

Bitdefender[®] **ANTIVIRUS FOR MAC**



PODRĘCZNIK UŻYTKOWNIKA





Bitdefender Antivirus for Mac Podręcznik użytkownika

Data publikacji 2019.09.09

Copyright© 2019 Bitdefender

Uwagi prawne

Wszelkie prawa zastrzeżone. Żadna część tej publikacji nie może być kopiowana w żadnej formie lub postaci elektronicznej, mechanicznej, w formie fotokopii lub w postaci nagrań głosowych, ani przechowywana w jakimkolwiek systemie udostępniania i wyszukiwania informacji, bez pisemnej zgody upoważnionego przedstawiciela firmy Bitdefender. Umieszczenie krótkich cytatów w recenzjach może być dopuszczalne tylko z powołaniem się na cytowane źródło. Zawartość nie może być w żaden sposób modyfikowana.

Ostrzeżenie i zrzeczenie się odpowiedzialności. Ten produkt i jego dokumentacja są chronione prawami autorskimi. Informacja w tym dokumencie została dostarczona w stanie „w jakim jest” i bez żadnych dodatkowych gwarancji. Dołożyliśmy wszelkich starań w przygotowanie tego dokumentu, jednak autorzy nie ponoszą żadnej odpowiedzialności w stosunku do żadnych osób lub jednostek, w przypadku szkód lub strat spowodowanych lub stwierdzenia, że wynikły one bezpośrednio lub pośrednio z powodu informacji zawartych w tej pracy.

Dokument zawiera odnośniki do stron internetowych, które nie są pod kontrolą firmy Bitdefender. Firma Bitdefender nie odpowiada za zawartość serwisów zewnętrznych. Jeśli odwiedzasz zewnętrzną stronę internetową, wymienioną w tej instrukcji - robisz to na własne ryzyko. Firma Bitdefender umieszcza te odnośniki tylko dla wygody użytkownika, a umieszczenie takiego odnośnika nie pociąga za sobą żadnej odpowiedzialności firmy Bitdefender za zawartość zewnętrznych stron internetowych.

Znaki handlowe. W tym dokumencie mogą występować nazwy i znaki handlowe. Wszystkie zarejestrowane i niezarejestrowane znaki handlowe w tym dokumencie są własnością ich poszczególnych właścicieli, i tak powinny być traktowane.



Spis treści

Jak używać tego przewodnika	v
1. Cel i grupa docelowa	v
2. Jak używać tego przewodnika	v
3. Znaki umowne stosowane w przewodniku	v
3.1. Konwencje Typograficzne	v
3.2. Uwagi	vi
4. Komentarze	vii
1. Instalacja i Usuwanie	1
1.1. Wymagania systemowe	1
1.2. Instalacja Bitdefender Antivirus for Maca	1
1.2.1. Proces instalacji	2
1.3. Usuwanie Bitdefender Antivirus for Mac	7
2. Pierwsze kroki	8
2.1. o programie Bitdefender Antivirus for Mac	8
2.2. Otwieranie Bitdefender Antivirus for Mac	8
2.3. Główne Okno Aplikacji	9
2.4. Ikona App Dock	10
2.5. Menu Nawigacyjne	10
2.6. Tryb ciemny	11
3. Ochrona przeciw złośliwemu oprogramowaniu	12
3.1. Zasady dobrego postępowania	12
3.2. Skanowanie twojego komputera Mac	13
3.3. Kreator skanowania	14
3.4. Kwarantanna	15
3.5. Bitdefender Shield (ochrona w czasie rzeczywistym)	16
3.6. Wyjątki skanowania	16
3.7. Ochrona sieciowa	17
3.8. Anti-tracker	19
3.8.1. Interfejs Anti-Trackera	20
3.8.2. Wyłączanie Bitdefender Anti-tracker	21
3.8.3. Umożliwienie śledzenia witryny	21
3.9. Bezpieczne pliki	21
3.9.1. Zarządzanie Aplikacjami	22
3.10. Ochrona Time Machine	23
3.11. Naprawianie	24
3.12. Powiadomienia	25
3.13. Aktualizacje	26
3.13.1. Prośba o Aktualizację	26
3.13.2. Pobieranie aktualizacji poprzez serwer Proxy	27
3.13.3. Upgrade do nowej wersji	27
3.13.4. Szukanie informacji o Bitdefender Antivirus for Mac	27
4. VPN	28
4.1. O VPN	28
4.2. Otwieranie VPN	28



4.3. Interfejs	29
4.4. Subskrypcje	31
5. konfiguracja Preferencji	32
5.1. Preferencje dostępu	32
5.2. Preferencje Ochrony	32
5.3. Zaawansowane Preferencje	33
5.4. Oferty specjalne	33
6. Bitdefender Central	34
6.1. Na temat Bitdefender Central	34
6.2. Uzyskiwanie dostępu do Bitdefender Central	35
6.3. Uwierzytelnienie dwuskładnikowe	35
6.4. Dodawanie zaufanych urządzeń	37
6.5. Moje Subskrypcje	37
6.5.1. Aktywuj subskrypcje	37
6.5.2. Kup subskrypcję	38
6.6. Moje urządzenia	38
6.6.1. Dostosuj swoje urządzenie	38
6.6.2. Zdalne akcje	39
7. Często Zadawane pytania (FAQ)	41
8. Otrzymywanie pomocy	46
8.1. Wsparcie	46
8.1.1. Zasoby internetowe	46
8.1.2. Prośba o pomoc	48
8.2. Informacje o produkcie	48
8.2.1. Adresy Internetowe	48
8.2.2. Lokalni Dystrybutorzy	49
8.2.3. Biura Bitdefender	49
Rodzaje złośliwego Oprogramowania	51



Jak używać tego przewodnika

1. Cel i grupa docelowa

Ten podręcznik jest przeznaczony dla wszystkich użytkowników Macintosh, którzy wybrali **Bitdefender Antivirus for Mac** jako narzędzie bezpieczeństwa dla swojego komputera. Informacje przedstawione w tej instrukcji są przeznaczone zarówno dla zaawansowanych, jak i początkujących użytkowników Macintosh'a.

Dowiesz się, jak skonfigurować i używać Bitdefender Antivirus for Mac, aby siebie chronić przed zagrożeniami i innym złośliwym oprogramowaniem. Dowiesz się, jak uzyskać to co najlepsze z Bitdefender.

Życzymy Państwu miłej i owocnej nauki.

2. Jak używać tego przewodnika

Ten poradnik jest zorganizowana wokół kilku głównych tematów:

Pierwsze kroki (p. 8)

Rozpocznij korzystanie z Bitdefender Antivirus for Mac i jego interfejsu użytkownika.

Ochrona przeciw złośliwemu oprogramowaniu (p. 12)

Naucz się jak używać Bitdefender Antivirus for Mac, aby chronić się przed złośliwym oprogramowaniem.

konfiguracja Preferencji (p. 32)

Dowiedz się więcej o preferencjach Bitdefender Antivirus for Mac.

Otrzymywanie pomocy (p. 46)

Gdzie zwrócić i kogo zapytać o radę kiedy coś idzie nie tak, jak powinno.

3. Znaki umowne stosowane w przewodniku

3.1. Konwencje Typograficzne

Większość stylów tekstu została użyta by przewodnik był bardziej czytelny. Ich wygląd i znaczenie zostały przedstawione w poniższej tabeli.



Wygląd	Opis
próbka składni	Przykłady i niektóre dane liczbowe są wydrukowane czcionką szeryfową.
http://www.bitdefender.pl	Nawiązania (linki) URL odnoszą do innych miejsc takich jak serwery http czy ftp.
documentation@bitdefender.com	Adresy Email zostały umieszczone w tekście dla informacji kontaktowych.
Jak używać tego przewodnika (p. v)	To odnośnik do linka wewnętrznego umiejscowionego w dokumencie.
nazwa pliku	Pliki i foldery są wydrukowane czcionką szeryfową.
opcja	Wszystkie opcje produktu są napisane z użyciem pogrubionych znaków.
słowo kluczowe	Ważne słowa kluczowe lub frazy są wyróżniane poprzez użycie pogrubionych znaków.

3.2. Uwagi

Uwagi, są to notatki graficznie wyróżnione, zwracające Państwa uwagę na dodatkowe informacje odnoszące się do aktualnego paragrafu.



Notatka

Wskazówka jest krótką poradą. Choć można by ją ominąć, jednak wskazówki zawierają użyteczne informacje, takie jak specyficzne działanie lub powiązania z podobnym tematem.



WAŻNE

Ten znak wymaga Państwa uwagi i jego pomijanie nie jest zalecane. Zazwyczaj nie są to wiadomości krytyczne, ale znaczące.



Ostrzeżenie

To jest krytyczna informacja, którą należy traktować ze zwiększoną ostrożnością. Nic złego się nie stanie jeśli podążasz za tymi wskazówkami. Powinieneś to przeczytać i zrozumieć, ponieważ opisuje coś ekstremalnie ryzykowanego.



4. Komentarze

Zapraszamy do pomocy aby wzbogacić tą książeczkę. Testowaliśmy i sprawdzaliśmy wszystkie informacje, ale może się okazać, że niektóre funkcje uległy zmianie. Prosimy kierować do nas wszelkie uwagi dotyczące błędów i propozycji ulepszenia tej książeczki, abyśmy mogli ją poprawić w celu dostarczenia jak najlepszej dokumentacji.

Prosimy powiadomić nas na ten adres documentation@bitdefender.com. Wszystkie maile związane z dokumentacją prosimy pisać w języku Angielskim abyśmy mogli szybko je przeanalizować.



1. INSTALACJA I USUWANIE

Ten rozdział zawiera poniższe tematy:

- *Wymagania systemowe* (p. 1)
- *Instalacja Bitdefender Antivirus for Maca* (p. 1)
- *Usuwanie Bitdefender Antivirus for Mac* (p. 7)

1.1. Wymagania systemowe

Możesz zainstalować Bitdefender Antivirus for Mac na komputerach Macintosh z systemem OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS Sierra (10.12.6), macOS High Sierra (10.13.6) lub macOS Mojave (10.14 lub nowszy).

Twój komputer Mac musi również mieć co najmniej 1 GB wolnego miejsca na dysku twardym.

Połączenie internetowe jest wymagane, aby zarejestrować i zaktualizować Bitdefender Antivirus for Mac.

Jak uzyskać informacje o wersji macOS i sprzęcie Twojego komputera Mac

Kliknij ikonę Apple w lewym górnym rogu ekranu i wybierz **Ten Mac...** W wyświetlonym oknie można zobaczyć wersję systemu operacyjnego i inne przydatne informacje. Kliknij **Raport Systemu**, aby uzyskać szczegółowe informacje sprzętowe.

1.2. Instalacja Bitdefender Antivirus for Maca

Aplikację Bitdefender Antivirus for Mac można zainstalować z konta Bitdefender w następujący sposób:

1. Zaloguj się jako administrator.
2. Idź do: <https://central.bitdefender.com>.
3. Zaloguj się do swojego konta Bitdefender, używając swojego adresu e-mail i hasła.
4. W panelu **Moje Urządzenia**, kliknij **ZAINSTALUJ OCHRONĘ**.
5. Wybierz jedną z dwóch dostępnych opcji:



● Chroń to urządzenie

- a. Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.
- b. Zapisz plik instalacyjny.

● Chroń inne urządzenia

- a. Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.
- b. Kliknij **WYŚLIJ PLIK DO POBRANIA**.
- c. W odpowiednim polu wpisz adres e-mail i kliknij **WYŚLIJ EMAIL**.
Miej na uwadze, że wygenerowany link do pobierania jest ważny tylko przez następne 24 godziny. Jeśli link wygaśnie, będziesz musiał wygenerować nowy, wykonując te same kroki.
- d. Na urządzeniu, na którym chcesz zainstalować Bitdefender, sprawdź konto e-mail, które wpisałeś, a następnie naciśnij odpowiedni przycisk pobierania.

