bitdefender
INTERNET SECURITY 2011

Podręcznik użytkownika

BitDefender Internet Security 2011
Podręcznik użytkownika

Data wydania 2010.09.02

Uwagi Prawne


bitdefender

Spis treści

Instalacja i Usuwanie

1. Wymagania Systemowe

Możesz zainstalować BitDefender Internet Security 2011 tylko na komputerach z zainstalowanymi następującymi systemami operacyjnymi:

- Windows XP z dodatkiem Service Pack 3 (32 bit) / Windows XP z dodatkiem Service Pack 2 (64 bit)
- Windows Vista z dodatkiem Service Pack 1 lub nowszym (32/64 bit)
- Windows 7 (32/64 bit)

Przed instalacją proszę się upewnić że komputer spełnia minimalne wymagania sprzętowe oraz programowe.

Notatka

Aby sprawdzić system operacyjny Windows oraz sprzęt na twoim komputerze kliknij prawym klawiszem myszy na **Mój Komputer** na pulpicie i następnie **Właściwości** z menu.

1.1. Minimalne Wymagania Sprzętowe

- 1 GB wolnej przestrzeni na dysku twardym
- procesor 800 MHz
- Pamięć RAM:
  - 512 MB dla Windows XP
  - 1 GB dla Windows Vista i Windows 7
- Internet Explorer 6.0
- .NET Framework 2 (dostępny także w zestawie instalatora)
- Adobe Flash Player 10.0.45.2

1.2. Rekomendowane Wymagania Sprzętowe

- 1 GB wolnej przestrzeni na dysku twardym
- Intel CORE Duo (1.66 GHz) lub procesor o podobnej wydajności
- Pamięć RAM:
  - 1 GB dla Windows XP i Windows 7
  - 1.5 GB dla Windows Vista
- Internet Explorer 7
- .NET Framework 2 (dostępny także w zestawie instalatora)
- Adobe Flash Player 10.0.45.2

1.3. Wymagania Systemowe

Ochrona antyphishingowa jest zapewniana dla:

- Internet Explorer 6.0 (lub nowszy)
- Mozilla Firefox 3.x
- Yahoo! Messenger 8.1

- Microsoft Windows Live Messenger 8

Szyfrowanie komunikatorów (IM) jest zapewniane dla:

- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

Ochrona antyspamowa jest zapewniona dla wszystkich klientów email POP3/SMTP.Jednakże pasek narzędzi BitDefender Antyspam jest zintegrowany tylko z:

- Microsoft Outlook 2003 / 2007 / 2010
- Microsoft Outlook Express 6
- Microsoft Windows Mail
- Mozilla Thunderbird 3.0.4

2. Przygotowywanie do Instalacji

Zanim zainstalujesz BitDefender Internet Security 2011, wykonaj następujące przygotowania aby instalacja przebiegała płynnie i bez problemów:

- Upewnij się że komputer na którym chcesz zainstalować oprogramowanie BitDefender spełnia minimalne wymagania systemowe.Jeśli komputer nie spełnia minimalnych wymagań systemowych, BitDefender nie zostanie zainstalowany, lub zainstaluje się i nie będzie działał poprawnie, w znacznym stopniu zwalniając pracę systemu i czyniąc go niestabilnym.Aby zobaczyć pełną listę wymagań systemowych, przejdź do „*Wymagania Systemowe*” (p. 2).
- Zaloguj się do systemu na konto administratora.
- Usuń inne oprogramowanie zabezpieczające z tego komputera.Korzystanie z dwóch programów zabezpieczeń naraz może wpłynąć negatywnie na ich działanie i spowodować problemy z systemem.Windows Defender zostanie domyślnie zablokowany przed rozpoczęciem instalacji.
- Zablokuj lub usuń oprogramowanie zapory sieciowej, które może być uruchomione na tym komputerze.Korzystanie z dwóch zapór sieciowych naraz może wpłynąć negatywnie na ich działanie i spowodować problemy z systemem.Zapora sieciowa Windows zostanie domyślnie zablokowana przed rozpoczęciem instalacji.

3. Instalacja BitDefendera

Możesz zainstalować BitDefender z płyty instalacyjnej CD BitDefender lub korzystając z pliku instalacyjnego pobranego na twój komputer ze strony WWW BitDefender lub innych autoryzowanych stron (np. strony oficjalnego partnera BitDefender lub sklepu internetowego).Możesz pobrać plik instalacyjny ze strony BitDefender pod adresem: http://www.bitdefender.com/site/Downloads/.

- Aby zainstalowac BitDefender z płyty CD, umieść płytę w napędzie. Po chwili, powinien wyświetlić się ekran powitalny. Podążaj za instrukcjami aby uruchomić instalację.

  Notatka

  Ekran powitalny udostępnia opcję skopiowania pakietu instalacyjnego z płyty CD na dysk USB. Jest to szczególnie przydatne w przypadku, gdy nie posiadasz napędu CD (np. w netbooku).Podłącz urządzenie magazynujące USB i kliknij **Kopiuj na USB**.Następnie na komputerze bez napędu CD, podłącz urządzenie magazynujące USB i kliknij dwukrotnie na `runsetup.exe` w folderze, gdzie zapisano pakiet instalacyjny.

  Jeśli ekran powitalny nie pojawi się, przejdź do katalogu głównego płyty CD i dwukrotnie kliknij plik `autorun.exe`.

- Aby zainstalować BitDefender z pliku instalacyjnego pobranego na komputer, odnajdź go i kliknij na nim dwukrotnie.

Program instalacyjny najpierw sprawdzi twój system, aby móc określić poprawność instalacji.Jeśli instalacja została zatwierdzona, przed pojawieniem się kreatora konfiguracji zostaniesz poproszony o wybór języka.

Kreator ten pomoże ci zainstalować BitDefender na komputerze, jak również pozwoli skonfigurować ustawienia główne i interfejs użytkownika.

3.1. Krok 1 - Wprowadzenie

Przeczytaj Umowę licencyjną i wybierz **Zaznaczając to pole akceptuję umowę licencyjną BitDefender**.Kliknij **Dalej** aby kontynuować.

Jeśli nie zgadzasz się z Umowę Licencyjną kliknij **Anuluj** Proces instalacji zostanie zakończony i wyjdziesz z kreatora instalacji programu.

3.2. Krok 2 - Przygotowanie instalacji

BitDefender skanuje system i sprawdza, czy zainstalowane jest w nim inne oprogramowanie zabezpieczające.

Szybkie skanowanie

Wykonywany jest szybki skan najważniejszych obszarów systemu, w celu sprawdzenia, czy nie ma w nich aktywnego złośliwego oprogramowania.

Skanowanie to nie powinno trwać dłużej niż kilka minut. W dowolnej chwili można je anulować, korzystając z dostępnego przycisku.

WAŻNE
Zaleca się ukończenie skanowania.
Aktywne złośliwe oprogramowanie może zakłócić instalację, a nawet ją uniemożliwić.

Po ukończeniu skanowania zostaną wyświetlone wyniki. Jeśli zostaną wykryte jakiekolwiek zagrożenia, postępuj zgodnie z poleceniami, aby usunąć je przed kontynuowaniem instalacji.

Kliknij **Dalej** aby kontynuować.

Usuwanie Obecnie Zainstalowanego Oprogramowania Zabezpieczającego

BitDefender Internet Security 2011 ostrzega, gdy na danym komputerze zainstalowano inne produkty zabezpieczające.Kliknij odpowiedni przycisk, aby rozpocząć proces deinstalacji i postępuj zgodnie z poleceniami, aby usunąć wszelkie wykryte produkty.

Ostrzeżenie
Zalecamy odinstalowanie innych produktów antywirusowych przed instalacją BitDefendera. Uruchomienie dwóch lub więcej produktów antywirusowych na komputerze blokuje system operacyjny.

BitDefender zaleca także podejmowanie działań w systemie Windows z włączonymi funkcjami bezpieczeństwa.

- **Wyłącz Zaporę Sieciową Windows** - aby wyłączyć Zaporę Sieciową Windows.

WAŻNE
Zalecamy wyłączenie Zapory sieciowej Windows, ponieważ BitDefender Internet Security 2011 zawiera zaawansowany moduł Zapory sieciowej. Używanie dwóch zapór na tym samym komputerze może spowodować problemy.

- **Wyłącz programu Windows Defender** - aby wyłączyć program Windows Defender.

Kliknij **Dalej** aby kontynuować.

3.3. Krok 3 - Rejestracja

Proces rejestracji BitDefender składa się z zarejestrowania produktu za pomocą klucza licencyjnego oraz aktywowania funkcji poprzez utworzenie konta BitDefender.

Zarejestruj swój produkt

Postępuj zgodnie ze swoją sytuacją:

- **Zakupiłem BitDefender Internet Security 2011 na płycie CD lub przez Internet**

  W tym wypadku musisz zarejestrować produkt:

  1. Wpisz w polu klucz licencyjny.

     Notatka
     Klucz licencyjny możesz znaleźć:
     - na etykiecie płyty CD.
     - na karcie rejestracyjnej produktu.
     - w emailu potwierdzającym zakup.

     Jeśli nie masz klucza licencyjnego BitDefendera, kliknij link aby przejść do internetowego sklepu BitDefender i kupić go.

  2. Kliknij **Zarejestruj Teraz**.
  3. Kliknij **Dalej**.

- **Pobrałem BitDefender Internet Security 2011, aby dokonać jego oceny.**

  W tym wypadku można korzystać z wszystkich funkcji produktu przez okres 30 dni.Aby rozpocząć okres próbny, zaznacz **Chcę oceniać BitDefender Internet Security 2011 przez okres 30 dni** i kliknij **Dalej**.

Aktywuj opcje online

MUSISZ utworzyć konto BitDefender aby otrzymywać aktualizacje BitDefendera.Konto BitDefender zapewnia również dostęp do internetowej kontroli rodzicielskiej, darmowej pomocy technicznej oraz specjalnych ofert i promocji.Jeśli stracisz klucz licencyjny BitDefender, będziesz mógł zalogować się do swojego konta w http://myaccount.bitdefender.com, aby go odzyskać.

Jeśli w danej chwili nie chcesz tworzyć konta BitDefender, wybierz opcję **Utwórz konto później** i kliknij **Następne**.

Notatka
Jeśli instalujesz BitDefender Internet Security 2011, aby go przetestować, musisz w tym momencie utworzyć konto BitDefender.
Jeśli zakupiłeś produkt, konto musisz utworzyć w ciągu 30 dni od jego instalacji.

W przeciwnym razie postępuj w zależności od sytuacji:

- **Nie posiadam konta BitDefender**

  Aby pomyślnie utworzyć konto BitDefender, podążaj według tych kroków:

  1. Wybierz **Utwórz nowe konto**.
  2. Wprowadź wymaganą informację w odpowiednich polach.Dane które teraz wprowadzisz pozostaną tajne.
     - **Nazwa użytkownika** - wpisz swój adres e-mail.
     - **Hasło** - wpisz hasło dla konta BitDefender.Hasło musi zawierać od 6 do 16 znaków.
     - **Wpisz ponownie hasło** - wpisz ponownie hasło podane wcześniej.

       Jeśli podczas wpisywania hasła nie zaznaczyłeś opcji jego maskowania, nie musisz ponownie go wpisywać.

     Notatka
     Jak tylko konto zostanie aktywowane, możesz korzystać z dołączonego adresu e-mail aby zalogować się na nie pod adresem http://myaccount.bitdefender.com.

  3. Opcjonalnie, BitDefender może informować ciebie o specjalnych ofertach oraz promocjach korzystając z adresu email twojego konta.Kliknij **Zobacz opcje kontaktu** i z okna, które pojawi się na ekranie, wybierz jedną z dostępnych opcji.
     - **Wyślij mi wszystkie wiadomości**
     - **Przysyłaj mi ważne wiadomości**
     - **Nie wysyłaj mi żadnych wiadomości**
  4. Kliknij **Wyślij**.
  5. Kliknij **Dalej** aby kontynuować.

     Notatka
     Zanim zaczniesz korzystać z konta, musisz je aktywować.
     Sprawdź swoją pocztę i postępuj według instrukcji zawartych w e-mailu przysłanym ci przez usługę rejestracji BitDefender.

- **Już posiadam konto BitDefender**

  BitDefender automatycznie wykryje czy poprzednio rejestrowałeś konto BitDefender na swoim komputerze.W tym przypadku, wpisz hasło do konta i kliknij **Zaloguj się**.Kliknij **Dalej** aby kontynuować.

  Jeśli już posiadasz aktywne konto, ale BitDefender go nie wykrywa, wykonaj następujące kroki aby zarejestrować produkt dla tego konta:

  1. Wybierz **Zaloguj się (Poprzednie konto)**.

2. W odpowiednich polach wprowadź adres e-mail i hasło do twojego konta.

   Notatka
   Jeżeli zapomniałeś hasła kliknij **Nie pamiętasz hasła?** i wykonuj instrukcje.

3. Opcjonalnie, BitDefender może informować ciebie o specjalnych ofertach oraz promocjach korzystając z adresu email twojego konta.Kliknij **Zobacz opcje kontaktu** i z okna, które pojawi się na ekranie, wybierz jedną z dostępnych opcji.
   - **Wyślij mi wszystkie wiadomości**
   - **Przysyłaj mi ważne wiadomości**
   - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Wyślij**.
5. Kliknij **Dalej** aby kontynuować.

3.4. Krok 4 - Wybór widoku

W tym miejscu można wybrać typ instalacji oraz tryb wyświetlania interfejsu.

Wybierz rodzaj instalacji

Dostępne są następujące opcje konfiguracji:

- **Łatwa instalacja** - wybierz tę opcję, jeśli wolisz szybką instalację i nie zamierzasz konfigurować ustawień BitDefender.
- **Instalacja własna** - wybierz tę opcję, jeśli wolisz dostosować instalację i ustawienia BitDefender.

Aby zobaczyć film instruktażowy poświęcony instalacji, kliknij **Uzyskaj pomoc**.

Notatka
Aby zainstalować BitDefender w konfiguracji domyślnej i przejść od razu do ostatniego kroku kreatora instalacji, wybierz **Pomiń instalację**.

Kliknij **Dalej** aby kontynuować.

Wybierz katalog docelowy

Notatka
Krok ten pojawia się tylko wtedy, gdy wybrałeś **Instalację własną**.

Domyślnie, BitDefender Internet Security 2011 instalowany jest w `C:\Program Files\BitDefender\`.Jeżeli chcesz wybrać inny folder instalacji, kliknij **Przeglądaj** i wybierz folder w którym chcesz zainstalować BitDefendera.

Sygnatury i pliki produktu można udostępniać innym użytkownikom BitDefender.Dzięki temu aktualizacje BitDefender mogą przebiegać szybciej.Jeśli nie chcesz włączać tej funkcji, zaznacz odpowiednie pole wyboru.

Notatka
Gdy funkcja ta jest włączona, udostępnienie jakichkolwiek danych osobowych staje się niemożliwe.

Kliknij **Dalej** aby kontynuować.

Wybór Interfejsu Użytkownika

Wybierz tryb wyświetlania interfejsu użytkownika, który najlepiej odpowiada twoim potrzebom.BitDefender Internet Security 2011 oferuje wybór trzech interfejsów, z których każdy dopasowany jest do potrzeb innego typu użytkownika.

Widok Podstawowy

Odpowiedni dla początkujących użytkowników komputera oraz osób, które chcą, aby BitDefender chronił je bez informowania o tym. Jest to prosty interfejs, który wymaga od użytkownika jedynie minimalnej uwagi.

Jedyne co musisz zrobić, to naprawić zagadnienia dotyczące bezpieczeństwa, wskazywane przez BitDefender. Umożliwia to intuicyjny kreator, który prowadzi użytkownika krok po kroku, przez proces rozwiązywania problemów.Dodatkowo, możesz przeprowadzić podstawowe zadania, takie jak aktualizacja plików BitDefendera i sygnatur wirusów lub skanowanie komputera.

Widok średniozaawansowany

Możesz konfigurować główne ustawienia BitDefender, osobno naprawiać problemy, zarządzać produktami BitDefender zainstalowanymi na komputerach w domu oraz określić zagadnienia, które mają być monitorowane.Co więcej, poprzez odpowiednie skonfigurowanie modułu Kontroli Rodzicielskiej można określić sposób użytkowania komputera i Internetu przez dzieci.

Widok eksperta

Przeznaczony dla osób posiadających techniczną wiedzę, ten tryb pozwala w dogłębny sposób skonfigurować każdy moduł BitDefender.Możesz także skorzystać ze wszystkich udostępnionych zadań aby chronić swój komputer i dane.

Dokonaj wyboru i kliknij **Dalej**, aby kontynuować.

3.5. Krok 5 - Konfiguracja

W tym miejscu można dostosować produkt.

Ustawienia konfiguracji

Notatka
Krok ten pojawia się tylko wtedy, gdy interfejs BitDefender pracuje w trybie **Widok eksperta**.

Tutaj można włączać / wyłączać funkcje BitDefender podzielone na dwie kategorie.Aby zmienić stan ustawienia, kliknij odpowiedni przełącznik.

- **Ustawienia Zabezpieczeń**

  W tym obszarze możesz odblokować lub zablokować ustawienia zabezpieczeń programu, które obejmują różne aspekty bezpieczeństwa komputera i jego danych.

Ustawienie	Opis
Antywirus	Ochrona w czasie rzeczywistym dba o to, aby wszystkie pliki, z których korzystasz Ty lub aplikacje działające w systemie, były skanowane.
Automatyczna Aktualizacja	Automatyczna Aktualizacja gwarantuje automatyczne pobieranie i instalowanie sygnatur i plików BitDefendera.
Sprawdzanie Podatności	Automatyczne sprawdzanie podatności na zagrożenia sprawdza, czy najważniejsze oprogramowanie na twoim PC jest aktualne.
Antyspam	Antyspam filtruje odbierane wiadomości e-mail, oznaczając te, których nie chcesz odbierać i śmieci jako SPAM.
Antyphishing	Antyphishing wykrywa i informuje w czasie rzeczywistym, czy strona WWW próbuje wykraść prywatne informacje.
Kontrola tożsamości	Kontrola Tożsamości pomaga chronić prywatne dane przed wysłaniem ich do Internetu bez wiedzy użytkownika. Blokuje rozmowy IM, wiadomości e-mail i dane przesyłane w formularzach, w których pojawiają się prywatne informacje przesyłane do nieautoryzowanych odbiorców.
Szyfrowanie rozmów	Szyfrowanie rozmów zabezpiecza rozmowy przez programy Yahoo! Messenger i Windows Live Messenger, pod warunkiem że kontakty IM korzystają z kompatybilnego produktu BitDefender i oprogramowania IM.

Ustawienie	Opis
Kontrola Rodzcielska	Kontrola Rodzicielska ogranicza dostęp do komputera i Internetu dla twoich dzieci opierając się na regułach które stworzysz.Restrykcje mogą obejmować blokowanie nieprawidłowych stron WWW, oraz limitowanie czasu korzystania z gier i Internetu, według określonego harmonogramu.
Zapora Sieciowa	Zapora Sieciowa chroni twój komputer przed zewnętrznymi atakami szkodliwego programowania i hakerów.

- **Ustawienia Ogólne**

W tym obszarze możesz odblokować lub zablokować ustawienia które wpływają na zachowanie programu i sposób współpracy z użytkownikiem.

Ustawienie	Opis
Tryb Gry	Tryb Gry tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na wydajność systemu podczas grania.
Wykrycie Trybu Laptopa	Tryb Laptopa tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na żywotność baterii.
Hasło Ustawień	To zapewnia że ustawienia BitDefendera mogą być zmienione tylko przez osobę znającą hasło. Kiedy włączysz tą opcję, program zapyta o skonfigurowanie hasła do ustawień.Wpisz pożądane hasło w obydwu polach i kliknij **OK** aby je ustawić.
Nowości BitDefendera	Włączając tą opcje, będziesz otrzymywać ważne informacje firmowe, aktualizacje produktu lub nowości o nowych zagrożeniach od BitDefendera.
Alarm Informacyjny Produktu	Włączając tą opcje, będziesz otrzymywał alarmy informacyjne.
Pasek Aktywności Skanera	Pasek aktywności skanera to małe, przezroczyste okno wskazujące postęp i aktywność skanera BitDefender.Aby uzyskać więcej informacji, odwołaj się do *„Pasek Aktywności Skanera”* (p. 20).
Wyślij Raporty o Wirusach	Włączając tą opcje, będziesz wysyłał raporty skanowania wirusów do Laboratorium BitDefendera

Ustawienie	Opis
	do analizy. Proszę pamiętać że te raporty nie zawierają żadnych danych osobistych, takich jak adres imię lub IP i nie będą wykorzystywane w celach komercyjnych.
Wykrywanie Epidemii	Włączając tą opcje, będziesz wysyłał raporty dotyczące potencjalnych włamań wirusów do Laboratorium BitDefendera do analizy. Proszę pamiętać że te raporty nie zawierają żadnych danych osobistych, takich jak adres imię lub IP i nie będą wykorzystywane w celach komercyjnych.

Kliknij **Dalej** aby kontynuować.

Konfiguracja Moich Narzędzi

Notatka
Krok ten pojawia się tylko wtedy, gdy interfejs BitDefender pracuje w trybie **Widok podstawowy** lub **Widok średniozaawansowany**.

Korzystając z **Moich narzędzi** można spersonalizować pulpit poprzez dodanie skrótów do najważniejszych narzędzi.W ten sposób możesz zapewnić do nich łatwy dostęp.

Za pośrednictwem tego ekranu można dodawać skróty do któregokolwiek z następujących narzędzi:

- Kontrola Rodzicielska - kontroluje i monitoruje użytkowanie komputera przez dzieci.
- Tryb Gry - konfiguruje BitDefender tak, aby nie przeszkadzał on rozgrywce.
- Tryb Laptopa - tymczasowo modyfikuje ustawienia zabezpieczeń, aby zminimalizować ich wpływ na żywotność baterii.
- Zarządzanie siecią domową - zarządzaj produktami BitDefender zainstalowanymi na komputerach sieci domowej z pojedynczego komputera.

Dokonaj wyboru narzędzi, które chcesz dodać i kliknij **Dalej**, aby kontynuować.

Ustaw kontrolę rodzicielską

Notatka
Krok ten pojawia się tylko wtedy, gdy do Moich narzędzi dodana została opcja Kontroli Rodzicielskiej.

Można wybrać jedną z trzech opcji:

- **Ustawienie Kontroli Rodzicielskiej na kontach dzieci**

  Wybierz tę opcję, aby włączyć Kontrolę Rodzicielską dla kont Windows utworzonych dla dzieci i zarządzaj nią z konta administratora.

- **Ustaw Kontrolę Rodzicielską na bieżącym koncie**

  Wybierz tę opcję, aby uruchomić Kontrolę Rodzicielską dla bieżącego konta Windows. To oznacza, że dla swoich dzieci nie będziesz musiał tworzyć osobnych kont. Reguły Kontroli Rodzicielskiej będą odnosić się do wszystkich osób, które używają bieżącego konta.

  W tym wypadku do ochrony ustawień Kontroli Rodzicielskiej potrzebne jest hasło.Możesz ustalić to teraz lub w późniejszym terminie z okna BitDefender.

- **Na razie pomiń konfigurację.**

  Wybierz tę opcję, aby skonfigurować tę funkcję w późniejszym terminie z okna BitDefender.

Kliknij **Dalej** aby kontynuować.

Zarządzanie siecią domową

Notatka

Krok ten pojawia się tylko wtedy, gdy do Moich narzędzi dodana została opcja Zarządzanie siecią domową.

Można wybrać jedną z trzech opcji:

- **Skonfiguruj ten komputer jako Serwer**

  Wybierz tę opcję, jeśli planujesz zarządzać z tego komputera PC produktami BitDefender na innych komputerach w sieci domowej.

  Aby dołączyć do sieci, musisz podać hasło.Wpisz hasło w podanych polach tekstowych i kliknij **Wyślij**.

- **Ustaw ten komputer jako klienta**

  Wybierz tę opcję, jeśli BitDefender będzie zarządzany z innego komputera w sieci domowej, na którym BitDefender jest uruchomiony.

  Aby dołączyć do sieci, musisz podać hasło.Wpisz hasło w podanych polach tekstowych i kliknij **Wyślij**.

- **Na razie pomiń konfigurację.**

  Wybierz tę opcję, aby skonfigurować tę funkcję w późniejszym terminie z okna BitDefender.

Kliknij **Dalej** aby kontynuować.

3.6. Krok 6 - Opcje pomocy technicznej

W tym miejscu można dostosować opcje pomocy i wsparcia technicznego:

- Włącz / wyłącz **Inteligentne wskazówki**.Inteligentne wskazówki to spersonalizowane wiadomości wyświetlane na pulpicie BitDefender, które pomagają w uzyskaniu lepszej wydajności pracy komputera.
- Potwierdź adres e-mail, którego będziesz używał w przypadku konieczności skontaktowania się z obsługą klienta BitDefender. Jeśli nie planujesz wykonywania tego za pomocą poczty elektronicznej, zaznacz odpowiednie pole.

3.7. Krok 7 - Potwierdzenie

W tym miejscu można przejrzeć wybraną konfigurację.

Domyślnie zaplanowano także dwa zadania:

- Pełne skanowanie uruchamiane jest tuż po zakończeniu instalacji.

  Zaleca się wykonanie dokładnego skanu, który wykryje wszelkie złośliwe oprogramowanie obecne w systemie.

- Skanowanie systemu zaplanowane jest co niedzielę o godzinie 2.00 w nocy.

  Zaleca się wykonanie przynajmniej jednego skanowania systemu na tydzień.Wybierz inny dzień i godzinę, jeśli harmonogram domyślny jest dla ciebie nieodpowiedni.Jeśli komputer jest wyłączony w momencie, kiedy ma odbyć się zaplanowane zadanie, zostanie ono przeprowadzone po jego następnym uruchomieniu.

Kliknij **Zakończ**.

3.8. Krok 8 - Zakończenie

Instalacja zbliża się do końca. Ustalane są finalne ustawienia i pobierane aktualizacje.

Po zakończeniu instalacji kreator zostanie automatycznie zamknięty.Jeśli w poprzednim kroku wybrano tę opcję, rozpocznie się pełne skanowanie.

Kreator konfiguracji wykryje sieć, do której jesteś podłączony i pozwoli ci ją sklasyfikować jako domową/biurową lub publiczną.

Notatka
Wymagane może być ponowne uruchomienie systemu.

4. Uaktualnianie ze Starszej Wersji BitDefender

Jeśli używasz wersji beta, 2008, 2009 lub 2010 BitDefender Internet Security 2011, możesz dokonać uaktualnienia do BitDefender Internet Security 2011.

Są dwa sposoby na wykonanie aktualizacji (upgrade):

- Zainstaluj BitDefender Internet Security 2011 bezpośrednio na starą wersję.Jeśli instalacja odbywa się bezpośrednio na wersji 2010, listy przyjaciół i spamerów oraz kwarantanna zostają zaimportowane automatycznie.
- W pierwszej kolejności należy usunąć poprzednią wersję, następnie uruchomić ponownie komputer i zainstalować nową wersję jak opisano w rozdziale *„Instalacja BitDefendera”* (p. 5).Nie zachowano żadnych ustawień programu.Użyj tej metody gdy inne zawiodą.

5. Naprawianie lub Usuwanie BitDefendera

Jeśli chcesz naprawić lub usunąć BitDefender Internet Security 2011, podążaj za ścieżką w menu startowym Windows: **Start → Programy → BitDefender 2011 → Napraw lub Usuń**.

Pojawi się kreator, który pomoże ci wykonać wybrane zadanie.

1. **Napraw lub Usuń**

   Wybierz działanie, które chcesz wykonać:

   - **Napraw** - aby zainstalować ponownie wszystkie składniki programu.
   - **Usuń** - aby usunąć zainstalowane składniki.

   Notatka
   Zalecamy wybrać **Usuń** aby dokonać czystej reinstalacji.

2. **Potwierdź działanie**

   Zanim klikniesz **Dalej**, aby potwierdzić tę czynność, zapoznaj się dokładnie z wyświetlonymi informacjami.

3. **Postęp**

   Poczekaj aż BitDefender zakończy wybraną operację.Zajmie to kilka minut.

4. **Zakończ**

   Wyniki są wyświetlone.

   Aby zakończyć proces, musisz ponownie uruchomić komputer. Kliknij **Uruchom ponownie**, aby natychmiast uruchomić komputer ponownie lub **Zakończ**, aby zamknąć okno i uruchomić komputer ponownie później.

Pierwsze Kroki

6. Przegląd

Po zainstalowaniu BitDefender Internet Security 2011 twój komputer jest chroniony przed wszystkimi rodzajami złośliwego oprogramowania (tzn. wirusami, oprogramowaniem szpiegującym i trojanami) i zagrożeń internetowych (hakerami, phishingiem i spamem).

Konfigurowanie ustawień BitDefender innych niż te, które zostały skonfigurowane podczas instalacji, nie jest konieczne.Możesz jednak wykorzystać ustawienia BitDefender, aby wyregulować i usprawnić swoją ochronę.

Od czasu do czasu należy otworzyć BitDefender i naprawić istniejące zagadnienia.Być może będziesz musiał skonfigurować niektóre komponenty BitDefender lub podjąć akcje prewencyjne aby ochronić komputer i swoje dane.Jeśli chcesz, możesz skonfigurować BitDefender aby nie powiadamiał cię o niektórych problemach.

Jeśli nie zarejestrowałeś produktu (włączając w to utworzenie konta BitDefender), pamiętaj aby to zrobić zanim darmowy okres testowy się skończy.Musisz utworzyć konto w ciągu 15 dni od zainstalowania BitDefendera (jeśli go zarejestrujesz za pomocą klucza licencyjnego, termin jest przedłużany do 30 dni).W przeciwnym wypadku, BitDefender nie będzie się aktualizował.Aby uzyskać więcej informacji na temat procesu rejestracji, przejdź do *„Rejestracja i Moje Konto”* (p. 50).

6.1. Otwieranie BitDefender

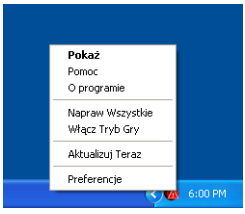
Aby przejść do głównego interfejsu BitDefender Internet Security 2011, użyj menu Start systemu Windows, kierując się do **Start → Wszystkie programy → BitDefender 2011 → BitDefender Internet Security 2011** lub szybciej, klikając dwa razy ikonę BitDefender w zasobniku systemowym na pasku zadań.

Więcej informacji na temat głównego okna aplikacji zawiera *„Główne okno aplikacji”* (p. 23).

6.2. Ikona w Zasobniku Systemowym

Aby sprawniej zarządzać całym programem, możesz skorzystać z ikony BitDefender w zasobniku systemowym.Jeżeli klikniesz dwukrotnie na tą ikonę otworzy się BitDefender. Dodatkowo po kliknięciu prawym klawiszem myszy, pojawi się menu kontekstowe które pozwala szybkie zarządzanie BitDefenderem.

- **Pokaż** - otwiera główny interfejs BitDefendera.
- **Pomoc** - otwiera plik pomocy, który w drobnych szczegółach wyjaśnia jak konfigurować i korzystać z BitDefender Internet Security 2011.
- **O programie** - otwiera okno, w którym możesz przeczytać o BitDefenderze i gdzie szukać pomocy jeśli zdarzy się coś niespodziewanego.
- **Napraw Wszystkie** - pomaga usunąć wszystkie problemy z zabezpieczeniami.Jeśli ta opcja jest niedostępna, nie ma żadnych problemów, które należałoby naprawić.Aby uzyskać więcej informacji, odwołaj się do *„Naprawianie”* (p. 40).



Ikona w Zasobniku

- **Włącz/Wyłącz Tryb Gry** - aktywuje/deaktywuje Tryb Gry.
- **Zaktualizuj Teraz** - uruchamia aktualizację.Pojawi się nowe okno w którym możesz obserwować status aktualizacji.
- **Preferencje** - otwiera okno, w którym można włączyć lub wyłączyć główne ustawienia produktu oraz ponownie skonfigurować profil użytkownika.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Ustawień Głównych”* (p. 43).

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

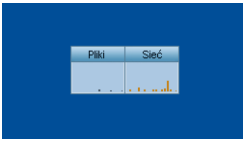
Czerwony trójkąt ze znakiem wykrzyknika: Krytyczne zagadnienia wpływające na bezpieczeństwo systemu. Wymagają natychmiastowej naprawy.
Litera G: Oprogramowanie działa w Trybie Gry.

Jeśli BitDefender nie działa, ikona w zasobniku systemowym jest szara .Dzieje się tak zazwyczaj kiedy klucz licencyjny wygasa. Może także wystąpić gdy usługi BitDefender nie odpowiadają lub inne błędy zakłócają normalną pracę BitDefendera.

6.3. Pasek Aktywności Skanera

Okienko czynności skanowania jest graficznym odzwierciedleniem wykonywanych czynności skanowania na twoim systemie.To małe okno jest domyślnie dostępne tylko w Widoku eksperta.

Zielone linie (**Pliki**) pokazują ilość przeskanowanych plików/sek w skali od 0 do 50.Pomarańczowy pasek w **Sieć** pokazuje ilość kilobitów (wysłanych oraz odebranych z Internetu) w każdej sekundzie, w skali od 0 do 100.



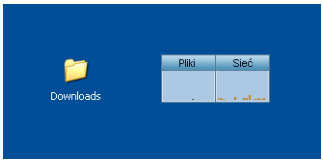
Pasek Aktywności Skanera

Notatka

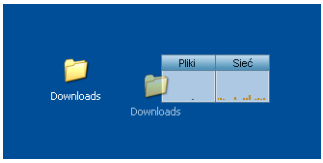
Pasek aktywności skanera powiadomi cię kiedy ochrona czasu rzeczywistego zostanie wyłączona przez wyświetlenie czerwonego krzyżyka na odpowiednim polu (**Pliki** lub **Sieć**).

6.3.1. Skanuj Pliki i Foldery

Możesz użyć Paska aktywności skanowania aby szybko skanować pliki lub foldery.Przeciągnij plik lub folder który chcesz przeskanować i upuść na **Pasek Aktywności Skanera** jak pokazano poniżej.



Przeciągnij Plik



Upuść Plik

Pojawi się Kreator skanowania antywirusowego i przeprowadzi cię przez proces skanowania.

Opcje skanowania. Opcje skanowania są skonfigurowane wcześniej tak, aby zapewnić najlepszą wykrywalność.Wszystkie zainfekowane pliki zostały rozpoznane, BitDefender spróbuje usunąć z nich szkodliwy kod. Jeśli to zawiedzie, kreator skanowania antywirusowego pozwoli na wybranie innych akcji, które zostaną podjęte na uszkodzonych plikach.Opcje skanowania są standardowe i nie możesz ich zmienić.

6.3.2. Zablokuj/Odblokuj Pasek Aktywności Skanera

Jeżeli nigdy więcej nie chcesz aby pokazywana była graficzna wizualizacja, po prostu kliknij prawy przyciski myszy i wybierz **Ukryj**.Aby odblokować pasek aktywności skanera, wykonaj następujące kroki:

1. Otwórz BitDefender.
2. W prawym górnym rogu okna kliknij **Opcje** i wybierz **Preferencje**.

3. W kategorii Ustawienia Ogólne użyj przełącznika odpowiadającego **Paskowi czynności skanowania**, aby go włączyć.
4. Kliknij **OK** aby zapisać i zastosować zmiany.

6.4. Automatyczne Wykrywanie Urządzeń

BitDefender automatycznie wykrywa, kiedy podłączasz przenośne urządzenia do swojego komputera i oferuje możliwość ich przeskanowania.Jest to zalecane, ze względu na możliwość zainfekowania komputera złośliwym oprogramowaniem.

Wykryte urządzenia są przyporządkowywane do jednej z tych kategorii:

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

Kiedy takie urządzenie zostanie wykryte, wyświetlane jest okno z alarmem.

Aby zeskanować urządzenie, kliknij **Tak**.Pojawi się Kreator skanowania antywirusowego i przeprowadzi cię przez proces skanowania.

Jeśli nie chcesz skanować urządzenia, kliknij **Nie**. W tym przypadku, mogą przydać się następujące opcje:

- **Nie pytaj mnie więcej o ten typ urządzenia** - BitDefender nie będzie oferował skanowania tego typu urządzeń, kiedy zostaną podłączone do komputera.
- **Zablokuj automatyczne wykrywanie urządzeń** - program nie będzie więcej pytał o skanowanie nowego urządzenia, kiedy zostanie podłączone do komputera.

Jeśli przypadkowo zablokowałeś automatyczne wykrywanie urządzeń i chcesz je odblokować, lub chcesz skonfigurować jego ustawienia, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **skanowania antywirusowego**.
3. Na liście zadań skanowania znajdź zadanie **Skanowanie urządzenia**.
4. Prawym przyciskiem myszy kliknij zadanie i wybierz **Właściwości**.Pojawi się nowe okno.
5. W zakładce **Podgląd** możesz skonfigurować opcje skanowania.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Ustawień Skanowania”* (p. 74).
6. W zakładce **Wykrywanie** możesz wybrać, które typy urządzeń mają być wykrywane.
7. Kliknij **OK** aby zapisać i zastosować zmiany.

7. Główne okno aplikacji

BitDefender Internet Security 2011 spełnia wymagania zaawansowanych użytkowników, jak i tych którzy swoją przygodę z komputerami dopiero zaczynają. Graficzny interfejs użytkownika jest tak zaprojektowany, aby mogli z niego korzystać wszyscy użytkownicy.

Możesz wybrać jeden z trzech trybów pracy interfejsu użytkownika, w zależności od twoich umiejętności korzystania z komputera i wcześniejszego doświadczenia z pracy z produktami BitDefender.

Widok Podstawowy

Odpowiedni dla początkujących oraz osób, które chcą chronić swój komputer bez dodatkowych interakcji z programem.

Jedyne co musisz zrobić, to naprawić zagadnienia dotyczące bezpieczeństwa, wskazywane przez BitDefender. Umożliwia to intuicyjny kreator, który prowadzi użytkownika krok po kroku, przez proces rozwiązywania problemów.Dodatkowo, możesz przeprowadzić podstawowe zadania, takie jak aktualizacja plików BitDefendera i sygnatur wirusów lub skanowanie komputera.

Widok średniozaawansowany

Przeznaczony dla użytkowników o przeciętnych umiejętnościach korzystania z komputerów, interfejs ten rozszerza zakres operacji, które można wykonać w Widoku podstawowym.

Możesz naprawić zagadnienia osobno i wybrać które z nich mają być monitorowane.Dodatkowo, możesz zdalnie zarządzać oprogramowaniem BitDefender zainstalowanym na innych komputerach w twojej sieci domowej.

Widok eksperta

Przeznaczony dla osób posiadających techniczną wiedzę, ten tryb pozwala w dogłębny sposób skonfigurować każdy moduł BitDefender.Możesz także skorzystać ze wszystkich udostępnionych zadań aby chronić swój komputer i dane.

Tryb wyświetlania wybierany jest podczas instalacji.

Zmiana trybu wyświetlania:

1. Otwórz BitDefender.
2. W prawym górnym rogu okna kliknij przycisk **Opcje**.
3. Wybierz tryb wyświetlania z menu.

7.1. Widok Podstawowy

Jeśli jesteś początkującym użytkownikiem komputera, najlepszym wyborem dla ciebie jest interfejsu użytkownika Widok podstawowy.Ten tryb jest prosty i wymaga minimalnej interakcji ze strony użytkownika.

Okna podzielono na trzy główne obszary:

Obszar stanu
: Informacje o stanie widoczne są w lewej części okna.

Obszar Chroń swój Komputer
: W tym miejscu można wykonać działania niezbędne do zarządzania ochroną.

Obszar Pomocy
: W tym miejscu można dowiedzieć się, w jaki sposób należy używać BitDefender Internet Security 2011 i uzyskać pomoc.

Przycisk **Opcje**, który znajduje się w prawym górnym rogu okna, pozwala zmieniać tryb wyświetlania interfejsu użytkownika oraz konfigurować główne ustawienia programu.

W prawym dolnym rogu okna, możesz znaleźć kilka przydatnych linków.

Link	Opis
Informacje o licencji	Otwiera okno, w którym można przejrzeć aktualne informacje dotyczące klucza licencji oraz zarejestrować produkt za pomocą nowego klucza.
Pokaż Dzienniki	Pozwala tobie zobaczyć szczegółową historię wszystkich zadań przeprowadzonych przez BitDefendera na twoim systemie.
Pomoc i wsparcie	Kliknij to łącze, jeśli potrzebujesz pomocy przy BitDefender.
?	Umożliwia dostęp do pliku pomocy który pokazuje jak korzystać z BitDefendera.

7.1.1. Pole Stanu

Informacje o stanie widoczne są w lewej części okna.

- **Stan Zabezpieczeń** informuje użytkownika o zagadnieniach mogących wpływać niekorzystnie na bezpieczeństwo komputera i pomaga je naprawić.Klikając na **Napraw Wszystkie** uruchomisz kreator pozwalający na usunięcie wszystkich problemów dotyczących bezpieczeństwa twojego komputera.Aby uzyskać więcej informacji, odwołaj się do *„Naprawianie”* (p. 40).
- **Status licencji** wyświetla liczbę dni pozostałych do wygaśnięcia licencji.Jeśli używasz wersji testowej lub twoja licencja wkrótce wygaśnie, możesz kliknąć **Kup**

teraz, aby zakupić klucz licencji.Aby uzyskać więcej informacji, odwołaj się do *„Rejestracja i Moje Konto”* (p. 50).

7.1.2. Obszar Chroń swój Komputer

W tym miejscu można wykonać działania niezbędne do zarządzania ochroną.

Trzy przyciski są dostępne:

- **Bezpieczeństwo** zapewnia dostęp do skrótów zadań i ustawień.
- **Aktualizuj teraz** pozwala zaktualizować sygnatury wirusów i pliki produktów BitDefender.Pojawi się nowe okno w którym możesz obserwować status aktualizacji.Jeśli wykryto aktualizacje, są one automatyczne pobierane i instalowane na komputerze.
- **Moje narzędzia** pozwalają tworzyć skróty do ulubionych zadań i ustawień.

Aby wykonać zadanie lub skonfigurować ustawienia, kliknij odpowiedni przycisk i wybierz z menu dane narzędzie.Aby dodać lub usunąć skróty, kliknij odpowiedni przycisk i wybierz **Więcej opcji**.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

7.1.3. Obszar Pomocy

W tym miejscu można dowiedzieć się, w jaki sposób należy używać BitDefender Internet Security 2011 i uzyskać pomoc.

Inteligentne wskazówki to zabawny i prosty sposób poznania najlepszych metod ochrony komputera i użytkowania BitDefender Internet Security 2011.

Jeśli potrzebujesz pomocy, w polu **Pomoc i wsparcie techniczne** wpisz słowo kluczowe lub pytanie i kliknij **Wyszukaj**.

7.2. Widok średniozaawansowany

Przeznaczony dla użytkowników o przeciętnych umiejętnościach korzystania z komputerów. Widok średniozaawansowany jest prostym interfejsem, który zapewnia dostęp do wszystkich modułów na poziomie podstawowym. Będziesz musiał śledzić ostrzeżenia i alarmy krytyczne oraz naprawiać niepożądane zagadnienia.

Okno Widoku średniozaawansowanego podzielono na kilka zakładek.

Panel
: Pulpit pozwala w łatwy sposób monitorować i zarządzać ochroną.

Zabezpieczenia
: Wyświetla stan ustawień zabezpieczeń i pomaga naprawić wykryte zagadnienia.Możesz uruchamiać zadania dotyczące ochrony lub konfigurować ustawienia zabezpieczeń.

Sieć

Pokazuje strukturę domowej sieci BitDefendera.Tutaj możesz wykonać różne akcje aby skonfigurować i zarządzać produktami BitDefender zainstalowanymi w twojej domowej sieci.W ten sposób, możesz zarządzać bezpieczeństwem twojej domowej sieci z jednego komputera.

Przycisk **Opcje**, który znajduje się w prawym górnym rogu okna, pozwala zmieniać tryb wyświetlania interfejsu użytkownika oraz konfigurować główne ustawienia programu.

W prawym dolnym rogu okna, możesz znaleźć kilka przydatnych linków.

Link	Opis
Informacje o licencji	Otwiera okno, w którym można przejrzeć aktualne informacje dotyczące klucza licencji oraz zarejestrować produkt za pomocą nowego klucza.
Pokaż Dzienniki	Pozwala tobie zobaczyć szczegółową historię wszystkich zadań przeprowadzonych przez BitDefendera na twoim systemie.
Kup/Odnów	Pozwala zakupić klucz licencji dla produktu BitDefender Internet Security 2011.
Pomoc i wsparcie	Kliknij to łącze, jeśli potrzebujesz pomocy przy BitDefender.
	Umożliwia dostęp do pliku pomocy który pokazuje jak korzystać z BitDefendera.

7.2.1. Panel

Pulpit pozwala w łatwy sposób monitorować i zarządzać ochroną.

Panel składa się z następujących sekcji:

- **Szczegóły statusu** wskazują stan każdego z głównych modułów za pomocą zdań i jednej z następujących ikon:

  Zielone kółko: Nie ma zagadnień wpływających na bezpieczeństwo komputera.Twój komputer i dane są chronione.

  Czerwone kółko z wykrzyknikiem: Są zagadnienia, które wpływają na bezpieczeństwo twojego komputera.Krytyczne zagadnienia wymagają twojej natychmiastowej uwagi. Nie-krytyczne zagadnienia także powinny zostać jak najszybciej rozwiązane.

  Szare kółko z wykrzyknikiem: Aktywność komponentów tego modułu nie jest śledzona, nie ma więc żadnej informacji na temat jego stanu zabezpieczeń.Mogą istnieć pewne zagadnienia związane z tym modułem.

Kliknij na nazwę modułu aby zobaczyć więcej szczegółów na temat jego stanu oraz skonfiguruj śledzenie stanu dla jego komponentów.

- **Status licencji** wyświetla liczbę dni pozostałych do wygaśnięcia licencji.Jeśli używasz wersji testowej lub twoja licencja wkrótce wygaśnie, możesz kliknąć **Kup teraz**, aby zakupić klucz licencji.Aby uzyskać więcej informacji, odwołaj się do *„Rejestracja i Moje Konto”* (p. 50).
- **Moje narzędzia** pozwalają tworzyć skróty do ulubionych zadań i ustawień.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).
- **Inteligentne wskazówki** to zabawny i prosty sposób poznania najlepszych metod ochrony komputera i użytkowania BitDefender Internet Security 2011.

7.2.2. Zabezpieczenia

Zakładka Bezpieczeństwo pozwala zarządzać bezpieczeństwem komputera i danych.

„Pole Stanu” (p. 27)
„Szybkie zadania” (p. 28)

Pole Stanu

Pole stanu zawiera kompletną listę monitorowanych komponentów bezpieczeństwa i ich aktualny stan.Dzięki monitorowaniu każdego modułu zabezpieczeń, BitDefender poinformuje użytkownika nie tylko wtedy, gdy trzeba skonfigurować ustawienia mogące wpływać na bezpieczeństwo komputera, ale także gdy zapomni on o ważnych zadaniach.

Obecny stan tego komponentu jest wskazywany poprzez określone zdania i jedną z tych ikon:

Zielone kółko: Brak zagadnień dotyczących tego komponentu.
Czerwone kółko z wykrzyknikiem: Są zagadnienia dotyczące tego komponentu.

Kliknij na przycisk **Napraw** przy odpowiednim zdaniu aby naprawić zgłaszane zagadnienie.Jeżeli jakiś problem nie naprawi się od razu, skorzystaj z kreatora.

Konfigurowanie składników, które mają podlegać monitorowaniu:

1. Kliknij **Dodaj/Edytuj listę**.
2. Aby wyłączyć monitorowanie określonego elementu, użyj odpowiedniego przełącznika.
3. Aby zapisać zmiany, kliknij **Zakończ** i zamknij okno.

WAŻNE
Aby mieć pewność że twój system jest w pełni chroniony, włącz śledzenie wszystkich komponentów i napraw wszystkie zagadnienia.

Szybkie zadania

Tutaj możesz odnaleźć skróty do najważniejszych zadań bezpieczeństwa:

- **Zaktualizuj Teraz** - uruchamia aktualizację.
- **Pełne Skanowanie** - uruchamia standardowe skanowanie komputera (z wyłączeniem archiwów). Aby uzyskać dodatkowe zadania skanowania na żądanie, kliknij strzałkę na tym przycisku i wybierz inne zadanie skanowania.
- **Własne Skanowanie** - uruchamia kreator, który pozwala tworzyć i uruchamiać własne zadania skanowania.
- **Skanowanie podatności** - uruchamia kreator który sprawdza czy twój system jest podatny na zagrożenia i posiada luki w zabezpieczeniach, a następnie pomaga je naprawić.
- **Konfigurowanie Zapory Sieciowej** - otwiera okno, w którym można przejrzeć i skonfigurować ustawienia Zapory Sieciowej.Aby uzyskać więcej informacji, odwołaj się do *„Zapora Sieciowa”* (p. 125).

7.2.3. Sieć

Tutaj możesz wykonać różne akcje aby skonfigurować i zarządzać produktami BitDefender zainstalowanymi w twojej domowej sieci.W ten sposób, możesz zarządzać bezpieczeństwem twojej domowej sieci z jednego komputera.

Aby uzyskać więcej informacji, odwołaj się do *„Sieć Domowa”* (p. 148).

7.3. Widok eksperta

Widok eksperta zapewnia dostęp do każdego składnika BitDefender. W tym miejscu można szczegółowo skonfigurować BitDefender.

Notatka

Widok eksperta przeznaczony jest dla użytkowników o ponadprzeciętnych umiejętnościach korzystania z komputerów, którzy znają zagrożenia, na jakie wystawiony jest komputer oraz wiedzą, w jaki sposób pracują programy zapewniające ochronę.

Po lewej stronie okna jest menu zawierające wszystkie moduły zabezpieczeń.Każdy moduł ma jedną lub więcej zakładek gdzie możesz skonfigurować odpowiadające im ustawienia zabezpieczeń lub wykonać zadania bezpieczeństwa i administracyjne.Następująca lista krótko opisuje każdy moduł.Aby uzyskać więcej informacji, odwołaj się do „Konfiguracja i zarządzanie” (p. 54) części podręcznika użytkownika.

Ogólne

Pozwala otworzyć ogólne ustawienia zobaczeniu interfejsu oraz szczegółowych informacji o systemie.

Antywirus
Pozwala tobie na szczegółowe skonfigurowanie ochrony antywirusowej oraz operacji skanowania, aby ustawić wyjątki oraz skonfigurować moduł kwarantanny.Tutaj możesz także skonfigurować ochronę antyphishingową oraz Asystenta wyszukiwania.

Antyspam
Pozwala zachować skrzynkę poczty przychodzącej wolną od spamu i dokładnie skonfigurować ustawienia antyspamowe.

Kontrola Rodzcielska
Pozwala tobie chronić dzieci przed niewłaściwymi treściami korzystając z ustawionych reguł dostępu.

