swoje poświadczenia online w Menadżerze Haseł Bitdefender ale zauważyłeś, że auto uzupełnianie nie działa. Zwykle taka sytuacja występuje, gdy rozszerzenie Portfel Bitdefender nie jest zainstalowane w Twojej przeglądarce.

Wykonaj następujące czynności, aby naprawić ten przypadek:

- W **Microsoft Edge**
  1. Otwórz Microsoft Edge.
  2. Kliknij Więcej...
  3. Kliknij Rozszerzenia.
  4. Odnajdź **Portfel Bitdefender** i kliknij **Włącz**.
- W **Internet Explorer:**
  1. Otwórz przeglądarkę Internet Explorer.
  2. Kliknij Narzędzia.
  3. Kliknij Zarządzaj dodatkami.
  4. Kliknij Paski narzędziowe i Rozszerzenia.
  5. Odnajdź **Portfel Bitdefender** i kliknij **Włącz**.
- W **Mozilla Firefox:**
  1. Otwórz Mozilla Firefox.
  2. Kliknij Narzędzia.
  3. Kliknij Dodatki.
  4. Kliknij Rozszerzenia.
  5. Odnajdź **Portfel Bitdefender** i kliknij **Włącz**.
- W **Google Chrome:**
  1. Otwórz Google Chrome.
  2. Przejdź do ikony Menu.

3. Kliknij Ustawienia.
4. Kliknij Rozszerzenia.
5. Odnajdź **Portfel Bitdefender** i kliknij **Włącz**.

Notatka
Dodatek zostanie włączony po ponownym otwarciu Twojej przeglądarki.

Sprawdź teraz, czy funkcja automatycznego uzupełniania danych przez Portfel działa w przypadku Twoich kont online.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

29.13. Usunięcie produktu Bitdefender nie powiodło się

Jeśli zechcesz usunąć swój program Bitdefender i zauważysz, że ten proces nie odpowiada lub system jest zawieszony, kliknij **Anuluj**, aby przerwać to działanie. Jeśli to nie zadziała, uruchom ponownie system.

Jeśli usuwanie nie powiedzie się, niektóre wpisy do rejestru i pliki programu Bitdefender mogą pozostać w Twoim systemie. Takie pozostałości mogą blokować nową próbę instalacji programu Bitdefender. Mogą także wpłynąć na wydajność i stabilność systemu.

Aby całkowicie usunąć Bitdefender z Twojego systemu:

- W systemie **Windows 7**:
  1. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
  2. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
  3. Kliknij **USUŃ** w oknie, które się pojawi.
  4. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
- W systemach **Windows 8 i Windows 8.1**:
  1. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.

2. Kliknij **Odinstaluj program** lub **Programy i funkcje**.
3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
4. Kliknij **USUŃ** w oknie, które się pojawi.
5. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

- W systemie **Windows 10**:
  1. Kliknij **Start**, a następnie kliknij Ustawienia.
  2. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.
  3. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.
  4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.
  5. Kliknij **USUŃ** w oknie, które się pojawi.
  6. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

29.14. Mój system nie uruchamia się po instalacji produktu Bitdefender

Może być wiele powodów, dla których nie możesz ponownie uruchomić systemu w trybie normalnym po zainstalowaniu produktu Bitdefender.

Najprawdopodobniej jest to spowodowane przez poprzednio zainstalowaną wersję Bitdefender, która nie została prawidłowo odinstalowana lub inny program zabezpieczający na Twoim komputerze.

Dostępne są następujące działania zależnie od sytuacji:

- **Miałeś już zainstalowany produkt Bitdefender i nie usunąłeś go w odpowiedni sposób.**

  Aby to rozwiązać:

  1. Uruchom ponownie system w Trybie awaryjnym. Informacje, jak należy to zrobić, znajdują się w *„Jak uruchomić ponownie komputer w Trybie awaryjnym?"* (p. 84).
  2. Usuń Bitdefender z systemu:
     - W systemie **Windows 7**:

a. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.

b. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

c. Kliknij **USUŃ** w oknie, które się pojawi.

d. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

e. Uruchom swój system ponownie w Trybie normalnym.

- W systemach **Windows 8 i Windows 8.1**:

a. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.

b. Kliknij **Odinstaluj program** lub **Programy i funkcje**.

c. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

d. Kliknij **USUŃ** w oknie, które się pojawi.

e. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

f. Uruchom swój system ponownie w Trybie normalnym.

- W systemie **Windows 10**:

a. Kliknij **Start**, a następnie kliknij Ustawienia.

b. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.

c. Wyszukaj **Bitdefender Internet Security 2018** i wybierz opcję **Odinstaluj**.

d. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.

e. Kliknij **USUŃ** w oknie, które się pojawi.

f. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

g. Uruchom swój system ponownie w Trybie normalnym.

3. Zainstaluj ponownie swój program Bitdefender.

- **Miałeś już zainstalowane inne rozwiązanie ochronne i nie usunąłeś go w odpowiedni sposób.**

  Aby to rozwiązać:

  1. Uruchom ponownie system w Trybie awaryjnym. Informacje, jak należy to zrobić, znajdują się w *„Jak uruchomić ponownie komputer w Trybie awaryjnym?"* (p. 84).
  2. Usuń inne rozwiązanie bezpieczeństwa ze swojego systemu:
     - W systemie **Windows 7**:
       a. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
       b. Znajdź nazwę programu, który chcesz usunąć i wybierz **Usuń**.
       c. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
     - W systemach **Windows 8 i Windows 8.1**:
       a. W oknie ekranu menu Start systemu Windows zlokalizuj **Panel sterowania** (przykładowo, możesz zacząć pisać "Panel sterowania" bezpośrednio na ekranie menu Start), a następnie kliknij na jego ikonę.
       b. Kliknij **Odinstaluj program** lub **Programy i funkcje**.
       c. Znajdź nazwę programu, który chcesz usunąć i wybierz **Usuń**.
       d. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.
     - W systemie **Windows 10**:
       a. Kliknij **Start**, a następnie kliknij Ustawienia.
       b. Kliknij ikonę **System** w obszarze Ustawienia, następnie wybierz **Zainstalowane aplikacje**.
       c. Znajdź nazwę programu, który chcesz usunąć i wybierz **Odinstaluj**.
       d. Zaczekaj na zakończenie procesu odinstalowania, a następnie ponownie uruchom system.

  Aby poprawnie odinstalować inne oprogramowanie, udaj się na stronę producenta tego oprogramowania i uruchom narzędzie deinstalacji lub

skontaktuj się bezpośrednio z producentem w celu otrzymania wytycznych odnośnie deinstalacji.

3. Uruchom ponownie system w Trybie normalnym i przeinstaluj Bitdefender.

Wykonałeś już powyższe czynności, a problem nadal nie został rozwiązany.

Aby to rozwiązać:

1. Uruchom ponownie system w Trybie awaryjnym. Informacje, jak należy to zrobić, znajdują się w *„Jak uruchomić ponownie komputer w Trybie awaryjnym?"* (p. 84).
2. Użyj opcji odzyskiwania systemu Windows, aby przywrócić komputer do stanu sprzed zainstalowania produktu Bitdefender.
3. Uruchom ponownie system w Trybie normalnym i skontaktuj się z naszymi przedstawicielami pomocy technicznej, aby uzyskać pomoc opisaną w sekcji *„Prośba o pomoc"* (p. 219).