6. Uruchom produkt Bitdefender, który pobrałeś.

7. Wykonaj czynności instalacyjne.

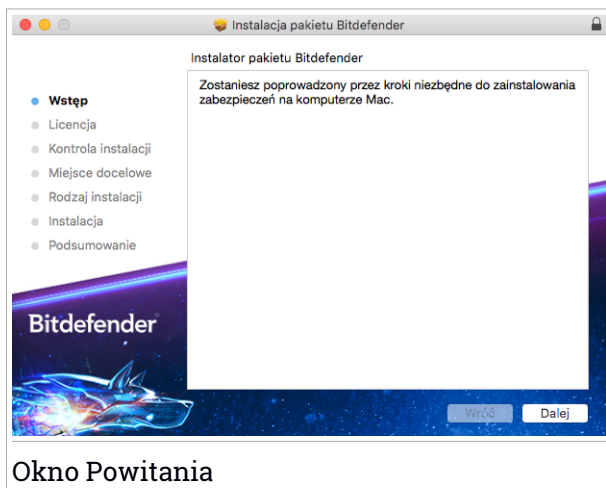
1.2.1. Proces instalacji

Aby zainstalować Bitdefender Antivirus for Mac:

1. Kliknij pobrany plik. Spowoduje to uruchomienie instalatora, który poprowadzi Cię przez proces instalacji.
2. Postępuj zgodnie z instrukcjami kreatora instalacji.



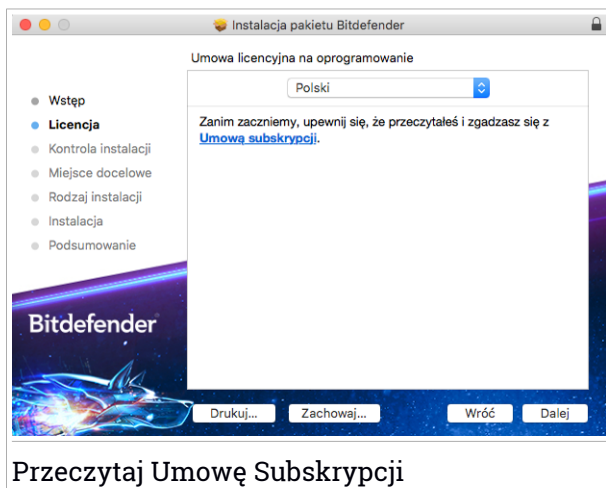
Krok 1 - Okno Powitalne



Kliknij **"Kontynuuj"**.



Krok 2 – Przeczytaj Umowę Subskrypcji



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

Z tego okna możesz także wybrać język, w którym chcesz zainstalować produkt.

Kliknij **Kontynuuj**, a następnie kliknij **Zgadzam się**.

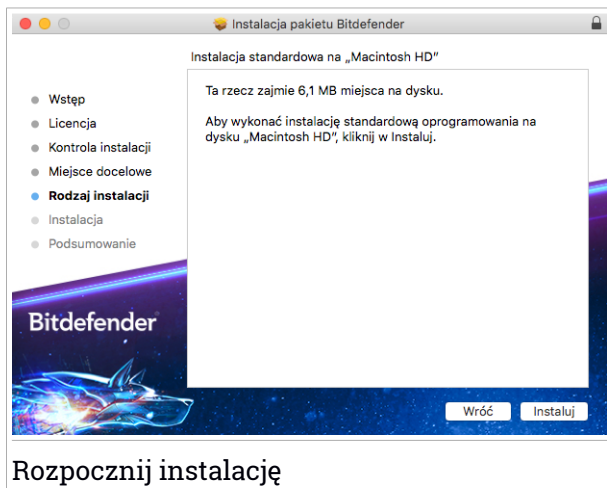


WAŻNE

Jeśli nie zgadzasz się na te warunki, kliknij **Kontynuuj**, a następnie kliknij **Nie zgadzam się**, aby przerwać instalację i zamknąć instalatora.



Krok 3 – Rozpocznij Instalację

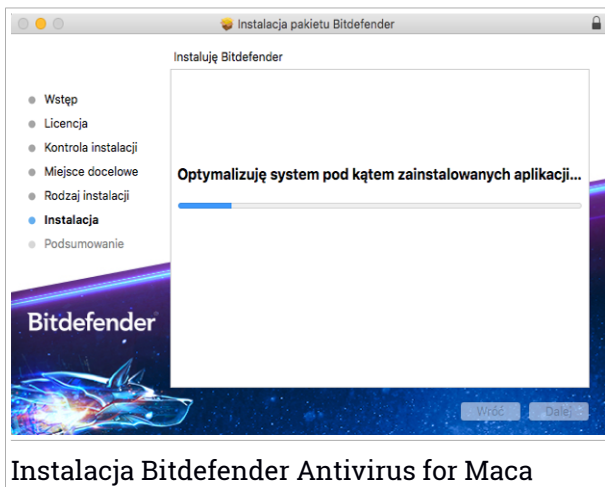


Bitdefender Antivirus for Mac zostanie zainstalowany w Macintosh HD/Biblioteka/Bitdefender. Ścieżka instalacji nie może zostać zmieniona.

Kliknij **Zainstaluj**, aby rozpocząć instalację.

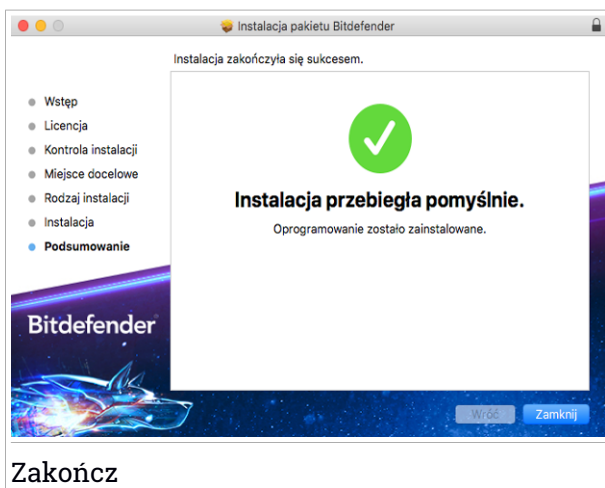


Krok 4 - Instalowanie Bitdefender Antivirus for Mac



Poczekaj aż instalacja się zakończy, a następnie kliknij **Kontynuuj**.

Krok 5 - Zakończenie



Kliknij **Zamknij**, aby zamknąć okno instalacyjne.
Proces instalacji jest już ukończony.



WAŻNE

- Jeśli instalujesz Bitdefender Antivirus for Mac na macOS High Sierra 10.13.0 lub nowszej wersji, wyświetlone zostanie powiadomienie **Rozszerzenie Systemu Zablokowane**. Powiadomienie informuje Cię, że rozszerzenia podpisane przez Bitdefender zostały zablokowane i muszą zostać włączone ręcznie. Kliknij **OK** aby kontynuować. W wyświetlonym oknie Bitdefender Antivirus for Mac kliknij link **Zabezpieczenia & Prywatność**. Kliknij **Zezwól** w dolnej części okna lub zaznacz SRL Bitdefender z listy, a następnie kliknij przycisk **OK**.
- Jeśli instalujesz Bitdefender Antivirus for Mac na macOS Mojave 10.14 lub nowszej wersji, pojawi się powiadomienie. To powiadomienie informuje Cię, że musisz ręcznie zezwolić Bitdefender Antivirus for Mac na załadowanie jego plików do twojego systemu. Aby kontynuować, kliknij link **Zabezpieczenia & Prywatność**, a następnie kliknij **OK**. Kliknij przycisk **Zezwól** obok Bitdefender SRL.

1.3. Usuwanie Bitdefender Antivirus for Mac

Będąc kompleksowym rozwiązaniem, Bitdefender Antivirus for Mac nie może być usunięty w normalny sposób, przeciągając ikonę aplikacji z folderu Aplikacje do Kosza.

Aby usunąć Bitdefender Antivirus for Mac, wykonaj następujące kroki:

1. Otwórz okno **Finder**, a następnie przejdź do folderu Aplikacje.
2. Otwórz folder Bitdefender, a następnie kliknij dwukrotnie Bitdefender Deinstalator.
3. Kliknij **Odinstaluj** i czekaj aż proces zostanie zakończony.
4. Kliknij **Zamknij**, aby zakończyć.



WAŻNE

Jeśli pojawi się błąd, możesz skontaktować się z Obsługą Klienta Bitdefender jak opisano w [Wsparcie \(p. 46\)](#).



2. PIERWSZE KROKI

Ten rozdział zawiera poniższe tematy:

- *o programie Bitdefender Antivirus for Mac* (p. 8)
- *Otwieranie Bitdefender Antivirus for Mac* (p. 8)
- *Główne Okno Aplikacji* (p. 9)
- *Ikona App Dock* (p. 10)
- *Menu Nawigacyjne* (p. 10)
- *Tryb ciemny* (p. 11)

2.1. o programie Bitdefender Antivirus for Mac


Bitdefender Antivirus for Mac jest potężnym skaner antywirusowym, który potrafi wykryć i usunąć wszystkie rodzaje złośliwego oprogramowania ("zagrożenia"), w tym:

- ransomware
- adware
- wirusom
- spyware
- Trojany
- keylogger'y
- robaki

Ta aplikacja wykrywa i usuwa nie tylko zagrożenia na komputerach Mac, ale również zagrożenia Windows, a to zabezpieczy cię przed przypadkową wysyłką zainfekowanych plików do twojej rodziny, przyjaciół i znajomych używających komputerów PC.

2.2. Otwieranie Bitdefender Antivirus for Mac


Istnieje kilka sposobów, aby otworzyć Bitdefender Antivirus for Mac.

- Kliknij ikonę Bitdefender Antivirus for Mac w Launchpad.
- Kliknij ikonę  w pasku menu i wybierz **Otwórz Okno Główne**.
- Otwórz okno Finder, przejdź do Aplikacje i kliknij dwa razy ikonę Bitdefender Antivirus for Mac.



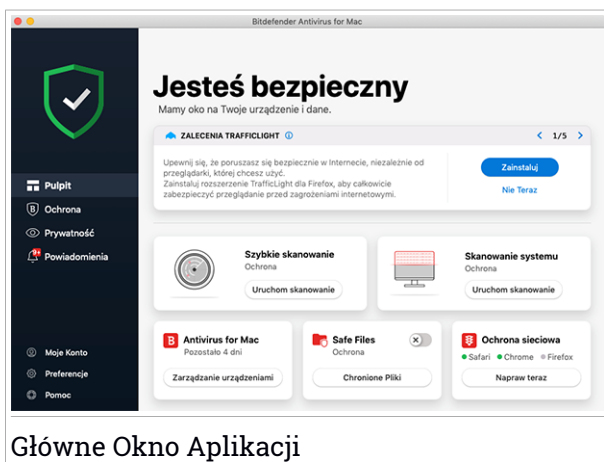
WAŻNE

Przy pierwszym uruchomieniu Bitdefender Antivirus for Mac na macOS Mojave 10.14 lub nowszej wersji pojawia się zalecenie dotyczące ochrony. Zalecenie to pojawia się, ponieważ potrzebujemy uprawnień do skanowania całego systemu w poszukiwaniu zagrożeń. Musisz być zalogowany jako administrator i wykonać następujące kroki:

1. Kliknij link **Preferencje Systemowe**.
2. Kliknij ikonę , a następnie wpisz poświadczenia administratora.
3. Otworzy się nowe okno. Przeciągnij plik **BDLDaemon** na listę dozwolonych aplikacji.