Kontrola prywatności
Pozwala tobie zapobiec kradzieży danych z twojego komputera oraz chroni twoją prywatność kiedy korzystasz z internetu.

Zapora Sieciowa
Pozwala chronić twój komputer przed nieautoryzowanymi próbami połączeń. Jest to bardzo podobne do straży przy bramie - program będzie pilnował twoich połączeń internetowych i decydował kto może wejść, a kto zostanie zablokowany.

Podatności
Pozwala tobie bieżące aktualizowanie najważniejszego oprogramowania na komputerze.

Szyfrowanie
Pozwala tobie szyfrowanie komunikacji przez Yahoo oraz Windows Live (MSN) Messenger

Tryb Gry/Laptopa
Pozwala tobie na ograniczenie zaplanowanych zadań BitDefendera gdy twój laptop pobiera zasilanie z baterii oraz eliminuje wszelkie alarmy oraz wyskakujące okienka podczas grania.

Sieć Domowa
Pozwala tobie na skonfigurowanie i zarządzanie kilkoma komputerami w sieci domowej.

Aktualizacje
Pozwala tobie na uzyskanie najnowszych aktualizacji, zaktualizować produkt oraz szczegółowo skonfigurować proces aktualizacji.

Rejestracja
Pozwala na zarejestrowanie BitDefender Internet Security 2011, zmianę klucza licencyjnego i utworzenie konta BitDefender.

Przycisk **Opcje**, który znajduje się w prawym górnym rogu okna, pozwala zmieniać tryb wyświetlania interfejsu użytkownika oraz konfigurować główne ustawienia programu.

W prawym dolnym rogu okna, możesz znaleźć kilka przydatnych linków.

Link	Opis
Informacje o licencji	Otwiera okno, w którym można przejrzeć aktualne informacje dotyczące klucza licencji oraz zarejestrować produkt za pomocą nowego klucza.
Pokaż Dzienniki	Pozwala tobie zobaczyć szczegółową historię wszystkich zadań przeprowadzonych przez BitDefendera na twoim systemie.
Kup/Odnów	Pozwala zakupić klucz licencji dla produktu BitDefender Internet Security 2011.
Pomoc i wsparcie	Kliknij to łącze, jeśli potrzebujesz pomocy przy BitDefender.
?	Umożliwia dostęp do pliku pomocy który pokazuje jak korzystać z BitDefendera.

8. Moje narzędzia

Używając BitDefender w Widoku podstawowym lub średniozaawansowanym, możesz dostosować pulpit poprzez dodanie skrótów do zadań i ustawień, które uważasz za najważniejsze.W ten sposób, bez konieczności przełączania się do bardziej zaawansowanych trybów wyświetlania interfejsu, można szybko uzyskać dostęp do często używanych funkcji oraz ustawień zaawansowanych.

W zależności od wybranego trybu wyświetlania interfejsu użytkownika skróty dodawane do Moich narzędzi dostępne są jako:

Widok Podstawowy
: W obszarze Chroń swój komputer kliknij Moje narzędzia.Pojawi się menu.Kliknij skrót, aby uruchomić odpowiednie narzędzie.

Widok średniozaawansowany
: Skrót pojawi się w Moich narzędziach.Kliknij skrót, aby uruchomić odpowiednie narzędzie.

Aby otworzyć okno, z którego można wybrać skróty pojawiające się w Moich narzędziach, postępuj zgodnie z poleceniami:

Widok Podstawowy
: W obszarze Chroń swój Komputer kliknij Moje narzędzia i wybierz **Więcej opcji**.

Widok średniozaawansowany
: Kliknij jeden z przycisków w Moich narzędziach lub łącze **Konfiguracja Moich Narzędzi**.

Użyj przełączników, żeby wybrać narzędzia, które mają zostać dodane do Moich narzędzi.Można wybrać dowolną z następujących kategorii narzędzi.

- **Zadania Skanowania**

  Aby przeskanować system pod kątem zagrożeń bezpieczeństwa, dodaj regularnie używane zadania.

Zadanie Skanowania	Opis
Głębokie Skanowanie	Skanuje cały system.W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.
Pełne Skanowanie	Skanuje cały system wyłączając archiwa.W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów.
Szybkie skanowanie	Do wykrywania w systemie złośliwego oprogramowania Szybkie Skanowanie wykorzystuje

Zadanie Skanowania	Opis
	skanowanie w chmurze.Wykonanie Szybkiego Skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.
Skanowanie Użytkownika	Uruchamia kreatora, który pozwala utworzyć własne zadanie skanowania.
Skanuj Moje Dokumenty	Użyj tego zadania do skanowania ważnych folderów aktualnego użytkownika: `Moje Dokumenty`, `Pulpit` oraz `Autostart`. To zapewni bezpieczeństwo dokumentów, miejsca pracy oraz uruchamianych aplikacji.
Ustaw harmonogram Mojego skanowania	Przenosi cię do okna ustawień Antywirusa, w którym możesz dostosować zadania skanowania na żądanie.

Więcej informacji na temat zadań skanowania zawiera *„Zarządzanie Istniejącymi Zadaniami Skanowania”* (p. 71).

- **Ustawienia**

  Dodaj skróty do ustawień BitDefender, które chcesz skonfigurować:

Ustawienia	Opis
Ustawienia Antywirusa	Skonfiguruj moduł Antywirusa. Więcej informacji zawiera *„Ochrona antywirusowa”* (p. 59).
Konfiguruj Zaporę sieciową	Skonfiguruj moduł Zapory Sieciowej. Więcej informacji zawiera *„Zapora Sieciowa”* (p. 125).
Kontrola Rodzcielska	Skonfiguruj moduł Kontroli Rodzicielskiej. Więcej informacji zawiera *„Kontrola Rodzcielska”* (p. 99).
Tryb Gry	Włącz/wyłącz Tryb Gry. Więcej informacji zawiera *„Tryb Gry”* (p. 143).
Tryb Laptopa	Włącz/wyłącz Tryb Laptopa. Więcej informacji zawiera *„Tryb Laptopa”* (p. 146).
Aktualizuj Teraz	Uruchom aktualizację BitDefender. Więcej informacji zawiera *„Aktualizacje”* (p. 152).
Zobacz & Napraw Wszystkie Zagadnienia	Otwórz kreatora, który pomoże ci naprawić wszystkie zagadnienia bezpieczeństwa, mające wpływ na system. Więcej informacji zawiera *„Naprawianie”* (p. 40).

- **Pomoc & Wsparcie**

  Wejdź do działu pomocy. Więcej informacji zawiera „Skontaktuj się z nami bezpośrednio za pośrednictwem produktu BitDefender.” (p. 196).

9. Alarmy i wyskakujące okna

BitDefender używa wyskakujących okien i alarmów, by informować o swoich działaniach lub specjalnych zdarzeniach mogących cię zainteresować oraz monitować o podjęcie działań, gdy jest to konieczne.Niniejszy rozdział przedstawia wyskakujące okna i alarmy BitDefender, z którymi możesz się zetknąć.

Wyskakujące okienka to małe okna, które czasowo wyświetlane są na ekranie, w celu poinformowania cię o różnych zdarzeniach dotyczących BitDefender. Może to być skanowanie wiadomości e-mail, logowanie nowego komputera do twojej sieci bezprzewodowej, dodanie reguły zapory sieciowe, itp.Gdy pojawi się okno, konieczne będzie kliknięcie przycisku **OK** lub przynajmniej łącza.

Alarmy to większe okna monitujące o podjęcie działania w związku z czymś bardzo ważnym (na przykład wykryciem wirusa).Poza oknami alarmu, możesz otrzymywać wiadomości e-mail, wiadomości komunikatorów oraz alarmy dotyczące stron internetowych.

Wyskakujące okna i alarmy BitDefender obejmują:

- Alerty antywirusowe
- Alarmy Aktywnej Kontroli Wirusowej
- Alarmy Wykrywania Urządzeń
- Wyskakujące okna i alarmy Zapory Sieciowej
- Strony internetowe ostrzegające przed phishingiem
- Wiadomości z ostrzeżeniami Kontroli Rodzicielskiej
- Alerty kontroli prywatności

9.1. Alerty antywirusowe

BitDefender zapewnia ochronę przed różnymi rodzajami złośliwego oprogramowania, takimi jak wirusy, oprogramowanie szpiegujące i rootkity.W przypadku wykrycia wirusa lub innego złośliwego oprogramowania BitDefender wykona określone działanie względem zainfekowanego pliku i poinformuje cię o tym za pomocą okna alarmu.

Możesz zobaczyć nazwę wirusa, ścieżkę dostępu do zainfekowanego pliku oraz działanie wykonane przez BitDefender.

Kliknij **OK** aby zamknąć okno.

WAŻNE

W przypadku wykrycia wirusa najlepiej przeskanować jest cały komputer, aby wykluczyć obecność innych wirusów.Aby uzyskać więcej informacji, odwołaj się do *„Jak skanować pliki i foldery?”* (p. 157).
Jeśli wirus nie został zablokowany, zapoznaj się z informacjami w *„Usuwanie Złośliwego Oprogramowania z Systemu”* (p. 186).

9.2. Alarmy Aktywnej Kontroli Wirusowej

Aktywna Kontrola Wirusowa może zostać skonfigurowana tak, alarmowała użytkownika i pytała o podjęcie działania kiedy jakaś aplikacja chce przeprowadzić potencjalnie niebezpieczną akcję.

Jeśli korzystasz z interfejsu pracującego w trybie Widok podstawowy lub Widok średniozaawansowany, o każdym zablokowaniu potencjalnie szkodliwej aplikacji przez moduł Aktywnej ochrony wirusowej będziesz informowany przez wyświetlające się okno.Jeśli korzystasz z Widoku eksperta, w przypadku, gdy aplikacja zacznie przejawiać cechy złośliwego oprogramowania, za pośrednictwem okna alarmu zostaniesz poproszony o podjęcie działania.

Jeżeli znasz i ufasz wykrytej aplikacji, kliknij **Zezwól**.

Jeżeli chcesz natychmiast zamknąć aplikacje, kliknij **OK**.

Jeśli przed dokonaniem wyboru zaznaczysz pole **Pamiętaj wybraną akcję dla tej aplikacji**, BitDefender będzie wykonywał w przyszłości tę samą operację w przypadku zaatakowania tej aplikacji.Reguła, która została dodana będzie widoczna w oknie konfiguracyjnym Aktywnej Kontroli Wirusowej.

9.3. Alarmy Wykrywania Urządzeń

BitDefender automatycznie wykrywa, kiedy podłączasz przenośne urządzenia do swojego komputera i oferuje możliwość ich przeskanowania.Jest to zalecane, ze względu na możliwość zainfekowania komputera złośliwym oprogramowaniem.

Wykryte urządzenia są przyporządkowywane do jednej z tych kategorii:

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

Kiedy takie urządzenie zostanie wykryte, wyświetlane jest okno z alarmem.

Aby zeskanować urządzenie, kliknij **Tak**.Pojawi się kreator skanera antywirusowego i poprowadzi Cię przez proces skanowania.

Jeśli nie chcesz skanować urządzenia, kliknij **Nie**. W tym przypadku, mogą przydać się następujące opcje:

- **Nie pytaj mnie więcej o ten typ urządzenia** - BitDefender nie będzie oferował skanowania tego typu urządzeń, kiedy zostaną podłączone do komputera.
- **Zablokuj automatyczne wykrywanie urządzeń** - program nie będzie więcej pytał o skanowanie nowego urządzenia, kiedy zostanie podłączone do komputera.

Jeśli przypadkowo zablokowałeś automatyczne wykrywanie urządzeń i chcesz je odblokować, lub chcesz skonfigurować jego ustawienia, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **skanowania antywirusowego**.
3. Na liście zadań skanowania znajdź zadanie **Skanowanie urządzenia**.
4. Prawym przyciskiem myszy kliknij zadanie i wybierz **Właściwości**.Pojawi się nowe okno.
5. W zakładce **Podgląd** możesz skonfigurować opcje skanowania.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Ustawień Skanowania”* (p. 74).
6. W zakładce **Wykrywanie** możesz wybrać, które typy urządzeń mają być wykrywane.
7. Kliknij **OK** aby zapisać i zastosować zmiany.

9.4. Wyskakujące okna i alarmy Zapory Sieciowej

Zapora Sieciowa używa wyskakujących okien, aby informować o różnych zdarzeniach związanych z połączeniem sieciowym (na przykład, gdy do sieci Wi-Fi podłączony zostaje nowy komputer, gdy nowa aplikacja uzyskuje zezwolenie na dostęp do Internetu lub gdy skanowanie portów zostaje zablokowane).Te wyskakujące okna mogą być bardzo przydatne w wykrywaniu prób włamań oraz zabezpieczaniu się przed zagrożeniami sieciowymi.

Jeśli korzystasz z Widoku eksperta, a nieznana aplikacja próbuje połączyć się z Internetem, za pośrednictwem okna alarmu otrzymasz monit o podjęcie działania.

Możesz zobaczyć: aplikacje która próbuje uzyskać dostęp do Internetu, protokół, ścieżkę do pliku tej aplikacji, przeznaczenie, oraz port na którym aplikacja próbuje się połączyć.

Kliknij **Zezwól** by zezwolić na cały ruch (przychodzący i wychodzący) generowany przez tę aplikację od lokalnego hosta do każdego adresu, przez podany protokół IP i wszystkie inne porty. Jeśli klikniesz **Zablokuj**, aplikacja nie otrzyma dostępu do Internetu przez podany protokół IP.

WAŻNE

Zezwól przychodzącym próbom połączenia tylko z adresów IP albo domen którym w pełni ufasz.

Zgodnie z twoją odpowiedzią, reguła zostanie utworzona, zastosowana i umieszczona w tabeli. Następnym razem gdy aplikacja spróbuje się połączyć, ta reguła zostanie domyślnie zastosowana.

Jeśli korzystasz z Widoku podstawowego lub średniozaawansowanego, próba nawiązania połączenia zostanie automatycznie zablokowana.

9.5. Alarmy antyphishingowe

Jeśli ochrona antyphishingowa jest włączona, BitDefender alarmuje, gdy próbujesz odwiedzić stronę, która może być skonfigurowana z myślą o kradzieży informacji osobistych.Zanim przejdziesz na taką stronę internetową, BitDefender zablokuje ją i wyświetli zamiast niej ogólną stronę alarmu.

W pasku adresu przeglądarki internetowej sprawdź adres strony.Wyszukaj wskazówki sugerujące, że ta strona internetowa jest używana do phishingu.Jeśli adres internetowy jest podejrzany, zaleca się, aby go nie otwierać.

Oto kilka wskazówek, które mogą okazać się przydatne:

- Jeśli wpisałeś adres dozwolonej witryny internetowej, sprawdź, czy jest on prawidłowy. Jeśli nie jest, wpisz go ponownie i przejdź na tę stronę.
- Jeśli kliknąłeś łącze w wiadomości e-mail lub komunikatora, sprawdź, od kogo pochodzi. Jeśli nadawca jest nieznany, jest to prawdopodobnie próba phishingu. Jeśli znasz nadawcę, powinieneś sprawdzić, czy osoba ta rzeczywiście wysłała to łącze.
- Jeśli dotarłeś do tej strony internetowej przeglądając Internet, sprawdź stronę internetową, na której znalazłeś to łącze (kliknij przycisk Cofnij w swojej przeglądarce internetowej).

Jeśli chcesz zobaczyć daną stronę internetową, kliknij odpowiednie łącze, aby wykonać jedną z następujących operacji:

- **Pokaż tę stronę internetową tylko tym razem.** Nie ma żadnego ryzyka, o ile na stronę internetową nie są wysyłane żadne informacje.Jeśli dana strona internetowa jest legalna, możesz dodać ją do Białej listy (kliknij Pasek antyphisingowy BitDefender i wybierz **Dodaj do Białej listy**).
- **Dodaj stronę internetową do Białej listy.** Od razu wyświetlona zostanie niniejsza strona internetowa i BitDefender nie będzie już więcej o tym informował.

WAŻNE

Do Białej listy dodawaj tylko strony internetowe, którym w pełni ufasz (na przykład stronę swojego banku, znane sklepy internetowe, itp).BitDefender nie sprawdza stron internetowych pod kątem phishingu względem Białej listy.

Korzystając z paska narzędziowego BitDefender, znajdującego się w przeglądarce internetowej, możesz zarządzać ochroną antyphishingową i Białą listą.Aby uzyskać więcej informacji, odwołaj się do *„Zarządzanie Ochroną antyphishingową BitDefender w programach Internet Explorer i Firefox”* (p. 83).

9.6. Wiadomości z ostrzeżeniami Kontroli Rodzicielskiej

Możesz skonfigurować Kontrole Rodzicielską aby blokowała:

- Nieodpowiednie strony internetowe.
- dostęp do Internetu w podanych okresach czasu (np. gdy jest czas na odrabianie lekcji).
- Strony internetowe, wiadomości e-mail oraz wiadomości IM które zawierają podane w regułach kontroli rodzicielskiej słowa kluczowe.
- Aplikacje takie jak gry, komunikatory, programy do udostępniania plików i wiele innych.
- Wiadomości odbierane od kontaktów IM innych niż wcześniej dozwolone.

Użytkownik informowany jest o zablokowaniu działania poprzez określoną wiadomość z ostrzeżeniem (na przykład standardową stronę internetową z ostrzeżeniem, wiadomość e-mail lub wiadomość komunikatora).Użytkownik otrzymuje szczegółowe informacje, tak aby wiedział, dlaczego dane działanie zostało zablokowane.

9.7. Alerty kontroli prywatności

Kontrola prywatności oferuje zaawansowanym użytkownikom dodatkowe funkcje chroniące ich prywatność.Jeśli postanowisz włączyć którykolwiek z tych składników, poprzez określone okna alarmów będziesz monitowany o podjęcie działań:

- Kontrola Rejestru – pyta o Twoją zgodę za każdym razem, gdy jakiś program chce wprowadzić zmiany w rejestrze aby być uruchamianym przy starcie Windows.
- Kontrola Ciasteczek - pyta o Twoją zgodę za każdym razem, gdy nowa strona chce ustawić pliki ciasteczek.
- Kontrola Skryptów - pyta o Twoją zgodę za każdym razem, gdy strona próbuje uruchomić skrypt lub inną aktywną zawartość.

9.7.1. Alarmy rejestru

Jeśli włączysz Kontrolę rejestru, będziesz monitowany o wydanie zezwolenia przy każdej próbie zmodyfikowania rejestru przez nowy program, próbujący uruchomiać się przy starcie systemu Windows.

Możesz zobaczyć program który próbuje zmodyfikować rejestr Windows.

Notatka

BitDefender zwykle będzie cię ostrzegał, kiedy instalować będziesz nowe programy, które wymagają włączenia po następnym uruchomieniu twojego komputera. W większości przypadków programy te są godne zaufania.

Jeśli nie rozpoznajesz tego programu i wygląda on podejrzenie, kliknij **Blokuj** aby zabronić mu zmianę rejestru.W przeciwnym razie, kliknij **Zezwól** - aby zezwolić na modyfikacje.

W zależności od twojej odpowiedzi reguła jest tworzona w tabeli reguł.To same działanie jest stosowane kiedy ten program próbuje modyfikować rejestr.

Aby uzyskać więcej informacji, odwołaj się do „*Kontrola rejestru*” (p. 121).

9.7.2. Alarmy skryptów

Jeśli włączysz Kontrolę Skryptów, będziesz proszony o zgodę za każdym razem, gdy nowa witryna internetowa będzie próbowała uruchomić skrypt lub inną zawartość aktywną.

Możesz obejrzeć nazwę źródła.

Kliknij **Tak** lub **Nie** a reguła zostanie stworzona, dodana i wyświetlona w tabeli reguł.Ta sama operacja będzie stosowana automatycznie za każdym razem, gdy dana witryna będzie próbowała uruchomić zawartość aktywną.

Notatka
Jeśli zablokujesz aktywną zawartość, niektóre strony internetowe mogą nie być wyświetlane w prawidłowy sposób.

Aby uzyskać więcej informacji, odwołaj się do „*Kontrola Skryptów*” (p. 123).

9.7.3. Alarmy ciasteczek

Jeśli jest włączona, Kontrola Ciasteczek będzie monitować o zgodę za każdym razem, gdy nowy witryna internetowa będzie próbowała ustanowić lub zażądać ciasteczka.

Możesz obejrzeć nazwę aplikacji, która próbuje przesłać plik ciasteczka.

Kliknij **Tak** lub **Nie** a reguła zostanie stworzona, dodana i wyświetlona w tabeli reguł.Ta sama operacja będzie stosowana automatycznie za każdym razem, gdy połączysz się z odpowiednią witryną.

Aby uzyskać więcej informacji, odwołaj się do „*Kontrola Ciasteczek*” (p. 122).

10. Naprawianie

BitDefender używa systemu śledzenia zagadnień aby wykryć i poinformować o problemach mogących mieć negatywny wpływ na bezpieczeństwo danych i komputera. Domyślnie, monitorowane są tylko grupy zagadnień uważanych za najważniejsze. Możesz także skonfigurować, jeśli potrzebujesz, wyświetlanie powiadomień dotyczących tylko konkretnych zagadnień.

Oto w jaki sposób wyświetlane są informacje o istniejących zagadnieniach:

- Nad ikoną BitDefender w zasobniku wyświetlony zostaje specjalny symbol wskazujący zagadnienia będące w trakcie rozwiązywania.Dodatkowo, jeśli przesuniesz kursor nad ikonę, pojawi się okienko z potwierdzeniem istnienia pewnych zagadnień.
- Kiedy otworzysz BitDefender, pole Stan Bezpieczeństwa będzie wskazywać na liczbę zagadnień, które wpływają na bezpieczeństwo systemu.
  - W Widoku podstawowym stan bezpieczeństwa wyświetlony jest w lewej części okna.
  - Aby sprawdzić status bezpieczeństwa, w Widoku eksperta przejdź do **Ogólne > Pulpit**.

10.1. Kreator Naprawiania Zagadnień

Najprostszym sposobem usunięcia istniejących zagadnień jest wykonanie poleceń **Kreator Naprawiania Zagadnień**.Aby otworzyć ten kreator, wykonaj następujące czynności:

- Kliknij prawym przyciskiem myszy na ikonę BitDefender w zasobniku systemowym paska zadań i wybierz **Napraw Wszystkie Zagadnienia**.
- Aby dodać pliki do sejfu, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:
  - W Widoku podstawowym kliknij **Zobacz wszystkie zagadnienia**.
  - W Widoku eksperta przejdź do **Ogólne > Pulpit** i kliknij **Zobacz wszystkie zagadnienia**.

    Notatka
    Możesz też dodać skrót do Moich narzędzi.

Wyświetlona zostanie lista istniejących zagrożeń, które są niebezpieczne dla komputera.

Do naprawy wybrano wszystkie bieżące zagadnienia. Jeśli istnieje zagadnienie, którego nie chcesz naprawiać, po prostu usuń zaznaczenie odpowiedniego pola wyboru. Jeśli tak zrobisz, jego stan zmieni się na **Pomiń**.

Notatka

Jeśli nie chcesz być informowany o określonych zagadnieniach, musisz w odpowiedni sposób skonfigurować system alarmowy. Jest to opisane w następnej sekcji.

Aby naprawić wybrane zagadnienia, kliknij **Start**. Niektóre zagadnienia są naprawiane od razu. Inne wymagają użycia kreatora.

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

- **Zablokowane ustawienia zabezpieczeń.** Takie zagadnienia są rozwiązywane natychmiastowo, poprzez odblokowanie odpowiednich ustawień zabezpieczeń.
- **Zapobiegawcze zadania bezpieczeństwa które musisz wykonać.** Przykład takiego zadania to skanowanie twojego komputera. Zaleca się aby skanować komputer przynajmniej raz w tygodniu. W większości przypadków BitDefender zrobi to automatycznie. Jeśli jednak harmonogram skanowania został zmieniony lub nie jest kompletny, zostaniesz poinformowany(a) o tym problemie.

  Podczas naprawiania zagadnień tego typu, kreator pomaga wykonać każde z zadań.
- **Podatności systemu.** BitDefender automatycznie sprawdza system w poszukiwaniu podatności na zagrożenia i alarmuje o nich.Do podatności systemu należą:
  - słabe hasła do kont Windows.
  - nieaktualne oprogramowanie zainstalowane na twoim komputerze.
  - brakujące aktualizacje Windows.
  - Automatyczne Aktualizacje Windows są wyłączone.

  Kiedy te zagadnienia mają zostać naprawione, uruchamiany jest odpowiedni kreator. Pozwala on naprawić wykryte luki w bezpieczeństwie systemu.Aby uzyskać więcej informacji, odwołaj się do sekcji *„Sprawdzanie Podatności”* (p. 138).

10.2. Skonfiguruj powiadamianie o problemach

System alarmowania jest skonfigurowany z myślą o monitorowaniu i alarmowaniu użytkownika o najważniejszych zagadnieniach mogących mieć wpływ na bezpieczeństwo komputera i danych.Oprócz domyślnie monitorowanych zagadnień, istnieje wiele dodatkowych, o których możesz być informowany(a).

System alarmowy można skonfigurować, tak aby najlepiej służył zapewnieniu ochrony poprzez wybranie zagadnień, o których chcesz być informowany.Można to zrobić zarówno w Widoku średniozaawansowanym, jak i Widoku eksperta.

- W Widoku średniozaawansowanym system alarmowania można konfigurować z osobnych miejsc.Podążaj tymi krokami:
  1. Przejdź do zakładki **Bezpieczeństwo**.
  2. Kliknij łącze **Dodaj/Edytuj listę** w obszarze stanu.
  3. Aby zmienić stan alarmu, użyj przełącznika odpowiadającego danemu elementowi.
- W Widoku eksperta system alarmowy można konfigurować z określonego miejsca.Podążaj tymi krokami:
  1. Przejdź do **Ogólne > Pulpit**.
  2. Kliknij **Dodaj/Edytuj alarmy**.
  3. Aby zmienić stan alarmu, użyj przełącznika odpowiadającego danemu elementowi.

11. Konfigurowanie Ustawień Głównych

Z okna Preferencje można skonfigurować główne ustawienia produktu (w tym także zmienić konfigurację profilu użytkowania). Aby je otworzyć, wykonaj jedną z następujących czynności:

- Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Preferencje**.
- Kliknij prawym przyciskiem myszy ikonę BitDefender w w zasobniku i wybierz **Ustawienia**.

Notatka

Do szczegółowego skonfigurowania ustawień produktu użyj interfejsu w Widoku eksperta.Aby uzyskać więcej informacji, odwołaj się do „Konfiguracja i zarządzanie” (p. 54) części podręcznika użytkownika.

Ustawienia są podzielone na trzy kategorie:

- Ustawienia Zabezpieczeń
- Ustawienia alertów
- Ustawienia Ogólne

Aby włączyć lub wyłączyć dane ustawienie, użyj odpowiedniego przełącznika.

Aby zastosować i zapisać zmiany, kliknij na **OK**. Aby zamknąć to okno bez zapisywania zmian, klinij na **Anuluj**.

Łącze **Rekonfiguruj Profil**, które znajduje się w prawym górnym rogu okna, pozwala ponownie skonfigurować profil użytkowania.Aby uzyskać więcej informacji, odwołaj się do *„Zmiana Konfiguracji Profilu Użytkowania”* (p. 47).

11.1. Ustawienia Zabezpieczeń

W tym obszarze możesz odblokować lub zablokować ustawienia zabezpieczeń programu, które obejmują różne aspekty bezpieczeństwa komputera i jego danych.Aby włączyć lub wyłączyć dane ustawienie, użyj odpowiedniego przełącznika.

Ostrzeżenie

Proszę zachować ostrożność przy wyłączaniu zabezpieczenia antywirusowego, zapory sieciowej lub automatycznych aktualizacji.Zablokowanie tych funkcji może narazić twój komputer na niebezpieczeństwa. Jeśli naprawdę chce je zablokować, pamiętaj o ich późniejszym, jak najszybszym odblokowaniu.

To są dostępne ustawienia:

Antywirus
: Ochrona w czasie rzeczywistym dba o to, aby wszystkie pliki, z których korzystasz Ty lub aplikacje działające w systemie, były skanowane.

Automatyczna Aktualizacja
: Automatyczna Aktualizacja gwarantuje automatyczne pobieranie i instalowanie sygnatur i plików BitDefendera.Domyślnie, aktualizacje wykonywane są co godzinę.

Skaner Podatności
: Automatyczny Skaner Podatności ostrzega i pomaga naprawiać podatności w systemie, które mogą mieć wpływ na jego bezpieczeństwo. Podatności takie mogą obejmować nieaktualne oprogramowanie, słabe hasła do kont użytkowników lub brak aktualizacji Windows.

Antyspam
: Antyspam filtruje odbierane wiadomości e-mail, oznaczając te, których nie chcesz odbierać i śmieci jako SPAM.

Antyphishing
: Antyphishing wykrywa i informuje w czasie rzeczywistym, czy strona WWW próbuje wykraść prywatne informacje.

Szukaj doradców
: Asystent wyszukiwania skanuje łącza w wynikach wyszukiwania i informuje, które z nich są bezpieczne, a które nie.

Kontrola tożsamości
: Kontrola Tożsamości pomaga chronić prywatne dane przed wysłaniem ich do Internetu bez wiedzy użytkownika. Blokuje rozmowy IM, wiadomości e-mail i dane przesyłane w formularzach, w których pojawiają się prywatne informacje przesyłane do nieautoryzowanych odbiorców.

Szyfrowanie rozmów
: Szyfrowanie rozmów zabezpiecza rozmowy przez programy Yahoo! Messenger i Windows Live Messenger, pod warunkiem że kontakty IM korzystają z kompatybilnego produktu BitDefender i oprogramowania IM.

Kontrola Rodzicielska (obecny użytkownik)
: Kontrola Rodzicielska ogranicza dostęp do komputera i Internetu dla twoich dzieci opierając się na regułach które stworzysz.Restrykcje mogą obejmować blokowanie nieprawidłowych stron WWW, oraz limitowanie czasu korzystania z gier i Internetu, według określonego harmonogramu.

Zapora Sieciowa
: Zapora Sieciowa chroni twój komputer przed zewnętrznymi atakami szkodliwego programowania i hakerów.

Stan niektórych z tych ustawień może być monitorowany przez system śledzenia zagadnień BitDefender.Jeśli zablokujesz monitorowane ustawienie, BitDefender będzie wskazywał na nie jako na zagadnienie które wymaga naprawy.

Jeśli nie chcesz, aby wyłączone monitorowanie ustawienia było wskazywane jako problem, musisz odpowiednio skonfigurować system śledzenia. Można to zrobić zarówno w Widoku średniozaawansowanym, jak i Widoku eksperta.Aby uzyskać więcej informacji, odwołaj się do *„Skonfiguruj powiadamianie o problemach”* (p. 41).

11.2. Ustawienia alertów

W tym miejscu można wyłączyć wyskakujące okna i alarmy BitDefender.BitDefender używa alarmów, aby monitować użytkownika o podjęcie działania, oraz wyskakujących okien, aby informować o czynnościach wykonanych automatycznie lub innych zdarzeniach.Aby włączyć lub wyłączyć daną kategorię alarmów, użyj odpowiedniego przełącznika.

WAŻNE

Aby uniknąć potencjalnych problemów, większość tych alarmów i wyskakujących okien powinna być włączona.

To są dostępne ustawienia:

Alerty antywirusowe

Alerty antywirusowe informują o wykryciu lub zablokowaniu wirusa przez BitDefender.W przypadku wykrycia wirusa najlepiej przeskanować jest cały komputer, aby wykluczyć obecność innych wirusów.

Wyskakujące okna aktywnej kontroli wirusowej

Jeśli korzystasz z interfejsu pracującego w trybie Widok podstawowy lub Widok średniozaawansowany, o każdym zablokowaniu potencjalnie szkodliwej aplikacji przez moduł Aktywnej ochrony wirusowej będziesz informowany przez wyświetlające się okno.Jeśli korzystasz z Widoku eksperta, w przypadku, gdy aplikacja zacznie przejawiać cechy złośliwego oprogramowania, za pośrednictwem okna alarmu zostaniesz poproszony o podjęcie działania.

Skanuj wyskakujące okna w e-mailach

Te wyskakujące okna wyświetlane są, w celu informowania, iż BitDefender skanuje wiadomości e-mail pod kątem obecności złośliwego oprogramowania.

Alerty Zarządzanie siecią domową

Alarmy te informują użytkownika o podjęciu zdalnych działań administratora.

Wyskakujące okna zapory ogniowej

Zapora Sieciowa używa wyskakujących okien, aby informować o różnych zdarzeniach związanych z połączeniem sieciowym (na przykład, gdy do sieci Wi-Fi podłączony zostaje nowy komputer, gdy nowa aplikacja uzyskuje

zezwolenie na dostęp do Internetu lub gdy skanowanie portów zostaje zablokowane).Jeśli korzystasz z Widoku eksperta, a nieznana aplikacja próbuje połączyć się z Internetem, za pośrednictwem okna alarmu otrzymasz monit o podjęcie działania.

Te wyskakujące okna mogą być bardzo przydatne w wykrywaniu prób włamań oraz zabezpieczaniu się przed zagrożeniami sieciowymi.

Alerty kwarantanny
Alerty kwarantanny informują o usunięciu starych plików kwarantanny.

Alerty kontroli rodzicielskiej
Gdy Kontrola Rodzicielska blokuje jakieś działanie, na ekranie wyświetlany jest alarm, informujący użytkownika o powodach zablokowania tej czynności (na przykład zamiast zablokowanej strony internetowej wyświetlona zostanie strona z ostrzeżeniem).

Wyskakujące okna rejestracji
Wyskakujące okno rejestracji służy do przypomnienia o konieczności zarejestrowania BitDefender lub poinformowania, że klucz licencji zaraz wygaśnie lub już wygasł.

11.3. Ustawienia Ogólne

W tym obszarze możesz odblokować lub zablokować ustawienia które wpływają na zachowanie programu i sposób współpracy z użytkownikiem.Aby włączyć lub wyłączyć dane ustawienie, użyj odpowiedniego przełącznika.

To są dostępne ustawienia:

Tryb Gry
Tryb Gry tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na wydajność systemu podczas grania.

Wykrycie Trybu Laptopa
Tryb Laptopa tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na żywotność baterii.

Hasło Ustawień
Aby uniemożliwić innym osobom zmianę ustawień BitDefender, możesz zabezpieczyć je hasłem.Kiedy włączysz tą opcję, program zapyta o skonfigurowanie hasła do ustawień.Wpisz pożądane hasło w obydwu polach i kliknij **OK** aby je ustawić.

Nowości BitDefendera
Włączając tą opcje, będziesz otrzymywać ważne informacje firmowe, aktualizacje produktu lub nowości o nowych zagrożeniach od BitDefendera.

Alarm Informacyjny Produktu
Włączając tą opcje, będziesz otrzymywał alarmy informacyjne.

Pasek Aktywności Skanera

Pasek aktywności skanera to małe, przezroczyste okno wskazujące postęp i aktywność skanera BitDefender.

Wyślij Raporty o Wirusach

Włączając tą opcje, będziesz wysyłał raporty skanowania wirusów do Laboratorium BitDefendera do analizy. Proszę pamiętać że te raporty nie zawierają żadnych danych osobistych, takich jak adres imię lub IP i nie będą wykorzystywane w celach komercyjnych.

Wykrywanie Epidemii

Włączając tą opcje, będziesz wysyłał raporty dotyczące potencjalnych włamań wirusów do Laboratorium BitDefendera do analizy. Proszę pamiętać że te raporty nie zawierają żadnych danych osobistych, takich jak adres imię lub IP i nie będą wykorzystywane w celach komercyjnych.

11.4. Zmiana Konfiguracji Profilu Użytkowania

Podczas instalowania można skonfigurować profil użytkowania.Profil użytkowania odzwierciedla główne czynności wykonywane na komputerze. W zależności od tego profilu, interfejs programu jest zorganizowany tak, aby umożliwić szybki dostęp do preferowanych zadań.

Aby ponownie skonfigurować profil użytkowania, kliknij **Rekonfiguruj profil**, a następnie wykonuj polecenia kreatora.Możliwość poruszania się w kreatorze zapewniają przyciski **Dalej** i **Cofnij**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Wybierz widok**

   Wybierz preferowany widok interfejsu użytkownika.

2. **Konfiguracja Moich Narzędzi**

   Jeśli wybrałeś Widok podstawowy lub średniozaawansowany, wybierz funkcje, dla których chcesz utworzyć skróty na pulpicie.

3. **Ustawienia konfiguracji**

   Jeśli wybrałeś Widok eksperta, skonfiguruj ustawiania BitDefender według uznania.Aby włączyć lub wyłączyć dane ustawienie, użyj odpowiedniego przełącznika.

4. **Ustaw kontrolę rodzicielską**

   Notatka

   Krok ten pojawia się tylko wtedy, gdy do Moich narzędzi dodana została opcja Kontroli Rodzicielskiej.

   Można wybrać jedną z trzech opcji:

   - **Ustawienie Kontroli Rodzicielskiej na kontach dzieci**

Wybierz tę opcję, aby włączyć Kontrolę Rodzicielską dla kont Windows utworzonych dla dzieci i zarządzaj nią z konta administratora.

- **Ustaw Kontrolę Rodzicielską na bieżącym koncie**

  Wybierz tę opcję, aby uruchomić Kontrolę Rodzicielską dla bieżącego konta Windows. To oznacza, że dla swoich dzieci nie będziesz musiał tworzyć osobnych kont. Reguły Kontroli Rodzicielskiej będą odnosić się do wszystkich osób, które używają bieżącego konta.

  W tym wypadku do ochrony ustawień Kontroli Rodzicielskiej potrzebne jest hasło.Możesz ustalić to teraz lub w późniejszym terminie z okna BitDefender.

- **Na razie pomiń konfigurację.**

  Wybierz tę opcję, aby skonfigurować tę funkcję w późniejszym terminie z okna BitDefender.

5. **Zarządzanie siecią domową**

   Notatka
   Krok ten pojawia się tylko wtedy, gdy do Moich narzędzi dodana została opcja Zarządzanie siecią domową.

   Można wybrać jedną z trzech opcji:

   - **Skonfiguruj ten komputer jako "Serwer"**

     Wybierz tę opcję, jeśli planujesz zarządzać z tego komputera PC produktami BitDefender na innych komputerach w sieci domowej.

     Aby dołączyć do sieci, musisz podać hasło.Wpisz hasło w podanych polach tekstowych i kliknij **Wyślij**.

   - **Skonfiguruj ten komputer jako Klienta**

     Wybierz tę opcję, jeśli BitDefender będzie zarządzany z innego komputera w sieci domowej, na którym BitDefender jest uruchomiony.

     Aby dołączyć do sieci, musisz podać hasło.Wpisz hasło w podanych polach tekstowych i kliknij **Wyślij**.

   - **Na razie pomiń konfigurację.**

     Wybierz tę opcję, aby skonfigurować tę funkcję w późniejszym terminie z okna BitDefender.

6. **Instalacja zakończona**

   Kliknij **Zakończ**.

12. Historia i Zdarzenia

Łącze **Pokaż Dzienniki** na dole głównego okna BitDefender otwiera kolejne okno z historią zdarzeń w programie. To okno oferuje podgląd zdarzeń powiązanych z bezpieczeństwem systemu.Przykładowo, możesz łatwo sprawdzić czy aktualizacja została zakończona sukcesem, czy na komputerze znaleziono wirusa itp.

Aby pomóc tobie filtrować zdarzenia historii BitDefendera, po lewej stronie dostępne są następujące kategorie:

- **Panel**
- **Antywirus**
- **Antyspam**
- **Kontrola Rodzcielska**
- **Kontrola prywatności**
- **Zapora Sieciowa**
- **Podatności**
- **Szyfrowanie rozmów**
- **Tryb Gry/Laptopa**
- **Sieć Domowa**
- **Aktualizacje**
- **Rejestracja**

Dla każdej kategorii dostępna jest lista zdarzeń. Każdemu zdarzeniu towarzyszy następująca informacja: krótki opis, działanie wykonane przez BitDefender, gdy doszło do zdarzenia, data i czas jego wystąpienia. Jeśli chcesz uzyskać więcej informacji na temat określonego zdarzenia z listy, dwukrotnie je kliknij.

W tym miejscu możesz także przejrzeć szczegółowe informacje i statystyki dotyczące zdarzeń Kontroli Rodzicielskiej, na przykład uzyskania przez dzieci dostępu do witryn internetowych lub aplikacji.

Kliknij **Wyczyść wszystkie dzienniki** aby usunąć stare dzienniki lub **Odśwież** aby upewnić się, że wyświetlane są ostatnie dzienniki.

13. Rejestracja i Moje Konto

Rejestracja to dwuczęściowy proces:

1. **Aktywacja produktu (rejestracja konta BitDefender).** Musisz utworzyć konto BitDefender aby móc korzystać z aktualizacji i dostępu do darmowego wsparcia technicznego.Jeśli już posiadasz konto BitDefender, zarejestruj produkt przy jego użyciu.BitDefender powiadomi cię o konieczności aktywowania produktu i pomoże w wykonaniu tej czynności.

   WAŻNE

   Konto należy utworzyć w ciągu 15 dni od zainstalowania BitDefender.W przeciwnym wypadku, BitDefender nie będzie się aktualizował.

2. **Rejestracja z kluczem licencyjnym.** klucz specyfikuje jak długo będziesz mógł korzystać z produktu.Jak tylko twój klucz licencyjny wygaśnie, BitDefender przestanie chronić twój komputer.Musisz wykupić klucz licencyjny lub odnowić swoją licencję kilka dni zanim obecny klucz straci ważność.

Jeśli zakupiłeś BitDefender Internet Security 2011 na dysku CD/DVD lub przez Internet, w czasie instalacji otrzymałeś monit o zarejestrowanie produktu za pomocą klucza licencji.

Jeśli pobrałeś BitDefender Internet Security 2011, w celu jego przetestowania, musisz zarejestrować produkt za pomocą klucza licencji, by móc z niego korzystać po upływie 30 dni okresu próbnego.Podczas okresu darmowego korzystania z aplikacji, produkt pozostaje w pełni funkcjonalny, aby użytkownik mógł sprawdzić czy spełnia on jego oczekiwania.

13.1. Rejestrowanie BitDefender Internet Security 2011

Jeśli chcesz zarejestrować produkt za pomocą klucza licencji lub zmienić aktualny klucz licencji, kliknij łącze **Informacje o licencji**, znajdujące się w dolnej części okna BitDefender.Zostanie otwarte okno rejestracji produktu.

Możesz zobaczyć status rejestracji BitDefendera, aktualny klucz licencyjny oraz ile dni pozostało do wygaśnięcia rejestracji.

Aby zarejestrować BitDefender Internet Security 2011:

1. Wpisz w polu klucz licencyjny.

   Notatka

   Klucz licencyjny możesz znaleźć:
   - na etykiecie płyty CD.
   - na karcie rejestracyjnej produktu.
   - w emailu potwierdzającym zakup.

Jeśli nie masz klucza licencyjnego BitDefender, kliknij podane łącze, aby uruchomić kreatora, który pomoże ci w zakupie klucza.

2. Kliknij **Zarejestruj Teraz**.
3. Kliknij **Zakończ**.

13.2. Aktywacja BitDefendera

Aby aktywować BitDefender, musisz stworzyć nowe lub zalogować się do istniejącego konta BitDefender.Jeśli nie zarejestrowałeś konta BitDefender w czasie instalacji, możesz zrobić to, wykonując następujące czynności:

Widok Podstawowy
Kliknij **Zobacz wszystkie zagadnienia**.Ten kreator pozwoli ci naprawić wszystkie bieżące zagadnienia oraz aktywować twój produkt.

Widok średniozaawansowany
Przejdź do zakładki **Bezpieczeństwo** i kliknij przycisk **Zobacz & Napraw** odpowiadający zagadnieniu, które dotyczy aktualizacji produktu.Aby aktywować produkt, kliknij **Start** w oknie kreatora.

Widok eksperta
Przejdź do **Rejestracja** i kliknij przycisk **Aktywuj produkt**.

Zostanie otwarte okno rejestracji.Tutaj możesz stworzyć nowe lub zalogować się do istniejącego konta BitDefender.

Jeśli w danej chwili nie chcesz tworzyć konta BitDefender, wybierz opcję **Utwórz konto później** i kliknij **Zakończ**.W przeciwnym razie postępuj w zależności od sytuacji:

- „Nie mam osobistego konta na MyBitDefender” (p. 51).
- „Już posiadam konto BitDefender” (p. 52).

WAŻNE

Konto należy utworzyć w ciągu 15 dni od zainstalowania BitDefender.W przeciwnym wypadku, BitDefender nie będzie się aktualizował.

Nie mam osobistego konta na MyBitDefender

Aby pomyślnie utworzyć konto BitDefender, podążaj według tych kroków:

1. Wybierz **Utwórz nowe konto**.
2. Wprowadź wymaganą informację w odpowiednich polach.Dane które teraz wprowadzisz pozostaną tajne.
   - **Nazwa użytkownika** - wpisz swój adres e-mail.

- **Hasło** - wpisz hasło dla konta BitDefender.Hasło musi zawierać od 6 do 16 znaków.
- **Wpisz ponownie hasło** - wpisz ponownie hasło podane wcześniej.

  Jeśli podczas wpisywania hasła nie zaznaczyłeś opcji jego maskowania, nie musisz ponownie go wpisywać.
- **Podpowiedź do hasła** - podaj słowo lub wyrażenie, które pomoże ci przypomnieć sobie hasło, gdybyś go zapomniał.

Notatka
Jak tylko konto zostanie aktywowane, możesz korzystać z dołączonego adresu e-mail aby zalogować się na nie pod adresem http://myaccount.bitdefender.com.

3. Opcjonalnie, BitDefender może informować ciebie o specjalnych ofertach oraz promocjach korzystając z adresu email twojego konta.Kliknij **Zobacz opcje kontaktu** i z okna, które pojawi się na ekranie, wybierz jedną z dostępnych opcji.
   - **Wyślij mi wszystkie wiadomości**
   - **Przysyłaj mi ważne wiadomości**
   - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Wyślij**.
5. Aby zamknąć to okno, kliknij **Zakończ**.

Notatka
Zanim zaczniesz korzystać z konta, musisz je aktywować.
Sprawdź swoją pocztę i postępuj według instrukcji zawartych w e-mailu przysłanym ci przez usługę rejestracji BitDefender.

Już posiadam konto BitDefender

BitDefender automatycznie wykryje czy poprzednio rejestrowałeś konto BitDefender na swoim komputerze.W tym przypadku, wpisz hasło do konta i kliknij **Zaloguj się**.Aby zamknąć to okno, kliknij **Zakończ**.

Jeśli już posiadasz aktywne konto, ale BitDefender go nie wykrywa, wykonaj następujące kroki aby zarejestrować produkt dla tego konta:

1. Wybierz **Zaloguj się (Poprzednie konto)**.
2. W odpowiednich polach wprowadź adres e-mail i hasło do twojego konta.

Notatka
Jeżeli zapomniałeś hasła kliknij **Nie pamiętasz hasła?** i wykonuj instrukcje.

3. Opcjonalnie, BitDefender może informować ciebie o specjalnych ofertach oraz promocjach korzystając z adresu email twojego konta.Kliknij **Zobacz opcje kontaktu** i z okna, które pojawi się na ekranie, wybierz jedną z dostępnych opcji.
   - **Wyślij mi wszystkie wiadomości**
   - **Przysyłaj mi ważne wiadomości**
   - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Wyślij**.
5. Aby zamknąć to okno, kliknij **Zakończ**.

13.3. Kupno lub Odnawianie Kluczy Licencji

Jeśli okres testowy wkrótce się zakończy, musisz zakupić nowy klucz licencyjny i zarejestrować swój produkt.

Podobnie, jeśli aktualny klucz licencyjny wkrótce wygaśnie, konieczne jest odnowienie licencji.Jako klientowi BitDefender, przysługuje ci zniżka przy odnawianiu licencji dla twoich produktów. Możesz także wykonać ugprade swojej starej wersji do najnowszej, po specjalnej zniżce lub za darmo.

Aby uruchomić prostą i bezpieczną czterostopniową procedurę, która umożliwi ci zakup nowego klucza lub odnowienie istniejącego, otwórz BitDefender w Widoku średniozaawansowanym lub eksperta i kliknij łącze **Kup** / **Odnów** umieszczone w dolnej części okna.

Konfiguracja i zarządzanie

14. Ustawienia Ogólne

Moduł Ogólny zapewnia informacje o aktywności BitDefendera oraz systemu.Możesz tutaj również zmienić ogólne zachowanie BitDefednera.

Konfigurowanie ustawień ogólnych:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Ogólne > Ustawienia**.

- **Włącz zabezpieczenie ustawień produktu hasłem** - umożliwia ustawianie hasła do ochrony konfiguracji BitDefendera.

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

  Wpisz hasło w pole **Hasło** następnie wpisz je ponownie w polu **Potwierdź hasło** i kliknij **OK**.

  Gdy ustawisz hasło, będziesz o nie pytany za każdym razem gdy będziesz chciał modyfikować ustawienia BitDefendera.Inni administratorzy systemu (jeśli są) też będą musieli wprowadzić hasło przy dokonywaniu zmian w ustawieniach BitDefendera.

  Jeśli chcesz być monitowany o podanie hasła tylko przy konfigurowaniu Kontroli Rodzicielskiej, musisz także zaznaczyć opcję **Zastosuj hasło tylko do Ustawień Kontroli Rodzicielskiej**.Z drugiej strony, jeśli hasło było ustawione tylko dla Kontroli Rodzicielskiej i odznaczysz tą opcje, pytanie o to hasło będzie przy zmianie dowolnego ustawienia Bitdefendera.

  WAŻNE
  Jeżeli zapomnisz hasła będziesz musiał naprawić program, aby móc dokonywać modyfikacji konfiguracji BitDefender.

- **Pytaj czy chce zastosować hasło przy włączaniu Kontroli Rodzicielskiej** - monituje o założenie hasła w przypadku włączenia Kontroli Rodzicielskiej, gdy nie jest ustawione żadne hasło.Ustawiając hasło, uniemożliwisz innym użytkownikom z prawami administracyjnymi zmienianie ustawień Kontroli Rodzicielskiej które skonfigurujesz dla konkretnego użytkownika.
- **Pokaż Wiadomości BitDefendera (związane z bezpieczeństwem)** - pokazuje informacje związane z bezpieczeństwem, wysyłane przez serwer BitDefendera.
- **Pokaż wyskakujące okienka** - pokazuje okienka dotyczące statusu produktu.BitDefender można skonfigurować, tak aby wyświetlał wyskakujące okna

tylko wtedy, gdy interfejs pracuje w Widoku podstawowym, średniozaawansowanym lub eksperta.

- **Pokaż Pasek Aktywności Skanera (graficzny wykres na ekranie, pokazujący aktywność programu)** - wyświetla Pasek Aktywności Skanera po każdym zalogowaniu do Windows.Odznacz to pole jeśli nie chcesz aby Pasek Aktywności Skanera był wyświetlany.

