McAfee®

VirusScan® 2008

# Virus and Spyware Protection

## Podręcznik użytkownika

# Spis treści

**McAfee VirusScan** **3**

Program McAfee SecurityCenter ..... 5
Funkcje programu SecurityCenter ..... 6
Korzystanie z programu SecurityCenter ..... 7
Aktualizowanie oprogramowania SecurityCenter ..... 13
Naprawianie lub ignorowanie problemów dotyczących ochrony ..... 17
Praca z alertami ..... 23
Przeglądanie zdarzeń ..... 29
McAfee VirusScan ..... 31
Funkcje programu VirusScan ..... 33
Włączanie ochrony przed wirusami w czasie rzeczywistym ..... 34
Uruchamianie dodatkowej ochrony ..... 37
Konfigurowanie ochrony przed wirusami ..... 41
Skanowanie komputera ..... 59
Wykonywanie operacji na wynikach skanowania ..... 63
McAfee QuickClean ..... 67
Funkcje programu QuickClean ..... 68
Oczyszczanie komputera ..... 69
Defragmentowanie komputera ..... 73
Planowanie zadania ..... 74
Program McAfee Shredder ..... 81
Funkcje programu Shredder ..... 82
Niszczenie plików, folderów i zawartości dysków ..... 83
Program McAfee Network Manager ..... 85
Funkcje programu Network Manager ..... 86
Ikony programu Network Manager ..... 87
Konfigurowanie zarządzanej sieci ..... 89
Zdalne zarządzanie siecią ..... 97
Opis ..... 102

**Słownik** **103**

**Informacje o firmie McAfee** **119**

Copyright ..... 119
Licencja ..... 120
Biuro obsługi klienta i pomoc techniczna ..... 121
Korzystanie z narzędzia McAfee Virtual Technician ..... 122
Pomoc techniczna i produkty do pobrania ..... 123

**Indeks** **131**

ROZDZIAŁ 1

# McAfee VirusScan

Oprogramowanie VirusScan z programem SiteAdvisor zawiera zaawansowane usługi wykrywania i ochrony, które optymalizują zabezpieczenia komputera przed najnowszymi zagrożeniami bezpieczeństwa, takimi jak wirusy, konie trojańskie, śledzące pliki cookie, oprogramowanie szpiegujące, reklamowe i inne potencjalnie niepożądane programy. Oprogramowanie VirusScan obejmuje ochroną nie tylko pliki i foldery na komputerze stacjonarnym lub przenośnym, ale także chroni przed innymi zagrożeniami pochodzącymi z różnych źródeł, takich jak poczta e-mail, wiadomości błyskawiczne i sieć Web. Oceny bezpieczeństwa witryn sieci Web udostępniane przez program McAfee SiteAdvisor ułatwiają unikanie niebezpiecznych witryn.

## W tym rozdziale

Program McAfee SecurityCenter ..... 5
McAfee VirusScan ..... 31
McAfee QuickClean ..... 67
Program McAfee Shredder ..... 81
Program McAfee Network Manager ..... 85
Opis ..... 102
Informacje o firmie McAfee ..... 119
Biuro obsługi klienta i pomoc techniczna ..... 121

ROZDZIAŁ 2

# Program McAfee SecurityCenter

Program McAfee SecurityCenter umożliwia monitorowanie stanu zabezpieczeń komputera, przedstawia na bieżąco informacje o tym, czy usługi ochrony przed wirusami, oprogramowaniem szpiegującym, ochrona poczty e-mail oraz zapora są aktualne, a także podejmuje odpowiednie działania w celu zabezpieczenia przez powstaniem potencjalnych luk w zabezpieczeniach. Zawiera narzędzia i elementy nawigacyjne potrzebne do koordynowania wszystkich obszarów ochrony komputera i zarządzania nimi.

Przed rozpoczęciem konfigurowania mechanizmów ochrony komputera i zarządzania nimi należy zapoznać się z interfejsem oprogramowania SecurityCenter i przeanalizować różnice między stanami ochrony, jej rodzajami oraz usługami. Następnie należy zaktualizować program SecurityCenter w celu uzyskania z firmy McAfee najnowszej wersji mechanizmów ochronnych.

Po zakończeniu wstępnych zadań konfiguracyjnych można używać programu SecurityCenter do monitorowania stanu ochrony komputera. Jeśli ten pakiet wykryje problem dotyczący ochrony, ostrzega użytkownika, aby ten mógł go wyeliminować lub zignorować (w zależności od stopnia zagrożenia). Można również przeglądać w dzienniku zdarzenia programu SecurityCenter, takie jak zmiany w konfiguracji skanowania w poszukiwaniu wirusów.

**Uwaga:** Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

## W tym rozdziale

Funkcje programu SecurityCenter ..... 6
Korzystanie z programu SecurityCenter ..... 7
Aktualizowanie oprogramowania SecurityCenter ..... 13
Naprawianie lub ignorowanie problemów dotyczących ochrony ..... 17
Praca z alertami ..... 23
Przeglądanie zdarzeń ..... 29

# Funkcje programu SecurityCenter

Program SecurityCenter jest wyposażony w następujące funkcje:

### Uproszczone informacje o stanie ochrony

Łatwe przeglądanie informacji o stanie ochrony komputera, sprawdzanie dostępności aktualizacji i usuwanie potencjalnych problemów związanych z ochroną.

### Zautomatyzowane aktualizacje i uaktualnienia

Automatyczne pobieranie i instalowanie aktualizacji zarejestrowanych programów. Gdy tylko zostaje udostępniona nowa wersja zarejestrowanego programu firmy McAfee, użytkownik w okresie subskrypcji otrzymuje ją bezpłatnie w sposób automatyczny, co zapewnia ciągłą skuteczną ochronę przed najnowszymi zagrożeniami.

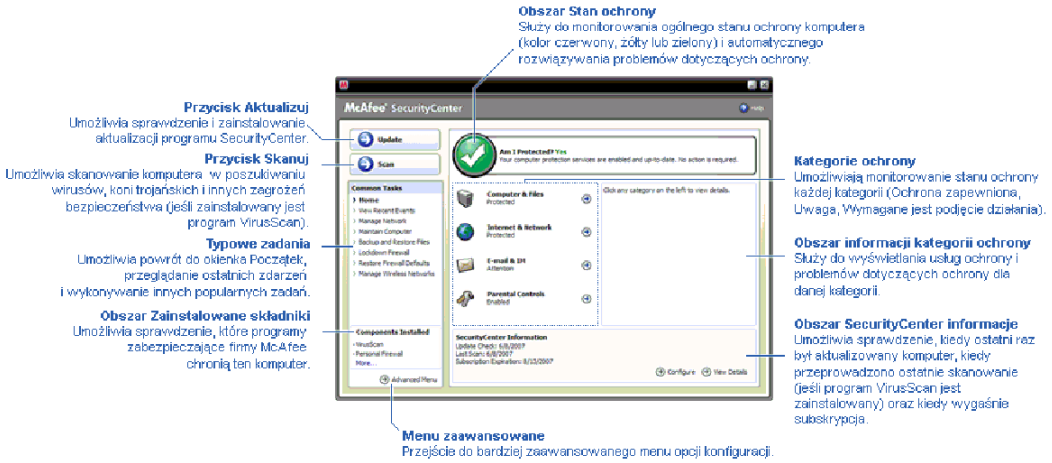
### Wyświetlanie na bieżąco alertów

Alerty zabezpieczeń powiadamiają o epidemiach wirusowych i zagrożeniach bezpieczeństwa oraz umożliwiają usunięcie, zneutralizowanie zagrożenia i uzyskanie dodatkowych informacji na jego temat.

ROZDZIAŁ 3

# Korzystanie z programu SecurityCenter

Przed rozpoczęciem korzystania z programu SecurityCenter należy zapoznać się ze wszystkimi składnikami i obszarami konfiguracji, które służą do zarządzania stanem ochrony komputera. Aby uzyskać więcej informacji na temat terminologii użytej na tej ilustracji, zobacz część *Jak działa stan ochrony* (strona 8) i część *Jak działają kategorie ochrony* (strona 9). Następnie można przejrzeć informacje na temat konta McAfee i sprawdzić ważność subskrypcji.




## W tym rozdziale

Jak działa stan ochrony ..... 8
Jak działają kategorie ochrony ..... 9
Jak działają usługi ochrony ..... 10
Zarządzanie kontem McAfee ..... 11

## Jak działa stan ochrony

Informacje o stanie ochrony komputera są widoczne w obszarze stanu ochrony w okienku Początek programu SecurityCenter. W tym miejscu można się dowiedzieć, czy komputer jest całkowicie chroniony przed najnowszymi zagrożeniami bezpieczeństwa i czy na jego stan mogą mieć wpływ zewnętrzne ataki, inne programy zabezpieczające oraz programy, które korzystają z sieci Internet.

Stanowi ochrony komputera mogą odpowiadać kolory: czerwony, żółty lub zielony.

| Stan ochrony | Opis |
|---|---|
| Czerwony | Komputer nie jest chroniony. Obszar stanu ochrony w okienku Początek programu SecurityCenter jest czerwony, co oznacza, że komputer nie jest chroniony. Program SecurityCenter zgłasza co najmniej jeden problem z zabezpieczeniami o znaczeniu krytycznym.<br><br>W celu uzyskania pełnej ochrony należy wyeliminować wszystkie problemy z zabezpieczeniami o znaczeniu krytycznym należące do wszystkich kategorii ochrony (stan kategorii problemu jest wyświetlany jako **Wymagane jest podjęcie działania**, również w kolorze czerwonym). Aby uzyskać więcej informacji na temat sposobu rozwiązywania problemów z ochroną, zobacz część *Naprawianie problemów dotyczących ochrony* (strona 18). |
| Żółty | Komputer jest częściowo chroniony. Obszar stanu ochrony w okienku Początek programu SecurityCenter jest żółty, co oznacza, że komputer nie jest chroniony. Program SecurityCenter zgłasza co najmniej jeden problem z zabezpieczeniami o znaczeniu mniejszym niż krytyczne.<br><br>W celu uzyskania pełnej ochrony należy wyeliminować lub zignorować niekrytyczne problemy z zabezpieczeniami należące do wszystkich kategorii ochrony. Aby uzyskać więcej informacji na temat sposobu rozwiązywania lub ignorowania problemów z zabezpieczeniami, zobacz część *Naprawianie lub ignorowanie problemów dotyczących ochrony* (strona 17). |
| Zielony | Komputer jest w pełni chroniony. Obszar stanu ochrony w okienku Początek programu SecurityCenter jest zielony, co oznacza, że komputer jest chroniony. Program SecurityCenter nie zgłasza żadnego problemu z zabezpieczeniami o znaczeniu krytycznym lub mniejszym.<br><br>Poszczególne kategorie ochrony zawierają listy usług, które chronią komputer. |

## Jak działają kategorie ochrony

Usługi ochrony oprogramowania SecurityCenter dzielą się na cztery kategorie: Komputer i pliki, Internet i sieć, Poczta e-mail i wiadomości błyskawiczne oraz Funkcje ochrony rodzicielskiej. Te kategorie ułatwiają przeglądanie i konfigurowanie usług związanych z zabezpieczeniami, które chronią komputer.

Po kliknięciu nazwy kategorii można skonfigurować należące do niej usługi związane z zabezpieczeniami oraz wyświetlić informacje o problemach wykrytych przez te usługi. Jeśli stan ochrony komputera jest czerwony lub żółty, co najmniej w jednej kategorii jest wyświetlany komunikat *Wymagane jest podjęcie działania* lub *Uwaga*, co wskazuje na wykrycie problemu w danej kategorii przez program SecurityCenter. Aby uzyskać więcej informacji na temat stanu ochrony, zobacz część *Jak działa stan ochrony* (strona 8).

| Kategoria ochrony | Opis |
|---|---|
| Komputer i pliki | Kategoria Komputer i pliki umożliwia skonfigurowanie następujących usług ochrony:<br>▪ Ochrona przed wirusami<br>▪ Ochrona przed programami potencjalnie niepożądanymi<br>▪ Monitory systemu<br>▪ Ochrona systemu Windows |
| Internet i sieć | Kategoria Internet i sieć umożliwia skonfigurowanie następujących usług ochrony:<br>▪ Ochrona przy użyciu zapory<br>▪ Ochrona tożsamości |
| Poczta e-mail i wiadomości błyskawiczne | Kategoria Poczta e-mail i wiadomości błyskawiczne umożliwia skonfigurowanie następujących usług ochrony:<br>▪ Ochrona poczty e-mail<br>▪ Ochrona przed spamem |
| Funkcje ochrony rodzicielskiej | Kategoria Funkcje ochrony rodzicielskiej umożliwia skonfigurowanie następujących usług ochrony:<br>▪ Blokowanie zawartości |

## Jak działają usługi ochrony

Usługi ochrony są podstawowymi składnikami programu SecurityCenter. Są one konfigurowane przez użytkownika w celu zapewnienia ochrony komputera. Usługi ochrony odpowiadają bezpośrednio programom firmy McAfee. Na przykład po zainstalowaniu programu VirusScan stają się dostępne następujące usługi: Ochrona przed wirusami, Ochrona przed programami potencjalnie niepożądanymi, Monitory systemu oraz Ochrona systemu Windows. Aby uzyskać szczegółowe informacje na temat tych konkretnych usług ochrony, zobacz Pomoc oprogramowania VirusScan.

Domyślnie wszystkie usługi ochrony związane z programem są włączone po jego zainstalowaniu, można jednak każdą z nich wyłączyć w dowolnym momencie. Na przykład po zainstalowaniu programu Privacy Service są włączane usługi Blokowanie zawartości oraz Ochrona tożsamości. Jeśli użytkownik nie zamierza używać usługi Blokowanie zawartości, może wyłączyć ją całkowicie. Można również tymczasowo wyłączyć usługę ochrony, wykonując zadania konfiguracyjne lub konserwacyjne.

# Zarządzanie kontem McAfee

Kontem McAfee można łatwo zarządzać za pomocą programu SecurityCenter, uzyskując dostęp do informacji o koncie i przeglądając je oraz sprawdzając bieżący stan subskrypcji.

**Uwaga:** Jeśli programy firmy McAfee zostały zainstalowane z dysku CD, należy zarejestrować je w witrynie sieci Web firmy McAfee, aby umożliwić skonfigurowanie lub zaktualizowanie konta McAfee. Tylko wtedy użytkownik jest upoważniony do otrzymywania regularnych automatycznych aktualizacji programu.

## Zarządzanie kontem McAfee

Dostęp do informacji o koncie McAfee (Moje konto) można łatwo uzyskać za pomocą programu SecurityCenter.

1. W obszarze **Typowe zadania** kliknij opcję **Moje konto**.
2. Zaloguj się na koncie McAfee.

## Weryfikowanie subskrypcji

Weryfikacja subskrypcji ma na celu upewnienie się, że jej okres nie minął.

- Kliknij prawym przyciskiem myszy ikonę programu SecurityCenter znajdującą się w obszarze powiadomień, z boku po prawej stronie paska zadań, następnie kliknij polecenie **Weryfikuj subskrypcję**.

ROZDZIAŁ 4

# Aktualizowanie oprogramowania SecurityCenter

Program SecurityCenter zapewnia najnowszą wersję zarejestrowanych programów firmy McAfee poprzez sprawdzanie ich dostępności i instalowanie aktualizacji w trybie online co cztery godziny. W zależności od zainstalowanych i zarejestrowanych programów aktualizacje online mogą obejmować najnowsze definicje wirusów oraz uaktualnienia dotyczące działalności hakerów, spamu, programów szpiegujących oraz ochrony prywatności. Sprawdzenie dostępności aktualizacji jest możliwe w dowolnym momencie w trakcie domyślnego okresu czterogodzinnego. Gdy program SecurityCenter sprawdza dostępność aktualizacji, użytkownik może kontynuować wykonywanie innych zadań.

Sposób, w jaki program SecurityCenter sprawdza i instaluje aktualizacje, można zmienić, ale nie jest to zalecane. Na przykład można skonfigurować program SecurityCenter tak, aby aktualizacje były pobierane, ale nie instalowane, bądź aby użytkownik był powiadamiany przed pobraniem lub zainstalowaniem aktualizacji. Można również wyłączyć automatyczne aktualizowanie.

**Uwaga:** Jeśli programy firmy McAfee zostały zainstalowane z dysku CD, regularne, automatyczne aktualizacje tych programów nie będą dostępne do momentu zarejestrowania ich na witrynie sieci Web firmy McAfee.

## W tym rozdziale

Sprawdzanie dostępności aktualizacji ..... 13
Konfigurowanie automatycznych aktualizacji ..... 14
Wyłączanie automatycznych aktualizacji ..... 14

## Sprawdzanie dostępności aktualizacji

Domyślnie program SecurityCenter automatycznie sprawdza dostępność aktualizacji co cztery godziny, gdy komputer jest podłączony do sieci Internet. Użytkownik może jednak sprawdzić dostępność aktualizacji w dowolnym momencie. Po wyłączeniu automatycznych aktualizacji należy regularnie sprawdzać dostępność aktualizacji.

- W okienku Początek programu SecurityCenter kliknij przycisk **Aktualizuj**.

**Wskazówka:** Dostępność aktualizacji można sprawdzać bez konieczności uruchamiania programu SecurityCenter, klikając prawym przyciskiem myszy ikonę programu SecurityCenter znajdującą się w obszarze powiadomień, z boku po prawej stronie paska zadań, a następnie klikając polecenie **Aktualizacje**.

## Konfigurowanie automatycznych aktualizacji

Gdy komputer jest podłączony do Internetu, program SecurityCenter domyślnie co cztery godziny automatycznie sprawdza, czy są dostępne aktualizacje, i instaluje je. Aby zmienić ten domyślny sposób działania, można skonfigurować program SecurityCenter do automatycznego pobierania aktualizacji i powiadamiania użytkownika, gdy aktualizacje są gotowe do zainstalowania, lub do powiadamiania przed pobraniem aktualizacji.

**Uwaga:** W celu sygnalizowania gotowości aktualizacji do pobrania lub zainstalowania program SecurityCenter używa alertów. Z poziomu alertów można pobrać aktualizacje, zainstalować je lub odroczyć. W przypadku aktualizowania programów z poziomu alertu może się pojawić monit o zweryfikowanie subskrypcji przed pobraniem i zainstalowaniem aktualizacji. Aby uzyskać więcej informacji, zobacz *Praca z alertami* (strona 23).

1 Otwórz okienko Konfiguracja programu SecurityCenter.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
   2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.

2 W okienku Konfiguracja programu SecurityCenter w obszarze **Opcja automatycznych aktualizacji jest wyłączona** kliknij przycisk **Włączone**, a następnie kliknij przycisk **Zaawansowane**.

3 Kliknij jeden z poniższych przycisków:

   - **Instaluj aktualizacje automatycznie i powiadamiaj mnie, gdy usługi zostaną zaktualizowane (zalecane)**
   - **Pobieraj aktualizacje automatycznie i powiadamiaj mnie, gdy są gotowe do zainstalowania**
   - **Powiadamiaj przed pobieraniem aktualizacji**

4 Kliknij przycisk **OK**.

## Wyłączanie automatycznych aktualizacji

Wyłączywszy automatyczne aktualizacje, użytkownik sam odpowiada za regularne sprawdzanie dostępności aktualizacji — w przeciwnym razie komputer nie będzie mieć najnowszych zabezpieczeń. Aby uzyskać informacje na temat ręcznego sprawdzania dostępności aktualizacji, zobacz *Sprawdzanie aktualizacji* (strona 13).

1 Otwórz okienko Konfiguracja programu SecurityCenter.

   Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.

**2** W okienku Konfiguracja programu SecurityCenter w obszarze **Opcja automatycznych aktualizacji jest włączona** kliknij przycisk **Wyłączone**.

**Wskazówka:** Automatyczne aktualizacje włącza się przez kliknięcie przycisku **Włączone** bądź wyczyszczenie pola wyboru **Wyłącz aktualizacje automatyczne i zezwól na ręczne sprawdzanie aktualizacji** w okienku Opcje aktualizacji.

ROZDZIAŁ 5

# Naprawianie lub ignorowanie problemów dotyczących ochrony

Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Krytyczne problemy dotyczące ochrony wymagają niezwłocznego działania i powodują obniżenie stanu ochrony (kolor jest zmieniany na czerwony). Niekrytyczne problemy dotyczące ochrony nie wymagają niezwłocznego działania i nie muszą, choć mogą, skutkować obniżeniem stanu ochrony (zależy to od typu problemu). Aby osiągnąć zielony stan ochrony, należy naprawić wszystkie problemy krytyczne oraz naprawić lub zignorować wszystkie problemy niekrytyczne. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician. Aby uzyskać więcej informacji na temat narzędzia McAfee Virtual Technician, zobacz Pomoc tego narzędzia.

## W tym rozdziale

Naprawianie problemów dotyczących ochrony .....18
Ignorowanie problemów dotyczących ochrony .....20

## Naprawianie problemów dotyczących ochrony

Większość problemów dotyczących zabezpieczeń jest naprawiana automatycznie, ale niektóre problemy wymagają interwencji użytkownika. Na przykład, jeśli ochrona przy użyciu zapory jest wyłączona, program SecurityCenter może ją włączyć automatycznie, lecz jeśli nie jest zainstalowana, trzeba ją zainstalować samodzielnie. W poniższej tabeli opisano kilka innych działań podejmowanych w przypadku ręcznego naprawiania problemów dotyczących ochrony:

| Problem | Action (Akcja) |
|---|---|
| Pełne skanowanie systemu nie zostało wykonane w przeciągu ostatnich 30 dni. | Ręczne przeskanowanie komputera. Aby uzyskać więcej informacji, zobacz Pomoc narzędzia VirusScan. |
| Pliki sygnatur wykrywania (DAT) są nieaktualne. | Ręczna aktualizacja zabezpieczeń. Aby uzyskać więcej informacji, zobacz Pomoc narzędzia VirusScan. |
| Program nie jest zainstalowany. | Instalacja programu z witryny sieci Web firmy McAfee lub dysku CD. |
| Brakuje pewnych składników programu. | Ponowna instalacja programu z witryny sieci Web firmy McAfee lub dysku CD. |
| Program nie jest zarejestrowany i nie może uzyskać pełnej ochrony. | Rejestracja programu w witrynie sieci Web firmy McAfee. |
| Ważność programu wygasła. | Sprawdzenie stanu swojego konta w witrynie sieci Web firmy McAfee. |

**Uwaga:** Często jeden problem dotyczący ochrony jest związany z więcej niż jedną kategorią ochrony. W takim przypadku naprawienie problemu w jednej kategorii powoduje usunięcie go z pozostałych kategorii.

### Automatyczne naprawianie problemów dotyczących ochrony

Program SecurityCenter automatycznie naprawia większość problemów dotyczących ochrony. Zmiany konfiguracji wprowadzane przez program SecurityCenter podczas automatycznego naprawiania problemów dotyczących ochrony nie są rejestrowane w dzienniku zdarzeń. Aby uzyskać więcej informacji na temat zdarzeń, zobacz *Przeglądanie zdarzeń* (strona 29).

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Strona główna programu SecurityCenter w obszarze stanu ochrony kliknij przycisk **Napraw**.

### *Ręczne naprawianie problemów dotyczących ochrony*

Jeśli jakieś problemy występują nadal mimo prób ich automatycznego naprawienia, można je naprawić ręcznie.

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Strona główna programu SecurityCenter kliknij kategorię ochrony, której dotyczy problem zgłaszany przez program SecurityCenter.
3. Kliknij łącze znajdujące się po opisie problemu.

## Ignorowanie problemów dotyczących ochrony

Problem niekrytyczny wykryty przez program SecurityCenter można naprawić lub zignorować. Inne problemy niekrytyczne (np. brak zainstalowanego oprogramowania antyspamowego lub produktu Privacy Service) są ignorowane automatycznie. Zignorowane problemy nie są wyświetlane w obszarze informacji danej kategorii ochrony w okienku Strona główna programu SecurityCenter, chyba że stan ochrony komputera jest zielony. Jeśli użytkownik zdecyduje, że zignorowany problem jednak powinien być wyświetlany w obszarze informacji danej kategorii ochrony, gdy stan ochrony komputera nie jest zielony, może włączyć jego wyświetlanie.

### Ignorowanie problemu dotyczącego ochrony

Jeśli użytkownik nie chce naprawić problemu niekrytycznego wykrytego przez program SecurityCenter, może go zignorować. Zignorowanie spowoduje usunięcie problemu z obszaru informacji danej kategorii ochrony w oknie programu SecurityCenter.

