

F-Secure Anti-Virus 2013

Spis treści

Rozdział 1: Instalacja.....	5
Przed pierwszą instalacją	6
Instalowanie produktu po raz pierwszy.....	6
Instalowanie i uaktualnianie aplikacji.....	6
Pomoc i wsparcie techniczne.....	7
 Rozdział 2: Rozpoczynanie pracy.....	 9
Jak korzystać z aktualizacji automatycznych.....	10
Sprawdzanie stanu aktualizacji.....	10
Zmianie ustawień połączenia internetowego.....	10
Sprawdzanie stanu Sieci ochrony w czasie rzeczywistym.....	11
Sprawdzanie czynności wykonanych przez produkt.....	11
Wyświetlenie historii powiadomień	11
Zmianie ustawień powiadomień	11
Sieć ochrony w czasie rzeczywistym.....	12
Co to jest sieć ochrony w czasie rzeczywistym.....	12
Zalety sieci ochrony w czasie rzeczywistym.....	12
Jakie dane są przysyłane.....	13
W jaki sposób chronimy Twój prywatność	14
Dołączanie do sieci ochrony w czasie rzeczywistym.....	15
Pytania dotyczące sieci ochrony w czasie rzeczywistym.....	15
Jak sprawdzić, czy subskrypcja jest ważna.....	15
Centrum akcji.....	16
Aktywowanie subskrypcji.....	16
 Rozdział 3: Wprowadzenie.....	 17
Wyświetlanie ogólnego stanu ochrony.....	18
Wyświetlanie statystyki produktu.....	18
Obsługiwanie aktualizacji produktu.....	19
Wyświetlenie wersji baz danych.....	19
Zmianie ustawień połączeń internetowych na urządzeniu przenośnym.....	19
Co to są wirusy i inne złośliwe oprogramowanie?.....	20
Wirusy.....	20
Oprogramowanie szpiegujące.....	21
Programy typu rootkit.....	21
Ryzykowne oprogramowanie.....	21

Rozdział 4: Ochrona komputera przed złośliwym oprogramowaniem.23

Jak przeskanować komputer.....	24
Automatyczne skanowanie plików.....	24
Ręczne skanowanie plików.....	26
Skanowanie poczty e-mail.....	30
Wyświetlanie wyników skanowania.....	30
Jak wykluczyć pliki ze skanowania.....	31
Wykluczanie typów plików.....	31
Wykluczanie plików według lokalizacji.....	31
Wyświetlanie aplikacji wykluczonych.....	32
Jak korzystać z funkcji kwarantanny?.....	33
Wyświetlanie elementów poddanych kwarantannie.....	33
Przywracanie elementów poddanych kwarantannie.....	34
Co to jest technologia DeepGuard?.....	34
Włączanie i wyłączanie funkcji DeepGuard.....	34
Zezwalanie na aplikacje zablokowane przez funkcję DeepGuard.....	35
Używanie funkcji DeepGuard w trybie zgodności.....	35
Co robi w przypadku ostrzeżenia o podejrzanych działaniach.....	35

Instalacja

Tematy:

- *Przed pierwszą instalacją*
- *Instalowanie produktu po raz pierwszy*
- *Instalowanie i uaktualnianie aplikacji*
- *Pomoc i wsparcie techniczne*


Przed pierwszą instalacją

Dziękujemy za wybranie produktu firmy F-Secure.

Do zainstalowania tego produktu potrzebne są następujące składniki:

- Instalacyjny dysk CD lub pakiet. W przypadku użycia komputera przenośnego bez stacji dysków CD można pobrać pakiet instalacyjny z witryny www.f-secure.com/netbook.
- Klucz subskrypcji.
- Połączenie internetowe.

Jeżeli na komputerze jest już zainstalowany produkt zabezpieczający innego producenta, instalator podejmie próbę automatycznego usunięcia tego produktu. Jeżeli to usuwanie nie powiedzie się, należy usunąć ten produkt ręcznie.

 **Informacje:** Jeżeli na komputerze utworzono wcześniej jedno konto użytkownika, w celu przeprowadzenia instalacji należy zalogować się na koncie z uprawnieniami administratora.

Instalowanie produktu po raz pierwszy

Instrukcje dotyczące instalowania produktu.

Aby zainstalować produkt, wykonaj następujące czynności:

1. Włóż do stacji dysk CD lub kliknij dwukrotnie pobrany plik instalatora.

Jeżeli dysk CD nie zostanie uruchomiony automatycznie, otwórz program Eksplorator Windows, kliknij dwukrotnie ikonę stacji dysków CD-ROM, a następnie kliknij dwukrotnie plik instalacyjny w celu rozpoczęcia instalacji.

2. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

- Jeżeli produkt został nabyty na dysku CD w sklepie, klucz subskrypcji można znaleźć na okładce przewodnika szybkiej instalacji.
- Jeżeli produkt został pobrany ze sklepu elektronicznego F-Secure eStore, klucz subskrypcji jest dołączony do wiadomości e-mail z potwierdzeniem zamówienia.

Przed potwierdzeniem subskrypcji i pobraniem najnowszych aktualizacji z Internetu konieczne może być ponowne uruchomienie komputera. W przypadku instalowania za pomocą dysku CD pamiętaj o wyjęciu instalacyjnego dysku CD ze stacji dysków przed ponownym uruchomieniem komputera.

Instalowanie i uaktualnianie aplikacji

Instrukcja dotycząca aktywowania nowej subskrypcji.

Postępuj zgodnie z poniższymi instrukcjami, aby aktywować nową subskrypcję lub zainstalować nową aplikację za pomocą panelu głównego:

 **Informacje:** Ikona panelu głównego znajduje się na pasku zadań systemu Windows.

1. W panelu głównym kliknij prawym przyciskiem myszy ostatnią ikonę po prawej. Zostanie wyświetlone menu podręczne.
2. Wybierz polecenie **Wyświetl moje subskrypcje**.

3. W obszarze **Moje subskrypcje** przejdź na stronę **Stan subskrypcji** i kliknij opcję **Aktywuj subskrypcję**.
Zostanie otwarte okno **Aktywuj subskrypcję**.
4. Wprowadź klucz subskrypcji aplikacji i kliknij przycisk **OK**.
5. Gdy subskrypcja zostanie potwierdzona i aktywowana, kliknij przycisk **Zamknij**.
6. W obszarze **Moje subskrypcje** przejdź na stronę **Stan instalacji**. Jeśli instalacja nie zostanie rozpoczęta automatycznie, wykonaj następujące czynności:
 - a) Kliknij przycisk **Zainstaluj**.
Zostanie otwarte okno instalacji.
 - b) Kliknij przycisk **Dalej**.
Aplikacja zostanie pobrana, a następnie rozpocznie się instalacja.
 - c) Po ukończeniu instalacji kliknij przycisk **Zamknij**.

Nowa subskrypcja została aktywowana.

Pomoc i wsparcie techniczne

W celu uzyskania dostępu do pomocy dla produktu online możesz kliknąć ikonę **Pomoc** lub nacisnąć klawisz **F1** na dowolnym ekranie produktu.

Zarejestrowanie licencji uprawnia użytkownika do korzystania z dodatkowych usług, takich jak bezpłatne aktualizacje produktu i pomoc techniczna. Rejestrację możesz przeprowadzić pod adresem www.f-secure.com/register.

Rozpoczynanie pracy

Tematy:

- *Jak korzystać z aktualizacji automatycznych*
- *Sprawdzanie czynności wykonanych przez produkt*
- *Ścieżki ochrony w czasie rzeczywistym*
- *Jak sprawdzić, czy subskrypcja jest włączona*

Informacje dotyczące rozpoczynania pracy z produktem.

W tej sekcji opisano sposób zmieniania wspólnych ustawień i zarządzania subskrypcjami za pomocą panelu głównego.

Wspólne ustawienia w panelu głównym dotyczą wszystkich programów zainstalowanych w tym panelu. Zamiast zmieniać ustawienia oddzielnie w poszczególnych programach możesz po prostu edytować wspólne ustawienia, które są stosowane do wszystkich zainstalowanych programów.

Wspólne ustawienia w panelu głównym obejmują następujące opcje:

- Pobrane pliki udostępniają informacje o pobranych aktualizacjach i umożliwiają ręczne sprawdzanie dostępności aktualizacji.
- Ustawienia połączenia służące do zmieniania sposobu nawiązywania połączenia internetowego przez komputer.
- Powiadomienia umożliwiają wyświetlanie wyświetlonych w przeszłości powiadomień i ustawianie typów wyświetlanych powiadomień.
- Ustawienia prywatności, które pozwalają określić, czy komputer może nawiązywać połączenie z sieci ochrony w czasie rzeczywistym.

Ponadto za pośrednictwem panelu głównego możesz zarządzać swoimi subskrypcjami dla zainstalowanych programów.

Jak korzystać z aktualizacji automatycznych

Dziękujemy za aktualizację automatyczną mechanizmu ochrony komputera — zawsze aktualne.

Produkt pobiera na komputer najnowsze aktualizacje po nawiązaniu połączenia z Internetem — wykrywa ruch sieciowy i nie przeszkadza w korzystaniu z Internetu w innych celach nawet w przypadku wolnego połączenia sieciowego.


Sprawdzanie stanu aktualizacji

Możliwe jest wyświetlenie daty i godziny ostatniej aktualizacji.

Gdy aktualizacje automatyczne są włączone i jest dostępne połączenie z Internetem, produkt automatycznie otrzymuje najnowsze aktualizacje.

Aby upewnić się, że najnowsze aktualizacje zostały zainstalowane:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Aktualizacje automatyczne** > **Pobrane pliki**.
4. Kliknij przycisk **Sprawdź teraz**.
Produkt nawiąże połączenie z Internetem i sprawdzi dostępność najnowszych aktualizacji. Jeśli ochrona nie jest aktualna, zostaną pobrane najnowsze aktualizacje.


 **Informacje:** Jeśli dostęp do Internetu jest uzyskiwany za pomocą modemu lub łącza ISDN, to aby możliwe było sprawdzenie aktualizacji, połączenie musi być aktywne.