Notatka

Ta opcja może być konfigurowana tylko dla obecnego użytkownika Windows.Pasek Aktywności Skanera dostępny jest tylko w interfejsie działającym w Widoku eksperta.

Ustawienia Raportów Wirusowych

- **Wyślij raport o wirusach** - wysyła do laboratorium BitDefender raporty dotyczące zidentyfikowanych wirusów na twoim komputerze. Pomoże to nam ustalić gdzie wybuchają epidemie wirusów.

  Raporty nie będą zawierały żadnych tajnych danych takich jak: nazwa, adres IP i inne oraz nie będą wykorzystywane do celów komercyjnych. Dostarczona informacja będzie zawierała wyłącznie nazwę wirusa i wykorzystywana będzie jedynie w celu tworzenia statystyk raportów.

- **Włącz Wykrywanie Włamań BitDefendera** - wysyła raporty dotyczące potęcjalnych włamań wirusów do Laboratorium BitDefendera.

  Raporty nie będą zawierały żadnych tajnych danych takich jak: nazwa, adres IP itp. oraz nie będą wykorzystywane do celów komercyjnych. Dostarczona informacja będzie zawierała wyłącznie nazwę wirusa i wykorzystywana będzie jedynie w celu wykrywania nowych wirusów.

Ustawienia połączeń

Kilka składników BitDefender (Zapora Sieciowa, LiveUpdate, moduły Raportowanie wirusów w czasie rzeczywistym i Raportowanie spamu w czasie rzeczywistym) wymaga dostępu do Internetu. BitDefender jest wyposażony w menedżera proxy, który z jednego miejsca pozwala konfigurować ustawienia proxy używane przez składniki BitDefender, by uzyskać dostęp do Internetu.

Jeśli twoja firma korzysta z serwera proxy by łączyć się z Internetem, musisz określić ustawienia proxy w celu aktualizacji BitDefendera. W innym przypadku wykorzysta on ustawienia serwera proxy administratora, który zainstalował produkt lub domyślnej przeglądarki obecnego użytkownika, jeśli taką ma.Aby uzyskać więcej informacji, odwołaj się do *„Gdzie znaleźć informacje na temat Ustawień Proxy?”* (p. 203).

Notatka
Ustawienia proxy mogą zostać skonfigurowane tylko przez użytkowników z prawami administratora na komputerze lub zaufanego użytkownika (użytkownicy którzy znają hasło do ustawień produktu).

Aby zarządzać ustawieniami proxy, kliknij **Ustawienia Proxy**.

Dostępne są trzy zestawy ustawień proxy:

- **Proxy wykryte w czasie instalacji** - w czasie instalacji wykryto ustawienie proxy na koncie administratora, które można skonfigurować tylko po zalogowaniu się do tego konta. Jeśli serwer proxy wymaga nazwy użytkownika i hasła, musisz je podać w odpowiednich polach.
- **Domyślny Proxy Przeglądarki** - ustawienia proxy dla aktualnego użytkownika, odczytane z domyślnej przeglądarki. Jeśli serwer proxy wymaga nazwy użytkownika i hasła, musisz je wpisać w odpowiadające im pola.

  Notatka
  Obsługiwane przeglądarki internetowe to, Internet Explorer, Mozilla Firefox i Opera. Jeśli używasz innej domyślnej przeglądarki, BitDefender nie będzie w stanie uzyskać ustawień proxy aktualnego użytkownika.

- **Własne Proxy** - ustawienia proxy które możesz skonfigurować z poziomu konta administratora.

  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.

BitDefender będzie używał zestawów ustawień proxy w następującej kolejności aż do nawiązania połączenia Internetem:

1. określone ustawienia proxy.
2. ustawienia proxy wykryte podczas instalacji.
3. ustawienia proxy bieżącego użytkownika.

Przy łączeniu się z Internetem, wszystkie ustawienia proxy są sprawdzane kolejno, aż BitDefender zdoła się połączyć.

Najpierw zostaną użyte twoje ustawienia proxy do połączenia się z Internetem. Jeśli to nie zadziała, ustawienia proxy wykryte przy instalacji zostaną wypróbowane. Jeśli i to nie zadziała ustawienia proxy obecnego użytkownika zostaną wykorzystane z domyślnej przeglądarki do połączenia się z Internetem.

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

Kliknij **Zastosuj** aby zapisać zmiany albo kliknij **Domyślne** aby wczytać domyślne ustawienia.

Informacje Systemowe

BitDefender pozwala na zobaczenie, z jednego miejsca, wszystkie ustawienia systemowe i aplikacje zarejestrowane do działania przy uruchamianiu systemu. W ten sposób możesz monitorować aktywność systemu i aplikacji zainstalowanych w nim jak i identyfikować możliwe infekcje systemu.

Uzyskiwanie informacji o systemie:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Ogólne > Informacje**.

Lista zawiera wszystkie pozycje załadowane podczas startu systemu jak również pozycje załadowane przez inne aplikacje.

Trzy przyciski są dostępne:

- **Przywróć** - przywraca powiązania wybranego pliku do domyślnego stanu.Dostępne tylko dla ustawień **Powiązań Pliku**!
- **Idź do** - otwiera okno gdzie wybrana pozycja się znajduje (na przykład **Rejestr**).

Notatka
Zależnie od wybranego elementu, przycisk **Idź do** może się nie pojawić.

- **Odśwież** - ponownie otwiera sekcję **Informacje Systemowe**.

15. Ochrona antywirusowa

BitDefender chroni twój komputer przed wszystkimi rodzajami zagrożeń (wirusy, trojany, spyware, rootkity i nie tylko).Ochrona BitDefendera jest podzielona na dwie kategorie:

- Ochrona w Czasie Rzeczywistym - zapobiega infekcji komputera przez złośliwe oprogramowanie.Na przykład BitDefender przeskanuje dokument Word, kiedy go otworzysz, oraz wiadomość email kiedy ją otrzymasz.

  Ochrona w Czasie Rzeczywistym dotyczy również skanowanie przy dostępie - pliki są skanowane gdy użytkownik z nich korzysta.

  WAŻNE
  Aby zapobiec zainfekowaniu komputera wirusami miej włączoną opcję **Ochrona w Czasie Rzeczywistym**.

- Skanowanie Na Żądanie - pozwala wykrywać i usuwać złośliwe oprogramowanie znajdujące się już w systemie.Jest to klasyczne skanowanie wirusów zainicjowane przez użytkownika – wybierasz jaki dysk, folder lub plik BitDefender ma skanować, a BitDefender skanuje go - na żądanie.Zadania skanowania pozwala tobie stworzyć własny schematy skanowania i mogą być one regularnie uruchamiane.

W przypadku wykrycia wirusa lub innego złośliwego oprogramowania, BitDefender dokona automatycznej próby usunięcia kodu złośliwego oprogramowania z zainfekowanego pliku i odtworzenia oryginalnego pliku.Ta operacja określana jest mianem dezynfekcji.Plików, których nie można zdezynfekować, są poddawane kwarantannie, aby powstrzymać infekcję.Aby uzyskać więcej informacji, odwołaj się do *„Kwarantanna”* (p. 81).

Jeśli komputer został zainfekowany złośliwym oprogramowaniem, zapoznaj się z informacjami w *„Usuwanie Złośliwego Oprogramowania z Systemu”* (p. 186).

Zaawansowani użytkownicy, którzy nie chcą skanować określonych plików, mogą ustawiać wyjątki skanowania.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Wyjątków Skanowania”* (p. 78).

15.1. Ochrona W Czasie Rzeczywistym

BitDefender zapewnia stałą ochronę w czasie rzeczywistym, przeciw szerokiemu zakresowi zagrożeń skanując używane pliki, wiadomości e-mail oraz komunikacje prowadzoną przez komunikatory (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

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

zgodne z potrzebami użytkownika zapewniają zdefiniowane wcześniej poziomy ochrony.Jeśli jesteś użytkownikiem zaawansowanym, możesz szczegółowo skonfigurować ustawienia skanowania poprzez utworzenie własnego poziomu ochrony.

Więcej informacji zawierają następujące tematy:

- *„Dostosowywanie Poziomu Ochrony w Czasie Rzeczywistym”* (p. 60)
- *„Tworzenie własnego poziomu ochrony”* (p. 61)
- *„Zmiana Działań Podejmowanych Względem Wykrytych Plików.”* (p. 62)
- *„Przywracanie Ustawień Domyślnych”* (p. 63)

Aby chronić cię przed nieznanymi, złośliwymi aplikacjami, BitDefender wykorzystuje zaawansowaną technologię heurystyczną (Aktywną ochronę wirusową) oraz System wykrywania włamań, które nieustannie monitorują cały system.Więcej informacji zawierają następujące tematy:

- *„Konfigurowanie Aktywnej Ochrony Wirusowej”* (p. 64)
- *„Konfigurowanie Systemu Wykrywania Włamań”* (p. 66)

15.1.1. Dostosowywanie Poziomu Ochrony w Czasie Rzeczywistym

Poziom ochrony w czasie rzeczywistym określa ustawienia skanowania dla ochrony w tym czasie.Łatwe zmienianie ustawień ochrony w czasie rzeczywistym zgodne z potrzebami użytkownika zapewniają zdefiniowane wcześniej poziomy ochrony.

Dostosowywanie poziomu ochrony w czasie rzeczywistym:

1. Otwórz BitDefender.
2. W zależności od wybranego trybu wyświetlania interfejsu użytkownika postępuj zgodnie z poleceniami:

   Widok średniozaawansowany

   Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Antywirusa**.

   Przejdź do zakładki **Tarcza**.

   Widok eksperta

   Przejdź do **Antywirus > Tarcza**.

Notatka

W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

3. Aby ustawić wybrany poziom ochrony, przeciągnij suwak wzdłuż skali.Użyj opisów po prawej stronie skali, aby wybrać poziom ochrony najlepiej spełniający twoje wymagania.

15.1.2. Tworzenie własnego poziomu ochrony

Zaawansowani użytkownicy mogą dokonywać zmian w ustawieniach skanowania oferowanych przez BitDefendera. Skaner może być ustawiony, aby skanować podane rozszerzenia plików, skanować przed konkretnym zagrożeniem lub pomijać archiwa. Może to znacząco zredukować czas skanowania i poprawić komfort pracy podczas skanowania.

Możesz szczegółowo skonfigurować ochronę w czasie rzeczywistym poprzez utworzenie własnego poziomu ochrony.Tworzenie własnego poziomu ochrony:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Poziom własny**.
4. Skonfiguruj ustawienia skanowania według uznania.Aby dowiedzieć się za co odpowiada dana opcja, przytrzymaj nad nią kursor myszy i przeczytaj informację która pojawi się na dole okna.
5. Kliknij **OK** aby zapisać zmiany i zamknąć okno.

Ta informacja może być przydatna:

- Jeśli nie znasz pewnych określeń, sprawdź je w słowniku.Możesz także uzyskać więcej informacji przeszukując Internet.
- **Skanuj uruchamiane pliki.** BitDefender można ustawić na skanowanie wszystkich plików, które były używane lub tylko aplikacji (plików programów) albo określonych typów plików, które użytkownik uznał za niebezpieczne.Najlepszą ochronę zapewnia skanowanie wszystkich użytych plików, natomiast lepszą wydajność zapewnia skanowanie tylko aplikacji.

  Aplikacje (lub pliki programów) są bardziej narażone na ataki złośliwego oprogramowania od plików innego typu.Ta kategoria obejmuje następujące rozszerzenia plików:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Jeśli wybierasz **Skanowanie tylko zdefiniowanych rozszerzeń**, zaleca się objęcie nim rozszerzeń wszystkich aplikacji oraz innych rozszerzeń plików, które uznasz za niebezpieczne.

- **Skanuj tylko nowe i zmienione pliki.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Skanowanie wewnatrz archiwów.** Skanowanie wewnątrz archiwów to powolny i zasobożerny proces, który z tego powodu nie jest zalecany dla użycia w ochronie w czasie rzeczywistym.Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu.Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym.
- **Opcje dzialania.** Jeśli zastanawiasz się nad zmianą działań podejmowanych względem plików, w których wykryto infekcje, sprawdź porady w *„Zmiana Działań Podejmowanych Względem Wykrytych Plików.”* (p. 62).
- **Opcje skanowania ruchu sieciowego związanego z pocztą, siecią WWW i komunikacją natychmiastową.** Aby uniemożliwić pobieranie złośliwego oprogramowania na komputer, BitDefender automatycznie skanuje następujące punkty wejściowe złośliwego oprogramowania:
  - przychodzące wiadomości e-mail
  - Ruch sieciowy
  - Pliki otrzymane za pośrednictwem Yahoo! Messenger i Windows Live Messenger

  Skanowanie ruchu sieciowego może nieco spowolnić przeglądanie sieci, ale będzie blokować złośliwe oprogramowanie pochodzące z Internetu, w tym także przypadkowe pobieranie plików.

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

15.1.3. Zmiana Działań Podejmowanych Względem Wykrytych Plików.

Pliki wykryte przez moduł ochrony w czasie rzeczywistym są dzielone na dwie kategorie:

- **Pliki zainfekowane.** Pliki, w których wykryto infekcje, są zgodne z sygnaturami w Bazie Danych Sygnatur Złośliwego Oprogramowania BitDefender.BitDefender może usunąć kod złośliwego oprogramowania z zainfekowanego pliku i odtworzyć oryginalny plik. Operacja ta znana jest jako dezynfekcja.

Notatka

Sygnatury złośliwego oprogramowania to urywki kodu wypakowane z rzeczywistych próbek tego oprogramowania. Są one używane przez programy antywirusowe do porównywania wzorców i wykrywania złośliwego oprogramowania.

Baza Danych Sygnatur Złośliwego Oprogramowania BitDefender to zbiór sygnatur złośliwego oprogramowania uaktualniany co godzinę przez naukowców BitDefender, zajmujących się złośliwym oprogramowaniem.

- **Podejrzane pliki.** Pliki są wykrywane jako podejrzane przez analizę heurystyczną.Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.

W zależności od typu wykrytego pliku, automatycznie podejmowane są następujące działania:

- W przypadku wykrycia zainfekowanego pliku BitDefender podejmie automatyczną próbę jego dezynfekcji.Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.

  WAŻNE
  W przypadku określonych typów złośliwego oprogramowania dezynfekcja jest niemożliwa, ponieważ złośliwy jest cały plik. W takich wypadkach jest on usuwany z dysku.

- W przypadku wykrycia podejrzanego pliku, dostęp do niego zostaje zablokowany, aby zapobiec potencjalnej infekcji.

Bez posiadania ważnego powodu nie powinno się zmieniać domyślnych działań podejmowanych względem wykrytych plików.

Zmiana domyślnych działań podejmowanych względem wykrytych zainfekowanych lub podejrzanych plików:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Poziom własny**.
4. Skonfiguruj działania, które będą podejmowane dla każdej kategorii wykrytych plików.W przypadku niepowodzenia pierwszego działania podjęte zostaje drugie (na przykład, jeśli przeprowadzenie dezynfekcji nie jest możliwe, zainfekowany plik zostaje poddany kwarantannie).

15.1.4. Przywracanie Ustawień Domyślnych

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

Przywracanie domyślnych ustawień ochrony w czasie rzeczywistym:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.

2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Poziom domyślny**.

15.1.5. Konfigurowanie Aktywnej Ochrony Wirusowej

Aktywna ochrona wirusowa BitDefender wykrywa potencjalnie szkodliwe aplikacje w oparciu o ich zachowanie.

Moduł Aktywnej ochrony wirusowej nieustannie monitoruje aplikacje działające w komputerze, wyszukując działania charakterystyczne dla złośliwego oprogramowania. Każde z tych działań jest oceniane, a dla każdego procesu wystawiana jest ocena ogólna.Gdy ogólny wynik dla danego procesu osiągnie podany próg, proces ten zostaje uznany za szkodliwy. W zależności od ustawień programu, proces ten jest blokowany automatycznie lub użytkownik otrzymuje monit o konieczności podjęcia działania.

Aktywna Kontrola Wirusowa może zostać skonfigurowana tak, alarmowała użytkownika i pytała o podjęcie działania kiedy jakaś aplikacja chce przeprowadzić potencjalnie niebezpieczną akcję.

Jeżeli znasz i ufasz wykrytej aplikacji, kliknij **Zezwól**.

Jeżeli chcesz natychmiast zamknąć aplikacje, kliknij **OK**.

Jeśli przed dokonaniem wyboru zaznaczysz pole **Pamiętaj wybraną akcję dla tej aplikacji**, BitDefender będzie wykonywał w przyszłości tę samą operację w przypadku zaatakowania tej aplikacji.Reguła, która została dodana będzie widoczna w oknie konfiguracyjnym Aktywnej Kontroli Wirusowej.

Konfigurowanie Aktywnej Kontroli Wirusowej:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Zaawansowane**.
4. Przejdź do zakładki **AVC**.
5. Zaznacz odpowiadające pole aby włączyć Active Virus Control.
6. Aby ustawić wybrany poziom ochrony, przeciągnij suwak wzdłuż skali.Użyj opisów po prawej stronie skali, aby wybrać poziom ochrony najlepiej spełniający twoje wymagania.

Dostosowywanie Poziomu Agresywności

Konfigurowanie poziomu ochrony Aktywnej Kontroli Wirusowej:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.

2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Zaawansowane**.
4. Przejdź do zakładki **AVC**.
5. Aby ustawić wybrany poziom ochrony, przeciągnij suwak wzdłuż skali.Użyj opisów po prawej stronie skali, aby wybrać poziom ochrony najlepiej spełniający twoje wymagania.

Konfigurowanie Reakcji na Przejawy Złośliwego Zachowania

Jeśli aplikacja zdradza cechy złośliwego oprogramowania, otrzymasz monit o jej dopuszczenie lub zablokowanie.

Konfigurowanie reakcji na przejawy złośliwego zachowania:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Zaawansowane**.
4. Przejdź do zakładki **AVC**.
5. Jeśli chcesz otrzymywać monity o podjęcie działania w przypadku wykrycia przez moduł Aktywnej ochrony wirusowej potencjalnie szkodliwej aplikacji, zaznacz pole **Powiadom mnie przed podjęciem działania**.Aby automatycznie blokować aplikację zdradzającą cechy złośliwego oprogramowania (bez wyświetlenia okna alarmu), usuń zaznaczenie tego pola wyboru.

Zarządzanie Zaufanymi / Niezaufanymi Aplikacjami

Aplikacje które znasz i którym ufasz możesz dodać do listy zaufanych aplikacji. Te aplikacje nie będą więcej sprawdzane przez BitDefender Active Virus Control i automatycznie uzyskają pełny dostęp.

Zarządzanie aplikacjami, które nie są monitorowane przez Aktywną Kontrolę Wirusową:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Zaawansowane**.
4. Przejdź do zakładki **AVC**.
5. Kliknij zakładkę **Wyjątki**.

Aplikacje dla których stworzono reguły są wyświetlone w tabeli **Wyjątki**.Obok każdej reguły wyświetlone są: ścieżka do aplikacji i akcja którą dla niej ustawiłeś (Zezwolone lub Zablokowane).

Aby zmienić działanie dla aplikacji, kliknij na aktualne działanie i wybierz inne z menu.

Aby zarządzać listą, użyj przycisków znajdujących się nad tabelą:

- **Dodaj** - dodaj nową aplikację do listy.
- **Usuń** - usuwa aplikację z listy.
- **Edytuj** - edytuje regułę aplikacji.

15.1.6. Konfigurowanie Systemu Wykrywania Włamań

System wykrywania włamań BitDefender monitoruje sieć i aktywność systemu pod kątem złośliwego zachowania lub naruszeń reguł.

Konfigurowanie Systemu Wykrywania Włamań:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Zaawansowane**.
4. Przejdź do zakładki **IDS**.
5. Aby włączyć Systemu Wykrywania Włamań, zaznacz odpowiednie pole wyboru.
6. Aby ustawić odpowiedni poziom agresywności, przeciągnij suwak wzdłuż skali.Użyj opisów po prawej stronie skali, aby wybrać poziom agresywności najlepiej spełniający twoje wymagania.

15.2. Skanowanie na żądanie

Głównym zadaniem BitDefender jest zabezpieczenie twojego komputera przed wirusami. Wykonywane jest to przede wszystkim poprzez uniemożliwianie dostępu do komputera nowym wirusom oraz przez skanowanie twoich wiadomości e-mail i każdych nowych plików załadowywanych lub kopiowanych do twojego systemu.

Istnieje ryzyko, że wirus już umiejscowił się w systemie, zanim zainstalowałeś BitDefender. Dlatego też ważne jest przeskanowanie twojego komputera w poszukiwaniu obecnych wirusów, po zainstalowaniu BitDefender. Ważne również jest regularne skanowanie komputera.

Skanowanie na żądanie oparte jest na zadaniach skanowania. Zadania skanowania określają ustawienia skanowania i elementy, które mają być przeskanowane.Możesz skanować komputer kiedy tylko chcesz przez uruchamianie domyślnych lub własnych zadań. Możesz także zaplanować aby skanowania były uruchamiane regularnie lub gdy system jest bezczynny, tak aby nie przeszkadzać sobie w pracy.Aby uzyskać szybkie porady, przejrzyj następujące tematy:

● *„Jak skanować pliki i foldery?”* (p. 157)

- *„Jak utworzyć niestandardowe zadanie skanowania?"* (p. 160)
- *„Jak zaplanować skanowanie komputera?"* (p. 162)

15.2.1. Skanowanie Plików i Folderów

Pliki i foldery należy skanować zawsze, gdy istnieje podejrzenie, że są zainfekowane.Kliknij prawym przyciskiem myszy plik lub folder, który ma być przeskanowany i wybierz opcję **Skanuj z BitDefender**.Pojawi się Kreator skanowania antywirusowego i przeprowadzi cię przez proces skanowania.

Jeśli chcesz skanować określone miejsca komputera, możesz skonfigurować i uruchomić własne zadanie skanowania.Aby uzyskać więcej informacji, odwołaj się do *„Jak utworzyć niestandardowe zadanie skanowania?"* (p. 160).

Aby przeskanować cały komputer lub jego część możesz użyć domyślnego zadania skanowania lub lub własnych zadań skanowania.Aby uruchomić zadanie skanowania, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok Podstawowy
: Kliknij przycisk **Bezpieczeństwo** i wybierz jedno z dostępnych zadań skanowania.

Widok średniozaawansowany
: Przejdź do zakładki **Bezpieczeństwo**.W Szybkich zadaniach, po lewej stronie, kliknij **Pełne Skanowanie** i wybierz jedno z dostępnych zadań skanowania.

Widok eksperta
: Przejdź do **Antywirus > Skanowanie**.Aby uruchomić zadanie systemowe lub zdefiniowane przez użytkownika, kliknij odpowiadający mu przycisk **Uruchom Zadanie**.

Domyślne zadania, których można używać do skanowania komputera, są następujące:

Pełne Skanowanie
: Skanuje cały system wyłączając archiwa.W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów.

Szybkie skanowanie
: Do wykrywania w systemie złośliwego oprogramowania Szybkie Skanowanie wykorzystuje skanowanie w chmurze.Wykonanie Szybkiego Skanowania trwa zwykle mniej niż minutę i używa tylko niewielkiej części zasobów systemowych niezbędnych dla normalnego skanowania.

Głębokie Skanowanie
: Skanuje cały system.W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.

Zanim rozpoczniesz proces skanowania, powinieneś upewnić się, że BitDefender jest zaktualizowany. Skanowanie komputera z nieaktualnymi sygnaturami wirusów może spowodować niewykrycie przez BitDefendera nowego szkodliwego oprogramowania, które mogło się pojawić od ostatniej aktualizacji.

Aby BitDefender wykonał całkowite skanowanie, musisz zamknąć wszystkie otwarte programy. Szczególnie twój klient e-mail (tj. Outlook, Outlook Express lub Eudora) powinien być zamknięty.

Wskazówki na temat skanowania

Oto kilka wskazówek dotyczących skanowania, które mogą ci się przydać:

- W zależności od miejsca na dysku twardym, uruchomienie dokładnego skanowania komputera (takiego jak Głębokie Skanowanie Systemu lub Skanowanie Systemu) może chwilę potrwać (do godziny lub dłużej).Właśnie dlatego powinieneś takie skanowanie uruchomić w momencie kiedy przez dłuższy okres czasu komputer nie będzie używany (na przykład w nocy).

  Możesz harmonogramować zadania skanowania aby uruchamiać je w odpowiedniej chwili.Upewnij się że pozostawiasz swój komputer włączony.Korzystając z Windows Vista, upewnij się że system nie przejdzie do trybu uśpienie w momencie gdy zaplanowane są zadania.

- Jeśli często podbierasz pliki z Internetu do konkretnego folderu, stwórz nowe zadanie i Ustaw ten folder jako cel skanowania.Ustaw zadanie, aby uruchamiało się codziennie lub częściej.

- Istnieją wirusy które ustawiają swoje wywołanie podczas uruchomienia systemu Windows zmieniając jego ustawienia.Aby chronić komputer przed tego typu zagrożeniami, możesz zaplanować zadanie **Skaner Autologowania**.Pamiętaj, że skanowanie przy zalogowaniu się do systemu może wpłynąć na jego wydajność przez krótki czas po starcie.

15.2.2. Kreator Skanowania Antywirusowego

Gdy w dowolnym momencie rozpoczniesz skanowanie na żądanie (np. klikniesz prawym przyciskiem myszy na folder i wybierzesz **Skanuj z BitDefender**), pojawi się Kreator Skanowania Antywirusowego.Wykonaj następujące trzy kroki procedury aby zakończyć skanowanie komputera.

Notatka

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

Krok 1/3 – Skanowanie

BitDefender rozpocznie skanowanie zaznaczonych elementów.

Zobaczysz status skanowania oraz statystyki (szybkość skanowania, czas, liczbę przeskanowanych / zainfekowanych / podejrzanych / ukrytych oraz innych elementów).

Zaczekaj aż BitDefender zakończy skanowanie.

Notatka
Proces skanowania może chwilę potrwać, w zależności od złożoności skanowania.

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:

- **Chcę podać hasło do tego obiektu.** Jeśli chcesz aby BitDefender przeskanował archiwum, wybierz tą opcję i podaj hasło.Jeśli nie znasz hasła, wybierz jedną z pozostałych opcji.
- **Nie chcę podawać hasła.** Wybierz tą opcję aby pominąć skanowanie tego archiwum.
- **Nie chcę podawać hasła do żadnego z archiwów (pomiń wszystkie obiekty zabezpieczone hasłem).** Wybierz tą opcję jeśli nie chcesz być pytany o archiwa zabezpieczone hasłem.BiDefender nie będzie w stanie ich skanować, ale informacja na ich temat zostanie zostanie zapisana w dzienniku skanera.

Kliknij **OK** aby kontynuować skanowanie.

Przerywanie lub zatrzymywanie skanowania. Możesz przerwać skanowanie klikając **Stop&Tak**. Przejdziesz bezpośrednio do ostatniego kroku kreatora.Aby tymczasowo wstrzymać skanowanie kliknij **Wstrzymaj**. Będziesz musiał kliknąć **Wznów** aby wznowić skanowanie.

Krok 2/3 – Wybierz Działanie

Po zakończeniu skanowania, pojawi się nowe okno zawierające wyniki skanowania.

Jeśli brak jest zagrożeń, które nie zostały rozwiązane, kliknij **Kontynuuj**.W przeciwnym razie musisz skonfigurować nowe działania, które będą podejmowane względem nierozwiązanych zagrożeń, w celu ochrony systemu.

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:

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

Usuń wirusa
Usuwa złośliwy kod z zainfekowanych plików.

Usuń
Usuwa wykryte pliki z dysku.

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 *„Kwarantanna”* (p. 81).

Zmień nazwę pliku
Zmienia nazwę ukrytych plików dodając `.bd.ren` do ich nazwy.Dzięki temu, będziesz mógł znaleźć tego typu pliki na swoim komputerze, jeśli takowe istnieją.

Zwróć uwagę na to, że ukryte pliki to nie te, które sam celowo ukrywasz przy użyciu Windows. Chodzi o pliki ukryte przez specjalne programy, znane jako rootkity.Rootkity z reguły nie powodują zniszczeń. Ich zadanie polega na ukrywaniu wirusów i oprogramowania szpiegującego przed oprogramowaniem antywirusowym.

Kliknij **Kontynuuj** aby zastosować wybrane działanie.

Krok 3/3 – Wyświetl Wyniki

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
Jeśli będzie to wymagane, proszę zrestartować system aby zakończyć proces czyszczenia.

Kliknij **Zamknij** aby zamknąć okno.

BitDefender Nie Mógł Rozwiązać Niektórych Zagadnień

W większości wypadków BitDefender leczy zarażone pliki lub izoluje je.Istnieją jednak zagadnienia, których nie można rozwiązać automatycznie.Więcej informacji na temat ręcznego usuwania złośliwego oprogramowania zawiera *„Usuwanie Złośliwego Oprogramowania z Systemu”* (p. 186).

BitDefender Wykrył Podejrzane Pliki

Podejrzane pliki to pliki wykrywane przez analizę heurystyczną jako potencjalnie zainfekowane wirusem którego sygnatura jeszcze nie została wydana.

Jeśli podejrzane pliki zostały wykryte podczas skanowania, zostaniesz poproszony o wysłanie ich do Laboratorium BitDefendera.Kliknij **OK** aby wysłać pliki do laboratorium BitDefendera w cel dalszej analizy.

15.2.3. Przeglądanie Dzienników Skanowania

Po każdym skanowaniu tworzy jest dziennik skanowania.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 **Pokaż dziennik**.

Sprawdzanie dzienników skanowania w późniejszym terminie:

1. Otwórz BitDefender.
2. Kliknij łącze **Pokaż dzienniki** znajdujące się w prawym dolnym rogu okna.
3. Kliknij **Antyvirus** w menu po lewej stronie.
4. W sekcji **Zadania na żądanie** można sprawdzić ostatnio wykonywane skanowania.Kliknij dwukrotnie zdarzenie na liście, aby zobaczyć więcej szczegółów na jego temat.Aby otworzyć dziennik skanowania, kliknij **Pokaż dziennik skanowania**.Dziennik skanowania otworzy się w twojej domyślnej przeglądarce internetowej.

Aby usunąć wpis dziennika, kliknij go prawym przyciskiem myszy i wybierz **Usuń**.

15.2.4. Zarządzanie Istniejącymi Zadaniami Skanowania

BitDefender mak kilka domyślnych zadań, które zaspokajają najczęstsze zagadnienia bezpieczeństwa. Możesz również tworzyć swoje własne zadania skanowania.Aby uzyskać więcej informacji, odwołaj się do *„Jak utworzyć niestandardowe zadanie skanowania?”* (p. 160).

Zarządzanie istniejącymi zadaniami skanowania:

1. Otwórz BitDefender.
2. W zależności od wybranego trybu wyświetlania interfejsu użytkownika postępuj zgodnie z poleceniami:

   Widok średniozaawansowany

   Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Antywirusa**.

   Przejdź do zakładki **Skanowanie**.

Widok eksperta

Przejdź do **Antywirus > Skanowanie**.

Notatka

W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

Są trzy kategorie zadań skanowania:

- **Zadania Systemowe** - zawiera listę domyślnych zadań systemowych. Dostępne są następujące zadania:

  Pełne Skanowanie

  Skanuje cały system wyłączając archiwa.W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów.

  Szybkie skanowanie

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

  Skaner Autologowania

  Skanuje elementy które są uruchamiane podczas logowania użytkownika do systemu Windows.Domyślnie, skaner autologowania jest wyłączony.

  Jeżeli chcesz korzystać z tego narzędzia zaznacz **Harmonogram** i ustaw uruchomienia zadania **przy starcie systemu**.Możesz określić jak długo po starcie systemu zadanie powinno się ono uruchomić (w minutach).

  Głębokie Skanowanie

  Skanuje cały system.W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.

  Notatka

  Ponieważ **Głębokie Skanowanie** oraz **Pełne Skanowanie** skanują cały system, może to chwile potrwać. Zatem, sugerujemy uruchomić to na niskim priorytecie, lub lepiej kiedy nie korzystasz z komputera.

- **Zadania użytkownika** - zawiera zadania zdefiniowane przez użytkownika.

  Zadanie nazwane `Moje Dokumenty` utworzone.Użyj tego zadania do skanowania ważnych folderów aktualnego użytkownika: `Moje Dokumenty`, `Pulpit` oraz `Autostart`. To zapewni bezpieczeństwo dokumentów, miejsca pracy oraz uruchamianych aplikacji.

- **Pomniejsze zadania** - zawiera listę różnych zadań skanowania. Zadania te odpowiadają alternatywnym typom skanowania, które nie mogą być uruchomione z tego okienka. Możesz tylko modyfikować ich ustawienia lub zobaczyć raporty skanowania.Dostępne są następujące zadania:

  Skanowanie urządzenia
  BitDefender może automatycznie wykrywać podłączenie do komputera nowego urządzenia magazynującego i skanować je.Użyj tego zadania do skonfigurowania opcji automatycznego wykrywania i skanowania urządzeń magazynujących (napędów CD/DVD, urządzeń magazynujących USB lub zmapowanych dysków sieciowych).

  Skanowanie kontekstowe
  Zadania tego używa się podczas skanowania za pośrednictwem menu kontekstowego Windows lub przy użyciu paska aktywności skanera.Opcje skanowania możesz modyfikować, tak aby lepiej odpowiadały twoim potrzebom.

Zadaniami skanowania można zarządzać za pomocą przycisków lub skrótów menu.

Aby uruchomić zadanie systemowe lub zdefiniowane przez użytkownika, kliknij odpowiadający mu przycisk **Uruchom Zadanie**.Pojawi się Kreator skanowania antywirusowego i przeprowadzi cię przez proces skanowania.

Aby skonfigurować automatyczne uruchamianie zadania skanowania w późniejszym terminie lub w regularnych odstępach czasu, kliknij odpowiedni przycisk **Harmonogram** i według uznania skonfiguruj harmonogram zadania.

Możesz skasować zadanie z którego już nie korzystasz (stworzone przez użytkownika) klikając na przycisk **Usuń**, który znajduje się po prawej.Nie możesz usuwać zadań systemowych.

Każde zadanie skanowania posiada okno Właściwości, w którym można skonfigurować ustawienia skanowania i przejrzeć dzienniki skanowania.Aby otworzyć to okno, kliknij na przycisk **Właściwości** po lewej stronie zadania (lub kliknij prawym przyciskiem myszy na zadanie i wybierz **Właściwości**).

Więcej informacji zawierają następujące tematy:

- *„Konfigurowanie Ustawień Skanowania”* (p. 74)
- *„Ustawianie Celu Skanowania”* (p. 76)
- *„Planowanie Zadania Skanowania”* (p. 77)

Używanie Menu Skrótów

Menu Skrótów jest dostępne dla każdego zadania. Aby je otworzyć kliknij prawym przyciskiem na wybranym zadaniu.

Dla zadań zdefiniowanych przez użytkownika dostępne są następujące komendy z menu skrótów:

- **Skanuj Teraz** - uruchamia zaznaczone zadanie.
- **Ścieżki** - otwiera okno **Właściwości**,zakładkę Ścieżki, gdzie możesz zmienić miejsce które ma być skanowane przez to zadanie.W przypadku zadań systemowych, ta opcja jest zastąpiona przez **Pokaż Skanowane Ścieżki**, ponieważ możesz zobaczyć tylko skanowany obiekt.
- **Harmonogram** - otwiera okno **Właściwości**, zakładkę Harmonogram , gdzie możesz zaplanować zaznaczone zadanie.
- **Pokaż Dzienniki** - otwiera okno**Właściwości**, zakładka Dzienniki umożliwia sprawdzenie wszystkich dzienników wygenerowanych dla wybranego zadania.
- **Klonuj zadanie** - duplikuje wybrane zadanie.Jest to szczególnie przydatne podczas tworzenia nowego zadania, ponieważ możesz modyfikować ustawienia zduplikowanego zadanie.
- **Usuń** - usuwa wybrane zadanie.

Notatka

Dostępny tylko dla zadań utworzonych przez użytkownika. Domyślnego zadania nie można usunąć.

- **Właściwości** - otwiera okno **Wlasciwości**, zakładka Przegląd umożliwia zmianę ustawień wybranego zadania.

Ze względu na specyficzną naturę kategorii **Różne Zadania**, tylko opcje **Pokaż Dzienniki** i **Właściwości** są dostępne.

Konfigurowanie Ustawień Skanowania

Aby skonfigurować opcje skanowania wybranego zadania, kliknij je prawym klawiszem myszy i wybierz **Właściwości**.

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

Skonfigurować można także następujące opcje ogólne:

- **Uruchom zadanie z niskim priorytetem.** Obniża priorytet procesu skanowania. Pozwala innym programom działać szybciej i zwiększa czas potrzebny na zakończenie skanowania.
- **Minimalizuj Kreator Skanowania do zasobnika w pasku systemowym.** Minimalizuje okno skanowania do paska systemowego. Kliknij dwukrotnie ikonę BitDefender aby otworzyć okno skanowania.
- Określ działanie, które zostanie podjęte w przypadku nieznalezienia zagrożenia.

Zaawansowani użytkownicy mogą dokonywać zmian w ustawieniach skanowania oferowanych przez BitDefendera. Skaner może być ustawiony, aby skanować podane rozszerzenia plików, skanować przed konkretnym zagrożeniem lub pomijać archiwa. Może to znacząco zredukować czas skanowania i poprawić komfort pracy podczas skanowania.

Szczegółowe konfigurowanie ustawień skanowania:

1. Kliknij **Własny**.
2. Skonfiguruj ustawienia skanowania według uznania.Aby dowiedzieć się za co odpowiada dana opcja, przytrzymaj nad nią kursor myszy i przeczytaj informację która pojawi się na dole okna.
3. Kliknij **OK** aby zapisać zmiany i zamknąć okno.

Ta informacja może być przydatna:

- Jeśli nie znasz pewnych określeń, sprawdź je w słowniku.Możesz także uzyskać więcej informacji przeszukując Internet.
- **Poziom skanowania.** Określ typ złośliwego oprogramowania, które BitDefender ma wyszukać poprzez wybranie odpowiednich opcji.
- **Skanowanie plików.** BitDefender można ustawić na skanowanie wszystkich typów plików lub tylko aplikacji (plików programów) albo określonych typów plików, które użytkownik uznał za niebezpieczne.Najlepszą ochronę zapewnia skanowanie wszystkich plików, natomiast skanowanie jedynie aplikacji jest szybsze.

  Aplikacje (lub pliki programów) są bardziej narażone na ataki złośliwego oprogramowania od plików innego typu.Ta kategoria obejmuje następujące rozszerzenia plików:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Jeśli wybierasz **Skanowanie tylko zdefiniowanych rozszerzeń**, zaleca się objęcie nim rozszerzeń wszystkich aplikacji oraz innych rozszerzeń plików, które uznasz za niebezpieczne.
- **Skanuj tylko nowe i zmienione pliki.** Skanując tylko nowe lub zmienione pliki można znacząco poprawić ogólny czas reakcji systemu kosztem rezygnacji z niewielkiej tylko części ochrony.
- **Skanowanie wewnatrz archiwów.** Archiwa zawierające zainfekowane pliki nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa systemu.Złośliwe oprogramowanie może zaatakować system tylko wtedy, gdy zainfekowany plik zostanie wypakowany i uruchomiony bez włączonej ochrony w czasie rzeczywistym.Zaleca się użycie tej opcji, w celu wykrycia i usunięcia wszelkich potencjalnych zagrożeń, nawet jeśli nie jest to zagrożenie bezpośrednie.

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

- **Opcje dzialania.** Określ akcje, które zostaną podjęte dka poszczególnych typów wykrytych plików korzystając z opcji w tej kategorii.Wykryte pliki dzielą się na trzy kategorie:
  - **Pliki zainfekowane.** Pliki, w których wykryto infekcje, są zgodne z sygnaturami w Bazie Danych Sygnatur Złośliwego Oprogramowania BitDefender.BitDefender może usunąć kod złośliwego oprogramowania z zainfekowanego pliku i odtworzyć oryginalny plik. Operacja ta znana jest jako dezynfekcja.

    Notatka
    Sygnatury złośliwego oprogramowania to urywki kodu wypakowane z rzeczywistych próbek tego oprogramowania. Są one używane przez programy antywirusowe do porównywania wzorców i wykrywania złośliwego oprogramowania.
    Baza Danych Sygnatur Złośliwego Oprogramowania BitDefender to zbiór sygnatur złośliwego oprogramowania uaktualniany co godzinę przez naukowców BitDefender, zajmujących się złośliwym oprogramowaniem.

  - **Podejrzane pliki.** Pliki są wykrywane jako podejrzane przez analizę heurystyczną.Podejrzanych plików nie można zdezynfekować, ponieważ brak jest służących do tego procedur.
  - **Ukryte pliki (rootkity).** Zwróć uwagę na to, że ukryte pliki to nie te, które sam celowo ukrywasz przy użyciu Windows. Chodzi o pliki ukryte przez specjalne programy, znane jako rootkity.Rootkity z reguły nie powodują zniszczeń. Ich zadanie polega na ukrywaniu wirusów i oprogramowania szpiegującego przed oprogramowaniem antywirusowym.

  Bez posiadania ważnego powodu nie powinno się zmieniać domyślnych działań podejmowanych względem wykrytych plików.

  Aby ustawić nową akcję, kliknij na **Pierwsza akcja** i wybierz opcję z menu.Określ **Drugą akcję** która zostanie podjęta, jeśli pierwsza zawiedzie.

Kliknij **OK** aby zapisać zmiany i zamknąć okno. Aby uruchomić zadanie po prostu kliknij **Skanuj**.

Ustawianie Celu Skanowania

Nie możesz modyfikować celu skanowania zadań skanowania z kategorii **Zadania Systemowe**.Możesz tylko zobaczyć ich cel skanowania.Aby zobaczyć cel skanowania określonego zadania systemowego skanowania, kliknij prawym przyciskiem myszy zadanie i wybierz **Pokaż Ścieżki Skanowania**.

Aby ustawić cel skanowania dla wybranego zadania użytkownika, kliknij prawym przyciskiem na zadanie i wybierz **Ścieżki**. Alternatywnie, jeśli już znajdujesz się w oknie Właściwości zadania, wybierz zakładkę **Ścieżki**.

Możesz zobaczyć listę dysków lokalnych, sieciowych i przenośnych oraz pliki i foldery wcześniej dodane. Wszystkie zaznaczone elementy będą skanowane po uruchomieniu zadania.

Dostępne są następujące przyciski:

- **Dodaj Element(y)** - otwiera okno przeglądania gdzie możesz wybrać plik(i) / folder(y) które chcesz skanować.

Notatka
Użyj przeciągnij i upuść, aby dodać pliki/foldery do listy.

- **Usuń Plik(i)** - usuwa plik(i) / folder(y) poprzednio wybrane z listy obiektów do skanowania.

Poza tymi przyciskami, jest jeszcze kilka opcji, które pozwalają szybko wybrać lokalizacje do skanowania.

- **Dyski Lokalne** - aby skanować dyski lokalne.
- **Dyski Sieciowe** - aby skanować wszystkie dyski sieciowe.
- **Dyski Przenośne** - aby skanować dyski przenośne (CD-ROM, stacja dyskietek, itp.)
- **Wszystko** - aby skanować wszystkie dyski, bez względu na to czy są lokalne, sieciowe czy przenośne.

Kliknij **OK** aby zapisać zmiany i zamknąć okno. Aby uruchomić zadanie po prostu kliknij **Skanuj**.

Planowanie Zadania Skanowania

Przy złożonych zadaniach, proces skanowania zajmuje trochę czasu i działa najlepiej jeśli zamkniesz wszystkie programy. Dlatego najlepszym rozwiązaniem będzie zaplanowanie takich zadań wtedy, gdy nie korzystasz z komputera i jest on w trybie oczekiwania.

Aby zobaczyć harmonogram dla wybranego zadania albo go zmodyfikować, kliknij prawym przyciskiem myszy na zadanie i wybierz **Harmonogram**. Jeśli już znajdujesz się w oknie Właściwości zadania, wybierz zakładkę **Harmonogram**.

Możesz zobaczyć harmonogram zadania, jeśli taki jest.

Podczas planowania zadanie, musisz wybrać jedną z opcji:

- **Nie** - uruchamia zadanie tylko na prośbę użytkownika.
- **Raz** - uruchamia skanowanie tylko raz w określonym momencie. Ustaw datę i czas rozpoczęcia w polach **Data/Czas Rozpoczęcia**.

- **Okresowo** - uruchamia skanowanie okresowo, w określonym przedziale (minuty, godziny, dni, tygodnie, miesiące) zaczynając o ustalonej dacie i czasie.
- **Przy uruchomieniu systemu** - uruchamia skanowanie po podanej ilości minut po zalogowaniu użytkownika do systemu.

Kliknij **OK** aby zapisać zmiany i zamknąć okno. Aby uruchomić zadanie po prostu kliknij **Skanuj**.

15.3. Konfigurowanie Wyjątków Skanowania

Występują przypadki gdy musisz wykluczyć niektóre pliki ze skanowania. Na przykład, możesz chcieć wykluczyć plik testowy EICAR ze skanowania przy dostępie lub pliki `.avi` ze skanowania na żądanie.

BitDefender zezwala na wykluczanie obiektów ze skanowania przy dostępie lub na żądanie (lub obu). Ta cecha jest przeznaczona do zmniejszenia czasu skanowania oraz uniknięcia przeszkadzania w pracy.

Dwa rodzaje obiektów mogą zostać wykluczone ze skanowania:

- **Ścieżki** - plik lub folder (ze wszystkimi elementami wewnątrz niego) ze wskazaną ścieżką zostanie wykluczony ze skanowania.
- **Rozszerzenia** - wszystkie pliki o określonym rozszerzeniu będą wykluczone ze skanowania bez względu na to, gdzie są umieszczone na twardym dysku.

Obiekty wykluczone ze skanowania przy dostępie nie zostaną przeskanowane, nie ważne czy zostały otwarte przez ciebie czy przez aplikację.

Notatka

W skanowaniu kontekstowym wyjątki NIE są stosowane.Skanowanie kontekstwowe jest typem skanowania na żądanie: klikasz prawym przyciskiem myszy na folder który chcesz skanować i wybierasz **Skanuj z BitDefender**.

15.3.1. Wyłączanie Plików lub Folderów ze Skanowania

Wykluczanie ścieżek ze skanowania:

1. Otwórz BitDefender.
2. W zależności od wybranego trybu wyświetlania interfejsu użytkownika postępuj zgodnie z poleceniami:

   Widok średniozaawansowany

   Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Antywirusa**.

   Przejdź do zakładki **Wyjątki**.

   Widok eksperta

   Przejdź do **Antywirus > Wyjątki**.

Notatka

W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

3. Aby włączyć wyjątki skanowania, zaznacz odpowiednie pole wyboru.
4. Uruchom kreatora konfiguracji, wykonując następujące polecenia:
   - Prawym przyciskiem myszy kliknij tabelę Pliki i Foldery, i wybierz **Dodaj nową ścieżkę**.
   - Kliknij przycisk **Dodaj**, znajdujący się w górnej części tabeli wyjątków.
5. Witamy w Kreatorze Konfiguracji.Możliwość poruszania się w kreatorze zapewniają przyciski **Dalej** i **Cofnij**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.
   a. Wybierz opcję wykluczenia ścieżki ze skanowania.Krok ten pojawia się tylko wtedy, gdy uruchamiasz kreatora, klikając przycisk **Dodaj**.
   b. By wykluczyć ścieżki ze skanowania użyj którejś z następujących metod:
      - Kliknij **Przeglądaj**, wybierz plik lub folder, który chcesz wykluczyć, ze skanowania i kliknij **Dodaj**.
      - Wpisz ścieżkę, którą chcesz wykluczyć ze skanowania w polu edycji i kliknij **Dodaj**.

      Ścieżki pojawią się na liście gdy będziesz je dodawał. Możesz dodać tyle ścieżek ile chcesz.
   c. Domyślnie, wybrane ścieżki są wykluczone ze skanowania przy dostępie i na żądanie. Aby zmienić to przy dodawaniu wyjątku, kliknij prawą kolumnę i wybierz odpowiednią opcję z listy.
   d. Wysoce zalecane jest skanowanie podanych ścieżek aby się upewnić że nie są one zainfekowane.Zaznacz odpowiednie pole aby skanować te pliki przed wykluczeniem ich ze skanowania.

      Kliknij **Zakończ**, aby dodać wyjątki skanowania.
6. Kliknij **Zastosuj** aby zapisać zmiany.

15.3.2. Wyłączanie Rozszerzeń Plików ze Skanowania

Wykluczanie rozszerzeń plików ze skanowania:

1. Otwórz BitDefender.
2. W zależności od wybranego trybu wyświetlania interfejsu użytkownika postępuj zgodnie z poleceniami:

Widok średniozaawansowany

Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Antywirusa**.

Przejdź do zakładki **Wyjątki**.

Widok eksperta

Przejdź do **Antywirus > Wyjątki**.

Notatka

W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

3. Aby włączyć wyjątki skanowania, zaznacz odpowiednie pole wyboru.
4. Uruchom kreatora konfiguracji, wykonując następujące polecenia:
   - Prawym przyciskiem myszy kliknij tabelę Wyjątki i wybierz **Dodaj nowe wyjątki**.
   - Kliknij przycisk **Dodaj**, znajdujący się w górnej części tabeli wyjątków.
5. Witamy w Kreatorze Konfiguracji.Możliwość poruszania się w kreatorze zapewniają przyciski **Dalej** i **Cofnij**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.
   a. Wybrano opcję wykluczenia rozszerzeń ze skanowana.Krok ten pojawia się tylko wtedy, gdy uruchamiasz kreatora, klikając przycisk **Dodaj**.
   b. Aby określić rozszerzenia do wykluczenia ze skanowania użyj którejś z następujących metod:
      - Wybierz z menu rozszerzenie które chcesz wykluczyć ze skanowania i kliknij **Dodaj**.

        Notatka

        Menu zawiera listę wszystkich rozszerzeń zarejestrowanych w twoim komputerze. Gdy wybierasz rozszerzenie, możesz zobaczyć jego opis jeśli jest dostępny.

      - Wpisz rozszerzenie, które chcesz wykluczyć ze skanowania w polu edycji i kliknij **Dodaj**.

      Rozszerzenia pojawią się w tabeli gdy je dodasz. Możesz dodać tyle rozszerzeń ile chcesz.

   c. Domyślnie, wybrane rozszerzenia są wykluczone ze skanowania dostępowego i na żądanie. Aby zmienić kiedy zastosować wyjątki, kliknij na prawą kolumnę i wybierz opcję z listy.
   d. Zaleca się skanowanie plików o określonych rozszerzeniach, w celu upewnienia się, iż nie są zainfekowane.

Kliknij **Zakończ**, aby dodać wyjątki skanowania.

6. Kliknij **Zastosuj** aby zapisać zmiany.

15.3.3. Zarządzanie Wyjątkami Skanowania

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

Zarządzanie wyjątkami skanowania:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Wyjątki**.

Aby usunąć element z tabeli, zaznacz go i kliknij **Usuń**.

