F-Secure Anti-Virus 2013

Spis tre ci

Rozdział 1: Instalacja.....5

Przed pierwsz instalacj 6
Instalowanie produktu po raz pierwszy.....6
Instalowanie i uaktualnianie aplikacji.....6
Pomoc i wsparcie techniczne.....7

Rozdział 2: Rozpoczynanie pracy.....9

Jak korzysta z aktualizacji automatycznych.....10
Sprawdzanie stanu aktualizacji.....10
Zmienianie ustawie poł czenia internetowego.....10
Sprawdzanie stanu Sieci ochrony w czasie rzeczywistym.....11
Sprawdzanie czynno ci wykonanych przez produkt.....11
Wy wietl histori powiadomie 11
Zmienianie ustawie powiadomie 11
Sie ochrony w czasie rzeczywistym.....12
Co to jest sie ochrony w czasie rzeczywistym.....12
Zalety sieci ochrony w czasie rzeczywistym.....12
Jakie dane s przesyłane.....13
W jaki sposób chronimy Twoj prywatno 14
Doł czanie do sieci ochrony w czasie rzeczywistym.....15
Pytania dotycz ce sieci ochrony w czasie rzeczywistym.....15
Jak sprawdzi , czy subskrypcja jest wa na.....15
Centrum akcji.....16
Aktywowanie subskrypcji.....16

Rozdział 3: Wprowadzenie.....17

Wy wietlanie ogólnego stanu ochrony.....18
Wy wietlanie statystyki produktu.....18
Obsługiwanie aktualizacji produktu.....19
Wy wietl wersje baz danych.....19
Zmienianie ustawie poł cze internetowych na urz dzeniu przeno nym.....19
Co to s wirusy i inne zło liwe oprogramowanie?.....20
Wirusy.....20
Oprogramowanie szpieguj ce.....21
Programy typu rootkit.....21
Ryzykowne oprogramowanie.....21

Rozdział 4: Ochrona komputera przed zło liwym oprogramowaniem.23

Jak przeskanowa komputer.....24
Automatyczne skanowanie plików.....24
R czne skanowanie plików.....26
Skanowanie poczty e-mail.....30
Wy wietlanie wyników skanowania.....30
Jak wykluczy pliki ze skanowania.....31
Wykluczanie typów plików.....31
Wykluczanie plików według lokalizacji.....31
Wy wietlanie aplikacji wykluczonych.....32
Jak korzysta z funkcji kwarantanny?.....33
Wy wietlanie elementów poddanych kwarantannie.....33
Przywracanie elementów poddanych kwarantannie.....34
Co to jest technologia DeepGuard?.....34
Wł czanie i wył czanie funkcji DeepGuard.....34
Zezwalanie na aplikacje zablokowane przez funkcj DeepGuard.....35
U ywanie funkcji DeepGuard w trybie zgodno ci.....35
Co robi w przypadku ostrze e o podejrzanych działaniach.....35

Rozdział

1

Instalacja

Tematy:

- *Przed pierwsz instalacj*
- *Instalowanie produktu po raz pierwszy*
- *Instalowanie i uaktualnianie aplikacji*
- *Pomoc i wsparcie techniczne*

Przed pierwsz instalacj

Dzi kujemy za wybranie produktu firmy F-Secure.

Do zainstalowania tego produktu potrzebne s nast puj ce składniki:

- Instalacyjny dysk CD lub pakiet. W przypadku u ywania komputera przeno nego bez stacji dysków CD mo na pobra pakiet instalacyjny z witryny *www.f-secure.com/netbook*.
- Klucz subskrypcji.
- Poł czenie internetowe.

Je li na komputerze jest ju zainstalowany produkt zabezpieczaj cy innego producenta, instalator podejmie prób automatycznego usuni cia tego produktu. Je li to usuwanie nie powiedzie si , nale y usun ten produkt r cznie.

Informacje: Je li na komputerze utworzono wi cej ni jedno konto u ytkownika, w celu przeprowadzenia instalacji nale y zalogowa si na koncie z uprawnieniami administratora.

Instalowanie produktu po raz pierwszy

Instrukcje dotycz ce instalowania produktu.

Aby zainstalowa produkt, wykonaj nast puj ce czynno ci:

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

   Je li dysk CD nie zostanie uruchomiony automatycznie, otwórz program Eksplorator Windows, kliknij dwukrotnie ikon stacji dysków CD-ROM, a nast pnie kliknij dwukrotnie plik instalacyjny w celu rozpocz cia instalacji.

2. Post puj zgodnie z instrukcjami wy wietlanymi na ekranie.

   - Je li produkt został nabyty na dysku CD w sklepie, klucz subskrypcji mo na znale na okładce przewodnika szybkiej instalacji.
   - Je li produkt został pobrany ze sklepu elektronicznego F-Secure eStore, klucz subskrypcji jest doł czony do wiadomo ci e-mail z potwierdzeniem zamówienia.

   Przed potwierdzeniem subskrypcji i pobraniem najnowszych aktualizacji z Internetu konieczne mo e by ponowne uruchomienie komputera. W przypadku instalowania za pomoc dysku CD pami taj o wyj ciu instalacyjnego dysku CD ze stacji dysków przed ponownym uruchomieniem komputera.

Instalowanie i uaktualnianie aplikacji

Instrukcja dotycz ce aktywowania nowej subskrypcji.

Post puj zgodnie z poni szymi instrukcjami, aby aktywowa now subskrypcj lub zainstalowa now aplikacj za pomoc panelu głównego:

Informacje: Ikona panelu głównego znajduje si na pasku zada systemu Windows.

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
   Zostanie wy wietlone menu podr czne.
2. Wybierz polecenie **Wy wietl moje subskrypcje**.

3. W obszarze **Moje subskrypcje** przejd na stron **Stan subskrypcji** i kliknij opcj **Aktywuj subskrypcj** . Zostanie otwarte okno **Aktywuj subskrypcj** .
4. Wprowad klucz subskrypcji aplikacji i kliknij przycisk **OK**.
5. Gdy subskrypcja zostanie potwierdzona i aktywowana, kliknij przycisk **Zamknij**.
6. W obszarze **Moje subskrypcje** przejd na stron **Stan instalacji**. Je li instalacja nie zostanie rozpocz ta automatycznie, wykonaj nast puj ce czynno ci:
   a) Kliknij przycisk **Zainstaluj**.
      Zostanie otwarte okno instalacji.
   b) Kliknij przycisk **Dalej**.
      Aplikacja zostanie pobrana, a nast pnie rozpocznie si instalacja.
   c) Po uko czeniu instalacji kliknij przycisk **Zamknij**.

Nowa subskrypcja została aktywowana.

Pomoc i wsparcie techniczne

W celu uzyskania dost pu do pomocy dla produktu online mo na klikn ikon Pomoc lub nacisn klawisz F1 na dowolnym ekranie produktu.

Zarejestrowanie licencji uprawnia u ytkownika do korzystania z dodatkowych usług, takich jak bezpłatne aktualizacje produktu i pomoc techniczna. Rejestracj mo na przeprowadzi pod adresem *www.f-secure.com/register*.

Rozdział

2

Rozpoczynanie pracy

Tematy:

- *Jak korzysta z aktualizacji automatycznych*
- *Sprawdzanie czynno ci wykonanych przez produkt*
- *Sie ochrony w czasie rzeczywistym*
- *Jak sprawdzi , czy subskrypcja jest wa na*

Informacje dotycz ce rozpoczynania pracy z produktem.

W tej sekcji opisano sposób zmieniania wspólnych ustawie i zarz dzania subskrypcjami za pomoc panelu głównego.

Wspólne ustawienia w panelu głównym dotycz wszystkich programów zainstalowanych w tym panelu. Zamiast zmienia ustawienia oddzielnie w poszczególnych programach mo esz po prostu edytowa wspólne ustawienia, które s stosowane do wszystkich zainstalowanych programów.

Wspólne ustawienia w panelu głównym obejmuj nast puj ce opcje:

- Pobrane pliki udost pniaj ce informacje o pobranych aktualizacjach i umo liwiaj ce r czne sprawdzanie dost pno ci aktualizacji.
- Ustawienia poł cze słu ce do zmieniania sposobu nawi zywania poł czenia internetowego przez komputer.
- Powiadomienia umo liwiaj ce wy wietlanie wy wietlonych w przeszło ci powiadomie i ustawianie typów wy wietlanych powiadomie .
- Ustawienia prywatno ci, które pozwalaj okre li , czy komputer mo e nawi zywa poł czenie z sieci ochrony w czasie rzeczywistym.

Ponadto za po rednictwem panelu głównego mo esz zarz dza swoimi subskrypcjami dla zainstalowanych programów.

Jak korzysta z aktualizacji automatycznych

Dzi ki aktualizacjom automatycznym mechanizmy ochrony komputera s zawsze aktualne.

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

Sprawdzanie stanu aktualizacji

Mo liwe jest wy wietlenie daty i godziny ostatniej aktualizacji.

Gdy aktualizacje automatyczne s wł czone i jest dost pne poł czenie z Internetem, produkt automatycznie otrzymuje najnowsze aktualizacje.

