



bitdefender
antivirus **2010**

Podręcznik użytkownika

BitDefender Antivirus 2010 *Podręcznik użytkownika*

Data wydania 2009.08.27

Copyright© 2009 BitDefender

Uwagi Prawne

Wszelkie prawa zastrzeżone. Żadna część tej książki nie może być reprodukowana albo transmitowana w żadnej formie ani znaczeniu, elektronicznym lub mechanicznym, włączając fotokopie, nagrywanie, albo przy wykorzystaniu jakichkolwiek systemów zapisu i utrwalania bez pisemnej zgody firmy BitDefender, za wyjątkiem krótkich cytatów w artykułach. Zawartość nie może być modyfikowana w żaden sposób.

Ostrzeżenia i Odpowiedzialność. Ten produkt i jego dokumentacja są chronione prawami autorskimi. Informacja w tym dokumencie jest dostarczona w stanie, „w jakim jest” i bez gwarancji. Dołożyliśmy wszelkich starań w przygotowaniu tego dokumentu, jednak autorzy nie ponoszą żadnej odpowiedzialności w stosunku do żadnych osób lub jednostek w przypadku szkód albo uszkodzeń spowodowanych albo stwierdzonych że wynikły bezpośrednio lub pośrednio z powodu informacji zawartych w tej pracy.

Książka zawiera odnośniki do stron internetowych, które nie są pod kontrolą firmy BitDefender zatem BitDefender nie odpowiada za zawartość stron z odnośników. Jeśli odwiedzasz stronę wymienioną w tej instrukcji, robisz to na własne ryzyko. BitDefender umieszcza te odnośniki tylko dla ułatwienia i zawarcie tego odnośnika nie pociąga za sobą żadnej odpowiedzialności za zawartość tych stron.

Znaki handlowe. Nazwy znaków handlowych mogą występować w tej książce. Wszystkie zarejestrowane i niezarejestrowane znaki handlowe w tym dokumencie są własnością ich poszczególnych właścicieli.



Spis treści

Umowa Licencyjna Oprogramowania Użytkownika Końcowego	ix
Wstęp	xiv
1. Znaki umowne stosowane w instrukcji	xiv
1.1. Konwencje Typograficzne	xiv
1.2. Uwagi	xiv
2. Struktura Książki	xv
3. Komentarze	xvi
 Instalacja i Usuwanie	1
1. Wymagania Systemowe	2
1.1. Minimalne Wymagania Sprzętowe	2
1.2. Rekomendowane Wymagania Sprzętowe	2
1.3. Obsługiwane oprogramowanie	2
2. Przygotowywanie do Instalacji	4
3. Instalacja BitDefendera	5
3.1. Kreator rejestracji	8
3.1.1. Krok 1 - Zarejestruj BitDefender Antivirus 2010	8
3.1.2. Krok 2 - Utwórz Konto BitDefender	9
3.2. Kreator Konfiguracji	11
3.2.1. Krok 1 - Wybierz Profil Użytkownika	12
3.2.2. Step 2 - Opisz Komputer	13
3.2.3. Krok 3 - Wybierz Interfejs Użytkownika	14
3.2.4. Krok 4 - Skonfiguruj Sieć BitDefender	15
3.2.5. Krok 5 - Wybierz Zadania do Uruchomienia	16
3.2.6. Krok 6 - Zakończenie	17
4. Aktualizacja	19
5. Naprawianie lub Usuwanie BitDefendera	20
 Pierwsze Kroki	21
6. Przegląd	22
6.1. Otwieranie BitDefender	22
6.2. Tryby Widoku Interfejsu Użytkownika	22
6.2.1. Tryb Początkujący	23
6.2.2. Tryb Średniozaawansowany	25
6.2.3. Tryb Eksperta	27
6.3. Ikona w Zasobniku Systemowym	29
6.4. Pasek Aktywności Skanera	30
6.4.1. Skanuj Pliki i Foldery	31
6.4.2. Zablokuj/Odblokuj Pasek Aktywności Skanera	31
6.5. Skanowanie Ręczne BitDefender	32
6.6. Tryb Gry i Tryb Laptopa	33
6.6.1. Tryb Gry	34

6.6.2. Tryb Laptopa	35
6.7. Automatyczne Wykrywanie Urządzeń	35
7. Naprawianie	37
7.1. Kreator Naprawiania Wszystkich Zagadnień	37
7.2. Konfiguracja Śledzenia Zagadnień	39
8. Konfigurowanie Ustawień Podstawowych	41
8.1. Ustawienia Interfejsu Użytkownika	42
8.2. Ustawienia Zabezpieczeń	43
8.3. Ustawienia Ogólne	44
9. Historia i Zdarzenia	46
10. Rejestracja i Moje Konto	48
10.1. Rejestrowanie BitDefender Antivirus 2010	48
10.2. Aktywacja BitDefendera	49
10.3. Zakup kluczy licencyjnych	52
10.4. Odnawianie licencji	52
11. Kreatory	53
11.1. Kreator Skanowania Antywirusowego	53
11.1.1. Krok 1/3 - Skanowanie	53
11.1.2. Krok 2/3 - Wybierz Działanie	54
11.1.3. Krok 3/3 - Wyświetl Wyniki	56
11.2. Kreator Własnego Skanowania	57
11.2.1. Krok 1/6 - Okno Powitalne	57
11.2.2. Step 2/6 - Wybierz Cel	58
11.2.3. Step 3/6 - Wybierz Działanie	60
11.2.4. Step 4/6 - Dodatkowe Ustawienia	62
11.2.5. Step 5/6 - Skanowanie	63
11.2.6. Krok 6/6 - Wyświetl Rezultat	64
11.3. Kreator Sprawdzania Podatności	65
11.3.1. Krok 1/6 - Wybierz Podatności do Sprawdzenia	66
11.3.2. Krok 2/6 - Sprawdzanie Podatności	67
11.3.3. Krok 3/6 - Aktualizacja Windows	68
11.3.4. Krok 4/6 - Aktualizuj Aplikacje	69
11.3.5. Krok 5/6 - Zmień Słabe Hasła	70
11.3.6. Krok 6/6 - Wyświetl Rezultat	71
Tryb Średniozaawansowany	72
12. Pulpit	73
13. Antywirus	75
13.1. Pole Stanu	75
13.1.1. Konfiguracja Śledzenia Stanu	76
13.2. Szybkie zadania	77
13.2.1. Aktualizowanie BitDefendera	77
13.2.2. Skanowanie BitDefenderem	78
14. Antyphishing	80

14.1. Pole Stanu	80
14.2. Szybkie zadania	81
14.2.1. Aktualizowanie BitDefendera	81
14.2.2. Skanowanie BitDefenderem	82
15. Podatności	83
15.1. Pole Stanu	83
15.2. Szybkie zadania	84
16. Sieć	85
16.1. Szybkie zadania	85
16.1.1. Dołączanie do Sieci BitDefender	86
16.1.2. Dodawanie Komputerów do Sieci BitDefender	86
16.1.3. Zarządzanie Siecią BitDefender	88
16.1.4. Skanowanie Wszystkich Komputerów	90
16.1.5. Aktualizowanie Wszystkich Komputerów	91
16.1.6. Rejestrowanie Wszystkich Komputerów	92
Tryb Eksperta	93
17. Ogólne	94
17.1. Pulpit	94
17.1.1. Ogólny Stan	95
17.1.2. Statystyki	97
17.1.3. Przegląd	98
17.2. Ustawienia	98
17.2.1. Ustawienia Ogólne	99
17.2.2. Ustawienia Raportów Wirusowych	100
17.3. Informacje Systemowe	101
18. Antywirus	103
18.1. Ochrona W Czasie Rzeczywistym	103
18.1.1. Konfigurowanie Poziomu Ochrony	104
18.1.2. Dostosowywanie Poziomu Ochrony	105
18.1.3. Konfiguracja Ustawień Active Virus Control	109
18.1.4. Wyłączanie Ochrony w Czasie Rzeczywistym	112
18.1.5. Konfigurowanie Ochrony Antyphishingowej	112
18.2. Skanowanie na żądanie	113
18.2.1. Zadania Skanowania	114
18.2.2. Używanie Menu Skrótów	116
18.2.3. Tworzenia Zadania Skanowania	117
18.2.4. Konfiguracja Zadania Skanowania	117
18.2.5. Skanowanie Plików i Folderów	129
18.2.6. Przeglądanie Dzienników Skanowania	137
18.3. Elementy Wykluczone ze Skanowania	138
18.3.1. Wykluczanie Ścieżek ze Skanowania	140
18.3.2. Wykluczanie Rozszerzeń ze Skanowania	143
18.4. Kwarantanna	147
18.4.1. Zarządzanie Plikami w Kwarantannie	148
18.4.2. Konfigurowanie Ustawień Kwarantanny	149

19. Kontrola prywatności	151
19.1. Status Kontroli Prywatności	151
19.1.1. Konfigurowanie Poziomu Ochrony	152
19.2. Kontrola tożsamości	152
19.2.1. Tworzenie Reguł Tożsamości	154
19.2.2. Definiowanie Wyjątków	158
19.2.3. Zarządzanie Regułami	159
19.2.4. Reguły Zdefiniowane przez Innych Administratorów	159
19.3. Kontrola rejestru	160
19.4. Kontrola cookie	161
19.4.1. Okno Konfiguracji	163
19.5. Kontrola Skryptów	165
19.5.1. Okno Konfiguracji	166
20. Podatności	168
20.1. Status zadania	168
20.1.1. Naprawianie Podatności	169
20.2. Ustawienia	169
21. Szyfrowanie Komunikatorów (IM)	171
21.1. Wyłączanie szyfrowania dla Podanych Użytkowników	172
22. Tryb Gry / Laptopa	174
22.1. Tryb Gry	174
22.1.1. Konfiguracja Automatycznego Trybu Gry	175
22.1.2. Zarządzanie Listą Gier	176
22.1.3. Konfigurowanie Ustawień Trybu Gry	177
22.1.4. Zmienianie klawiszy skrótu Trybu Gry	177
22.2. Tryb Laptopa	178
22.2.1. Konfigurowanie Ustawień Trybu Laptopa	179
23. Sieć Domowa	180
23.1. Dołączanie do Sieci BitDefender	180
23.2. Dodawanie Komputerów do Sieci BitDefender	181
23.3. Zarządzanie Siecią BitDefender	183
24. Aktualizacje	186
24.1. Automatyczna Aktualizacja	186
24.1.1. Prośba o Aktualizację	187
24.1.2. Wyłączanie Automatycznej Aktualizacji	188
24.2. Ustawienia Aktualizacji	188
24.2.1. Ustawienia Lokalizacji Aktualizacji	189
24.2.2. Konfiguracja Automatycznej Aktualizacji	190
24.2.3. Konfiguracja Ręcznej Aktualizacji	190
24.2.4. Konfigurowanie Ustawień Zaawansowanych	190
24.2.5. Zarządzanie Proxy	191
25. Rejestracja	193
25.1. Rejestrowanie BitDefender Antivirus 2010	193
25.2. Tworzenie Konta BitDefender	194

Integracja z Windows i Oprogramowaniem Third-Party	198
26. Integracja z Menu Kontekstowym Windows	199
26.1. Skanowanie z BitDefender	199
27. Integracja z Przeglądarką Internetową	201
28. Integracja z programami Instant Messenger	204
Jak to zrobić	205
29. Jak skanować Pliki i Foldery	206
29.1. Korzystając z Menu Kontekstowego Windows	206
29.2. Korzystanie z Zadań Skanowania	206
29.3. Korzystanie z Ręcznego Skanowania BitDefenderem	208
29.4. Używanie Paska Aktywności Skanera	209
30. Jak Harmonogramować Skanowanie Komputera	211
Rozwiązywanie Problemów i Uzyskiwanie Pomocy	213
31. Rozwiązywanie Problemów	214
31.1. Problemy Dotyczące Instalacji	214
31.1.1. Błędy Walidacji Instalacji	214
31.1.2. Instalacja Nieudana	215
31.2. Usługi BitDefender Nie Odpowiadają	216
31.3. Nie Można Usunąć BitDefendera	217
32. Otrzymywanie pomocy	219
32.1. Baza wiedzy BitDefender	219
32.2. Pytanie o Pomoc	219
32.3. Informacje Kontaktowe	220
32.3.1. Adresy Internetowe	220
32.3.2. Biura BitDefender	220
CD Ratunkowy BitDefender	222
33. Przegląd	223
33.1. Wymagania Systemowe	223
33.2. Dołączone Oprogramowanie	224
34. Dysk Ratunkowy BitDefender	226
34.1. Uruchom Dysk Ratunkowy BitDefender	226
34.2. Zatrzymaj Dysk Ratunkowy BitDefender	227
34.3. Jak przeprowadzić skanowanie antywirusowe?	228
34.4. Jak mam skonfigurować połączenie z Internetem ?	229
34.5. Jak mam zaktualizować BitDefendera?	230
34.5.1. Jak mogę zaktualizować BitDefendera przez proxy?	231
34.6. Jak mogę zapisać moje dane?	232
34.7. Jak korzystać z trybu konsoli?	234
Słownik	235

Umowa Licencyjna Oprogramowania Użytkownika Końcowego

JEŻELI NIE ZGADZASZ SIĘ NA NINIEJSZE WARUNKI NIE INSTALUJ OPROGRAMOWANIA. WYBIERAJĄC "AKCEPTUJĘ", "OK", "DALEJ", "TAK" LUB INSTALUJĄC ALBO UŻYTKUJĄC NINIEJSZE OPROGRAMOWANIE W DOWOLNY SPOSÓB, WSKAZUJESZ NA CAŁKOWITE ZROZUMIENIE I AKCEPTACJĘ WARUNKÓW NINIEJSZEJ UMOWY.

REJESTRACJA PRODUKTU. Akceptując tą Umowę, zgadzasz się na zarejestrowanie Swojego Oprogramowania, korzystając z "Mojego Konta", jako warunek swojego korzystania z Oprogramowania (otrzymywanie aktualizacji) oraz prawa do jego Utrzymywania. Ta kontrola zapewnia, że Oprogramowanie działa tylko na licencjonowanych Komputerach oraz że tylko licencjonowani użytkownicy otrzymują dostęp do usług Technicznych. Rejestracja wymaga prawidłowego numeru seryjnego produktu, konta e-mail w celu odnawiania jej odnawiania i otrzymywania innych informacji.

Niniejsze warunki obejmują rozwiązania i usługi BitDefender dla użytkowników domowych licencjonowane dla użytkownika, w tym związaną dokumentację oraz wszelkie aktualizacje i modyfikacje dostarczonych aplikacji w ramach zakupionej licencji lub wszelkie związane umowy serwisowe zgodnie z definicją w dokumentacji oraz wszelkich kopiach.

Ta umowa licencyjna jest prawnym porozumieniem pomiędzy tobą (osobą indywidualną lub prawną), a firmą BITDEFENDER dotyczącym użytkowania określonego powyżej oprogramowania BITDEFENDER, które obejmuje oprogramowanie komputerowe i usługi oraz może obejmować związane media, drukowane materiały oraz dokumentację „Online” lub elektroniczną („BitDefender”), które chronione są przez amerykańskie i międzynarodowe prawa autorskie oraz międzynarodowe traktaty. Przez zainstalowanie, kopiowanie lub inne użytkowanie programu BitDefender wyrażasz zgodę na związanie się warunkami tej umowy.

Jeżeli nie zgadzasz się na warunki tej umowy, nie instaluj, ani nie używaj programu BitDefender.

Licencja BitDefender. BitDefender jest chroniony przez prawa autorskie, międzynarodowe traktaty oraz inne prawa własności intelektualnej i traktaty. BitDefender jest licencjonowanym produktem i nie podlega dalszej sprzedaży.

PRZYZNANIE LICENCJI. Firma BITDEFENDER udziela tobie i tylko tobie, innym osobom następującej niewyłączonej, ograniczonej, nie podlegającej przeniesieniu, zachowującej opłaty licencyjne, licencji do korzystania z oprogramowania BitDefender.

OPROGRAMOWANIE APLIKACYJNE. Możesz instalować i korzystać z BitDefender na tak wielu komputerach jak to konieczne, z uwzględnieniem ograniczeń wynikających z całkowitej liczby zakupionych licencji. Możesz wykonać jedną dodatkową kopię jako kopię zapasową.

LICENCJA UŻYTKOWNIKA NA KOMPUTERZE. Licencja niniejsza dotyczy oprogramowania BitDefender, które może być zainstalowane na pojedynczym komputerze, który nie zapewnia usług sieciowych. Każdy pierwszy użytkownik może zainstalować to oprogramowanie na pojedynczym komputerze i może wykonać jedną dodatkową kopię na innym urządzeniu jako kopię zapasową. Dopuszczalna ilość pierwotnych użytkowników jest liczbą użytkowników licencji.

WARUNKI LICENCJI. Przyznana licencja rozpoczyna się od daty zakupu programu BitDefender i wygasa na koniec okresu, na jaki została zakupiona.

WYGAŚNIĘCIE. Produkt przestanie działać natychmiast po wygaśnięciu licencji.

UAKTUALNIENIA. Jeżeli BitDefender jest oznakowany jako uaktualnienie, musisz posiadać odpowiednią licencję na użytkowanie produktu określonego przez firmę BITDEFENDER jako uprawnionego do uaktualnień produktu BitDefender. Uaktualnienie BitDefender zastępuje i/lub uzupełnia produkt stanowiący podstawę aktualizacji. Takiego produktu możesz używać tylko zgodnie z warunkami zawartymi w umowie licencyjnej. Jeżeli BitDefender jest uaktualnieniem części pakietu oprogramowania, na który masz przyznaną licencję jako na pojedynczy produkt, BitDefender może być użytkowany i przesyłany wyłącznie jako część takiego pojedynczego pakietu i nie może być przekazywany do użytkowania na więcej niż jednym stanowisku komputerowym. Warunki niniejszej licencji zastępują wszelkie poprzednie umowy, które mogą istnieć między tobą i BITDEFENDER dotyczące oryginalnego produktu lub wynikowego produktu zaktualizowanego.

PRAWA AUTORSKIE. Wszystkie prawa, tytuły własności i korzyści z i do BitDefender oraz wszelkie prawa autorskie BitDefender (włączając, ale nie ograniczając wyłącznie do zdjęć, logo, animacji, wideo, audio, muzyki, tekstu i apletów zawartych w BitDefender), towarzyszące materiały wydrukowane i wszelkie kopie BitDefender są własnością BITDEFENDER. BitDefender jest chroniony przez prawa autorskie i klauzule traktatów międzynarodowych. Dlatego też musisz traktować BitDefender jak każdy inny materiał objęty prawem autorskim. Nie możesz kopiować drukowanych materiałów BitDefender. Kopiując musisz uwzględniać wszystkie uwagi dotyczące praw autorskich w ich pierwotnej i oryginalnej postaci we wszystkich kopiach utworzonych, bez względu na formę w jakiej BitDefender występuje. Nie możesz udzielać sublicencji, wypożyczać, sprzedawać, oddawać w leasing lub współdzielić licencji BitDefender. Nie możesz: wykonywać inżynierii wstecznej, kompilować ponownie, dezasemblować, tworzyć produktów pochodnych, modyfikować, tłumaczyć lub próbować poznać kod źródłowy programu BitDefender.

OGRANICZENIA GWARANCJI. BITDEFENDER gwarantuje, że nośnik, na którym BitDefender jest rozprowadzany będzie pozbawiony błędów przez okres trzydziestu dni od daty dostarczenia tobie BitDefender. BITDEFENDER może według swojego uznania, w ramach gwarancji, jedynie wymienić uszkodzony nośnik na wolny od wad po otrzymaniu uszkodzonego, lub zwrócić pieniądze zapłacone za BitDefender. BITDEFENDER nie gwarantuje, że BitDefender będzie pracował nieprzerwanie, będzie

wolny od błędów lub, że błędy zostaną naprawione. BITDEFENDER nie gwarantuje, że BitDefender spełni twoje oczekiwania.

ZA WYJĄTKIEM, KIEDY JEST TO WYRAŹNIE OKREŚLONE W NINIEJSZEJ UMOWIE, BITDEFENDER NIE UWZGLĘDNI INNYCH GWARANCJI WYRAŹNYCH LUB DOMNIEMANYCH DOTYCZĄCYCH PRODUKTU, UDOSKONAŁEŃ, ZARZĄDZANIA LUB WSPARCIA LUB WSZELKICH INNYCH MATERIAŁÓW (MATERIALNYCH LUB NIEMATERIALNYCH) LUB USŁUG DOSTARCZANYCH Z PRODUKTEM. BITDEFENDER NINIEJSZYM WYRAŹNIE WYŁĄCZA WSZELKIE DOMNIEMANE GWARANCJE I WARUNKI, W TYM BEZ OGRANICZEŃ DOMYŚLNE GWARANCJE PRZYDATNOŚCI DO SPRZEDAŻY, PRZYDATNOŚCI DO OKREŚLONEGO CELU, TYTUŁU, NIEZAKŁÓCANIA, DOKŁADNOŚCI DANYCH, DOKŁADNOŚCI ZAWARTOŚCI INFORMACYJNEJ, INTEGRACJI SYSTEMU ORAZ BRAKU NARUSZENIA PRAW STRON TRZECICH PRZEZ FILTROWANIE, DEASSEMBLIZACJĘ LUB USUWANIE OPROGRAMOWANIA STRON TRZECICH, SPYWARE, ADWARE, CIASTECZEK, EMAILI, DOKUMENTÓW, OGŁOSZEŃ LUB PODOBNYCH, NIEZALEŻNIE OD TEGO CZY WYNIKA Z PRZEPISÓW, PRAWA, SPOSOBU PROWADZENIA DZIAŁALNOŚCI, ZWYCZAJU I PRAKTYKI LUB ZASTOSOWANIA HANDLOWEGO.

ZRZECZENIE SIĘ ODPOWIEDZIALNOŚCI ZA USZKODZENIA: Ktokolwiek użytkuje, testuje lub ocenia BitDefender, ponosi całkowite ryzyko wynikające z jakości i działania BitDefender. W żadnym przypadku BITDEFENDER nie będzie ponosił odpowiedzialności za jakiegokolwiek uszkodzenia, w tym bezpośrednie lub pośrednie uszkodzenia wynikające z użytkowania, działania lub dostarczania BitDefender, nawet jeśli BITDEFENDER był poinformowany o istnieniu lub możliwości pojawienia się takich uszkodzeń.

NIKTÓRE STANY NIE POZWALAJĄ OGRANICZAĆ LUB WYKLUCZAĆ ODPOWIEDZIALNOŚCI ZA PRZYPADKOWE LUB UMYŚLNE USZKODZENIA. TAK WIĘC POWYŻSZE OGRANICZENIA LUB WYKLUCZENIA MOGĄ NIE DOTYCZYĆ CIEBIE.

W ŻADNYM PRZYPADKU ODPOWIEDZIALNOŚĆ BITDEFENDER NIE MOŻE PRZEKROCZYĆ CENY ZAKUPU PRODUKTU BITDEFENDER. Ograniczenia poruszone wyżej będą miały zastosowanie bez względu na to czy akceptujesz, użytkujesz, oceniasz czy testujesz BitDefendera.

WAŻNA INFORMACJA DLA UŻYTKOWNIKÓW. TO OPROGRAMOWANIE NIE JEST ODPORNE NA BŁĘDY I NIE JEST ZAPROJEKTOWANE DO PRACY W NIEBEZPIECZNYM ŚRODOWISKU WYMAGAJĄCY DZIAŁANIA LUB PRACY SAMOISTNIE BEZPIECZNEJ. OPROGRAMOWANIE NIE JEST PRZEZNACZONE DO UŻYTKU W OBSŁUDZE NAWIGACJI LOTNICZEJ, OBIEKTÓW NUKLEARNYCH LUB SYSTEMACH KOMUNIKACJI, SYSTEMACH UZBROJENIA, SYSTEMACH BEZPOŚREDNIEGO LUB POŚREDNIEGO ZABEZPIECZENIA ŻYCIA, KONTROLI RUCHU LOTNICZEGO LUB JAKIEJKOLWIEK APLIKACJI BĄDŹ INSTALACJI, KTÓRYCH BŁĄD MÓGŁBY SPOWODOWAĆ ŚMIERĆ, OBRAŻENIA FIZYCZNE LUB USZKODZENIE WŁASNOŚCI.

ZGODA NA KOMUNIKACJĘ ELEKTRONICZNĄ. BitDefender może wysyłać tobie informacje lub komunikować się odnośnie Oprogramowania oraz Zarządzania wykupionymi usługami oraz aby skorzystać z dostarczonych przez ciebie informacji

("Wiadomości"). BitDefender będzie przysyłał Wiadomości poprzez produkt lub pocztą e-mail na główne zarejestrowane konto e-mail użytkownika, lub będzie zamieszczać Wiadomości na swojej stronie. Akceptując tą Umowę, zgadzasz się na otrzymywanie wszystkich Wiadomości tylko drogą elektroniczną i otrzymujesz dostęp do Wiadomości na Stronie.

TECHNOLOGIA ZBIERANIA DANYCH - BitDefender informuje cię że w określonych programach lub produktach może korzystać z technologii zbierania danych które stanowią tylko informację techniczną (włączając w to podejrzane pliki), aby móc polepszać swoje produkty, zapewniać usługi na odpowiednim poziomie, przystosowywać je i uniemożliwić korzystanie z nielegalnego oprogramowania, zapobiegać powstawaniu szkód spowodowanych przez złośliwe oprogramowanie. Akceptujesz że BitDefender może użyć takiej informacji jako część usług dostarczanych jako produkt w celu ochrony twojego komputera przed wszystkimi typami złośliwego oprogramowania.

Potwierdzasz i akceptujesz że BitDefender może wprowadzać aktualizacje lub poprawki do programu lub produktu, które są automatycznie pobierane na twój komputer.

Poprzez akceptację tej Umowy, zgadzasz się na przesyłanie wykonywalnych plików w celu zeskanowania ich przez serwery BitDefender. Podobnie, w ramach korzystania z oprogramowania musisz udostępnić firmie BitDefender określone dane osobowe. BitDefender informuje cię że będą one (dane osobowe) traktowane zgodnie z obowiązującą legislacją i tak jak to zostało opisane w Polityce Prywatności.

ZBIERANIE DANYCH. Dostęp do strony internetowej przez Użytkownika i nabywanie produktów i usług oraz wykorzystanie narzędzi lub treści poprzez stronę internetową wiąże się z przetwarzaniem danych osobowych. Przestrzeganie prawa związanego z ochroną danych osobowych stanowi dla firmy BitDefender najwyższy priorytet. Czasami, aby uzyskać dostęp do produktów, usług lub narzędzi, użytkownik będzie musiał podać pewne dane osobowe. BitDefender gwarantuje że te dane są traktowane poufnie i zgodnie z obowiązującym prawem ochrony danych osobowych i informacji dla komercyjnych usług elektronicznych.

BitDefender spełnia wymagania prawne dotyczące ochrony danych osobowych, dodatkowo podjęte zostały techniczne i administracyjne kroki aby zagwarantować maksymalne bezpieczeństwo zbieranych danych osobowych.

Deklarujesz że wszystkie dane które udostępniasz są prawdziwe i poprawne i zgadzasz się na poinformowanie BitDefender o jakichkolwiek zmianach w tych danych. Masz prawo sprzeciwić się przetwarzaniu danych które nie są potrzebne do spełnienia umowy i jeśli służą one celom innym niż konserwacja i udoskonalanie produktu.

W przypadku udostępnienia szczegółów dotyczących osób trzecich, BitDefender nie ponosi żadnej odpowiedzialności, użytkownik oprogramowania deklaruje że jest

właścicielem podanych danych i jest jedyną osobą odpowiedzialną prawnie za taki stan rzeczy.

BitDefender, podległe mu jednostki i partnerzy będą przysyłać informacje marketingowe tylko drogą e-mailową lub innymi kanałami komunikacji elektronicznej dla tych użytkowników, którzy zgodzili się na otrzymywanie informacji dotyczących produktów i usług BitDefender lub innych wiadomości.

Polityka prywatności firmy BitDefender gwarantuje prawo do dostępu, sprostowania, usunięcia lub sprzeciwienia się przetwarzaniu danych osobowych powiadamiając firmę poprzez e-mail pod adresem: juridic@bitdefender.com.

UWAGI OGÓLNE. Niniejsza umowa będzie regulowana przez prawo rumuńskie oraz przez międzynarodowe umowy i traktaty dotyczące praw autorskich. Wyłącznym miejscem jurysdykcji i realizacji czynności prawnych mających na celu rozstrzygnięcie wszystkich sporów powstałych w wyniku warunków niniejszej licencji będą sądy rumuńskie.

W przypadku nieważności któregokolwiek postanowienia niniejszej Umowy, nieważność ta nie ma wpływu na ważność pozostałych części Umowy.

BitDefender i logo BitDefender są zastrzeżonymi znakami towarowymi BITDEFENDER. Wszystkie pozostałe zastrzeżone znaki towarowe używane w produkcie lub materiale towarzyszącym należą do odpowiednich właścicieli.

Ważność licencji wygasa natychmiast i bez uprzedzenia w przypadku naruszenia któregokolwiek warunku. Użytkownik nie będzie uprawniony do zwrotu kosztów od BITDEFENDER lub jakiegokolwiek sprzedawcy BitDefender w przypadku wygaśnięcia ważności. Po wygaśnięciu ważności nadal obowiązują warunki dotyczące poufności oraz ograniczeń użytkowania.

BITDEFENDER może w dowolnym momencie dokonać zmiany niniejszych warunków, a nowe warunki będą automatycznie obowiązywać dla odpowiednich wersji oprogramowania dystrybuowanego ze zmienionymi warunkami. W przypadku stwierdzenia nieważności lub nieobowiązania którejkolwiek z części niniejszych warunków, nie ma to wpływu na obowiązywanie pozostałych warunków, które pozostaną ważne i obowiązujące.

W przypadku niejasności lub niespójności między tłumaczeniami niniejszych warunków na inne języki, pierwszeństwo ma wersja angielska wydana przez BITDEFENDER.

Skontaktuj się z BITDEFENDER, 24, Preciziei Boulevard, West Gate Budynek H2, parter, Sektor 6, Bukareszt, Rumunia, lub telefonicznie na numer: 40-21-206.34.70 lub Fax: 40-21-264.17.99, adres email: office@bitdefender.com.

Wstęp

Ta instrukcja obsługi przeznaczona jest dla wszystkich użytkowników, którzy wybrali **BitDefender Antivirus 2010** jako narzędzie bezpieczeństwa dla swojego komputera. Informacje przedstawione w tej instrukcji są przeznaczone dla użytkowników zarówno zaawansowanych jak i początkujących.

Ta książka przedstawia BitDefender Antivirus 2010, prowadzi przez proces jego instalacji i konfiguracji. Dzięki niej uzyskasz informacje jak skonfigurować BitDefender Antivirus 2010, jak go uaktualnić i dostosować do własnych wymagań. Nauczysz się optymalnie wykorzystywać BitDefender.

Życzymy Państwu miłej i owocnej nauki.

1. Znaki umowne stosowane w instrukcji

1.1. Konwencje Typograficzne

Aby ta książeczka była bardziej czytelna, użyto kilka stylów tekstu. Ich wygląd i znaczenie zostały przedstawione na poniższej liście.

Wygląd	Opis
sample syntax	Przykłady i niektóre dane liczbowe są wydrukowane czcionką szeryfową.
http://www.bitdefender.com	Nawiązania (linki) URL odnoszą do innych miejsc takich jak serwery http czy ftp.
sales@bitdefender.com	Adresy Email zostały umieszczone w tekście dla informacji kontaktowych.
„Wstęp” (p. xiv)	To odnośnik do linka wewnętrznego umiejscowionego w dokumencie.
filename	Pliki i foldery są wydrukowane czcionką szeryfową.
option	Wszystkie opcje są wydrukowane pogrubioną czcionką .
sample code listing	Kody są wydrukowane czcionką szeryfową.

1.2. Uwagi

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



Notatka

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



WAŻNE

Ten znak wymaga Państwa uwagi, nie zaleca się pominięcia go. Zazwyczaj podaje on wiadomości nie krytyczne, ale znaczące.



Ostrzeżenie

Zaznacza wiadomości krytyczne, które należy uważnie przeczytać. Nic złego nie może się stać jeśli podążasz za tymi wskazówkami. Trzeba przeczytać i zrozumieć, ponieważ ten znak opisuje ryzykowną operację.

2. Struktura Książki

Instrukcja składa się z kilku części zawierających główne tematy. Ponadto dostępny jest słownik, który wyjaśnia niektóre terminy techniczne.

Instalacja i Usuwanie. Instrukcje krok po kroku dotyczące instalacji oprogramowania BitDefender na komputerze osobistym. Zaczynając od podstaw prawidłowej instalacji, jesteś prowadzony(a) przez jej cały proces. Na końcu omówiono procedurę odinstalowywania programu.

Pierwsze Kroki. Zawiera wszystkie informacje potrzebne do rozpoczęcia korzystania z BitDefendera. Przedstawia interfejs użytkownika programu, wyjaśnia jak naprawiać zagadnienia, skonfigurować proste ustawienia i zarejestrować produkt.

Tryb Średniozaawansowany. Przedstawia Tryb Średniozaawansowany interfejsu użytkownika BitDefender.

Tryb Eksperta. Szczegółowa prezentacja interfejsu użytkownika BitDefender w Trybie Eksperta. Nauczysz się jak konfigurować i używać wszystkie moduły BitDefender aby chronić swój komputer przed wszystkimi rodzajami zagrożeń (wirusy, spyware, rootkity, itd.)

Integracja z Windows i Oprogramowaniem Third-Party. Pokazuje jak korzystać z opcji BitDefender w menu kontekstowym Windows oraz pasków narzędziowych zintegrowanych w innych obsługiwanych programach.

Jak to zrobić. Dostarcza procedur aby szybko wykonywać większość zadań w BitDefender.

Rozwiązywanie Problemów i Uzyskiwanie Pomocy. Gdzie zajrzeć i kogo zapytać o radę kiedy coś idzie nie tak, jak powinno.

CD Ratunkowy BitDefender. Opis ratunkowej płyty CD programu BitDefender. Ułatwia zrozumienie i korzystanie z funkcji umożliwiającej uruchamianie systemu operacyjnego płyty CD.

Słownik. Słownik zawiera terminy techniczne i te mniej znane, które pojawiają się w tej książeczce.

3. 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 ją w celu dostarczenia jak najlepszej dokumentacji.

Prosimy powiadomić nas na ten adres documentation@bitdefender.com.



WAŻNE

Wszystkie maile związane z dokumentacją prosimy pisać w języku Angielskim abyśmy mogli szybko je przeanalizować.

Instalacja i Usuwanie

1. Wymagania Systemowe

Możesz zainstalować BitDefender Antywirus 2010 tylko na komputerach z następującymi systemami operacyjnymi:

- Windows XP (32/64 bit) z Service Pack 2 lub wyższy
- Windows Vista (32/64 bit) lub Windows Vista z Service Pack 1 lub wyższym
- 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

- 450 MB wolnego miejsca na twardym dysku
- procesor 800 MHz
- Pamięć RAM:
 - ▶ 512 MB dla Windows XP
 - ▶ 1 GB dla Windows Vista i Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (dostępny również w instalatorze)

1.2. Rekomendowane Wymagania Sprzętowe

- 600 MB wolnego miejsca na twardym dysku
- 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 (lub nowszy)
- .NET Framework 1.1 (dostępny również w instalatorze)

1.3. Obsługiwane oprogramowanie

Ochrona antyphishingowa jest zapewniana dla:

- Internet Explorer 6.0 (lub nowszy)
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Windows Live Messenger 8

Szyfrowanie komunikatorów (IM) jest zapewniane dla:

- Yahoo Messenger 8.5
- Windows Live Messenger 8

2. Przygotowywanie do Instalacji

Zanim zainstalujesz BitDefender Antivirus 2010, 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.

3. Instalacja BitDefendera

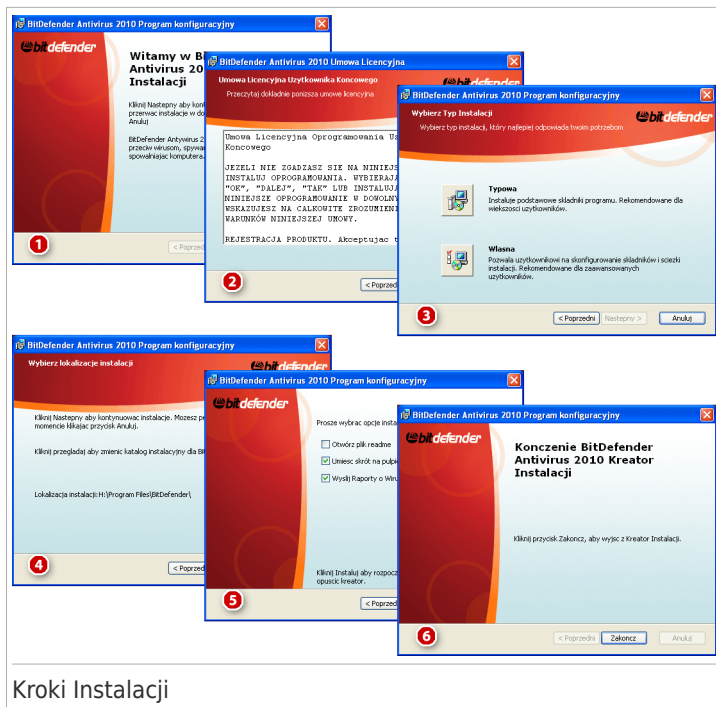
Możesz zainstalować BitDefender z płyty instalacyjnej CD BitDefender lub korzystając z pliku instalacyjnego pobranego na twój komputer ze strony WWW BitDefender lub innych autoryzowanych stron (np. strony oficjalnego partnera BitDefender lub sklepu internetowego). Możesz pobrać plik instalacyjny ze strony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

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

Jeśli nie pojawi się napis powitalny, przejdź do katalogu `Products\Antivirus\install\en\` na płycie instalacyjnej i kliknij dwukrotnie na `runsetup.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 zostanie zatwierdzona, pojawi się okno instalatora. Poniższy obrazek przedstawia poszczególne kroki instalatora.



Wykonaj następujące kroki aby zainstalować BitDefender Antivirus 2010:

1. Kliknij **Dalej**. Możesz przerwać instalację w dowolnym momencie klikając na **Anuluj**.

BitDefender Antywirus 2010 powiadomi Cię, jeżeli masz zainstalowane na komputerze inne produkty antywirusowe. Kliknij **Usuń** aby odinstalować odpowiedni produkt. Jeżeli chcesz kontynuować bez usuwania wykrytych produktów, kliknij **Dalej**.



Ostrzeżenie

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

2. Proszę przeczytać Umowę Licencyjną i kliknąć **Zgadzam Się**.



WAŻNE

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

3. Wybierz typ instalacji, jaka ma zostać przeprowadzona.
 - **Typowa** - rozpoczyna instalację natychmiast, korzystając z domyślnych opcji instalacji. Jeśli wybierzesz tę opcję, przejdź do Kroku 6.
 - **Własna** - aby skonfigurować opcje instalacji i zainstalować program. Ta opcja pozwala na zmianę ścieżki instalacji.
4. Domyślnie, BitDefender Antivirus 2010 zostanie zainstalowany w folderze C:\Program Files\BitDefender\BitDefender 2010. Jeżeli chcesz wybrać inny folder instalacji, kliknij **Przeglądaj** i wybierz folder w którym chcesz zainstalować BitDefendera.

Kliknij **Dalej**.

5. Wybierz opcje instalacji. Niektóre opcje są wybrane domyślnie:
 - **Otwórz plik readme** - aby otworzyć plik readme na końcu instalacji.
 - **Utwórz skrót na pulpicie** - aby umieścić skrót do BitDefender Antivirus 2010 na pulpicie na końcu instalacji.
 - **Wyciągnij CD po zakończeniu instalacji** - ta opcja pojawi się podczas instalacji produktu z płyty CD.
 - **Zablokuj Caching DNS** - aby zablokować przechowywanie wpisów DNS (Domain Name System). Usługa Klienta DNS może zostać użyta przez szkodliwe oprogramowania do wysyłania informacji przez sieć bez twojej zgody.
 - **Wyłącz Windows Defender** wyłącza Windows Defender; opcja ta pojawia się tylko w Windows Vista.

Kliknij **Instaluj** aby rozpocząć instalację programu. Jeśli nie ma zainstalowanego .NET Framework 1.1 to zostanie on zainstalowany przed BitDefenderem.

6. Poczekać aż instalacja się zakończy i kliknij **Zakończ**. Możesz zostać poproszony o zrestartowanie systemu, aby zakończyć proces instalacji. Zalecamy wybranie tej opcji.



WAŻNE

Po zakończeniu instalacji oraz restarcie komputera, pojawią się **kreатор rejestracji** oraz **kreатор konfiguracji**. Przejdź przez wszystkie kreatory aby zarejestrować i skonfigurować BitDefender Antivirus 2010 i stworzyć konto BitDefender.

Jeżeli zaakceptowałeś ustawienia domyślne dla ścieżki instalacji, w Program Files zobaczysz nowy folder o nazwie BitDefender, który zawiera podfolder BitDefender 2010.

3.1. Kreator rejestracji

Przy pierwszym uruchomieniu komputera po instalacji pojawi się kreator rejestracji. Ten kreator pomoże tobie zarejestrować BitDefendera oraz skonfigurować konto BitDefender.

MUSISZ utworzyć konto BitDefender aby otrzymywać aktualizacje BitDefendera. Konto BitDefender daje tobie również dostęp do darmowej pomocy technicznej oraz specjalnych ofert i promocji. Jeśli zgubisz klucz licencyjny BitDefendera, możesz się zalogować na swoje konto na <http://myaccount.bitdefender.com> aby go odzyskać.



Notatka

Jeżeli nie chcesz przechodzić kreatora kliknij **Anuluj**. Możesz otworzyć kreator rejestracji w każdej chwili klikając **Zarejestruj** na dole okna.

3.1.1. Krok 1 - Zarejestruj BitDefender Antivirus 2010

BitDefender Antivirus 2010

Kreator rejestracji

Rejestracja BitDefender

☐ Chcę wypróbować BitDefender

☒ Chcę zarejestrować BitDefender z kluczem licencyjnym

Wprowadź klucz licencyjny:

Klucz licencji: **Zarejestruj teraz**

[Nie masz klucza licencyjnego? Kup go teraz!](#)

Aby dowiedzieć się więcej o dowolnej opcji wyświetlanej w Interfejsie Użytkownika BitDefender, nakeruj kursor myszy na okno, a pojawi się odpowiednia informacja pomocnicza.

Anuluj **Wstecz** **Dalej**

Rejestracja

BitDefender Antywirus 2010 posiada 30-dniowy okres próbny. Aby kontynuować testowanie produktu, wybierz **Chcę wypróbować BitDefender** i kliknij **Dalej**.

Aby zarejestrować BitDefender Antivirus 2010:

1. Wybierz **Chcę zarejestrować BitDefender z kluczem licencyjnym**.
2. 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.

3. Kliknij **Zarejestruj Teraz**.

4. Kliknij **Dalej**.

Jeśli w systemie zostanie wykryty ważny klucz licencyjny BitDefender, możesz dalej korzystać z tego klucza klikając na **Dalej**.

3.1.2. Krok 2 - Utwórz Konto BitDefender

Tworzenie Konta

Jeśli nie chcesz zakładać konta BitDefender w tym momencie, wybierz **Zarejestruj Później** i kliknij **Zakończ**. W przeciwnym razie postępuj w zależności od sytuacji:

- „Nie mam osobistego konta na MyBitDefender” (p. 10)
- „Już posiadam konto BitDefender” (p. 10)



WAŻNE

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.

Nie mam osobistego konta na MyBitDefender

Aby pomyślnie utworzyć konto BitDefender, podążaj według tych kroków:

1. Wybierz **Stwórz nowe konto**.
2. Wprowadź wymaganą informację w odpowiednich polach. Dane które teraz wprowadzisz pozostaną tajne.
 - **Adres email** - wpisz swój adres email.
 - **Hasło** - wpisz hasło dla konta BitDefender. Hasło musi zawierać od 6 do 16 znaków.
 - **Powtórz hasło** - wpisz ponownie wcześniej podane hasło.



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. Wybierz jedną z dostępnych w menu opcji:
 - **Wysyłaj mi wszystkie wiadomości**
 - **Wysyłaj mi tylko informacje o produktach**
 - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Utwórz**.
5. Kliknij **Zakończ** aby zakończyć kreator.
6. **Przeprowadź aktywację swojego konta**. 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 **Zakończ** aby zakończyć kreator.