Aby edytować element z tabeli, zaznacz go i kliknij **Edytuj**.Pojawi się nowe okno w którym możesz zmienić rozszerzenia, ścieżki do wykluczenia i typ skanowania, które chcesz wykluczyć, według potrzeb. Dokonaj wymaganych zmian i kliknij **OK**.

Notatka

Możesz również kliknąć prawym klawiszem myszy na obiekt i wykorzystać opcje menu do edytowania lub usunuęcia go.

Aby wyłączyć wyjątki skanowania, usuń zaznaczenie odpowiednich pól wyboru.

15.4. Kwarantanna

BitDefender pozwala na izolowanie zainfekowanych lub podejrzanych plików w bezpiecznym obszarze pod nazwą kwarantanna. Przez izolowanie tych plików w kwarantannie ryzyko zainfekowania nie ma miejsca, a w tym samym czasie masz możliwość wysłać te pliki do laboratorium BitDefender w celu dalszej analizy.

Notatka

Kiedy wirus znajduje się w kwarantannie nie może uczynić żadnej szkody ponieważ nie może być uruchomiony lub otwierany.

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

Przeglądanie i zarządzanie plikami poddanymi kwarantannie oraz konfigurowanie ustawień kwarantanny:

1. Otwórz BitDefender.
2. W zależności od wybranego trybu wyświetlania interfejsu użytkownika postępuj zgodnie z poleceniami:

Widok średniozaawansowany

Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Antywirusa**.

Przejdź do zakładki **Kwarantanna**.

Widok eksperta

Przejdź do **Antywirus > Kwarantanna**.

Notatka

W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

Zarządzanie Plikami w Kwarantannie

Możesz wysłać zaznaczony plik z kwarantanny do laboratorium BitDefender klikając **Wyślij**.Domyślnie, BitDefender automatycznie wyśle pliki z kwarantanny co 60 minut.

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**.

Konfigurowanie Ustawień Kwarantanny

Aby skonfigurować ustawienia kwarantanny kliknij **Ustawienia**.Używając ustawień kwarantanny, możesz ustawić BitDefendera aby automatycznie wykonywał następujące działania:

Usuń stare pliki. Aby automatycznie usuwać stare pliki z kwarantanny, zaznacz odpowiednią opcje.Musisz określić liczb dni po których pliki z kwarantanny zostaną usunięte i częstotliwość z jaką BitDefender powinien sprawdzać stare pliki.

Automatycznie wysyłaj pliki. Aby automatycznie wysyłać pliki z kwarantanny, zaznacz odpowiednią opcje.Musisz określić częstotliwość z jaką pliki mają być wysyłane.

Skanuj pliki z kwarantanny po aktualizacji. Aby automatycznie skanować pliki z kwarantanny po przeprowadzeniu aktualizacji, zaznacz odpowiednią opcje.Możesz wybrać aby czyste pliki były automatycznie przywracane do ich oryginalnych lokacji zaznaczając **Przywróć czyste pliki**.

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

16. Ochrona antyphishing

BitDefender Antyphishing zapobiega wykradzeniu danych osobowych podczas przeglądania Internetu informując o potencjalnych stronach phishingowych.

BitDefender zapewnia ochronę w czasie rzeczywistym dla:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

16.1. Konfigurowanie Antyphishingowej Białej Listy

Możesz skonfigurować i zarządzać białą listą witryn internetowych, które nie będą skanowane przez BitDefender.Biała lista powinna zawierać tylko strony którym całkowicie ufasz.Przykładowo, dodaj stronę www na której aktualnie robisz zakupy online.

Notatka

Możesz łatwo dodawać strony do białej listy z paska narzędzi BitDefender Antyphishing zintegrowanego z twoją przeglądarką www.Aby uzyskać więcej informacji, odwołaj się do *„Zarządzanie Ochroną antyphishingową BitDefender w programach Internet Explorer i Firefox”* (p. 83).

Konfigurowanie i zarządzanie antyphishingową białą listą:

- Jeśli korzystasz z obsługiwanej przeglądarki internetowej, kliknij pasek narzędziowy BitDefender i wybierz z menu **Białą listę**
- Możesz także wykonać następujące kroki:
  1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
  2. Przejdź do **Antywirus > Tarcza**.
  3. Kliknij **Biała lista**.

By dodać witrynę do Białej Listy, podaj jej adres w odpowiednim polu i kliknij **Dodaj**.

Jeśli chcesz usunąć stronę www z białej listy, kliknij **Usuń**.

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

16.2. Zarządzanie Ochroną antyphishingową BitDefender w programach Internet Explorer i Firefox

BitDefender integruje się bezpośrednio poprzez łatwy w użyciu pasek narzędzi z następującymi przeglądarkami:

- Internet Explorer

- Mozilla Firefox

Możesz łatwo i wydajnie zarządzać ochroną antyphishingową oraz Białą Listą używając paska zadań BitDefender Antypishing zintegrowanego z jedną z powyższych przeglądarek.

Pasek narzędziowy antyphishing, reprezentowany przez ikonę BitDefender, znajduje się w górnej części okna przeglądarki.Kliknij go by otworzyć menu paska zadań.

Notatka

Jeśli nie widzisz paska zadań, otwórz **Widok**menu, pokaż**paski zadań** i sprawdź **BitDefender pasek zadań**.

Następujące opcje są dostępne w menu paska zadań:

- **Włącz / Wyłącz** - włącza lub wyłącza zabezpieczenie antyphishingowe dla wybranej przeglądarki.
- **Ustawienia** - otwiera okno, w którym możesz wybrać ustawienia paska narzędzi antypishingu.Dostępne są następujące opcje:
  - **Ochrona Antyphishingowa WWW w czasie rzeczywistym** - wykrywa i informuje cię, gdy strona www chce wykraść twoje prywatne dane.Ta opcja kontroluje zabezpieczenie antyphishingowe BitDefender tylko w obecnej przeglądarce www.
  - **Pytaj przed dodaniem do Białej Listy** - pyta przed dodaniem strony internetowej do Białej Listy.
- **Dodaj do Białej Listy** - dodaje stronę internetową do Białej Listy.

WAŻNE

Dodanie strony internetowej do Białej Listy oznacza, że BitDefender nie będzie jej skanował przed phishingiem. Zalecamy dodanie do Białej Listy tylko stron do których masz pełne zaufanie.

- **Biała Lista** - otwiera Białą Listę.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Antyphishingowej Białej Listy”* (p. 83).
- **Zgłoś jako Phishing** - informuje BitDefender Lab o tym, że podejrzewasz daną stronę o próby kradzieży poufnych informacji.Przez zgłaszanie stron www pomagasz chronić innych użytkowników przed próbami kradzieży poufnych danych.
- **Pomoc** - otwiera elektroniczną dokumentację.
- **O programie** - otwiera okno, w którym możesz przeczytać o BitDefenderze i gdzie szukać pomocy jeśli zdarzy się coś niespodziewanego.

17. Szukaj doradców

Asystent wyszukiwania zwiększa ochronę przed zagrożeniami z Internetu, ostrzegając przed phishingowymi lub niegodnymi zaufania stronami internetowymi bezpośrednio na stronie z wynikami wyszukiwania.

Asystent wyszukiwania działa z każdą przeglądarką internetową i sprawdza wyniki wyszukiwania wyświetlane przez większość popularnych wyszukiwarek:

- Google
- Yahoo!
- Bing

Asystent wyszukiwania wskazuje, czy wynik wyszukiwania jest bezpieczny. W tym celu przed łączem umieszcza małą ikonę stanu.

Zielone kółko: Możesz bezpiecznie użyć tego łącza.

Czerwone kółko z wykrzyknikiem: Jest to strona phishingowa lub niegodna zaufania.Nie powinieneś otwierać tego łącza.Jeśli korzystasz z programu Internet Explorer lub Firefox i próbujesz otworzyć dane łącze, BitDefender automatycznie zablokuje tę stronę internetową i zamiast niej wyświetli stronę alarmu.Jeśli chcesz zignorować alarm i przejść na daną stronę, postępuj zgodnie z instrukcjami wyświetlonymi na stronie alarmu.

17.1. Wyłączanie Asystenta Wyszukiwania

Wyłączanie Asystenta wyszukiwania:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Preferencje**.
2. Przejdź do **Ustawień Zabezpieczeń**.
3. Użyj przełącznika, aby wyłączyć Asystenta wyszukiwania.

18. Antyspam

Spam to termin określający niechcianą pocztę.Spam jest narastającym problemem zarówno dla użytkowników indywidualnych jak i instytucjonalnych. Nie chciałbyś, aby twoje dzieci go oglądały gdyż może zawierać np. treści erotyczne. Możesz być zwolniony z pracy za otrzymywanie poczty o treściach erotycznych. Z reguły nie możesz nic zrobić, aby zaprzestać otrzymywania Spamów. Niestety Spamów jest wiele i pojawiają się w szerokiej gamie kształtów i rozmiarów.

BitDefender Antyspam zawiera wiele innowacji technologiczne i oferujące najwyższe standardy filtry antyspamowe by odnaleźć spam zanim dotrze on do twojej Skrzynki Odbiorczej.Aby uzyskać więcej informacji, odwołaj się do *„Wnikliwość Antyspamu”* (p. 86).

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

Notatka

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

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

- W Microsoft Outlook, wiadomości te przenoszone są do folderu **Spam**, zlokalizowanego w folderze **Usunięte**.Folder **Spam** jest tworzony podczas instalacji BitDefendera.
- W Outlook Express i Windows Mail, wiadomości spam są przenoszone automatycznie do folderu **Elementy usunięte**.
- W Mozilla Thunderbird, wiadomości są przenoszone do folderu **Spam**, zlokalizowanego w folderze **Kosz**.Folder **Spam** jest tworzony podczas instalacji BitDefendera.

Jeśli używasz innych klientów poczty, musisz utworzyć regułę do przenoszenia wiadomości e-mail oznakowanych jako [spam] Według BitDefender do niestandardowego folderu kwarantanny.

18.1. Wnikliwość Antyspamu

18.1.1. Filtry Antyspamu

Silnik Antyspamowy BitDefendera zawiera kilka różnych filtrów aby zabezpieczyć twoją skrzynkę przed spamem: Lista przyjaciół, Lista spamerów, Filtr języków, Filtr obrazków, Filtr URL, Filtr Heurystyczny i Filtr Bayesian.

Lista Przyjaciół / Lista Spamerów

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

Notatka

Zalecamy dodawać nazwę twojej listy przyjaciół i adresów email do **Listy przyjaciół**. BitDefender nie blokuje wiadomości od osób na tej liście, dlatego też dodawanie przyjaciół zapewnia przepływ ważnych wiadomości.

Filtr Języków

Wiele wiadomości Spam jest napisana Cyrylicą i / lub czcionką Azjatycką. Filtr Języków wykrywa tego typu wiadomości i oznacza je jako SPAM.

Filtr Obrazków

Ostatnio skrzynki odbiorcze są zapełniane coraz większą ilością maili zawierających tylko grafiki z nie chcianą zawartością, które unikają wykrycia przez filtry heurystyczne. BitDefender zaproponował rozwiązanie narastającego problemu poprzez zastosowanie **Filtra Obrazków** który porównuje sygnatury obrazu z sygnaturami w bazie danych BitDefendera. W przypadku dopasowania, e-mail będzie zaznaczony jako spam.

Filtr URL

Niemal wszystkie wiadomości spam zawierają linki do różnych stron www. Które zawierają reklamy oferujące możliwości zakupienia reklamowanych towarów oraz czasami są używane do phishingu.

BitDefender zawiera bazę danych takich linków.Filtr URL sprawdza każdy link URL w wiadomości porównując go z bazą danych. Jeśli je dopasuje wiadomość jest oznaczana jako SPAM.

Filtr Heurystyczny

The **Filtr Heurystyczny** wykonuje zestaw testów na wszystkich składnikach wiadomości (tj. nie tylko w nagłówku, ale także całej wiadomości zarówno w formacie HTML jak i w tekstowym) szukając słów, zwrotów, linków i innych cech SPAMU.Bazując na rezultacie analizy, dodaje zapis SPAM do wiadomości.

Filtr wykrywa również wiadomości oznaczone jako TREŚCI EROTYCZNE: w temacie wiadomości i oznacza je jako SPAM.

Notatka
Począwszy od 19 maja 2004 roku spam, który zawiera materiały o tematyce seksualnej musi zawierać ostrzeżenie TREŚCI EROTYCZNE: w linii tematu lub złamie prawo.

Filtr Bayesian

Moduł **Filtra Bayesian** klasyfikuje wiadomości na podstawie informacji statystycznej dotyczącej wskaźnika, przy którym pojawiają się określone słowa w wiadomościach sklasyfikowanych jako Spam w porównaniu do tych - nie Spam (przez ciebie lub filtr heurystyczny).

Oznacza to np., że jeżeli pewne czteroliterowe słowo pojawia się dużo częściej w spamie, zakłada się wzrost prawdopodobieństwa, że następna przychodząca wiadomość jest Spamem. Wszystkie istotne słowa w wiadomości są brane pod uwagę. Przez dokonywanie syntezy informacji statystycznej prawdopodobieństwo, że cała wiadomość jest spamem jest obliczona.

Ten moduł przedstawia kolejną interesującą cechę: elastyczność. Szybko przystosowuje się do typu wiadomości otrzymywanych przez danego użytkownika i przechowuje informacje o wszystkim. Aby funkcjonować wydajnie filtr musi być uczony, aby był prezentowany z próbkami spam i istotnymi wiadomościami. Czasami filtr musi być poprawiony – ponaglony, aby się przystosował, kiedy podejmie błędną decyzję.

WAŻNE
Możesz dokonać korekty filtru Bayesian korzystając z przycisków **To jest Spam** and **To nie jest Spam** w w pasku narzędziowym Antyspamu .

18.1.2. Działanie Antyspamu

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

Każdy e-mail, który przychodzi jest najpierw sprawdzany w przez filtr Lista przyjaciół / Lista spamerów. Jeżeli adres nadawcy jest znaleziony w Lista przyjaciół email bezpośrednio jest przenoszony do **Skrzynka odbiorcza**.

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

Innaczej, Filtr językowy sprawdzi czy email jest napisany Cyrylicą lub czcionką Azjatycką. Jeżeli tak, email będzie potraktowany jako SPAM i przeniesiony do folderu **Spam**.

Jeżeli email nie jest napisany Cyrylicą lub czcionką Azjatycką, zostanie on przepuszczony do Filtr obrazków. **Filtr obrazków** będzie wykrywał wszystkie e-maile z załączonymi obrazkami zawierającymi spam.

Filtr URL porówna łącza znalezione w wiadomości e-mail z łączami z bazy danych znanych łączy spamowych BitDefender. W przypadku znalezienia wspólnych cech, wiadomość zostanie uznana za SPAM.

Filtr (heurystyczny) NeuNet przejmie e-mail i przeprowadzi serię testów na wszystkich składnikach tej wiadomości, szukając słów, wyrażeń, łączy oraz innych cech charakterystycznych dla spamu.W oparciu o wyniki analizy, dana wiadomość e-mail otrzyma ocenę spamową.

Notatka
Jeżeli email jest oznaczony jako SEKSUALNY w linii tematu, BitDefender potraktuje go jako SPAM.

Moduł Filtra Bayesian będzie analizował wiadomość na podstawie informacji statystycznej dotyczącej wskaźnika, przy którym pojawiają się określone słowa w wiadomościach sklasyfikowanych jako Spam w porównaniu do tych jako nie Spam (przez ciebie lub filtr heurystyczny). Wynik Spam zostanie dodany do email.

Jeśli suma ocen spamu (ocena heurystyczna + ocena bayesowska) przekracza poziom progowy, wiadomość e-mail zostaje uznana za SPAM.Poziom progowy jest określony przez poziom ochrony antyspamowej.Aby uzyskać więcej informacji, odwołaj się do *„Dostosowywanie Poziomu Ochrony”* (p. 94).

18.1.3. Aktualizacje Antyspamu

Za każdym razem gdy wykonujesz aktualizacje:

- nowe sygnatury obrazów będą dodawane do **Filtra Obrazków**.
- nowe adresy będą dodane do **Filtra URL**.
- nowe reguły będą dodane do **Filtra Heurystycznyego**.

Dzięki temu zwiększa się skuteczność silnika Antspamowego.

Aby chronić Cię przed spamerami BitDefender może przeprowadzać automatyczne aktualizację. Miej włączoną opcje **Automatycznej Aktualizacji**.

18.2. Kreator Optymalizacji Modułu Antyspam

Gdy pierwszy raz uruchomisz klienta poczty po zainstalowaniu BitDefendera, pojawi się kreator który pomoże tobie skonfigurować Listę Przyjaciół i Listę Spamerów oraz nauczyć Filtr Baysian aby zwiększyć efektywność filtrów Antyspamu.

Notatka
Kreator może być uruchomiony w każdej chwili kiedy klikniesz przycisk **Kreator** na pasku narzędzi Antyspamu.

Możliwość poruszania się w kreatorze zapewniają przyciski **Dalej** i **Cofnij**.Jeśli chcesz pominąć etap konfiguracji, wybierz **Pomiń ten krok**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Okno Powitania**
2. **Dodaj Kontakty do Listy przyjaciół**

   Tutaj możesz obejrzeć wszystkie adresy zawarte w twojej **Książce Adresowej**. Proszę wybierz te, które chcesz, aby były dodane do twojej **Listy Przyjaciół** (zalecamy wybrać je wszystkie). Będziesz otrzymywać wszystkie wiadomości email z tych adresów bez względu na ich zawartość.

   Aby dodać wszystkie kontakty do listy przyjaciół, zaznacz **Wybierz wszystko**.
3. **Usuń Bazę Danych Bayesian**

   Notatka
   Gdy po raz pierwszy uruchomisz tego kreatora, przejdź do kolejnego kroku.

   Możesz zauważyć, że twój Filtr Antyspamu zaczął tracić wydajność. Przyczyną może być niewłaściwe nauczenie (tj. pomyłkowo oznaczyłeś dużą ilość istotnych wiadomości jako spam lub na odwrót). Jeżeli twój filtr jest bardzo niedokładny konieczne może okazać się wyczyszczenie bazy danych filtra i ponowne nauczenie filtra podążając za kolejnymi krokami kreatora.

   Wybierz **Wyczyść bazę danych filtra Antyspam** jeżeli chcesz zresetować Bazę danych Bayesian.

   Możesz zachować bazę danych filtra Bayesian do pliku, tak aby móc z niej skorzystać ponownie, np. po reinstalacji oprogramowania.Aby zachować bazę danych filtra Bayesian kliknij na przycisk **Zapisz filtr Bayesian** i zapisz ją do wybranej lokalizacji.Plik będzie miał rozszerzenie `.dat`.

   Aby załadować poprzednio załadowaną bazę Bayesian, kliknij na przycisk **Wczytaj filtr Bayesian** i otwórz odpowiedni plik.
4. **Trenowanie Filtru Bayesowskiego na Dozwolonych Wiadomościach Spamowych (nie będących spamem)**

   Proszę wybierz folder, który zawiera ważne wiadomości email. Te wiadomości będą wykorzystane do nauki filtra Bayesian.

   Są dwie zaawansowane opcje w liście adresów:
   - **Uwzględnij wszystkie podfoldery** - aby do zaznaczenia dodać także wszystkie podfoldery.
   - **Automatycznie dodaj do listy Przyjaciół** - dodaje nadawców do listy Przyjaciół.
5. **Trenowanie Filtru Bayesowskiego na Wiadomościach Spamowych**

   Proszę wybierz folder, który zawiera wiadomości Spam. Te wiadomości będą wykorzystane do nauki Filtra Antispam.

WAŻNE
Proszę upewnij się, że folder, który wybrałeś nie zawiera ważnych email, w przeciwnym razie wykonanie antyspam będzie zredukowane.

Są dwie zaawansowane opcje w liście adresów:

- **Uwzględnij wszystkie podfoldery** - aby do zaznaczenia dodać także wszystkie podfoldery.
- **Automatycznie dodaj do listy Spamerów** - dodaje nadawców do listy Spamerów.Wiadomości e-mail od tych odbiorców będą zawsze oznaczone jako SPAM i odpowiednio traktowane.

6. **Podsumowanie**

   W tym oknie możesz obejrzeć wszystkie ustawienia, dla konfiguracji instalatora i możesz dokonywać zmian przez powrót do poprzednich kroków (kliknij **Cofnij**).

   Jeśli nie chcesz robić żadnych zmian kliknij **Zakończ**.

18.3. Korzystanie z Paska Narzędziowego Antyspamu w Oknie Klienta Poczty

W górnej części okna twojego klienta e-mail powinieneś zobaczyć pasek Antyspamu.Pasek Antyspamu pomaga ci zarządzać zabezpieczeniem antyspamowym bezpośrednio z poziomu klienta poczty.Możesz poprawić BitDefender, jeśli błędnie zakwalifikował wiadomości e-mail jako spam.

WAŻNE
BitDefender jest zintegrowany z najbardziej popularnymi klientami poczty dzięki wykorzystaniu łatwego w użyciu paska narzędziowego antyspam.W celu uzyskania kompletnej listy obsługiwanych klientów poczty e-mail, odwołaj się do *„Wymagania Systemowe”* (p. 2).

Każdy klawisz jest wyjaśniony poniżej:

- **To jest Spam** - wysyła wiadomość do modułu Bayesian wskazując że ta wiadomość jest spamem. Wiadomość zostanie oznaczona jako SPAM i przeniesiona do folderu **Spam**.

  Podobne wiadomości przychodzące w przyszłości będą oznaczone jako SPAM.

- **To nie jest Spam** - wysyła wiadomość do modułu Bayesian wskazując że ta wiadomość nie jest spamem i BitDefender nie powinien był jej tak oznaczać.Wiadomość zostanie przeniesiona z folderu **Spam** do folderu **Skrzynka Odbiorcza**.

  Podobne wiadomosci przychodzace w przyszlosci beda oznaczone nie jako SPAM.

WAŻNE

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

- **Dodaj Spamera** - dodaje nadawcę wybranej wiadomości e-mail do listy Spamerów.Możesz zostać zapytany(a) o potwierdzenie, klikając na **OK**.Wiadomości e-mail pochodzące od adresów zawartych w liście Spamerów są automatycznie oznaczane jako `[spam]`.
- **Dodaj Przyjaciela** - dodaje nadawcę wybranej wiadomości e-mail do listy Przyjaciół.Możesz zostać zapytany(a) o potwierdzenie, klikając na **OK**.Będziesz zawsze otrzymywał wiadomości email z tego adresu bez względu na zawartość wiadomości.
- **Spamerzy** - otwiera **Liste Spamerów** która zawiera wszystkie adresy email z których nie chcesz otrzymywać wiadomości bez względu na ich zawartość.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Listy Spamerów"* (p. 96).
- **Przyjaciele** - otwiera **Listę Przyjaciół**, która zawiera wszystkie adresy email, z których zawsze chcesz odbierać wiadomości bez względu na ich zawartość.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Listy Przyjaciół"* (p. 95).
- **Ustawienia** - otwiera okno **Ustawienia** w którym możesz skonfigurować niektóre opcje modułu **Antyspamu**.
- **Kreator** - otwiera kreatora optymalizacji modułu antyspam.Ten kreator pomaga w trenowaniu Filtru bayesowskiego, dzięki czemu można uzyskać lepszą wydajność ochrony antyspamowej.Możesz także dodać adresy z Książki Adresowej do listy Przyjaciół lub Spamerów.
- **Antyspam BitDefender** - otwiera okno, w którym można skonfigurować poziom ochrony antyspamowej oraz filtry antyspamowe.

18.3.1. Wskazywanie Błędów Wykrywania

Jeśli używasz obsługiwanych klientów poczty, możesz łatwo poprawić filtr antyspam (przez wskazanie które wiadomości e-mail nie powinny być oznaczane jako `[spam]`). Dzięki temu znacząco poprawisz skuteczność filtra antyspam.Podążaj tymi krokami:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu śmieci, gdzie zostały przeniesione wiadomości spam.
3. Wybierz dozwoloną wiadomość nieprawidłowo oznaczoną przez BitDefender jako `[spam]`.

4. Kliknij przycisk **Dodaj Przyjaciela** znajdujący się na pasku narzędziowym antyspamu aby dodać nadawcę do listy Przyjaciół.Możesz zostać zapytany(a) o potwierdzenie, klikając na **OK**.Będziesz zawsze otrzymywał wiadomości email z tego adresu bez względu na zawartość wiadomości.
5. Kliknij przycisk **To nie jest Spam** znajdujący się w pasku antyspamu BitDefender (zazwyczaj znajduje się on w górnej części okna klienta poczty). Filtr uczący potraktuje tą wiadomość jako prawidłową. Wszystkie następne wiadomości tego typu będą przenoszone do folderu Skrzynki Odbiorczej.Następne wiadomości e-mail pasujące do tego samego wzoru nie będą oznaczane jako `[spam]`.

18.3.2. Wskazywanie Niewykrytych Wiadomości o Spamie

Jeśli używasz obsługiwanego klienta poczty, możesz łatwo wskazać, które z wiadomości mają być traktowane jako spam. Dzięki temu w dużym stopniu zwiększysz skuteczność filtra antyspamowego.Podążaj tymi krokami:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu Skrzynki Odbiorczej.
3. Wybierz niewykryte wiadomości spam.
4. Kliknij przycisk **To jest Spam** znajdujący się w pasku antyspamu BitDefender (zazwyczaj znajduje się on w górnej części okna klienta poczty). Filtr uczący potraktuje tą wiadomość jako spam. Wszystkie następne wiadomości tego typu będą oznaczane jako `[spam]` i będą trafiać do folderu na śmieci.Następne wiadomości e-mail pasujące do tego samego wzoru będą oznaczane jako `[spam]`.

18.3.3. Ponowny trening mechanizmu uczącego się (bayesowskiego)

Jeśli filtr antyspamowy jest bardzo niedokładny, konieczne może być wymazanie Bayesowskiej bazy danych i ponownie uczenie Filtru Bayesowskiego.

Zanim przystąpisz do trenowania uczącego się filtra (Bayesian), przygotuj dwa foldery - jeden zawierający wyłącznie spam i drugi, zawierający wyłącznie poprawne wiadomości.Uczący się filtr analizuje je i uczy się z określonych charakterystyk opisujących spam i poprawne wiadomości które otrzymujesz. Aby trenowanie filtra zwiększyło jego skuteczność, potrzeba przynajmniej 50 wiadomości w każdym z folderów.

Aby wyczyścić bazę danych Bayesian i wytrenować uczący się filtr od nowa, wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Na pasku narzędziowym antyspamu, kliknij przycisk **Kreator** aby uruchomić kreator konfiguracji antyspamu.
3. Kliknij **Dalej**.

4. Wybierz **Pomiń ten krok** i kliknij **Dalej**.
5. Wybierz **Wyczyść bazę danych filtra antyspamowego** i kliknij **Dalej**.
6. Wybierz folder zawierający prawidłowe wiadomości i kliknij **Dalej**.
7. Wybierz folder zawierający wiadomości SPAM i kliknij **Dalej**.
8. Kliknij **Zakończ** aby rozpocząć proces trenowania.
9. Kiedy trenowanie się zakończy, kliknij na **Zamknij**.

18.3.4. Zapisywanie i Wczytywanie Bayesowskiej Bazy Danych

Możesz zachować bazę danych filtra Bayesian do pliku, tak aby móc z niej skorzystać ponownie, np. po reinstalacji oprogramowania.

Kliknij przycisk **Ustawienia**, znajdujący się na pasku narzędziowym antyspamu BitDefender.

Aby zachować bazę danych filtra Bayesian kliknij na przycisk **Zapisz filtr Bayesian** i zapisz ją do wybranej lokalizacji.Plik będzie miał rozszerzenie `.dat`.

Aby załadować poprzednio załadowaną bazę Bayesian, kliknij na przycisk **Wczytaj filtr Bayesian** i otwórz odpowiedni plik.

18.3.5. Konfigurowanie Głównych Ustawień

Aby skonfigurować ogólne ustawienia antyspamu dla klienta poczty, kliknij przycisk **Ustawienia** na pasku antyspam BitDefender.

Dostępne są następujące opcje:

- **Przenieś wiadomość do Elementy Usunięte** - aby przenieść wiadomości spam do **Elementy Usunięte** (tylko dla Microsoft Outlook Express / Windows Mail);
- **Zaznacz wiadomośc jako przeczytane** - aby zaznaczyć wszystkie wiadomości Spam jako przeczytane tak aby tobie nie przeszkadzały kiedy przyjdzie nowa wiadomość Spam.

Kliknij zakładkę **Alarmy** jeśli chcesz wejść do sekcji gdzie możesz wyłączyć okno potwierdzenia dla przycisków **Dodaj Spamera** i **Dodaj Przyjaciela**.

W oknie **Alarmy** możesz ponadto właczyć/wyłączyć alarm **Proszę zaznacz wiadomość email**. Alarm ten pojawia się kiedy zaznaczysz grupę zamiast wiadomości email.

18.4. Dostosowywanie Poziomu Ochrony

Niektóre filtry antyspamowe mogą identyfikować wiadomości spamowe bezpośrednio, inne natomiast dodają do wiadomości ocenę, która przydzielana jest na podstawie wykrytych cech charakterystycznych.

Poziomu ochrony antyspamowej używa się do określenia, czy wiadomość e-mail można uznać za spam w oparciu o jej łączną ocenę (otrzymaną po dokonaniu kontroli przez wszystkie filtry antyspamowe).

Poziomu ochrony antyspamowej nie powinno się zmieniać, chyba że nie działa ona zgodnie z oczekiwaniami.Problemu nie należy rozwiązywać poprzez niezależną zmianę poziomu ochrony, lecz raczej poprzez zapoznanie się z *„Filt Antyspamu Nie Działa Poprawnie”* (p. 178) i postępowanie zgodne z podanymi instrukcjami.

Dostosowywanie poziomu ochrony antyspamowej:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antyspam > Stan**.
3. Przeciągnij suwak wzdłuż skali, aby ustawić odpowiedni poziom ochrony.Aby ustawić domyślny poziom bezpieczeństwa (**Umiarkowany do Agresywnego**) kliknij **Domyślny**.

Użyj opisów po prawej stronie skali, aby wybrać poziom ochrony najlepiej spełniający twoje wymagania.Opis informuje także o wszelkich dodatkowych działaniach, które należy podjąć, aby uniknąć potencjalnych problemów lub zwiększyć wydajność wykrywania spamu.

18.5. Konfigurowanie Listy Przyjaciół

Listy przyjaciół jest listą wszystkich adresów email, z których zawsze chcesz otrzymywać wiadomości bez względu na ich zawartość. Wiadomości od twoich przyjaciół nie są oznaczane jako Spam nawet jeżeli ich zawartość przypomina Spam.

Notatka

Każdy przychodzący mail z **listy przyjaciół**, będzie automatycznie dostarczany do twojej skrzynki Przychodzące bez dalszych procesów.

Konfigurowanie i zarządzanie listą przyjaciół:

- Jeśli używasz programu Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, kliknij przycisk **Przyjaciele** znajdujący się na pasku narzędziowym antyspamu BitDefender zintegrowanym z klientem poczty.
- Możesz także wykonać następujące kroki:
  1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
  2. Przejdź do **Antyspam > Stan**.
  3. Kliknij na **Zarządzaj Przyjaciółmi**.

Aby dodać adres e-mail, wybierz opcję **Adres e-mail**, wpisz go i kliknij przycisk znajdujący się obok pola edycji.Składnia: nazwa@omena.com.

Aby dodać adres e-mail z określonej domeny, wybierz opcję **Nazwa domeny**, wpisz nazwę domeny i kliknij przycisk znajdujący się obok pola edycji.Składnia:

- @domena.com, *domena.com i domena.com - wszystkie przychodzące maile z domena.com dostaną się do twojej poczty **Przychodzące** bez względu na ich zawartość;
- *domena* - wszystkie przychodzące maile z domena ((bez względu na przyrostki domeny) dostaną się do twojej poczty **Przychodzące** bez względu na ich zawartość;
- *com - wszystkie maile posiadające przyrostek domeny com dostaną się do twojej poczty **Przychodzące** bez względu na ich zawartość;

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

Aby usunąć element z listy, zaznacz go i kliknij na przycisk **Usuń**.Aby usunąć wszystkie wpisy z tej listy, kliknij na **Wyczyść listę** a następnie **Tak**, aby potwierdzić wybór.

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

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

Kliknij **Zastosuj** oraz **OK** aby zapisać i zamknąć **listę przyjaciół**.

18.6. Konfigurowanie Listy Spamerów

Listy Spamerów jest listą wszystkich adresów email, z których nie chcesz otrzymywać wiadomości bez względu na ich zawartość.Każdy przychodzący mail z adresu z **listy spamerów** będzie automatycznie oznaczony jako Spam, bez dalszego procesu.

Konfigurowanie i zarządzanie listą spamerów:

- Jeśli używasz programu Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, kliknij przycisk **Spamerzy**, który znajduje się na zintegrowanym z klientem poczty pasku narzędziowym antyspamu BitDefender.
- Możesz także wykonać następujące kroki:
  1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
  2. Przejdź do **Antyspam > Stan**.
  3. Kliknij na **Zarządzaj Spamerami**.

Aby dodać adres e-mail, wybierz opcję **Adres e-mail**, wpisz go i kliknij przycisk znajdujący się obok pola edycji.Składnia: nazwa@omena.com.

Aby dodać adres e-mail z określonej domeny, wybierz opcję **Nazwa domeny**, wpisz nazwę domeny i kliknij przycisk znajdujący się obok pola edycji.Składnia:

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

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

Ostrzeżenie

Nie dodawaj do listy Spamerów domen pochodzących ze znanych serwisów (takich jak Onet, WP, Interia, Gmail, Hotmail lub inne). Każda wiadomość od użytkowników zarejestrowanych w takiej usłudze zostałaby oznaczona jako spam.Na przykład, jeśli dodasz `yahoo.com` do listy Spamerów, wszystkie wiadomości przychodzące z adresów `yahoo.com` będą oznaczone jako `[spam]`.

Aby usunąć element z listy, zaznacz go i kliknij na przycisk **Usuń**.Aby usunąć wszystkie wpisy z tej listy, kliknij na **Wyczyść listę** a następnie **Tak**, aby potwierdzić wybór.

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

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

Kliknij **Zastosuj** oraz **OK** aby zapisać i zamknąć **listę spamerów**.

18.7. Konfigurowanie Ustawień i Filtrów Antyspamu

Zgodnie z tym, co opisano w *„Wnikliwość Antyspamu”* (p. 86), do identyfikowania spamu BitDefender używa kombinacji różnych filtrów antyspamowych.Filtry antyspamowe są skonfigurowane wcześniej, aby zapewnić skuteczną ochronę.

Można wyłączyć lub zmienić ustawienia dowolnego z tych filtrów, jednak nie jest to zalecane.Oto niektóre zmiany, które możesz zechcieć wprowadzić:

- W zależności od tego, czy otrzymujesz dozwolone wiadomości pisane w językach azjatyckich lub cyrylicą, wyłącz lub włącz ustawienie, które automatycznie blokuje takie wiadomości e-mail.

  Notatka

  Odpowiednie ustawienie jest wyłączone w zlokalizowanych wersjach programu, korzystających z takich właśnie zestawów znaków (na przykład w wersji rosyjskiej lub chińskiej).

- Jeśli nie chcesz automatycznie dodawać odbiorców wysłanych wiadomości e-mail do listy przyjaciół, wyłącz odpowiednie ustawienie.W tym wypadku dodaj swoje kontakty do listy przyjaciół w sposób opisany w *„Konfigurowanie Listy Przyjaciół"* (p. 95).
- Zaawansowani użytkownicy mogą próbować dostosować rozmiar słownika bayesowskiego, aby uzyskać lepszą wydajność antyspamową.Mniejsza liczba słów oznacza szybsze, lecz mniej precyzyjne przetwarzanie spamu.Duża liczba słów zwiększa dokładność wykrywania spamu, ale uzyskanie dostępu do wiadomości e-mail zabiera więcej czasu.

  Notatka

  Osiągnięcie wymaganej wydajności może wymagać kilku zmian rozmiaru słownika bayesowskiego.Jeśli wynik nie jest zgodny z oczekiwaniami, przywróć domyślny i zalecany rozmiar 200 tys. słów.

Konfigurowanie ustawień antyspamu i filtrów:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antyspam > Ustawienia**.
3. Skonfiguruj ustawienia według uznania.Aby dowiedzieć się za co odpowiada dana opcja, przytrzymaj nad nią kursor myszy i przeczytaj informację która pojawi się na dole okna.
4. Kliknij **Zastosuj** aby zapisać zmiany.

Aby zastosować domyślne ustawienia, kliknij **Domyślne**.

19. Kontrola Rodzcielska

Konfiguracja Kontroli Rodzicielskiej BitDefendera pozwala tobie na kontrolowanie dostępu do Internetu i podanych aplikacji dla każdego użytkownika mającego konto w systemie.

Możesz skonfigurować Kontrole Rodzicielską aby blokowała:

- Nieodpowiednie strony internetowe.
- dostęp do Internetu w podanych okresach czasu (np. gdy jest czas na odrabianie lekcji).
- Strony internetowe, wiadomości e-mail oraz wiadomości IM które zawierają podane w regułach kontroli rodzicielskiej słowa kluczowe.
- Aplikacje takie jak gry, komunikatory, programy do udostępniania plików i wiele innych.
- Wiadomości odbierane od kontaktów IM innych niż wcześniej dozwolone.

WAŻNE

Tylko użytkownicy z prawami administracyjnymi (administratorzy systemu) mają dostęp do Kontroli rodzicielskiej.Aby się upewnić że tylko ty możesz zmieniać ustawieni Kontroli Rodzicielskiej dla użytkowników, możesz chronić ustawienia hasłem.Zostaniesz poproszony o skonfigurowanie hasła kiedy włączysz moduł Kontroli Rodzicielskiej dla któregoś użytkownika.

Po skonfigurowaniu Kontroli Rodzicielskiej możesz łatwo dowiedzieć się, co twoje dzieci robiły na komputerze.

Możesz sprawdzać aktywność dzieci oraz zmieniać ustawienia Kontroli Rodzicielskiej za pomocą Zdalnej Kontroli Rodzicielskiej, nawet gdy nie ma cię w domu.

19.1. Konfigurowanie Kontroli Rodzicielskiej

Przed skonfigurowaniem Kontroli Rodzicielskiej utwórz osobne konta użytkowników Windows przeznaczone dla dzieci. Dzięki temu będziesz dokładnie wiedział, co każde z nich robi przy komputerze. Powinieneś utworzyć ograniczone (standardowe) konta użytkownika, aby nie mogły one zmieniać ustawień Kontroli Rodzicielskiej.Aby uzyskać więcej informacji, odwołaj się do *„Jak utworzyć konto użytkownika Windows?”* (p. 164).

Jeśli dziecko ma na swoim komputerze dostęp do konta administratora, musisz skonfigurować hasło, aby chronić ustawienia Kontroli Rodzicielskiej.Aby uzyskać więcej informacji, odwołaj się do *„Ochrona Ustawień Kontroli Rodzicielskiej”* (p. 101).

Konfigurowanie Kontroli Rodzicielskiej:

1. Upewnij się, że jesteś zalogowany na komputerze z kontem administratora.Tylko użytkownicy z prawami administracyjnymi (administratorzy systemu) mają dostęp do Kontroli rodzicielskiej.
2. Otwórz BitDefender.
3. Przejdź do ustawień Kontroli Rodzicielskiej. W zależności od trybu wyświetlania interfejsu użytkownika wykonaj następujące polecenia:

   Widok średniozaawansowany
   Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Kontrola Rodzicielska**.

   Widok eksperta
   W menu po lewej stronie kliknij **Kontrolę Rodzicielską**.

   Notatka

   W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

Możesz zobaczyć informację dotyczącą stanu Kontroli Rodzicielskiej dla każdego konta użytkownika Windows.Jeśli Kontrola Rodzicielska jest włączona, pod nazwą każdego użytkownika wyświetlana jest kategoria wiekowa.Jeśli Kontrola Rodzicielska jest wyłączona, jej stan to **nie skonfigurowana**.

Konfigurowanie Kontroli Rodzicielskiej dla określonego konta użytkownika:

1. Użyj przełącznika, aby włączyć Kontrolę Rodzicielską dla tego konta.
2. Zostaniesz poproszony o założenie hasła Kontroli Rodzicielskiej.Ustaw hasło aby chronić ustawienia Kontroli Rodzicielskiej.Aby uzyskać więcej informacji, odwołaj się do *„Ochrona Ustawień Kontroli Rodzicielskiej”* (p. 101).
3. Ustaw kategorię wiekową aby pozwolić twojemu dziecku na dostęp do tych stron które są odpowiednie w jego wieku.Ustawienie wieku dziecka spowoduje automatyczne wczytanie ustawień uznanych za właściwe dla tej kategorii wiekowej, ustalonej na bazie standardów rozwoju dziecka.
4. Jeśli chcesz skonfigurować szczegółowe ustawienia Kontroli Rodzicielskiej, kliknij **Ustawienia**.Kliknij zakładkę, aby skonfigurować odpowiednią funkcję Kontroli Rodzicielskiej:

   - **Strony WWW** - aby filtrować przeglądane strony internetowe w zależności od reguł ustawionych w sekcji Strony WWW.
   - **Aplikacje** - aby blokować dostęp do aplikacji określonych w sekcji Aplikacje.
   - **Słowa Kluczowe** - aby filtrować strony WWW, wiadomości komunikatorów IM i wiadomości e-mail ze słów określonych w sekcji Słowa Kluczowe.

- **Komunikowanie** - zezwala lub blokuje czat z kontaktami IM zgodnie z regułami ustalonymi przez użytkownika w sekcji Komunikowanie.

Notatka
Aby nauczyć się jak je konfigurować, proszę odnieść się do następujących tematów w tym rozdziale.

Skonfiguruj opcje monitorowania według uznania:

- **Wyślij mi raport aktywności jako wiadomość e-mail.** Powiadomienie e-mail jest wysyłane za każdym razem, gdy Kontrola Rodzicielska BitDefender zablokuje określoną czynność.Najpierw musisz skonfigurować ustawienia powiadamiania.
- **Zapisz ruch internetowy w dzienniku.** Zapisuje adresy stron odwiedzanych przez użytkowników z włączoną Kontrolą Rodzicielską.

Aby uzyskać więcej informacji, odwołaj się do *„Monitorowanie Dziecięcej Aktywności”* (p. 108).

Jeśli chcesz zdalnie monitorować i kontrolować aktywność dzieci przy komputerze i w Internecie, za pomocą przełącznika włącz Zdalną Kontrolę Rodzicielską.Aby uzyskać więcej informacji, odwołaj się do *„Zdalna kontrola rodzicielska”* (p. 111).

19.1.1. Ochrona Ustawień Kontroli Rodzicielskiej

Jeżeli nie jesteś jedynym użytkownikiem danego komputera z prawami administratora, zaleca się żebyś chronił swoje ustawienia Kontroli Rodzicielskiej hasłem.Ustawiając hasło, uniemożliwisz innym użytkownikom z prawami administracyjnymi zmienianie ustawień Kontroli Rodzicielskiej które skonfigurujesz dla konkretnego użytkownika.

BitDefender domyślnie zapyta ciebie o ustawienie hasła przy włączaniu Kontroli Rodzicielskiej.Aby ustawić zabezpieczenie hasłem, wykonaj następujące kroki:

1. Wpisz hasło w polu **Hasło**.
2. Wpisz hasło ponownie w polu **Potwierdź hasło** by je potwierdzić.
3. Kliknij **OK** aby zapisać hasło i zamknąć okno.

Gdy ustawisz hasło, przy każdej próbie zmiany ustawień Kontroli Rodzicielskiej, będziesz poproszony o wprowadzenie hasła.Inni administratorzy systemowi (jeśli są) także będą musieli podać to hasło by zmienić ustawienia Kontroli Rodzicielskiej.

Notatka
To hasło nie będzie chronić innych ustawień BitDefendera.

Jeśli nie ustawisz hasła i nie będziesz chciał aby to okno się ukazało ponownie, zaznacz **Nie pytaj o hasło przy włączaniu Kontroli Rodzicielskiej**.

WAŻNE
Jeśli zapomnisz hasła, będziesz musiał ponownie zainstalować program lub skontaktować się z BitDefender, w celu uzyskania pomocy.

Usuwanie ochrony hasłem:

1. Otwórz BitDefender i w prawym górnym rogu okna kliknij przycisk **Opcje**.
2. Przejdź do **Ustawień ogólnych**.
3. Użyj przełącznika, aby wyłączyć opcję **Ustawianie hasła**.
4. Wpisz hasło.
5. Kliknij **OK**.

19.1.2. Kontrola Stron WWW

Kontrola stron www pomaga blokować dostęp do serwisów webowych z nieodpowiednią zawartością. Lista kandydatów do zablokowania zarówno całych serwisów jak i ich części jest również częścią aktualizacji BitDefender, jak zwykły proces aktualizacji. Strony zawierające referencje (odnośniki) do serwisów www znajdujących się na czarnej liście również będą blokowane.

Notatka
Gdy włączysz Kontrolę Rodzicielską i określisz wiek dziecka, automatycznie włączy się Kontrola stron WWW. Zostanie ona skonfigurowana w taki sposób, aby blokować dostęp do witryn internetowych uznanych za nieodpowiednie dla danego wieku dziecka.

Konfigurowanie Kontroli stron WWW dla określonego konta użytkownika:

1. Przejdź do okna Ustawienia Kontroli Rodzicielskiej BitDefender dla tego konta użytkownika.
2. Kliknij zakładkę **Sieć WWW**.
3. Użyj przełącznika, aby włączyć Kontrolę stron WWW.
4. Możesz sprawdzić, jakie kategorie stron WWW są automatycznie blokowane / ograniczane dla aktualnie wybranej grupy wiekowej.Jeśli nie jesteś zadowolony z ustawień domyślnych, możesz skonfigurować je według własnego uznania.

   Aby zmienić działania skonfigurowane dla określonej kategorii treści internetowych, kliknij bieżący stan i wybierz z menu daną operację.
5. Jeśli chcesz, utwórz własne reguły dopuszczające lub blokujące dostęp do określonych witryn internetowych.Jeśli Kontrola Rodzicielska automatycznie blokuje dostęp do witryny internetowej, możesz utworzyć regułę, która wyjątkowo umożliwia dostęp do tej witryny.

6. Możesz określić, ile czasu dziecko może spędzać w Internecie.Aby uzyskać więcej informacji, odwołaj się do „Ograniczanie Dostępu do Internetu Według Czasu” (p. 103).

Tworzenie Reguł Kontroli Stron WWW

Aby zezwolić lub zablokować dostęp do strony, wykonaj następujące kroki:

1. Kliknij **Dopuść witrynę internetową** lub **Zablokuj witrynę internetową**.
2. Wprowadź adres strony w polu **Strona WWW**.
3. Wybierz akcję dla tej reguły - **Zezwól** lub **Blokuj**.
4. Kliknij **Zakończ** aby dodać regułę.

Zarządzanie Regułami Kontroli Stron WWW

Reguły Kontroli Stron WWW które zostały skonfigurowane są wyświetlone w tabeli w dolnej części okna. Obok każdej reguły znajduje się adres strony i jej obecny stan.

Aby usunąć regułę, wybierz ją i kliknij przycisk **Usuń**.

Aby edytować regułę, dwukrotnie ją kliknij lub zaznacz i kliknij **Edytuj**.Wprowadź niezbędne zmiany w oknie konfiguracji.

Ograniczanie Dostępu do Internetu Według Czasu

W części Harmonogram dostępu do sieci WWW można określić, ile czasu dziecko może spędzać w Internecie.

Aby całkowicie zablokować dostęp do Internetu, wybierz **Blokuj dostęp do sieci WWW**.

Ograniczanie dostępu do Internetu do określonych pór dnia:

1. Wybierz **Ogranicz czas dostępu do sieci WWW**.
2. Kliknij **Zmiana harmonogramu**.
3. Wybierz z siatki przedziały czasowe, w których dostęp do Internetu ma być zablokowany.Możesz klikać pojedyncze komórki lub kliknąć i przeciągać, aby objąć dłuższe okresy czasu.
4. Kliknij **Zapisz**.

Notatka

BitDefender będzie dokonywał aktualizacji bez względu na to, czy dostęp do Internetu jest zablokowany, czy nie.

19.1.3. Kontrola Aplikacji

Kontrola Aplikacji pomaga zablokować jakąkolwiek aplikację przed uruchomieniem. Możesz blokować gry, oprogramowanie typu komunikatory i czaty, jak również inne kategorie oprogramowania i złośliwy kod. Tak zablokowane aplikację są również chronione przed modyfikacjami i nie mogą być kopiowane ani przenoszone.Możesz zablokować aplikacje permanentnie lub podczas określonych przedziałów czasowych, np. gdy twoje dzieci powinny odrabiać zadanie domowe.

Konfigurowanie Kontroli Aplikacji dla określonego konta użytkownika:

1. Przejdź do okna Ustawienia Kontroli Rodzicielskiej BitDefender dla tego konta użytkownika.
2. Kliknij zakładkę **Aplikacje**.
3. Użyj przełącznika, aby włączyć Kontrolę Aplikacji.
4. Twórz reguły dla aplikacji, które chcesz blokować lub ograniczać do nich dostęp.

Tworzenie Reguł Kontroli Aplikacji

Aby zablokować lub ograniczyć dostęp do aplikacji, wykonaj następujące kroki:

1. Kliknij **Blokuj aplikację** lub **Ogranicz aplikację**.
2. Kliknij **Przeglądaj**, aby zlokalizować aplikację której chcesz zablokować lub ograniczyć dostęp.Aplikacje znajdują się zazwyczaj w folderze `C:\Program Files`.
3. Wybierz działanie reguły.
   - **Blokuj permanentnie** aby kompletnie zablokować dostęp aplikacji.
   - **Blokowanie oparte na tym harmonogramie** aby ograniczyć dostęp w określonych przedziałach czasowych.

   Jeśli zdecydujesz się ograniczyć dostęp zamiast zablokować w całości aplikację, musisz także ustawić na siatce przedziały czasowe w których dostęp ma być blokowany.
4. Aby dodać regułę, kliknij **Zapisz**.

Zarządzanie Regułami Kontroli Aplikacji

Reguły Kontroli Aplikacji które zostały skonfigurowane, są wyświetlane w tabeli w dolnej części okna. Nazwa każdej aplikacji, jej ścieżka oraz obecny stan są wyświetlane obok każdej reguły.

Aby usunąć regułę, wybierz ją i kliknij przycisk **Usuń**.

Aby edytować regułę, dwukrotnie ją kliknij lub zaznacz i kliknij **Edytuj**.Wprowadź niezbędne zmiany w oknie konfiguracji.

19.1.4. Kontrola słów kluczowych

Kontrola Słów Kluczowych pomaga blokować użytkownikom dostęp do wiadomości e-mail, stron WWW i rozmów IM które zawierają określone słowa.Za pomocą Kontroli Słów Kluczowych możesz uniemożliwić dziecku korzystającemu z Internetu zobaczenie nieodpowiednich słów lub wyrażeń.