Zmianie ustawień połączenia internetowego


Zazwyczaj nie trzeba zmieniać ustawień domyślnych. Jednak można skonfigurować sposób nawiązania połączenia z Internetem przez serwer na potrzeby automatycznego otrzymywania aktualizacji.

Aby zmienić ustawienia połączenia internetowego, wykonaj następujące czynności:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Aktualizacje automatyczne** > **Połączenie**.
4. Za pomocą listy **Połączenie internetowe** wybierz używany na komputerze sposób nawiązania połączenia z Internetem.
 - Wybierz opcję **Uznaj za zawsze połączone**, jeśli komputer ma stałe połączenie sieciowe.

 **Informacje:** Jeśli komputer nie ma stałego połączenia sieciowego i został skonfigurowany do nawiązania połączenia na żądanie, to wybranie opcji **Uznaj za zawsze połączone** może powodować inicjowanie wielu połączeń telefonicznych.

- Wybierz opcję **Wykryj połączenie**, aby pobierać aktualizacje tylko po wykryciu przez produkt aktywnego połączenia sieciowego.
- Wybierz opcję **Wykryj ruch**, jeśli aktualizacje mają być pobierane tylko po wykryciu przez produkt innego ruchu sieciowego.

 **Wskazówka:** W przypadku nietypowej konfiguracji sprzętowej, w której ustawienie **Wykryj połączenie** zawsze wskazuje istnienie aktywnego połączenia sieciowego, nawet jeśli nie zostało ono nawiązane, należy wybrać opcję **Wykryj ruch**.

5. Za pomocą listy **Serwer proxy HTTP** określi, czy komputer korzysta z *serwera proxy* do nawiązywania połączenia z Internetem.
 - Wybierz opcję **Bez serwera proxy HTTP**, jeśli komputer jest połączony z Internetem bezpośrednio.
 - Wybierz opcję **Ręcznie konfiguruje serwer proxy HTTP**, aby skonfigurować ustawienia *serwera proxy HTTP*.
 - Wybierz opcję **Użyj serwera proxy HTTP przeglądarki**, aby zastosować ustawienia *serwera proxy HTTP* skonfigurowane w przeglądarce internetowej.

Sprawdzanie stanu Sieci ochrony w czasie rzeczywistym

W celu prawidłowego działania wiele funkcji produktu polega na połączeniu z Siecią ochrony w czasie rzeczywistym.

W przypadku wystąpienia problemów z połączeniem sieciowym, lub gdy zaporę blokuje ruch Sieci ochrony w czasie rzeczywistym, wyświetlany jest stan „nie połączono”. Jeśli natomiast żadna funkcja wymagająca dostępu do Sieci ochrony w czasie rzeczywistym nie została zainstalowana, wyświetlana jest informacja o tym, że sieć nie jest używana.

Aby sprawdzić aktualny stan, wykonaj następujące czynności:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej. Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Aktualizacje automatyczne > Połączenie**.

W obszarze **Sieć ochrony w czasie rzeczywistym** wyświetlane są informacje o bieżącym stanie tej funkcji.

Sprawdzanie czynności wykonanych przez produkt

Na stronie **Powiadomienia** możesz zobaczyć listę czynności wykonanych przez produkt w celu ochrony komputera.

Produkt wyświetla powiadomienia o wykonaniu czynności, na przykład po wykryciu i zablokowaniu wirusa. Niektóre powiadomienia mogą być wysyłane przez usługodawcę, na przykład w celu przekazania informacji o nowych usługach.

Wyświetlenie historii powiadomień

W historii powiadomień możesz zobaczyć powiadomienia, które zostały wyświetlone.

Aby wyświetlić historię powiadomień, wykonaj następujące czynności:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej. Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Inne > Powiadomienia**.
4. Kliknij opcję **Pokaż historię powiadomień**. Zostanie otwarta lista historii powiadomień.

Zmianie ustawień powiadomień

Możesz określić typy powiadomień wyświetlanych przez produkt.

Aby zmienić ustawienia powiadomień, wykonaj następujące czynności:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Inne** > **Powiadomienia**.
4. Zaznacz lub wyczyść pole wyboru **Zezwalaj na komunikaty programu**, aby włączyć lub wyłączyć komunikaty programu.
Po zaznaczeniu tego ustawienia produkt wyświetla powiadomienia z zainstalowanych programów.
5. Zaznacz lub wyczyść pole wyboru **Zezwalaj na wiadomości promocyjne**, aby włączyć lub wyłączyć wiadomości promocyjne.
6. Kliknij przycisk **OK**.

Sieć ochrony w czasie rzeczywistym

W tym dokumencie opisano sieć ochrony w czasie rzeczywistym — usługę internetową firmy F-Secure Corporation służącą do identyfikowania bezpiecznych aplikacji i witryn internetowych oraz zabezpieczania przed złośliwym oprogramowaniem i witrynami wykorzystującymi luki w zabezpieczeniach.

Co to jest sieć ochrony w czasie rzeczywistym

Sieć ochrony w czasie rzeczywistym jest usługą online zapewniającą błyskawiczne reakcje na nowe zagrożenia internetowe.

Uczestnicząc w sieci ochrony w czasie rzeczywistym, możesz pomóc nam wzmocnić nasze zabezpieczenia przed nowymi i powstającymi zagrożeniami. Sieć ochrony w czasie rzeczywistym gromadzi dane statystyczne dotyczące nieznanych, złośliwych i podejrzanych aplikacji z uwzględnieniem informacji o ich działaniu na urządzeniu. Te informacje mają charakter anonimowy i są wysyłane do analizy zbiorczej w firmie F-Secure Corporation. Korzystając z wyników takich analiz, udoskonalamy zabezpieczenia urządzeń przed najnowszymi zagrożeniami i złośliwymi plikami.

Jak działa sieć ochrony w czasie rzeczywistym

Uczestnicząc w sieci ochrony w czasie rzeczywistym, możesz udostępnić informacje dotyczące nieznanych aplikacji i witryn internetowych oraz złośliwych programów i witryn zawierających próby wykorzystania luk w zabezpieczeniach. Sieć ochrony w czasie rzeczywistym nie prowadzi działań użytkowników w Internecie, nie gromadzi informacji na temat witryn, które zostały już przeanalizowane, ani nie zbiera informacji o bezpiecznych aplikacjach zainstalowanych na komputerze.

Jeśli nie chcesz udostępnić takich danych, żadne informacje dotyczące zainstalowanych aplikacji i odwiedzanych witryn nie będą gromadzone. Jednak produkt musi wysyłać do serwerów firmy F-Secure zapytania dotyczące reputacji aplikacji, witryn internetowych, wiadomości i innych obiektów. Zapytania są przeprowadzane przy użyciu kryptograficznej sumy kontrolnej, gdzie sam obiekt, którego zapytanie dotyczy, nie jest wysyłany do firmy F-Secure. Nie ledzimy danych dla poszczególnych użytkowników — tylko liczba zapytań dla pliku lub witryny jest zwracana.

Całkowite zatrzymanie komunikacji z siecią ochrony w czasie rzeczywistym nie jest możliwe, ponieważ stanowi ona integralną część ochrony zapewnianej przez produkt.

Zalety sieci ochrony w czasie rzeczywistym

Sieć ochrony w czasie rzeczywistym zapewnia szybszą i dokładniejszą ochronę przed najnowszymi zagrożeniami — bez niepotrzebnych alertów dotyczących podejrzanych aplikacji, które nie są złośliwe.

Uczestnicząc w sieci ochrony w czasie rzeczywistym, możesz pomóc nam w wykrywaniu nowych i nieznanych form złośliwego oprogramowania oraz eliminowaniu obiektów niepoprawnie uznanych za niebezpieczne z naszej bazy danych definicji wirusów.

Wszyscy uczestnicy sieci ochrony w czasie rzeczywistym pomagają sobie wzajemnie. W przypadku wykrycia podejrzanego programu na urządzeniu Twoje wyniki analizy tego programu wykrytego wcześniej na innych urządzeniach. Sieć ochrony w czasie rzeczywistym zwraca uwagę ogólnie na urządzenia, ponieważ zainstalowany program zabezpieczający nie musi skanować aplikacji przeanalizowanych i uznanych za bezpieczne przez sieć ochrony w czasie rzeczywistym. Podobnie informacje dotyczące złośliwych witryn internetowych i niechcianych wiadomości zbiorczych są udostępniane za pomocą sieci ochrony w czasie rzeczywistym, umożliwiając zapewnienie dokładniejszej ochrony przed witrynami wykorzystującymi luki w zabezpieczeniach i spamem.

Im więcej osób uczestniczy w sieci ochrony w czasie rzeczywistym, tym indywidualna ochrona użytkowników staje się lepsza.

Jakie dane są przesyłane

Uczestnicząc w sieci ochrony w czasie rzeczywistym, udostępniasz informacje dotyczące aplikacji zapisanych na Twoim urządzeniu i odwiedzanych przez Ciebie witryn internetowych. Te dane umożliwiają sieci ochrony w czasie rzeczywistym zapewnienie ochrony przed najnowszymi złośliwymi aplikacjami i podejrzanymi witrynami internetowymi.

Analizowanie reputacji plików

Sieć ochrony w czasie rzeczywistym gromadzi informacje dotyczące tylko aplikacji bez określonej reputacji i znanych plików, które są podejrzane lub zawierają złośliwe oprogramowanie.

Sieć ochrony w czasie rzeczywistym gromadzi anonimowe informacje na temat bezpiecznych i podejrzanych aplikacji znajdujących się na urządzeniu, jednak tylko przenośne pliki wykonywalne są uwzględniane (takie jak pliki z rozszerzeniami cpl, exe, dll, ocx, sys, scr i drv na platformie systemu Windows).