2.3. Główne Okno Aplikacji

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



Główne Okno Aplikacji

Aby przejść przez interfejs Bitdefender, wprowadzenie zawierające szczegóły o tym jak pracować z produktem i jak konfigurować go, jest wyświetlony w na górze po lewej stronie. Wybierz prawy nawias aby kontynuować bycie prowadzonym, bądź też **Opuść wycieczkę** aby zamknąć kreator.

Pasek statusu na górze okna informuje o statusie bezpieczeństwa systemu używając jawnych wiadomości i sugestyjnych kolorów. Jeśli Bitdefender



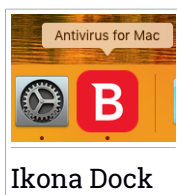
Antivirus for Mac nie ma ostrzeżeń, pasek stanu jest zielony. Po wykryciu problemu dotyczącego zabezpieczeń, pasek stanu zmieni kolor na czerwony. Szczegółowe informacje o problemach i jak je rozwiązać, możesz znaleźć na [Naprawianie \(p. 24\)](#).

Aby zapewnić Ci skuteczną obsługę i zwiększoną ochronę podczas wykonywania różnych czynności, **Bitdefender Autopilot** będzie działał jako osobisty doradca ds. Bezpieczeństwa, w zależności od wykonywanej aktywności. Pracujesz, czy dokonujesz płatności online Bitdefender Autopilot przedstawi zalecenia kontekstowe w oparciu o wykorzystanie twojego urządzenia i jego potrzeby, co pomoże ci odkryć i korzystać z zalet oferowanych przez funkcje zawarte w aplikacji Bitdefender Antivirus for Mac.

Z menu nawigacji po lewej stronie można przejść do sekcji Bitdefender, aby uzyskać szczegółową konfigurację i zaawansowane zadania administracyjne (zakładki **Ochrona** i **Prywatność**), powiadomienia, Twoje **konto Bitdefender** i **Preferencje**. Jeśli masz pytania, możesz się z nami skontaktować (zakładka **Pomoc**).


2.4. Ikona App Dock

Ikony Bitdefender Antivirus for Mac można zauważyć w Dock, jak tylko otworzysz aplikację. Ikona w Dock zapewnia łatwy sposób na skanowanie plików i folderów pod kontem zagrożeń. Złap i puść plik lub folder nad ikoną Dock, skanowanie rozpocznie się natychmiast.









2.5. Menu Nawigacyjne

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

-  **Panel**. Z tego miejsca możesz szybko naprawić problemy związane z bezpieczeństwem, wyświetlić zalecenia zgodne z potrzebami systemu i



wzorcami użytkownika, wykonać szybkie działania i przejść do konta Bitdefender, aby zarządzać urządzeniami dodanymi do subskrypcji Bitdefender.

-  **Ochrona.** Stąd możesz uruchomić skan antywirusowy, dodać pliki do listy wyjątków, zabezpieczyć pliki i aplikacje przed atakami ransomware, zabezpieczyć kopie zapasowe Time Machine i konfigurować ochronę podczas surfowania w Internecie.
-  **Prywatność.** Tutaj możesz otworzyć Bitdefender aplikację VPN i zainstalować rozszerzenie Anti-tracer w swojej przeglądarce.
-  **Powiadomienia.** Tu możesz zobaczyć szczegóły o działaniach podejmowanych na zeskanowanych plikach.
-  **Moje Konto.** Stąd możesz uzyskać dostęp do swojego konta Bitdefender, aby zweryfikować subskrypcję i wykonać zadania bezpieczeństwa na urządzeniach, którymi zarządzasz. Dostępne są również szczegóły dotyczące konta Bitdefender i wykorzystywanej subskrypcji.
-  **Preferencje.** Tutaj możesz konfigurować Bitdefender ustawienia.
-  **Pomoc.** Tutaj możesz skontaktować się z działem Wsparcia Technicznego, gdy potrzebujesz pomocy w rozwiązaniu problemu z produktem Bitdefender, a także przesłać nam swoją opinię, aby pomóc nam ulepszyć nasz produkt.

2.6. Tryb ciemny

Aby zapewnić swoim oczom ochronę przed blaskiem i światłem podczas pracy w nocy lub w warunkach słabego oświetlenia, Bitdefender Antivirus for Mac obsługuje tryb ciemny dla Mojave w wersji 10.14 lub nowszej. Kolory w interfejsie zostały zoptymalizowane, dzięki czemu bez zbędnego wpatrywania się można korzystać z Maca Interfejs Bitdefender Antivirus for Mac dostosowuje się w zależności od ustawień wyglądu urządzenia.



3. OCHRONA PRZECIW ZŁOŚLIWEMU OPROGRAMOWANIU

Ten rozdział zawiera poniższe tematy:

- *Zasady dobrego postępowania* (p. 12)
- *Skanowanie twojego komputera Mac* (p. 13)
- *Kreator skanowania* (p. 14)
- *Kwarantanna* (p. 15)
- *Bitdefender Shield (ochrona w czasie rzeczywistym)* (p. 16)
- *Wyjątki skanowania* (p. 16)
- *Ochrona sieciowa* (p. 17)
- *Anti-tracker* (p. 19)
- *Bezpieczne pliki* (p. 21)
- *Ochrona Time Machine* (p. 23)
- *Naprawianie* (p. 24)
- *Powiadomienia* (p. 25)
- *Aktualizacje* (p. 26)

3.1. Zasady dobrego postępowania

Aby utrzymać system bezpiecznym od zagrożeń i zapobiegać przypadkowym infekcjom systemu, pamiętaj o poniższych dobrych praktykach:

- Włącz **Bitdefender Shield**, aby umożliwić automatyczne skanowanie plików systemowych przez Bitdefender Antivirus for Mac.
- Zadbaj o produkt Bitdefender Antivirus for Mac dzięki najnowszym informacjom o zagrożeniach i aktualizacjom produktów.
- Sprawdź i napraw problemy zgłaszane regularnie przez Bitdefender Antivirus for Mac. Aby uzyskać szczegółowe informacje, odwołaj się do *Naprawianie* (p. 24).
- Sprawdź szczegółowy dziennik zdarzeń dotyczący aktywności Bitdefender Antivirus for Mac na komputerze. Gdy nastąpi coś istotnego dla bezpieczeństwa systemu lub danych, nowa wiadomość zostanie dodana



do obszaru Powiadomień Bitdefender. Po więcej szczegółów, uzyskaj dostęp [Powiadomienia \(p. 25\)](#).

- Należy również stosować się do tych najlepszych praktyk:
 - Dodaj zwyczaj skanowania plików jakie pobierasz z pamięci zewnętrznej (takiej jak pamięć USB lub CD), szczególnie kiedy nie znasz ich źródła.
 - Jeżeli masz plik DMG, zamontuj go i przeskanuj kontenery (pliki w zamontowanym woluminie/obrazie).

Najprostsza droga aby przeskanować plik, folder lub wolumin jest złapać&puścić go nad oknem Bitdefender Antivirus for Mac lub ikony w Dock.

Żadna inna konfiguracja ani działanie nie są wymagane. Jednakże, jeśli chcesz, możesz dostosować ustawienia aplikacji i preferencji w celu lepszego dopasowania do Twoich potrzeb. Aby uzyskać więcej informacji, odwołaj się do [konfiguracja Preferencji \(p. 32\)](#).

3.2. Skanowanie twojego komputera Mac

Poza funkcją **Bitdefender Shield**, która regularnie monitoruje zainstalowane aplikacje w poszukiwaniu zagrożeń i chroniąc przed nowymi zagrożeniami próbującymi dostać się do twojego systemu, możesz skanować swojego Mac'a lub określone pliki kiedykolwiek chcesz.

Najprostsza droga aby przeskanować plik, folder lub wolumin jest złapać&puścić go nad oknem Bitdefender Antivirus for Mac lub ikony w Dock. Kreator skanowania pokaże się i poprowadzi Cię przez proces skanowania.

Możesz również rozpocząć skanowanie według poniższych wskazówek:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Antywirus**.
3. Naciśnij jeden z trzech przycisków skanowania aby rozpocząć skanowanie.
 - **Quick Scan (Szybkie skanowanie)** - sprawdza pod kątem zgrożeń najbardziej narażone miejsca w systemie (na przykład foldery zawierające dokumenty, pobrane pliki, pobrane maile i pliki tymczasowe każdego użytkownika).
 - **Full Scan (Pełne skanowanie)** - wykonuje kompleksowe sprawdzenie całego systemu pod kątem zagrożeń. Wszystkie połączone obrazy dysków będą również skanowane.



Notatka

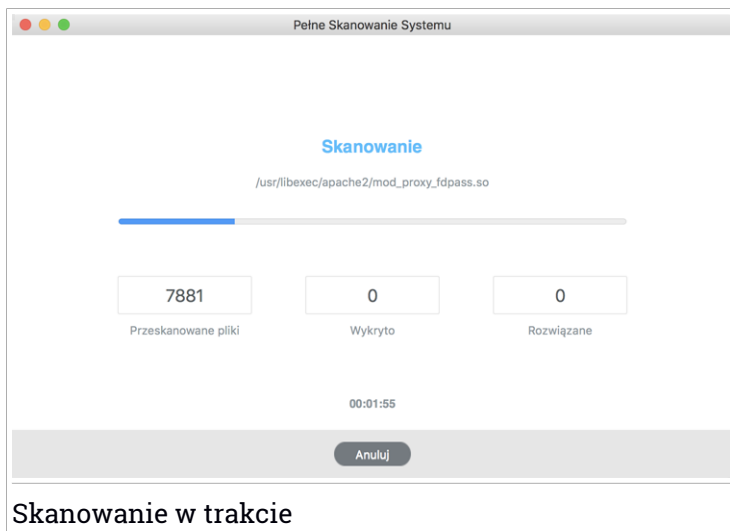
W zależności od wielkości dysku twardego, skanowanie całego systemu może chwilę potrwać (do godziny lub nawet więcej). W celu poprawy wydajności, zaleca się nie uruchamiać tego zadania, podczas wykonywania innych zasobożernych zadań (takich jak edycja wideo). Jeśli wolisz, możesz zdecydować się na skanowanie konkretnych zamontowanych woluminów, dodając je do listy **Wykluczenia** z okna Preferencje.

- **Skanowanie Niestandardowe** - pomaga Ci sprawdzić konkretne pliki, foldery lub woluminy w poszukiwaniu zagrożeń.

Możesz także uruchomić Skanowanie Systemu lub Szybkie Skanowanie z pulpitu nawigacyjnego.

3.3. Kreator skanowania

Kiedykolwiek zainicjujesz skanowanie, pojawi się kreator skanowania Bitdefender Antivirus for Mac.



Skanowanie w trakcie

Informacja w czasie rzeczywistym o wykrytych zagrożeniach i rozwiązanych zagrożeniach jest wyświetlana podczas każdego skanowania.

Zaczekaj, aż Bitdefender Antivirus for Mac zakończy skanowanie.

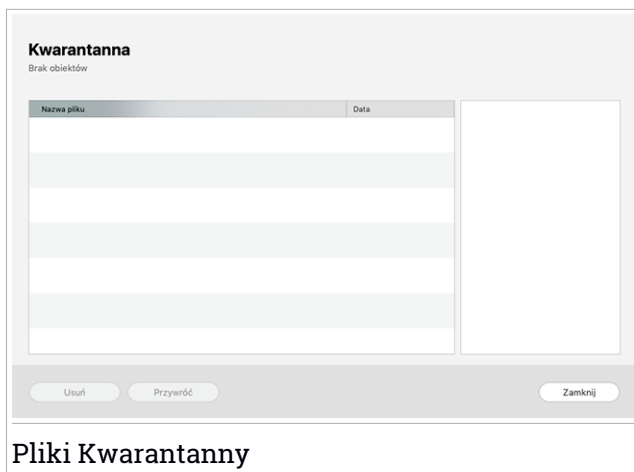


Notatka

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

3.4. Kwarantanna

Bitdefender Antivirus for Mac umożliwia izolowanie zainfekowanych i podejrzanych plików w bezpiecznym miejscu zwanym kwarantanną. Kiedy zagrożenie znajduje się w kwarantannie nie może uczynić żadnej szkody ponieważ nie może być wykonywane lub czytane.