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

1. Wybierz **Zaloguj się (poprzednio stworzone 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. Wybierz jedną z dostępnych w menu opcji:
 - **Wysyłaj mi wszystkie wiadomości**
 - **Wysyłaj mi tylko informacje o produktach**
 - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Zaloguj się**.
5. Kliknij **Zakończ** aby zakończyć kreator.

3.2. Kreator Konfiguracji

Gdy zakończysz kreator rejestracji, pojawi się kreator konfiguracji. Ten kreator pomaga skonfigurować główne ustawienia BitDefender i interfejs użytkownika tak, aby lepiej odpowiadały twoim wymaganiom. Na końcu kreatora, możesz zaktualizować pliki programu i sygnatury wirusów a następnie przeskanować pliki systemu i aplikacje aby upewnić się że nie zostały zainfekowane.

Ten kreator składa się z kilku prostych kroków. Liczba kroków zależy od podejmowanych wyborów. Wszystkie możliwe kroki są tutaj przedstawione, wraz z informacją kiedy podejmowane wybory mogą zmniejszyć ich liczbę.

Wykonanie tego kreatora nie jest obowiązkowe; jednak, zalecamy aby to zrobić i oszczędzić czas oraz mieć pewność że twój system jest bezpieczny nawet przed instalacją BitDefender Antywirus 2010. Jeżeli nie chcesz przechodzić kreatora kliknij **Anuluj**. Gdy otworzysz interfejs użytkownika BitDefender powiadomi ciebie o komponentach które powinieneś skonfigurować.

3.2.1. Krok 1 - Wybierz Profil Użytkowania



Kliknij na przycisk który najlepiej opisuje czynności wykonywane na tym komputerze (profil użytkowania).

Opcje	Opis
Typowe	Kliknij tutaj, jeśli ten komputer jest używany głównie do przeglądania Internetu i zastosowań multimedialnych.
Gracz	Kliknij tutaj, jeśli ten komputer jest używany głównie do gier.
Niestandardowy	Kliknij tutaj, jeśli chcesz skonfigurować wszystkie główne ustawienia BitDefendera.

Możesz później zresetować profil użytkowania korzystając z interfejsu programu.

3.2.2. Step 2 - Opisz Komputer



Wybierz opcje, które odnoszą się do tego komputera:

- **Ten komputer znajduje się w sieci domowej.** Wybierz tę opcję, jeśli chcesz zarządzać oprogramowaniem BitDefender zainstalowanym na tym komputerze zdalnie (z innego komputera). Dodatkowy krok pozwoli ci na skonfigurowanie modułu Zarządzania Siecią Domową.
- **Ten komputer to laptop.** Wybierz tę opcję jeśli chcesz aby Tryb Laptopa był domyślnie włączony. W Trybie Laptopa, wszystkie zaplanowane zadania skanowania nie są wykonywane, ponieważ ich praca mogłaby wpłynąć na większe zużycie zasobów i co się z tym wiąże, energii elektrycznej.

Kliknij **Dalej** aby kontynuować.

3.2.3. Krok 3 - Wybierz Interfejs Użytkownika



Aby wybrać wygląd interfejsu użytkownika, kliknij na przycisk który najlepiej opisuje twoje umiejętności korzystania z komputera. 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.

Tryb	Opis
Tryb Podstawowy	Odpowiedni dla początkujących oraz osób, które chcą chronić swój komputer bez dodatkowych interakcji z programem. Jedynie co musisz zrobić, to naprawić zagrożenia 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.
Tryb Średniozaawansowany	Dla użytkowników o przeciętnym poziomie wiedzy na temat komputera, ten tryb stanowi rozwinięcie trybu podstawowego. Możesz naprawić zagrożenia osobno i wybrać które z nich mają być monitorowane. Dodatkowo, możesz zdalnie

Tryb	Opis
Tryb 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.

3.2.4. Krok 4 - Skonfiguruj Sieć BitDefender



Notatka

Ten krok pojawia się tylko jeśli wybrano, czy komputer jest podłączony do sieci domowej w Kroku 2.

BitDefender Kreator Konfiguracji

Konfiguracja Zarządzania Siecią Domową

BitDefender Antivirus 2010 zawiera nowy komponent, Zarządzanie Siecią Domową, który pozwala na tworzenie wirtualnych sieci komputerów, tak aby zarządzać wszystkimi produktami BitDefender zainstalowanymi w tych sieciach. Możesz działać jako administrator sieci, którą stworzyłeś lub być częścią sieci zarządzanej z innego komputera.

☒ Włącz Sieć Domową

Hasło Zarządzania Siecią Domową:

Wpisz ponownie hasło:

Aby dowiedzieć się więcej o dowolnej opcji wyświetlanej w Interfejsie Użytkownika BitDefender, nakieruj kursor myszy na okno, a pojawi się odpowiednia informacja pomocnicza.

Anuluj Wstecz Dalej

Konfiguracja Sieci BitDefender

BitDefender umożliwia tobie tworzenie wirtualnych sieci z komputerów domowych oraz zarządzać produktami BitDefender zainstalowanymi w tej sieci.

Jeżeli chcesz aby ten komputer był częścią Domowej Sieci BitDefender, wykonaj następujące kroki:

1. Wybierz **Włącz Sieć Domową**.
2. Wpisz to samo hasło administracyjne w każdym polu edycji. Hasło umożliwia administratorowi zarządzanie tym produktem BitDefendera z innego komputera.

Kliknij **Dalej** aby kontynuować.

3.2.5. Krok 5 - Wybierz Zadania do Uruchomienia



Skonfiguruj BitDefender aby mógł wykonywać ważne zadania w celu zabezpieczenia twojego systemu. Dostępne są następujące opcje:

- **Aktualizuj BitDefender i wykonaj zadanie szybkiego skanowania systemu teraz** - podczas następnego kroku, sygnatury wirusów i pliki programu BitDefender zostaną zaktualizowane w celu ochrony twojego komputera przed najnowszymi zagrożeniami. Zaraz po zakończeniu aktualizacji, BitDefender przeskanuje pliki w katalogach Windows i Program Files aby upewnić się, że nie są zainfekowane. Te foldery zawierają pliki systemu operacyjnego i zainstalowanych aplikacji, które najczęściej infekowane są w pierwszej kolejności.
- **Uruchom Skanowanie Systemu codziennie o 2 rano** - ustawia BitDefender aby wykonywał skanowanie komputera codziennie o 2 rano. Aby zmienić czas kiedy uruchomione jest skanowanie, kliknij menu i wybierz pożądany czas uruchomienia. Jeśli komputer jest wyłączony w momencie, kiedy ma odbyć się zaplanowane zadanie, zostanie ono przeprowadzone po jego następnym uruchomieniu.



Notatka

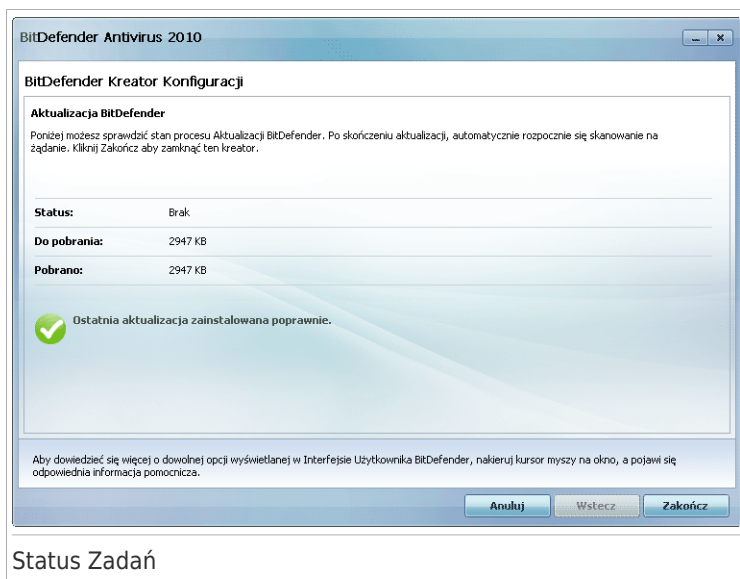
Jeśli chcesz w przyszłości zmienić czas kiedy ma zostać przeprowadzane skanowanie, wykonaj następujące kroki:

1. Otwórz BitDefender i przestaw interfejs użytkownika na Tryb Eksperta.
2. Kliknij **Antyvirus** w menu po lewej stronie.
3. Kliknij zakładkę **Skanowanie**.
4. Kliknij prawym przyciskiem na zadanie **skanowanie Systemu** i wybierz **Harmonogram**. Pojawi się nowe okno.
5. Jeśli chcesz, zmień częstotliwość i czas uruchamiania.
6. Kliknij **Zastosuj** aby zapisać zmiany.

Zalecamy uruchomienie tych opcji przed przejściem do następnego kroku dla zapewnienia bezpieczeństwa systemu. Kliknij **Dalej** aby kontynuować.

Jeśli odznaczysz pierwsze pole, żadne zadanie nie będzie wykonane w ostatnim kroku tego kreatora. Kliknij **Zakończ** aby zakończyć kreator.

3.2.6. Krok 6 - Zakończenie



Poczekaj aż BitDefender zaktualizuje swoje silniki antywirusowe i sygnatury wirusów. Po zakończeniu aktualizacji, uruchomi się szybkie skanowanie systemu. Skanowanie zostanie wykonane w tle. Możesz zaobserwować, że ikona z postępem skanowania pojawiła się w **zasobniku systemowym na pasku zadań**. Możesz kliknąć tę ikonę aby otworzyć okno skanowania i zobaczyć jego postępy.

Kliknij **Zakończ** aby zakończyć kreator. Nie musisz czekać aż skanowanie się zakończy.



Notatka

Skanowanie potrwa kilka minut. Kiedy się zakończy, otwórz okno skanowania i sprawdź rezultaty aby zobaczyć czy system jest czysty. Jeśli jakieś wirusy zostały wykryte podczas skanowania, powinieneś od razu otworzyć okno BitDefender i wykonać pełne skanowanie systemu.

4. Aktualizacja

Jeśli korzystasz z BitDefender Antivirus 2010 beta lub starszych wersji 2008 lub 2009, możesz je zaktualizować do wersji BitDefender Antivirus 2010.

Są dwa sposoby na wykonanie aktualizacji (upgrade):

- Zainstaluj BitDefender Antivirus 2010 bezpośrednio na starą wersję. Jeśli instalujesz bezpośrednio na wersję 2009, Kwarantanna jest importowana 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 Antivirus 2010, podążaj za ścieżką w menu startowym Windows: **Start** → **Programy** → **BitDefender 2010** → **Napraw lub Usuń**.

Będziesz proszony o potwierdzenie twojego wyboru przez kliknięcie **Dalej**. Pojawi się nowe okno, w którym będziesz mógł wybrać:

- **Napraw** - reinstaluje wszystkie składniki programu z poprzedniej instalacji.

Jeśli wybierzesz naprawę BitDefendera, pojawi się nowe okno. Kliknij **Napraw** aby rozpocząć proces naprawy.

Zrestartuj komputer, gdy zostaniesz o to poproszony, a następnie kliknij **Instaluj** aby przeinstalować BitDefender Antivirus 2010.

Po zakończeniu procesu instalacji pojawi się nowe okno. Kliknij **Zakończ**.

- **Usuń** - aby usunąć zainstalowane składniki.



Notatka

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

Jeśli wybierzesz usunięcie BitDefendera, pojawi się nowe okno.



WAŻNE

Tylko dla Windows Vista! Po usunięciu BitDefendera, nie będziesz już chroniony przed zagrożeniami typu wirusy i spyware. Jeżeli chcesz aby Windows Defender był aktywny po odinstalowaniu BitDefendera, wybierz odpowiednią opcję.

Kliknij **Usuń** aby rozpocząć usuwanie BitDefender Antivirus 2010 z twojego komputera.

Po zakończeniu procesu odinstalowywania, pojawi się nowe okno. Kliknij **Zakończ**.



Notatka

Po zakończeniu procesu odinstalowywania, zalecamy usunięcie folderu BitDefender z folderu Program Files.

Pierwsze Kroki

6. Przegląd

Po zainstalowaniu BitDefendera twój komputer jest chroniony. Jeśli nie ukończyłeś **kreatora konfiguracji**, musisz otworzyć BitDefender i jak najszybciej naprawić bieżące problemy. 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. 48).

6.1. Otwieranie BitDefender

Aby wejść do głównego interfejsu BitDefender Antivirus 2010, użyj menu Start, klikając kolejno **Start** → **Programy** → **BitDefender 2010** → **BitDefender Antywirus 2010** lub szybciej, klikając dwa razy ikonę  w zasobniku systemowym na pasku zadań.

6.2. Tryby Widoku Interfejsu Użytkownika

BitDefender Antivirus 2009 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.

Tryb	Opis
Tryb 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

Tryb	Opis
	aktualizacja plików BitDefendera i sygnatur wirusów lub skanowanie komputera.
Tryb Średniozaawansowany	Dla użytkowników o przeciętnym poziomie wiedzy na temat komputera, ten tryb stanowi rozwinięcie trybu podstawowego. 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.
Tryb 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 interfejsu użytkownika jest wybierany w kreatorze konfiguracji. Ten kreator pojawia się po kreatorze rejestracji, pierwszy raz po uruchomieniu komputera po instalacji produktu. Jeśli przerwiesz kreator konfiguracji, tryb interfejsu użytkownika zostanie ustawiony domyślnie na Średniozaawansowany.

Aby zmienić tryb użytkownika, wykonaj następujące kroki:

1. Otwórz BitDefender.
2. Kliknij na przycisk **Ustawienia** w górnym prawym rogu okna.
3. W kategorii Ustawienia Interfejsu Użytkownika, kliknij na strzałkę  na przycisku i wybierz pożądany tryb z menu.
4. Kliknij **OK** aby zapisać i zastosować zmiany.

6.2.1. Tryb Początkujący

Jeśli jesteś początkującym użytkownikiem komputera, uruchomienie interfejsu w Trybie Podstawowym może być najbardziej adekwatnym wyborem. Ten tryb jest prosty i wymaga minimalnej interakcji ze strony użytkownika.



Tryb Początkujący

Okno jest podzielone na cztery główne sekcje:

- **Stan Zabezpieczeń** informuje użytkownika o zagrożeniach mogących wpływać niekorzystnie na bezpieczeństwo komputera i pomagają je naprawić. Klikając na **Napraw Wszystkie Zagadnienia** uruchomisz kreator pozwalający na usunięcie wszystkich problemów dotyczących bezpieczeństwa twojego komputera. Aby uzyskać więcej informacji, przejdź do „*Naprawianie*” (p. 37).
- **Chroń Swoj PC** - tutaj znajdziesz potrzebne zadania, które pomogą Ci lepiej chronić Twój komputer i dane. Dostępne zadania które możesz wykonać różnią się w zależności od wybranego profilu użytkownika.
 - ▶ Przycisk **Skanuj Teraz** uruchamia standardowe skanowanie systemu w poszukiwaniu wirusów, oprogramowania szpiegującego i innych złośliwych programów. Pojawi się kreator skanera antywirusowego i poprowadzi Cię przez proces skanowania. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Skanowania Antywirusowego*” (p. 53).
 - ▶ Przycisk **Aktualizuj Teraz** pozwala zaktualizować sygnatury wirusów i pliki programu BitDefender. Pojawi się nowe okno w którym możesz obserwować status aktualizacji. Jeśli wykryto aktualizacje, są one automatycznie pobierane i instalowane na komputerze.
 - ▶ Kiedy wybrany zostanie **Typowy** profil, przycisk **Sprawdzenie Podatności** uruchamia kreator, który pozwala odnaleźć i naprawić dziury w systemie, takie jak nieaktualne oprogramowanie albo brakujące aktualizacje Windows. Aby

uzyskać więcej informacji, odwołaj się do sekcji „*Kreator Sprawdzania Podatności*” (p. 65).

- ▶ Kiedy zostanie wybrany profil **Gracza**, przycisk **Włącz/Wyłącz Tryb Gry** pozwala na włączenie/wyłączenie **Trybu Gry**. Tryb Gry tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na wydajność systemu.
- **Konserwacja Twojego Komputera** - tutaj odnajdziesz dodatkowe zadania pomagające lepiej chronić twój komputer i dane.
 - ▶ **Głębokie Skanowanie Systemu** uruchamia dokładne skanowanie systemu wyszukując wszystkie typy złośliwego oprogramowania.
 - ▶ **Skanowanie Moich Dokumentów** skanuje najczęściej używane foldery: Moje Dokumenty i Pulpit. Dzięki temu twoje dokumenty są bezpieczne i masz pewność że aplikacje uruchamiane przy starcie są czyste.
 - ▶ **Skaner Autologowania** skanuje elementy uruchamiane podczas logowania do Windows.
- **Profil Użytkownika** pokazuje aktualnie wybrany profil użytkownika. Profil użytkownika odzwierciedla główne czynności wykonywane na komputerze. W zależności od tego profilu, interfejs programu jest zorganizowany tak, aby umożliwić szybki dostęp do preferowanych zadań.

Jeśli chcesz przełączyć się na inny profil lub edytować bieżący, kliknij na profil i podążaj według zaleceń **kreatora konfiguracji**.

W prawym górnym rogu okna, możesz zobaczyć przycisk **Ustawienia**. Otwiera on okno, gdzie możesz zmienić tryb interfejsu użytkownika i odblokować lub zablokować główne ustawienia programu BitDefender. Aby uzyskać więcej informacji, odwołaj się do „*Konfigurowanie Ustawień Podstawowych*” (p. 41).

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

Link	Opis
Kup/Odnów	Otwiera stronę na której możesz zakupić klucz licencyjny dla twojego produktu BitDefender Antivirus 2010.
Rejestracja	Pozwala tobie wpisanie nowego klucza rejestracyjnego lub zobaczenie aktualnego klucza licencyjnego oraz status rejestracji.
Pomoc & Wsparcie	Umożliwia dostęp do pliku pomocy który pokazuje jak korzystać z BitDefendera.

6.2.2. Tryb Średniozaawansowany

Przeznaczony dla użytkowników, którzy posiadają już pewną wiedzę z zakresu zabezpieczeń komputerowych, Tryb Średniozaawansowany to prosty interfejs

umożliwiający dostęp do wszystkich modułów na podstawowym poziomie. Wymaga śledzenia komunikatów i alarmów systemowych oraz umiejętności radzenia sobie z nimi.



Tryb Średniozaawansowany

Okno Trybu Średniozaawansowanego składa się z pięciu zakładek. Poniższa tabela skrótkowo opisuje każdą z nich. Aby uzyskać więcej informacji, odwołaj się do „Tryb Średniozaawansowany” (p. 72) części podręcznika użytkownika.

Zakładka	Opis
Panel	Wyświetla stan bezpieczeństwa twojego systemu i pozwala zresetować profil użytkownika.
Antywirus	Pokazuje status modułu antywirusowego który pomaga zachować BitDefendera aktualnego oraz komputer wolny od wirusów.
Antyphishing	Wyświetla stan modułów które chronią twój system przeciwko atakom phisingu (kradzież danych osobowych) kiedy jesteś online.
Podatności	Pokazuje status modułu podatności który pomaga mieć najważniejsze oprogramowanie na komputerze aktualne. Tutaj możesz łatwo naprawić wszystkie problemy które mogą mieć wpływ na bezpieczeństwo twojego komputera.

Zakładka	Opis
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.

W prawym górnym rogu okna, możesz zobaczyć przycisk **Ustawienia**. Otwiera on okno, gdzie możesz zmienić tryb interfejsu użytkownika i odblokować lub zablokować główne ustawienia programu BitDefender. Aby uzyskać więcej informacji, odwołaj się do „*Konfigurowanie Ustawień Podstawowych*” (p. 41).

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

Link	Opis
Kup/Odnów	Otwiera stronę na której możesz zakupić klucz licencyjny dla twojego produktu BitDefender Antivirus 2010.
Rejestracja	Pozwala tobie wpisanie nowego klucza rejestracyjnego lub zobaczenie aktualnego klucza licencyjnego oraz status rejestracji.
Otrzymywanie pomocy	Pozwala tobie skontaktowanie się z Pomocą Techniczną BitDefendera.
Pomoc	Umożliwia dostęp do pliku pomocy który pokazuje jak korzystać z BitDefendera.
Pokaż Dzienniki	Pozwala tobie zobaczyć szczegółową historię wszystkich zadań przeprowadzonych przez BitDefendera na twoim systemie.

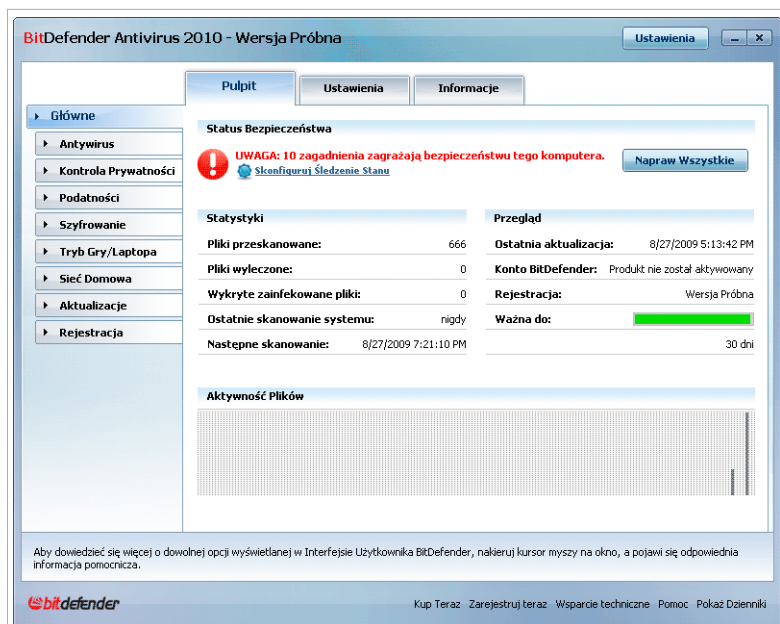
6.2.3. Tryb Eksperta

Tryb Eksperta umożliwia kontrolę nad każdym komponentem BitDefendera. Tutaj skonfigurujesz swój BitDefender w najdrobniejszych szczegółach.



Notatka

Tryb Eksperta jest odpowiedni dla użytkowników, którzy posiadają ponadprzeciętne umiejętności, którzy wiedzą jakie na jakie typy zagrożeń jest wystawiony komputer i jak działają programy zabezpieczające.



Tryb Eksperta

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. Poniższa tabela krótko opisuje każdy z modułów. Aby uzyskać więcej informacji, odwołaj się do „Tryb Eksperta” (p. 93) części podręcznika użytkownika.

Moduł	Opis
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.
Kontrola Prywatności	Pozwala tobie zapobiec kradzieży danych z twojego komputera oraz chroni twoją prywatność kiedy korzystasz z internetu.
Podatności	Pozwala tobie bieżące aktualizowanie najważniejszego oprogramowania na komputerze.

Moduł	Opis
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	Pozwala tobie na skonfigurowanie i zarządzanie kilkoma komputerami w sieci domowej.
Aktualizacja	Pozwala tobie na uzyskanie najnowszych aktualizacji, zaktualizować produkt oraz szczegółowo skonfigurować proces aktualizacji.
Rejestracja	Umożliwia rejestrację BitDefender Antivirus 2010, zmianę klucza licencyjnego lub założenie konta BitDefender.

W prawym górnym rogu okna, możesz zobaczyć przycisk **Ustawienia**. Otwiera on okno, gdzie możesz zmienić tryb interfejsu użytkownika i odblokować lub zablokować główne ustawienia programu BitDefender. Aby uzyskać więcej informacji, odwołaj się do „*Konfigurowanie Ustawień Podstawowych*” (p. 41).

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

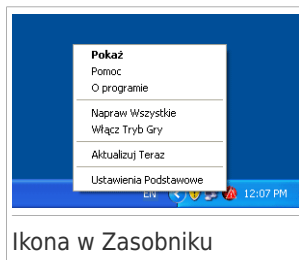
Link	Opis
Kup/Odnów	Otwiera stronę na której możesz zakupić klucz licencyjny dla twojego produktu BitDefender Antivirus 2010.
Rejestracja	Pozwala tobie wpisanie nowego klucza rejestracyjnego lub zobaczenie aktualnego klucza licencyjnego oraz status rejestracji.
Otrzymywanie pomocy	Pozwala tobie skontaktowanie się z Pomocą Techniczną BitDefendera.
Pomoc	Umożliwia dostęp do pliku pomocy który pokazuje jak korzystać z BitDefendera.
Pokaż Dzienniki	Pozwala tobie zobaczyć szczegółową historię wszystkich zadań przeprowadzonych przez BitDefendera na twoim systemie.

6.3. 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 Antivirus 2010.
- **O programie** - otwiera okno, w którym możesz przeczytać o BitDefenderze i gdzie szukać pomocy jeśli zdarzy się coś niespodziewanego.
- **Napraw Wszystkie Zagadnienia** - pomaga usunąć wszystkie problemy z zabezpieczeniami. Jeśli ta opcja jest niedostępna, nie ma żadnych problemów, które należałoby naprawić. Aby uzyskać więcej informacji, przejdź do „*Naprawianie*” (p. 37).
- **Włącz/Wyłącz Tryb Gry** - aktywuje/deaktywuje **Tryb Gry**.
- **Zaktualizuj Teraz** - uruchamia aktualizację. Pojawi się nowe okno w którym możesz obserwować status aktualizacji.
- **Podstawowe Ustawienia** - otwiera okno w którym możesz zmienić tryb interfejsu użytkownika i odblokować lub zablokować główne ustawienia programu. Aby uzyskać więcej informacji, odwołaj się do „*Konfigurowanie Ustawień Podstawowych*” (p. 41).



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

- **Czerwony trójkąt ze znakiem wykrzyknika:** Krytyczne zagrożenia wpływające na bezpieczeństwo systemu. Wymagają natychmiastowej naprawy.
- **Żółty trójkąt ze znakiem wykrzyknika:** Nie-krytyczne zagrożenia wpływają na bezpieczeństwo twojego systemu. Powinieneś sprawdzić i naprawić je przy najbliższej okazji.
- **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.

6.4. Pasek Aktywności Skanera

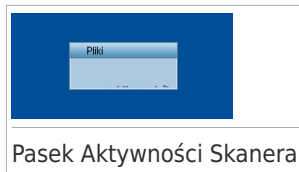
Okienko czynności skanowania jest graficznym odzwierciedleniem wykonywanych czynności skanowania na twoim systemie. To małe okienko jest domyślnie dostępne tylko w **Trybie Eksperta**.

Zielone linie (**Pliki**) pokazują ilość przeskanowanych plików/sek w skali od 0 do 50.



Notatka

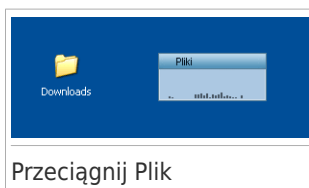
Pasek Aktywności Skanowania powiadomi cię kiedy ochrona w czasie rzeczywistym zostanie wyłączona przez wyświetlenie czerwonego krzyżyka na polu **Pliki**.



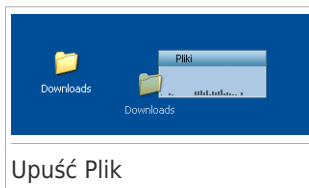
Pasek Aktywności Skanera

6.4.1. 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 skanera antywirusowego i poprowadzi Cię przez proces skanowania. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Skanowania Antywirusowego*” (p. 53).

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.

6.4.2. Zablokuj/Odblokuj Pasek Aktywności Skanera

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

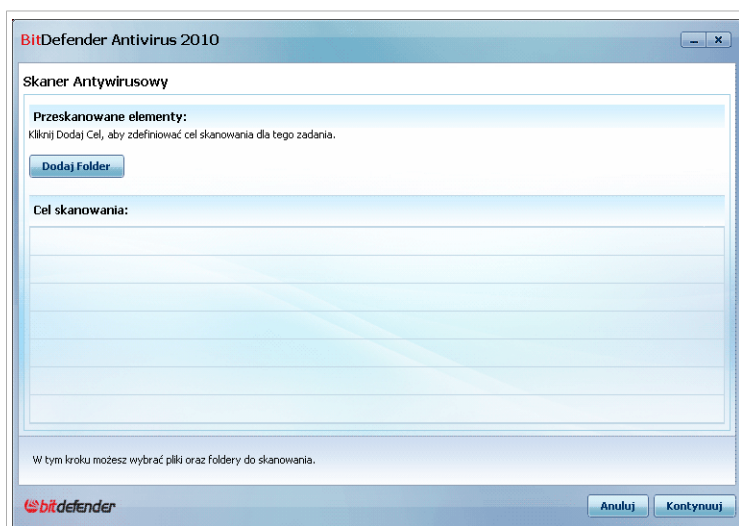
1. Otwórz BitDefender.

2. Kliknij na przycisk **Ustawienia** w górnym prawym rogu okna.
3. W kategorii Ustawienia Główne, wybierz pole odpowiadające **Paskowi Aktywności Skanera**
4. Kliknij **OK** aby zapisać i zastosować zmiany.

6.5. Skanowanie Ręczne BitDefender

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 twój system jest zainfekowany przez odpornego wirusa, możesz spróbować usunąć go uruchamiając Windows w Trybie Awaryjnym i skanować każdy z dysków twardych za pomocą opcji Ręcznego Skanowania w BitDefenderze.

Aby uzyskać dostęp do Skanowania Ręcznego, skorzystaj z menu Start: **Start** → **Programs** → **BitDefender 2010** → **Skanowanie Ręczne BitDefender**. Pojawi się następujące okno:



Skanowanie Ręczne BitDefender

Kliknij **Dodaj Folder**, wybierz lokalację, którą chcesz dodać i kliknij **OK**. Jeśli chcesz skanować wiele folderów, powtórz tę czynność dla każdej dodatkowej lokalizacji.

Ścieżki do wybranej lokalizacji pojawią się w kolumnie **Cel Skanowania**. Jeśli rozmyśliłeś się odnośnie danej lokalizacji, kliknij **Usuń** obok niej. Kliknij na przycisk **Usuń Wszystkie Ścieżki** aby usunąć wszystkie ścieżki znajdujące się na liście.

Kiedy skończysz wybierać lokalacje, kliknij **Kontynuuj**. Pojawi się kreator skanera antywirusowego i poprowadzi Cię przez proces skanowania. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Skanowania Antywirusowego*” (p. 53).

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.

Co to jest Tryb Awaryjny?

Tryb awaryjny to opcja przeznaczona do rozwiązywania problemów z systemem Windows, które mają niekorzystny wpływ na jego normalną pracę. Dzięki temu możliwe jest rozwiązywanie wielu problemów, od konfliktów sterowników, po usuwanie wirusów uniemożliwiających uruchomienie systemu w trybie podstawowym. W Trybie Awaryjnym, Windows uruchamia się tylko z ograniczonym zestawem funkcji i sterowników. Tylko kilka aplikacji może pracować w tym trybie. To dlatego, większość wirusów nie jest wtedy aktywna i może zostać łatwo usunięta.

Aby uruchomić Windows w Trybie Awaryjnym, uruchom ponownie komputer i naciśnij F8 przed załadowaniem systemu. Pojawi się menu wyboru trybu uruchomienia systemu. Możesz wybrać jedną z kilku opcji uruchomienia Windows w Trybie awaryjnym. Jeśli chcesz korzystać z Internetu, powinieneś wybrać opcję **Tryb Awaryjny z obsługą sieci**.



Notatka

Aby uzyskać więcej informacji na temat Trybu Awaryjnego, przejdź do Centrum Pomocy Systemu Windows (w menu Start, kliknij **Centrum Pomocy**). Ta nazwa może się różnić w zależności od wersji systemu Windows. Możesz także uzyskać więcej informacji przeszukując Internet.

6.6. Tryb Gry i Tryb Laptopa

Niektóre aplikacje takie jak gry lub prezentacje, wymagają zwiększonej wydajności komputera i nie przerywania ich pracy poprzez wyświetlanie zbędnych komunikatów. Kiedy twój laptop pracuje na zasilaniu z baterii, najlepiej jest przesunąć dodatkowe operacje, które zwiększają zużycie prądu, na później, kiedy znowu zostanie podłączony do zasilania A/C.

Aby przystosować się do tych dwóch szczególnych sytuacji, BitDefender Antivirus 2010 posiada dwa tryby operacyjne:

- Tryb Gry
- Tryb Laptopa

6.6.1. Tryb Gry

Tryb Gry tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na wydajność systemu. W Trybie Gry, następujące ustawienia są stosowane:

- Minimalizacja użycia procesora oraz pamięci
- Wstrzymanie skanowań oraz automatycznych aktualizacji
- Wyłączenie alarmów oraz wyskakujących okienek
- Skanowanie tylko najważniejszych plików

W Trybie Gry, możesz zobaczyć literę G nad  ikoną BitDefendera.

Używanie Trybu Gry

Domyślnie, BitDefender automatycznie włącza Tryb Gry gdy uruchomisz grę będącą na liście znanych gier BitDefendera lub aplikację działającą w trybie pełnoekranowym. BitDefender automatycznie powróci do normalnego trybu operacyjnego kiedy zamkniesz grę lub wykryta aplikacja wyjdzie z trybu pełnoekranowego.

Jeśli chcesz ręcznie włączyć Tryb Gry, skorzystaj z jednej z następujących metod:

- Kliknij prawym przyciskiem myszki ikonę BitDefender w pasku systemowym i wybierz **Włącz Tryb Gry**.
- Wciśnij **Ctrl+Shift+Alt+G**(domyślne klawisze skrótu).



WAŻNE

Nie zapomnij wyłączyć Trybu Gry kiedy skończysz. Aby to zrobić użyj tych samych metod co przy włączaniu.

Zmienianie klawiszy skrótu Trybu Gry

Jeżeli chcesz zmienić klawisze skrótu, wykonaj następujące kroki:

1. Otwórz BitDefender i przestaw interfejs użytkownika na Tryb Eksperta.
2. Kliknij **Tryb Gry / Laptopa** w menu po lewej stronie.
3. Kliknij zakładkę **Tryb Gry**.
4. Kliknij **Zaawansowane**.
5. 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

Odznaczenie pola **Użyj klawisza skrótu** wyłączy klawisz z kombinacji skrótu.

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

6.6.2. 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, wszystkie zaplanowane zadania skanowania nie są wykonywane, ponieważ ich praca mogłaby wpłynąć na większe zużycie zasobów i co się z tym wiąże, energii elektrycznej.

BitDefender wykrywa kiedy laptop korzysta z baterii i automatycznie włącza tryb laptopa. Identyfikując, BitDefender automatycznie wyłącza Tryb Laptopa, kiedy wykryje że laptop nie korzysta już z baterii.

Aby skorzystać z Trybu Laptopa, w **kreatorze konfiguracji** musisz zaznaczyć, że komputer z którego korzystasz to laptop. Jeśli nie wybrałeś odpowiedniej opcji podczas pracy kreatora, Tryb Laptopa możesz także odblokować następująco:

1. Otwórz BitDefender.
2. Kliknij na przycisk **Ustawienia** w górnym prawym rogu okna.
3. W kategorii Ustawienia Główne, wybierz pole odpowiadające **Wykrywaniu Trybu Laptopa**
4. Kliknij **OK** aby zapisać i zastosować zmiany.

6.7. 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 skanera antywirusowego i poprowadzi Cię przez proces skanowania. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Skanowania Antywirusowego*” (p. 53).

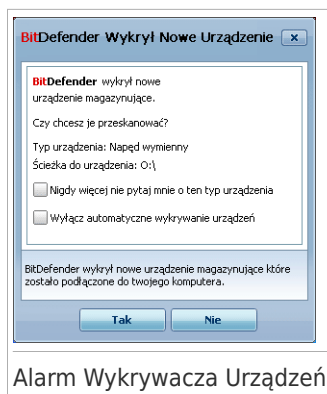
Jeśli nie chcesz skanować urządzenia, kliknij **Nie**. W tym przypadku, mogą przydać się następujące opcje:

- **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 i przestaw interfejs użytkownika na Tryb Eksperta.
2. Przejdź do **skanowania antywirusowego**.
3. Na liście zadań skanowania, odszukaj zadanie **Skanowania Wykrytych Urządzeń**.
4. Kliknij prawym przyciskiem myszy na zadanie i wybierz **Otwórz**. Pojawi się nowe okno.
5. W zakładce **Podgląd** możesz skonfigurować opcje skanowania. Aby uzyskać więcej informacji, odwołaj się do „*Konfigurowanie Ustawień Skanowania*” (p. 118).
6. W zakładce **Wykrywanie** możesz wybrać, które typy urządzeń mają być wykrywane.
7. Kliknij **OK** aby zapisać i zastosować zmiany.



7. 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, która znajduje się w **zasobniku systemowym paska zadań** wyświetlana jest specjalna ikona, aby wskazać że pojawiły się zagadnienia wymagające uwagi użytkownika.

 **Czerwony trójkąt ze znakiem wykrzyknika:** Krytyczne zagadnienia wpływające na bezpieczeństwo systemu. Wymagają natychmiastowej naprawy.

 **Żółty trójkąt ze znakiem wykrzyknika:** Nie-krytyczne zagadnienia wpływające na bezpieczeństwo twojego systemu. Powinieneś sprawdzić i naprawić je przy najbliższej okazji.

Dodatkowo, jeśli przesuniesz kursor nad ikonę, pojawi się okienko z potwierdzeniem istnienia pewnych zagadnień.

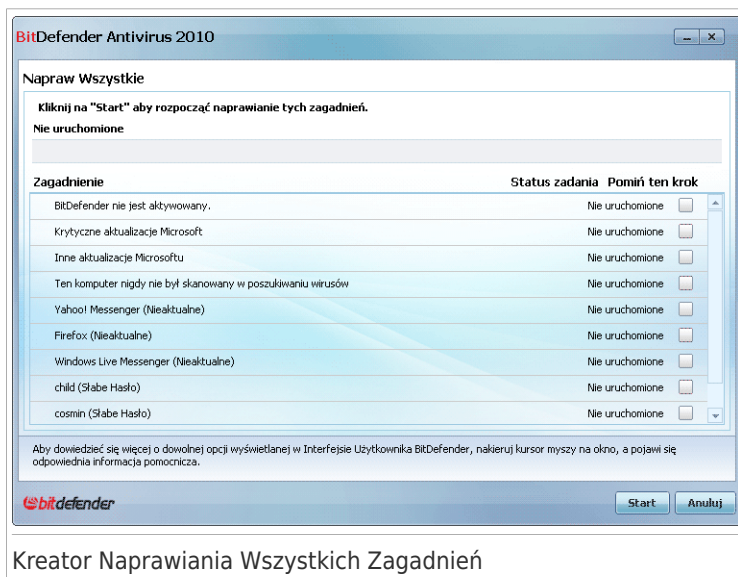
- Kiedy utworzysz BitDefender, pole Stan Bezpieczeństwa będzie wskazywać na liczbę zagadnień, które wpływają na bezpieczeństwo systemu.
 - ▶ W Trybie Średniozaawansowanym, stan zabezpieczeń jest wyświetlany w zakładce **Panel**.
 - ▶ W Trybie Eksperta, przejdź do **Główne i Pulpit** aby sprawdzić stan zabezpieczeń.

7.1. Kreator Naprawiania Wszystkich Zagadnień

Najprostszym sposobem na naprawienie istniejących zagadnień jest skorzystanie z kreatora **Napraw Wszystkie Zagadnienia**. Ten kreator pomaga łatwo usuwać wszystkie zagrożenia związane z twoim komputerem i bezpieczeństwem danych. Aby otworzyć ten kreator, wykonaj następujące czynności:

- Kliknij prawym przyciskiem myszy na ikonę BitDefender  w **zasobniku systemowym paska zadań** i wybierz **Napraw Wszystkie Zagadnienia**.
- Otwórz BitDefender. W zależności od trybu interfejsu użytkownika, postępuj kolejno:
 - ▶ W Trybie Początkującym, kliknij na **Napraw Wszystkie Zagadnienia**.
 - ▶ W Trybie Średniozaawansowanym przejdź do zakładki **Panel** i kliknij na **Napraw Wszystkie Zagadnienia**.

- W Trybie Eksperta, przejdź do **Główne i Panel** i kliknij na **Napraw Wszystkie Zagadnienia**.



Kreator wyświetla listę istniejących dziur w zabezpieczeniach twojego komputera.

Do naprawy wybrano wszystkie zagadnienia. Jeśli istnieje jakieś zagadnienie, którego nie chcesz naprawiać, zaznacz odpowiadające mu pole. Jeśli to zrobisz, jego stan zmieni się na **Pomiń**.



Notatka

Jeśli chcesz wyłączyć powiadomianie o konkretnych zagadnieniach, musisz odpowiednio skonfigurować system, tak jak to opisano 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 „*Kreator Sprawdzania Podatności*” (p. 65).

7.2. Konfiguracja Śledzenia Zagadnień

System śledzenia zagadnień jest skonfigurowany tak, aby monitorować i chronić najważniejsze zagadnienia, które mogą wpłynąć na obniżenie bezpieczeństwa twojego komputera i danych. Możesz monitorować dodatkowe zagadnienia, korzystając z **kreatora konfiguracji** (w oknie konfiguracji twojego profilu użytkownika). Oprócz domyślnie monitorowanych zagadnień, istnieje wiele dodatkowych, o których możesz być informowany(a).

Możesz skonfigurować system śledzenia według własnego uznania, wybierając określone zagadnienia o których ma on informować. Możesz to zrobić w Trybie Średniozaawansowanym lub Eksperta.

- W Trybie Średniozaawansowanym, system śledzenia można konfigurować z oddzielnych lokacji. Podążaj tymi krokami:
 1. Przejdź do **Antywirus, Antyphishing** lub zakładki **Podatności**.
 2. Kliknij **Skonfiguruj Śledzenie Stanu**.
 3. Zaznacz pola odpowiadające elementom które mają być monitorowane.

Aby uzyskać więcej informacji, odwołaj się do „*Tryb Średniozaawansowany*” (p. 72) części podręcznika użytkownika.

- W Trybie Eksperta, system śledzenia można konfigurować z jednej, centralnej lokalizacji. Podążaj tymi krokami:
 1. Przejdź do **Głównego Pulpitu**.
 2. Kliknij **Skonfiguruj Śledzenie Stanu**.
 3. Zaznacz pola odpowiadające elementom które mają być monitorowane.

Aby uzyskać więcej informacji, odwołaj się do rozdziału „*Pulpit*” (p. 94).

8. Konfigurowanie Ustawień Podstawowych

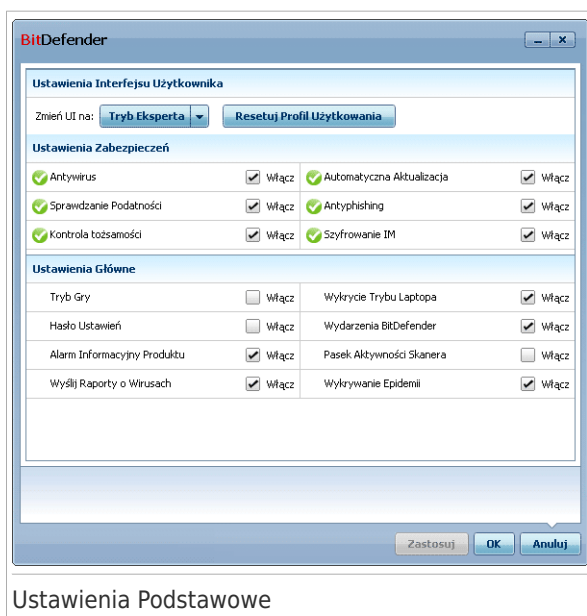
Możesz skonfigurować główne ustawienia produktu (wliczając w to zmianę trybu interfejsu użytkownika) z okna ustawień podstawowych. Aby je otworzyć, wykonaj następujące czynności:

- Otwórz BitDefender i kliknij na przycisk **Ustawienia** w górnym prawym rogu okna.
- Kliknij prawym przyciskiem myszy na ikonę BitDefender  w **zasobniku systemowym** i wybierz **Podstawowe Ustawienia**.



Notatka

Aby szczegółowo skonfigurować ustawienia programu, skorzystaj z Trybu Eksperta interfejsu użytkownika. Aby uzyskać więcej informacji, odwołaj się do „Tryb Eksperta” (p. 93) części podręcznika użytkownika.



Ustawienia Podstawowe

Ustawienia są podzielone na trzy kategorie:

- **Ustawienia Interfejsu Użytkownika**
- **Ustawienia Zabezpieczeń**
- **Ustawienia Główne**

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

8.1. Ustawienia Interfejsu Użytkownika

W tym obszarze możesz zmienić tryb interfejsu użytkownika i zresetować profil użytkownika.