Gromadzone informacje obejmują :

- ścieżkę pliku aplikacji na urządzeniu;
- rozmiar oraz datę utworzenia lub zmodyfikowania pliku;
- atrybuty i uprawnienia pliku;
- informacje o sygnaturze pliku;
- bieżącą wersję pliku i nazwę firmy, w której został utworzony;
- źródło pliku lub adres URL pobierania;
- wyniki skanowania plików przy użyciu technologii F-Secure DeepGuard i mechanizmów antywirusowych;
- inne podobne informacje.

Adne informacje dotyczące dokumentów osobistych nie są gromadzone w sieci ochrony w czasie rzeczywistym, o ile takie pliki nie są zainfekowane. W przypadku dowolnego typu złośliwego oprogramowania zbierane są informacje o nazwie infekcji i stanie czyszczenia pliku.

Ponadto przy użyciu sieci ochrony w czasie rzeczywistym możesz przesyłać podejrzone aplikacje do analizy. Podczas przesyłania takich aplikacji uwzględniane są tylko przenośne pliki wykonywalne. Sieć ochrony w czasie rzeczywistym nigdy nie gromadzi jakichkolwiek informacji dotyczących dokumentów osobistych ani nie przesyła ich automatycznie do analizy.

Przesyłanie plików do analizy

Ponadto sieć ochrony w czasie rzeczywistym umożliwia przesyłanie podejrzanych aplikacji do analizy.


Pojedyncze podejrzone aplikacje możesz przesyłać również po wyświetleniu odpowiedniego monitu produktu. Dotyczy to tylko przenośnych plików wykonywalnych. Sieć ochrony w czasie rzeczywistym nigdy nie przesyła osobistych dokumentów.

Analizowanie reputacji witryn internetowych

Sie ochrony w czasie rzeczywistym nie ledzi działa u ytkowników w Internecie ani nie gromadzi informacji dotyczących witryn, które zostały już przeanalizowane, a jedynie sprawdza bezpieczeństwo odwiedzanych witryn podczas przeglądania Internetu. Po otwarciu witryny sie ochrony w czasie rzeczywistym sprawdza, czy jest ona bezpieczna, a następnie powiadamia o poziomie ewentualnego zagrożenia (w przypadku podejrzanych lub szkodliwych witryn).

Jeśli witryna zawiera podejrzane lub złośliwe obiekty bądź próby wykorzystania znanej luki w zabezpieczeniach, cały adres URL tej witryny jest zapisywany przez sie ochrony w czasie rzeczywistym w celu przeanalizowania jej zawartości.

W przypadku odwiedzenia witryny, która nie została jeszcze oceniona, sie ochrony w czasie rzeczywistym gromadzi nazwę domeny i jej poddomen, a w niektórych sytuacjach również adres odwiedzonej strony, na potrzeby przeanalizowania i oceny tej witryny. Wszystkie parametry adresu URL zawierające informacje, które mogą zostać skojarzone z danymi identyfikującymi to samo u ytkownika, są usuwane w trosce o ochronę prywatności.

 **Informacje:** Sie ochrony w czasie rzeczywistym nie ocenia ani nie analizuje stron w prywatnych sieciach, czyli dane informacje dotyczące adresów IP prywatnych sieci (takich jak firmowe sieci intranet) nie są gromadzone.

Analizowanie informacji systemowych

W ramach sieci ochrony w czasie rzeczywistym gromadzone są informacje o nazwie i wersji systemu operacyjnego, połączeniu internetowym oraz dane statystyczne dotyczące u ytkowania sieci ochrony w czasie rzeczywistym, takie jak liczba zapytań o reputację witryny i średni czas uzyskiwania wyników zapytania, na potrzeby monitorowania i ulepszania naszej usługi.

W jaki sposób chronimy Twój prywatność

Wszystkie informacje są przesyłane w bezpieczny sposób po automatycznym usunięciu jakichkolwiek danych osobowych.

Sie ochrony w czasie rzeczywistym usuwa wszelkie dane umożliwiające identyfikację przed wysłaniem informacji na serwery firmy F-Secure. Ponadto wszystkie zgromadzone informacje są zaszyfrowane podczas przesyłania, uniemożliwiając nieautoryzowany dostęp. Zgromadzone informacje nie są przetwarzane indywidualnie, ale w zbiorowej postaci obejmującej informacje uzyskane od innych uczestników sieci ochrony w czasie rzeczywistym. Wszystkie dane są anonimowo analizowane pod kątem statystycznym, co oznacza, że nie można ich skojarzyć z poszczególnymi u ytkownikami.

Dane umożliwiające identyfikację to samo ci u ytkowników nie są uwzględniane w gromadzonych danych. Sie ochrony w czasie rzeczywistym nie gromadzi prywatnych adresów IP ani innych danych osobowych, takich jak adresy e-mail, nazwy u ytkowników i hasła. Mimo że podejmujemy wszelkie starania w celu usunięcia wszystkich identyfikujących danych osobowych, istnieje możliwość pozostania identyfikujących danych w gromadzonych informacjach. W takich sytuacjach nie będziemy używać przypadkowo uzyskanych danych w celu określenia tożsamości u ytkowników.

Stosujemy rygorystyczne metody ochrony oraz fizyczne, administracyjne i techniczne zabezpieczenia gromadzonych danych podczas ich przesyłania, przechowywania i przetwarzania. Informacje są przechowywane w bezpiecznych lokalizacjach na kontrolowanych przez nas serwerach, które znajdują się w naszych biurach lub w biurach naszych podwykonawców. Tylko upoważniony personel ma dostęp do gromadzonych informacji.

Firma F-Secure może udostępnić zgromadzone dane swoim podmiotom stowarzyszonym, podwykonawcom, dystrybutorom i partnerom, jednak zawsze w anonimowej postaci uniemożliwiając identyfikację u ytkowników.

Dołączanie do sieci ochrony w czasie rzeczywistym

Udostępniaj c informacje dotyczące złośliwych programów i witryn internetowych, mo esz pomóc nam w ulepszaniu zabezpieczeń oferowanych w ramach sieci ochrony w czasie rzeczywistym.

Opcja uczestniczenia w sieci ochrony w czasie rzeczywistym jest dostępna podczas instalacji. Domyślne ustawienia instalacji powodują przesyłanie danych do sieci ochrony w czasie rzeczywistym. To ustawienie mo esz zmienić później w produkcie.

Postępuj zgodnie z następującymi instrukcjami, aby zmienić ustawienia sieci ochrony w czasie rzeczywistym:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Inne** > **Prywatno**.
4. Zaznacz odpowiednie pole wyboru, aby zostać uczestnikiem sieci ochrony w czasie rzeczywistym.

Pytania dotyczące sieci ochrony w czasie rzeczywistym

Informacje kontaktowe w przypadku jakichkolwiek pytań dotyczących sieci ochrony w czasie rzeczywistym.

Jeśli masz jakiegokolwiek inne pytania dotyczące sieci ochrony w czasie rzeczywistym, skontaktuj się z nami pod adresem:

F-Secure Corporation

Tammasaarekatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

Najnowsza wersja tego dokumentu jest zawsze dostępna w naszej witrynie internetowej.

Jak sprawdzić, czy subskrypcja jest ważna

Na stronie **Stan subskrypcji** wyświetlane są informacje na temat typu i stanu Twojej subskrypcji.

Jeśli ważność subskrypcji ma wkrótce wygasnąć lub już wygasła, ogólny stan ochrony programu przy odpowiedniej ikonie na panelu głównym zostaje zmieniony.

Aby sprawdzić ważność subskrypcji:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Wyświetl moje subskrypcje**.
3. Wybierz opcję **Stan subskrypcji**, aby wyświetlić informacje na temat subskrypcji i zainstalowanych programów.
4. Wybierz opcję **Stan instalacji**, aby zobaczyć, jakie programy są dostępne do zainstalowania.

Informacje o stanie subskrypcji i dacie wa no ci s r ównie dost pne w programie na stronie [Statystyka](#). Je li wa no subskrypcji wygasła, musisz odnowi subskrypcj , aby otrzymywa aktualizacje i kontynuowa u ywanie produktu.


 **Informacje:** W przypadku wyga ni cia subskrypcji miga ikona stanu produktu na pasku zada systemu.

Centrum akcji

W centrum akcji wy wietlane s powiadomienia dotycz ce wszystkich wa nych informacji.

Je li wa no subskrypcji wygasła lub wkrótce wyga nie, w centrum akcji wy wietlane jest odpowiednie powiadomienie. Kolor tła i tre komunikatu w centrum akcji s zale ne od stanu i typu subskrypcji:

- Je li wa no subskrypcji ma wkrótce wygasn i dost pne s wolne subskrypcje, tło komunikatu jest białe, a sam komunikat zawiera przycisk [Aktywuj](#).
- Je li wa no subskrypcji ma wkrótce wygasn i wolne subskrypcje nie s dost pne, tło komunikatu jest ółte, a sam komunikat zawiera przyciski [Kup](#) i [Wprowad klucz](#). W przypadku gdy nowa subskrypcja została ju zakupiona, mo na klikn przycisk [Wprowad klucz](#) i poda klucz subskrypcji w celu aktywowania nowej subskrypcji.
- Je li wa no subskrypcji wygasła i dost pne s wolne subskrypcje, tło komunikatu jest czerwone, a sam komunikat zawiera przycisk [Aktywuj](#).
- Je li wa no subskrypcji wygasła i wolne subskrypcje nie s dost pne, tło komunikatu jest czerwone, a sam komunikat zawiera przyciski [Kup](#) i [Wprowad klucz](#). W przypadku gdy nowa subskrypcja została ju zakupiona, mo na klikn przycisk [Wprowad klucz](#) i poda klucz subskrypcji w celu aktywowania nowej subskrypcji.


 **Informacje:** Dost pne w centrum akcji ł cze [Poka histori powiadomie](#) słu y do wy wietlania listy komunikatów z powiadomieniami dotycz cymi produktów, a nie wcze niejszych powiadomie z centrum akcji.

Aktywowanie subskrypcji

Po uzyskaniu nowego klucza subskrypcji lub kodu kampanii produktu musisz go aktywowa .