30. USUWANIE SZKODLIWEGO OPROGRAMOWANIA Z SYSTEMU

Złośliwe oprogramowanie może wpływać na system na wiele różnych sposobów, a rodzaj pracy Bitdefender zależy od typu ataku tego oprogramowania. Ponieważ wirusy często zmieniają swoje zachowanie, ustalenie wzorca ich zachowania i działania jest bardzo trudne.

Istnieją sytuacje, gdy Bitdefender nie może automatycznie usunąć z systemu infekcji złośliwego oprogramowania. W takich wypadkach wymagana jest interwencja użytkownika.

Jeśli nie możesz w tym miejscu znaleźć pomocy dla swojego problemu lub przedstawione rozwiązania nie pomagają, możesz skontaktować się z przedstawicielem pomocy technicznej Bitdefender, korzystając z metody przedstawionej w rozdziale *„Prośba o pomoc"* (p. 219).

30.1. Bitdefender Tryb Ratunkowy (Środowisko Ratunkowe w Windows 10)

Tryb Ratunkowy to funkcja produktu Bitdefender, która pozwala na skanowanie i oczyszczanie wszystkich istniejących partycji dysku twardego wewnątrz i poza systemem operacyjnym.

Po instalacji Bitdefender Internet Security 2018 na **Windows 7, Windows 8 i Windows 8.1** i pobraniu Obrazu Płyty Ratunkowej Bitdefender, Tryb

Ratunkowy może być użyty nawet wtedy, gdy nie można już uruchomić systemu Windows.

W systemie Windows 10, Środowisko Ratunkowe Bitdefender jest zintegrowane z systemem Windows RE, co oznacza, że nie trzeba pobierać Obrazu Płyty Ratunkowej w tym systemie operacyjnym, a funkcja nie może być używana w przypadku problemów z uruchamianiem. Aby wyczyścić system przed załadowaniem usług systemu Windows, zalecamy użycie Ratunkowej Płyty CD Bitdefender.

Ratunkowa Płyta Bitdefender jest bezpłatnym narzędziem, które skanuje i czyści komputer, gdy podejrzewasz, że zagrożenie malware ma wpływ na jego działanie. Artykuły zawierające szczegółowe informacje na temat tworzenia i korzystania z nich dostępne są na platformie Centrum Wsparcia Bitdefender na https://www.bitdefender.pl/kontakt1.

Pobieranie Dysku Ratunkowego Bitdefender

Aby móc korzystać z Trybu Ratunkowego na **Windows 7, Windows 8 i Windows 8.1**, pobierz jego plik graficzny w następujący sposób:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **ANTYWIRUS**, kliknij **Tryb ratunkowy**.
4. Kliknij **TAK** w oknie, które się pojawi aby potwierdzić ponowne uruchomienie komputera.

   Poczekaj aż Dysk Ratunkowy Bitdefender pobierze się z serwerów Bitdefender. Jak tylko proces pobierania się zakończy, komputer uruchomi się ponownie.

   W menu zostaniesz poproszony o wybranie startowego systemu operacyjnego. W tym kroku możesz wybrać aby startować system w Trybie Ratunkowym lub normalnym.

Notatka

Ze względu na integrację ze Środowiskiem Odzyskiwania systemu Windows w **systemie Windows 10**, nie ma potrzeby pobierania Płyty Ratunkowej w tym systemie operacyjnym.

Uruchamianie systemu w Trybie Ratunkowym w systemach Windows 7, Windows 8 i Windows 8.1

Możesz wejść w Tryb ratunkowy na dwa sposoby:

Z interfejsu Bitdefender

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **ANTYWIRUS**, kliknij **Tryb ratunkowy**.
4. Kliknij **TAK** w oknie, które się pojawi aby potwierdzić ponowne uruchomienie komputera.
5. Po ponownym uruchomieniu komputera pojawi się menu, w którym zostaniesz poproszony o wybór systemu operacyjnego. Wybierz **Tryb ratunkowy Bitdefender**, aby uruchomić komputer w środowisku produktu Bitdefender, gdzie możesz oczyścić partycję Windows.
6. W okienku, które się pojawi, naciśnij klawisz **Enter** i wybierz rozdzielczość ekranu najbliższą tej, której zwykle używasz. Następnie ponownie naciśnij **Enter**.

   Tryb ratunkowy produktu Bitdefender ładuje się w ciągu kilku chwil.

Uruchom komputer bezpośrednio w Trybie ratunkowym

Jeśli system Windows się nie uruchamia, możesz uruchomić komputer bezpośrednio w Trybie ratunkowym produktu Bitdefender, wykonując następujące czynności:

- W systemie **Windows 7**:
  1. Naciśnij klawisz **F8**, aż pojawi się ekran **Zaawansowane Opcje Rozruchu**.
  2. Użyj strzałek aby wybrać Tryb Ratunkowy Bitdefender, następnie naciśnij **Enter**.

     Tryb ratunkowy produktu Bitdefender niedługo się załaduje.
- W systemach **Windows 8 i Windows 8.1**:
  1. Naciśnij klawisz **Shift**, aż pojawi się ekran **Zaawansowane Opcje Rozruchu**.
  2. Wybierz opcję **Użyj innego systemu operacyjnego**, a następnie opcję Tryb Ratunkowy Bitdefender.

Tryb ratunkowy produktu Bitdefender niedługo się załaduje.

Notatka
Uruchomienie komputera w Trybie Ratunkowym jest możliwe tylko jeśli Dysk Ratunkowy został wcześniej pobrany zgodnie z opisem w „Pobieranie Dysku Ratunkowego Bitdefender" (p. 209).

Uruchamianie systemu w Środowisku Ratunkowym systemu Windows 10

Środowisko Ratunkowe można wprowadzić tylko z produktu Bitdefender w następujący sposób:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Kliknij link **POKAŻ FUNKCJE**.
3. W okienku **ANTYWIRUS**, kliknij **Środowisko Ratunkowe**.
4. Kliknij **Uruchom ponownie** w oknie, które się pojawi.

   Środowisko Ratunkowe Bitdefender niedługo się załaduje.

Skanowanie systemu w Trybie Ratunkowym (Środowisko Ratunkowe systemu Windows 10)

Aby zeskanować system w Trybie Ratunkowym (Środowisko Ratunkowe):

- W systemach **Windows 7, Windows 8 i Windows 8.1**:
  1. Przejdź do Trybu ratunkowego, tak jak to opisano tutaj: „Uruchamianie systemu w Trybie Ratunkowym w systemach Windows 7, Windows 8 i Windows 8.1" (p. 210).
  2. Pojawi się logo produktu Bitdefender i rozpocznie się kopiowanie silnika antywirusowego.
  3. Następnie pojawi się okno powitalne. Kliknij "**Kontynuuj**".
  4. Rozpoczęto aktualizację sygnatur antywirusowych.
  5. Po ukończeniu aktualizacji pojawia się Antywirusowy Skaner Na Żądanie produktu Bitdefender.
  6. Kliknij "**Skanuj teraz**", wskaż cel skanowania w wyskakującym okienku i kliknij "**Otwórz**", aby rozpocząć skanowanie.

Zaleca się przeskanowanie całej partycji, na której zainstalowany jest system Windows.

Notatka
Jeśli pracujesz w Trybie ratunkowym, pojawiają się nazwy partycji charakterystyczne dla systemów Linux. Pojawi się partycja sda1, która prawdopodobnie będzie się odnosić do systemowej partycji (C:), sda2 do (D:) itd.