Zmiana trybu interfejsu użytkownika. Tak jak przedstawiono w sekcji „*Tryby Widoku Interfejsu Użytkownika*” (p. 22), istnieją trzy tryby interfejsu użytkownika. Każdy tryb został stworzony z myślą o określonej kategorii użytkowników, w oparciu o ich umiejętności i wiedzę na temat komputerów i oprogramowania. W ten sposób, z interfejsu użytkownika mogą korzystać wszyscy użytkownicy, zarówno ci zaczynający przygodę z komputerem jak i eksperci.

Pierwszy przycisk pokazuje obecny tryb pracy interfejsu użytkownika. Aby zmienić tryb interfejsu użytkownika, kliknij na strzałkę  na przycisku i wybierz pożądaný tryb z menu.

Tryb	Opis
Tryb 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.
Tryb Średniozaawansowany	Dla użytkowników o przeciętnym poziomie wiedzy na temat komputera, ten tryb stanowi rozwinięcie trybu podstawowego. 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.
Tryb 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.

Resetowanie profilu użytkownika. Profil użytkownika odzwierciedla główne czynności wykonywane na komputerze. W zależności od tego profilu, interfejs programu jest zorganizowany tak, aby umożliwić szybki dostęp do preferowanych zadań.

Aby przekonfigurować profil użytkownika, kliknij **Resetuj Profil Użytkownika** i podążaj za kreatorem konfiguracji.

8.2. Ustawienia Zabezpieczeń

W tym obszarze możesz odblokować lub zablokować ustawienia zabezpieczeń programu, które obejmują różne aspekty bezpieczeństwa komputera i jego danych. Obecny stan ustawień jest wskazywany za pomocą jednej z tych ikon:

 **Zielone kółko:** Ustawienie jest odblokowane.

 **Czerwone kółko z wykrzyknikiem:** Ustawienie jest zablokowane.

Aby odblokować / zablokować ustawienie, zaznacz / odznacz odpowiednie pole **Odblokuj**.



Ostrzeżenie

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

Poniższa tabela przedstawia listę ustawień i ich opis:

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.
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

Ustawienie	Opis
	i dane przesyłane w formularzach, w których pojawiają się prywatne informacje przesyłane do nieautoryzowanych odbiorców.
Szyfrowanie IM	Szyfrowanie komunikatorów (Instant Messaging) zabezpiecza dane przesyłane w rozmowach za pośrednictwem komunikatorów Yahoo! Messenger i Windows Live Messenger, ale wymaga, aby obydwie strony korzystały z kompatybilnego oprogramowania BitDefender.

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 dane ustawienie które jest monitorowane pojawiało się jako zagadnienie wymagające naprawy, musisz odpowiednio skonfigurować system śledzenia. Możesz to zrobić w Trybie Średniozaawansowanym lub Eksperta.

- W Trybie Średniozaawansowanym, system śledzenia zagadnień może być konfigurowany w różnych lokalizacjach, w oparciu o kategorie ustawień. Aby uzyskać więcej informacji, odwołaj się do „Tryb Średniozaawansowany” (p. 72) części podręcznika użytkownika.
- W Trybie Eksperta, system śledzenia można konfigurować z jednej, centralnej lokalizacji. Podążaj tymi krokami:
 1. Przejdź do **Głównego Pulpitu**.
 2. Kliknij **Skonfiguruj Śledzenie Stanu**.
 3. Wyczyść pole odpowiadające elementowi, którego nie chcesz monitorować.

Aby uzyskać więcej informacji, odwołaj się do rozdziału „Pulpit” (p. 94).

8.3. Ustawienia Ogólne

W tym obszarze możesz odblokować lub zablokować ustawienia które wpływają na zachowanie programu i sposób współpracy z użytkownikiem. Aby odblokować / zablokować ustawienie, zaznacz / odznacz odpowiednie pole **Odblokuj**.

Poniższa tabela przedstawia listę ustawień i ich opis:

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

Ustawienie	Opis
Wykrywanie 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 opcję, będziesz otrzymywać ważne informacje firmowe, aktualizacje produktu lub nowości o nowych zagrożeniach od BitDefendera.
Alarmy Powiadomień Produktu	Włączając tą opcję, 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 „ <i>Pasek Aktywności Skanera</i> ” (p. 30).
Wyślij Raport Wirusów	Włączając tą opcję, będziesz wysyłał raporty skanowania wirusów do Laboratorium BitDefendera do analizy. Proszę pamiętać że te raporty nie zawierają żadnych danych osobowych, takich jak adres imię lub IP i nie będą wykorzystywane w celach komercyjnych.
Wykrywanie Włamań	Włączając tą opcję, będziesz wysyłał raporty dotyczące potencjalnych włamań wirusów do Laboratorium BitDefendera do analizy. Proszę pamiętać że te raporty nie zawierają żadnych danych osobowych, takich jak adres imię lub IP i nie będą wykorzystywane w celach komercyjnych.

9. 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.



Notatka

Ten odnośnik jest dostępny tylko w Trybie Średniozaawansowanym lub Eksperta.

Historia & Zdarzenia

Antywirus

- Kontrola Prywatności
- Podatności
- Szyfrowanie IM
- Tryb Gry/Laptopa
- Sieć Domowa
- Aktualizacje
- Rejestracja

Ochrona w czasie rzeczywistym

Nazwa akcji	Podjęte Działanie	Data
Ochrona w czasie rzeczywistym...	Wyłączone	8/26/2009 6:50:18 PM
Ochrona w czasie rzeczywistym...	Wyłączone	8/26/2009 6:48:53 PM
Ochrona w czasie rzeczywistym...	Wyłączone	8/26/2009 6:42:29 PM
Ochrona w czasie rzeczywistym...	Wyłączone	8/26/2009 6:42:26 PM
Skaner Behawioralny wykry...	Aplikacja została zamknięta...	8/26/2009 6:42:17 PM

Zadania na żądanie

Nazwa akcji	Nazwa zadania:	Data
Skanowanie wykonane pom...	Zadanie skanowania	8/26/2009 6:48:39 PM
Skanowanie zostało przerw...	Skanowanie obiektów ob...	8/26/2009 6:44:09 PM
Skanowanie zostało zatrzy...	Głębokie Skanowanie	8/26/2009 6:42:50 PM
Skanowanie zostało przerw...	Szybkie Skanowanie	8/26/2009 6:41:02 PM

Aby dowiedzieć się więcej o dowolnej opcji wyświetlanej w Interfejsie Użytkownika BitDefender, nakieruj kursor myszy na okno, a pojawi się odpowiednia informacja pomocnicza.

bitdefender Wyczyść dzienniki Odśwież OK

Zdarzenia

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

- **Antywirus**
- **Kontrola Prywatności**
- **Podatności**
- **Szyfrowanie IM**
- **Tryb Gry/Laptopa**
- **Sieć Domowa**

- **Aktualizacja**
- **Rejestracja**
- **Dziennik Internetowy**

Dla każdej kategorii dostępna jest lista zdarzeń. Każde zdarzenie posiada informacje: krótki opis, akcja którą podjął BitDefender, datę i czas wystąpienia. Jeżeli chcesz uzyskać więcej informacji, kliknij dwa razy na dane zdarzenie.

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

10. Rejestracja i Moje Konto

BitDefender Antywirus 2010 posiada 30-dniowy okres próbny. Podczas okresu darmowego korzystania z aplikacji, produkt pozostaje w pełni funkcjonalny, aby użytkownik mógł sprawdzić czy spełnia on jego oczekiwania. Proszę pamiętać, że po 15 dniach korzystania, produkt przestanie się aktualizować, dopóki nie założysz konta BitDefender. Założenie konta BitDefender jest wymaganym warunkiem w procesie rejestracji.

Zanim zakończy się darmowy okres testowy, musisz zarejestrować produkt jeśli chcesz aby twój komputer był chroniony. 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.



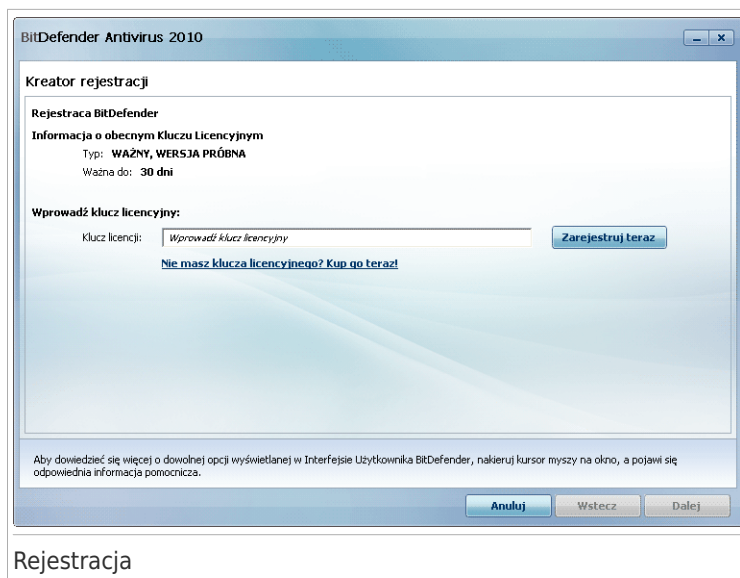
WAŻNE

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.

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 zarejestrować produkt z kluczem licencyjnym kiedy darmowy okres testowy się zakończy. Musisz wykupić klucz licencyjny lub odnowić swoją licencję kilka dni zanim obecny klucz straci ważność.

10.1. Rejestrowanie BitDefender Antivirus 2010

Jeśli chcesz zarejestrować produkt z kluczem licencyjnym lub zmienić obecny klucz, kliknij na odnośnik **Zarejestruj teraz** położony w dolnej części okna BitDefender. Zostanie otwarte okno rejestracji produktu.



Rejestracja

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

Aby zarejestrować BitDefender Antivirus 2010:

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 **Zakończ**.

10.2. Aktywacja BitDefendera

Aby aktywować BitDefender, musisz stworzyć nowe lub zalogować się do istniejącego konta BitDefender. Jeśli nie zarejestrujesz konta BitDefender podczas wstępnego kreatora rejestracji, możesz to zrobić później następująco:

- W Trybie Początkującym, kliknij na **Napraw Wszystkie Zagadnienia**. Ten kreator pozwoli ci naprawić wszystkie bieżące zagadnienia oraz aktywować twój produkt.
- W Trybie Średniozaawansowanym, przejdź do zakładki **Zabezpieczenia** i kliknij na przycisk **Napraw**, odpowiadający zagadnieniu dotyczącemu aktywacji produktu.
- W Trybie Eksperta, przejdź do **Rejestracja** i kliknij przycisk **Aktywuj Produkt**.

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

BitDefender Antivirus 2010

Kreator rejestracji

Konto BitDefender

Aby mieć dostęp do aktualizacji i wsparcia technicznego, aktywuj BitDefender przez stworzenie/zalogowanie się do istniejącego konta. Możesz odłożyć aktywację na okres 15 dni dla wersji próbnych i 30 dni dla wersji zarejestrowanych.

☒ Stwórz nowe konto

Adres e-mail:

Hasło: Wpisz ponownie hasło:

Opcje e-mail:

☐ Zaloguj się (poprzednio stworzone konto)

☐ Zarejestruj później (rejestracja jest obowiązkowa)

Aby dowiedzieć się więcej o dowolnej opcji wyświetlanej w Interfejsie Użytkownika BitDefender, nakieruj kursor myszy na okno, a pojawi się odpowiednia informacja pomocnicza.

Tworzenie Konta

Jeśli nie chcesz zakładać konta BitDefender w tym momencie, wybierz **Zarejestruj Później** i kliknij **Zakończ**. W przeciwnym razie postępuj w zależności od sytuacji:

- „Nie mam osobistego konta na MyBitDefender” (p. 50)
- „Już posiadam konto BitDefender” (p. 51)



WAŻNE

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.

Nie mam osobistego konta na MyBitDefender

Aby pomyślnie utworzyć konto BitDefender, podążaj według tych kroków:

1. Wybierz **Stwórz nowe konto**.
2. Wprowadź wymaganą informację w odpowiednich polach. Dane które teraz wprowadzisz pozostaną tajne.
 - **Adres email** - wpisz swój adres email.
 - **Hasło** - wpisz hasło dla konta BitDefender. Hasło musi zawierać od 6 do 16 znaków.
 - **Powtórz hasło** - wpisz ponownie wcześniej podane hasło.



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. Wybierz jedną z dostępnych w menu opcji:
 - **Wysyłaj mi wszystkie wiadomości**
 - **Wysyłaj mi tylko informacje o produktach**
 - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Utwórz**.
5. Kliknij **Zakończ** aby zakończyć kreator.
6. **Przeprowadź aktywację swojego konta**. 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 **Zakończ** aby zakończyć kreator.

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

1. Wybierz **Zaloguj się (poprzednio stworzone 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. Wybierz jedną z dostępnych w menu opcji:

- **Wysyłaj mi wszystkie wiadomości**
- **Wysyłaj mi tylko informacje o produktach**
- **Nie wysyłaj mi żadnych wiadomości**

4. Kliknij **Zaloguj się**.

5. Kliknij **Zakończ** aby zakończyć kreator.

10.3. Zakup kluczy licencyjnych

Jeśli okres testowy wkrótce się zakończy, musisz zakupić nowy klucz licencyjny i zarejestrować swój produkt. Otwórz BitDefender i kliknij na link **Kup/Odnów**, znajdujący się na dole okna. Ten link przekieruje cię na stronę gdzie możesz zakupić klucz licencyjny dla swojego produktu BitDefender.

10.4. Odnawianie licencji.

Jako klientowi BitDefender, przysługuje ci zniżka przy odnawianiu licencji dla twoich produktów. Możesz także wykonać ugrację swojej starej wersji do najnowszej, po specjalnej zniżce lub za darmo.

Jeśli twój obecny klucz licencyjny wkrótce straci ważność, musisz odnowić swoją licencję. Otwórz BitDefender i kliknij na link **Kup/Odnów**, znajdujący się na dole okna. Ten link zabierze cię na stronę gdzie będziesz mógł odnowić swoją licencję.

11. Kreatory

Dzięki kreatorom możesz szybko i w prosty sposób skonfigurować zaawansowane ustawienia programu. Ten rozdział przedstawia poszczególne kreatory, z których możesz skorzystać podczas pracy z BitDefenderem. Inne kreatory konfiguracji są opisane oddzielnie w części „Tryb Eksperta” (p. 93).

11.1. 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.

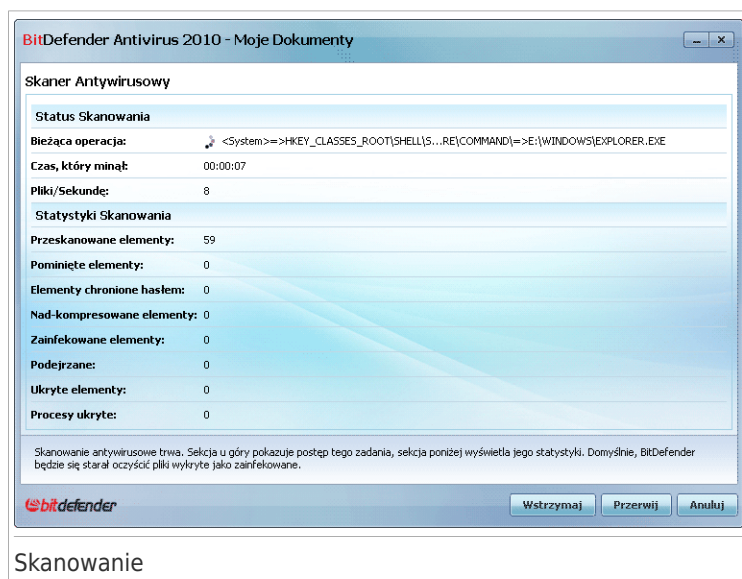


Notatka

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.

11.1.1. 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. Jeśli BitDefender natrafi na archiwum chronione hasłem podczas skanowania i ustawiona jest domyślna akcja **Pytaj o hasło**, zostaniesz poproszony o podanie hasła. Archiwa chronione hasłem nie mogą być skanowane chyba że podasz hasło. Dostępne są następujące opcje:

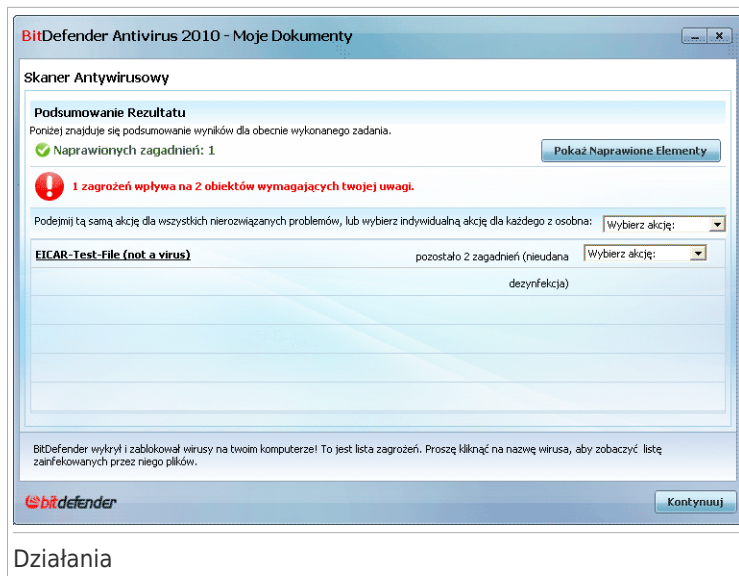
- **Chcę podać hasło do tego obiektu.** Jeśli chcesz aby BitDefender przeskanował archiwum, wybierz tą opcję i podaj hasło. Jeśli nie znasz hasła, wybierz jedną z pozostałych opcji.
- **Nie chcę podawać hasła.** Wybierz tą opcję aby pominąć skanowanie tego archiwum.
- **Nie chcę podawać hasła do żadnego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

Kliknij **OK** aby kontynuować skanowanie.

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

11.1.2. Krok 2/3 – Wybierz Działanie

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



Działania

Możesz zobaczyć ilość zdarzeń zagrażających twojemu systemowi.

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:

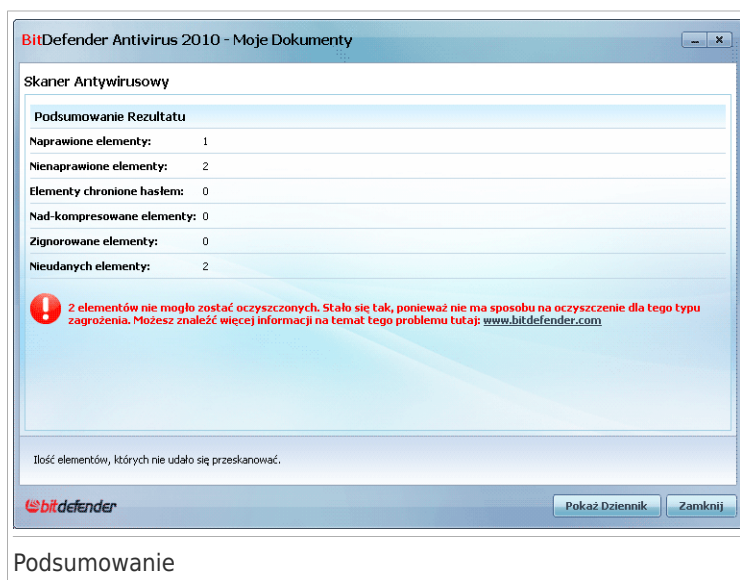
Działania	Opis
Brak Działań	Żadne działanie nie zostanie podjęte na wykrytych plikach. Po zakończeniu skanowania, możesz otworzyć dziennik skanowania i zobaczyć informacje o tych plikach.
Usuń wirusa	Usuwa złośliwy kod z zainfekowanych plików.
Usuń	Usuwa wykryte pliki.
Przenieś do kwarantanny	Przenosi pliki wykryte jako zainfekowane do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.

Działania	Opis
Zmień nazwę plików	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.

11.1.3. Krok 3/3 – Wyświetl Wyniki

Kiedy BitDefender zakończy naprawianie zagadnień, w nowym oknie pojawi się rezultat skanowania.



Podsumowanie

Możesz zobaczyć podsumowanie wyników. Jeśli chcesz uzyskać wyczerpujące informacje na temat procesu skanowania, kliknij na **Pokaż plik dziennika** aby przejrzeć dziennik.



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. Jednakże, są zagadnienia których nie można rozwiązać.

W takim przypadku zalecamy skontaktować się ze Pomocą Techniczną BitDefendera na www.bitdefender.com. Nasze wsparcie techniczne pomoże tobie rozwiązać problemy na które natrafiasz.

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.

11.2. Kreator Własnego Skanowania

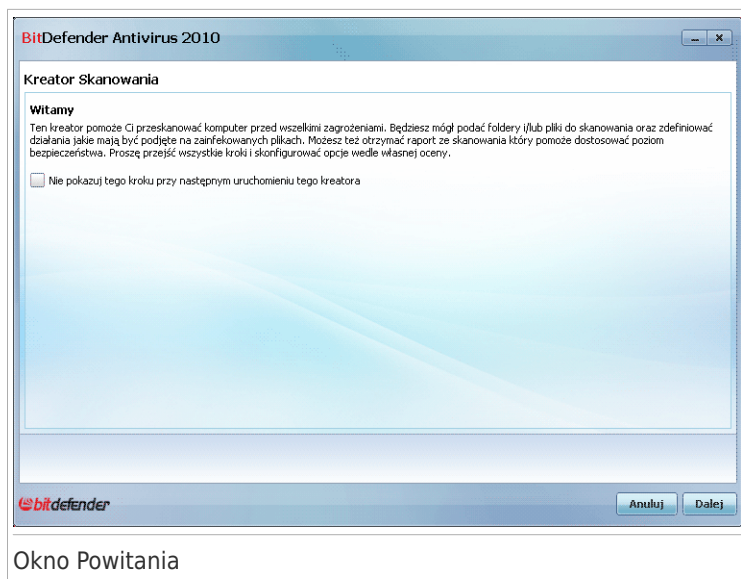
Kreator Własnego Skanowania pozwala na tworzenie i uruchamianie własnych zadań skanowania i opcjonalnie zachowywanie ich jako Szybkie Zadania gdy BitDefender działa w Trybie Średniozaawansowanym.

Aby uruchomić własne zadanie skanowania korzystając z Kreatora Własnego Skanowania, musisz wykonać następujące kroki:

1. W Trybie Średniozaawansowanym, przejdź do zakładki **Antywirus**.
2. W polu Szybkie Zadania, kliknij **Niestandardowe**.
3. Podążaj za instrukcją aby zakończyć proces skanowania.

11.2.1. Krok 1/6 - Okno Powitalne

To jest okno powitalne.

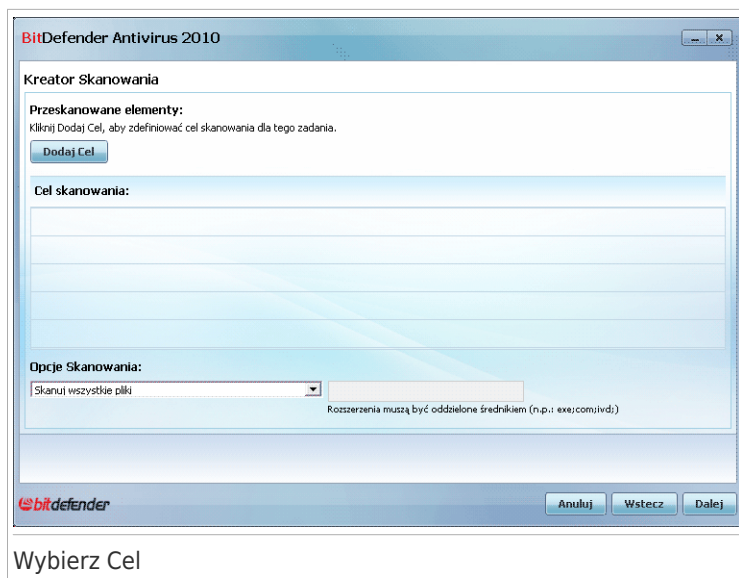


Jeśli chcesz pominąć to okno podczas uruchamiania tego kreatora w przyszłości, zaznacz pole **Nie pokazuj tego kroku przy następnym uruchomieniu tego kreatora**.

Kliknij **Dalej**.

11.2.2. Step 2/6 - Wybierz Cel

Tutaj możesz określić pliki lub foldery do przeskanowania oraz opcje skanowania.



Wybierz Cel

Kliknij **Dodaj Cel**, wybierz plik lub folder który chcesz dodać i kliknij **OK**. Ścieżki do wybranych lokacji pojawią się w kolumnie **Cel Skanowania**. Jeśli rozmyśliłeś się odnośnie danej lokalizacji, kliknij **Usuń** obok niej. Kliknij na przycisk **Usuń Wszystkie** aby usunąć wszystkie lokacje, które zostały dodane do listy.

Kiedy skończysz wybierać lokacje, ustaw **Opcje Skanowania**. Oto dostępne możliwości:

Opcje	Opis
Skanowanie wszystkich plików	Zaznacz tą opcję, aby przeskanować wszystkie pliki w wybranych folderach.
Skanuj tylko pliki z rozszerzeniami aplikacji	Wyłącznie pliki programowe zostaną przeskanowane tzn. pliki z następującymi rozszerzeniami: .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 i .nws.

Opcje	Opis
Skanowanie tylko rozszerzeń zdefiniowanych przez użytkownika	Wyłącznie pliki z rozszerzeniami określonymi przez użytkownika zostaną przeskanowane. Te rozszerzenia muszą być oddzielone przez ",".

Kliknij **Dalej**.

11.2.3. Step 3/6 - Wybierz Działanie

Tutaj możesz określić ustawienia skanera i poziom skanowania.

Wybierz Działanie

- Wybierz działanie, które ma zostać podjęte na wykrytych zainfekowanych i podejrzanych plikach. Dostępne są następujące opcje:

Działania	Opis
Brak Działań	Żadna reakcja nie będzie podjęta na zainfekowane pliki. Te pliki będą występować w pliku raportu.
Wylecz pliki	Usuwa szkodliwy kod z wykrytego zainfekowanego pliku.

Działania	Opis
Usuń pliki	Natychmiastu usuwa zainfekowane pliki, bez żadnego ostrzeżenia.
Przenieś do Kwarantanny	Przenosi zainfekowane pliki do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.

- Wybierz działanie, które ma być podjęte na ukrytych plikach (rootkitach). Dostępne są następujące opcje:

Działania	Opis
Brak Działań	Żadna działanie nie będzie podjęte na ukrytych plikach. Pliki te będą zawarte w raporcie.
Zmień nazwę	Zmienia nazwę ukrytych plików dodając .bd.ren do ich nazwy. Dzięki temu, będziesz mógł znaleźć tego typu pliki na swoim komputerze, jeśli takowe istnieją.

- Skonfiguruj agresywność skanera. Są 3 poziomy, które można wybrać. Przesuń suwak po skali i wybierz odpowiedni poziom zabezpieczeń:

P o z i o m skanowania	Opis
Tolerancyjny	Tylko pliki aplikacji są skanowane i tylko w poszukiwaniu wirusów. Poziom zużycia zasobów jest niski.
Domyślny	Poziom zużycia zasobów jest średni. Wszystkie pliki są skanowane w poszukiwaniu wirusów i oprogramowania szpiegującego (spyware).
Agresywny	Wszystkie pliki (łącznie z archiwami) są skanowane w poszukiwaniu wirusów i oprogramowania szpiegującego (spyware). Skanowanie obejmuje także ukryte pliki i procesy. Zużycie zasobów jest większe.

Zaawansowani użytkownicy mogą chcieć skorzystać z ustawień skanowania, jakie oferuje BitDefender. Skaner może być ustawiony tak, aby skanował konkretne zagrożenia. Może to w dużym stopniu zmniejszyć czas potrzebny na skanowanie oraz obciążenie systemu podczas skanowania.

Przesuń suwak aby wybrać **Użytkownika** i kliknij na przycisk **Poziom niestandardowy**. Pojawi się okno. Określ typ złośliwego oprogramowania, którego BitDefender ma szukać, przez wybranie odpowiednich opcji:

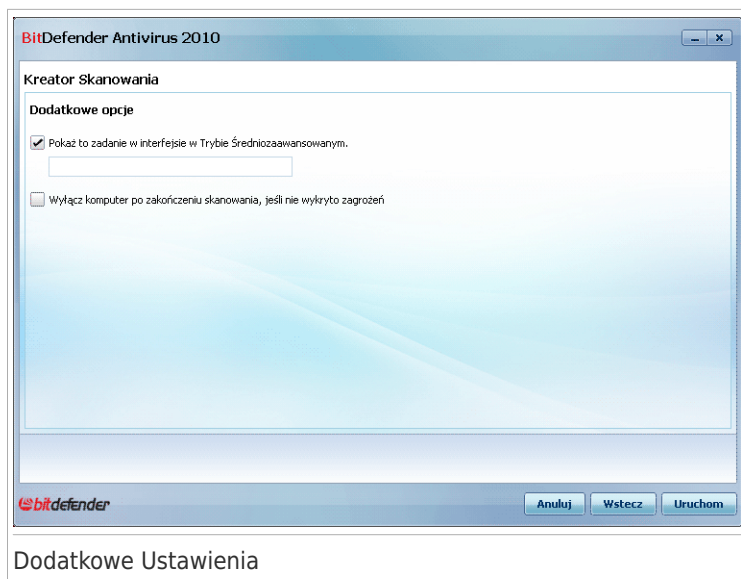
Opcje	Opis
Skanuj przed wirusami	Skanuje szukając znanych wirusów. BitDefender wykrywa również niekompletne wirusy, w celu usunięcia zagrożeń które mogły by wpłynąć na zabezpieczenia systemu.
Skanuj przed adware	Szuka aplikacji adware. Pliki tego typu będą traktowane jako zainfekowane. Oprogramowanie, które zawiera komponenty adware może przestać działać jeśli ta opcja jest włączona.
Skanuj przed spyware	Szuka znanych zagrożeń szpiegujących. Wykryte pliki spyware będą traktowane jako zainfekowane.
Skanuj w poszukiwaniu aplikacji	Szuka legalnych aplikacji które mogą być użyte jako narzędzie szpiegujące, do ukrycia szkodliwej aplikacji lub w innych szkodliwych celach.
Skanuj przed dialerami	Szuka aplikacji dzwoniących pod drogie numery. Takie pliki zostaną oznaczone jako zainfekowane. Oprogramowanie które zawiera komponenty dialer może przestać działać jeśli ta opcja jest włączona.
Skanuj przed rootkitami	Szuka ukrytych obiektów (plików i procesów), ogólnie znanych jako rootkity.
Skanowanie w poszukiwaniu keyloggerów	Skanuje w poszukiwaniu złośliwych aplikacji które rejestrują wciskane klawisze.

Kliknij **OK** aby zamknąć okno.

Kliknij **Dalej**.

11.2.4. Step 4/6 - Dodatkowe Ustawienia

Zanim rozpocznie się skanowanie, dostępnych jest kilka opcji:



- Aby zapisać własne zadanie skanowania i móc użyć je w przyszłości, zaznacz pole **Pokaż to zadanie w Trybie Średniozaawansowanym** i wprowadź dla niego nazwę.

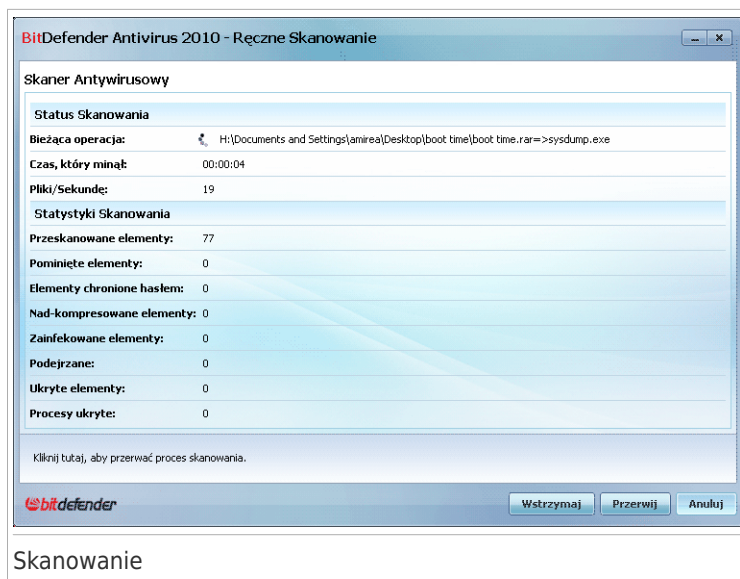
To zadanie zostanie dodane do listy Szybkich Zadań dostępnej w zakładce Bezpieczeństwo oraz pojawi się także w **Trybie Eksperta > Antywirus > Skanowanie**.

- Aby wyłączyć komputer po zakończeniu skanowania, zaznacz pole **Wyłącz komputer po zakończeniu skanowania jeśli nie znaleziono żadnych zagrożeń**.

Kliknij **Uruchom**.

11.2.5. Step 5/6 - Skanowanie

BitDefender rozpocznie skanowanie zaznaczonych elementów:

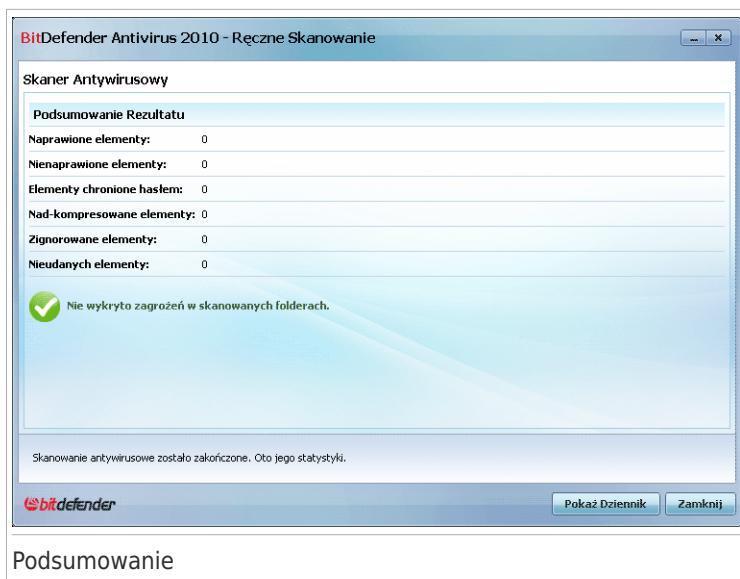


Notatka

Proces skanowania może chwilę potrwać, w zależności od złożoności skanowania. Możesz kliknąć na ikonę postępu skanowania  w **zasobniku systemowym** aby otworzyć okno skanowania i zobaczyć postępy.

11.2.6. Krok 6/6 – Wyświetl Rezultat

Kiedy BitDefender zakończy proces skanowania, w nowym oknie pojawią się wyniki skanowania:



Możesz zobaczyć podsumowanie. Jeśli chcesz wyczerpującej informacji na temat procesu skanowania, kliknij na **Pokaż Dziennik** aby zobaczyć dziennik skanowania.



WAŻNE

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

Kliknij **Zamknij** aby zamknąć okno.

11.3. Kreator Sprawdzania Podatności

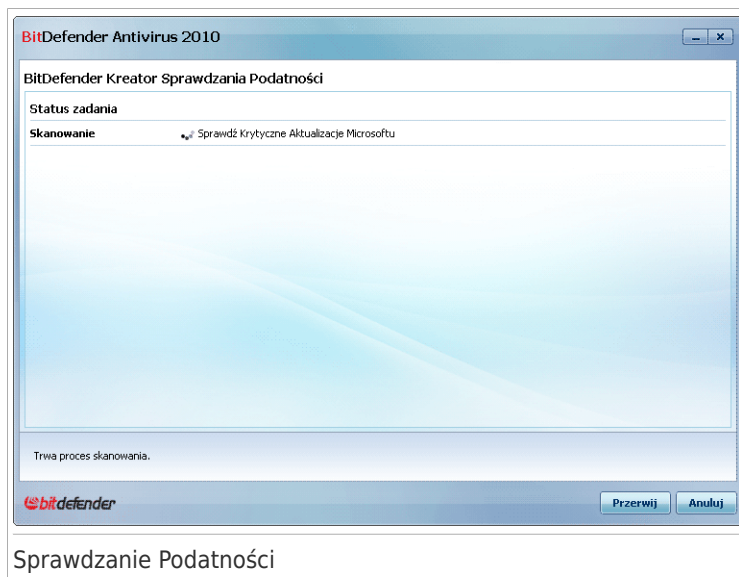
Ten kreator sprawdza podatności systemu na zagrożenia i pomaga je naprawić.

11.3.1. Krok 1/6 – Wybierz Podatności do Sprawdzenia



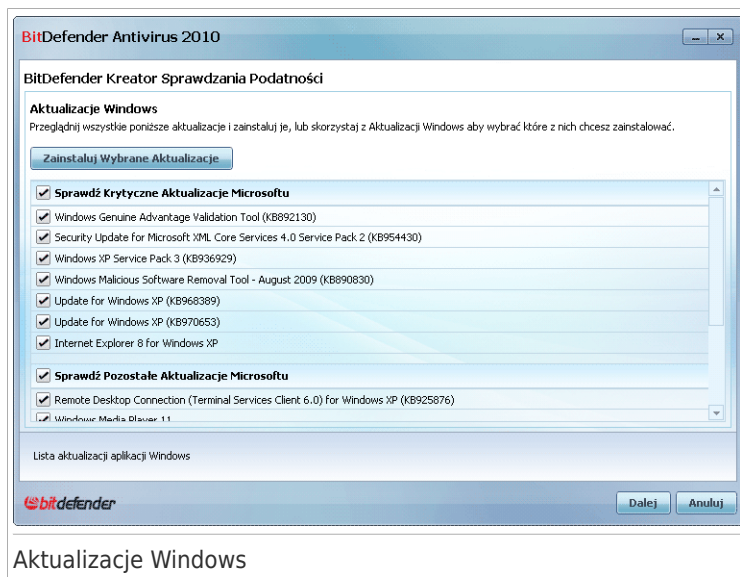
Kliknij **Dalej** aby sprawdzić wybrane podatności w systemie.

11.3.2. Krok 2/6 – Sprawdzanie Podatności



Zaczekaj aż BitDefender zakończy sprawdzanie podatności.

11.3.3. Krok 3/6 - Aktualizacja Windows

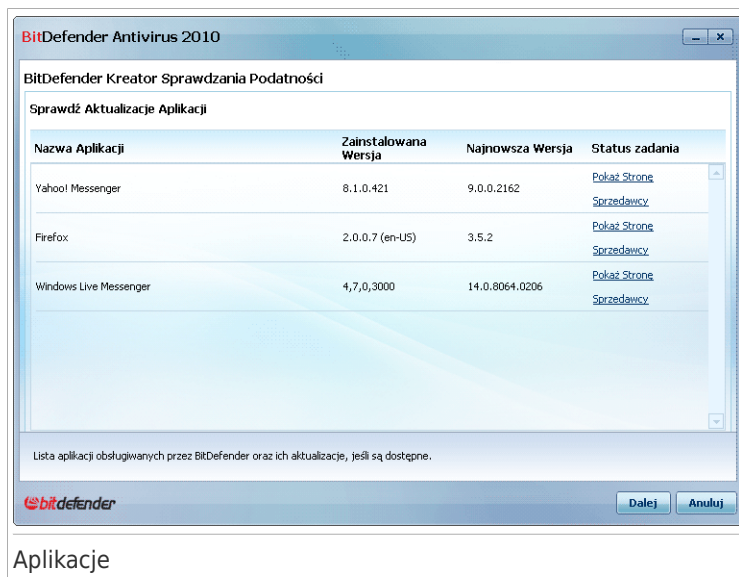


Aktualizacje Windows

Możesz zobaczyć listę krytycznych oraz nie krytycznych aktualizacji Windows które aktualnie nie są zainstalowane na twoim komputerze. Kliknij **Instaluj Wszystkie Aktualizacje Systemu** aby zainstalować wszystkie dostępne aktualizacje systemu.

Kliknij **Dalej**.

11.3.4. Krok 4/6 – Aktualizuj Aplikacje

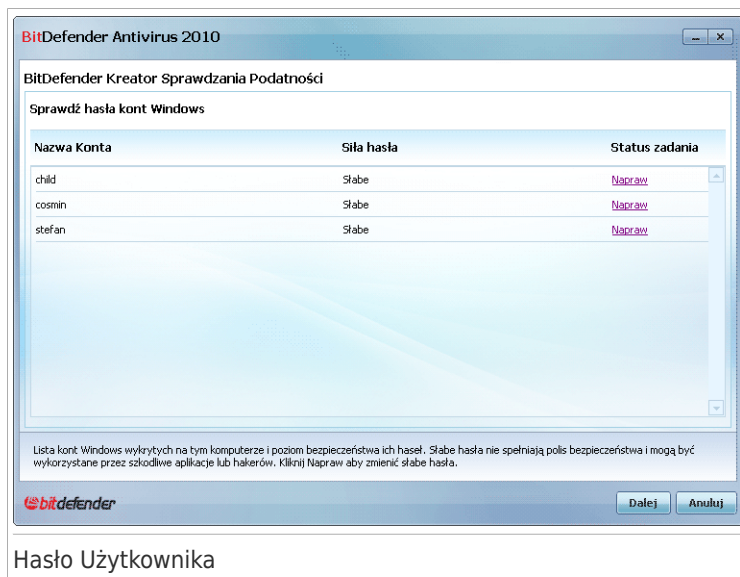


Aplikacje

Możesz zobaczyć listę aplikacji sprawdzonych przez BitDefendera oraz czy są one aktualne. Jeśli aplikacja jest nieaktualna, kliknij podany link aby pobrać najnowszą wersję.

Kliknij **Dalej**.

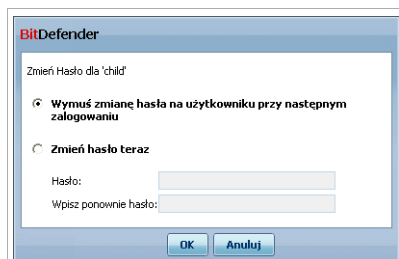
11.3.5. Krok 5/6 - Zmień Słabe Hasła



Hasło Użytkownika

Możesz zobaczyć listę użytkowników kont Windows skonfigurowanych na twoim komputerze i poziom ochrony jaki te hasła zapewniają. Siła hasła może być **silna** (trudne do odgadnięcia) lub **słaba** (łatwe do złamania przez ludzi o złych zamiarach korzystających ze specjalnego oprogramowania).

Kliknij **Napraw** aby zmodyfikować słabe hasła. Pojawi się nowe okno.



Zmień Hasło

Wybierz metodę naprawienia zagadnienia:

- **Wymuś zmianę hasła na użytkownika przy następnym zalogowaniu.** BitDefender poinstruuje użytkownika aby zmienił hasło przy następnym zalogowaniu do Windows.
- **Zmień hasło użytkownika.** Musisz wpisać nowe hasło do odpowiedniego pola edycji. Pamiętaj, że musisz poinformować użytkownika o zmianie hasła.



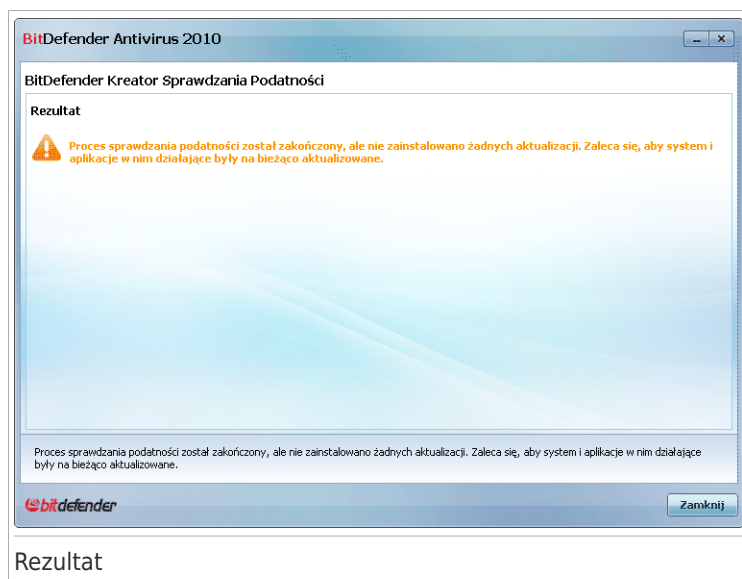
Notatka

Aby hasło było silne, użyj kombinacji dużych i małych liter, cyfr oraz znaków specjalnych (takich jak #, \$ lub @). Możesz przeszukać Internet aby znaleźć więcej informacji i wskazówek jak tworzyć silne hasła.