Notatka
Kontrola Słów Kluczowych w aplikacjach komunikatorów jest dostępna tylko dla programów Yahoo Messenger i Windows Live (MSN) Messenger.

Konfigurowanie Kontroli słów kluczowych dla określonego konta użytkownika:

1. Przejdź do okna Ustawienia Kontroli Rodzicielskiej BitDefender dla tego konta użytkownika.
2. Kliknij zakładkę **Słowa kluczowe**.
3. Użyj przełącznika, żeby włączyć Kontrolę słów kluczowych.
4. Aby blokować nieprawidłowe słowa kluczowe, utwórz reguły Kontroli słów kluczowych.
5. Aby uniemożliwić dzieciom przekazywanie informacji osobistych (takich jak adres domowy lub numer telefonu) osobom, które spotkają w Internecie, musisz utworzyć reguły Kontroli tożsamości.Aby uzyskać więcej informacji, odwołaj się do „Tworzenie Reguł Kontroli Tożsamości” (p. 106).

Tworzenie Reguł Kontroli Słów Kluczowych

Aby zablokować słowo lub wyrażenie, wykonaj następujące kroki:

1. Kliknij **Blokuj słowo kluczowe**.
2. W polu edycji, wpisz słowo lub wyrażenie które chcesz zablokować. Jeśli chcesz aby wykrywane były tylko słowa, które pasują do niego w całości wybierz **Dopasuj całe słowa**.
3. Wybierz typ ruchu który BitDefender powinien skanować w poszukiwaniu zdefiniowanych słów.

Opcje	Opis
HTTP	Strony internetowe, które zawierają słowo kluczowe będą zablokowane.
POP3	Wiadomości e-mail, które zawierają słowo kluczowe będą zablokowane.
Komunikatory	Wiadomości IM które zawierają słowo kluczowe będą zablokowane.

4. Kliknij **Zakończ** aby dodać regułę.

Zarządzanie Regułami Kontroli Słów Kluczowych

Skonfigurowane reguły Kontroli słów kluczowych umieszczono w tabeli. Dla każdej reguły podano szczegółowe informacje.

Aby usunąć regułę, wybierz ją i kliknij przycisk **Usuń**.

Aby edytować regułę, dwukrotnie ją kliknij lub zaznacz i kliknij **Edytuj**.Wprowadź niezbędne zmiany w oknie konfiguracji.

Tworzenie Reguł Kontroli Tożsamości

Aby utworzyć regułę Kontroli tożsamości, kliknij odpowiedni przycisk **Blokuj słowo kluczowe**, a następnie wykonuj polecenia kreatora.Możliwość poruszania się w kreatorze zapewniają przyciski **Dalej** i **Cofnij**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Okno Powitania**
2. **Wybierz Typ i Dane Reguły**

   Ustaw następujące parametry:

   - **Nazwa Reguły** - wpisz nazwę reguły w polu edycji.
   - **Typ Reguły** - wybierz typ reguły (adres, imię, karta kredytowa, PIN, SSN itp).
   - **Dane Reguły** - wpisz dane które chcesz chronić w polu edycji.Przykładowo, jeśli chcesz chronić swój numer karty kredytowej, wpisz go lub jego część tutaj.

     WAŻNE
     Jeśli wpiszesz mniej niż trzy znaki, zostaniesz poproszony o wpisanie poprawnych danych. Zalecamy abyś wpisał przynajmniej trzy znaki w celu pominięcia błędu zablokowania wiadomości i stron www.

   Wszystkie wprowadzane dane są szyfrowane. Dla dodatkowego zabezpieczenia nie podawaj wszystkich danych które chcesz chronić.

3. **Wybieranie Opcji Skanowania**

   Wybierz rodzaj ruchu jaki ma być skanowany przez BitDefendera.

   - **Skanuj ruch internetowy (HTTP)** - skanuje ruch HTTP (strony WWW) i blokuje wysyłane dane które pasują do tych zapisanych w regule.
   - **Skanuj wiadomości e-mail (ruch SMTP)** - skanuje ruch SMTP (wiadomości) i blokuje wszystkie wychodzące wiadomości e-mail, które zawierają podane w regule ciągi znaków.
   - **Skanuj ruch IM (komunikatory)** - skanuje ruch IM i blokuje wszystkie wysyłane wiadomości, które zawierają podane w regule ciągi znaków.

Możesz wybrać zastosowanie reguły tylko jeśli zawartość reguły zgadza się z całymi słowami lub jeśli zawartość reguły i jakikolwiek wykryty ciąg znaków są identyczne.

4. **Opisz Regułę**

   Wprowadź krótki opis reguły w polu edycji.Ponieważ zablokowane dane (ciąg znaków) nie jest wyświetlany jako tekst przy dostępie do reguły, opis powinien pomóc w identyfikacji.

   Kliknij **Zakończ**.Reguła pojawi się w tabeli.

Od tej chwili każda próba wysłania podanych danych (przez wiadomość e-mail, komunikację natychmiastową lub stronę internetową) zakończy się niepowodzeniem. Wyświetlona zostanie wiadomość z ostrzeżeniem, wskazująca, że BitDefender zablokował wysłanie treści zawierającej informacje osobiste.

19.1.5. Kontrola Komunikatorów (IM)

Kontrola Komunikatorów (IM) umożliwia Ci wybranie kontaktów IM z którymi mogą rozmawiać twoje dzieci.

Notatka
Kontrola IM jest dostępna tylko dla Yahoo Messenger i Windows Live (MSN) Messenger.

Konfigurowanie Kontroli IM dla określonego konta użytkownika:

1. Przejdź do okna Ustawienia Kontroli Rodzicielskiej BitDefender dla tego konta użytkownika.
2. Kliknij zakładkę **Komunikowanie**.
3. Użyj przełącznika, żeby włączyć Kontrolę Komunikatorów.
4. Wybierz preferowaną metodę filtrowania i, w zależności od dokonanego wyboru, utwórz odpowiednie reguły.

   - **Zezwól na wszystkie kontakty IM, oprócz tych z listy.**

     W tym wypadku musisz określić identyfikatory IM, które mają zostać zablokowane (ludzi, z którymi dzieci nie powinny rozmawiać).

   - **Zablokuj rozmowy IM z wszystkimi kontaktami, oprócz tych na liście**

     W tym wypadku musisz określić identyfikatory IM, z którymi twoje dziecko może się komunikować.Na przykład, możesz dopuszczać komunikację natychmiastową z członkami rodziny, przyjaciółmi ze szkoły lub sąsiadami.

     Druga opcja zalecana jest w przypadku dzieci, mających mniej niż 14 lat.

Tworzenie Reguł Kontroli Komunikatorów (IM)

Aby zezwolić na lub blokować wymianę wiadomości z danym kontaktem, wykonaj następujące kroki:

1. Kliknij **Blokuj kontakt** lub **Dopuść kontakt**.
2. Wprowadź adres e-mail lub nazwę używaną przez kontakt IM w polu **E-mail lub identyfikator IM**.
3. Wybierz program IM który ma być przypisany do użytkownika.
4. Wybierz akcję dla tej reguły - **Zezwól** lub **Blokuj**.
5. Kliknij **Zakończ** aby dodać regułę.

Zarządzanie Regułami Kontroli Komunikatorów (IM)

Skonfigurowane reguły Kontroli IM umieszczone są w tabeli w dolnej części okna.

Aby usunąć regułę, wybierz ją i kliknij przycisk **Usuń**.

Aby edytować regułę, dwukrotnie ją kliknij lub zaznacz i kliknij **Edytuj**.Wprowadź niezbędne zmiany w oknie konfiguracji.

19.2. Monitorowanie Dziecięcej Aktywności

BitDefender pomaga śledzić czynności, które na komputerze wykonują przez twoje dzieci.

Gdy Kontrola Rodzicielska jest włączona, aktywność dzieci jest domyślnie rejestrowana. Dzięki temu można zawsze sprawdzić, jakie witryny internetowe odwiedziły, jakich używały aplikacji, jakie działania zostały zablokowane przez Kontrolę Rodzicielską, itp.

BitDefender można skonfigurować również w taki sposób, aby wysyłał powiadomienia przez e-mail, gdy Kontrola Rodzicielska zablokuje jakieś działanie.

19.2.1. Sprawdzanie Dzienników Kontroli Rodzicielskiej

Aby sprawdzić, co dzieci robiły ostatnio na komputerze, przejdź do dzienników Kontroli Rodzicielskiej.Podążaj tymi krokami:

1. Otwórz BitDefender.
2. Kliknij łącze **Pokaż dzienniki** znajdujące się w prawym dolnym rogu okna.
3. W menu po lewej stronie kliknij **Kontrolę Rodzicielską**.

Notatka
Dzienniki te można także otworzyć z poziomu okna Kontroli Rodzicielskiej, klikając **Pokaż dziennik**.

Jeśli nie korzystasz z komputera wraz z dziećmi, możesz skonfigurować sieć domową BitDefender w taki sposób, aby uzyskać zdalny dostęp do dzienników Kontroli Rodzicielskiej (ze swojego komputera).Aby uzyskać więcej informacji, odwołaj się do *„Sieć Domowa”* (p. 148).

Dzienniki Kontroli Rodzicielskiej zapewniają szczegółowe informacje na temat aktywności dzieci przy komputerze i w Internecie.Informacje rozmieszczone są w kilku zakładkach:

Ogólne
Zapewnia ogólne informacje na temat tego, co twoje dzieci robiły ostatnio, jakie witryny internetowe odwiedzały, z jakich korzystały aplikacji, itp.

Informacje można filtrować według użytkownika i okresu czasu.

Log aplikacji
Pozwala dowiedzieć się, jakie aplikacje były ostatnio używane przez dzieci.

Kliknij dwukrotnie zdarzenie na liście, aby zobaczyć więcej szczegółów na jego temat.Aby usunąć wpis dziennika, kliknij go prawym przyciskiem myszy i wybierz **Usuń**.

Dziennik Internetowy
Pozwala dowiedzieć się, jakie witryny internetowe zostały odwiedzone ostatnio przez dzieci.

Informacje można filtrować według użytkownika i okresu czasu.

Inne wydarzenia
Pozwala uzyskać szczegółowe informacje o aktywności modułu Kontroli Rodzicielskiej (na przykład kiedy włączono / wyłączono Kontrolę Rodzicielską, jakie zdarzenia zablokowano).

Kliknij dwukrotnie zdarzenie na liście, aby zobaczyć więcej szczegółów na jego temat.Aby usunąć wpis dziennika, kliknij go prawym przyciskiem myszy i wybierz **Usuń**.

19.2.2. Konfigurowanie Powiadomień E-mail

Otrzymywanie powiadomień przez e-mail w przypadku zablokowania aktywności przez Kontrolę Rodzicielską:

1. Otwórz BitDefender.
2. Przejdź do ustawień Kontroli Rodzicielskiej. W zależności od trybu wyświetlania interfejsu użytkownika wykonaj następujące polecenia:

   Widok średniozaawansowany
   Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Kontrola Rodzicielska**.

Widok eksperta

W menu po lewej stronie kliknij **Kontrolę Rodzicielską**.

Notatka

W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

3. W części Ustawienia wybierz **Wyślij mi raport aktywności przez e-mail**.
4. Zostaniesz powiadomiony(a) aby skonfigurować ustawienia konta e-mail. Kliknij **Tak** aby otworzyć okno konfiguracji.

Notatka

Możesz otworzyć okno konfiguracyjne później, klikając na **Ustawienia Powiadomień**.

5. Podaj adres e-mail, na który ma zostać wysłane powiadomienie.
6. Skonfiguruj ustawienia e-mail serwera używanego do wysyłania powiadomień przez e-mail.

Do konfigurowania ustawień e-mail służą trzy opcje:

Wykorzystaj aktualne ustawienia klienta poczty

Opcja ta jest domyślnie zaznaczona, gdy BitDefender dokonuje importu ustawień serwera poczty z klienta poczty użytkownika.

Aby zatwierdzić ustawienia, kliknij **Testuj ustawienia**. Jeśli w czasie zatwierdzania zostaną wykryte jakieś zagadnienia, zostaniesz poinformowany, co należy zrobić, aby je naprawić.

Wybierz jeden ze znanych serwerów

Wybierz tę opcję, jeśli posiadasz konto e-mail w jednej z internetowych usług pocztowych wymienionych na liście.

Aby zatwierdzić ustawienia, kliknij **Testuj ustawienia**. Jeśli w czasie zatwierdzania zostaną wykryte jakieś zagadnienia, zostaniesz poinformowany, co należy zrobić, aby je naprawić.

Chcę własnoręcznie skonfigurować ustawienia serwera

Jeśli znasz ustawienia serwera poczty, wybierz tę opcję i skonfiguruj ustawienia w następujący sposób:

- **Wychodzący Serwer SMTP** - wpisz adres serwera używanego do wysyłania wiadomości e-mail.
- Jeśli serwer używa innego portu niż domyślny port 25, wpisz go w odpowiednie pole.

- Jeśli serwer wymaga autoryzacji, zaznacz pole **Mój serwer SMTP wymaga autoryzacji** i wpisz nazwę i hasło w odpowiednich polach.

Aby zatwierdzić ustawienia, kliknij **Testuj ustawienia**. Jeśli w czasie zatwierdzania zostaną wykryte jakieś zagadnienia, zostaniesz poinformowany, co należy zrobić, aby je naprawić.

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

19.3. Zdalna kontrola rodzicielska

Zdalna Kontrola Rodzicielska pozwala monitorować aktywność dzieci oraz zmieniać ustawienia Kontroli Rodzicielskiej, nawet gdy nie ma cię w domu.Potrzebujesz jedynie komputera z dostępem do Internetu i przeglądarką internetową.

Zdalna Kontrola Rodzicielska pozwala w dyskretny sposób, bez wtrącania się, kontrolować dzieci w Internecie.

19.3.1. Wymagania Zdalnej Kontroli Rodzicielskiej

Aby korzystać ze zdalnej Kontroli Rodzicielskiej, należy spełnić następujące warunki:

1. Na komputerze dziecka zainstaluj albo BitDefender Internet Security 2011, albo BitDefender Total Security 2011.
2. Aktywuj produkt za pomocą konta BitDefender.
3. Włącz Zdalną Kontrolę Rodzicielską.
4. Komputer, z którego chcesz uzyskać dostęp do Zdalnej Kontroli Rodzicielskiej musi być podłączony do Internetu.

19.3.2. Włączanie Zdalnej Kontroli Rodzicielskiej

Włączanie Zdalnej Kontroli Rodzicielskiej:

1. Zaloguj się na komputer, na którym zainstalowany jest BitDefender, korzystając z konta administratora.Możesz użyć tego samego konta, które używałeś, aby zainstalować produkt.
2. Otwórz BitDefender.
3. Przejdź do ustawień Kontroli Rodzicielskiej. W zależności od trybu wyświetlania interfejsu użytkownika wykonaj następujące polecenia:

   Widok średniozaawansowany
   Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Kontrola Rodzicielska**.

   Widok eksperta
   W menu po lewej stronie kliknij **Kontrolę Rodzicielską**.

Notatka

W Widoku podstawowym lub średniozaawansowanym można skonfigurować skrót, tak aby uzyskać dostęp do tych ustawień z poziomu pulpitu.Aby uzyskać więcej informacji, odwołaj się do *„Moje narzędzia”* (p. 31).

4. Użyj przełącznika, żeby włączyć Zdalną Kontrolę Rodzicielską.Zdalna Kontrola Rodzicielska będzie włączona w systemie dla wszystkich kont użytkowników.

19.3.3. Uzyskiwanie Dostępu do Zdalnej Kontroli Rodzicielskiej

Do Zdalnej Kontroli Rodzicielskiej można przejść z konta BitDefender.

1. W komputerze mającym dostęp do Internetu otwórz przeglądarkę internetową i przejdź do:

   http://myaccount.bitdefender.com

2. Zaloguj się do konta BitDefender za pomocą swojej nazwy użytkownika i hasła.
3. Kliknij zakładkę **Kontrola Rodzicielska**, aby uzyskać dostęp do pulpitu Zdalnej Kontroli Rodzicielskiej.
4. Możesz zobaczyć wszystkie konta użytkowników, dla których włączona jest opcja Kontroli Rodzicielskiej.

   Aby sprawdzić działania zablokowane na określonym koncie użytkownika od momentu ostatniego logowania, kliknij łącze wskazujące istniejące alarmy.

   Aby sprawdzić, co twoje dzieci robiły ostatnio, kliknij łącze **Nowa aktywność** odpowiadające ich kontu.

   Aby zmienić ustawienia Kontroli Rodzicielskiej dla określonego konta użytkownika, kliknij odpowiednie łącze **Ustawienia**.

19.3.4. Zdalne Monitorowanie Aktywności Dzieci

Aby móc zdalnie monitorować aktywność dzieci przy komputerze i w Internecie, musisz włączyć na tym komputerze Zdalną Kontrolę Rodzicielską.Aby uzyskać więcej informacji, odwołaj się do *„Włączanie Zdalnej Kontroli Rodzicielskiej”* (p. 111).

Zdalne sprawdzanie aktywności dzieci przy komputerze:

1. W komputerze mającym dostęp do Internetu otwórz przeglądarkę internetową i przejdź do:

   http://myaccount.bitdefender.com

2. Zaloguj się do konta BitDefender za pomocą swojej nazwy użytkownika i hasła.
3. Kliknij zakładkę **Kontrola Rodzicielska**, aby uzyskać dostęp do pulpitu Zdalnej Kontroli Rodzicielskiej.

4. Aby sprawdzić działania zablokowane na określonym koncie użytkownika od momentu ostatniego logowania, kliknij łącze wskazujące istniejące alarmy.Aby sprawdzić, co twoje dzieci robiły ostatnio, kliknij łącze **Nowa aktywność** odpowiadające ich kontu.

Na stronie alarmów można znaleźć witryny internetowe, aplikacje lub kontakty komunikatorów zablokowane od czasu ostatniego logowania.

Na stronie Nowa aktywność udostępniono przydatne informacje na temat tego, co dzieci robiły ostatnio:

- które są najczęściej otwieranymi i blokowanymi witrynami internetowymi.
- które są aplikacjami najczęściej otwieranymi i blokowanymi.
- które są najczęściej używanymi i blokowanymi identyfikatorami komunikatorów.

Witrynę internetową, aplikację lub identyfikator komunikacji natychmiastowej można zablokować bezpośrednio, klikając odpowiednie łącze **Blokuj**.

Aby usunąć ograniczenie, kliknij odpowiednie łącze **Zezwól**.

19.3.5. Zdalna Zmiana Ustawień Kontroli Rodzicielskiej

Aby móc zdalnie zmieniać ustawienia Kontroli Rodzicielskiej dla swoich dzieci, musisz włączyć na ich komputerze Zdalną Kontrolę Rodzicielską.Aby uzyskać więcej informacji, odwołaj się do *„Włączanie Zdalnej Kontroli Rodzicielskiej”* (p. 111).

Zdalna zmiana ustawień Kontroli Rodzicielskiej:

1. W komputerze mającym dostęp do Internetu otwórz przeglądarkę internetową i przejdź do:

   http://myaccount.bitdefender.com

2. Zaloguj się do konta BitDefender za pomocą swojej nazwy użytkownika i hasła.
3. Kliknij zakładkę **Kontrola Rodzicielska**, aby uzyskać dostęp do pulpitu Zdalnej Kontroli Rodzicielskiej.
4. Możesz zobaczyć wszystkie konta użytkowników, dla których włączona jest opcja Kontroli Rodzicielskiej.Aby zmienić ustawienia Kontroli Rodzicielskiej dla określonego konta użytkownika, kliknij odpowiednie łącze **Ustawienia**.

Strona Ustawień wyświetla witryny internetowe, aplikacje i identyfikatory komunikatorów zablokowane przez Kontrolę Rodzicielską.Aby usunąć ograniczenie, kliknij odpowiednie łącze **Zezwól**.

Ustawianie ograniczeń omawiane jest przez następujące tematy:

„Ograniczanie Dostępu do Internetu Według Czasu” (p. 114)
„Blokowanie Witryn Internetowych” (p. 114)
„Blokowanie Aplikacji” (p. 114)
„Blokowanie Kontaktów IM” (p. 114)

Ograniczanie Dostępu do Internetu Według Czasu

Wybierz opcję z menu, aby określić czas dostępu dzieci do Internetu.Ograniczanie dostępu do Internetu do określonych pór dnia:

1. Wybierz **Harmonogram dostępu do Internetu**.
2. Wybierz z siatki przedziały czasowe, w których dostęp do Internetu ma być zablokowany.Możesz klikać pojedyncze komórki lub kliknąć i przeciągać, aby objąć dłuższe okresy czasu.Aby rozpocząć nową selekcję, kliknij **Blokuj wszystko** lub **Dopuszczaj wszystko**.
3. Kliknij **Wyślij zmiany**.Zmiany zostaną skonfigurowane i zastosowane w komputerze dziecka po następnej synchronizacji z witryną internetową Zdalnej Kontroli Rodzicielskiej (w ciągu maksymalnie 10 minut).

Blokowanie Witryn Internetowych

Blokowanie witryny internetowej:

1. Kliknij **Blokuj inną witrynę internetową**.
2. W odpowiednim polu podaj adres witryny internetowej. Z kolei jeśli chcesz zablokować jedną z najczęściej odwiedzanych witryn internetowych, wybierz ją z menu.
3. Kliknij **Blokuj**.Dana witryna internetowa zostanie dodana do listy zablokowanych witryn internetowych.Reguła zostanie skonfigurowana i zastosowana w komputerze dziecka po następnej synchronizacji z witryną internetową Zdalnej Kontroli Rodzicielskiej (w ciągu maksymalnie 10 minut).

Jeśli zmieniłeś zdanie, kliknij odpowiednie łącze **Zezwól**.

Blokowanie Aplikacji

Blokowanie aplikacji:

1. Kliknij **Blokuj inną aplikację**.
2. Z listy najczęściej używanych aplikacji wybierz to, które ma zostać zablokowane.
3. Kliknij **Blokuj**.Dana aplikacja zostanie dodana do listy zablokowanych aplikacji.Reguła zostanie skonfigurowana i zastosowana w komputerze dziecka po następnej synchronizacji z witryną internetową Zdalnej Kontroli Rodzicielskiej (w ciągu maksymalnie 10 minut).

Jeśli zmieniłeś zdanie, kliknij odpowiednie łącze **Zezwól**.

Blokowanie Kontaktów IM

Blokowanie komunikacji natychmiastowej z określonym kontaktem:

1. Kliknij **Blokuj inny kontakt**.

2. W odpowiednim polu wpisz identyfikator komunikatora. Z kolei jeśli chcesz zablokować jeden z najczęściej używanych identyfikatorów komunikatora, wybierz go z menu.
3. Kliknij **Blokuj**.Do listy zablokowanych identyfikatorów komunikacji natychmiastowej zostanie dodany ten identyfikator komunikacji natychmiastowej.Reguła zostanie skonfigurowana i zastosowana w komputerze dziecka po następnej synchronizacji z witryną internetową Zdalnej Kontroli Rodzicielskiej (w ciągu maksymalnie 10 minut).

Jeśli zmieniłeś zdanie, kliknij odpowiednie łącze **Zezwól**.

20. Kontrola prywatności

BitDefender monitoruje wiele potencjalnych punktów ataku, którymi mogą dostać się do systemu spywarey, sprawdza też wszelkie zmiany wprowadzane do systemu i oprogramowania. Jest efektywny w blokowaniu koni trojańskich i innych narzędzi instalowanych przez hakerów próbujących przejąć prywatne informacje z twojego komputera, takie jak numery kart kredytowych.

Kontrola prywatności zawiera następujące składniki:

- Kontrola tożsamości - pomaga zachować pewność, że informacje osobiste nie są wysyłane z komputera bez zgody użytkownika. Skanuje wiadomości e-mail i wiadomości błyskawiczne wysyłane z komputera, jak również wszelkie dane wysłane za pośrednictwem stron internetowych oraz blokuje każdą informację chronioną przez reguły Kontroli tożsamości utworzone przez użytkownika.
- Kontrola Rejestru – pyta o Twoją zgodę za każdym razem, gdy jakiś program chce wprowadzić zmiany w rejestrze aby być uruchamianym przy starcie Windows.
- Kontrola Ciasteczek - pyta o Twoją zgodę za każdym razem, gdy nowa strona chce ustawić pliki ciasteczek.
- Kontrola Skryptów - pyta o Twoją zgodę za każdym razem, gdy strona próbuje uruchomić skrypt lub inną aktywną zawartość.

Domyślnie włączona jest jedynie Kontrola Tożsamości.Musisz skonfigurować odpowiednie reguły Kontroli tożsamości, aby uniemożliwić nieautoryzowane wysyłanie informacji poufnych.Aby uzyskać więcej informacji, odwołaj się do *„Konfigurowanie Kontroli tożsamości”* (p. 118).

Pozostałe składniki Kontroli prywatności są interaktywne. Jeśli je włączysz, za pomocą okien alarmów będziesz proszony o wyrażenie zgody lub zablokowanie określonych operacji wykonywanych podczas przeglądania nowych witryn internetowych lub instalowania nowego oprogramowania. Z tego powodu są one zwykle używane przez zaawansowanych użytkowników.

20.1. Konfigurowanie Poziomu Ochrony

Poziom ochrony ułatwia włączanie i wyłączanie składników Kontroli prywatności.

Konfigurowanie poziomu ochrony:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Kontrola prywatności > Stan**.
3. Upewnij się, że Kontrola prywatności jest włączona.
4. Dostępne są dwie opcje:

- Przeciągnij suwak wzdłuż skali, aby ustawić odpowiedni poziom ochrony.Kliknij **Domyślny** aby przywrócić suwak na domyślny poziom.

  Użyj opisów po prawej stronie skali, aby wybrać poziom ochrony najlepiej spełniający twoje wymagania.

- Możesz dostosować poziom ochrony klikając **Użytkownika**.W oknie które się pojawi, wybierz kontrole zabezpieczeń które chcesz włączyć i kliknij **OK**.

20.2. Kontrola tożsamości

Kontrola Tożsamości chroni ciebie przed kradzieżą ważnych danych kiedy korzystasz z internetu.

Weź pod uwagę prosty przykład: utworzyłeś regułę Kontroli tożsamości, która chroni numer twojej karty kredytowej.Jeśli oprogramowanie szpiegujące zdoła w jakiś sposób zainstalować się na komputerze, nie będzie mogło wysłać numeru twojej karty kredytowej przez pocztę, wiadomość komunikatora lub strony internetowe. Ponadto twoje dzieci nie będą mogły jej użyć, aby dokonać zakupów w Internecie lub ujawnić ją osobom, które spotkają w Internecie.

Więcej informacji zawierają następujące tematy:

- *„Informacje o Kontroli tożsamości”* (p. 117).
- *„Konfigurowanie Kontroli tożsamości”* (p. 118).
- *„Zarządzanie Regułami”* (p. 121).

20.2.1. Informacje o Kontroli tożsamości

Bezpieczeństwo prywatnych danych jest dla nas wszystkich bardzo ważne. Kradzieże danych opierają się na nowych metodach oszukiwania ludzi w celu zdobycia prywatnych informacji.

Nie ważne czy jest to Twój adres e-mail, czy też numer karty kredytowej, kiedy dostaną się w niepowołane ręce mogą spowodować szkody: będziesz zalewany spamem lub zastaniesz puste konto.

Kontrola Tożsamości chroni ciebie przed kradzieżą ważnych danych kiedy korzystasz z internetu.W oparciu o reguły które utworzysz, Kontrola Tożsamości skanuje ruch w postaci odwiedzanych stron, wysyłanych e-maili oraz wiadomości wysyłanych z komunikatorów IM, szukając podanych ciągów znaków (przykładowo numeru twojej karty kredytowej). Jeśli znajdzie pasujący tekst, strona WWW, e-mail lub wiadomość komunikatora jest natychmiast blokowana.

Możesz tworzyć reguły aby chronić dowolną informacje którą uważasz za prywatną, poczynając od numeru telefonu lub adresie email a skończywszy na danych konta bankowego.Obsługa Wielu Użytkowników jest zapewniona więc użytkownicy logujący się na różne konta Windows mogą skonfigurować swoje własne reguły ochrony tożsamości.Jeśli twoje konto Windows jest kontem administratora, reguły które

tworzysz mogą zostać skonfigurowane tak, aby obowiązywały także innych użytkowników, zalogowanych do Windows na swoich kontach.

Po co korzystać z Kontroli Tożsamości?

- Kontrola Tożsamości jest bardzo efektywna w blokowaniu oprogramowania szpiegującego i keyloggerów.Aplikacje tego typu zapamiętują naciskane przez ciebie klawisze i wysyłają te informacje poprzez 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.

  Zakładając że takie aplikacje są w stanie uniknąć wykrycia przez oprogramowanie antywirusowe, nie mogą one wysłać skradzionych danych przez email, stronę www lub komunikator jeśli utworzyłeś odpowiednią regułę ochrony tożsamości.

- Kontrola Tożsamości może ochronić ciebie przed próbami Phishingu (próby kradzieży danych osobowych).Najczęstsze próby phishingu korzystają z fałszywych wiadomości email aby oszukać i nakłonić ciebie do podania danych osobowych na fałszywej stronie.

  Przykładowo, możesz otrzymać podrobiony email z twojego banku proszący o pilne zaktualizowanie informacji o koncie bankowym.Email zawiera link do strony na której musisz podać swoje dane osobowe.Mimo że wyglądają na oryginalne, email oraz strona korzystają z mylnych linków przekierowujących do fałszywej strony.Jeśli klikniesz link w emailu i podasz swoje dane osobowe na fałszywej stronie, ujawnisz te informacje osobie która zorganizowała próbę phishingu.

  Jeśli odpowiednie reguły ochrony tożsamości są ustawione, to nie możesz podać danych osobowych (takich jak numer karty kredytowej) na stronach internetowych chyba że utworzyłeś wyjątek dla konkretnej strony internetowej.

- Korzystając z reguł Kontroli tożsamości możesz uniemożliwić dzieciom udostępnienie informacji osobistych (takich jak adres domowy lub numer telefonu) osobom, które spotkają w Internecie. Ponadto, jeśli utworzysz reguły chroniące twoją kartę kredytową, nie będą mogły dokonywać zakupów w Internecie bez twojej zgody.

20.2.2. Konfigurowanie Kontroli tożsamości

Jeżeli chcesz korzystać z Kontroli Tożsamości, proszę wykonać następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Kontrola prywatności > Tożsamość**.
3. Upewnij się, że Kontrola tożsamości jest włączona.

Notatka
Jeśli danej opcji nie można skonfigurować, przejdź do zakładki **Stan** i włącz Kontrolę prywatności.

4. Utwórz reguły mające chronić twoje ważne dane.Aby uzyskać więcej informacji, odwołaj się do *„Tworzenie Reguł Ochrony Tożsamości”* (p. 119).
5. Jeśli trzeba, zdefiniuj wyjątki od reguł które utworzyłeś.Na przykład, jeśli utworzyłeś regułę, która chroni numer twojej karty kredytowej, dodaj do listy wyjątków witryny internetowe, w których zwykle korzystasz ze swojej karty.Aby uzyskać więcej informacji, odwołaj się do *„Definiowanie Wyjątków”* (p. 120).

Tworzenie Reguł Ochrony Tożsamości

Aby utworzyć regułę ochrony tożsamości kliknij **Dodaj** aby rozpocząć kreator konfiguracji.Możliwość poruszania się w kreatorze zapewniają przyciski **Dalej** i **Cofnij**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Okno Powitania**
2. **Wybierz Typ i Dane Reguły**

   Ustaw następujące parametry:

   - **Nazwa Reguły** - wpisz nazwę reguły w polu edycji.
   - **Typ Reguły** - wybierz typ reguły (adres, imię, karta kredytowa, PIN, SSN itp).
   - **Dane Reguły** - wpisz dane które chcesz chronić w polu edycji.Przykładowo, jeśli chcesz chronić swój numer karty kredytowej, wpisz go lub jego część tutaj.

     WAŻNE
     Jeśli wpiszesz mniej niż trzy znaki, zostaniesz poproszony o wpisanie poprawnych danych. Zalecamy abyś wpisał przynajmniej trzy znaki w celu pominięcia błędu zablokowania wiadomości i stron www.

   Wszystkie wprowadzane dane są szyfrowane. Dla dodatkowego zabezpieczenia nie podawaj wszystkich danych które chcesz chronić.
3. **Wybierz Typy Ruchu i Użytkowników**

   a. Wybierz rodzaj ruchu jaki ma być skanowany przez BitDefendera.

   - **Skanuj ruch internetowy (HTTP)** - skanuje ruch HTTP (strony WWW) i blokuje wysyłane dane które pasują do tych zapisanych w regule.
   - **Skanuj wiadomości e-mail (ruch SMTP)** - skanuje ruch SMTP (wiadomości) i blokuje wszystkie wychodzące wiadomości e-mail, które zawierają podane w regule ciągi znaków.
   - **Skanuj ruch IM (komunikatory)** - skanuje ruch IM i blokuje wszystkie wysyłane wiadomości, które zawierają podane w regule ciągi znaków.

   Możesz wybrać zastosowanie reguły tylko jeśli zawartość reguły zgadza się z całymi słowami lub jeśli zawartość reguły i jakikolwiek wykryty ciąg znaków są identyczne.

b. Określ użytkowników, dla których stosuje się wybraną regułę.

- **Tylko dla mnie (obecny użytkownik)** - ta reguła będzie stosowana tylko dla twojego konta użytkownika.
- **Ograniczone konta użytkowników** - ta reguła zostanie zastosowana dla twojego konta oraz innych kont Windows z ograniczonym prawami.
- **Wszyscy użytkownicy** - reguła zostanie zastosowana dla wszystkich kont Windows.

4. **Opisz Regułę**

   Wprowadź krótki opis reguły w polu edycji.Ponieważ zablokowane dane (ciąg znaków) nie jest wyświetlany jako tekst przy dostępie do reguły, opis powinien pomóc w identyfikacji.

   Kliknij **Zakończ**.Reguła pojawi się w tabeli.

Od tej chwili każda próba wysłania podanych danych (przez wiadomość e-mail, komunikację natychmiastową lub stronę internetową) zakończy się niepowodzeniem. Wyświetlona zostanie wiadomość z ostrzeżeniem, wskazująca, że BitDefender zablokował wysłanie treści zawierającej informacje osobiste.

Definiowanie Wyjątków

Są przypadki gdy musisz określić wyjątki do podanych reguł tożsamości.Rozważmy przypadek gdy tworzysz regułę, która chroni numer karty kredytowej przed wysłaniem przez HTTP (strony internetowe). Zawsze kiedy z twojego konta użytkownika zostanie podany numer twojej karty kredytowej do strony internetowej zostanie ona automatycznie zablokowana. Jeśli na przykład, chcesz kupić obuwie w sklepie internetowym (o którym wiesz, że jest bezpieczny), będziesz musiał ustawić wyjątek w odpowiedniej regule.

Aby otworzyć okno w którym możesz zarządzać wyjątkami, kliknij **Wyjątki**.

Aby dodać wyjątek, wykonaj następujące kroki:

1. Kliknij **Dodaj** aby dodać nową pozycję do tabeli.
2. Kliknij dwukrotnie na **Określ element objęty wyjątkiem** i podaj adres strony WWW lub email, który chcesz dodać jako wyjątek.
3. Kliknij dwukrotnie **Typ ruchu** i wybierz z menu opcję odpowiadającą typowi adresu, który wcześniej został podany.
   - Jeśli podałeś adres strony internetowej, wybierz **HTTP**.
   - Jeśli podałeś adres e-mail, wybierz E-mail **(SMTP)**.
   - Jeśli podałeś kontakt IM, kliknij **IM**.

Aby usunąć wyjątek z listy, wybierz go i kliknij na przycisk **Usuń**.

Kliknij **Zastosuj** aby zapisać zmiany.

20.2.3. Zarządzanie Regułami

Zarządzanie regułami Kontroli tożsamości:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Kontrola prywatności > Tożsamość**.

W tabeli możesz zobaczyć wszystkie dotychczas utworzone reguły.

Aby usunąć regułę, wybierz ją i kliknij **Usuń**.

Aby edytować regułę zaznacz ją i kliknij **Edytuj** lub kliknij w nią dwukrotnie. Pojawi się nowe okno.Możesz tutaj zmienić nazwę, opis i parametry reguły (typ, dane i ruch). Kliknij **OK** aby zapisać zmiany.

20.3. Kontrola rejestru

Rejestrystanowią bardzo ważną część systemu operacyjnego Windows. Jest to miejsce, w którym Windows przechowuje ustawienia o zainstalowanych programów, ustawienia użytkownika i inne.

Rejestry są także użytkowane w celu określenia, które programy powinny być automatycznie uruchamiane, kiedy Windows startuje. Wirusy często wykorzystują to, aby automatycznie dostać się do systemu, kiedy użytkownik restartuje swój komputer.

Kontrola Rejestrów dba o rejestry Windows – jest użyteczna przy wykrywaniu Koni Trojańskich. Kiedy program przy starcie Windows będzie próbował zmodyfikować rejestry zostaniesz o tym powiadomiony.Aby uzyskać więcej informacji, odwołaj się do *„Alarmy rejestru”* (p. 38).

Konfigurowanie Kontroli rejestru:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Kontrola prywatności > Rejestr**.
3. Zaznacz odpowiednie pole, aby włączyć Kontrolę Rejestru.

Notatka
Jeśli danej opcji nie można skonfigurować, przejdź do zakładki **Stan** i włącz Kontrolę prywatności.

Zarządzanie Regułami

Aby usunąć regułę, wybierz ją i kliknij **Usuń**.

20.4. Kontrola Ciasteczek

Ciasteczka występują powszechnie w Internecie. Są one małymi plikami przechowywanymi w twoim komputerze. Strony sieci tworzą je, aby śledzić szczegółową informację o tobie.

Generalnie, ciasteczka są tworzone, aby ułatwiały użytkownikowi pracę. Np. mogą pomóc stronie WWW zapamiętać twoją nazwę i preferencje tak abyś nie musiał wpisywać ich za każdym razem.

Ciasteczka mogą także być także używane, aby zagrozić twojej prywatności np. poprzez śledzenie twojego ruchu w Internecie.

To tutaj przydaje się Kontrola Ciasteczek.Jeśli jest włączona, Kontrola Ciasteczek będzie prosić o zgodę za każdym razem, gdy nowa witryna internetowa będzie próbowała ustanowić lub zażądać ciasteczka.Aby uzyskać więcej informacji, odwołaj się do *„Alarmy ciasteczek”* (p. 39).

Konfigurowanie Kontroli Ciasteczek:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Kontrola prywatności > Ciasteczka**.
3. Zaznacz odpowiednie pole, aby włączyć Kontrolę ciasteczek.

   Notatka
   Jeśli danej opcji nie można skonfigurować, przejdź do zakładki **Stan** i włącz Kontrolę prywatności.

4. Możesz skonfigurować reguły dla regularnie odwiedzanych witryn internetowych, jednak nie jest to konieczne.Reguły tworzone są automatycznie w oknie alarmu w oparciu o odpowiedzi użytkownika.

Notatka
Z powodu dużej ilości ciasteczek wykorzystywanych w Internecie **Kontrola Ciasteczek** może na początku wymagać więcej uwagi. Użytkownik może być zasypywany pytaniami o strony próbujące ustawić ciasteczko. Z czasem liczba pytań zmaleje do minimum.

Ręczne Tworzenie Reguł

Aby ręcznie utworzyć regułę, kliknij **Dodaj** i skonfiguruj parametry reguły w oknie konfiguracyjnym.Możesz ustawić parametry:

- **Wprowadz domene** - wpisz w domenę, która reguła ma być zastosowana.
- **Działanie** - wybierz działanie reguły.

Działania	Opis
Zezwól	Ciasteczka z tej domeny będą zapisywane.
Zabroń	Ciasteczka z tej domeny nie będą zapisywane i uruchamiane.

- **Kierunek** - wybierz kierunek ruchu.

Kierunek	Opis
Wysyłane	Reguła będzie zastosowana wyłącznie dla ciasteczek, które są wysyłane z powrotem do podłączonych stron.
Odbierane	Reguła będzie zastosowana wyłącznie dla ciasteczek, które są otrzymane z powrotem z podłączonych stron.
Obydwa	Reguła będzie dotyczyła obu kierunków.

Notatka

Możesz zaakceptować ciasteczka, ale nigdy nie będziesz mógł przywrócić ich po zastosowaniu akcji**Zabroń** i przekierowaniu na **Wychodzące**.

Kliknij **Zakończ**.

Zarządzanie Regułami

Aby usunąć regułę, wybierz ją i kliknij **Usuń**.Aby zmienić parametry regułu, kliknij ją dwukrotnie lub kliknij przycisk **Edytuj**. Wprowadź porządane zmiany w oknie konfiguracyjnym.

20.5. Kontrola Skryptów

Scrypty i inne kody takie jak Kontrole ActiveX i aplety Java, które są wykorzystywane do tworzenia interaktywnych stron w sieci, mogą też być zaprogramowane aby wywoływać szkodliwe efekty. Elementy ActiveX mogą przykładowo mieć całkowity dostęp do twoich danych, mogą czytać dane z twojego komputera, usuwać informacje, przechwytywać hasła i wiadomości gdy jesteś połączony do internetu. Powinieneś akceptować wyłącznie aktywne składniki ze stron które dobrze znasz i którym w pełni ufasz.

Jeśli włączysz Kontrolę Skryptów, będziesz proszony o zgodę za każdym razem, gdy nowa witryna internetowa będzie próbowała uruchomić skrypt lub inną zawartość aktywną.Aby uzyskać więcej informacji, odwołaj się do *„Alarmy skryptów”* (p. 39).

Konfigurowanie Kontroli Skryptów:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Kontrola prywatności > Skrypty**.
3. Zaznacz odpowiednie pole, aby włączyć Kontrolę Skryptów.

Notatka
Jeśli danej opcji nie można skonfigurować, przejdź do zakładki **Stan** i włącz Kontrolę prywatności.

4. Możesz skonfigurować reguły dla regularnie odwiedzanych witryn internetowych, jednak nie jest to konieczne.Reguły tworzone są automatycznie w oknie alarmu w oparciu o odpowiedzi użytkownika.

Ręczne Tworzenie Reguł

Aby ręcznie utworzyć regułę, kliknij **Dodaj** i skonfiguruj parametry reguły w oknie konfiguracyjnym.Możesz ustawić parametry:

- **Wprowadz domene** - wpisz w domenę, która reguła ma być zastosowana.
- **Działanie** - wybierz działanie reguły.

Działania	Opis
Zezwól	Skrypty w tej domenie będą wykonane.
Zabroń	Skrypty w domenie nie będą wykonane.

Kliknij **Zakończ**.

Zarządzanie Regułami

Aby usunąć regułę, wybierz ją i kliknij **Usuń**.Aby zmienić parametry regułu, kliknij ją dwukrotnie lub kliknij przycisk **Edytuj**. Wprowadź porządane zmiany w oknie konfiguracyjnym.

21. Zapora Sieciowa

Zapora Sieciowa chroni twój komputer przed nieautoryzowanymi próbami połączeń. Jest to bardzo podobne do straży przy bamie - będzie pilnował twoich połączeń internetowych i będzie pilnował kogo wpuszczać a kogo blokować.

Notatka
Firewall jest niezbędna, jeżeli masz broadband lub połączenia DSL.

W Trybie Niewidzialności twój komputer jest "ukryty" przed złośliwym oprogramowaniem i hakerami. Moduł Zapory Sieciowej potrafi automatycznie wykrywać i chronić przed skanowaniem portów (ciąg pakietów wysłanych do komputera w celu znalezienia "dostępnych punktów", często stosowane przed atakiem).

21.1. Ustawienia ochrony

Aby włączyć/wyłączyć oraz skonfigurować ochronę zapory sieciowej, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany
Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Zaporę Sieciową**.W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Ustawienia**.

Widok eksperta
Przejdź do **Zapora Sieciowa > Ustawienia**.

WAŻNE
Aby podlegać ochronie przed zagrożeniami pochodzącymi z internetu, miej włączoną **Firewall**.

W górnej części widoczne są różne statystyki dotyczące wykrytych operacji.

W dolnej części tej sekcji znajdują się statystyki BitDefender dotyczące ruchu przychodzącego i wychodzącego. Wykres ten przedstawia natężenie ruchu internetowego przez ostatnie dwie minuty.

Notatka
Wykres ten wyświetlany jest jedynie w Widoku eksperta.

21.1.1. Ustawianie Domyślnego Działania

Domyślnie, BitDefender zezwala znanym programom ze swojej białej listy na dostęp do usług sieciowych i Internetu.W przypadku wszelkiego innego oprogramowania,

BitDefender pyta ciebie poprzez okienko alarmujące jakie działanie ma podjąć.Działanie które wybierzesz będzie stosowane za każdym razem kiedy dana aplikacja poprosi o dostęp do sieci/Internetu.

Notatka

To view the BitDefender white list, click the corresponding button located in the **Settings** tab in Expert View or the **Programs** tab in Intermediate View.

Możesz przeciągnąć suwak po skali aby ustawić domyślne działanie które ma być podejmowane wobec aplikacji proszących o dostęp do sieci/Internetu.

- Pozwól Wszystkim
- Zezwól Znanym Programom
- Raportuj
- Blokuj Wszystkie

Po wybraniu danej operacji wyświetlany jest jej krótki opis.

21.1.2. Konfigurowanie Zaawansowanych Ustawień Zapory Sieciowej

Aby skonfigurować zaawansowane ustawienia zapory sieciowej, w Widoku eksperta kliknij **Ustawienia zaawansowane**.

Dostępne są następujące opcje:

- **Włącz obsługę Współdzielenie Połączenia Internetowego** - włącza wsparcie dla Współdzielenia Połączenia Internetowego (Internet Connection Sharing - ICS).

  Notatka

  Opcja ta nie włącza automatycznie ICS w twoim systemie, tylko zezwala na tego typu połączenia w przypadku gdy włączysz je w systemie operacyjnym.

- **Wykryj aplikacje które zmieniły się od utworzenia reguły zapory sieciowej** - sprawdza każdą z aplikacji, która chce połączyć się z Internetem, czy zmieniła się od czasu utworzenia reguły. Jeśli tak, wyświetli się alarm z pytaniem czy zablokować, czy udzielić jej dostępu.

  Notatka

  Aplikacje mogą zostać zmienione przez złośliwe oprogramowanie.Zalecamy by ta opcja była zaznaczona i żebyś zezwalał na dostęp tylko tym aplikacjom, których zmiany się spodziewasz po utworzeniu reguły zezwalającej im na dostęp.

  Podpisane aplikacje powinny być zaufane i mieć wyższy poziom zabezpieczeń.Możesz zaznaczyć **Nie wykrywaj zmian w cyfrowo podpisanych aplikacjach** aby automatycznie udzielić dostępu do Internetu tym aplikacjom, bez wyświetlania alarmu na ten temat.

- **Włącz Powiadomienia Wi-Fi** - jeśli jesteś podłączony do sieci bezprzewodowej, pokazuje okno informacyjne dotyczące konkretnych zdarzeń w sieci (przykładowo, podłączenie się do sieci nowego komputera).
- **Blokuj Skanowanie Portów** - wykrywa i blokuje próby sprawdzenia które porty są otwarte.

  Skanowanie portów jest często wykorzystywane przez hakerów w celu znalezienia otwartych portów na komputerze.Następnie mogą się włamać do komputera jeśli znajdą słabo zabezpieczony lub podatny port.
- **Włącz Rygorystyczne Automatyczne Reguły** - tworzy rygorystyczne reguły używając okna alarmowego zapory sieciowej.Przy tej opcji zaznaczonej, BitDefender będzie pytał ciebie o działanie i tworzył reguły dla każdego procesu otwierającego aplikacje wymagającą dostępu do sieci lub Internetu.

21.2. Reguły Dostępu do Aplikacji

Aby zarządzać regułami zapory sieciowej, kontrolującymi dostęp aplikacji do zasobów sieciowych, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany
: Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Zaporę Sieciową**.W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Programy**.

Widok eksperta
: Przejdź do **Zapora Sieciowa > Programy**.

Widok średniozaawansowany zapewnia dostęp do podstawowych ustawień konfiguracji. Aby uzyskać więcej opcji dostosowania, użyj Widoku eksperta.

21.2.1. Przeglądanie Bieżących Reguł

W tabeli widoczne są programy (procesy), dla których utworzono reguły zapory sieciowej.

W Widoku eksperta można uzyskać szczegółowe informacje na temat każdej reguły, zgodnie z kolumnami tabeli.Aby zobaczyć reguły utworzone dla aplikacji, kliknij pole + obok danej aplikacji.Odznacz pole **Ukryj Reguły Systemowe** jeśli chcesz widzieć również reguły dotyczące procesów systemowych i BitDefednera.

- **Typ procesu/sieci** - typ procesu i karty sieciowej, do których odnoszą się te reguły.Reguły tworzone automatycznie, tak aby filtrować dostęp do sieci i Internetu przez dowolny adapter.Możesz ręcznie dodać regułę lub edytować już istniejące reguły aby filtrować dostęp aplikacji do sieci lub Internetu przez wybrany adapter (przykładowo, karę sieci bezprzewodowej).

- **Linia Komend** - polecenia używane do uruchamiania procesów w linii komend systemu Windows (**cmd**).
- **Protokół** - protokół IP do którego stosowana jest reguła.Możesz zobaczyć jeden z następujących:

Protokol	Opis
Dowolna	Dotyczy wszystkich protokołów IP.
TCP	Transmission Control Protocol - TCP umożliwia dwojga hostom ustanowić połączenie do wymiany strumieni danych. TCP gwarantuje dostarczenie danych i także gwarantuje że pakiety będą dostarczone w tej samej kolejności co zostały wysłane.
UDP	User Datagram Protocol - UDP jest transportem bazującym na IP zaprojektowanym dla uzyskania wysokiej wydajności. Gry i inne bazujące na przesyłaniu obrazu aplikacje często używają UDP.
Numer	Pokazuje konkretny protokół IP (inny niż TCP lub UDP).Kompletną listę protokołów IP możesz znaleźć na www.iana.org/assignments/protocol-numbers.

- **Zdarzenia Sieciowe** - zdarzenia sieciowe dotyczące reguły.Następująca zdarzenia mogą być zawarte:

Zdarzenie	Opis
Połącz	Wstępna wymiana standardowych wiadomości używanych przez protokoły komunikacyjne (takie jak TCP) do nawiązania połączenia.W przypadku protokołów komunikacyjnych, ruch danych pomiędzy dwoma komputerami następuje dopiero po nawiązaniu połączenia.
Ruch sieciowy	Przepływ danych pomiędzy dwoma komputerami.
Słuchaj	Stan w którym aplikacja monitoruje ruch sieciowy czekając na nawiązanie połączenia lub odebranie informacji z aplikacji przesyłającej dane.

- **Lokalne Porty** -porty na twoim komputerze których dotyczy reguła.
- **Zdalne Porty** - porty na zdalnym komputerze których dotyczy reguła.
- **Lokalne** - czy reguła dotyczy tylko komputerów w sieci lokalnej.
- **Działanie** - czy aplikacja ma mieć dozwolony lub zablokowany dostęp do sieci lokalnej i Internetu przy podanych warunkach.