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Strona główna programu SecurityCenter kliknij kategorię ochrony, której dotyczy zgłoszony problem.
3. Kliknij łącze **Ignoruj** znajdujące się obok tego problemu dotyczącego ochrony.

### Wyświetlanie lub ukrywanie zignorowanych problemów

Zignorowany problem dotyczący ochrony można wyświetlać lub ukrywać, w zależności od stopnia zagrożenia.

1. Otwórz okienko Opcje alertów.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
   2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
   3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.
2. W okienku Konfiguracja programu SecurityCenter kliknij opcję **Zignorowane problemy**.
3. W okienku Zignorowane problemy wykonaj następujące czynności:
   - Aby ignorować problem, zaznacz jego pole wyboru.
   - Aby problem był zgłaszany w obszarze informacji danej kategorii ochrony, wyczyść jego pole wyboru.

4 Kliknij przycisk **OK**.

**Wskazówka:** Problem można zignorować także przez kliknięcie łącza **Ignoruj** znajdującego się obok zgłoszonego problemu w obszarze informacji danej kategorii ochrony.

ROZDZIAŁ 6

# Praca z alertami

Alerty to małe wyskakujące okna dialogowe wyświetlane w prawym dolnym rogu ekranu, gdy wystąpią określone zdarzenia programu SecurityCenter. Alert udostępnia szczegółowe informacje o zdarzeniu, a także zalecenia i opcje dotyczące rozwiązywania problemów, które mogą być związane z danym zdarzeniem. Niektóre alerty zawierają też łącza do dodatkowych informacji o zdarzeniu. Łącza te umożliwiają otwarcie ogólnoświatowej witryny sieci Web firmy McAfee lub wysłanie informacji do firmy McAfee w celu uzyskania rozwiązania problemu.

Dostępne są trzy typy alertów: czerwony, żółty i zielony.

| Typ alertu | Opis |
|---|---|
| Czerwony | Czerwony alert to krytyczne powiadomienie, które wymaga reakcji użytkownika. Czerwone alerty występują, gdy program SecurityCenter nie może określić, jak automatycznie rozwiązać dany problem dotyczący ochrony. |
| Żółty | Żółty alert to niekrytyczne powiadomienie, które zazwyczaj wymaga odpowiedzi ze strony użytkownika. |
| Zielony | Zielony alert to niekrytyczne powiadomienie, które nie wymaga reakcji użytkownika. Zielone alerty udostępniają podstawowe informacje o zdarzeniu. |

Ponieważ alerty są tak istotne dla monitorowania stanu ochrony i zarządzania nim, nie można ich wyłączyć. Można jednak określić, czy alerty informacyjne pewnych typów mają być wyświetlane, a także skonfigurować niektóre opcje alertów (na przykład, czy program SecurityCenter ma odtwarzać dźwięk, wyświetlając alert, lub czy podczas uruchamiania systemu ma być wyświetlany ekran powitalny programu firmy McAfee).

## W tym rozdziale

Wyświetlanie i ukrywanie alertów informacyjnych.....24
Konfigurowanie opcji alertów.....26

## Wyświetlanie i ukrywanie alertów informacyjnych

Alerty informacyjne powiadamiają o wystąpieniu zdarzeń, które nie powodują zagrożenia bezpieczeństwa komputera. Na przykład, jeśli została skonfigurowana ochrona przy użyciu zapory, alert informacyjny jest domyślnie wyświetlany za każdym razem, gdy jakiś program na komputerze uzyska dostęp do Internetu. Jeśli alert informacyjny pewnego typu nie ma być wyświetlany, można go ukryć. Jeśli żadne alerty informacyjne nie mają być wyświetlane, można ukryć je wszystkie. Można też ukryć wszystkie alerty informacyjne na czas korzystania z gier w trybie pełnoekranowym. Gdy użytkownik zakończy grę i zamknie tryb pełnoekranowy, program SecurityCenter ponownie zacznie wyświetlać alerty informacyjne.

Jeśli jakiś alert informacyjny zostanie ukryty przez pomyłkę, w każdej chwili można ponownie włączyć jego wyświetlanie. Domyślnie program SecurityCenter wyświetla wszystkie alerty informacyjne.

### Wyświetlanie lub ukrywanie alertów informacyjnych

Program SecurityCenter można skonfigurować tak, aby wyświetlał niektóre alerty informacyjne, a ukrywał inne, lub aby ukrywał wszystkie alerty informacyjne.

**1** Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

**2** W okienku Konfiguracja programu SecurityCenter kliknij opcję **Alerty informacyjne**.

**3** W okienku Alerty informacyjne wykonaj następujące czynności:

- Aby alert informacyjny był wyświetlany, wyczyść odpowiadające mu pole wyboru.
- Aby ukryć alert informacyjny, zaznacz odpowiadające mu pole wyboru.
- Aby ukryć wszystkie alerty informacyjne, zaznacz pole wyboru **Nie pokazuj alertów informacyjnych**.

**4** Kliknij przycisk **OK**.

**Wskazówka:** Alert informacyjny można ukryć także przez zaznaczenie pola wyboru **Nie wyświetlaj tego alertu ponownie** w samym oknie alertu. Aby później ponownie włączyć wyświetlanie tego alertu informacyjnego, należy wyczyścić odpowiednie pole wyboru w okienku Alerty informacyjne.

### *Wyświetlanie lub ukrywanie alertów informacyjnych na czas korzystania z gier*

Alerty informacyjne można ukryć na czas korzystania z gier w trybie pełnoekranowym na komputerze. Gdy użytkownik zakończy grę i zamknie tryb pełnoekranowy, program SecurityCenter ponownie zacznie wyświetlać alerty informacyjne.

**1** Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

**2** W okienku Opcje alertów zaznacz lub wyczyść pole wyboru **Pokaż alerty informacyjne, gdy zostanie wykryty tryb gier**.

**3** Kliknij przycisk **OK**.

## Konfigurowanie opcji alertów

Wygląd i częstotliwość alertów są konfigurowane przez program SecurityCenter; można jednak zmieniać niektóre podstawowe opcje alertów. Na przykład można włączyć odtwarzanie dźwięku wraz z alertem lub wyłączyć wyświetlanie ekranu powitalnego alertu podczas uruchamiania systemu Windows. Można też ukryć alerty powiadamiające o epidemiach wirusowych i innych zagrożeniach bezpieczeństwa społeczności online.

### Włączanie odtwarzania dźwięku podczas wyświetlania alertów

Jeśli wyświetleniu alertu ma towarzyszyć sygnał dźwiękowy, można skonfigurować program SecurityCenter do odtwarzania dźwięku w przypadku każdego alertu.

**1** Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

**2** W okienku Opcje alertów w obszarze **Dźwięk** zaznacz pole wyboru **Odtwórz dźwięk przy wystąpieniu alertu**.

### Ukrywanie ekranu powitalnego podczas uruchamiania

Domyślnie podczas uruchamiania systemu Windows jest przez krótką chwilę wyświetlany ekran powitalny programu firmy McAfee, powiadamiając użytkownika, że komputer jest chroniony przez program SecurityCenter. Ekran ten można jednak ukryć, jeśli się nie chce, by był wyświetlany.

**1** Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

**2** W okienku Opcje alertów w obszarze **Ekran powitalny** wyczyść pole wyboru **Pokazuj ekran powitalny firmy McAfee przy uruchamianiu systemu Windows**.

**Wskazówka:** W każdej chwili można ponownie włączyć wyświetlanie ekranu powitalnego, zaznaczając pole wyboru **Pokazuj ekran powitalny firmy McAfee przy uruchamianiu systemu Windows**.

### *Ukrywanie alertów o epidemiach wirusowych*

Alerty powiadamiające o epidemiach wirusowych i innych zagrożeniach bezpieczeństwa społeczności online można ukryć.

**1** Otwórz okienko Opcje alertów.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W prawym okienku w obszarze **SecurityCenter — informacje** kliknij polecenie **Konfiguruj**.
3. W obszarze **Alerty** kliknij przycisk **Zaawansowane**.

**2** W okienku Opcje alertów wyczyść pole wyboru **Powiadom, gdy pojawi się wirus lub zagrożenie bezpieczeństwa**.

**Wskazówka:** W każdej chwili można ponownie włączyć wyświetlanie alertów o epidemiach wirusowych, zaznaczając pole wyboru **Powiadom, gdy pojawi się wirus lub zagrożenie bezpieczeństwa**.

ROZDZIAŁ 7

# Przeglądanie zdarzeń

Zdarzenie jest akcją lub zmianą konfiguracji, która ma miejsce w ramach kategorii ochrony i jest związana z usługami ochrony. W przypadku różnych usług ochrony są rejestrowane różnego typu zdarzenia. Na przykład program SecurityCenter rejestruje zdarzenie, jeśli usługa ochrony zostanie włączona lub wyłączona, funkcja ochrony przed wirusami rejestruje zdarzenie za każdym razem, gdy wirus zostanie wykryty i usunięty, a funkcja ochrony przy użyciu zapory rejestruje zdarzenie za każdym razem, gdy zostanie zablokowana próba ustanowienia połączenia internetowego. Aby uzyskać więcej informacji na temat kategorii ochrony, zobacz *Jak działają kategorie ochrony* (strona 9).

Zdarzenia można przeglądać w celu rozwiązywania problemów z konfiguracją i przeglądania operacji wykonywanych przez innych użytkowników. Wielu rodziców monitoruje zachowania swoich dzieci w Internecie właśnie za pomocą dziennika zdarzeń. Jeśli chce się sprawdzić tylko ostatnie 30 zdarzeń, można wyświetlić tylko ostatnie zdarzenia. Jeśli chce się sprawdzić pełną listę wszystkich zdarzeń, można wyświetlić wszystkie zdarzenia. Dla potrzeb wyświetlenia wszystkich zdarzeń program SecurityCenter uruchamia dziennik zdarzeń posortowany według kategorii ochrony, w których dane zdarzenia miały miejsce.

## W tym rozdziale

Wyświetlanie ostatnich zdarzeń ..... 29
Wyświetlanie wszystkich zdarzeń ..... 30

## Wyświetlanie ostatnich zdarzeń

Jeśli chce się sprawdzić tylko ostatnie 30 zdarzeń, można wyświetlić tylko ostatnie zdarzenia.

- W obszarze **Typowe zadania** kliknij opcję **Przeglądaj ostatnie zdarzenia**.

## *Wyświetlanie wszystkich zdarzeń*

Jeśli chce się sprawdzić pełną listę wszystkich zdarzeń, można wyświetlić wszystkie zdarzenia.

1 W obszarze **Typowe zadania** kliknij opcję **Przeglądaj ostatnie zdarzenia**.

2 W okienku Ostatnie zdarzenia kliknij opcję **Wyświetl dziennik**.

3 W lewym okienku okna dziennika zdarzeń kliknij typ zdarzeń, które chcesz przejrzeć.

ROZDZIAŁ 8

# McAfee VirusScan

Zaawansowane usługi wykrywania i ochrony udostępniane przez program VirusScan bronią użytkownika i jego komputer przed najnowszymi zagrożeniami bezpieczeństwa, takimi jak wirusy, konie trojańskie, śledzące pliki cookie, oprogramowanie szpiegujące, oprogramowanie reklamowe i inne potencjalnie niepożądane programy. Ochrona wykracza poza pliki i foldery znajdujące się na komputerze, eliminując zagrożenia z różnych punktów wejścia — poczty e-mail, wiadomości błyskawicznych i sieci Web.

Dzięki programowi VirusScan ochrona komputera działa natychmiastowo i stale (nie są wymagane żadne uciążliwe czynności administracyjne). Gdy użytkownik pracuje, korzysta z gier, przegląda sieć Web i sprawdza pocztę e-mail, program ten działa w tle, monitorując, skanując i wykrywając potencjalne zagrożenia w czasie rzeczywistym. Okresowo, według harmonogramu, jest wykonywane wszechstronne skanowanie w celu sprawdzenia komputera przy użyciu bardziej zaawansowanego zestawu opcji. Sposób działania programu VirusScan w tym zakresie można dostosowywać, lecz jeśli użytkownik nie skorzysta z tej możliwości, komputer i tak będzie chroniony.

Podczas normalnego użytkowania komputera mogą się do niego dostać wirusy, robaki i inne potencjalne źródła zagrożenia. Gdy tak się stanie, program VirusScan powiadamia użytkownika o zagrożeniu, ale zwykle sam sobie radzi z problemem, czyszcząc i poddając kwarantannie zainfekowane elementy, zanim dojdzie do uszkodzenia systemu. Czasami mogą być konieczne dodatkowe działania. W takich przypadkach program VirusScan pozostawia użytkownikowi decyzję, co robić (ponownie wykonać skanowanie po następnym uruchomieniu komputera, zachować wykryty element czy usunąć go).

**Uwaga:** Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

## W tym rozdziale

Funkcje programu VirusScan....33
Włączanie ochrony przed wirusami w czasie rzeczywistym....34
Uruchamianie dodatkowej ochrony....37
Konfigurowanie ochrony przed wirusami....41
Skanowanie komputera....59
Wykonywanie operacji na wynikach skanowania....63

# Funkcje programu VirusScan

Program VirusScan jest wyposażony w następujące funkcje.

## Wszechstronna ochrona przed wirusami

Zaawansowane usługi wykrywania i ochrony udostępniane przez program VirusScan bronią użytkownika i jego komputer przed najnowszymi zagrożeniami bezpieczeństwa, takimi jak wirusy, konie trojańskie, śledzące pliki cookie, oprogramowanie szpiegujące, oprogramowanie reklamowe i inne potencjalnie niepożądane programy. Ochrona wykracza poza pliki i foldery znajdujące się na komputerze, eliminując zagrożenia z różnych punktów wejścia — poczty e-mail, wiadomości błyskawicznych i sieci Web. Nie są wymagane żadne uciążliwe czynności administracyjne.

## Opcje skanowania z rozpoznawaniem zasobów

Jeśli skanowanie przebiega powoli, można wyłączyć opcję używania minimalnych zasobów komputera, pamiętając jednak, że wówczas ochrona przed wirusami będzie miała priorytet przed innymi zadaniami. Program VirusScan umożliwia dostosowywanie opcji skanowania w czasie rzeczywistym i skanowania ręcznego, lecz jeśli użytkownik nie skorzysta z tej możliwości, komputer i tak będzie chroniony.

## Automatyczne naprawy

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje zagrożenie bezpieczeństwa, próbuje automatycznie je usunąć w sposób odpowiedni dla rodzaju zagrożenia. Dzięki temu większość zagrożeń może być wykrywana i neutralizowana bez udziału użytkownika. Czasami program VirusScan może nie być w stanie zneutralizować zagrożenia. W takich przypadkach program VirusScan pozostawia użytkownikowi decyzję, co robić (ponownie wykonać skanowanie po następnym uruchomieniu komputera, zachować wykryty element czy usunąć go).

## Wstrzymywanie zadań w trybie pełnoekranowym

Podczas oglądanie filmów i korzystania z gier lub podczas wykonywania innych czynności, które zajmują cały ekran komputera, program VirusScan wstrzymuje pewną liczbę zadań, w tym aktualizacje automatyczne i skanowanie ręczne.

# Włączanie ochrony przed wirusami w czasie rzeczywistym

Program VirusScan zapewnia dwa rodzaje ochrony przed wirusami: w czasie rzeczywistym i ręczną. Ochrona przed wirusami w czasie rzeczywistym stale monitoruje komputer pod kątem działalności wirusów, skanując pliki za każdym razem, gdy użytkownik lub jego komputer próbuje uzyskać do nich dostęp. Ręczna ochrona przed wirusami pozwala na skanowanie plików na żądanie. Aby mieć pewność, że komputer jest chroniony przed najnowszymi zagrożeniami bezpieczeństwa, należy pozostawić włączoną ochronę przed wirusami w czasie rzeczywistym i skonfigurować harmonogram regularnego, bardziej wszechstronnego skanowania ręcznego. Domyślnie raz w tygodniu uruchamiane jest w programie VirusScan skanowanie zaplanowane. Aby uzyskać więcej informacji na temat skanowania w czasie rzeczywistym i ręcznego, zobacz *Skanowanie komputera* (strona 59).

Czasami może być konieczne tymczasowe zatrzymanie skanowania w czasie rzeczywistym (na przykład po to, by zmienić jakieś opcje skanowania lub rozwiązać problem dotyczący wydajności). Jeśli ochrona przed wirusami w czasie rzeczywistym jest wyłączona, komputer nie jest chroniony i w programie SecurityCenter jest sygnalizowany czerwony stan ochrony. Aby uzyskać więcej informacji na temat stanu ochrony, zobacz „Jak działa stan ochrony” w Pomocy programu SecurityCenter.

## Włączanie ochrony przed wirusami w czasie rzeczywistym

Domyślnie ochrona przed wirusami w czasie rzeczywistym jest włączona i chroni komputer przed wirusami, końmi trojańskimi i innymi zagrożeniami bezpieczeństwa. Jeśli ochrona przed wirusami w czasie rzeczywistym zostanie wyłączona, trzeba ją włączyć z powrotem, aby komputer był chroniony.

1. Otwórz okienko konfiguracji Komputer i pliki.

   Jak to zrobić?

   1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
   2. Kliknij przycisk **Konfiguruj**.
   3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

2. W polu **Ochrona przed wirusami** kliknij opcję **Włączona**.

## *Zatrzymywanie ochrony przed wirusami w czasie rzeczywistym*

Ochronę przed wirusami w czasie rzeczywistym można tymczasowo wyłączyć, a następnie określić, kiedy ma zostać wznowiona. Ochrona może zostać wznowiona automatycznie po 15, 30, 45 lub 60 minutach, gdy komputer zostanie uruchomiony ponownie lub nigdy.

**1** Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

**2** W polu **Ochrona przed wirusami** kliknij opcję **Wyłączona**.

**3** W oknie dialogowym wybierz, kiedy skanowanie w czasie rzeczywistym ma zostać wznowione.

**4** Kliknij przycisk **OK**.

ROZDZIAŁ 9

# Uruchamianie dodatkowej ochrony

Oprócz ochrony przed wirusami w czasie rzeczywistym program VirusScan zapewnia zaawansowaną ochronę przed skryptami, oprogramowaniem szpiegującym, potencjalnie szkodliwymi wiadomościami oraz załącznikami przesyłanymi przez komunikatory internetowe. Funkcje skanowania skryptów, oprogramowania szpiegującego, wiadomości e-mail i wiadomości błyskawicznych są domyślnie włączone i zapewniają ochronę komputera.

## Ochrona przez skanowanie skryptów

Ochrona przez skanowanie skryptów wykrywa potencjalnie szkodliwe skrypty i uniemożliwia ich wykonywanie na komputerze. Funkcja monitoruje komputer w poszukiwaniu podejrzanej aktywności skryptów, takiej jak tworzenie, kopiowanie i usuwanie plików czy otwieranie rejestru systemu Windows, a następnie ostrzega użytkownika przed mogącym wystąpić uszkodzeniem.

## Ochrona przed oprogramowaniem szpiegującym

Ochrona przed oprogramowaniem szpiegującym wykrywa oprogramowanie szpiegujące, reklamowe i inne potencjalnie niepożądane programy. Oprogramowanie szpiegujące to potajemnie zainstalowane na komputerze programy, które monitorują zachowanie użytkownika, zbierają informacje osobiste, a nawet ograniczają kontrolę nad komputerem poprzez instalowanie dodatkowego oprogramowania czy przekierowanie żądań przeglądarki.

## Ochrona poczty e-mail

Ochrona poczty e-mail wykrywa podejrzaną aktywność w wysyłanych i odbieranych wiadomościach e-mail oraz załącznikach.

## Ochrona wiadomości błyskawicznych

Ochrona wiadomości błyskawicznych wykrywa potencjalnie niebezpieczne zagrożenia w odbieranych załącznikach przesyłanych przez komunikatory. Funkcja blokuje także programy wiadomości błyskawicznych przed udostępnianiem informacji osobistych.

## W tym rozdziale

Uruchamianie ochrony przez skanowanie skryptów.....38
Uruchamianie ochrony przed oprogramowaniem szpiegującym.....38
Uruchamianie ochrony poczty e-mail .....39
Uruchamianie ochrony wiadomości błyskawicznych .....39

## Uruchamianie ochrony przez skanowanie skryptów

Włączenie ochrony przez skanowanie skryptów umożliwia wykrywanie potencjalnie szkodliwych skryptów i uniemożliwia ich wykonywanie na komputerze. Ochrona przez skanowanie skryptów ostrzega użytkownika, gdy skrypt próbuje utworzyć, skopiować lub usunąć pliki na komputerze bądź wprowadzić zmiany w rejestrze systemu Windows.

**1** Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

**2** W polu **Ochrona przez skanowanie skryptów** kliknij opcję **Włączona**.

**Uwaga:** Ochronę przez skanowanie skryptów można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie szkodliwych skryptów.

## Uruchamianie ochrony przed oprogramowaniem szpiegującym

Włączenie ochrony przed oprogramowaniem szpiegującym umożliwia wykrywanie i usuwanie programów szpiegujących i reklamowych oraz innych potencjalnie niepożądanych programów, które gromadzą i wysyłają dane bez wiedzy i zgody użytkowników.

**1** Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

**2** W polu **Ochrona przez skanowanie skryptów** kliknij opcję **Włączona**.

**Uwaga:** Ochronę przed oprogramowaniem szpiegującym można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie potencjalnie niepożądanych programów.

## Uruchamianie ochrony poczty e-mail

Włączenie ochrony poczty e-mail umożliwia wykrywanie robaków, a także potencjalnych zagrożeń w wychodzących (SMTP) i przychodzących (POP3) wiadomościach e-mail oraz załącznikach.

1 Otwórz okienko konfiguracji Poczta e-mail i wiadomości błyskawiczne.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.

2 W polu **Ochrona poczty e-mail** kliknij opcję **Włączona**.

**Uwaga:** Ochronę poczty e-mail można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie zagrożeń w wiadomościach e-mail.

## Uruchamianie ochrony wiadomości błyskawicznych

Włączenie ochrony wiadomości błyskawicznych umożliwia wykrywanie zagrożeń bezpieczeństwa w wychodzących i przychodzących załącznikach przesyłanych przez komunikatory internetowe.

1 Otwórz okienko konfiguracji Poczta e-mail i wiadomości błyskawiczne.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Poczta e-mail i wiadomości błyskawiczne**.

2 Pod polu **Ochrona wiadomości błyskawicznych** kliknij opcję **Włączona**.

**Uwaga:** Ochronę wiadomości błyskawicznych można wyłączyć w dowolnym momencie, jednak spowoduje to, że komputer będzie narażony na działanie szkodliwych załączników przesyłanych przez komunikatory internetowe.

ROZDZIAŁ 10

# Konfigurowanie ochrony przed wirusami

Program VirusScan zapewnia dwa rodzaje ochrony przed wirusami: skanowanie w czasie rzeczywistym i ręczne. Funkcja ochrony przed wirusami w czasie rzeczywistym skanuje pliki za każdym razem, gdy użytkownik lub system próbują uzyskać do nich dostęp. Ręczna ochrona przed wirusami pozwala na skanowanie plików na żądanie. Dla każdego rodzaju ochrony można ustawić różne opcje. Na przykład, ponieważ ochrona w czasie rzeczywistym ciągle monitoruje komputer, to można wybrać dla niej pewien podstawowy zestaw opcji skanowania, zachowując bardziej szeroki zestaw opcji skanowania dla ochrony ręcznej, uruchamianej na żądanie.

## W tym rozdziale

Ustawianie opcji skanowania w czasie rzeczywistym .....42
Ustawianie opcji skanowania ręcznego.....44
Korzystanie z opcji aplikacji SystemGuard .....48
Używanie list zaufanych .....55

## Ustawianie opcji skanowania w czasie rzeczywistym

Po uruchomieniu ochrony przed wirusami w czasie rzeczywistym program VirusScan używa domyślnego zestawu opcji, które użytkownik może zmienić stosownie do swoich potrzeb.

Aby zmienić opcje skanowania w czasie rzeczywistym, należy podjąć decyzję dotyczącą tego, co będzie sprawdzane przez program VirusScan podczas skanowania oraz określić lokalizacje i typy skanowanych plików. Na przykład można określić, czy program VirusScan ma szukać nieznanych wirusów lub plików cookie, których witryny sieci Web mogą używać do śledzenia zachowania użytkownika, lub czy ma skanować dyski sieciowe zmapowane na komputerze czy tylko dyski lokalne. Można także określić, jakie typy plików mają być skanowane (wszystkie pliki czy tylko pliki programów i dokumentów, w których wykrywanych jest najwięcej wirusów).