Aby aktywowa subskrypcj , wykonaj nast puj ce czynno ci:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
Zostanie wy wietlone menu podr czne.
2. Wybierz opcj [Wy wietl moje subskrypcje](#).
3. Wybierz jedn z nast puj cych opcji:
 - Kliknij pozycj [Aktywuj subskrypcj](#) .
 - Kliknij pozycj [Aktywuj kod kampanii](#).
4. W otwartym oknie dialogowym wprowad nowy klucz subskrypcji lub kod kampanii, a nast pnie kliknij przycisk [OK](#).

 **Wskazówka:** Je li klucz subskrypcji został dostarczony w wiadomo ci e-mail, mo esz skopiowa klucz z wiadomo ci i wklei go w odpowiednim polu.

Po wprowadzeniu nowego klucza subskrypcji data wa no ci nowej subskrypcji zostanie wy wietlona na stronie [Stan subskrypcji](#).

Wprowadzenie

Tematy:

- *Wyświetlanie ogólnego stanu ochrony*
- *Wyświetlanie statystyki produktu*
- *Obsługiwanie aktualizacji produktu*
- *Co to są wirusy i inne złośliwe oprogramowanie?*

Ten produkt chroni komputer przed wirusami i innymi szkodliwymi aplikacjami.

Produkt automatycznie skanuje pliki i analizuje aplikacje oraz jest automatycznie aktualizowany. Nie wymaga on żadnych działań ze strony użytkownika.

Wyświetlanie ogólnego stanu ochrony






Na stronie **Stan** wyświetlane są podstawowe informacje o zainstalowanych funkcjach produktu i ich bieżącym stanie.

Aby otworzyć stronę **Stan**, wykonaj następujące czynności:

Na stronie głównej kliknij opcję **Stan**.

Zostanie otwarta strona **Stan**.

Ikony przedstawiają stan programu i jego funkcji zabezpieczenia.

Ikona stanu	Nazwa stanu	Opis
	OK	Komputer jest chroniony. Funkcja jest włączona i działa poprawnie.
	Informacja	Produkt informuje o specjalnym stanie funkcji. Na przykład funkcja jest aktualizowana.
	Ostrzeżenie	Komputer nie jest w pełni chroniony. Na przykład produkt długo nie był aktualizowany lub stan funkcji wymaga uwagi użytkownika.
	Błąd	Komputer nie jest chroniony. Na przykład wygasła subskrypcja lub jest wyłączona krytyczna funkcja.
	Wyłączone	Niekrytyczna funkcja jest wyłączona.

Wyświetlanie statystyki produktu

Na stronie **Statystyka** można sprawdzić, co produkt robił od momentu zainstalowania.

Aby otworzyć stronę **Statystyka**:

Na stronie głównej kliknij opcję **Statystyka**.

Zostanie otwarta strona **Statystyka**.

- W polu **Ostatnie pomiary sprawdzanie aktualizacji** wyświetlane są informacje o czasie przeprowadzenia ostatniej aktualizacji.

- **Skanowanie w poszukiwaniu wirusów i oprogramowania szpieguj cego** zawiera informacje o liczbach plików przeskanowanych i oczyszczonych przez produkt od momentu zainstalowania.
- **Aplikacje** wskazuje liczbę programów, którym technologia DeepGuard umożliwiła działanie lub które zablokowała od momentu zainstalowania produktu.
- W obszarze **Połączenia zapory** jest wyświetlana liczba dozwolonych i zablokowanych połączeń od momentu zainstalowania.
- W obszarze **Filtrowanie spamu i wiadomości typu phishing** widoczna jest liczba wiadomości e-mail określonych przez produkt jako poprawne lub zawierające spam.

Obsługiwanie aktualizacji produktu


Produkt zapewnia automatyczną aktualizację zabezpieczeń komputera.

Wyświetl wersje baz danych

Terminy i numery wersji najnowszych aktualizacji można wyświetlić na stronie **Aktualizacje baz danych**.

Aby otworzyć stronę **Aktualizacje baz danych**, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Ustawienia**.


 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Wersje bez danych**.


Na stronie **Wersje baz danych** są wyświetlane informacje o datach ostatniego aktualizowania definicji wirusów i oprogramowania szpiegującego, funkcji DeepGuard oraz filtrowania spamu i phishingu wraz z odpowiednimi numerami wersji.

Zmianie ustawień połączeń internetowych na urządzeniu przenośnym

Te ustawienia pozwalają określić, czy aktualizacje zabezpieczeń mają być pobierane podczas używania szerokopasmowego połączenia na urządzeniu przenośnym.


 **Informacje:** Ta funkcja jest dostępna tylko w systemie Microsoft Windows 7.

Domyślnie aktualizacje zabezpieczeń są zawsze pobierane, gdy urządzenie znajduje się w zasięgu sieci głównego operatora. Jeśli natomiast sieć głównego operatora jest niedostępna, aktualizacje zostają wstrzymane. Dzieje się tak, ponieważ ceny połączeń mogą różnić się u poszczególnych operatorów, na przykład w innych krajach. Aby zmniejszyć koszty przepustowości i prawdopodobnie ograniczyć wydatki, zalecane jest pozostawienie tych ustawień bez zmian podczas wyjazdów.

 **Informacje:** To ustawienie dotyczy tylko szerokopasmowych połączeń transmisji danych. Gdy komputer jest podłączony do zwykłej sieci (przewodowej lub bezprzewodowej), produkt jest automatycznie aktualizowany.

Aby zmienić to ustawienie, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Połączenia szerokopasmowe na urządzeniu przenośnym** > **Pobierz aktualizacje zabezpieczeń**.
3. Wybierz preferowaną opcję aktualizacji dla połączenia na urządzeniu przenośnym:
 - **Tylko w sieci głównego operatora**

Aktualizacje s zawsze pobierane, gdy urządzenie znajduje się w zasięgu sieci głównego operatora. Jeśli natomiast sie głównego operatora jest niedostępna, aktualizacje zostają wstrzymane. Wybranie tej opcji jest zalecane. Pozwala to utrzymywać aktualny stan produktu zabezpieczając go bez nieoczekiwanych kosztów.

- **Nigdy**

Aktualizacje nie są pobierane przy użyciu połączenia internetowego na urządzeniu przenośnym.

- **Zawsze**

Aktualizacje s zawsze pobierane, niezależnie od używanej sieci. Wybierając tę opcję, można upewnić się, że zabezpieczenia komputera są zawsze aktualne, bez względu na koszty.

4. Aby zdecydować oddzielnie za każdym razem, gdy nawiązywane jest połączenie z inną siecią, wybierz opcję **Zapytaj za każdym razem, gdy sie głównego operatora jest niedostępna**.

Wstrzymane aktualizacje zabezpieczeń

Aktualizacje zabezpieczeń mogą zostać wstrzymane na czas używania połączenia szerokopasmowego na urządzeniu przenośnym poza zasięgiem sieci podstawowego operatora.

W takim przypadku w prawym dolnym rogu ekranu zostaje wyświetlone powiadomienie o treści **Wstrzymano**. Aktualizacje są wstrzymywane, ponieważ ceny połączeń mogą różnić się u poszczególnych operatorów, na przykład w innych krajach. Aby zmniejszyć użycie przepustowości i prawdopodobnie ograniczyć wydatki, zalecane jest pozostawienie tych ustawień bez zmian podczas wyjazdów. Jeśli jednak chcesz modyfikować te ustawienia, kliknij ikonę **Zmień**.



Informacje:

Ta funkcja jest dostępna tylko w systemie Microsoft Windows 7.

Co to są wirusy i inne złoliwe oprogramowanie?

Złoliwe oprogramowanie to programy utworzone specjalnie w celu czynienia szkód na komputerze, używania komputera w niedozwolonych celach bez wiedzy użytkownika lub kradzieży informacji z komputera.

Złoliwe oprogramowanie może:

- przejąć kontrolę nad przeglądarką sieci Web,
- przekierowywać próby wyszukiwania,
- wyświetlać niepożądane reklamy,
- odwiedzić witryny odwiedzane przez użytkownika,
- kraść informacje osobiste, takie jak informacje dotyczące bankowości elektronicznej,
- używać komputera użytkownika do wysyłania spamu,
- używać komputera użytkownika do ataku na inne komputery.

Złoliwe oprogramowanie może też spowalniać pracę komputera i powodować jego niestabilność. Podejrzanie, że na komputerze znajduje się *złoliwe oprogramowanie*, może się pojawić, gdy komputer nagle zaczyna pracować bardzo wolno lub często ulega awariom.

Wirusy

Wirusy to zwykle programy, które dołączają się do plików i powielają się wielokrotnie. Wirusy mogą modyfikować i zastąpić zawartość innych plików w sposób, który może spowodować uszkodzenie komputera.

Wirus to program, który zazwyczaj jest instalowany na komputerze bez wiedzy użytkownika. Po zainstalowaniu wirus podejmuje próbę powielenia się. Wirus:

- korzysta z zasobów systemowych komputera,

- może modyfikować lub uszkadzać pliki na komputerze,
- prawdopodobnie próbuje użyć komputera do zainfekowania innych komputerów,
- może umożliwić użycie komputera w niedozwolonych celach.

Oprogramowanie szpiegujące

Oprogramowanie szpiegujące jest używane do gromadzenia informacji osobistych użytkownika.

Oprogramowanie szpiegujące może zbierać informacje osobiste, w tym dotyczące:

- przeglądanych stron internetowych,
- adresów e-mail przechowywanych na komputerze,
- haseł,
- numerów kart kredytowych.

Oprogramowanie szpiegujące prawie zawsze instaluje się samoczynnie bez wiadomej zgody użytkownika. Oprogramowanie szpiegujące może zostać zainstalowane razem z przydatnym programem lub w wyniku nakłonienia użytkownika do kliknięcia opcji w mylnym oknie podręcznym.

Programy typu rootkit

Programy typu rootkit utrudniają znalezienie innego *złośliwego oprogramowania*.