7. Poczekaj na zakończenie skanowania. Jeśli zostanie wykryte szkodliwe oprogramowanie, postępuj zgodnie z instrukcjami, żeby się go pozbyć.
8. Aby wyjść z Trybu ratunkowego, kliknij prawym przyciskiem myszy na puste miejsce na pulpicie, wybierz **Zamknij** z wyświetlonego menu, a następnie albo uruchom ponownie albo wyłącz komputer.

- W systemie **Windows 10**:

1. Wejdź do Środowiska Ratunkowego, jak opisano w„Uruchamianie systemu w Środowisku Ratunkowym systemu Windows 10" (p. 211)
2. Proces skanowania Bitdefender rozpoczyna się automatycznie, gdy tylko system zostanie załadowany do Środowiska Ratunkowego.
3. Poczekaj na zakończenie skanowania. Jeśli zostanie wykryte szkodliwe oprogramowanie, postępuj zgodnie z instrukcjami, żeby się go pozbyć.
4. Aby opuścić Środowisko Ratunkowe, kliknij **ZAMKNIJ** w oknie z rezultatem skanowania.

30.2. Co zrobić, kiedy Bitdefender znajdzie wirusy na Twoim komputerze?

O obecności wirusa na komputerze można dowiedzieć się w następujący sposób:

- Przeskanowałeś komputer i Bitdefender znalazł w nim zainfekowane elementy.
- Alarm wirusowy informuje o zablokowaniu przez Bitdefender jednego lub więcej wirusów w komputerze.

W takich sytuacjach zaktualizuj Bitdefender, aby mieć pewność, że masz aktualne sygnatury szkodliwego oprogramowania i uruchom skanowanie systemu.

Po zakończeniu skanowania systemu, wybierz odpowiednie działanie wobec zainfekowanych elementów (Wylecz, Usuń, Przenieś do kwarantanny).

Ostrzeżenie

Jeśli przypuszczasz, że dany plik jest częścią systemu operacyjnego Windows lub, że nie jest zainfekowany, nie wykonuj tych kroków i jak najszybciej skontaktuj się z obsługą klienta Bitdefender.

Jeśli nie można przeprowadzić wybranej operacji, a dzienniki skanowania ujawnią infekcję, której nie można usunąć, musisz usunąć dany plik ręcznie:

Pierwsza metoda może być użyta w Trybie normalnym:

1. Wyłącz ochronę antywirusową w czasie rzeczywistym Bitdefender:
   a. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
   b. Kliknij link **POKAŻ FUNKCJE**.
   c. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
   d. W oknie **OCHRONA** kliknij przełącznik WŁĄCZ/WYŁĄCZ.
2. Wyświetl ukryte obiekty w systemie Windows. Informacje, jak należy to zrobić, znajdują się w *„Jak wyświetlić ukryte obiekty w systemie Windows?”* (p. 82).
3. Przejdź do miejsca, w którym znajduje się zainfekowany plik (sprawdź dziennik skanowania) i usuń go.
4. Włącz ochronę antywirusową w czasie rzeczywistym Bitdefender.

W przypadku, kiedy pierwsza metoda zawiedzie przy usunięciu infekcji:

1. Uruchom ponownie system w Trybie awaryjnym. Informacje, jak należy to zrobić, znajdują się w *„Jak uruchomić ponownie komputer w Trybie awaryjnym?”* (p. 84).
2. Wyświetl ukryte obiekty w systemie Windows. Informacje, jak należy to zrobić, znajdują się w *„Jak wyświetlić ukryte obiekty w systemie Windows?”* (p. 82).
3. Przejdź do miejsca, w którym znajduje się zainfekowany plik (sprawdź dziennik skanowania) i usuń go.
4. Uruchom ponownie system w Trybie normalnym.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

30.3. Jak usunąć wirusa z archiwum?

Archiwum to plik lub zbiór plików skompresowany w specjalnym formacie, w celu ograniczenia ilości miejsca niezbędnego do jego zapisania na dysku.

Niektóre z tych formatów to formaty otwarte. Bitdefender może dzięki temu skanować je od środka i podejmować odpowiednie działania, aby je usunąć.

Inne formaty archiwów są częściowo lub całkowicie zamknięte. Bitdefender może wykryć w nich obecność wirusów, ale nie może podjąć jakichkolwiek działań.

Jeśli Bitdefender informuje, iż w archiwum znaleziono wirusa i nie może podjąć żadnych działań, oznacza to, że usunięcie wirusa jest niemożliwie z powodu ograniczeń w ustawieniach zezwoleń tego archiwum.

Oto, w jaki sposób można usunąć wirusa z archiwum:

1. Zidentyfikuj archiwum zawierające wirusa, wykonując skanowanie systemu.
2. Wyłącz ochronę antywirusową w czasie rzeczywistym Bitdefender:
   a. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
   b. Kliknij link **POKAŻ FUNKCJE**.
   c. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
   d. W oknie **OCHRONA** kliknij przełącznik WŁĄCZ/WYŁĄCZ.
3. Przejdź do miejsca, w którym znajduje się archiwum i zdekompresuj je, używając do tego celu aplikacji do archiwizacji danych, takiej jak WinZip.
4. Zidentyfikuj zainfekowany plik i usuń go.
5. Aby mieć pewność, że infekcja została usunięta całkowicie, usuń oryginalne archiwum.
6. Pliki skompresuj ponownie w nowym archiwum, używając do tego celu aplikacji do archiwizacji danych, takiej jak WinZip.
7. Włącz ochronę antywirusową w czasie rzeczywistym Bitdefender i uruchom pełne skanowanie systemu, aby upewnić się, że nie ma żadnej innej infekcji.

Notatka
Należy zwrócić uwagę, iż wirus zapisany w archiwum nie jest bezpośrednim zagrożeniem dla systemu, ponieważ aby mógł go zainfekować, musi być najpierw rozpakowany i uruchomiony.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

30.4. Jak usunąć wirusa z archiwum wiadomości e-mail?

Bitdefender może również identyfikować wirusy w bazach danych e-mail oraz archiwach e-mail zapisanych na dysku.

Czasami trzeba zidentyfikować zainfekowaną wiadomość, korzystając z informacji podanych w raporcie ze skanowania i usunąć ją ręcznie.

Oto, w jaki sposób można usunąć wirusa zapisanego w archiwum poczty:

1. Skanuj bazę danych e-mail przy użyciu Bitdefender.
2. Wyłącz ochronę antywirusową w czasie rzeczywistym Bitdefender:
   a. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
   b. Kliknij link **POKAŻ FUNKCJE**.
   c. Wybierz ikonę w prawym dolnym rogu panelu **ANTYWIRUS**.
   d. W oknie **OCHRONA** kliknij przełącznik WŁĄCZ/WYŁĄCZ.
3. Otwórz raport ze skanowania i użyj informacji identyfikacyjnych (Temat, Od, Do) zainfekowanych wiadomości, aby odnaleźć je w kliencie poczty.
4. Usuń zainfekowane wiadomości. Większość klientów poczty przenosi usunięte wiadomości do folderu odzyskiwania, skąd można je odzyskać. Powinieneś upewnić się, że wiadomość została usunięta także z folderu odzyskiwania.
5. Kompaktuj folder zawierający zainfekowaną wiadomość.
   - W Microsoft Outlook 2007: W menu "Plik" kliknij "Zarządzanie plikami danych". Zaznacz pliki folderów osobistych (.pst), które chcesz kompaktować i kliknij "Ustawienia". Kliknij "Kompaktuj teraz".
   - W Microsoft Outlook 2010 / 2013/ 2016: W menu "Plik" kliknij "Informacje", a następnie "Ustawienia konta" (Dodawaj i usuwaj konta

lub zmieniaj istniejące ustawienia połączeń). Następnie kliknij "Plik danych", wybierz foldery plików osobistych (.pst), które zamierzasz kompaktować i kliknij "Ustawienia". Kliknij "Kompaktuj teraz".

