Bitdefender ANTIVIRUS PLUS

PODRĘCZNIK UŻYTKOWNIKA

Bitdefender Antivirus Plus
Podręcznik użytkownika

Data publikacji 07/20/2020

Uwagi prawne

Bitdefender

Spis treści

INSTALACJA

1. PRZYGOTOWANIE DO INSTALACJI

Zanim zainstalujesz Bitdefender Antivirus Plus, wykonaj odpowiednie przygotowania, aby instalacja przebiegała płynnie i bez problemów:

- Upewnij się, że urządzenie, na którym chcesz zainstalować Bitdefender spełnia wymagania systemowe. Jeśli urządzenie nie spełnia wszystkich wymagań systemowych, Bitdefender nie zostanie zainstalowany lub, jeśli zostanie zainstalowany, nie będzie działał poprawnie i spowoduje spowolnienie systemu i niestabilność. Aby zobaczyć pełną listę wymagań systemowych, przejdź do *„Wymagania systemowe”* (p. 3).
- Zaloguj się do urządzenia za pomocą konta administratora.
- Usuń inne podobne oprogramowanie z urządzenia. 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.
- Zaleca się, aby podczas instalacji urządzenie było podłączone do Internetu, nawet 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 Antivirus Plus tylko na urządzeniach z następującymi systemami operacyjnymi:

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

- 2.5 GB wolnego miejsca na dysku twardym (przynajmniej 800 MB na dysku systemowym)
- 2 GB pamięci (RAM)

WAŻNE
Może mieć wpływ na wydajność systemu na urządzeniach z procesorami starszej generacji.

Notatka
Aby znaleźć system operacyjny Windows, na którym działa Twoje urządzenie i informacje o sprzęcie:

- 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. Wymagania programowe

Aby być w stanie używać Bitdefender i wszystkich jego funkcji, Twoje urządzenie musi spełniać następujące wymagania oprogramowania:

- Microsoft Edge 40 lub wyższa
- Internet Explorer 10 lub nowszy

- Mozilla Firefox 51 lub wyższa
- Google Chrome 34 i wyższa

3. INSTALOWANIE PRODUKTU BITDEFENDER

Możesz zainstalować Bitdefender z dysku instalacyjnego lub za pomocą sieciowego instalatora pobranego na urządzenie z Bitdefender Central.

Jeśli zakup obejmuje więcej niż jedno urządzenie (na przykład zakupiony) Bitdefender Antivirus Plus dla 3 PC), powtórz proces instalacji i aktywuj swój produkt za pomocą tego samego konta na każdym urządzeniu. 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 Antivirus Plus jest aktywny.

Aby pobrać Bitdefender Antivirus Plus z Bitdefender Central:

1. Uzyskaj dostęp do Bitdefender Central.
2. W panelu **Moje Urządzenia**, kliknij **ZAINSTALUJ OCHRONĘ**.
3. Wybierz jedną z dwóch dostępnych opcji:

   - **Chroń to urządzenie**

     a. Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.

     b. Zapisz plik instalacyjny.

   - **Chroń inne urządzenia**

     a. Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.

     b. Kliknij **WYŚLIJ PLIK DO POBRANIA**.

     c. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ EMAIL**.

     Miej na uwadze, że wygenerowany link do pobierania jest ważny tylko przez następne 24 godziny. Jeśli link wygaśnie, będziesz musiał wygenerować nowy, wykonując te same kroki.

     d. Na urządzeniu, na którym chcesz zainstalować Bitdefender, sprawdź konto e-mail, które wpisałeś, a następnie naciśnij odpowiedni przycisk pobierania.

4. 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 jakiegokolwiek niekompatybilnego rozwiązania bezpieczeństwa lub starszej wersji Bitdefender zostaniesz poproszony o jego usunięcie z systemu. Postępuj według wskazówek, aby usunąć oprogramowanie z systemu i dzięki temu uniknąć problemów w przyszłości. Konieczne może być ponowne uruchomienie urządzenia, aby dokończyć usuwanie wykrytych rozwiązań bezpieczeństwa.

Pakiet instalacyjny Bitdefender Antivirus Plus 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 Antivirus Plus, wykonaj poniższe kroki.

Krok 1 - instalacja Bitdefender

Przed przystąpieniem do instalacji musisz zgodzić się z umową subskrypcji. Poświęć trochę czasu na przeczytanie Umowy Subskrypcji, ponieważ zawiera ona warunki, w których możesz używać Bitdefender Antivirus Plus.

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

Dwa dodatkowe zadania mogą być wykonane w tym kroku:

- Zachowaj opcję **Wyślij raporty produktu** 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.

Kliknij przycisk **ZAINSTALUJ**, aby rozpocząć proces instalacji produktu Bitdefender.

Krok 2 - Instalacja w toku

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

Krok 3 - Ukończenie instalacji

Twój produkt Bitdefender został pomyślnie zainstalowany.

Wyświetlane jest podsumowanie instalacji. Jeśli w czasie instalacji zostanie wykryte i usunięte jakiekolwiek aktywne zagrożenie, może być konieczne ponowne uruchomienie systemu.

Krok 4 - Analiza Urządzenia

Zostaniesz teraz zapytany, czy chcesz przeprowadzić analizę swojego urządzenia, aby upewnić się, że jest ono bezpieczne. W czasie tego kroku, Bitdefender będzie skanował krytyczne obszary systemu. Kliknij **Rozpocznij Analizę Urządzenia**, aby ją zainicjować.

Możesz ukryć interfejs skanowania, klikając na **Uruchom Skanowanie w Tle**. Następnie wybierz, czy chcesz być informowany o zakończeniu skanowania, czy nie.

Po zakończeniu skanowania kliknij **Otwórz Interfejs Bitdefender**.

Notatka

Alternatywnie, jeśli nie chcesz wykonywać skanowania, możesz po prostu kliknąć na **Pomiń**.

Krok 5 - Rozpocznij

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

Kliknij **Zakończ**, aby uzyskać dostęp do interfejsu Bitdefender Antivirus Plus.

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 jakiegokolwiek niekompatybilnego rozwiązania bezpieczeństwa lub starszej wersji Bitdefender zostaniesz poproszony o jego usunięcie z systemu. Postępuj według wskazówek, aby usunąć oprogramowanie z systemu i dzięki temu uniknąć problemów w przyszłości. Konieczne może być ponowne uruchomienie urządzenia, aby dokończyć usuwanie wykrytych rozwiązań bezpieczeństwa.

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

Po sprawdzeniu poprawności instalacji wyświetlony zostanie kreator konfiguracji. Aby zainstalować Bitdefender Antivirus Plus, wykonaj poniższe kroki.

Krok 1 - Instalacja Bitdefender

Przed przystąpieniem do instalacji musisz zgodzić się z umową subskrypcji. Poświęć trochę czasu na przeczytanie Umowy Subskrypcji, ponieważ zawiera ona warunki, w których możesz używać Bitdefender Antivirus Plus.

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

Dwa dodatkowe zadania mogą być wykonane w tym kroku:

- Zachowaj opcję **Wyślij raporty produktu** 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.

Kliknij przycisk **ZAINSTALUJ**, aby rozpocząć proces instalacji produktu Bitdefender.

Krok 2 - Instalacja w toku

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

Krok 3 - Ukończenie instalacji

Wyświetlane jest podsumowanie instalacji. Jeśli w czasie instalacji zostanie wykryte i usunięte jakiekolwiek aktywne zagrożenie, może być konieczne ponowne uruchomienie systemu.

Krok 4 - Analiza Urządzenia

Zostaniesz teraz zapytany, czy chcesz przeprowadzić analizę swojego urządzenia, aby upewnić się, że jest ono bezpieczne. W czasie tego kroku, Bitdefender będzie skanował krytyczne obszary systemu. Kliknij **Rozpocznij Analizę Urządzenia**, aby ją zainicjować.

Możesz ukryć interfejs skanowania, klikając na **Uruchom Skanowanie w Tle**. Następnie wybierz, czy chcesz być informowany o zakończeniu skanowania, czy nie.

Po zakończeniu skanowania kliknij **Kontynuuj z Utwórz konto**.

Notatka
Alternatywnie, jeśli nie chcesz wykonywać skanowania, możesz po prostu kliknąć na **Pomiń**.

Krok 5 - konto Bitdefender

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. 30).

Postępuj zgodnie z zaistniałą sytuacją.

- **Chcę utworzyć konto Bitdefender**

  1. W odpowiednich polach wprowadź wymagane informacje. Wprowadzone dane pozostaną poufne. Hasło musi mieć co najmniej 8 znaków, zawierać co najmniej jedną cyfrę lub symbol i zawierać małe i wielkie litery.
  2. Zanim przejdziesz dalej, musisz zgodzić się z Warunkami użytkowania. Uzyskaj dostęp do warunków użytkowania i przeczytaj je uważnie, ponieważ zawierają one warunki korzystania z Bitdefender.

     Dodatkowo możesz uzyskać dostęp i przeczytać Politykę Prywatności.
  3. Kliknij **UTWÓRZ KONTO**.

     Notatka
     Kiedy konto zostanie utworzone, możesz użyć dostarczonego adresu email i hasła, aby zalogować się do swojego konta https://central.bitdefender.com bądź też do konta Bitdefender Central dostarczonego przez aplikację, która jest zainstalowana na jednym z Twoich urządzeń z Android bądź iOS. Aby zainstalować aplikację Bitdefender Central na Androidzie, musisz uzyskać dostęp do Google Play, poszukać Bitdefender Central, a następnie wybrać odpowiednią opcję instalacji. Aby zainstalować aplikację Bitdefender Central na iOS, musisz uzyskać dostęp do AppStore, poszukać Bitdefender Central, a następnie wybrać odpowiednią opcję instalacji.

- **Już posiadam konto Bitdefender**

  1. Kliknij **Zaloguj się**.
  2. W odpowiednim polu wpisz adres e-mail, a następnie kliknij **DALEJ**.

3. Wprowadź hasło i kliknij **ZALOGUJ SIĘ**.

   Jeśli zapomniałeś hasła do swojego konta lub chcesz zresetować to, które już ustawiłeś:

   a. Kliknij **Zapomniałeś hasła?**

   b. Wprowadź swój adres e-mail, następnie kliknij **DALEJ**.

   c. Sprawdź swoje konto e-mail, wpisz otrzymany kod bezpieczeństwa, a następnie kliknij **DALEJ**.

      Możesz też kliknąć **Zmień hasło** w e-mailu, który Ci wysłaliśmy.

   d. Wpisz nowe hasło, które chcesz ustawić, a następnie wpisz je ponownie. Kliknij **ZAPISZ**.

> **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 6 - 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 7 - Rozpocznij

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

Kliknij **Zakończ**, aby uzyskać dostęp do interfejsu Bitdefender Antivirus Plus.

PIERWSZE KROKI

4. PODSTAWY

Po zainstalowaniu Bitdefender Antivirus Plus Twoje urządzenie jest chronione przede wszystkimi rodzajami zagrożeń (tj. malware, ransomware, exploitami, botnetami, oprogramowaniem szpiegującym i trojanami).

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.

Podłączenie do publicznych sieci bezprzewodowych na lotniskach, w centrach handlowych, kawiarniach lub hotelach bez zabezpieczenia, może być niebezpieczne dla Twojego urządzenia i Twoich danych. Dzieje się tak głównie dlatego, że oszuści mogą śledzić Twoją aktywność i znaleźć najlepszy moment na kradzież danych osobowych, ale także dlatego, że każdy może zobaczyć Twój adres IP, a tym samym uczynić Twój komputer ofiarą przyszłych cyberataków. Aby uniknąć takich sytuacji, zainstaluj i użyj aplikacji *„VPN"* (p. 121).

Możesz zarządzać swoimi hasłami i kontami online poprzez przechowywanie ich w *„Ochrona Manager Haseł dla Twoich poświadczeń"* (p. 111) w portfelu. Z jednym głównym hasłem możesz chronić swoją prywatność przed intruzami, którzy mogą próbować pozbawić cię pieniędzy.

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. 104).

Pliki zaszyfrowane przez ransomware mogą już być odzyskane bez konieczności wydania pieniędzy żaden żądany okup. Aby uzyskać informację, jak odzyskać zaszyfrowane pliki, skieruj się na *„Naprawa Ransomware"* (p. 108).

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. 131).

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. 16).

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 urządzenie i swoje dane.

Aby korzystać z funkcji internetowych Bitdefender Antivirus Plus i zarządzać swoimi subskrypcjami i urządzeniami, wejdź do swojego konta Bitdefender. Aby uzyskać więcej informacji, odwołaj się do *„Bitdefender Central"* (p. 30).

W sekcji „Jak to zrobić?" (p. 43) znajdziesz instrukcje krok po kroku dotyczące wykonywania typowych zadań. W przypadku wystąpienia problemów podczas korzystania z Bitdefender, sprawdź sekcję *„Rozwiązywanie typowych problemów"* (p. 140) w poszukiwaniu rozwiązań najczęstszych problemów.

4.1. Otwieranie okna Bitdefender

Aby uzyskać dostęp do głównego interfejsu Bitdefender Antivirus Plus, kliknij ikonę na pulpicie.

W razie potrzeby możesz również wykonać następujące czynności:

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

  Na ekranie menu Start systemu Windows zlokalizuj Bitdefender (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 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 w zasobniku systemowym.

Więcej informacji o oknie programu i ikonie Bitdefender w zasobniku systemowym znajdziesz w *„Interfejs produktu Bitdefender”* (p. 20).

4.2. Powiadomienia

Bitdefender prowadzi szczegółowy rejestr zdarzeń dotyczących jego aktywności na Twoim urządzeniu. 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 urządzeniu znaleziono zagrożeń lub luk w zabezpieczeniach itp. Ponadto, możesz podjąć dalsze działania lub zmienić działania podejmowane przez produkt Bitdefender.

Aby uzyskać dostęp do logu Powiadomień, kliknij **Powiadomienia** w menu nawigacji w interfejsie 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.

4.3. 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.

4.3.1. 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.

Podczas pierwszego dostępu do **Profili** zostaniesz poproszony o aktywację automatycznych profili. Aby to zrobić, możesz kliknąć **WŁĄCZ** w wyświetlonym oknie.

Możesz kliknąć **NIE TERAZ** jeśli chcesz później włączyć tę funkcję.

Aby zezwolić Bitdefender na automatyczną aktywację profili:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
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. Spośród pierwszych trzech profili tylko jeden może zostać manualnie aktywowany w danym momencie,

Aby uzyskać więcej informacji na temat Profili, odwołaj się do„*Tryby*" (p. 131)

4.4. Ustawienia ochrony hasłem Bitdefender

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

Aby skonfigurować ochronę hasłem dla ustawień Bitdefender:

1. Kliknij **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. W oknie **General** włącz **Ochronę hasłem**.
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 **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. W oknie **General** wyłącz **Ochronę hasłem**.
3. Wprowadź hasło i kliknij **OK**.

Notatka

Aby zmodyfikować hasło dla produktu, kliknij **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.

4.5. Raporty o produktach

Raporty produktu zawierają informacje o tym, jak używasz Bitdefender który zainstalowałeś. Informacje te są konieczne do ulepszenia produktu. Pomogą nam zapewnić Ci wygodniejszą jego obsługę w przyszłości.

Miej na uwadze, iż raporty te nie będą zawierały żadnych prywatnych danych, takich jak Twoja nazwa użytkownika, czy adres IP. Dodatkowo, raporty nigdy nie zostaną wykorzystane do celów komercyjnych.

Jeżeli podczas instalacji wybrałeś wysyłanie tego rodzaju raportów na serwery Bitdefender a teraz chciałbyś zatrzymać ten proces:

1. Kliknij **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Zaawansowane**.
3. Wyłącz **Raporty produktu**.

4.6. 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 **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. W oknie **OGÓLNE** kliknij odpowiedni przełącznik WŁĄCZ lub WYŁĄCZ.

Powiadomienia o specjalnych ofertach są domyślnie włączone.

5. INTERFEJS PRODUKTU BITDEFENDER

Bitdefender Antivirus Plus 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 prawy nawias aby kontynuować bycie prowadzonym, bądź też **Opuść wycieczkę** aby zamknąć kreator.

ikona w zasobniku systemowymBitdefender jest dostępna w dowolnym czasie, nie ma znaczenia, czy chcesz otworzyć okno główne, uruchomić aktualizację produktu, bądź też zobaczyć informacje na temat zainstalowanej wersji.

Główne okno wyświetla informacje na temat Twojego statusu bezpieczeństwa. Bazując na Twoim użyciu urządzenia i potrzebach, Autopilot wyświetla tam różne typy zaleceń, aby pomóc Ci zwiększyć poziom bezpieczeństwa i wydajność Twojego urządzenia. Ponadto, możesz dodać szybkie akcje, których używasz najczęściej, tak więc możesz mieć je pod ręką kiedy tylko ich potrzebujesz.

Z menu nawigacyjnego po lewej stronie można uzyskać dostęp do obszaru ustawień, powiadomień i Sekcji Bitdefender po szczegółową konfigurację i zaawansowane zadania administracyjne.

Z górnej części głównego interfejsu można uzyskać dostęp do konta Bitdefender. Co więcej, możesz się skontaktować z naszym działem wsparcia w razie, gdybyś miał pytania bądź też zdarzyłoby się coś nieoczekiwanego.

5.1. Ikona zasobnika systemowego

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

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

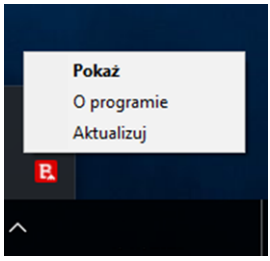
- W systemach **Windows 7, Windows 8 i Windows 8.1**:
  1. Kliknij strzałkę w prawym dolnym rogu ekranu.

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. Kliknij prawym przyciskiem myszy na pasek zadań i wybierz opcję **Ustawienia paska zadań**.
  2. Przewiń w dół i kliknij **Wybierz jakie ikony pojawiają się na pasku zadań** linkuj pod **Strefa powiadomień**.
  3. 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.

- **"Pokaż"** - otwiera główne okno Bitdefender.
- **O** - otwiera okno, gdzie możesz zobaczyć informacje o Bitdefender, gdzie szukać pomocy w razie, gdy zdarzy się coś nieoczekiwanego, gdzie uzyskać dostęp i zobaczyć Umowę Subskrypcji, komponenty od firm zewnętrznych i Politykę Prywatności.
- **"Aktualizuj teraz"** - uruchamia aktualizację. Możesz śledzić stan aktualizacji w panelu Aktualizacji, w głównym oknie Bitdefender.



Tray Icon

Ikona zasobnika systemowego Bitdefender informuje o problemach z urządzeniem lub sposobie działania produktu, wyświetlając specjalny symbol w następujący sposób:

Żadne problemy nie wpływają na bezpieczeństwo twojego systemu.
Krytyczne zagadnienia wpływające na bezpieczeństwo systemu. Wymagają błyskawicznego sprawdzenia oraz jak bezzwłocznej naprawy.