21.2.2. Automatyczne Dodawanie Reguł

Jeśli **Zapora Sieciowa** jest włączona, BitDefender monitoruje wszystkie aplikacje i automatycznie tworzy regułę, gdy dana aplikacja próbuje połączyć się z Internetem.W zależności od aplikacji i ustawień zapory sieciowej BitDefender odbywa się to przy lub bez udziału użytkownika.

Jeśli korzystasz z Widoku podstawowego lub Widoku średniozaawansowanego, próby nawiązania połączenia pochodzące z nieznanych aplikacji będą automatycznie blokowane.

Jeśli korzystasz z Widoku eksperta, a nieznana aplikacja próbuje połączyć się z Internetem, za pośrednictwem okna alarmu otrzymasz monit o podjęcie działania.

Możesz zobaczyć: aplikacje która próbuje uzyskać dostęp do Internetu, protokół, ścieżkę do pliku tej aplikacji, przeznaczenie, oraz port na którym aplikacja próbuje się połączyć.

Kliknij **Zezwól** by zezwolić na cały ruch (przychodzący i wychodzący) generowany przez tę aplikację od lokalnego hosta do każdego adresu, przez podany protokół IP i wszystkie inne porty. Jeśli klikniesz **Zablokuj**, aplikacja nie otrzyma dostępu do Internetu przez podany protokół IP.

WAŻNE

Zezwól przychodzącym próbom połączenia tylko z adresów IP albo domen którym w pełni ufasz.

Zgodnie z twoją odpowiedzią, reguła zostanie utworzona, zastosowana i umieszczona w tabeli. Następnym razem gdy aplikacja spróbuje się połączyć, ta reguła zostanie domyślnie zastosowana.

21.2.3. Ręczne Dodawanie Reguł

Ręczne tworzenie reguł różni się w zależności od wybranego trybu wyświetlania interfejsu użytkownika.

Widok średniozaawansowany

1. W **Dodaj nowy program** kliknij **Przeglądaj**.
2. Znajdź program, dla którego chcesz utworzyć regułę i kliknij **Otwórz**.
3. Kliknij **Dodaj regułę**.

   Zauważ, że reguła jest teraz wyświetlona w tabeli.
4. W kolumnie **Działanie** wybierz opcję: zezwól na lub zablokuj dostęp.

   Ta operacja zostanie zastosowana do wszystkich parametrów reguł.

Widok eksperta

1. Kliknij przycisk **Dodaj regułę**.Wyświetlone zostanie okno konfiguracji.

2. Skonfiguruj w zależności główne oraz zaawansowane parametry.
3. Kliknij **OK** aby dodać nową regułę.

Reguły można modyfikować tylko w czasie konfigurowania zapory sieciowej w Widoku eksperta.Aby zmodyfikować istniejącą regułę, wykonaj następujące kroki:

1. Kliknij przycisk **Edytuj regułę** lub dwukrotnie kliknij regułę.Wyświetlone zostanie okno konfiguracji.
2. Skonfiguruj w zależności główne oraz zaawansowane parametry.
3. Kliknij **Zastosuj** aby zapisać zmiany.

Konfigurowanie Głównych Parametrów

Zakładka **Główne** okna konfiguracyjnego umożliwia skonfigurowanie głównych parametrów reguły.

Możesz skonfigurować następujące parametry:

- **Ścieżka do Programu.** Kliknij **Przeglądaj** i wybierz aplikacje do której ma być zastosowana reguła.Jeśli chcesz zastosować regułę do wszystkich aplikacji, zaznacz **Dowolne**.
- **Wiersz poleceń.** Jeśli chcesz zastosować regułę tylko kiedy wybrana aplikacja jest uruchomiona przez komendę z interfejsu linii komend Windows, odznacz pole **Dowolne** i wpisz komendę w polu edycji.
- **Protokol.** Wybierz z menu protokół IP dla którego ma być stosowana reguła.
  - Jeśli chcesz aby reguła była stosowana dla wszystkich protokołów, zaznacz **Dowolne**.
  - Jeśli chcesz zastosować tą regułę do protokołu TCP, wybierz **TCP**.
  - Jeśli chcesz zastosować tą regułę do protokołu UDP, wybierz **UDP**.
  - Jeśli chcesz aby reguła była stosowana dla konkretnego protokołu, zaznacz **Inne**.Pojawi się okno edycji.Wpisz w polu edycji numer przypisany do protokołu który chcesz filtrować.

    Notatka

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

- **Zdarzenia.** W zależności od wybranego protokołu, wybierz zdarzenia sieciowe do których ma być zastosowana reguła.Następująca zdarzenia mogą być zawarte:

Zdarzenie	Opis
Połącz	Wstępna wymiana standardowych wiadomości używanych przez protokoły komunikacyjne (takie jak TCP) do nawiązania połączenia.W przypadku protokołów komunikacyjnych, ruch danych pomiędzy dwoma komputerami następuje dopiero po nawiązaniu połączenia.
Ruch sieciowy	Przepływ danych pomiędzy dwoma komputerami.
Słuchaj	Stan w którym aplikacja monitoruje ruch sieciowy czekając na nawiązanie połączenia lub odebranie informacji z aplikacji przesyłającej dane.

- **Typy Adapterów.** Wybierz typy adapterów dla których ma zostać zastosowana ta reguła.
- **Działania.** Wybierz jedno z dostępnych działań:

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

Konfigurowanie Zaawansowanych Parametrów

Zakładka **Zaawansowane** - okna konfiguracyjnego umożliwia skonfigurowanie zaawansowanych parametrów reguły.

Możesz skonfigurować następujące zaawansowane parametry:

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

Adres	Opis
Wysyłane	Reguła będzie dotyczyła tylko ruchu wychodzącego.
Odbierane	Reguła będzie dotyczyła tylko ruchu przychodzącego.
Obydwa	Reguła będzie dotyczyła obu kierunków.

- **Wersja IP.** Wybierz z menu wersje IP (IPv4, IPv6 lub dowolną) dla którego ma być stosowana reguła.

- **Adres Lokalny.** Podaj lokalny adres IP i port dla których ma być stosowana reguła w następujący sposób:
  - Jeśli masz więcej niż jeden adapter sieciowy, możesz odznaczyć pole **Dowolny** i podać adres IP.
  - Jeśli jako protokół zaznaczyłeś TCP lub UDP możesz podać port lub zakres między 0 i 65535. Jeśli chcesz aby reguła była stosowana do wszystkich portów, zaznacz **Dowolne**.
- **Zdalne Adresy.** Podaj zdalny adres IP oraz port dla których reguła ma być zastosowana w następujący sposób:
  - Aby filtrować ruch pomiędzy komputerami twoim oraz podanym przez ciebie, odznacz pole **Dowolne** i wpisz jego adres IP.
  - Jeśli jako protokół zaznaczyłeś TCP lub UDP możesz podać port lub zakres między 0 i 65535. Jeśli chcesz aby reguła była stosowana do wszystkich portów, zaznacz **Dowolne**.
- **Zastosuj tą regułę tylko do komputerów bezpośrednio podłączonych.** Zaznacz to pole tylko jeśli chcesz zastosować tą regułę do prób połączeń z sieci lokalnej.
- **Sprawdź łańcuch procesów oryginalnego zdarzenia.** Możesz modyfikować ten parametr tylko jeśli zaznaczyłeś **Ścisłe Automatyczne Reguły** (kliknij Ustawienia i następnie **Zaawansowane**).Rygorystyczne reguły oznaczają, że BitDefender będzie prosił o działanie za każdym razem, gdy żądanie dostępu do sieci/Internetu wychodzące od aplikacji będzie inne od procesu nadrzędnego.

21.2.4. Zaawansowane Zarządzanie Regułami

Jeśli chcesz zobaczyć i edytować szczegółowe reguły kontrolujące aplikacje, kliknij przycisk **Zaawansowane**, który jest dostępny w Widoku eksperta podczas konfigurowania zapory sieciowej.

Możesz zobaczyć listę reguły zgodnie z kolejnością ich sprawdzania.Kolumny tabeli zawierają informacje dotyczące każdej reguły.

Notatka

Gdy następuje próba połączenia (obojętne przychodzącego czy wychodzącego), BitDefender stosuje pierwszą regułę pasującą do tego połączenia.Dlatego, kolejność według której reguły są sprawdzane jest bardzo ważna.

Aby usunąć regułę, wybierz ją i kliknij przycisk **Usuń regułę**.

Aby edytować istniejącą regułę, wybierz ją i kliknij przycisk **Edytuj Regułę** lub dwukrotnie ją kliknij.

Możesz zwiększyć lub zmniejszyć priorytet reguły. Kliknij **Przenieś wyżej** aby zwiększyć priorytet zaznaczonej reguły o jeden poziom lub kliknij **Przenieś niżej**

aby zmniejszyć priorytet zaznaczonej reguły o jeden poziom.Aby przypisać regule najwyższy priorytet, kliknij **Przenieś na Szczyt**. Aby przypisać regule najniższy priorytet, kliknij **Przenieś na Spód**.

Kliknij **Zamknij** aby zamknąć okno.

21.2.5. Kasowanie i Resetowanie Reguł

Usunięcie i ponowne skonfigurowanie reguł możliwe jest tylko podczas konfigurowania zapory sieciowej w Widoku eksperta.

Aby usunąć regułę, wybierz ją i kliknij przycisk **Usuń regułę**.Możesz zaznaczyć i usunąć wiele reguł jednocześnie.

Jeśli chcesz usunąć wszystkie reguły utworzone dla określonej aplikacji, wybierz daną aplikację z listy i kliknij przycisk **Usuń regułę**.

Jeśli chcesz załadować domyślny zestaw reguł dla wybranego poziomu zaufania, kliknij na **Resetuj Reguły**.

21.3. Ustawienia Sieci

Aby skonfigurować połączenia sieciowe, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany
: Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj zaporę sieciową**. W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Sieć**.

Widok eksperta
: Przejdź do **Zapora Sieciowa > Sieć**.

Kolumny w tabeli **Konfiguracja Sieci** zapewniają szczegółowe informacje o sieci, do której jesteś podłączony oraz pozwalają skonfigurować ustawienia tego połączenia:

- **Adapter** - urządzenie sieciowe z którego korzysta twój komputer aby połączyć się z siecią lub Internetem.
- **Typ sieci** - typ sieci, do której podłączony jest adapter.W zależności od konfiguracji karty sieciowej BitDefender może automatycznie określać typ sieci lub prosić o podanie większej ilości informacji.

  Zmień typ, klikając strzałkę z kolumny **Typy sieci** i wybierając jeden z dostępnych typów z listy.

Typ sieci	Opis
Zaufane (Pozwól wszystkim)	Wyłącza zaporę sieciową dla odpowiedniego adaptera.

Typ sieci	Opis
Dom/Biuro	Zezwala na wszelki ruch pomiędzy twoim komputerem i komputerami w sieci lokalnej.
Miejsce publiczne	Cały ruch jest filtrowany.
Niezaufane (Blokuj wszystko)	Kompletnie blokuje ruch sieciowy i Internetowy poprzez odpowiedni adapter.

- **VPN** - określa, czy to połączenie VPN.

  Ruch biegnący przez połączenie VPN jest filtrowany inaczej niż ruch biegnący przez inne połączenia sieciowe.Jeśli korzystasz z połączenia typu VPN, kliknij strzałkę ▾ z kolumny **VPN** i wybierz **Tak**.

W Widoku eksperta wyświetlone są dwie dodatkowe kolumny:

- **Tryb Niewidzialności** - czy twój komputer jest wykrywany przez inne komputery w sieci.

  Aby skonfigurować Tryb Niewidzialności, w kolumnie **Tryb Niewidzialności** kliknij strzałkę ▾ i wybierz odpowiednią opcję.

Opcje Niewidzialności	Opis
Włączony	Tryb Niewidzialności jest włączony.Twój komputer jest niewidoczny zarówno z sieci lokalnej jak i z Internetu.
Wyłączony	Tryb Niewidzialności jest wyłączony.Każdy w sieci lokalnej i Internecie może pingować i wykryć twój komputer.
Zdalne	Twój komputer nie może być wykryty z Internetu.Użytkownicy sieci lokalnej mogą pingować i wykryć twój komputer.

- **Ogólne** - określa, czy dla tego połączenia stosowane są reguły ogólne.

  Jeśli adres IP karty sieciowej został zmieniony, BitDefender odpowiednio zmodyfikuje typ sieciJeśli chcesz zachować ten sam typ, kliknij strzałkę ▾ w kolumnie **Ogólne** i wybierz **Tak**.

21.3.1. Strefy Sieciowe

Możesz dodawać dozwolone lub zablokowane komputery dla wybranego adaptera.

Zaufana strefa to komputer któremu w pełni ufasz.Cały ruch pomiędzy twoim komputerem i komputerem zaufanym jest dozwolony.Aby udostępniać zasoby z

wybranymi komputerami w niezabezpieczonej sieci bezprzewodowej, dodaj je jako zaufane komputery.

Blokowana strefa to komputer z którym nie chcesz się komunikować.

Tabela **Strefy sieci** przedstawia aktualne strefy sieci dla każdego adaptera.

Aby dodać strefę, wybierz kartę i kliknij **Dodaj strefę**.Pojawi się nowe okno.

Wykonaj następujące kroki:

1. Wybierz adres IP komputera który chcesz dodać.
2. Wybierz działanie:
   - **Zezwól** - aby zezwolić na cały ruch pomiędzy twoim komputerem i wybranym komputerem.
   - **Zabroń** - zablokuje cały ruch pomiędzy twoim komputerem i wybranym komputerem.
3. Kliknij **OK**.

21.4. Urządzenia

Aby zarządzać urządzeniami podłączonymi do sieci, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany
: Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Zaporę Sieciową**.W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Urządzenia**.

Widok eksperta
: Przejdź do **Zapora Sieciowa > Urządzenia**.

W tabeli wymienione są drukarki, faksy i skanery wykryte w sieci oraz ustawione dla nich operacje domyślne.Aby zmienić stan urządzenia, kliknij je dwukrotnie w tabeli i w oknie, które pojawi się na ekranie, wybierz daną operację: zezwól na lub zablokuj komunikację z urządzeniem.

Do zarządzania listą urządzeń użyj dostępnych przycisków:

- **Dodaj** - dodaj urządzenie, którego nie ma na liście.
- **Usuń** - usuń wybrane urządzenie z listy.
- **Odśwież urządzenia** - uruchom nowy skan sieci, aby zaktualizować listę urządzeń.

21.5. Kontrola Połączenia

Aby monitorować bieżącą aktywność w sieci / Internecie (dla protokołu TCP i UDP) uszeregowaną według aplikacji i otworzyć dziennik Zapory sieciowej BitDefender postępuj wg wskazówek:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Zapora Sieciowa > Aktywność**.

Możesz zobaczyć ruch posortowany według aplikacji. Dla każdej aplikacji, widać połączenia i otwarte porty a także statystyki odnośnie wychodzącej & przychodzącej szybkości ruchu i pełna liczba wysłanych / odebranych danych.

Jeśli chcesz widzieć też nieaktywne procesy, odznacz pole **Ukryj Nieaktywne Procesy**.

Ikony mają następujące znaczenia:

- Wskazuje na wychodzące połączenie.
- Wskazuje na przychodzące połączenie.
- Oznacza otwarty port na komputerze.

Okno przedstawia obecną aktywność sieci / Internetu w czasie rzeczywistym. Gdy połączenia lub porty są zamykane, możesz zobaczyć, że odpowiednie statystyki zmniejszają się i ewentualnie wkrótce znikają.To samo dzieje się ze wszystkimi statystykami odpowiadającymi aplikacjom, które generują ruch lub mają otwarte porty, które zamykasz.

Aby uzyskać kompleksową listę zdarzeń dotyczących użytkowania modułu Zapory Sieciowej (włączania/wyłączania zapory, blokowania ruchu, modyfikowania ustawień) lub utworzoną przez operacje wykryte w tym module (skanowanie portów, blokowanie prób nawiązania łączności lub ruchu zgodnie z regułami), zobacz plik dziennika Zapory Sieciowej BitDefender. Aby to zrobić, kliknij **Pokaż dziennik**.Plik jest znajduje się w folderze Common Files aktualnego użytkownika Windows, a dokładnie w `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Jeżeli chcesz aby dziennik zawierał więcej informacji, zaznacz opcję **Zwiększ Objętość Dziennika**.

21.6. Rozwiązywanie Problemów z Zaporą Sieciową

Jeśli podejrzewasz, że dane zagadnienie spowodowane jest przez Zaporę Sieciową BitDefender, pomocą w jego rozwiązaniu może być Kreator Rozwiązywania Problemów.

Aby uruchomić kreatora, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany

Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Zaporę Sieciową**.W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Widok eksperta

Przejdź do **Zapora Sieciowa > Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Kreator może pomóc w szybkim rozwiązaniu następujących problemów dotyczących łączności, które zwykle wiążą się z konfiguracją zapory sieciowej:

- Próbuję drukować, ale nie udaje mi się.
- Próbuję uzyskać dostęp do komputera w mojej sieci, ale nie udaje mi się to.
- Próbuję połączyć się z Internetem, ale nie udaje mi się.

Jeśli żadna z tych sytuacji nie opisuje problemu, na który się natknąłeś, wybierz **Inny problem z zaporą sieciową**, aby otworzyć okno **Narzędzia pomocy technicznej**.

Więcej informacji na temat kreatora zawiera sekcja Rozwiązywanie problemów tego przewodnika.

22. Podatności

Ważnym krokiem w ochronie twojego komputera przeciw szkodliwym aplikacjom i osobom jest aktualizowanie systemu oraz aplikacji z których często korzystasz.Co więcej, aby zapobiec nieautoryzowanemu dostępowi do twojego komputera, silne hasło (hasło które jest trudne do odgadnięcia) musi być ustawione dla każdego konta użytkownika Windows.

BitDefender regularnie sprawdza twój system szukając podatności i informując cię o zaistniałych zagadnieniach.

22.1. Sprawdzanie Podatności

Można dokonać sprawdzenia pod kątem podatności oraz naprawić je, korzystając z kreatora **Skanowania Podatności**.Aby uruchomić kreatora, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany
: Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Skanowanie Podatności**.

Widok eksperta
: Przejdź do **Podatności > Stan** i kliknij **Sprawdź teraz**.

Wykonaj następującą, sześciopunktową procedurę, aby usunąć podatności z systemu.Możliwość poruszania się w kreatorze zapewnia przycisk **Dalej**. Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Chroń swój Komputer**

   Wybierz podatności do sprawdzenia.

2. **Skanuj wybrane zagadnienia...**

   Poczekaj aż BitDefender zakończy sprawdzanie systemu pod kątem podatności.

3. **Aktualizacje Windows**

   Możesz zobaczyć listę krytycznych oraz nie krytycznych aktualizacji Windows które aktualnie nie są zainstalowane na twoim komputerze.Wybierz aktualizacje, które chcesz zainstalować.

4. **Aktualizacje Aplikacji**

   Jeśli aplikacja jest nieaktualna, kliknij podany link aby pobrać najnowszą wersję.

5. **Słabe Hasło**

   Możesz zobaczyć listę użytkowników kont Windows skonfigurowanych na twoim komputerze i poziom ochrony jaki te hasła zapewniają.Kliknij **Napraw** aby zmodyfikować słabe hasła.

6. **Podsumowanie**

   W tym miejscu można zobaczyć wynik operacji.

22.2. Status zadania

Aby zobaczyć bieżący stan podatności i włączyć/wyłączyć jej automatyczne skanowanie, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Podatności > Stan**.

Ta tabela pokazuje zagadnienia wykryte w ostatnim skanowaniu podatności i sprawdza ich status.Możesz zobaczyć działanie które musisz podjąć aby naprawić podatności (jeśli są).Jeśli działanie jest **Brak**, to dane zagadnienie nie jest podatnością.

WAŻNE

Aby być automatycznie informowanym o podatności systemu lub aplikacji, nie wyłączaj opcji **Automatycznego skanowania podatności**.

W zależności od zagadnienia, naprawienie określonej podatności wygląda następująco:

- Jeśli są dostępne aktualizacje Windows, kliknij na **Instaluj** w kolumnie **Akcja** aby je zainstalować.
- Jeśli aplikacja jest przestarzała, kliknij **Więcej informacji**, aby zobaczyć informacje o wersji i znaleźć łącze do witryny internetowej sprzedawcy, z której można zainstalować najnowszą wersję tej aplikacji.
- Jeśli konto użytkownika Windows ma słabe hasło, kliknij **Zobacz & Napraw**, aby przy następnym logowaniu zmusić użytkownika do jego zmiany lub zmień je sam.Aby hasło było silne, użyj kombinacji dużych i małych liter, cyfr oraz znaków specjalnych (takich jak #, $ lub @).
- Jeśli funkcja Autoodtwarzanie Multimediów jest w systemie Windows włączona, kliknij **Napraw**, aby ją wyłączyć.

22.3. Ustawienia

Aby skonfigurować ustawienia automatycznego sprawdzania podatności, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Podatności > Ustawienia**.

3. Zaznacz pola odpowiednich podatności systemu które chcesz aby były regularnie sprawdzane.
   - **Krytyczne Aktualizacje Windows**
   - **Zwykłe Aktualizacje Windows**
   - **Aktualizacje Aplikacji**
   - **Słabe Hasło**
   - **Autoodtwarzanie multimediów**

Notatka

Jeśli odznaczysz pole obok podatności, BitDefender nie będzie informował ciebie o zagadnieniach z nią związanych.

23. Szyfrowanie rozmów

Zawartość wiadomości komunikatora powinna zostać pomiędzy użytkownikiem i jego rozmówcą.Dzięki szyfrowaniu rozmów możesz mieć pewność, że każda osoba, która spróbuje przechwycić je w drodze między tobą a twoim rozmówcą, nie będzie w stanie odczytać ich zawartości.

Domyślnie, Bitdefender szyfruje wszystkie twoje rozmowy prowadzone przez:

- Twój rozmówca ma zainstalowaną wersję BitDefender, która obsługuje szyfrowanie rozmów dla komunikatorów IM.
- Ty oraz twój rozmówca używacie komunikatora Yahoo Messenger lub Windows Live (MSN) Messenger.

WAŻNE

BitDefender nie będzie szyfrował rozmowy, jeśli rozmówca korzysta z komunikatora bazującego na stronie WWW, takiego jak Czateria, lub innej aplikacji do rozmów która obsługuje Yahoo Messenger lub MSN.

Konfigurowanie szyfrowania komunikacji natychmiastowej:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Szyfrowanie > Szyfrowanie rozmów**.

Notatka

Korzystając z paska narzędziowego BitDefender umieszczonego w oknie rozmowy, można łatwo konfigurować szyfrowanie komunikacji natychmiastowej.

Domyślnie, Szyfrowanie IM jest włączone zarówno dla Yahoo Messenger jak i Windows Live (MSN) Messenger.Możesz wybrać wyłączenie Szyfrowania IM dla podanego komunikatora lub całkowicie.

Dwie tabele są wyświetlane:

- **Wyjątki Szyfrowania** - lista ID użytkowników oraz przypisanych komunikatorów IM dla których szyfrowanie jest wyłączone.Aby usunąć kontakt z listy zaznacz go i kliknij **Usuń**.
- **Aktualne Połączenia** - lista aktualnych połączeń dla komunikatorów IM (ID użytkownika oraz przypisany komunikator) oaz czy szyfrowanie jest włączone czy też nie.Połączenie nie może być szyfrowane z następujących powodów:
  - Wyłączyłeś szyfrowanie komunikacji z tym kontaktem.
  - Twój kontakt nie ma zainstalowanego BitDefendera w wersji obsługującej szyfrowanie IM.

23.1. Wyłączanie szyfrowania dla Podanych Użytkowników

Aby wyłączyć szyfrowanie dla podanych użytkowników, wykonaj następujące kroki:

1. Aby otworzyć okno konfiguracji, kliknij przycisk **Dodaj**.
2. Wpisz w polu edycji ID swojego kontaktu.
3. Wybierz komunikator przypisany do tego kontaktu.
4. Kliknij **OK**.

23.2. Pasek narzędziowy BitDefender w Oknie rozmów

Możesz łatwo skonfigurować szyfrowanie rozmów w komunikatorach używając paska narzędzi BitDefender w oknie komunikatora.

Pasek narzędziowy powinien znajdować się w prawym dolnym ekranie okna rozmowy. Szukaj loga BitDefender aby go odnaleźć.

Notatka

Pasek narzędzi pokazuje że rozmowa jest szyfrowana wyświetlając mały klucz obok loga BitDefender.

Klikając na pasku narzędzi BitDefendera masz dostęp do następujących opcji:

- **Zablokuj szyfrowanie na stałe dla kontaktu.**
- **Zaproś kontakt do korzystania z szyfrowania.** Aby szyfrować rozmowy, twój kontakt musi zainstalować BitDefender i używać kompatybilnego programu IM.
- **Dodaj kontakt do czarnej listy Ochrony Rodzicielskiej.** Jeśli dodasz kontakt do czarnej listy Kontroli Rodzicielskiej i jest ona odblokowana, nie zobaczysz żadnych informacji przysyłanych przez ten kontakt.Aby usunąc kontakt z czarnej listy kliknij na pasek i wybierz **Usuń kontakt z czarnej listy Kontroli Rodzicielskiej.**.

24. Tryb Gry / Laptopa

Tryb Gry / Laptopa pozwala tonie na skonfigurowanie specjalnych trybów działania BitDefendera:

- Tryb Gry tymczasowo modyfikuje ustawienia produktu aby zminimalizować zużycie zasobów podczas grania.
- Tryb Laptopa blokuje wykonanie zaplanowanych zadań gdy laptop korzysta z baterii aby zmniejszyć pobór mocy.
- Tryb Cichy tymczasowo modyfikuje ustawienia produktu, tak aby zminimalizować liczbę monitów podczas oglądania filmów lub prezentacji.

24.1. Tryb Gry

Tryb Gry tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na wydajność systemu.W Trybie Gry, następujące ustawienia są stosowane:

- Wszystkie alarmy i wyskakujące okienka BitDefendera są zablokowane.
- Poziom ochrony w czasie rzeczywistym BitDefendera jest ustawiony na **Tolerancyjny**.
- Zapora sieciowa BitDefendera jest ustawiona na **Zezwól Wszystkim**.Oznacza to że wszystkie połączenia (zarówno przychodzące jak i wychodzące) automatycznie dostają zezwolenie, bez względu na port i protokół których używają.
- Domyślnie aktualizacje nie są wykonywane.

> **Notatka**
> Aby zmienić te ustawienia, kliknij Aktualizacja>Ustawienia i odznacz pole **Nie aktualizuj jeśli włączony jest Tryb Gry**.

Domyślnie, BitDefender automatycznie włącza Tryb Gry gdy uruchomisz grę będącą na liście znanych gier BitDefendera lub aplikacje działającą w trybie pełno ekranowym.Możesz ręcznie włączyć Tryb Gry używając domyślnych klawiszy skrótów `Ctrl+Alt+Shift+G`.Wysoce zalecane jest wyłączenie Trybu Gry kiedy kończysz grać (możesz użyć tej samej kombinacji klawiszy skrótów `Ctrl+Alt+Shift+G`).

> **Notatka**
> W Trybie Gry, możesz zobaczyć literę G nad ikoną BitDefendera.

Konfigurowanie Trybu Gry:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Tryb Gry/Laptopa > Tryb Gry**.

Na górze tej sekcji, możesz zobaczyć status Trybu Gry.Aby zmienić bieżący stan, możesz kliknąć **Tryb Gry jest włączony** lub **Tryb Gry jest wyłączony**.

24.1.1. Konfiguracja Automatycznego Trybu Gry

Automatyczny Tryb Gry umożliwia BitDefenderowi włączenie trybu gry automatycznie przy wykryciu uruchomienia gry.Możesz skonfigurować następujące opcje:

- **Użyj domyślnej listy gier dostarczonej przez BitDefendera** - automatycznie włącza Tryb Gry kiedy uruchomisz grę z listy znanych gier BitDefendera.Aby zobaczyć tą listę, kliknij na **Zarządzaj Grami** a następnie wybierz **Lista Gier**.
- **Działanie w trybie pełnoekranowym** - pozwala automatycznie włączać Tryb Gry lub Tryb Cichy, gdy aplikacja przechodzi do trybu pełnoekranowego.
- **Pytaj, czy aplikacje pełnoekranowe powinny być dodawane do listy gier** - aby otrzymywać monity o dodanie nowej aplikacji do listy gier podczas wychodzenia z trybu pełnoekranowego.Dodając nową aplikacje do listy gier, przy następnym uruchomieniu jej BitDefender automatycznie włączy Tryb Gry.

Notatka

Jeśli nie chcesz, aby BitDefender automatycznie uruchamiał Tryb Gry, usuń zaznaczenie pola wyboru **Automatyczny Tryb Gry jest włączony**

24.1.2. Zarządzanie Listą Gier

BitDefender automatycznie włącza Tryb Gry gdy uruchomisz aplikacje z listy gier.Aby zobaczyć i zarządzać listą gier, kliknij **Zarządzaj Grami**.Pojawi się nowe okno.

Nowe aplikacje są automatycznie dodawane do listy gdy:

- Uruchomiłeś grę z listy znanych gier BitDefendera.Aby zobaczyć tą listę, kliknij na **Lista Gier**.
- Po wyłączeniu trybu pełnoekranowego, dodasz aplikacje do listy używając okienka pytającego.

Jeśli chcesz wyłączyć Automatyczny Tryb Gry dla aplikacji z listy, odznacz odpowiednie pole.Powinieneś wyłączyć Automatyczny Tryb Gry dla zwykłych aplikacji korzystających z trybu pełnoekranowego, takich jak przeglądarka internetowa czy odtwarzacz filmów.

Aby zarządzać listą gier, możesz skorzystać z przycisków u góry tabeli:

- **Dodaj** - dodaje nową aplikacje do listy gier.
- **Usuń** - usuwa aplikacje z listy gier.
- **Edytuj** - edytuje wpis w liście gier.

24.1.3. Dodawanie lub Edytowanie Gier

Gdy dodajesz lub edytujesz wpis z listy gier, pojawia się nowe okno.

Kliknij **Przeglądaj** aby wybrać aplikacje lub podaj pełną ścieżkę do aplikacji w polu edycji.

Jeżeli nie chcesz automatycznie włączać Trybu Gry gdy podana aplikacja zostanie włączona, zaznacz **Wyłącz**.

Kliknij **OK** aby dodać pozycję do tabeli.

24.1.4. Konfigurowanie Ustawień Trybu Gry

Aby skonfigurować zachowanie zaplanowanych zadań, użyj opcji:

- **Pozwól temu modułowi aby modyfikować harmonogram zadań modułu Antywirusowego** - aby uniemożliwić uruchamianie zaplanowanych zadań gdy włączony jest Tryb Gry.Możesz wybrać jedną z następujących opcji:

Opcje	Opis
Pomiń Zadanie	Nie uruchamiaj zaplanowanego zadania.
Przełóż Zadanie	Uruchom wybrane zadanie natychmiast po wyłączeniu Trybu Gry.

Aby automatycznie wyłączyć zaporę sieciową BitDefendera przy włączonym Trybie Gry, wykonaj następujące kroki:

1. Kliknij **Zaawansowane**.Pojawi się nowe okno.
2. Zaznacz pole **Ustaw zaporę sieciową na Zezwól Wszystkim (Tryb Gry) w Trybie Gry**.
3. Kliknij **Zastosuj** aby zapisać zmiany.

24.1.5. Zmienianie klawiszy skrótu Trybu Gry

Tryb Gry można włączyć ręcznie za pomocą`Ctrl+Alt+Shift+G`Klawisz szybkiego dostępu.Jeżeli chcesz zmienić klawisze skrótu, wykonaj następujące kroki:

1. Kliknij **Zaawansowane**.Pojawi się nowe okno.
2. W polu **użyj Klawiszy Skrótu** ustaw klawisze skrótu które tobie odpowiadają:
   - Wybierz które klawisze mają być używane zaznaczając odpowiednio: Klawisz Ctrl (`Ctrl`), Klawisz Shift (`Shift`) lub klawisz Alt (`Alt`).
   - W polu edycji wpisz literę klawisza, którego chcesz użyć.

   Na przykład, Jeżeli chcesz użyć klawiszy `Ctrl+Alt+D` jako skrótu musisz ustawić tylko `Ctrl` i `Alt` raz wpisać `D`.

Notatka
Odznaczając pole obok **Użyj Klawiszy Skrótów** wyłączy skrót klawiszowy.

3. Kliknij **Zastosuj** aby zapisać zmiany.

24.2. Tryb Laptopa

Tryb Laptopa jest specjalnie zaprojektowany dla użytkowników laptopów i notebooków. Pomaga on zminimalizować wpływ BitDefendera na pobór prądu gdy korzystają one z baterii.

W Trybie Laptopa, zaplanowane zadania są domyślnie nie uruchamiane.

BitDefender wykrywa kiedy laptop korzysta z baterii i automatycznie włącza tryb laptopa.Identycznie, BitDefender automatycznie wyłącza Tryb Laptopa, kiedy wykryje że laptop nie korzysta już z baterii.

Konfigurowanie Trybu Laptopa:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Tryb Gry/Laptopa > Tryb Laptopa**.

Możesz zobaczyć czy Tryb Laptopa jest włączony czy nie.Jeśli Tryb Laptopa jest włączony, BitDefender zastosuje wcześniej skonfigurowane ustawienia na do czasu aż laptop przestanie korzystać z baterii.

24.2.1. Konfigurowanie Ustawień Trybu Laptopa

Aby skonfigurować zachowanie zaplanowanych zadań, użyj opcji:

- **Pozwól temu modułowi aby modyfikować harmonogram zadań modułu Antywirusowego** - aby uniemożliwić uruchamianie zaplanowanych zadań gdy włączony jest Tryb Laptopa.Możesz wybrać jedną z następujących opcji:

Opcje	Opis
Pomiń Zadanie	Nie uruchamiaj zaplanowanego zadania.
Przełóż Zadanie	Uruchom wybrane zadanie natychmiast po wyłączeniu Trybu Laptopa.

24.3. Tryb cichy

Tryb Cichy tymczasowo modyfikuje ustawienia zabezpieczeń, tak aby zminimalizować ich wpływ na wydajność systemu.W Trybie Cichym stosuje się następujące ustawienia:

- Wszystkie alarmy i wyskakujące okienka BitDefendera są zablokowane.
- Zapora sieciowa BitDefendera jest ustawiona na **Zezwól Wszystkim**.Oznacza to że wszystkie połączenia (zarówno przychodzące jak i wychodzące) automatycznie dostają zezwolenie, bez względu na port i protokół których używają.
- Domyślnie zadania zaplanowane są wyłączone.

Domyślnie, BitDefender automatycznie włącza tryb Cichy, gdy oglądasz film lub prezentację, lub gdy aplikacja przechodzi do trybu pełnoekranowego.Po zakończeniu oglądania filmu lub prezentacji zaleca się wyjście z Trybu Cichego.

Notatka
Gdy włączony jest Tryb Cichy, można dostrzec drobną zmianę małej ikony BitDefender, która znajduje się obok zegara.

Konfigurowanie Trybu Cichego:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Tryb Gry/Laptopa > Tryb Cichy**.

W górnej części sekcji widoczny jest stan Trybu Cichego.Aby zmienić bieżący stan, możesz kliknąć **Tryb Cichy jest włączony** lub **Tryb Cichy jest wyłączony**.

24.3.1. Konfigurowanie Działania w Trybie Pełnoekranowym

Możesz skonfigurować następujące opcje:

- **Działanie w trybie pełnoekranowym** - pozwala automatycznie włączać Tryb Gry lub Tryb Cichy, gdy aplikacja przechodzi do trybu pełnoekranowego.

Notatka
Jeśli nie chcesz, aby BitDefender automatycznie uruchamiał Tryb Cichy, usuń zaznaczenie pola wyboru **Działanie w trybie pełnoekranowym**.

24.3.2. Konfigurowanie Ustawień Trybu Cichego

Aby skonfigurować zachowanie zaplanowanych zadań, użyj opcji:

- **Włącz ten moduł, aby modyfikować zadania skanowania antywirusowego** - aby uniemożliwić uruchamianie zaplanowanych zadań skanowania w Trybie Cichym.Możesz wybrać jedną z następujących opcji:

Opcje	Opis
Pomiń Zadanie	Nie uruchamiaj zaplanowanego zadania.
Przełóż Zadanie	Wykonaj zaplanowane zadanie zaraz po wyjściu z Trybu Cichego.

25. Sieć Domowa

Moduł Sieci pozwala tobie na zarządzanie produktami BitDefender zainstalowanymi na komputerach w twoim domu z pojedynczego komputera.Aby uzyskać dostęp do modułu Sieci domowej, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany
Przejdź do zakładki **Sieć**.

Widok eksperta
Przejdź do **Sieć domowa**.

Notatka
Możesz też dodać skrót do Moich narzędzi.

Aby móc zarządzać produktami BitDefender zainstalowanymi na twoich domowych komputerach, musisz wykonać następujące kroki:

1. Włącz na komputerze sieć domową BitDefender.Skonfiguruj komputer jako Serwer.
2. Idź do każdego komputera którym chcesz zarządzać i dołącz go do swojej sieci (ustaw hasło)Skonfiguruj każdy komputer jako Zwykły.
3. Wróć do swojego komputera i dodaj komputery którymi chcesz zarządzać.

25.1. Włączanie Sieci BitDefender

Aby włączyć sieć domową BitDefender, wykonaj następujące kroki:

1. Kliknij na **Odblokuj Sieć**.Zostaniesz poproszony o ustawienie hasła domowego zarządzania.
2. Wpisz to samo hasło we wszystkie pola edycji.
3. Określ rolę komputera w sieci domowej BitDefender:
   - **Komputer - Serwer** - wybierz tę opcję na komputerze, który będzie używany do zarządzania innymi komputerami.
   - **Zwykły komputer** - wybierz tę opcję na komputerach, które będą zarządzane przez Komputer - Serwer.
4. Kliknij **OK**.

Możesz zobaczyć nazwę komputerów pojawiających się w sieci.

Pojawi się przycisk **Zablokuj Sieć**.

25.2. Dodawanie Komputerów do Sieci BitDefender

Do sieci automatycznie dodany zostanie każdy komputer, który spełnia następujące kryteria:

- Sieć domowa BitDefender została do tego włączona.
- rolę ustawiono na Zwykły komputer.
- Hasło ustawione podczas włączania sieci jest takie samo jak hasło ustawione na komputerze będącym serwerem.

Notatka

W Widoku eksperta możesz w dowolnym czasie przeskanować sieć domową w poszukiwaniu komputerów, które spełniają te kryteria. W tym celu kliknij przycisk **Automatyczne odkrywanie**.

Aby z komputera będącego serwerem dodać ręcznie komputer do sieci domowej BitDefender, wykonaj następujące kroki:

1. Kliknij na **Dodaj Komputer**.
2. Wprowadź swoje hasło domowego zarządzania i kliknij **OK**.Pojawi się nowe okno.

   Możesz zobaczyć listę komputerów w sieci.Ikony mają następujące znaczenie:

    Pokazuje komputer włączony i z nie zainstalowanym produktem BitDefender.

    Pokazuje komputer włączony i z zainstalowanym BitDefenderem.

    Pokazuje komputer wyłączony i z zainstalowanym BitDefenderem.
3. Wykonaj jedną z czynności:
   - Wybierz z listy nazwę komputera do dodania.
   - Wpisz nazwę lub adres IP komputera do dodania w odpowiednie pole.
4. Kliknij **Dodaj**.Zostaniesz poproszony o podanie hasła domowego zarządzania dodawanego komputera.
5. Wpisz hasło domowego zarządzania na danym komputerze.
6. Kliknij **OK**.Jeśli podałeś prawidłowe hasło, nazwa wybranego komputera pojawi się na mapie sieci.

25.3. Zarządzanie Siecią BitDefender

Gdy już utworzysz domową sieć BitDefender, możesz zarządzać wszystkimi produktami BitDefender z jednego komputera.

Jeśli umieścisz kursor myszy nad komputerem na mapie sieci, możesz zobaczyć informacje o nim (nazwa, adres IP, ilość zagadnień wpływających na bezpieczeństwo systemu, status rejestracji BitDefendera).

Jeśli klikniesz na nazwę komputera na mapie sieci, możesz zobaczyć wszystkie zadania administracyjne które możesz przeprowadzić zdalnie na tym komputerze.

- **Zarejestruj BitDefender na tym komputerze**

  Pozwala zarejestrować BitDefender na tym komputerze przez wprowadzenie klucza licencyjnego.

- **Ustaw hasło dla ustawień na zdalnym komputerze**

  Pozwala na stworzenie hasła ograniczającego dostęp do ustawień BitDefendera na tym komputerze.

- **Uruchom zadanie skanowania na żądanie**

  Pozwala uruchomić skanowanie na żądanie zdalnie, z innego komputera. Możesz wykonywać następujące zadania skanowania: Skanowanie Moich Dokumentów, Skanowanie Systemu lub Głębokie Skanowanie Systemu.

- **Napraw wszystkie zagadnienia na tym komputerze**

  Pozwala naprawić zagadnienia, które wpływają na bezpieczeństwo komputera za pomocą kreatora Napraw Wszystkie.

- **Podgląd Historii/Zdarzeń**

  Pozwala na dostęp do modułu **Historia&Zdarzenia** BitDefendera zainstalowanego na tym komputerze.

- **Aktualizuj Teraz**

  Rozpoczyna proces Aktualizacji dla oprogramowania BitDefender zainstalowanego na tym komputerze.

- **Ustaw Profil Kontroli Rodzicielskiej**

  Pozwala określić kategorię wiekową dla filtru WWW Kontroli Rodzicielskiej na tym komputerze.

- **Ustaw jako Serwer Aktualizacji dla tej sieci**

  Pozwala na ustawienie tego komputera jako serwer aktualizacji dla wszystkich produktów BitDefender zainstalowanych na komputerach w tej sieci.Skorzystanie z tego rozwiązania zmniejszy ruch internetowy, ponieważ tylko jeden komputer w sieci będzie łączył się z Internetem i pobierał aktualizacje.

- **Usuń komputer z sieci domowej**

  Pozwala na usunięcie komputera z sieci.

Gdy interfejs BitDefender działa w trybie Widoku średniozaawansowanego, klikając odpowiednie przyciski można uruchomić jednocześnie kilka zadań na wszystkich zarządzanych komputerach.

- **Skanuj Wszystkie** - pozwala skanować wszystkie zarządzane komputery jednocześnie.

- **Aktualizuj Wszystkie** - pozwala aktualizować wszystkie zarządzane komputery jednocześnie.
- **Zarejestruj Wszystkie** - pozwala tobie zarejestrować wszystkie zarządzane komputery jednocześnie.

Przed uruchomieniem zadania na konkretnym komputerze, będziesz poproszony o podanie lokalnego hasła zarządzania domowego.Wprowadź swoje hasło domowego zarządzania i kliknij **OK**.

Notatka

Jeżeli planujesz uruchomić kilka zadań, możesz zaznaczyć**Nie pokazuj tej wiadomości ponownie w tej sesji**.Zaznaczając tą opcje, nie będziesz pytany pnownie o hasło podczas tej sesji.

26. Aktualizacje

Nowe złośliwe oprogramowanie jest znajdywane i identyfikowane każdego dnia. Dlatego bardzo ważnym jest aby na bieżąco aktualizować BitDefendera najnowszymi sygnaturami.

Jeśli jesteś podłączony do Internetu za pomocą łącza szerokopasmowego lub DSL, BitDefender sam o siebie zadba. Domyślnie sprawdza dostępność aktualizacji po uruchamianiu komputera, a następnie co **godzinę**.

Jeśli wykryje aktualizację, możesz zostać zapytany o potwierdzenie aktualizacji lub proces aktualizacjo zostanie przeprowadzony automatycznie, w zależności od Ustawień automatycznej aktualizacji.

Proces aktualizacji wykonywany jest w tle co znaczy że pliki są kolejno aktualizowane. Dzięki temu proces aktualizacji nie wpływa na działanie produktu i jednocześnie eliminuje wszelkie podatności.

WAŻNE

Aby być chronionym przed najnowszymi zagrożeniami miej włączony moduł **Automatycznej Aktualizacji**.

Aktualizacje są dostarczane w następujący sposób:

- **Aktualizacje silników antywirusowych** - jako nowe zagrożenia pojawiające się, pliki zawierające sygnatury wirusów mogą być nieustannie aktualizowane. Ten typ aktualizacji jest także znany pod nazwą **Aktualizacja Definicji Wirusów**.
- **Aktualizacje silników antyspamowych** - nowe reguły są dodawane do heurystyki i filtra URL oraz nowe obraz zostaną dodane do filtra Obrazów. Pomaga to zwiększyć efektywność silników antyspamowych. Ten typ aktualizacji jest także znany pod nazwą **Aktualizacja Antyspamu**.
- **Aktualizacja silników antyspywareowych** - nowe sygnatury spyware są dodawane do bazy danych. Ten typ aktualizacji jest także znany pod nazwą **Aktualizacja Antyspyware**.
- **Aktualizacje produktów** - kiedy wychodzi nowa wersja programu, nowe cechy i technologie skanowania są wprowadzane aby efektywnie zwiększyć wydajność produktu. Ten typ aktualizacji jest także znany pod nazwą **Aktualizacja Produktu**.

26.1. Wykonywanie Aktualizacji

Automatyczna aktualizacja może być także zrobiona w dowolnym czasie, kiedy tylko chcesz za pomocą kliknięcia **Aktualizuj Teraz**. Aktualizacja ta jest także zwana jako **Aktualizacją na żądanie**.

Aby zaktualizować BitDefender, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok Podstawowy
W obszarze Chroń swój Komputer kliknij ikonę **Aktualizuj teraz**.

Widok średniozaawansowany
Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Aktualizuj teraz**.

Widok eksperta
Przejdź do **Aktualizacja > Aktualizacja** .

Moduł **Aktualizacja** połączy się z serwerami aktualizacji BitDefendera i sprawdzi czy są dostępne aktualizacje. Jeśli będą dostępne aktualizacje to zależnie od ustawień w Ustawienia Ręcznej Aktualizacji, zostaniesz zapytany czy chcesz aktualizować program albo aktualizacja zostanie przeprowadzona automatycznie.

WAŻNE
Może być konieczne ponowne uruchomienie komputera gdy zakończysz aktualizacje. Zalecamy to zrobić jak najszybciej.

Notatka
Jeśli łączysz się z Internetem za pomocą modemu, zalecane jest regularne aktualizowanie BitDefendera na żądanie.Aby uzyskać więcej informacji, odwołaj się do *„Jak aktualizować BitDefender przy wolnym połączeniu internetowym?”* (p. 177).

26.2. Konfigurowanie Ustawień Aktualizacji

Aktualizacje mogą być preprowadzone z lokalnej sieci, bezpośrednio przez Internet albo przez serwer proxy.Domyślnie, BitDefender sprawdzi co godzinę czy są aktualizacje w Internecie, i zainstaluj je bez powiadamiania cię.

Konfigurowanie ustawień aktualizacji:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Aktualizacja > Ustawienia**.
3. Skonfiguruj ustawienia według uznania.Aby dowiedzieć się za co odpowiada dana opcja, przytrzymaj nad nią kursor myszy i przeczytaj informację która pojawi się na dole okna.
4. Kliknij **Zastosuj** aby zapisać zmiany.

Aby zastosować domyślne ustawienia, kliknij **Domyślne**.

Ustawienia aktualizacji są podzielone na 4 kategorie (**Ustawienia Lokalizacji Aktualizacji**, **Ustawienia Automatycznej Aktualizacji**, **Ustawienia Ręcznej Aktualizacji** i **Zaawansowane**). Każda kategoria zostanie opisana oddzielnie.

26.2.1. Ustawienia Lokalizacji Aktualizacji

Aby ustawić miejsce aktualizacji, użyj opcji z kategorii **Ustawienia Lokalizacji Aktualizacji**.

Notatka

Skonfiguruj te ustawienia tylko jeśli jesteś połączony z siecią lokalną, która zawiera sygnatury szkodliwego oprogramowania dla BitDefender lokalnie lub jeśli łączysz się z Internetem przez serwer proxy.

Dla pewniejszych i szybszych aktualizacji, możesz ustawić dwie lokalizacje aktualizacji: **Podstawowy serwer aktualizacji** i **Alternatywny serwer aktualizacji**. Domyślnie oba te miejsca są identyczne: `http://upgrade.bitdefender.com`.

By zmodyfikować jedno z miejsc aktualizacji, wprowadź adres URL lokalnego serwera aktualizacyjnego w polu **URL** dla lokalizacji którą chcesz zmienić.

Notatka

Zalecamy ustawienie podstawowej lokalizacji na serwer lokalny i zostawienie alternatywnej lokalizacji aktualizacji bez zmian jako zabezpieczenie w razie gdyby lokalny serwer był niedostępny.

W przypadku gdy twoja firma korzysta z serwera proxy do połączenia się z Internetem, zaznacz **Użyj proxy** i kliknij na **Ustawienia Proxy** aby skonfigurować ustawienia proxy.Więcej informacji zawiera„Ustawienia połączeń” (p. 56)

26.2.2. Konfiguracja Automatycznej Aktualizacji

Aby skonfigurować proces automatycznej aktualizacji BitDefendera, użyj opcji w kategorii **Ustawienia Automatycznej Aktualizacji**.

Możesz określić liczbę godzin między dwoma kolejnymi próbami wyszukiwania aktualizacji w polu **Aktualizuj co**. Domyślnie, odstęp czasowy między kolejnymi aktualizacjami wynosi 1 godzinę.

By określić jak automatyczny proces aktualizacji ma być wykonany wybierz jedną z opcji:

- **Cicha aktualizacja** - BitDefender automatycznie pobiera i implementuje aktualizacje.
- **Pytaj przed pobraniem aktualizacji** - za każdym razem, gdy jest dostępna aktualizacja, zostaniesz zapytany przed jej pobraniem.
- **Pytaj przed instalacją** - za każdym razem, gdy aktualizacja zostanie pobrana zostaniesz zapytany przed jej zainstalowaniem.

26.2.3. Konfiguracja Ręcznej Aktualizacji

By określić jak ręczna aktualizacja (na prośbę użytkownika) powinna być wykonana, wybierz jedną z następujących opcji w kategorii **Ustawienia Ręcznej Aktualizacji**:

- **Cicha aktualizacja** - ręczna aktualizacja zostanie przeprowadzona automatycznie w tle.
- **Pytaj przed pobraniem aktualizacji** - za każdym razem, gdy jest dostępna aktualizacja, zostaniesz zapytany przed jej pobraniem.