Kliknij **OK** aby zmienić hasło.

Kliknij **Dalej**.

11.3.6. Krok 6/6 – Wyświetl Rezultat



Kliknij **Zamknij**.

Tryb Średniozaawansowany

12. Pulpit

Zakładka Panel udostępnia informacje odnoszące się do stanu zabezpieczeń twojego komputera i pozwala naprawić istniejące zagrożenia.



Panel składa się z następujących sekcji:

- **Ogólny Stan** - Wskazuje na liczbę zagadnień wpływających na bezpieczeństwo komputera i pomaga je naprawić. Jeśli pojawiły się jakieś zagrożenia, zobaczysz **czerwone kółko z wykrzyknikiem** i przycisk **Napraw Wszystkie Zagadnienia**. Kliknij na przycisk, aby uruchomić kreator **Naprawiania Wszystkich Zagadnień**.
- **Szczegóły** - Wskazuje na stan każdego z modułów głównych za pomocą określonego zdania i jednej z następujących ikon:
 - ✓ **Zielone kółko:** Nie ma zagadnień wpływających na bezpieczeństwo komputera. Twój komputer i dane są chronione.
 - ⊗ **Szare kółko z wykrzyknikiem:** Aktywność komponentów tego modułu nie jest śledzona, nie ma więc żadnej informacji na temat jego stanu zabezpieczeń. Mogą istnieć pewne zagrożenia związane z tym modułem.
 - ! **Czerwone kółko z wykrzyknikiem:** Są zagrożenia, które wpływają na bezpieczeństwo twojego komputera. Krytyczne zagrożenia wymagają twojej natychmiastowej uwagi. Nie-krytyczne zagrożenia także powinny zostać jak najszybciej rozwiązane.

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

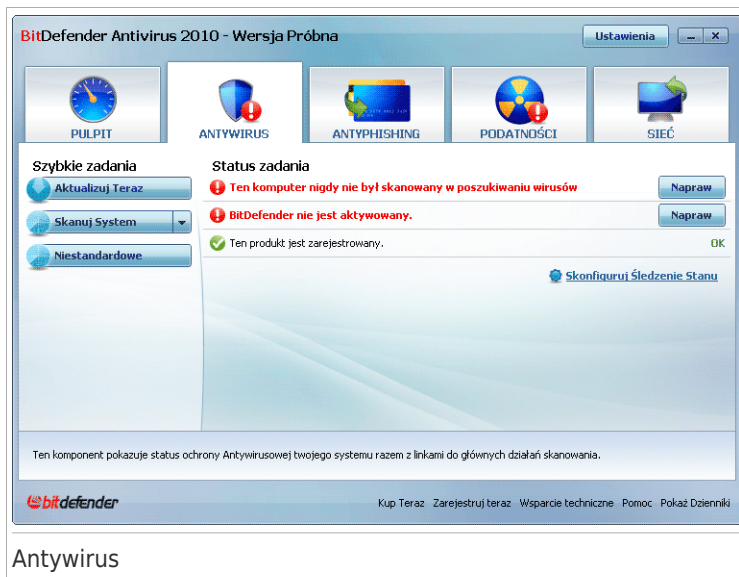
● **Profil Użytkowania** - Wskazuje na obecnie wybrany poziom użytkowania i oferuje skróty do odpowiednich zadań dla tego profilu:

- ▶ Kiedy zostanie wybrany profil **Typowy**, przycisk **Skanuj Teraz** pozwala na przeskanowanie systemu korzystając z **Kreatora Skanowania Antywirusowego**. Zostanie przeskanowany cały system, z wyjątkiem archiwów. W domyślnej konfiguracji, skanuje dla wszystkich typów złośliwego oprogramowania, oprócz **rootkitów**.
- ▶ Kiedy zostanie wybrany profil **Gracza**, przycisk **Włącz/Wyłącz Tryb Gry** pozwala na włączenie/wyłączenie **Trybu Gry**. Tryb Gry tymczasowo modyfikuje ustawienia zabezpieczeń aby zminimalizować ich wpływ na wydajność systemu.
- ▶ Kiedy profil **Użytkownika** jest wybrany, przycisk **Aktualizuj Teraz** rozpoczyna aktualizację. Pojawi się nowe okno w którym możesz obserwować status aktualizacji.

Jeśli chcesz przełączyć się na inny profil lub edytować bieżący, kliknij na profil i podążaj według zaleceń **kreatora konfiguracji**.

13. Antywirus

BitDefender zawiera moduł Antywirusowy, który pomaga na bieżąco aktualizować i chronić komputer przed wirusami. Aby wejść do modułu Antywirusowego kliknij zakładkę **Antywirus**.



Moduł Antywirusowy zawiera dwie sekcje:

- **Pole Stanu** - Wyświetla aktualny stan monitorowanych komponentów i pozwala wybrać, które z nich mają być monitorowane.
- **Szybkie Zadania** - Tutaj możesz znaleźć linki do najważniejszych zadań: aktualizacji, skanowania systemu, głębokiego skanowania systemu, skanowania moich dokumentów oraz skanowania zdefiniowanego przez użytkownika.

13.1. Pole Stanu

Pole stanu zawiera kompletną listę modułów bezpieczeństwa i ich aktualny stan. Poprzez monitorowanie modułu bezpieczeństwa, BitDefender pokazuje kiedy skonfigurować ustawienia, które wpływają na bezpieczeństwo komputera i informuje o ważnych zadaniach o których zapomniał użytkownik.

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.

Zdania opisujące zagadnienia są oznaczone czerwoną czcionką. Kliknij na przycisk **Napraw** przy odpowiednim zdaniu aby naprawić zgłaszane zagadnienie. Jeżeli jakiś problem nie naprawi się od razu, skorzystaj z kreatora.

13.1.1. Konfiguracja Śledzenia Stanu

Aby wybrać komponenty, które BitDefender powinien monitorować, kliknij **Konfiguruj Stan Śledzenia** i zaznacz pole **Włącz alarmy** odpowiadające zagadnieniu, które chcesz śledzić.



WAŻNE

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

BitDefender może śledzić stan następujących komponentów:

- **Antywirus** - BitDefender monitoruje stan dwóch komponentów: ochrony w czasie rzeczywistym i skanowania na żądanie. Najczęściej zgłaszane zagadnienia dla tego komponentu są wypisane w poniższej tabeli.

Zagadnienie	Opis
Ochrona w czasie rzeczywistym jest zablokowana	Pliki nie są skanowane przy dostępie do nich przez użytkownika lub aplikacji uruchomionych w systemie.
Ten komputer nigdy nie był skanowany w poszukiwaniu wirusów	Skanowanie systemu na żądanie nigdy nie było przeprowadzone aby sprawdzić, czy pliki przechowywane na komputerze są wolne od wirusów.
Ostatnie uruchomione skanowanie systemu nie zostało ukończone	Uruchomione pełne skanowanie systemu nie zostało zakończone.
Antywirus znajduje się w stanie krytycznym	Ochrona w czasie rzeczywistym jest wyłączona a skanowanie systemu nie było od dawna przeprowadzane.

- **Aktualizacja** - BitDefender monitoruje czy sygnatury wirusów są aktualne. Najczęściej zgłaszane zagadnienia dla tego komponentu są wypisane w poniższej tabeli.

Zagadnienie	Opis
Automatyczna aktualizacja jest wyłączona	Sygnatury wirusów twojego BitDefendera nie są automatycznie i regularnie aktualizowane.
Aktualizacja nie była wykonywana x dni	Sygnatury wirusów twojego BitDefendera są nieaktualne.

13.2. Szybkie zadania

Tutaj możesz odnaleźć skróty do najważniejszych zadań bezpieczeństwa:

- **Zaktualizuj Teraz** - uruchamia aktualizację.
- **Skanowanie Systemu** - uruchamia pełne skanowanie całego komputera (bez archiwów). Aby uruchomić inne zadania skanowania na żądanie, kliknij na  ten przycisk i wybierz inne zadanie skanowania: Skanowanie Moich Dokumentów lub Głębokie Skanowanie Systemu.
- **Własne Skanowanie** - uruchamia kreator, który pozwala tworzyć i uruchamiać własne zadania skanowania.

13.2.1. Aktualizowanie BitDefendera

Nowe złośliwe oprogramowanie jest znajduwane i identyfikowane każdego dnia. Dlatego bardzo ważnym jest aby na bieżąco aktualizować BitDefendera najnowszymi sygnaturami.

Domyślnie BitDefender sprawdza aktualizacje w trakcie włączania komputera i potem **co godzinę**. Jednak jeżeli chcesz zaktualizować BitDefender po prostu kliknij **Zaktualizuj Teraz**. Proces aktualizacji zostanie rozpoczęty i pojawi się następujące okno:



W tym oknie możesz zobaczyć status procesu aktualizacji.

Proces aktualizacji wykonywany jest w trakcie, co oznacza że pliki będą aktualizowane na bieżąco. W ten sposób, aktualizacja nie będzie miała wpływu na pracę produktu i jednocześnie podatności zostaną wyeliminowane.

Jeżeli chcesz zamknąć to okno, kliknij **Anuluj**. Jednak nie zatrzyma to procesu aktualizacji.



Notatka

Jeśli łączysz się z Internetem za pomocą modemu, zalecane jest regularne aktualizowanie BitDefendera na żądanie.

Uruchom ponownie komputer jeśli jest to wymagane. W przypadku znaczących aktualizacji zostaniesz poproszony o restart komputera. Kliknij **Zrestartuj** aby natychmiast zrestartować komputer.

Jeżeli chcesz zrestartować komputer później, po prostu kliknij **OK**. Zalecamy zrestartować system najszybciej jak to możliwe.

13.2.2. Skanowanie BitDefenderem

Aby skanować komputer pod kątem złośliwego oprogramowania, uruchom odpowiednie zadanie klikając na odpowiadający mu przycisk lub wybierając je z rozwijanego menu. Poniższa tabela przedstawia dostępne zadania skanowania, wraz z ich opisem:

Zadanie	Opis
Skanowanie Systemu	Skanuje cały system wyłączając archiwa. W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów .
Skanuj Moje Dokumenty	Użyj tego zadania aby przeskanować ważne foldery aktywnego użytkownika: Moje Dokumenty, Pulpit i Autostart. To zapewni bezpieczeństwo twoim dokumentom, bezpieczne środowisko pracy i aplikacje wolne od wirusów.
Głębokie Skanowanie	Skanuje cały system. W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.
Skanowanie Użytkownika	Użyj tego zadania aby podać pliki oraz foldery do skanowania.



Notatka

Głębokie Skanowanie Systemu i **Skanowanie Systemu** mogą chwilę potrwać, obciążając przy tym zasoby komputera. Zadania tego typu najlepiej uruchamiać z niskim priorytetem, lub kiedy nie korzystasz z komputera.

Kiedy uruchomisz Skanowanie Systemu, Głębokie Skanowanie Systemu lub Skanowanie Moich Dokumentów, pojawi się kreator skanowania antywirusowego. Wykonaj następujące trzy kroki procedury aby zakończyć skanowanie komputera. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Skanowania Antywirusowego*” (p. 53).

Kiedy uruchomisz Własne Skanowanie, pojawi się odpowiedni kreator i poprowadzi przez proces skanowania. Podążaj za procedurą aby przeskanować poszczególne pliki i katalogi. Aby uzyskać więcej informacji na temat tego kreatora, odwołaj się do „*Kreator Własnego Skanowania*” (p. 57).

14. Antyphishing

BitDefender zawiera moduł Antyphishingowy, który zapewnia, że wszystkie strony www przeglądane przez Internet Explorer lub Firefox są bezpieczne. Aby wejść do modułu Antyphishingowego kliknij zakładkę **Antyphishing**.



Moduł Antyphishingowy zawiera dwie sekcje:

- **Pole Stanu** - Wyświetla aktualny stan modułu Antyphishing i pozwala wybrać, które z jego opcji mają być monitorowane.
- **Szybkie Zadania** - Tutaj możesz znaleźć linki do najważniejszych zadań: aktualizacji, skanowania systemu i głębokiego skanowania systemu.

14.1. Pole Stanu

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.
- Zdania opisujące zagadnienia są oznaczone czerwoną czcionką. Kliknij na przycisk **Napraw** przy odpowiednim zdaniu aby naprawić zgłaszane zagadnienie.

Najczęściej zgłaszanym zagadnieniem dla tego modułu jest **Antyphishing jest zablokowany**. Oznacza to, że Antyphishing nie jest włączony dla jakiejkolwiek z obsługiwanych aplikacji: Internet Explorer, Mozilla Firefox, Yahoo! Messenger lub Windows Live Messenger.

14.2. Szybkie zadania

Tutaj możesz odnaleźć skróty do najważniejszych zadań bezpieczeństwa:

- **Zaktualizuj Teraz** - uruchamia aktualizację.
- **Skanowanie Systemu** - uruchamia pełne skanowanie komputera (bez archiwów).
- **Głębokie Skanowanie Systemu** - uruchamia pełne skanowanie komputera (także archiwa).

14.2.1. Aktualizowanie BitDefendera

Nowe złośliwe oprogramowanie jest znajduwane i identyfikowane każdego dnia. Dlatego bardzo ważnym jest aby na bieżąco aktualizować BitDefendera najnowszymi sygnaturami.

Domyślnie BitDefender sprawdza aktualizacje w trakcie włączania komputera i potem **co godzinę**. Jednak jeżeli chcesz zaktualizować BitDefender po prostu kliknij **Zaktualizuj Teraz**. Proces aktualizacji zostanie rozpoczęty i pojawi się następujące okno:



Aktualizowanie BitDefendera

W tym oknie możesz zobaczyć status procesu aktualizacji.

Proces aktualizacji wykonywany jest w trakcie, co oznacza że pliki będą aktualizowane na bieżąco. W ten sposób, aktualizacja nie będzie miała wpływu na pracę produktu i jednocześnie podatności zostaną wyeliminowane.

Jeżeli chcesz zamknąć to okno, kliknij **Anuluj**. Jednak nie zatrzyma to procesu aktualizacji.



Notatka

Jeśli łączysz się z Internetem za pomocą modemu, zalecane jest regularne aktualizowanie BitDefendera na żądanie.

Uruchom ponownie komputer jeśli jest to wymagane. W przypadku znaczących aktualizacji zostaniesz poproszony o restart komputera. Kliknij **Zrestartuj** aby natychmiast zrestartować komputer.

Jeżeli chcesz zrestartować komputer później, po prostu kliknij **OK**. Zalecamy zrestartować system najszybciej jak to możliwe.

14.2.2. Skanowanie BitDefenderem

Aby skanować komputer pod kątem złośliwego oprogramowania, uruchom odpowiednie zadanie klikając na odpowiadający mu przycisk lub wybierając je z rozwijanego menu. Poniższa tabela przedstawia dostępne zadania skanowania, wraz z ich opisem:

Zadanie	Opis
Skanowanie Systemu	Skanuje cały system wyłączając archiwa. W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów .
Głębokie Skanowanie	Skanuje cały system. W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.



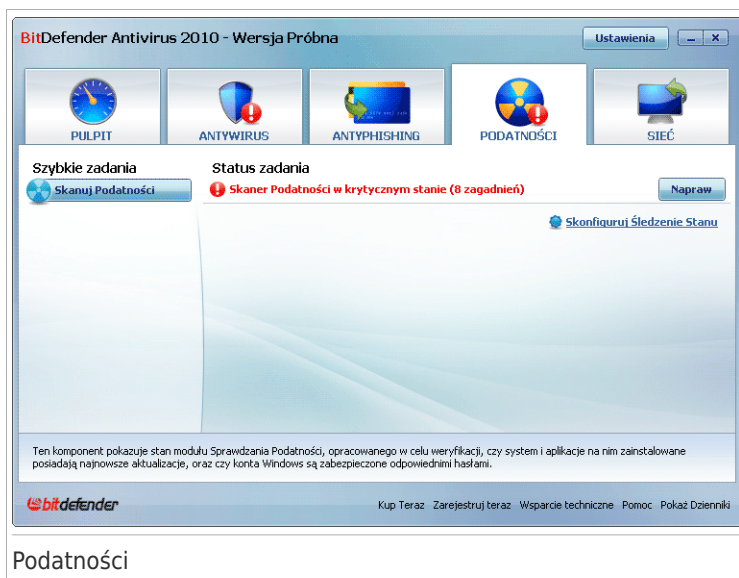
Notatka

Głębokie Skanowanie Systemu i **Skanowanie Systemu** mogą chwilę potrwać, obciążając przy tym zasoby komputera. Zadania tego typu najlepiej uruchamiać z niskim priorytetem, lub kiedy nie korzystasz z komputera.

Kiedy uruchomisz Skanowanie Systemu lub Głębokie Skanowanie Systemu, pojawi się kreator skanowania antywirusowego. Wykonaj następujące trzy kroki procedury aby zakończyć skanowanie komputera. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Skanowania Antywirusowego*” (p. 53).

15. Podatności

BitDefender zawiera moduł Podatności, który pomaga dokonywać aktualizacji najważniejszego oprogramowania na twoim PC. Aby monitorować i naprawiać luki w systemie, kliknij na zakładkę **Podatności**.



Moduł Podatności zawiera dwie sekcje:

- **Pole Stanu** - Wyświetla aktualny stan modułu Sprawdzanie Podatności i pozwala wybrać, które z jego opcji mają być monitorowane.
- **Szybkie Zadania** - Tutaj znajdziesz link do kreatora sprawdzania podatności.

15.1. Pole Stanu

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.

Zdania opisujące zagadnienia są oznaczone czerwoną czcionką. Wystarczy że klikniesz na przycisk **Napraw** lub **Instaluj** przy odpowiednim zdaniu aby naprawić zgłaszane zagadnienie.

Najczęściej zgłaszane zagadnienia dla tego komponentu są wypisane w poniższej tabeli.

Status zadania	Opis
Sprawdzanie Podatności jest wyłączone	BitDefender nie sprawdza potencjalnych podatności dotyczących brakujących aktualizacji Windows lub innych aplikacji, oraz słabych haseł.
Wykryto wiele podatności	BitDefender odnalazł brakujące aktualizacje Windows lub innych aplikacji i/lub słabe hasła.
Krytyczne aktualizacje Microsoft	Krytyczne aktualizacje Microsoft są dostępne, ale nie zostały zainstalowane.
Inne aktualizacje Microsoft	Nie-krytyczne aktualizacje Microsoft są dostępne, ale nie zostały zainstalowane.
Automatyczne Aktualizacje Windows są wyłączone	Nowe aktualizacje zabezpieczeń Windows nie są automatycznie instalowane.
Aplikacja (przedawniona)	Nowa wersja Aplikacji jest dostępna, ale nie jest zainstalowana.
Użytkownik (Słabe Hasło)	Hasło użytkownika może zostać łatwo złamane przez inne osoby lub specjalistyczne oprogramowanie.

15.2. Szybkie zadania

Jest tylko jedno dostępne zadanie:

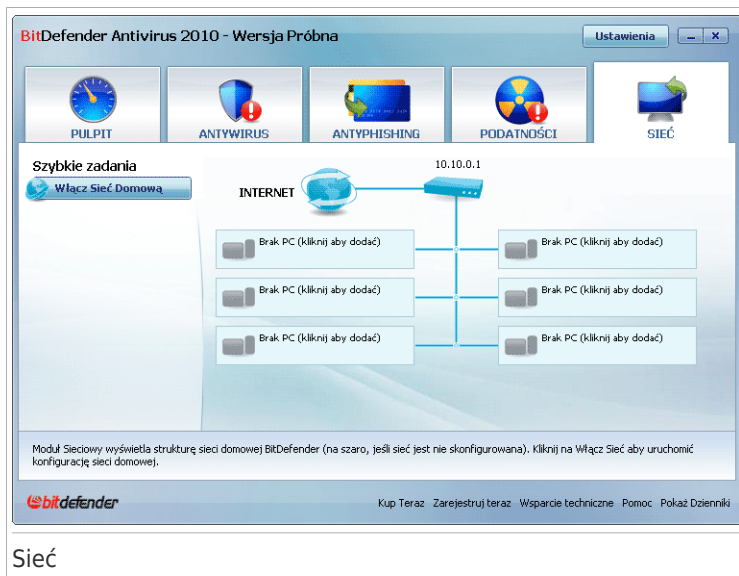
- **Skanowanie podatności** - uruchamia kreator który sprawdza czy twój system jest podatny na zagrożenia i posiada luki w zabezpieczeniach, a następnie pomaga je naprawić.

Skanowanie Podatności sprawdza aktualizacje Microsoft Windows, Microsoft Windows Office oraz hasło do twojego konta w systemie Windows aby mieć pewność że twój system jest aktualny oraz niepodatny na złamanie hasła.

Aby sprawdzić czy twój komputer jest podatny na zagrożenia, kliknij na **Skanowanie Podatności** i podążaj według „*Kreator Sprawdzania Podatności*” (p. 65).

16. Sieć

Moduł Sieci pozwala tobie na zarządzanie produktami BitDefender zainstalowanymi na komputerach w twoim domu z pojedynczego komputera. Aby przejść do modułu sieciowego, kliknij zakładkę **Sieć**.



Aby móc zarządzać produktami BitDefender zainstalowanymi na twoich domowych komputerach, musisz wykonać następujące kroki:

1. Dołącz do sieci domowej BitDefender. Dołączenie do sieci wymaga skonfigurowania hasła administracyjnego do zarządzania siecią domową.
2. Idź do każdego komputera którym chcesz zarządzać i dołącz go do swojej sieci (ustaw hasło)
3. Wróć do swojego komputera i dodaj komputery którymi chcesz zarządzać.

16.1. Szybkie zadania

Początkowo tylko jeden przycisk jest dostępny.

● **Odblokuj Sieć** - pozwala ustawić hasło, stworzyć i dołączyć się do sieci.

Po dołączeniu do sieci, pojawi się kilka nowych przycisków.

● **Zablokuj Sieć** - pozwala opuścić sieć.

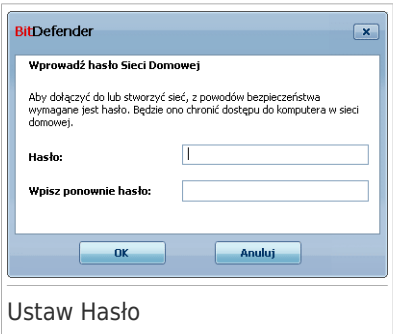
● **Dodaj komputer** - pozwala dodawać komputery do twojej sieci.

- **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.

16.1.1. Dołączanie do Sieci BitDefender

Aby dołączyć do sieci domowej BitDefender, wykonaj następujące kroki:

1. Kliknij na **Odblokuj Sieć**. Zostaniesz poproszony o ustawienie hasła domowego zarządzania.



Ustaw Hasło

2. Wpisz to samo hasło we wszystkie pola edycji.

3. Kliknij **OK**.

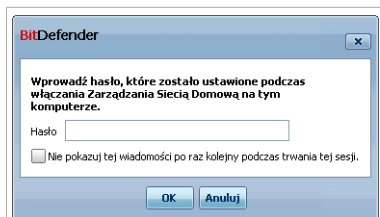
Możesz zobaczyć nazwę komputerów pojawiających się w sieci.

16.1.2. Dodawanie Komputerów do Sieci BitDefender

Zanim będziesz mógł dodać komputer do domowej sieci BitDefender, musisz ustawić hasło domowego zarządzania na tym komputerze.

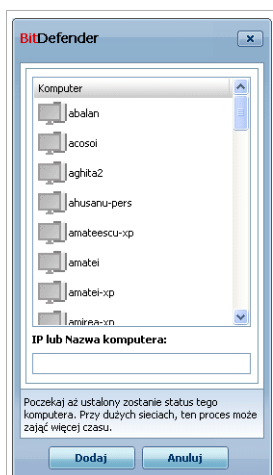
Aby dodać komputer do domowej sieci BitDefendera, wykonaj następujące kroki:

1. Kliknij na **Dodaj Komputer**. Zostaniesz poproszony o podanie hasła domowego zarządzania.



Wpisz Hasło

2. Wprowadź swoje hasło domowego zarządzania i kliknij **OK**. Pojawi się nowe okno.

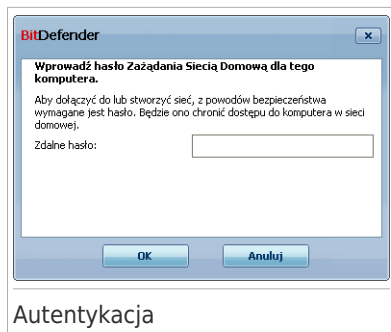


Dodaj Komputer

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.

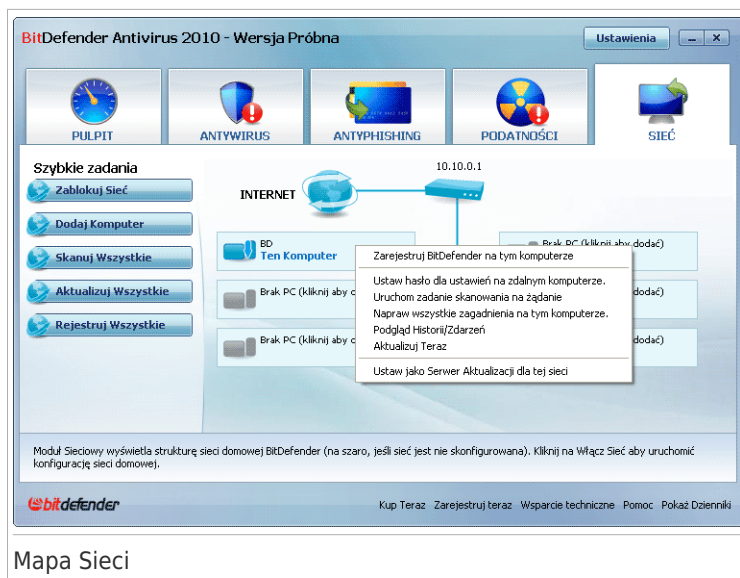


Notatka

Możesz dodać do pięciu komputerów do sieci.

16.1.3. 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 prawym klawiszem na komputerze na mapie sieci, możesz zobaczyć wszystkie zadania administracyjne które możesz przeprowadzić zdalnie na komputerze.

● **Usuń komputer z sieci domowej**

Pozwala na usunięcie komputera z sieci.

● **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 zagrożenia na tym komputerze**

Pozwala naprawić zagadnienia, które wpływają na bezpieczeństwo komputera za pomocą kreatora **Napraw Wszystkie Zagadnienia**.

● Pokaż Historię/Zdarzenia

Pozwala na dostęp do modułu **Historia&Zdarzenia** BitDefendera zainstalowanego na tym komputerze.

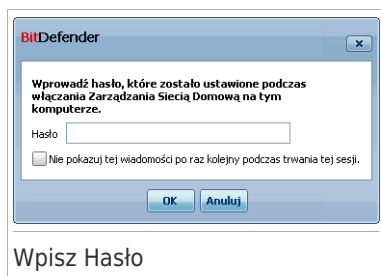
● Aktualizuj Teraz

Rozpoczyna proces Aktualizacji dla oprogramowania BitDefender zainstalowanego na tym komputerze.

● Ustaw 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.

Przed uruchomieniem zadania na konkretnym komputerze, będziesz poproszony o podanie lokalnego hasła zarządzania domowego.



Wprowadź swoje hasło domowego zarządzania i kliknij **OK**.



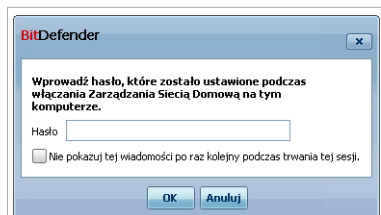
Notatka

Jeśli planujesz uruchamiać kilka zadań, możesz zaznaczyć **Nie pokazuj tej wiadomości ponownie w tej sesji**. Zaznaczając tę opcję, nie będziesz pytany ponownie o hasło podczas tej sesji.

16.1.4. Skanowanie Wszystkich Komputerów

Aby przeskanować wszystkie zarządzane komputery, wykonaj następujące kroki:

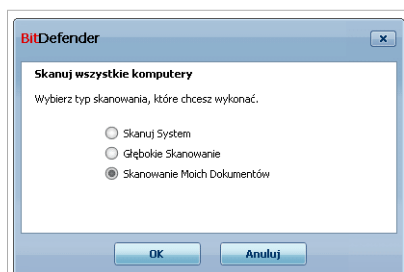
1. Kliknij **Skanuj Wszystkie**. Zostaniesz poproszony o podanie hasła domowego zarządzania.



Wpisz Hasło

2. Wybierz typ skanowania.

- **Skanowanie Systemu** - uruchamia pełne skanowanie komputera (bez archiwów).
- **Głębokie Skanowanie Systemu** - rozpoczyna pełne skanowanie twojego komputera (łącznie z archiwami).
- **Skanuj Moje Dokumenty** - rozpoczyna szybkie skanowanie twoich dokumentów i ustawień.



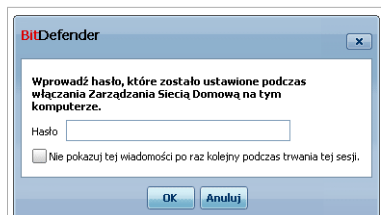
Wybierz Typ Skanowania

3. Kliknij **OK**.

16.1.5. Aktualizowanie Wszystkich Komputerów

Aby zaktualizować wszystkie zarządzane komputery, wykonaj następujące kroki:

1. Kliknij **Aktualizuj Wszystkie**. Zostaniesz poproszony o podanie hasła domowego zarządzania.



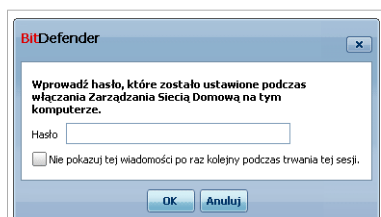
Wpisz Hasło

2. Kliknij **OK**.

16.1.6. Rejestrowanie Wszystkich Komputerów

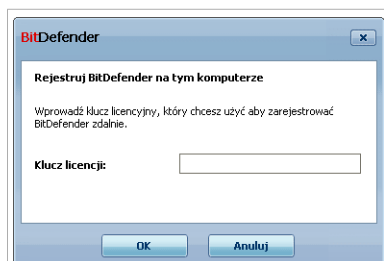
Aby zarejestrować wszystkie zarządzane komputery, wykonaj następujące kroki:

1. Kliknij **Zarejestruj Wszystkie**. Zostaniesz poproszony o podanie hasła domowego zarządzania.



Wpisz Hasło

2. Wpisz klucz którym chcesz je zarejestrować.



Rejestruj Wszystkie

3. Kliknij **OK**.

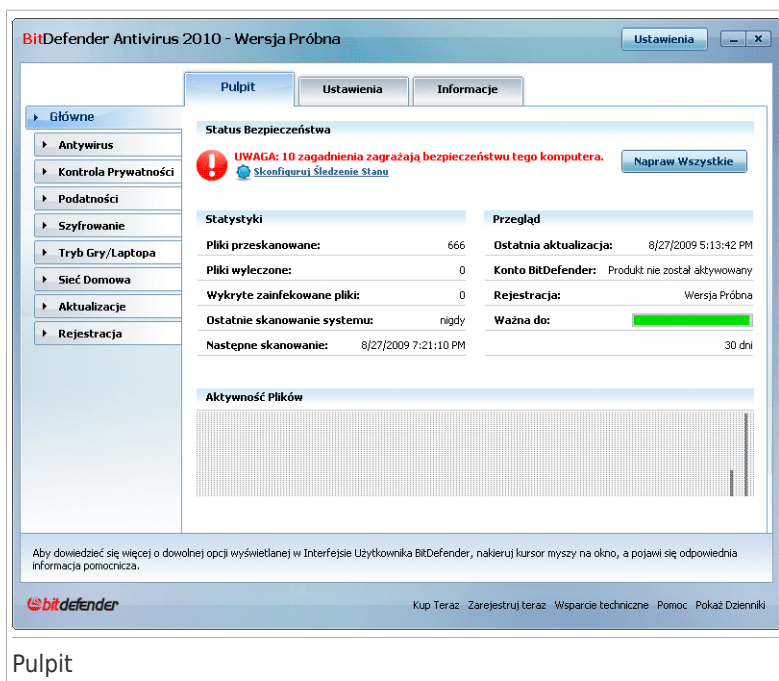
Tryb Eksperta

17. Ogólne

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

17.1. Pulpit

Aby sprawdzić czy są jakieś zagrożenia dotyczące bezpieczeństwa komputera, oraz zobaczyć statystyki aktywności i stan rejestracji, przejdź **Główne i Panel** w Trybie Eksperta.



Pulpit składa się z kilku części:

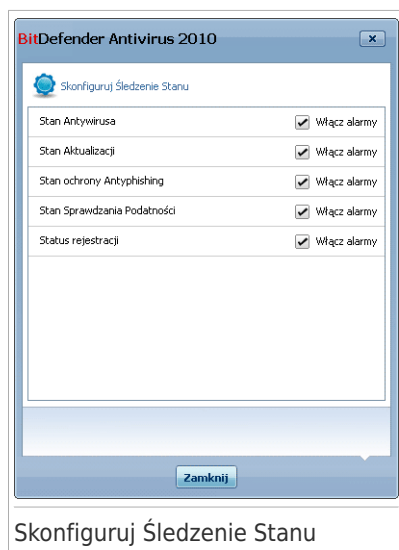
- **Ogólny Stan** - Informuje o zagrożeniach wpływających na bezpieczeństwo twojego komputera.
- **Statystyki** - Wyświetla ważne informacje dotyczące aktywności BitDefendera.
- **Podgląd** - Wyświetla status aktualizacji, status twojego konta, informacje o rejestracji i licencji.

- **Pliki** - Wyświetla ilość obiektów przeskanowanych przez BitDefender. Wysokość pasków pokazuje intensywność ruchu w danym okresie czasu.

17.1.1. Ogólny Stan

Tutaj możesz sprawdzić liczbę zagadnień które wpływają na bezpieczeństwo twojego komputera. Aby usunąć wszystkie zagrożenia, kliknij **Napraw wszystkie zagadnienia**. Uruchom się kreator **Naprawiania Wszystkich Zagadnień**.

Aby skonfigurować, które moduły mają być śledzone przez BitDefender Antivirus 2010, kliknij **Konfiguruj Stan Śledzenia**. Pojawi się nowe okno:



Jeśli chcesz aby BitDefender monitorował komponent, zaznacz pole **Włącz alarmy** dla wybranego komponentu. BitDefender może śledzić stan następujących komponentów:

- **Antywirus** - BitDefender monitoruje stan dwóch komponentów tego modułu: ochrony w czasie rzeczywistym i skanowania na żądanie. Najczęściej zgłaszane zagadnienia dla tego komponentu są wypisane w poniższej tabeli.

Zagadnienie	Opis
Ochrona w czasie rzeczywistym jest zablokowana	Pliki nie są skanowane przy dostępie do nich przez użytkownika lub aplikacji uruchomionych w systemie.

Zagadnienie	Opis
Nigdy nie skanowałeś komputera w poszukiwaniu wirusów	Skanowanie systemu na żądanie nigdy nie było przeprowadzone aby sprawdzić, czy pliki przechowywane na komputerze są wolne od wirusów.
Ostatnie uruchomione skanowanie systemu nie zostało ukończone	Uruchomione pełne skanowanie systemu nie zostało zakończone.
Antywirus znajduje się w stanie krytycznym	Ochrona w czasie rzeczywistym jest wyłączona a skanowanie systemu nie było od dawna przeprowadzane.

- **Aktualizacja** - BitDefender monitoruje czy sygnatury wirusów są aktualne. Najczęściej zgłaszane zagadnienia dla tego komponentu są wypisane w poniższej tabeli.

Zagadnienie	Opis
Automatyczna aktualizacja jest wyłączona	Sygnatury wirusów twojego BitDefendera nie są automatycznie i regularnie aktualizowane.
Aktualizacja nie była wykonywana x dni	Sygnatury wirusów twojego BitDefendera są nieaktualne.

- **Antyphishing** - BitDefender monitoruje stan modułu Antyphishing. Jeśli nie został odblokowany dla wszystkich obsługiwanych aplikacji, pojawi się zagadnienie **Antyphishing jest wyłączony**.
- **Sprawdzanie Podatności** - BitDefender śledzi moduł Sprawdzania Podatności. Sprawdzanie Podatności pomaga określić, czy wymagana jest instalacja nowych aktualizacji dla Windows i innych aplikacji oraz czy są hasła które należy wzmocnić. Najczęściej zgłaszane zagadnienia dla tego komponentu są wypisane w poniższej tabeli.

Status zadania	Opis
Sprawdzanie Podatności jest wyłączone	BitDefender nie sprawdza potencjalnych podatności dotyczących brakujących aktualizacji Windows lub innych aplikacji, oraz słabych haseł.
Wykryto wiele podatności	BitDefender odnalazł brakujące aktualizacje Windows lub innych aplikacji i/lub słabe hasła.

Status zadania	Opis
Krytyczne aktualizacje Microsoft	Krytyczne aktualizacje Microsoft są dostępne, ale nie zostały zainstalowane.
Inne aktualizacje Microsoft	Nie-krytyczne aktualizacje Microsoft są dostępne, ale nie zostały zainstalowane.
Automatyczne Aktualizacje Windows są wyłączone	Nowe aktualizacje zabezpieczeń Windows nie są automatycznie instalowane.
Aplikacja (przedawniona)	Nowa wersja Aplikacji jest dostępna, ale nie jest zainstalowana.
Użytkownik (Słabe Hasło)	Hasło użytkownika może zostać łatwo złamane przez inne osoby lub specjalistyczne oprogramowanie.



WAŻNE

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

17.1.2. Statystyki

Jeśli chcesz mieć oko na aktywność BitDefendera, dobrym miejscem do zaczęcia jest sekcja Statystyk. Możesz zobaczyć następujące elementy:

Element	Opis
Pliki przeskanowane	Pokazuje ilość plików które zostały sprawdzone przed zagrożeniami w czasie ostatniego skanowania.
Pliki wyleczone	Pokazuje ilość plików które zostały wyleczone w czasie ostatniego skanowania.
Wykryte zainfekowane pliki	Pokazuje ilość zainfekowanych plików, które zostały wykryte podczas ostatniego skanowania.
Ostatnie skanowanie systemu	Wskazuje kiedy twój komputer był ostatni raz skanowany. Jeśli ostatnie skanowanie nie zostało przeprowadzone od ponad tygodnia, proszę przeskanować system tak szybko jak to możliwe. Możesz przeskanować cały komputer, przejść do zakładki Antyvirus , Virus Scan i uruchomić pełne lub głębokie skanowanie systemu.
Następne skanowanie	Wskazuje czas, kiedy twój komputer będzie następny raz skanowany.

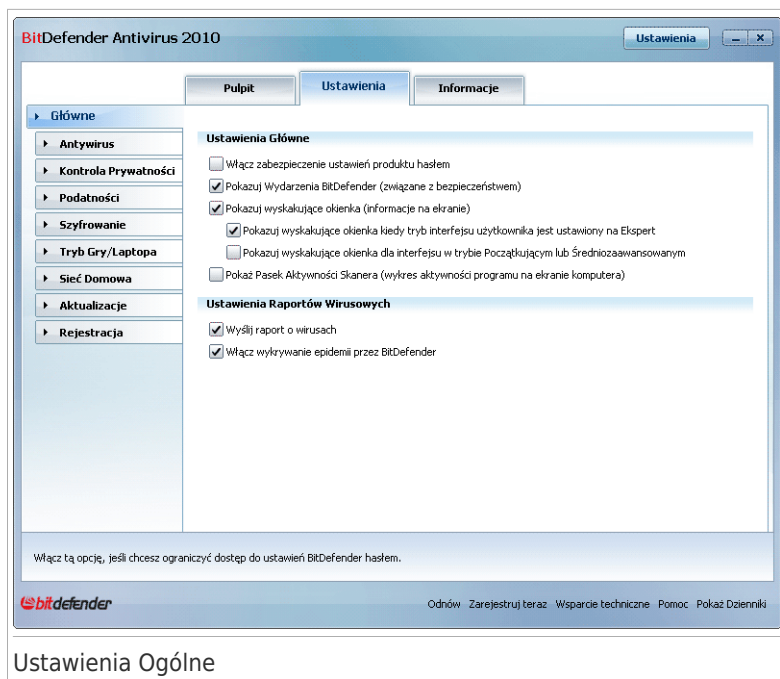
17.1.3. Przegląd

Tutaj możesz obejrzeć status aktualizacji, status konta, rejestracji i informacji o licencji.

Element	Opis
Ostatnia aktualizacja	Wskazuje kiedy twój produkt BitDefender był ostatni raz aktualizowany. Aby w pełni chronić system, wykonuj aktualizacje regularnie.
Konto BitDefender	Pokazuje adres email którego możesz użyć aby dostać się na swoje konto online aby odzyskać starzony klucz licencyjny BitDefendera skorzystać z pomocy technicznej oraz innych usług. Musisz stworzyć konto BitDefender, aby móc aktywować ten produkt. Aby uzyskać więcej informacji na temat konta BitDefender, odwołaj się do „ <i>Rejestracja i Moje Konto</i> ” (p. 48).
Rejestracja	Pokazuje typ oraz status twojej licencji. Aby zachować ochronę systemu musisz odnowić lub zaktualizować BitDefendera jeśli twój klucz wygaśnie.
Wygaśnięcie za	Pokazuje ilość dni jakie pozostały do wygaśnięcia klucza licencyjnego. Jeśli klucz licencyjny wygaśnie ciągu najbliższych dni, proszę zarejestrować produkt aby otrzymać nowy klucz. Aby zakupić nowy klucz licencyjny lub odnowić licencję, kliknij na Kup/Odnów , w dolnej części okna.

17.2. Ustawienia

Aby skonfigurować ogólne ustawienia dla BitDefendera i zarządzać jego ustawieniami, przejdź do **Ustawienia Główne** w Trybie Eksperta.



Tutaj możesz ustawić całkowite działanie BitDefender. Przez domyślne, BitDefender jest ładowany przy starcie Windows, a następnie uruchamia się zminimalizowany w system tray.

17.2.1. Ustawienia Ogólne

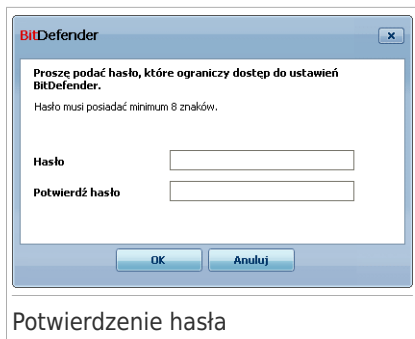
- **Włącz zabezpieczenie ustawień produktu hasłem** - umożliwia ustawianie hasła do ochrony konfiguracji BitDefendera.



Notatka

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

Jeśli wybierzesz tę opcję, pojawi się następne okno:



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

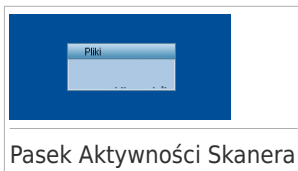
Gdy ustawisz hasło, będziesz o nie pytany za każdym razem gdy będziesz chciał modyfikować ustawienia BitDefendera. Inni administratorzy systemu (jeśli są) też będą musieli wprowadzić hasło przy dokonywaniu zmian w ustawieniach BitDefendera.



WAŻNE

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

- **Pokaż Wiadomości BitDefendera (związane z bezpieczeństwem)** - pokazuje informacje związane z bezpieczeństwem, wysyłane przez serwer BitDefendera.
- **Pokaż wyskakujące okienka** - pokazuje okienka dotyczące statusu produktu. Możesz skonfigurować BitDefender tak aby wyświetlał okienka informacyjne tylko wtedy, gdy interfejs użytkownika znajduje się w Trybie Początkującym / 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 jest dostępny tylko gdy interfejs znajduje się w Trybie Eksperta.

17.2.2. 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.