Sekcja Kwarantanny pokazuje wszystkie pliki aktualnie odizolowane w folderze Kwarantanny.

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

Aby wyświetlić listę ze wszystkimi produktami dodanymi do kwarantanny:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Otworzy się okno **Antivirus**.

Kliknij **Otwórz** w panelu **Kwarantanna**.



3.5. Bitdefender Shield (ochrona w czasie rzeczywistym)

Bitdefender zapewnia ochronę w czasie rzeczywistym przed szeroką gamą zagrożeń poprzez skanowanie wszystkich zainstalowanych aplikacji, ich zaktualizowanych wersji oraz nowych i zmodyfikowanych plików.

Wyłączanie ochrony w czasie rzeczywistym

1. Kliknij **Preferencje** w menu nawigacji w interfejsie Bitdefender.
2. Wyłącz **Bitdefender Shield** w oknie **Ochrona**.



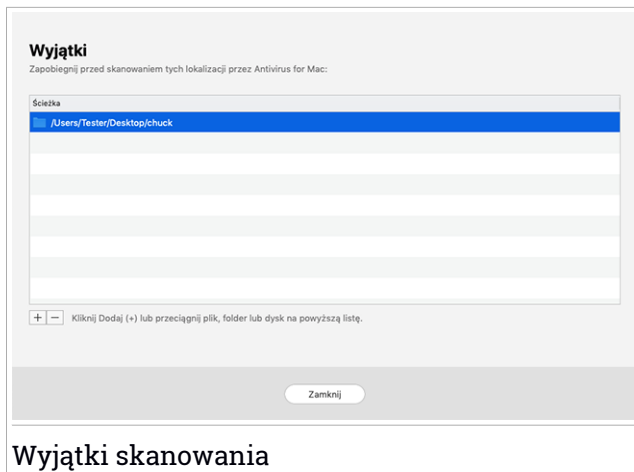
Ostrzeżenie

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

3.6. Wyjątki skanowania

Jeśli chcesz, możesz ustawić Bitdefender Antivirus for Mac by nie skanował określonych plików, folderów lub nawet całego woluminu. Na przykład, może chcesz wykluczyć ze skanowania:

- Pliki, które są błędnie zidentyfikowane jako zainfekowane (znane jako fałszywe alarmy)
- Pliki, które powodują błędy skanowania
- Objętość kopii zapasowych



Lista wykluczeń zawiera ścieżki, które zostały wyłączone ze skanowania.

Aby uzyskać dostęp do listy wykluczeń:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Otworzy się okno **Antivirus**.

Kliknij **Otwórz** w panelu **Wyjątki**.

Istnieją dwa sposoby, aby ustawić wykluczenia skanowania:

- Przeciągnij&u puść plik, folder lub wolumin nad listę wykluczeń.
- Kliknij przycisk ze znakiem plus (+), który znajduje się pod listą wykluczeń. Następnie wybierz plik, folder lub wolumin, które chcesz wykluczyć ze skanowania.

Aby usunąć wyjątek skanowania, wybierz go z listy i kliknij przycisk ze znakiem minus (-), znajdujący się na liście wykluczeń.

3.7. Ochrona sieciowa

Bitdefender Antivirus for Mac korzysta z rozszerzeń TrafficLight, aby całkowicie zabezpieczyć przeglądanie Internetu. Rozszerzenie Trafficlight przechwytyj, przetwarza i filtruje cały ruch sieciowy, blokując każdą złośliwą zawartość.



Rozszerzenie pracuje i integruje się z poniższymi przeglądarkami internetowymi: Mozilla Firefox, Google Chrome i Safari.

Włączanie rozszerzeń TrafficLight

Aby włączyć rozszerzenia TrafficLight:

1. Kliknij **Napraw Teraz** w karcie **Ochrona sieci** w panelu.
2. Otworzy się okno **Ochrona Web**.

Wykryta przeglądarka internetowa, którą zainstalowałeś w swoim systemie. Aby zainstalować rozszerzenie TrafficLight w twojej przeglądarce, naciśnij **Pobierz rozszerzenie**.

3. Zostaniesz przekierowany do:

<https://bitdefender.com/solutions/trafficlight.html>

4. Wybierz **Darmowe Pobieranie**.

5. Postępuj według poniższych kroków aby odinstalować rozszerzenie TrafficLight w twojej przeglądarce.

Zarządzanie ustawieniami rozszerzeń

Tablica funkcji dostępna jest do ochrony przed wszelkiego rodzaju zagrożeniami, które można napotkać podczas przeglądania stron internetowych. Aby uzyskać do nich dostęp, kliknij ikonę TrafficLight obok ustawień przeglądarki, a następnie kliknij **Ustawienia**:

● Ustawienia Bitdefender TrafficLight

- Zaawansowany Filtr Zagrożeń - uniemożliwia dostęp do stron internetowych używanych do złośliwego oprogramowania, ataków typu phishing i oszustw.
- Powiadomienie Tracker - wykrywa trackery na odwiedzanych stronach internetowych i informuje o ich obecności.
- Analizator Wyników Wyszukiwania - zapewnia zaawansowane ostrzeżenia o ryzykownych stronach w obrębie wyników wyszukiwania.

Jeśli wszystkie ustawienia są wyłączone, żadna strona internetowa nie zostanie zeskanowana.

● Biała lista



Strony internetowe mogą być wykluczone z skanowania przez silniki Bitdefender. W odpowiednim polu wpisz nazwę strony internetowej, którą chcesz dodać do listy wykluczeń, a następnie kliknij **DODAJ**.

W przypadku wykrycia zagrożeń na wykluczonych stronach nie będzie wyświetlane ostrzeżenie, dlatego do listy tej należy dodać tylko witryny, którym w pełni ufasz.

Strona ocen i alarmów

W zależności od sposobu w jaki TrafficLight klasyfikuje stronę internetową, którą obecnie przeglądasz, jedna z następujących ikon jest wyświetlana w tym obszarze:

- ✔ Ta strona jest bezpieczna. Możesz kontynuować swoją pracę.
- ⚠ Ta strona może zawierać niebezpieczną treść. Należy zachować ostrożność, jeśli zdecydujesz się ją odwiedzić.
- ✖ Powinieneś natychmiast opuścić stronę, ponieważ zawiera złośliwe oprogramowanie lub inne zagrożenia.

Tło ikon TrafficLight w Safari jest czarne.

3.8. Anti-tracker

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

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

Rozszerzenie Bitdefender jest zgodne z następującymi przeglądarkami internetowymi:

- Google Chrome
- Mozilla Firefox
- Safari



Wykryte przez nas trackery są pogrupowane w następujące kategorie:


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

Uruchamianie Bitdefender Anti-tracker

Aby aktywować Bitdefender rozszerzenie Anti-tracker w swojej przeglądarce:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Moduł Antykradzieżowy**.
3. Kliknij **Włącz rozszerzenie** obok przeglądarki internetowej, dla której chcesz aktywować rozszerzenie.

3.8.1. Interfejs Anti-Trackera

Gdy rozszerzenie Bitdefender Anti-Tracker jest aktywne, ikona  pojawia się obok paska wyszukiwania w przeglądarce internetowej. Za każdym razem, gdy odwiedzasz stronę internetową, na ikonie można zauważyć licznik, odnoszący się do wykrytych i zablokowanych trackerów. Aby wyświetlić więcej szczegółów o zablokowanych trackerach, kliknij ikonę, aby otworzyć interfejs. Oprócz liczby zablokowanych trackerów możesz wyświetlić czas potrzebny na załadowanie strony i kategorie, do których należą wykryte trackery. Aby wyświetlić listę śledzących witryn, kliknij żadaną kategorię.



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



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



3.8.2. Wyłączenie Bitdefender Anti-tracker


Żeby wyłączyć Bitdefender Anti-tracker w twojej przeglądarce:

1. Otwórz przeglądarkę.
2. Kliknij ikonę  obok paska adresu w przeglądarce internetowej.
3. Kliknij ikonę  w prawym górnym rogu.
4. Użyj odpowiedniego przełącznika, aby wyłączyć
Ikona Bitdefender zmienia kolor na szary.

3.8.3. Umożliwienie śledzenia witryny

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

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

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

3.9. Bezpieczne pliki

Ransomware to złośliwe oprogramowanie, które atakuje podatne systemy blokując je, i prosi o pieniądze, aby użytkownik mógł odzyskać kontrolę nad swoim systemem. To złośliwe oprogramowanie działa inteligentnie wyświetlając fałszywe wiadomości, aby sprawić, że użytkownik spanikuje i dokona płatności, o którą go poproszono.

Korzystając z najnowszej technologii, Bitdefender zapewnia integralność systemu, chroniąc ważne obszary systemu przed atakami ransomware bez



wpływu na system. Możesz też zabezpieczyć swoje osobiste pliki, takie jak dokumenty, zdjęcia lub filmy przed dostępem do niezauważanych aplikacji. Dzięki Bezpiecznym Plikom Bitdefender można osadzać osobiste pliki w schronisku i skonfigurować samodzielnie, które aplikacje powinny mieć prawo wprowadzania zmian w chronionych plikach, a które nie powinny.

Aby później dodać pliki do chronionego środowiska:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Anti-Ransomware**.
3. Kliknij **Chronione Pliki** w obszarze Bezpieczne Pliki.
4. Kliknij przycisk ze znakiem plus (+), który znajduje się pod listą chronionych plików. Następnie wybierz plik, folder lub wolumin, który ma być chroniony w przypadku, gdy ataki ransomware będą próbowały uzyskać do nich dostęp.

Aby uniknąć spowolnienia systemu, zaleca się dodanie maksymalnie 30 folderów lub zapisanie wielu plików w jednym folderze.

Domyślnie, foldery Obrazki, Dokumenty, Pulpit i Pobrane są chronione przed atakami zagrażeń.



Notatka

Foldery niestandardowe mogą być chronione tylko dla obecnych użytkowników. Dyski zewnętrzne, pliki systemowe i aplikacje nie mogą być dodawane do środowiska ochrony.

Będziesz informowany za każdym razem, gdy nieznana aplikacja o nietypowym zachowaniu spróbuje zmodyfikować dodawane pliki. Kliknij opcję **Zezwalaj** lub **Zablokuj**, aby dodać do listy **Zarządzanie aplikacjami**.

3.9.1. Zarządzanie Aplikacjami

Te aplikacje, które próbują zmienić lub usunąć chronione pliki, mogą zostać oznaczone jako potencjalnie niebezpieczne oraz dodane do listy zablokowanych aplikacji. Jeśli dana aplikacja jest blokowana, ale jesteś pewien, że działa normalnie, możesz dodać ją do wyjątków w następujących krokach:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie Bitdefender
2. Wybierz zakładkę **Anti-Ransomware**.



3. Kliknij **Dostęp do Aplikacji** w obszarze Bezpieczne Pliki.

4. Zmień status na Zezwól obok zablokowanej aplikacji.

Aplikacje ustawione na Zezwalaj można również ustawić na Zablokowane.

Użyj metody przeciągnij& i upuść lub kliknij znak plus (+), aby dodać więcej aplikacji do listy.