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. Menu nawigacyjne

Po lewej stronie interfejsu Bitdefender znajduje się menu nawigacyjne, które umożliwia szybki dostęp do funkcji Bitdefender i narzędzi potrzebnych do obsługi produktu. Karty dostępne w tym obszarze to:

- **Panel**. Z tego miejsca można szybko rozwiązywać problemy z zabezpieczeniami, przeglądać zalecenia zgodnie z potrzebami i wzorcami użycia Twojego systemu oraz wykonywać szybkie akcje.
-
- **Ochrona**. Stąd możesz uruchomić i skonfigurować skanowanie antywirusowe, odzyskać dane na wypadek ich zaszyfrowania przez oprogramowanie ransomware oraz skonfigurować ochronę podczas surfowania w Internecie.
- **Prywatność**. Stąd możesz tworzyć menedżery haseł do swoich kont online, dokonywać płatności online w bezpiecznym środowisku i otwierać aplikację VPN.
- **Narzędzia**. Stąd możesz zarządzać profilami i uzyskiwać dostęp do funkcji ochrony danych.
- **Powiadomienia**. Z tego miejsca, masz dostęp do generowanych powiadomień.
- **Ustawienia**. Stąd masz dostęp do ustawień ogólnych.

W górnej części głównego interfejsu znajdziesz funkcje **Moje konto** i **Wsparcie**.

- **Wsparcie**. Z tego miejsca, kiedy potrzebujesz pomocy w rozwiązaniu sytuacji z Twoim Bitdefender Antivirus Plus, możesz skontaktować się z Wsparciem Technicznym Bitdefender
- **Moje Konto**. Stąd możesz uzyskać dostęp do swojego konta Bitdefender, aby zweryfikować subskrypcje i wykonać zadania bezpieczeństwa na urządzeniach, którymi zarządzasz. Dostępne są również szczegóły dotyczące konta Bitdefender i wykorzystywanej subskrypcji.

5.3. Pulpit

Okno Panelu pozwala Ci wykonywać standardowe zadania, szybko naprawić problemy związane z bezpieczeństwem, przeglądać informacje o operacjach wykonywanych przez produkt i uzyskać dostęp do paneli, gdzie konfigurowane są ustawienia produktu.

Wystarczy kilka kliknięć.

Okno jest podzielone na trzy główne obszary:

Obszar statusu bezpieczeństwa
: Jest to miejsce, gdzie możesz sprawdzić status bezpieczeństwa Twojego urządzenia.

Autopilot
: Tutaj możesz sprawdzić zalecenia Autopilota, aby zapewnić prawidłowe działanie systemu.

Szybkie działania
: To jest miejsce, gdzie możesz uruchamiać różne zadania, aby chronić swój system.

5.3.1. Obszar statusu bezpieczeństwa

Bitdefender używa systemu śledzenia problemów, aby wykryć i poinformować Cię o zagadnieniach mogących mieć negatywny wpływ na bezpieczeństwo urządzenia i Twoich danych. Wykryte problemy mogą dotyczyć ważnych ustawień ochrony, które są wyłączone oraz innych czynników, które mogą stwarzać zagrożenia bezpieczeństwa.

Ilekroć problemy wpływają na bezpieczeństwo twojego urządzenia, status, który pojawia się w górnej części interfejsu Bitdefender zmienia się na czerwony. Wyświetlany status wskazuje na rodzaj problemów mających wpływ na system. Ikona zasobnika systemowego zmienia się także w a jeśli przesuniesz kursor myszy nad ikoną, okienko pop-up potwierdzi istnienie oczekujących problemów.

Ponieważ wykryte problemy mogą uniemożliwić Bitdefender ochronę przed zagrożeniami lub stanowić poważne zagrożenie bezpieczeństwa, zalecamy zwrócenie uwagi i naprawienie ich tak szybko, jak to tylko możliwe. Aby naprawić problem, kliknij przycisk obok wykrytego problemu.

5.3.2. Autopilot

Aby zapewnić Ci wydajną pracę i zwiększoną ochronę podczas wykonywania różnych czynności, Bitdefender Autopilot będzie działał jako Twój osobisty doradca bezpieczeństwa. W zależności od wykonywanej czynności: pracujesz, dokonujesz płatności online, oglądasz filmy lub grasz w gry Bitdefender Autopilot przedstawi zalecenia kontekstowe bazujące na wykorzystaniu i potrzebach Twojego urządzenia. Proponowane zalecenia mogą również odnosić się do działań, które należy wykonać, aby zapewnić pełne działanie produktu.

Aby rozpocząć korzystanie z sugerowanej funkcji lub ulepszyć produkt, kliknij odpowiedni przycisk.

wyłączanie powiadomień Autopilota

Aby zwrócić Twoją uwagę na zalecenia Autopilota, produkt Bitdefender jest skonfigurowany tak, aby powiadamiał Cię przez okienko pop-up.

Aby wyłączyć powiadomienia Autopilota:

1. Kliknij **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. W oknie **Ogólne** wyłącz **Powiadomienia o zaleceniach**.

5.3.3. Szybkie działania

Używając szybkich działań możesz szybko uruchamiać zadania, które uważasz za istotne dla utrzymania ochrony Twojego systemu i podniesienia standardu Twojej pracy.

Domyślnie Bitdefender zawiera kilka szybkich działań, które można zastąpić tymi, co do których wiesz, że są najbardziej dla Ciebie przydatne. W celu zastąpienia szybkiej akcji:

1. Kliknij ikonę w prawym górnym rogu zakładki, którą chcesz usunąć.
2. Wskaż zadanie, które chcesz dodać do głównego interfejsu, a następnie kliknij przycisk **DODAJ**.

Zadaniami, które możesz dodać do głównego interfejsu są:

- **Szybkie skanowanie**. Uruchom szybkie skanowanie, aby niezwłocznie wykryć potencjalne zagrożenia, które mogą znajdować się na urządzeniu.
- **Skanowanie systemu**. Uruchom skanowanie systemu aby upewnić się, że Twoje urządzenie jest wolne od zagrożeń.

- **Skanowanie luk**. Skanowanie urządzenia w poszukiwaniu luk, aby upewnić się, że wszystkie zainstalowane aplikacje, wraz z Systemem Operacyjnym, są aktualizowane i prawidłowo funkcjonują.
- **Doradca Ochrony Wi-Fi**. Otwórz okno Doradcy ds. Bezpieczeństwa Wi-Fi w module Luki w zabezpieczeniach.
- **Portfele**. Pokaż portfele i zarządzaj nimi.
- **Otwórz Safepay**. Otwórz Bitdefender Safepay™, aby chronić poufne dane podczas przeprowadzania transakcji online.
- **Otwórz VPN**. Otwórz Bitdefender VPN, aby dodać dodatkową warstwę ochrony podczas połączenia z Internetem.
- **Niszczarka Plików**. Uruchom narzędzie Niszczarka Plików aby usunąć ślady danych wrażliwych ze swojego komputera.

Aby zacząć chronić dodatkowe urządzenia przez Bitdefender:

1. Kliknij **Zainstaluj na innym urządzeniu**

   Nowe okno pojawi się na Twoim ekranie.

2. Kliknij **PODZIEL SIĘ LINKIEM DO ŚCIĄGNIĘCIA**.

3. Aby zainstalować Bitdefender wykonaj kroki wyświetlone na ekranie.

W zależności od Twojego wyboru, produkt Bitdefender zostanie zainstalowany:

- Bitdefender Antivirus Plus na urządzeniach opartych na systemie Windows.
- Bitdefender Antivirus dla Mac dla urządzeń opartych na macOS.
- Bitdefender Mobile Security dla urządzeń opartych na Androidzie.
- Bitdefender Mobile Security na urządzeniach opartych na iOS-ie.

5.4. Sekcje Bitdefender

Bitdefender jest wyposażony w kilka przydatnych funkcjonalności, które pomogą Ci pozostać chronionym w trakcie pracy, surfowania po internecie lub gdy chcesz dokonać płatności online, poprawić szybkość systemu i w wielu innych przypadkach.

Gdy tylko chcesz uzyskać dostęp do funkcji dla określonej sekcji lub rozpocząć konfigurację produktu, uzyskaj dostęp do następujących ikon znajdujących się w menu nawigacji w interfejsie Bitdefender:

-  Ochrona

-  Prywatność
-  Narzędzia

5.4.1. Ochrona

W zakładce Ochrona można skonfigurować zaawansowane ustawienia zabezpieczeń, skonfigurować funkcje Bezpieczne pliki i Zapobieganie zagrożeniom online, sprawdzić i naprawić potencjalne luki w systemie oraz ocenić bezpieczeństwo sieci bezprzewodowych, z którymi się łączysz.

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 zagrożeń, czyli malware, trojanami, adware, programami szpiegowskimi itd.

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

- Szybkie Skanowanie
- Skanowanie systemu
- Zarządzanie skanowaniem
- Środowisko Ratunkowe

Więcej informacji o zadaniach skanowania antywirusowego oraz sposobach konfiguracji ochrony antywirusowej znajdziesz w *„Ochrona antywirusowa”* (p. 73).

Zapobieganie Zagrożeniom Online

Zapobieganie Zagrożeniom online pomaga Ci pozostać chronionym przed atakami phishingowymi, próbami oszustw i wyciekami danych prywatnych podczas surfowania po internecie.

Więcej informacji o tym, jak skonfigurować Bitdefender, żeby lepiej chronił Twoją aktywność w sieci, znajduje się tutaj *„Zap. Zagroż. Online”* (p. 97).

AKTYWNA KONTROLA ZAGROŻEŃ

Zaawansowana Ochrona przed Zagrożeniami aktywnie chroni system przed zagrożeniami 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 zagrożeniami, przejdź do *„Zaaw. Ochr. przed Zagroż."* (p. 94).

LUKA

Moduł Skanowania luk, pomaga utrzymać Twój system oraz aplikacje, z których regularnie korzystasz zaktualizowane, a także identyfikuje połączone niezabezpieczone sieci bezprzewodowe. Kliknij **Otwórz** w module Luki w zabezpieczeniach, aby uzyskać dostęp do jego funkcji.

Funkcja **Skanowanie luk** umożliwia identyfikację krytycznych aktualizacji systemu Windows, aktualizacji aplikacji, słabych haseł, należących do kont Windows i niezabezpieczonych sieci bezprzewodowych. Kliknij **Rozpocznij Skanowanie** by wykonać skanowanie urządzenia.

Kliknij **Doradca Ochrony Wi-Fi** aby zobaczyć listę bezprzewodowych sieci z którymi się łączysz, razem z naszą oceną ich reputacji dla każdej z nich i akcji jakie możesz podjąć by zabezpieczyć się przed potencjalnymi szpiegami.

Więcej informacji o konfiguracji ochrony przed lukami znajdziesz w sekcji *„Luki"* (p. 100).

NAPRAWA RANSOMWARE

Cecha działań naprawczych w stosunku do ransomware pomaga Ci w odzyskaniu plików w przypadku, gdy zostały one zaszyfrowane przez ransomware.

Aby uzyskać więcej informacji o odzyskiwaniu zaszyfrowanych plików, zapoznaj się z *„Naprawa Ransomware"* (p. 108).

5.4.2. Prywatność

W sekcji Prywatność możesz otworzyć aplikację Bitdefender VPN i chronić swoje transakcje online i zachować bezpieczne przeglądanie.

Funkcje, którymi możesz zarządzać w sekcji Prywatność to:

VPN

VPN zabezpiecza Twoją aktywność online i ukrywa adres IP za każdym razem, gdy łączysz się z niezabezpieczonymi sieciami bezprzewodowymi na lotniskach, w centrach handlowych, kawiarenkach lub hotelach. Co więcej, możesz mieć dostęp do treści, które są ograniczone w niektórych obszarach.

Więcej informacji o tej funkcji znajdziesz w *„VPN"* (p. 121).

PASSWORD MANAGER

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. 111).

SAFEPAY

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

Więcej informacji na temat modułu Bitdefender Safepay zawiera sekcja *„Bezpieczne płatności online"* (p. 124).

ANTI-TRACKER

Funkcjonalność Anti-tracker pomaga Ci unikać śledzenia, tak więc Twoje dane pozostają prywatne kiedy przeglądasz internet, a czas konieczny na załadowanie poszczególnych stron internetowych zostaje zredukowany.

Aby uzyskać więcej informacji na temat funkcjonalności Anti-tracker sprawdź *„Anti-tracker"* (p. 118).

5.4.3. Narzędzia

Ochrona danych

Niszczarka plików Bitdefender umożliwia trwałe usunięcie danych przez fizyczne usunięcie ich z dysku twardego.

Aby uzyskać więcej informacji, odwołaj się do *„Ochrona danych"* (p. 138).

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.

Więcej informacji o tej funkcji znajdziesz w *„Tryby"* (p. 131).

5.5. Zmień język produktu

Interfejs Bitdefender jest dostępny w kilku językach i można go zmienić, wykonując następujące kroki:

1. Kliknij **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. W oknie **Ogólne** kliknij **Zmień język**.
3. Wybierz żądany język z listy, a następnie kliknij **ZAPISZ**.
4. Poczekaj chwilę, aż ustawienia zostaną zastosowane.

6. BITDEFENDER CENTRAL

Bitdefender Central jest platformą sieciową, gdzie masz dostęp do funkcji i usług online produktu i możesz zdalnie przeprowadzić ważne zadania na urządzeniach, na których jest zainstalowany Bitdefender. Możesz zalogować się do swojego konta Bitdefender z dowolnego urządzenia podłączonego do Internetu, przechodząc do https://central.bitdefender.com lub bezpośrednie z aplikacji Bitdefender Central na urządzeniach z systemami Android i iOS.

Aby zainstalować aplikację Bitdefender Central na swoich urządzeniach:

- **Na Androidzie** - wyszukaj Bitdefender Central w Google Play, a następnie pobierz i zainstaluj aplikację. Wykonaj wymagane kroki, aby zakończyć instalację.
- **Na iOS** - wyszukaj Bitdefender Central w App Store, a następnie pobierz i zainstaluj aplikację. Wykonaj wymagane kroki, aby zakończyć instalację.

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 Antivirus Plus
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security dla systemu Android
  - Bitdefender Mobile Security na systemy iOS
- Zarządzaj i odnów swoją subskrypcję Bitdefender.
- Dodaj nowe urządzenia do sieci i zarządzaj nimi, gdziekolwiek jesteś.

6.1. Uzyskiwanie dostępu do Bitdefender Central

Jest wiele sposobów na uzyskanie dostępu do Bitdefender Central:

- Z głównego interfejsu Bitdefender:
  1. Kliknij **Moje konto** w menu nawigacji w interfejsie Bitdefender.
  2. Kliknij **Idź 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.
- Z urządzenia z systemem Android lub iOS:

  Otwórz zainstalowaną aplikację Bitdefender Central.

Notatka
W tym materiale znajdują się opcje i instrukcje dostępne na platformie internetowej.

6.2. Uwierzytelnienie dwuskładnikowe

Metoda Uwierzytelniania Dwuskładnikowego to dodatkowa warstwa bezpieczeństwa dla konta Bitdefender, wymagająca kodu uwierzytelniającego oprócz danych uwierzytelniających do logowania. W ten sposób zapobiegniesz przejęciu konta i zachowasz ochronę przed atakami cybernetycznymi, takimi jak keyloggery, brute-force czy ataki słownikowe.

Włączanie Uwierzytelnienia Dwuskładnikowego

Włączenie funkcji Uwierzytelnienia dwuskładnikowego znacznie zwiększy bezpieczeństwo konta Bitdefender. Twoja tożsamość będzie weryfikowana przy każdym logowaniu się z różnych urządzeń, w celu zainstalowania produktów Bitdefender, sprawdzenia statusu subskrypcji lub zdalnego wykonywania zadań na Twoich urządzeniach.

Aby włączyć Uwierzytelnienie Dwuskładnikowe:

1. Uzyskaj dostęp do Bitdefender Central.
2. Kliknij ikonę w prawym górnym rogu ekranu.
3. Kliknij **Konto Bitdefender** w rozwijanym menu.
4. Wybierz zakładkę **Hasło i bezpieczeństwo**.
5. Kliknij **Uwierzytelnienie Dwuskładnikowe**.
6. Kliknij **ROZPOCZNIJ**.

Wybierz jedną z następujących metod:

- **Aplikacja Authenticator** - Użyj aplikacji Authenticator, aby wygenerować kod za każdym razem, gdy chcesz zalogować się na swoje konto Bitdefender.

  Jeśli chcesz korzystać z aplikacji uwierzytelniającej, ale nie wiesz, co wybrać, lista z aplikacjami uwierzytelniającymi, które polecamy, jest dostępna.

  a. Aby rozpocząć, kliknij **UŻYJ APLIKACJI AUTHENTICATOR**.

  b. Aby zalogować się na urządzeniu Android lub iOS, użyj urządzenia do zeskanowania kodu QR.

  Aby zalogować się na laptopie lub komputerze, możesz ręcznie dodać wyświetlany kod.

  Kliknij **KONTYNUUJ**.

  c. Wprowadź kod podany przez aplikację lub kod wyświetlony w poprzednim kroku, a następnie kliknij **AKTYWUJ**.

- **E-mail** - za każdym razem, gdy zalogujesz się na swoje konto Bitdefender, na skrzynkę odbiorczą zostanie wysłany kod weryfikacyjny. Sprawdź swoje konto e-mail, a następnie wpisz otrzymany kod.

  a. Kliknij **UŻYJ EMAILA**, aby rozpocząć.

  b. Sprawdź swoje konto e-mail i wpisz otrzymany kod.

  Masz pięć minut, aby sprawdzić swoje konto e-mail i wpisać wygenerowany kod. Jeśli czas upłynie, będziesz musiał wygenerować nowy kod wykonując te same kroki.

  c. Kliknij **AKTYWUJ**.

  d. Masz do dyspozycji dziesięć kodów aktywacyjnych. Możesz skopiować, pobrać lub wydrukować listę i użyć jej w przypadku utraty adresu e-mail lub niemożności zalogowania się. Każdy kod może być użyty tylko raz.

  e. Kliknij **ZROBIONE**.

Jeśli nie chcesz już używać Uwierzytelnienia Dwuskładnikowego:

1. Kliknij **WŁĄCZ UWIERZYTELNIENIE DWUSKŁADNIKOWE**.
2. Sprawdź swoją aplikację lub konto e-mail i wpisz otrzymany kod.

Jeśli zdecydowałeś się na otrzymywanie kodu uwierzytelniającego za pośrednictwem poczty elektronicznej, masz pięć minut na sprawdzenie swojego konta e-mail i wpisanie wygenerowanego kodu. Jeśli czas upłynie, będziesz musiał wygenerować nowy kod wykonując te same kroki.

3. Potwierdź swój wybór.

6.2.1. Dodawanie zaufanych urządzeń

Aby mieć pewność, że tylko Ty masz dostęp do swojego konta Bitdefender, najpierw możemy wymagać kodu bezpieczeństwa. Jeśli chcesz pominąć ten krok przy każdym połączeniu z tego samego urządzenia, zalecamy wyznaczyć je jako urządzenie zaufane.