Aby upewni si , e najnowsze aktualizacje zostały zainstalowane:

1. W panelu głównym kliknij prawym przyciskiem myszy ostatni ikon po prawej.
   Zostanie wy wietlone menu podr czne.
2. Wybierz opcj **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Aktualizacje automatyczne** > **Pobrane pliki**.
4. Kliknij ł cze **Sprawd teraz**.
   Produkt nawi e poł czenie z Internetem i sprawdzi dost pno najnowszych aktualizacji. Je li ochrona nie jest aktualna, zostan pobrane najnowsze aktualizacje.

   Informacje: Je eli dost p do Internetu jest uzyskiwany za pomoc modemu lub ł cza ISDN, to aby mo liwe było sprawdzenie aktualizacji, poł czenie musi by aktywne.

Zmienianie ustawie poł czenia internetowego

Zazwyczaj nie trzeba zmienia ustawie domy lnych. Jednak mo na skonfigurowa sposób nawi zywania poł czenia z Internetem przez serwer na potrzeby automatycznego otrzymywania aktualizacji.

Aby zmieni ustawienia poł czenia internetowego, 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 **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Aktualizacje automatyczne** > **Poł czenie**.
4. Za pomoc listy **Poł czenie internetowe** wybierz u ywany na komputerze sposób nawi zywania poł czenia z Internetem.
   - Wybierz opcj **Uznaj za zawsze poł czone**, je li komputer ma stałe poł czenie sieciowe.

     Informacje: Je eli komputer nie ma stałego poł czenia sieciowego i został skonfigurowany do nawi zywania poł czenia na danie, to wybranie opcji **Uznaj za zawsze poł czone** mo e powodowa inicjowanie wielu poł cze telefonicznych.
   - Wybierz opcj **Wykryj poł czenie**, aby pobiera aktualizacje tylko po wykryciu przez produkt aktywnego poł czenia sieciowego.
   - Wybierz opcj **Wykryj ruch**, je li aktualizacje maj by pobierane tylko po wykryciu przez produkt innego ruchu sieciowego.

     Wskazówka: W przypadku nietypowej konfiguracji sprz towej, w której ustawienie **Wykryj poł czenie** zawsze wskazuje istnienie aktywnego poł czenia sieciowego, nawet je li nie zostało ono nawi zane, nale y wybra opcj **Wykryj ruch**.

5. Za pomoc listy **Serwer proxy HTTP** okre l, czy komputer korzysta z *serwera proxy* do nawi zywania poł czenia z Internetem.
   - Wybierz opcj **Bez serwera proxy HTTP**, je li komputer jest poł czony z Internetem bezpo rednio.
   - Wybierz opcj **R cznie konfiguruj serwer proxy HTTP**, aby skonfigurowa ustawienia *serwera proxy HTTP*.
   - Wybierz opcje **U yj serwera proxy HTTP przegl darki**, aby zastosowa ustawienia *serwera proxy HTTP* skonfigurowane w przegl darce internetowej.

Sprawdzanie stanu Sieci ochrony w czasie rzeczywistym

W celu prawidłowego działania wiele funkcji produktu polega na poł czeniu z Sieci ochrony w czasie rzeczywistym.

W przypadku wyst pienia problemów z poł czeniem sieciowym, lub gdy zapora blokuje ruch Sieci ochrony w czasie rzeczywistym, wy wietlany jest stan „nie poł czono”. Je li natomiast adna funkcja wymagaj ca dost pu do Sieci ochrony w czasie rzeczywistym nie została zainstalowana, wy wietlana jest informacja o tym, e sie nie jest u ywana.

Aby sprawdzi aktualny stan, 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 **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Aktualizacje automatyczne** > **Poł czenie**.

W obszarze **Sie ochrony w czasie rzeczywistym** wy wietlane s informacje o bie cym stanie tej funkcji.

Sprawdzanie czynno ci wykonanych przez produkt

Na stronie **Powiadomienia** mo esz zobaczy list czynno ci wykonanych przez produkt w celu ochrony komputera.

Produkt wy wietla powiadomienia o wykonaniu czynno ci, na przykład po wykryciu i zablokowaniu wirusa. Niektóre powiadomienia mog by wysyłane przez usługodawc , na przykład w celu przekazania informacji o nowych usługach.

Wy wietl histori powiadomie

W historii powiadomie mo esz zobaczy powiadomienia, które zostały wy wietlone.

Aby wy wietli histori powiadomie , 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 **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Inne** > **Powiadomienia**.
4. Kliknij opcj **Poka histori powiadomie** .
   Zostanie otwarta lista historii powiadomie .

Zmienianie ustawie powiadomie

Mo na okre li typy powiadomie wy wietlanych przez produkt.

Aby zmieni ustawienia powiadomie , 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 **Otwórz typowe ustawienia**.
3. Wybierz kolejno opcje **Inne** > **Powiadomienia**.
4. Zaznacz lub wyczy pole wyboru **Zezwalaj na komunikaty programu**, aby wł czy lub wył czy komunikaty programu.

   Po zaznaczeniu tego ustawienia produkt wy wietla powiadomienia z zainstalowanych programów.
5. Zaznacz lub wyczy pole wyboru **Zezwalaj na wiadomo ci promocyjne**, aby wł czy lub wył czy wiadomo ci promocyjne.
6. Kliknij przycisk **OK**.

Sie ochrony w czasie rzeczywistym

W tym dokumencie opisano sie ochrony w czasie rzeczywistym — usług internetow firmy F-Secure Corporation słu c do identyfikowania bezpiecznych aplikacji i witryn internetowych oraz zabezpieczania przed zło liwym oprogramowaniem i witrynami wykorzystuj cymi luki w zabezpieczeniach.

Co to jest sie ochrony w czasie rzeczywistym

Sie ochrony w czasie rzeczywistym jest usług online zapewniaj c błyskawiczne reakcje na nowe zagro enia internetowe.

Uczestnicz c w sieci ochrony w czasie rzeczywistym, mo esz pomóc nam wzmocni nasze zabezpieczenia przed nowymi i powstaj cymi zagro eniami. Sie ochrony w czasie rzeczywistym gromadzi dane statystyczne dotycz ce nieznanych, zło liwych i podejrzanych aplikacji z uwzgl dnieniem informacji o ich działaniu na urz dzeniu. Te informacje maj charakter anonimowy i s wysyłane do analizy zbiorczej w firmie F-Secure Corporation. Korzystaj c z wyników takich analiz, udoskonalamy zabezpieczenia urz dze przed najnowszymi zagro eniami i zło liwymi plikami.

Jak działa sie ochrony w czasie rzeczywistym

Uczestnicz c w sieci ochrony w czasie rzeczywistym, mo esz udost pnia informacje dotycz ce nieznanych aplikacji i witryn internetowych oraz zło liwych programów i witryn zawieraj cych próby wykorzystania luk w zabezpieczeniach. Sie ochrony w czasie rzeczywistym nie ledzi działa u ytkowników w Internecie, nie gromadzi informacji na temat witryn, które zostały ju przeanalizowane, ani nie zbiera informacji o bezpiecznych aplikacjach zainstalowanych na komputerze.

Je li nie chcesz udost pnia takich danych, adne informacje dotycz ce zainstalowanych aplikacji i odwiedzanych witryn nie b d gromadzone. Jednak produkt musi wysyła do serwerów firmy F-Secure zapytania dotycz ce reputacji aplikacji, witryn internetowych, wiadomo ci i innych obiektów. Zapytania s przeprowadzane przy u yciu kryptograficznej sumy kontrolnej, gdzie sam obiekt, którego zapytanie dotyczy, nie jest wysyłany do firmy F-Secure. Nie ledzimy danych dla poszczególnych u ytkowników — tylko liczba zapyta dla pliku lub witryny jest zwi kszana.

Całkowite zatrzymanie komunikacji z sieci ochrony w czasie rzeczywistym nie jest mo liwe, poniewa stanowi ona integraln cz ochrony zapewnianej przez produkt.

Zalety sieci ochrony w czasie rzeczywistym

Sie ochrony w czasie rzeczywistym zapewnia szybsz i dokładniejsz ochron przed najnowszymi zagro eniami — bez niepotrzebnych alertów dotycz cych podejrzanych aplikacji, które nie s zło liwe.

Uczestnicz c w sieci ochrony w czasie rzeczywistym, mo esz pomóc nam w wykrywaniu nowych i nieznanych form zło liwego oprogramowania oraz eliminowaniu obiektów niepoprawnie uznanych za niebezpieczne z naszej bazy danych definicji wirusów.

Wszyscy uczestnicy sieci ochrony w czasie rzeczywistym pomagaj sobie wzajemnie. W przypadku wykrycia podejrzanej aplikacji na urz dzeniu u ywane s wyniki analizy tej aplikacji wykrytej wcze niej na innych urz dzeniach. Sie ochrony w czasie rzeczywistym zwi ksza ogóln wydajno urz dzenia, poniewa zainstalowany produkt zabezpieczaj cy nie musi skanowa aplikacji przeanalizowanych i uznanych za bezpieczne przez sie ochrony w czasie rzeczywistym. Podobnie informacje dotycz ce zło liwych witryn internetowych i niechcianych wiadomo ci zbiorczych s udost pniane za pomoc sieci ochrony w czasie rzeczywistym, umo liwiaj c zapewnianie dokładniejszej ochrony przed witrynami wykorzystuj cymi luki w zabezpieczeniach i spamem.