3.10. Ochrona Time Machine

Ochrona Time Machine Bitdefender służy jako dodatkowa warstwa zabezpieczeń dla dysku kopii zapasowej, w tym wszystkich plików, które zdecydowałeś się w nim przechowywać, poprzez blokowanie dostępu do jakiegokolwiek zewnętrznego źródła. W przypadku plików z napędu Time Machine, gdy będą szyfrowane przez ransomware, będziesz w stanie odzyskać je bez płacenia okupu.

Jeśli potrzebujesz przywrócić elementy z kopii zapasowej Time Machine, sprawdź stronę pomocy technicznej Apple.

Włączanie lub wyłączenie Ochrony Time Machine

Aby włączyć lub wyłączyć Ochronę Time Machine:

1. Kliknij **Narzędzia** w menu nawigacji w interfejsie **Bitdefender**
2. Wybierz zakładkę **Anti-Ransomware**.



3. Włącz lub wyłącz przełącznik **Ochrona Time Machine**.

3.11. Naprawianie

Bitdefender Antivirus for Mac automatycznie wykrywa i informuje o serii problemów, które mogą mieć wpływ na bezpieczeństwo systemu i danych. W ten sposób można łatwo naprawić zagrożenia bezpieczeństwa w określonym czasie.

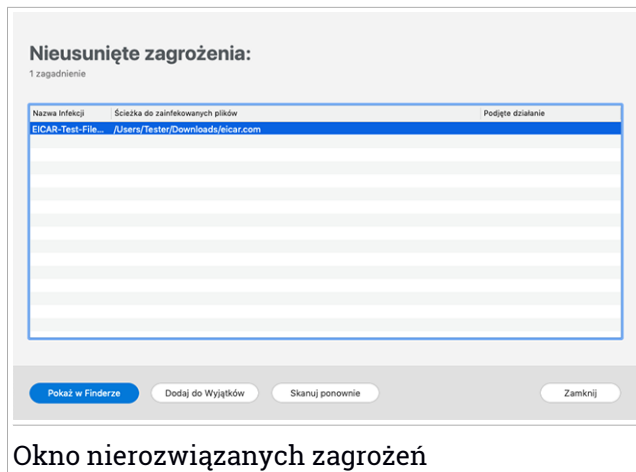
Naprawianie problemów wskazanych przez Bitdefender Antivirus for Mac jest szybkim i łatwym sposobem, aby zapewnić optymalną ochronę systemu i danych.

Wykryte problemy to:

- Nowa aktualizacja informacji o zagrożeniach nie została pobrana z naszych serwerów.
- W systemie wykryto zagrożenia i produkt nie może ich automatycznie wyczyścić.
- Ochrona w czasie rzeczywistym jest wyłączona

Aby sprawdzić i naprawić wykryte problemy:

1. Jeśli Bitdefender nie ma ostrzeżeń, pasek stanu jest zielony. Po wykryciu problemu dotyczącego zabezpieczeń, pasek stanu zmieni kolor na czerwony.
2. Sprawdź opis, aby uzyskać więcej informacji.
3. Po wykryciu problemu kliknij odpowiedni przycisk, aby wykonać czynność.



Okno nierozwiązanych zagrożeń

Lista nierozwiązanych zagrożeń jest aktualizowana po każdym skanowaniu systemu, niezależnie od tego, czy skanowanie jest wykonywane automatycznie w tle, czy inicjowane przez Ciebie.


Możesz wybrać aby wykonać poniższe działania na odkrytych zagrożeniach:

- **Usuń ręcznie.** Wykonaj tę akcję, żeby usunąć infekcję ręcznie.
- **Dodaj do Wyjątków.** Ta akcja jest niedostępna dla zagrożeń znalezionych wewnątrz archiwów.

3.12. Powiadomienia

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

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

Aby uzyskać dostęp do logu Powiadomień, kliknij **Powiadomienia** w menu nawigacji w interfejsie Bitdefender. Za każdym razem kiedy dojdzie do krytycznego zdarzenia pojawi się ikona z odliczaniem .



Zależnie od typu i istotności, powiadomienia są pogrupowane w:

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

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

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

3.13. Aktualizacje

Nowe zagrożenia są znajdowane i identyfikowane każdego dnia. aby Bitdefender Antivirus for Mac był zawsze na bieżąco z najnowszymi aktualizacjami informacji o zagrożeniach.

Aktualizacja informacji o zagrożeniach odbywa się w locie, co oznacza, że pliki są aktualizowane na bieżąco. W ten sposób, aktualizacja nie ma wpływu na działanie produktu i żadna luka nie zostanie wykluczona.

- Jeśli Bitdefender Antivirus for Mac jest zaktualizowany, może wykrywać najnowsze odkryte zagrożenia i oczyścić zainfekowane pliki.
- Jeśli Bitdefender Antivirus for Mac nie jest zaktualizowany, nie będzie w stanie wykryć i usunąć ostatnio wykrytych przez Laboratoria Bitdefender zagażeń.

3.13.1. Prośba o Aktualizację

Możesz żądać aktualizacji ręcznej kiedy tylko chcesz.

aktywne połączenie internetowe jest wymagane do sprawdzania dostępnych aktualizacji i pobierania ich.

Prośba o aktualizację ręczną:

1. Kliknij przycisk **Akcje** w pasku menu.



2. Wybierz **Uaktualnij informacje z bazy danych zagrożeń**.

Alternatywnie, możesz zażądać aktualizacji ręcznie naciskając CMD + U.

Możesz zobaczyć proces aktualizacji i pobierania plików.

3.13.2. Pobieranie aktualizacji poprzez serwer Proxy

Bitdefender Antivirus for Mac może być aktualizowany tylko poprzez serwery proxy, które nie potrzebują uwierzytelniania. Nie możesz skonfigurować żadnych ustawień programów.

Jeżeli łączysz się z internetem za pośrednictwem serwera proxy, który wymaga uwierzytelnienia, musisz przełączyć się do bezpośredniego połączenia z internetem aby zaktualizować informacje o zagrożeniach.

3.13.3. Upgrade do nowej wersji

Czasami zdarza się, że uruchamiamy aktualizacje produktów, aby dodać nowe funkcje i ulepszenia lub rozwiązać problemy dotyczące produktu. Aktualizacje te mogą wymagać ponownego uruchomienia systemu, aby rozpocząć instalację nowych plików. Domyślnie, jeżeli aktualizacja wymaga ponownego uruchomienia komputera, Bitdefender Antivirus for Mac będzie działał z poprzednimi plikami dopóki komputer nie zostanie uruchomiony ponownie. W tym przypadku, proces aktualizacji nie będzie zakłócać pracy użytkownika.

Po zakończeniu aktualizacji produktów, okno pop-up poinformuje Cię, o ponownym uruchomieniu komputera. Jeżeli przegapiłeś to powiadomienie, możesz nacisnąć **Uruchom ponownie aktualizację** z paska menu lub ręcznie uruchom ponownie komputer,

3.13.4. Szukanie informacji o Bitdefender Antivirus for Mac

To find information about the Bitdefender Antivirus for Mac version you have installed, access the **About** window. W tym samym oknie możesz zobaczyć Umowę Subskrypcji i Politykę Prywatności oraz przejrzeć licencje Open Source.

Aby uzyskać dostęp do okna O:

1. Otwórz Bitdefender Antivirus for Mac.
2. Kliknij Bitdefender Antivirus for Mac w pasku menu i wybierz **O Antywirusie dla MAC**.



4. VPN

Ten rozdział zawiera poniższe tematy:

- *O VPN* (p. 28)
- *Otwieranie VPN* (p. 28)
- *Interfejs* (p. 29)
- *Subskrypcje* (p. 31)

4.1. O VPN

Z Bitdefender VPN możesz chronić swoje prywatne dane za każdym razem, gdy łączysz się z niezabezpieczonymi sieciami bezprzewodowymi na lotniskach, w centrach handlowych, w kawiarenkach lub w hotelach. W ten sposób możesz uniknąć sytuacji takich jak kradzież danych osobowych lub próby udostępnienia hakerom adresów IP urządzenia.

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



Notatka

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

4.2. Otwieranie VPN

Istnieją trzy sposoby otwierania aplikacji sieci VPN Bitdefender:

- Kliknij **Narzędzia** w menu nawigacji w interfejsie **Bitdefender**
Kliknij **Otwórz** na karcie Bitdefender VPN.



- Kliknij ikonę  na pasku menu.
- Przejdź do folderu Aplikacje, otwórz folder Bitdefender, a następnie dwukrotnie kliknij ikonę Bitdefender VPN.

Przy pierwszym uruchomieniu aplikacji musisz zezwolić Bitdefender na dodawanie konfiguracji. Pozwalając Bitdefender dodawać konfiguracje, zgadzasz się, że cała aktywność sieciowa twojego urządzenia może być filtrowana lub monitorowana podczas korzystania z aplikacji VPN.



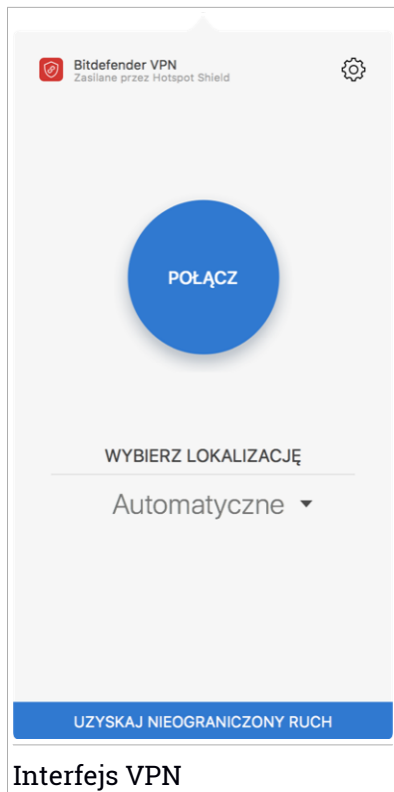
Notatka

Aplikacja Bitdefender VPN może być zainstalowana tylko na macOS Sierra (10.12.6), macOS High Sierra (10.13.6) lub macOS Mojave (10.14 lub nowszy).

4.3. Interfejs

Interfejs VPN wyświetla status aplikacji - włączona lub wyłączona. Lokalizacja serwera dla użytkowników z bezpłatną wersją jest automatycznie ustawiana przez Bitdefender na najbardziej odpowiednią. Użytkownicy premium mają możliwość zmiany lokalizacji serwera, wybierając ją z listy **WYBIERZ LOKALIZACJĘ**. Więcej informacji na temat subskrypcji VPN można znaleźć w sekcji *Subskrypcje* (p. 31).

Aby połączyć lub rozłączyć, wystarczy kliknąć na stan wyświetlony u góry ekranu. Ikona paska menu jest wyświetlana na czarno, gdy jest podłączona sieć VPN, a na biało, gdy jest ona wyłączona.



Interfejs VPN

Po podłączeniu, w dolnej części interfejsu wyświetlany jest upływający czas. Aby uzyskać dostęp do większej liczby opcji, kliknij ikonę ⚙️ w prawym górnym rogu:

- **Moje konto** - zostaną wyświetlone szczegóły dotyczące Twojego konta Bitdefender i subskrypcji VPN. Kliknij **Zmień konto**, jeśli chcesz się zalogować na inne konto.
- **Ustawienia** - w zależności od potrzeb, możesz dostosować zachowanie swojego produktu:
 - ustaw VPN, aby uruchomił się podczas uruchamiania systemu
 - otrzymuj powiadomienia, gdy VPN automatycznie się łączy lub rozłącza



- **Przejdź na Premium** - jeśli używasz darmowej wersji, możesz tutaj uaktualnić pakiet Premium. Kliknij **UAKTUALNIJ TERAZ**, aby zostać przekierowany na stronę, na której możesz kupić subskrypcję.
- **Wsparcie** - zostajesz przekierowany się do naszej platformy Centrum Wsparcia, gdzie możesz przeczytać pomocny artykuł na temat korzystania z sieci Bitdefender VPN.
- **O aplikacji** - wyświetlane są informacje o zainstalowanej wersji.
- **Wyjdź** - opuść aplikację.