Aby dodać urządzenia jako zaufane:

1. Uzyskaj dostęp do Bitdefender Central.
2. Kliknij ikonę w prawym górnym rogu ekranu.
3. Kliknij **Konto Bitdefender** w rozwijanym menu.
4. Wybierz zakładkę **Hasło i bezpieczeństwo**.
5. Kliknij **Zaufane Urządzenia**.
6. Zostanie wyświetlona lista urządzeń z zainstalowanym Bitdefender. Kliknij wybrane urządzenie.

Można dodać dowolną liczbę urządzeń, pod warunkiem, że mają one zainstalowany Bitdefender i że subskrypcja jest ważna.

6.3. Moje Subskrypcje

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

6.3.1. 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).

6.3.2. Dodaj nowe urządzenie

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

1. Uzyskaj dostęp do Bitdefender Central.
2. W panelu **Moje Urządzenia**, kliknij **ZAINSTALUJ OCHRONĘ**.
3. Wybierz jedną z dwóch dostępnych opcji:
   - **Chroń to urządzenie**

     Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.
   - **Chroń inne urządzenia**

     Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.

     Kliknij **WYŚLIJ PLIK DO POBRANIA**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ EMAIL**. Miej na uwadze, że wygenerowany link do pobierania jest ważny tylko przez następne 24 godziny. Jeśli link wygaśnie, będziesz musiał wygenerować nowy, wykonując te same kroki.

     Na urządzeniu, na którym chcesz zainstalować Bitdefender, sprawdź konto e-mail, które wpisałeś, a następnie naciśnij odpowiedni przycisk pobierania.
4. Poczekaj na zakończenie pobierania, a następnie uruchomm instalator.

6.3.3. Odnów Subskrypcję

Jeśli wyłączyłeś automatyczne odnawianie się subskrypcji Twojego Bitdefender, możesz manualnie odnowić ją poprzez wykonanie następujących kroków:

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.

6.3.4. 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 **AKTYWUJ**, aby kontynuować.

Subskrypcja jest teraz aktywna. Idź do panelu **Moje Urządzenia** i wybierz **ZAINSTALUJ OCHRONĘ** aby zainstalować produkt na jednym z Twoich urządzeń.

6.4. 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, status ochrony i ryzyka zabezpieczeń mających wpływ na Twoje urządzenie.

Aby wyświetlić listę urządzeń posortowanych według ich statusu lub użytkowników, kliknij strzałkę w prawym górnym rogu ekranu.

Aby łatwo zidentyfikować swoje urządzenie, możesz dostosować nazwę urządzenia:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. Stuknij żądaną kartę urządzenia, a następnie ikonę ⋮ w prawym górnym rogu ekranu.
4. Wybierz **Ustawienia**.
5. Wpisz nową nazwę w polu **Nazwa urządzenia**, a następnie wybierz **ZAPISZ**.

Możesz tworzyć i przypisywac właściciela swoich urządzeń dla lepszego zarządzania:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. Stuknij żądaną kartę urządzenia, a następnie ikonę ⋮ w prawym górnym rogu ekranu.
4. Wybierz **Profil**.
5. Stuknij **Dodaj właściciela**, a następnie wypełnij odpowiednie pola. Dostosuj profil dodając zdjęcie i datę urodzenia.
6. Kliknij **DODAJ**, aby zapisać profil.
7. Wybierz pożądanego właściciela z listy **Własciciel urządzenia**, a następnie kliknij **PRZYPISZ**.

Aby zdalnie zaktualizować Bitdefender na urządzeniu z systemem operacyjnym Windows:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. Stuknij żądaną kartę urządzenia, a następnie ikonę ⋮ w prawym górnym rogu ekranu.
4. Wybierz **Uaktualnij**.

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 zobaczyć szczegóły dotyczące wybranego urządzenia, sprawdzić stan jego zabezpieczeń, status Bitdefender VPN i liczbę zagrożeń, które zostały zablokowane w ciągu ostatnich siedmiu dni. Stan zabezpieczeń może być zielony, gdy nie ma żadnych problemów z urządzeniem, żółty, gdy urządzenie wymaga uwagi, lub czerwony, gdy urządzenie jest zagrożone. W przypadku problemów z urządzeniem kliknij strzałkę w górnym obszarze statusu, aby uzyskać więcej informacji. 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 Sekcja 13.2.3, *„Uruchamianie Skanowania systemu"* oraz do *„Uruchamianie szybkiego skanowania"* (p. 79).
- **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 informacji na temat tej funkcji, należy zapoznać się z *„Luki"* (p. 100).

6.5. Aktywność

W obszarze Aktywność użytkownik ma dostęp do informacji o urządzeniach, na których zainstalowany jest Bitdefender.

Po otwarciu okna **Aktywność** dostępne będą następujące karty:

- **Moje urządzenia**. Tutaj możesz zobaczyć liczbę podłączonych urządzeń wraz ze stanem ich zabezpieczeń. Aby rozwiązać problemy na wykrytych urządzeniach zdalnie, kliknij **Napraw problemy**, a następnie kliknij **PROBLEMY SKANOWANIA I POPRAWEK**.

Aby wyświetlić szczegółowe informacje o wykrytych problemach, kliknij **Wyświetl problemy**.

Informacje o wykrytych zagrożeniach nie mogą zostać pobrane z urządzeń z systemem iOS.

- **Zablokowane zagrożenia**. Tutaj możesz wyświetlić wykres przedstawiający ogólną statystykę, w tym informacje o zagrożeniach zablokowanych w ciągu ostatnich 24 godzin i siedmiu dni. Wyświetlane informacje są pobierane w zależności od złośliwego zachowania wykrytego na dostępnych plikach, aplikacjach i adresach URL.
- **Najbardziej popularni użytkownicy z zablokowanymi zagrożeniami**. Tutaj możesz zobaczyć użytkowników, u których znaleziono największe zagrożenia.
- **Najbardziej popularne urządzenia z zablokowanymi zagrożeniami**. Tutaj możesz zobaczyć urządzenia, na których znaleziono najwięcej zagrożeń.

6.6. 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 zagrożenia są znajdowane i identyfikowane każdego dnia. Właśnie dlatego bardzo ważne jest, aby Bitdefender był na bieżąco aktualizowany w najnowszej bazie danych zagrożeń.

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

Proces aktualizacji wykonywany jest na bieżąco, co oznacza że pliki będą aktualizowane na bieżąco. W ten sposób proces aktualizacji nie będzie miał wpływu na działanie produktu i w tym czasie wszelkie podatności zostaną wykluczone.

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 Twoje urządzenie 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. 66).
- 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. 40).

7.1. Sprawdzanie aktualności produktu Bitdefender

Aby sprawdzić czas ostatniej aktualizacji Twojego Bitdefender:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie 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 rozpocząć aktualizację, kliknij prawym przyciskiem myszy ikonę Bitdefender w zasobniku systemowym a następnie wybierz **Zaktualizuj 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 urządzenie 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 z systemem operacyjnym Windows:

1. Uzyskaj dostęp do Bitdefender Central.
2. Wybierz panel **Moje Urządzenia**.
3. Stuknij żądaną kartę urządzenia, a następnie ikonę w prawym górnym rogu ekranu.
4. Wybierz **Uaktualnij**.

7.3. Włączanie i wyłączanie aktualizacji automatycznych

Aby włączyć lub wyłączyć automatyczne aktualizacje:

1. Kliknij **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Aktualizacja**.
3. Włącz bądź wyłącz odpowiedni przełącznik.

4. Pojawia się okno ostrzegawcze. Musisz potwierdzić swój wybór, określając w menu czas, w którym automatyczna aktualizacja ma być wyłączona. Możesz wyłączyć automatyczne aktualizacje na 5, 15 lub 30 minut, na godzinę lub 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 **Ustawienia** w menu nawigacji w interfejsie 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.

Reguły przetwarzania aktualizacji

Każdorazowo kiedy dostępna jest aktualizacja, Bitdefender automatycznie ściągnie i zaimplementuje aktualizację bez pokazywania powiadomień. Wyłącz opcję**Cichej aktualizacji** jeśli chcesz być informowany za każdym razem, kiedy nowa aktualizacja jest dostępna.

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 urządzenia. Uniemożliwi to procesowi aktualizacji Bitdefender przeszkadzanie w pracy użytkownika.

Jeśli chcesz być pytany gdy aktualizacja wymaga restartu, włącz **Powiadomienie o restarcie**.

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 2020.

JAK TO ZROBIĆ?

8. INSTALACJA

8.1. Jak zainstalować Bitdefender na drugim urządzeniu?

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

Aby zainstalować Bitdefender na drugim urządzeniu:

1. Kliknij **Zainstaluj na innym urządzeniu** w dolnym lewym rogu interfejsu Bitdefender.

   Nowe okno pojawi się na Twoim ekranie.

2. Kliknij **PODZIEL SIĘ LINKIEM DO ŚCIĄGNIĘCIA**.
3. Podążaj za instrukcjami pokazującymi się na ekranie aby zainstalować Bitdefender.

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 Antivirus Plus** i wybierz opcję **Odinstaluj**.
  3. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
  4. Aby zakończyć proces, musisz ponownie uruchomić urządzenie.
- 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 Antivirus Plus** i wybierz opcję **Odinstaluj**.
4. Kliknij **PRZEINSTALUJ** w oknie, które się pojawi.
5. Aby zakończyć proces, musisz ponownie uruchomić urządzenie.

- 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 Antivirus Plus** i wybierz opcję **Odinstaluj**.
4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.
5. Kliknij **PRZEINSTALUJ**.
6. Aby zakończyć proces, musisz ponownie uruchomić urządzenie.

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 urządzenie z platformy Bitdefender Central.

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

Aby zainstalować Bitdefender z Bitdefender Central:

1. Uzyskaj dostęp do Bitdefender Central.

2. W panelu **Moje Urządzenia**, kliknij **ZAINSTALUJ OCHRONĘ**.
3. Wybierz jedną z dwóch dostępnych opcji:
   - **Chroń to urządzenie**

     Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.
   - **Chroń inne urządzenia**

     Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.

     Kliknij **WYŚLIJ PLIK DO POBRANIA**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ EMAIL**. Miej na uwadze, że wygenerowany link do pobierania jest ważny tylko przez następne 24 godziny. Jeśli link wygaśnie, będziesz musiał wygenerować nowy, wykonując te same kroki.

     Na urządzeniu, na którym chcesz zainstalować Bitdefender, sprawdź konto e-mail, które wpisałeś, a następnie naciśnij odpowiedni przycisk pobierania.
4. Uruchom produkt Bitdefender, który pobrałeś.

8.4. Jak mogę zmienić język mojego produktu Bitdefender?

Interfejs Bitdefender jest dostępny w kilku językach i można go zmienić, wykonując następujące kroki:

1. Kliknij **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. W oknie **Ogólne** kliknij **Zmień język**.
3. Wybierz żądany język z listy, a następnie kliknij **ZAPISZ**.
4. Poczekaj chwilę, aż ustawienia zostaną zastosowane.

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 Antivirus Plus** 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 Antivirus Plus** 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 **Aplikacje**.
  3. Wyszukaj **Bitdefender Antivirus Plus** 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. W panelu **Moje Urządzenia**, kliknij **ZAINSTALUJ OCHRONĘ**.
     c. Wybierz jedną z dwóch dostępnych opcji:
        - **Chroń to urządzenie**

          Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.
        - **Chroń inne urządzenia**

Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.

Kliknij **WYŚLIJ PLIK DO POBRANIA**. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ EMAIL**. Miej na uwadze, że wygenerowany link do pobierania jest ważny tylko przez następne 24 godziny. Jeśli link wygaśnie, będziesz musiał wygenerować nowy, wykonując te same kroki.

Na urządzeniu, na którym chcesz zainstalować Bitdefender, sprawdź konto e-mail, które wpisałeś, a następnie naciśnij odpowiedni przycisk pobierania.

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?

Od teraz, ulepszenie do najnowszej wersji jest możliwe bez wykonywania ręcznej dezinstalacji i reinstalacji. 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 2020, 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**. Poczekaj na ponowne uruchomienie urządzenia.

   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. BITDEFENDER CENTRAL

9.1. Jak zalogować się na konto Bitdefender na innym koncie?

Utworzono nowe konto Bitdefender i można już z niego korzystać.

Aby pomyślnie zalogować się na inne konto Bitdefender:

1. Kliknij na swoją nazwę konta w górnej części interfejsu Bitdefender.
2. Kliknij **Zmień konto** w górnym prawym rogu ekranu aby zmienić konto powiązane z urządzeniem.
3. W odpowiednim polu wpisz adres e-mail, a następnie kliknij **DALEJ**.
4. Wprowadź hasło i 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. 161).

9.2. 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. Kliknij **Ustawienia** w rozwijanym menu.
5. Wyłącz informacje pomocnicze **Włącz/Wyłącz wiadomości pomocy**

9.3. 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 **Moje konto** w menu nawigacji w interfejsie Bitdefender.
  2. Kliknij **Zmień konto** w prawym górnym rogu ekranu.

     Pojawi się nowe okno.
  3. Wprowadź swój adres e-mail, następnie kliknij **DALEJ**.

     Pojawi się nowe okno.
  4. Kliknij **Zapomniałeś hasła?**
  5. Kliknij **Dalej**.
  6. Sprawdź swoje konto e-mail, wpisz otrzymany kod bezpieczeństwa, a następnie kliknij **DALEJ**.

     Możesz też kliknąć **Zmień hasło** w e-mailu, który Ci wysłaliśmy.
  7. Wpisz nowe hasło, które chcesz ustawić, a następnie wpisz je ponownie. Kliknij **ZAPISZ**.
- Z Twojej przeglądarki internetowej:
  1. Idź do: https://central.bitdefender.com.
  2. Kliknij **ZALOGUJ SIĘ**.
  3. Wprowadź swój adres e-mail, następnie kliknij **DALEJ**.
  4. Kliknij **Zapomniałeś hasła?**
  5. Kliknij **Dalej**.
  6. 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.

9.4. 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 **Sesje** w rozwijanym menu.
4. W zakładce **Aktywne sesje** wybierz opcję **WYLOGUJ się** obok urządzenia jeśli chcesz zakończyć sesje.

10. SKANOWANIE PRZY POMOCY BITDEFENDER

10.1. 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.
- Skanuj dzielone zasoby sieciowe przed skopiowaniem ich na Twoje urządzenie.

10.2. Jak mogę przeskanować swój system?

Aby wykonać kompletne skanowanie na systemie:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. Kliknij **Uruchom skanowanie** obok **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. 83).

10.3. Jak zaplanować skanowanie?

Możesz ustawić swój produkt Bitdefender tak, aby zaczął skanować ważne lokalizacje systemu, gdy nie jesteś przy urządzeniu.

Aby zaplanować skanowanie:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. Kliknij ••• obok rodzaju skanowania jakie chcesz zaplanować, Skanowanie Systemu lub Szybkie Skanowanie, w dolnej części interfejsu, potem wybierz **Edytuj**.

   Alternatywnie, możesz utworzyć typ skanowania, aby dostosować go do własnych potrzeb klikając **Utwórz nowe zadanie skanowania** obok **Zarządzaj Skanowaniem**.
4. Dostosuj skanowanie do własnych potrzeb, potem kliknij **Dalej**.
5. Zaznacz okno obok **Wybierz kiedy zaplanować te zadanie**.

   Wybierz jedną z odpowiednich opcji, aby ustalić harmonogram:

   - Przy uruchomieniu systemu
   - Codziennie
   - Tygodniowo
   - Miesięcznie

   Jeśli wybierzesz Codziennie, Miesięcznie lub Co tydzień, przeciągnij suwak wzdłuż skali, aby ustawić żądany okres czasu, od którego powinno rozpocząć się zaplanowane skanowanie.

Jeśli zdecydujesz się utworzyć nowe skanowanie niestandardowe, pojawi się okno **Zadanie skanowania**. Z tego miejsca możesz wybrać lokalizacje, które chcesz skanować.

10.4. Jak utworzyć niestandardowe zadanie skanowania?

Jeśli chcesz skanować określone lokalizacje na urządzeniu lub skonfigurować opcje skanowania, skonfiguruj i uruchom niestandardowe zadanie skanowania.

Aby utworzyć niestandardowe zadanie skanowania, wykonaj następujące czynności:

1. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
2. Kliknij **Utwórz Skanowanie** obok **Zarządzaj Skanowanie**.
3. W polu Nazwa zadania wpisz nazwę skanu, a następnie wybierz lokalizacje, które chcesz przeskanować, a następnie kliknij **Dalej**.
4. Skonfiguruj następujące opcje ogólne:
   - **Skanowanie tylko aplikacji**. Możesz ustawić Bitdefender aby skanował tylko użyte przez Ciebie aplikacje.
   - **Priorytet zadania skanowania**. Możesz wybrać wpływ procesu skanowania na wydajność systemu.
     - Auto - Priorytet procesu skanowania zależy od aktywności systemu. Aby upewnić się, że proces skanowania nie wpłynie na aktywność systemu, Bitdefender zdecyduje, czy proces skanowania powinien być uruchamiany z priorytetem wysokim czy niskim.
     - Wysoki - priorytet procesu skanowania będzie wysoki. Wybierając tę opcję, pozwolisz innym programom działać wolniej i skrócić czas potrzebny na zakończenie procesu skanowania.
     - Niski - priorytet procesu skanowania będzie niski. Wybierając tę opcję, pozwolisz innym programom działać szybciej i wydłużyć czas potrzebny do zakończenia procesu skanowania.
   - **Działania po skanowaniu**. Wybierz, jaką akcję powinien podjąć Bitdefender w przypadku braku zagrożeń:
     - Pokaż okno podsumowania
     - Wyłącz urządzenie
     - Zamknij okno skanowania
5. Jeśli chcesz skonfigurować szczegółowe opcje skanowania, kliknij **Pokaż zaawansowane opcje**.

   Kliknij **Dalej**.
6. Możesz włączyć **Zaplanuj zadanie skanowania**, a następnie wybierz, kiedy utworzone skanowanie niestandardowe ma się rozpocząć.
   - Przy uruchomieniu systemu

- Codziennie
- Miesięcznie
- Tygodniowo

Jeśli wybierzesz Codziennie, Miesięcznie lub Co tydzień, przeciągnij suwak wzdłuż skali, aby ustawić żądany okres czasu, od którego powinno rozpocząć się zaplanowane skanowanie.

7. Kliknij **Zapisz**, aby zapisać ustawienia i zamknąć okno konfiguracji.

   W zależności od lokalizacji do przeskanowania, czynność może zająć więcej czasu. Jeśli podczas skanowania zostaną wykryte zagrożenia, zostaniesz poproszony o wybranie działań, które mają zostać podjęte na wykrytych plikach.

Jeśli chcesz, możesz szybko ponownie uruchomić poprzednie własne skanowanie poprzez kliknięcie odpowiedniego wpisu na dostępnej liście.