6. Włącz ochronę antywirusową w czasie rzeczywistym Bitdefender.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 219).

30.5. Co zrobić, jeśli podejrzewam, że dany plik jest niebezpieczny?

Możesz podejrzewać, że plik na Twoim komputerze jest niebezpieczny, nawet jeśli Twój Bitdefender tego nie wykrył.

Aby upewnić się, że system jest chroniony:

1. Uruchom **Skanowanie systemu** z poziomu Bitdefender. Informacje, jak należy to zrobić, znajdują się w *„Jak mogę przeskanować swój system?"* (p. 62).
2. Jeśli skanowanie nic nie wykryło, ale nadal nie masz pewności co do jakiegoś pliku, skontaktuj się z działem pomocy technicznej.

   Informacje, jak należy to zrobić, znajdują się w *„Prośba o pomoc"* (p. 219).

30.6. Czym są pliki chronione hasłem w dzienniku skanowania?

Jest to tylko informacja, która wskazuje, że Bitdefender wykrył te pliki, które są zabezpieczone hasłem lub zaszyfrowane w inny sposób.

Elementy chronione hasłem to najczęściej:

- Pliki, które należą do innego rozwiązania zabezpieczającego.
- Pliki, które należą do systemu operacyjnego.

Aby faktycznie przeprowadzić skanowanie zawartości, pliki te muszą być wypakowane lub w inny sposób rozszyfrowane.

W przypadku rozpakowania tej zawartości, działający w czasie rzeczywistym skaner Bitdefender automatycznie przeskanuje ją, aby zapewnić komputerowi ochronę. Jeśli chcesz skanować te pliki przy użyciu Bitdefender, musisz skontaktować się z producentem produktu, aby uzyskać więcej informacji na ich temat.

Zalecamy zignorowanie tych plików, ponieważ nie stanowią one zagrożenia dla systemu.

30.7. Które elementy pominięto w dzienniku skanowania?

Wszystkie pliki, które w raporcie skanowania zostaną oznaczone jako "Pominięte", są czyste.

Aby zwiększyć wydajność, Bitdefender nie skanuje plików, które nie uległy zmianie od czasu ostatniego skanowania.

30.8. Czym są nadmiernie skompresowane pliki w dzienniku skanowania?

Nadmiernie skompresowane elementy to takie, które nie zostały wypakowane przez mechanizm skanujący lub elementy, których rozszyfrowanie zajęłoby zbyt dużo czasu, czyniąc system niestabilnym.

Nadmierna kompresja oznacza, że Bitdefender pominął skanowanie tego archiwum, gdyż jego wypakowanie pochłonęłoby zbyt wiele zasobów systemowych. Zawartość w razie potrzeby zostanie przeskanowana w czasie rzeczywistym.

30.9. Dlaczego Bitdefender automatycznie usunął zarażony plik?

W przypadku wykrycia zainfekowanego pliku Bitdefender podejmie automatyczną próbę jego leczenia. Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.

W przypadku określonych typów złośliwego oprogramowania oczyszczanie jest niemożliwe, ponieważ złośliwy jest cały plik. W takich wypadkach zainfekowany plik jest usuwany z dysku.

Zwykle dotyczy to plików instalacyjnych pobranych z witryn internetowych, którym nie można ufać. W przypadku wystąpienia takiej sytuacji, pobierz plik instalacyjny z witryny producenta lub innej zaufanej strony.

WYŚLIJ NAM SWOJĄ OPINIĘ

31. PROŚBA O POMOC

Bitdefender dostarcza swoim klientom szybkiego i drobiazgowego wsparcia na niezrównanym poziomie. Jeśli zetkniesz się z jakimś problemem lub będziesz mieć jakieś pytanie dotyczące programu Bitdefender, możesz skorzystać z szeregu zasobów internetowych, aby znaleźć rozwiązanie lub odpowiedź. W tym samym czasie, możesz się skontaktować z zespołem obsługi klienta Bitdefender. Nasi przedstawiciele ds. pomocy technicznej szybko odpowiedzą na Twoje pytania oraz zapewnią Ci niezbędną pomoc.

Sekcja *„Rozwiązywanie typowych problemów”* (p. 185) dostarcza niezbędnych informacji na temat najczęściej występujących zagadnień, które mogą pojawić się podczas korzystania z tego produktu.

Jeśli nie znajdziesz odpowiedzi na swoje pytanie w udostępnionych zasobach, możesz skontaktować się bezpośrednio z nami:

- „Skontaktuj się z nami bezpośrednio z twojego produktu Bitdefender” (p. 219)
- „Skontaktuj się z naszym centrum wsparcia technicznego online” (p. 220)

Skontaktuj się z nami bezpośrednio z twojego produktu Bitdefender

Jeśli jesteś połączony z Internetem, możesz poprosić Bitdefender o wsparcie bezpośrednio z poziomu interfejsu produktu.

Wykonaj następujące kroki:

1. Kliknij ikonę po lewej stronie interfejsu Bitdefender.
2. Możesz wybrać spośród dostępnych opcji:
   - **Dokumentacja produktu**

     Wejdź do naszej bazy danych i wyszukaj niezbędne informacje.
   - **Kontakt z działem Pomocy technicznej**

     Użyj przycisku **Skontaktuj się z Pomocą techniczną**, aby uruchomić narzędzie Pomocy technicznejBitdefender i skontaktować się z działem obsługi klienta. Możliwość poruszania się w kreatorze zapewnia przycisk "**Dalej**". Aby zakończyć pracę kreatora, kliknij "**Anuluj**".

     a. Zaznacz pole wyboru oznaczające zgodę, a następnie kliknij **„Dalej”**.

b. Wypełnij pola formularza niezbędnymi danymi:

i. Wprowadź swój adres e-mail.

ii. Wprowadź swoje imię i nazwisko.

iii. Opisz problem, który napotkałeś.

iv. Sprawdź opcję **Spróbuj odtworzyć ten problem, przed zgłoszeniem** w przypadku napotkania problemu z produktem. Kontynuuj zgodnie z wymaganymi krokami.

c. Poczekaj kilka minut, aż Bitdefender zgromadzi informacje dotyczące produktu. Pomogą one naszym inżynierom w znalezieniu rozwiązania twojego problemu.

d. Kliknij **Zakończ**, aby wysłać informację do działu Obsługi Klienta Bitdefender. Otrzymasz odpowiedź tak szybko, jak to tylko możliwe.

- **Poszukaj pomocy online**

  Uzyskaj dostęp do naszych artykułów online.

Skontaktuj się z naszym centrum wsparcia technicznego online

Jeśli nie możesz znaleźć potrzebnych ci informacji, używając produktu Bitdefender, skontaktuj się z naszym Centrum Pomocy Technicznej online.

1. Odwiedź https://www.bitdefender.pl/kontakt1.

   W centrum pomocy technicznej produktu Bitdefender znajduje się wiele artykułów zawierających rozwiązania problemów produktu Bitdefender.