4.4. Subskrypcje

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

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

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

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

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



5. KONFIGURACJA PREFERENCJI

Ten rozdział zawiera poniższe tematy:

- *Preferencje dostępu* (p. 32)
- *Preferencje Ochrony* (p. 32)
- *Zaawansowane Preferencje* (p. 33)
- *Oferty specjalne* (p. 33)

5.1. Preferencje dostępu

Aby otworzyć okno Preferencje Bitdefender Antivirus for Mac:

1. Wykonaj jedną z czynności:
 - Kliknij **Preferencje** w menu nawigacji w interfejsie Bitdefender.
 - Kliknij Bitdefender Antivirus for Mac w past menu i wybierz **Preferencje**.
 - Naciśnij Command-Przecinek(,).

5.2. Preferencje Ochrony

Okno preferencji ochrony pozwala konfigurować ogólne podejście skanowania. Możesz skonfigurować działania podejmowane na wykrytych zainfekowanych i podejrzanych plikach oraz innych ustawieniach ogólnych.

- **Bitdefender Shield.** Bitdefender Shield zapewnia ochronę w czasie rzeczywistym przed szeroką gamą zagrożeń poprzez skanowanie wszystkich zainstalowanych aplikacji, ich zaktualizowanych wersji oraz nowych i zmodyfikowanych plików. Nie zalecamy wyłączenia Bitdefender Shield, ale jeśli musisz, rób to przez jak najkrótszy czas. Jeśli Bitdefender Shield jest wyłączony, nie będziesz chroniony przed zagrożeniami
- **Skanowanie tylko nowych i zmienionych plików.** Zaznacz to pole wyboru, aby ustawić Bitdefender Antivirus for Mac, aby skanował tylko te pliki, które nie zostały wcześniej przeskanowane lub które zostały zmodyfikowane od czasu ostatniego skanowania.

Możesz nie stosować tego ustawienia w przypadku skanowania niestandardowego oraz skanowania metodą drag&drop, usuwając odpowiednie pole wyboru.

- **Nie skanuj zawartości w backup'ach.** Zaznacz to pole wyboru, aby wykluczyć pliki kopii zapasowych ze skanowania. Jeśli zainfekowane pliki



są przywracane w późniejszym czasie, Bitdefender Antivirus for Mac automatycznie wykryje je i podejmie odpowiednie działania.

5.3. Zaawansowane Preferencje

Możesz wybrać ogólne działanie, które należy podjąć w przypadku wszystkich problemów i podejrzanych elementów znalezionych podczas procesu skanowania.

Działanie, podejmowane na zainfekowanych elementach

Spróbuj wyczyścić lub przenieść do kwarantanny - W przypadku wykrycia zainfekowanych plików Bitdefender spróbuje je wyczyścić (usunąć złośliwy kod) lub przenieść do kwarantanny.

Nie podejmuj działania Żadne działanie nie zostanie podjęte na wykrytych plikach.

Działanie, podejmowane na podejrzanych elementach

Przenieś pliki do kwarantanny - w przypadku wykrycia podejrzanych plików Bitdefender przeniesie je do kwarantanny.

Nie podejmuj działania Żadne działanie nie zostanie podjęte na wykrytych plikach.

5.4. Oferty specjalne

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

Aby wyłączyć specjalne oferty oraz powiadomienia o produkcie:

1. Kliknij **Preferencje** w menu nawigacji w interfejsie Bitdefender.
2. Wybierz zakładkę **Inne**.
3. Włącz lub wyłącz przełącznik **Moje oferty**.

Opcja **Moje oferty** jest domyślnie włączona.



6. BITDEFENDER CENTRAL

Ten rozdział zawiera poniższe tematy:

- *Na temat Bitdefender Central* (p. 34)
- *Moje Subskrypcje* (p. 37)
- *Moje urządzenia* (p. 38)

6.1. Na temat Bitdefender Central

Bitdefender Central jest platformą sieciową, gdzie masz dostęp do funkcji i usług online produktu i możesz zdalnie przeprowadzić ważne zadania na urządzeniach, na których jest zainstalowany Bitdefender. Możesz się zalogować do swojego konta Bitdefender z jakiegokolwiek komputera lub urządzenia mobilnego połączonego z Internetem przechodząc do <https://central.bitdefender.com> lub bezpośrednio z aplikacji Bitdefender Central na urządzeniach Android i iOS.

Aby zainstalować aplikację Bitdefender Central na swoich urządzeniach:

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

Gdy jesteś zalogowany, możesz rozpocząć w następujący sposób:

- Pobierz i zainstaluj Bitdefender na systemach operacyjnych Windows, macOS, iOS i Android. Produkty dostępne do pobrania są:
 - Bitdefender Antivirus for Mac
 - Bitdefender linia produktów Windows
 - Bitdefender Mobile Security dla systemu Android
 - Bitdefender Mobile Security na systemy iOS
- Zarządzaj i odnow swoje subskrypcje Bitdefender.
- Dodaj nowe urządzenia do sieci i zarządzaj nimi, gdziekolwiek jesteś.



6.2. Uzyskiwanie dostępu do Bitdefender Central

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

- Z głównego interfejsu Bitdefender Antivirus for Mac:
 1. Kliknij link **Przejdź do swojego konta** w dolnej prawej części ekranu.
- Z Twojej przeglądarki internetowej:
 1. Otwórz przeglądarkę internetową na jakimkolwiek urządzeniu z dostępem do Internetu.
 2. Idź do: <https://central.bitdefender.com>.
 3. Zaloguj się na konto, używając swojego adresu e-mail i hasła.
- Z urządzeń Adroid i iOS:

Otwórz zainstalowaną aplikację Bitdefender Central.



Notatka

W tym materiale zamieściliśmy opcje, które można znaleźć w interfejsie internetowym.

6.3. Uwierzytelnienie dwuskładnikowe

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


Włączanie Uwierzytelnienia Dwuskładnikowego

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

Aby włączyć Uwierzytelnienie Dwuskładnikowe:

1. Uzyskaj dostęp do **Bitdefender Central**.



2. Kliknij ikonę  w prawym górnym rogu ekranu.
3. Kliknij **Konto Bitdefender** w rozwijanym menu.
4. Wybierz zakładkę **Hasło i bezpieczeństwo**.
5. Kliknij **ROZPOCZNIJ**.

Wybierz jedną z następujących metod:

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

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

- a. Aby rozpocząć, kliknij **UŻYJ APLIKACJI AUTHENTICATOR**.
- b. Aby zalogować się na urządzeniu Android lub iOS, użyj urządzenia do zeskanowania kodu QR.

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

Kliknij **KONTYNUUJ**.

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

- **E-mail** - za każdym razem, gdy zalogujesz się na swoje konto Bitdefender, na skrzynkę odbiorczą zostanie wysłany kod weryfikacyjny. Sprawdź skrzynkę pocztową i następnie użyj otrzymanego kodu.

- a. Kliknij **UŻYJ EMAILA**, aby rozpocząć.
- b. Sprawdź swoje konto e-mail i wpisz otrzymany kod.
- c. Kliknij **AKTYWUJ**.

Jeśli nie chcesz już używać Uwierzytelnienia Dwuskładnikowego:


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



6.4. Dodawanie zaufanych urządzeń

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

Aby dodać urządzenia jako zaufane:

1. Uzyskaj dostęp do **Bitdefender Central**.
2. Kliknij ikonę  w prawym górnym rogu ekranu.
3. Kliknij **Konto Bitdefender** w rozwijanym menu.
4. Wybierz zakładkę **Hasło i bezpieczeństwo**.
5. Kliknij **Zaufane Urządzenia**.
6. Wyświetlana jest lista urządzeń, na których zainstalowany jest Bitdefender. Kliknij wybrane urządzenie.

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

6.5. Moje Subskrypcje


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

6.5.1. Aktywuj subskrypcje

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

Jeśli zakupiłeś kod aktywacyjny od jednego z naszych sprzedawców lub otrzymałeś go w prezencie, możesz dodać jego dostępność do subskrypcji Bitdefender.

Aby aktywować subskrypcję korzystając z kodu aktywacyjnego, wykonaj następujące kroki:

1. Uzyskaj dostęp do **Bitdefender Central**.
2. Kliknij ikonę  zlokalizowaną w lewym górnym rogu okna, a następnie wybierz panel **Moje Subskrypcje**.



3. Kliknij przycisk **KOD AKTYWACYJNY**, a następnie wpisz kod w odpowiednie pole.


4. Kliknij **AKTYWUJ**, aby kontynuować.

Subskrypcja jest teraz aktywna.

Aby rozpocząć instalowanie produktu na swoich urządzeniach, przejdź do *Instalacja Bitdefender Antivirus for Maca* (p. 1).

6.5.2. Kup subskrypcję

Możesz kupić subskrypcję bezpośrednio ze swojego konta Bitdefender wykonując następujące kroki:

1. Uzyskaj dostęp do **Bitdefender Central**.
2. Kliknij ikonę  zlokalizowaną w lewym górnym rogu okna, a następnie wybierz panel **Moje Subskrypcje**.
3. Kliknij link **Kup Teraz**. Zostałeś przekierowany do strony internetowej, z której możesz dokonać zakupu.


Jak tylko zakończysz proces, dostępność subskrypcji będzie widoczna w prawym dolnym rogu głównego interfejsu produktu.

6.6. Moje urządzenia


Obszar **MOJE URZĄDZENIA** w Twoim koncie Bitdefender daje Ci możliwość zainstalowania, zarządzania i podjęcia zdalnych działań na Twoim produkcie Bitdefender na jakimkolwiek urządzeniu, pod warunkiem, że jest ono włączone i podłączone do Internetu. Karty urządzeń wyświetlają nazwę urządzenia, status ochrony i ryzyka zabezpieczeń mających wpływ na Twoje urządzenie.

6.6.1. Dostosuj swoje urządzenie

Aby łatwo zidentyfikować swoje urządzenie, możesz dostosować nazwę urządzenia:


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



5. Wpisz nową nazwę w polu **Nazwa urządzenia**, a następnie wybierz **ZAPISZ**. Możesz tworzyć i przypisywać właściciela swoich urządzeń dla lepszego zarządzania:
 1. Uzyskaj dostęp do **Bitdefender Central**.
 2. Wybierz panel **Moje Urządzenia**.
 3. Stuknij żądaną kartę urządzenia, a następnie ikonę  w prawym górnym rogu ekranu.
 4. Wybierz **Profil**.
 5. Stuknij **Dodaj właściciela**, a następnie wypełnij odpowiednie pola. Dostosuj profil dodając zdjęcie, datę urodzenia oraz adres email i numer telefonu.
 6. Kliknij **DODAJ**, aby zapisać profil.
 7. Wybierz pożądanego właściciela z listy **Właściciel urządzenia**, a następnie kliknij **PRZYPISZ**.

6.6.2. Zdalne akcje

Aby zdalnie zaktualizować Bitdefender na urządzeniu:

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

Po kliknięciu na kartę urządzenia, dostępne są następujące zakładki:

- **Panel nawigacyjny.** W tym oknie możesz zobaczyć szczegóły dotyczące wybranego urządzenia, sprawdzić stan jego zabezpieczeń i liczbę zagrożeń, które zostały zablokowane w ciągu ostatnich siedmiu dni. Stan zabezpieczeń może być zielony, gdy nie ma żadnych problemów z urządzeniem, żółty, gdy urządzenie wymaga uwagi, lub czerwony, gdy urządzenie jest zagrożone. W przypadku problemów z urządzeniem kliknij strzałkę w górnym obszarze statusu, aby uzyskać więcej informacji. Stąd można ręcznie naprawić problemy, które wpływają na bezpieczeństwo Twoich urządzeń.