10.5. Jak można wyłączyć folder ze skanowania?

Bitdefender pozwala na wyłączenie konkretnych plików, folderów bądź rozszerzeń plików ze skanowania.

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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. Kliknij zakładkę **Ustawienia**.
4. Kliknij **Zarządzaj wyjątkami**.
5. Kliknij **+Dodaj Wyjątek**.
6. Wprowadź ścieżkę do folderu, który chcesz pominąć ze skanowania w odpowiednim polu.

Możesz także znaleźć folder klikając przycisk przeglądaj z prawej strony interfejsu, wybierz plik i kliknij **OK**.

7. Włącz przełącznik obok funkcji ochrony, która nie powinna skanować folderu. Dostępne są trzy opcje:
   - Antywirus
   - Zap. Zagroż. Online
   - Zaaw. Ochr. przed Zagroż.
8. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

10.6. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
   b. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
   c. W oknie **Zaawansowane** wyłącz ochronę **Bitdefender**.

      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. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak wyświetlić ukryte obiekty w systemie Windows?”* (p. 68).
3. Odzyskaj plik z sektora kwarantanny:
   a. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
   b. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
   c. Przejdź do **Ustawienia** i kliknij **Zarządzaj kwarantanną**.
   d. Zaznacz plik, a następnie kliknij **Przywróć**.

4. Dodaj plik do listy wykluczeń. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak można wyłączyć folder ze skanowania?”* (p. 57).

   Domyślnie, Bitdefender automatyczne dodaje przywrócone pliki do listy wyjątków.

5. Włącz ochronę antywirusową w czasie rzeczywistym Bitdefender.

6. Skontaktuj się z przedstawicielem pomocy technicznej, żebyśmy mogli usunąć wykrywanie aktualizacji informacji o zagrożeniach. Aby dowiedzieć się, jak to zrobić, sprawdź *„Prośba o pomoc”* (p. 161).

10.7. Jak mogę sprawdzić, jakie zagrożenia 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender

2. W zakładce **Wszystko**, zaznacz powiadomienia dotyczące ostatniego skanowania

   Tutaj znajdziesz wszystkie zdarzenia skanowania w poszukiwaniu obecności zagrożeń, 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**.

11. PRIVACY PROTECTION

11.1. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W okienku **SAFEPAY** kliknij opcję **Ustawienia** .
3. W oknie **Safepay**, kliknij **Uruchom Safepay**.
4. Kliknij przycisk , aby uzyskać dostęp do **klawiatury wirtualnej**.

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

11.2. 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 na Twoim urządzeniu, korzystając z menu kontekstowego Windows i wykonując następujące kroki:

1. Kliknij prawym przyciskiem myszy plik lub katalog, który chcesz trwale usunąć, wskaż Bitdefender i wybierz **Niszczarka plików**.
2. Kliknij **Usuń permanentnie**, a potem potwierdź, że chcesz kontynuować proces.

   Poczekaj, aż Bitdefender zakończy niszczenie plików.

3. Wyniki są wyświetlane. Kliknij "**Zakończ**", aby wyjść z kreatora.

11.3. Jak mogę manualnie odzyskać zaszyfrowane pliki kiedy proces odzyskiwania zawiedzie?

W przypadku gdyby zaszyfrowane pliki nie mogły zostać automatycznie odzyskane, możesz odzyskać je manualnie realizując poniższe kroki:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Na karcie **Wszystkie** wybierz powiadomienie dotyczące wykrytego ostatniego wykrycia zachowania ransomware, a następnie kliknij **Zaszyfrowane pliki**.
3. Lista zawierająca zaszyfrowane pliki jest wyświetlana.

   Kliknij **Odzyskaj Pliki**, aby kontynuować.
4. W przypadku niepowodzenia całego lub części procesu przywracania musisz wybrać lokalizację, w której powinny zostać zapisane odszyfrowane pliki. Kliknij **Lokalizacja odzyskiwania**, a następnie wybierz lokalizację na swoim PC.
5. Pojawia się okno potwierdzające.

   Kliknij **Zakończ** w celu zakończenia procesu odzyskiwania.

Pliki z następującymi rozszerzeniami mogą być odzyskane w razie, gdyby zostały zaszyfrowane:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

12. PRZYDATNE INFORMACJE

12.1. Jak sprawdzić swoje rozwiązanie bezpieczeństwa?

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

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

Aby przetestować swoje rozwiązanie bezpieczeństwa:

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 plik testowy EICAR-Test-File (nie jest on zagrożeniem).

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

   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. 161).

12.2. W jaki sposób usunąć Bitdefender?

Jeśli chcesz usunąć swój Bitdefender Antivirus Plus:

- W systemie **Windows 7**:
  1. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
  2. Wyszukaj **Bitdefender Antivirus Plus** 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 Antivirus Plus** 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 **Aplikacje**.
3. Wyszukaj **Bitdefender Antivirus Plus** 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.

12.3. Jak usunąć Bitdefender VPN?

Procedura usuwania Bitdefender VPN jest podobna do usunięcia innych programów na Twoim urządzeniu.

- W systemie **Windows 7**:

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

2. Wyszukaj **Bitdefender VPN** i wybierz opcję **Odinstaluj**.

   Zaczekaj na zakończenie procesu dezinstalacji.

- 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 VPN** i wybierz opcję **Odinstaluj**.

     Zaczekaj na zakończenie procesu dezinstalacji.

- 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 VPN** i wybierz opcję **Odinstaluj**.
  4. Kliknij **Odinstaluj**, aby potwierdzić swój wybór.

     Zaczekaj na zakończenie procesu dezinstalacji.

12.4. Jak mogę usunąć rozszerzenie Bitdefender Anti-Tracker?

W zależności od używanej przeglądarki internetowej wykonaj następujące kroki, aby odinstalować rozszerzenie Bitdefender Anti-tracker :

- Internet Explorer

  1. Kliknij  obok paska wyszukiwania, a następnie wybierz Zarządzaj dodatkami.

     Pojawi się lista z zainstalowanymi rozszerzeniami.
  2. Kliknij Bitdefender Anti-tracker.
  3. Kliknij **Wyłącz** w prawym dolnym rogu.

- Google Chrome

  1. Kliknij obok paska wyszukiwania.

2. Wybierz **Więcej narzędzi**, a następnie **Rozszerzenia**.

   Pojawi się lista z zainstalowanymi rozszerzeniami.

3. Kliknij **Usuń** na karcie Bitdefender Anti-Tracker.
4. Kliknij **Usuń** w oknie, które się pojawi.

- Mozilla Firefox

1. Kliknij ☰ obok paska wyszukiwania.
2. Wybierz **Dodatki**, a następnie **Rozszerzenia**.

   Pojawi się lista z zainstalowanymi rozszerzeniami.

3. Kliknij ••• i wybierz **Usuń**.

12.5. Jak automatycznie wyłączyć urządzenie po zakończeniu skanowania?

Bitdefender oferuje wiele zadań skanowania, które można wykorzystać, aby upewnić się czy system nie jest zainfekowany zagrożeniem. Wykonanie skanowania całego urządzenia może potrwać dłużej, w zależności od konfiguracji sprzętowej i programowej systemu.

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

Rozważmy następujący przykład: skończyłeś pracę i chcesz iść spać. Chcesz aby Bitdefender sprawdził cały system w poszukiwaniu zagrożeń.

Aby wyłączyć urządzenie po zakończeniu Szybkiego Skanowania lub Skanowania Systemu:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Skany** kliknij ••• obok Szybkiego Skanowania lub Skanowania Systemu i wybierz **Edytuj**.
4. Dostosuj skanowanie do własnych potrzeb, potem kliknij **Dalej**.
5. Kliknij pole obok **Wybierz kiedy zaplanować te zadanie**, potem wybierz kiedy ma się rozpocząć.

Jeśli wybierzesz Codziennie, Miesięcznie lub Co tydzień, przeciągnij suwak wzdłuż skali, aby ustawić żądany okres czasu, od którego powinno rozpocząć się zaplanowane skanowanie.

6. Kliknij **Zapisz**.

Aby wyłączyć urządzenie po zakończeniu skanowania niestandardowego:

1. Kliknij ••• obok utworzonego niestandardowego skanu.
2. Kliknij **Następny** a potem ponownie kliknij **Następny**
3. Kliknij pole obok **Wybierz kiedy zaplanować te zadanie**, potem wybierz kiedy ma się rozpocząć.
4. Kliknij **Zapisz**.

Jeśli zagrożenia nie zostaną odnalezione, urządzenie zostanie wyłączone.

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. 83).

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

Jeśli Twoje urządzenie łączy się z Internetem za pośrednictwem serwera proxy, musisz skonfigurować Bitdefender za pomocą ustawień proxy. 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 **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Zaawansowane**.
3. Włącz **Serwer proxy**
4. Kliknij **Zmień 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.

12.7. 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.

12.8. Jak wyświetlić ukryte obiekty w systemie Windows?

Kroki te są przydatne w tych przypadkach, gdy ma się do czynienia z zagrożeniem 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**.

12.9. 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 urządzeniu uruchomione jest więcej niż jedno rozwiązanie bezpieczeństwa, system staje się niestabilny. Instalator Bitdefender Antivirus Plus 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 **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.

12.10. 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 zagrożenia 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 zagrożeń nie jest aktywna i może być łatwo usunięta.

Uruchamianie systemu Windows w Trybie awaryjnym:

- W systemie **Windows 7**:
  1. Uruchom ponownie urządzenie.
  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

13. OCHRONA ANTYWIRUSOWA

Bitdefender chroni Twoje urządzenie przed wszelkiego rodzaju zagrożeniami (malware, trojanami, spyware, rootkitami itd.). Ochrona Bitdefender jest podzielona na dwie kategorie:

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

  Skanowanie dostępowe zapewnia ochronę przed zagrożeniami, stanowiąc podstawowy komponent każdego programu chroniącego komputer.

  WAŻNE
  Aby zapobiec zainfekowaniu urządzenia przez zagrożenia, zachowaj włączone **Skanowanie dostępowe**.

- Skanowanie dostępowe - pozwala na wykrywanie i usuwanie zagrożeń, które już się znajdują 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 wszystkie nośniki wymienne podłączone do urządzenia, aby zapewnić bezpieczny dostęp do niego. Aby uzyskać więcej informacji, odwołaj się do *„Automatyczne skanowanie wymiennych nośników danych”* (p. 87).

Zaawansowani użytkownicy mogą konfigurować wykluczenia ze skanowania jeśli nie chcą, aby określone pliki bądź typy plików były skanowane. Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie wyjątków skanowania”* (p. 89).

W przypadku wykrycia zagrożenia, 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. 92).

Jeśli Twoje urządzenie zostało zainfekowane zagrożeniami, zapoznaj się z *„Usuwanie zagrożeń z Twojego systemu”* (p. 153). Aby pomóc wyczyścić urządzenie z zagrożeń, których nie można usunąć z systemu operacyjnego Windows, Bitdefender zapewnia Ci*„Środowisko Ratunkowe”* (p. 153). Jest to

zaufane środowisko, zaprojektowane specjalnie do usuwania zagrożeń, które umożliwia uruchomienie urządzenia niezależnie od systemu Windows. Gdy urządzenie działa w Środowisku Ratunkowym, zagrożenia systemu Windows są nieaktywne, co ułatwia ich usunięcie.

13.1. Skanowanie dostępowe (ochrona w czasie rzeczywistym)

Bitdefender zapewnia ochronę w czasie rzeczywistym przed szerokim spektrum zagrożeń przez skanowanie wszystkich plików i wiadomości email, do których uzyskano dostęp.

13.1.1. Włączanie lub wyłączanie ochrony w czasie rzeczywistym

Aby włączyć bądź wyłączyć ochronę przed zagrożeniami w czasie rzeczywistym:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Zaawansowane** włącz bądź wyłącz Ochronę **Bitdefender**.
4. 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 dezaktywowana, nie będziesz chroniony przed zagrożeniami.

13.1.2. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Zaawansowane** możesz skonfigurować ustawienia skanowania, jeśli potrzeba.

Informacje o opcjach skanowania

Ta informacja może być przydatna:

- **Skanowanie tylko aplikacji.** Możesz ustawić Bitdefender aby skanował tylko użyte przez Ciebie aplikacje.
- **Skanuj potencjalnie niechciane aplikacje.** Wybierz tą opcję aby skanować w poszukiwaniu nie chcianych aplikacji. Potencjalnie niechciana aplikacja (PUA) bądź potencjalnie niechciany program (PUP) jest to oprogramowanie, które z reguły jest powiązane z oprogramowaniem freeware i będzie wyświetlać okienka pop-up bądź instalować paski narzędziowe w domyślnej przeglądarce. Niektóre z nich zmieniają stronę startową bądź engine wyszukiwania, inne uruchamiają kilka procesów w tle, zwalniając PC bądź też wyświetlają liczne ogłoszenia. Te programy mogą zostać zainstalowane bez Twojej zgody (nazywane również adware) bądź też będą zawarte domyślnie w instalacji ekspresowej (tzw. ad-supported).
- **Skanuj skrypty.** Funkcja skanuj skrypty umożliwia Bitdefender skanowanie skryptów PowerShell i dokumentów biurowych, które mogą zawierać złośliwe oprogramowanie oparte na skryptach.
- **Skanuj zasoby sieciowe.** Aby uzyskiwać dostęp do odległych sieci z Twojego urządzenia w sposób bezpieczny, zalecamy pozostawianie opcji skanowania udziałów sieciowych jako włączonej.
- **Skanuj archiwa.** 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. Zagrożenie może mieć bezpośredni wpływ na Twój system tylko jeśli zainfekowany plik zostanie wypakowany z archiwum i wykonany, podczas gdy ochrona w czasie rzeczywistym nie jest włączona.

Jeśli zdecydujesz się użyć tej opcji, włącz ją, a następnie przeciągnij suwak wzdłuż skali, aby wykluczyć ze skanowania archiwa dłuższe niż dana wartość w MB (megabajty).

- **Skanowanie sektorów startowych.** Możesz ustawić Bitdefender tak, aby skanował sektory rozruchowe dysku twardego. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu rozruchu. Gdy zagrożenie infekuje sektor rozruchowy, dysk może stać się niedostępny i może nie być możliwe uruchomienie systemu i uzyskanie dostępu do danych.
- **Skanuj tylko nowe i zmodyfikowane pliki.** Skanując tylko nowe lub zmodyfikowane pliki można znacząco poprawić ogólny czas reakcji systemu, bez znaczącego wpływu na bezpiczeństwo.
- **Skanuj w poszukiwaniu keyloggerów (programy rejestrujące wciskane klawisze).** 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.** Wybierz opcje **skan przy rozruchu** aby skanować system przy starcie jak tylko załaduję się wszystkie kluczowe usługi. Zadaniem tej funkcji jest poprawa wykrywania zagrożeń przy starcie systemu i czasu uruchamiania systemu.

Działanie podjęte wobec wykrytych zagrożeń

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

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Zaawansowane** zjedź na dół, aż zobaczysz opcje **Reakcja na Zagrożenia**
4. 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 wykryte jako zainfekowane pasują do informacji o zagrożeniach znajdujących się w Bazie Danych Informacji o zagrożeniach 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. 92).

  WAŻNE

  W przypadku określonych typów zagrożeń, 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 zagrożeń dokonywanej przez analityków Bitdefender. Jeśli obecność zagrożenia zostanie potwierdzona, aktualizacja informacji o zagrożeniach jest udostępniana, aby umożliwić usunięcie zagrożenia.

- **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 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. 92).

Blokuj dostęp
W przypadku wykrycia zainfekowanego pliku dostęp do niego zostanie zablokowany.

13.1.3. Przywracanie ustawień domyślnych

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

Przywracanie domyślnych ustawień ochrony w czasie rzeczywistym:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Zaawansowane** zjedź na dół, aż zobaczysz opcje **Zresetuj zaawansowane ustawienia**. Zaznacz tę opcję, aby zresetować ustawienia antywirusa do ustawień domyślnych.

13.2. Skanowanie na żądanie

Głównym celem dla Bitdefender jest utrzymanie Twojego urządzenia czystego od zagrożeń. Odbywa się to przez trzymanie nowych zagrożeń z dala od urządzenia i przez skanowanie wiadomości e-mail oraz wszelkich nowych plików pobranych lub kopiowanych do systemu.

Istnieje ryzyko, że zagrożenie już umiejscowiło się w systemie, zanim zainstalowałeś Bitdefender. Dlatego też dobrym pomysłem jest przeskanowanie Twojego urządzenia po zainstalowaniu Bitdefender w poszukiwaniu rezydentnych zagrożeń. Ponadto zdecydowanie ważne również jest regularne skanowanie urządzenia pod kątem zagrożeń.

Skanowanie na żądanie oparte jest na zadaniach skanowania. Zadania skanowania określają opcje skanowania i elementy do przeskanowania. Można przeskanować urządzenie w dowolnej chwili, uruchamiając zadania

domyślne albo niestandardowe (zadania zdefiniowane przez użytkownika). Jeśli chcesz przeskanować konkretną lokalizację na swoim urządzeniu lub skonfigurować opcje skanowania, ustaw i uruchom skanowanie niestandardowe.

13.2.1. Skanowanie pliku lub folderu w poszukiwaniu zagrożeń

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.

13.2.2. Uruchamianie szybkiego skanowania

Do wykrywania w systemie zagrożeń 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Skany** kliknij **Uruchom Skanowanie** obok **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.

13.2.3. Uruchamianie Skanowania systemu

Zadanie Skanowania Systemu skanuje całe urządzenie w poszukiwaniu wszystkich rodzajów zagrożeń bezpieczeństwa, takich jak malware, 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 urządzenia.

Zanim uruchomisz Skanowanie systemu, zalecane jest:

- Upewnij się, że Bitdefender jest aktualny w bazie informacji o zagrożeniach. Skanowanie urządzenia w momencie posiadania nieaktualnych informacji o zagrożeniach w bazie danych może spowodować niewykrycie przez Bitdefender nowych zagrożeń, które mogły się pojawić od czasu ostatniej aktualizacji. Aby uzyskać więcej informacji, odwołaj się do *„Dbanie o aktualizacje Bitdefender"* (p. 39).
- Zamknij wszystkie otwarte programy.

Jeśli chcesz przeskanować konkretną lokalizację na swoim urządzeniu lub skonfigurować opcje skanowania, ustaw i uruchom skanowanie niestandardowe. Aby uzyskać więcej informacji, odwołaj się do *„Konfiguracja skanowania niestandardowego"* (p. 80).

Aby uruchomić Skanowanie Systemu:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Skany** kliknij **Uruchom Skanowanie** obok **Skanowanie Systemu**.
4. Przy pierwszym uruchomieniu Skanowania Systemu użytkownik zostaje wprowadzony do tej funkcji. Następnie kliknij **Ok, rozumiem**, aby kontynuować.
5. 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.