Zmieniając opcje skanowania w czasie rzeczywistym, należy także określić, czy ma zostać włączona funkcja ochrony bufora przed przepełnieniem. Bufor to części pamięci używana przez komputer do tymczasowego przechowywania danych. Przepełnienia buforów mogą występować, gdy ilość informacji przechowywanych w buforze przez podejrzane programy lub procesy przekracza pojemność buforu. W przypadku wystąpienia takiego przepełnienia, komputer staje się bardziej narażony na ataki na zabezpieczenia.

### Ustawianie opcji skanowania w czasie rzeczywistym

Opcje skanowania w czasie rzeczywistym ustawia się, aby dostosować to, czego program VirusScan będzie szukał podczas skanowania w czasie rzeczywistym, oraz określić lokalizacje i typy skanowanych plików. Opcje obejmują skanowanie nieznanych wirusów i śledzenie plików cookie, a także ochronę przed przepełnieniem bufora. Można też skonfigurować skanowanie w czasie rzeczywistym tak, aby były sprawdzane dyski sieciowe zmapowane na komputerze.

**1** Otwórz okienko Skanowanie w czasie rzeczywistym.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.

**2** Określ opcje skanowania w czasie rzeczywistym, a następnie kliknij przycisk **OK**.

| Aby... | Wykonaj następujące czynności: |
|---|---|
| Wykrywać nieznane wirusy i nowe warianty znanych wirusów | Zaznacz pole wyboru **Skanuj w poszukiwaniu nieznanych wirusów przy użyciu heurystyk**. |
| Wykrywać pliki cookie | Zaznacz pole wyboru **Skanuj i usuwaj śledzące pliki cookie**. |
| Wykrywać wirusy i inne potencjalne zagrożenia na dyskach sieciowych | Zaznacz pole wyboru **Skanuj dyski sieciowe**. |
| Chronić komputer przed przepełnieniem bufora | Zaznacz pole wyboru **Włącz ochronę przed przepełnieniem buforu**. |
| Określić typy plików, które będą skanowane | Zaznacz opcję **Wszystkie pliki (zalecane)** lub **Tylko pliki programów i dokumenty**. |

## Ustawianie opcji skanowania ręcznego

Ręczna ochrona przed wirusami pozwala na skanowanie plików na żądanie. Po uruchomieniu skanowania ręcznego program VirusScan sprawdza komputer w poszukiwaniu wirusów i innych potencjalnie szkodliwych elementów przy użyciu szerszego zestawu opcji skanowania. Aby zmienić opcje skanowania ręcznego, należy podjąć decyzję dotyczącą tego, co będzie sprawdzane przez program VirusScan podczas skanowania. Na przykład można określić, czy program VirusScan ma szukać nieznanych wirusów, potencjalnie niepożądanych programów (takich jak oprogramowanie szpiegujące i reklamowe), programów typu stealth (takich jak rootkit, które mogą przyznawać nieupoważniony dostęp do komputera) oraz plików cookie (których witryny sieci Web mogą używać do śledzenia zachowania użytkownika). Należy także zdecydować o tym, jakie typu plików mają być sprawdzane. Na przykład można określić, czy program VirusScan ma sprawdzać wszystkie pliki czy tylko pliki programów i dokumentów (w których wykrywanych jest najwięcej wirusów). Oprócz tego można określić, czy mają być skanowane pliki archiwów (np. pliki ZIP).

Domyślnie program VirusScan po uruchomieniu skanowania ręcznego sprawdza wszystkie dyski i foldery w komputerze, jednak domyślne lokalizacje można zmienić, dostosowując je do własnych potrzeb. Na przykład można skanować tylko krytyczne pliki systemowe, elementy znajdujące się na pulpicie lub w folderze Program Files. Jeśli użytkownik nie chce być odpowiedzialny za samodzielne uruchamianie skanowania ręcznego, może skonfigurować uruchamianie skanowania według harmonogramu. Zaplanowane skanowania zawsze sprawdzają cały komputer, używając domyślnych opcji skanowania. Domyślnie raz w tygodniu uruchamiane jest w programie VirusScan skanowanie zaplanowane.

Jeśli szybkość skanowania będzie mała, można rozważyć wyłączenie opcji używania minimalnych zasobów komputera, jednak należy pamiętać, że zadanie ochrony przed wirusami będzie miało wyższy priorytet niż inne zadania wykonywane na komputerze.

**Uwaga:** Podczas oglądanie filmów i korzystania z gier lub podczas wykonywania innych czynności, które zajmują cały ekran komputera, program VirusScan wstrzymuje pewną liczbę zadań, w tym aktualizacje automatyczne i skanowanie ręczne.

### Ustawianie opcji skanowania ręcznego

Opcje skanowania ręcznego ustawia się, aby dostosować to, czego program VirusScan będzie szukał podczas skanowania ręcznego, oraz określić lokalizacje i typy skanowanych plików. Opcje obejmują skanowanie nieznanych wirusów, plików archiwów, oprogramowania szpiegującego i potencjalnie niepożądanych programów, śledzenie plików cookie oraz programów typu rootkit i stealth.

**1** Otwórz okienko Skanowanie ręczne.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Skanowanie ręczne** w okienku Ochrona przed wirusami.

**2** Określ opcje skanowania ręcznego, a następnie kliknij przycisk **OK**.

| Aby... | Wykonaj następujące czynności: |
|---|---|
| Wykrywać nieznane wirusy i nowe warianty znanych wirusów | Zaznacz pole wyboru **Skanuj w poszukiwaniu nieznanych wirusów przy użyciu heurystyk**. |
| Wykrywać i usuwać wirusy w plikach ZIP i innych archiwach | Zaznacz pole wyboru **Skanuj pliki .zip i inne pliki archiwów**. |
| Wykrywać oprogramowanie szpiegujące, reklamowe i inne potencjalnie niepożądane programy | Zaznacz pole wyboru **Skanuj w poszukiwaniu programów szpiegujących i potencjalnie niepożądanych**. |
| Wykrywać pliki cookie | Zaznacz pole wyboru **Skanuj i usuwaj śledzące pliki cookie**. |
| Wykrywać programy typu rootkit i stealth, które mogą zmienić i wykorzystać istniejące pliki systemu Windows | Zaznacz pole wyboru **Skanuj w poszukiwaniu programów typu rootkit i stealth**. |
| Wykorzystywać mniejszą moc obliczeniową procesora podczas skanowania, umożliwiając innym zadaniom (takim jak przeglądanie sieci Web czy otwieranie dokumentów) uzyskanie wyższego priorytetu | Zaznacz pole wyboru **Skanuj, używając minimalnej ilości zasobów komputera**. |
| Określić typy plików, które będą skanowane | Zaznacz opcję **Wszystkie pliki (zalecane)** lub **Tylko pliki programów i dokumenty**. |

### *Ustawianie lokalizacji skanowania ręcznego*

Lokalizację skanowania ręcznego ustawia się, aby określić, gdzie program VirusScan będzie szukał wirusów i innych szkodliwych elementów podczas skanowania ręcznego. Można skanować wszystkie pliki, foldery i dyski w komputerze lub ograniczyć skanowanie do konkretnych folderów i dysków.

**1** Otwórz okienko Skanowanie ręczne.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Skanowanie ręczne** w okienku Ochrona przed wirusami.

**2** Kliknij opcję **Domyślna lokalizacja do skanowania**.

**3** Określ lokalizację skanowania ręcznego, a następnie kliknij przycisk **OK**.

| **Aby...** | **Wykonaj następujące czynności:** |
|---|---|
| Skanować wszystkie pliki i foldery w komputerze | Zaznacz pole wyboru **(Mój) Komputer**. |
| Skanować konkretne pliki, foldery i dyski w komputerze | Usuń zaznaczenie pola wyboru **(Mój) Komputer** i wybierz jeden albo więcej folderów lub dysków. |
| Skanować krytyczne pliki systemowe | Usuń zaznaczenie pola wyboru **(Mój) Komputer** i zaznacz pole wyboru **Krytyczne pliki systemowe**. |

### *Planowanie skanowania*

Możliwe jest zaplanowanie skanowania na dowolną godzinę i dzień tygodnia w celu kompleksowego sprawdzenia komputera pod kątem obecności wirusów i innych zagrożeń. Zaplanowane skanowania zawsze sprawdzają cały komputer, używając domyślnych opcji skanowania. Domyślnie raz w tygodniu uruchamiane jest w programie VirusScan skanowanie zaplanowane. Jeśli szybkość skanowania będzie mała, można rozważyć wyłączenie opcji używania minimalnych zasobów komputera, jednak należy pamiętać, że zadanie ochrony przed wirusami będzie miało wyższy priorytet niż inne zadania wykonywane na komputerze.

**1** Otwórz okienko Zaplanowane skanowanie.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Zaplanowane skanowanie** w okienku Ochrona przed wirusami.

**2** Zaznacz opcję **Włącz zaplanowane skanowanie**.

**3** Aby zmniejszyć moc obliczeniową procesora wykorzystywaną normalnie do skanowania, zaznacz opcję **Skanuj, używając minimalnej ilości zasobów komputera**.

**4** Wybierz jeden lub większą liczbę dni.

**5** Określ godzinę rozpoczęcia.

**6** Kliknij przycisk **OK**.

**Wskazówka:** Domyślny harmonogram można przywrócić, klikając przycisk **Resetuj**.

## *Korzystanie z opcji aplikacji SystemGuard*

Aplikacje SystemGuard monitorują, rejestrują w dzienniku i raportują potencjalnie nieupoważnione zmiany wykonane w rejestrze systemu Windows lub w krytycznych plikach systemowych oraz umożliwiają zarządzanie tymi zmianami. Nieuprawnione zmiany w rejestrze i plikach mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych.

Zmiany w rejestrze i plikach są operacjami typowymi i często występującymi na komputerze. Ponieważ wiele takich zmian jest niebezpiecznych, domyślne ustawienia aplikacji SystemGuard są tak skonfigurowane, aby zapewnić pewną, inteligentną i rzeczywistą ochronę przed nieupoważnionymi zmianami, które wydają się być niebezpieczne. Na przykład gdy aplikacje SystemGuard wykryją zmiany, które są nietypowe i stwarzają potencjalnie znaczne zagrożenie, ich aktywność jest natychmiast rejestrowana w dzienniku i tworzone są raporty. Zmiany, które są bardziej typowe, ale ciągle stwarzają pewną potencjalną możliwość powstania uszkodzeń, są tylko rejestrowane. Natomiast monitorowanie zmian typowych i o niskim zagrożeniu jest domyślnie wyłączone. Technologia aplikacji SystemGuard może zostać skonfigurowana w celu rozciągnięcia ochrony na dowolne środowisko.

Istnieją trzy rodzaje aplikacji SystemGuard: Programowi strażnicy systemu, aplikacje SystemGuard z kategorii Windows oraz Strażnicy systemu dla przeglądarki.

### Programowi strażnicy systemu

Programowi strażnicy systemu wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Te ważne elementy rejestru i pliki obejmują instalacje formantów ActiveX, elementy uaktywniane podczas uruchamiania systemu, uchwyty uruchamiania powłoki systemu Windows oraz opóźnione ładowanie obiektów usług powłoki. Monitorując te elementy, Programowi strażnicy systemu oprócz oprogramowania szpiegującego i potencjalnie niepożądanych programów zatrzymują także podejrzane formanty ActiveX (pobrane z Internetu), które mogą uruchamiać się automatycznie wraz ze startem systemu Windows.

## Aplikacje SystemGuard z kategorii Windows

Aplikacje SystemGuard z kategorii Windows także wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Te ważne elementy rejestru i pliki obejmują programy obsługi menu kontekstowego, biblioteki DLL AppInit oraz plik Hosts systemu Windows. Monitorując te elementy, aplikacje SystemGuard z kategorii Windows pomagają w zapobieganiu przed wysyłaniem i odbieraniem nieupoważnionych informacji z komputera przez Internet. Oprócz tego pomagają także w zatrzymywaniu podejrzanych programów, które wprowadzają niepożądane zmiany do wyglądu i działania programów ważnych dla użytkowników komputera.

## Strażnicy systemu dla przeglądarki

Strażnicy systemu dla przeglądarki, podobnie jak aplikacje z kategorii Program i Windows, także wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Strażnicy systemu dla przeglądarki monitorują także zmiany w ważnych pozycjach rejestru i plikach, takich jak dodatki do programu Internet Explorer, adresy URL programu Internet Explorer oraz strefy zabezpieczeń programu Internet Explorer. Monitorując te elementy, Strażnicy systemu dla przeglądarki pomagają w zapobieganiu nieupoważnionym działaniom przeglądarki, takim jak przekierowania do podejrzanych witryn sieci Web, zmiany opcji i ustawień przeglądarki bez wiedzy użytkownika czy niepożądane dodawanie podejrzanych witryn sieci Web do zaufanych.

### *Włącz ochronę za pomocą aplikacji SystemGuard*

Włączenie aplikacji SystemGuard umożliwia wykrywanie potencjalnie nieupoważnionych zmian w rejestrze systemu Windows i plikach komputera oraz ostrzeganie przed takimi zmianami. Nieuprawnione zmiany w rejestrze i plikach mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych.

1 Otwórz okienko konfiguracji Komputer i pliki.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij przycisk **Konfiguruj**.
3. W okienku konfiguracji kliknij opcję **Komputer i pliki**.

2 W polu **Ochrona przez program SystemGuard** kliknij opcję **Włączona**.

**Uwaga:** Ochronę przez program SystemGuard można wyłączyć, klikając opcję **Wyłączone**.

### *Konfigurowanie opcji aplikacji SystemGuard*

Do konfigurowania opcji ochrony i ostrzegania przed nieupoważnionymi zmianami w rejestrze i plikach związanych z plikami systemu Windows, programami i przeglądarką Internet Explorer oraz rejestrowania tych zmian w dzienniku służy okienko Programy SystemGuard. Nieuprawnione zmiany w rejestrze i plikach mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych.

**1** Otwórz okienko Programy SystemGuard.

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki ochrona przez program SystemGuard jest włączona, a następnie kliknij przycisk **Zaawansowane**.

**2** Wybierz z listy typ aplikacji SystemGuard.

- **Programowi strażnicy systemu**
- **Aplikacje SystemGuard z kategorii Windows**
- **Strażnicy systemu dla przeglądarki**

**3** W obszarze **Działanie** wykonaj jedną z następujących czynności:

- Aby wykrywać, rejestrować i raportować nieupoważnione zmiany w rejestrze i plikach skojarzone z aplikacjami SystemGuard z kategorii Program, Windows i Przeglądarka, kliknij opcję **Pokaż alerty.**
- Aby wykrywać i rejestrować nieupoważnione zmiany w rejestrze i plikach skojarzone z aplikacjami SystemGuard z kategorii Program, Windows i Przeglądarka, kliknij opcję **Rejestruj tylko zmiany.**
- Aby wyłączyć wykrywanie nieupoważnionych zmian w rejestrze i plikach skojarzone z aplikacjami SystemGuard z kategorii Program, Windows i Przeglądarka, kliknij opcję **Wyłącz ten program SystemGuard.**

**Uwaga:** Aby uzyskać więcej informacji na temat aplikacji SystemGuard, zobacz *Rodzaje aplikacji SystemGuard — informacje* (strona 51).

### *Rodzaje aplikacji SystemGuard — informacje*

Aplikacje SystemGuard wykrywają potencjalnie nieupoważnione zmiany w rejestrze komputera i innych plikach krytycznych, które mają zasadnicze znaczenie dla systemu Windows. Istnieją trzy rodzaje aplikacji SystemGuard: Programowi strażnicy systemu, aplikacje SystemGuard z kategorii Windows oraz Strażnicy systemu dla przeglądarki.

## Programowi strażnicy systemu

Programowi strażnicy systemu oprócz oprogramowania szpiegującego i potencjalnie niepożądanych programów zatrzymują także podejrzane formanty ActiveX (pobrane z Internetu), które mogą uruchamiać się automatycznie wraz ze startem systemu Windows.

| SystemGuard | Wykrywa... |
|---|---|
| Instalacje formantów ActiveX | Nieuprawnione zmiany w rejestrze dotyczące instalacji formantów ActiveX, które mogą spowodować uszkodzenie komputera, obniżenie poziomu jego zabezpieczeń lub zniszczenie cennych plików systemowych. |
| Elementy uaktywniane podczas uruchamiania systemu | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą instalować pliki zmieniające elementy uaktywniane podczas uruchamiania systemu, umożliwiając uruchamianie podejrzanych programów podczas uruchamiania komputera. |
| Uchwyty uruchamiania powłoki systemu Windows | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą instalować uchwyty uruchamiania powłoki systemu Windows, aby uniemożliwić prawidłowe działanie programów zabezpieczających. |
| Shell Service Object Delay Load (Opóźnione ładowanie obiektów usług powłoki) | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące opóźnionego ładowania obiektów usług powłoki, umożliwiając uruchamianie szkodliwych plików podczas uruchamiania komputera. |

Aplikacje SystemGuard z kategorii Windows

Aplikacje SystemGuard z kategorii Windows pomagają w zapobieganiu przed wysyłaniem i odbieraniem nieupoważnionych informacji z komputera przez Internet. Oprócz tego pomagają także w zatrzymywaniu podejrzanych programów, które wprowadzają niepożądane zmiany do wyglądu i działania programów ważnych dla użytkowników komputera.

| SystemGuard | Wykrywa... |
|---|---|
| Programy obsługi menu kontekstowego | Nieuprawnione zmiany w rejestrze dotyczące programów obsługi menu kontekstowego w systemie Windows, które mogą spowodować zmianę wyglądu i zachowania tych menu. Menu kontekstowe umożliwiają wykonywanie na komputerze różnych akcji, na przykład po kliknięciu pliku prawym przyciskiem myszy. |
| Biblioteki DLL AppInit | Nieuprawnione zmiany w rejestrze dotyczące bibliotek AppInit_DLL w systemie Windows, które mogą umożliwić uruchamianie potencjalnie szkodliwych plików przy uruchomieniu komputera. |
| Plik Hosts systemu Windows | Oprogramowanie szpiegujące, oprogramowanie reklamowe i potencjalnie niepożądane programy, które mogą wprowadzać nieuprawnione zmiany w pliku Hosts systemu Windows, co umożliwi przekierowywanie przeglądarki do podejrzanych witryn sieci Web oraz blokowanie aktualizacji oprogramowania. |
| Powłoka Winlogon | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące powłoki Winlogon, umożliwiając zastępowanie przeglądarki Windows Explorer przez inne programy. |
| Winlogon User Init | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące usługi Winlogon User Init, umożliwiając uruchamianie podejrzanych programów podczas logowania użytkownika do systemu Windows. |
| Protokoły systemu Windows | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące protokołów systemu Windows, wpływając na sposób wysyłania i odbierania informacji między komputerem a Internetem. |
| Dostawcy usługi warstwowej (Winsock) | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące dostawców usługi warstwowej (LSP) Winsock, aby przechwytywać i zmieniać informacje wysyłane i odbierane przez Internet. |

| | |
|---|---|
| Polecenia Otwórz powłoki systemu Windows | Nieuprawnione zmiany w poleceniach Otwórz powłoki systemu Windows, które mogą umożliwić uruchamianie na komputerze robaków i innych szkodliwych programów. |
| Udostępniony harmonogram zadań | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze i plikach dotyczących Udostępnionego harmonogramu zadań, umożliwiając uruchamianie potencjalnie szkodliwych plików podczas uruchamiania komputera. |
| Usługa Posłaniec systemu Windows | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące usługi Windows Messenger, umożliwiając wyświetlanie niechcianych reklam i zdalne uruchamianie programów na komputerze. |
| Plik win.ini systemu Windows | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w pliku Win.ini, umożliwiając uruchamianie podejrzanych programów podczas uruchamiania komputera. |

Strażnicy systemu dla przeglądarki

Strażnicy systemu dla przeglądarki pomagają w zapobieganiu nieupoważnionym działaniom przeglądarki, takim jak przekierowania do podejrzanych witryn sieci Web, zmiany opcji i ustawień przeglądarki bez wiedzy użytkownika czy niepożądane dodawanie podejrzanych witryn sieci Web do zaufanych.

| SystemGuard | Wykrywa... |
|---|---|
| Obiekty pomocnicze przeglądarki | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą używać obiektów pomocniczych przeglądarki do śledzenia przeglądanych stron sieci Web i wyświetlania niechcianych reklam. |
| Paski przeglądarki Internet Explorer | Nieuprawnione zmiany w rejestrze dotyczące programów na pasku programu Internet Explorer, takich jak Szukaj i Ulubione, które mogą spowodować zmianę wyglądu i zachowania programu Internet Explorer. |
| Dodatki do programu Internet Explorer | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą instalować dodatki do programu Internet Explorer, aby śledzić przeglądane strony sieci Web i pokazywać niechciane reklamy. |
| Obiekt ShellBrowser przeglądarki Internet Explorer | Nieuprawnione zmiany w rejestrze dotyczące obiektu ShellBrowser przeglądarki Internet Explorer, które mogą spowodować zmianę wyglądu i zachowania przeglądarki internetowej. |

| | |
|---|---|
| Obiekt WebBrowser przeglądarki Internet Explorer | Nieuprawnione zmiany w rejestrze dotyczące obiektu Web Browser przeglądarki Internet Explorer, które mogą spowodować zmianę wyglądu i zachowania przeglądarki. |
| Uchwyty wyszukiwania adresów URL przeglądarki Internet Explorer | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące uchwytów wyszukiwania adresów URL w przeglądarce Internet Explorer, umożliwiając przekierowywanie przeglądarki do podejrzanych witryn sieci Web podczas przeszukiwania Internetu. |
| Adresy URL przeglądarki Internet Explorer | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące adresów URL programu Internet Explorer, zmieniając ustawienia przeglądarki. |
| Ograniczenia przeglądarki Internet Explorer | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące ograniczeń programu Internet Explorer, zmieniając ustawienia i opcje przeglądarki. |
| Strefy zabezpieczeń przeglądarki Internet Explorer | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące stref zabezpieczeń programu Internet Explorer, umożliwiając uruchamianie potencjalnie szkodliwych plików podczas uruchamiania komputera. |
| Zaufane witryny przeglądarki Internet Explorer | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące zaufanych witryn przeglądarki Internet Explorer, powodując, że przeglądarka będzie traktowała podejrzane witryny sieci Web jako zaufane. |
| Zasady przeglądarki Internet Explorer | Oprogramowanie szpiegujące, oprogramowanie reklamowe oraz inne potencjalnie niepożądane programy, które mogą wprowadzać zmiany w rejestrze dotyczące zasad przeglądarki Internet Explorer, zmieniając wygląd i zachowanie przeglądarki. |

## Używanie list zaufanych

Jeśli program VirusScan wykryje zmianę w rejestrze lub pliku (SystemGuard), program lub przepełnienie bufora, wyświetli monit o zaufanie wykrytemu elementowi bądź jego usunięcie. Jeśli użytkownik ufa elementowi i wskaże, że nie chce być ponownie powiadamiany o takiej aktywności, element zostanie dodany do listy zaufanych elementów, a program VirusScan nie będzie w przyszłości wykrywał ani powiadamiał o takiej aktywności. Jeśli element zostanie dodany do listy zaufanych, ale użytkownik zdecyduje, że chce blokować jego aktywność, możliwe jest późniejsze jego usunięcie z listy. Blokowanie zapobiega przed uruchomianiem elementu lub wprowadzaniem zmian w komputerze bez powiadomienia za każdym razem, gdy podejmowana jest taka próba. Element może zostać także usunięty z listy zaufanych. Usunięcie spowoduje, że program VirusScan będzie ponownie wykrywał aktywność takiego elementu.

### Zarządzanie listami zaufanych

Opcje w okienku Listy zaufanych umożliwiają zezwolenie lub zablokowanie działania elementów, które zostały już wcześniej wykryte i dodane do zaufanych. Można również usuwać elementy z listy — wtedy program VirusScan wykryje je od nowa.

**1** Otwórz okienko Listy zaufanych

Jak to zrobić?

1. W obszarze **Typowe zadania** kliknij opcję **Strona główna**.
2. W okienku Początek programu SecurityCenter kliknij opcję **Komputer i pliki**.
3. W obszarze informacji kategorii Komputer i pliki kliknij opcję **Konfiguruj**.
4. Upewnij się, że w okienku konfiguracji Komputer i pliki jest włączona ochrona przed wirusami, a następnie kliknij przycisk **Zaawansowane**.
5. Kliknij opcję **Listy zaufanych** w okienku Ochrona przed wirusami.