- **Ochrona.** z tego okna możesz zdalnie uruchomić Szybkie lub Pełne Skanowanie na swoich urządzeniach. Kliknij przycisk **SKANUJ**, aby rozpocząć proces. Możesz również sprawdzić, kiedy zostało przeprowadzone ostatnio skanowanie na urządzeniu, dostępny jest też raport z ostatniego skanowania z najważniejszymi informacjami. Aby uzyskać więcej informacji na temat tych dwóch procesów skanowania, przejdź do *Skanowanie twojego komputera Mac (p. 13)*.



7. CZĘSTO ZADAWANE PYTANIA (FAQ)

Jak mogę wypróbować Bitdefender Antivirus for Mac przed ubieganiem się o subskrypcję?

Jesteś nowym klientem Bitdefender i chciałbyś wypróbować nasz produkt przed zakupem. Okres próbny wynosi 30 dni i można nadal korzystać z zainstalowanego produktu tylko wtedy, gdy kupisz subskrypcję Bitdefender. Aby wypróbować Bitdefender Antivirus for Mac, musisz:

1. Utwórz konto Bitdefender wykonując następujące kroki:
 - a. Idź do: <https://central.bitdefender.com>.
 - b. W odpowiednich polach wprowadź wymagane informacje. Wprowadzone dane pozostaną poufne.
 - c. Zanim przejdziesz dalej, musisz zgodzić się z Warunkami użytkowania. Uzyskaj dostęp do warunków użytkowania i przeczytaj je uważnie, ponieważ zawierają one warunki korzystania z Bitdefender.

Dodatkowo możesz uzyskać dostęp i przeczytać Politykę Prywatności.
 - d. Kliknij **UTWÓRZ KONTO**.
2. Pobierz Bitdefender Antivirus for Mac w następujący sposób:
 - a. W panelu **Moje Urządzenia**, kliknij **ZAINSTALUJ OCHRONĘ**.
 - b. Wybierz jedną z dwóch dostępnych opcji:
 - **Chroń to urządzenie**
 - i. Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.
 - ii. Zapisz plik instalacyjny.
 - **Chroń inne urządzenia**
 - i. Wybierz tę opcję, a następnie wybierz właściciela urządzenia. Jeśli urządzenie należy do kogoś innego, kliknij odpowiedni przycisk.
 - ii. Kliknij **WYŚLIJ PLIK DO POBRANIA**.



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

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


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

c. Uruchom produkt Bitdefender, który pobrałeś.

Mam kod aktywacyjny. Jak mogę dodać jego ważność do mojej subskrypcji?

Jeśli zakupiłeś kod aktywacyjny od jednego z naszych sprzedawców lub otrzymałeś go w prezencie, możesz dodać jego dostępność do subskrypcji Bitdefender.

Aby aktywować subskrypcję korzystając z kodu aktywacyjnego, wykonaj następujące kroki:

1. Uzyskaj dostęp do **Bitdefender Central**.
2. Kliknij ikonę  zlokalizowaną w lewym górnym rogu okna, a następnie wybierz panel **Moje Subskrypcje**.
3. Kliknij przycisk **KOD AKTYWACYJNY**, a następnie wpisz kod w odpowiednie pole.
4. Kliknij **AKTYWUJ**, aby kontynuować.

Rozszerzenie jest teraz widoczne w Twoim koncie Bitdefender i w Twoim zainstalowanym produkcie Bitdefender Antivirus for Mac, w prawej dolnej części ekranu.

Dziennik skanowania wskazuje, że nadal istnieją nierozwiązane pozycje. Jak mogę je usunąć?

Nierozwiązane pozycje w dzienniku skanowania mogą być:

- ograniczony dostęp do archiwów (xar, rar, itp)
Rozwiązani: Użyj opcji **Odkryj w Finder** aby znaleźć plik i usunąć go ręcznie. Upewnij się, że opróżniłeś kosz.
- ograniczony dostęp do skrzynek pocztowych (Thunderbird itp)
Rozwiązanie Użyj aplikacji do usunięcia wpisu zawierającego zainfekowany plik.



- Zawartość w kopiach zapasowych

Rozwiązanie: Włącz opcję **Nie skanuj zawartości kopii zapasowych** w Preferencjach Ochrony lub **Dodaj do Wykluczeń** wykryte pliki.

Jeśli zainfekowane pliki są przywracane w późniejszym czasie, Bitdefender Antivirus for Mac automatycznie wykryje je i podejmie odpowiednie działania.



Notatka

Ograniczony dostęp do plików oznacza, że pliki Bitdefender Antivirus for Mac można tylko otwierać, ale nie można ich modyfikować.

Gdzie mogę znaleźć informacje o działaniu produktu?

Bitdefender tworzy raport wszystkich ważnych działań i zmian statusu oraz innych istotnych wiadomości związanych ze swoją aktywnością. Aby uzyskać dostęp do tych informacji, kliknij **Powiadomienia** w menu nawigacyjnym interfejsu Bitdefender.

Czy mogę zaktualizować Bitdefender Antivirus for Mac za pomocą Serwera Proxy?

Bitdefender Antivirus for Mac może być aktualizowany tylko poprzez serwery proxy, które nie potrzebują uwierzytelniania. Nie możesz skonfigurować żadnych ustawień programów.

Jeżeli łączysz się z internetem za pośrednictwem serwera proxy, który wymaga uwierzytelnienia, musisz przełączać się do bezpośredniego połączenia z internetem aby zaktualizować informacje o zagrożeniach.

W jaki sposób usunąć Bitdefender Antivirus for Mac?

Aby usunąć Bitdefender Antivirus for Mac, wykonaj następujące kroki:

1. Otwórz okno **Finder**, a następnie przejdź do folderu Aplikacje.
2. Otwórz folder Bitdefender, a następnie kliknij dwukrotnie Bitdefender Deinstalator.
3. Kliknij **Odinstaluj** i czekaj aż proces zostanie zakończony.
4. Kliknij **Zamknij**, aby zakończyć.





WAŻNE

Jeśli pojawi się błąd, możesz skontaktować się z Obsługą Klienta Bitdefender jak opisano w **Wsparcie** (p. 46).



Jak mogę usunąć rozszerzenia TrafficLight z mojej przeglądarki?

- Aby usunąć rozszerzenie TrafficLight z Mozilla Firefox, postępuj według poniższych kroków:
 1. Przejdź do **Narzędzia** i wybierz **Add-ons**.
 2. wybierz **Rozszerzenia** w lewej kolumnie.
 3. Wybierz rozszerzenia i naciśnij **Usuń**.
 4. Uruchom ponownie przeglądarkę aby zakończyć proces usuwania.
- Aby usunąć rozszerzenie TrafficLight z Google Chrome, postępuj według poniższych kroków:
 1. W prawym górnym rogu kliknij **Więcej** .
 2. Przejdź do **Więcej Narzędzi** i wybierz **Rozszerzenia**.
 3. Kliknij ikonę **Usuń...**  obok rozszerzenia, które chcesz usunąć.
 4. Naciśnij **Usuń** aby potwierdzić proces usuwania.
- Aby usunąć Bitdefender TrafficLight z Safari, wykonaj poniższe kroki:
 1. Przejdź do **Preferencje** albo naciśnij **Klawisz-przecinek(,)**.
 2. Zaznacz **Rozszerzenia**.

Pojawi się lista z zainstalowanymi rozszerzeniami.
 3. Zaznacz Bitdefender rozszerzenie TrafficLight, a następnie kliknij **Odinstaluj**.
 4. Kliknij ponownie **Odinstaluj** aby potwierdzić proces usunięcia.

Kiedy należy używać Bitdefender VPN?

Musisz być ostrożny podczas uzyskiwania dostępu, pobierania lub przesyłania zawartości w Internecie. Aby upewnić się, że jesteś bezpieczny podczas przeglądania sieci, zalecamy korzystanie z Bitdefender VPN, gdy:

- chcesz połączyć się z publiczną siecią bezprzewodową
- chcesz uzyskać dostęp do treści, która normalnie jest ograniczona w określonych obszarach, bez względu na to, czy jesteś w domu czy za granicą



- chcesz aby Twoje dane osobiste były prywatne (nazwy użytkownika, hasła, dane karty kredytowej etc.)
- chcesz ukryć swój adres IP

Czy Bitdefender VPN będzie miał negatywny wpływ na żywotność baterii mojego urządzenia?

Bitdefender VPN ma na celu ochronę Twoich prywatnych danych, ukrywanie adresu IP przy połączeniu z niezabezpieczonymi sieciami bezprzewodowymi oraz dostęp do ograniczonych treści w niektórych krajach. Aby uniknąć zbędnego zużycia baterii Twojego urządzenia, zalecamy korzystanie z sieci VPN tylko wtedy, gdy jest to potrzebne oraz wyłączenie VPN w trybie offline.

Dlaczego Internet zwalnia, gdy jestem połączony z Bitdefender VPN?

Bitdefender VPN oferuje przyjemne doświadczenia podczas surfowania w sieci, ale łączność internetowa lub dystans między serwerem, z którym się łączysz, mogą spowodować spowolnienie. W przypadku, gdy nie ma potrzeby połączenia z odległym serwerem (np. z USA do Chin), zalecamy zezwolenie Bitdefender VPN na automatyczne połączenie z najbliższym serwerem lub znalezienie serwera bliżej bieżącej lokalizacji.



8. OTRZYMYWANIE POMOCY

Ten rozdział zawiera poniższe tematy:

- *Wsparcie* (p. 46)
- *Informacje o produkcji* (p. 48)

8.1. Wsparcie

Bitdefender stara się zapewnić swoim klientom najwyższy poziom szybkości 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 ds. pomocy technicznej szybko odpowiedzą na twoje pytania oraz zapewnią ci niezbędną pomoc.

8.1.1. Zasoby internetowe

W rozwiązywaniu problemów związanych z Bitdefender pomoc zapewnia kilka zasobów internetowych.

- Bitdefender Wsparcie Techniczne:
<https://www.bitdefender.pl/kontakt1>
- Bitdefender Forum Pomocy:
<http://forum.bitdefender.com>
- Portal bezpieczeństwa komputerowego HOTforSecurity:
<http://www.hotforsecurity.com>

Możesz również użyć ulubionej wyszukiwarki, aby znaleźć więcej informacji o ochronie komputera, produktach Bitdefender i firmie.

Bitdefender Wsparcie Techniczne

Centrum pomocy technicznej Bitdefender to internetowy magazyn informacji o produktach Bitdefender. Przechowuje czytelne raporty z trwających działań zespołu Bitdefender odnośnie pomocy technicznej i naprawiania błędów oraz bardziej ogólne artykuły dotyczące ochrony przed zagrożeniami, szczegółowego zarządzania rozwiązaniami produktu Bitdefender oraz wielu innych zagadnień.



Centrum wsparcia Bitdefender jest publicznie dostępne i łatwe do przeszukania. Informacje, które zawiera, stanowią kolejny sposób na dostarczenie klientom Bitdefender, potrzebnej wiedzy technicznej i wsparcia. Prawidłowe żądania informacji lub raportów o błędach, pochodzące od klientów Bitdefender, w końcu znajdują drogę do Wsparcia technicznego Bitdefender, jako raporty informujące o poprawkach, sposoby ominięcia problemów czy pliki pomocy produktu i teksty informacyjne.