13.2.4. Konfiguracja skanowania niestandardowego

W oknie **Zarządzaj skanowaniem** możesz skonfigurować Bitdefender, aby uruchamiał skanowanie, gdy uznasz, że urządzenie wymaga sprawdzenia potencjalnych zagrożeń. Możesz zaplanować Skanowanie systemu lub Szybkie skanowanie lub możesz utworzyć niestandardowe skanowanie według własnych potrzeb.

Aby szczegółowo skonfigurować nowe niestandardowe skanowanie:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Skany** kliknij **Utwórz skanowanie**.
4. W polu **Nazwa zadania** wpisz nazwę skanu, a następnie wybierz lokalizacje, które chcesz przeskanować, a następnie kliknij **Dalej**.
5. Skonfiguruj następujące opcje ogólne:
   - **Skanowanie tylko aplikacji**. Możesz ustawić Bitdefender aby skanował tylko użyte przez Ciebie aplikacje.
   - **Priorytet zadania skanowania**. Możesz wybrać wpływ procesu skanowania na wydajność systemu.
     - Auto - Priorytet procesu skanowania zależy od aktywności systemu. Aby upewnić się, że proces skanowania nie wpłynie na aktywność systemu, Bitdefender zdecyduje, czy proces skanowania powinien być uruchamiany z priorytetem wysokim czy niskim.
     - Wysoki - priorytet procesu skanowania będzie wysoki. Wybierając tę opcję, pozwolisz innym programom działać wolniej i skrócić czas potrzebny na zakończenie procesu skanowania.
     - Niski - priorytet procesu skanowania będzie niski. Wybierając tę opcję, pozwolisz innym programom działać szybciej i wydłużyć czas potrzebny do zakończenia procesu skanowania.
   - **Działania po skanowaniu**. Wybierz, jaką akcję powinien podjąć Bitdefender w przypadku braku zagrożeń:
     - Pokaż okno podsumowania
     - Wyłącz urządzenie
     - Zamknij okno skanowania
6. Jeśli chcesz skonfigurować szczegółowe opcje skanowania, kliknij **Pokaż zaawansowane opcje**. Informacje o wymienionych skanach można znaleźć na końcu tej sekcji.

   Kliknij **Dalej**.
7. Możesz włączyć **Zaplanuj zadanie skanowania**, a następnie wybierz, kiedy utworzone skanowanie niestandardowe ma się rozpocząć.

- Przy uruchomieniu systemu
- Codziennie
- Miesięcznie
- Tygodniowo

Jeśli wybierzesz Codziennie, Miesięcznie lub Co tydzień, przeciągnij suwak wzdłuż skali, aby ustawić żądany okres czasu, od którego powinno rozpocząć się zaplanowane skanowanie.

8. Kliknij **Zapisz**, aby zapisać ustawienia i zamknąć okno konfiguracji.

   W zależności od lokalizacji do przeskanowania, czynność może zająć więcej czasu. Jeśli podczas skanowania zostaną wykryte zagrożenia, zostaniesz poproszony o wybranie działań, które mają zostać podjęte na wykrytych plikach.

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.
- **Skanuj potencjalnie niechciane aplikacje.** Wybierz tą opcję aby skanować w poszukiwaniu nie chcianych aplikacji. Potencjalnie niechciana aplikacja (PUA) bądź potencjalnie niechciany program (PUP) jest to oprogramowanie, które z reguły jest powiązane z oprogramowaniem freeware i będzie wyświetlać okienka pop-up bądź instalować paski narzędziowe w domyślnej przeglądarce. Niektóre z nich zmieniają stronę startową bądź engine wyszukiwania, inne uruchamiają kilka procesów w tle, zwalniając PC bądź też wyświetlają liczne ogłoszenia. Te programy mogą zostać zainstalowane bez Twojej zgody (nazywane również adware) bądź też będą zawarte domyślnie w instalacji ekspresowej (tzw. ad-supported).
- **Skanuj archiwa.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu. Zagrożenie może mieć bezpośredni wpływ na Twój system tylko jeśli zainfekowany plik zostanie wypakowany z archiwum i wykonany, podczas gdy ochrona w czasie rzeczywistym nie jest włączona. Zaleca się jednak użycie tej opcji do wykrywania i usuwania wszelkich potencjalnych zagrożeń, nawet jeśli nie jest to natychmiastowe zagrożenie.

Przeciągnij suwak wzdłuż skali, aby wykluczyć ze skanowania archiwa dłuższe niż dana wartość w MB (megabajty).

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

- **Skanuj tylko nowe i zmodyfikowane pliki.** Skanując tylko nowe lub zmodyfikowane pliki można znacząco poprawić ogólny czas reakcji systemu, bez znaczącego wpływu na bezpieczeństwo.
- **Skanowanie sektorów startowych.** Możesz ustawić Bitdefender tak, aby skanował sektory rozruchowe dysku twardego. Ten sektor dysku twardego zawiera kod, niezbędny do uruchomienia procesu rozruchu. Gdy zagrożenie infekuje sektor rozruchowy, dysk może stać się niedostępny i może nie być możliwe uruchomienie systemu i uzyskanie dostępu do danych.
- **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 tą opcję, aby przeskanować cookies zapisane przez przeglądarkę na Twoim urządzeniu.
- **Skanuj w poszukiwaniu keyloggerów (programy rejestrujące wciskane klawisze).** 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.

13.2.5. 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 wykryte jako zainfekowane pasują do informacji o zagrożeniach znajdujących się w Bazie Danych Informacji o zagrożeniach 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. 92).

  ### WAŻNE

  W przypadku określonych typów zagrożeń, 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 zagrożeń dokonywanej przez

analityków Bitdefender. Jeśli obecność zagrożenia zostanie potwierdzona, aktualizacja informacji o zagrożeniach jest udostępniana, aby umożliwić ich usunięcie.

- **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.

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 zagrożeń znajdziesz w *„Usuwanie zagrożeń z Twojego systemu”* (p. 153).

13.2.6. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Wszystko**, zaznacz powiadomienia dotyczące ostatniego skanowania

   Tutaj znajdziesz wszystkie zdarzenia skanowania w poszukiwaniu obecności zagrożeń, 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"**.

13.3. Automatyczne skanowanie wymiennych nośników danych

Bitdefender automatycznie wykrywa podłączenie wymiennego nośnika danych do urządzenia i skanuje go w tle, gdy opcja Automatycznego Skanowania jest włączona. Jest to zalecane, aby zapobiec zainfekowaniu Twojego urządzenia przez zagrożenia.

Wykryte urządzenia są przyporządkowywane do jednej z tych kategorii:

- CD/DVD
- Napędy flash, takie jak pamięci 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.

13.3.1. Jak to działa?

Kiedy Bitdefender wykryje przenośne urządzenie magazynujące, zaczyna w tle skanować je pod kątem zagrożeń (pod warunkiem, że skanowanie automatyczne jest wyłączone dla takich urządzeń). Wyskakujące okienko powiadomi Cię, że nowe urządzenia zostały wykryte i są skanowane.

Ikona skanowania Bitdefender będzie widoczna w zasobniku systemowym. Możesz kliknąć tą ikonę, aby otworzyć okno skanowania i zobaczyć jego postępy.

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

Z reguły Bitdefender automatycznie usuwa wykryte zagrożenia 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.

Te informacje mogą Ci się przydać:

- Zachowaj ostrożność używając nośników CD/DVD zainfekowanych zagrożeniami, ponieważ nie można ich z nich usunąć (są to nośniki tylko do odczytu). Upewnij się, że ochrona w czasie rzeczywistym jest włączona, aby ochraniać Twój system przed zagrożeniami. Zaleca się skopiowanie ważnych danych z płyty na komputer, a następnie zniszczenie płyty.
- W niektórych przypadkach Bitdefender może nie być w stanie usunąć zagrożeń 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).

Aby dowiedzieć się, jak radzić sobie z zagrożeniami, zapoznaj się z „*Usuwanie zagrożeń z Twojego systemu*" (p. 153).

13.3.2. Zarządzanie skanowaniem wymiennych nośników danych

Aby automatycznie zarządzać skanowaniem wymiennych nośników danych:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. Wybierz zakładkę **Ustawienia**.

Opcje skanowania są skonfigurowane wcześniej tak, aby zapewnić najlepszą wykrywalność. Jeśli zostaną wykryte zainfekowane pliki, Bitdefender spróbuje je oczyścić (usunąć złośliwy 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.

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

13.4. 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 **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Zaawansowane**.
3. Włącz lub wyłącz **Skanuj plik hosta**.

13.5. Konfigurowanie wyjątków skanowania

Bitdefender pozwala na wyłączenie konkretnych plików, folderów bądź rozszerzeń plików ze skanowania. 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 nie są stosowane wykluczenia. Skanowanie kontekstowe jest typem skanowania na żądanie: klikasz prawym przyciskiem myszy na folder, który chcesz skanować i wybierasz **Skanuj z Bitdefender**.

13.5.1. Wykluczanie plików i folderów ze skanowania

Aby wykluczyć określone pliki i foldery ze skanowania:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Ustawienia** kliknij **Zarządzaj Wyjątkami**
4. Kliknij **+Dodaj Wyjątek**.
5. Wprowadź ścieżkę do folderu, który chcesz pominąć ze skanowania w odpowiednim polu.

   Możesz także znaleźć folder klikając przycisk przeglądaj z prawej strony interfejsu, wybierz plik i kliknij **OK**.
6. Włącz przełącznik obok funkcji ochrony, która nie powinna skanować folderu. Dostępne są trzy opcje:
   - Antywirus
   - Zap. Zagroż. Online
   - Zaaw. Ochr. przed Zagroż.
7. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

13.5.2. Wykluczanie rozszerzeń plików ze skanowania

Gdy wykluczasz rozszerzenie pliku ze skanowania, Bitdefender nie będzie już skanować plików z tym rozszerzeniem, niezależnie od ich lokalizacji na twoim urządzeniu. Wykluczenie dotyczy również nośników wymiennych, takich jak płyty CD, DVD, urządzenia magazynujące USB lub dyski sieciowe.

WAŻNE
Zachowaj ostrożność, wyłączając rozszerzenia ze skanowania, ponieważ takie wyjątki mogą narazić urządzenie na zagrożenia.

Aby wykluczyć rozszerzenie plików ze skanowania:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Ustawienia** kliknij **Zarządzaj Wyjątkami**
4. Kliknij **+Dodaj Wyjątek**.
5. Wprowadź rozszerzenia, które mają być wykluczone ze skanowania z kropką przed nimi, oddzielając je średnikami (;).

   txt;avi;jpg
6. Włącz przełącznik obok funkcji ochrony, która nie powinna skanować rozszerzenia.
7. Kliknij **Zapisz**.

13.5.3. Zarządzanie wyjątkami skanowania

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

Aby zarządzać wyjątkami skanowania:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. W oknie **Ustawienia** kliknij **Zarządzaj Wyjątkami** Wyświetlona zostanie lista wszystkich twoich wyjątków.
4. Aby usunąć lub edytować wyjątki skanowania, kliknij jeden z dostępnych przycisków. Wykonaj następujące kroki:

- Aby usunąć wpis z listy, kliknij przycisk obok wpisu
- Aby edytować element z tabeli, kliknij przycisk **Edytuj** obok elementu. Pojawi się nowe okno, w którym możesz zmienić rozszerzenia lub ścieżki dostępowe do wykluczenia i funkcje ochronne, które chcesz wykluczyć, w zależności od potrzeb. Dokonaj zmian, a następnie kliknij "**Zmodyfikuj**".

13.6. Zarządzanie plikami w kwarantannie

Bitdefender izoluje pliki zainfekowane zagrożeniem, których nie może wyleczyć, oraz inne podejrzane pliki w bezpiecznym obszarze, zwanym kwarantanną. Kiedy zagrożenie znajduje się w kwarantannie nie może uczynić żadnej szkody ponieważ nie może być wykonywane lub czytane.

Pliki poddane kwarantannie są domyślnie wysyłane do laboratoriów firmy Bitdefender w celu analizy zagrożeń dokonywanej przez analityków Bitdefender. Jeśli obecność zagrożenia zostanie potwierdzona, aktualizacja informacji o zagrożeniach jest udostępniana, aby umożliwić ich usunięcie.

Ponadto Bitdefender skanuje pliki kwarantanny za każdym razem, gdy baza danych informacji o zagrożeniach jest aktualizowana. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji.

Aby sprawdzać i zarządzać plikami poddanymi kwarantannie:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. Przejdź do okna **Ustawienia**.

   Tutaj możesz zobaczyć nazwę plików z kwarantanny, ich oryginalną lokalizację i nazwę wykrytych zagrożeń.
4. Pliki poddane kwarantannie są automatycznie zarządzane przez Bitdefender zgodnie z domyślnymi ustawieniami kwarantanny.

   Mimo że nie jest to zalecane, możesz dostosować ustawienia kwarantanny zgodnie ze swoimi preferencjami, klikając **Wyświetl Ustawienia**.

   Kliknij przyciski, aby włączyć lub wyłączyć:

   Przeskanuj ponownie kwarantannę po aktualizacji informacji o zagrożeniach

   Włącz tę opcję, aby automatycznie skanować pliki poddane kwarantannie po zaktualizowaniu każdej bazy danych informacji o

zagrożeniach. Wyleczone pliki są automatycznie przenoszone do ich oryginalnej lokalizacji.

Usuń zawartość starszą niż 30 dni
Pliki poddane kwarantannie starsze niż 30 dni są automatycznie usuwane.

Utwórz wykluczenie dla przywróconych plików
Pliki przywrócone z kwarantanny są przenoszone z powrotem do ich pierwotnej lokalizacji bez ich naprawy i automatycznie wykluczane z przyszłych skanów.

5. 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**.

14. ZAAW. OCHR. PRZED ZAGROŻ.

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 urządzeniu w poszukiwaniu aktywności charakterystycznej dla złośliwego oprogramowania. Każde z tych działań jest oceniane, a dla każdego procesu obliczana jest ocena ogólna.

Jako środek bezpieczeństwa będziesz powiadamiany za każdym razem, gdy zagrożenia i potencjalnie szkodliwe procesy zostaną wykryte i zablokowane.

14.1. Włączanie i wyłączanie Aktywnej Kontroli Zagrożeń

Aby włączyć i wyłączyć Aktywną Kontrolę Zagrożeń:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ZAAWANSOWANA OCHRONA PRZED ZAGROŻENIAMI**, kliknij **Otwórz**
3. Przejdź do **Ustawienia** i kliknij przełącznik obok **Zaawansowana Ochrona Przed Zagrożeniami Bitdefender**

> **Notatka**
> Aby chronić system przed oprogramowaniem ransomware i innymi zagrożeniami, zalecamy wyłączanie funkcji Advanced Threat Defense na jak najmniej czasu.

14.2. Sprawdzanie wykrytych złośliwych ataków

Gdy tylko zostaną wykryte zagrożenia lub potencjalnie szkodliwe procesy, Bitdefender zablokuje je, aby zapobiec zainfekowaniu urządzenia przez oprogramowanie ransomware lub inne złośliwe oprogramowanie. W każdej chwili możesz sprawdzić listę wykrytych złośliwych ataków, wykonując następujące kroki:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender

2. W panelu **ZAAWANSOWANA OCHRONA PRZED ZAGROŻENIAMI**, kliknij **Otwórz**
3. Przejdź do okna **Ochrona przed Zagrożeniami**.

   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.

14.3. 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 działań złośliwych.

Aby rozpocząć dodawanie procesów do listy wyjątków Zaawansowanej ochrony przed zagrożeniami:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ZAAWANSOWANA OCHRONA PRZED ZAGROŻENIAMI**, kliknij **Otwórz**
3. W oknie **Ustawienia** kliknij **Zarządzaj Wyjątkami**
4. Kliknij **+Dodaj Wyjątek**.
5. Wprowadź ścieżkę do folderu, który chcesz pominąć ze skanowania w odpowiednim polu.

   Możesz także znaleźć plik wykonywalny klikając przycisk przeglądaj z prawej strony interfejsu, wybierz plik i kliknij **OK**.
6. Włącz przełącznik obok **Zaawansowana Ochrona przed Zagrożeniami**.
7. Kliknij **Zapisz**.

14.4. Wykrywanie exploitów

Sposobem wykorzystywanym przez hakerów do łamania systemów jest wykorzystanie określonych błędów lub luk w zabezpieczeniach oprogramowania komputerowego (aplikacji lub wtyczek) i sprzętu. Aby upewnić się, że twoje urządzenie jest chronione przed takimi atakami, które normalnie rozprzestrzeniają się bardzo szybko, Bitdefender korzysta z najnowszych technologii anty-exploitowych.

Włączanie lub wyłączanie wykrywania exploitów

Aby włączyć lub wyłączyć wykrywanie exploitów.

- Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
- W panelu **ZAAWANSOWANA OCHRONA PRZED ZAGROŻENIAMI**, kliknij **Otwórz**
- Przejdź do **Ustawienia** i kliknij przełącznik obok **Wykrywanie Exploitów** aby włączyć lub wyłączyć tę funkcję.

Notatka

Opcja wykrywania wykorzystania jest domyślnie włączona.

15. ZAP. ZAGROŻ. ONLINE

Bitdefender Zapobieganie Zagrożeniom Online zapewnia bezpieczne korzystanie z witryny, powiadamiając Cię o potencjalnych złośliwych stronach internetowych.

Bitdefender zapewnia zapobieganie zagrożeniom online w czasie rzeczywistym dla:

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

Aby skonfigurować ustawienia zapobiegania zagrożeniom online:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ZAPOBIEGANIE ZAGROŻENIOM ONLINE**, kliknij **Ustawienia**.

W sekcji **Ochrona Sieci** kliknij przełączniki aby ją włączyć lub wyłączyć:

- Ochrona przed atakami sieciowymi blokuje zagrożenia płynące z Internetu, w tym pliki pobierane na dysk.
- 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

- Szyfrowanie skanowanie sieci.

  Bardziej zaawansowany atak może używać zabezpieczonego ruchu sieciowego w celu zmylenia ofiary. Dlatego zalecamy pozostawienie włączonej opcji skanowania zaszyfrowanych stron internetowych.

- Ochrona przed oszustwami.
- Ochrona antyphishingowa.

Przewiń w dół i dojdziesz do sekcji **Ochrona przed zagrożeniami sieci**. Tutaj znajdziesz opcję **Zapobieganie zagrożeniom sieci**. Aby utrzymać urządzenie z dala od ataków złożonego złośliwego oprogramowania (takiego jak ransomware) poprzez wykorzystanie luk w zabezpieczeniach, pozostaw tą opcję włączoną.

Możesz utworzyć listę stron internetowych, domen i adresów IP, które nie będą skanowane przez silniki anti-threat, antiphishing, and antifraud Bitdefender . Lista powinna zawierać tylko strony internetowe, domeny i adresy IP, którym w pełni ufasz.