Programy typu rootkit ukrywają pliki i procesy. Zazwyczaj ma to na celu ukrycie działania złośliwych programów na komputerze. Kiedy program typu rootkit ukrywa *złośliwe oprogramowanie*, użytkownik nie jest w stanie łatwo zorientować się, gdzie takie oprogramowanie znajduje się na komputerze.

Niniejszy produkt posiada skaner programów typu rootkit, który skanuje komputer w poszukiwaniu programów typu rootkit, dzięki czemu *złośliwe oprogramowanie* nie może tak łatwo się ukrywać.

Ryzykowne oprogramowanie

Ryzykowne oprogramowanie nie powstaje z myślą o wyrządzaniu szkód na komputerach, ale nieodpowiednio używane może powodować uszkodzenia.

Ryzykowne oprogramowanie nie jest, ściśle rzecz biorąc, złośliwym oprogramowaniem. Pełni ono użyteczne, jednak potencjalnie niebezpieczne funkcje.

Przykładami takich programów są:

- klienty wiadomości błyskawicznych, np. usługa IRC (Internet Relay Chat);
- programy służące do przesyłania plików w Internecie między komputerami;
- programy telefonii internetowej, np. VoIP (*Voice over Internet Protocol*);
- oprogramowanie do zdalnego uzyskiwania dostępu, na przykład program VNC;
- oprogramowanie straszące (scareware), które zaprojektowano w celu przestraszenia użytkownika i nakłonienia go do zakupu fałszywego oprogramowania zabezpieczającego;
- oprogramowanie używane w celu omijania zabezpieczeń przed kopiowaniem i narzędzi do sprawdzania obecności dysków CD.

Jeśli program ten został wiadomie zainstalowany i prawidłowo skonfigurowany przez użytkownika, prawdopodobnie jego szkodliwe działanie jest mniejsze.

Jeśli ryzykowne oprogramowanie zostało zainstalowane bez wiedzy użytkownika, najprawdopodobniej zostało zainstalowane w złośliwym celu i powinno zostać usunięte.

Ochrona komputera przed złośliwym oprogramowaniem

Tematy:

- *Jak przeskanować komputer*
- *Jak wykluczyć pliki ze skanowania*
- *Jak korzystać z funkcji kwarantanny?*
- *Co to jest technologia DeepGuard?*

Funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego chroni komputer przed programami, które mogą wykraść przechowywane na nim informacje osobiste, uszkodzić go lub użyć w niedozwolonych celach.

Domylnie wszystkie typy złośliwego oprogramowania są przetwarzane natychmiast po wykryciu, uniemożliwiając wyrządzenie jakichkolwiek szkód.

Domylnie skanowanie w poszukiwaniu wirusów automatycznie sprawdza lokalne dyski twarde, nośniki wymienne (takie jak pamięć przenośna, dyski CD/DVD) i pobierane pliki. W zależności od ustawień automatyczne sprawdzanie może obejmować również pocztę e-mail.

Ponadto skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego monitoruje komputer pod kątem zmian, które mogą wskazywać na obecność *złośliwego oprogramowania*. W przypadku wykrycia jakiegokolwiek niebezpiecznej zmiany w systemie, takiej jak modyfikacja ustawień systemowych lub próba manipulowania w nim procesem systemowym, funkcja DeepGuard zatrzymuje określony program, który prawdopodobnie stanowi *złośliwe oprogramowanie*.

Jak przeskanować komputer

Gdy funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego jest włączona, komputer jest automatycznie skanowany w poszukiwaniu szkodliwych plików. Można tak również skanować pliki ręcznie i skonfigurować skanowanie zaplanowane.

Zaleca się, aby funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego była cały czas włączona. Pliki należy skanować ręcznie, aby się upewnić, że na komputerze nie ma szkodliwych plików, lub w celu przeskanowania plików wykluczonych ze skanowania w czasie rzeczywistym.

Po skonfigurowaniu skanowania zaplanowanego funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego usuwa szkodliwe pliki z komputera o ustalonym czasie.

Automatyczne skanowanie plików

Funkcja skanowania w czasie rzeczywistym chroni komputer, skanując wszystkie pliki przy każdej próbie dostępu i blokując dostęp do plików zawierających *złośliwe oprogramowanie*.


Gdy komputer próbuje uzyskać dostęp do pliku, funkcja skanowania w czasie rzeczywistym skanuje ten plik w poszukiwaniu złośliwego oprogramowania, zanim zezwoli komputerowi na dostęp do tego pliku. Jeśli funkcja skanowania w czasie rzeczywistym wykryje jakkolwiek szkodliwą zawartość, umieści dany plik w kwarantannie, zanim spowoduje on szkody.

Czy skanowanie w czasie rzeczywistym ma wpływ na wydajność komputera?

Zazwyczaj użytkownik nie dostrzega procesu skanowania, ponieważ trwa on krótko i nie korzysta z wielu zasobów systemowych. Ilość czasu i zasobów systemowych wykorzystywanych podczas skanowania w czasie rzeczywistym zależy między innymi od zawartości, lokalizacji oraz typu pliku.

Pliki, których skanowanie trwa dłużej:

- Pliki na nośnikach wymiennych, takich jak dyski CD i DVD oraz przenośne dyski USB.
- Pliki skompresowane, takie jak archiwa *zip*.

 **Informacje:** Domyślnie pliki skompresowane nie są skanowane.

Skanowanie w czasie rzeczywistym może spowolnić pracę komputera w następujących przypadkach:

- Komputer użytkownika nie spełnia wymagań systemowych.
- Użytkownik uzyskuje dostęp do wielu plików jednocześnie, na przykład podczas otwierania katalogu zawierającego wiele plików, które należy przeskanować.

Włączenie lub wyłączenie skanowania w czasie rzeczywistym

Aby powstrzymać *złośliwe oprogramowanie*, zanim zdoła ono wyrządzić szkody na komputerze, skanowanie w czasie rzeczywistym powinno być zawsze włączone.

Aby włączyć lub wyłączyć skanowanie w czasie rzeczywistym, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Stan**.
2. Kliknij pozycję **Zmień ustawienia na tej stronie**.

 **Informacje:** Do wyłączenia funkcji zabezpieczeń wymagane są uprawnienia administratora.


3. Włącz lub wyłącz opcję **Skanowanie w poszukiwaniu wirusów**.
4. Kliknij przycisk **Zamknij**.

Automatyczne przetwarzanie szkodliwych plików

Funkcja skanowania w czasie rzeczywistym może przetwarzać szkodliwe pliki automatycznie bez wywołania zapytania.

Aby funkcja skanowania w czasie rzeczywistym przetwarzała szkodliwe pliki automatycznie, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**.
3. Wybierz opcję **Przetwarzaj szkodliwe pliki automatycznie**.

Jeśli użytkownik wybierze opcję, aby szkodliwe pliki nie były przetwarzane automatycznie, funkcja skanowania w czasie rzeczywistym będzie wywoływać pytanie o czynności, jaka ma zostać wykonana dla wykrycia szkodliwego pliku.

Przetwarzanie oprogramowania szpiegującego

Funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego natychmiast blokuje oprogramowanie szpiegujące przy próbie uruchomienia.

Zanim aplikacja szpiegująca zostanie uruchomiona, produkt blokuje ją i pozwala użytkownikowi wybrać, co z nią zrobić.

Po wykryciu oprogramowania szpiegującego należy wybrać jedną z następujących czynności:

Czynność do wykonania	Co dzieje się z oprogramowaniem szpiegującym
Przetwórz automatycznie	Pozwól programowi wybrać najlepsze działanie w zależności od wykrytego oprogramowania szpiegującego.
Poddawaj oprogramowanie szpiegujące kwarantannie	Przenieś oprogramowanie szpiegujące do kwarantanny, skąd nie może uszkodzić komputera.
Usuń oprogramowanie szpiegujące	Usuń wszystkie pliki związane z oprogramowaniem szpiegującym z komputera.
Tylko zablokuj oprogramowanie szpiegujące	Zablokuj dostęp do oprogramowania szpiegującego, ale pozostaw je na komputerze.
Wyklucz oprogramowanie szpiegujące ze skanowania	Zezwól na uruchomienie oprogramowania szpiegującego i wyklucz je ze skanowania w przyszłości.

Przetwarzanie ryzykownego oprogramowania

Funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego natychmiast blokuje ryzykowne oprogramowanie przy próbie uruchomienia.

Zanim ryzykowna aplikacja zostanie uruchomiona, produkt blokuje ją i pozwala użytkownikowi wybrać, co z nią zrobić.

Po wykryciu ryzykownego oprogramowania należy wybrać jedną z następujących czynności:

Czynność do wykonania	Co dzieje się z ryzykownym oprogramowaniem
Tylko zablokuj ryzykowne oprogramowanie	Zablokuj dostęp do ryzykownego oprogramowania, ale pozostaw je na komputerze.
Poddawaj ryzykowne oprogramowanie kwarantannie	Przenieś ryzykowne oprogramowanie do kwarantanny, skąd nie może uszkodzić komputera.


Czynno do wykonania	Co dzieje si z ryzykownym oprogramowaniem
Usu ryzykowne oprogramowanie	Usu wszystkie pliki zwi zane z ryzykownym oprogramowaniem z komputera.
Wyklucz ryzykowne oprogramowanie ze skanowania	Zezwól na uruchomienie ryzykownego oprogramowania i wyklucz je ze skanowania w przyszło ci.

Automatyczne usuwanie ledz cych plików cookie

Usuwa c ledz ce pliki cookie, mo na powstrzyma wityrny internetowe przed monitorowaniem stron odwiedzanych w Internecie.

ledz ce pliki cookie to małe pliki, które umo liwiaj wityrnom rejestrowanie stron odwiedzanych przez u ytkownika. Aby ledz ce pliki cookie nie były przechowywane na komputerze, wykonaj poni sze instrukcje.

1. Na stronie głównej kliknij opcj **Ustawienia**.

 **Informacje:** Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**.
3. Wybierz opcj **Usu ledz ce pliki cookie**.
4. Kliknij przycisk **OK**.