Centrum Wsparcia Bitdefender jest dostępne o każdej porze pod następującym adresem: <https://www.bitdefender.pl/kontakt1>.

Bitdefender forum pomocy

Forum pomocy technicznej Bitdefender pozwala użytkownikom Bitdefender uzyskać pomoc oraz pomagać innym osobom korzystającym z produktu. Możesz tu opublikować dowolny problem lub pytanie dotyczące twoich produktów Bitdefender.

Pracownicy ds. pomocy technicznej Bitdefender monitorują forum sprawdzając nowe wpisy i zapewniając pomoc. Odpowiedź lub rozwiązanie można także uzyskać od bardziej zaawansowanego użytkownika programu Bitdefender.

Przed zamieszczeniem problemu lub pytania przeszukaj forum w celu znalezienia podobnych lub powiązanych tematów.

Forum pomocy technicznej Bitdefender jest dostępne pod adresem <http://forum.bitdefender.com> w 5 językach: angielskim, niemieckim, francuskim, hiszpańskim i rumuńskim. Aby uzyskać dostęp do sekcji poświęconej produktom konsumenckim, kliknij łącze **Ochrona w domu & Biurze domowym**.

Portal HOTforSecurity

Portal HOTforSecurity jest bogatym źródłem informacji na temat bezpieczeństwa komputerowego. Tu możesz dowiedzieć się więcej o różnych zagrożeniach, na które narażony jest komputer połączony z Internetem (malware, 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.



Stroną HOTforSecurity jest <http://www.hotforsecurity.com>.

8.1.2. Prośba o pomoc

Prosimy o kontakt w celu uzyskania pomocy za pośrednictwem naszego Centrum pomocy online:

1. Odwiedź <https://www.bitdefender.pl/kontakt1>.
2. Przeszukaj Centrum Wsparcia, aby znaleźć artykuły, które być może pomogą rozwiązać twój problem.
3. Przeczytaj stosowne artykuły oraz dokumenty i wypróbuj zaproponowane rozwiązania.
4. Jeśli nie znalazłeś rozwiązania, kliknij **Skontaktuj się z nami** na dole okna.
5. Skorzystaj z formularza kontaktowego, aby otworzyć pomoc e-mail lub uzyskać dostęp do innych dostępnych opcji kontaktu.

8.2. Informacje o produkcie

Skuteczna komunikacja jest kluczem do udanej współpracy. Od 2001 roku BITDEFENDER cieszy się doskonałą reputacją dzięki ciągłemu dążeniu do poprawy komunikacji z klientami, aby przewyższyć oczekiwania partnerów oraz klientów. Jeśli miałbyś jakiegokolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

8.2.1. Adresy Internetowe

Dział sprzedaży: sprzedaz@bitdefender.pl

Centrum pomocy: <https://www.bitdefender.pl/kontakt1>

Dokumentacja: documentation@bitdefender.com

Lokalni dystrybutorzy: <http://bitdefender.pl/partnerzy1>

Program partnerski: kontakt@bitdefender.pl

PR: pr@bitdefender.com

Praca: jobs@bitdefender.com

Zgłaszanie wirusa: virus_submission@bitdefender.com

Wysyłanie spamu: spam_submission@bitdefender.com

Zgłoś naruszenie: abuse@bitdefender.com

Strona: <http://www.bitdefender.pl>



8.2.2. 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://bitdefender.pl/partnerzy1>.
2. Przejdź do **Lokalizator Partnera**.
3. Informacje kontaktowe lokalnych dystrybutorów Bitdefender powinny wyświetlić się automatycznie. Jeśli to się nie stanie, wybierz kraj, w którym mieszkasz, aby wyświetlić te informacje.
4. Jeśli w swoim kraju nie możesz znaleźć dystrybutora Bitdefender, skontaktuj się z nami, wysyłając email na adres sales@bitdefender.com. Abyśmy mogli szybko zapewnić pomoc, prosimy o pisanie wiadomości e-mail w języku angielskim.

8.2.3. Biura Bitdefender

Biura Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych. Ich adresy oraz dane kontaktowe są wypisane poniżej.

U.S.A

Bitdefender, LLC

6301 NW 5th Way, Suite 4300

Fort Lauderdale, Florida 33309

Telefon (biuro i sprzedaż): 1-954-776-6262

Sprzedaż: sales@bitdefender.com

Pomoc Techniczna: <https://www.bitdefender.com/support/consumer.html>

Internet: <https://www.bitdefender.com>

Zjednoczone Emiraty Arabskie

Dubai Internet City

Building 17, Office # 160

Dubai, UAE

Telefon do sprzedaży: 00971-4-4588935 / 00971-4-4589186

Email do sprzedaży: mena-sales@bitdefender.com



Pomoc Techniczna: <https://www.bitdefender.com/support/consumer.html>
Strona: <https://www.bitdefender.com>

Niemcy

Bitdefender GmbH

TechnoPark Schwerte

Lohbachstrasse 12

D - 58239 Schwerte

Biura: +49 2304 9 45 - 162

Faks: +49 2304 9 45 - 169

Sprzedaż: vertrieb@bitdefender.de

Pomoc Techniczna: <https://www.bitdefender.de/support/consumer.html>

Internet: <https://www.bitdefender.de>

Hiszpania

Bitdefender España, S.L.U.

C/Bailén, 7, 3-D

08010 Barcelona

Faks: +34 93 217 91 28

Telefon: +34 902 19 07 65

Sprzedaż: comercial@bitdefender.es

Pomoc Techniczna: <https://www.bitdefender.es/support/consumer.html>

Strona: <https://www.bitdefender.es>

Rumunia

BITDEFENDER SRL

Orhideea Towers, 15A Orhideelor Street, Sector 6

Bucharest

Faks: +40 21 2641799

Telefon do sprzedaży: +40 21 2063470

Email do sprzedaży: sales@bitdefender.ro

Pomoc Techniczna: <https://www.bitdefender.ro/support/consumer.html>

Strona: <https://www.bitdefender.ro>



Rodzaje złośliwego Oprogramowania

Adware

Adware jest często łączony z aplikacją, która może być używana bezpłatnie tak długo, jak użytkownik zgadza się na adware. Ponieważ aplikacje typu adware są zazwyczaj instalowane po zaakceptowaniu przez użytkownika warunków umowy licencyjnej określającej cele aplikacji, zadanie ochrony przed takim adware nie jest wykonywane.

Jednak reklamy typu pop-up mogą być irytujące, a w niektórych wypadkach mogą obniżyć wydajność systemu. Ponadto informacje zbierane przez niektóre aplikacje tego typu mogą rodzić obawę naruszenia prywatności użytkowników, którzy nie byli w pełni świadomi warunków umowy licencyjnej.

Atak Brute Force

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

Atak Słownikowy

Ataki polegające na odgadywaniu haseł służyły do włamania się do systemu komputerowego poprzez wprowadzenie kombinacji typowych słów w celu wygenerowania potencjalnych haseł. Ta sama metoda służy do odgadywania kluczy deszyfrowania zaszyfrowanych wiadomości lub dokumentów. Ataki słownikowe kończą się sukcesem, ponieważ wiele osób skłania się do wybierania haseł krótkich i pojedynczych słów, które są łatwe do odgadnięcia.

Keylogger

Keylogger to aplikacja, która rejestruje wszystko, co wpisujesz.

Keyloggery nie są szkodliwe z założenia. Można ich używać dla celów zgodnych z prawem, np. po to, żeby legalnie monitorować aktywność pracowników lub dzieci. Jednak cyberprzestępcy coraz częściej używają ich w celu wyrządzenia szkody (np. do zbierania prywatnych danych, takich jak dane do logowania lub numer ubezpieczenia społecznego).

Oprogramowanie szpiegujące (spyware)

Każde oprogramowanie, które zbiera dane o użytkowniku podczas połączenia z internetem bez jego wiedzy, zazwyczaj w celach



reklamowych. Aplikacje spyware występują zazwyczaj jako ukryte komponenty programów freeware albo shareware, które mogą być pobrane z internetu. Jednakże należy pamiętać że większość aplikacji shareware oraz freeware nie ma w sobie żadnego spyware. Po zainstalowaniu, spyware monitoruje aktywność użytkownika w internecie i przesyła informacje w tle do kogoś innego. Spyware może także zbierać informacje o adresach e-mail, a nawet hasła i numery kart kredytowych.

Spyware jest prostym programem podobnym do konia trojańskiego, którego użytkownicy instalują nieświadomie podczas instalacji innego programu. Pospolitym sposobem by zostać ofiarą spyware jest pobranie niektórych z obecnie dostępnych programów współdzielonych w sieciach typu peer-to-peer.

Abstrahując od kwestii etyki i prywatności, spyware okrada użytkownika używając pamięci komputera i także zużywając przepustowość łącza internetowego podczas wysyłania informacji z powrotem do swojej bazy drogą internetową. Ponieważ spyware zużywa pamięć i zasoby systemowe, aplikacje pracujące w tle mogą powodować zawieszenie się systemu lub jego ogólną niestabilność.

Ransomware

Ransomware to złośliwy program, który stara się zarobić pieniądze na użytkownikach poprzez zablokowanie ich wrażliwych systemów. CryptoLocker, CryptoWall, i TeslaWall, to tylko niektóre warianty, które polują na prywatne systemy użytkowników.

Infekcja może rozprzestrzeniać się poprzez dostęp do wiadomości spam, pobieranie załączników lub instalowanie aplikacji, nie pozwalając użytkownikowi wiedzieć o tym, co dzieje się w jego systemie. Codziennie użytkownicy i firmy są celem hakerów ransomware.

Robak

Program, który propaguje się przez sieć mnożąc się w czasie poruszania. Nie może się podłączyć do innych programów.

Rootkit

Rootkit jest zestawem narzędzi programowych, który daje dostęp do systemu na poziomie administratora. Termin ten był początkowo używany dla systemów operacyjnych UNIX w odniesieniu do zrekompileowanych narzędzi, które udostępniały intruzom prawa



administracyjne, pozwalając im ukryć ich obecność, żeby nie byli widoczni dla administratorów systemu.

Głównym zadaniem rootkitów jest ukrywanie procesów, plików, zdarzeń logowania i raportów. Mogą również przechwytywać dane z terminali, połączeń sieciowych lub urządzeń peryferyjnych, jeśli zawierają odpowiedni rodzaj oprogramowania.

Rootkity nie są zagrożeniem z założenia. Na przykład systemy, a nawet niektóre aplikacje ukrywają krytyczne pliki używając właśnie rootkitów. Jednak często są one używane do ukrywania złośliwego oprogramowania lub intruza w systemie. Gdy są połączone z wirusami, są wielkim zagrożeniem dla spójności działania i bezpieczeństwa systemu. Mogą monitorować ruch, tworzyć backdoory w systemie, zmieniać pliki i logi oraz unikać wykrycia.

Trojan

Niszczycielski program, który ukrywa się jako niegroźna aplikacja. W przeciwieństwie do złośliwego oprogramowania i wormsów, Trojany nie powielają się. Jednym z najniebezpieczniejszych typów Trojanów jest program zapewniający, że pozbędzie się zagrożeń z Twojego komputera, a który w rzeczywistości wprowadza je do komputera.

Nazwa pochodzi z powieści Homera "Iliada", w której Grecy podarowali olbrzymiego konia swoim wrogom, Trojanom, pozornie jako znak pokoju. Gdy jednak Trojanie wprowadzili konia do miasta, greccy żołnierze wymknęli się z pustego wnętrza konia i otworzyli bramy miasta pozwalając pozostałym na wejście i podbicie Troi.

Wirus polimorficzny

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

Zagrożenie

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



typem zagrożenia jest takie, które jest zdolne przenosić się przez sieci i łamać systemy bezpieczeństwa.