Aby skonfigurować witryny internetowe, domeny i adresy IP i zarządzać nimi za pomocą funkcji Zapobieganie Zagrożeniom Online udostępnionej przez Bitdefender:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ZAPOBIEGANIE ZAGROŻENIOM ONLINE**, kliknij **Ustawienia**.
3. Kliknij **Zarządzaj wyjątkami**.
4. Kliknij **+Dodaj Wyjątek**.
5. Wpisz w odpowiednie pole nazwę strony internetowej, nazwę domeny lub adres IP, który chcesz dodać do wyjątków.
6. Kliknij przełącznik obok **Zapobieganie Zagrożeniom Online**.
7. Aby usunąć wpis z listy, kliknij przycisk obok wpisu

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

15.1. 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 DO BEZPIECZEŃSTWA**.
- Przejdź do strony internetowej, mimo ostrzeżenia, klikając **Rozumiem ryzyko, zabierz mnie tam mimo wszystko**.
- Jeśli masz pewność, że wykryta witryna jest bezpieczna, kliknij **PRZEŚLIJ**, aby dodać ją do wyjątków. Zalecamy dodawanie tylko stron internetowych, którym w pełni ufasz.

16. LUKI

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

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.

16.1. Skanowanie Twojego komputera w poszukiwaniu luk

Aby wykryć luki w systemie, Bitdefender wymaga aktywnego połączenia z Internetem.

Aby zeskanować system w poszukiwaniu luk:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **Luki**, kliknij **Otwórz**.
3. W zakładce **Skanowanie Luk** kliknij **Rozpocznij Skanowanie**, a potem zaczekaj aż Bitdefender przeskanuje twój system w poszukiwaniu podatności. Wykryte luki są podzielone na trzy kategorie:
   - **SYSTEM OPERACYJNY**
     - **Bezpieczeństwo Systemu Operacyjnego**

       Zmienione ustawienia systemowe mogą narazić twoje urządzenia i dane, takie jak wyświetlanie ostrzeżeń gdy uruchamiane pliki wykonują zmiany w systemie bez twojej zgody lub gdy urządzenia MTP takie jak telefony lub kamery łączą się i wykonują inne operacje bez twojej zgody.

- **Krytyczne aktualizacje Windows**

  Zostanie wyświetlona lista krytycznych aktualizacji systemu Windows, które nie są zainstalowane na komputerze. Może być wymagane ponowne uruchomienie systemu, aby umożliwić Bitdefender zakończenie instalacji. Pamiętaj, że zainstalowanie aktualizacji może chwilę potrwać.

- **Słabe konta systemu Windows**

  Możesz zobaczyć listę użytkowników kont Windows skonfigurowanych na Twoim urządzeniu i poziom ochrony, jaki te hasła zapewniają. Możesz wybrać między poproszeniem użytkownika o zmianę hasła przy następnym logowaniu lub samemu zmienić hasło natychmiast. Aby ustawić nowe hasło do swojego systemu, wybierz **Zmień hasło teraz**.

  Aby hasło było silne, użyj kombinacji dużych i małych liter, cyfr oraz znaków specjalnych (takich jak: #, $ lub @).

- **APLIKACJE**
  - **Ochrona przeglądarki internetowej**

    Zmiana w ustawieniach Twojego urządzenia, która umożliwia wykonywanie plików i programów pobranych przez Internet Explorer bez sprawdzania ich integralności, dlatego ich wykonanie może narazić Twoje urządzenie na niebezpieczeństwo.

  - **Aktualizacje aplikacji**

    Aby zobaczyć informacje o aplikacji, która wymagaja aktualizacji, kliknij jej nazwę na liście.

    Jeśli aplikacja jest nieaktualna, kliknij **Pobierz nową wersję**, aby pobrać najnowszą wersję.

- **SIEĆ**
  - **Sieć i Poświadczenia**

    Zmienione ustawienia systemowe takie jak automatyczne łączenie się z otwartymi hotspotami bez twojej wiedzy lub niewymuszanie szyfrowania na wychodzącym ruchu z bezpiecznego kanału.

  - **Sieci Wi-Fi i routery**

Aby dowiedzieć się więcej o sieci bezprzewodowej i routerze, do którego jesteś podłączony, kliknij jej nazwę na liście. Jeśli zalecane jest ustawienie silniejszego hasła do sieci domowej, upewnij się, że postępujesz zgodnie z naszymi instrukcjami, dzięki czemu możesz pozostać w kontakcie bez obaw o swoją prywatność.

Kiedy zalecenia są dostępne, kieruj się dostępnymi instrukcjami, aby upewnić się, że Twoja sieć domowa pozostaje bezpieczna

16.2. 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 **Narzędzia** w menu nawigacji w interfejsie 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **Luki**, kliknij **Otwórz**.

   ! WAŻNE
   Aby być automatycznie powiadamianym o lukach systemowych i aplikacji, **Automatyczne skanowanie luk** powinno być zawsze włączone.

3. Przejdź do strony **Ustawienia**.
4. Przy użyciu odpowiednich przełączników wybierz luki systemu, które chcesz regularnie sprawdzać.

   Windows updates
   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.

   Hasła Użytkownika
   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 @).

   Autoplay
   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 zagrożeń używają funkcji autoodtwarzania, aby automatycznie rozprzestrzeniać się z wymiennych nośników danych na komputer. Dlatego zaleca się wyłączenie tej opcji systemu Windows.

Doradca 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.

16.3. Doradca Ochrony Wi-Fi

Będąc w trasie, pracując na terenie kawiarni, czekając na lotnisku, łączanie 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 zagrożeniami nieszyfrowanych i niezabezpieczonych publicznych bezprzewodowych hotspotów. Doradca Bezpieczeństwa Wi-Fi Bitdefender analizuje jak chroniona jest sieć, i jeśli to potrzebne zaleca skorzystanie z Bitdefender VPN.

Doradca Wi-Fi Bitdefender daje Ci informacje na temat:

- Domowe sieci Wi-Fi
- Biurowe sieci Wi-Fi
- Publiczne sieci Wi-Fi

16.3.1. Włączanie lub wyłączanie powiadomień Doradcy Ochrony Wi-Fi

Aby włączyć lub wyłączyć powiadomienia Doradcy Ochrony Wi-Fi:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **Luki**, kliknij **Otwórz**.
3. Przejdź do **Ustawienia** i włącz lub włącz **Doradca Ochrony Wi-Fi**.

16.3.2. Konfigurowanie Domowej sieci Wi-Fi

Aby rozpocząć konfigurowanie Twojej sieci domowej:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **Luki**, kliknij **Otwórz**.
3. Przejdź do **Doradca Ochrony Wi-Fi** i kliknij **Domowe 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**.

Aby dodać nową sieć bezprzewodową jako dom, kliknij **Wybierz nowe domowe wi-fi**.

16.3.3. Konfigurowanie Biurowej sieci Wi-Fi

Aby rozpocząć konfigurowanie Twojej sieci biurowej:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **Luki**, kliknij **Otwórz**.
3. Przejdź do **Doradca Ochrony Wi-Fi** i kliknij **Biurowe Wi-Fi**.
4. W zakładce **Biurowe Wi-Fi**, kliknij przycisk **WYBIERZ BIUROWE WI-FI**.

Lista sieci bezprzewodowych, do których łączyłeś się do teraz jest wyświetlana.

5. Wskaż swoją sieć biurową, a następnie kliknij **WYBIERZ**.

Jeżeli sieć biurowa jest uważana za niezabezpieczoną lub niebezpieczną, wyświetlane są porady konfiguracyjnych, aby poprawić jej bezpieczeństwo.

Aby usunąć sieć bezprzewodową, którą ustawiłeś jako sieć biurową, kliknij **USUŃ**.

Aby dodać nową sieć bezprzewodową jako biuro, kliknij **Wybierz nowe biurowe wi-fi**.

16.3.4. Publiczne Wi-Fi

Podczas połączenia z niezabezpieczoną lub niebezpieczną siecią bezprzewodową, profil publiczny Wi-Fi jest włączony. Kiedy pracując na tym profilu Bitdefender Antivirus Plus automatycznie stosuje następujące ustawienia:

- Zaawansowana Ochrona Przed Zagrożeniami jest włączona
- Następujące ustawienia z Zapobiegania Zagrożeniom Online są włączone:
  - Skanowanie szyfrowanej sieci
  - Ochrona przed oszustwami
  - Ochrona przed phishingiem
- Przycisk, który otwiera Bitdefender Safepay™ jest dostępny. W tym przypadku, Ochrona Hotspotu dla niechronionych sieci jest domyślnie włączona.

16.3.5. Sprawdzanie informacji na temat sieci Wi-Fi

Aby sprawdzić informacje o sieciach bezprzewodowych, do których na ogół się łączysz:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **Luki**, kliknij **Otwórz**.
3. Przejdź do okna **Doradca Ochrony Wi-Fi**.
4. W zależności od informacji, których potrzebujesz, wybierz jedną z trzech zakładek, **DOMOWE Wi-Fi**, **BIUROWE 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.

17. NAPRAWA RANSOMWARE

Bitdefender Naprawa Ransomware tworzy kopie zapasowe twoich plików, takich jak dokumenty, zdjęcia, filmy lub muzyka, aby upewnić się, że są chronione przed uszkodzeniem lub utratą w przypadku szyfrowania oprogramowania ransomware. Za każdym razem, gdy zostanie wykryty atak ransomware, Bitdefender zablokuje wszystkie procesy związane z atakiem i rozpocznie proces naprawczy. W ten sposób będzie można odzyskać zawartość wszystkich plików bez płacenia okupu.

17.1. Włączanie lub wyłączanie Ochrony Ransomware

Aby włączyć lub wyłączyć Naprawę Ransomware

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **NAPRAWA RANSOMWARE** włącz lub wyłącz przełącznik.

> **Notatka**
> Aby upewnić się, że twoje pliki są chronione przed ransomware, zalecamy pozostawienie włączonej funkcji Naprawa Ransomware.

17.2. Włączanie lub wyłączanie automatycznego przywracania

Funkcja Automatycznego Przywracania zapewnia automatyczne przywracanie plików w przypadku szyfrowania ransomware.

Włączanie lub wyłączanie automatycznego przywracania:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. w panelu **NAPRAWA RANSOMWARE**, kliknij **Ustawienia**.
3. W oknie Ustawienia włącz lub wyłącz **Automatyczne przywracanie**.

17.3. Wyświetlanie plików, które zostały automatycznie przywrócone

Gdy opcja **Automatyczne przywracanie** jest włączona, Bitdefender automatycznie przywróci pliki zaszyfrowane przez oprogramowanie ransomware. W ten sposób możesz cieszyć się bezproblemową obsługą urządzenia, wiedząc, że pliki są bezpieczne.

Aby wyświetlić pliki, które zostały automatycznie przywrócone:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W karcie **Wszystkie** wybierz powiadomienie dotyczące ostatniego naprawionego zachowania ransomware, a następnie kliknij **Przywrócone Pliki**.

   Wyświetla się lista przywróconych plików. Tutaj możesz również zobaczyć lokalizację, w której pliki zostały przywrócone.

17.4. Ręczne przywracanie zaszyfrowanych plików

Jeśli musisz ręcznie przywrócić pliki zaszyfrowane przez oprogramowanie ransomware, wykonaj następujące kroki:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Na karcie **Wszystkie** wybierz powiadomienie dotyczące wykrytego ostatniego wykrycia zachowania ransomware, a następnie kliknij **Zaszyfrowane pliki**.
3. Lista zawierająca zaszyfrowane pliki jest wyświetlana.

   Kliknij **Odzyskaj Pliki**, aby kontynuować.
4. W przypadku niepowodzenia całego lub części procesu przywracania musisz wybrać lokalizację, w której powinny zostać zapisane odszyfrowane pliki. Kliknij **Lokalizacja odzyskiwania**, a następnie wybierz lokalizację na swoim PC.
5. Pojawia się okno potwierdzające.

   Kliknij **Zakończ** w celu zakończenia procesu odzyskiwania.

Pliki z następującymi rozszerzeniami mogą być odzyskane w razie, gdyby zostały zaszyfrowane:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

17.5. Dodawanie aplikacji do wyjątków

Możesz skonfigurować reguły wyjątków dla zaufanych aplikacji, aby funkcja Ransomware Ransowmare nie blokowała ich, jeśli wykonują akcje podobne do ransomware.

Aby dodać aplikacje do listy wyjątków Naprawy Ransomware:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. w panelu **NAPRAWA RANSOMWARE**, kliknij **Ustawienia**.
3. Przejdź do okna **Wyjątki** i kliknij **+Dodaj Wyjątek**.

18. OCHRONA MANAGER HASEŁ DLA TWOICH POŚWIADCZEŃ

Używamy naszych urządzeń do robienia zakupów online lub płacenia rachunków, łączenia się z platformami społecznościowymi lub logowania się za pomocą aplikacji do komunikacji błyskawicznej.

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

18.1. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. W oknie **Moje Portfele**, kliknij **Dodaj portfel**.
4. Kliknij **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.
   - Podpowiedź - wpisz wskazówkę, aby zapamiętać hasło.
6. Kliknij "**Kontynuuj**".
7. Podczas tego kroku możesz zdecydować się na przechowywanie informacji w chmurze poprzez aktywowanie przełącznika obok **Synchronizuj na wszystkich moich urządzeniach**. Wybierz pożądaną opcję, a następnie kliknij **Kontynuuj**.
8. Wybierz przeglądarkę internetową, z której chcesz zaimportować poświadczenia.
9. Kliknij "**Zakończ**".

18.2. Importuj istniejącą bazę danych

Aby zaimportować bazę danych portfela przechowywaną lokalnie:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. W oknie **Moje Portfele**, kliknij **Dodaj portfel**.
4. Kliknij **Importuj istniejącą bazę danych**.
5. Przejdź do lokalizacji na urządzeniu, w której zapisałeś portfel i go zaznacz.
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**.

18.3. Eksportuj bazę danych Portfela

Aby wyeksportować bazę danych Portfela:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. Przejdź do okna **Moje Portfele**.
4. Kliknij ikonę • • • na wybranym Portfelu, a następnie wybierz **Exportuj**.
5. Przejdź do lokalizacji na urządzeniu w której chcesz zapisać bazę danych portfela a następnie wybierz jej nazwę.
6. Kliknij **Zapisz**.

Notatka
Portfel musi być otwarty, aby opcja **Eksportuj** była dostępna.
Jeśli portfel, który chcesz eksportować jest zamknięty, kliknij **Aktywuj portfel** następnie wpisz hasło, które jest do niego przypisane od początku.

18.4. Synchronizuj swoje portfele w chmurze

Aby włączyć lub wyłączyć synchronizację portfeli w chmurze:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. Przejdź do okna **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 **AKTYWUJ PORTFEL** następnie wpisz hasło, które jest do niego przypisane od początku.

18.5. Zarządzaj danymi logowania Portfela

Aby zarządzać swoimi hasłami:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. Przejdź do okna **Moje Portfele**.
4. Wybierz bazę danych Portfela, a następnie kliknij **Aktywuj portfel**.
5. Wpisz hasło główne, a następnie kliknij **OK**.

Pojawi się nowe okno. W górnej części okna wybierz wymaganą kategorię:

- Tożsamość
- stron 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** znajdujący się z prawej strony.
- Aby usunąć wpis, zaznacz go i kliknij przycisk **Usuń**.

18.6. Włączanie lub wyłączanie ochrony Managera Haseł

Aby włączyć lub wyłączyć ochronę Managera Haseł:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MENEDŻER HASEŁ** włącz lub wyłącz przełącznik.

18.7. Zarządzanie ustawieniami Manager Haseł

Aby skonfigurować szczegółowo hasło główne:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. Przejdź do okna **Ustawienia**.

W sekcji **Ustawienia zabezpieczeń**, dostępne są następujące opcje:

- **Pytaj o moje główne hasło, kiedy zaloguję się na komputerze** - przy próbie dostępu do urządzenia 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.
- **Nie pytaj o moje główne hasło** - przy próbie dostępu do urządzenia, przeglądarki lub aplikacji nie zostanie wyświetlona prośba o podanie głównego hasła.
- **Automatycznie blokuj Portfel, kiedy jestem z dala od urządzenia** - prośba o podanie głównego hasła zostanie wyświetlona po 15-minutowej bezczynności urządzenia.

> **!** 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. Wybierz zakładkę **Ustawienia**.

Włącz przełącznik obok aplikacji aby używać Menedżera Haseł i poprawić swoje doświadczenie:

- 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **MANAGER HASEŁ**, kliknij **Ustawienia**.
3. W oknie **Ustawienia**, zjedź do tabeli **Wypełnij ustawienia automatycznie**.
4. Skonfiguruj następujące opcje:
   - **Skonfiguruj, jak Manager Haseł 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.

19. ANTI-TRACKER

Wiele odwiedzanych witryn używa trackerów do zbierania informacji o swoim zachowaniu, aby udostępniać je firmom zewnętrznym lub wyświetlać reklamy, które są dla Ciebie bardziej odpowiednie. Niniejszym właściciele witryn zarabiają pieniądze, aby móc udostępniać Ci treści za darmo lub kontynuować działalność. Oprócz zbierania informacji, trackery mogą spowalniać przeglądanie lub marnować przepustowość.

Po włączeniu rozszerzenia Bitdefender Anti-tracker w przeglądarce internetowej unikniesz śledzenia, dzięki czemu Twoje dane pozostaną prywatne podczas przeglądania online i przyspieszysz ładowanie stron internetowych.

Rozszerzenie Bitdefender jest zgodne z następującymi przeglądarkami internetowymi:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Wykryte przez nas trackery są pogrupowane w następujące kategorie:

- **Reklamy** - służy do analizowania ruchu w witrynie, zachowania użytkowników lub wzorców ruchu odwiedzających.
- **Interakcja z klientem** - służy do pomiaru interakcji użytkownika z różnymi formularzami wejściowymi, takimi jak czat lub wsparcie.
- **Podstawowe** używane do monitorowania funkcji krytycznych stron internetowych.
- **Analiza Strony** - służy do gromadzenia danych dotyczących korzystania ze stron internetowych.
- **Media Społecznościowe** - służy do monitorowania aktywności i zaangażowania użytkowników na różnych platformach społecznościowych.

19.1. Interfejs Anti-Trackera

Gdy rozszerzenie Bitdefender Anti-Tracker jest aktywne, ikona  pojawia się obok pasek wyszukiwania w przeglądarce internetowej. Za każdym razem, gdy odwiedzasz stronę internetową, na ikonie można zauważyć licznik,

odnoszący się do wykrytych i zablokowanych trackerów. Aby wyświetlić więcej szczegółów o zablokowanych trackerach, kliknij ikonę, aby otworzyć interfejs. Oprócz liczby zablokowanych trackerów możesz wyświetlić czas potrzebny na załadowanie strony i kategorie, do których należą wykryte trackery. Aby wyświetlić listę śledzących witryn, kliknij żądaną kategorię.

Aby wyłączyć blokowanie trackerów witryny, którą aktualnie odwiedzasz przez Bitdefender kliknij **Wstrzymaj ochronę na tej stronie**. To ustawienie ma zastosowanie tylko wtedy, gdy witryna jest otwarta i zostanie przywrócona do stanu początkowego po zamknięciu witryny.