R czne skanowanie plików

Pliki mo na skanowa r cznie, na przykład po podł czeniu do komputera urz dzenia zewn trznego, aby upewni si , e nie zawiera ono zło liwego oprogramowania.

Uruchamianie skanowania r cznego

Skanowanie mo e obejmowa cały komputer lub dotyczy tylko okre lonego typu *zło liwego oprogramowania* lub okre lonej lokalizacji.

W razie podejrzenia istnienia okre lonego typu *zło liwego oprogramowania* mo na przeprowadzi skanowanie tylko w poszukiwaniu tego typu. Je li podejrzenie dotyczy tylko okre lonej lokalizacji na komputerze, mo na przeprowadzi skanowanie tylko w tej sekcji. Takie skanowanie b dzie trwa znacznie krócej ni skanowanie całego komputera.

Aby uruchomi skanowanie r czne komputera, wykonaj nast puj ce czynno ci:

1. Na stronie głównej kliknij strzałk w dół obok przycisku **Skanuj**.
Zostan wy wietlone opcje skanowania.
2. Wybierz typ skanowania.
Wybierz opcj **Zmie ustawienia skanowania**, aby zoptymalizowa sposób r cznego skanowania komputera w poszukiwaniu wirusów i innych szkodliwych aplikacji.
3. W przypadku wybrania opcji **Wybierz obiekty do skanowania** zostanie wy wietlone okno umo liwiaj ce okre lenie lokalizacji do przeskanowania.
Zostanie otwarty **Kreator skanowania**.

Typy skanowania

Skanowanie mo e obejmowa cały komputer lub dotyczy tylko okre lonego typu *zło liwego oprogramowania* albo okre lonej lokalizacji.

Poni ej wymieniono ró ne typy skanowania:

Typ skanowania	Skanowane elementy	Zalecane użycie
Skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego	Określone obszary komputera w poszukiwaniu wirusów, oprogramowania szpiegującego i ryzykownego oprogramowania	Skanowanie tego typu jest dużo szybsze niż pełne skanowanie. Przeszukiwane są tylko obszary systemu zawierające zainstalowane pliki programów. Skanowanie tego typu jest zalecane, gdy trzeba szybko sprawdzić, czy komputer nie jest zainfekowany, ponieważ umożliwia ono wydajne wyszukiwanie i usuwanie wszelkiego aktywnego złośliwego oprogramowania znajdującego się na komputerze.
Pełne skanowanie komputera	Cały komputer (wewnętrzne i zewnętrzne dyski twarde) w poszukiwaniu wirusów, oprogramowania szpiegującego i ryzykownego oprogramowania	W celu uzyskania całkowitej pewności, że na komputerze nie ma złośliwego oprogramowania ani ryzykownego oprogramowania. Skanowanie tego typu zajmuje najwięcej czasu. Stanowi połączenie funkcji szybkiego skanowania w poszukiwaniu złośliwego oprogramowania i funkcji skanowania dysku twardego. Ta funkcja przeprowadza również sprawdzanie pod kątem plików ukrytych przez programy typu „rootkit”.
Wybierz elementy do przeskanowania	Określony plik, folder lub dysk w poszukiwaniu wirusów, oprogramowania szpiegującego i ryzykownego oprogramowania	W przypadku podejrzenia, że określona lokalizacja na komputerze zawiera złośliwe oprogramowanie. Na przykład miejsce zapisywania plików pobieranych z potencjalnie niebezpiecznych źródeł, takich jak sieci udostępniania plików typu „peer-to-peer”. Czas potrzebny na przeprowadzenie skanowania zależy od wielkości skanowanego obiektu docelowego. Skanowanie trwa krótko, jeżeli na przykład wybrano folder zawierający tylko kilka małych plików.
Skanowanie w poszukiwaniu programów rootkit	Ważne lokalizacje systemowe, w których podejrzany element może oznaczać problem związany z zabezpieczeniami. Przeprowadzane jest skanowanie w poszukiwaniu ukrytych plików, folderów, dysków i procesów.	W przypadku podejrzenia, że na komputerze może być zainstalowany program typu rootkit, jeżeli na przykład wykryto ostatnio na komputerze złośliwe oprogramowanie i trzeba się upewnić, że nie zainstalowało ono programu typu rootkit.

Skanowanie w Eksploratorze Windows

Skanowanie dysków, folderów i plików w poszukiwaniu *wirusów, oprogramowania szpiegującego i ryzykownego oprogramowania* można wykonywać w Eksploratorze Windows.

Aby przeskanować dysk, folder lub plik:


1. Umieść kursor myszy na dysku, folderze lub pliku, który chcesz przeskanować, a następnie kliknij go prawym przyciskiem myszy.
2. W wyświetlonym menu wybierz polecenie **Skanuj foldery w poszukiwaniu wirusów**. Nazwa tej opcji różni się w zależności od tego, czy skanowany jest dysk, folder czy plik.
Zostanie otwarte okno **Kreator skanowania** i rozpocznie się skanowanie.

W przypadku znalezienia *wirusa* lub *oprogramowania szpiegującego* **Kreator skanowania** przeprowadzi użytkownika przez proces oczyszczania.

Wybieranie plików do skanowania

Użytkownik może wybrać typy plików, które mają być skanowane w poszukiwaniu *wirusów* i *oprogramowania szpiegującego* podczas skanowania ręcznego i zaplanowanego.

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie ręczne**.

3. W obszarze **Opcje skanowania** określ następujące ustawienia:

Skanuj tylko znane typy plików


Skanowanie tylko plików, w przypadku których istnieje największe prawdopodobieństwo infekcji, na przykład plików wykonywalnych. Wybranie tej opcji zapewnia szybsze skanowanie. Takie skanowanie obejmuje pliki z następującymi rozszerzeniami: ani, asp, ax, bat, bin, boo, chm, cmd, com, cpl, dll, doc, dot, drv, eml, exe, hlp, hta, html, http, inf, ini, job, js, jse, lnk, lsp, mdb, mht, mpp, mpt, msg, ocx, pdf, php, pif, pot, ppt, rtf, scr, shs, swf, sys, tld, vbe, vbs, vxd, wbk, wma, wmv, wmf, wsc, wsf, wsh, wri, xls, xlt, xml, zip, jar, arj, lzh, tar, tgz, gz, cab, rar, bz2 oraz hqx.

Skanuj wewnątrz plików skompresowanych


Skanowanie zarchiwizowanych plików i folderów.

Użyj zaawansowanej heurystyki

Podczas skanowania zostaną użyte wszystkie dostępne zasoby heurystyki w celu skuteczniejszego wykrywania nowego i nieznanego złośliwego oprogramowania.

 **Informacje:** Zaznaczenie tej opcji wydłuży czas skanowania i może powodować zwiększenie liczby zgłoszeń programów niepoprawnie uznanych za niebezpieczne (nieszkodliwych plików zgłoszonych jako podejrzane).

4. Kliknij przycisk **OK**.


 **Informacje:** Wykluczone pliki z listy wykluczonych obiektów nie są skanowane, nawet jeśli zostaną tutaj wybrane do skanowania.

Co zrobić w przypadku wykrycia szkodliwych plików

Sposób postępowania z wykrytymi szkodliwymi plikami można wybrać.

Aby wybrać czynność, która ma zostać wykonana w przypadku wykrycia szkodliwej zawartości podczas skanowania ręcznego:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie ręczne**.



3. W sekcji **W przypadku wykrycia wirusa lub oprogramowania szpiegującego** wybierz odpowiednią opcję:

Opcja

Opis

Zapytaj (domyślnie)

Użytkownik może wybrać czynność, która ma zostać wykonana w przypadku każdego elementu wykrytego podczas skanowania ręcznego.

Opcja	Opis
Wyczyść pliki	<p>Produkt próbuje automatycznie usunąć zainfekowane pliki wykryte podczas skanowania ręcznego.</p> <p> Informacje: Jeśli produkt nie może usunąć zainfekowanego pliku, jest on poddawany kwarantannie (chyba że plik znajduje się w sieci lub na dysku przenośnym), aby uszkodzenie komputera było niemożliwe.</p>
Poddawaj pliki kwarantannie	Produkt przenosi szkodliwe pliki wykryte podczas skanowania ręcznego do kwarantanny, uniemożliwiając uszkodzenie komputera.
Usuń pliki	Produkt usuwa każdy szkodliwy plik wykryty podczas skanowania ręcznego.
Tylko zgłoś	<p>Produkt pozostawia bez zmian każdy szkodliwy plik wykryty podczas skanowania ręcznego i rejestruje to wykrycie w raporcie skanowania.</p> <p> Informacje: W przypadku gdy skanowanie w czasie rzeczywistym jest wyłączone, złośliwe oprogramowanie może nadal uszkodzić komputer, jeśli zostanie wybrana ta opcja.</p>


 **Informacje:** Szkodliwe pliki wykryte podczas skanowania zaplanowanego są automatycznie usuwane.

Planowanie skanowania

Możesz skonfigurować automatyczne skanowanie komputera w poszukiwaniu wirusów i innych szkodliwych aplikacji i usuwanie ich, gdy komputer nie jest używany, lub okresowe uruchamianie skanowania, aby mieć pewność, że komputer nie jest zainfekowany.

Aby zaplanować skanowanie:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie zaplanowane**.
3. Włącz opcję **Skanowanie zaplanowane**.
4. Wybierz czas rozpoczęcia skanowania.

Opcja	Opis
Codziennie	Komputer będzie skanowany codziennie.
Co tydzień	Komputer będzie skanowany w wybrane dni tygodnia. Wybierz dni z listy.
Co miesiąc	<p>Komputer będzie skanowany w wybrane dni miesiąca. Aby wybrać dni:</p> <ol style="list-style-type: none"> 1. Wybierz jedną z opcji Dzień. 2. Wybierz dzień miesiąca z listy znajdującej się obok wybranego dnia.

5. Określ czas rozpoczęcia skanowania w wybrane dni.

Opcja	Opis
Godzina rozpoczęcia	Skanowanie będzie uruchamiane o określonej godzinie.
Jeśli komputer nie jest używany przez	Skanowanie będzie uruchamiane, jeśli komputer nie będzie używany przez określony czas.