2. Użyj paska wyszukiwania w górnej części tego okna, aby znaleźć artykuły, które mogą zawierać rozwiązanie Twojego problemu. Aby rozpocząć, wpisz szukane słowo w pasku wyszukiwania i kliknij **Szukaj**.

3. Przeczytaj stosowne artykuły oraz dokumenty i wypróbuj zaproponowane rozwiązania.

4. Jeśli to nie rozwiązuje Twojego problemu, przejdź do

   https://www.bitdefender.pl/kontakt1 i skontaktuj się z naszym Działem Wsparcia.

32. ZASOBY ONLINE

W rozwiązywaniu problemów związanych z Bitdefender pomoc zapewnia kilka zasobów internetowych.

- Centrum wsparcia Bitdefender:

  https://www.bitdefender.pl/kontakt1

- Forum pomocy technicznej Bitdefender:

  http://forum.bitdefender.com

- Portal bezpieczeństwa komputerowego HOTforSecurity:

  http://www.bitdefender.marken.com.pl/

Możesz również użyć ulubionej wyszukiwarki, aby znaleźć więcej informacji o ochronie komputera, produktach Bitdefender i firmie.

32.1. Centrum pomocy technicznej produktu Bitdefender

Centrum pomocy technicznej Bitdefender to internetowy magazyn informacji o produktach Bitdefender. Przechowuje czytelne raporty z trwających działań zespołu Bitdefender odnośnie pomocy technicznej i naprawiania błędów oraz bardziej ogólne artykuły dotyczące ochrony antywirusowej, szczegółowego zarządzania rozwiązaniami produktu Bitdefender oraz wielu innych zagadnień.

Centrum wsparcia Bitdefender jest publicznie dostępne i łatwe do przeszukania. Informacje, które zawiera, stanowią kolejny sposób na dostarczenie klientom Bitdefender, potrzebnej wiedzy technicznej i wsparcia. Prawidłowe żądania informacji lub raportów o błędach, pochodzące od klientów Bitdefender, w końcu znajdują drogę do Wsparcia technicznego Bitdefender jako raporty informujące o poprawkach, sposoby ominięcia problemów czy pliki pomocy produktu i teksty informacyjne.

Centrum wsparcia Bitdefender jest dostępne o każdej porze na

https://www.bitdefender.pl/kontakt1.

32.2. Forum pomocy technicznej Bitdefender

Forum pomocy technicznej Bitdefender pozwala użytkownikom Bitdefender uzyskać pomoc oraz pomagać innym osobom korzystającym z produktu.

Jeśli produkt Bitdefender nie działa dobrze, jeśli nie może usuwać z komputera określonych wirusów lub jeśli masz wątpliwości co do jego pracy, zamieść swój problem lub pytanie na forum.

Pracownicy ds. pomocy technicznej Bitdefender monitorują forum sprawdzając nowe wpisy i zapewniając pomoc. Odpowiedź lub rozwiązanie można także uzyskać od bardziej zaawansowanego użytkownika programu Bitdefender.

Przed zamieszczeniem problemu lub pytania przeszukaj forum w celu znalezienia podobnych lub powiązanych tematów.

Forum pomocy technicznej Bitdefender jest dostępne pod adresem http://forum.bitdefender.com w 5 językach: angielskim, niemieckim, francuskim, hiszpańskim i rumuńskim. Aby uzyskać dostęp do sekcji poświęconej produktom konsumenckim, kliknij łącze **Ochrona w domu & Biurze domowym**.

32.3. Portal HOTforSecurity

Strona HOTforSecurity jest bogatym źródłem informacji na temat bezpieczeństwa komputerowego. Tu możesz dowiedzieć się więcej o różnych zagrożeniach, na które narażony jest komputer połączony z Internetem (złośliwe oprogramowanie, phishing, spam, cyberprzestępcy).

Regularnie zamieszczane są nowe artykuły, dzięki którym będziesz posiadał informacje o najnowszych odkrytych zagrożeniach, bieżących trendach ochrony oraz inne, dotyczące branży bezpieczeństwa komputerowego.

Stroną HOTforSecurity jest http://www.bitdefender.marken.com.pl/.

33. INFORMACJE O PRODUKCIE

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 16 lat BITDEFENDER uzyskał niekwestionowaną reputację dzięki ciągłemu dążeniu do poprawy komunikacji z klientami, aby przewyższyć oczekiwania partnerów oraz klientów. Jeśli miałbyś jakiekolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

33.1. Adresy WWW

Dział sprzedaży: sprzedaz@bitdefender.pl
Centrum pomocy:https://www.bitdefender.pl/kontakt1
Dokumentacja: documentation@bitdefender.com
Lokalni dystrybutorzy:http://bitdefender.pl/partnerzy1
Program partnerski: kontakt@bitdefender.pl
PR: pr@bitdefender.com
Praca: jobs@bitdefender.com
Zgłaszanie wirusa: virus_submission@bitdefender.com
Wysyłanie spamu: spam_submission@bitdefender.com
Zgłoś naruszenie: abuse@bitdefender.com
Strona internetowa:http://www.bitdefender.pl

33.2. Lokalni dystrybutorzy

Lokalni dystrybutorzy Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych.

Wyszukiwanie dystrybutora Bitdefender w danym kraju:

1. Odwiedź http://www.bitdefender.com/partners/partner-locator.html.
2. Wybierz swój kraj i miasto, używając odpowiednich opcji.
3. Jeśli w swoim kraju nie możesz znaleźć dystrybutora Bitdefender, skontaktuj się z nami, wysyłając e-mail na adres sprzedaz@bitdefender.pl. Abyśmy mogli szybko zapewniać pomoc, prosimy o pisanie wiadomości e-mail w języku angielskim.

33.3. Biura Bitdefender

Biura Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych. Ich adresy oraz dane kontaktowe są wypisane poniżej.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefon (biuro i sprzedaż): 1-954-776-6262
Sprzedaż: sales@bitdefender.com
Pomoc Techniczna: https://www.bitdefender.com/support/consumer.html
Internet: https://www.bitdefender.com

Anglia i Irlandia

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Adres e-mail: info@bitdefender.co.uk
Telefon: (+44) 2036 080 456
Sprzedaż: sales@bitdefender.co.uk
Pomoc Techniczna: https://www.bitdefender.co.uk/support/
Internet: https://www.bitdefender.co.uk

Niemcy

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Biura: +49 2304 9 45 - 162
Faks: +49 2304 9 45 - 169
Sprzedaż: vertrieb@bitdefender.de
Pomoc Techniczna: https://www.bitdefender.de/support/consumer.html
Internet: https://www.bitdefender.de

Dania

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Biura: +45 7020 2282
Pomoc Techniczna: http://bitdefender-antivirus.dk/
Internet: http://bitdefender-antivirus.dk/

Hiszpania

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Faks: +34 93 217 91 28
Telefon: +34 902 19 07 65
Sprzedaż: comercial@bitdefender.es
Pomoc Techniczna: https://www.bitdefender.es/support/consumer.html
Strona internetowa: https://www.bitdefender.es

Rumunia

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Faks: +40 21 2641799
Telefon do sprzedaży: +40 21 2063470
E-mail do sprzedaży: sales@bitdefender.ro
Pomoc Techniczna: https://www.bitdefender.ro/support/consumer.html
Strona internetowa: https://www.bitdefender.ro

Zjednoczone Emiraty Arabskie

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefon do sprzedaży: 00971-4-4588935 / 00971-4-4589186
E-mail do sprzedaży: mena-sales@bitdefender.com
Pomoc Techniczna: https://www.bitdefender.com/support/consumer.html
Strona internetowa: https://www.bitdefender.com

Słowniczek

Abonament

Umowa sprzedaży, która daje użytkownikowi prawo do korzystania z określonego produktu lub usługi na konkretnej liczbie urządzeń i przez pewien okres czasu. Subskrypcja, która wygasła może być automatycznie przedłużona na podstawie informacji dostarczonych przez użytkownika przy pierwszym zakupie.