26.2.4. Konfigurowanie Ustawień Zaawansowanych

Aby zapobiec zakłócaniu twojej pracy przez proces aktualizacji BitDefendera, skonfiguruj opcje w kategorii **Zaawansowane**:

- **Oczekuj na ponowne uruchomienie bez pytania** - Jeśli aktualizacja wymaga restartu, program będzie pracował na starych plikach do momentu ponownego uruchomienia komputera. Użytkownik nie zostanie poproszony o ponowne uruchomienie komputera dzięki temu aktualizacja nie będzie przeszkadzała użytkownikowi w pracy.
- **Nie przeprowadzaj aktualizacji w trakcie skanowania** - BitDefender nie będzie wtedy aktualizowany. Dzięki temu proces aktualizacji BitDefender nie będzie przeszkadzał zadaniom skanowania.

Notatka

Jeżeli program BitDefender będzie aktualizowany w trakcie procesu przeszukiwania, przeszukiwanie zostanie przerwane.

- **Nie przeprowadzaj aktualizacji, kiedy Tryb Gry jest włączony** - BitDefender nie będzie aktualizowany, gdy Tryb Gry jest włączony.W ten sposób możesz zminimalizować wpływ produktu na wydajność systemu w trakcie grania.
- **Włącz dzielenie się aktualizacjami** - Jeśli chcesz zminimalizować wpływ ruchu sieciowego na wydajność systemu podczas aktualizacji, użyj opcji udostępniania.
- **Wyślij pliki BitDefender z tego komputera** - BitDefender pozwala udostępniać innym użytkownikom BitDefender najnowsze sygnatury wirusów dostępne na danym komputerze.

Jak to zrobić

27. Jak skanować pliki i foldery?

Skanowanie z BitDefender jest łatwe i elastyczne.Istnieje kilka sposobów ustawienia BitDefender pod kątem skanowania plików i folderów w poszukiwaniu wirusów oraz innego złośliwego oprogramowania:

- Korzystając z Menu Kontekstowego Windows
- Korzystanie z Zadań Skanowania
- Używanie Paska Aktywności Skanera

Jak tylko uruchomisz skanowanie, pojawi się kreator skanowania antywirusowego i przeprowadzi cię przez cały proce.Aby uzyskać więcej informacji na temat tego kreatora, odwołaj się do *„Kreator Skanowania Antywirusowego”* (p. 68).

Notatka

Informacje o tym, w jaki sposób można wykonać skanowanie za pomocą BitDefender w Trybie awaryjnym Windows, znajdują się w *„Jak skanować komputer w Trybie awaryjnym?”* (p. 190).

27.1. Korzystając z Menu Kontekstowego Windows

To najprostsza i rekomendowana metoda na skanowanie plików i folderów na twoim komputerze.Kliknij prawym przyciskiem na obiekt który chcesz skanować i w menu wybierz **Skanowanie z BitDefender**.Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

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 twój komputer.

27.2. Korzystanie z Zadań Skanowania

Jeśli chcesz skanować swój komputer albo specyficzne foldery regularnie, możesz rozważyć korzystanie z zadań skanowania.Zadania skanowania instruują BitDefender, które lokalizacje ma skanować oraz które opcje i akcje wybierać. Na dodatek możesz takie zadania dodać do harmonogramu, aby uruchamiać je w odpowiednim czasie.

Aby skanować komputer korzystając z zadań skanowania, musisz otworzyć interfejs BitDefender i uruchomić pożądane zadanie.W zależności od trybu widoku interfejsu użytkownika, aby uruchomić to zadanie muszą zostać podjęte różne kroki.

Uruchamianie Zadań Skanowania w Widoku Podstawowym

W Widoku podstawowym można uruchomić pewne skonfigurowane wcześniej zadania skanowania.Kliknij przycisk **Bezpieczeństwo** i wybierz zadanie skanowania.Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

Uruchamianie Zadań Skanowania w Widoku Średniozaawansowanym

W Widoku średniozaawansowanym można uruchomić pewne skonfigurowane wcześniej zadania skanowania. Można także skonfigurować i uruchomić własne zadania skanowania, by przeskanować określone miejsca komputera za pomocą opcji skanowania niestandardowego.Wykonaj następujące kroki, aby uruchomić zadanie skanowania w Widoku średniozaawansowanym:

1. Kliknij zakładkę **Bezpieczeństwo**.
2. Po lewej stronie obszaru Szybkich zadań kliknij **Pełne Skanowanie** i wybierz zadanie skanowania.Aby skonfigurować i uruchomić własne skanowanie, kliknij **Własne Skanowanie**.
3. Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.Jeśli zdecydujesz się na uruchomienie własnego skanowania, musisz przeprowadzić Kreator Własnego Skanowania.

Uruchamianie Zadań Skanowania w Widoku eksperta

W Widoku eksperta można uruchomić wszystkie skonfigurowane wcześniej zadania skanowania, jak również zmienić ich opcje skanowania. Co więcej, jeśli chcesz przeskanować określone miejsca na komputerze, możesz utworzyć własne zadania skanowania.Wykonaj następujące kroki, aby uruchomić zadanie skanowania w Widoku eksperta:

1. Kliknij **Antyvirus** w menu po lewej stronie.
2. Kliknij zakładkę **Skanowanie**.Tutaj możesz znaleźć kilka podstawowych zadań skanowania i możesz tworzyć własne.
3. Dwukrotnie kliknij zadanie skanowania, które chcesz uruchomić.
4. Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

27.3. Używanie Paska Aktywności Skanera

Okienko czynności skanowania jest graficznym odzwierciedleniem wykonywanych czynności skanowania na twoim systemie.To małe okno jest domyślnie dostępne tylko w Widoku eksperta.

Możesz użyć Paska aktywności skanowania aby szybko skanować pliki lub foldery.Przenieś i upuść do

Pasek Aktywności Skanera

paska aktywności skanera plik lub folder który chcesz przeskanować.Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

Notatka

Aby uzyskać więcej informacji, odwołaj się do *„Pasek Aktywności Skanera”* (p. 20).

28. Jak utworzyć niestandardowe zadanie skanowania?

Aby utworzyć zadanie skanowania, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany

Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Skanowanie niestandardowe**.

Pojawi się kreator, który pomoże ci utworzyć zadanie skanowania.Możliwość poruszania się w kreatorze zapewniają przyciski **Dalej** i **Cofnij**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Witamy**
2. **Wybierz cel**

   Kliknij **Dodaj element docelowy**, aby wybrać pliki lub foldery przeznaczone do skanowania.

   Kliknij **Zaawansowane**.W zakładce **Przegląd** dostosuj opcje skanowania przesuwając suwak.Jeśli chcesz skonfigurować szczegółowe opcje skanowania, kliknij **Własne**.Aby określić termin uruchomienia zadania, przejdź do zakładki **Harmonogram**.
3. **Zakończ**

   W tym miejscu można podać nazwę zadania oraz, jeśli to konieczne, do obszaru Szybkich zadań dodać skanowanie.

   Kliknij **Uruchom skanowanie**, aby utworzyć zadanie i uruchomić kreatora skanowania.

Widok eksperta

1. Przejdź do **Antywirus > Skanowanie**.
2. Kliknij **Nowe zadanie**. Pojawi się nowe okno.

   Notatka

   Możesz także kliknąć prawym przyciskiem myszy wcześniej zdefiniowane zadanie skanowania, takie jak **Głębokie Skanowanie**, i wybrać **Klonuj Zadanie**.Jest to przydatne przy tworzeniu nowych zadań, ponieważ można w ten sposób modyfikować ustawienia powielonych zadań.
3. W zakładce **Przegląd** wpisz nazwę zadania i dostosuj opcje skanowania, przesuwając suwak.

   Jeśli chcesz skonfigurować szczegółowe opcje skanowania, kliknij **Własne**.
4. Przejdź do zakładki **Ścieżki** i wskaż cel skanowania. Kliknij **Dodaj element(y)**, aby wskazać pliki lub foldery przeznaczone do skanowania.

5. Aby określić termin uruchomienia zadania, przejdź do zakładki **Harmonogram**.
6. Kliknij **Ok**, aby zapisać zadanie.Nowe zadanie pojawi się wśród Zadań Zdefiniowanych przez Użytkownika i może być w dowolnym momencie edytowane, usunięte lub uruchomione w tym oknie.

29. Jak zaplanować skanowanie komputera?

Okresowe skanowanie komputera jest najlepszą praktyką aby utrzymać system wolny od złośliwego oprogramowania.BitDefender pozwala ci na harmonogramowanie zadań skanowania tak, aby automatycznie skanować twój komputer.

Aby zaplanować skanowanie komputera, wykonaj następujące kroki:

1. Otwórz BitDefender.
2. W zależności od wybranego trybu wyświetlania interfejsu użytkownika postępuj zgodnie z poleceniami:

   Widok średniozaawansowany
   Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Antywirusa**.

   Widok eksperta
   Kliknij **Antyvirus** w menu po lewej stronie.
3. Kliknij zakładkę **Skanowanie**.Tutaj możesz znaleźć kilka podstawowych zadań skanowania i możesz tworzyć własne.

   - Zadania systemowe są dostępne i mogą być uruchamiane na koncie każdego użytkownika Windows.
   - Zadania użytkowników są dostępne tylko dla i mogą być uruchamiane wyłącznie przez użytkowników którzy je stworzyli.

   To są domyślne zadania skanowania które możesz zaplanować:

   Pełne Skanowanie
   Skanuje cały system wyłączając archiwa.W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów.

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

   Skaner Autologowania
   Skanuje elementy które są uruchamiane podczas logowania użytkownika do systemu Windows.Aby skorzystać z tego zadania, musisz je zaplanować tak, aby było uruchomione przy starcie systemu.Domyślnie, skaner autologowania jest wyłączony.

   Głębokie Skanowanie
   Skanuje cały system.W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.

Moje Dokumenty

Użyj tego zadania do skanowania ważnych folderów aktualnego użytkownika: `Moje Dokumenty`, `Pulpit` oraz `Autostart`. To zapewni bezpieczeństwo dokumentów, miejsca pracy oraz uruchamianych aplikacji.

Jeśli żadne z zadań skanowania nie spełniają twoich potrzeb, możesz stworzyć nowe zadanie skanowania, które możesz zaplanować według własnych potrzeb.

4. Kliknij prawym przyciskiem na wybranym zadaniu i wybierz **Zaplanuj**.Pojawi się nowe okno.
5. Zaplanuj zadanie aby uruchamiało się według twoich potrzeb:
   - Aby uruchomić zadanie tylko jeden raz, wybierz **Tylko raz** i określ czas jego uruchomienia.
   - Aby uruchomić zadanie w czasie startu systemu, wybierz **W czasie startu systemu**.Możesz określić jak długo po starcie systemu zadanie powinno się ono uruchomić (w minutach).
   - Aby uruchomić zadanie skanowania regularnie, wybierz **Okresowo** i określ jak często powinno być uruchamiane, oraz jego start - datę i czas.

   Notatka

   Na przykład, aby skanować komputer w każdą sobotę o 2-giej w nocy, musisz skonfigurować harmonogram następująco:

   a. Wybierz **Okresowo**.

   b. W polu **Co każdy** wpisz 1, a później z menu wybierz **tydzień**.W ten sposób, zadanie jest uruchamiane raz w tygodniu.

   c. Jako datę wybierz najbliższą sobotę.

   d. Ustaw czas rozpoczęcia na `2:00:00 AM`.

6. Kliknij na **OK** aby zapisać harmonogram.Zadanie skanowania uruchomi się automatycznie według zaplanowanego harmonogramu który zdefiniowałeś.Jeśli komputer jest wyłączony w momencie kiedy ma odbyć się zaplanowane zadanie, zostanie ono przeprowadzone po jego następnym włączeniu.

30. Jak utworzyć konto użytkownika Windows?

Konto użytkownika Windows jest unikalnym profilem, który zawiera wszystkie ustawienia, przywileje oraz pliki osobiste dla każdego użytkownika.

Konta Windows pozwalają administratorowi domowego komputera kontrolować dostęp dla każdego użytkownika.

Skonfigurowanie kont użytkowników przydaje się, gdy komputer używany jest zarówno przez rodziców, jak i dzieci - rodzice mogą skonfigurować konto dla każdego z dzieci.

Wskaż swój system operacyjny, aby dowiedzieć się, jak utworzyć konta systemu Windows.

- Windows XP:
  1. Zaloguj się na komputerze jako administrator.
  2. Kliknij Start, Panel sterowania, a następnie Konta użytkownika.
  3. Kliknij Utwórz nowe konto.
  4. Podaj nazwę dla użytkownika. Możesz użyć pełnego imienia i nazwiska, imienia lub przezwiska danej osoby. Następnie kliknij Dalej.
  5. Dla typu konta wybierz Ograniczone, a następnie Utwórz konto. Konta ograniczone są odpowiednie dla dzieci, ponieważ nie mogą one wprowadzać zmian odnoszących się do całego systemu lub instalować określonych aplikacji.
  6. Nowe konto użytkownika zostało utworzone. Można je zobaczyć na ekranie Zarządzanie kontami.
- Windows Vista lub Windows 7:
  1. Zaloguj się na komputerze jako administrator.
  2. Kliknij Start, Panel sterowania, a następnie Konta użytkownika.
  3. Kliknij Utwórz nowe konto.
  4. Podaj nazwę dla użytkownika. Możesz użyć pełnego imienia i nazwiska, imienia lub przezwiska danej osoby. Następnie kliknij Dalej.
  5. W przypadku typu konta kliknij Standardowe, a następnie Utwórz konto. Konta ograniczone są odpowiednie dla dzieci, ponieważ nie mogą one wprowadzać zmian odnoszących się do całego systemu lub instalować określonych aplikacji.
  6. Nowe konto użytkownika zostało utworzone. Można je zobaczyć na ekranie Zarządzanie kontami.

Notatka

Teraz, gdy dodałeś konta nowych użytkowników, możesz utworzyć dla nich hasła.

31. Jak zaktualizować BitDefender za pomocą serwera proxy?

Zwykle BitDefender automatycznie wykrywa i importuje z systemu ustawienia proxy.Jeśli łączysz się z Internetem przez serwer proxy, konieczne może być znalezienie ustawień proxy i odpowiednie skonfigurowanie BitDefender.Informacje, jak należy to zrobić, znajdują się w *„Gdzie znaleźć informacje na temat Ustawień Proxy?”* (p. 203).

Po ustaleniu ustawień proxy wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Ogólne > Ustawienia**.
3. W **Ustawieniach połączenia** kliknij **Ustawienia Proxy**.
4. Wpisz w odpowiednich polach ustawienia proxy.
5. Kliknij **OK**.

Notatka

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

32. Jak dokonać uaktualnienia do innego produktu 2011 BitDefender?

Dzięki BitDefender 2011 można w łatwy sposób dokonać uaktualnienia z jednego produktu BitDefender 2011 do drugiego.

Rozważmy następujący scenariusz: od pewnego czasu używasz BitDefender Internet Security 2011 2011, a ostatnio postanowiłeś skorzystać z BitDefender Total Security 2011 i dodatkowych funkcji oferowanych przez ten program.

Musisz jedynie zakupić klucz licencji BitDefender 2011, do którego chcesz uaktualnić produkt i wpisać go w oknie rejestracji produktu BitDefender 2011, z którego aktualnie korzystasz.

Podążaj tymi krokami:

1. Otwórz BitDefender.
2. Kliknij łącze **Informacje o licencji** umieszczone w dolnej części okna.Pojawi się okno rejestracji.
3. Podaj klucz licencji i kliknij **Zarejestruj teraz**.
4. BitDefender poinformuje cię, że ten klucz licencji przeznaczony jest dla innego oprogramowania i zapewni ci możliwość jego zainstalowania.Aby dokonać uaktualnienia, kliknij odpowiednie łącze i wykonaj następującą trzypunktową procedurę.
   a. **Potwierdź działanie**
   b. **Aktualizacja w toku**

      Poczekaj, aż BitDefender zakończy proces uaktualniania.Zajmie to kilka minut.
   c. **Aktualizacja ukończona**

      Proces został ukończony. Wymagane może być ponowne uruchomienie systemu.

Rozwiązywanie Problemów i Uzyskiwanie Pomocy

33. Rozwiązywanie Problemów

Ten rozdział przedstawia niektóre problemy, na jakie można się natknąć w trakcie użytkowania BitDefender oraz ich potencjalne rozwiązania.Większość tych problemów można rozwiązać poprzez odpowiednie skonfigurowanie ustawień produktu.

Jeśli nie możesz w tym miejscu znaleźć pomocy dla swojego problemu lub przedstawione rozwiązania nie pomagają, możesz skontaktować się z przedstawicielem pomocy technicznej BitDefender, korzystając z metody przedstawionej w rozdziale *„Otrzymywanie pomocy”* (p. 194).

33.1. Problemy Dotyczące Instalacji

Ten artykuł pozwala na rozwiązanie typowych problemów dotyczących instalacji BitDefendera.Problemy te można pogrupować w kilka następujących kategorii:

- Błędy walidacji instalacji: instalator nie mógł zostać uruchomiony z powodu specyficznych warunków panujących w twoim systemie.
- Instalacje zakończone niepowodzeniem: udało się uruchomić instalator, ale proces instalacji nie zakończył się pomyślnie.

33.1.1. Błędy Walidacji Instalacji

Kiedy uruchomisz instalator, przed rozpoczęciem procesu instalacji, zostaje sprawdzonych kilka warunków.Poniższa tabela przedstawia najczęstsze powody błędów walidacji i sposoby ich uniknięcia.

Błąd	Opis&Rozwiązanie
Nie posiadasz odpowiednich praw do instalacji programu.	Aby uruchomić instalator i zainstalować BitDefender wymagane są prawa administratora.Wykonaj jedną z czynności: ● Zaloguj się na konto administratora Windows i uruchom kreator instalacji ponownie. ● Kliknij prawym przyciskiem myszy na plik i wybierz **Uruchom jako**.Wpisz nazwę użytkownika i hasło do konta administratora systemu Windows.
Instalator wykrył poprzednią wersję BitDefender która nie została poprawnie odinstalowana.	BitDefender był poprzednio zainstalowany w twoim systemie, ale nie został w całości usunięty. Ten warunek blokuje nową instalację BitDefender. Aby rozwiązać ten problem i zainstalować BitDefender, wykonaj następujące kroki:

Błąd	Opis&Rozwiązanie
	1. Przejdź do www.bitdefender.com/uninstall i pobierz specjalne narzędzie do odinstalowywania BitDefendera. 2. Korzystając z praw administratora, uruchom narzędzie do odinstalowywania. 3. Uruchom ponownie komputer. 4. Uruchom instalator ponownie aby zainstalować BitDefender.
Ten produkt BitDefender nie jest kompatybilny z wersją twojego systemu operacyjnego.	Próbujesz zainstalować BitDefender w nieobsługiwanym systemie operacyjnym.Sprawdź *„Wymagania Systemowe”* (p. 2) aby dowiedzieć się, na jakich systemach możesz zainstalować BitDefender. Jeśli twój system operacyjny to Windows XP z Service Pack 1 lub bez Service Pack, możesz zainstalować Service Pack 2 i uruchomić instalator ponownie.
Plik instalacji został stworzony dla innego typu procesora.	Jeśli zobaczysz taki błąd, oznacza to że próbujesz uruchomić nieprawidłową wersję pliku instalacyjnego.Istnieją dwie wersje pliku instalacyjnego BitDefender: jeden dla procesorów 32-bitowych i drugi, dla procesorów 64-bitowych. Aby upewnić się, że pobrałeś poprawną wersję dla swojego systemu, pobierz plik instalacyjny bezpośrednio z www.bitdefender.com.

33.1.2. Instalacja Nieudana

Może być kilka przyczyn tego niepowodzenia:

- Podczas instalacji pojawia się ekran błędu.Możesz zostać poproszony o anulowanie instalacji albo pojawi się przycisk umożliwiający uruchomienie narzędzia deinstalacji, które oczyści system.

  Notatka

  Zaraz po włączeniu instalacji, instalator może poinformować o niewystarczającej ilości wolnego miejsca na dysku aby zainstalować BitDefender. W tym przypadku, zwolnij miejsce na dysku do wymaganego poziomu, na partycji gdzie chcesz zainstalować BitDefender i wznów instalację.

- Instalator przestaje reagować, prawdopodobnie zawiesza się też system.Tylko ponowne uruchomienie systemu przywraca go do prawidłowego stanu.

- Instalacja została zakończona, ale nie możesz korzystać z kilku lub wszystkich funkcji BitDefender.

Aby rozwiązać problem nieudanej instalacji i zainstalować BitDefender, wykonaj następujące kroki:

1. **Wyczyść system po nieudanej instalacji.** Jeśli instalacja zakończy się niepowodzeniem, niektóre wpisy oraz pliki mogą pozostać w systemie. Takie pozostałości mogą blokować następną instalację BitDefender. Mogą także wpłynąć na stabilność i wydajność systemu. Dlatego powinny zostać usunięte przed kolejną próbą instalacji BitDefendera w systemie.

   Jeśli jest to ten przypadek, najłatwiejszym rozwiązaniem jest całkowite usunięcie BitDefender z systemu, a następnie ponowne zainstalowanie go.Aby uzyskać więcej informacji, odwołaj się do *„Jak całkowicie usunąć BitDefender?”* (p. 203).

2. **Zweryfikuj poniższe przyczyny w przypadku gdy instalacja zawiodła.** Zanim zaczniesz procedurę reinstalacji, sprawdź i usuń możliwe przeszkody które mogły się przyczynić do niepoprawnego zakończenia pierwszej instalacji:

   a. Sprawdź czy posiadasz zainstalowane inne oprogramowanie zabezpieczające, które może zakłócić normalną pracę BitDefender. Jeśli tak, zalecamy usunięcie wszystkich programów tego typu przed rozpoczęciem instalacji.

   b. Należy także sprawdzić czy system jest zainfekowany.Wykonaj jedną z czynności:

      - Skorzystaj z dysku ratunkowego BitDefender Rescue CD aby przeskanować swój komputer i usunąć istniejące zagrożenia.Aby uzyskać więcej informacji, odwołaj się do *„CD Ratunkowy BitDefender”* (p. 186).
      - Otwórz okno Internet Explorer, przejdź do www.bitdefender.com i uruchom skanowanie online (kliknij przycisk **skanuj online**).

3. Spróbuj ponownie zainstalować BitDefender.Zaleca się pobranie i uruchomienie ostatniej wersji pliku instalacyjnego z www.bitdefender.com.

4. Jeśli nie uda się zainstalować programu ponownie, skontaktuj się z pomocą BitDefender, tak jak to opisano w *„Otrzymywanie pomocy”* (p. 194).

33.2. Mój system wydaje się działać zbyt 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 zapewniające ochronę programy znalezione w czasie instalacji, przed rozpoczęciem instalacji BitDefender zaleca się usunięcie wszelkich programów chroniących przed złośliwym oprogramowaniem.Aby uzyskać więcej informacji, odwołaj się do *„Jak usunąć inne rozwiązania bezpieczeństwa?”* (p. 201).

- **Minimalne wymagania sprzętowe do uruchomienia BitDefender nie są spełnione.**

  Jeśli komputer nie spełnia minimalnych wymagań sprzętowych, będzie działał wolniej, zwłaszcza gdy jednocześnie uruchomiono kilka aplikacji.Aby uzyskać więcej informacji, odwołaj się do *„Minimalne Wymagania Sprzętowe”* (p. 2).

- **Dyski twarde są zbyt mocno pofragmentowane.**

  Fragmentacja plików spowalnia dostęp do plików oraz zmniejsza wydajność systemu.

  Aby zdefragmentować dysk za pomocą systemu operacyjnego Windows, kieruj się ścieżką z menu start systemu Windows: **Start → Wszystkie programy → Akcesoria → Narzędzia systemowe → Defragmentator dysków**.

33.3. Skanowanie nie uruchamia się

Ten rodzaj problemu może mieć dwie główne przyczyny:

- **Wcześniejsza instalacja BitDefender, która nie została całkowicie usunięta lub nieprawidłowa instalacja BitDefender**.

  Jeśli jest to ten przypadek, najłatwiejszym rozwiązaniem jest całkowite usunięcie BitDefender z systemu, a następnie ponowne zainstalowanie go.Aby uzyskać więcej informacji, odwołaj się do *„Jak całkowicie usunąć BitDefender?”* (p. 203).

- **BitDefender nie jest jedynym rozwiązaniem bezpieczeństwa zainstalowanym w systemie**.

  W tym wypadku wykonaj następujące kroki:

  1. Usuń inne rozwiązanie bezpieczeństwa.Aby uzyskać więcej informacji, odwołaj się do *„Jak usunąć inne rozwiązania bezpieczeństwa?”* (p. 201).
  2. Całkowicie usuń BitDefender z systemu.
  3. Ponownie zainstaluj BitDefender w systemie.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.4. Nie mogę korzystać z aplikacji

Problem ten zachodzi, gdy próbujesz użyć programu, który działał normalnie przed zainstalowaniem BitDefender.

Możesz zetknąć się z jedną z następujących 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 ochrony wirusowej błędnie określa określone aplikacje jako złośliwe.

Aktywna ochrona wirusowa to moduł BitDefender, który nieustannie monitoruje aplikacje działające w systemie i raportuje te, których zachowanie wskazuje, iż jest to oprogramowanie złośliwe.Ponieważ funkcja ta bazuje na systemie heurystycznym, mogą występować przypadki, gdy dozwolone aplikacje są raportowane przez moduł Aktywnej ochrony wirusowej.

Gdy dojdzie do takiej sytuacji, można wyłączyć monitorowanie danej aplikacji przez moduł Aktywnej ochrony wirusowej.

Aby dodać program do listy wyjątków, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus > Tarcza**.
3. Kliknij **Zaawansowane**.
4. W nowym oknie przejdź do zakładki **Wyjątki** i kliknij przycisk **Dodaj** i przejdź do miejsca, w którym znajduje się plik .exe programu (zazwyczaj będzie on w `C:\Program Files`).
5. Kliknij **OK** aby zapisać zmiany i zamknąć okno.
6. Zamknij okno BitDefender i sprawdź, czy problem nadal występuje.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.5. Nie mogę połączyć się z Internetem

Po zainstalowaniu BitDefender program może przestać łączyć się z Internetem lub usługami sieciowymi.

W identyfikowaniu i rozwiązywaniu problemów z połączeniem pomoże ci Kreator rozwiązywania problemów.Aby uruchomić kreatora, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany

Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Zaporę Sieciową**.W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Widok eksperta

Przejdź do **Zapora Sieciowa > Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Wykonaj następującą, trzypunktową procedurę, aby rozpocząć rozwiązywanie problemów.Możliwość poruszania się w kreatorze zapewnia przycisk **Dalej**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Witamy**

   Wybierz **Próbuję połączyć się z Internetem, ale operacja się nie udaje**.

2. **Zidentyfikuj problem**

   Kliknij **Wybierz aplikację** i **Przeglądaj**, aby znaleźć plik .exe danego programu (zwykle znajduje się w `C:\Program Files`, np. Firefox.exe).Kliknij **Dodaj**.

3. **Zalecane rozwiązanie**

   Wybierz **Tak, zezwól na dostęp**.Kliknij **Zakończ** i sprawdź, czy problem nadal występuje.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.6. Nie mogę używać drukarki

W zależności od sieci, do której jesteś podłączony, zapora sieciowa BitDefender może blokować łączność między twoim komputerem, a drukarką sieciową.

W tym wypadku najlepszym rozwiązaniem jest skonfigurowanie BitDefender, tak aby automatycznie zezwalał na połączenia do i z odpowiedniej drukarki.

W identyfikowaniu i rozwiązywaniu problemów z połączeniem pomoże ci Kreator rozwiązywania problemów.Aby uruchomić kreatora, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany

Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Zaporę Sieciową**.W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Widok eksperta

Przejdź do **Zapora Sieciowa > Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Wykonaj następującą, trzypunktową procedurę, aby rozpocząć rozwiązywanie problemów.Możliwość poruszania się w kreatorze zapewnia przycisk **Dalej**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Witamy**

   Wybierz **Próbuję drukować, ale operacja nie udaje się**.

2. **Zidentyfikuj problem**

   Kliknij **Wybierz drukarkę**.Wybierz drukarkę z listy według nazwy lub adresu IP.Jeśli nie możesz znaleźć urządzenia na liście, podaj adres IP ręcznie w polu edycji.Kliknij **Dodaj**.

3. **Zalecane rozwiązanie**

   Wybierz **Tak, zezwól na dostęp**.Kliknij **Zakończ** i sprawdź, czy problem nadal występuje.

Jeśli Kreator rozwiązywania problemów wskazuje, że problem nie jest wywołany przez zaporę sieciową BitDefender, sprawdź inne potencjalne przyczyny, takie jak:

- Udostępnianie plików i drukarki twojemu komputerowi może być blokowane przez zaporę sieciową drugiego komputera.
  - Jeśli komputer korzysta z zapory sieciowej Windows, można ją skonfigurować tak, aby zezwolić na dzielenie plików i drukarek: otworzyć okno ustawień zapory Windows, wybrać zakładkę **Wyjątki** i zaznaczyć pole **Udostępnianie Plików i Drukarek**.
  - Jeśli komputer posiada inną zaporę sieciową, odwołaj się do jej dokumentacji lub pliku pomocy.
- Główne warunki, które mogą przeszkodzić w używaniu lub podłączaniu się udostępnionej drukarki:
  - Aby korzystać z dzielenia się drukarkami w sieci, może być wymagane zalogowanie się na konto użytkownika Windows.
  - Aby udzielić dostępu dla konkretnego komputera i użytkownika, dla każdej dzielonej drukarki ustawiane są zezwolenia.Jeśli już współdzielisz drukarkę, sprawdź jak ustawione są zezwolenia aby dowiedzieć się czy użytkownik na innym komputerze posiada do niej dostęp.Jeśli próbujesz podłączyć się do udostępnionej drukarki, sprawdź czy użytkownik na drugim komputerze udzielił zgody na korzystanie z drukarki.
  - Drukarka podłączona do twojego lub innego komputera nie jest udostępniona.
  - Udostępniona drukarka nie została dodana do komputera.

Notatka

Aby nauczyć się zarządzać udostępnianiem drukarek w sieci (dzielenie się drukarką, dodawanie lub usuwanie praw dostępu dla drukarki, łączenie się z drukarką sieciową), przejdź do Centrum Pomocy i Wsparcia Windows, (w menu Start, kliknij **Pomoc**).

- Dostęp do drukarki sieciowej może być ograniczony tylko do określonych komputerów i użytkowników. Powinieneś zapytać administratora sieci, czy masz uprawnienia do połączenia się z tą drukarką.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.7. Nie mogę udostępniać plików innemu komputerowi

W zależności od sieci, do której jesteś podłączony, zapora sieciowa BitDefender może blokować łączność między twoim systemem a innym komputerem.W rezultacie udostępnianie plików innym komputerom może stać się niemożliwe.W tym wypadku najlepszym rozwiązaniem jest skonfigurowanie BitDefender, tak aby automatycznie zezwalał na połączenia do i z odpowiedniego systemu.

W identyfikowaniu i rozwiązywaniu problemów z połączeniem pomoże ci Kreator rozwiązywania problemów.Aby uruchomić kreatora, otwórz BitDefender i, w zależności od wybranego trybu wyświetlania interfejsu użytkownika, postępuj zgodnie z poleceniami:

Widok średniozaawansowany

Przejdź do zakładki **Bezpieczeństwo** i w obszarze Szybkie zadania, znajdującym się po lewej stronie okna, kliknij **Konfiguruj Zaporę Sieciową**.W nowym oknie, które pojawi się na ekranie, wybierz zakładkę **Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Widok eksperta

Przejdź do **Zapora Sieciowa > Ustawienia** i kliknij **Rozwiązywanie Problemów**.

Wykonaj następującą, trzypunktową procedurę, aby rozpocząć rozwiązywanie problemów.Możliwość poruszania się w kreatorze zapewnia przycisk **Dalej**.Aby zakończyć pracę kreatora, kliknij **Anuluj**.

1. **Witamy**

   Wybierz **Nie mogę uzyskać dostępu do komputera w mojej sieci**.

2. **Zidentyfikuj problem**

   Kliknij **Wybierz komputer**.Wybierz komputer z listy według nazwy lub adresu IP.Jeśli nie możesz znaleźć komputera na liście, podaj adres IP ręcznie w polu edycji.Kliknij **Dodaj**.

3. **Zalecane rozwiązanie**

   Wybierz **Tak, zezwól na dostęp**.Kliknij **Zakończ** i sprawdź, czy problem nadal występuje.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.8. Mój Internet działa powoli

Sytuacja ta może zaistnieć po zainstalowaniu BitDefender.Problem ten może być wywoływany przez błędy w konfiguracji zapory sieciowej BitDefender.

Aby rozwiązać problem, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Zapora Sieciowa > Ustawienia**.
3. Odznacz pole wyboru **Zapora Sieciowa jest włączona**, aby czasowo wyłączyć zaporę.
4. Sprawdź, czy możesz połączyć się z Internetem, mając wyłączoną zaporę sieciową BitDefender.
   - Jeśli nadal nie możesz połączyć się z Internetem, problem prawdopodobnie nie jest wywołany przez BitDefender. Powinieneś skontaktować się ze swoim dostawcą usług internetowych, aby sprawdzić, czy połączenie działa po jego stronie.

     Jeśli otrzymasz potwierdzenie od swojego dostawcy usług internetowych, że połączenie jest sprawne po jego stronie, a problem mimo to nadal występuje, skontaktuj się z BitDefender w sposób opisany w *„Otrzymywanie pomocy”* (p. 194).
   - Jeśli uda ci się połączyć z Internetem po wyłączeniu zapory sieciowej BitDefender, wykonaj następujące kroki:
     a. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
     b. Przejdź do **Zapora Sieciowa > Ustawienia** i zaznacz to pole wyboru, aby włączyć Zaporę Sieciową.
     c. Kliknij **Ustawienia zaawansowane**, wybierz **Uaktywnij współdzielenie połączenia internetowego** i usuń zaznaczenie **Zablokuj skanowanie portów**.
     d. W oknie głównym przejdź do zakładki **Sieć** .
     e. Wysuń rozwijane menu z kolumny **Typ sieci** i wybierz **Dom/ Biuro**.

f. Przejdź do kolumny **Typowe** i ustaw ją na **Tak**. Ustaw **Tryb Niewidzialności** na **Zdalny**.

g. Sprawdź, czy możesz połączyć się z Internetem.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.9. Jak aktualizować BitDefender przy wolnym połączeniu internetowym?

Jeśli masz wolne połączenie z Internetem (takie jak połączenie telefoniczne), w trakcie procesu aktualizacji mogą występować błędy.

Aby dokonać aktualizacji systemu o najnowsze sygnatury złośliwego oprogramowania BitDefender, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Aktualizacja > Ustawienia**.
3. W **Ustawieniach ręcznej aktualizacji** wybierz opcję **Pytaj przed pobraniem aktualizacji**.
4. Kliknij **Zastosuj** i przejdź do zakładki **Aktualizuj**.
5. Kliknij **Aktualizuj teraz**, a zobaczysz nowe okno.
6. Wybierz tylko **Aktualizacje sygnatur**, a następnie kliknij **Ok**.
7. BitDefender pobierze i zainstaluje jedynie aktualizacje sygnatur złośliwego oprogramowania.

33.10. Komputer nie jest podłączony do Internetu. Jak zaktualizować BitDefender?

Jeśli komputer nie ma połączenia z Internetem, aktualizacje należy pobrać ręcznie na komputer, który ma dostęp do Internetu i przenieść je na swój komputer za pomocą urządzenia wymiennego, takiego jak dysk flash.

Podążaj tymi krokami:

1. W komputerze mającym dostęp do Internetu otwórz przeglądarkę internetową i przejdź do:

   www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. W kolumnie **Aktualizacja ręczna** kliknij łącze wskazujące twój produkt i architekturę systemu.Jeśli nie wiesz, czy twój system Windows to wersja 32-, czy 64-bitowa, zapoznaj się z informacjami w *„Czy używam 32-, czy 64-bitowej wersji systemu Windows?”* (p. 202).

3. Zapisz w systemie plik o nazwie `weekly.exe`.
4. Przenieś pobrany plik na urządzenie wymienne, takie jak dysk flash, a następnie na swój komputer.
5. Dwukrotnie kliknij plik i postępuj zgodnie z poleceniami kreatora.

33.11. Usługi BitDefender Nie Odpowiadają

Ten artykuł pozwala na rozwiązanie problemów z *nieodpowiadającymi usługami BitDefender*.Możesz napotkać na ten błąd w następujący sposób:

- Ikona BitDefender w zasobniku systemowym jest szara, pojawia się informacja o nie odpowiadających usługach BitDefender.
- Okno BitDefender wskazuje na nieodpowiadające usługi BitDefender.

Ten błąd może pojawić się w następujących okolicznościach:

- ważna aktualizacja jest właśnie instalowana.
- tymczasowe błędy w komunikacji pomiędzy usługami BitDefender.
- niektóre z usług BitDefender są zatrzymane.
- oprócz BitDefendera, inne oprogramowanie zabezpieczające jest uruchomione na twoim komputerze.
- wirusy na tym komputerze uniemożliwiają normalną pracę 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 komputer ponownie i odczekaj kilka chwil, aż BitDefender załaduje się. Następnie otwórz program i sprawdź, czy błąd dalej występuje.Uruchomienie komputera ponownie zazwyczaj rozwiązuje ten problem.
3. Sprawdź czy posiadasz zainstalowane inne oprogramowanie zabezpieczające, które może zakłócić normalną pracę BitDefender. Jeśli tak, zalecamy usunięcie wszystkich programów tego typu przed rozpoczęciem instalacji.
4. Jeśli błąd będzie się powtarzał, może istnieć poważny problem (na przykład, możesz zostać zainfekowany wirusem który uniemożliwia poprawną pracę BitDefendera).Proszę skontaktować się ze wsparciem BitDefender tak jak to przedstawiono w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.12. Filt Antyspamu Nie Działa Poprawnie

Ten artykuł pomaga rozwiązać następujące problemy, które mogą się pojawić w przypadku korzystania z filtra antyspamowego BitDefender:

- Liczba prawidłowych wiadomości e-mail oznaczonych jako `[spam]`.

- Wiele wiadomości zawierających spam nie zostało poprawnie oznaczonych przez filtr antyspamowy.
- Filtr antyspamowy nie wykrywa żadnych wiadomości spam.

33.12.1. Prawidłowa Poczta jest Oznaczona jako [spam]

Prawidłowe wiadomości są oznaczane jako `[spam]` ponieważ wyglądają jak spam dla filtra antyspamowego BitDefender.Możesz rozwiązać te problemy przez właściwą konfigurację filtra Antyspam.

BitDefender automatycznie dodaje odbiorców twoich wiadomości e-mail do listy Przyjaciół.Wiadomości e-mail odebrane od kontaktów z listy Przyjaciół są traktowane jako prawidłowe. Nie są weryfikowane przez filtr antyspamowy i w związku z tym, nie są nigdy oznaczane jako `[spam]`.

Automatyczna konfiguracja listy Przyjaciół nie zapobiega błędom wykrycia i może się zdarzyć w następujących sytuacjach:

- Z powodu zapisania się do wielu różnych stron, otrzymano wiele komercyjnych wiadomości e-mail.W tym przypadku, rozwiązaniem jest dodanie adresów e-mail od których otrzymujesz te wiadomości do listy Przyjaciół.
- Duża część prawidłowej poczty pochodzi od ludzi z którymi nigdy nie kontaktowano się drogą e-mailową, np. klientami, potencjalnymi partnerami biznesowymi itd.W tym przypadku wymagane są inne rozwiązania.

Jeśli używasz jednego z klientów poczty, z którymi BitDefender jest zintegrowany, spróbuj jednego z poniższych rozwiązań:

1. Wskaż Błędy Wykrycia. Używane do trenowania uczącego się filtra antyspamu (Bayesian) co pomaga przeciwdziałać błędną klasyfikacją wiadomości w przyszłości.Uczący się filtr analizuje wskazywane wiadomości i uczy się ich wzorów.Następne wiadomości e-mail pasujące do tego samego wzoru będą oznaczane jako `[spam]`.
2. Obniż poziom ochrony antyspamu. Przez zmniejszenie poziomu ochrony, filtr antyspamowy będzie potrzebował więcej wskazań przez użytkownika, aby klasyfikować wiadomości e-mail jako spam.Spróbuj tego rozwiązania tylko jeśli wiele prawidłowych wiadomości (włączając w to komercyjną pocztę) zostało nieprawidłowo sklasyfikowane jako spam.
3. Ponowne trenowanie uczącego się filtra (Bayesian). Spróbuj tego rozwiązania tylko jeśli poprzednie nie dały oczekiwanych rezultatów.

Notatka

BitDefender jest zintegrowany z najbardziej popularnymi klientami poczty dzięki wykorzystaniu łatwego w użyciu paska narzędziowego antyspam.W celu uzyskania kompletnej listy obsługiwanych klientów poczty e-mail, odwołaj się do *„Wymagania Systemowe”* (p. 2).

Jeśli używasz innego klienta poczty, nie możesz wskazywać na błędy rozpoznania i trenować uczącego się filtra. Aby rozwiązać ten problem, spróbuj obniżyć poziom zabezpieczeń antyspamu.

Dodaj Kontakty do Listy przyjaciół

Jeśli używasz obsługiwanego klienta poczty, możesz łatwo dodawać prawidłowych nadawców do listy Przyjaciół.Podążaj tymi krokami:

1. W programie klienta poczty, zaznacz wiadomość e-mail od nadawcy którego chcesz dodać do listy Przyjaciół.
2. Kliknij na przycisk **Dodaj Przyjaciela** na pasku narzędziowym antyspamu.
3. Możesz zostać zapytany(a) aby potwierdzić adresy dodane do listy Przyjaciół.Wybierz **Nie pokazuj tego komunikatu ponownie** i kliknij **OK**.

Będziesz zawsze otrzymywał wiadomości email z tego adresu bez względu na zawartość wiadomości.

Jeśli używasz innego klienta poczty, możesz dodać kontakty do listy Przyjaciół, korzystając z interfejsu BitDefender.Podążaj tymi krokami:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Kliknij **Antyspam** w menu po lewej stronie.
3. Kliknij na zakładkę **Stan**.
4. Kliknij na **Zarządzaj Przyjaciółmi**.Pojawi się okno konfiguracji.
5. Wprowadź adres e-mail od którego chcesz zawsze otrzymywać wiadomości e-mail i kliknij przycisk aby dodać adres do listy Przyjaciół.
6. Kliknij **OK** aby zapisać zmiany i zamknąć okno.

Wskaż Błędy Wykrycia

Jeśli używasz obsługiwanych klientów poczty, możesz łatwo poprawić filtr antyspam (przez wskazanie które wiadomości e-mail nie powinny być oznaczane jako `[spam]`). Dzięki temu znacząco poprawisz skuteczność filtra antyspam.Podążaj tymi krokami:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu śmieci, gdzie zostały przeniesione wiadomości spam.
3. Wybierz dozwoloną wiadomość nieprawidłowo oznaczoną przez BitDefender jako `[spam]`.
4. Kliknij przycisk **Dodaj Przyjaciela** znajdujący się na pasku narzędziowym antyspamu aby dodać nadawcę do listy Przyjaciół.Możesz zostać zapytany(a) o potwierdzenie, klikając na **OK**.Będziesz zawsze otrzymywał wiadomości email z tego adresu bez względu na zawartość wiadomości.

5. Kliknij przycisk **To nie jest Spam** znajdujący się w pasku antyspamu BitDefender (zazwyczaj znajduje się on w górnej części okna klienta poczty). Filtr uczący potraktuje tą wiadomość jako prawidłową. Wszystkie następne wiadomości tego typu będą przenoszone do folderu Skrzynki Odbiorczej.Następne wiadomości e-mail pasujące do tego samego wzoru nie będą oznaczane jako `[spam]`.

Zmniejsz Poziom Ochrony Antyspamu

Aby zmniejszyć poziom ochrony antyspamu, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Kliknij **Antyspam** w menu po lewej stronie.
3. Kliknij na zakładkę **Stan**.
4. Przesuń suwak niżej na skali.

Zaleca się aby obniżyć poziom zabezpieczeń o jeden i poczekać na wyniki.Jeśli dużo poprawnej poczty dalej jest klasyfikowane jako `[spam]`, możesz ponownie obniżyć poziom ochrony. Jeśli zauważysz, że duża część wiadomości zawierających spam nie jest wykrywana, nie powinieneś tego robić.

Wytrenuj Ponownie Uczący się Filtr (Bayesian)

Zanim przystąpisz do trenowania uczącego się filtra (Bayesian), przygotuj dwa foldery - jeden zawierający wyłącznie spam i drugi, zawierający wyłącznie poprawne wiadomości.Uczący się filtr analizuje je i uczy się z określonych charakterystyk opisujących spam i poprawne wiadomości które otrzymujesz. Aby trenowanie filtra zwiększyło jego skuteczność, potrzeba przynajmniej 50 wiadomości w każdym z folderów.

Aby wyczyścić bazę danych Bayesian i wytrenować uczący się filtr od nowa, wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Na pasku narzędziowym antyspamu, kliknij przycisk **Kreator** aby uruchomić kreator konfiguracji antyspamu.
3. Kliknij **Dalej**.
4. Wybierz **Pomiń ten krok** i kliknij **Dalej**.
5. Wybierz **Wyczyść bazę danych filtra antyspamowego** i kliknij **Dalej**.
6. Wybierz folder zawierający prawidłowe wiadomości i kliknij **Dalej**.
7. Wybierz folder zawierający wiadomości SPAM i kliknij **Dalej**.
8. Kliknij **Zakończ** aby rozpocząć proces trenowania.
9. Kiedy trenowanie się zakończy, kliknij na **Zamknij**.

Zapytaj o Pomoc

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.12.2. Wiele wiadomości Spam nie zostało wykrytych

Jeśli odbierasz dużo wiadomości spam, które nie są oznaczone jako [spam], musisz skonfigurować filtr antyspamu BitDefender tak, aby zwiększyć jego wydajność.

Jeśli używasz jednego z klientów, z którymi BitDefender jest zintegrowany, spróbuj jednego z poniższych rozwiązań:

1. Informuj o niewykrytych wiadomościach spam. Jest używany do trenowania Uczącego się Silnika (Bajezjańskiego) dla filtra antyspamowego i zazwyczaj poprawia jego wykrywalność.Uczący się filtr analizuje wskazywane wiadomości i uczy się ich wzorów.Następne wiadomości e-mail pasujące do tego samego wzoru będą oznaczane jako [spam].
2. Dodaj spamerów do listy Spamerów. Wiadomości e-mail pochodzące od adresów zawartych w liście Spamerów są automatycznie oznaczane jako [spam].
3. Zwiększ poziom ochrony antyspamu. Przez zwiększenie poziomu ochrony, filtr antyspamowy będzie potrzebował mniej wskazań przez użytkownika, aby klasyfikować wiadomości e-mail jako spam.
4. Ponowne trenowanie uczącego się filtra (Bayesian). Skorzystaj z tego rozwiązania jeśli poziom wykrywalności antyspamu nie jest satysfakcjonujący i wskazywanie na niewykryte wiadomości e-mail nie pomaga.

Notatka

BitDefender jest zintegrowany z najbardziej popularnymi klientami poczty dzięki wykorzystaniu łatwego w użyciu paska narzędziowego antyspam.W celu uzyskania kompletnej listy obsługiwanych klientów poczty e-mail, odwołaj się do *„Wymagania Systemowe”* (p. 2).

Jeśli używasz innego klienta poczty, nie możesz wskazywać na błędy rozpoznania i trenować uczącego się filtra. Aby rozwiązać ten problem, spróbuj zwiększyć poziom zabezpieczeń antyspamu i dodać spamerów do listy Spamerów.

Wskaż Niewykryte Wiadomości Spam

Jeśli używasz obsługiwanego klienta poczty, możesz łatwo wskazać, które z wiadomości mają być traktowane jako spam. Dzięki temu w dużym stopniu zwiększysz skuteczność filtra antyspamowego.Podążaj tymi krokami:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu Skrzynki Odbiorczej.

3. Wybierz niewykryte wiadomości spam.
4. Kliknij przycisk **To jest Spam** znajdujący się w pasku antyspamu BitDefender (zazwyczaj znajduje się on w górnej części okna klienta poczty). Filtr uczący potraktuje tą wiadomość jako spam. Wszystkie następne wiadomości tego typu będą oznaczane jako [spam] i będą trafiać do folderu na śmieci.Następne wiadomości e-mail pasujące do tego samego wzoru będą oznaczane jako [spam].

Dodaj Spamerów do listy Spamerów

Jeśli używasz obsługiwanego klienta poczty, możesz łatwo dodawać nadawców wiadomości zawierających spam do listy Spamerów.Podążaj tymi krokami:

1. Otwórz swojego klienta pocztowego.
2. Przejdź do folderu śmieci, gdzie zostały przeniesione wiadomości spam.
3. Wybierz wiadomości oznaczone przez BitDefender jako [spam].
4. Kliknij przycisk **Dodaj Spamera** na pasku narzędziowym BitDefender Antyspam.
5. Możesz zostać zapytany(a) aby potwierdzić adresy dodane do listy Spamerów.Wybierz **Nie pokazuj tego komunikatu ponownie** i kliknij **OK**.

Jeśli korzystasz z innego klienta poczty, możesz dodać spamerów do listy Spamerów ręcznie, korzystając z interfejsu BitDefender. Najlepiej zrobić to tylko jeśli już otrzymano kilka wiadomości spam od tego adresu.Podążaj tymi krokami:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Kliknij **Antyspam** w menu po lewej stronie.
3. Kliknij na zakładkę **Stan**.
4. Kliknij na **Zarządzaj Spamerami**.Pojawi się okno konfiguracji.
5. Wprowadź adres nadawcy wiadomości spam i kliknij przycisk aby dodać go do listy Spamerów.
6. Kliknij **OK** aby zapisać zmiany i zamknąć okno.

Zwiększ Poziom Ochrony Antyspamu

Aby zwiększyć poziom ochrony antyspamu, wykonaj następujące kroki:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Kliknij **Antyspam** w menu po lewej stronie.
3. Kliknij na zakładkę **Stan**.
4. Przesuń suwak wyżej na skali.

Wytrenuj Ponownie Uczący się Filtr (Bayesian)

Zanim przystąpisz do trenowania uczącego się filtra (Bayesian), przygotuj dwa foldery - jeden zawierający wyłącznie spam i drugi, zawierający wyłącznie poprawne wiadomości.Uczący się filtr analizuje je i uczy się z określonych charakterystyk opisujących spam i poprawne wiadomości które otrzymujesz. Aby trenowanie filtra zwiększyło jego skuteczność, potrzeba przynajmniej 50 wiadomości w każdym z folderów.

Aby wyczyścić bazę danych Bayesian i wytrenować uczący się filtr od nowa, wykonaj następujące kroki:

1. Otwórz swojego klienta pocztowego.
2. Na pasku narzędziowym antyspamu, kliknij przycisk **Kreator** aby uruchomić kreator konfiguracji antyspamu.
3. Kliknij **Dalej**.
4. Wybierz **Pomiń ten krok** i kliknij **Dalej**.
5. Wybierz **Wyczyść bazę danych filtra antyspamowego** i kliknij **Dalej**.
6. Wybierz folder zawierający prawidłowe wiadomości i kliknij **Dalej**.
7. Wybierz folder zawierający wiadomości SPAM i kliknij **Dalej**.
8. Kliknij **Zakończ** aby rozpocząć proces trenowania.
9. Kiedy trenowanie się zakończy, kliknij na **Zamknij**.