Im wi cej osób uczestniczy w sieci ochrony w czasie rzeczywistym, tym indywidualna ochrona u ytkowników staje si lepsza.

Jakie dane s przesyłane

Uczestnicz c w sieci ochrony w czasie rzeczywistym, udost pniasz informacje dotycz ce aplikacji zapisanych na Twoim urz dzeniu i odwiedzanych przez Ciebie witryn internetowych. Te dane umo liwiaj sieci ochrony w czasie rzeczywistym zapewnianie ochrony przed najnowszymi zło liwymi aplikacjami i podejrzanymi witrynami internetowymi.

Analizowanie reputacji plików

Sie ochrony w czasie rzeczywistym gromadzi informacje dotycz ce tylko aplikacji bez okre lonej reputacji i znanych plików, które s podejrzane lub zawieraj zło liwe oprogramowanie.

Sie ochrony w czasie rzeczywistym gromadzi anonimowe informacje na temat bezpiecznych i podejrzanych aplikacji znajduj cych si na urz dzeniu, jednak tylko przeno ne pliki wykonywalne s uwzgl dniane (takie jak pliki z rozszerzeniami cpl, exe, dll, ocx, sys, scr i drv na platformie systemu Windows).

Gromadzone informacje obejmuj :

- cie k pliku aplikacji na urz dzeniu;
- rozmiar oraz dat utworzenia lub zmodyfikowania pliku;
- atrybuty i uprawnienia pliku;
- informacje o sygnaturze pliku;
- bie c wersj pliku i nazw firmy, w której został utworzony;
- ródło pliku lub adres URL pobierania;
- wyniki skanowania plików przy u yciu technologii F-Secure DeepGuard i mechanizmów antywirusowych;
- inne podobne informacje.

 adne informacje dotycz ce dokumentów osobistych nie s gromadzone w sieci ochrony w czasie rzeczywistym, o ile takie pliki nie s zainfekowane. W przypadku dowolnego typu zło liwego oprogramowania zbierane s informacje o nazwie infekcji i stanie czyszczenia pliku.

Ponadto przy u yciu sieci ochrony w czasie rzeczywistym mo esz przesyła podejrzane aplikacje do analizy. Podczas przesyłania takich aplikacji uwzgl dniane s tylko przeno ne pliki wykonywalne. Sie ochrony w czasie rzeczywistym nigdy nie gromadzi jakichkolwiek informacji dotycz cych dokumentów osobistych ani nie przesyła ich automatycznie do analizy.

Przesyłanie plików do analizy

Ponadto sie ochrony w czasie rzeczywistym umo liwia przesyłanie podejrzanych aplikacji do analizy.

Pojedyncze podejrzane aplikacje mo na przesyła r cznie po wy wietleniu odpowiedniego monitu produktu. Dotyczy to tylko przeno nych plików wykonywalnych. Sie 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 dotycz cych witryn, które zostały ju przeanalizowane, a jedynie sprawdza bezpiecze stwo odwiedzanych witryn podczas przegl dania Internetu. Po otwarciu witryny sie ochrony w czasie rzeczywistym sprawdza, czy jest ona bezpieczna, a nast pnie powiadamia o poziomie ewentualnego zagro enia (w przypadku podejrzanych lub szkodliwych witryn).

Je li witryna zawiera podejrzane lub zło liwe obiekty b d prób wykorzystania znanej luki w zabezpieczeniach, cały adres URL tej witryny jest zapisywany przez sie ochrony w czasie rzeczywistym w celu przeanalizowania jej zawarto ci.

W przypadku odwiedzenia witryny, która nie została jeszcze oceniona, sie ochrony w czasie rzeczywistym gromadzi nazw domeny i jej poddomen, a w niektórych sytuacjach równie cie k odwiedzonej strony, na potrzeby przeanalizowania i oceny tej witryny. Wszystkie parametry adresu URL zawieraj ce informacje, które mog zosta skojarzone z danymi identyfikuj cymi to samo u ytkownika, s usuwane w trosce o ochron prywatno ci.

Informacje: Sie ochrony w czasie rzeczywistym nie ocenia ani nie analizuje stron w prywatnych sieciach, czyli adne informacje dotycz ce adresów IP prywatnych sieci (takich jak firmowe sieci intranet) nie s gromadzone.

Analizowanie informacji systemowych

W ramach sieci ochrony w czasie rzeczywistym gromadzone s informacje o nazwie i wersji systemu operacyjnego, poł czeniu internetowym oraz dane statystyczne dotycz ce u ytkowania sieci ochrony w czasie rzeczywistym, takie jak liczba zapyta o reputacj witryny i redni czas uzyskiwania wyników zapytania, na potrzeby monitorowania i ulepszania naszej usługi.

W jaki sposób chronimy Twoj prywatno

Wszystkie informacje s przesyłane w bezpieczny sposób po automatycznym usuni ciu jakichkolwiek danych osobistych.

Sie ochrony w czasie rzeczywistym usuwa wszelkie dane umo liwiaj ce identyfikacj przed wysłaniem informacji na serwery firmy F-Secure. Ponadto wszystkie zgromadzone informacje s zaszyfrowane podczas przesyłania, uniemo liwiaj c nieautoryzowany dost p. Zgromadzone informacje nie s przetwarzane indywidualnie, ale w zbiorowej postaci obejmuj cej informacje uzyskane od innych uczestników sieci ochrony w czasie rzeczywistym. Wszystkie dane s anonimowo analizowane pod k tem statystycznym, co oznacza, e nie mo na ich skojarzy z poszczególnymi u ytkownikami.

 adne informacje umo liwiaj ce identyfikowanie to samo ci u ytkowników nie s uwzgl dniane 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 e podejmujemy wszelkie starania w celu usuni cia wszystkich identyfikuj cych danych osobistych, istnieje mo liwo pozostania identyfikuj cych danych w gromadzonych informacjach. W takich sytuacjach nie b dziemy u ywa tych przypadkowo uzyskanych danych w celu okre lania to samo ci u ytkowników.

Stosujemy rygorystyczne metody ochrony oraz fizyczne, administracyjne i techniczne zabezpieczenia gromadzonych danych podczas ich przesyłania, przechowywania i przetwarzania. Informacje s przechowywane w bezpiecznych lokalizacjach na kontrolowanych przez nas serwerach, które znajduj si w naszych biurach lub w biurach naszych podwykonawców. Tylko upowa niony personel ma dost p do gromadzonych informacji.

Firma F-Secure mo e udost pnia zgromadzone dane swoim podmiotom stowarzyszonym, podwykonawcom, dystrybutorom i partnerom, jednak zawsze w anonimowej postaci uniemo liwiaj cej identyfikowanie u ytkowników.

Doł czanie do sieci ochrony w czasie rzeczywistym

Udost pniaj c informacje dotycz ce zło liwych programów i witryn internetowych, mo esz pomóc nam w ulepszaniu zabezpiecze oferowanych w ramach sieci ochrony w czasie rzeczywistym.

Opcja uczestniczenia w sieci ochrony w czasie rzeczywistym jest dost pna podczas instalacji. Domy lne ustawienia instalacji powoduj przesyłanie danych do sieci ochrony w czasie rzeczywistym. To ustawienie mo esz zmieni pó niej w produkcie.

Post puj zgodnie z nast puj cymi instrukcjami, aby zmieni ustawienia sieci ochrony w czasie rzeczywistym:

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

Pytania dotycz ce sieci ochrony w czasie rzeczywistym

Informacje kontaktowe w przypadku jakichkolwiek pyta dotycz cych sieci ochrony w czasie rzeczywistym.

Je li masz jakiekolwiek inne pytania dotycz ce sieci ochrony w czasie rzeczywistym, skontaktuj si z nami pod adresem:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

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

Najnowsza wersja tego dokumentu jest zawsze dost pna w naszej witrynie internetowej.

Jak sprawdzi , czy subskrypcja jest wa na

Na stronie **Stan subskrypcji** wy wietlane s informacje na temat typu i stanu Twojej subskrycji.

Je li wa no subskrypcji ma wkrótce wygasn lub ju wygasła, ogólny stan ochrony programu przy odpowiedniej ikonie na panelu głównym zostaje zmieniony.

Aby sprawdzi wa no subskrypcji:

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 opcj **Stan subskrypcji**, aby wy wietli informacje na temat subskrypcji i zainstalowanych programów.
4. Wybierz opcj **Stan instalacji**, aby zobaczy , jakie programy s dost pne do zainstalowania.

Informacje o stanie subskrypcji i dacie wa no ci s równie 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**.

Rozdział

3

Wprowadzenie

Tematy:

- *Wy wietlanie ogólnego stanu ochrony*
- *Wy wietlanie statystyki produktu*
- *Obsługiwanie aktualizacji produktu*
- *Co to s wirusy i inne zło liwe 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 adnych działa ze strony u ytkownika.