ActiveX

ActiveX jest modelem do pisania programów, tak aby inne programy i systemy operacyjne mogły ich używać. Technologia ActiveX jest wykorzystywana w Microsoft Internet Explorer, aby tworzyć interaktywne strony sieci, które raczej wyglądałyby i zachowywałyby się jak programy komputerowe, niż jak statyczne strony. Z ActiveX użytkownik może zadawać pytania lub na nie odpowiadać, używać przycisków. Może także współpracować w inny sposób ze stronami sieci. Kontrolki ActiveX są często pisane w Visual Basic.

Active X jest znany z kompletnego braku kontroli zabezpieczeń - eksperci do spraw bezpieczeństwa komputerowego nie zalecają korzystać z niego w internecie.

Adware

Adware jest często łączony z aplikacją, która może być używana bezpłatnie tak długo, jak użytkownik zgadza się na adware. Ponieważ aplikacje typu adware są zazwyczaj instalowane po zaakceptowaniu przez użytkownika warunków umowy licencyjnej określającej cele aplikacji, zadanie ochrony przed takim adware nie jest wykonywane.

Jednak reklamy typu pop-up mogą być irytujące, a w niektórych wypadkach mogą obniżyć wydajność systemu. Ponadto informacje zbierane przez niektóre aplikacje tego typu mogą rodzić obawę naruszenia prywatności użytkowników, którzy nie byli w pełni świadomi warunków umowy licencyjnej.

Aktualizacja

Nowa wersja oprogramowania lub sprzętu przeznaczona do zastąpienia starszej wersji tego samego produktu. Dodatkowo standardowe procedury instalacyjne dla aktualizacji często sprawdzają, czy na

komputerze zainstalowana jest starsza wersja produktu. Jeśli nie, nie możesz zainstalować aktualizacji.

Bitdefender posiada własny moduł aktualizacji, który pozwala Ci ręcznie uruchamiać aktualizacje produktu lub przeprowadzać to zadanie automatycznie.

Aplet Java

Program Java, który jest zaprojektowany tak, aby uruchamiał się wyłącznie na stronie internetowej. Aby użyć apletu na stronie internetowej, powinieneś określić nazwę apletu i rozmiar (długość i szerokość w pikselach), których aplet może używać. Po uzyskaniu dostępu do strony internetowej, przeglądarka pobiera aplet z serwera i uruchamia go na urządzeniu użytkownika (na kliencie). Aplety różnią się od aplikacji tym, że zarządza nimi ściśle określony protokół bezpieczeństwa.

Na przykład nawet jeśli aplety działają po stronie klienta, nie mogą odczytywać ani zapisywać danych na maszynie klienta. Dodatkowo, aplety również podlegają późniejszym ograniczeniom, żeby mogły tylko odczytywać i zapisywać dane z tej samej domeny, która je udostępnia.

Archiwum

Dysk, taśma, lub katalog, który zawiera pliki kopii zapasowej.

Plik, który zawiera jeden lub więcej plików w skompresowanym formacie.

Backdoor

Luka w obszarze bezpieczeństwa systemu celowo pozostawiona przez projektantów lub administratorów systemu. Luki nie zawsze są pozostawione w złej wierze. Niektóre systemy operacyjne są dostarczane z kontami uprzywilejowanymi przeznaczonymi do użytku przez serwis techniczny lub opiekunów ds. programowania po stronie sprzedawcy.

Botnet

Słowo "botnet" jest połączeniem słów "robot" oraz "network"(sieć). Botnety to urządzenia połączone z internetem, zainfekowane złośliwym oprogramowaniem, które mogą być wykorzystywane do wysyłania spamu, kradzieży danych, zdalnego sterowania urządzeniami podatnymi na zagrożenia lub rozprzestrzeniania oprogramowania szpiegującego, ransomware i innych rodzajów złośliwego oprogramowania. Ich celem jest zarażanie jak największej liczby podłączonych urządzeń, takich jak

komputery PC, serwery, urządzenia przenośne lub IOT należące do dużych firm lub branż.

Ciasteczka

W przemyśle internetowym ciasteczka (ang. cookies) są określane jako małe pliki zawierające informacje o poszczególnych komputerach, które mogą być analizowane i wykorzystywane przez reklamodawców, aby śledzić online Twoje zainteresowania i gusta. W tej dziedzinie technologia związana z plikami cookie nadal się rozwija, a celem tego jest profilowanie reklam tak, aby były bezpośrednio związane z Twoimi zainteresowaniami. Z jednej strony dla wielu ludzi stanowi to obosieczny miecz: jest efektywne i trwałe, gdyż wyświetlane są tylko reklamy na interesujący Cię temat. Z drugiej strony śledzi każdy Twój ruch oraz kliknięcie. Dlatego są one tematem publicznej dyskusji w kwestii prywatności. Wiele osób czuje się obrażonymi z powodu bycia obserwowanymi jako "Numer SKU" (kod kreskowy na opakowaniu, który jest skanowany przez sklepy przy zakupach). Mimo że ten ten punkt widzenia może się wydawać ekstremalny, w niektórych przypadkach ma swoje uzasadnienie.

E-mail

Poczta elektroniczna. Usługa, która przesyła wiadomości na komputery za pomocą sieci lokalnej lub sieci globalnych.

Elementy startowe

Wszystkie pliki umiejscowione w tym folderze będą uruchomione podczas startu systemu. Elementami startowymi mogą być np. ekran startowy, plik dźwiękowy odtwarzany podczas pierwszego startu komputera, kalendarz lub aplikacje programowe. Normalnie nie sam plik, lecz alias pliku znajduje się w danym folderze.

Fałszywy alarm

Pojawia się, kiedy skaner identyfikuje plik jako zainfekowany, gdy w rzeczywistości nie jest zainfekowany.

Heurystyczny

Oparta na regułach metoda rozpoznawania nowych wirusów. Ta metoda skanowania nie polega na określonych sygnaturach wirusów. Zaletą skanowania heurystycznego jest to, że nie jest ono podatne na zmylenie przez nowy wariant znanych wirusów. Jednakże może czasami zgłaszać

wykrycie podejrzanego kodu w normalnych programach generując tzw. "fałszywe alarmy".

Honeypot

Komputer-wabik ustawiony aby przyciągać hakerów w celu badania sposobu ich działania oraz identyfikacji metod heurystycznych, których używają do zbierania informacji o systemie. Kompanie i korporacje są coraz bardziej zainteresowany wdrożeniem i korzystaniem z honeypotów do zwiększenia ich ogólnego statusu ochrony.

IP

Protokół internetowy – protokół routingu w protokole TCP/IP który jest odpowiedzialny za adresowanie IP, fragmentację oraz ponowne składanie pakietów IP.

Keylogger

Keyloggery to aplikacje, które zapisują wszystkie naciśnięcia klawiszy.