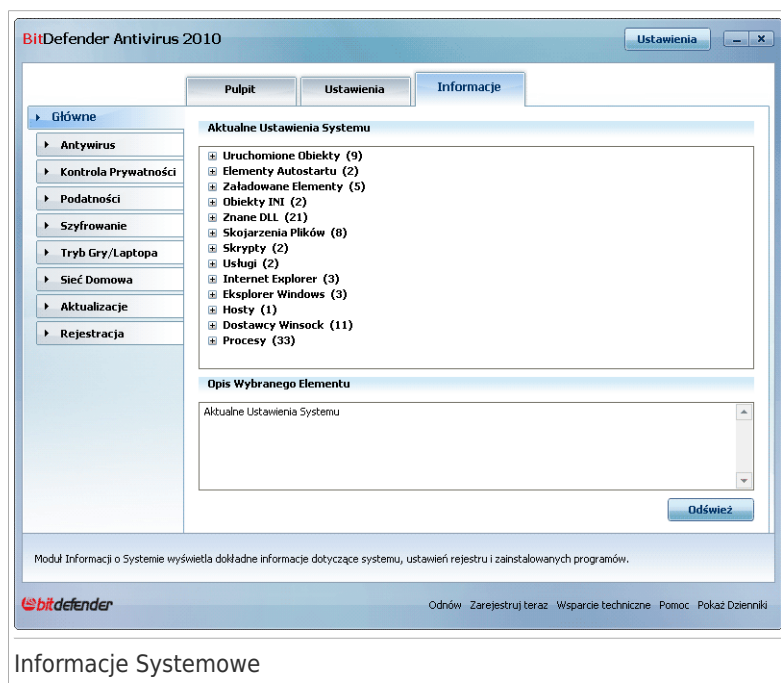
- **Włącz Wykrywanie Włamań BitDefendera** - wysyła raporty dotyczące potencjalnych włamań wirusów do Laboratorium BitDefendera.

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.

17.3. 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.

By uzyskać informacje o systemie, kliknij **Główne>Informacje Systemowe** w Trybie Eksperta.



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**.

18. Antywirus

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.



Notatka

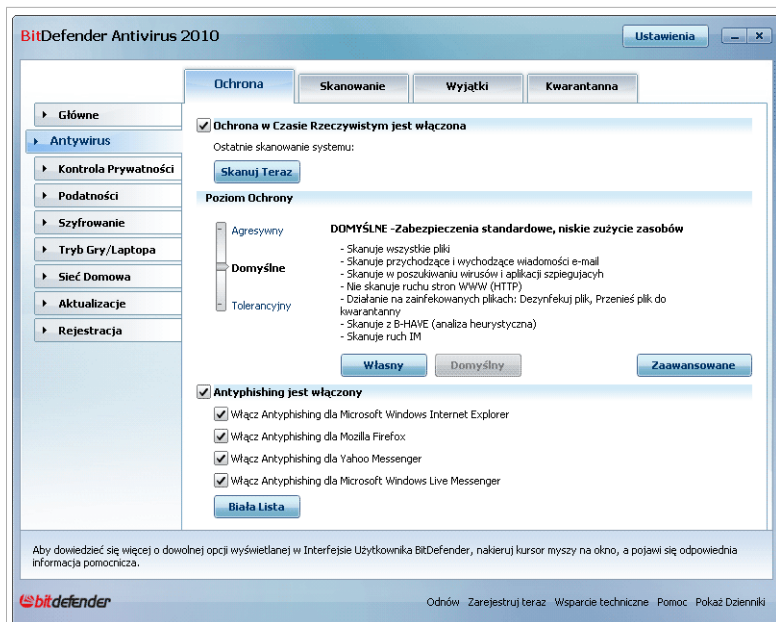
Ochrona w Czasie Rzeczywistym dotyczy również skanowanie przy dostępie - pliki są skanowane gdy użytkownik z nich korzysta.

- **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.

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

Aby skonfigurować ochronę w czasie rzeczywistym i BitDefender Antyphishing, kliknij **Antywirus>Ochrona** w Trybie Eksperta.



Ochrona W Czasie Rzeczywistym

Możesz zobaczyć czy Ochrona w Czasie Rzeczywistym jest włączona czy wyłączona. Jeżeli chcesz zmienić status ochrony w Czasie Rzeczywistym, zaznacz lub odznacz odpowiednie pole.



WAŻNE

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

Aby rozpocząć skanowanie systemu kliknij **Skanuj Teraz**.

18.1.1. Konfigurowanie Poziomu Ochrony

Możesz wybrać poziom ochrony, który najbardziej odpowiada twoim potrzebom. Przeciągnij suwak po skali aby ustawić odpowiedni poziom ochrony.

Dostępne są 3 poziomy ochrony:

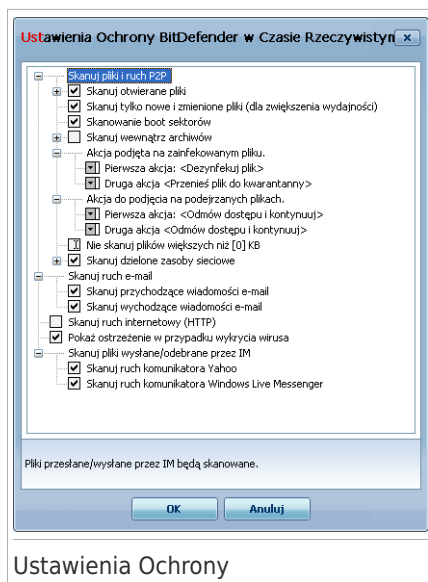
P o z i o m y ochrony	Opis
Tolerancyjny	Zapewnia podstawowe funkcje bezpieczeństwa. Zużycie zasobów komputera jest w tym przypadku bardzo niskie. Tylko programy i przychodzące wiadomości e-mail są skanowane pod kątem wirusów. Ponadto używane jest klasyczne skanowanie oparte na sygnaturach . Na zainfekowanych plikach można wykonać następujące akcje: wylecz plik/przenieś plik do kwarantanny.
Domyślny	Oferuje standardowe zabezpieczenia. Zużycie zasobów komputera jest w tym przypadku niskie. Wszystkie pliki oraz przychodzące i wychodzące maile są skanowane pod kątem wirusów i spyware. Poza klasycznym skanowaniem opartym na sygnaturach, używana jest analiza heurystyczna. Następujące działania są podejmowane na zainfekowanych plikach: wylecz plik/przenieś do kwarantanny.
Agresywny	Oferuje wysoką ochronę. Zużycie zasobów komputera jest w tym przypadku umiarkowane. Wszystkie pliki, ruch stron WWW oraz przychodzące i wychodzące maile są skanowane pod kątem wirusów i spyware. Poza klasycznym skanowaniem opartym na sygnaturach, używana jest analiza heurystyczna. Następujące działania są podejmowane na zainfekowanych plikach: wylecz plik/przenieś do kwarantanny.

Aby zastosować domyślne ustawienia ochrony czasu rzeczywistego kliknij **Poziom Domyślny**.

18.1.2. Dostosowywanie 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 dostosować **Ochronę w Czasie Rzeczywistym** klikając **Użytkownika**. Pojawi się następujące okno:



Opcje skanowania są zorganizowane jako rozwijalne menu, bardzo podobne do tych w systemie Windows. Kliknij na okienko "+" aby otworzyć opcję lub "-" aby zamknąć opcję.



Notatka

Możesz zaobserwować, że niektóre opcje skanowania, mimo że są odznaczone "+" nie mogą być otwarte. Dzieje się tak dlatego, że te opcje nie zostały jeszcze wybrane. Zaobserwujesz, że mogą być one otwarte, gdy je wybierzesz.

- **Opcje skanowania otwieranych plików i transferów P2P** - skanuje otwierane pliki i komunikację pomiędzy komunikatorami internetowymi (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Wybierz typ plików, jakie mają być skanowane.

Opcje	Opis
Skanuj uruchamiane pliki	S k a n o w a n i e wszystkich plików Wszystkie pliki zostaną przeskanowane podczas otwierania, bez względu na ich typ.
Skanuj aplikacje	Skanuj tylko Wyłącznie pliki programowe zostaną przeskanowane tzn. pliki z następującymi rozszerzeniami: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz;

Opcje	Opis
	.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 i .nws.
Skanowanie tylko zdefiniowanych rozszerzeń	Wyłącznie pliki z rozszerzeniami określonymi przez użytkownika zostaną przeskanowane. Te rozszerzenia muszą być oddzielone przez ",".
Skanuj w poszukiwaniu riskware	Skanuje pod potencjalnie niebezpiecznych programów. Wykryte pliki będą traktowane jako zainfekowane. Oprogramowanie, które zawiera komponenty adware może przestać działać jeśli ta opcja jest włączona. Wybierz Pomiń dialery i aplikacje w skanowaniu i/lub Pomiń keyloggery w skanowaniu jeśli nie chcesz skanować tych plików.
Skanuj tylko nowe i zmienione pliki	Skanuj wyłącznie pliki, które nie były skanowane poprzednio lub też zmieniły się od czasu ich ostatniego skanowania. Wybierając tą opcję, możesz w dużym stopniu poprawić wydajność systemu, bez dużego wpływu na bezpieczeństwo.
Przeskanuj boot sektory	Aby skanować boot sektor systemu.
Skanowanie wewnątrz archiwów	Także dostępne archiwa zostaną przeskanowane. Ta opcja spowalnia pracę komputera. Możesz ustawić maksymalny rozmiar archiwów, które mają być skanowane (w kilobajtach, wpisz 0 jeśli chcesz skanować wszystkie) i maksymalny poziom podkatalogów do skanowania.
Pierwsze działanie	Wybierz z menu rozwijalnego pierwsze działanie do podjęcia na zainfekowanych lub podejrzanych plikach.
Odmowa dostępu i kontynuuj	W przypadku wykrycia zainfekowanego pliku dostęp do niego zostanie zablokowany.

Opcje		Opis
	Wylecz plik	Usuwa złośliwy kod z zainfekowanych plików.
	Usun plik	Natychmiastu usuwa zainfekowane pliki, bez żadnego ostrzeżenia.
	Przenieść plik do kwarantanny	Przenosi zainfekowane pliki do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.
	Drugie działanie	Wybierz z menu rozwijalnego drugie działanie do podjęcia na zainfekowanych lub podejrzanych plikach, w przypadku niepowodzenia pierwszego działania.
	Odmowa dostępu i kontynuuj	W przypadku wykrycia zainfekowanego pliku dostęp do niego zostanie zablokowany.
	Usun plik	Natychmiastu usuwa zainfekowane pliki, bez żadnego ostrzeżenia.
	Przenieść plik do kwarantanny	Przenosi zainfekowane pliki do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.
Nie skanuj plików większych niż [x] Kb		Wpisz maksymalny rozmiar plików jakie mają być skanowane. Jeżeli wpiszesz 0 Kb, wszystkie pliki zostaną przeskanowane, niezależnie od ich rozmiaru.
Skanuj zasoby sieciowe	S k a n o w a n i e wszystkich plików	Wszystkie pliki udostępnione w sieci będą skanowane, niezależnie od ich typu.
	Skanuj tylko aplikacje	Wyłącznie pliki programowe zostaną przeskanowane tzn. pliki z następującymi rozszerzeniami: .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 i .nws.

Opcje	Opis
Skanowanie tylko zdefiniowanych rozszerzeń	Wyłącznie pliki z rozszerzeniami określonymi przez użytkownika zostaną przeskanowane. Te rozszerzenia muszą być oddzielone przez " , " .

- **Skanuj pocztę elektroniczną** - skanuje cały ruch poczty elektronicznej.

Dostępne są następujące opcje:

Opcje	Opis
Skanuj przychodzące wiadomości e-mail	Skanuje wszystkie przychodzące wiadomości e-mail
Skanuj wychodzące wiadomości e-mail	Skanuje wszystkie wychodzące wiadomości e-mail

- **Skanuj ruch internetowy (HTTP)** - skanuje ruch http.
- **Pokaż ostrzeżenie gdy wirus zostanie wykryty** - okno alarmu wyświetli się, gdy wirus zostanie znaleziony w pliku, lub w wiadomości e-mail.

W przypadku zainfekowanych plików, okno będzie zawierało nazwę wirusa, ścieżkę do niego i akcję jaką wykonał BitDefender oraz link do stron BitDefendera, gdzie możesz znaleźć więcej informacji o danym wirusie. Natomiast, w przypadku zainfekowanych e-maili, okno alarmu będzie zawierało dodatkowo informacje o nadawcy i odbiorcy poczty.

W wypadku wykrycia podejrzanego pliku, możesz uruchomić kreatora z okna alarmu, który pomoże Ci wysłać plik do Laboratorium BitDefendera do analizy. Możesz także wpisać swój e-mail aby otrzymać informacje dotyczące tego raportu.

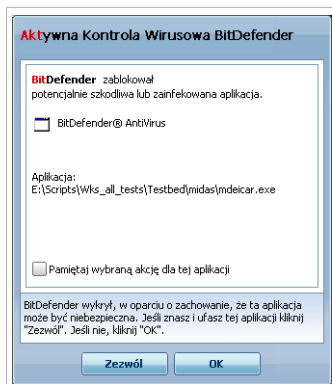
- **Skanuj pliki odbierane/wysyłane przez IM.** Aby skanować pliki pobierane lub wysyłane przy użyciu Yahoo Messenger lub Windows Live Messenger, zaznacz odpowiednie pole.

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

18.1.3. Konfiguracja Ustawień Active Virus Control

BitDefender Active Virus Control (AVC) zapewnia dodatkową warstwę ochrony przed nowymi zagrożeniami których sygnatury nie zostały jeszcze opublikowane. Monitoruje on i analizuje zachowanie aplikacji uruchomionych w twoim komputerze i informuje jeśli aplikacja zachowuje się podejrzanie.

AVC może zostać skonfigurowany tak, aby alarmował użytkownika i pytał o podjęcie działania kiedy aplikacja chce przeprowadzić potencjalnie niebezpieczną akcję.



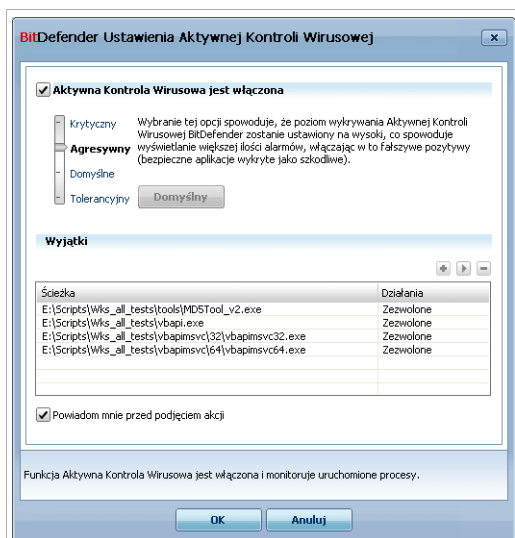
Alarm BitDefender AVC

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

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

Zaznacz pole **Pamiętaj wybraną akcję dla tej aplikacji** aby BitDefender podejmował to samo działanie dla wybranej aplikacji w przyszłości. Reguła która została stworzona będzie wyświetlona w tabeli w polu **Wyjątki**.

Aby skonfigurować Active Virus Control, kliknij na **Ustawienia BD AVC**.



Ustawienia BitDefender AVC

Zaznacz odpowiadające pole aby włączyć Active Virus Control.



WAŻNE

Active Virus Control powinien być zawsze włączony, aby chronić komputer przed nieznanymi wirusami.

Jeśli chcesz być powiadamiany i alarmowany o akcjach podejmowanych przez Active Virus Control za każdym razem, kiedy aplikacja chce wykonać niedozwoloną akcję, zaznacz pole **Zapytaj mnie przed podjęciem akcji**.

Konfigurowanie Poziomu Ochrony

Poziom zabezpieczeń AVC zmienia się automatycznie gdy ustawisz nowy poziom zabezpieczeń dla ochrony w czasie rzeczywistym. Jeśli nie jesteś usatysfakcjonowany ustawieniami domyślnymi, możesz ręcznie skonfigurować poziom ochrony.



Notatka

Pamiętaj, że jeśli zmienisz poziom zabezpieczeń ochrony w czasie rzeczywistym, zmieni się także poziom zabezpieczeń AVC. Jeśli ustawiłeś poziom zabezpieczenia w czasie rzeczywistym na **Tolerancyjny**, BitDefender Active Virus Control jest automatycznie wyłączany i nie można go konfigurować.

Przesuń suwak po skali aby ustawić poziom bezpieczeństwa który najlepiej spełni twoje wymagania.

P o z i o m y ochrony	Opis
Krytyczne	Restrykcyjne monitorowanie wszystkich aplikacji przeciwko możliwym niebezpiecznym akcjom.
Domyślny	Poziom wykrywalności jest wysoki i mogą występować fałszywe pozytywy.
Średni	Poziom wykrywalności jest średni, czasami możliwe występowanie fałszywych pozytywów.
Tolerancyjny	Poziom wykrywalności jest niski i nie występują fałszywe pozytywy.

Zarządzanie Listami Zaufanych / Zablokowanych Aplikacji

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. Podobnie, aplikacje którym chcesz na stałe zablokować dostęp, mogą być dodane do listy aplikacji którym nie należy ufać i BitDefender Active Virus Control automatycznie je zablokuje.

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

Aby zarządzać listą, użyj przycisków znajdujących się nad tabelą:

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

18.1.4. Wyłączanie Ochrony w Czasie Rzeczywistym.

Jeśli chcesz wyłączyć ochronę w czasie rzeczywistym, pojawi się następne okno ostrzegawcze: Musisz potwierdzić swój wybór wybierając na jak długo ochrona w czasie rzeczywistym ma być wyłączona. Możesz ją wyłączyć na 5, 15 lub 30 minut, na godzinę, na stałe lub do restartu komputera.



Ostrzeżenie

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

18.1.5. Konfigurowanie Ochrony Antyphishingowej

BitDefender zapewnia ochronę w czasie rzeczywistym dla:

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

Możesz kompletnie wyłączyć ochronę antyphishingową lub tylko dla podanej aplikacji.

Możesz kliknąć **Biała Lista** aby skonfigurować i zarządzać listą stron www które nie powinny być skanowane przez silnik Antyphishingowy BitDefendera.



Możesz zobaczyć listę wszystkich stron www których BitDefender aktualnie nie sprawdza pod kątem zawartości phishingowej.

Aby dodać nową stronę www do białej listy, wpisz jej adres url w polu **Nowy dres** i kliknij **Dodaj**. 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 „*Integracja z Przeglądarką Internetową*” (p. 201).

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

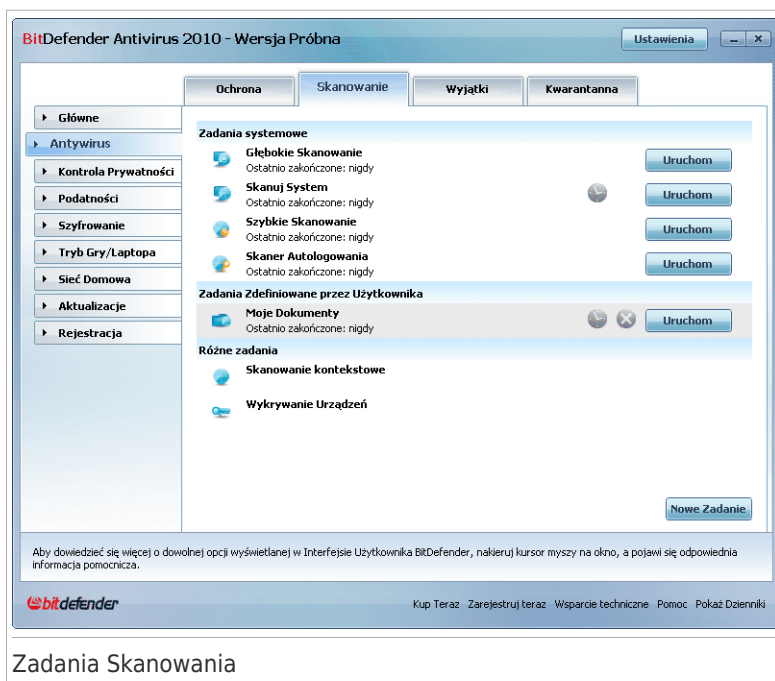
Kliknij **Zapisz** aby zapisać zmiany i zamknąć to okno.

18.2. 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 każdego 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.

Aby skonfigurować i zainicjować skanowanie na żądanie, przejdź do **Skanowanie Antywirusowe** w Trybie Eksperta.



Zadania Skanowania

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 zadań lub swoich własnych. Możesz także zaplanować aby skanowania były uruchamiane co jakiś okres czasu lub gdy system jest bezczynny żeby nie przeszkadzać tobie w pracy.

18.2.1. Zadania Skanowania

BitDefender ma kilka domyślnych zadań, które zaspokajają najczęstsze zagrożenia bezpieczeństwa. Możesz również tworzyć swoje własne zadania skanowania.

Każde zadanie posiada okno **Właściwości**, które pozwala konfigurować zadanie i oglądać wyniki skanowania. Aby uzyskać więcej informacji, odwołaj się do „*Konfiguracja Zadania Skanowania*” (p. 117).

Są trzy kategorie zadań skanowania:

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

Zadania Domyślne	Opis
Głębokie Skanowanie	Skanuje cały system. W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.
Skanowanie Systemu	Skanuje cały system wyłączając archiwa. W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów .
Szybkie Skanowanie Systemu	Skanuje katalogi Windows i Program Files. W konfiguracji domyślnej, skanuje pod kątem wszystkich zagrożeń, z wyjątkiem rootkitów, lecz nie skanuje pamięci, rejestru ani plików ciasteczek.
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).



Notatka

Głębokie Skanowanie Systemu i Skanowanie Systemu mogą chwilę potrwać, obciążając przy tym zasoby komputera. Zadania tego typu najlepiej uruchamiać z niskim priorytetem, lub 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.

Na prawo od każdego zadania dostępne są 3 przyciski:

-  **Harmonogram** - oznacza, że dane zadanie jest zaplanowane na później. Kliknij ten przycisk aby przejść do okna **Właściwości Harmonogramu** gdzie możesz zobaczyć zaplanowane zadania i je modyfikować.
-  **Usuń** - usuwa zaznaczone zadanie.



Notatka

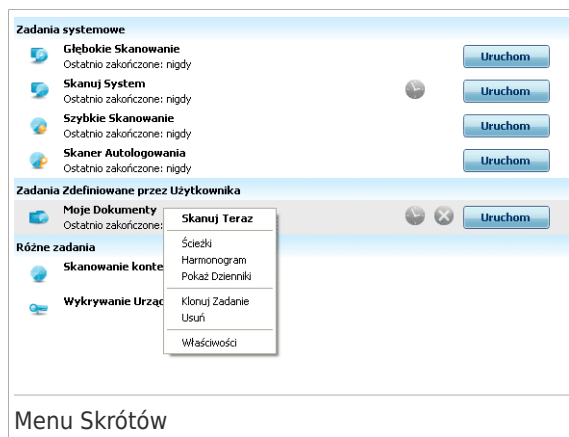
Niedostępne dla zadań systemowych. Nie możesz usunąć zadań systemowych.

-  **Skanuj Teraz** - uruchamia zaznaczone zadanie, rozpoczynając **natychmiastowe skanowanie**.

Po lewej stronie każdego zadania znajduje się przycisk **Właściwości**, umożliwiający konfigurację zadania oraz zobaczenie dzienników skanowania.

18.2.2. Używanie Menu Skrótów

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



Dostępne są następujące opcje w Menu Skrótów:

- **Skanuj Teraz** - uruchamia zaznaczone zadanie.
- **Ścieżki** - otwiera okno **Właściwości**, zakładkę **Ścieżki**, gdzie możesz zmienić miejsce które ma być skanowane przez to zadanie.



Notatka

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 zadania.
- **Usuń** - usuwa wybrane zadanie.



Notatka

Niedostępne dla zadań systemowych. Nie możesz usunąć zadań systemowych.

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



Notatka

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

18.2.3. Tworzenia Zadania Skanowania

Aby utworzyć zadanie skanowania, skorzystaj z jednej z następujących metod:

- **Klonuj** istniejące zadanie, zmień nazwę i wprowadź niezbędne zmiany w oknie **Właściwości**.
- Kliknij **Nowe Zadanie** aby utworzyć nowe zadanie i je skonfigurować.

18.2.4. Konfiguracja Zadania Skanowania

Każde zadanie skanowania ma swoje okno **Właściwości**, gdzie możesz konfigurować opcje skanowania, ustawić cel skanowania, zaplanować zadanie lub zobaczyć raporty. Aby otworzyć to okno, kliknij na przycisk **Właściwości** po lewej stronie zadania (lub kliknij prawym przyciskiem myszy na zadanie i wybierz **Właściwości**).

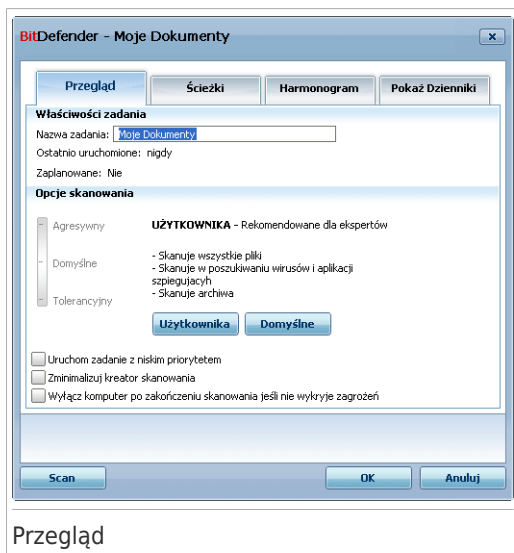


Notatka

Aby uzyskać więcej szczegółów dotyczących przeglądania dzienników i zakładki **Dzienniki** odwołaj się do „*Przeglądanie Dzienników Skanowania*” (p. 137).

Konfigurowanie Ustawień Skanowania

Aby skonfigurować opcje skanowania wybranego zadania, kliknij je prawym klawiszem myszy i wybierz **Właściwości**. Pojawi się następujące okno:



Możesz tutaj zobaczyć informacje o zadaniu (nazwa, ostatnie uruchomienie i status terminarza) oraz skonfigurować ustawienia skanowania.

Wybieranie Poziomu Skanowania

Możesz łatwo skonfigurować ustawienia skanowania wybierając poziom skanowania. Przeciągnij suwak po skali aby wybrać odpowiedni poziom.

Dostępne są 3 poziomy skanowania:

P o z i o m y ochrony	Opis
Tolerancyjny	Oferuje rozsądną skuteczność wykrywania. Poziom zużycia zasobów komputera jest niski. Pod kątem wirusów są skanowane tylko programy. Ponadto uruchomione jest klasyczne skanowanie oparte na sygnaturach, oraz analiza heurystyczna.
Domyślny	Oferuje dobrą skuteczność wykrywania. Poziom zużycia zasobów komputera jest umiarkowany.

P o z i o m y ochrony	Opis
	Wszystkie pliki są skanowane pod kątem wirusów i spywareów. Ponadto uruchomione jest klasyczne skanowanie oparte na sygnaturach, oraz analiza heurystyczna.
Wysoki	Oferuje maksymalną skuteczność wykrywania. Poziom zużycia zasobów komputera jest wysoki. Wszystkie pliki i archiwa są skanowane pod kątem wirusów i spywareów. Ponadto uruchomione jest klasyczne skanowanie oparte na sygnaturach, oraz analiza heurystyczna.

Ponadto dostępna jest seria ogólnych opcji procesu skanowania:

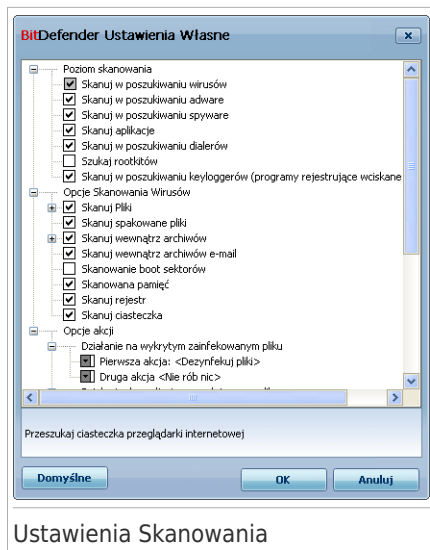
- **Uruchom zadanie z niskim priorytetem.** Obniża priorytet procesu skanowania. Pozwala innym programom działać szybciej i zwiększa czas potrzebny na zakończenie skanowania.
- **Minimalizuj Kreator Skanowania do zasobnika w pasku systemowym.** Minimalizuje okno skanowania do **paska systemowego**. Kliknij dwukrotnie ikonę BitDefender aby otworzyć okno skanowania.
- **Wyłącz komputer po zakończeniu skanowania jeśli nie wykryje żadnego zagrożenia**

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

Dostosowywanie Poziomu Skanowania

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.

Kliknij **Użytkownika** aby ustawić własne opcje. Pojawi się nowe okno.



Ustawienia Skanowania

Opcje skanowania są zorganizowane jako rozwijalne menu, bardzo podobne do tych w systemie Windows. Kliknij na okienko "+" aby otworzyć opcję lub "-" aby zamknąć opcję.

Opcje skanowania są podzielone na 3 kategorie:

- **Poziom Skanowania.** Wybierz typ szkodliwego oprogramowania którego BitDefender ma szukać wybierając odpowiednie opcje z kategorii **Poziom Skanowania**.

Opcje	Opis
Skanuj przed wirusami	Skanuje szukając znanych wirusów. BitDefender wykrywa również niekompletne wirusy, w celu usunięcia zagrożeń które mogły by wpłynąć na zabezpieczenia systemu.
Skanuj przed adware	Szuka aplikacji adware. Pliki tego typu będą traktowane jako zainfekowane. Oprogramowanie, które zawiera komponenty adware może przestać działać jeśli ta opcja jest włączona.
Skanuj przed spyware	Szuka znanych zagrożeń szpiegujących. Wykryte pliki spyware będą traktowane jako zainfekowane.

Opcje	Opis
Skanuj aplikacje	Szuka legalnych aplikacji które mogą być użyte jako narzędzie szpiegujące, do ukrycia szkodliwy aplikacji lub w innych szkodliwych celach.
Skanuj przed dialerami	Szuka aplikacji dzwoniących pod drogie numery. Takie pliki zostaną oznaczone jako zainfekowane. Oprogramowanie które zawiera komponenty dialer może przestać działać jeśli ta opcja jest włączona.
Skanuj przed rootkitami	Szuka ukrytych obiektów (plików i procesów), ogólnie znanych jako rootkity.

- **Opcje skanowania wirusów.** Wybierz typ obiektów do skanowania (typy plików, archiwa, itp.) zaznaczając odpowiednie z kategorii **Opcje skanowania wirusów.**

Opcje	Opis
Skanowanie plików	Skanowanie wszystkich plików Wszystkie pliki są skanowane, bez względu na ich typ. Skanowanie tylko plików wykonywalnych Wyłącznie pliki programowe zostaną przeskanowane tzn. pliki z następującymi rozszerzeniami: 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 i nws. Skanowanie tylko zdefiniowanych rozszerzeń Wyłącznie pliki z rozszerzeniami określonymi przez użytkownika zostaną przeskanowane. Te rozszerzenia muszą być oddzielone przez ",".
Skanowanie spakowanych plików	Aby skanować spakowane pliki.
Skanowanie wewnątrz archiwów	Skanuje w archiwach takich jak .zip, .rar, .ace, .iso i innych. Zaznacz pole Skanuj instalatory i pliki chm jeśli chcesz aby te typy plików były skanowane. Skanowanie plików archiwów zwiększa czas skanowania oraz zużycie zasobów

Opcje	Opis
	systemowych. Możesz ustalić maksymalny rozmiar archiwów, które mają być skanowane w kilobajtach (KB) przez wprowadzenie rozmiaru w to pole Ogranicz rozmiar skanowanych archiwów do .
Skanuj wewnątrz archiwów e-mail	Aby skanować pocztę wewnętrzną archiwów.
Przeskanuj boot sektory	Aby skanować boot sektor systemu.
Skanuj pamięć	Skanuje pamięć przed wirusami i innego typu złośliwym oprogramowaniem.
Przeszukaj rejestr	skanuje wpisu rejestru na obecność spyware.
Przeskanuj ciasteczka	Skanuje pliki ciasteczek.

- **Opcje działania.** Określ akcje, które zostaną podjęte dla poszczególnych typów wykrytych plików korzystając z opcji w tej kategorii.



Notatka

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

- Wybierz działanie które ma być podjęte na zainfekowanych plikach. Dostępne są następujące opcje:

Działania	Opis
Brak Działań	Żadna reakcja nie będzie podjęta na zainfekowane pliki. Te pliki będą występować w pliku raportu.
Wylecz pliki	Usuwa szkodliwy kod z wykrytego zainfekowanego pliku.
Usuń pliki	Natychmiastu usuwa zainfekowane pliki, bez żadnego ostrzeżenia.
Przenieś do Kwarantanny	Przenosi zainfekowane pliki do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.

- Wybierz działanie które ma być podjęte na podejrzanych ukrytych plikach. Dostępne są następujące opcje:

Działania	Opis
Brak Działań	Żadna działanie nie będzie podjęte na podejrzanych plikach. Pliki te będą zawarte w raporcie.
Usuń pliki	Natychmiast usuwa zainfekowane pliki, bez żadnego ostrzeżenia.
Przenieś do Kwarantanny	Przenosi zainfekowane pliki do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.



Notatka

Pliki są wykrywane jako podejrzane przez analizę heurystyczną. Zalecamy wysłanie tych plików do Laboratorium BitDefendera.

- Wybierz działanie które ma być podjęte na ukrytych elementach (rootkitach). Dostępne są następujące opcje:

Działania	Opis
Brak Działań	Żadna działanie nie będzie podjęte na ukrytych plikach. Pliki te będą zawarte w raporcie.
Zmień nazwę plików	Zmienia nazwę ukrytych plików dodając .bd . ren do ich nazwy. Dzięki temu, będziesz mógł znaleźć tego typu pliki na swoim komputerze, jeśli takowe istnieją.
Przenieś do Kwarantanny	Przenosi ukryte pliki do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.



Notatka

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.

- **Akcje podejmowane w przypadku zaszyfrowanych lub zabezpieczonych hasłem plików.** Pliki zaszyfrowane przez Windows mogą być dla Ciebie ważne. Dlatego właśnie możesz skonfigurować różne akcje podejmowane przeciwko zainfekowanym lub podejrzany plikom, które zostały zaszyfrowane w systemie

Windows. Inna kategoria plików, które wymagają podjęcia specjalnych akcji to archiwa chronione hasłem. Archiwa chronione hasłem nie mogą być skanowane chyba że podasz hasło. Korzystaj z tych opcji do konfiguracji akcji, które zostaną podjęte w przypadku archiwów zabezpieczonych hasłem lub zaszyfrowanych w Windows plików.

- **Działanie na zainfekowanym pliku.** Wybierz akcję, która zostanie podjęta w przypadku znalezienia zainfekowanego pliku, który został zaszyfrowany przy użyciu Windows Dostępne są następujące opcje:

Działania	Opis
Brak działań	W przypadku zainfekowanych plików, które są zaszyfrowane przez Windows, tylko zapisuj informację w dzienniku. Po zakończeniu skanowania, możesz otworzyć dziennik skanowania i zobaczyć informacje o tych plikach.
Wylecz pliki	Usuwa szkodliwy kod z wykrytego zainfekowanego pliku. W niektórych przypadkach wyleczenie pliku może się nie udać, przykładowo kiedy zainfekowany plik jest wewnątrz archiwum email.
Usuń pliki	Natychmiast usuwa zainfekowane pliki z dysku, bez żadnego ostrzeżenia.
Przenieś do Kwarantanny	Przenieś zainfekowane pliki z ich oryginalnej lokalizacji do folderu kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.

- **Działanie na podejrzanym i zaszyfrowanym pliku.** Wybierz akcję, która zostanie podjęta w przypadku znalezienia podejrzanego pliku, który został zaszyfrowany przy użyciu Windows Dostępne są następujące opcje:

Działania	Opis
Brak działań	W przypadku podejrzanых plików, które są zaszyfrowane przez Windows, tylko zapisuj informację w dzienniku. Po zakończeniu skanowania, możesz otworzyć dziennik skanowania i zobaczyć informacje o tych plikach.

Działania	Opis
Usuń pliki	Natychmiast usuwa zainfekowane pliki, bez żadnego ostrzeżenia.
Przenieś do Kwarantanny	Przenosi zainfekowane pliki do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.

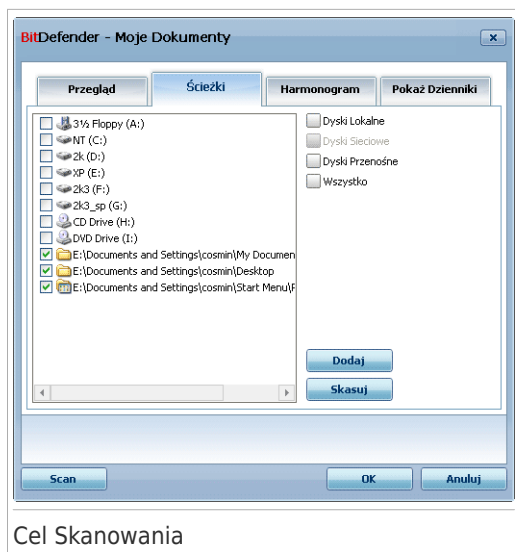
- **Działanie na pliku chronionym hasłem.** Wybierz działanie które ma być podjęte na wykrytych plikach chronionych hasłem. Dostępne są następujące opcje:

Działania	Opis
Zapisuj w dzienniku	Tylko zapisuje informacje o plikach chronionych hasłem w dzienniku skanowania. Po zakończeniu skanowania, możesz otworzyć dziennik skanowania i zobaczyć informacje o tych plikach.
Pytaj o hasło	Kiedy plik chroniony hasłem zostanie wykryty, pyta użytkownika o podanie hasła aby przeskanować plik.

Jeśli klikniesz **Domyślne** wczytasz ustawienia domyślne. Kliknij **OK** aby zapisać zmiany i zamknąć okno.

Ustawianie Celu 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**. Pojawi się następujące okno:



Cel Skanowania

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

Ta sekcja zawiera następujące klawisze:

- **Dodaj Folder(y)** - otwiera okno w którym można wybrać plik(i) / folder(y), które mają być przeskanowane.



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.



Notatka

Tylko plik(i) / folder(y), które potem dodano mogą być usunięte ale nie te, które były automatycznie "widziane" przez BitDefender.

Poza przyciskami opisanymi powyżej, 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.



Notatka

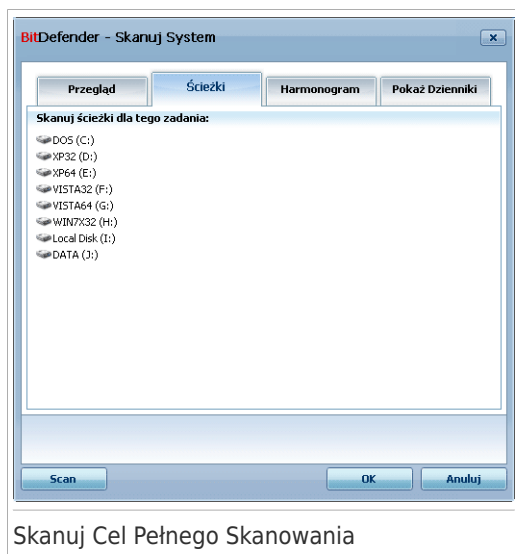
Jeżeli chcesz skanować cały swój komputer, wybierz opcję **Wszystko**.

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

Zobacz Cel Skanowania Zadań Systemowych

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 Zadania**. Dla **Skanowania Systemu**, na przykład, pojawi się następujące okno:



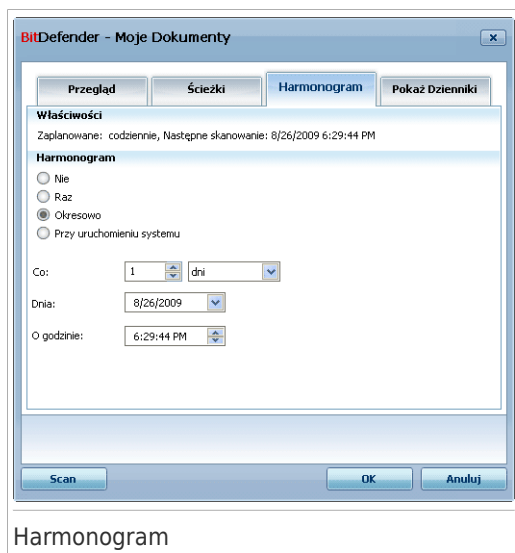
Skanowanie Systemu oraz **Głębokie Skanowanie Systemu** skanują wszystkie lokalne dyski, zaś **Szybkie Skanowanie Systemu** skanuje tylko foldery Windows i Program Files.

Kliknij **OK** aby zamknąć okno. Aby uruchomić zadanie, kliknij tylko **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**. Pojawi się następujące okno:



Możesz zobaczyć harmonogram zadania, jeśli taki jest.

Podczas planowania zadanie, musisz wybrać jedną z opcji:

- **Nie zaplanowane** - uruchamia zadanie tylko gdy chce tego użytkownik.
- **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.

Jeżeli chcesz żeby skanowanie było powtarzane w określonym przedziale czasowym, wybierz **Okresowo** i wpisz w polu edycji **Każdego** ilość minut / godzin / dni / tygodni / miesięcy, kiedy chcesz powtarzać ten proces. Musisz także określić datę i czas rozpoczęcia w polu **Data/Czas Rozpoczęcia**.

- **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**.

18.2.5. Skanowanie Plików i Folderów

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 zweryfikować kiedy ostatni raz wykonywana była aktualizacja, przejdź do **Aktualizacje** w Widoku Zaawansowanym.



Notatka

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 uśpienia w momencie gdy zaplanowane są zadania.

- Jeśli często pobierasz 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.

Metody Skanowania

BitDefender pozwala na cztery typy skanowania na żądanie:

- **Skanowanie natychmiastowe** - uruchamia zadanie skanowania z zadań użytkownika / systemu.
- **Skanowanie kontekstowe** - kliknij prawym przyciskiem myszy na plik lub folder i wybierz **Skanuj z BitDefender**.
- **Skanowanie Przeciągnij i Upuść** - przeciągnij i upuść plik lub folder na **Pasek Aktywności Skanera**.
- **Skanowanie ręczne** - korzystaj ze Skanowania Ręcznego BitDefendera aby bezpośrednio wybrać pliki lub foldery do skanowania.

Skanowanie Natychmiastowe

Aby przeskanować cały komputer lub jego część możesz użyć domyślnego zadania skanowania lub własnych zadań skanowania. To się nazywa natychmiastowe skanowanie.

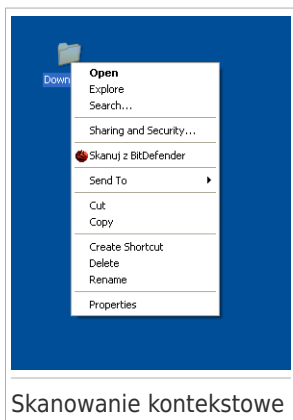
Aby uruchomić zadanie, użyj jednej z następujących metod:

- kliknij dwukrotnie na wybrane zadanie skanowania z listy.
- kliknij przycisk  **Skanuj teraz** odpowiedniego zadania.
- zaznacz zadanie i następnie kliknij **Wykonaj zadanie**.

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

Skanowanie Kontekstowe

Aby przeskanować plik lub folder bez konfigurowania nowego zadania, możesz użyć menu kontekstowego. To się nazywa skanowanie kontekstowe.

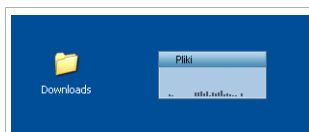


Kliknij prawym przyciskiem myszy plik lub folder, który ma być przeskanowany i wybierz opcję **Skanuj z BitDefender**. Pojawi się **Kreator skanowania antywirusowego** i przeprowadzi cię przez proces skanowania.

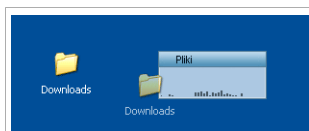
Możesz modyfikować opcje skanowania i zobaczyć pliki raportu poprzez dostęp do okna **Właściwości** zadania **Menu Skanowania Kontekstowego**.

Skanowanie Przeciągnij i Upuść

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.

Skanowanie Ręczne

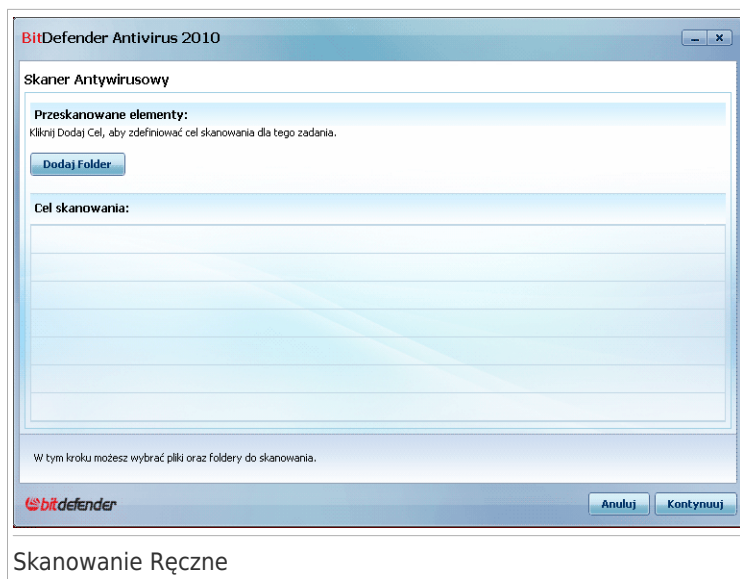
Skanowanie ręczne polega na wybraniu obiektu który ma być skanowany z użyciem Skanowania ręcznego BitDefender z grupy programów Bitdefender w Menu Start.