**2** Zaznacz jeden z następujących typów list zaufanych elementów:

- **Programowi strażnicy systemu**
- **Aplikacje SystemGuard z kategorii Windows**
- **Strażnicy systemu dla przeglądarki**
- **Zaufane programy**
- **Zaufane przepełnienia buforu**

3 W obszarze **Działanie** wykonaj jedną z następujących czynności:

- Aby zezwolić wykrytemu elementowi na wprowadzanie zmian w rejestrze systemu Windows lub kluczowych plikach systemowych na komputerze bez powiadamiania Cię, zaznacz opcję **Ufaj**.
- Aby zablokować wykrytemu elementowi możliwość wprowadzania zmian w rejestrze systemu Windows lub kluczowych plikach systemowych na komputerze bez powiadamiania Cię, zaznacz opcję **Zablokuj**.
- Aby usunąć wykryty element z listy zaufanych, zaznacz opcję **Usuń**.

4 Kliknij przycisk **OK**.

**Uwaga:** Aby uzyskać więcej informacji na temat rodzajów list zaufanych, zobacz *Typy list zaufanych — informacje* (strona 56).

## *Typy list zaufanych — informacje*

Wpisy aplikacji SystemGuard znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania. Opcje zawarte w okienku umożliwiają zarządzanie pięcioma rodzajami list: Programowi strażnicy systemu, Aplikacje SystemGuards z kategorii Windows, Strażnicy systemu dla przeglądarki, Zaufane programy i Zaufane przepełnienia buforu.

| Opcja | Opis |
|---|---|
| Programowi strażnicy systemu | Wpisy programowych strażników systemu znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania.<br><br>Strażnicy ci wykrywają nieuprawnione zmiany w rejestrze i plikach związane z instalacją formantów ActiveX, elementami uaktywnianymi podczas uruchamiania systemu, uchwytami uruchamiania powłoki systemu Windows oraz opóźnionym ładowaniem obiektów usług powłoki. Opisane zmiany mogą spowodować uszkodzenie komputera, obniżenie poziomu jego bezpieczeństwa lub zniszczenie cennych plików systemowych. |

| | |
|---|---|
| Aplikacje SystemGuard z kategorii Windows | Wpisy aplikacji SystemGuard z kategorii Windows znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania.<br><br>Aplikacje te wykrywają nieuprawnione zmiany w rejestrze i plikach związane z programami obsługi menu kontekstowych, bibliotekami DLL inicjowania aplikacji, plikiem Hosts systemu Windows, powłoką Winlogon, dostawcami usługi warstwowej (LSP) Winsock itd. Opisane zmiany mogą wpływać na wysyłanie i odbieranie informacji między komputerem a Internetem oraz wygląd i działanie programów, a także umożliwiać uruchamianie podejrzanych programów na komputerze. |
| Strażnicy systemu dla przeglądarki | Wpisy strażników systemu dla przeglądarki znajdujące się w okienku Listy zaufanych adresów ukazują wcześniejsze nieautoryzowane modyfikacje rejestru i plików wykryte przez program VirusScan, które użytkownik dopuścił z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania.<br><br>Strażnicy ci wykrywają nieuprawnione zmiany w rejestrze i inne podejrzane zachowania związane z obiektami pomocniczymi przeglądarek, dodatkami do przeglądarki Internet Explorer, adresami URL otwieranymi w przeglądarce Internet Explorer, strefami zabezpieczeń przeglądarki Internet Explorer itd. Opisane zmiany mogą prowadzić do wykonywania niepożądanych operacji w przeglądarce, takich jak przekierowywanie do podejrzanych witryn sieci Web, modyfikowanie ustawień i opcji przeglądarki czy obdarzanie zaufaniem podejrzanych witryn sieci Web. |
| Zaufane programy | Zaufane programy to potencjalnie niepożądane programy wykryte przez aplikację VirusScan, wobec których z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania użytkownik określił relację zaufania. |
| Zaufane przepełnienia buforu | Zaufane przepełnienia buforu to wcześniejsze niepożądane działania wykryte przez program VirusScan, wobec których z poziomu komunikatu alertu lub okienka Wyniki wyszukiwania użytkownik określił relację zaufania.<br><br>Przepełnienia buforów mogą spowodować uszkodzenie komputera i zniszczenie plików. Przepełnienia buforów występują, gdy ilość informacji przechowywanych w buforze przez podejrzane programy lub procesy przekracza pojemność buforu. |

ROZDZIAŁ 11

# Skanowanie komputera

Podczas pierwszego uruchomienia programu SecurityCenter moduł ochrony antywirusowej w czasie rzeczywistym zawarty w aplikacji VirusScan zaczyna chronić komputer przed potencjalnie szkodliwymi wirusami, koniami trojańskimi i innymi zagrożeniami bezpieczeństwa. Jeśli ów moduł ochrony pozostanie włączony, aplikacja na bieżąco monitoruje komputer w poszukiwaniu objawów aktywności wirusów, skanując pliki w reakcji na każdą operację dostępu. Skanowanie odbywa się przy użyciu opcji skanowania w czasie rzeczywistym ustawionych przez użytkownika. Aby mieć pewność, że komputer jest skutecznie chroniony przez najnowszymi zagrożeniami, moduł powinien być cały czas włączony, a dodatkowo należy przygotować harmonogram regularnych, bardziej kompleksowych skanowań ręcznych. Aby uzyskać więcej informacji na temat konfigurowania opcji skanowania w czasie rzeczywistym i skanowania ręcznego, zobacz *Konfigurowanie ochrony przed wirusami* (strona 41).

Aplikacja VirusScan zawiera zestaw bardziej szczegółowych opcji skanowania przeznaczonych dla wariantu ręcznej ochrony antywirusowej. Umożliwiają one okresowe przeprowadzanie sesji skanowania rozszerzonego. Skanowania ręczne można inicjować z poziomu programu SecurityCenter, wybierając określone lokalizacje zgodnie z ustalonym harmonogramem. W razie potrzeby skanowanie takie można zainicjować również z poziomu Eksploratora Windows, w trakcie pracy. Zaletą inicjowania skanowania z programu SecurityCenter jest możliwość zmiany opcji skanowania w trakcie sesji, jednak skanowanie za pośrednictwem Eksploratora Windows jest wygodniejsze z perspektywy bezpieczeństwa komputera.

W obu przypadkach po zakończeniu skanowania można obejrzeć jego wyniki. Dzięki temu można ustalić, czy program VirusScan wykrył, naprawił lub poddał kwarantannie wirusy, konie trojańskie, oprogramowanie szpiegujące, oprogramowanie reklamowe, pliki cookie lub inne potencjalnie szkodliwe programy. Rezultaty skanowania mogą być wyświetlane na różne sposoby. Można na przykład obejrzeć sumaryczne (ogólne) wyniki sesji albo szczegółowe informacje, obejmujące np. stan i rodzaj infekcji. Aplikacja pozwala również wyświetlić zbiorcze statystyki skanowania i wykrywania.

## W tym rozdziale

Skanowanie komputera ..... 60
Wyświetl wyniki skanowania ..... 61

## Skanowanie komputera

Ręczne skanowanie komputera można zainicjować zarówno z zaawansowanego, jak i podstawowego menu programu SecurityCenter. W przypadku menu zaawansowanego przed rozpoczęciem skanowania można potwierdzić jego ustawienia. W przypadku menu podstawowego skanowanie rozpoczyna się natychmiast, z użyciem aktualnie ustawionych opcji skanowania. Skanowanie z poziomu Eksploratora Windows również bazuje na istniejących ustawieniach.

- Wykonaj jedną z następujących czynności:

  Skanowanie z poziomu programu SecurityCenter

| Aby... | Wykonaj następujące czynności: |
|---|---|
| Skanować przy użyciu istniejących ustawień | W menu podstawowym kliknij opcję **Skanuj**. |
| Skanować przy użyciu zmodyfikowanych ustawień | W menu zaawansowanym kliknij opcję **Skanuj**, zaznacz lokalizacje, które chcesz przeskanować, wybierz opcje skanowania i kliknij przycisk **Skanuj teraz**. |

  Skanowanie z poziomu Eksploratora Windows

  1. Otwórz Eksploratora Windows.
  2. Kliknij prawym przyciskiem myszy żądany plik, folder lub dysk, a następnie kliknij przycisk **Skanuj**.

**Uwaga:** Wyniki skanowania są wyświetlane w oknie alertu Skanowanie zostało zakończone. W wynikach znajdują się informacje o liczbie obiektów zeskanowanych, wykrytych, naprawionych, poddanych kwarantannie i usuniętych. Aby uzyskać więcej informacji o wynikach skanowania lub wykonać operacje na zainfekowanych plikach, kliknij przycisk **Wyświetl szczegóły skanowania**.

## Wyświetl wyniki skanowania

Po zakończeniu skanowania ręcznego można wyświetlić jego wyniki i zobaczyć dzięki temu, jakie zagrożenia zostały wykryte oraz jaki jest obecny stan ochrony komputera. Wyniki pokazują, czy program VirusScan wykrył, naprawił lub poddał kwarantannie wirusy, konie trojańskie, oprogramowanie szpiegujące, oprogramowanie reklamowe, pliki cookie czy inne potencjalnie szkodliwe programy.

- W menu podstawowym lub zaawansowanym kliknij polecenie **Skanuj**, a następnie wykonaj jedną z następujących operacji:

| Aby... | Wykonaj następujące czynności: |
|---|---|
| Wyświetlić wyniki skanowania w oknie alertu | Obejrzyj wyniki skanowania w oknie alertu Skanowanie zostało zakończone. |
| Wyświetlić dokładniejsze informacje o wynikach skanowania | W oknie alertu Skanowanie zostało zakończone kliknij przycisk **Wyświetl szczegóły skanowania**. |
| Wyświetlić streszczenie wyników skanowania | Na pasku zadań w obszarze powiadomień umieść wskaźnik myszy na ikonie **Skanowanie zostało zakończone**. |
| Wyświetlić statystykę skanowania i wykrywania | Na pasku zadań w obszarze powiadomień kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**. |
| Wyświetlić szczegółowe informacje o wykrytych elementach oraz stanie i rodzaju infekcji | Na pasku zadań w obszarze powiadomień kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**, a następnie w okienku Postęp skanowania: Skanowanie ręczne kliknij przycisk **Wyświetl wyniki**. |

ROZDZIAŁ 12

# Wykonywanie operacji na wynikach skanowania

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje zagrożenie bezpieczeństwa, próbuje automatycznie je usunąć w sposób odpowiedni dla rodzaju zagrożenia. Na przykład w reakcji na wykryty wirus, konia trojańskiego lub śledzący plik cookie próbuje wyczyścić zainfekowany plik. Jeśli nie można wykonać czyszczenia, plik jest poddawany kwarantannie.

W przypadku niektórych zagrożeń aplikacja VirusScan może nie być w stanie ani wyczyścić pliku, ani poddać go kwarantannie. Wtedy wyświetla monit o podjęcie działania przez samego użytkownika. Wybór zależy od rodzaju zagrożenia. Jeśli na przykład w pliku został wykryty wirus, w razie niepowodzenia obu operacji aplikacja blokuje do niego dostęp. W przypadku śledzących plików cookie użytkownik może zdecydować o ich usunięciu lub obdarzeniu zaufaniem. Gdy zostaną wykryte potencjalnie niepożądane programy, aplikacja VirusScan automatycznie nie podejmuje żadnych działań, pozostawiając użytkownikowi wybór między ustanowieniem relacji zaufania a poddaniem programu kwarantannie.

Kwarantanna polega na zaszyfrowaniu, a następnie odizolowaniu plików, programów czy plików cookie w osobnym folderze, dzięki czemu nie zagrażają one już komputerowi. Elementy poddane kwarantannie można przywracać lub trwale usuwać. Przeważnie pliki cookie poddane kwarantannie można usunąć bez szkody dla systemu, jeśli jednak kwarantanna będzie dotyczyła programu, który użytkownik zna i z którego korzysta, warto rozważyć jego przywrócenie.

## W tym rozdziale

Wykonywanie operacji na wirusach i koniach trojańskich 64
Wykonywanie operacji na potencjalnie niepożądanych programach ..... 64
Wykonywanie operacji na plikach poddanych kwarantannie ..... 65
Wykonywanie operacji na programach i plikach cookie poddanych kwarantannie ..... 66

## Wykonywanie operacji na wirusach i koniach trojańskich

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje w pliku na komputerze wirusa lub konia trojańskiego, próbuje wyczyścić taki plik. Jeśli jest to niemożliwe, próbuje poddać go kwarantannie. Jeśli również ta operacja kończy się niepowodzeniem, blokuje dostęp do takiego pliku (dotyczy tylko skanowań w czasie rzeczywistym).

**1** Otwórz okienko Wyniki skanowania.

Jak to zrobić?

1. Na pasku zadań w obszarze powiadomień (prawy koniec paska) kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**.
2. W okienku Postęp skanowania: Skanowanie ręczne kliknij przycisk **Wyświetl wyniki**.

**2** Na liście wyników skanowania zaznacz pozycję **Wirusy i konie trojańskie**.

Uwaga: Informacje o możliwych działaniach na plikach poddanych kwarantannie przez program VirusScan znajdują się w części *Wykonywanie operacji na plikach poddanych kwarantannie* (strona 65).

## Wykonywanie operacji na potencjalnie niepożądanych programach

Jeśli podczas skanowania w czasie rzeczywistym lub skanowania ręcznego aplikacja VirusScan wykryje na komputerze potencjalnie niepożądany program, oferuje możliwość usunięcia go lub obdarzenia zaufaniem. Usunięcie programu w rzeczywistości nie powoduje wykasowania go z komputera, a jedynie poddanie kwarantannie, tak aby nie uszkodził komputera lub plików.

**1** Otwórz okienko Wyniki skanowania.

Jak to zrobić?

1. Na pasku zadań w obszarze powiadomień (prawy koniec paska) kliknij dwukrotnie ikonę **Skanowanie zostało zakończone**.
2. W okienku Postęp skanowania: Skanowanie ręczne kliknij przycisk **Wyświetl wyniki**.

**2** Na liście wyników skanowania zaznacz pozycję **Potencjalnie niepożądane programy**.

**3** Zaznacz potencjalnie niepożądany program.

**4** W obszarze **Działanie** zaznacz opcję **Usuń** lub **Ufaj**.

**5** Potwierdź zaznaczenie opcji.

## *Wykonywanie operacji na plikach poddanych kwarantannie*

Kwarantanna zainfekowanych plików polega na ich zaszyfrowaniu, a następnie przeniesieniu do osobnego folderu, skąd nie zagrażają już komputerowi. Pliki poddane kwarantannie można przywracać lub trwale usuwać.

**1** Otwórz okienko Pliki poddane kwarantannie.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Przywróć**.
3. Kliknij opcję **Pliki**.

**2** Zaznacz plik poddany kwarantannie.

**3** Wykonaj jedną z następujących czynności:

- Aby naprawić zainfekowany plik i przywrócić go do pierwotnej lokalizacji na komputerze, zaznacz opcję **Przywróć**.
- Aby usunąć zainfekowany plik z komputera, zaznacz opcję **Usuń**.

**4** Kliknij przycisk **Tak**, aby potwierdzić wybór opcji.

**Wskazówka:** W jednym kroku można przywrócić lub usunąć kilka plików.

## *Wykonywanie operacji na programach i plikach cookie poddanych kwarantannie*

Kwarantanna potencjalnie niepożądanych programów lub śledzących plików cookie polega na ich zaszyfrowaniu, a następnie przeniesieniu do chronionego folderu, skąd nie zagrażają już komputerowi. Elementy poddane kwarantannie można przywracać lub trwale usuwać. Najczęściej usunięcie takiego elementu nie powoduje negatywnych skutków w systemie.

**1** Otwórz okienko Programy w folderze kwarantanny i śledzące pliki cookie.

Jak to zrobić?

1. W okienku po lewej stronie kliknij opcję **Menu zaawansowane**.
2. Kliknij opcję **Przywróć**.
3. Kliknij opcję **Programy i pliki cookie**.

**2** Zaznacz program lub plik poddany kwarantannie.

**3** Wykonaj jedną z następujących czynności:

- Aby naprawić zainfekowany plik i przywrócić go do pierwotnej lokalizacji na komputerze, zaznacz opcję **Przywróć**.
- Aby usunąć zainfekowany plik z komputera, zaznacz opcję **Usuń**.

**4** Kliknij przycisk **Tak**, aby potwierdzić operację.

**Wskazówka:** W jednym kroku można przywrócić lub usunąć kilka programów/plików cookie.

ROZDZIAŁ 13

# McAfee QuickClean

Program QuickClean poprawia wydajność komputera, usuwając pliki, które mogą zaśmiecać komputer. Program opróżnia Kosz i usuwa tymczasowe pliki, skróty, zagubione fragmenty plików, pliki rejestru, pliki zbuforowane, pliki cookie, pliki historii przeglądarki, wysłaną i usuniętą pocztę, listy ostatnio używanych plików, pliki ActiveX i pliki punktu przywracania systemu. Program QuickClean zapewnia także ochronę prywatności użytkownika dzięki składnikowi McAfee Shredder, który służy do bezpiecznego i trwałego usuwania elementów zawierających poufne informacje osobiste, takie jak dane osobowe użytkownika. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

Defragmentator dysku rozmieszcza pliki i foldery na komputerze w sposób zapewniający ich nierozpraszanie (czyli niedzielenie na fragmenty) podczas zapisywaniu na dysku twardym komputera. Dzięki okresowemu defragmentowaniu dysku twardego można mieć pewność, że podzielone pliki i foldery zostaną połączone, co umożliwi ich szybkie pobieranie w późniejszym terminie.

Jeśli nie chcesz ręcznie obsługiwać swojego komputera, możesz zaplanować automatyczne uruchamianie programów QuickClean i Defragmentator dysku w postaci niezależnych zadań wykonywanych z dowolną częstotliwością.

**Uwaga:** Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

## W tym rozdziale

Funkcje programu QuickClean ..... 68
Oczyszczanie komputera ..... 69
Defragmentowanie komputera ..... 73
Planowanie zadania ..... 74

# Funkcje programu QuickClean

Program QuickClean pozwala wykonywać różne operacje oczyszczania, które usuwają niepotrzebne pliki w sposób bezpieczny i efektywny. Usuwając te pliki, użytkownik zwiększa ilość miejsca na dysku twardym komputera i poprawia jego wydajność.

# Oczyszczanie komputera

Program QuickClean usuwa pliki, które mogą zaśmiecać komputer. Program opróżnia Kosz i usuwa tymczasowe pliki, skróty, zagubione fragmenty plików, pliki rejestru, pliki zbuforowane, pliki cookie, pliki historii przeglądarki, wysłaną i usuniętą pocztę, listy ostatnio używanych plików, pliki ActiveX i pliki punktu przywracania systemu. Program QuickClean usuwa te elementy, nie naruszając innych istotnych informacji.

Niepotrzebne pliki można usunąć z komputera za pomocą dowolnej operacji oczyszczania dostępnej w programie QuickClean. W poniższej tabeli opisano operacje oczyszczania dostępne w programie QuickClean:

| Nazwa | Przeznaczenie |
|---|---|
| Oczyszczanie kosza | Usuwa pliki znajdujące się w Koszu. |
| Oczyszczanie plików tymczasowych | Usuwa pliki zapisane w folderach tymczasowych. |
| Oczyszczanie skrótów | Usuwa uszkodzone skróty i skróty bez skojarzonych z nimi programów. |
| Oczyszczanie zagubionych fragmentów plików | Usuwa z komputera zagubione fragmenty plików. |
| Oczyszczanie rejestru | Usuwa informacje rejestru systemu Windows® dotyczące programów nieistniejących już na komputerze.<br>Rejestr jest bazą danych, w której system Windows przechowuje informacje dotyczące konfiguracji. Rejestr zawiera profile wszystkich użytkowników komputera, informacje o zainstalowanym sprzęcie i programach oraz ustawienia właściwości. System Windows w trakcie działania stale odwołuje się do tych informacji. |
| Oczyszczanie pamięci podręcznej | Usuwa buforowane pliki, które zbierają się podczas przeglądania stron sieci Web. Pliki te zwykle przechowywane są jako pliki tymczasowe w folderze pamięci podręcznej.<br>Folder pamięci podręcznej jest miejscem zapisu tymczasowych danych komputera. Aby zwiększyć szybkość i sprawność przeglądania sieci Web, przeglądarka przy następnym wyświetlaniu strony sieci Web może ją pobierać z pamięci podręcznej (a nie ze zdalnego serwera). |

| | |
|---|---|
| Oczyszczanie plików cookie | Usuwa pliki cookie. Pliki te zwykle przechowywane są jako pliki tymczasowe.<br><br>Plik cookie jest małym plikiem zawierającym informacje (najczęściej nazwę użytkownika oraz bieżącą datę i godzinę), który jest przechowywany na komputerze osoby przeglądającej sieć Web. Pliki cookie są używane przede wszystkim przez strony sieci Web w celu identyfikowania użytkowników, którzy zostali wcześniej zarejestrowani w witrynie albo ją odwiedzali. Mogą również stanowić źródło informacji dla hakerów. |
| Oczyszczanie historii przeglądarki | Usuwa historię przeglądanych stron sieci Web. |
| Oczyszczanie wiadomości e-mail programów Outlook Express i Outlook (elementy wysłane i usunięte) | Usuwa wysłane i usunięte wiadomości e-mail z programów Outlook® i Outlook Express. |
| Oczyszczanie ostatnio używanych elementów | Usuwa listę ostatnio używanych plików, które zostały utworzone w dowolnym z następujących programów:<br><br>▪ Adobe Acrobat®<br>▪ Corel® WordPerfect® Office (Corel Office)<br>▪ Jasc®<br>▪ Lotus®<br>▪ Microsoft® Office®<br>▪ RealPlayer™<br>▪ Historia systemu Windows<br>▪ Windows Media Player<br>▪ WinRAR®<br>▪ WinZip® |
| Czyszczenie formantów ActiveX | Usuwa formanty ActiveX.<br><br>ActiveX jest składnikiem oprogramowania używanym przez programy lub strony sieci Web w celu poszerzenia zakresu funkcji. Ten składnik integruje się z programem lub stroną sieci Web i działa jako zwykła część programu lub strony. Formanty ActiveX są w większości niegroźne, jednak niektóre z nich mogą przechwytywać informacje z komputera. |
| Oczyszczanie punktu przywracania systemu | Usuwa z komputera stare punkty przywracania systemu (poza najnowszym punktem).<br><br>Punkty przywracania systemu są tworzone przez system Windows w celu oznaczania wszelkich zmian wprowadzanych do komputera, dzięki czemu w razie wystąpienia jakichkolwiek problemów można przywrócić poprzedni stan systemu. |

## Oczyszczanie komputera

Niepotrzebne pliki można usunąć z komputera za pomocą dowolnej operacji oczyszczania dostępnej w programie QuickClean. Po zakończeniu oczyszczania w obszarze **Program QuickClean — podsumowanie** można sprawdzić ilość miejsca odzyskanego na dysku, liczbę usuniętych plików oraz datę i godzinę uruchomienia ostatniej operacji programu QuickClean na komputerze.

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **McAfee QuickClean** kliknij przycisk **Start**.
3. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować domyślne operacje oczyszczania na liście.
   - Zaznacz lub usuń zaznaczenie odpowiednich operacji oczyszczania, a następnie kliknij przycisk **Dalej**. W przypadku wybrania operacji Oczyszczanie ostatnio używanych elementów można kliknąć opcję **Właściwości** w celu wybrania lub wyczyszczenia plików utworzonych ostatnio za pomocą programów znajdujących się na liście, a następnie kliknąć przycisk **OK**.
   - Kliknij przycisk **Przywróć ustawienia domyślne**, aby przywrócić domyślne operacje oczyszczania, a następnie kliknij przycisk **Dalej**.
4. Po wykonaniu analizy kliknij przycisk **Dalej**.
5. Kliknij przycisk **Dalej**, aby potwierdzić usuwanie pliku.
6. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować domyślnie opcję **Nie, chcę usunąć pliki, korzystając ze standardowego sposobu usuwania plików w systemie Windows**.
   - Kliknij opcję **Tak, chcę bezpiecznie wymazać moje pliki za pomocą programu Shredder**, podaj liczbę przebiegów niszczenia (do 10), a następnie kliknij przycisk **Dalej**. W przypadku wymazywania dużych ilości informacji proces niszczenia plików może zająć dużo czasu.