Aby zezwolić trackerom z określonej kategorii na monitorowanie aktywności, kliknij żądaną aktywność, a następnie kliknij odpowiedni przycisk. Jeśli zmienisz zdanie, ponownie kliknij przycisk.

19.2. Wyłączanie Bitdefender Anti-tracker

Aby wyłączyć Bitdefender Anti-tracker

- Z Twojej przeglądarki internetowej:
  1. Otwórz przeglądarkę.
  2. Kliknij ikonę obok paska adresu w przeglądarce internetowej.
  3. Kliknij ikonę w prawym górnym rogu.
  4. Użyj odpowiedniego przełącznika, aby wyłączyć

     Ikona Bitdefender zmieni kolor na szary.
- Z interfejsu Bitdefender:
  1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
  2. W panelu **ANTI-TRACKER** kliknij **Ustawienia**.
  3. Obok przeglądarki internetowej, dla której chcesz wyłączyć rozszerzenie, wyłącz odpowiedni przełącznik.

19.3. Umożliwienie śledzenia witryny

Jeśli chcesz być śledzony podczas odwiedzania określonej witryny, możesz dodać jej adres do wyjątków w następujący sposób:

1. Otwórz przeglądarkę.

2. Kliknij ikonę obok paska wyszukiwania.
3. Kliknij ikonę w prawym górnym rogu.
4. Jeśli jesteś na stronie, którą chcesz dodać do wyjątków, kliknij **Dodaj bieżącą witrynę do listy**.

   Jeśli chcesz dodać inną witrynę, wpisz jej adres w odpowiednim polu, a następnie kliknij

20. VPN

Aplikację VPN można zainstalować z produktu Bitdefender i używać za każdym razem, gdy chcesz dodać dodatkową warstwę ochrony do połączenia. VPN służy jako tunel pomiędzy urządzeniem a siecią, z którą się łączysz - zabezpiecza połączenie, szyfruje dane przy użyciu szyfrowania na poziomie banku i ukrywa twój adres IP gdziekolwiek się znajdujesz. Twój ruch jest przekierowywany przez oddzielny serwer; sprawiając, że Twoje urządzenie jest prawie niemożliwe do zidentyfikowania przez niezliczoną ilość innych urządzeń korzystających z naszych usług. Co więcej, podczas połączenia z Internetem za pośrednictwem sieci VPN Bitdefender, możesz uzyskać dostęp do treści, które są zazwyczaj ograniczone do określonych obszarów.

Notatka

Niektóre kraje stosują cenzurę internetową i dlatego korzystanie z VPN na ich terytorium zostało zakazane przez prawo. Aby uniknąć konsekwencji prawnych, przy próbie pierwszego użycia aplikacji Bitdefender VPN może pojawić się komunikat ostrzegawczy. Kontynuując korzystanie z aplikacji, potwierdzasz, że znasz odpowiednie przepisy obowiązujące w danym kraju i ryzyko, na jakie możesz być narażony.

20.1. Otwieranie VPN

Aby uzyskać dostęp do głównego interfejsu Bitdefender VPN, skorzystaj z jednej z następujących metod:

- Z zasobnika systemowego
  1. Kliknij prawym przyciskiem myszy ikonę na pasku zadań, a następnie kliknij przycisk **Pokaż**.
- Z interfejsu Bitdefender:
  1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
  2. W panelu **VPN** kliknij **Otwórz VPN**.

20.2. Interfejs VPN

Interfejs VPN wyświetla status aplikacji - włączona lub wyłączona. Lokalizacja serwera dla użytkowników z bezpłatną wersją jest automatycznie ustawiana przez Bitdefender na najbardziej odpowiedni serwer, a użytkownicy premium mają możliwość zmiany lokalizacji serwera, z którą chcą się połączyć. Aby

uzyskać więcej informacji na temat subskrypcji [VPN], przejdź do *„Subskrypcje ”* (p. 123).

Aby połączyć lub rozłączyć, wystarczy kliknąć na status wyświetlony u góry ekranu lub kliknąć prawym przyciskiem myszy ikonę zasobnika systemowego. Ikona zasobnika systemowego wyświetla zielony znacznik wyboru po podłączeniu VPN i czerwony znacznik wyboru po odłączeniu VPN.

Podczas połączenia, czas który upłynął, oraz wykorzystanie przepustowości są wyświetlane w dolnej części interfejsu.

Aby zobaczyć w całości obszar **Menu**, kliknij ikonę z górnej lewej strony. Oto dostępne możliwości:

- **Moje konto** - zostaną wyświetlone szczegóły dotyczące Twojego konta Bitdefender i subskrypcji VPN. Kliknij **Zmień konto**, jeśli chcesz się zalogować na inne konto.

  Kliknij **Dodaj tutaj** aby dodać kod aktywacyjny dla Bitdefender Premium VPN

- **Ustawienia** – w zależności od potrzeb, możesz dostosować zachowanie swojego produktu. Ustawienia są podzielone na dwie kategorie:

  - **Ogólne**
    - Powiadomienia
    - Uruchomienie - wybierz czy chcesz uruchomić Bitdefender VPN podczas uruchomienia czy nie
    - Raporty o produktach - wysyła anonimowe raporty o produkcie w celu ulepszenia twojego doświadczenia
    - Ciemny tryb
    - Język
  - **Zaawansowane**
    - Kill-Swtich Internetu - ta funkcja tymczasowo zawiesza cały ruch internetowy jeśli przypadkowo rozłączy się połączenie z VPN. Gdy znowu będziesz online połączenie zostanie przywrócone.
    - Automatyczne połączenie - Automatycznie połącz się z Bitdefender VPN gdy korzystasz z publicznej/niezabezpieczonej sieci Wi-Fi lub gdy jest włączona aplikacja p2p.

- **Wsparcie** - zostajesz przekierowany się do naszej platformy Centrum Wsparcia, gdzie możesz przeczytać pomocny artykuł na temat korzystania z sieci Bitdefender VPN lub podzielić się z nami opinią.
- **O aplikacji** - wyświetlane są informacje o zainstalowanej wersji.

20.3. Subskrypcje

Bitdefender VPN oferuje bezpłatny dzienny przydział 200 MB na urządzenie, aby zabezpieczyć połączenie za każdym razem, gdy jest to potrzebne oraz automatycznie łączy Cię z optymalną lokalizacją serwera.

Aby uzyskać nieograniczony ruch i nieograniczony dostęp do treści na całym świecie dzięki opcji wyboru lokalizacji serwera w dowolnej chwili, uaktualnij ją do wersji premium.

W każdej chwili można zaktualizować do wersji Bitdefender Premium VPN, naciskając przycisk **Aktualizuj**, dostępny w interfejsie produktu.

Subskrypcja Bitdefender Premium VPN jest niezależna od subskrypcji Bitdefender Antivirus Plus, co oznacza, że można z niej korzystać niezależnie od stanu subskrypcji rozwiązania bezpieczeństwa. W przypadku, gdy subskrypcja Bitdefender Premium VPN wygaśnie, a subskrypcja Bitdefender Antivirus Plus jest nadal aktywna, zostaniesz przywrócony bezpłatnego planu.

Bitdefender VPN jest produktem wieloplatformowym, dostępnym w produktach Bitdefender kompatybilnych z systemami Windows, Mac OS, Android i iOS. Po przejściu na plan premium, możliwe będzie korzystanie z subskrypcji na wszystkich produktach, pod warunkiem, że zalogujesz się z tego samego konta Bitdefender.

21. 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. 111).

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 Twoje urządzenie jest podłączone 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.

21.1. Używanie modułu Bitdefender Safepay

Domyślnie, Bitdefender wykrywa przejście do witryny bankowości internetowej lub sklepu internetowego w dowolnej przeglądarce na urządzeniu i monituje o jej uruchomienie za pomocą Bitdefender Safepay™.

Aby uzyskać dostęp do głównego interfejsu modułu Bitdefender Safepay, skorzystaj z jednej z następujących metod:

- Z interfejsu Bitdefender:
  1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
  2. W okienku **SAFEPAY** kliknij opcję **Ustawienia** .
  3. W oknie **Safepay**, kliknij **Uruchom 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.

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 i wybierając **Drukuj**.

Notatka
Aby przełączyć się między Bitdefender Safepay™ i pulpitem Windows, naciśnij klawisze **Alt+Tab** lub kliknij opcję **Przełącz na pulpit** w lewym górnym rogu okna.

21.2. Konfigurowanie ustawień

Kliknij i wybierz **Ustawienia**, aby skonfigurować Bitdefender Safepay™:

Zastosuj reguły Bitdefender Safepay dla domen, do których uzyskiwany jest dostęp

Pojawią się tutaj witryny dodane do Zakładek z włączoną opcją **Automatycznie otwieraj w Safepay**. Jeśli chcesz przestać automatycznie otwierać stronę Bitdefender Safepay™ z listy, kliknij × obok żądanego wpisu w kolumnie **Usuń**.

Blokuj wyskakujące okienka
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.

Manage Plugins
Możesz wybrać czy chcesz włączyć lub wyłączyć wybrane wtyczki w Bitdefender Safepay™.

Zarządzaj certyfikatami
Możesz zaimportować certyfikaty ze swojego systemu do magazynu certyfikatów.

Kliknij **IMPORT** i podążaj za kreatorem, aby użyć certyfikatów w Bitdefender Safepay™.

Użyj Klawiatury Wirtualnej
Klawiatura wirtualna pojawi się automatycznie gdy wybierzesz pole z hasłem.

Użyj odpowiedniego przełącznika, aby włączyć lub wyłączyć funkcję.

Drukowanie potwierdzenia
Włącz tą opcje jeśli chcesz potwierdzać przed rozpoczęciem procesu drukowania.

21.3. 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 ••• i wybierz **Zakładki**, 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".

21.4. Wyłączanie powiadomień Safepay.

Po wykryciu witryny bankowej produkt Bitdefender jest skonfigurowany w taki sposób, aby powiadamiał użytkownika za pomocą wyskakującego okienka.

Żeby wyłączyć powiadomienia Safepay:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W okienku **SAFEPAY** kliknij opcję **Ustawienia** .
3. W oknie **Ustawienia**, wyłącz przełącznik obok **Powiadomienia Safepay**.

21.5. Użycie VPN z Safepay

Aby płatności online odbywały się w bezpiecznym środowisku, będąc podłączonym do niezabezpieczonych sieci, produkt Bitdefender może być skonfigurowany tak, aby automatycznie uruchamiał aplikację VPN w tym samym czasie co program Safepay.

Żeby rozpocząć używanie aplikacji VPN razem z Safepay należy:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W okienku **SAFEPAY** kliknij opcję **Ustawienia** .
3. W oknie **Ustawienia**, włącz przełącznik obok **Użyj VPN z Safepay**.

22. USB IMMUNIZER

Funkcja Autorun wbudowana w systemy operacyjne Windows jest bardzo przydatnym narzędziem, które pozwala urządzeniom na automatyczne wykonanie pliku z podłączonego do niego nośnika. Na przykład instalowanie oprogramowania może być uruchomione automatycznie po włożeniu płyty CD do napędu optycznego.

Niestety, z tej funkcji mogą również korzystać zagrożenia, które automatycznie uruchamiają i infiltrują urządzenie z nośników wielokrotnego zapisu, takich jak dyski flash USB i karty pamięci podłączone za pomocą czytników kart. W ostatnich latach stworzono wiele ataków opartych o autoodtwarzanie.

Za pomocą USB Immunizer można zapobiec automatycznemu wykonywaniu zagrożeń z pamięci flash sformatowowanych w systemach NTFS, FAT32 lub FAT. Po uodpornieniu urządzenia USB zagrożenia nie mogą już skonfigurować go do uruchamiania określonej aplikacji, gdy urządzenie jest podłączone do urządzenia z systemem Windows.

Aby uodpornić urządzenie USB:

1. Podłącz dysk flash do swojego urządzenia.
2. Przeglądaj swoje urządzenie 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 komunikat **Urządzenie USB jest chronione przed zagrożeniem opartym na automatycznym uruchamianiu** zamiast opcji Uodpornij.

Aby uniemożliwić uruchamianie zagrożeń ze strony nie zabezpieczonych urządzeń USB, wyłącz funkcję automatycznego uruchamiania multimediów. Aby uzyskać więcej informacji, odwołaj się do *„Korzystanie z automatycznego monitorowania luk"* (p. 102).

NARZĘDZIA

23. 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 Antivirus Plus automatycznie stosuje następujące ustawienia:

- Zaawansowana Ochrona Przed Zagrożeniami jest włączona
- Następujące ustawienia z Zapobiegania Zagrożeniom Online są włączone:
  - Skanowanie szyfrowanej sieci
  - Ochrona przed oszustwami
  - Ochrona przed phishingiem

23.1. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
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 wchodzi automatycznie do profilu roboczego po uruchomieniu określonej aplikacji roboczej, możesz ręcznie dodać aplikację do **Listy aplikacji roboczych**.

Żeby ręcznie dodać aplikacje do listy aplikacji roboczych w profilu służbowym należy:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Modułu Praca.
4. W oknie **Ustawienia profilu służbowego** kliknąć pozycję **Lista aplikacji**.
5. Kliknij **Dodaj**.

   Pojawi się nowe okno. Przejdź do pliku wykonywalnego aplikacji, zaznacz go i kliknij "**OK**", aby dodać go do listy.

23.2. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
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 wejdzie automatycznie do Trybu filmu po uruchomieniu określonej aplikacji odtwarzacza wideo, możesz ręcznie dodać aplikację do **Lista aplikacji filmu**.

Aby ręcznie dodać odtwarzacze wideo do listy aplikacji Film w profilu filmu należy:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Modułu Film.
4. W oknie **Ustawienia profilu filmu** kliknij **Lista odtwarzaczy**.
5. Kliknij **Dodaj**.

   Pojawi się nowe okno. Przejdź do pliku wykonywalnego aplikacji, zaznacz go i kliknij "**OK**", aby dodać go do listy.

23.3. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
3. Kliknij przycisk **Konfiguruj** w obszarze Profil Gry.
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 wchodzi automatycznie do Profilu gry po uruchomieniu określonej gry lub aplikacji, możesz ręcznie dodać aplikację do **Listy aplikacji gier**.

Aby ręcznie dodać aplikację do listy gier w Profilu gracza:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
3. Kliknij przycisk **KONFIGURUJ** w obszarze Profilu Gra.
4. W oknie **Ustawienia profilu gry** kliknij **Lista gier**.
5. Kliknij **Dodaj**.

   Pojawi się nowe okno. Przejdź do pliku wykonywalnego gry, zaznacz go i kliknij "**OK**", aby dodać go do listy.

23.4. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender

2. W zakładce **Profile** kliknij **Ustawieni**.
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**.

23.5. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
3. Kliknij przycisk **Konfiguruj** w obszarze Tryb Pracy a 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.

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.

23.6. 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W zakładce **Profile** kliknij **Ustawieni**.
3. Przewiń w dół, aż zobaczysz opcję optymalizacji czasu rzeczywistego, a następnie użyj odpowiedniego przełącznika, aby ją włączyć lub wyłączyć.

24. OCHRONA DANYCH

24.1. 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 na urządzeniu za pomocą menu kontekstowego systemu 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. Kliknij **Usuń permanentnie**, a potem potwierdź, że chcesz kontynuować proces.

   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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **Ochrona Danych** kliknij **Niszczarka Plików**.
3. Postępuj z godnie z instrukcjami Kreatora Niszczarki plików:
   a. Kliknij przycisk **Dodaj Foldery**, aby dodać pliki i foldery, które chcesz permanentnie usunąć.

      Alternatywnie, przeciągnij te pliki lub foldery do tego okna.

   b. Kliknij **Usuń permanentnie**, a potem potwierdź, że chcesz kontynuować proces.

      Poczekaj, aż Bitdefender zakończy niszczenie plików.

   c. **Podsumowanie wyników**

      Wyniki są wyświetlane. Kliknij **Zakończ**, aby wyjść z kreatora.

ROZWIĄZYWANIE PROBLEMÓW

25. 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.

- *„Mój system działa wolno"* (p. 140)
- *„Skanowanie się nie rozpoczyna"* (p. 141)
- *„Nie mogę już używać aplikacji"* (p. 144)
- *„Co zrobić, gdy Bitdefender blokuje stronę internetową, domenę, adres IP lub aplikację internetową, które są bezpieczne"* (p. 145)
- *„Jak zaktualizować produkt Bitdefender przy użyciu wolnego połączenia internetowego?"* (p. 146)
- *„Usługi produktu Bitdefender nie odpowiadają"* (p. 146)
- *„Nie działa u mnie automatyczne uzupełnianie danych przez Portfel "* (p. 147)
- *„Usunięcie produktu Bitdefender nie powiodło się"* (p. 148)
- *„Mój system nie uruchamia się po instalacji produktu Bitdefender"* (p. 149)

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. 161).

25.1. 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 innych rozwiązań bezpieczeństwa. Aby

uzyskać więcej informacji, odwołaj się do *„Jak usunąć inne rozwiązania bezpieczeństwa?"* (p. 69).

- **Wymagania systemowe do uruchomienia Bitdefender nie są spełnione.**

  Jeśli twoje urządzenie nie spełnia wymagań systemowych, może ono działać wolno, zwłaszcza przy kilku aplikacjach uruchomionych jednocześnie. Aby uzyskać więcej informacji, odwołaj się do *„Wymagania systemowe"* (p. 3).

- **Zainstalowałeś aplikacje, których nie używasz**.

  Każde urządzenie ma programy lub aplikacje, których nie używasz. 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**.

  Zagrożenia mogą wpłynąć na szybkość działania Twojego systemu oraz jego ogólne zachowanie. Oprogramowanie szpiegujące, malware, trojany i adware - wszystkie one mają wpływ na wydajność Twojego urządzenia. Skanuj swój system regularnie, przynajmniej raz w tygodniu. Zalecane jest Skanowanie Systemu przez Bitdefender, ze względu na konieczność wykrycia wszelkich zagrożeń, na które narażone jest bezpieczeństwo Twojego systemu.

  Aby rozpocząć Skanowanie Systemu:

  1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
  2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
  3. W oknie **Skany** kliknij **Uruchom Skanowanie** obok **Skanowanie Systemu**.
  4. Postępuj zgodnie z poleceniami kreatora.

25.2. 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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 69).
  2. Przeinstaluj Bitdefender:
     - W systemie **Windows 7**:
       a. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Programy i funkcje**.
       b. Wyszukaj **Bitdefender Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 161).

25.3. Nie mogę już używać aplikaci

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 Zaawanowanej Kontroli Zagrożeń.

Aby dodać program do listy wyjątków:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ZAAWANSOWANA OCHRONA PRZED ZAGROŻENIAMI**, kliknij **Otwórz**

3. W oknie **Ustawienia** kliknij **Zarządzaj Wyjątkami**
4. Kliknij **+Dodaj Wyjątek**.
5. Wprowadź ścieżkę do pliku wykonywalnego, który chcesz pominąć ze skanowania w odpowiednim polu.