Notatka

Skanowanie ręczne jest przydatne ponieważ może również być wykonane gdy Windows pracuje w Trybie Awaryjnym.

Aby wybrać obiekt do skanowania przez BitDefendera, skorzystaj z menu Start: **Start → Programy → BitDefender 2010 → BitDefender Skanowanie Ręczne**. Pojawi się następujące okno:



Skanowanie Ręczne

Kliknij **Dodaj Folder**, wybierz lokalację, którą chcesz dodać i kliknij **OK**. Jeśli chcesz skanować wiele folderów, powtórz tę czynność dla każdej dodatkowej lokalizacji.

Ścieżki do wybranej lokalizacji pojawią się w kolumnie **Cel Skanowania**. Jeśli rozmyśliłeś się odnośnie danej lokalizacji, kliknij **Usuń** obok niej. Kliknij na przycisk **Usuń Wszystkie Ścieżki** aby usunąć wszystkie ścieżki znajdujące się na liście.

Kiedy skończysz wybierać lokalacje, kliknij **Kontynuuj**. Pojawi się **Kreator skanowania antywirusowego** i przeprowadzi cię przez proces skanowania.

Kreator Skanowania Antywirusowego

Kiedy uruchomisz skanowanie na żądanie, pojawi się kreator skanowania antywirusowego. Wykonaj następujące trzy kroki procedury aby zakończyć skanowanie komputera.

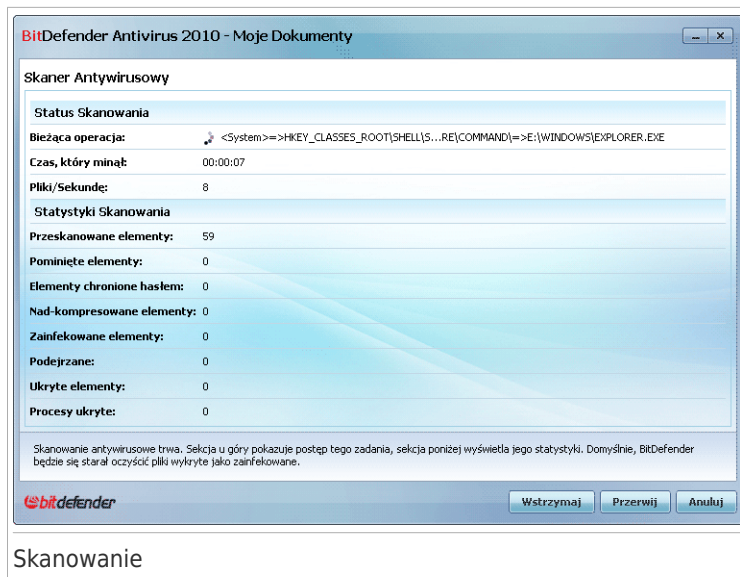


Notatka

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.



Skanowanie

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. Jeśli BitDefender natrafi na archiwum chronione hasłem podczas skanowania i ustawiona jest domyślna akcja **Pytaj o hasło**, zostaniesz poproszony o podanie hasła. Archiwa chronione hasłem nie mogą być skanowane chyba że podasz hasło. Dostępne są następujące opcje:

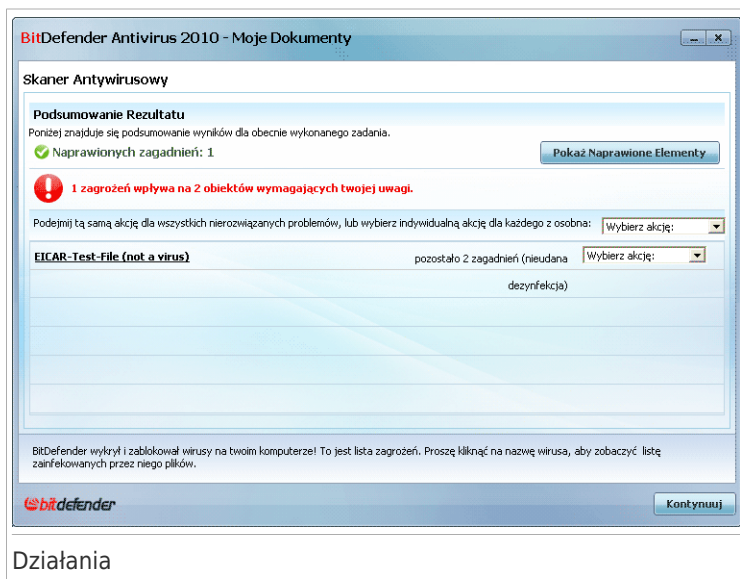
- **Hasło.** Jeśli chcesz aby BitDefender przeskanował archiwum, wybierz tę opcję i podaj hasło. Jeśli nie znasz hasła, wybierz jedną z pozostałych opcji.
- **Nie pytaj o hasło i pomini ten obiekt w skanowaniu.** Wybierz tę opcję aby pominąć skanowanie tego archiwum.
- **Pomiń wszystkie elementy chronione hasłem i nie skanuj ich.** Wybierz tę opcję jeśli nie chcesz być pytany o archiwa zabezpieczone hasłem. BitDefender nie będzie w stanie ich skanować, ale informacja na ich temat zostanie zapisana w dzienniku skanera.

Kliknij **OK** aby kontynuować skanowanie.

Przerywanie lub zatrzymywanie skanowania. Możesz przerwać skanowanie klikając **Stop&Tak**. Przejdiesz 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.



Możesz zobaczyć ilość zdarzeń zagrażających twojemu systemowi.

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:

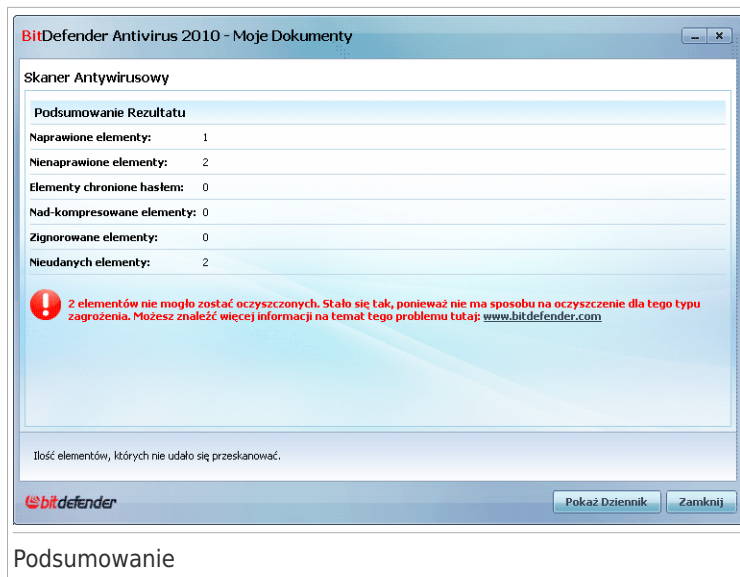
Działania	Opis
Brak Działań	Żadne działanie nie zostanie podjęte na wykrytych plikach. Po zakończeniu skanowania, możesz otworzyć dziennik skanowania i zobaczyć informacje o tych plikach.
Usuń wirusa	Usuwa złośliwy kod z zainfekowanych plików.

Działania	Opis
Usuń	Usuwa wykryte pliki.
Przenieś do kwarantanny	Przenosi pliki wykryte jako zainfekowane do kwarantanny. Pliki w kwarantannie nie mogą być uruchomione ani otwarte; teoretycznie, ryzyko zainfekowania nimi znika.
Zmień nazwę plików	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.



Możesz zobaczyć podsumowanie wyników. Jeśli chcesz uzyskać wyczerpujące informacje na temat procesu skanowania, kliknij na **Pokaż dziennik** aby przejrzeć 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. Jednakże, są zagadnienia których nie można rozwiązać.

W takim przypadku zalecamy skontaktować się ze Pomocą Techniczną BitDefendera na www.bitdefender.com. Nasze wsparcie techniczne pomoże tobie rozwiązać problemy na które natrafiasz.

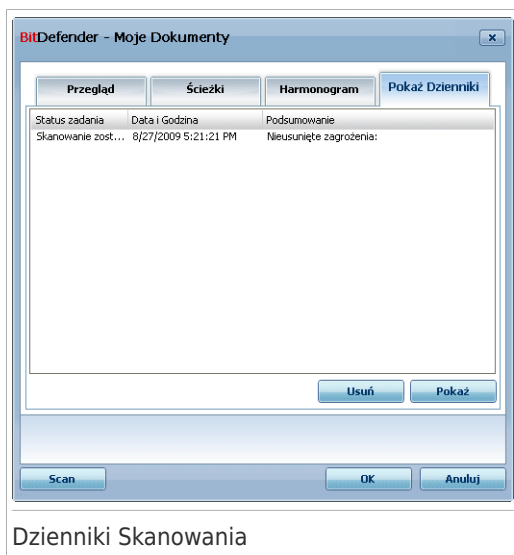
BitDefender Wykrył Podejrzane Pliki

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.

18.2.6. Przeglądanie Dzienników Skanowania

Aby zobaczyć wyniki skanowania po wykonaniu zadania, kliknij prawym przyciskiem myszy zadanie i wybierz **Dzienniki**. Pojawi się następujące okno:



Tu możesz zobaczyć pliki raportów generowanych po każdym wykonaniu zadania. Każdy plik zawiera informację o statusie procesu skanowania, datę i czas wykonania oraz podsumowanie rezultatów skanowania.

Dostępne są dwa przyciski:

- **Usuń** - usuwa wybrany plik dziennika.
- **Pokaż** - otwiera wybrany plik dziennika. Dziennik skanowania otworzy się w twojej domyślnej przeglądarce internetowej.



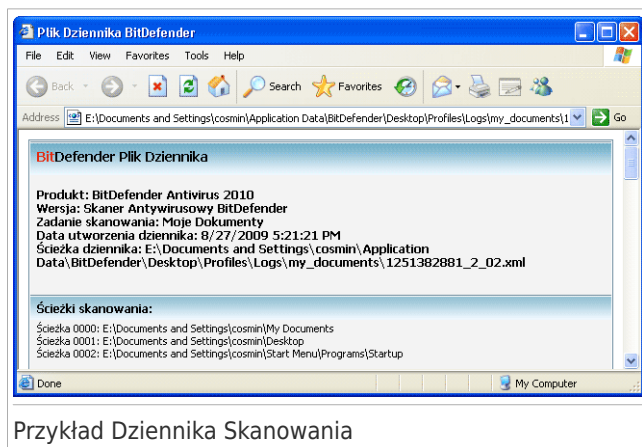
Notatka

Ponadto, aby wyświetlić lub usunąć plik kliknij na niego prawym przyciskiem i wybierz odpowiednią opcję z menu.

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

Przykład Dziennika Skanowania

Następująca pozycja przedstawia przykład dziennika skanowania:



Przykład Dziennika Skanowania

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

18.3. Elementy Wykluczone ze 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:

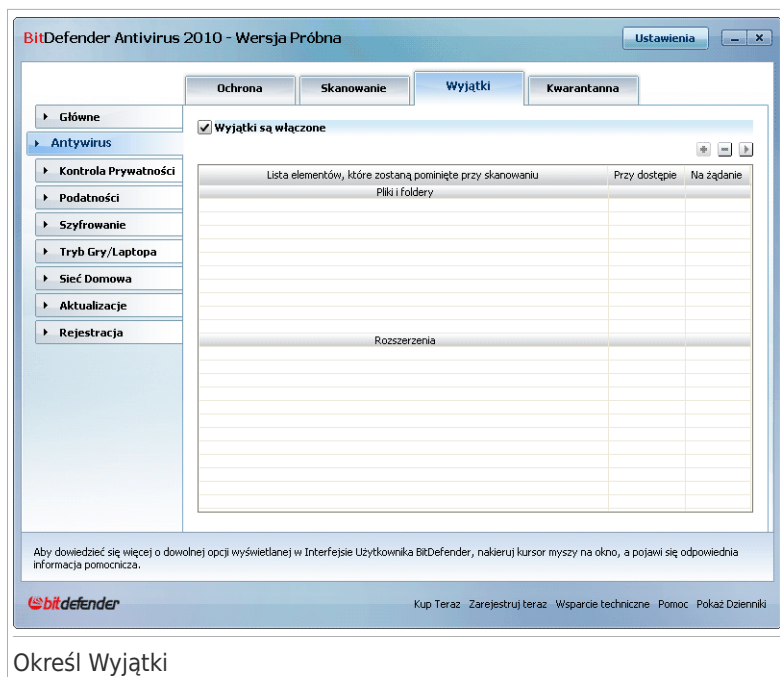
- **Ścieżki** - plik lub folder (ze wszystkimi elementami wewnątrz niego) ze wskazaną ścieżką zostanie wykluczony ze skanowania.
- **Rozszerzenia** - wszystkie pliki posiadające podane rozszerzenie zostaną wykluczone ze skanowania.



Notatka

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

Aby zobaczyć i zarządzać obiektami wykluczonymi ze skanowania, kliknij **Antywirus>Wyjątki** w Trybie Eksperta.



Określ Wyjątki

Możesz zobaczyć obiekty (pliki, foldery, rozszerzenia), które są wyłączone ze skanowania. Dla każdego obiektu, który widzisz, że jest wykluczony ze skanowania przy dostępie czy na żądanie (lub obydwu).



Notatka

Wyjątki podane tutaj **NIE** będą stosowane do skanowania kontekstowego. Skanowanie kontekstowe jest typem skanowania na żądanie: klikasz prawym przyciskiem myszy na folder który chcesz skanować i wybierasz **Skanuj z BitDefender**.

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

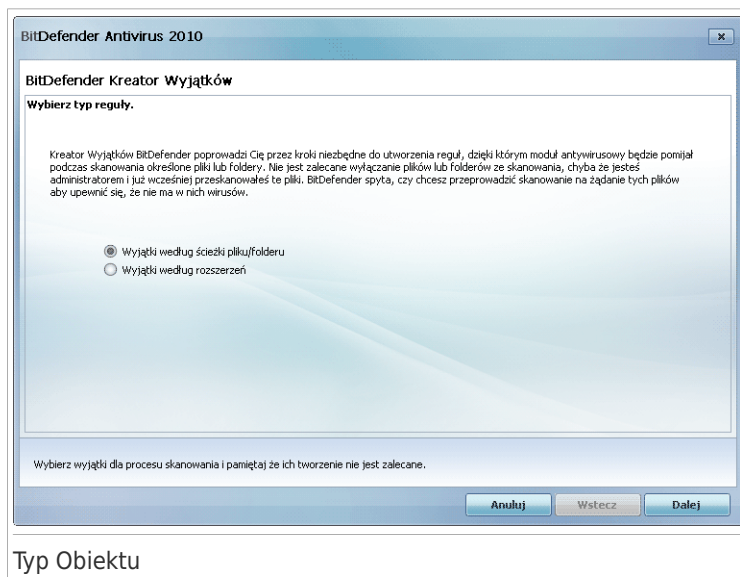
Możesz również kliknąć prawym klawiszem myszy na obiekt i wykorzystać opcje menu do edytowania lub usuwania go.

Możesz kliknąć **Odrzuć** aby odwrócić zmiany dokonane w tabeli reguł, jeśli ich nie zapisałeś klikając **Zastosuj**.

18.3.1. Wykluczanie Ścieżek ze Skanowania

Aby wykluczyć ścieżki ze skanowania, kliknij  **Add**. Zostaniesz przeprowadzony przez proces wykluczania ścieżek ze skanowania przez kreator konfiguracji, który się pojawi.

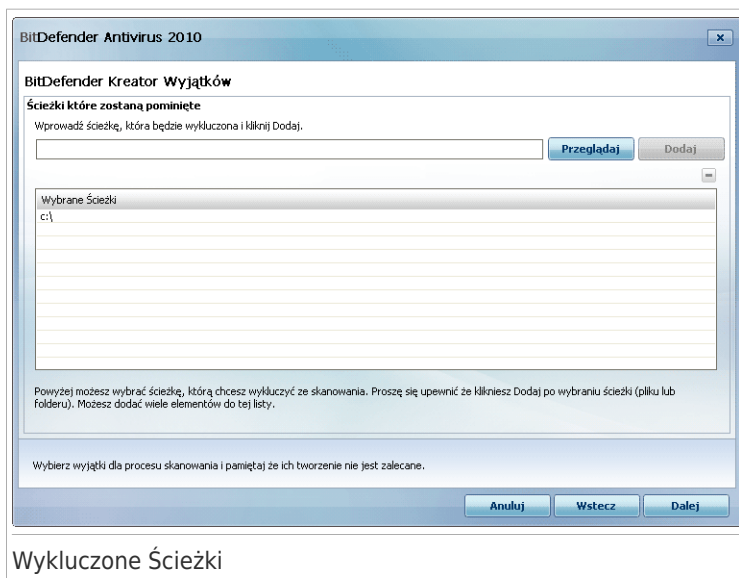
Krok 1/4 – Wybierz Typ Obiektu



Wybierz opcję wykluczenia ścieżki ze skanowania.

Kliknij **Dalej**.

Krok 2/4 – Określ Wykluczone Ścieżki



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**.



Notatka

Jeśli podana ścieżka nie istnieje, pojawi się wiadomość o błędzie. Kliknij **OK** i sprawdź poprawność ścieżki.

Ścieżki pojawiają się na liście gdy będziesz je dodawał. Możesz dodać tyle ścieżek ile chcesz.

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

Kliknij **Dalej**.

Krok 3/4 -Wybierz Typ Skanowania

BitDefender Antivirus 2010

Wybierz typ skanowania

Proszę wybrać typ skanowania który będzie stosowany wobec wybranych wyjątków: na żądanie, przy dostępie do pliku lub obydwu. Kliknij tekst w każdym polu w prawej kolumnie poniższej tabeli i wybierz opcję, które najbardziej Ci odpowiadają.

Wybrane obiekty	Wybierz typ skanowania
c:\	Obydwu

Wybierz wyjątki dla procesu skanowania i pamiętaj że ich tworzenie nie jest zalecane.

Anuluj Wstecz Dalej

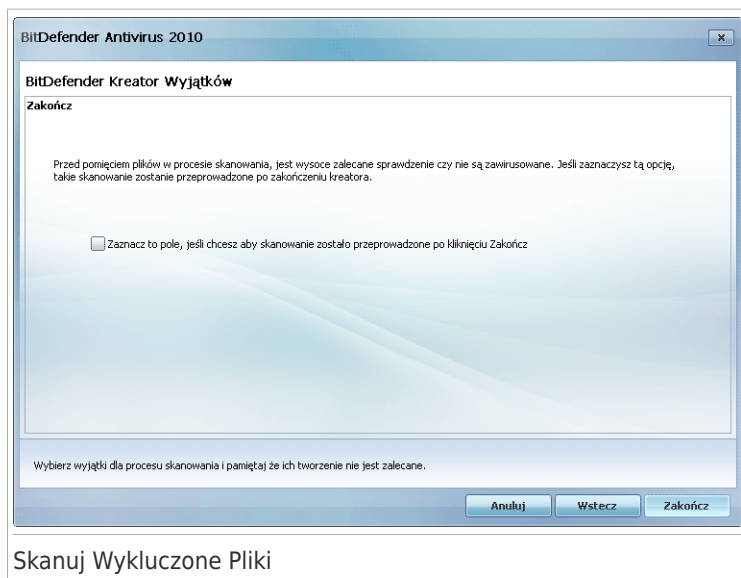
Typ Skanowania

Możesz zobaczyć tabelę zawierającą wykluczone ze skanowania ścieżki i typ skanowania z którego są wykluczone.

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.

Kliknij **Dalej**.

Krok 4/4 – Skanuj Wykluczone Pliki



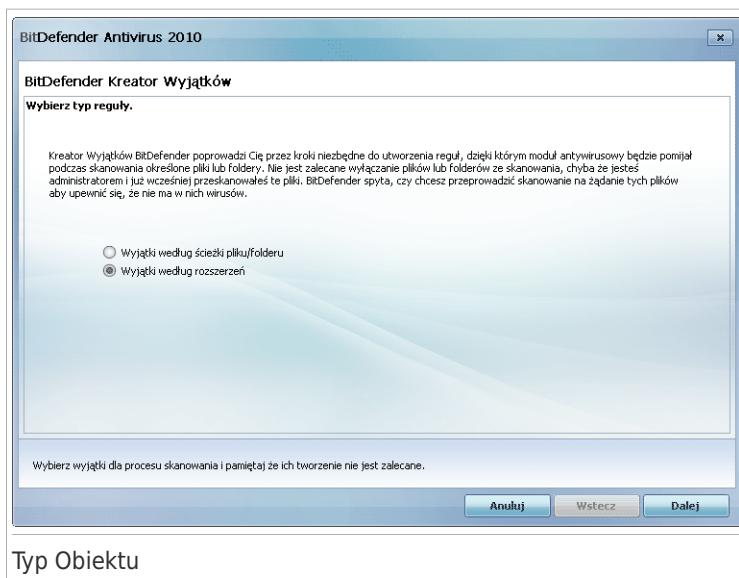
Wysoce zalecane jest skanowanie podanych ścieżek aby się upewnić że nie są one zainfekowane. Zaznacz odpowiednie pole aby skanować te pliki przed wykluczeniem ich ze skanowania.

Kliknij **Zakończ**.

18.3.2. Wykluczanie Rozszerzeń ze Skanowania

Aby wykluczyć rozszerzenia ze skanowania, kliknij przycisk  **Dodaj**. Zostaniesz przeprowadzony przez proces wykluczania rozszerzeń ze skanowania przez kreator konfiguracyjny który się pojawi.

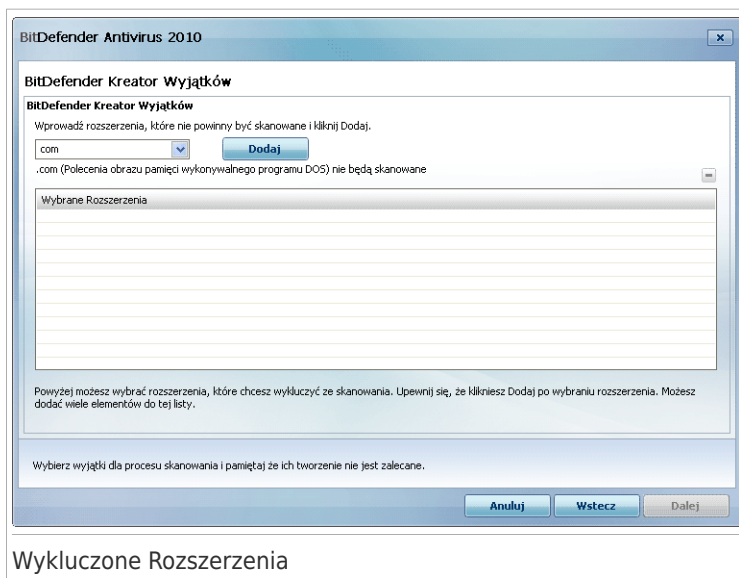
Krok 1/4 – Wybierz Typ Obiektu



Wybrano opcję wykluczenia rozszerzeń ze skanowania.

Kliknij **Dalej**.

Krok 2/4 – Określanie Wykluczonych Rozszerzeń



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

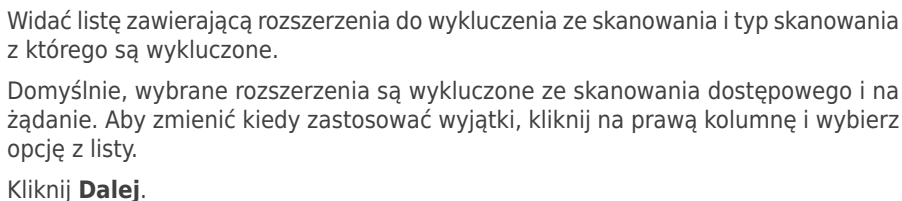
Menu zawiera listę wszystkich rozszerzeń zarejestrowanych w twoim komputerze. Gdy wybierasz rozszerzenie, możesz zobaczyć jego opis jeśli jest dostępny.

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

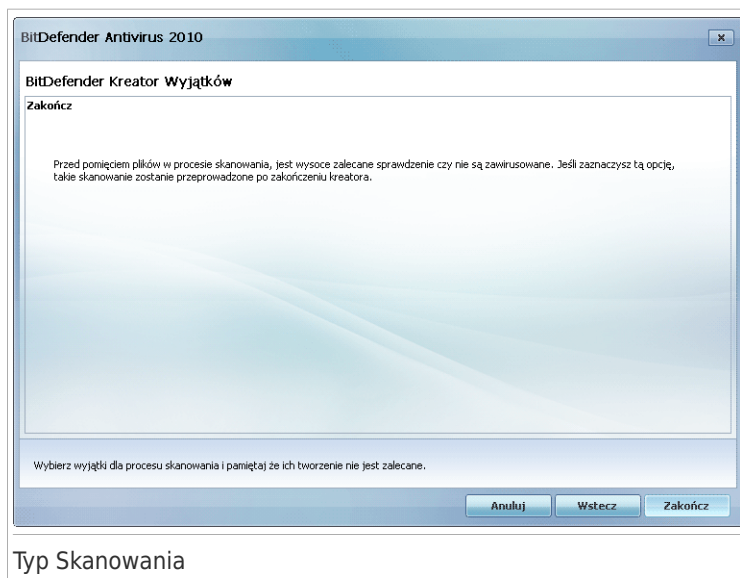
Rozszerzenia pojawią się w tabeli gdy je dodasz. Możesz dodać tyle rozszerzeń ile chcesz.

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

Kliknij **Dalej**.



Krok 4/4 Wybierz Typ Skanowania



Wysoce zalecane jest skanowanie plików mających podane rozszerzenia aby się upewnić że nie są zainfekowane.

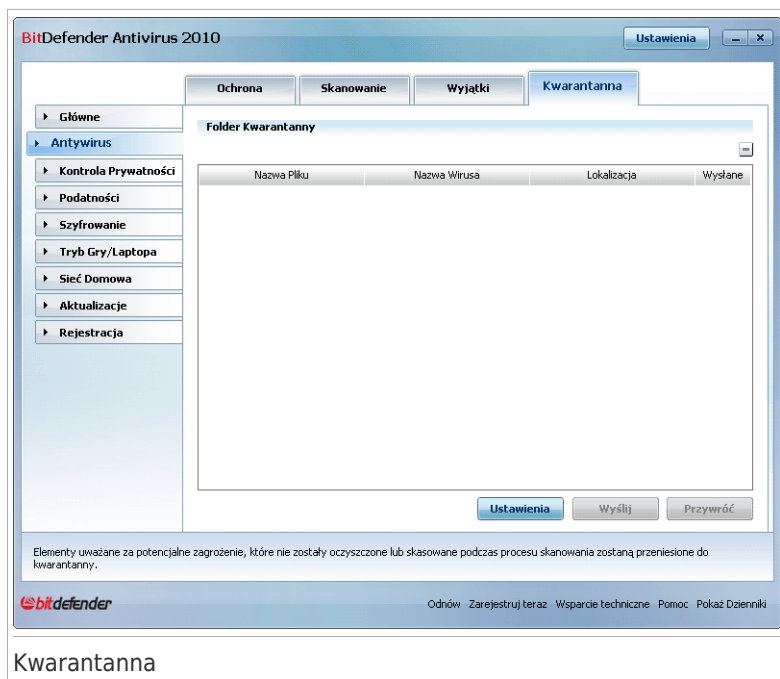
Kliknij **Zakończ**.

18.4. 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.

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

Aby zobaczyć i zarządzać plikami w kwarantannie oraz skonfigurować ustawienia kwarantanny, kliknij **Antywirus>Kwarantanna** w Trybie Eksperta.



Sekcja Kwarantanny pokazuje wszystkie pliki aktualnie odizolowane w folderze Kwarantanny. Dla każdego pliku możesz zobaczyć jego nazwę, nazwę wykrytego w nim wirusa, oryginalną ścieżkę oraz datę przeniesienia.



Notatka

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

18.4.1. Zarządzanie Plikami w Kwarantannie

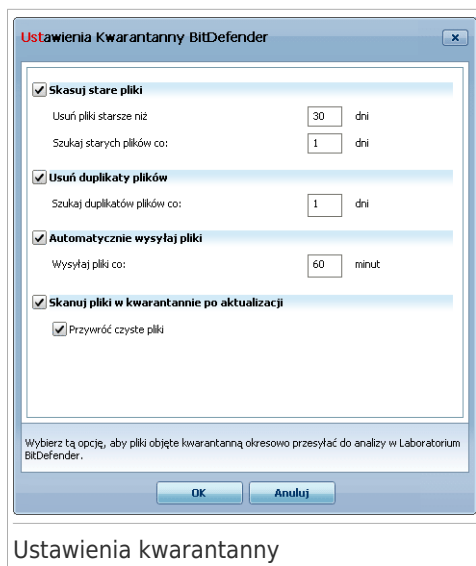
Możesz wysłać zaznaczony plik z kwarantanny do laboratorium BitDefender klikając **Wyślij**. Domyślnie, BitDefender automatycznie wyśle pliki z kwarantanny co 60 minut.

Aby usunąć zaznaczony plik z kwarantanny, kliknij przycisk  **Usuń**. Jeżeli chcesz przywrócić zaznaczony plik do jego pierwotnej lokalizacji, kliknij **Przywróć**.

Menu Kontekstowe. Menu kontekstowe jest dostępne, pozwala ono na łatwe zarządzanie plikami w kwarantannie. dostępne są te same opcje co wymienione wcześniej. Możesz również wybrać **Odśwież** aby odświeżyć sekcję Kwarantanny.

18.4.2. Konfigurowanie Ustawień Kwarantanny

Aby skonfigurować ustawienia kwarantanny kliknij **Ustawienia**. Pojawi się nowe okno.



Ustawienia kwarantanny

Używając ustawień kwarantanny, możesz ustawić BitDefendera aby automatycznie wykonywał następujące działania:

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



Notatka

Domyślnie, BitDefender szuka starych plików codziennie i usuwa pliki starsze niż 30 dni.

Skasuj duplikaty plików. Aby automatycznie usunąć duplikaty plików w kwarantannie, zaznacz odpowiednią opcję. Musisz określić liczbę dni między dwoma następnymi sprawdzeniami duplikatów.



Notatka

Domyślnie, BitDefender szuka duplikatów plików w kwarantannie codziennie.

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



Notatka

Domyślnie, BitDefender automatycznie wyśle pliki z kwarantanny co 60 minut.

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

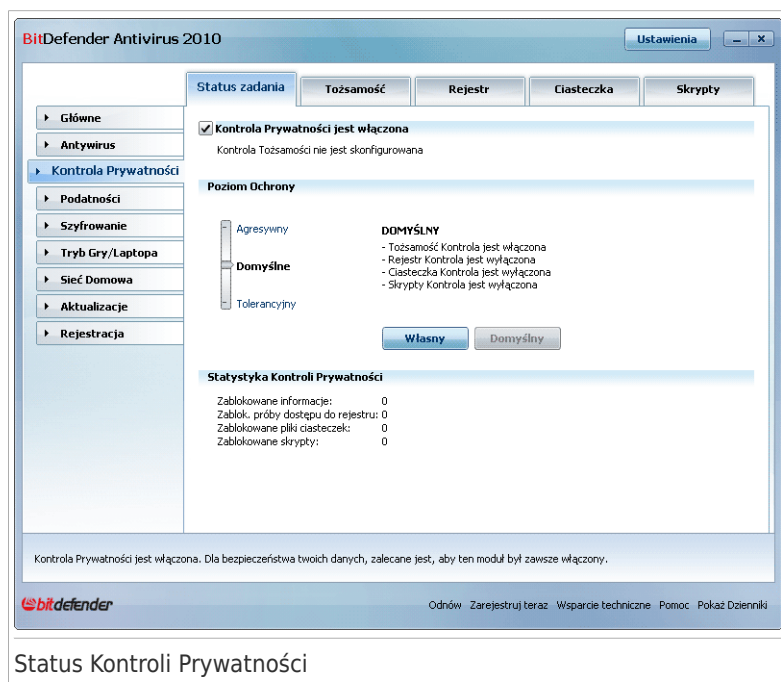
Kliknij **OK** aby zapisać zmiany i zamknąć okno.

19. 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.

19.1. Status Kontroli Prywatności

Aby skonfigurować Kontrolę Prywatności i zobaczyć informacje dotyczące jej aktywności, kliknij **Kontrola Prywatności>Status** w Trybie Eksperta.



Możesz zobaczyć czy Kontrola Prywatności jest włączona czy wyłączona. Jeżeli chcesz zmienić status Kontroli Prywatności, zaznacz lub odznacz odpowiednią opcję.



WAŻNE

Aby ochronić dane przed kradzieżą i zachować prywatność miej **Kontrolę Prywatności** włączoną.

Kontrola Prywatności chroni twój komputer używając tych ważnych modułów ochrony:

- **Kontrola Tożsamości** - chroni Twoje prywatne dane filtrując cały wychodzący ruch stron www (HTTP) i pocztę (SMTP) zgodnie z regułami stworzonymi w sekcji **Tożsamość**.
- **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.

W dolnej części tej sekcji możesz zobaczyć **sStatystyka Kontroli Prywatności**.

19.1.1. Konfigurowanie Poziomu Ochrony

Możesz wybrać poziom ochrony, który najbardziej odpowiada twoim potrzebom. Przeciągnij suwak po skali aby ustawić odpowiedni poziom ochrony.

Dostępne są 3 poziomy ochrony:

Poziomy ochrony	Opis
Tolerancyjny	Kontrola wszystkich zabezpieczeń jest zablokowane.
Domyślny	Włączona jest tylko Kontrola Tożsamości
Agresywny	Kontrola Tożsamości, Kontrola Rejestru, Kontrola Ciasteczek i Kontrola Skryptów są odblokowane.

Możesz dostosować poziom ochrony klikając **Użytkownika**. W oknie które się pojawi, wybierz kontrole zabezpieczeń które chcesz włączyć i kliknij **OK**.

Kliknij **Domyślny** aby przywrócić suwak na domyślny poziom.

19.2. Kontrola 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 informację 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 stworzysz 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. Hacker może poznać ważne informacje z ukradzionych danych, takie jak numer i hasło do konta bankowego i użyć ich na własną korzyść.

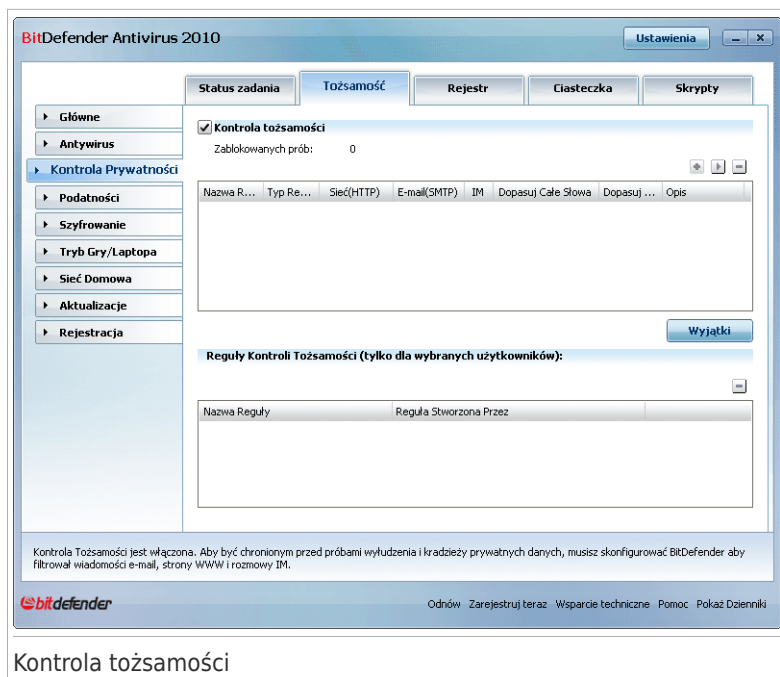
Zakładając że takie aplikacje są w stanie uniknąć wykrycia przez oprogramowanie antywirusowe, nie mogą one wysłać skradzionych danych przez email, stronę www lub komunikator jeśli utworzyłeś odpowiednią regułę ochrony tożsamości.

- 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.

Aby skonfigurować Kontrolę Tożsamości kliknij **Kontrola Prywatności>Tożsamość** w Trybie Eksperta.



Kontrola tożsamości

Jeżeli chcesz korzystać z Kontroli Tożsamości, proszę wykonać następujące kroki:

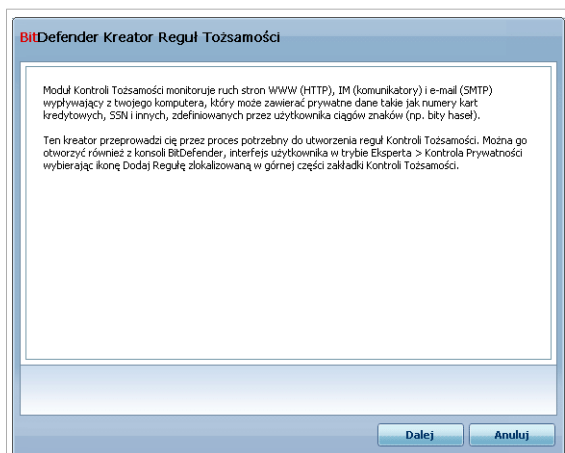
1. Zaznacz pole **Włącz Kontrolę Tożsamości**.
2. Utwórz reguły mające chronić twoje ważne dane. Aby uzyskać więcej informacji, odwołaj się do „*Tworzenie Reguł Tożsamości*” (p. 154).
3. Jeśli trzeba, zdefiniuj wyjątki od reguł które utworzyłeś. Aby uzyskać więcej informacji, odwołaj się do „*Definiowanie Wyjątków*” (p. 158).
4. Jeśli jesteś administratorem komputera, możesz wyłączyć siebie z reguł kontroli tożsamości tworzonych przez innych administratorów.

Aby uzyskać więcej informacji, odwołaj się do „*Reguły Zdefiniowane przez Innych Administratorów*” (p. 159).

19.2.1. Tworzenie Reguł Tożsamości

Aby utworzyć regułę ochrony tożsamości kliknij  **Dodaj** aby rozpocząć kreator konfiguracji.

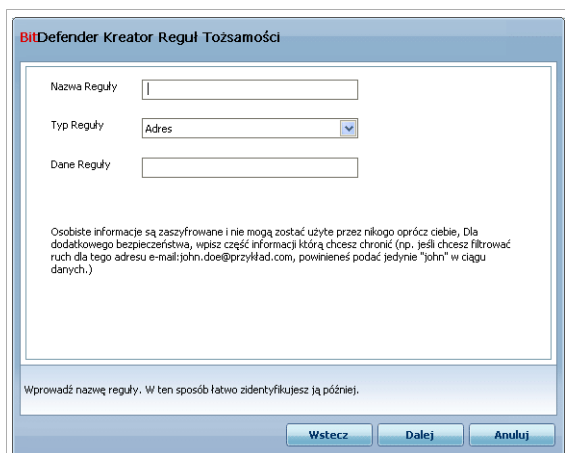
Krok 1/4 - Powitanie



Okno Powitania

Kliknij **Dalej**.

Krok 2/4 - Wybierz Typ i Dane Reguły



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.



Notatka

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.

Kliknij **Dalej**.

Krok 3/4 - Wybierz Typy Ruchu i Użytkowników

Wybierz Typy Ruchu i Użytkowników

Wybierz rodzaj ruchu jaki ma być skanowany przez BitDefendera. Dostępne są następujące opcje:

- **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.

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 ograniczonymi prawami.
- **Wszyscy użytkownicy** - reguła zostanie zastosowana dla wszystkich kont Windows.

Kliknij **Dalej**.

Krok 4/4 – Opisz Regułę

BitDefender Kreator Reguł Tożsamości

Opis Reguły

Wprowadź opis tej reguły. Opis ten powinien pomóc Tobie oraz innym administratorom systemu w łatwiejszym zidentyfikowaniu informacji, które blokuje dana reguła.

Wprowadź opis reguły. Kreator nie pozwoli ci na wpisanie w tym polu danych które chcesz chronić.

Wstecz Zakończ Anuluj

Opisz Regułę

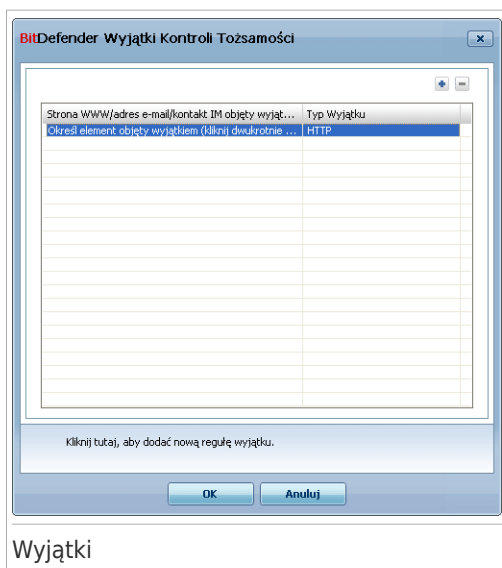
Wprowadź krótki opis reguły w polu edycji. Ponieważ zablokowane dane (ciąg znaków) nie jest wyświetlany jako tekst przy dostępie do reguły, opis powinien pomóc w identyfikacji.

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

19.2.2. 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**.

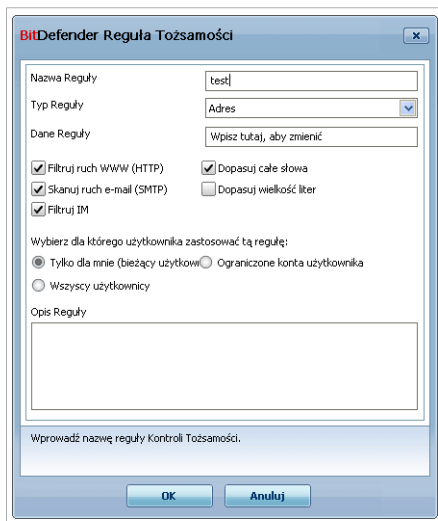
Kliknij **Zastosuj** aby zapisać zmiany.

19.2.3. Zarządzanie Regułami

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.



Edytuj regułę

Możesz tutaj zmienić nazwę, opis i parametry reguły (typ, dane i ruch). Kliknij **OK** aby zapisać zmiany.

19.2.4. Reguły Zdefiniowane przez Innych Administratorów

Gdy nie jesteś jedynym użytkownikiem systemu z prawami administratora, inni administratorzy też mogą tworzyć reguły. W przypadku gdy chcesz, aby reguły tworzone przez innych użytkowników nie były wprowadzane po zalogowaniu się do systemu, BitDefender pozwala na wyłączenie użytkownika z listy reguł których sam nie stworzył.

W tabeli **Reguły Kontroli Tożsamości** możesz zobaczyć pełną listę reguł stworzonych przez innych administratorów. Dla każdej reguły, obok jej nazwy, wyświetlany jest jej twórca.

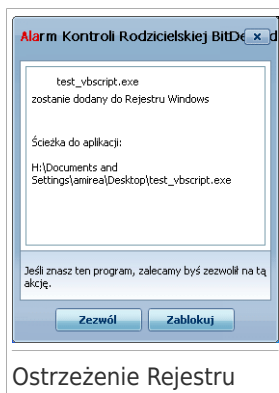
Aby pominąć siebie w tej regule, wybierz regułę w tabeli i kliknij przycisk  **Usuń**.

19.3. Kontrola rejestru

Rejestr stanowią 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.



Ostrzeżenie Rejestru

Możesz zobaczyć program który próbuje zmodyfikować rejestr Windows.