Keyloggery nie są szkodliwe z założenia. Można ich używać dla celów zgodnych z prawem, np. po to, żeby legalnie monitorować aktywność pracowników lub dzieci. Jednak cyberprzestępcy coraz częściej używają ich w celu wyrządzenia szkody (np. do zbierania prywatnych danych, takich jak dane do logowania lub numer ubezpieczenia społecznego).

Klient poczty

Klient e-mail jest aplikacją, która umożliwia Ci wysyłanie i otrzymywanie wiadomości e-mail.

Kod aktywacyjny

Jest unikalnym kluczem, który można kupić w detalu i używać do aktywacji konkretnego produktu lub usługi. Kod aktywacyjny umożliwia aktywację ważnej subskrypcji przez pewien okres czasu oraz dla pewnej ilości urządzeń i może być również wykorzystany do rozszerzenia subskrypcji pod warunkiem, że będzie generowana dla tego samego produktu lub usługi.

Makrowirus

Typ wirusa komputerowego, który jest zakodowany jako makro w danym dokumencie. Wiele aplikacji jak np. Microsoft Word i Excel wspiera makra.

Aplikacje te pozwalają Ci umiejscowić makro w dokumencie i wykonywać je za każdym razem, kiedy dokument jest otwierany.

Napęd dysków

Jest to urządzenie, które czyta i zapisuje dane na dysku.

Twardy dysk czyta i zapisuje dane na twardym dysku.

Stacja dyskietek czyta i zapisuje dane na dyskietce.

Dyski mogą być zarówno wewnętrzne (wewnątrz komputera) jak i zewnętrzne (w oddzielnej obudowie na zewnątrz komputera).

Nieheurystyczny

Ta metoda skanowania opiera się na określonych sygnaturach wirusów. Zaletą skanowania nieheurystycznego jest to, że nie jest ono podatne na wprowadzanie w błąd przez obiekty wydające się być wirusem, a także nie generuje fałszywych alarmów.

Oprogramowanie szpiegujące (spyware)

Każde oprogramowanie, które zbiera dane o użytkowniku podczas połączenia z internetem bez jego wiedzy, zazwyczaj w celach reklamowych. Aplikacje spyware występują zazwyczaj jako ukryte komponenty programów freeware albo shareware, które mogą być pobrane z internetu. Jednakże należy pamiętać że większość aplikacji shareware oraz freeware nie ma w sobie żadnego spyware. Po zainstalowaniu, spyware monitoruje aktywność użytkownika w internecie i przesyła informacje w tle do kogoś innego. Spyware może także zbierać informacje o adresach e-mail, a nawet hasła i numery kart kredytowych.

Spyware jest prostym programem podobnym do konia trojańskiego, którego użytkownicy instalują nieświadomie podczas instalacji innego programu. Pospolitym sposobem by zostać ofiarą spyware jest pobranie niektórych z obecnie dostępnych programów współdzielonych w sieciach typu peer-to-peer.

Abstrahując od kwestii etyki i prywatności, spyware okrada użytkownika używając pamięci komputera i także zużywając przepustowość łącza internetowego podczas wysyłania informacji z powrotem do swojej bazy drogą internetową. Ponieważ spyware zużywa pamięć i zasoby systemowe, aplikacje pracujące w tle mogą powodować zawieszenie się systemu lub jego ogólną niestabilność.

Phishing

Wysyłanie wiadomości e-mail do użytkownika przez osobę podającą się za przedstawiciela uprawnionego do tego przedsiębiorstwa, będące

próbą skłonienia użytkownika do podania informacji poufnych, wykorzystywanych w akcie kradzieży tożsamości. E-mail przekierowuje użytkownika na stronę internetową gdzie jest on proszony o zaktualizowanie informacji osobistych np. haseł, informacji dotyczących kart kredytowych, ubezpieczenia socjalnego i konta bankowego, które uprawniona organizacja już posiada. Strona internetowa jest fałszywa i umieszczona w internecie tylko po to, żeby wykraść informacje o użytkowniku.

Photon

Photon to innowacyjna, nieinwazyjna technologia firmy Bitdefender, zaprojektowana, aby zminimalizować wpływ produktu na wydajność ochrony antywirusowej. Monitorując aktywność Twojego komputera w tle, tworzy wzorce użytkowania, które pomagają zoptymalizować procesy uruchamiania systemu i skanowania.

Plik raportu

Plik, który zapisuje zaistniałe akcje. Bitdefender utrzymuje plik raportu udostępniając skanowaną ścieżkę dostępu, foldery, ilość archiwów i skanowanych plików, ilość zainfekowanych i podejrzanych plików, jakie zostały znalezione.

Pobierz

Aby kopiować dane (zwykle cały plik) z głównego źródła do urządzenia peryferyjnego. Termin ten jest często używany, aby opisać proces kopiowania pliku z usługi online na komputer użytkownika. Pobieranie może także oznaczać kopiowanie pliku z sieciowego serwera plików na komputer podłączony do danej sieci.

Port

Interfejs komputera, do którego podłączasz urządzenie. Komputery osobiste mają różne rodzaje portów. Wewnątrz znajduje się kilka portów dla połączeń dyskowych, podłączania monitorów i klawiatur. Na zewnątrz komputery osobiste mają porty dla połączeń modemowych, drukarek, myszy i innych urządzeń peryferyjnych.

Natomiast w sieciach TCP/IP i UDP jest to punkt końcowy połączenia logicznego. Numer portu pokazuje, jakiego typu jest dany port. Np. port 80 jest używany dla ruchu HTTP.

Przeglądarka

Aplikacja używana do lokalizowania i wyświetlania stron internetowych. Popularne przeglądarki to Microsoft Internet Explorer, Mozilla Firefox i Google Chrome. Są graficznymi przeglądarkami, co oznacza, że mogą pokazywać grafikę oraz tekst. W dodatku większość nowoczesnych przeglądarek może pokazywać informacje multimedialne wraz z dźwiękiem i obrazem video, jednak wymagają one wtyczek dla niektórych formatów.

Ransomware

Ransomware to złośliwy program, który stara się zarobić pieniądze na użytkownikach poprzez zablokowanie ich wrażliwych systemów. CryptoLocker, CryptoWall, i TeslaWall, to tylko niektóre warianty, które polują na prywatne systemy użytkowników.

Infekcja może rozprzestrzeniać się poprzez dostęp do wiadomości spam, pobieranie załączników lub instalowanie aplikacji, nie pozwalając użytkownikowi wiedzieć o tym, co dzieje się w jego systemie. Codziennie użytkownicy i firmy są celem hakerów ransomware.

Robak

Program, który propaguje się przez sieć mnożąc się w czasie poruszania. Nie może się podłączyć do innych programów.

Rootkit

Rootkit jest zestawem narzędzi programowych, który daje dostęp do systemu na poziomie administratora. Termin ten był początkowo używany dla systemów operacyjnych UNIX w odniesieniu do zrekompilowanych narzędzi, które udostępniały intruzom prawa administracyjne, pozwalając im ukryć ich obecność, żeby nie byli widoczni dla administratorów systemu.

Głównym zadaniem rootkitów jest ukrywanie procesów, plików, zdarzeń logowania i raportów. Mogą również przechwytywać dane z terminali, połączeń sieciowych lub urządzeń peryferyjnych, jeśli zawierają odpowiedni rodzaj oprogramowania.