Wy wietlanie ogólnego stanu ochrony

Na stronie **Stan** wy wietlane s podstawowe informacje o zainstalowanych funkcjach produktu i ich bie cym stanie.

Aby otworzy stron **Stan**, wykonaj nast puj ce czynno ci:

Na stronie głównej kliknij opcj **Stan**.

Zostanie otwarta strona **Stan**.

Ikony przedstawiaj stan programu i jego funkcji zabezpiecze .

Ikona stanu	Nazwa stanu	Opis
	OK	Komputer jest chroniony. Funkcja jest wł czona i działa poprawnie.
	Informacja	Produkt informuje o specjalnym stanie funkcji. Na przykład funkcja jest aktualizowana.
	Ostrze enie	Komputer nie jest w pełni chroniony. Na przykład produkt długo nie był aktualizowany lub stan funkcji wymaga uwagi u ytkownika.
	Bł d	Komputer nie jest chroniony Na przykład wygasła wa no subskrypcji lub jest wył czona krytyczna funkcja.
	Wył czone	Niekrytyczna funkcja jest wył czona.

Wy wietlanie statystyki produktu

Na stronie **Statystyka** mo na sprawdzi , co produkt robił od momentu zainstalowania.

Aby otworzy stron **Statystyka**:

Na stronie głównej kliknij opcj **Statystyka**.

Zostanie otwarta strona **Statystyka**.

- W polu **Ostatnie pomy lne sprawdzanie aktualizacji** wy wietlane s 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 liczb programów, którym technologia DeepGuard umo liwiła działanie lub które zablokowała od momentu zainstalowania produktu.
- W obszarze **Poł czenia zapory** jest wy wietlana liczba dozwolonych i zablokowanych poł cze od momentu zainstalowania.
- W obszarze **Filtrowanie spamu i wiadomo ci typu phishing** widoczna jest liczba wiadomo ci e-mail okre lonych przez produkt jako poprawne lub zawieraj ce spam.

Obsługiwanie aktualizacji produktu

Produkt zapewnia automatyczn aktualizacj zabezpiecze komputera.

Wy wietl wersje baz danych

Terminy i numery wersji najnowszych aktualizacji mo na wy wietli na stronie **Aktualizacje baz danych**.

Aby otworzy stron **Aktualizacje baz danych**, wykonaj nast puj ce czynno ci:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

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

Na stronie **Wersje baz danych** s wy wietlane informacje o datach ostatniego aktualizowania definicji wirusów i oprogramowania szpieguj cego, funkcji DeepGuard oraz filtrowania spamu i phishingu wraz z odpowiednimi numerami wersji.

Zmienianie ustawie poł cze internetowych na urz dzeniu przeno nym

Te ustawienia pozwalaj okre li , czy aktualizacje zabezpiecze maj by pobierane podczas u ywania szerokopasmowego poł czenia na urz dzeniu przeno nym.

Informacje: Ta funkcja jest dost pna tylko w systemie Microsoft Windows 7.

Domy lnie aktualizacje zabezpiecze s zawsze pobierane, gdy urz dzenie znajduje si w zasi gu sieci głównego operatora. Je li natomiast sie głównego operatora jest niedost pna, aktualizacje zostaj wstrzymane. Dzieje si tak, poniewa ceny poł cze mog ró ni si u poszczególnych operatorów, na przykład w innych krajach. Aby zmniejszy u ycie przepustowo ci i prawdopodobnie ograniczy wydatki, zalecane jest pozostawienie tych ustawie bez zmian podczas wyjazdów.

Informacje: To ustawienie dotyczy tylko szerokopasmowych poł cze transmisji danych. Gdy komputer jest podł czony do zwykłej sieci (przewodowej lub bezprzewodowej), produkt jest automatycznie aktualizowany.

Aby zmieni to ustawienie, wykonaj nast puj ce czynno ci:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Poł czenie szerokopasmowe na urz dzeniu przeno nym** > **Pobierz aktualizacje zabezpiecze** .
3. Wybierz preferowan opcj aktualizacji dla poł cze na urz dzeniu przeno nym:
   - **Tylko w sieci głównego operatora**

Aktualizacje s zawsze pobierane, gdy urz dzenie znajduje si w zasi gu sieci głównego operatora. Je li natomiast sie głównego operatora jest niedost pna, aktualizacje zostaj wstrzymane. Wybranie tej opcji jest zalecane. Pozwala to utrzymywa aktualny stan produktu zabezpieczaj cego bez nieoczekiwanych kosztów.

- **Nigdy**

  Aktualizacje nie s pobierane przy u yciu poł czenia internetowego na urz dzeniu przeno nym.

- **Zawsze**

  Aktualizacje s zawsze pobierane, niezale nie od u ywanej sieci. Wybieraj c t opcj , mo na upewni si , e zabezpieczenia komputera s zawsze aktualne, bez wzgl du na koszty.

4. Aby decydowa oddzielnie za ka dym razem, gdy nawi zywane jest poł czenie z inn sieci , wybierz opcj **Zapytaj za ka dym razem, gdy sie głównego operatora jest niedost pna**.

Wstrzymane aktualizacje zabezpiecze

Aktualizacje zabezpiecze mog zosta wstrzymane na czas u ywania poł czenia szerokopasmowego na urz dzeniu przeno nym poza zasi giem sieci podstawowego operatora.

W takim przypadku w prawym dolnym rogu ekranu zostaje wy wietlone powiadomienie o tre ci **Wstrzymano**. Aktualizacje s wstrzymywane, poniewa ceny poł cze mog ró ni si u poszczególnych operatorów, na przykład w innych krajach. Aby zmniejszy u ycie przepustowo ci i prawdopodobnie ograniczy wydatki, zalecane jest pozostawienie tych ustawie bez zmian podczas wyjazdów. Je li jednak chcesz modyfikowa te ustawienia, kliknij ł cze **Zmie** .

Informacje:

Ta funkcja jest dost pna tylko w systemie Microsoft Windows 7.

Co to s wirusy i inne zło liwe oprogramowanie?

Zło liwe oprogramowanie to programy utworzone specjalnie w celu czynienia szkód na komputerze, u ywania komputera w niedozwolonych celach bez wiedzy u ytkownika lub kradzie y informacji z komputera.

Zło liwe oprogramowanie mo e:

- przej kontrol nad przegl dark sieci Web,
- przekierowywa próby wyszukiwania,
- wy wietla niepo dane reklamy,
- ledzi witryny odwiedzane przez u ytkownika,
- kra informacje osobiste, takie jak informacje dotycz ce bankowo ci elektronicznej,
- u ywa komputera u ytkownika do wysyłania spamu,
- u ywa komputera u ytkownika do ataku na inne komputery.

Zło liwe oprogramowanie mo e te spowalnia prac komputera i powodowa jego niestabilno . Podejrzenie, e na komputerze znajduje si *zło liwe oprogramowanie*, mo e si pojawi , gdy komputer nagle zaczyna pracowa bardzo wolno lub cz sto ulega awariom.

Wirusy

Wirusy to zwykle programy, które doł czaj si do plików i powielaj si wielokrotnie. Wirusy mog modyfikowa i zast powa zawarto innych plików w sposób, który mo e spowodowa uszkodzenie komputera.

Wirus to program, który zazwyczaj jest instalowany na komputerze bez wiedzy u ytkownika. Po zainstalowaniu wirus podejmuje prób powielenia si . Wirus:

- korzysta z cz ci zasobów systemowych komputera,

- mo e modyfikowa lub uszkadza pliki na komputerze,
- prawdopodobnie próbuje u y komputera do zainfekowania innych komputerów,
- mo e umo liwi u ycie komputera w niedozwolonych celach.

Oprogramowanie szpieguj ce

Oprogramowanie szpieguj ce jest u ywane do gromadzenia informacji osobistych u ytkownika.

Oprogramowanie szpieguj ce mo e zbiera informacje osobiste, w tym dotycz ce:

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

Oprogramowanie szpieguj ce prawie zawsze instaluje si samoczynnie bez wiadomej zgody u ytkownika. Oprogramowanie szpieguj ce mo e zosta zainstalowane razem z przydatnym programem lub w wyniku nakłonienia u ytkownika do klikni cia opcji w myl cym oknie podr cznym.

Programy typu rootkit

Programy typu rootkit utrudniaj znalezienie innego *zło liwego oprogramowania*.

Programy typu rootkit ukrywaj pliki i procesy. Zazwyczaj ma to na celu ukrycie działania zło liwych programów na komputerze. Kiedy program typu rootkit ukrywa *zło liwe oprogramowanie*, u ytkownik nie jest w stanie łatwo zorientowa si , e takie oprogramowanie znajduje si na komputerze.

Niniejszy produkt posiada skaner programów typu rootkit, który skanuje komputer w poszukiwaniu programów typu rootkit, dzi ki czemu *zło liwe oprogramowanie* nie mo e tak łatwo si ukrywa .

Ryzykowne oprogramowanie

Ryzykowne oprogramowanie nie powstaje z my l w wyrz dzaniu szkód na komputerach, ale nieodpowiednio u ywane mo e powodowa uszkodzenia.