Zapytaj o Pomoc

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

33.12.3. Filtr Antyspamu Nie Wykrywa Żadnego Spamu

Jeśli żadna wiadomość nie jest oznaczana jako `[spam]`, problem może dotyczyć filtra BitDefender Antyspam.Przed próbą rozwiązania tego problemu, sprawdź czy nie jest spowodowany przez jeden z poniższych warunków:

- Ochrona BitDefender Antyspam jest dostępna tylko dla klientów poczty e-mail skonfigurowanych na odbieranie wiadomości przez protokół POP3.To oznacza poniższe:
  - Wiadomości e-mail odbierane przez usługi oparte na stronach WWW (takie jak Interia, Gmail, Wp.pl i inne) nie będą przez BitDefender filtrowane ze spamu.
  - Jeśli twój klient e-mail jest skonfigurowany aby odbierać wiadomości poprzez inne protokoły niż POP3 (takie jak np. IMAP4), BitDefender nie będzie filtrował spamu.

Notatka

POP3 jest najbardziej popularnym protokołem używanym do pobierania wiadomości e-mail z serwera poczty.Jeśli nie znasz protokołu, z którego korzysta twój klient poczty, spytaj osoby która go konfigurowała.

- BitDefender Internet Security 2011 nie skanuje ruchu POP3 programu Lotus Notes.

Powinno się także zweryfikować poniższe możliwe przyczyny:

1. Sprawdź czy Antyspam jest włączony.
   a. Otwórz BitDefender.
   b. W prawym górnym rogu okna kliknij **Opcje** i wybierz **Preferencje**.
   c. W kategorii Ustawień Zabezpieczeń, sprawdź stan antyspamu.

   Jeśli Antyspam jest zablokowany, może to być przyczyną problemu.Włącz Antyspam i sprawdź czy problem został naprawiony.
2. Jest to mało prawdopodobne, ale być może przez przypadek sam zaznaczyłeś/aś te wiadomości aby były oznaczane jako `[spam]`.
   a. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
   b. Kliknij **Antyspam** w menu po lewej i zakładkę **Ustawienia**.
   c. Sprawdź czy opcja **Oznacz wiadomości spam w temacie** jest zaznaczona.

Możliwym rozwiązaniem jest naprawa lub ponowna instalacja produktu. Można jednak również skontaktować się z BitDefender, korzystając z metody przedstawionej w *„Otrzymywanie pomocy”* (p. 194), aby uzyskać pomoc techniczną.

33.13. Nie Można Usunąć BitDefendera

Ten artykuł pomaga rozwiązać problemy związane z usuwaniem BitDefendera.Istnieją dwie możliwe sytuacje:

- Podczas usuwania pojawia się ekran z błędem.Ekran zawiera przycisk z odnośnikiem do narzędzia odinstalowującego, które oczyszcza system z instalacji.
- Podczas odinstalowywania program przestaje reagować i co możliwe, zawiesza się także cały system.Kliknij **Anuluj** aby przerwać proces usuwania programu. Jeśli to nie zadziała, uruchom ponownie komputer.

Jeśli instalacja zakończy się niepowodzeniem, niektóre wpisy oraz pliki mogą pozostać w systemie. Takie pozostałości mogą blokować następną instalację BitDefender. Mogą także wpłynąć na stabilność i wydajność systemu.Aby kompletnie usunąć BitDefender z twojego systemu, musisz uruchomić narzędzie odinstalowujące.

Aby uzyskać więcej informacji, odwołaj się do *„Jak całkowicie usunąć BitDefender?”* (p. 203).

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

34. Usuwanie Złośliwego Oprogramowania z Systemu

Złośliwe oprogramowanie może wpływać na system na wiele różnych sposobów, a rodzaj pracy BitDefender zależy od typu ataku tego oprogramowania.Ponieważ wirusy często zmieniają swoje zachowanie, ustalenie wzorca ich zachowania i działania jest bardzo trudne.

Istnieją sytuacje, gdy BitDefender nie może automatycznie usunąć z systemu infekcji złośliwego oprogramowania.W takich wypadkach wymagana jest interwencja użytkownika.

Jeśli nie możesz w tym miejscu znaleźć pomocy dla swojego problemu lub przedstawione rozwiązania nie pomagają, możesz skontaktować się z przedstawicielem pomocy technicznej BitDefender, korzystając z metody przedstawionej w rozdziale *„Otrzymywanie pomocy”* (p. 194).

34.1. CD Ratunkowy BitDefender

Dysk Rescue CD BitDefender to funkcja udostępniona w większości instalacyjnych płyt CD BitDefender. Pozwala ona skanować i dezynfekować istniejące dyski twarde przed uruchomieniem systemu operacyjnego.Może ci również pomóc w zapisaniu danych z uszkodzonego komputera na urządzeniu wymiennym.

Jeśli nie posiadasz dysku Rescue CD BitDefender, możesz pobrać go z tego miejsca w postaci obrazu ISO:

http://download.bitdefender.com/rescue_cd/

Pobierz plik .iso i wypal go na płycie CD lub DVD za pomocą wybranego narzędzia.

Skanowanie Systemu za Pomocą Dysku Rescue CD BitDefender

Aby przeskanować system za pomocą dysku Rescue CD BitDefender, wykonaj następujące kroki:

1. Skonfiguruj BIOS, aby uruchomienie komputera następowało z płyty CD.
2. Włóż do napędu płytę CD i ponownie uruchom komputer.
3. Poczekaj aż pojawi się ekran BitDefender i w preferowanych językach wybierz opcję **Uruchom dysk Rescue CD BitDefender**.
4. Poczekaj aż proces uruchamiania zakończy się. Może to chwilę potrwać.
5. Gdy tylko zakończy się proces uruchamiania komputera, sygnatury BitDefender są aktualizowane i rozpoczęte zostaje skanowanie wszystkich wykrytych partycji dysków twardych.

Zapisywanie Danych za Pomocą Dysku Rescue CD BitDefender

Załóżmy, że nie możesz włączyć swojego komputera w Windows z nieznanych powodów. Jednocześnie musisz skorzystać z ważnych danych znajdujących się na twoim komputerze. Tutaj przydaje się Dysk Ratunkowy BitDefendera.

Aby zapisać dane z komputera na urządzeniu wymiennym, takim jak dysk flash USB, wykonaj następujące kroki:

1. Skonfiguruj BIOS, aby uruchomienie komputera następowało z płyty CD.
2. Włóż do napędu płytę CD i ponownie uruchom komputer.
3. Poczekaj aż pojawi się ekran BitDefender i w preferowanych językach wybierz opcję **Uruchom dysk Rescue CD BitDefender**.
4. Poczekaj aż proces uruchamiania zakończy się. Może to chwilę potrwać.
5. Gdy tylko zakończy się proces uruchamiania komputera, sygnatury BitDefender są aktualizowane i rozpoczęte zostaje skanowanie wszystkich wykrytych partycji dysków twardych.

   Partycje dysków twardych zostaną wyświetlone na pulpicie. Dwukrotnie kliknij dysk, aby przejrzeć jego zawartość w oknie podobnym do okna programu Windows Explorer.

   Notatka

   Pracując z dyskiem Rescue CD BitDefender, będziesz miał do czynienia z nazwami partycji stosowanymi w systemie Linux. Dyski, które nie zostały opatrzone nazwą w systemie Windows, będą widoczne jako `[LocalDisk-0]` odpowiadający prawdopodobnie partycji `(C:)` stosowanej w systemie Windows, `[LocalDisk-1]` odpowiadający partycji `(D:)` i tak dalej.

6. Podłącz urządzenie wymienne do portu USB komputera.Za chwilę pojawi się okno pokazujące zawartość urządzenia.
7. Możesz kopiować pliki i foldery, tak jak normalnie czynisz to w środowisku Windows.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

34.2. Co robić, gdy BitDefender znajdzie wirusy w komputerze?

O obecności wirusa na komputerze można dowiedzieć się w następujący sposób:

- Przeskanowałeś komputer i BitDefender znalazł w nim zainfekowane elementy.
- Alert wirusa informuje o zablokowaniu przez BitDefender jednego lub więcej wirusów w komputerze.

W takich sytuacjach zaktualizuj BitDefender, aby mieć pewność, że posiadasz najnowsze sygnatury złośliwego oprogramowania i uruchom Głębokie Skanowanie, aby dokonać analizy systemu.

Zaraz po zakończeniu głębokiego skanowania wybierz działanie względem zainfekowanych elementów (Dezynfekuj, 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(i) ręcznie:

Pierwszą metodę można użyć w trybie zwykłym:

1. Wyłącz ochronę antywirusową w czasie rzeczywistym BitDefender.Informacje, jak należy to zrobić, znajdują się w *„Jak włączyć / wyłączyć ochronę w czasie rzeczywistym?”* (p. 203).
2. Wyświetl ukryte obiekty w systemie Windows.Informacje, jak należy to zrobić, znajdują się w *„Jak wyświetlić ukryte obiekty w systemie Windows?”* (p. 204).
3. Przejdź do miejsca, w którym znajduje się zainfekowany plik (sprawdź dziennik skanowania) i usuń go.
4. Włącz ochronę antywirusową w czasie rzeczywistym BitDefender.

Jeśli pierwsza metoda usunięcia infekcji zawiedzie, wykonaj następujące kroki:

1. Uruchom ponownie system w Trybie awaryjnym.Informacje, jak należy to zrobić, znajdują się w *„Jak ponownie uruchomić komputer w Trybie awaryjnym?”* (p. 202).
2. Wyświetl ukryte obiekty w systemie Windows.
3. Przejdź do miejsca, w którym znajduje się zainfekowany plik (sprawdź dziennik skanowania) i usuń go.
4. Uruchom ponownie system w trybie zwykłym.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

34.3. Jak usunąć wirusa z archiwum?

Archiwum to plik lub zbiór plików skompresowany w specjalnym formacie, w celu ograniczenia ilości miejsca niezbędnego do jego zapisania na dysku.

Niektóre z tych formatów to formaty otwarte. BitDefender może dzięki temu skanować je od środka i podejmować odpowiednie działania, aby je usunąć.

Inne formaty archiwów są częściowo lub całkowicie zamknięte. BitDefender może wykryć w nich obecność wirusów, ale nie może podjąć jakichkolwiek działań.

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

Oto w jaki sposób można usunąć wirusa z archiwum:

1. Zidentyfikuj archiwum zawierające wirusa, wykonując Głębokie Skanowanie systemu.
2. Wyłącz ochronę antywirusową w czasie rzeczywistym 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 Głębokie skanowanie, aby upewnić się, że w systemie nie ma żadnych innych infekcji.

Notatka

Należy zwrócić uwagę, iż wirus zapisany w archiwum nie jest bezpośrednim zagrożeniem dla systemu, ponieważ aby mógł go zainfekować, musi być najpierw zdekompresowany i uruchomiony.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

34.4. Jak usunąć wirusa z archiwum e-mail?

BitDefender może również identyfikować wirusy w bazach danych e-mail oraz archiwach e-mail zapisanych na dysku.

Czasami trzeba zidentyfikować zainfekowaną wiadomość, korzystając z informacji podanych z raporcie ze skanowania i usunąć ją ręcznie.

Oto w jaki sposób można usunąć wirusa zapisanego w archiwum poczty:

1. Skanuj bazę danych e-mail przy użyciu BitDefender.
2. Wyłącz ochronę antywirusową w czasie rzeczywistym BitDefender.
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 programie Outlook Express:W menu Plik kliknij Folder, a następnie Kompaktuj wszystkie foldery.
   - In Microsoft Outlook:W menu Plik kliknij Zarządzanie Plikami Danych.Zaznacz pliki folderów osobistych (.pst), które chcesz kompaktować i kliknij Ustawienia.Kliknij Kompaktuj.
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 *„Otrzymywanie pomocy”* (p. 194).

34.5. Jak skanować komputer w Trybie awaryjnym?

Ręczne Skanowanie BitDefender pozwala na skanowanie specyficznych folderów lub partycji dysków twardych bez potrzeby tworzenia oddzielnego zadania skanowania.

Ta opcja została stworzona z myślą o sytuacji w której Windows pracuje w Trybie Awaryjnym.

Jeśli system jest zainfekowany wirusem, którego nie da się usunąć w normalnym trybie, można uruchomić Windows w Trybie awaryjnym i przeskanować każdą partycję dysku twardego, korzystając z Ręcznego Skanowania BitDefender.

Informacje o tym, w jaki sposób można uzyskać dostęp do Trybu awaryjnego znajdują się w *„Jak ponownie uruchomić komputer w Trybie awaryjnym?”* (p. 202).

1. Aby przeskanować komputer za pomocą Ręcznego Skanowania BitDefender, kieruj się ścieżką z menu start systemu Windows: **Start → Wszystkie programy → BitDefender 2011 → BitDefender Ręczne Skanowanie**.
2. Kliknij **Dodaj folder**, aby wskazać cel skanowania. Pojawi się nowe okno.
3. Wskaż cel skanowania:
   - Aby przeskanować pulpit, wybierz **Pulpit**.
   - Aby przeskanować całą partycję twardego dysku, wybierz ją z **Mojego komputera**.
   - Aby przeskanować folder, wyszukaj i wybierz odpowiedni folder.
4. Kliknij **Ok** i **Kontynuuj**, aby rozpocząć skanowanie.
5. Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

34.6. Co robić, gdy BitDefender określa czysty plik jako zainfekowany?

Zdarza się, że BitDefender błędnie uznaje dozwolony plik za zagrożenie (nieistniejące zagrożenie).Aby naprawić ten błąd, dodaj dany plik do obszaru Wyjątków BitDefender:

1. Wyłącz ochronę antywirusową w czasie rzeczywistym BitDefender.Informacje, jak należy to zrobić, znajdują się w *„Jak włączyć / wyłączyć ochronę w czasie rzeczywistym?”* (p. 203).
2. Wyświetl ukryte obiekty w systemie Windows.Informacje, jak należy to zrobić, znajdują się w *„Jak wyświetlić ukryte obiekty w systemie Windows?”* (p. 204).
3. Przywróć plik z obszaru kwarantanny.
4. Umieść plik w obszarze Wyjątki.
5. 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 *„Otrzymywanie pomocy”* (p. 194).

34.7. Jak usunąć zainfekowane pliki z folderu Informacje o woluminie systemowym?

Folder Informacje o woluminie systemowym to strefa na dysku twardym utworzona przez System operacyjny i używana przez system Windows do przechowywania ważnych informacji odnoszących się do konfiguracji systemu.

Mechanizmy BitDefender mogą wykryć każdego wirusa zapisanego przez moduł Informacje o woluminie systemowym. Ponieważ jest to obszar chroniony, mogą jednak nie być w stanie ich usunąć.

Zainfekowane pliki wykryte w folderach Przywracania systemu zostaną umieszczone w Dzienniku skanowania:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Aby całkowicie i natychmiast usunąć zainfekowany plik lub pliki z zapisanych danych, wyłącz, a następnie włącz ponownie funkcję Przywracania systemu.

Gdy Przywracanie systemu jest wyłączone, punkty przywracania zostają usunięte.

Gdy Przywracanie systemu jest ponownie włączone, nowe punkty przywracania tworzone są zgodnie z harmonogramem i zdarzeniami.

Aby wyłączyć Przywracanie systemu, wykonaj następujące kroki:

- **Dla Windows XP:**
  1. Przejdź do: **Start → Wszystkie programy → Akcesoria → Narzędzia systemowe → Przywracanie systemu**

2. Kliknij **Ustawienia przywracania systemu**, znajdujące się po lewej stronie okna.
3. Zaznacz pole wyboru **Wyłącz przywracanie systemu** przy wszystkich napędach i kliknij **Zastosuj**.
4. Gdy zostaniesz ostrzeżony o usunięciu wszystkich Punktów przywracania, kliknij **Tak**, aby kontynuować.
5. Aby włączyć Przywracanie systemu, odznacz pole wyboru **Wyłącz przywracanie systemu** przy wszystkich napędach i kliknij **Zastosuj**.

- **Dla Windows Vista:**
  1. Przejdź do: **Start** → **Panel sterowania** → **System i konserwacja** → **System**
  2. W lewym panelu kliknij **Ochrona systemu**.

     Jeśli zostaniesz poproszony o hasło administratora lub potwierdzenie, podaj jedno lub drugie.
  3. Aby wyłączyć Przywracanie systemu, odznacz pola wyboru odpowiadające każdemu napędowi i kliknij **Ok**.
  4. Aby włączyć Przywracanie systemu, zaznacz pola wyboru odpowiadające każdemu napędowi i kliknij **Ok**.
- **Dla Windows 7:**
  1. Kliknij **Start**, prawym przyciskiem myszy kliknij **Komputer**, a następnie kliknij **Właściwości**.
  2. W lewym panelu kliknij łącze **Ochrona systemu**.
  3. W opcjach **Ochrony systemu** zaznacz każdą literę napędu i kliknij **Konfiguruj**.
  4. Wybierz **Wyłącz ochronę systemu** i kliknij **Zastosuj**.
  5. Kliknij **Usuń**, gdy zostaniesz o to poproszony kliknij **Kontynuuj**, a następnie kliknij **Ok**.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji *„Otrzymywanie pomocy”* (p. 194).

34.8. Jakie pliki chronione hasłem wymieniono 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 innym sposób rozszyfrowane.

W przypadku rozpakowania tej zawartości, działający w czasie rzeczywistym skaner BitDefender automatycznie przeskanuje ją, aby zapewnić komputerowi ochronę.Jeśli chcesz skanować te pliki przy użyciu BitDefender, musisz skontaktować się z producentem produktu, aby uzyskać więcej informacji na ich temat.

Zalecamy zignorowanie tych plików, ponieważ nie stanowią one zagrożenia dla systemu.

34.9. Jakie elementy pominięte wymienione są w Dzienniku skanowania?

Wszystkie pliki, które w raporcie ze skanowania zostaną oznaczone jako Pominięte, są czyste.

Aby zwiększyć wydajność, BitDefender nie skanuje plików, które nie uległy zmianie od czasu ostatniego skanowania.

34.10. Jakie nadkompresowane pliki wymienione są w Dzienniku skanowania?

Nadkompresowane elementy to takie, które nie zostały wypakowane przez mechanizm skanujący lub elementy, których rozszyfrowania 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 zostanie przeskanowana w przypadku uzyskania dostępu w czasie rzeczywistym.

34.11. Dlaczego BitDefender automatycznie usuwa zainfekowany plik?

W przypadku wykrycia zainfekowanego pliku BitDefender podejmie automatyczną próbę jego dezynfekcji.Jeśli dezynfekcja nie powiedzie się, plik zostanie przeniesiony do kwarantanny, aby powstrzymać infekcję.

W przypadku określonych typów złośliwego oprogramowania dezynfekcja jest niemożliwa, ponieważ złośliwy jest cały plik. W takich wypadkach jest on 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 inne zaufanej strony.

35. Otrzymywanie pomocy

BitDefender stara się zapewnić swoim klientom najwyższy poziom szybkiej i dokładnej pomocy technicznej.Jeśli zetknąłeś się z jakimś zagadnieniem lub masz pytanie dotyczące produktu BitDefender, możesz skorzystać z kilku zasobów internetowych, które pozwolą ci szybko znaleźć rozwiązanie lub odpowiedź.Jeśli wolisz, możesz skontaktować się z obsługą klienta BitDefender. Nasi przedstawiciele pomocy technicznej szybko odpowiedzą na twoje pytania oraz zapewnią ci niezbędną pomoc.

35.1. Zasoby internetowe

W rozwiązywaniu problemów związanych z BitDefender pomoc zapewnia kilka zasobów internetowych.

- Baza wiedzy BitDefender:http://www.bitdefender.com/help
- Forum pomocy technicznej BitDefender:http://forum.bitdefender.com
- Portal bezpieczeństwa komputerowego Malware City:http://www.malwarecity.com
- Filmy instruktażowe

Możesz również użyć ulubionej wyszukiwarki, aby znaleźć więcej informacji o ochronie komputera, produktach BitDefender i firmie.

35.1.1. Baza wiedzy BitDefender

Baza wiedzy BitDefender jest informatyczną bazą on-line przeznaczoną oprogramowaniu BitDefender. Zawiera ona w łatwo dostępnym formacie raporty ze zdarzające się czasami problemów technicznych stwierdzone przez pomoc techniczną, oraz zespół naprawiający usterki BitDefender. A także z ogólnymi artykułami o działaniu antywirusa, rozwiązaniach BitDefender, szczegółowych informacjach i wiele innych artykułów.

Baza wiedzy BitDefender dostępna dla wszystkich i korzystanie jest bezpłatne. Wszystkie ważne zapytania o informacje albo raporty odnośnie błędów przychodzące od klientów BitDefender znajdują się w bazie danych BitDefender, dzięki temu klienci mogą znaleźć tam takie informacje jak raporty błędów, prace związane z programem, artykuły informacyjne, pliki pomocy dla produktów.

Baza wiedzy BitDefender jest non-stop dostępna na http://kb.bitdefender.com.

35.1.2. Forum pomocy technicznej BitDefender

Forum pomocy technicznej BitDefender pozwala użytkownikom BitDefender uzyskać pomoc oraz pomagać innym osobom korzystającym z produktu.

Jeśli produkt BitDefender nie działa dobrze, jeśli nie może usuwać z komputera określonych wirusów lub jeśli masz wątpliwości co do jego pracy, zamieść swój problem lub pytanie na forum.

Pracownicy pomocy technicznej BitDefender monitorują forum, sprawdzając nowe wpisy i zapewniając pomoc. Odpowiedź lub rozwiązanie można także uzyskać od bardziej doświadczonego użytkownika BitDefender.

Przed zamieszczeniem problemu lub pytania przeszukaj forum, w celu znalezienie 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**.

35.1.3. Portal Malware City

Portal Malware City jest bogatym źródłem informacji na temat ochrony komputerów. Możesz tutaj poznać różne zagrożenia, na które wystawiony jest komputer podłączony do Internetu (złośliwe oprogramowanie, phishing, spam, cyberprzestępcy).Przydatny słownik, który pomoże ci zrozumieć terminy z zakresu ochrony komputerów, których możesz nie znać.

Regularnie zamieszczane są nowe artykuły, dzięki którym będziesz posiadał informacje o najnowszych odkrytych zagrożeniach, bieżących trendach ochrony oraz inne dotyczące branży bezpieczeństwa komputerowego.

Strona internetowa Malware City jest dostępna pod adresem http://www.malwarecity.com.

35.1.4. Filmy instruktażowe

Filmy instruktażowe omawiają krok po kroku konfigurowanie produktu.Są one tworzone w prosty, nieskomplikowany sposób, który zrozumie każda osoba.

Najważniejszym celem jest zapewnienie miłego użytkowania poprzez podanie podstawowych i bardziej zaawansowanych informacji na temat zasad bezpieczeństwa, sposobów konfiguracji i użytkowania BitDefender.

Głównym celem jest zastąpienie wyspecjalizowanej pomocy filmami instruktażowymi, które zapewniają dokładne informacje o tym, w jaki sposób korzystać z i konfigurować BitDefender.

Na przykład, zamiast dzwonić do pomocy technicznej BitDefender, w celu uzyskania informacji lub podejmować próby wykonania skomplikowanych procedur, można obejrzeć działania przedstawione w filmach instruktażowych.

35.2. Pytanie o Pomoc

Sekcja **Rozwiązywanie problemów i uzyskiwanie pomocy** zapewnia niezbędne informacje na temat najczęściej występujących zagadnień, z jakimi możesz się zetknąć, gdy korzystasz z tego produktu.

Jeśli nie znajdziesz rozwiązania swojego problemu w udostępnionych zasobach, możesz skontaktować się bezpośrednio z nami:

- „Skontaktuj się z nami bezpośrednio za pośrednictwem produktu BitDefender.” (p. 196)
- „Kontakt przez Internetową Bazę Wiedzy” (p. 197)

WAŻNE

Aby skontaktować się z obsługą klienta BitDefender, musisz aktywować swój produkt BitDefender.Aby uzyskać więcej informacji, odwołaj się do *„Rejestracja i Moje Konto”* (p. 50).

Skontaktuj się z nami bezpośrednio za pośrednictwem produktu BitDefender.

Jeśli posiadasz działające połączenie z Internetem (dostęp do Internetu), możesz skontaktować się z BitDefender, w celu uzyskania pomocy bezpośrednio z interfejsu produktu (okna programu).

Aby poprosić o pomoc, użyj opcji Zintegrowanej pomocy dostępnej w produkcie.

Aby skorzystać ze Zintegrowanej pomocy, wykonaj następujące kroki:

1. Otwórz BitDefender.
2. Kliknij łącze **Pomoc i wsparcie**, znajdujące się w prawym dolnym rogu okna.
3. Do wyboru masz teraz dwie opcje:
   - Uruchom w naszej bazie wyszukiwanie informacji, których szukasz.
   - Wybierz dział odpowiedni dla zagadnienia, z którym się zetknąłeś.

     Obsługa klienta zajmuje się sprzedażą, licencjami, zwrotem pieniędzy oraz odnowieniami.

     Pomoc techniczna obejmuje zagadnienia dotyczące samego produktu i jego funkcji.

     Walcz ze szkodliwym oprogramowaniem omawia zagadnienia związane z wirusami.
4. Przeczytaj stosowne artykuły oraz dokumenty i wypróbuj zaproponowane rozwiązania.

5. Jeśli rozwiązanie to nie usuwa danego problemu, użyj łącza w artykule, aby uruchomić Narzędzie pomocy technicznej.
6. Podaj swój adres e-mail, wybierz dział i napisz krótki opis problemu.

   Kliknij **Dalej**.
7. Poczekaj kilka minut aż BitDefender zgromadzi informacje dotyczące produktu. Pomogą one naszym inżynierom w znalezieniu rozwiązania dla twojego problemu.

   Kliknij **Dalej**.
8. Kliknij **Zakończ**, aby wysłać informację do działu obsługi klienta BitDefender. Otrzymasz odpowiedź tak szybko, jak to tylko możliwe.

Kontakt przez Internetową Bazę Wiedzy

Jeśli nie możesz uzyskać niezbędnych informacji za pomocą produktu BitDefendera, przejrzyj naszą internetową bazę danych:

1. Odwiedź http://www.bitdefender.com/help.Baza Wiedzy BitDefender zawiera wiele artykułów, które mogą pomóc ci w znalezieniu odpowiedzi na pytania związane z BitDefenderem.
2. Przeszukaj Bazę Wiedzy BitDefender aby znaleźć artykuły, które być może pomogą rozwiązać twój problem.
3. Przeczytaj stosowne artykuły oraz dokumenty i wypróbuj zaproponowane rozwiązania.
4. Jeśli rozwiązanie to nie usuwa danego problemu, użyj łącza w artykule, aby skontaktować się z obsługą klienta BitDefender.
5. Skontaktuj się z przedstawicielem BitDefender za pomocą e-mail, czatu lub telefonu.

36. Informacje Kontaktowe

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 10 lat BITDEFENDER uzyskał niekwestionowaną reputację poprzez ciągłe dążenie do lepszego kontaktu z klientami, aby przewyższyć oczekiwania partnerów oraz klientów. Jeśli miałbyś jakiekolwiek problemy czy pytania, nie wahaj się skontaktować z nami.

36.1. Adresy Internetowe

Dział sprzedaży: sales@bitdefender.com
Pomoc Techniczna:www.bitdefender.com/help
Dokumentacja: documentation@bitdefender.com
Program partnerski: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Rzecznik prasowy: pr@bitdefender.com
Oferty pracy: jobs@bitdefender.com
Wysyłanie Próbek Wirusów: virus_submission@bitdefender.com
Wysyłanie Próbek Spamu: spam_submission@bitdefender.com
Raportowanie Abuse: abuse@bitdefender.com
Strona internetowa produktu:http://www.bitdefender.com
Archiwa FTP produktu:ftp://ftp.bitdefender.com/pub
Lokalni dystrybutorzy:http://www.bitdefender.com/site/Partnership/list/
Baza wiedzy BitDefender:http://kb.bitdefender.com

36.2. 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/site/Partnership/list/.
2. Informacje kontaktowe lokalnych dystrybutorów BitDefender powinny zostać wyświetlone automatycznie. Jeśli tak się nie stanie, użyj narzędzia Lokalizator partnerów, które znajduje się w menu po lewej stronie i wybierz region i kraj, w którym mieszkasz.
3. Jeśli w swoim kraju nie możesz znaleźć dystrybutora BitDefender, skontaktuj się z nami, wysyłając e-mail na adres sales@bitdefender.com.Abyśmy mogli szybko zapewniać pomoc, prosimy o pisanie wiadomości e-mail w języku angielskim.

36.3. Biura BitDefender

Biurom BitDefender zależy na szybkiej odpowiedzi na twoje pytania dotyczące ich dziedziny operacji, w zakresie handlu i ogólnie. Odpowiednio adresy i lista kontaktów zamieszczona jest poniżej.

Rumunia

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefon do sprzedaży: +40 21 2063470
E-mail do sprzedaży: sales@bitdefender.ro
Pomoc Techniczna: http://www.bitdefender.ro/suport
Strona: http://www.bitdefender.ro

U.S.A

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (biuro i sprzedaż): 1-954-776-6262
Sprzedaż: sales@bitdefender.com
Pomoc Techniczna: http://www.bitdefender.com/help
Internet: http://www.bitdefender.com

Niemcy

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Biura: +49 2301 91 84 222
Sprzedaż: vertrieb@bitdefender.de
Pomoc Techniczna: http://kb.bitdefender.de
Internet: http://www.bitdefender.de

Anglia i Irlandia

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
E-mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Sprzedaż: sales@bitdefender.co.uk
Pomoc Techniczna: http://www.bitdefender.com/help
Internet: http://www.bitdefender.co.uk

Hiszpania

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Sprzedaż: comercial@bitdefender.es
Pomoc Techniczna: www.bitdefender.es/ayuda
Strona: http://www.bitdefender.es

37. Przydatne informacje

Ten rozdział przedstawia pewne ważne procedury, o których należy pamiętać przed rozpoczęciem rozwiązywania problemu technicznego.

Rozwiązywanie problemów technicznych dotyczących BitDefender wymaga pewnej wiedzy na temat systemu Windows. Kolejne kroki są w związku z tym związane z systemem operacyjnym Windows.

37.1. Jak usunąć inne rozwiązania bezpieczeństwa?

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

Gdy na jednym komputerze uruchomione jest więcej niż jedno rozwiązanie bezpieczeństwa, system staje się niestabilny.Instalator BitDefender Internet Security 2011 automatycznie wykrywa inne programy zabezpieczające i oferuje możliwość ich deinstalacji.

Jeśli podczas instalacji nie usuniesz innych rozwiązań bezpieczeństwa, wykonaj następujące kroki:

- Dla **Windows XP**:
  1. Kliknij **Start**, przejdź do **Panelu sterowania** i dwukrotnie kliknij **Dodaj / usuń programy**.
  2. Poczekaj chwilę aż pojawi się lista zainstalowanych programów.
  3. Znajdź nazwę programu, który chcesz usunąć i wybierz **Usuń**.
  4. Poczekaj na zakończenie procesu deinstalacji, a następnie ponownie uruchom system.
- Dla **Windows Vista** i **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. Poczekaj na zakończenie procesu deinstalacji, 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 temat deinstalacji.

37.2. Jak ponownie uruchomić komputer w Trybie awaryjnym?

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

Uruchamianie systemu Windows w Trybie awaryjnym:

1. Uruchom ponownie komputer.
2. Aby przejść do menu uruchamiania, naciśnij kilka razy klawisz **F8** przed załadowaniem systemu Windows.
3. W menu uruchamiania wybierz **Tryb awaryjny** i naciśnij **Enter**.
4. 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.

37.3. Czy używam 32-, czy 64-bitowej wersji systemu Windows?

Aby dowiedzieć się, czy twój system operacyjny jest 32- czy 64-bitowy, wykonaj następujące kroki:

- Dla **Windows XP**:
  1. Kliknij **Start**.
  2. W menu **Start** znajdź **Mój komputer**.
  3. Kliknij prawym przyciskiem myszy **Mój komputer** i wybierz **Właściwości**.
  4. Jeśli w polu **System** widnieje wpis **x64 Edition**, masz 64-bitową wersję systemu Windows XP.

     Jeśli nie widzisz wpisu **x64 Edition**, masz 32-bitową wersję systemu Windows XP.
- Dla **Windows Vista** i **Windows 7**:
  1. Kliknij **Start**.
  2. W menu **Start** znajdź **Komputer**.
  3. Kliknij prawym przyciskiem myszy **Komputer** i wybierz **Właściwości**.
  4. W polu **System** sprawdź informacje na temat systemu.

37.4. Gdzie znaleźć informacje na temat Ustawień Proxy?

Aby znaleźć te ustawienia, wykonaj następujące kroki:

- W przypadku programu Internet Explorer 8:
  1. Otwórz Internet Explorera.
  2. Wybierz **Narzędzia** > **Opcje internetowe**.
  3. W zakładce **Połączenia** kliknij **Ustawienia sieci LAN**.
  4. W obszarze **Użyj serwera proxy dla sieci LAN** znajdują się pola **Adres** i **Port** proxy.
- W przypadku programu Mozilla Firefox 3.6:
  1. Otwórz Firefoxa.
  2. Wybierz **Narzędzia** > **Opcje**.
  3. W zakładce **Zaawansowane** przejdź do zakładki **Sieć**.
  4. Kliknij **Ustawienia**.
- W przypadku programu Opera 10.51:
  1. Otwórz przeglądarkę Opera.
  2. Wybierz **Narzędzia** > **Preferencje**.
  3. W zakładce **Zaawansowane** przejdź do zakładki **Sieć**.
  4. Aby otworzyć okno dialogowe ustawień proxy, kliknij przycisk **Serwery proxy**.

37.5. Jak całkowicie usunąć BitDefender?

Aby prawidłowo usunąć BitDefender, wykonaj następujące kroki:

1. Przejdź do www.bitdefender.com/uninstall i pobierz specjalne narzędzie do odinstalowywania BitDefendera.
2. Korzystając z praw administratora, uruchom narzędzie do odinstalowywania.
3. Uruchom ponownie komputer.

37.6. Jak włączyć / wyłączyć ochronę w czasie rzeczywistym?

BitDefender zapewnia stałą ochronę w czasie rzeczywistym, przeciw szerokiemu zakresowi zagrożeń skanując używane pliki, wiadomości e-mail oraz komunikacje prowadzoną przez komunikatory (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Ochrona w czasie rzeczywistym zapewniana przez BitDefender jest normalnie włączona i nie powinna być wyłączana.

Do rozwiązania problemu technicznego lub usunięcia wirusa konieczne może być wyłączenie ochrony w czasie rzeczywistym. Odnoszą się one do jednej z następujących sytuacji:

- Zagadnienie spowolnienia systemu po zainstalowaniu BitDefender
- Problem z jednym z programów lub aplikacją po zainstalowaniu BitDefender
- Krótko po zainstalowaniu BitDefender mogą pojawić się komunikaty o błędach

Wykonaj następujące kroki, aby włączyć/ wyłączyć tymczasowo ochronę w czasie rzeczywistym:

1. Otwórz BitDefender, w prawym górnym rogu okna kliknij **Opcje** i wybierz **Widok eksperta**.
2. Przejdź do **Antywirus** > **Tarcza**.
3. Odznacz pole wyboru **Ochrona w Czasie Rzeczywistym jest włączona**, aby czasowo wyłączyć ochronę antywirusową (lub zaznacz je, aby ją włączyć).
4. Musisz potwierdzić swój wybór, określając w menu czas, w którym ochrona w czasie rzeczywistym ma być wyłączona.

Notatka
Kroki służące do wyłączenia ochrony w czasie rzeczywistym BitDefender powinny być używane jako rozwiązanie tymczasowe jedynie na krótki okres.

37.7. Jak wyświetlić ukryte obiekty w systemie Windows?

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

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

1. Kliknij **Start**, przejdź do **Panel sterowania** i wybierz **Opcje folderów**.
2. Przejdź do zakładki **Widok**.
3. Wybierz **Wyświetlaj zawartość folderów systemowych** (tylko w systemie Windows XP).
4. Wybierz **Pokaż ukryte pliki i foldery**.
5. Usuń **Ukryj rozszerzenia plików dla znanych typów plików**.
6. Usuń **Ukryj chronione pliki systemu operacyjnego**.
7. Kliknij **Zastosuj**, a następnie **Ok**.

Słownik

ActiveX

ActiveX jest modelem do pisania programów, używanym przez inne programy i system operacyjny. Technologia ActiveX jest wykorzystywana w Microsoft Internet Explorer, aby tworzyć interaktywne i dynamiczne strony WWW, zamiast statycznych treści. Z ActiveX użytkownik może zadawać pytania lub na nie odpowiadać, może klikać w przycisku lub wchodzić w różne interakcje ze stronami WWW. Kontrolki ActiveX są najczęściej pisane w Visual Basic.

Active X jest znany z kompletnego braku kontroli zabezpieczeń; eksperci do spraw bezpieczeństwa komputerowego nie zalecają korzystać z nich w Internecie.

Adware

Adware jest często łączone z aplikacją która jest dostarczana bez opłat tak długo jak użytkownik zgadza się na adware. Ponieważ aplikacje adware są zazwyczaj instalowane po zaakceptowaniu licencji która określa cele aplikacji, ochrone przed takim adwere nie jest wymagana.

Jednak reklamy pop-up mogą być kłopotliwe, i w niektórych wypadkach obniżyć wydajność. Także niektóre te aplikacje mogą kolekcjonować informacje które mogą naruszać prywatność w pełni nie powiadamiając użytkownika w zasadach licencji.

Archiwum

Dysk, taśma, lub katalog, który zawiera pliki kopii zapasowej.

Plik, który zawiera jeden lub więcej plików w skompresowanym formacie.

Backdoor

Plik, który zawiera jeden lub więcej plików w skompresowanym formacie.

Boot sektor

Sektor na początku każdego dysku, który identyfikuje budowę dysku (rozmiar sektora, rozmiar cluster itd.). Dla startu dysku, boot sektor zawiera również program ładujący system operacyjny.

Boot wirus

Wirus, który infekuje boot sektor lub stację dyskietek. Próba startowania z zainfekowanej dyskietki wirusem boot sektor spowoduje, że wirus stanie się aktywny w pamięci. Za każdym razem, kiedy postępujesz w ten sposób wirus będzie aktywny w pamięci.

Przeglądaj

Skrót Przeglądaj sieć, aplikacja oprogramowania używana do lokowania i pokazywania stron Sieci. Najpopularniejszymi przeglądarkami są: Netscape Navigator i Microsoft Internet Explorer. Obie są graficznymi przeglądarkami, co oznacza, że mogą pokazywać grafikę oraz tekst. W dodatku większość

nowoczesnych przeglądarek może pokazywać informacje multimedialne wraz z dźwiękiem i wizją, chociaż wymagają one wtyczek dla niektórych formatów.

Wiersz poleceń

W interface linii poleceń użytkownik wpisuje polecenia w przestrzeni znajdującej się na ekranie, używając języka poleceń.

Ciasteczka

W przemyśle internetowym ciasteczka (cookie) są określane jako małe pliki zawierające informacje o indywidualnych komputerach, mogą być analizowane i używane przez reklamodawców, aby śledzić online twoje zainteresowania i gusta. Technologia ciasteczek nadal się rozwija. Intencją ciasteczek jest dostosowanie reklam bezpośrednio do twoich zainteresowań. Ciasteczko może także stać się mieczem obosiecznym. Z jednej strony jest ciekawym rozwiązaniem, ponieważ pokazuje reklamy i treści zgodne z zainteresowaniami odwiedzających. Z drugiej strony śledzi każdy ich ruch i kliknięcie. Stanowi kwestię sporną w sprawie "Zasad prywatności", bowiem wielu osobom nie podoba się, że są naznaczani tym specjalnym "kodem kreskowym".

Disk

Jest to urzadzenie, 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).

Ładuj

Aby kopiować dane (zwykle cały plik) z głównego źródła do peryferyjnego urządzenia. Termin ten jest często używany, aby opisać proces kopiowania pliku z usługi online na komputer. Ładowanie może także oznaczać kopiowanie pliku z serwera pliku sieciowego na komputer sieci.

Email

Poczta elektroniczna. Usługa, która przesyła wiadomości na komputery za pomocą sieci lokalnych lub globalnych.

Zdarzenia

Działanie lub wydarzenie wykryte przez program. Zdarzenia mogą być czynnościami użytkownika takimi jak: klikanie myszą, naciskanie klawisza lub systemem wydarzeń takim jak kończenie się pamięci.

Fałszywe pozytywny

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

Rozszerzenia pliku

Część nazwy pliku, która wskazuje na rodzaj danych przechowywanych w pliku.

Wiele systemów operacyjnych używa rozszerzeń nazw pliku takich jak Unix, VMS, i MS-DOS. Zwykle posiadają od jednego do trzech znaków. Przykłady obejmują „c" jak kod źródłowy C, „ps" jak PostScript, "txt" jak text.

Heurystyczny

Metoda oparta na regule identyfikowania nowych wirusów. Ta metoda skanowania nie polega na wyszczególnieniu nowych sygnatur wirusów. Zaletą skanowania heurystycznego jest to, że nie jest podatna na zmylenie przez nowy wariant obecnych wirusów. Jednakże może czasami zapisać podejrzany kod w normalnych programach generując tzw. "fałszywie pozytywne".

IP

Protokół internetowy – protokół w protokole TCP/IP który jest odpowiedzialny za adresowanie IP, powtarzanie czynności, fragmentację oraz ponowne montowanie pakietów IP.

Java applet

Program Java, który jest zaprojektowany, aby uruchamiał wyłącznie strony sieci. Aby użyć applet na stronie sieci, powinieneś określić nazwę applet i rozmiar (długość i szerokość w pikselach), które applet może używać. Kiedy strona sieci jest dostępna przeglądarka załadowuje applet z serwera i uruchamia go na komputerze użytkownika (klienta). Applety różnią się od aplikacji tym, że są zarządzane zgodnie ze ściśle określonym protokołem bezpieczeństwa.

Na przykład, nawet jeśli aplety pracują u klienta, nie mogą czytać ani zapisywać danych na tej maszynie. Dodatkowo, aplety są później poddawane restrykcjom dzięki którym mogą one tylko czytać i zapisywać dane z tej samej domeny z jakiej pochodzą.

Makro wirus

Typ wirusa komputerowego, który jest zakodowany jako makro w danym dokumencie. Wiele aplikacji takich jak Microsoft Word i Excel, wspierają makro języki.

Wszystkie aplikacje pozwalają tobie umiejscowić makro w dokumencie i wykonywać je za każdym razem, kiedy dokument jest otwierany.

Klient poczty

Klient e-mail jest aplikacją, która umożliwia tobie wysyłanie i otrzymywanie email.

Pamięć

Wewnętrzny obszar przechowywania informacji w komputerze. Termin pamięć identyfikuje przechowywane dane. Każdy komputer posiada pewną ilość pamięci zwykle nazywanej pamięcią główną lub RAM.

Nie-heurystyczny

Ta metoda skanowania polega na określonych sygnaturach wirusów. Zaletą skanowania nie heurystycznego jest to że nie jest on wprowadzony w błąd przez wirus metod nie generuje on fałszywych alarmów.

Spakowane programy

Plik w formacie skompresowanym. Wiele systemów operacyjnych i aplikacji zawiera polecenia, które umożliwiają tobie pakowanie pliku tak, aby zabierał on mniej pamięci. Np. masz plik tekstowy zawierający 10 kolejnych znaków. Normalnie wymagałoby to przechowania 10 bitów.

Jednakże program pakujący pliki powoduje, że ilość miejsca zajmowanego po spakowaniu ulega redukcji. W tym przypadku plik po spakowaniu może zawierać 2 bity. To tylko jedna z wielu technik pakowania - jest ich wiele więcej.

Ścieżka

Dokładne umiejscowienie pliku na komputerze. Umiejscowienia są zwykle opisywane jako sposób hierarchicznego wypełniania systemu od góry w dół.

Droga pomiędzy pewnymi punktami, takimi jak kanały komunikacyjne pomiędzy dwoma komputerami.

Phishing

Proces wysyłania wiadomości pocztowych z nieprawdziwymi danymi, często danymi zafałszowanymi w ten sposób, aby użytkownik myślał, ze wiadomość pochodzi z prawidłowego źródła, przez co proceder taki służy oszustom do wyciągania poufnych danych od użytkownika. E-maile kierują użytkownika na stronę Internetową gdzie są proszeni o aktualizacje informacji osobistych, takich jak hasło, karta kredytowa, ubezpieczenie socjalne i nr konta bankowego, informacje te odpowiednia organizacja posiada. Strona Internetowa jest sfałszowana i istnieje tylko aby wykraść informacje o użytkowniku.

Wirus Polymorphic

Wirus, który zmienia swoją formę w każdym zainfekowanym pliku. Ponieważ wirusy nie mają stałego wzoru binarnego, są one trudne do identyfikacji.

Port

Interface na komputerze, do którego podłączasz urządzenie. Komputery osobiste mają różne typy portów. Wewnętrznie, znajduje się kilka portów dla połączeń dyskowych, monitorów i klawiatur. Zewnętrznie, komputery osobiste mają port dla połączeń modemowych, drukarek, myszy i innych urządzeń peryferyjnych.

W TCP/IP i sieciach UDP zakończenie logicznego połączenia. Numer portu identyfikuje typ portu. Np. port 80 jest używany dla ruchu HTTP.

Plik raportu

Plik, który zapisuje akcje, które się zdarzyły. BitDefender utrzymuje plik raportu zapisując skanowaną ścieżkę, foldery, ilość archiwów i skanowanych plików, ile zainfekowanych i podejrzanych plików zostało znalezione.

Rootkit

Rootkit jest zestawem narzędzi programowych, który oferuje dostęp do komputera na poziomie administratora. Termin ten był początkowo używany dla systemów UNIX, oraz dotyczy skompilowanych narzędzi które dają hakerowi prawa administracyjne oraz umożliwiające ukrycie ich przed administratorami systemu.

Głównym zadaniem rootkitów jest ukrywanie procesów, plików, logowań i dzienników. Mogą również przechwytywać dane z terminali lub połączeń sieciowych i urządzeń peryferyjnych.

Rootkity z natury nie są zagrożeniem. Na przykład systemy oraz niektóre aplikacje ukrywają krytyczne pliki używając rootkitów. Niestety, bardzo często są one używane do ukrywania oprogramowania złośliwego lub intruza w systemie. Gdy są połączone z wirusami, stanowią wielkie zagrożenie dla działania i bezpieczeństwa systemu. Mogą monitorować ruch, tworzyć backdoory w systemie, zmieniać pliki i logi aby uniknąć wykrycia.

Skrypty

Inna nazwa dla makr; skrypt jest listą komend, które mogą być wykonywane bez udziału użytkownika.

Spam

Śmieci elektronicznej poczty albo śmieci-posty na grupach dyskusyjnych. Ogólnie znane jako niechciane wiadomości e-mail.

Spyware

Szpieguje połączenie użytkownika z Internetem bez jego wiedzy, zazwyczaj w celach reklamowych. Aplikacje spyware są zazwyczaj jako ukryty komponent programów freeware albo shareware które mogą być pobrane z Internetu; jednak, to powinno być wiadome które aplikacje shareware i freeware nie przychodzą z spyware. Raz zainstalowane spyware nasłuchuje poruszanie się użytkownika po Internecie i przesyła te informacje w tle do kogoś innego. Spyware mogą także wykradać informacje o adresach e-mail, a nawet o hasłach i numerach kart kredytowych.

Spyware jest prostym koniem trojańskim którego użytkownicy instalują nieświadomie gdy instalują coś innego. Pospolitym sposobem by zostać ofiarą spyware jest pobranie niektórych programów peer-to-peer dosępnych dzisiaj.

Poza kwestiami etyki i prywatności, spyware okrada użytkownika używając pamięci komputera i także zmniejszając przepustowość połączenia Internetowego gdy wysyła informacje do bazy spyware. Ponieważ spyware zużywa pamięć i zasoby systemowe aplikacje pracujące w tle mogą zawieszać i powodować niestabilność systemu.

Cechy startowe

Wszystkie umiejscowione pliki w tym folderze będą uruchomione kiedy komputer staruje. Np. ekran startowy, plik dźwiękowy odtwarzany podczas pierwszego

startu komputera, przypominacz, lub aplikacje programowe, które uruchamiają jakieś cechy.

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 zobaczyć daną ikonę i uzyskać dostęp do informacji szczegółowych i sterowania, kliknij ją dwukrotnie lub kliknij ją prawym przyciskiem myszy.

TCP/IP

Protokół Kontroli Transmisji/Protokół Internetowy – Zespół protokołów sieciowych szeroko używanych w internecine, który zapewnia komunikację przez połączenia sieciowe komputerów z różną architekturą sprzętową i różnymi systemami operacyjnymi. TCP/IP zawierają standardy dotyczące komunikacji komputerów oraz połączeń sieciowych i ruchu.

Trojan

Niszczycielski program, który ukrywa się jako aplikacja. W przeciwieństwie do wirusów, konie trojańskie nie powielają się. Jednym z najniebezpieczniejszych typów koni trojańskich jest program zapewniający, że pozbył się wirusów z twojego komputera a w rzeczywistości wprowadzający wirusy do komputera.

Nazwa pochodzi z powieści Homera “Iliada”, w której Grecy podarowali olbrzymiego konia wrogom jako znak pokoju. Ale gdy trojanie wprowadzili konia do miasta, żołnierze greccy wyszli z konia i otworzyli bramy miasta pozwalając pozostałym na wejście i podbicie Troi.

Aktualizacje

Nowa wersja produktu oprogramowania zaprojektowana, aby zamienić starszą wersję na nowszą. Proces instalacji, w celu uaktualnień, często przyczynia się do tego, że starsza wersja jest już zainstalowana w twoim komputerze. Gdyby nie była zainstalowana, nie mógłbyś dokonać uaktualnień.

BitDefender posiada wlasny modul uaktualnienia, który pozwala tobie manualnie wprowadzać uaktualnienia lub przeprowadzać to automatycznie.

Wirus

Program lub część kodu, która jest załadowana do twojego komputera bez twojej wiedzy i uruchamia się wbrew twojej woli. Większość wirusów może się powielać. Wszystkie wirusy komputerowe są tworzone przez człowieka. Prosty wirus, który umie się kopiować kilka razy jest stosunkowo łatwy do utworzenia. Nawet tak prosty wirus jest niebezpieczny, ponieważ szybko wykorzysta całą dostępną pamięć i przyczyni się zatrzymania pracy systemu. Bardziej niebezpiecznym typem wirusa jest ten, który jest zdolny przenosić się prze sieci i łamać systemy bezpieczeństwa.

Definicja wirusa

Wzór binarny wirusa używany przez program antywirusowy, aby wykryć i wyeliminować wirusa.

Robak

Program, który propaguje się przez sieć mnożąc, się w czasie poruszania. Robak nie może się przyłączać do innych programów.