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

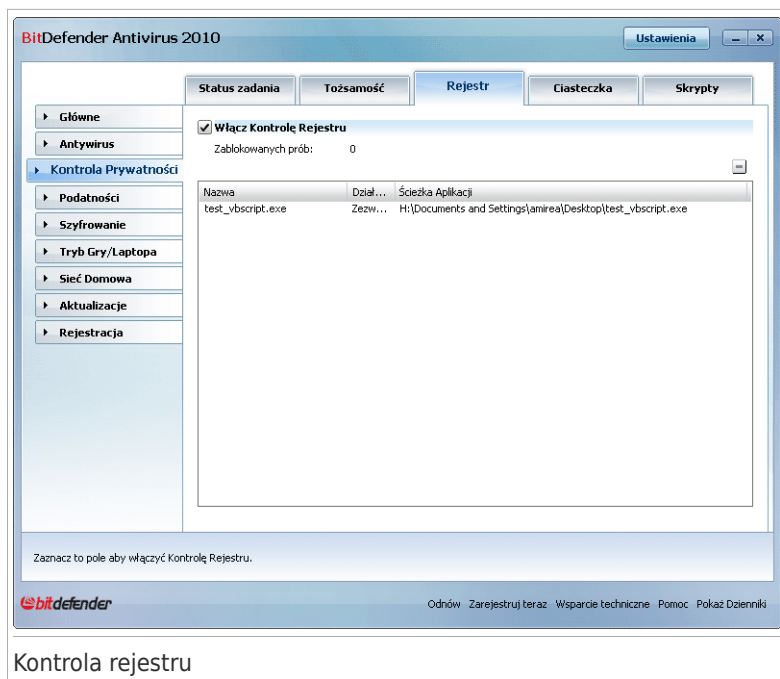
W zależności od twojej odpowiedzi reguła jest tworzona w tabeli reguł. To same działanie jest stosowane kiedy ten program próbuje modyfikować rejestr.



Notatka

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

Aby skonfigurować Kontrolę Rejestru **Kontrola Prywatności>Rejest** w Trybie Eksperta.



Kontrola rejestru

W tabeli możesz zobaczyć wszystkie dotychczas utworzone reguły.

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

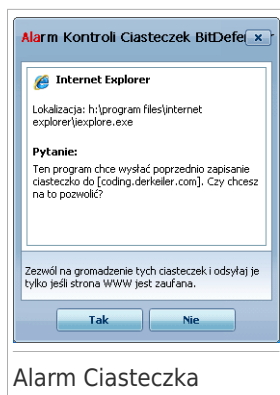
19.4. Kontrola cookie

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 ułatwiać 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 używane, aby zagrozić twojej prywatności np. poprzez śledzenie twojego ruchu w Internecie.

W tym przypadku pomaga **Kontrola Ciasteczek**. Kiedy jest włączona, **Kontrola Ciasteczek** będzie za każdym razem pytać o pozwolenie, kiedy nowa strona sieci będzie próbowała ustawić ciasteczko:



Możesz obejrzeć nazwę aplikacji, która próbuje przesłać plik ciasteczka.

Kliknij **Tak** lub **Nie** a reguła zostanie stworzona, dodana i wyświetlona w tabeli reguł.

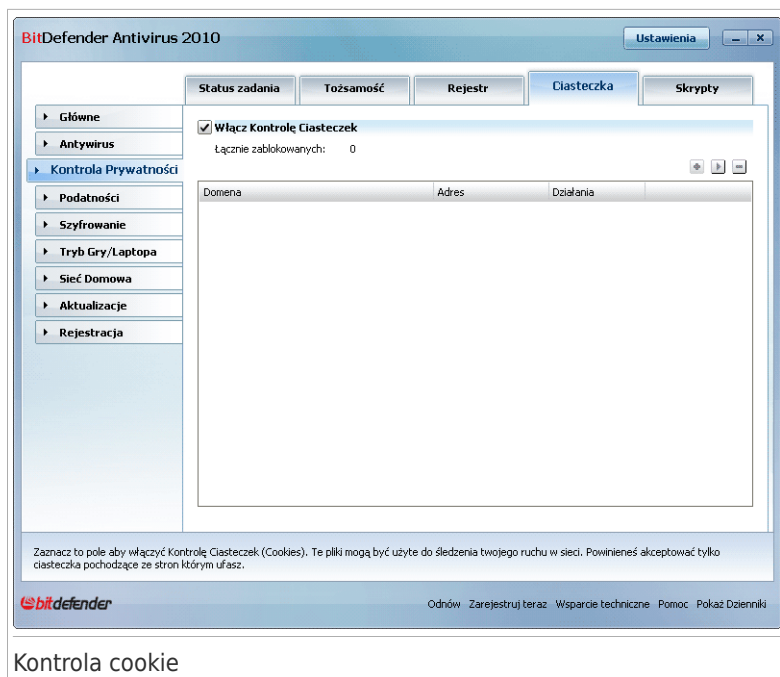
Pomoże to tobie wybrać strony sieci, którym ufasz a którym nie.



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.

Aby skonfigurować Kontrolę Ciasteczek, przejdź do **Kontrola Prywatności>Ciasteczka** w Trybie Eksperta.



W tabeli możesz zobaczyć wszystkie dotychczas utworzone reguły.



WAŻNE

Reguły są ustawione według priorytetu, zaczynając od najwyższego. Uchwyć i przeciągnij reguły aby zmienić ich priorytet.

Aby usunąć regułę, wybierz ją i kliknij **Usuń**. Aby zmienić parametry reguły, kliknij ją dwukrotnie lub kliknij przycisk **Edytuj**. Wprowadź porządane zmiany w oknie konfiguracyjnym.

Aby ręcznie dodać regułę, kliknij **Dodaj** i skonfiguruj parametry reguły w oknie konfiguracyjnym.

19.4.1. Okno Konfiguracji

Gdy edytujesz lub ręcznie dodajesz regułę, pojawi się okno konfiguracyjne.

BitDefender Kreator Reguł Ciasteczek

Domena:

☒ Dowlina
☐ Domena:

Wybierz Działanie

☒ Zezwolone
☐ Zabroń

Wybierz Kierunek

☐ Wysyłane
☐ Odbierane
☒ Obydwa

Wybierz strony internetowe i domeny, których ciasteczka akceptujesz lub odrzucasz. Pliki ciasteczek mogą być używane do śledzenia użytkowników. Uwaga - niektóre strony nie działają prawidłowo bez ciasteczek.

Wybierz Adres, Działanie i Kierunek

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
Wychodzące	Reguła będzie zastosowana wyłącznie dla ciasteczek, które są wysyłane z powrotem do podłączonych stron.
Przychodzące	Reguła będzie zastosowana wyłącznie dla ciasteczek, które są otrzymane z powrotem z podłączonych stron.
Oba	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**.

19.5. Kontrola Skryptów

Skrypty i inne kody takie jak **Kontrola 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.

BitDefender pozwala wybrać czy chcesz uruchamiać te elementy czy blokować ich wykonywanie.

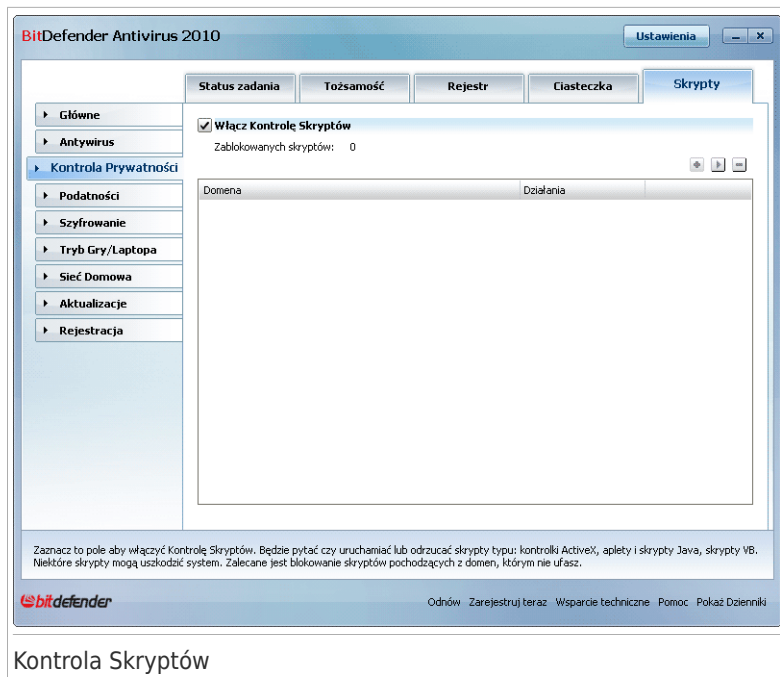
Ze **Skryptem Kontroli** będziesz decydował, którym stronom sieci ufasz, a którym nie. BitDefender będzie cię prosił o pozwolenie za każdym razem gdy strona sieci będzie próbowała aktywować skrypt lub inny aktywny składnik:



Możesz obejrzeć nazwę źródła.

Kliknij **Tak** lub **Nie** a reguła zostanie stworzona, dodana i wyświetlona w tabeli reguł.

Aby skonfigurować Kontrolę Skryptów, przejdź do **Kontrola Prywatności>Skrypt** w Trybie Eksperta.



W tabeli możesz zobaczyć wszystkie dotychczas utworzone reguły.



WAŻNE

Reguły są ustawione według priorytetu, zaczynając od najwyższego. Uchwyć i przeciągnij reguły aby zmienić ich priorytet.

Aby usunąć regułę, wybierz ją i kliknij **Usuń**. Aby zmienić parametry reguły, kliknij ją dwukrotnie lub kliknij przycisk **Edytuj**. Wprowadź porządane zmiany w oknie konfiguracyjnym.

Aby ręcznie utworzyć regułę, kliknij **Dodaj** i skonfiguruj parametry reguły w oknie konfiguracyjnym.

19.5.1. Okno Konfiguracji

Gdy edytujesz lub ręcznie dodajesz regułę, pojawi się okno konfiguracyjne.

BitDefender Kreator Reguł Skryptów

Domena:

☒ Dowolna

☐ Domena:

Wybierz Działanie

☒ Zezwolone

☐ Zabroń

Wybierz określoną domenę(domeny), którym chcesz pozwolić lub zablokować uruchamianie skryptów.
Ogólnie, powinieneś używać tego kreatora dla określonych domen, którym chcesz zezwolić na uruchamianie skryptów. Zalecamy blokować skrypty ze wszystkich domen, którym nie ufasz.

Zakończ **Anuluj**

Wybierz Adres i Działanie

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**.

20. 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 zagrożeniach.

20.1. Status zadania

Aby skonfigurować automatyczne sprawdzanie podatności lub uruchomić sprawdzanie podatności, kliknij **Podatności>Status** w Trybie Eksperta.

BitDefender Antivirus 2010 - Wersja Próba

Ustawienia

Status zadania Ustawienia

☒ Automatyczne Sprawdzanie Podatności jest włączone

Sprawdź Teraz

Stan Sprawdzania Podatności

Zagadnienie	Status zadania	Działania
Krytyczne aktualizacje Microsoft	Najnowsze	Brak
Inne aktualizacje Microsoftu	Najnowsze	Brak
Status Automatycznej Aktualizacji	Włączone	Brak
Yahoo! Messenger	Nieaktualne	Wiecej Inform...
Firefox	Nieaktualne	Wiecej Inform...
Windows Live Messenger	Nieaktualne	Wiecej Inform...
child	Słabe Hasło	Napraw
cosmin	Słabe Hasło	Napraw
stefan	Słabe Hasło	Napraw

Aby dowiedzieć się więcej o dowolnej opcji wyświetlanej w Interfejsie Użytkownika BitDefender, nakieruj kursor myszy na okno, a pojawi się odpowiednia informacja pomocnicza.

bitdefender

Kup Teraz Zarejestruj teraz Wsparcie techniczne Pomoc Pokaż Dziennik

Status Podatności

Ta tabela pokazuje zagrożenia 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 zagrożenie nie jest podatnością.



WAŻNE

Aby być automatycznie informowanym o podatnościach systemu oraz aplikacji, miej włączone **Automatyczne Sprawdzanie Podatności Aktualizacja**.

20.1.1. Naprawianie Podatności

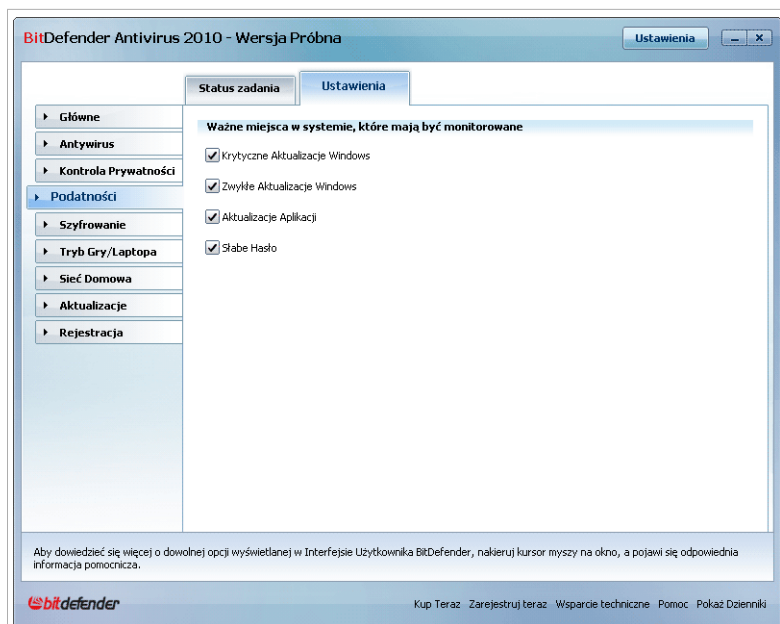
W zależności od zagadnienia, naprawienie określonej podatności wygląda następująco:

- Jeśli są dostępne aktualizacje Windows, kliknij na **Instaluj** w kolumnie **Akcja** aby je zainstalować.
- Jeśli aplikacja jest nieaktualna wejdź na jej **Stronę Domową** aby pobrać i zainstalować najnowszą wersję tej aplikacji.
- Jeśli użytkownik Windows posiada słabe hasło, kliknij **Napraw** aby zmusić użytkownika do jego zmiany przy następnym logowaniu lub sam(a) zmień hasło. Aby hasło było silne, użyj kombinacji dużych i małych liter, cyfr oraz znaków specjalnych (takich jak #, \$ lub @).

Możesz kliknąć **Sprawdź Teraz** i przejść kreator aby naprawić podatności krok po kroku. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Sprawdzania Podatności*” (p. 65).

20.2. Ustawienia

Aby skonfigurować ustawienia automatycznego sprawdzania podatności, kliknij **Podatności>Ustawienia** w Trybie Eksperta.



Ustawienia Automatycznego Sprawdzania Podatności

Zaznacz pola odpowiednich podatności systemu które chcesz aby były regularnie sprawdzane.

- **Krytyczne Aktualizacje Windows**
- **Regularne Aktualizacje Windows.**
- **Aktualizacje Aplikacji**
- **Słabe Hasło.**



Notatka

Jeśli odznaczysz pole obok podatności, BitDefender nie będzie informował ciebie o zagadnieniach z nią związanych.

21. Szyfrowanie Komunikatorów (IM)

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

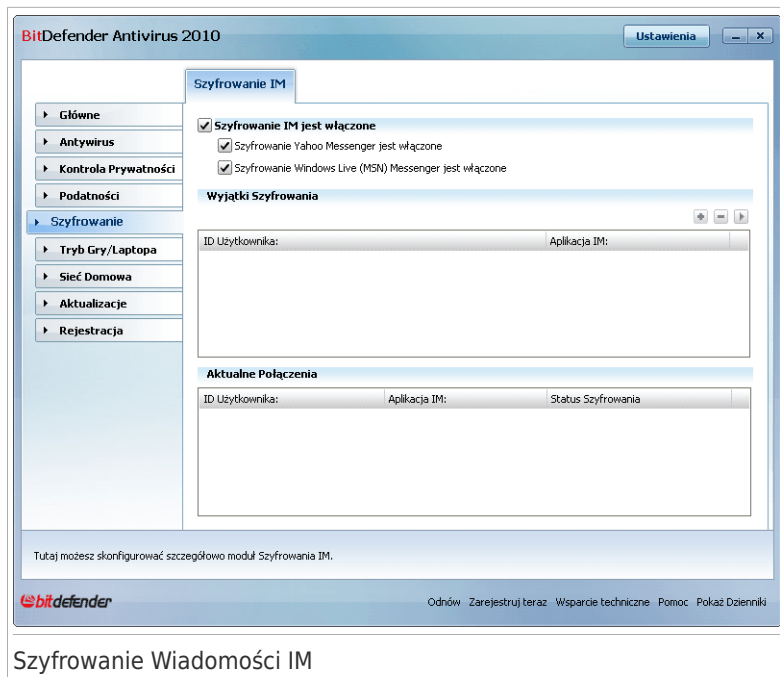
BitDefender nie będzie szyfrował rozmowy, jeśli rozmówca korzysta z komunikatora bazującego na stronie WWW, takiego jak Czateria, lub innej aplikacji do rozmów która obsługuje Yahoo Messenger lub MSN.

Aby skonfigurować szyfrowanie wiadomości Instant Messaging, kliknij **Szyfrowanie>Szyfrowanie IM** w Trybie Eksperta.



Notatka

Możesz łatwo skonfigurować szyfrowanie rozmów w komunikatorach używając paska narzędzi BitDefender w oknie komunikatora. Aby uzyskać więcej informacji, odwołaj się do „*Integracja z programami Instant Messenger*” (p. 204).



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.

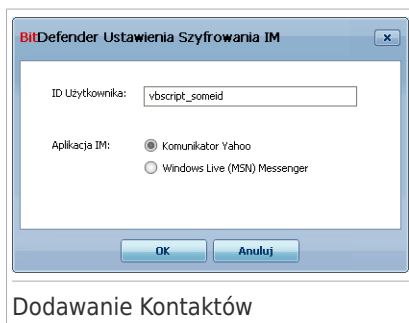
Dwie tabele są wyświetlane:

- **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) oraz 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.

21.1. Wyłączanie szyfrowania dla Podanych Użytkowników

Aby wyłączyć szyfrowanie dla podanych użytkowników, wykonaj następujące kroki:

1. Kliknij  **Dodaj** aby otworzyć okno konfiguracyjne.



2. Wpisz w polu edycji ID swojego kontaktu.
3. Wybierz komunikator przypisany do tego kontaktu.
4. Kliknij **OK**.

22. 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.

22.1. 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**.
- Domyślnie aktualizacje nie są wykonywane.



Notatka

Aby zmienić te ustawienia, kliknij **Aktualizacja>Ustawienia** i odznacz pole **Nie aktualizuj jeśli włączony jest Tryb Gry**.

- Domyślnie zadania zaplanowane są wyłączone.

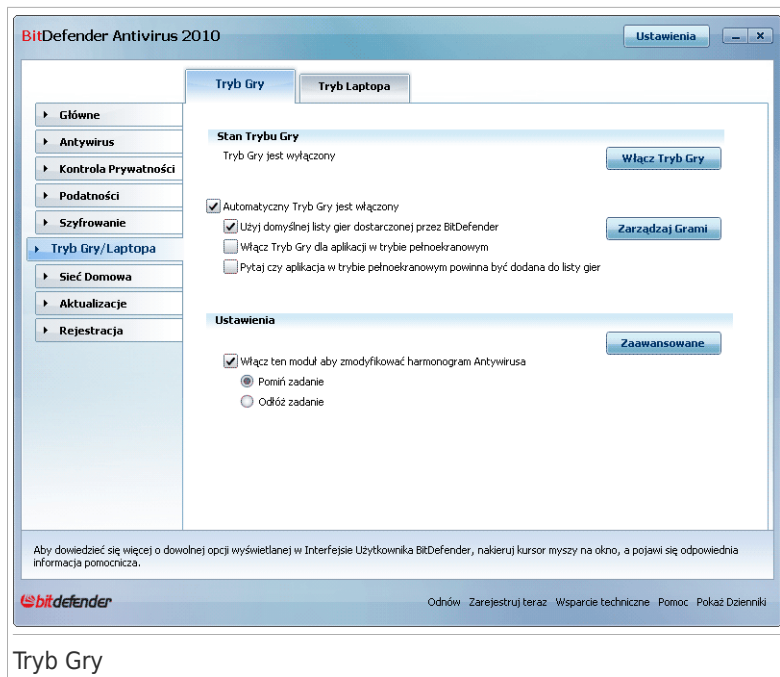
Domyślnie, BitDefender automatycznie włącza Tryb Gry gdy uruchomisz grę będącą na liście znanych gier BitDefendera lub aplikację działającą w trybie pełno ekranowym. Możesz ręcznie włączyć Tryb Gry używając domyślnych klawiszy skrótów Ctrl+Alt+Shift+G. Wysoce zalecane jest wyłączenie Trybu Gry kiedy kończysz grać (możesz użyć tej samej kombinacji klawiszy skrótów Ctrl+Alt+Shift+G).



Notatka

W Trybie Gry, możesz zobaczyć literę G nad ikoną BitDefendera.

Aby skonfigurować Tryb Gry, kliknij **Tryb Gry / Laptopa>Tryb Gry** w Trybie Eksperta.



Tryb Gry

Na górze tej sekcji, możesz zobaczyć status Trybu Gry. Możesz kliknąć na **Włącz Tryb Gry** lub **Wyłącz Tryb Gry** aby zmienić obecny stan.

22.1.1. 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**.
- **Włącz Tryb Gry przy kiedy aplikacja znajduje się w trybie pełnoekranowym** - automatycznie włącza Tryb Gry kiedy aplikacja uruchamia się w trybie pełnoekranowym.
- **Dodać aplikacje do listy gier?** - zostaniesz zapytany czy dodać nową aplikację do listy gier kiedy wyjdiesz z trybu pełnoekranowego. Dodając nową aplikację do listy gier, przy następnym uruchomieniu jej BitDefender automatycznie włączy Tryb Gry.

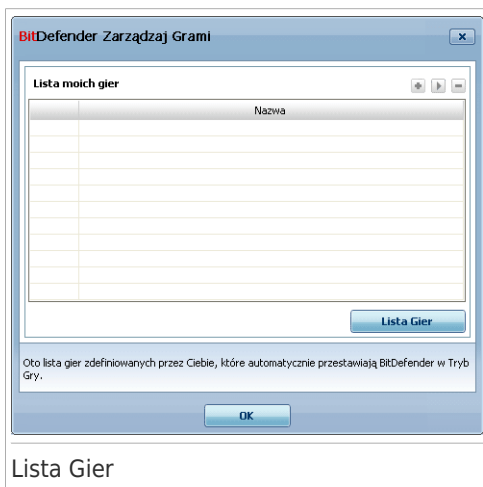


Notatka

Jeśli nie chcesz aby BitDefender automatycznie włączał Tryb Gry, odznacz pole **Automatyczny Tryb Gry**.

22.1.2. Zarządzanie Listą Gier

BitDefender automatycznie włącza Tryb Gry gdy uruchomisz aplikację 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 aplikację do listy używając okienka pytającego.

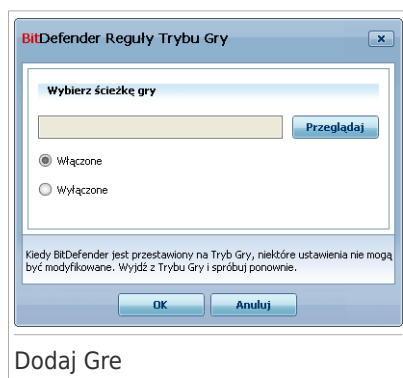
Jeśli chcesz wyłączyć Automatyczny Tryb Gry dla aplikacji z listy, odznacz odpowiednie pole. Powinieneś wyłączyć Automatyczny Tryb Gry dla zwykłych aplikacji korzystających z trybu pełnoekranowego, takich jak przeglądarka internetowa czy odtwarzacz filmów.

Aby zarządzać listą gier, możesz skorzystać z przycisków u góry tabeli:

- **Dodaj** - dodaje nową aplikację do listy gier.
- **Usuń** - usuwa aplikację z listy gier.
- **Edytuj** - edytuje wpis w liście gier.

Dodawanie lub Edytowanie Gier

Kiedy dodajesz lub edytujesz pozycje na liście gier, pojawia się następujące 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.

22.1.3. Konfigurowanie Ustawień Trybu Gry

Aby skonfigurować zachowanie zaplanowanych zadań, użyj opcji:

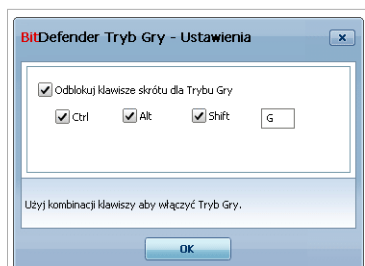
- **Pozwól temu modułowi aby modyfikować harmonogram zadań modułu Antywirusowego** - aby uniemożliwić uruchamianie zaplanowanych zadań gdy włączony jest Tryb Gry. Możesz wybrać jedną z następujących opcji:

Opcje	Opis
Pomiń Zadanie	Nie uruchamiaj zaplanowanego zadania.
Przełóż Zadanie	Uruchom wybrane zadanie natychmiast po wyłączeniu Trybu Gry.

22.1.4. Zmienianie klawiszy skrótu Trybu Gry

Możesz ręcznie włączyć Tryb Gry używając domyślnych klawiszy skrótów Ctrl+Alt+Shift+G. Jeżeli chcesz zmienić klawisze skrótu, wykonaj następujące kroki:

1. Kliknij **Zaawansowane**. Pojawi się nowe okno.



Zaawansowane

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** wyłączysz skrót klawiszowy.

3. Kliknij **Zastosuj** aby zapisać zmiany.

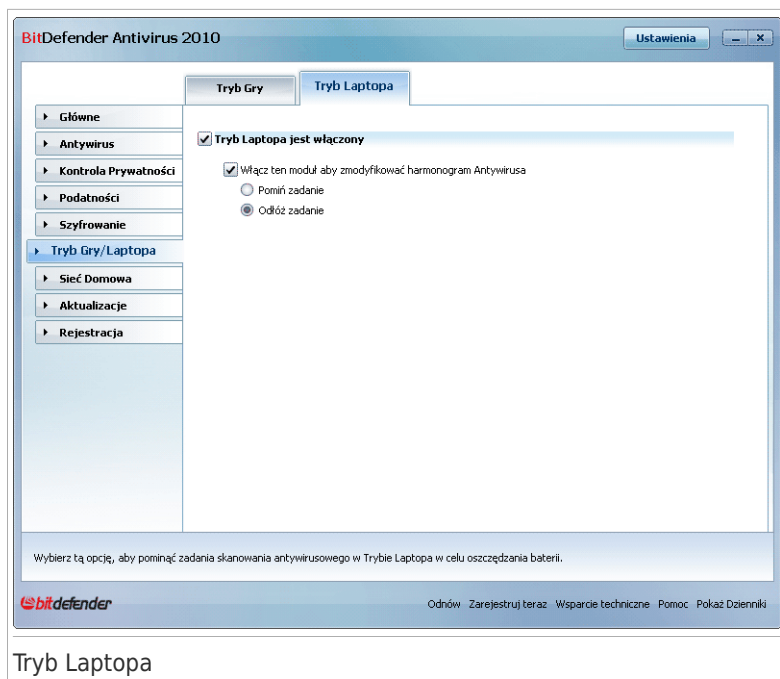
22.2. Tryb Laptopa

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.

Aby skonfigurować Tryb Laptopa, kliknij **Tryb Gry / Laptopa > Tryb Laptopa** w Trybie Eksperta.



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.

22.2.1. Konfigurowanie Ustawień Trybu Laptopa

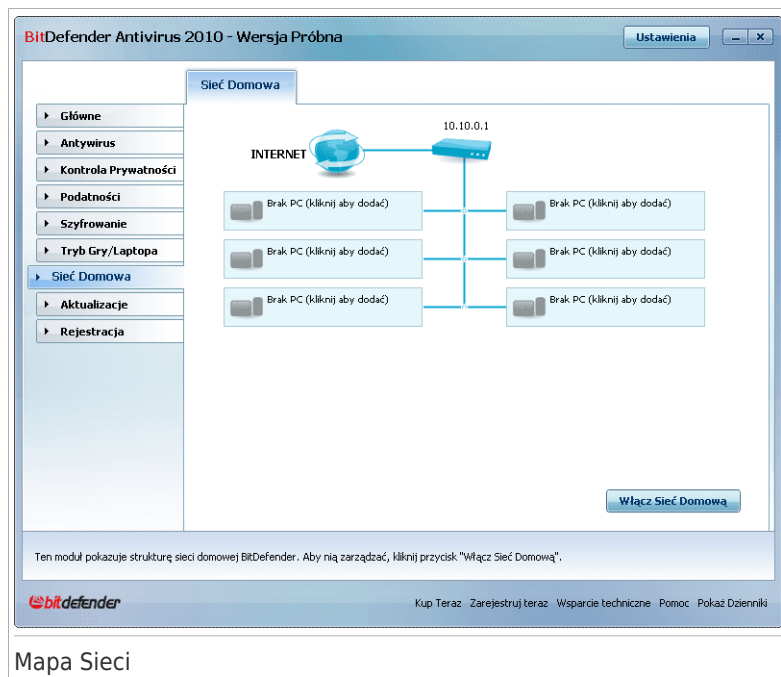
Aby skonfigurować zachowanie zaplanowanych zadań, użyj opcji:

- **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.

23. Sieć Domowa

Moduł Sieci pozwala tobie na zarządzanie produktami BitDefender zainstalowanymi na komputerach w twoim domu z pojedynczego komputera.



Mapa Sieci

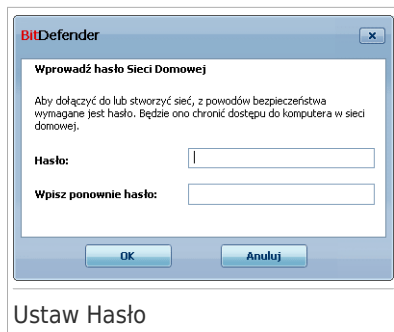
Aby móc zarządzać produktami BitDefender zainstalowanymi na twoich domowych komputerach, musisz wykonać następujące kroki:

1. Dołącz do sieci domowej BitDefender. Dołączenie do sieci wymaga skonfigurowania hasła administracyjnego do zarządzania siecią domową.
2. Idź do każdego komputera którym chcesz zarządzać i dołącz go do swojej sieci (ustaw hasło)
3. Wróć do swojego komputera i dodaj komputery którymi chcesz zarządzać.

23.1. Dołączanie do Sieci BitDefender

Aby dołączyć do sieci domowej 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. Kliknij **OK**.

Możesz zobaczyć nazwę komputerów pojawiających się w sieci.

23.2. Dodawanie Komputerów do Sieci BitDefender

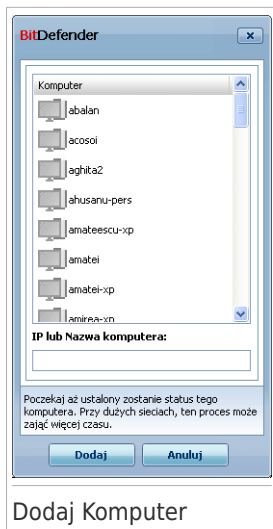
Zanim będziesz mógł dodać komputer do domowej sieci BitDefender, musisz ustawić hasło domowego zarządzania na tym komputerze.

Aby dodać komputer do domowej sieci BitDefendera, wykonaj następujące kroki:

1. Kliknij na **Dodaj Komputer**. Zostaniesz poproszony o podanie hasła domowego zarządzania.



2. Wprowadź swoje hasło domowego zarządzania i kliknij **OK**. Pojawi się nowe okno.



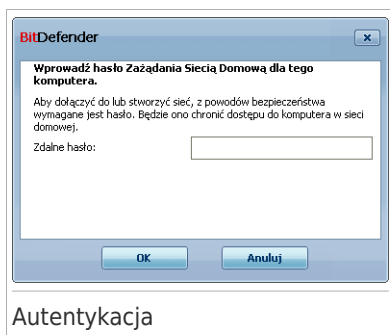
Możesz zobaczyć listę komputerów w sieci. Ikony mają następujące znaczenie:

-  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.

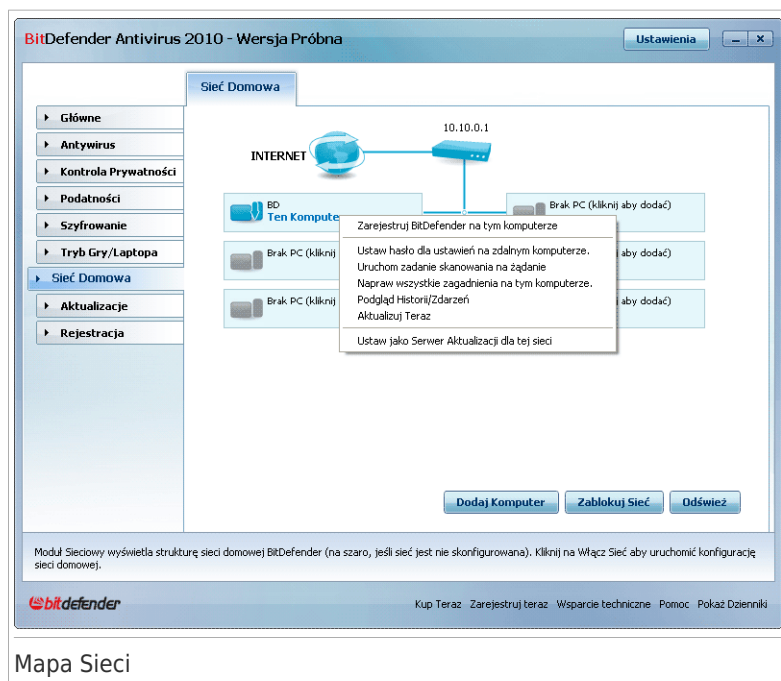


Notatka

Możesz dodać do pięciu komputerów do sieci.

23.3. 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.

● Usuń komputer z sieci domowej

Pozwala na usunięcie komputera z sieci.

● 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 Zagadnienia**.

● Pokaż Historię/Zdarzenia

Pozwala na dostęp do modułu **Historia&Zdarzenia** BitDefendera zainstalowanego na tym komputerze.

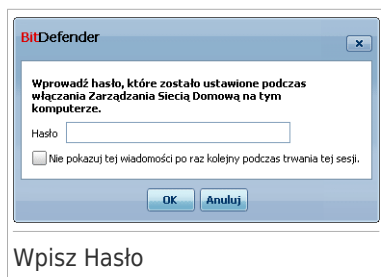
● Aktualizuj Teraz

Rozpoczyna proces Aktualizacji dla oprogramowania BitDefender zainstalowanego na tym komputerze.

● Ustaw 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.

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 opcję, nie będziesz pytany ponownie o hasło podczas tej sesji.

24. Aktualizacje

Nowe złośliwe oprogramowanie jest znajduwane 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 aktualizacji zostanie przeprowadzony automatycznie, w zależności od **Ustawień automatycznej aktualizacji**.

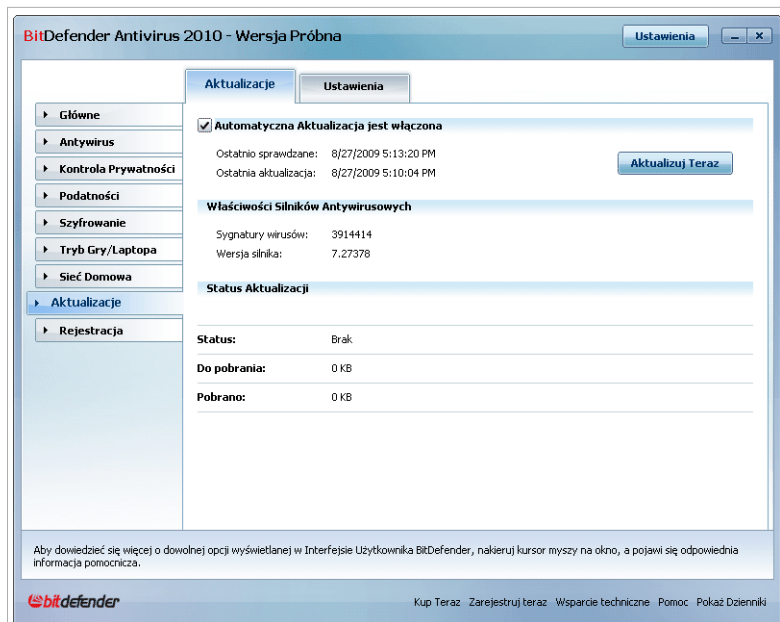
Proces aktualizacji wykonywany jest w tle co znaczy że pliki są kolejno aktualizowane. Dzięki temu proces aktualizacji nie wpływa na działanie produktu i jednocześnie eliminuje wszelkie podatności.

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**.
- **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**.

24.1. Automatyczna Aktualizacja

Aby zobaczyć informacje dotyczące aktualizacji i dokonać automatycznej aktualizacji, kliknij **Aktualizacja> Aktualizacja** w Trybie Eksperta.



Automatyczna Aktualizacja

Tu możesz zobaczyć kiedy ostatnio szukano nowej aktualizacji i kiedy została ona dokonana ostatnio (czy dokonano jej poprawnie czy wystąpiły błędy). Wyświetlane są również wersja silnika i ilość sygnatur.

Jeśli otworzysz tę sekcję podczas aktualizacji, zobaczysz stan pobierania.



WAŻNE

Aby być chronionym przed najnowszymi zagrożeniami miej włączony moduł **Automatycznej Aktualizacji**.

Możesz pobrać nowe sygnatury dla BitDefendera klikając **Pokaż Listę Wirusów**. Stworzony zostanie plik w formacie HTML, który będzie zawierał wszystkie dostępne sygnatury i zostanie otwarty w przeglądarce internetowej. Możesz przeszukać bazę danych aby znaleźć sygnaturę konkretnego zagrożenia lub kliknąć **BitDefender Lista Wirusów** aby przejść do internetowej bazy danych sygnatur BitDefendera.

24.1.1. Prośba o Aktualizację

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**.

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 aktualizację. Zalecamy to zrobić jak najszybciej.



Notatka

Jeśli łączysz się z Internetem za pomocą modemu, zalecane jest regularne aktualizowanie BitDefendera na żądanie.

24.1.2. Wyłączanie Automatycznej Aktualizacji

Jeśli chcesz wyłączyć automatyczną aktualizację, pojawi się następne okno ostrzegające. Musisz potwierdzić swój wybór wybierając z menu jak długo ma być wyłączona automatyczna aktualizacja. Możesz wyłączyć automatyczną aktualizację na 5, 15 lub 30 minut, godzinę, całkowicie albo aż do restartu systemu.



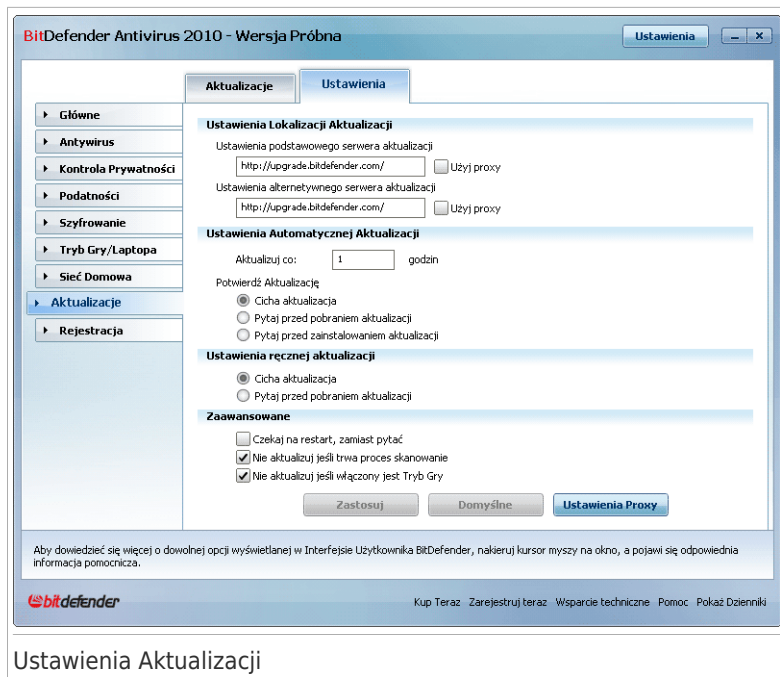
Ostrzeżenie

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

24.2. Ustawienia Aktualizacji

Aktualizacje mogą być przeprowadzone z lokalnej sieci, bezpośrednio przez Internet albo przez serwer proxy. Domyślnie, BitDefender sprawdzi co godzinę czy są aktualizacje w Internecie, i zainstaluj je bez powiadamiania cię.

Aby skonfigurować ustawienia aktualizacji i zarządzać proxy, kliknij **Aktualizacja>Ustawienia** w Trybie Eksperta.



Ustawienia Aktualizacji

Ustawienia aktualizacji są podzielone na 4 kategorie (**Ustawienia Lokalizacji Aktualizacji**, **Ustawienia Automatycznej Aktualizacji**, **Ustawienia Ręcznej Aktualizacji** i **Zaawansowane**). Każda kategoria zostanie opisana oddzielnie.

24.2.1. 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. Aby uzyskać więcej informacji przejdź do „**Zarządzanie Proxy**” (p. 191)

24.2.2. 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 aktualizację.
- **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.

24.2.3. 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.

24.2.4. 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 aktualizuj jeśli trwa skanowanie** - BitDefender nie przeprowadza aktualizacji, gdy trwa proces przeszukiwania. Dzięki temu proces aktualizacji programu BitDefender nie zakłóci przeszukiwania.



Notatka

Jeżeli program BitDefender będzie aktualizowany w trakcie procesu przeszukiwania, przeszukiwanie zostanie przerwane.

- **Nie aktualizuj jeśli włączony jest Tryb Gry** - BitDefender nie zaktualizuje się jeśli Tryb Gry będzie włączony. W ten sposób możesz zminimalizować wpływ produktu na wydajność systemu w trakcie gry.

24.2.5. Zarządzanie Proxy

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.



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**. Pojawi się nowe okno.

BitDefender Ustawienia Proxy

Proxy wykryte w czasie instalacji

Adres: Port: Nazwa użytkownika:
Hasło:

Domyślny Proxy Przeglądarki

Adres: Port: Nazwa użytkownika:
Hasło:

Własne Proxy

Adres: Port: Nazwa użytkownika:
Hasło:

Tutaj możesz zmienić ustawienia proxy wykryte podczas instalacji.

OK Anuluj

Zarządzanie Proxy

Dostępne są trzy zestawy ustawień proxy:

- **Ustawienia proxy (wykryte w czasie instalacji)** - ustawienia proxy wykryte na koncie administratora w czasie instalacji, mogą być skonfigurowane tylko jeśli jesteś zalogowany na to konto. Jeśli serwer proxy wymaga nazwy użytkownika i hasła, musisz podać je 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.

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.

25. Rejestracja

Aby znaleźć kompletne informacje dotyczące BitDefendera i statusu rejestracji, kliknij **Rejestracja** w Trybie Eksperta.

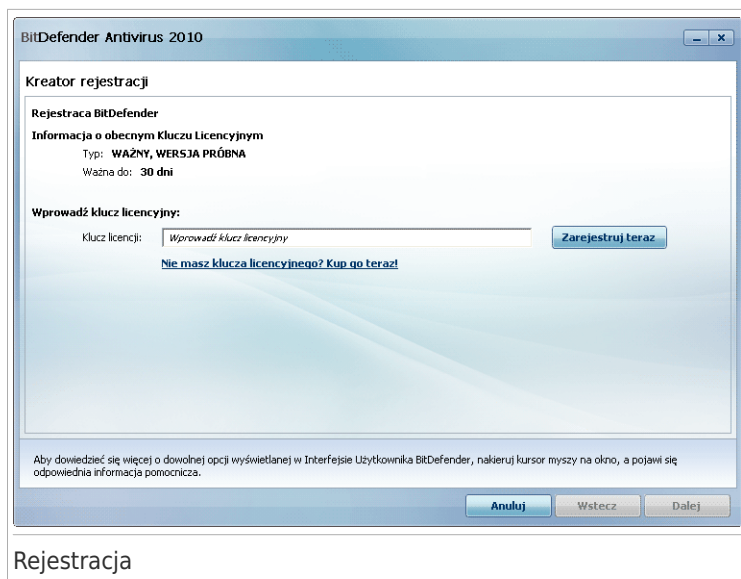


Ta sekcja wyświetla:

- **Informacje o Produkcie:** produkt BitDefendera i wersja.
- **Informacje o Rejestracji:** adres email użyty do logowania na twoim koncie BitDefender (jeśli skonfigurowane), aktualny klucz licencyjny oraz ilość dni do jego wygaśnięcia.

25.1. Rejestrowanie BitDefender Antivirus 2010

Kliknij **Zarejestruj teraz** aby otworzyć okno rejestracji produktu.



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

Aby zarejestrować BitDefender Antivirus 2010:

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 **Zakończ**.