Ryzykowne oprogramowanie nie jest, ci le rzecz bior c, zło liwym oprogramowaniem. Pełni ono u yteczne, jednak potencjalnie niebezpieczne funkcje.

Przykładami takich programów s :

- klienty wiadomo ci błyskawicznych, np. usługa IRC (Internet Relay Chat);
- programy słu ce do przesyłania plików w Internecie mi dzy komputerami;
- programy telefonii internetowej, np. VoIP (*Voice over Internet Protocol*);
- oprogramowanie do zdalnego uzyskiwania dost pu, na przykład program VNC;
- oprogramowanie strasz ce (scareware), które zaprojektowano w celu przestraszenia u ytkownika i nakłonienia go do zakupu fałszywego oprogramowania zabezpieczaj cego;
- oprogramowanie u ywane w celu omijania zabezpiecze przed kopiowaniem i narz dzi do sprawdzania obecno ci dysków CD.

Je li program ten został wiadomie zainstalowany i prawidłowo skonfigurowany przez u ytkownika, prawdopodobie stwo jego szkodliwego działania jest mniejsze.

Je li ryzykowne oprogramowanie zostało zainstalowane bez wiedzy u ytkownika, najprawdopodobniej zostało zainstalowane w zło liwym celu i powinno zosta usuni te.

Rozdział

4

Ochrona komputera przed zło liwym oprogramowaniem

Tematy:

- *Jak przeskanowa komputer*
- *Jak wykluczy pliki ze skanowania*
- *Jak korzysta z funkcji kwarantanny?*
- *Co to jest technologia DeepGuard?*

Funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpieguj cego chroni komputer przed programami, które mog wykra przechowywane na nim informacje osobiste, uszkodzi go lub u y w niedozwolonych celach.

Domy lnie wszystkie typy zło liwego oprogramowania s przetwarzane natychmiast po wykryciu, uniemo liwiaj c wyrz dzenie jakichkolwiek szkód.

Domy lnie skanowanie w poszukiwaniu wirusów automatycznie sprawdza lokalne dyski twarde, no niki wymienne (takie jak pami ci przeno ne, dyski CD/DVD) i pobierane pliki. W zale no ci od ustawie automatyczne sprawdzanie mo e te obejmowa poczt e-mail.

Ponadto skanowanie w poszukiwaniu wirusów i oprogramowania szpieguj cego monitoruje komputer pod k tem zmian, które mog wskazywa na obecno *zło liwego oprogramowania*. W przypadku wykrycia jakiejkolwiek niebezpiecznej zmiany w systemie, takiej jak modyfikacja ustawie systemowych lub próba manipulowania wa nym procesem systemowym, funkcja DeepGuard zatrzymuje okre lony program, który prawdopodobnie stanowi *zło liwe oprogramowanie*.

Jak przeskanowa komputer

Gdy funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpieguj cego jest wł czona, komputer jest automatycznie skanowany w poszukiwaniu szkodliwych plików. Mo na tak e skanowa pliki r cznie i skonfigurowa skanowanie zaplanowane.

Zaleca si , aby funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpieguj cego była cały czas wł czona. Pliki nale y skanowa r cznie, aby si upewni , e 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 szpieguj cego usuwa szkodliwe pliki z komputera o ustalonym czasie.

Automatyczne skanowanie plików

Funkcja skanowania w czasie rzeczywistym chroni komputer, skanuj c wszystkie pliki przy ka dej próbie dost pu i blokuj c dost p do plików zawieraj cych *zło liwe oprogramowanie*.

Gdy komputer próbuje uzyska dost p do pliku, funkcja skanowania w czasie rzeczywistym skanuje ten plik w poszukiwaniu zło liwego oprogramowania, zanim zezwoli komputerowi na dost p do tego pliku. Je li funkcja skanowania w czasie rzeczywistym wykryje jak kolwiek szkodliw zawarto , umie ci dany plik w kwarantannie, zanim spowoduje on szkody.

Czy skanowanie w czasie rzeczywistym ma wpływ na wydajno komputera?

Zazwyczaj u ytkownik nie dostrzega procesu skanowania, poniewa trwa on krótko i nie korzysta z wielu zasobów systemowych. Ilo czasu i zasobów systemowych wykorzystywanych podczas skanowania w czasie rzeczywistym zale y mi dzy innymi od zawarto ci, lokalizacji oraz typu pliku.

Pliki, których skanowanie trwa dłu ej:

- Pliki na no nikach wymiennych, takich jak dyski CD i DVD oraz przeno ne dyski USB.
- Pliki skompresowane, takie jak archiwa *zip*.

  Informacje: Domy lnie pliki skompresowane nie s skanowane.

Skanowanie w czasie rzeczywistym mo e spowolni prac komputera w nast puj cych przypadkach:

- Komputer u ytkownika nie spełnia wymaga systemowych.
- U ytkownik uzyskuje dost p do wielu plików jednocze nie, na przykład podczas otwierania katalogu zawieraj cego wiele plików, które nale y przeskanowa .

Wł czanie lub wył czanie skanowania w czasie rzeczywistym

Aby powstrzyma *zło liwe oprogramowanie*, zanim zdoła ono wyrz dzi szkody na komputerze, skanowanie w czasie rzeczywistym powinno by zawsze wł czone.

Aby wł czy lub wył czy skanowanie w czasie rzeczywistym, wykonaj nast puj ce czynno ci:

1. Na stronie głównej kliknij opcj **Stan**.
2. Kliknij pozycj **Zmie ustawienia na tej stronie**.

   Informacje: Do wył czenia funkcji zabezpiecze wymagane s uprawnienia administratora.

3. Wł cz lub wył cz opcj **Skanowanie w poszukiwaniu wirusów**.
4. Kliknij przycisk **Zamknij**.

Automatyczne przetwarzanie szkodliwych plików

Funkcja skanowania w czasie rzeczywistym mo e przetwarza szkodliwe pliki automatycznie bez wy wietlania zapytania.

Aby funkcja skanowania w czasie rzeczywistym przetwarzała szkodliwe pliki automatycznie, wykonaj nast puj ce czynno ci:

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 **Przetwarzaj szkodliwe pliki automatycznie**.

Je li u ytkownik wybierze opcj , aby szkodliwe pliki nie były przetwarzane automatycznie, funkcja skanowania w czasie rzeczywistym b dzie wy wietla pytanie o czynno , jaka ma zosta wykonana dla wykryciu szkodliwego pliku.

Przetwarzanie oprogramowania szpieguj cego

Funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpieguj cego natychmiast blokuje oprogramowanie szpieguj ce przy próbie uruchomienia.

Zanim aplikacja szpieguj ca zostanie uruchomiona, produkt blokuje j i pozwala u ytkownikowi wybra , co z ni zrobi .

Po wykryciu oprogramowania szpieguj cego nale y wybra jedn z nast puj cych czynno ci:

Czynno do wykonania	Co dzieje si z oprogramowaniem szpieguj cym
Przetwórz automatycznie	Pozwól programowi wybra najlepsze działanie w zale no ci od wykrytego oprogramowania szpieguj cego.
Poddaj oprogramowanie szpieguj ce kwarantannie	Przenie oprogramowanie szpieguj ce do kwarantanny, sk d nie mo e uszkodzi komputera.
Usu oprogramowanie szpieguj ce	Usu wszystkie pliki zwi zane z oprogramowaniem szpieguj cym z komputera.
Tylko zablokuj oprogramowanie szpieguj ce	Zablokuj dost p do oprogramowania szpieguj cego, ale pozostaw je na komputerze.
Wyklucz oprogramowanie szpieguj ce ze skanowania	Zezwól na uruchomienie oprogramowania szpieguj cego i wyklucz je ze skanowania w przyszło ci.

Przetwarzanie ryzykownego oprogramowania

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

Zanim ryzykowna aplikacja zostanie uruchomiona, produkt blokuje j i pozwala u ytkownikowi wybra , co z ni zrobi .