Podczas skanowania zaplanowanego komputera są używane ustawienia skanowania ręcznego, archiwa są skanowane za każdym razem i szkodliwe pliki są usuwane automatycznie.


Skanowanie poczty e-mail

Skanowanie poczty e-mail chroni przed otrzymywaniem szkodliwych plików w wiadomościach e-mail wysyłanych do użytkownika.

Aby skanować pocztę e-mail w poszukiwaniu wirusów, należy włączyć funkcję skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego.

Aby włączyć skanowanie poczty e-mail:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.


2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**.
3. Wybierz opcję **Usuń szkodliwe załączniki wiadomości e-mail**.
4. Kliknij przycisk **OK**.

Kiedy są skanowane wiadomości e-mail i załączniki?

Skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego usuwa szkodliwe obiekty z otrzymywanych wiadomości e-mail.

Skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego usuwa szkodliwe wiadomości e-mail otrzymywane w programach do obsługi poczty e-mail, takich jak Microsoft Outlook, Outlook Express, Microsoft Mail i Mozilla Thunderbird. Ta funkcja skanuje niezaszyfrowane wiadomości e-mail i załączniki za każdym razem, gdy program otrzymuje je z serwera pocztowego korzystającego z protokołu POP3.

Funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpiegującego nie może skanować wiadomości e-mail w poczcie internetowej, obejmującej aplikacje poczty e-mail działające w przeglądarce internetowej, takie jak Hotmail, Yahoo! Mail lub Gmail. Komputer jest nadal chroniony przed *wirusami*, nawet jeśli szkodliwe załączniki nie zostały usunięte lub używana jest poczta internetowa. Podczas otwierania załączników wiadomości e-mail skanowanie w czasie rzeczywistym usuwa wszystkie szkodliwe załączniki, zanim zdążą wyrządzić jakiegokolwiek szkody.

 **Informacje:** Skanowanie w czasie rzeczywistym chroni tylko komputer użytkownika, a nie komputery jego znajomych. Przeskanowanie załączonych plików może zostać przeprowadzone dopiero po ich otwarciu. Oznacza to, że używając poczty internetowej i przekazując dalej wiadomości zawierające nieotwarte załączniki, można rozsyłać zainfekowane wiadomości e-mail.


Wyświetlanie wyników skanowania

W oknie Historia wirusów i oprogramowania szpiegującego są wyświetlane informacje o wszystkich szkodliwych plikach wykrytych przez produkt.

Czasami po wykryciu szkodliwego obiektu produkt nie może wykonać akcji wybranej przez użytkownika. Jeśli na przykład zostanie wybrana opcja wyczyszczenia plików, a plików nie można wyczyścić, produkt przeniesie je do kwarantanny. Ta informacja może być wyświetlona w historii wirusów i oprogramowania szpiegującego.

Aby wyświetlić historię:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.


2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**.
3. Kliknij opcję **Wyświetl historię usuwania**.

W historii wirusów i oprogramowania szpieguj cego s wy wietlane nast puj ce informacje:

- data i godzina wykrycia szkodliwego pliku,
- nazwa zło liwego oprogramowania i jego lokalizacja na komputerze,
- wykonana akcja.

Jak wykluczy pliki ze skanowania

Czasami trzeba wykluczy niektóre pliki lub aplikacje ze skanowania. Wykluczone elementy nie s skanowane, dopóki nie zostaną usunięte z listy wykluczonych elementów.


-  **Informacje:** Istnieją osobne listy wykluczeń dla skanowania rzeczywistego i skanowania w czasie rzeczywistym. Jeśli na przykład plik zostanie wykluczony ze skanowania w czasie rzeczywistym, jest on skanowany podczas skanowania rzeczywistego, chyba że zostanie on też wykluczony ze skanowania rzeczywistego.

Wykluczanie typów plików

Po wykluczeniu plików według ich typu pliki z określonymi rozszerzeniami nie s skanowane w poszukiwaniu szkodliwej zawartości.

Aby dodać lub usunąć typ pliku, który ma zostać wykluczony, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz, czy chcesz wykluczyć typ pliku ze skanowania w czasie rzeczywistym, czy skanowania rzeczywistego:

- Wybierz kolejno pozycje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**, aby wykluczyć typ plików ze skanowania w czasie rzeczywistym.
- Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie rzeczywiste**, aby wykluczyć typ plików ze skanowania rzeczywistego.

3. Kliknij opcję **Wyklucz pliki ze skanowania**.

4. Aby wykluczyć typ pliku:

- a) Wybierz kartę **Typy plików**.
- b) Wybierz opcję **Wyklucz pliki z tymi rozszerzeniami**.
- c) W polu obok przycisku **Dodaj** wpisz rozszerzenie pliku określające typ plików, które chcesz wykluczyć. Aby uwzględnić pliki, które nie mają rozszerzenia, należy użyć znaku „.”. Można też zastosować symbol wieloznaczny „?” reprezentujący dowolny znak lub „*” reprezentujący dowolną liczbę znaków. Aby na przykład wykluczyć pliki wykonywalne, wpisz w tym polu wartość `exe`.
- d) Kliknij przycisk **Dodaj**.

5. Powtórz poprzedni krok dla każdego rozszerzenia, które ma zostać wykluczone ze skanowania w poszukiwaniu wirusów.

6. Kliknij przycisk **OK**, aby zamknąć okno dialogowe **Wykluczanie ze skanowania**.

7. Kliknij przycisk **OK**, aby zastosować nowe ustawienia.


Wybrane typy plików nie będą uwzględniane podczas skanowania przeprowadzanego w przyszłości.

Wykluczanie plików według lokalizacji

Po wykluczeniu plików według lokalizacji pliki znajdują się na określonych dyskach lub w określonych folderach i nie s skanowane w poszukiwaniu szkodliwej zawartości.

Aby dodać lub usunąć lokalizacje plików, które mają zostać wykluczone, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.


2. Wybierz, czy chcesz wykluczyć lokalizację ze skanowania w czasie rzeczywistym, czy skanowania ręcznego:

- Aby wykluczyć lokalizację ze skanowania w czasie rzeczywistym, wybierz kolejno opcje **Komputer** > **Skanowanie w poszukiwaniu wirusów**.
- Aby wykluczyć lokalizację ze skanowania ręcznego, wybierz kolejno opcje **Komputer** > **Skanowanie ręczne**.

3. Kliknij opcję **Wyklucz pliki ze skanowania**.

4. Aby wykluczyć plik, dysk lub folder:

- a) Wybierz kartę **Obiekty**.
- b) Wybierz opcję **Wyklucz obiekty (pliki, foldery itd.)**.
- c) Kliknij przycisk **Dodaj**.
- d) Wybierz plik, folder lub dysk, który chcesz wykluczyć ze skanowania antywirusowego.

 **Informacje:** Niektóre dyski mogą być wymienne, na przykład dyski CD lub DVD i dyski sieciowe. Nie można wykluczyć dysków sieciowych i pustych dysków wymiennych.

- e) Kliknij przycisk **OK**.

5. Powtórz poprzedni krok w celu wykluczenia innych plików, folderów lub dysków ze skanowania antywirusowego.

6. Kliknij przycisk **OK**, aby zamknąć okno dialogowe **Wykluczanie ze skanowania**.


7. Kliknij przycisk **OK**, aby zastosować nowe ustawienia.

Wybrane pliki, dyski i foldery nie będą uwzględniane podczas skanowania przeprowadzanego w przyszłości.

Wyświetlanie aplikacji wykluczonych

Aplikacje wykluczone ze skanowania można wyświetlić i usunąć z listy elementów wykluczonych, aby w przyszłości nie były uwzględniane podczas skanowania.


Jeśli funkcja skanowania w czasie rzeczywistym lub skanowania ręcznego wykryje aplikację, która zachowuje się jak oprogramowanie szpiegujące lub ryzykowne, ale użytkownik wie, że jest ona bezpieczna, można ją wykluczyć ze skanowania, aby produkt nie wyświetlał jej ostrzeżeń dotyczących tej aplikacji.

 **Informacje:** Jeśli aplikacja zachowuje się jak wirus lub inne złośliwe oprogramowanie, nie można jej wykluczyć.

Aplikacji nie można wykluczyć bezpośrednio. Nowe aplikacje są dodawane do listy wykluczonej tylko wtedy, gdy zostaną wykluczone podczas skanowania.

Aby wyświetlić aplikacje wykluczone ze skanowania:

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz, czy chcesz wyświetlić aplikacje wykluczone ze skanowania w czasie rzeczywistym, czy skanowania ręcznego:

- Aby wyświetlić aplikacje wykluczone ze skanowania w czasie rzeczywistym, wybierz kolejno opcje **Komputer** > **Skanowanie w poszukiwaniu wirusów**.
- Aby wyświetlić aplikacje wykluczone ze skanowania ręcznego, wybierz kolejno opcje **Komputer** > **Skanowanie ręczne**.

3. Kliknij opcję **Wyklucz pliki ze skanowania**.

4. Wybierz kartę **Aplikacje**.



Informacje: Ze skanowania można wyłączyć tylko oprogramowanie szpiegujące i ryzykowne, nie wirusy.

5. Aby ponownie przeskanować wykluczone aplikacje, wykonaj następujące czynności:

- a) Wybierz aplikację, którą chcesz uwzględnić podczas skanowania.
- b) Kliknij przycisk **Usuń**.

6. Kliknij przycisk **OK**, aby zamknąć okno dialogowe **Wykluczanie ze skanowania**.

7. Kliknij przycisk **OK**, aby zamknąć okno.

Jak korzystać z funkcji kwarantanny?

Kwarantanna to bezpieczne repozytorium dla plików, które mogą być szkodliwe.

Pliki poddane kwarantannie nie mogą się rozprzestrzeniać ani powodować uszkodzenia komputera.