25.2. Tworzenie Konta BitDefender

Jako część procesu rejestracji MUSISZ utworzyć Konto BitDefendera. Konto BitDefender daje tobie dostęp do darmowej pomocy technicznej oraz specjalnych ofert i promocji. Jeśli zgubisz klucz licencyjny BitDefendera, możesz się zalogować na swoje konto na <http://myaccount.bitdefender.com> aby go odzyskać.



WAŻNE

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.

Jeśli jeszcze nie posiadasz konta BitDefender, kliknij **Aktywuj Produkt** aby otworzyć okno rejestracji konta.

Jeśli nie chcesz zakładać konta BitDefender w tym momencie, wybierz **Zarejestruj Później** i kliknij **Zakończ**. W przeciwnym razie postępuj w zależności od sytuacji:

- „Nie mam osobistego konta na MyBitDefender” (p. 195)
- „Już posiadam konto BitDefender” (p. 196)

Nie mam osobistego konta na MyBitDefender

Aby pomyślnie utworzyć konto BitDefender, podążaj według tych kroków:

1. Wybierz **Stwórz nowe konto**.
2. Wprowadź wymaganą informację w odpowiednich polach. Dane które teraz wprowadzisz pozostaną tajne.
 - **Adres email** - wpisz swój adres email.

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



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. Wybierz jedną z dostępnych w menu opcji:
 - **Wysyłaj mi wszystkie wiadomości**
 - **Wysyłaj mi tylko informacje o produktach**
 - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Utwórz**.
5. Kliknij **Zakończ** aby zakończyć kreator.
6. **Przeprowadź aktywację swojego konta.** 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 **Zakończ** aby zakończyć kreator.

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

1. Wybierz **Zaloguj się (poprzednio stworzone 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.

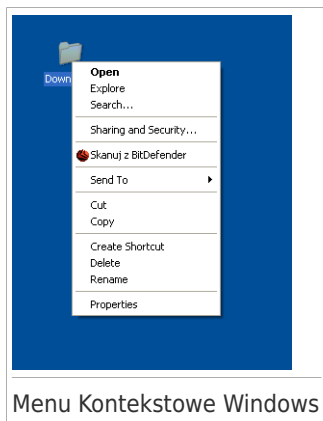
3. Opcjonalnie, BitDefender może informować ciebie o specjalnych ofertach oraz promocjach korzystając z adresu email twojego konta. Wybierz jedną z dostępnych w menu opcji:
 - **Wysyłaj mi wszystkie wiadomości**
 - **Wysyłaj mi tylko informacje o produktach**
 - **Nie wysyłaj mi żadnych wiadomości**
4. Kliknij **Zaloguj się**.

5. Kliknij **Zakończ** aby zakończyć kreator.

Integracja z Windows i Oprogramowaniem Third-Party

26. Integracja z Menu Kontekstowym Windows

Menu kontekstowe Windows pojawia się kiedy klikniesz prawym przyciskiem myszy na pliku lub folderze znajdującym się w twoim komputerze.



Menu Kontekstowe Windows

BitDefender integruje się z menu kontekstowym Windows, aby umożliwić użytkownikowi łatwiejsze skanowanie w poszukiwaniu wirusów. Możesz szybko zlokalizować opcję skanowania w menu kontekstowym szukając ikony BitDefender.

26.1. Skanowanie z BitDefender

Za pomocą menu kontekstowego Windows możesz łatwo skanować pliki, foldery a nawet całe dyski twarde. Kliknij prawym przyciskiem na obiekt który chcesz skanować i w menu wybierz **Skanowanie z BitDefender**. 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.

Jeżeli chcesz zmienić opcje skanowania, wykonaj następujące kroki:

1. Otwórz BitDefender i przestaw interfejs użytkownika na Tryb Eksperta.
2. Kliknij **Antyvirus** w menu po lewej stronie.
3. Kliknij zakładkę **Skanowanie**.
4. Kliknij prawym przyciskiem na **Skanowanie kontekstowe** i wybierz **Otwórz**. Pojawi się okno.

5. Kliknij na **Własne** i skonfiguruj opcje skanowania według własnych potrzeb. Aby dowiedzieć się za co odpowiada dana opcja, przytrzymaj nad nią kursor myszy i przeczytaj informację która pojawi się na dole okna.
6. Kliknij **Zastosuj** aby zapisać zmiany.
7. Kliknij **OK** aby zatwierdzić zmiany w opcjach skanowania.



WAŻNE

Nie powinno się zmieniać tych opcji skanowania, jeśli nie ma się ku temu ważnego powodu.

27. Integracja z Przeglądarką Internetową

BitDefender chroni cię przed phishingiem gdy surfujesz po Internecie. Skanuje otwarte strony Internetowe i zawiadamia o zagrożeniach phishingiem. Biała Lista stron sieciowych które nie będą skanowane przez BitDefender może zostać skonfigurowana.

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

- Internet Explorer
- Mozilla Firefox

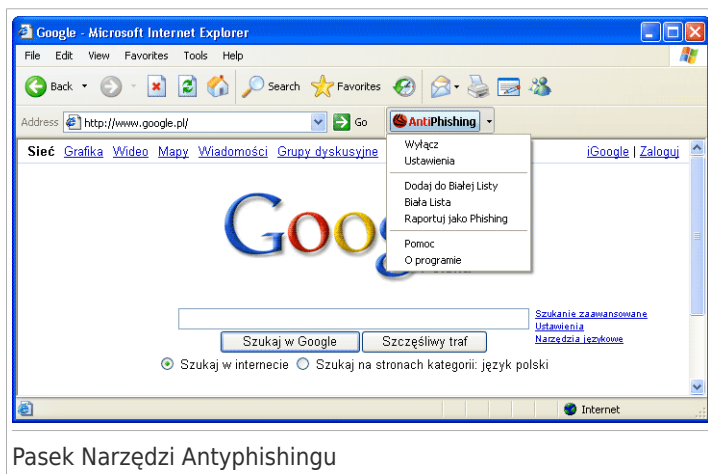
Możesz łatwo i wydajnie zarządzać ochroną antyphishingową oraz Białą Listą używając paska zadań BitDefender Antypishing zintegrowanego z jedną z powyższych przeglądarek.

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**.



Pasek Narzędzi Antyphishingu

Następujące opcje są dostępne w menu paska zadań:

- **Włącz / Wyłącz** - włącza lub wyłącza zabezpieczenie antyphishingowe dla wybranej przeglądarki.

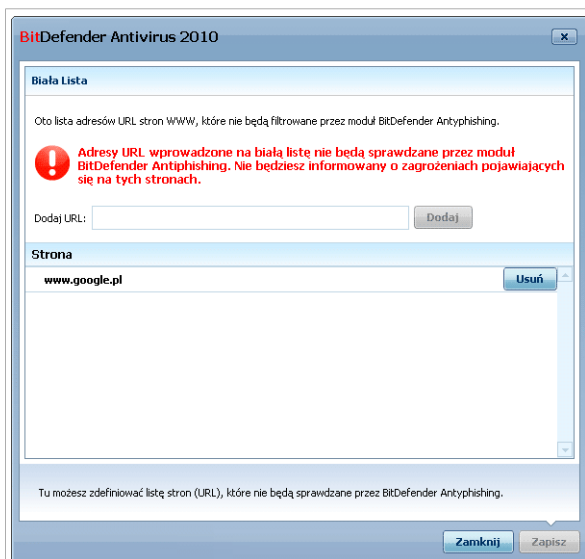
- **Ustawienia** - otwiera okno, w którym możesz wybrać ustawienia paska narzędzi antyphishingu. Dostępne są następujące opcje:
 - ▶ **Ochrona Antyphishingowa WWW w czasie rzeczywistym** - wykrywa i informuje cię, gdy strona www chce wykraść twoje prywatne dane. Ta opcja kontroluje zabezpieczenie antyphishingowe 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.



Notatka

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.



Biała Lista Antyphishingu

Możesz zobaczyć listę wszystkich stron internetowych, które nie są sprawdzone przez silniki antyphishingowe BitDefendera. Jeśli chcesz usunąć stronę z Białej Listy by zostać powiadomionym o istniejącym zagrożeniu phishingiem, kliknij **Usuń** obok danej strony.

Możesz dodać strony, którym w pełni ufasz do Białej Listy, żeby nie były skanowane przez silniki antyphishingowe. By dodać witrynę do Białej Listy, podaj jej adres w odpowiednim polu i kliknij **Dodaj**.

- **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.

28. Integracja z programami Instant Messenger

BitDefender oferuje możliwość szyfrowania aby chronić twoje poufne dokumenty oraz rozmowy prowadzone przez komunikatory Yahoo Messenger i MSN Messenger.

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

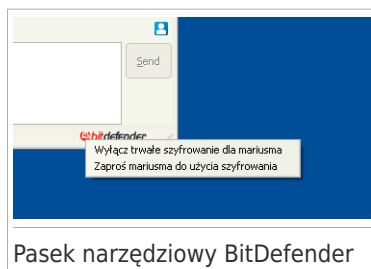
BitDefender nie będzie szyfrował rozmowy, jeśli rozmówca korzysta z komunikatora bazującego na stronie www, takiego jak Meebo, lub innej aplikacji do rozmów która obsługuje Yahoo Messenger lub MSN.

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 logo BitDefender aby go odnaleźć.



Notatka

Pasek narzędzi pokazuje że rozmowa jest szyfrowana wyświetlając mały klucz  obok logo 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.

Jak to zrobić

29. Jak skanować Pliki i Foldery

Skanowanie z BitDefender jest łatwe i elastyczne. Są 4 osoby na ustawienie BitDefendera aby skanował pliki i foldery w poszukiwaniu wirusów i innego złośliwego oprogramowania:

- Korzystanie z Menu Kontekstowego Windows
- Korzystanie z Zadań Skanowania
- Korzystanie z ręcznego skanowania
- Korzystanie z Paska aktywności skanera

Jak tylko uruchomisz skanowanie, pojawi się kreator skanowania antywirusowego i przeprowadzi cię przez cały proces. Aby uzyskać więcej informacji, odwołaj się do „*Kreator Skanowania Antywirusowego*” (p. 53).

29.1. 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.

29.2. Korzystanie z Zadań Skanowania

Jeśli chcesz skanować swój komputer albo specyficzne foldery regularnie, możesz rozważyć korzystanie z zadań skanowania. Zadania skanowania instruuja 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 Trybie Początkującym

W Trybie Początkującym, możesz uruchomić tylko standardowe skanowanie całego komputera klikając na **Skanuj Teraz**. Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

Uruchamianie Zadań Skanowania w Trybie Średniozaawansowanym

W Trybie Średniozaawansowanym, możesz uruchomić kilka gotowych skonfigurowanych zadań. Możesz także skonfigurować i uruchomić własne zadanie skanowania dla wybranych lokalizacji na twoim komputerze korzystając z opcji skanowania. Podążaj tymi krokami aby uruchomić zadanie skanowania w Trybie Średniozaawansowanym:

1. Kliknij zakładkę **Antywirus**.
2. Po lewej stronie obszaru Szybkie Zadania, kliknij **Skanowanie Systemowe** aby uruchomić standardowe skanowanie całego komputera. Aby uruchomić inne zadanie skanowanie, kliknij strzałkę  na przycisku i wybierz zadanie skanowania. Aby skonfigurować i uruchomić własne skanowanie, kliknij **Własne Skanowanie**. Te zadania skanowania są dostępne:

Zadanie Skanowania	Opis
Skanowanie Systemu	Skanuje cały system wyłączając archiwa. W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów .
Głębokie Skanowanie	Skanuje cały system. W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.
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.
Skanowanie Użytkownika	Ta opcja pomaga ci skonfigurować i uruchomić własne zadanie skanowania, pozwalając na określenie co ma zostać przeskanowane oraz ustawienie ogólnych opcji skanowania. Możesz zachować własne zadania skanowania w celu późniejszego użycia z Trybu Średniozaawansowanego lub Eksperta.

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 Trybie Eksperta

W Trybie Eksperta, możesz uruchamiać wszystkie skonfigurowane wcześniej zadania, a także zmieniać ich ustawienia. Dodatkowo możesz tworzyć własne zadania, jeśli chcesz skanować określone lokalizacje na swoim komputerze. Podążaj tymi krokami aby uruchomić zadanie skanowania w Trybie Eksperta:

1. Kliknij **Antyvirus** w menu po lewej stronie.
2. Kliknij zakładkę **Skanowanie**. Tutaj możesz znaleźć kilka podstawowych zadań skanowania i możesz tworzyć własne. To są domyślne ustawienia zadań skanowania które chcesz użyć:

Zadania Domyślne	Opis
Głębokie Skanowanie	Skanuje cały system. W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.
Skanowanie Systemu	Skanuje cały system wyłączając archiwa. W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów .
Szybkie Skanowanie Systemu	Skanuje katalogi Windows i Program Files. W konfiguracji domyślnej, skanuje pod kątem wszystkich zagrożeń, z wyjątkiem rootkitów, lecz nie skanuje pamięci, rejestru ani plików ciasteczek.
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.

3. Kliknij dwukrotnie na zadaniu skanowania aby je uruchomić.
4. Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

29.3. Korzystanie z Ręcznego Skanowania BitDefenderem

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 twój system jest zainfekowany przez odpornego wirusa, możesz spróbować usunąć go uruchamiając Windows w Trybie Awaryjnym i skanować każdy z dysków twardych za pomocą opcji Ręcznego Skanowania w BitDefenderze.

Aby przeskanować twój komputer używając Skanowania Ręcznego, podążaj tymi krokami:

1. W  menu Start Windows, przejdź do **Start → Programy → BitDefender 2010 → BitDefender Skanowanie Ręczne**. Pojawi się nowe okno.
2. Kliknij **Dodaj Folder** aby wybrać cel skanowania. Pojawi się nowe okno.
3. Wybierz cel skanowania:
 - Aby przeskanować pulpit, wybierz **Pulpit**.
 - Aby przeskanować całą partycję dysku twardego, wybierz ją z **Mój Komputer**.
 - Aby przeskanować konkretny folder, przeglądaj i wybierz go z listy.
4. Kliknij **OK**.
5. Kliknij **Kontynuuj** aby rozpocząć skanowanie.
6. Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.

Co to jest Tryb Awaryjny?

Tryb awaryjny to opcja przeznaczona do rozwiązywania problemów z systemem Windows, które mają niekorzystny wpływ na jego normalną pracę. Dzięki temu możliwe jest rozwiązywanie wielu problemów, od konfliktów sterowników, po usuwanie wirusów uniemożliwiających uruchomienie systemu w trybie podstawowym. W Trybie Awaryjnym, Windows uruchamia się tylko z ograniczonym zestawem funkcji i sterowników. Tylko kilka aplikacji może pracować w tym trybie. To dlatego, większość wirusów nie jest wtedy aktywna i może zostać łatwo usunięta.

Aby uruchomić Windows w Trybie Awaryjnym, uruchom ponownie komputer i naciśnij F8 przed załadowaniem systemu. Pojawi się menu wyboru trybu uruchomienia systemu. Możesz wybrać jedną z kilku opcji uruchomienia Windows w Trybie awaryjnym. Jeśli chcesz korzystać z Internetu, powinieneś wybrać opcję **Tryb Awaryjny z obsługą sieci**.



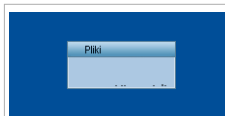
Notatka

Aby uzyskać więcej informacji na temat Trybu Awaryjnego, przejdź do Centrum Pomocy Systemu Windows (w menu Start, kliknij **Centrum Pomocy**). Ta nazwa może się różnić w zależności od wersji systemu Windows. Możesz także uzyskać więcej informacji przeszukując Internet.

29.4. Używanie Paska Aktywności Skanera

Okienko czynności skanowania jest graficznym odzwierciedleniem wykonywanych czynności skanowania na twoim systemie. To małe okienko jest domyślnie dostępne tylko w **Trybie Eksperta**.

Możesz użyć Paska aktywności skanowania aby szybko skanować pliki lub foldery. Przenieś i upuść do paska aktywności skanera plik lub folder który



Pasek Aktywności Skanera

chcesz przeskanować. Podążaj za kreatorem skanowania antywirusowego aby przeprowadzić skanowanie.



Notatka

Aby uzyskać więcej informacji, odwołaj się do „*Pasek Aktywności Skanera*” (p. 30).

30. Jak Harmonogramować 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 i przestaw interfejs użytkownika na Tryb Eksperta.
2. 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:

Zadania Domyślne	Opis
Głębokie Skanowanie	Skanuje cały system. W domyślnej konfiguracji skanuje pod kątem wszystkich zagrożeń takich jak wirusy, spyware, adware, rootkity i inne.
Skanowanie Systemu	Skanuje cały system wyłączając archiwa. W domyślnej konfiguracji, skanuje w poszukiwaniu wszystkich typów złośliwego oprogramowania oprócz rootkitów .
Szybkie Skanowanie Systemu	Skanuje katalogi Windows i Program Files. W konfiguracji domyślnej, skanuje pod kątem wszystkich zagrożeń, z wyjątkiem rootkitów, lecz nie skanuje pamięci, rejestru ani plików ciasteczek.
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.
Moje Dokumenty	Użyj tego zadania do skanowania ważnych folderów aktualnego użytkownika: Moje Dokumenty, Pulpit oraz Autostart. To zapewni

Zadania Domyślne	Opis
	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.

Rozwiązywanie Problemów i Uzyskiwanie Pomocy

31. Rozwiązywanie Problemów

Ten rozdział przedstawia problemy, z którymi możesz się spotkać podczas korzystania z BitDefender oraz ich możliwe rozwiązania. Większość z tych problemów może być rozwiązana poprzez właściwą konfigurację ustawień produktu.

Jeśli nie możesz znaleźć swojego problemu tutaj, lub prezentowane rozwiązanie nie pomogło ci go rozwiązać, możesz skontaktować się ze wsparciem technicznym BitDefender, tak jak przedstawiono to w rozdziale „*Otrzymywanie pomocy*” (p. 219).

31.1. 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.

31.1.1. 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 BitDefendera. 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 „<i>Wymagania Systemowe</i>” (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.

31.1.2. Instalacja Nieudana

Może być kilka przyczyn tego niepowodzenia:

- Podczas instalacji pojawia się ekran błędu. Instalator może zapytać o przerwanie instalacji albo wyświetlić przycisk do narzędzia odinstalowującego które oczyści system z poprzednich instalacji.



Notatka

Zaraz po włączeniu instalacji, instalator może poinformować o niewystarczającej ilości wolnego miejsca na dysku. 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 ekran błędu zawiera przycisk do narzędzia odinstalowującego, kliknij na ten przycisk aby oczyścić system. W innym przypadku, postępuj kolejno:

- a. Przejdź do www.bitdefender.com/uninstall i pobierz specjalne narzędzie do odinstalowywania BitDefendera.
 - b. Korzystając z praw administratora, uruchom narzędzie do odinstalowywania BitDefendera.
 - c. Uruchom ponownie komputer.
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. 222).
 - 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. 219).

31.2. 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. Poczekać kilka chwil i sprawdzić 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. 219).

31.3. 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.

Jeśli procedura usuwania zawiedzie wyświetlając ekran błędu, kliknij na przycisk aby uruchomić narzędzie odinstalowujące i wyczyść system. W innym przypadku, postępuj kolejno:

1. Przejdź do www.bitdefender.com/uninstall i pobierz specjalne narzędzie do odinstalowywania BitDefendera.
2. Korzystając z praw administratora, uruchom narzędzie do odinstalowywania BitDefendera. Narzędzie Odinstalowujące usunie wszystkie pliki i klucze rejestru, które nie zostały usunięte podczas procesu usuwania.
3. Uruchom ponownie komputer.

Jeśli ta informacja nie okazała się pomocna, możesz skontaktować się ze wsparciem BitDefender tak jak to opisano w sekcji „*Otrzymywanie pomocy*” (p. 219).

32. Otrzymywanie pomocy

Jako ceniony dostawca oprogramowania, BitDefender stara się udostępniać swoim klientom wysoki poziom usług i wsparcia technicznego. Baza Wiedzy BitDefender dostarcza wielu artykułów na temat rozwiązań dotyczących większości problemów i pytań z jakimi spotyka się klient korzystając z naszego oprogramowania. Jeśli nie znajdziesz rozwiązania w Bazie Wiedzy, możesz skontaktować się z Centrum Pomocy BitDefender. Nasi przedstawiciele odpowiedzą na wszystkie twoje pytania i szybko pomogą ci znaleźć optymalne rozwiązanie.

32.1. 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>.

32.2. Pytanie o Pomoc

Jeśli chcesz poprosić o pomoc, musisz skorzystać z usługi BitDefender Web Self-Service. Wykonaj następujące czynności:

1. Odwiedź <http://www.bitdefender.com/help>. Tutaj możesz znaleźć Bazę Wiedzy BitDefender. 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. Proszę przeczytać pokrewny artykuł i skorzystać z zaproponowanego rozwiązania.
4. Jeśli to rozwiązanie nie rozwiązuje wszystkich twoich problemów, korzystaj z linku w artykule, aby skontaktować się z Centrum Pomocy BitDefender.
5. Zaloguj się do konta BitDefender.
6. Skontaktuj się z przedstawicielem BitDefender za pomocą e-mail, czatu lub telefonu.

32.3. 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 jakiegokolwiek problemy czy pytania, nie wahaj się skontaktować z nami.

32.3.1. Adresy Internetowe

Dział sprzedaży: sales@bitdefender.com
Wsparcie techniczne: 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 Spam: spam_submission@bitdefender.com
Raportowanie Abuse: abuse@bitdefender.com
Strona internetowa produktu: <http://www.bitdefender.com>
Zasoby ftp: <ftp://ftp.bitdefender.com/pub>
Lokalni dystrybutorzy: <http://www.bitdefender.com/site/Partnership/list/>
Baza wiedzy BitDefender: <http://kb.bitdefender.com>

32.3.2. Biura BitDefender

Biurum 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.

U.S.A

BitDefender, LLC

6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
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 SLU

C/ Balmes, 191, 2º, 1ª, 08006

Barcelona

Fax: +34 932179128

Telefon: +34 902190765

Sprzedaż: comercial@bitdefender.es

Pomoc Techniczna: www.bitdefender.es/ayuda

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

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://kb.bitdefender.ro>

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

CD Ratunkowy BitDefender

33. Przegląd

BitDefender Antivirus 2010 jest dostarczany z bootowalnym CD (Dysk Ratunkowy BitDefender) zdolnym do skanowania i usuwania wirusów z wszystkich istniejących dysków twardych zanim system operacyjny zostanie uruchomiony.

Powinieneś użyć CD ratunkowego BitDefender za każdym razem gdy twój system przestanie pracować poprawnie z powodu infekcji wirusami. Zazwyczaj występuje to gdy nie jest używany program antywirusowy.

Aktualizacja sygnatur wirusów jest wykonywana automatycznie, bez interwencji użytkownika za każdym uruchomieniem CD ratunkowego BitDefender.

Dysk Ratunkowy BitDefendera jest przerobioną przez BitDefender dystrybucją Knoppix, która integruje najnowsze rozwiązanie bezpieczeństwa BitDefender dla Linux w GNU/Linux Knoppix Live CD, oferując antywirusa który może skanować i usuwać wirusy z dysków twardych (nawet partycje Windows NTFS). Jednocześnie Dysk Ratunkowy BitDefendera może być użyty do odzyskania ważnych danych kiedy nie możesz uruchomić swojego systemu Windows.



Notatka

Dysk Ratunkowy BitDefendera może zostać pobrany z:
http://download.bitdefender.com/rescue_cd/

33.1. Wymagania Systemowe

Przed uruchomieniem Dysku Ratunkowego BitDefendera, sprawdź czy twój system spełnia poniższe wymagania.

Procesor typu

Kompatybilny z x86, minimum 166 MHz, ale nie oczekuj wysokie wydajności w tym przypadku. Procesor generacji i686 z 800MHz zalecany.

Pamięć

Minimum 512 MB pamięci RAM (zalecane 1 GB)

CD-ROM

Dysk Ratunkowy BitDefendera uruchamiany jest z CD-ROM-u, zatem CD-ROM i BIOS zdolny do bootowania z niego jest wymagany.

Połączenie z Internetem

Mimo że Dysk Ratunkowy BitDefendera uruchomi się bez połączenia z Internetem, procedury aktualizacji wymagają aktywnego linka HTTP, nawet przez serwer proxy. Ponadto dla zaktualizowanej ochrony połączenie z Internetem jest WYMAGANE.

Rozdzielczość ekranu

Standardowa karta graficzna kompatybilna z SVGA.

33.2. Dołączone Oprogramowanie

Ratunkowy CD BitDefender zawiera następujące pakiety oprogramowania.

Xedit

To jest edytor tekstu.

Vim

To jest rozbudowany edytor tekstu, zawierający wyróżnienie składni, GUI i wiele więcej. Po więcej informacji, wejdź na stronę [Strona domowa Vim](#).

Xcalc

To jest kalkulator.

RoxFiler

RoxFiler jest narzędziem do zarządzania plikami graficznymi.

Po więcej informacji, wejdź na stronę [Strona domowa RoxFiler](#).

MidnightCommander

GNU Midnight Commander (mc) to menadżer plików tryb tekstowego.

Po więcej informacji wejdź na stronę [Strona domowa MC](#).

Pstree

Pstree pokazuje aktywne procesy.

Top

Top pokazuje zadania w Linux

Xkill

Xkill zabija klienta przy X zasobach.

Partition Image

Obraz partycji pomaga zapisać partycje w formatach plików EXT2, Reiserfs, NTFS, HPFS, FAT16 i Fat 32 w obraz pliku. Ten program jest dobry na potrzeby kopii zapasowych.

Po więcej informacji wejdź na stronę [Strona domowa Partimage](#).

GtkRecover

GtkRecover to wersja dla GTK konsoli programu odzyskiwania. Pomaga odzyskać pliki.

Po więcej informacji wejdź na stronę [Strona domowa GtkRecover](#).

ChkRootKit

ChkRootKit to narzędzie, które pomaga w poszukiwaniu rootkitów.

Po więcej informacji wejdź na stronę [Strona domowa ChkRootKit](#).

Nessus Network Scanner

Nessus jest zdalnym skanerem zabezpieczeń dla Linux, Solaris, FreeBSD i Mac OS X.

Po więcej informacji wejdź na stronę [Strona domowa Nessus](#).

Iptraf

Iptraf to Sieciowy Program Monitorowania IP.

Po więcej informacji wejdź na stronę [Strona domowa Iptraf](#).

Iftop

Iftop pokazuje szerokopasmowe wykorzystanie interfejsu.

Po więcej informacji wejdź na [Strona domowa Iftop](#).

MTR

MTR to sieciowe narzędzie diagnostyczne.

Po więcej informacji wejdź na [Strona domowa MTR](#).

PPPStatus

PPPStatus pokazuje statystyki przychodzących i wychodzących ruchu TCP/IP.

Po więcej informacji wejdź na [Strona domowa PPPStatus](#).

Wavemon

Wavemon to aplikacja monitorująca dla bezprzewodowych urządzeń sieciowych.

Po więcej informacji wejdź na [Strona domowa Wavemon](#).

USBView

USBView pokazuje informacje o urządzeniach połączonych przez USB.

Po więcej informacji wejdź na [Strona domowa USBView](#).

Pppconfig

PPPconfig pomaga w automatycznym ustawianiu połączenia dial up przez ppp.

DSL/PPPoE

DSL/PPPoE konfiguruje połączenie PPPoE (ADSL).

I810rotate

I810rotate przełącza sprzętową wydajność wideo i810 używając i810switch(1).

Po więcej informacji wejdź na stronę [Strona domowa I810rotate](#).

Mutt

Mutt to potężny tekstowy klient pocztowy MIME.

Po więcej informacji wejdź na stronę [Strona domowa Mutt](#).

Mozilla Firefox

Mozilla Firefox to dobrze znana przeglądarka internetowa.

Po więcej informacji wejdź na stronę [Strona domowa Mozilla Firefox](#).

Elinks

Elinks to przeglądarka internetowa w trybie tekstowym.

Po więcej informacji wejdź na stronę [Strona domowa Elinks](#).

34. Dysk Ratunkowy BitDefender

Ten rozdział zawiera informacje o tym jak uruchomić i zatrzymać Dysk Ratunkowy BitDefender, przeskanować komputer w poszukiwaniu szkodliwego oprogramowania i zapisać dane ze swojego komputera na przenośny dysk. Jednakże używając oprogramowania dołączonego do CD możesz wykonać wiele czynności, które wykraczają poza ten podręcznik użytkownika.

34.1. Uruchom Dysk Ratunkowy BitDefender

Aby uruchomić CD ustaw w BIOS twojego komputera bootowanie z CD, włóż CD do napędu i uruchom zrestartuj. Upewnij się że twój komputer ma możliwość bootowania z CD.

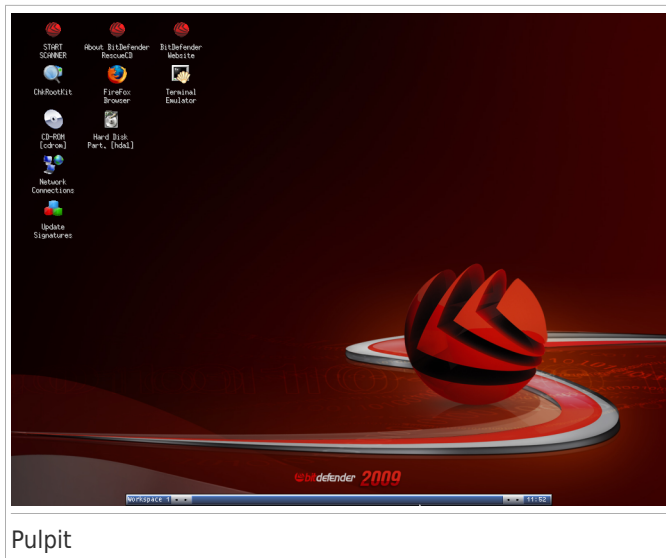
Poczekaj aż na ekranie pojawią się instrukcje i postępuj według nich aby uruchomić Dysk Ratunkowy BitDefendera.



Ekran Bootowania

Podczas bootowania aktualizacja sygnatur wirusów jest wykonywana automatycznie. To może zająć chwilę.

Gdy zakończy się proces bootowania zobaczysz pulpit. Możesz teraz używać Dysku Ratunkowego BitDefendera.



34.2. Zatrzymaj Dysk Ratunkowy BitDefender

Możesz bezpiecznie wyłączyć komputer klikając **Wyjdź** z menu kontekstowego Dysku Ratunkowego BitDefendnera (kliknij prawym klawiszem myszy aby je otworzyć) lub wpisując komendę **halt** w terminalu.



Wybierz "EXIT"

Gdy Dysk ratunkowy BitDefendera poprawnie zamknie wszystkie programy wyświetli na ekranie komunikaty taki jak na poniższym rysunku. Możesz wyciągnąć CD aby uruchomić system z twardego dysku. Teraz możesz wyłączyć komputer lub go zrestartować.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufs) (aufs) (aufs) (aufs)
(ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
(s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend)
(aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufs) (aufs) (aufs) (aufs)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
(A) (khsbpbkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Poczekaj na ten komunikat gdy wyłączasz

34.3. Jak przeprowadzić skanowanie antywirusowe?

Gdy proces ponownego uruchamiania się zakończy otworzy się kreator, który pozwoli na pełny skan twojego komputera. Wystarczy kliknąć **Start**.



Notatka

Jeśli rozdzielczość twojego ekranu nie jest wystarczająco wysoka zostaniesz poproszony o rozpoczęcie skanowania w trybie tekstowym.

Wykonaj następujące trzy kroki procedury aby zakończyć skanowanie komputera.

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



Notatka

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

2. Możesz zobaczyć ilość zdarzeń zagrażających twojemu systemowi.

Zagadnienia są wyświetlane w grupach. Kliknij okienko "+" aby otworzyć grupę lub "-" aby zamknąć grupę.

Możesz wybrać ogólne działanie dla wszystkich grup zagadnień lub wybrać osobne działanie dla każdego zagadnienia.

3. Możesz zobaczyć podsumowanie wyników.

Jeśli chcesz skanować tylko wybrany katalog, możesz skorzystać z kilku możliwości:

- Skorzystaj ze **Skanera BitDefender dla Uniksów**.

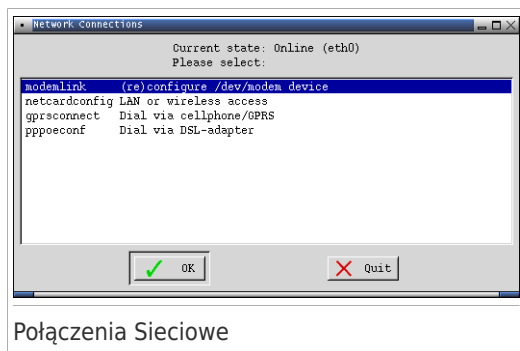
1. Kliknij dwukrotnie na ikonę **URUCHOM SKANER** na Pulpicie. Uruchomisz **Skaner BitDefender dla Unixów**.
 2. Kliknij na **Skaner**, a pojawi się nowe okno.
 3. Wybierz katalog który chcesz skanować i kliknij **Otwórz** aby zacząć skanować korzystając z tego samego kreatora, który pojawił się przy pierwszym uruchomieniu.
- Korzystaj z menu kontekstowego - przeglądaj foldery, kliknij prawym przyciskiem na plik lub katalog i wybierz **Wyślij do**. Następnie wybierz **Skaner BitDefender**.
 - Albo możesz wydać komendę jako root, z terminala. **BitDefender Antivirus Scanner** wystartuje skanując wybrany plik albo folder.

```
# bdscan /path/to/scan/
```

34.4. Jak mam skonfigurować połączenie z Internetem ?

Jeśli jesteś podłączony do sieci z serwerem DHCP to połączenie z Internetem powinno być automatycznie wykryte i skonfigurowane. Aby ręcznie skonfigurować należy wykonać następujące kroki.

1. Kliknij dwa razy skrót na pulpicie Połączenia Sieciowe. Pojawi się następujące okno:



2. Wybierz typ sieci z której korzystasz i kliknij OK.

Połączenia	Opis
Modem	Wybierz ten typ połączenia jeśli korzystasz z modemu i linii telefonicznej aby podłączyć się do Internetu.

Połączenia	Opis
LAN	Wybierz ten typ połączenia jeśli korzystasz z sieci lokalnej (LAN) aby podłączyć się do Internetu. Dotyczy to również sieci bezprzewodowych.
GPRS	Wybierz ten typ połączenia jeśli korzystasz z telefonu komórkowego korzystającego z protokołu GPRS (General Packet Radio Service) aby podłączyć się do Internetu. Oczywiście możesz również używać modemu GPRS zamiast telefonu komórkowego.
DSL	Wybierz ten typ połączenia jeśli korzystasz z modemu DSL (Digital Subscriber Line) aby podłączyć się do Internetu

- Postępuj według instrukcji na ekranie. Jeśli nie jesteś pewien co wpisać, skontaktuj się z administratorem sieci.



WAŻNE

Proszę pamiętać że modem włączasz tylko wybierając powyżej wymienione opcje. Aby skonfigurować sieć proszę wykonać następujące kroki:

- Kliknij prawym klawiszem na pulpit. Pojawi się menu kontekstowe Dysku Ratunkowego BitDefendera.
- Wybierz **Terminal (jako root)**.
- Wpisz następujące komendy:

```
# pppconfig
```

- Postępuj według instrukcji na ekranie. Jeśli nie jesteś pewien co wpisać, skontaktuj się z administratorem sieci.

34.5. Jak mam zaktualizować BitDefendera?

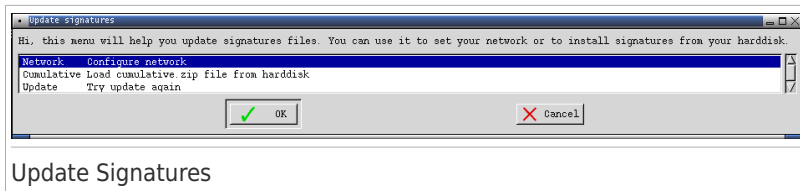
W czasie ponownego uruchomienia, aktualizacja sygnatur wirusów jest przeprowadzana automatycznie. Jeśli ten krok został pominięty, lub też nie chcesz wykonywać aktualizacji po uruchomieniu, są dwa sposoby na aktualizowanie BitDefender.

● Skorzystaj ze **Skanera BitDefender dla Unixów**.

- Kliknij dwukrotnie na ikonę URUCHOM SKANER na pulpicie. Uruchomisz **Skaner BitDefender dla Unixów**.
- Kliknij na **Aktualizacje**.

● Użyj skrótu **Aktualizuj Sygnatury** znajdującego się na Pulpicie.

- Kliknij dwukrotnie skrót na pulpicie Update Signatures. Pojawi się następujące okno.



2. Wykonaj jedną z czynności:

- ▶ Wybierz **Kumulacyjnie** aby zainstalować sygnatury już zapisane na twoim dysku poprzez przeglądanie komputera i załadowanie pliku cumulative.zip file.
- ▶ Wybierz **Update** aby natychmiast podłączyć się do Internetu i pobrać najnowsze sygnatury wirusów.

3. Kliknij **OK**.

34.5.1. Jak mogę zaktualizować BitDefendera przez proxy?

Jeśli twój komputer łączy się z Internetem przez serwer proxy, trzeba dokonać pewnych konfiguracji aby móc uaktualnić sygnatury wirusów.

Aby zaktualizować BitDefender poprzez proxy, skorzystaj z jednej z poniższych opcji:

● Skorzystaj ze **Skanera BitDefender dla Uniksów**.

1. Kliknij dwukrotnie na ikonę URUCHOM SKANER na Pulpicie. Uruchomisz **Skaner BitDefender dla Unixów**.
2. Kliknij na **Ustawienia**, a pojawi się nowe okno.
3. W **Ustawieniach Aktualizacji**, zaznacz pole **Włącz HTTP Proxy**. Określ hosta Proxy (następująco: host[:port]), użytkownika Proxy (następująco: [domena\]użytkownik) i hasło. Zaznacz pole **Pomiń serwer proxy jeśli nie jest dostępny** aby skorzystać z bezpośredniego połączenia kiedy serwer proxy nie jest dostępny.
4. Kliknij na **Zapisz**
5. Kliknij na **Aktualizuj**

● Użyj Terminala (jako root).

1. Kliknij prawym klawiszem na pulpit. Pojawi się menu kontekstowe Dysku Ratunkowego BitDefendera.
2. Wybierz **Terminal (jako root)**.
3. Wpisz polecenie: **cd /ramdisk/BitDefender-scanner/etc.**
4. Wpisz polecenie: **mcedit bdscan.conf** aby edytować ten plik używając GNU Midnight Commander (mc).
5. Odznacz następującą liniijkę: **#HttpProxy =** (po prostu usuń znak #) i podaj domenę, nazwę użytkownika, hasło i port serwera proxy. Na przykład, poprawna liniijka powinna wyglądać tak:

HttpProxy = myuser:mypassword@proxy.company.com:8080

6. Kliknij **F2** aby zapisać aktualny plik, potwierdź zapis i następnie kliknij **F10** aby je zamknąć.
7. Wpisz polecenie: **bdscan update**.

34.6. Jak mogę zapisać moje dane?

Założmy, że nie możesz włączyć swojego komputera w Windows z nieznanym powodem. Jednocześnie musisz skorzystać z ważnych danych znajdujących się na twoim komputerze. Tutaj przydaje się Dysk Ratunkowy BitDefendera.

By zapisać dane z komputera na dysku przenośnym takim jak klucz USB wykonaj następujące kroki:

1. Włóż płytę CD Dysku Ratunkowego BitDefendera do napędu CD, klucz USB do gniazda USB i zrestartuj komputer.



Notatka

Jeśli podłączysz klucz USB później, musisz zamontować napęd przenośny według następujących kroków:

- a. Kliknij dwukrotnie na Pulpicie skrót Terminal Emulator.
- b. Wpisz następującą komendę:

```
# mount /media/sdb1
```

Proszę pamiętać że w zależności od konfiguracji komputera to może być `sda1` zamiast `sdb1`.

2. Zaczekaj aż Dysk Ratunkowy BitDefendera się załaduje. Następujące okno się wyświetli.



Ekran Pulpitu.

3. Kliknij dwukrotnie partycję gdzie znajdują się dane które chcesz zapisać (na przykład [sda3]).



Notatka

Pracując z Dyskiem Ratunkowym BitDefendera, będziesz miał do czynienia z nazwami partycji typu Linux-owego. Zatem, [sda1] najprawdopodobniej będzie odnosił się do partycji (C:) w systemie Windows, [sda3] do (F:), a [sdb1] do klucza USB.



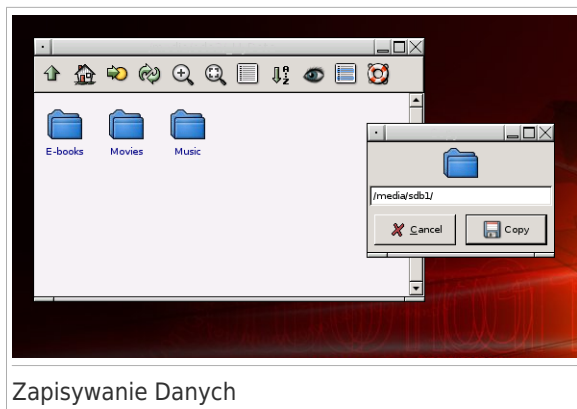
WAŻNE

Jeśli komputer nie został prawidłowo wyłączony, możliwe że określone partycje nie zostały automatycznie zamontowane. Aby zamontować partycje wykonaj następujące kroki.

- a. Kliknij dwukrotnie na Pulpicie skrót Terminal Emulator.
- b. Wpisz następującą komendę:

```
# mount /media/partition_name
```

4. Przeglądaj swoje foldery by otworzyć potrzebny folder. Na przykład, Moje Dokumenty który zawiera podfoldery Filmy, Muzyka oraz E-books.
5. Kliknij prawym klawiszem myszy odpowiedni folder i wybierz **Kopiuj**. Pojawi się następujące okno.



6. Wpisz `/media/sdb1/` w odpowiednie pole tekstowe i kliknij **Kopiuj**.

Proszę pamiętać że w zależności od konfiguracji komputera to może być `sda1` zamiast `sdb1`.

34.7. Jak korzystać z trybu konsoli?

Jeśli rozdzielczość ekranu jest zbyt niska aby uruchomić program w trybie graficznym, możesz skorzystać Dysku Naprawczego BitDefender w trybie konsoli. Prosty tryb tekstowy pozwala na przeprowadzenie całkowitego skanowania komputera.

Aby uruchomić tryb konsoli, ustaw BIOS tak, aby komputer najpierw uruchamiał się z płyty CD, wsadź dysk do napędu i uruchom ponownie komputer. Poczekać na ekran powitalny i wybierz **Uruchom Knoppix w trybie konsolowym**.

Po uruchomieniu, podążaj za instrukcjami na ekranie aby przeprowadzić kompletne skanowanie komputera.

BitDefender wykrywa partycje na twoim dysku twardym i automatycznie uaktualnia bazę sygnatur wirusów zanim rozpocznie proces skanowania. Jeśli zostanie znaleziony zainfekowany plik, BitDefender oczyści go. Po zakończeniu procesu skanowania, wyświetlony zostanie dziennik skanowania.



Notatka

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

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, ochronę przed takim adware 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 interfejsie 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 urządzenie, które czyta i zapisuje dane na dysku.

Twardy dysk czyta i zapisuje dane na twardym dysku.

Stacja dyskiekiet 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 uruchamiać 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 załaduje 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 applety pracują u klienta, nie mogą czytać ani zapisywać danych na tej maszynie. Dodatkowo, applety 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, że 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 aktualizację 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 pochodzą z spyware. Raz zainstalowane spyware nasłuchuje poruszanie się użytkownika po Internecie i przesyła te informacje w tle do kogoś innego. Spyware mogą także wykraść 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 dostępnych 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, przypominać, lub aplikacje programowe, które uruchamiają jakieś cechy.

Zasobnik systemowy

Wprowadzony przez Windows 95, system tray jest zlokalizowany w pasku zadań Windows (zwykle na dole, obok zegara) i zawiera miniaturowe ikony, służące łatwemu dostępowi do funkcji systemowych tj. fax, drukarki, modemu, itd. Podwójne kliknięcie lub kliknięcie prawym klawiszem myszy na ikonę spowoduje dostęp do danego elementu.

TCP/IP

Protokół Kontroli Transmisji/Protokół Internetowy – Zespół protokołów sieciowych szeroko używanych w internecie, 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 najmniejbezpiecznych 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 własny moduł 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 przez 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.