Po wykryciu ryzykownego oprogramowania nale y wybra jedn z nast puj cych czynno ci:

Czynno do wykonania	Co dzieje si z ryzykownym oprogramowaniem
Tylko zablokuj ryzykowne oprogramowanie	Zablokuj dost p do ryzykownego oprogramowania, ale pozostaw je na komputerze.
Poddaj ryzykowne oprogramowanie kwarantannie	Przenie ryzykowne oprogramowanie do kwarantanny, sk d nie mo e uszkodzi 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

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

 ledz ce pliki cookie to małe pliki, które umo liwiaj witrynom 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 u ycie
Skanowanie w poszukiwaniu wirusów i oprogramowania szpieguj cego	Okre lone obszary komputera w poszukiwaniu wirusów, oprogramowania szpieguj cego i ryzykownego oprogramowania	Skanowanie tego typu jest du o szybsze ni pełne skanowanie. Przeszukiwane s tylko obszary systemu zawieraj ce zainstalowane pliki programów. Skanowanie tego typu jest zalecane, gdy trzeba szybko sprawdzi , czy komputer nie jest zainfekowany, poniewa umo liwia ono wydajne wyszukiwanie i usuwanie wszelkiego aktywnego zło liwego oprogramowania znajduj cego si na komputerze.
Pełne skanowanie komputera	Cały komputer (wewn trzne i zewn trzne dyski twarde) w poszukiwaniu wirusów, oprogramowania szpieguj cego i ryzykownego oprogramowania	W celu uzyskania całkowitej pewno ci, e na komputerze nie ma zło liwego oprogramowania ani ryzykownego oprogramowania. Skanowanie tego typu zajmuje najwi cej czasu. Stanowi poł czenie funkcji szybkiego skanowania w poszukiwaniu zło liwego oprogramowania i funkcji skanowania dysku twardego. Ta funkcja przeprowadza równie sprawdzanie pod k tem plików ukrytych przez programy typu „rootkit”.
Wybierz elementy do przeskanowania	Okre lony plik, folder lub dysk w poszukiwaniu wirusów, oprogramowania szpieguj cego i ryzykownego oprogramowania	W przypadku podejrze , e okre lona lokalizacja na komputerze zawiera zło liwe oprogramowanie. Na przykład miejsce zapisywania plików pobieranych z potencjalnie niebezpiecznych ródeł, takich jak sieci udost pniania plików typu „peer-to-peer”. Czas potrzebny na przeprowadzenie skanowania zale y od wielko ci skanowanego obiektu docelowego. Skanowanie trwa krótko, je li na przykład wybrano folder zawieraj cy tylko kilka małych plików.
Skanowanie w poszukiwaniu programów rootkit	Wa ne lokalizacje systemowe, w których podejrzany element mo e oznacza problem zwi zany z zabezpieczeniami. Przeprowadzane jest skanowanie w poszukiwaniu ukrytych plików, folderów, dysków i procesów.	W przypadku podejrze , e na komputerze mo e by zainstalowany program typu rootkit, je li na przykład wykryto ostatnio na komputerze zło liwe oprogramowanie i trzeba si upewni , e nie zainstalowało ono programu typu rootkit.

Skanowanie w Eksploratorze Windows

Skanowanie dysków, folderów i plików w poszukiwaniu *wirusów*, *oprogramowania szpieguj cego* i *ryzykownego oprogramowania* mo na wykonywa w Eksploratorze Windows.

Aby przeskanowa dysk, folder lub plik:

1. Umie wska nik myszy na dysku, folderze lub pliku, który chcesz przeskanowa , a nast pnie kliknij go prawym przyciskiem myszy.
2. W wy wietlonym menu wybierz polecenie **Skanuj foldery w poszukiwaniu wirusów**. Nazwa tej opcji ró ni si w zale no ci od tego, czy skanowany jest dysk, folder czy plik.
   Zostanie otwarte okno **Kreator skanowania** i rozpocznie si skanowanie.

W przypadku znalezienia *wirusa* lub *oprogramowania szpieguj cego***Kreator skanowania** przeprowadzi u ytkownika przez proces oczyszczania.

Wybieranie plików do skanowania

U ytkownik mo e wybra typy plików, które maj by skanowane w poszukiwaniu *wirusów* i *oprogramowania szpieguj cego* podczas skanowania r cznego i zaplanowanego.

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie r czne**.
3. W obszarze **Opcje skanowania** okre l nast puj ce ustawienia:

Skanuj tylko znane typy plików	Skanowanie tylko plików, w przypadku których istnieje najwi ksze prawdopodobie stwo infekcji, na przykład plików wykonywalnych. Wybranie tej opcji zapewnia szybsze skanowanie. Takie skanowanie obejmuje pliki z nast puj cymi rozszerzeniami: ani, asp, ax, bat, bin, boo, chm, cmd, com, cpl, dll, doc, dot, drv, eml, exe, hlp, hta, htm, html, htt, inf, ini, job, js, jse, lnk, lsp, mdb, mht, mpp, mpt, msg, ocx, pdf, php, pif, pot, ppt, rtf, scr, shs, swf, sys, td0, 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 wewn trz plików skompresowanych	Skanowanie zarchiwizowanych plików i folderów.
U yj zaawansowanej heurystyki	Podczas skanowania zostan u yte wszystkie dost pne zasoby heurystyki w celu skuteczniejszego wykrywania nowego i nieznanego zło liwego oprogramowania. **Informacje:** Zaznaczenie tej opcji wydłu a czas skanowania i mo e powodowa zwi kszenie liczby zgłosze programów niepoprawnie uznanych za niebezpieczne (nieszkodliwych plików zgłoszonych jako podejrzane).

4. Kliknij przycisk **OK**.

Informacje: Wykluczone pliki z listy wykluczonych obiektów nie s skanowane, nawet je li zostan tutaj wybrane do skanowania.

Co zrobi w przypadku wykrycia szkodliwych plików

Sposób post powania z wykrytymi szkodliwymi plikami mo na wybra .

Aby wybra czynno , która ma zosta wykonana w przypadku wykrycia szkodliwej zawarto ci podczas skanowania r cznego:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie r czne**.
3. W sekcji **W przypadku wykrycia wirusa lub op. szpieguj cego** wybierz odpowiedni opcj :

Opcja	Opis
Zapytaj (domy lnie)	U ytkownik mo e wybra czynno , która ma zosta wykonana w przypadku ka dego elementu wykrytego podczas skanowania r cznego.

Opcja	Opis
Wyczy pliki	Produkt próbuje automatycznie usun zainfekowane pliki wykryte podczas skanowania r cznego. **Informacje:** Je li produkt nie mo e usun zainfekowanego pliku, jest on poddawany kwarantannie (chyba e plik znajduje si w sieci lub na dysku przeno nym), aby uszkodzenie komputera było niemo liwe.
Poddaj pliki kwarantannie	Produkt przenosi szkodliwe pliki wykryte podczas skanowania r cznego do kwarantanny, uniemo liwiaj c uszkodzenie komputera.
Usu pliki	Produkt usuwa ka dy szkodliwy plik wykryty podczas skanowania r cznego.
Tylko zgło	Produkt pozostawia bez zmian ka dy szkodliwy plik wykryty podczas skanowania r cznego i rejestruje to wykrycie w raporcie skanowania. **Informacje:** W przypadku gdy skanowanie w czasie rzeczywistym jest wył czone, zło liwe oprogramowanie mo e nadal uszkodzi komputer, je li zostanie wybrana ta opcja.

Informacje: Szkodliwe pliki wykryte podczas skanowania zaplanowanego s automatycznie usuwane.

Planowanie skanowania

Mo esz skonfigurowa automatyczne skanowanie komputera w poszukiwaniu wirusów i innych szkodliwych aplikacji i usuwanie ich, gdy komputer nie jest u ywany, lub okresowe uruchamianie skanowania, aby mie pewno , e komputer nie jest zainfekowany.

Aby zaplanowa skanowanie:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie zaplanowane**.
3. Wł cz opcj **Skanowanie zaplanowane**.
4. Wybierz czas rozpocz cia skanowania.

Opcja	Opis
Codziennie	Komputer b dzie skanowany codziennie.
Co tydzie	Komputer b dzie skanowany w wybrane dni tygodnia. Wybierz dni z listy.
Co miesi c	Komputer b dzie skanowany w wybrane dni miesi ca. Aby wybra dni: 1. Wybierz jedn z opcji **Dzie** . 2. Wybierz dzie miesi ca z listy znajduj cej si obok wybranego dnia.

5. Okre l czas rozpocz cia skanowania w wybrane dni.

Opcja	Opis
Godzina rozpocz cia	Skanowanie b dzie uruchamiane o okre lonej godzinie.
Je eli komputer nie jest u ywany przez	Skanowanie b dzie uruchamiane, je li komputer nie b dzie u ywany przez okre lony czas.

Podczas skanowania zaplanowanego komputera s u ywane ustawienia skanowania r cznego, archiwa s skanowane za ka dym razem i szkodliwe pliki s usuwane automatycznie.

Skanowanie poczty e-mail

Skanowanie poczty e-mail chroni przed otrzymywaniem szkodliwych plików w wiadomo ciach e-mail wysyłanych do u ytkownika.

Aby skanowa poczt e-mail w poszukiwaniu wirusów, nale y wł czy funkcj skanowania w poszukiwaniu wirusów i oprogramowania szpieguj cego.

Aby wł czy skanowanie poczty e-mail:

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 szkodliwe zał czniki wiadomo ci e-mail**.
4. Kliknij przycisk **OK**.

Kiedy s skanowane wiadomo ci e-mail i zał czniki?

Skanowanie w poszukiwaniu wirusów i oprogramowania szpieguj cego usuwa szkodliwe obiekty z otrzymywanych wiadomo ci e-mail.

Skanowanie w poszukiwaniu wirusów i oprogramowania szpieguj cego usuwa szkodliwe wiadomo ci 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 wiadomo ci e-mail i zał czniki za ka dym razem, gdy program otrzymuje je z serwera pocztowego korzystaj cego z protokołu POP3.