7 Jeśli podczas wykonywania operacji czyszczenia niektóre pliki lub elementy zostały zablokowane, może zostać wyświetlony monit o ponowne uruchomienie komputera. Kliknij przycisk **OK**, aby zamknąć monit.

8 Kliknij przycisk **Zakończ**.

**Uwaga:** Pliki usunięte za pomocą programu Shredder nie mogą zostać przywrócone. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

# Defragmentowanie komputera

Defragmentator dysku rozmieszcza pliki i foldery na komputerze w sposób zapewniający ich nierozpraszanie (czyli niedzielenie na fragmenty) podczas zapisywania na dysku twardym komputera. Dzięki okresowemu defragmentowaniu dysku twardego można mieć pewność, że podzielone pliki i foldery zostaną połączone, co umożliwi ich szybkie pobieranie w późniejszym terminie.

## Defragmentowanie komputera

W celu poprawienia dostępności plików i folderów oraz ułatwienia ich pobierania można wykonać defragmentację komputera.

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Defragmentator dysku** kliknij przycisk **Analizuj**.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

**Uwaga:** Aby uzyskać więcej informacji na temat programu Defragmentator dysku, zapoznaj się z Pomocą systemu Windows.

# Planowanie zadania

Harmonogram zadań automatyzuje częstotliwość uruchamiania programów QuickClean i Defragmentator dysku na komputerze. Można na przykład zaplanować zadanie uruchamiania programu QuickClean w celu opróżniania Kosza w każdą niedzielę o godzinie 21.00 lub zadanie uruchamiania programu Defragmentator dysku w celu wykonania defragmentacji dysku twardego komputera w ostatni dzień każdego miesiąca. Takie zadanie można w dowolnym momencie utworzyć, zmodyfikować lub usunąć. Aby umożliwić uruchomienie zaplanowanego zadania, użytkownik musi być zalogowany na komputerze. Jeśli z jakiegokolwiek powodu zadanie nie zostanie uruchomione, nastąpi zmiana harmonogramu i uruchomienie zadania zostanie zaplanowane na pięć minut po zalogowaniu się użytkownika.

## Planowanie zadania programu QuickClean

Istnieje możliwość zaplanowania zadania automatycznego czyszczenia komputera przy użyciu jednej lub kilku operacji oczyszczania dostępnych w programie QuickClean. Po zakończeniu wykonywania zadania w obszarze **Program QuickClean — podsumowanie** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

1. Otwórz okienko Harmonogram zadań.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
   2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2. Na liście **Wybierz operację do zaplanowania** kliknij pozycję **McAfee QuickClean**.
3. W polu **Nazwa zadania** wpisz nazwę zadania, a następnie kliknij przycisk **Utwórz**.
4. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Dalej**, aby zaakceptować operacje oczyszczania na liście.
   - Zaznacz lub usuń zaznaczenie odpowiednich operacji oczyszczania, a następnie kliknij przycisk **Dalej**. W przypadku wybrania operacji Oczyszczanie ostatnio używanych elementów można kliknąć opcję **Właściwości** w celu wybrania lub wyczyszczenia plików utworzonych ostatnio za pomocą programów znajdujących się na liście, a następnie kliknąć przycisk **OK**.
   - Kliknij przycisk **Przywróć ustawienia domyślne**, aby przywrócić domyślne operacje oczyszczania, a następnie kliknij przycisk **Dalej**.

5 Wykonaj jedną z poniższych czynności:

- Kliknij przycisk **Harmonogram**, aby zaakceptować domyślnie opcję **Nie, chcę usunąć pliki, korzystając ze standardowego sposobu usuwania plików w systemie Windows**.
- Kliknij opcję **Tak, chcę bezpiecznie wymazać moje pliki za pomocą programu Shredder**, podaj liczbę przebiegów niszczenia (do 10), a następnie kliknij przycisk **Harmonogram**.

6 W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

7 Jeśli wprowadzono zmiany we właściwościach oczyszczania ostatnio używanych elementów, może zostać wyświetlony monit o ponowne uruchomienie komputera. Kliknij przycisk **OK**, aby zamknąć monit.

8 Kliknij przycisk **Zakończ**.

**Uwaga:** Pliki usunięte za pomocą programu Shredder nie mogą zostać przywrócone. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

## *Modyfikowanie zadania programu QuickClean*

Zaplanowane zadanie programu QuickClean można modyfikować, zmieniając używane operacje oczyszczania lub częstotliwość automatycznego uruchamiania zadania na komputerze użytkownika. Po zakończeniu wykonywania zadania w obszarze **Program QuickClean — podsumowanie** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **McAfee QuickClean**.

3 Wybierz zadanie z listy **Wybierz istniejące zadanie**, a następnie kliknij opcję **Modyfikuj**.

4 Wykonaj jedną z poniższych czynności:

- Kliknij przycisk **Dalej**, aby zaakceptować operacje oczyszczania wybrane dla zadania.

- Zaznacz lub usuń zaznaczenie odpowiednich operacji oczyszczania, a następnie kliknij przycisk **Dalej**. W przypadku wybrania operacji Oczyszczanie ostatnio używanych elementów można kliknąć opcję **Właściwości** w celu wybrania lub wyczyszczenia plików utworzonych ostatnio za pomocą programów znajdujących się na liście, a następnie kliknąć przycisk **OK**.
- Kliknij przycisk **Przywróć ustawienia domyślne**, aby przywrócić domyślne operacje oczyszczania, a następnie kliknij przycisk **Dalej**.

5 Wykonaj jedną z poniższych czynności:

- Kliknij przycisk **Harmonogram**, aby zaakceptować domyślnie opcję **Nie, chcę usunąć pliki, korzystając ze standardowego sposobu usuwania plików w systemie Windows**.
- Kliknij opcję **Tak, chcę bezpiecznie wymazać moje pliki za pomocą programu Shredder**, podaj liczbę przebiegów niszczenia (do 10), a następnie kliknij przycisk **Harmonogram**.

6 W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

7 Jeśli wprowadzono zmiany we właściwościach oczyszczania ostatnio używanych elementów, może zostać wyświetlony monit o ponowne uruchomienie komputera. Kliknij przycisk **OK**, aby zamknąć monit.

8 Kliknij przycisk **Zakończ**.

**Uwaga:** Pliki usunięte za pomocą programu Shredder nie mogą zostać przywrócone. Aby uzyskać informacje na temat niszczenia plików, zapoznaj się z opisem programu McAfee Shredder.

## *Usuwanie zadania programu QuickClean*

Jeśli zaplanowane zadanie programu QuickClean nie ma być dłużej uruchamiane automatycznie, można je usunąć.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **McAfee QuickClean**.

3 Z listy **Wybierz istniejące zadanie** wybierz zadanie.

4 Kliknij przycisk **Usuń**, a następnie przycisk **Tak**, aby potwierdzić usunięcie.

5 Kliknij przycisk **Zakończ**.

## *Planowanie zadania programu Defragmentator dysku*

Istnieje możliwość zaplanowania zadania programu Defragmentator dysku w celu określenia częstotliwości, z jaką ma być wykonywana automatyczna defragmentacja dysku twardego komputera. Po zakończeniu wykonywania zadania w obszarze **Defragmentator dysku** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

1 Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

2 Na liście **Wybierz operację do zaplanowania** kliknij pozycję **Defragmentator dysku**.

3 W polu **Nazwa zadania** wpisz nazwę zadania, a następnie kliknij przycisk **Utwórz**.

4 Wykonaj jedną z poniższych czynności:

- Kliknij opcję **Harmonogram**, aby zaakceptować domyślną opcję **Wykonaj defragmentację mimo małej ilości wolnego miejsca**.
- Usuń zaznaczenie opcji **Wykonaj defragmentację mimo małej ilości wolnego miejsca**, a następnie kliknij opcję **Harmonogram**.

5 W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

6 Kliknij przycisk **Zakończ**.

## Modyfikowanie zadania programu Defragmentator dysku

Zaplanowane zadanie programu Defragmentator dysku można zmodyfikować w celu zmiany częstotliwości, z jaką zadanie ma być uruchamiane na komputerze. Po zakończeniu wykonywania zadania w obszarze **Defragmentator dysku** można sprawdzić datę i godzinę następnego zaplanowanego uruchomienia zadania.

**1** Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

**2** Na liście **Wybierz operację do zaplanowania** kliknij pozycję **Defragmentator dysku**.

**3** Wybierz zadanie z listy **Wybierz istniejące zadanie**, a następnie kliknij opcję **Modyfikuj**.

**4** Wykonaj jedną z poniższych czynności:

- Kliknij opcję **Harmonogram**, aby zaakceptować domyślną opcję **Wykonaj defragmentację mimo małej ilości wolnego miejsca**.
- Usuń zaznaczenie opcji **Wykonaj defragmentację mimo małej ilości wolnego miejsca**, a następnie kliknij opcję **Harmonogram**.

**5** W oknie dialogowym **Harmonogram** wybierz częstotliwość uruchamiania zadania, a następnie kliknij przycisk **OK**.

**6** Kliknij przycisk **Zakończ**.

## Usuwanie zadania programu Defragmentator dysku

Jeśli zaplanowane zadanie programu Defragmentator dysku nie ma być dłużej uruchamiane automatycznie, można je usunąć.

**1** Otwórz okienko Harmonogram zadań.

Jak to zrobić?

1. W obszarze **Typowe zadania** programu McAfee SecurityCenter kliknij opcję **Konserwacja komputera**.
2. W obszarze **Harmonogram zadań** kliknij przycisk **Start**.

**2** Na liście **Wybierz operację do zaplanowania** kliknij pozycję **Defragmentator dysku**.

**3** Z listy **Wybierz istniejące zadanie** wybierz zadanie.

**4** Kliknij przycisk **Usuń**, a następnie przycisk **Tak**, aby potwierdzić usunięcie.

**5** Kliknij przycisk **Zakończ**.

ROZDZIAŁ 14

# Program McAfee Shredder

Program McAfee Shredder w sposób trwały usuwa (niszczy) elementy znajdujące się na dysku twardym komputera. Nawet w przypadku ręcznego usunięcia plików i folderów, opróżnienia Kosza czy usunięcia tymczasowych plików internetowych, takie informacje można nadal odtworzyć za pomocą komputerowych narzędzi diagnostycznych. Ponadto istnieje możliwość odtworzenia usuniętego pliku, ponieważ niektóre programy tworzą tymczasowe, ukryte kopie otwieranych plików. Program Shredder zapewnia ochronę prywatności poprzez bezpieczne i trwałe usuwanie tych niepożądanych plików. Bardzo ważne: zniszczonych plików nie można już odtworzyć.

**Uwaga:** Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

## W tym rozdziale

Funkcje programu Shredder ..... 82
Niszczenie plików, folderów i zawartości dysków ..... 83

# Funkcje programu Shredder

Program Shredder usuwa elementy z dysku twardego komputera, dzięki czemu nie można odtworzyć powiązanych z nimi informacji. Program zapewnia ochronę prywatności, pozwalając bezpiecznie i trwale usuwać pliki i foldery, elementy znajdujące się w Koszu i w folderze tymczasowych plików internetowych oraz całą zawartość dysków komputerowych, takich jak dyski CD wielokrotnego zapisu, zewnętrzne dyski twarde czy dyskietki.

# Niszczenie plików, folderów i zawartości dysków

Dzięki programowi Shredder nie jest możliwe odtwarzanie informacji przechowywanych w usuniętych plikach i folderach, znajdujących się w Koszu i w folderze tymczasowych plików internetowych, nawet za pomocą specjalnych narzędzi. Program Shredder pozwala określić, ile razy dany element ma zostać zniszczony (maksymalnie 10 razy). Większa liczba przebiegów niszczenia zwiększa poziom bezpieczeństwa usuwania plików.

## Niszczenie plików i folderów

Istnieje możliwość zniszczenia plików i folderów znajdujących się na dysku twardym komputera, w tym elementów przechowywanych w Koszu i w folderze tymczasowych plików internetowych.

1 Otwórz program **Shredder**.

   Jak to zrobić?

   1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
   2. W okienku po lewej stronie kliknij opcję **Narzędzia**.
   3. Kliknij opcję **Shredder**.

2 W obszarze **Działanie** okienka Zniszcz pliki i foldery kliknij opcję **Wymazywanie plików i folderów**.

3 W obszarze **Poziom niszczenia** wybierz jeden z następujących poziomów niszczenia:

   - **Szybki**: Wybrane elementy są niszczone w 1 przebiegu.
   - **Dokładny**: Wybrane elementy są niszczone w 7 przebiegach.
   - **Niestandardowy**: Wybrane elementy są niszczone przez wykonanie do 10 przebiegów.

4 Kliknij przycisk **Dalej**.

5 Wykonaj jedną z poniższych czynności:

   - Na liście **Wybierz pliki do zniszczenia** kliknij jedną z następujących pozycji: **Zawartość Kosza** lub **Tymczasowe pliki internetowe**.
   - Kliknij przycisk **Przeglądaj**, przejdź do pliku, który chcesz zniszczyć, a następnie kliknij przycisk **Otwórz**.

6 Kliknij przycisk **Dalej**.

7 Kliknij opcję **Start**.

8 Po zakończeniu pracy programu Shredder kliknij opcję **Gotowe**.

**Uwaga:** Do czasu ukończenia tego zadania nie należy korzystać z żadnych plików.

## *Niszczenie całej zawartości dysku*

Istnieje możliwość jednorazowego usunięcia całej zawartości dysku. Operacja niszczenia dotyczy tylko dysków wymiennych, takich jak zewnętrzne dyski twarde, dyski CD z możliwością zapisu i dyskietki.

1 Otwórz program **Shredder**.

Jak to zrobić?

1. W obszarze **Typowe zadania** okna McAfee SecurityCenter kliknij opcję **Menu zaawansowane**.
2. W okienku po lewej stronie kliknij opcję **Narzędzia**.
3. Kliknij opcję **Shredder**.

2 W obszarze **Działanie** okienka Zniszcz pliki i foldery kliknij opcję **Wymazywanie całego dysku**.

3 W obszarze **Poziom niszczenia** wybierz jeden z następujących poziomów niszczenia:

- **Szybki**: Zawartość wybranego dysku jest niszczona w 1 przebiegu.
- **Dokładny**: Zawartość wybranego dysku jest niszczona w 7 przebiegach.
- **Niestandardowy**: Zawartość wybranego dysku jest niszczona przez wykonanie do 10 przebiegów.

4 Kliknij przycisk **Dalej**.

5 Na liście **Wybierz dysk** kliknij dysk, którego zawartość chcesz zniszczyć.

6 Kliknij przycisk **Dalej**, a następnie kliknij przycisk **Tak**, aby potwierdzić ustawienia.

7 Kliknij opcję **Start**.

8 Po zakończeniu pracy programu Shredder kliknij opcję **Gotowe**.

**Uwaga:** Do czasu ukończenia tego zadania nie należy korzystać z żadnych plików.

ROZDZIAŁ 15

# Program McAfee Network Manager

Program Network Manager przedstawia graficzną prezentację komputerów i urządzeń wchodzących w skład sieci domowej. Za jego pomocą można zdalnie monitorować stan ochrony każdego zarządzanego komputera działającego w sieci i usuwać zgłaszane luki w zabezpieczeniach tego komputera.

Przed rozpoczęciem korzystania z programu Network Manager można zapoznać się z niektórymi jego funkcjami. Szczegółowe informacje na temat konfigurowania i używania tych funkcji można znaleźć w pomocy programu Network Manager.

**Uwaga:** Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician.

## W tym rozdziale

Funkcje programu Network Manager ..... 86
Ikony programu Network Manager ..... 87
Konfigurowanie zarządzanej sieci ..... 89
Zdalne zarządzanie siecią ..... 97

# Funkcje programu Network Manager

Program Network Manager udostępnia następujące funkcje.

## Graficzna mapa sieci

Mapa sieci programu Network Manager dostarcza graficznego przeglądu stanu ochrony komputerów i pozostałych elementów, z których składa się sieć domowa. Po wprowadzeniu w sieci zmian (na przykład po dodaniu komputera) mapa sieci uwzględnia je. Aby dostosować widok mapy do potrzeb, można ją odświeżać, zmieniać nazwę sieci i wyświetlać lub ukrywać jej elementy. Można również wyświetlić szczegółowe informacje na temat dowolnego składnika wyświetlanego na mapie sieci.

## Zarządzanie zdalne

Mapę sieci programu Network Manager można wykorzystywać do zarządzania stanem ochrony komputerów tworzących sieć domową. Można zaprosić komputer do dołączenia do zarządzanej sieci, monitorować stan ochrony zarządzanego komputera i rozwiązywać problemy związane ze znanymi zagrożeniami bezpieczeństwa sieci pochodzącymi ze zdalnego komputera, który znajduje się w sieci.

# Ikony programu Network Manager

W poniższej tabeli omówiono ikony, z jakich korzysta się zwykle w przypadku mapy sieci prezentowanej w programie Network Manager.

| Ikona | Opis |
|---|---|
|  | Oznacza zarządzany komputer działający w trybie online |
|  | Oznacza zarządzany komputer działający w trybie offline |
|  | Oznacza niezarządzany komputer, na którym zainstalowano program SecurityCenter |
|  | Oznacza niezarządzany komputer działający w trybie offline |
|  | Oznacza komputer działający w trybie online, na którym nie jest zainstalowany program SecurityCenter, lub oznacza nieznane urządzenie sieciowe |
|  | Oznacza komputer działający w trybie offline, na którym nie jest zainstalowany program SecurityCenter, lub oznacza nieznane urządzenie sieciowe działające w trybie offline |
|  | Informuje, że dany element jest chroniony i podłączony |
|  | Informuje, że użytkownik powinien zwrócić uwagę na dany element |
|  | Informuje, że użytkownik powinien niezwłocznie zwrócić uwagę na dany element |
|  | Oznacza bezprzewodowy router sieci domowej |
|  | Oznacza standardowy router sieci domowej |
|  | Oznacza Internet, jeśli jest nawiązane z nim połączenie |
|  | Oznacza Internet, jeśli nie jest nawiązane z nim połączenie |

ROZDZIAŁ 16

# Konfigurowanie zarządzanej sieci

Konfigurowanie zarządzanej sieci odbywa się za pomocą elementów naniesionych na mapę sieci oraz poprzez dodawanie do sieci składników (komputerów). Aby było możliwe zdalne zarządzanie komputerem lub przyznanie mu uprawnienia do zdalnego zarządzania innymi komputerami, musi on stać się zaufanym składnikiem sieci. Przynależność do sieci jest przyznawana nowym komputerom przez dotychczasowe składniki sieci (komputery), które mają uprawnienia administracyjne.

Można wyświetlić szczegóły dotyczące dowolnego składnika przedstawionego na mapie sieci, nawet po dokonaniu zmian w tej sieci (np. po dodaniu komputera).

## W tym rozdziale

Korzystanie z mapy sieci ..... 90
Dołączanie do zarządzanej sieci ..... 92

## Korzystanie z mapy sieci

Po połączeniu komputera z siecią program Network Manager analizuje ją w celu określenia, czy występują w niej jakieś zarządzane lub niezarządzane składniki, oraz sprawdza atrybuty routera i stan Internetu. Jeśli nie zostaną znalezione żadne składniki, program Network Manager zakłada, że aktualnie podłączony komputer jest pierwszym komputerem w sieci i przyznaje mu status zarządzanego składnika z uprawnieniami administracyjnymi. Domyślnie nazwa sieci zawiera nazwę grupy roboczej lub domeny pierwszego komputera, który połączy się z siecią i ma zainstalowany program SecurityCenter. Nazwę sieci można jednak zmienić w dowolnym momencie.

Po wprowadzeniu zmian w sieci (np. dodaniu do niej komputera) można dostosować jej mapę. W tym celu można np. odświeżyć mapę, zmienić nazwę sieci oraz wyświetlić lub ukryć składniki na mapie. Można również wyświetlać szczegóły dotyczące dowolnego elementu przedstawionego na mapie sieci.

### Uzyskiwanie dostępu do mapy sieci

Mapa sieci przedstawia w sposób graficzny komputery i komponenty tworzące sieć domową.

- W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.

**Uwaga:** Przy pierwszym użyciu mapy sieci wyświetlany jest monit o potwierdzenie, że inne komputery w sieci są zaufane.

### Odświeżanie mapy sieci

Mapę sieci można odświeżyć w dowolnym momencie, np. po dodaniu do zarządzanej sieci kolejnego komputera.

1. W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
2. W menu **Działanie** kliknij opcję **Odśwież mapę sieci**.

**Uwaga:** Łącze **Odśwież mapę sieci** jest dostępne tylko wówczas, gdy na mapie sieci nie jest zaznaczony żaden element. Aby usunąć zaznaczenie elementu, kliknij wybrany element lub kliknij obszar białego tła na mapie sieci.

### *Zmiana nazwy sieci*

Domyślnie nazwa sieci zawiera nazwę grupy roboczej lub domeny pierwszego komputera, który połączy się z siecią i ma zainstalowany program SecurityCenter. Nazwę sieci można zmienić według uznania.

1. W menu podstawowym lub zaawansowanym kliknij polecenie **Zarządzaj siecią**.
2. W menu **Działanie** kliknij opcję **Zmień nazwę sieci**.
3. Wpisz nazwę sieci w polu **Nazwa sieci**.
4. Kliknij przycisk **OK**.

**Uwaga:** Łącze **Zmień nazwę sieci** jest dostępne tylko wówczas, gdy na mapie sieci nie jest zaznaczony żaden element. Aby usunąć zaznaczenie elementu, kliknij wybrany element lub kliknij obszar białego tła na mapie sieci.

### *Pokazywanie lub ukrywanie elementu na mapie sieci*

Domyślnie wszystkie komputery i komponenty wchodzące w skład sieci domowej są pokazywane na mapie. Jeśli jednak część elementów została ukryta, można je wyświetlić ponownie w dowolnym momencie. Można ukryć tylko niezarządzane elementy. Zarządzanych komputerów nie można ukryć.

| Aby... | W menu podstawowym lub zaawansowanym kliknij opcję **Zarządzaj siecią**, a następnie... |
|---|---|
| Ukrywanie elementu na mapie sieci | Kliknij element na mapie sieci, a następnie w menu **Działanie** kliknij opcję **Ukryj ten element**. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**. |
| Pokazywanie ukrytych elementów na mapie sieci | W obszarze **Działanie** kliknij opcję **Pokaż ukryte elementy**. |

### *Wyświetlanie szczegółów elementu*

Można wyświetlić szczegółowe informacje o dowolnym komponencie sieci, wybierając go na mapie sieci. Informacje te obejmują nazwę komponentu, stan jego ochrony oraz inne dane niezbędne do zarządzania nim.

1. Kliknij ikonę elementu na mapie sieci.
2. W obszarze **Szczegóły** są wyświetlane informacje o tym elemencie.

## Dołączanie do zarządzanej sieci

Aby było możliwe zdalne zarządzanie komputerem lub przyznanie mu uprawnienia do zdalnego zarządzania innymi komputerami, musi on stać się zaufanym składnikiem sieci. Przynależność do sieci jest przyznawana nowym komputerom przez dotychczasowe składniki sieci (komputery), które mają uprawnienia administracyjne. Aby zagwarantować, że do sieci będą dołączane tylko zaufane komputery, użytkownicy komputerów zarówno przyznających dostęp, jak i dołączających, muszą uwierzytelniać się nawzajem.

Gdy komputer dołącza do sieci, otrzymuje monit o ujawnienie swojego stanu ochrony McAfee innym komputerom w sieci. Jeśli komputer zgodzi się na ujawnienie swojego stanu ochrony, staje się zarządzanym składnikiem sieci. Jeśli komputer nie zgodzi się na ujawnienie swojego stanu ochrony, staje się niezarządzanym składnikiem sieci. Niezarządzane składniki sieci są zwykle komputerami-gośćmi, które chcą uzyskać dostęp do innych mechanizmów sieciowych (np. wysyłania plików lub współdzielenia drukarek).

**Uwaga:** Jeśli na komputerze są zainstalowane inne programy sieciowe firmy McAfee (np. EasyNetwork), po dołączeniu do sieci jest on ponadto rozpoznawany w tych programach jako zarządzany komputer. Poziom uprawnień, który zostanie przyznany komputerowi w programie Network Manager, obowiązuje we wszystkich programach sieciowych firmy McAfee. Więcej informacji na temat, czym są w programach sieciowych firmy McAfee uprawnienia gościa, pełne i administracyjne, można znaleźć w dokumentacji dołączonej do tych programów.