   Możesz także znaleźć plik wykonywalny klikając przycisk przeglądaj z prawej strony interfejsu, wybierz plik i kliknij **OK**.
6. Włącz przełącznik obok **Zaawansowana Ochrona przed Zagrożeniami**.
7. Kliknij **Zapisz**.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 161).

25.4. Co zrobić, gdy Bitdefender blokuje stronę internetową, domenę, adres IP lub aplikację internetową, które są bezpieczne

Bitdefender oferuje bezpieczne przeglądanie internetu poprzez filtrowanie całego ruchu w sieci i blokowanie szkodliwych treści. Jednak możliwe jest, że Bitdefender uważa bezpieczną stronę internetową, domenę, adres IP lub aplikację online jako niebezpieczne, co spowoduje ich nieprawidłowe blokowanie przez skanowanie ruchu HTTP Bitdefender.

Jeśli ta sama strona, domena, adres IP lub aplikacja online jest wielokrotnie blokowana, można je dodać do wyjątków, aby nie były skanowane przez silniki Bitdefender, zapewniając w ten sposób płynne przeglądanie Internetu.

Aby dodać witrynę do **wyjątków**:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ZAPOBIEGANIE ZAGROŻENIOM ONLINE**, kliknij **Ustawienia**.
3. Kliknij **Zarządzaj wyjątkami**.
4. Kliknij **+Dodaj Wyjątek**.
5. Wpisz w odpowiednie pole nazwę strony internetowej, nazwę domeny lub adres IP, który chcesz dodać do wyjątków.
6. Kliknij przełącznik obok **Zapobieganie Zagrożeniom Online**.
7. Kliknij **Zapisz**, aby zapisać zmiany i zamknąć to okno.

Tylko strony internetowe, domeny, adresy IP i aplikacje, którym w pełni ufasz, powinny zostać dodane do tej listy. Będą one wyłączone ze skanowania za pomocą następujących mechanizmów: zagrożenia, phishingu i oszustwa.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 161).

25.5. 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 zapewnić aktualność systemu dzięki najnowszej bazie danych zagrożeń Bitdefender:

1. Kliknij **Ustawienia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Aktualizacja**.
3. Wyłącz przełącznik **Cicha aktualizacja**.
4. Następnym razem, gdy aktualizacja będzie dostępna, zostaniesz poproszony o wybranie aktualizacji, którą chcesz pobrać. Wybierz tylko **Aktualizację sygnatur**.
5. Bitdefender pobierze i zainstaluje tylko bazę danych informacji o zagrożeniach.

25.6. 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.
- inne rozwiązania bezpieczeństwa działają na twoim urządzeniu w tym samym czasie z Bitdefender.

Aby naprawić ten błąd, spróbuj poniższych rozwiązań:

1. Poczekaj kilka chwil i sprawdź, czy coś się zmieniło. Ten błąd może być tymczasowy.
2. Uruchom urządzenie ponownie i odczekaj chwilę, aż Bitdefender się uruchomi. Uruchom program Bitdefender i sprawdź, czy błąd nadal występuje. Ponowne uruchomienie urządzenia 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. 69).

Jeśli błąd się powtarza, skontaktuj się z naszym przedstawicielem, tak jak opisano w sekcji *„Prośba o pomoc”* (p. 161).

25.7. 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 **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 przycisk **Otwórz menu** prawym górnym rogu ekranu.

3. Kliknij Dodatki.
4. Kliknij Rozszerzenia.
5. Wskaż na **Bitdefender Portfel** i kliknij przełącznik obok.

- W **Google Chrome:**
  1. Otwórz Google Chrome.
  2. Przejdź do ikony Menu.
  3. Wybierz Więcej Narzędzi.
  4. Kliknij Rozszerzenia.
  5. Wskaż na **Bitdefender Portfel** i kliknij odpowiedni przełącznik.

> **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. 161).

25.8. 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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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.

25.9. 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. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak uruchomić ponownie komputer w Trybie awaryjnym?"* (p. 70).
  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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak uruchomić ponownie komputer w Trybie awaryjnym?"* (p. 70).
  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. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak uruchomić ponownie komputer w Trybie awaryjnym?"* (p. 70).
2. Użyj opcji odzyskiwania systemu Windows, aby przywrócić urządzenie 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. 161).

26. USUWANIE ZAGROŻEŃ Z TWOJEGO SYSTEMU

Zagrożenia mogą wpływać na system na wiele różnych sposobów, a rodzaj działań Bitdefender zależy od typu ataku zagrożenia. Ponieważ zagrożenia często zmieniają swoje zachowanie, ustalenie wzorca ich zachowania i działania jest bardzo trudne.

Istnieją sytuacje, gdy Bitdefender nie może automatycznie usunąć z systemu infekcji zagrożenia. 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. 161).

26.1. Środowisko Ratunkowe

Tryb Ratunkowy to funkcja Bitdefender, która pozwala na skanowanie i oczyszczanie wszystkich istniejących partycji dysku twardego wewnątrz i poza systemem operacyjnym.

Środowisko Ratunkowe Bitdefender jest zintegrowane z Windows RE,

Włączanie Twojego komputera w Trybie ratunkowym

Środowisko Ratunkowe można wprowadzić tylko z produktu Bitdefender w następujący sposób:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
3. Kliknij **Otwórz** obok **Środowisko Ratunkowe**.
4. Kliknij **Uruchom ponownie** w oknie, które się pojawi.

   Środowisko Ratunkowe Bitdefender niedługo się załaduje.

Skanowanie Twojego komputera w trybie ratunkowym

Aby przeskanować system w Środowisku Ratunkowym:

1. Wejdź do Środowiska Ratunkowego, jak opisano w „Włączanie Twojego komputera w Trybie ratunkowym" (p. 153).
2. Proces skanowania Bitdefender rozpoczyna się automatycznie, gdy tylko system zostanie załadowany do Środowiska Ratunkowego.
3. Poczekaj na zakończenie skanowania. Jeśli wykryte zostanie jakiekolwiek zagrożenie, postępuj zgodnie z instrukcjami, aby je usunąć.
4. Aby opuścić Środowisko Ratunkowe, kliknij **Zamknij** w oknie z rezultatem skanowania.

26.2. Co zrobić, gdy Bitdefender znajdzie zagrożenia na twoim urządzeniu?

Możesz dowiedzieć się, że istnieje zagrożenie na twoim urządzeniu na jeden z następujących sposobów:

- Przeskanowałeś urządzenie i Bitdefender znalazł w nim zainfekowane elementy.
- Alarm zagrożeń informuje o zablokowaniu przez Bitdefender jednego lub więcej zagrożeń na Twoim urządzeniu.

W takich sytuacjach zaktualizuj Bitdefender, aby mieć pewność, że masz aktualną bazę danych informacji o zagrożeniach 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 **Narzędzia** w menu nawigacji w interfejsie Bitdefender
   b. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
   c. W oknie **Zaawansowane** wyłącz ochronę **Bitdefender**.
2. Wyświetl ukryte obiekty w systemie Windows. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak wyświetlić ukryte obiekty w systemie Windows?"* (p. 68).
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. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak uruchomić ponownie komputer w Trybie awaryjnym?"* (p. 70).
2. Wyświetl ukryte obiekty w systemie Windows. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak wyświetlić ukryte obiekty w systemie Windows?"* (p. 68).
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. 161).

26.3. Jak usunąć zagrożenie 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 zagrożeń, ale nie może podjąć jakichkolwiek działań.

Jeśli Bitdefender informuje, iż w archiwum znaleziono zagrożenie i nie może podjąć żadnych działań, oznacza to, że usunięcie zagrożenia jest niemożliwie z powodu ograniczeń w ustawieniach zezwoleń tego archiwum.

Oto, w jaki sposób można usunąć zagrożenie z archiwum:

1. Zidentyfikuj archiwum zawierające zagrożenie, wykonując skanowanie systemu.
2. Wyłącz ochronę antywirusową w czasie rzeczywistym Bitdefender:
   a. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
   b. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
   c. W oknie **Zaawansowane** wyłącz ochronę **Bitdefender**.
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 zagrożenie zapisane w archiwum nie jest bezpośrednim zagrożeniem dla systemu, ponieważ aby mogło go zainfekować, musi być najpierw rozpakowane i uruchomione.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem Bitdefender tak jak to opisano w sekcji *„Prośba o pomoc"* (p. 161).

26.4. Jak usunąć zagrożenie z archiwum wiadomości e-mail?

Bitdefender może także rozpoznawać zagrożenia w bazie danych e-maili oraz archiwów e-mail przechowywanych 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 zagrożenie zapisane w archiwum poczty:

1. Skanuj bazę danych e-mail przy użyciu Bitdefender.
2. Wyłącz ochronę antywirusową w czasie rzeczywistym Bitdefender:
   a. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
   b. W panelu **ANTYWIRUS**, kliknij **Otwórz**.
   c. W oknie **Zaawansowane** wyłącz ochronę **Bitdefender**.
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. 161).

26.5. 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. Aby dowiedzieć się, jak to zrobić, sprawdź *„Jak mogę przeskanować swój system?"* (p. 54).
2. Jeśli skanowanie nic nie wykryło, ale nadal nie masz pewności co do jakiegoś pliku, skontaktuj się z działem pomocy technicznej.

   Aby dowiedzieć się, jak to zrobić, sprawdź *„Prośba o pomoc"* (p. 161).

26.6. 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 ochronę urządzenia. 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.

26.7. 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.

26.8. 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.

26.9. 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 zagrożeń, 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.

CONTACT US

27. 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. 140) 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 Bitdefender Antivirus Plus" (p. 161)
- „Skontaktuj się z naszym centrum wsparcia technicznego online" (p. 162)

Skontaktuj się z nami bezpośrednio z Bitdefender Antivirus Plus

Jeśli jesteś połączony z Internetem, możesz poprosić Bitdefender o wsparcie bezpośrednio z poziomu interfejsu produktu.

Wykonaj następujące kroki:

1. Kliknij przycisk **Wsparcie**, reprezentowany przez **znak zapytania** w górnej części interfejsu Bitdefender.
2. Możesz wybrać spośród dostępnych opcji:
   - **INSTRUKCJA**

     Wejdź do naszej bazy danych i wyszukaj niezbędne informacje.
   - **CENTRUM WSPARCIA**

     Uzyskaj dostęp do naszych artykułów online i samouczków wideo.
   - **POMOC TECHNICZNA**

     Użyj przycisku **Skontaktuj się z Pomocą techniczną**, aby uruchomić narzędzie Pomocy technicznej Bitdefender i skontaktować się z działem obsługi klienta.

a. Wypełnij pola formularza niezbędnymi danymi:

   i. Wybierz rodzaj napotkanego problemu.

   ii. Opisz problem, który napotkałeś.

   iii. Kliknij **SPRÓBUJ ODTWORZYĆ TEN PROBLEM** w przypadku wystąpienia problemu z produktem. Odtwórz problem, a następnie kliknij przycisk **ZAKOŃCZ** w ramce ODTWARZANIE PROBLEMU.

   iv. Kliknij **POTWIERDŹ ZGŁOSZENIE**.

b. Uzupełnij formularz zgłoszeniowy o niezbędne dane:

   i. Wprowadź swoje imię i nazwisko.

   ii. Wprowadź swój adres e-mail.

   iii. Zaznacz pole zgody.

   iv. Kliknij **UTWÓRZ PAKIET DEBUGOWANIA**.

   Poczekaj kilka minut, aż Bitdefender zgromadzi informacje dotyczące produktu. Pomogą one naszym inżynierom w znalezieniu rozwiązania twojego problemu.

c. Kliknij **ZAMKNIJ**, aby wyjść z kreatora. Skontaktujemy się z Tobą najszybciej, jak to możliwe, przez jednego z naszych przedstawicieli.

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.

28. 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.

28.1. Centrum pomocy technicznej produktu Bitdefender

Centrum pomocy technicznej Bitdefender to internetowy magazyn informacji o produktach Bitdefender. Przechowuje czytelne raporty z trwających działań Bitdefender odnośnie pomocy technicznej i naprawiania błędów oraz bardziej ogólne artykuły dotyczące ochrony przed zagrożeniami, 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.

28.2. 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 urządzenia określonych zagrożeń 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**.

28.3. Portal HOTforSecurity

Strona HOTforSecurity jest bogatym źródłem informacji na temat bezpieczeństwa komputerowego. Tu możesz dowiedzieć się więcej o różnych zagrożeniach, na które narażone jest urządzenie połączone z Internetem (malware, 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/.

29. CONTACT INFORMATION

Skuteczna komunikacja jest kluczem do udanej współpracy. Od 2001 roku BITDEFENDER cieszy się doskonałą reputacją 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.

29.1. 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:http://www.bitdefender.pl

29.2. 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 email na adres sales@bitdefender.com. Abyśmy mogli szybko zapewniać pomoc, prosimy o pisanie wiadomości e-mail w języku angielskim.

29.3. 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
Email: info@bitdefender.co.uk
Phone: (+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
Phone: +34 902 19 07 65
Sprzedaż: comercial@bitdefender.es
Pomoc Techniczna: https://www.bitdefender.es/support/consumer.html
Strona: https://www.bitdefender.es

Rumunia

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Faks: +40 21 2641799
Telefon do sprzedaży: +40 21 2063470
Email do sprzedaży: sales@bitdefender.ro
Pomoc Techniczna: https://www.bitdefender.ro/support/consumer.html
Strona: 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
Email do sprzedaży: mena-sales@bitdefender.com
Pomoc Techniczna: https://www.bitdefender.com/support/consumer.html
Strona: 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.

Aktualizacja Informacji o Zagrożeniach

Binarny wzorzec zagrożenia, używany przez rozwiązanie bezpieczeństwa do wykrywania i eliminowania zagrożenia.

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.

Atak Brute Force

Atak z odgadnięciem haseł wykorzystywany jest do włamania się do systemu komputerowego poprzez wprowadzenie możliwych kombinacji haseł, zaczynając od najprostszego hasła.

Atak Słownikowy

Ataki polegające na odgadywaniu haseł służyły do włamania się do systemu komputerowego poprzez wprowadzenie kombinacji typowych słów w celu wygenerowania potencjalnych haseł. Ta sama metoda służy do odgadywania kluczy deszyfrowania zaszyfrowanych wiadomości lub dokumentów. Ataki słownikowe kończą się sukcesem, ponieważ wiele

osób skłania się do wybierania haseł krótkich i pojedynczych słów, które są łatwe do odgadnięcia.

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.

Boot sector

Sektor na początku każdego dysku, który rozpoznaje budowę dysku (rozmiar sektora, rozmiar klastra itd.). Sektor rozruchowy zawiera również program uruchamiający system operacyjny.

Botnet

Słowo "botnet" jest połączeniem słów "robot" oraz "network"(sieć). Botnety to urządzenia połączone z internetem, zainfekowane zagrożeniami, które mogą być wykorzystywane do wysyłania spamu, kradzieży danych, zdalnego sterowania urządzeniami podatnymi na zagrożenia lub rozprzestrzeniania oprogramowania szpiegującego, ransomware i innych rodzajów zagrożeń. 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.

Cyberprzemoc
Gdy koledzy lub obcy ludzie obrażają Twoje dzieci. Aby skrzywdzić emocjonalne, napastnicy wysyłają obraźliwe wiadomości lub zdjęcia, przez co ich ofiary izolują się od innych lub czują się sfrustrowane.

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.

Exploity
Sposób na wykorzystanie różnych błędów lub luk w zabezpieczeniach komputera (oprogramowania lub sprzętu). Dlatego hakerzy mogą uzyskać kontrolę nad komputerami lub sieciami.

Fałszywy alarm
Pojawia się, kiedy skaner identyfikuje plik jako zainfekowany, gdy w rzeczywistości nie jest zainfekowany.

Heurystyczny
Oparta na regułach metoda rozpoznawania nowych zagrożeń. Ta metoda skanowania nie opiera się na konkretnej bazie danych informacji o zagrożeniach. Zaletą skanowania heurystycznego jest to, że nie jest ono podatne na zmylenie przez nowy wariant znanych zagrożeń. 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

Keylogger to aplikacja, która rejestruje wszystko, co wpisujesz.

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 zagrożenia komputerowego, które jest zakodowane 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 konkretnej bazie danych informacji o zagrożeniach. Zaletą skanowania nieheurystycznego jest to, że nie jest ono podatne na wprowadzanie w błąd przez obiekty wydające się być zagrożeniem, 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.

Pamięć

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.

Phishing

Wysyłanie wiadomości e-mail do użytkownika przez osobę podającą się za przedstawiciela uprawnionego do tego przedsiębiorstwa, będące próba 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 nr 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 Twojego Rozwiązania Bezpieczeństwa. 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.

Przestępcy online

Osoby, które starają się nakłonić nieletnich lub nastolatków do rozmów, aby zaangażować ich w nielegalne działania seksualne. Sieci społecznościowe są idealnym miejscem, w którym łatwo można polować na wrażliwe dzieci i skłaniać je do podejmowania działań seksualnych, online lub face-to-face.

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 zagrożenia lub intruza w systemie. Gdy są połączone z zagrożeniami, stanowią ryzyko 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.

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.

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 złośliwego oprogramowania i wormsów, Trojany nie powielają się. Jednym z najniebezpieczniejszych typów Trojanów jest program zapewniający, że pozbędzie się zagrożeń z Twojego komputera, a który w rzeczywistości wprowadza je 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.

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

Zagrożenie, które zmienia swoją formę za każdym razem, kiedy zainfekuje kolejny plik. Ponieważ nie mają one stałego wzoru binarnego, są trudne do rozpoznania.

Wirus sektora rozruchowego

Zagrożenie, które infekuje boot sektor dysku stałego lub stację dyskietek. Próba uruchomienia systemu z dyskietki zainfekowanej wirusem tego typu spowoduje, że zagrożenie uaktywni się w pamięci. Od tego momentu za każdym razem, kiedy będziesz uruchamiał system, zagrożenie będzie aktywne 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 tych zagrożeń.

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 zagrożenia do sieci odbywa się za pośrednictwem pliku PDF lub dokumentu pakietu Office, który wygląda nieszkodliwe, tak aby każdy użytkownik mógł uruchomić plik.

Zagrożenie

Program lub fragment kodu, który jest załadowany na Twoim komputerze bez Twojej wiedzy i uruchamia się wbrew Twojej woli. Większość zagrożeń może się również replikować. Wszystkie zagrożenia są tworzone przez człowieka. Zagrożenie, które umie się skopiować kilka razy jest stosunkowo łatwe do utworzenia. Nawet tak proste zagrożenie jest niebezpieczne, ponieważ szybko wykorzysta całą dostępną pamięć i przyczyni się do zatrzymania pracy systemu. Bardziej niebezpiecznym typem zagrożenia jest takie, które jest zdolne przenosić się przez sieci i łamać systemy bezpieczeństwa.

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.