Funkcja skanowania w poszukiwaniu wirusów i oprogramowania szpieguj cego nie mo e skanowa wiadomo ci e-mail w poczcie internetowej, obejmuj cej aplikacje poczty e-mail działaj ce w przegl darce internetowej, takie jak Hotmail, Yahoo! Mail lub Gmail. Komputer jest nadal chroniony przed *wirusami*, nawet je li szkodliwe zał czniki nie zostały usuni te lub u ywana jest poczta internetowa. Podczas otwierania zał czników wiadomo ci e-mail skanowanie w czasie rzeczywistym usuwa wszystkie szkodliwe zał czniki, zanim zdołaj wyrz dzi jakiekolwiek szkody.

Informacje: Skanowanie w czasie rzeczywistym chroni tylko komputer u ytkownika, a nie komputery jego znajomych. Przeskanowanie zał czonych plików mo e zosta przeprowadzone dopiero po ich otwarciu. Oznacza to, e u ywaj c poczty internetowej i przekazuj c dalej wiadomo ci zawieraj ce nieotwarte zał czniki, mo na rozsyła zainfekowane wiadomo ci e-mail.

Wy wietlanie wyników skanowania

W oknie Historia wirusów i oprogramowania szpieguj cego s wy wietlane informacje o wszystkich szkodliwych plikach wykrytych przez produkt.

Czasami po wykryciu szkodliwego obiektu produkt nie mo e wykona akcji wybranej przez u ytkownika. Je li na przykład zostanie wybrana opcja wyczyszczenia plików, a plików nie mo na wyczy ci , produkt przeniesie je do kwarantanny. T informacj mo na wy wietli w historii wirusów i oprogramowania szpieguj cego.

Aby wy wietli histori :

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. Kliknij opcj **Wy wietl histori 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 zostan usni te z listy wykluczonych elementów.

Informacje: Istniej osobne listy wyklucze dla skanowania r cznego i skanowania w czasie rzeczywistym. Je li na przykład plik zostanie wykluczony ze skanowania w czasie rzeczywistym, jest on skanowany podczas skanowania r cznego, chyba e zostanie on te wykluczony ze skanowania r cznego.

Wykluczanie typów plików

Po wykluczeniu plików według ich typu pliki z okre lonymi rozszerzeniami nie s skanowane w poszukiwaniu szkodliwej zawarto ci.

Aby doda lub usun typ pliku, który ma zosta wykluczony, wykonaj nast puj ce czynno ci:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz, czy chcesz wykluczy typ pliku ze skanowania w czasie rzeczywistym, czy skanowania r cznego:
   - Wybierz kolejno pozycje **Zabezpieczenia komputera** > **Skanowanie w poszukiwaniu wirusów**, aby wykluczy typ plików ze skanowania w czasie rzeczywistym.
   - Wybierz kolejno pozycje **Inne ustawienia** > **Skanowanie r czne**, aby wykluczy typ plików ze skanowania r cznego.
3. Kliknij opcj **Wyklucz pliki ze skanowania**.
4. Aby wykluczy typ pliku:
   a) Wybierz kart **Typy plików**.
   b) Wybierz opcj **Wyklucz pliki z tymi rozszerzeniami**.
   c) W polu obok przycisku **Dodaj** wpisz rozszerzenie pliku okre laj ce typ plików, które chcesz wykluczy .

      Aby uwzgl dni pliki, które nie maj rozszerzenia, nale y u y znaku „.”. Mo na te zastosowa symbol wieloznaczny „?” reprezentuj cy dowolny znak lub „*” reprezentuj cy dowoln liczb znaków.

      Aby na przykład wykluczy pliki wykonywalne, wpisz w tym polu warto exe.
   d) Kliknij przycisk **Dodaj**.
5. Powtórz poprzedni krok dla ka dego rozszerzenia, które ma zosta wykluczone ze skanowania w poszukiwaniu wirusów.
6. Kliknij przycisk **OK**, aby zamkn okno dialogowe **Wykluczanie ze skanowania**.
7. Kliknij przycisk **OK**, aby zastosowa nowe ustawienia.

Wybrane typy plików nie b d uwzgl dniane podczas skanowania przeprowadzanego w przyszło ci.

Wykluczanie plików według lokalizacji

Po wykluczeniu plików według lokalizacji pliki znajduj ce si na okre lonych dyskach lub w okre lonych folderach nie s skanowane w poszukiwaniu szkodliwej zawarto ci.

Aby doda lub usun lokalizacje plików, które maj zosta wykluczone, wykonaj nast puj ce czynno ci:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz, czy chcesz wykluczy lokalizacj ze skanowania w czasie rzeczywistym, czy skanowania r cznego:
   - Aby wykluczy lokalizacj ze skanowania w czasie rzeczywistym, wybierz kolejno opcje **Komputer** > **Skanowanie w poszukiwaniu wirusów**.
   - Aby wykluczy lokalizacj ze skanowania r cznego, wybierz kolejno opcje **Komputer** > **Skanowanie r czne**.
3. Kliknij opcj **Wyklucz pliki ze skanowania**.
4. Aby wykluczy plik, dysk lub folder:
   a) Wybierz kart **Obiekty**.
   b) Wybierz opcj **Wyklucz obiekty (pliki, foldery itd.)**.
   c) Kliknij przycisk **Dodaj**.
   d) Wybierz plik, folder lub dysk, który chcesz wykluczy ze skanowania antywirusowego.

      Informacje: Niektóre dyski mog by wymienne, na przykład dyski CD lub DVD i dyski sieciowe. Nie mo na wykluczy 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 zamkn okno dialogowe **Wykluczanie ze skanowania**.
7. Kliknij przycisk **OK**, aby zastosowa nowe ustawienia.

Wybrane pliki, dyski i foldery nie b d uwzgl dniane podczas skanowania przeprowadzanego w przyszło ci.

Wy wietlanie aplikacji wykluczonych

Aplikacje wykluczone ze skanowania mo na wy wietla i usuwa z listy elementów wykluczonych, aby w przyszło ci były uwzgl dniane podczas skanowania.

Je li funkcja skanowania w czasie rzeczywistym lub skanowania r cznego wykryje aplikacj , która zachowuje si jak oprogramowanie szpieguj ce lub ryzykowne, ale u ytkownik wie, e jest ona bezpieczna, mo na wykluczy j ze skanowania, aby produkt nie wy wietlał wi cej ostrze e dotycz cych tej aplikacji.

Informacje: Je li aplikacja zachowuje si jak wirus lub inne zło liwe oprogramowanie, nie mo na jej wykluczy .

Aplikacji nie mo na wyklucza bezpo rednio. Nowe aplikacje s dodawane do listy wyklucze tylko wtedy, gdy zostan wykluczone podczas skanowania.

Aby wy wietli aplikacje wykluczone ze skanowania:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz, czy chcesz wy wietli aplikacje wykluczone ze skanowania w czasie rzeczywistym, czy skanowania r cznego:
   - Aby wy wietli aplikacje wykluczone ze skanowania w czasie rzeczywistym, wybierz kolejno opcje **Komputer** > **Skanowanie w poszukiwaniu wirusów**.
   - Aby wy wietli aplikacje wykluczone ze skanowania r cznego, wybierz kolejno opcje **Komputer** > **Skanowanie r czne**.

3. Kliknij opcj **Wyklucz pliki ze skanowania**.
4. Wybierz kart **Aplikacje**.

   Informacje: Ze skanowania mo na wykluczy tylko oprogramowanie szpieguj ce i ryzykowne, nie wirusy.

5. Aby ponownie przeskanowa wykluczone aplikacje, wykonaj nast puj ce czynno ci:
   a) Wybierz aplikacj , któr chcesz uwzgl dni podczas skanowania.
   b) Kliknij przycisk **Usu** .
6. Kliknij przycisk **OK**, aby zamkn okno dialogowe **Wykluczanie ze skanowania**.
7. Kliknij przycisk **OK**, aby zamkn okno.

Jak korzysta z funkcji kwarantanny?

Kwarantanna to bezpieczne repozytorium dla plików, które mog by szkodliwe.

Pliki poddane kwarantannie nie mog si rozprzestrzenia ani powodowa uszkodze komputera.

Kwarantannie mo na podda *zło liwe oprogramowanie*, *oprogramowanie szpieguj ce* oraz *ryzykowne oprogramowanie* w celu ich unieszkodliwienia. W razie potrzeby aplikacje i pliki mo na pó niej przywróci z kwarantanny.

Je li element poddany kwarantannie nie jest potrzebny, mo na go usun . Usuni cie elementu z kwarantanny powoduje jego trwałe usuni cie z komputera.

- Zazwyczaj u ytkownik mo e usuwa *zło liwe oprogramowanie* poddane kwarantannie.
- W wi kszo ci przypadków u ytkownik mo e usun *oprogramowanie szpieguj ce* poddane kwarantannie. Zdarza si , e *oprogramowanie szpieguj ce* poddane kwarantannie to cz nieszkodliwego programu i po usuni ciu go program ten przestaje działa poprawnie. Je li u ytkownik chce zachowa program na komputerze, mo e przywróci *oprogramowanie szpieguj ce* z kwarantanny.
- *Ryzykowne oprogramowanie* poddane kwarantannie mo e by nieszkodliwym programem. Je li u ytkownik sam zainstalował i skonfigurował ten program, mo e go przywróci z kwarantanny. Je li *ryzykowne oprogramowanie* zostało zainstalowane bez wiedzy u ytkownika, najprawdopodobniej zostało zainstalowane w zło liwym celu i powinno zosta usuni te.