### Dołączanie do zarządzanej sieci

Po otrzymaniu zaproszenia do dołączenia do zarządzanej sieci można je albo przyjąć, albo odrzucić. Można również określić, czy ten komputer i pozostałe komputery należące do sieci mają monitorować nawzajem swoje ustawienia zabezpieczeń (np. sprawdzać, czy usługi antywirusowe obecne na komputerze są aktualne).

1. Upewnij się, że pole wyboru **Zezwalaj wszystkim komputerom w tej sieci na monitorowanie ustawień zabezpieczeń** w oknie dialogowym Zarządzana sieć jest zaznaczone.
2. Kliknij przycisk **Dołącz**.
   Po przyjęciu zaproszenia zostaną wyświetlone dwie karty do gry.
3. Sprawdź, czy karty do gry są identyczne z wyświetlanymi na komputerze, który wysłał zaproszenie do dołączenia do zarządzanej sieci.
4. Kliknij przycisk **OK**.

**Uwaga:** Jeśli komputer, który wysłał zaproszenie do dołączenia do zarządzanej sieci, nie wyświetla takich samych kart do gry, jak wyświetlane w oknie dialogowym potwierdzenia zabezpieczeń, nastąpiło naruszenie bezpieczeństwa zarządzanej sieci. Dołączenie do sieci może spowodować zagrożenie dla komputera, dlatego w oknie dialogowym Zarządzana sieć kliknij przycisk **Odrzuć**.

### Zapraszanie komputera do dołączenia do sieci zarządzanej

Jeśli komputer jest dodawany do zarządzanej sieci lub w sieci znajduje się inny niezarządzany komputer, można go zaprosić do dołączenia do zarządzanej sieci. Tylko komputery z uprawnieniami administratora w sieci mogą zapraszać inne komputery do dołączenia do sieci. Przed wysłaniem zaproszenia można również określić poziom uprawnień, który zostanie przypisany dołączającemu komputerowi.

1. Kliknij ikonę niezarządzanego komputera na mapie sieci.
2. Kliknij opcję **Monitoruj ten komputer** w obszarze **Działanie**.
3. W oknie dialogowym Zaproś komputer do dołączenia do zarządzanej sieci kliknij jedną z następujących opcji:
   - Kliknij opcję **Zezwalaj na dostęp gościa do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci (można użyć tej opcji dla tymczasowych użytkowników w domu).
   - Kliknij opcję **Zezwalaj na dostęp pełny do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci.

- Kliknij opcję **Zezwalaj na dostęp administracyjny do zarządzanych programów sieciowych**, aby zezwolić komputerowi na dostęp do sieci z uprawnieniami administracyjnymi. Opcja ta uprawnia również komputer do udzielania dostępu innym komputerom, które zamierzają dołączyć do zarządzanej sieci.

4 Kliknij przycisk **OK**.
Do komputera zostanie wysłane zaproszenie do dołączenia do zarządzanej sieci. Gdy komputer zaakceptuje zaproszenie zostaną wyświetlone dwie karty do gry.

5 Sprawdź, czy karty do gry są takie same jak te wyświetlone na komputerze zaproszonym do dołączenia do zarządzanej sieci.

6 Kliknij opcję **Przyznaj prawa dostępu**.

**Uwaga:** Jeśli na komputerze zaproszonym do dołączenia do zarządzanej sieci w oknie dialogowym potwierdzenia zabezpieczeń nie są wyświetlone te same karty, w zarządzanej sieci nastąpiło naruszenie bezpieczeństwa. Zezwolenie na dołączenie komputera do sieci może spowodować zagrożenie dla innych komputerów; z tego powodu kliknij przycisk **Odmów dostępu** w oknie dialogowym potwierdzenia zabezpieczeń.

### *Utrata zaufania do komputerów w sieci*

Jeśli użytkownik zaufał innym komputerom przez pomyłkę, może cofnąć swoje zaufanie.

- Kliknij opcję **Przestań ufać komputerom w tej sieci** w obszarze **Działanie**.

**Uwaga:** Łącze **Przestań ufać komputerom w tej sieci** nie jest dostępne, gdy użytkownik ma uprawnienia administracyjne, a w sieci znajdują się inne zarządzane komputery.

ROZDZIAŁ 17

# Zdalne zarządzanie siecią

Po skonfigurowaniu zarządzanej sieci można zdalnie zarządzać komputerami i składnikami sieci. Można monitorować stan i poziomy uprawnień komputerów i składników oraz zdalnie naprawiać większość luk w zabezpieczeniach.

## W tym rozdziale

Monitorowanie stanu i uprawnień.....98
Naprawa luk w zabezpieczeniach .....100

## Monitorowanie stanu i uprawnień

W skład sieci zarządzanej wchodzą elementy zarządzane i niezarządzane. Elementy zarządzane zezwalają innym komputerom w sieci na monitorowanie swojego stanu ochrony McAfee, natomiast niezarządzane na to nie zezwalają. Elementy niezarządzane to zazwyczaj komputery-goście, które uzyskują dostęp do innych mechanizmów sieciowych (np. wysyłania plików lub współdzielenia drukarek). Zarządzany komputer w sieci może w dowolnym momencie zaprosić niezarządzany komputer, aby stał się zarządzanym. Podobnie zarządzany komputer może w dowolnym momencie zostać niezarządzanym.

Zarządzane komputery mają uprawnienia dostępu administracyjnego, pełnego lub typu Gość. Uprawnienia administracyjne umożliwiają zarządzanemu komputerowi zarządzanie stanem ochrony wszystkich pozostałych zarządzanych komputerów w sieci i przyznawanie innym komputerom członkostwa w sieci. Uprawnienia pełne i gościa umożliwiają komputerowi tylko uzyskanie dostępu do sieci. Poziom uprawnień komputera można modyfikować w dowolnym momencie.

Ponieważ zarządzana sieć składa się również z urządzeń (na przykład routerów), również nimi można zarządzać za pomocą programu Network Manager. Można także konfigurować i modyfikować właściwości wyświetlania urządzenia na mapie sieci.

### Monitorowanie stanu ochrony komputera

Jeśli stan ochrony komputera nie jest monitorowany w sieci (komputer nie jest elementem sieci lub jest jej elementem niezarządzanym), można zażądać jego monitorowania.

1. Kliknij ikonę niezarządzanego komputera na mapie sieci.
2. Kliknij opcję **Monitoruj ten komputer** w obszarze **Działanie**.

### Zakończenie monitorowania stanu ochrony komputera

Można zakończyć monitorowanie stanu ochrony zarządzanego komputera w sieci; komputer jednak staje się wówczas niezarządzany i nie można zdalnie monitorować stanu jego ochrony.

1. Kliknij ikonę zarządzanego komputera na mapie sieci.
2. Kliknij opcję **Zakończ monitorowanie tego komputera** w obszarze **Działanie**.
3. W oknie dialogowym potwierdzenia kliknij przycisk **Tak**.

### *Modyfikacja uprawnień zarządzanego komputera*

Uprawnienia zarządzanego komputera można w dowolnym momencie zmieniać. Umożliwia to ustalenie, które komputery mogą monitorować stan ochrony innych komputerów w sieci.

1. Kliknij ikonę zarządzanego komputera na mapie sieci.
2. Kliknij opcję **Modyfikuj uprawnienia dla tego komputera** w obszarze **Działanie**.
3. W oknie dialogowym modyfikacji uprawnień zaznacz pole wyboru lub usuń jego zaznaczenie, aby określić, czy ten i inne komputery w zarządzanej sieci mogą monitorować nawzajem swój stan ochrony.
4. Kliknij przycisk **OK**.

### *Zarządzanie urządzeniem*

Urządzeniem można zarządzać, uzyskując dostęp do jego administracyjnej strony sieci Web w programie Network Manager.

1. Kliknij ikonę urządzenia na mapie sieci.
2. Kliknij opcję **Zarządzaj tym urządzeniem** w obszarze **Działanie**.
   Administracyjna strona sieci Web urządzenia zostanie otwarta w przeglądarce sieci Web.
3. W przeglądarce sieci Web podaj informacje wymagane podczas logowania i skonfiguruj ustawienia zabezpieczeń urządzenia.

**Uwaga:** Jeśli urządzeniem jest bezprzewodowy router lub punkt dostępu chroniony programem Wireless Network Security, do konfiguracji ustawień zabezpieczeń urządzenia należy użyć programu Wireless Network Security.

### *Modyfikacja właściwości wyświetlania urządzenia*

Podczas modyfikacji właściwości wyświetlania urządzenia można zmienić nazwę urządzenia wyświetlaną na mapie sieci oraz określić, czy urządzenie jest routerem bezprzewodowym.

1. Kliknij ikonę urządzenia na mapie sieci.
2. Kliknij opcję **Modyfikuj właściwości urządzenia** w obszarze **Działanie**.
3. Aby określić wyświetlaną nazwę urządzenia, wpisz ją w polu **Nazwa**.
4. Aby określić typ urządzenia, kliknij opcję **Router standardowy**, jeśli nie jest to router bezprzewodowy, lub opcję **Router bezprzewodowy** w przypadku routera bezprzewodowego.
5. Kliknij przycisk **OK**.

## Naprawa luk w zabezpieczeniach

Zarządzane komputery z uprawnieniami administracyjnymi mogą monitorować stan ochrony McAfee innych zarządzanych komputerów w sieci i zdalnie naprawiać zgłoszone luki w zabezpieczeniach. Na przykład jeśli stan ochrony McAfee zarządzanego komputera wskazuje, że program VirusScan jest wyłączony, inny zarządzany komputer z uprawnieniami administracyjnymi może zdalnie włączyć program VirusScan.

Podczas zdalnego naprawiania luk w zabezpieczeniach program Network Manager naprawia najczęściej zgłaszane problemy. Jednak niektóre luki w zabezpieczeniach mogą wymagać ręcznej interwencji na lokalnym komputerze. W takim przypadku program Network Manager naprawia te problemy, które można naprawić zdalnie, a następnie monituje o naprawienie pozostałych poprzez zalogowanie do programu SecurityCenter na zagrożonym komputerze i postępowanie zgodnie z podanymi zaleceniami. W niektórych przypadkach sugerowanym sposobem naprawy jest instalacja najnowszej wersji programu SecurityCenter na zdalnym komputerze lub komputerach w sieci.

### Napraw luki w zabezpieczeniach

Programu Network Manager można użyć do naprawiania większości luk w zabezpieczeniach na zdalnych zarządzanych komputerach. Jeśli na przykład program VirusScan na zdalnym komputerze jest wyłączony, można go włączyć.

1. Kliknij ikonę elementu na mapie sieci.
2. Zapoznaj się ze stanem ochrony elementu w obszarze **Szczegóły**.
3. Kliknij opcję **Napraw luki w zabezpieczeniach** w obszarze **Działanie**.
4. Po naprawieniu problemów z zabezpieczeniami kliknij przycisk **OK**.

**Uwaga:** Mimo iż program Network Manager automatycznie naprawia większość luk w zabezpieczeniach, niektóre naprawy mogą wymagać uruchomienia programu SecurityCenter na zagrożonym komputerze i postępowania zgodnie z podanymi zaleceniami.

### *Instalowanie oprogramowania zabezpieczającego McAfee na zdalnych komputerach*

Jeśli jeden lub więcej komputerów w sieci nie posiada najnowszej wersji programu SecurityCenter, ich stan zabezpieczeń nie może być zdalnie monitorowany. Aby zdalnie monitorować te komputery, należy na każdym z nich zainstalować najnowszą wersję programu SecurityCenter.

1. Na komputerze, na którym ma zostać zainstalowane oprogramowanie zabezpieczające, otwórz program SecurityCenter.
2. W obszarze **Typowe zadania** kliknij opcję **Moje konto**.
3. Zaloguj się, używając tego samego adresu e-mail i hasła, które zostały użyte do rejestracji oprogramowania zabezpieczającego przy jego pierwszej instalacji.
4. Wybierz odpowiedni produkt, kliknij ikonę **Pobierz/Instaluj**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

# Opis

W Słowniku terminów znajdują się najczęściej stosowane w produktach firmy McAfee terminy związane z bezpieczeństwem oraz ich definicje.

# Słownik

## 8

### 802.11

Zestaw standardów IEEE określających sposób przesyłania danych w sieci bezprzewodowej. Standard 802.11 określa się często mianem Wi-Fi.

### 802.11a

Rozszerzenie standardu 802.11 umożliwiające przesyłanie danych z prędkością do 54 Mb/s w paśmie 5 GHz. Prędkość transmisji jest większa niż w przypadku standardu 802.11b, jednak zasięg jest znacznie mniejszy.

### 802.11b

Rozszerzenie standardu 802.11 umożliwiające przesyłanie danych z prędkością do 11 Mb/s w paśmie 2,4 GHz. Prędkość transmisji jest mniejsza niż w przypadku standardu 802.11a, jednak zasięg jest większy.

### 802.1x

Standard IEEE określający sposób uwierzytelniania w sieciach przewodowych i bezprzewodowych. Standard 802.1x jest często stosowany w sieciach bezprzewodowych 802.11.

## A

### ActiveX, formant

Składnik oprogramowania używany przez programy lub strony sieci Web w celu poszerzenia zakresu funkcji. Formant ActiveX jest widoczny jako zintegrowany element programu lub strony sieci Web. Formanty ActiveX są w większości niegroźne, jednak niektóre z nich mogą przechwytywać informacje z komputera.

### adres IP

Identyfikator komputera lub urządzenia w sieci TCP/IP. W sieciach działających na podstawie protokołu TCP/IP dane kierowane są na podstawie adresu IP miejsca docelowego. Format adresu IP to 32-bitowa wartość liczbowa zapisana jako cztery liczby oddzielone kropkami. Każda liczba mieści się w przedziale od 0 do 255 (na przykład 192.168.1.100).

### Adres MAC

(Media Access Control Address, adres kontroli dostępu do nośnika) Unikatowy numer seryjny przypisany do urządzenia fizycznego z dostępem do sieci.

### archiwizacja

Proces tworzenia kopii ważnych plików na dysku CD lub DVD, stacji USB, zewnętrznym dysku twardym lub dysku sieciowym.

### archiwizacja pełna

Proces archiwizowania pełnego zestawu danych w zależności od skonfigurowanych typów plików i lokalizacji. Patrz także: archiwizacja szybka.

### archiwizacja szybka

Proces archiwizowania tylko tych plików, które uległy zmianie od czasu ostatniej archiwizacji pełnej lub szybkiej. Zobacz też: archiwizacja pełna.

### atak słownikowy

Odmiana ataku typu „brute force” wykorzystująca słownik w celu odkrycia hasła.

### atak typu „brute force”

Metoda dekodowania zaszyfrowanych danych (np. haseł) przy użyciu znacznego nakładu mocy obliczeniowej (metoda „siłowa”) zamiast inteligentnych strategii. Atak typu „brute force” stanowi podejście niezawodne, ale czasochłonne. Ataki tego rodzaju określa się także mianem łamania zabezpieczeń metodą „brute force”.

### atak typu „man-in-the-middle”

Metoda przechwytywania i ewentualnego modyfikowania danych przesyłanych między dwoma stronami, które nie wiedzą o tym, że łącze komunikacyjne między nimi zostało naruszone.

### atak typu „phishing”

Internetowe oszustwo mające na celu kradzież cennych informacji (numerów kart kredytowych, numerów ubezpieczenia, identyfikatorów użytkownika, haseł) od niepodejrzewających niczego użytkowników w celu posłużenia się nimi jako fałszywą tożsamością.

### atak typu DoS (odmowa usługi)

Typ ataku, który powoduje spowolnienie lub zatrzymanie ruchu w sieci. Atak typu DoS (odmowa usługi) występuje w sytuacji, gdy sieć jest obciążona tyloma dodatkowymi żądaniami, że zwykły ruch jest utrudniony lub zupełnie zablokowany. Zwykle nie wiąże się to z kradzieżą informacji lub wykorzystaniem innych luk w zabezpieczeniach.

## B

### biała lista

Lista witryn sieci Web, do których dostęp jest dozwolony, ponieważ nie są one uznawane za fałszywe.

### biblioteka

Miejsce przechowywania danych w trybie online, w którym można umieścić zarchiwizowane i opublikowane pliki. Biblioteka programu Data Backup to witryna sieci Web dostępna dla wszystkich użytkowników Internetu.

### brama zintegrowana

Urządzenie łączące funkcje punktu dostępu, routera i zapory. Niektóre urządzenia mogą posiadać rozszerzenia zabezpieczeń i funkcje mostkowania.

# C

## czarna lista

W kontekście ochrony przed atakami typu „phishing” — lista witryn sieci Web uważanych za szkodliwe.

# D

## DAT

Pliki DAT (pliki sygnatur) zawierają definicje używane podczas wykrywania wirusów, koni trojańskich, oprogramowania szpiegującego, oprogramowania reklamowego i innych potencjalnie niepożądanych programów na komputerze lub stacji USB.

## dialer

Program, który pomaga w nawiązaniu połączenia internetowego. Dialery używane w celach destrukcyjnych mogą spowodować przekierowanie połączenia internetowego do kogoś innego niż domyślny usługodawca internetowy (ISP) bez poinformowania użytkownika o dodatkowych kosztach.

## DNS

(Domain Name System) System przekształcający nazwy hostów lub domen w adresy IP. W sieci Web system DNS służy do konwertowania zrozumiałych adresów sieciowych (na przykład www.mojanazwahosta.com) w adresy IP (na przykład 111.2.3.44) w celu pobrania witryny sieci Web. Bez systemu DNS użytkownik musiałby wpisać adres IP w przeglądarce internetowej.

## dodatek

Mały program współpracujący z większym programem w celu rozszerzenia jego funkcjonalności. Dodatki umożliwiają na przykład przeglądarce sieci Web dostęp i wykonywanie operacji na takich plikach osadzonych w dokumentach HTML, których format normalnie nie byłby przez nią rozpoznawany (animacje, pliki wideo, piki audio itd.).

## domena

Lokalna podsieć lub deskryptor witryn w Internecie.

W sieci lokalnej (LAN) domena to podsieć składająca się z komputerów klienckich i serwerów, którymi steruje jedna baza danych zabezpieczeń. W tym kontekście domeny pomagają w zwiększeniu wydajności. W Internecie domena to element każdego adresu WWW (na przykład w adresie www.abc.com domena to abc).

## dysk inteligentny

Zobacz: stacja USB.

## dysk sieciowy

Dysk twardy lub napęd taśmowy podłączony do serwera sieciowego, który jest udostępniany wielu użytkownikom. Dyski sieciowe są czasem nazywane dyskami zdalnymi.

# E

## ESS

(Extended Service Set) Zestaw dwóch lub więcej sieci tworzących pojedynczą podsieć.

# F

## filtrowanie obrazów

Opcja funkcji kontroli rodzicielskiej, która umożliwia blokowanie potencjalnie niepożądanych obrazów podczas przeglądania sieci Web.

## fragmenty plików

Pozostałości plików rozproszone na dysku. Do fragmentacji dochodzi podczas dodawania i usuwania plików. Fragmentacja może spowolnić działanie komputera.

## Funkcje ochrony rodzicielskiej

Ustawienia pomagające decydować, co dzieci będą widzieć i jakie operacje będą mogły wykonywać w trakcie przeglądania sieci Web. Ustawienia obejmują m.in. możliwość filtrowania obrazów, wybór grupy klasyfikacji treści oraz określenie limitów czasowych przeglądania sieci Web.

# G

## grupy klasyfikacji zawartości

W kontekście funkcji ochrony rodzicielskiej — grupa wiekowa, do której należy użytkownik. Zawartość jest udostępniana lub blokowana w zależności od grupy klasyfikacji zawartości, do której należy dany użytkownik. Grupy klasyfikacji zawartości to: małe dziecko, dziecko, młodszy nastolatek, starszy nastolatek i dorosły.

# H

## hasło

Kod (zazwyczaj złożony z liter i cyfr) pozwalający na uzyskanie dostępu do komputera, programu lub witryny sieci Web.

# I

## Internet

Internet to ogromna liczba połączonych ze sobą sieci, które korzystają z protokołów TCP/IP do odnajdywania i przesyłania danych. Internet rozwinął się z połączonych komputerów uniwersyteckich i szkolnych (na przełomie lat 60-tych i 70-tych ubiegłego wieku). Przedsięwzięcie to zostało sfinansowane przez Departament Obrony Stanów Zjednoczonych i było znane pod nazwą ARPANET. Dziś Internet jest ogólnoświatową siecią, na którą składa się prawie 100 000 niezależnych sieci.

## intranet

Prywatna sieć komputerowa stanowiąca zazwyczaj wewnętrzną sieć organizacji, do której dostęp mają wyłącznie autoryzowani użytkownicy.

# K

## karta PCI sieci bezprzewodowej

(PCI = Peripheral Component Interconnect) Karta sieci bezprzewodowej podłączana do gniazda PCI wewnątrz komputera.

## karta sieci bezprzewodowej

Urządzenie, dzięki któremu komputer lub asystent PDA uzyskuje możliwość pracy w sieci bezprzewodowej. Podłącza się ją do portu USB, gniazda kart PC Card (CardBus), gniazda karty pamięci lub do wewnętrznej magistrali PCI.

### *Karta sieciowa*

(NIC — Network Interface Card) Karta podłączana do komputera przenośnego lub innego urządzenia, która łączy je z siecią LAN.

### *karta USB sieci bezprzewodowej*

Karta sieci bezprzewodowej podłączana do gniazda USB w komputerze.

### *klient*

Aplikacja działająca na komputerze osobistym lub stacji roboczej i zależna od serwera podczas wykonywania pewnych operacji. Na przykład klient poczty e-mail to aplikacja umożliwiająca wysyłanie i odbieranie wiadomości e-mail.

### *klient poczty e-mail*

Program uruchamiany na komputerze w celu wysyłania i odbierania wiadomości e-mail (na przykład Microsoft Outlook).

### *klucz*

Seria liter i cyfr używana przez dwa urządzenia do uwierzytelniania ich komunikacji. Oba urządzenia muszą posiadać klucz. Patrz także: WEP, WPA, WPA2, WPA-PSK i WPA2- PSK.

### *kod uwierzytelniania komunikatów (MAC)*

Kod zabezpieczeń służący do szyfrowania komunikatów przesyłanych między komputerami. Komunikat jest akceptowany, jeśli komputer docelowy uznaje odszyfrowany kod za poprawny.

### *kompresja*

Proces, w wyniku którego pliki są kompresowane do postaci, w której zajmują mniej miejsca podczas przechowywania lub przesyłania.

### *koń trojański*

Aplikacja sprawiająca wrażenie normalnego programu, ale mogąca spowodować zniszczenie cennych plików, zmniejszenie wydajności i nieuprawniony dostęp do komputera.

### *Kosz*

Wirtualne miejsce na składowanie usuniętych plików i folderów w systemie Windows.

### *kwarantanna*

Izolowanie. Na przykład w aplikacji VirusScan podejrzane pliki są wykrywane i poddawane kwarantannie, dzięki czemu nie stanowią już zagrożenia dla komputera ani pozostałych plików.

## *L*

### *LAN*

(Local Area Network, sieć lokalna) Sieć komputerowa obejmująca stosunkowo niewielki obszar (na przykład pojedynczy budynek). Komputery w sieci LAN komunikują się ze sobą i udostępniają zasoby, takie jak drukarki i pliki.

### *Launchpad*

Składnik interfejsu platformy U3, który służy do uruchamiania programów zgodnych z platformą U3 ze stacji USB i do zarządzania tymi programami.

### *lista zaufanych*

Zawiera wpisy elementów, którym użytkownik ufa, w związku z czym nie są one więcej wykrywane. Jeśli okaże się, że elementowi (np. potencjalnie niepożądanemu programowi lub modyfikacji rejestru) zaufano przez pomyłkę lub jeśli ma on zostać ponownie wykryty, należy usunąć go z tej listy.

### *lokalizacja monitorowana częściowo*

Folder na komputerze, który jest monitorowany przez program Data Backup w celu wykrycia zmian. Po skonfigurowaniu lokalizacji monitorowanej częściowo program Data Backup tworzy kopie zapasowe wszystkich plików monitorowanych typów znajdujących się w tym folderze, ale pomija te w podfolderach.

### *lokalizacja monitorowana dokładnie*

Folder na komputerze, który jest monitorowany przez program Data Backup w celu wykrycia zmian. Po skonfigurowaniu lokalizacji monitorowanej dokładnie program Data Backup tworzy kopie zapasowe wszystkich plików monitorowanych typów znajdujących się w tym folderze i jego podfolderach.