Rootkity nie są zagrożeniem z założenia. Na przykład systemy, a nawet niektóre aplikacje ukrywają krytyczne pliki używając właśnie rootkitów. Jednak często są one używane do ukrywania złośliwego oprogramowania lub intruza w systemie. Gdy są połączone z wirusami, są wielkim zagrożeniem dla spójności działania i bezpieczeństwa systemu. Mogą

monitorować ruch, tworzyć backdoory w systemie, zmieniać pliki i logi oraz unikać wykrycia.

Rozszerzenie pliku

Część nazwy pliku, która wskazuje na rodzaj danych przechowywanych w pliku.

Wiele systemów operacyjnych, np. Unix, VMS, i MS-DOS, używa rozszerzeń nazwy pliku. Zwykle składają się z jednego do trzech znaków (niektóre stare systemy operacyjne akceptują nie więcej niż trzy). Przykłady obejmują "c" jako kod źródłowy C, "ps" jako PostScript, "txt" jako tekst.

Ścieżka

Dokładna lokalizacja pliku na komputerze. Lokalizacja jest zwykle opisywana jako hierarchiczny system porządkowania od góry do dołu.

Droga pomiędzy pewnymi punktami, takimi jak kanały komunikacyjne pomiędzy dwoma komputerami.

Sektor startowy:

Sektor na początku każdego dysku, który rozpoznaje budowę dysku (rozmiar sektora, rozmiar klastra itd.). Sektor rozruchowy zawiera również program uruchamiający system operacyjny.

Skrypt

Inna nazwa dla makra lub pliku wsadowego to skrypt. Skrypt jest listą komend, które mogą być wykonywane bez udziału użytkownika.

Spakowane programy

Plik w formacie skompresowanym. Wiele systemów operacyjnych i aplikacji zawiera polecenia, które umożliwiają spakowanie pliku tak, aby zajmował on mniej miejsca. Np. przypuśćmy, że masz plik tekstowy zawierający 10 kolejnych znaków spacji. Normalnie wymagałoby to 10 bajtów pamięci dla jego przechowania.

Jednakże program pakujący pliki zastępuje spacje specjalnym znakiem serii spacji, po którym następuje liczba spacji, które zostały w ten sposób zastąpione. W tym przypadku plik po spakowaniu będzie potrzebował tylko 2 bajtów miejsca. To tylko jedna z wielu technik pakowania - jest ich o wiele więcej.

Spam

Elektroniczne śmieci lub komentarze grup dyskusyjnych. Ogólnie znane jako niechciane wiadomości e-mail.

Sygnatura wirusa

Wzór binarny wirusa używany przez program antywirusowy, aby wykryć i wyeliminować wirusa.

Szkodliwe oprogramowanie

Program lub fragment kodu, który jest załadowany na Twoim komputerze bez Twojej wiedzy i uruchamia się wbrew Twojej woli. Większość wirusów może się również replikować. Wszystkie wirusy komputerowe są tworzone przez człowieka. Prosty wirus, który umie się skopiować kilka razy jest stosunkowo łatwy do utworzenia. Nawet tak prosty wirus jest niebezpieczny, ponieważ szybko wykorzysta całą dostępną pamięć i przyczyni się do zatrzymania pracy systemu. Bardziej niebezpiecznym typem wirusa jest ten, który jest zdolny przenosić się przez sieci i łamać systemy bezpieczeństwa.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol - Protokół Kontroli Transmisji/Protokół internetowy) – zespół protokołów sieciowych szeroko używanych w internecie, zapewniający komunikację pomiędzy połączonymi sieciami komputerów z różną architekturą sprzętową i różnymi systemami operacyjnymi. TCP/IP zawieraja standardy dotyczące komunikacji komputerów oraz połączeń sieciowych i ruchu.

Trojan

Niszczycielski program, który ukrywa się jako niegroźna aplikacja. W przeciwieństwie do wirusów, Trojany nie powielają się, ale mogą być tak samo szkodliwe. Jednym z najniebezpieczniejszych typów Trojanów jest program zapewniający, że pozbędzie się wirusów z Twojego komputera, a który w rzeczywistości wprowadza wirusy do komputera.

Nazwa pochodzi z powieści Homera "Iliada", w której Grecy podarowali olbrzymiego konia swoim wrogom, Trojanom, pozornie jako znak pokoju. Gdy jednak Trojanie wprowadzili konia do miasta, greccy żołnierze wymknęli się z pustego wnętrza konia i otworzyli bramy miasta pozwalając pozostałym na wejście i podbicie Troi.

Użycie pamięci

Wewnętrzne obszary przechowywania danych na komputerze. Termin pamięć oznacza przechowywanie danych, które pochodzą z chipów, a sformułowanie przechowywanie tekstu jest wykorzystywane w kontekście pamięci taśm i dysków. Każdy komputer posiada wbudowaną pewną ilość pamięci fizycznej zwykle nazywanej pamięcią główną lub RAM.

Wiersz poleceń

W interfejsie linii poleceń użytkownik wpisuje polecenia w przestrzeni znajdującej się na ekranie, używając języka poleceń.

Wirtualna sieć prywatna (VPN)

To technologia, która pozwala na tymczasowe i szyfrowane bezpośrednie połączenie do wybranej sieci w stosunku do mniej zabezpieczonej. Tym sposobem, wysyłane i odbierane dane są zabezpieczone i zaszyfrowane, trudne do zdobycia przez szpicli Autoryzacja może być wykonana tylko za pomocą loginu i hasła.

Wirus polimorficzny

Wirus, który zmienia swoją formę za każdym razem, kiedy zainfekuje kolejny plik. Ponieważ nie mają one stałego wzoru binarnego, są trudne do rozpoznania.

Wirus sektora rozruchowego

Wirus, który infekuje boot sektor dysku stałego lub stację dyskietek. Próba uruchomienia systemu z dyskietki zainfekowanej wirusem tego typu spowoduje, że wirus uaktywni się w pamięci. Od tego momentu za każdym razem, kiedy będziesz uruchamiał system, wirus będzie aktywny w pamięci.

Zaawansowane uporczywe zagrożenie

Zaawansowane uporczywe zagrożenia (APT) wykorzystują słabe punkty systemów do kradzieży ważnych informacji, aby dostarczyć je do źródła. Duże grupy, takie jak, firmy, organizacje lub urzędy, są celem tego złośliwego oprogramowania.

Celem zaawansowanego uporczywego zagrożenia jest pozostanie niewykrytym przez długi czas równocześnie będąc w stanie monitorować i zebrać ważne informacje bez uszkadzania docelowych maszyn. Metoda stosowana w celu wstrzyknięcia wirusa do sieci odbywa się za

pośrednictwem pliku PDF lub dokumentu pakietu Office, który wygląda nieszkodliwe, tak aby każdy użytkownik mógł uruchomić plik.

Zasobnik systemowy

Wprowadzony w systemie Windows 95 zasobnik systemowy znajduje się na pasku zadań Windows (zwykle u dołu obok zegara) i zawiera miniaturowe ikony zapewniające łatwy dostęp do funkcji systemowych, takich jak faks, drukarka, modem, głośność i nie tylko. Aby wyświetlić informacje szczegółowe i sterowniki, kliknij dwukrotnie ikonę lub kliknij ją prawym przyciskiem myszy.

Zdarzenia

Działanie lub wydarzenie wykryte przez program. Zdarzenia mogą być czynnościami użytkownika takimi jak: kliknięcie myszą lub naciśnięcie klawisza albo zdarzeniami systemowymi takimi, jak kończenie się pamięci.