Wy wietlanie elementów poddanych kwarantannie

Na temat elementów poddanych kwarantannie mo na wy wietla wi cej informacji.

Aby wy wietli szczegółowe informacje na temat elementów poddanych kwarantannie:

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. Kliknij opcj **Wy wietl kwarantann** .
   Na stronie **Kwarantanna** dost pne s informacje o ł cznej liczbie elementów w kwarantannie.
4. Aby wy wietli szczegółowe informacje na temat elementów poddanych kwarantannie, kliknij przycisk **Szczegóły**.

   Zawarto strony mo esz sortowa według nazwy zło liwego oprogramowania lub cie ki pliku.

   Na li cie wy wietlanych jest 100 pierwszych elementów wraz z informacjami o typach elementów poddanych kwarantannie, ich nazwach i cie kach instalacji plików.

5. Aby wy wietli dodatkowe informacje na temat obiektu poddanego kwarantannie, kliknij ikon obok wybranego obiektu w kolumnie **Stan**.

Przywracanie elementów poddanych kwarantannie

Potrzebne elementy mo na przywraca z kwarantanny.

Je li aplikacje lub pliki poddane kwarantannie s potrzebne, mo na je przywróci . Nie nale y przywraca adnych elementów poddanych kwarantannie, je li nie ma pewno ci, e nie stanowi one zagro enia. Przywrócone elementy s przenoszone z powrotem do oryginalnej lokalizacji na komputerze.

Przywracanie elementów poddanych kwarantannie

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. Kliknij opcj **Wy wietl kwarantann** .
4. Zaznacz elementy w kwarantannie do przywrócenia.
5. Kliknij pozycj **Przywró** .

Co to jest technologia DeepGuard?

Technologia DeepGuard analizuje zawarto plików i działanie aplikacji, a tak e monitoruje niezaufane programy.

Technologia DeepGuard blokuje nowe i dotychczas niewykryte *wirusy*, *robaki* i inne szkodliwe aplikacje, które próbuj wprowadza zmiany na komputerze, a tak e uniemo liwia podejrzanym aplikacjom dost p do Internetu.

W przypadku wykrycia przez technologi DeepGuard nowej aplikacji, która próbuje wprowadzi w systemie potencjalnie szkodliwe zmiany, taka aplikacja zostaje uruchomiona w bezpiecznej strefie. W bezpiecznej strefie aplikacja nie mo e uszkodzi komputera. Technologia DeepGuard analizuje zmiany, które aplikacja próbuje wprowadzi , i na tej podstawie okre la prawdopodobie stwo, czy ta aplikacja to *zło liwe oprogramowanie*. Je li aplikacja jest prawdopodobnie *zło liwym oprogramowaniem*, technologia DeepGuard blokuje j .

Potencjalne szkodliwe zmiany w systemie, które s wykrywane przez technologi DeepGuard, obejmuj :

- zmiany ustawie systemu (rejestru systemu Windows);
- próby wył czenia wa nych programów systemowych, na przykład programów zabezpieczaj cych, takich jak niniejszy produkt;
- próby edytowania wa nych plików systemowych.

Wł czanie i wył czanie funkcji DeepGuard

Aby uniemo liwi podejrzanym aplikacjom wprowadzanie potencjalnie szkodliwych zmian w systemie komputera, nale y mie wł czon funkcj DeepGuard.

W przypadku komputera z systemem Windows XP przed wł czeniem technologii DeepGuard nale y upewni si , e dodatek Service Pack 2 został zainstalowany.

Aby wł czy lub wył czy funkcj DeepGuard, wykonaj nast puj ce czynno ci:

1. Na stronie głównej kliknij opcj **Stan**.
2. Kliknij pozycj **Zmie ustawienia na tej stronie**.

   Informacje: Do wył czenia funkcji zabezpiecze wymagane s uprawnienia administratora.

3. Wł cz lub wył cz opcj **DeepGuard**.
4. Kliknij przycisk **Zamknij**.

Zezwalanie na aplikacje zablokowane przez funkcj DeepGuard

Aplikacje akceptowane i blokowane przez funkcj DeepGuard mo na kontrolowa .

Zdarza si , e funkcja DeepGuard blokuje uruchomienie aplikacji, z której u ytkownik chce skorzysta i o której wie, e jest bezpieczna. Dzieje si tak, poniewa aplikacja próbuje wprowadzi potencjalnie szkodliwe zmiany w systemie. Mo e si te zdarzy , e aplikacja zostanie przypadkowo zablokowana przez u ytkownika po wy wietleniu okna podr cznego funkcji DeepGuard.

Aby zezwoli na działanie aplikacji zablokowanej przez funkcj DeepGuard, wykonaj nast puj ce czynno ci:

1. Na stronie głównej kliknij opcj **Narz dzia**.
2. Kliknij pozycj **Aplikacje**.
   Zostanie wy wietlona lista **Aplikacje monitorowane**.
3. Znajd aplikacj , na uruchomienie której chcesz zezwoli .

   Informacje: Klikaj c nagłówki kolumn, mo esz sortowa list . Aby na przykład posortowa list według grup dozwolonych i zablokowanych programów, kliknij kolumn **Uprawnienie**.

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

Funkcja DeepGuard umo liwi aplikacji ponowne wprowadzanie zmian w systemie.

U ywanie funkcji DeepGuard w trybie zgodno ci

W celu zapewnienia maksymalnej ochrony funkcja DeepGuard tymczasowo modyfikuje uruchomione programy. Niektóre programy sprawdzaj , czy nie zostały uszkodzone lub zmodyfikowane, i mog nie by zgodne z t funkcj . Na przykład gry internetowe zawieraj ce narz dzia zapobiegaj ce oszukiwaniu po uruchomieniu stale sprawdzaj , czy nie zostały w jakikolwiek sposób zmodyfikowane. W takich przypadkach mo na wł czy tryb zgodno ci.

Aby wł czy tryb zgodno ci, wykonaj nast puj ce czynno ci:

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

   Informacje: Do zmiany tych ustawie wymagane s uprawnienia administratora.

2. Wybierz kolejno opcje **Zabezpieczenia komputera** > **DeepGuard**.
3. Wybierz opcj **U yj trybu zgodno ci**.
4. Kliknij przycisk **OK**.

Co robi w przypadku ostrze e o podejrzanych działaniach

Funkcja DeepGuard monitoruje niezaufane aplikacje. Je li taka aplikacja podejmie prób uzyskania dost pu do Internetu, wprowadzenia zmian w systemie lub wykonania podejrzanych działa , funkcja DeepGuard blokuje j .

Je li w ustawieniach funkcji DeepGuard wybrano opcj **Ostrzegaj o podejrzanych działaniach**, funkcja DeepGuard wy wietla powiadomienie, gdy wykryje potencjalnie szkodliw aplikacj lub gdy zostanie uruchomiona aplikacja o nieznanej reputacji.

Aby wybra czynno , która ma zosta wykonana w przypadku aplikacji zablokowanej przez funkcj DeepGuard, wykonaj nast puj ce czynno ci:

1. Kliknij opcj **Szczegóły**, aby wy wietli wi cej informacji o danym programie.
   W sekcji szczegółów s wy wietlane nast puj ce dane:
   - lokalizacja aplikacji,
   - reputacja aplikacji w sieci ochrony w czasie rzeczywistym,
   - stopie powszechno ci aplikacji.
2. Wybierz, czy aplikacja zablokowana przez funkcj DeepGuard jest zaufana:
   - Wybierz opcj **Ta aplikacja jest zaufana — kontynuuj**, je li nie chcesz blokowa aplikacji.

     Aplikacja jest prawdopodobnie bezpieczna, je li:
     - funkcja DeepGuard zablokowała t aplikacj w wyniku czynno ci wykonanej przez u ytkownika,
     - u ytkownik rozpoznaj aplikacj ,
     - aplikacja pochodzi z zaufanego ródła.
   - Wybierz opcj **Ta aplikacja nie jest zaufana. Zablokuj.**, je li aplikacja ma pozosta zablokowana.

     Aplikacja jest prawdopodobnie niebezpieczna, je li:
     - aplikacja nie jest powszechna,
     - aplikacja ma nieznan reputacj ,
     - u ytkownik nie zna aplikacji.
3. Je li chcesz przesła podejrzan aplikacj do analizy:
   a) Kliknij opcj **Zgło t aplikacj w firmie F-Secure**.
   Produkt wy wietli warunki dotycz ce przesłania próbki.
   b) Kliknij przycisk **Akceptuj** , je li akceptujesz warunki i chcesz przesła próbk .

   Wysłanie próbki jest zalecane, gdy:
   - funkcja DeepGuard zablokuje aplikacj , któr u ytkownik uwa a za bezpieczn ;
   - istnieje podejrzenie, e aplikacja mo e by *zło liwym oprogramowaniem*.