### *lokalizacje monitorowane*

Foldery w komputerze monitorowane przez program Data Backup.

## *M*

### *magazyn haseł*

Bezpieczny obszar pamięci masowej przeznaczony na osobiste hasła. Umożliwia przechowywanie haseł z gwarancją, że nikt inny (nawet administrator) nie ma do nich dostępu.

### *mapa sieci*

Graficzne przedstawienie komputerów i składników tworzących sieć domową.

### *MAPI*

(Messaging Application Programming Interface — interfejs programowy aplikacji komunikacyjnych) Specyfikacja interfejsu firmy Microsoft umożliwiająca różnym aplikacjom komunikacyjnym i aplikacjom dla grup roboczych (między innymi do obsługi poczty e-mail, poczty głosowej i faksów) współpracę z pojedynczym klientem, takim jak klient Exchange.

### *MSN*

(Microsoft Network) Zbiór usług internetowych oferowanych przez firmę Microsoft Corporation. Obejmuje aparat wyszukiwania, moduł poczty e-mail, moduł przesyłania wiadomości błyskawicznych oraz portal.

## *N*

### *niekontrolowany punkt dostępu*

Punkt dostępu, który działa nielegalnie. Niekontrolowane punkty dostępu instaluje się w bezpiecznych sieciach firmowych w celu umożliwienia dostępu do tych sieci nieuprawnionym osobom. Inne zastosowanie to stworzenie napastnikom możliwości przeprowadzenia ataków typu „man-in-the-middle”.

# P

## pamięć podręczna

Miejsce zapisu tymczasowych danych na komputerze. Na przykład, aby zwiększyć szybkość i sprawność przeglądania sieci Web, przeglądarka przy następnym wyświetlaniu danej strony może ją pobrać z pamięci podręcznej (a nie ze zdalnego serwera).

## plik cookie

Mały plik zawierający informacje (najczęściej nazwę użytkownika oraz bieżącą datę i godzinę), który jest przechowywany na komputerze osoby przeglądającej sieć Web. Pliki cookie są używane przede wszystkim przez strony sieci Web w celu identyfikowania użytkowników, którzy zostali wcześniej zarejestrowani w witrynie albo ją odwiedzali. Mogą również stanowić źródło informacji dla hakerów.

## plik tymczasowy

Plik tworzony w pamięci lub na dysku przez system operacyjny lub inny program z przeznaczeniem do użycia w ramach bieżącej sesji, a następnie usuwany.

## pluskwy internetowe

Małe pliki graficzne osadzające się na stronach HTML i umożliwiające nieautoryzowanym źródłom umieszczanie plików cookie na komputerze użytkownika. Te pliki cookie mogą następnie przesyłać informacje do nieautoryzowanego źródła. Pluskwy internetowe są także nazywane sygnalizatorami sieci Web, tagami pikselowymi, czystymi lub niewidocznymi plikami GIF.

## poczta e-mail

(poczta elektroniczna) Wiadomości wysyłane i odbierane elektronicznie w sieci komputerowej. Patrz także: poczta z sieci Web.

## Poczta w sieci Web

Wiadomości wysyłane i odbierane elektronicznie (przez Internet). Zobacz też: e-mail.

## podszywanie się pod adres IP

Fałszowanie adresu IP znajdującego się w pakiecie IP. To działanie stosowane jest w wielu typach ataków, między innymi w przechwytywaniu sesji. Często fałszowane są nagłówki wiadomości e-mail stanowiących spam, dzięki czemu nie można wyśledzić nadawcy.

## POP3

(Post Office Protocol 3) Interfejs między klientem poczty e-mail a serwerem poczty e-mail. Konta POP3 (zwane również standardowymi kontami e-mail) są wykorzystywane przez większość użytkowników domowych.

## port

Miejsce, przez które informacje wchodzą do komputera i z niego wychodzą. Na przykład konwencjonalny modem analogowy jest podłączony do portu szeregowego.

## potencjalnie niepożądany program (PUP)

Program gromadzący i wysyłający informacje osobiste użytkownika bez jego zgody (np. oprogramowanie szpiegujące albo reklamowe).

### PPPoE

(Point-to-Point Protocol Over Ethernet) Metoda wykorzystywania protokołu łączności telefonicznej (PPP), gdzie przesyłanie danych odbywa się przez sieć Ethernet.

### protokół

Forma (sprzętowy lub programowy) przesyłania danych między dwoma urządzeniami. Aby komputer/urządzenie użytkownika mogły się kontaktować z innymi komputerami, musi obsługiwać odpowiedni protokół.

### proxy

Komputer (lub oprogramowanie na nim uruchomione), który funkcjonuje jako bariera pomiędzy siecią a Internetem, prezentując witrynom zewnętrznym tylko pojedynczy adres sieciowy. Reprezentując wszystkie wewnętrzne komputery, serwer proxy chroni tożsamość komputerów w sieci i jednocześnie umożliwia dostęp do Internetu. Zobacz też: serwer proxy.

### przeglądarka

Program używany do wyświetlana stron sieci Web w Internecie. Do popularnych przeglądarek sieci Web należą programy Microsoft Internet Explorer i Mozilla Firefox.

### przepełnienie bufora

Stan występujący wtedy, gdy podejrzane programy lub procesy próbują zapisać więcej danych w buforze (miejscu zapisu tymczasowych danych na komputerze), niż może on pomieścić. Przepełnienie buforu może spowodować uszkodzenie lub nadpisanie danych w sąsiednich buforach.

### przepustowość

Ilość danych, którą można przesłać w określonym czasie.

### przywracanie

Proces przywracania kopii pliku z repozytorium kopii zapasowych online lub z archiwum.

### publiczny punkt dostępu

Określona lokalizacja geograficzna objęta zasięgiem punktu dostępu Wi-Fi (802.11). Użytkownicy znajdujący się w zasięgu publicznego punktu dostępu z komputerem przenośnym obsługującym sieć bezprzewodową mogą nawiązać połączenie z Internetem, pod warunkiem że punkt dostępu nadaje sygnał (ujawnia swoją obecność) i nie jest wymagane uwierzytelnianie. Publiczne punkty dostępu znajdują się zwykle w miejscach, w których przebywają duże grupy ludzi, na przykład na lotniskach.

### publikowanie

Proces publicznego udostępniania w Internecie pliku, który ma kopię zapasową. W celu uzyskania dostępu do opublikowanych plików należy przeszukać bibliotekę programu Data Backup.

### Punkt dostępu

Urządzenie sieciowe (określane często mianem routera bezprzewodowego), które jest podłączane do przełącznika lub koncentratora sieci Ethernet w celu poszerzenia fizycznego zasięgu usługi dla użytkowników bezprzewodowych. Gdy użytkownicy bezprzewodowi przemieszczają się wraz ze swoimi urządzeniami mobilnymi, transmisja jest przekazywana z jednego punktu dostępu do innego w celu zachowania łączności.

### *punkt przywracania systemu*

Migawka (obraz) zawartości pamięci komputera lub bazy danych. System Windows tworzy punkty przywracania systemu w regularnych odstępach czasu oraz w reakcji na poważne zdarzenia systemowe (np. przy instalacji programu lub sterownika). Użytkownik w każdej chwili może utworzyć i nazwać własny punkt przywracania.

## *R*

### *RADIUS*

(Remote Access Dial-In User Service) Protokół umożliwiający uwierzytelnianie użytkowników, zwykle podczas sesji zdalnego dostępu. Pierwotnie przeznaczony dla serwerów telefonicznego dostępu zdalnego, obecnie jest stosowany w wielu środowiskach uwierzytelniania, między innymi w uwierzytelnianiu 802.1x ze współdzielonym hasłem użytkownika sieci WLAN.

### *rejestr*

Baza danych, w której system Windows przechowuje swoje informacje konfiguracyjne. Rejestr zawiera profile wszystkich użytkowników komputera, informacje o zainstalowanym sprzęcie i programach oraz ustawienia właściwości. System Windows w trakcie działania stale odwołuje się do tych informacji.

### *repozytorium kopii zapasowych online*

Lokalizacja na serwerze online, w której są przechowywane powstające kopie zapasowe plików.

### *roaming*

Przemieszczanie się z obszaru zasięgu jednego punktu dostępu do drugiego, bez zakłócania dostępu do usług lub utraty połączenia.

### *robak*

Samopowielający się wirus, który ładuje się do aktywnej pamięci komputera i może rozsyłać swoje kopie za pomocą poczty e-mail. Robaki replikują się i zużywają zasoby systemu, spowalniając lub zatrzymując zadania.

### *rootkit*

Zbiór narzędzi (programów) przyznających użytkownikowi uprawnienia administratora wobec komputera lub sieci komputerowej. Mogą to być aplikacje szpiegujące i inne potencjalnie niepożądane programy, które zagrażają bezpieczeństwu danych na komputerze lub poufności informacji osobistych.

### *router*

Urządzenie sieciowe przekazujące pakiety danych z jednej sieci do drugiej. W oparciu o wewnętrzne tablice routingu routery analizują każdy przychodzący pakiet i na podstawie wszelkich możliwych kombinacji źródłowych i docelowych adresów oraz bieżących warunków ruchu w sieci (obciążenie, koszty połączenia, uszkodzenia łączy) wybierają sposób przekazania go. Czasami router jest nazywany „punktem dostępu”.

# S

## serwer

Komputer lub program, który akceptuje połączenia od innych komputerów lub programów, a następnie zwraca im właściwe odpowiedzi. Na przykład, zawsze gdy chcesz wysłać lub odebrać wiadomość e-mail, aplikacja pocztowa na Twoim komputerze łączy się z serwerem pocztowym.

## serwer DNS

(serwer systemu Domain Name System) Komputer, który zwraca adres IP powiązany z nazwą hosta lub domeny. Patrz także: DNS.

## serwer proxy

Składnik zapory zarządzający ruchem internetowym do i z sieci lokalnej (LAN). Serwer proxy może poprawić wydajność, dostarczając często żądane dane, takie jak popularne strony sieci Web. Może on również filtrować i odrzucać żądania uważane za niewłaściwe, takie jak żądania nieautoryzowanego dostępu do plików zastrzeżonych.

## sieć

Zbiór punktów dostępu i powiązanych z nimi użytkowników, czyli środowisko ESS.

## sieć domowa

Dwa lub większa liczba komputerów połączonych ze sobą w domu w celu udostępniania plików i połączenia internetowego. Patrz także: LAN.

## sieć zarządzana

Sieć domowa z dwoma typami użytkowników: użytkownikami zarządzanymi i użytkownikami niezarządzanymi. Użytkownicy zarządzani zezwalają na monitorowanie swojego stanu ochrony przez inne komputery w sieci; użytkownicy niezarządzani — nie zezwalają na to.

## skanowanie na żądanie

Skanowanie inicjowane przez użytkownika. W odróżnieniu od skanowania w czasie rzeczywistym skanowanie na żądanie nie jest uruchamiane automatycznie.

## skanowanie w czasie rzeczywistym

Skanowanie plików i folderów w poszukiwaniu wirusów i innych przejawów aktywności w czasie, gdy użytkownik lub komputer próbuje uzyskać dostęp do tych plików/folderów.

## skrót

Plik zawierający wyłącznie informację o lokalizacji innego pliku na komputerze.

## skrypt

Lista poleceń, które mogą być wykonywane automatycznie (tzn. bez udziału użytkownika). W odróżnieniu od programów skrypty są zazwyczaj przechowywane w postaci zwykłego tekstu i kompilowane dopiero po wywołaniu. Mianem skryptów są również określane pliki wsadowe i makra.

## słowo kluczowe

Słowo, które można przypisać do pliku posiadającego kopię zapasową w celu ustanowienia zależności lub połączenia z innymi plikami, do których przypisano to samo słowo kluczowe. Przypisywanie słów kluczowych do plików ułatwia wyszukiwanie plików opublikowanych w Internecie.

### SMTP

(Simple Mail Transfer Protocol) Protokół TCP/IP służący do przesyłania wiadomości z jednego komputera w sieci do drugiego. Ten protokół jest używany w Internecie do przesyłania wiadomości e-mail.

### SSID

(Service Set Identifier) Token (tajny klucz) identyfikujący sieć Wi-Fi (802.11). Identyfikator SSID jest ustalany przez administratora sieci. Użytkownicy chcący uzyskać dostęp do tej sieci muszą go podać podczas logowania.

### SSL

(Secure Sockets Layer) Opracowany przez firmę Netscape protokół służący do przesyłania prywatnych dokumentów w Internecie. Protokół SSL działa, korzystając z publicznego klucza do szyfrowania danych, które są następnie przesyłane połączeniem SSL. Adresy URL wymagające połączenia SSL rozpoczynają się przedrostkiem https zamiast http.

### Stacja USB

Niewielki dysk pamięci masowej wtykany do portu USB w komputerze. Stacja USB działa jak mały dysk twardy, który pozwala na sprawne przenoszenie plików między komputerami.

### standardowe konto e-mail

Zobacz: POP3.

### synchronizacja

Proces usuwania rozbieżności pomiędzy plikami przechowywanymi na lokalnym komputerze a ich kopiami zapasowymi. Synchronizacja jest wykonywana, gdy wersja pliku w repozytorium kopii zapasowych online jest nowsza niż ta znajdująca się w innych komputerach.

### SystemGuard

Aplikacje McAfee, które wykrywają nieautoryzowane zmiany w komputerze i powiadamiają użytkownika w chwili ich wystąpienia.

### szyfrowanie

Proces transformacji danych z tekstu na kod, mający na celu uniemożliwienie odczytania informacji przez osoby, które nie znają metody jego odszyfrowania. Dane przekształcone w ten sposób określa się także mianem tekstu zaszyfrowanego.

## T

### tekst zaszyfrowany

Tekst, który został zaszyfrowany. Tekstu zaszyfrowanego nie można odczytać, dopóki nie zostanie on przekonwertowany na zwykły tekst (odszyfrowany).

### TKIP

(Temporal Key Integrity Protocol) Protokół eliminujący luki w zabezpieczeniach WEP, w szczególności podczas ponownego użycia kluczy szyfrowania. Protokół TKIP zmienia klucze tymczasowe co 10 000 pakietów, zapewniając metodę dynamicznej dystrybucji, która znacząco zwiększa bezpieczeństwo sieci. Proces zabezpieczeń TKIP rozpoczyna się 128-bitowym kluczem tymczasowym współdzielonym przez klientów i punkty dostępu. Protokół TKIP łączy klucz tymczasowy z adresem MAC komputera klienckiego, a następnie dodaje stosunkowo duży 16-oktetowy wektor inicjowania. W efekcie powstaje klucz szyfrujący dane. Ta procedura gwarantuje, że każda stacja do szyfrowania danych używa strumieni o innym kluczu. Protokół TKIP do szyfrowania używa algorytmu RC4.

### tworzenie kopii zapasowej

Proces tworzenia kopii ważnych plików na bezpiecznym serwerze w trybie online.

### typy monitorowanych plików

Typy plików (na przykład .doc, .xls itd.) znajdujących się w lokalizacjach monitorowanych, dla których program Data Backup tworzy kopie zapasowe lub które archiwizuje.

## U

### U3

(You: Simplified, Smarter, Mobile) Platforma umożliwiająca uruchamianie programów dla środowisk Windows 2000 i Windows XP bezpośrednio z dysków USB. Inicjatywa U3 została zapoczątkowana w 2004 r. przez firmy M-Systems i SanDisk. Jej celem jest stworzenie użytkownikom programów zgodnych ze standardem U3 możliwości uruchamiania programów na komputerach z systemem Windows bez konieczności wykonywania jakichkolwiek czynności konfiguracyjnych ani zapisywania danych konfiguracyjnych na tych komputerach.

### udostępnianie

Umożliwianie odbiorcom wiadomości e-mail uzyskanie przez określony czas dostępu do wybranych kopii zapasowych plików. Podczas udostępniania pliku kopia zapasowa pliku jest wysyłana do określonych odbiorców wiadomości e-mail. Odbiorcy otrzymują wiadomość e-mail od programu Data Backup informującą, że udostępniono im pliki. Wiadomość e-mail zawiera również łącze do udostępnionych plików.

### URL

(Uniform Resource Locator) Standardowy format adresów internetowych.

### USB

(Universal Serial Bus) Ujednolicony interfejs szeregowy komputera umożliwiający podłączanie różnych urządzeń peryferyjnych: klawiatur, joysticków, drukarek itd.

### uwierzytelnianie

Proces identyfikacji osoby, na ogół oparty na weryfikacji unikatowej nazwy i hasła.

# V

## VPN

(Virtual Private Network) Prywatna sieć skonfigurowana wewnątrz sieci publicznej i wykorzystująca jej mechanizmy zarządzania. Sieci VPN są wykorzystywane przez firmy do budowania sieci rozległych (WAN) obejmujących swoim zasięgiem duże terytoria w celu zapewnienia łączności między poszczególnymi oddziałami lub umożliwienia użytkownikom mobilnym dostępu do firmowych sieci lokalnych.

# W

## wardriver

Osoba, która wyszukuje sieci Wi-Fi (802.11) za pomocą komputera obsługującego ten standard oraz specjalistycznego sprzętu lub oprogramowania, jeżdżąc po mieście.

## WEP

(Wired Equivalent Privacy) Protokół szyfrowania i uwierzytelniania zdefiniowany jako część standardu Wi-Fi (802.11). Wczesne wersje są oparte na algorytmach szyfrowania RC4 i mają istotne wady. Protokół WEP stara się zapewnić bezpieczeństwo poprzez szyfrowanie danych przesyłanych drogą radiową, dzięki czemu są one chronione podczas przesyłania z jednego punktu do drugiego. Jednak praktyka pokazała, że protokół WEP nie jest tak bezpieczny, jak kiedyś sądzono.

## węzeł

Pojedynczy komputer podłączony do sieci.

## Wi-Fi

(Wireless Fidelity) Pojęcie stosowane przez organizację Wi-Fi Alliance w odniesieniu do każdej sieci typu 802.11.

## Wi-Fi Alliance

Organizacja, w której skład wchodzą najważniejsi producenci sprzętu i oprogramowania do komunikacji bezprzewodowej. Jej celem jest weryfikowanie wszystkich urządzeń sieci 802.11 pod kątem zdolności współdziałania oraz promowanie pojęcia „Wi-Fi” jako globalnej marki dla wszystkich urządzeń tworzących sieci LAN zgodne ze standardem 802.11. Organizacja działa jako konsorcjum, laboratorium testowe i izba rozrachunkowa dla dostawców, którzy chcą wspierać rozwój branży.

## Wi-Fi Certified

Urządzenie sprawdzone i zatwierdzone przez organizację Wi-Fi Alliance. Produkty oznaczone logo Wi-Fi Certified uważa się za zgodne ze sobą, mimo iż mogą pochodzić od różnych producentów. Jeśli oba produkty noszą oznaczenie Wi-Fi Certified, użytkownik może korzystać z punktu dostępu dowolnego producenta w połączeniu ze sprzętem klienckim innego dowolnego producenta.

## wirus

Samopowielający się program, który może modyfikować pliki lub dane użytkownika. Wirusy często sprawiają wrażenie pochodzących od zaufanego nadawcy lub zawierających nieszkodliwą zawartość.

### WLAN

(Wireless Local Area Network) Sieć lokalna korzystająca z połączeń bezprzewodowych. W sieci WLAN do komunikacji pomiędzy komputerami zamiast przewodów stosuje się fale radiowe o wysokiej częstotliwości.

### WPA

(Wi-Fi Protected Access) Standard znacznie zwiększający poziom ochrony danych i kontroli dostępu w istniejących i przyszłych systemach bezprzewodowej sieci LAN. Zaprojektowany do pracy na istniejącym sprzęcie jako aktualizacja oprogramowania, standard WPA pochodzi od standardu IEEE 802.11i i jest z nim kompatybilny. Po prawidłowej instalacji gwarantuje użytkownikom bezprzewodowej sieci LAN, że ich dane są chronione, a do sieci mają dostęp tylko autoryzowani użytkownicy.

### WPA-PSK

Specjalny tryb WPA zaprojektowany dla użytkowników indywidualnych, którzy nie wymagają silnych zabezpieczeń klasy korporacyjnej i nie posiadają dostępu do serwerów uwierzytelniania. W tym trybie użytkownik indywidualny wprowadza hasło początkowe służące do aktywacji standardu Wi-Fi Protected Access z zastosowaniem klucza wstępnego. Hasło należy regularnie zmieniać na każdym komputerze bezprzewodowym i punkcie dostępu. Patrz także WPA2-PSK i TKIP.

### WPA2

Nowsza wersja standardu zabezpieczeń WPA, bazująca na standardzie 802.11i IEEE.

### WPA2-PSK

Specjalny tryb WPA bazujący na standardzie WPA2, podobny do standardu WPA-PSK. Popularną cechą urządzeń korzystających ze standardu WPA2-PSK jest ich zdolność do obsługi kilku trybów szyfrowania jednocześnie (np. AES, TKIP), podczas gdy starsze urządzenia na ogół obsługują tylko jeden tryb szyfrowania (tzn. wszystkie komputery klienckie muszą korzystać z tego samego trybu szyfrowania).

### współdzielone hasło

Ciąg tekstowy lub klucz (zazwyczaj hasło) ustalony wspólnie przez dwie strony przed zainicjowaniem komunikacji. Zadaniem współdzielonego hasła jest ochrona poufnych części komunikatów RADIUS.

### wyskakujące okna

Niewielkie okna pojawiające się na tle innych okien na ekranie komputera. Wyskakujące okna są często używane w przeglądarkach sieci Web do wyświetlania reklam.

## Z

### zapora

System (sprzętowy, programowy lub sprzętowo-programowy) zaprojektowany w celu zapobiegania nieautoryzowanemu dostępowi do lub z sieci prywatnej. Zapory są często stosowane w celu uniemożliwienia nieautoryzowanym użytkownikom Internetu uzyskania dostępu do sieci prywatnych podłączonych do Internetu, w szczególności sieci intranet. Wszystkie wiadomości wchodzące do intranetu i wychodzące z niego przechodzą przez zaporę, która analizuje każdą wiadomość i blokuje te, które nie spełniają określonych kryteriów zabezpieczeń.

### *zdarzenie*

Zdarzenie zainicjowane przez użytkownika, urządzenie lub komputer, które wywołuje określoną reakcję. W programie McAfee zdarzenia są rejestrowane w dzienniku zdarzeń.

### *zewnętrzny dysk twardy*

Dysk twardy znajdujący się na zewnątrz komputera.

### *zwykły tekst*

Tekst, który nie jest zaszyfrowany. Zobacz też: szyfrowanie.

# Informacje o firmie McAfee

Firma McAfee, Inc. z siedzibą w Santa Clara w Kalifornii, będąca światowym liderem w dziedzinie ochrony przed włamaniami i zarządzania ryzykiem wystąpienia zagrożeń, dostarcza proaktywne i sprawdzone rozwiązania i usługi służące zabezpieczaniu systemów i sieci na całym świecie. Dzięki bogatemu doświadczeniu w dziedzinie bezpieczeństwa oraz zaangażowaniu w dostarczanie innowacyjnych technologii firma McAfee daje użytkownikom indywidualnym, firmom i usługodawcom możliwość blokowania ataków, zapobiegania zakłóceniom oraz ciągłego śledzenia i ulepszania stanu swoich zabezpieczeń.

## Copyright

# Licencja

UWAGA DLA WSZYSTKICH UŻYTKOWNIKÓW: NALEŻY UWAŻNIE PRZECZYTAĆ ODPOWIEDNIĄ UMOWĘ PRAWNĄ (ZWIĄZANĄ Z NABYTĄ LICENCJĄ), W KTÓREJ OPISANE SĄ OGÓLNE WARUNKI UŻYTKOWANIA LICENCJONOWANEGO OPROGRAMOWANIA. W PRZYPADKU WĄTPLIWOŚCI CO DO TYPU UZYSKANEJ LICENCJI NALEŻY ZAPOZNAĆ SIĘ Z DOKUMENTAMI SPRZEDAŻY LUB INNYMI POKREWNYMI DOKUMENTAMI LICENCYJNYMI BĄDŹ ZAMÓWIENIAMI ZAKUPU DOŁĄCZONYMI DO OPAKOWANIA OPROGRAMOWANIA ALBO OTRZYMANYMI ODDZIELNIE W RAMACH ZAKUPU (W FORMIE KSIĄŻECZKI, PLIKU NA DYSKU CD Z PRODUKTEM ALBO PLIKU DOSTĘPNEGO NA STRONIE INTERNETOWEJ, Z KTÓREJ ZOSTAŁ POBRANY PAKIET OPROGRAMOWANIA). JEŚLI NIE SĄ AKCEPTOWANE WSZYSTKIE WARUNKI ZAWARTE W NINIEJSZEJ UMOWIE, NIE NALEŻY INSTALOWAĆ OPROGRAMOWANIA. JEŚLI JEST TO ZGODNE Z WARUNKAMI SPRZEDAŻY, W PRZYPADKU NIEZAAKCEPTOWANIA UMOWY MOŻNA ZWRÓCIĆ PRODUKT DO FIRMY MCAFEE, INC. LUB MIEJSCA ZAKUPU I OTRZYMAĆ CAŁKOWITY ZWROT KOSZTÓW.