Kwarantannie można poddać *złośliwe oprogramowanie*, *oprogramowanie szpiegujące* oraz *ryzykowne oprogramowanie* w celu ich unieszkodliwienia. W razie potrzeby aplikacje i pliki można później przywrócić z kwarantanny.

Jeśli element poddany kwarantannie nie jest potrzebny, można go usunąć. Usunięcie elementu z kwarantanny powoduje jego trwałe usunięcie z komputera.

- Zazwyczaj użytkownik może usuwać *złośliwe oprogramowanie* poddane kwarantannie.
- W niektórych przypadkach użytkownik może usunąć *oprogramowanie szpiegujące* poddane kwarantannie. Zdarza się, że *oprogramowanie szpiegujące* poddane kwarantannie to część nieszkodliwego programu i po usunięciu tego programu ten przestaje działać poprawnie. Jeśli użytkownik chce zachować program na komputerze, może przywrócić *oprogramowanie szpiegujące* z kwarantanny.
- *Ryzykowne oprogramowanie* poddane kwarantannie może być nieszkodliwym programem. Jeśli użytkownik sam zainstalował i skonfigurował ten program, może go przywrócić z kwarantanny. Jeśli *ryzykowne oprogramowanie* zostało zainstalowane bez wiedzy użytkownika, najprawdopodobniej zostało zainstalowane w złośliwym celu i powinno zostać usunięte.

Wyświetlanie elementów poddanych kwarantannie

Na temat elementów poddanych kwarantannie można wyświetlać więcej informacji.

Aby wyświetlić szczegółowe informacje na temat elementów poddanych kwarantannie:

1. Na stronie głównej kliknij opcję **Ustawienia**.



Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**.


3. Kliknij opcję **Wyświetl kwarantannę**.

Na stronie **Kwarantanna** dostępne są informacje o łącznej liczbie elementów w kwarantannie.

4. Aby wyświetlić szczegółowe informacje na temat elementów poddanych kwarantannie, kliknij przycisk **Szczegóły**.

Zawartość strony można sortować według nazwy złośliwego oprogramowania lub daty pliku.

Na liście wyświetlanych jest 100 pierwszych elementów wraz z informacjami o typach elementów poddanych kwarantannie, ich nazwach i datach instalacji plików.

5. Aby wyświetlić dodatkowe informacje na temat obiektu poddanego kwarantannie, kliknij ikonę  obok wybranego obiektu w kolumnie **Stan**.


Przywracanie elementów poddanych kwarantannie

Potrzebne elementy można przywrócić z kwarantanny.

Jeśli aplikacje lub pliki poddane kwarantannie są potrzebne, można je przywrócić. Nie należy przywracać żadnych elementów poddanych kwarantannie, jeśli nie ma pewności, że nie stanowi one zagrożenia. Przywrócone elementy są przenoszone z powrotem do oryginalnej lokalizacji na komputerze.

Przywracanie elementów poddanych kwarantannie

1. Na stronie głównej kliknij opcję **Ustawienia**.

 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**.
3. Kliknij opcję **Wyświetl kwarantannę**.
4. Zaznacz elementy w kwarantannie do przywrócenia.
5. Kliknij pozycję **Przywróć**.

Co to jest technologia DeepGuard?

Technologia DeepGuard analizuje zawartość plików i działanie aplikacji, a także monitoruje niezaufane programy.

Technologia DeepGuard blokuje nowe i dotychczas niewykryte wirusy, robaki i inne szkodliwe aplikacje, które próbują wprowadzać zmiany na komputerze, a także uniemożliwia podejrzanym aplikacjom dostęp do Internetu.

W przypadku wykrycia przez technologię DeepGuard nowej aplikacji, która próbuje wprowadzić w systemie potencjalnie szkodliwe zmiany, taka aplikacja zostaje uruchomiona w bezpiecznej strefie. W bezpiecznej strefie aplikacja nie może uszkodzić komputera. Technologia DeepGuard analizuje zmiany, które aplikacja próbuje wprowadzić, i na tej podstawie określa prawdopodobieństwo, czy ta aplikacja to *złośliwe oprogramowanie*. Jeśli aplikacja jest prawdopodobnie *złośliwym oprogramowaniem*, technologia DeepGuard blokuje ją.

Potencjalnie szkodliwe zmiany w systemie, które są wykrywane przez technologię DeepGuard, obejmują:

- zmiany ustawień systemu (rejestr systemu Windows);
- próby wyłączenia ważnych programów systemowych, na przykład programów zabezpieczających, takich jak niniejszy produkt;
- próby edytowania ważnych plików systemowych.

Wyłączanie i włączanie funkcji DeepGuard

Aby uniemożliwić podejrzanym aplikacjom wprowadzanie potencjalnie szkodliwych zmian w systemie komputera, należy mieć włączoną funkcję DeepGuard.

W przypadku komputera z systemem Windows XP przed włączeniem technologii DeepGuard należy upewnić się, że dodatek Service Pack 2 został zainstalowany.

Aby włączyć lub wyłączyć funkcję DeepGuard, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Stan**.
2. Kliknij pozycję **Zmień ustawienia na tej stronie**.

 **Informacje:** Do wyłączenia funkcji zabezpieczeń wymagane są uprawnienia administratora.

3. Włóż lub wyłącz opcję **DeepGuard**.
4. Kliknij przycisk **Zamknij**.


Zezwalanie na aplikacje zablokowane przez funkcję DeepGuard

Aplikacje akceptowane i blokowane przez funkcję DeepGuard można kontrolować.

Zdarza się, że funkcja DeepGuard blokuje uruchomienie aplikacji, z której użytkownik chce skorzystać i o której wie, że jest bezpieczna. Dzieje się tak, ponieważ aplikacja próbuje wprowadzić potencjalnie szkodliwe zmiany w systemie. Może się też zdarzyć, że aplikacja zostanie przypadkowo zablokowana przez użytkownika po wyświetleniu okna podręcznej funkcji DeepGuard.

Aby zezwolić na działanie aplikacji zablokowanej przez funkcję DeepGuard, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Narzędzia**.
2. Kliknij pozycję **Aplikacje**.
Zostanie wyświetlona lista **Aplikacje monitorowane**.
3. Znajdź aplikację, na uruchomienie której chcesz zezwolić.

 **Informacje:** Klikając nagłówki kolumn, możesz sortować listę. Aby na przykład posortować listę według grup dozwolonych i zablokowanych programów, kliknij kolumnę **Uprawnienie**.


4. Wybierz opcję **Zezwalaj** w kolumnie **Uprawnienie**.
5. Kliknij przycisk **Zamknij**.

Funkcja DeepGuard umożliwia aplikacji ponowne wprowadzanie zmian w systemie.

Ustawianie funkcji DeepGuard w trybie zgodności

W celu zapewnienia maksymalnej ochrony funkcja DeepGuard tymczasowo modyfikuje uruchomione programy. Niektóre programy sprawdzają, czy nie zostały uszkodzone lub zmodyfikowane, i mogą nie być zgodne z tą funkcją. Na przykład gry internetowe zawierające narzędzia zapobiegające oszukiwaniu po uruchomieniu stale sprawdzają, czy nie zostały w jakikolwiek sposób zmodyfikowane. W takich przypadkach można włączyć tryb zgodności.

Aby włączyć tryb zgodności, wykonaj następujące czynności:

1. Na stronie głównej kliknij opcję **Ustawienia**.
 **Informacje:** Do zmiany tych ustawień wymagane są uprawnienia administratora.
2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **DeepGuard**.
3. Wybierz opcję **Użyj trybu zgodności**.
4. Kliknij przycisk **OK**.

Co robi w przypadku ostrzeżenia o podejrzanym działaniu

Funkcja DeepGuard monitoruje niezaufane aplikacje. Jeśli taka aplikacja podejmie próbę uzyskania dostępu do Internetu, wprowadzenia zmian w systemie lub wykonania podejrzanego działania, funkcja DeepGuard blokuje ją.

Jeśli w ustawieniach funkcji DeepGuard wybrano opcję **Ostrzegaj o podejrzanym działaniu**, funkcja DeepGuard wyświetla powiadomienie, gdy wykryje potencjalnie szkodliwą aplikację lub gdy zostanie uruchomiona aplikacja o nieznanym reputacji.

Aby wybrać czynność, która ma zostać wykonana w przypadku aplikacji zablokowanej przez funkcję DeepGuard, wykonaj następujące czynności:

1. Kliknij opcję **Szczegóły**, aby wyświetlić więcej informacji o danym programie.

W sekcji szczegółów są wyświetlane następujące dane:

- lokalizacja aplikacji,
- reputacja aplikacji w sieci ochrony w czasie rzeczywistym,
- stopień powszechności aplikacji.

2. Wybierz, czy aplikacja zablokowana przez funkcję DeepGuard jest zaufana:

- Wybierz opcję **Ta aplikacja jest zaufana — kontynuuj**, jeśli nie chcesz blokować aplikacji.

Aplikacja jest prawdopodobnie bezpieczna, jeśli:

- funkcja DeepGuard zablokowała tę aplikację w wyniku czynności wykonanej przez użytkownika,
- użytkownik rozpoznał aplikację,
- aplikacja pochodzi z zaufanego źródła.

- Wybierz opcję **Ta aplikacja nie jest zaufana. Zablokuj**, jeśli aplikacja ma pozostać zablokowana.

Aplikacja jest prawdopodobnie niebezpieczna, jeśli:

- aplikacja nie jest powszechna,
- aplikacja ma nieznaną reputację,
- użytkownik nie zna aplikacji.

3. Jeśli chcesz przesłać podejrzaną aplikację do analizy:

a) Kliknij opcję **Zgłoś tę aplikację w firmie F-Secure**.

Produkt wyświetli warunki dotyczące przesłania próbki.

b) Kliknij przycisk **Akceptuj**, jeśli akceptujesz warunki i chcesz przesłać próbkę.

Wysyłanie próbki jest zalecane, gdy:

- funkcja DeepGuard zablokuje aplikację, którą użytkownik uważa za bezpieczną;
- istnieje podejrzenie, że aplikacja może być *złośliwym oprogramowaniem*.