ROZDZIAŁ 18

# Biuro obsługi klienta i pomoc techniczna

Program SecurityCenter zgłasza krytyczne i niekrytyczne problemy dotyczące ochrony natychmiast po ich wykryciu. Krytyczne problemy dotyczące ochrony wymagają niezwłocznego działania i powodują obniżenie stanu ochrony (kolor jest zmieniany na czerwony). Niekrytyczne problemy dotyczące ochrony nie wymagają niezwłocznego działania i nie muszą, choć mogą, skutkować obniżeniem stanu ochrony (zależy to od typu problemu). Aby osiągnąć zielony stan ochrony, należy naprawić wszystkie problemy krytyczne oraz naprawić lub zignorować wszystkie problemy niekrytyczne. Jeśli potrzebna jest pomoc w diagnozowaniu problemów dotyczących ochrony, można uruchomić narzędzie McAfee Virtual Technician. Aby uzyskać więcej informacji na temat narzędzia McAfee Virtual Technician, zobacz Pomoc tego narzędzia.

Jeśli oprogramowanie zabezpieczające zostało kupione od partnera lub dostawcy innego niż firma McAfee, otwórz przeglądarkę sieci Web i przejdź do witryny www.mcafeepomoc.com. Następnie w sekcji Partner Links zaznacz odpowiedniego partnera lub usługodawcę, co spowoduje zainicjowanie narzędzia McAfee Virtual Technician.

**Uwaga:** Aby zainstalować narzędzie McAfee Virtual Technician i go używać, należy się zalogować na swoim komputerze jako administrator systemu Windows. W przeciwnym razie narzędzie może nie być w stanie rozwiązywać problemów. Aby uzyskać informacje na temat logowania się jako administrator systemu Windows, zobacz Pomoc systemu Windows. W systemie Windows Vista™ po uruchomieniu narzędzia MVT jest wyświetlany monit. W oknie monitu należy kliknąć przycisk **Akceptuję**. Narzędzie Virtual Technician nie współpracuje z przeglądarką Mozilla® Firefox.

## W tym rozdziale

Korzystanie z narzędzia McAfee Virtual Technician .....122
Pomoc techniczna i produkty do pobrania .....123

# Korzystanie z narzędzia McAfee Virtual Technician

Narzędzie Virtual Technician, podobnie jak pracownik biura obsługi technicznej, gromadzi informacje na temat programów SecurityCenter, aby rozwiązać problemy dotyczące ochrony komputera. Po uruchomieniu narzędzie Virtual Technician sprawdza, czy programy SecurityCenter działają właściwie. W przypadku wykrycia problemów narzędzie przedstawia propozycje ich naprawienia lub szczegółowe informacje na ich temat. Po zakończeniu tego etapu narzędzie Virtual Technician wyświetla wyniki przeprowadzonej analizy i, jeśli to konieczne, pozwala uzyskać dalszą pomoc techniczną od firmy McAfee.

Aby zachować bezpieczeństwo oraz integralność komputera i plików, aplikacja nie gromadzi danych osobowych umożliwiających identyfikację użytkownika.

**Uwaga:** Aby uzyskać więcej informacji na temat narzędzia Virtual Technician, należy kliknąć ikonę **Pomoc** w tym narzędziu.

## Uruchamianie narzędzia Virtual Technician

Narzędzie Virtual Technician gromadzi informacje na temat programów SecurityCenter, aby rozwiązać problemy dotyczące ochrony komputera. Aby chronić prywatność użytkownika, informacje te nie obejmują danych osobowych umożliwiających jego identyfikację.

1. W obszarze **Typowe zadania** kliknij opcję **McAfee Virtual Technician**.
2. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby pobrać i uruchomić narzędzie Virtual Technician.

# Pomoc techniczna i produkty do pobrania

Aby uzyskać informacje o witrynach firmy McAfee dotyczących pomocy technicznej i produktów do pobrania (w tym podręczników użytkownika), skorzystaj z tabel zamieszczonych poniżej.

## Pomoc techniczna i produkty do pobrania

| Kraj | McAfee — Pomoc techniczna | McAfee — Produkty do pobrania |
|---|---|---|
| Australia | www.mcafeehelp.com | au.mcafee.com/root/downloads.asp |
| Brazylia | www.mcafeeajuda.com | br.mcafee.com/root/downloads.asp |
| Kanada (angielski) | www.mcafeehelp.com | ca.mcafee.com/root/downloads.asp |
| Kanada (francuski) | www.mcafeehelp.com | ca.mcafee.com/root/downloads.asp |
| Chiny (kontynentalne) | www.mcafeehelp.com | cn.mcafee.com/root/downloads.asp |
| Chiny (Tajwan) | www.mcafeehelp.com | tw.mcafee.com/root/downloads.asp |
| Czechy | www.mcafeenapoveda.com | cz.mcafee.com/root/downloads.asp |
| Dania | www.mcafeehjaelp.com | dk.mcafee.com/root/downloads.asp |
| Finlandia | www.mcafeehelp.com | fi.mcafee.com/root/downloads.asp |
| Francja | www.mcafeeaide.com | fr.mcafee.com/root/downloads.asp |
| Niemcy | www.mcafeehilfe.com | de.mcafee.com/root/downloads.asp |
| Wielka Brytania | www.mcafeehelp.com | uk.mcafee.com/root/downloads.asp |
| Włochy | www.mcafeeaiuto.com | it.mcafee.com/root/downloads.asp |
| Japonia | www.mcafeehelp.jp | jp.mcafee.com/root/downloads.asp |
| Korea | www.mcafeehelp.com | kr.mcafee.com/root/downloads.asp |
| Meksyk | www.mcafeehelp.com | mx.mcafee.com/root/downloads.asp |
| Norwegia | www.mcafeehjelp.com | no.mcafee.com/root/downloads.asp |

| | | |
|---|---|---|
| Polska | www.mcafeepomoc.com | pl.mcafee.com/root/downloads.asp |
| Portugalia | www.mcafeeajuda.com | pt.mcafee.com/root/downloads.asp |
| Hiszpania | www.mcafeeayuda.com | es.mcafee.com/root/downloads.asp |
| Szwecja | www.mcafeehjalp.com | se.mcafee.com/root/downloads.asp |
| Turcja | www.mcafeehelp.com | tr.mcafee.com/root/downloads.asp |
| Stany Zjednoczone | www.mcafeehelp.com | us.mcafee.com/root/downloads.asp |

## Podręczniki użytkownika pakietu McAfee Total Protection

| Kraj | Podręczniki użytkownika oprogramowania McAfee |
|---|---|
| Australia | download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf |
| Brazylia | download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf |
| Kanada (angielski) | download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf |
| Kanada (francuski) | download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf |
| Chiny (kontynentalne) | download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf |
| Chiny (Tajwan) | download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf |
| Czechy | download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf |
| Dania | download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf |
| Finlandia | download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf |
| Francja | download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf |
| Niemcy | download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf |
| Wielka Brytania | download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf |
| Holandia | download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf |
| Włochy | download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf |

| | |
|---|---|
| Japonia | download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf |
| Korea | download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf |
| Meksyk | download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf |
| Norwegia | download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf |
| Polska | download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf |
| Portugalia | download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf |
| Hiszpania | download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf |
| Szwecja | download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf |
| Turcja | download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf |
| Stany Zjednoczone | download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf |

## Podręczniki użytkownika pakietu McAfee Internet Security

| Kraj | Podręczniki użytkownika oprogramowania McAfee |
|---|---|
| Australia | download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf |
| Brazylia | download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf |
| Kanada (angielski) | download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf |
| Kanada (francuski) | download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf |
| Chiny (kontynentalne) | download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf |
| Chiny (Tajwan) | download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf |
| Czechy | download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf |
| Dania | download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf |
| Finlandia | download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf |

| | |
|---|---|
| Francja | download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf |
| Niemcy | download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf |
| Wielka Brytania | download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf |
| Holandia | download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf |
| Włochy | download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf |
| Japonia | download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf |
| Korea | download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf |
| Meksyk | download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf |
| Norwegia | download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf |
| Polska | download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf |
| Portugalia | download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf |
| Hiszpania | download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf |
| Szwecja | download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf |
| Turcja | download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf |
| Stany Zjednoczone | download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf |

## Podręczniki użytkownika programu McAfee VirusScan Plus

| Kraj | Podręczniki użytkownika oprogramowania McAfee |
|---|---|
| Australia | download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf |
| Brazylia | download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf |
| Kanada (angielski) | download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf |
| Kanada (francuski) | download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf |
| Chiny (kontynentalne) | download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf |

| | |
|---|---|
| Chiny (Tajwan) | download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf |
| Czechy | download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf |
| Dania | download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf |
| Finlandia | download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf |
| Francja | download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf |
| Niemcy | download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf |
| Wielka Brytania | download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf |
| Holandia | download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf |
| Włochy | download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf |
| Japonia | download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf |
| Korea | download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf |
| Meksyk | download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf |
| Norwegia | download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf |
| Polska | download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf |
| Portugalia | download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf |
| Hiszpania | download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf |
| Szwecja | download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf |
| Turcja | download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf |
| Stany Zjednoczone | download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf |

## Podręczniki użytkownika programu McAfee VirusScan

| Kraj | Podręczniki użytkownika oprogramowania McAfee |
|---|---|

| | |
|---|---|
| Australia | download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf |
| Brazylia | download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf |
| Kanada (angielski) | download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf |
| Kanada (francuski) | download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf |
| Chiny (kontynentalne) | download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf |
| Chiny (Tajwan) | download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf |
| Czechy | download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf |
| Dania | download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf |
| Finlandia | download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf |
| Francja | download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf |
| Niemcy | download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf |
| Wielka Brytania | download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf |
| Holandia | download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf |
| Włochy | download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf |
| Japonia | download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf |
| Korea | download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf |
| Meksyk | download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf |
| Norwegia | download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf |
| Polska | download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf |
| Portugalia | download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf |
| Hiszpania | download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf |
| Szwecja | download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf |
| Turcja | download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf |
| Stany Zjednoczone | download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf |

W tabeli poniżej przedstawiono Centrum zagrożeń firmy McAfee oraz witryny z informacjami o wirusach dostępne w poszczególnych krajach.

| Kraj | Centrala bezpieczeństwa | Informacje o wirusach |
|---|---|---|
| Australia | www.mcafee.com/us/threat_center | au.mcafee.com/virusInfo |
| Brazylia | www.mcafee.com/us/threat_center | br.mcafee.com/virusInfo |
| Kanada (angielski) | www.mcafee.com/us/threat_center | ca.mcafee.com/virusInfo |
| Kanada (francuski) | www.mcafee.com/us/threat_center | ca.mcafee.com/virusInfo |
| Chiny (kontynentalne) | www.mcafee.com/us/threat_center | cn.mcafee.com/virusInfo |
| Chiny (Tajwan) | www.mcafee.com/us/threat_center | tw.mcafee.com/virusInfo |
| Czechy | www.mcafee.com/us/threat_center | cz.mcafee.com/virusInfo |
| Dania | www.mcafee.com/us/threat_center | dk.mcafee.com/virusInfo |
| Finlandia | www.mcafee.com/us/threat_center | fi.mcafee.com/virusInfo |
| Francja | www.mcafee.com/us/threat_center | fr.mcafee.com/virusInfo |
| Niemcy | www.mcafee.com/us/threat_center | de.mcafee.com/virusInfo |
| Wielka Brytania | www.mcafee.com/us/threat_center | uk.mcafee.com/virusInfo |
| Holandia | www.mcafee.com/us/threat_center | nl.mcafee.com/virusInfo |
| Włochy | www.mcafee.com/us/threat_center | it.mcafee.com/virusInfo |
| Japonia | www.mcafee.com/us/threat_center | jp.mcafee.com/virusInfo |
| Korea | www.mcafee.com/us/threat_center | kr.mcafee.com/virusInfo |
| Meksyk | www.mcafee.com/us/threat_center | mx.mcafee.com/virusInfo |
| Norwegia | www.mcafee.com/us/threat_center | no.mcafee.com/virusInfo |
| Polska | www.mcafee.com/us/threat_center | pl.mcafee.com/virusInfo |
| Portugalia | www.mcafee.com/us/threat_center | pt.mcafee.com/virusInfo |
| Hiszpania | www.mcafee.com/us/threat_center | es.mcafee.com/virusInfo |
| Szwecja | www.mcafee.com/us/threat_center | se.mcafee.com/virusInfo |
| Turcja | www.mcafee.com/us/threat_center | tr.mcafee.com/virusInfo |
| Stany Zjednoczone | www.mcafee.com/us/threat_center | us.mcafee.com/virusInfo |

W tabeli poniżej przedstawiono witryny HackerWatch dostępne w poszczególnych krajach.

| Kraj | HackerWatch |
|---|---|
| Australia | www.hackerwatch.org |
| Brazylia | www.hackerwatch.org/?lang=pt-br |
| Kanada (angielski) | www.hackerwatch.org |
| Kanada (francuski) | www.hackerwatch.org/?lang=fr-ca |
| Chiny (kontynentalne) | www.hackerwatch.org/?lang=zh-cn |
| Chiny (Tajwan) | www.hackerwatch.org/?lang=zh-tw |
| Czechy | www.hackerwatch.org/?lang=cs |
| Dania | www.hackerwatch.org/?lang=da |
| Finlandia | www.hackerwatch.org/?lang=fi |
| Francja | www.hackerwatch.org/?lang=fr |
| Niemcy | www.hackerwatch.org/?lang=de |
| Wielka Brytania | www.hackerwatch.org |
| Holandia | www.hackerwatch.org/?lang=nl |
| Włochy | www.hackerwatch.org/?lang=it |
| Japonia | www.hackerwatch.org/?lang=jp |
| Korea | www.hackerwatch.org/?lang=ko |
| Meksyk | www.hackerwatch.org/?lang=es-mx |
| Norwegia | www.hackerwatch.org/?lang=no |
| Polska | www.hackerwatch.org/?lang=pl |
| Portugalia | www.hackerwatch.org/?lang=pt-pt |
| Hiszpania | www.hackerwatch.org/?lang=es |
| Szwecja | www.hackerwatch.org/?lang=sv |
| Turcja | www.hackerwatch.org/?lang=tr |
| Stany Zjednoczone | www.hackerwatch.org |

# Indeks


## 8

802.11 ..... 103
802.11a ..... 103
802.11b ..... 103
802.1x ..... 103

## A

ActiveX, formant ..... 103
adres IP ..... 103
Adres MAC ..... 103
Aktualizowanie oprogramowania SecurityCenter ..... 13
archiwizacja ..... 103
archiwizacja pełna ..... 104
archiwizacja szybka ..... 104
atak słownikowy ..... 104
atak typu ..... 104
atak typu DoS (odmowa usługi) ..... 104
Automatyczne naprawianie problemów dotyczących ochrony ..... 18

## B

biała lista ..... 104
biblioteka ..... 104
Biuro obsługi klienta i pomoc techniczna ... 121
brama zintegrowana ..... 104

## C

Copyright ..... 119
czarna lista ..... 105

## D

DAT ..... 105
Defragmentowanie komputera ..... 73
dialer ..... 105
DNS ..... 105
dodatek ..... 105
Dołączanie do zarządzanej sieci ..... 92, 93
domena ..... 105
dysk inteligentny ..... 105
dysk sieciowy ..... 105

## E

ESS ..... 105

## F

filtrowanie obrazów ..... 106
fragmenty plików ..... 106
Funkcje ochrony rodzicielskiej ..... 106
Funkcje programu Network Manager ..... 86
Funkcje programu QuickClean ..... 68
Funkcje programu SecurityCenter ..... 6
Funkcje programu Shredder ..... 82
Funkcje programu VirusScan ..... 33

## G

grupy klasyfikacji zawartości ..... 106

## H

hasło ..... 106

## I

Ignorowanie problemów dotyczących ochrony ..... 20
Ignorowanie problemu dotyczącego ochrony 20
Ikony programu Network Manager ..... 87
Informacje o firmie McAfee ..... 119
Instalowanie oprogramowania zabezpieczającego McAfee na zdalnych komputerach ..... 101
Internet ..... 106
intranet ..... 106

## J

Jak działa stan ochrony ..... 7, 8, 9
Jak działają kategorie ochrony ..... 7, 9, 29
Jak działają usługi ochrony ..... 10

## K

karta PCI sieci bezprzewodowej ..... 106
karta sieci bezprzewodowej ..... 106
Karta sieciowa ..... 107
karta USB sieci bezprzewodowej ..... 107
klient ..... 107
klient poczty e-mail ..... 107
klucz ..... 107
kod uwierzytelniania komunikatów (MAC) 107
kompresja ..... 107
Konfigurowanie automatycznych aktualizacji ..... 14

Konfigurowanie ochrony przed wirusami ....41, 59
Konfigurowanie opcji alertów .....26
Konfigurowanie opcji aplikacji SystemGuard .....50
Konfigurowanie zarządzanej sieci.....89
koń trojański .....107
Korzystanie z mapy sieci.....90
Korzystanie z narzędzia McAfee Virtual Technician.....122
Korzystanie z opcji aplikacji SystemGuard ..48
Korzystanie z programu SecurityCenter .....7
Kosz.....107
kwarantanna .....107

**L**

LAN.....107
Launchpad .....107
Licencja .....120
lista zaufanych.....108
lokalizacja monitorowana częściowo .....108
lokalizacja monitorowana dokładnie.....108
lokalizacje monitorowane.....108

**M**

magazyn haseł .....108
mapa sieci.....108
MAPI.....108
McAfee QuickClean.....67
McAfee VirusScan .....3, 31
Modyfikacja uprawnień zarządzanego komputera .....99
Modyfikacja właściwości wyświetlania urządzenia .....99
Modyfikowanie zadania programu Defragmentator dysku .....78
Modyfikowanie zadania programu QuickClean .....75
Monitorowanie stanu i uprawnień .....98
Monitorowanie stanu ochrony komputera.....98
MSN .....108

**N**

Napraw luki w zabezpieczeniach .....100
Naprawa luk w zabezpieczeniach.....100
Naprawianie lub ignorowanie problemów dotyczących ochrony .....8, 17
Naprawianie problemów dotyczących ochrony .....8, 18
niekontrolowany punkt dostępu .....108
Niszczenie całej zawartości dysku .....84
Niszczenie plików i folderów.....83
Niszczenie plików, folderów i zawartości dysków.....83

**O**

Oczyszczanie komputera ..... 69, 71
Odświeżanie mapy sieci ..... 90
Opis..... 102

**P**

pamięć podręczna ..... 109
Planowanie skanowania..... 47
Planowanie zadania ..... 74
Planowanie zadania programu Defragmentator dysku ..... 77
Planowanie zadania programu QuickClean.. 74
plik cookie ..... 109
plik tymczasowy ..... 109
pluskwy internetowe..... 109
poczta e-mail..... 109
Poczta w sieci Web..... 109
podszywanie się pod adres IP ..... 109
Pokazywanie lub ukrywanie elementu na mapie sieci ..... 91
Pomoc techniczna i produkty do pobrania.. 123
POP3 ..... 109
port..... 109
potencjalnie niepożądany program (PUP) .. 109
PPPoE ..... 110
Praca z alertami ..... 14, 23
Program McAfee Network Manager ..... 85
Program McAfee SecurityCenter ..... 5
Program McAfee Shredder..... 81
protokół..... 110
proxy..... 110
Przeglądanie zdarzeń ..... 18, 29
przeglądarka..... 110
przepełnienie bufora ..... 110
przepustowość ..... 110
przywracanie..... 110
publiczny punkt dostępu..... 110
publikowanie ..... 110
Punkt dostępu ..... 110
punkt przywracania systemu..... 111

**R**

RADIUS ..... 111
rejestr ..... 111
repozytorium kopii zapasowych online..... 111
Ręczne naprawianie problemów dotyczących ochrony ..... 19
roaming..... 111
robak ..... 111
Rodzaje aplikacji SystemGuard — informacje ..... 50, 51
rootkit ..... 111
router..... 111

## S

serwer ....112
serwer DNS ....112
serwer proxy ....112
sieć ....112
sieć domowa ....112
sieć zarządzana ....112
Skanowanie komputera ....34, 59, 60
skanowanie na żądanie ....112
skanowanie w czasie rzeczywistym ....112
skrót ....112
skrypt ....112
słowo kluczowe ....112
SMTP ....113
Sprawdzanie dostępności aktualizacji ....13, 14
SSID ....113
SSL ....113
Stacja USB ....113
standardowe konto e-mail ....113
synchronizacja ....113
SystemGuard ....113
szyfrowanie ....113

## T

tekst zaszyfrowany ....113
TKIP ....114
tworzenie kopii zapasowej ....114
Typy list zaufanych — informacje ....56
typy monitorowanych plików ....114

## U

U3 ....114
udostępnianie ....114
Ukrywanie alertów o epidemiach wirusowych ....27
Ukrywanie ekranu powitalnego podczas uruchamiania ....26
URL ....114
Uruchamianie dodatkowej ochrony ....37
Uruchamianie narzędzia Virtual Technician ....122
Uruchamianie ochrony poczty e-mail ....39
Uruchamianie ochrony przed oprogramowaniem szpiegującym ....38
Uruchamianie ochrony przez skanowanie skryptów ....38
Uruchamianie ochrony wiadomości błyskawicznych ....39
USB ....114
Ustawianie lokalizacji skanowania ręcznego 46
Ustawianie opcji skanowania ręcznego ....44
Ustawianie opcji skanowania w czasie rzeczywistym ....42
Usuwanie zadania programu Defragmentator dysku ....78
Usuwanie zadania programu QuickClean ....76
Utrata zaufania do komputerów w sieci ....95
uwierzytelnianie ....114
Uzyskiwanie dostępu do mapy sieci ....90
Używanie list zaufanych ....55

## V

VPN ....115

## W

wardriver ....115
WEP ....115
Weryfikowanie subskrypcji ....11
węzeł ....115
Wi-Fi ....115
Wi-Fi Alliance ....115
Wi-Fi Certified ....115
wirus ....115
WLAN ....116
Włącz ochronę za pomocą aplikacji SystemGuard ....49
Włączanie ochrony przed wirusami w czasie rzeczywistym ....34
Włączanie ochrony przed wirusami w czasie rzeczywistym ....34
Włączanie odtwarzania dźwięku podczas wyświetlania alertów ....26
WPA ....116
WPA2 ....116
WPA2-PSK ....116
WPA-PSK ....116
współdzielone hasło ....116
Wykonywanie operacji na plikach poddanych kwarantannie ....64, 65
Wykonywanie operacji na potencjalnie niepożądanych programach ....64
Wykonywanie operacji na programach i plikach cookie poddanych kwarantannie ..66
Wykonywanie operacji na wirusach i koniach trojańskich ....64
Wykonywanie operacji na wynikach skanowania ....63
Wyłączanie automatycznych aktualizacji ....14
wyskakujące okna ....116
Wyświetl wyniki skanowania ....61
Wyświetlanie i ukrywanie alertów informacyjnych ....24
Wyświetlanie lub ukrywanie alertów informacyjnych ....24
Wyświetlanie lub ukrywanie alertów informacyjnych na czas korzystania z gier 25

Wyświetlanie lub ukrywanie zignorowanych problemów ....20
Wyświetlanie ostatnich zdarzeń ....29
Wyświetlanie szczegółów elementu....91
Wyświetlanie wszystkich zdarzeń....30

## Z

Zakończenie monitorowania stanu ochrony komputera ....98
zapora ....116
Zapraszanie komputera do dołączenia do sieci zarządzanej ....93
Zarządzanie kontem McAfee ....11
Zarządzanie listami zaufanych ....55
Zarządzanie urządzeniem ....99
Zatrzymywanie ochrony przed wirusami w czasie rzeczywistym ....35
Zdalne zarządzanie siecią....97
zdarzenie....117
zewnętrzny dysk twardy....117
Zmiana nazwy sieci ....91
zwykły tekst....117