TOYA

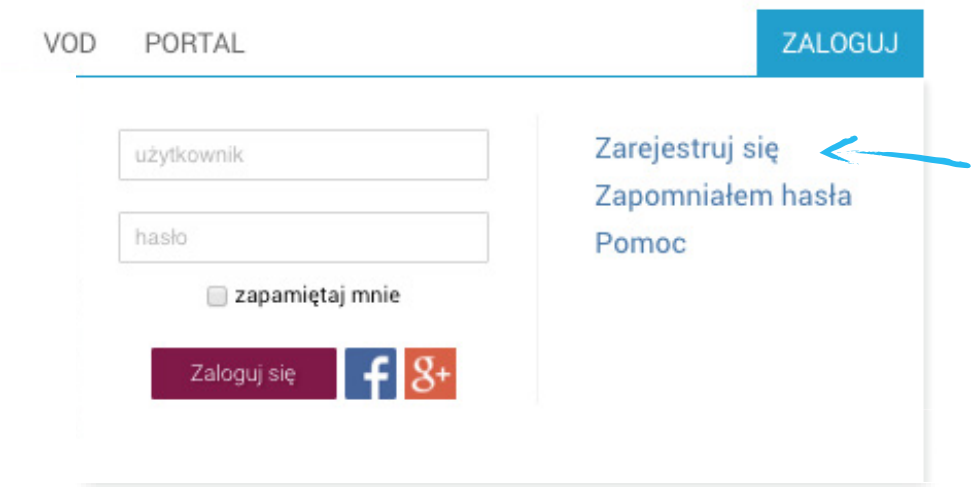
APLIKACJA BEZPIECZNY INTERNET TOYA
dla komputerów
z systemem Windows

Telewizja Internet Telefonia Mobilna VOD TV 3G GO

- Aby pobrać i zainstalować program należy zalogować się swoimi danymi autoryzacyjnymi do Portalu Abonenta TOYA na stronie www.toya.net.pl lub, jeżeli nie mają Państwo konta w Portalu Abonenta, skorzystać z poniższej instrukcji w celu jego założenia.

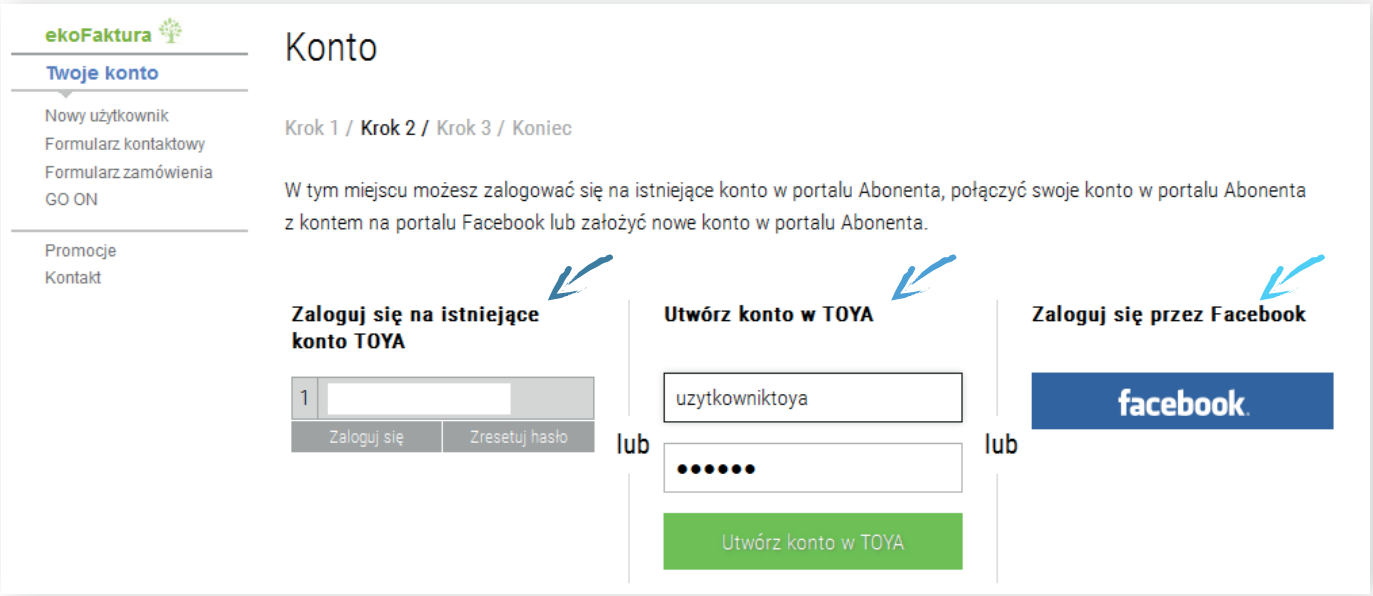
Założenie konta w Portalu Abonenta

- Aby założyć konto w Portalu Abonenta należy:
  - upewnić się, że posiadają Państwo Kartę Aktywacji Konta, którą powinni Państwo otrzymać przy podpisaniu umowy. (W przypadku jej braku lub zagubienia prosimy o skontaktowanie się z **Infolinią TOYA 42 6333 8888**, **info@toya.net.pl**)
  - Kliknąć **„Zarejestruj się”** w oknie, które wysunie się po kliknięciu na napis ,,Zaloguj” na stronie www.toya.net.pl.

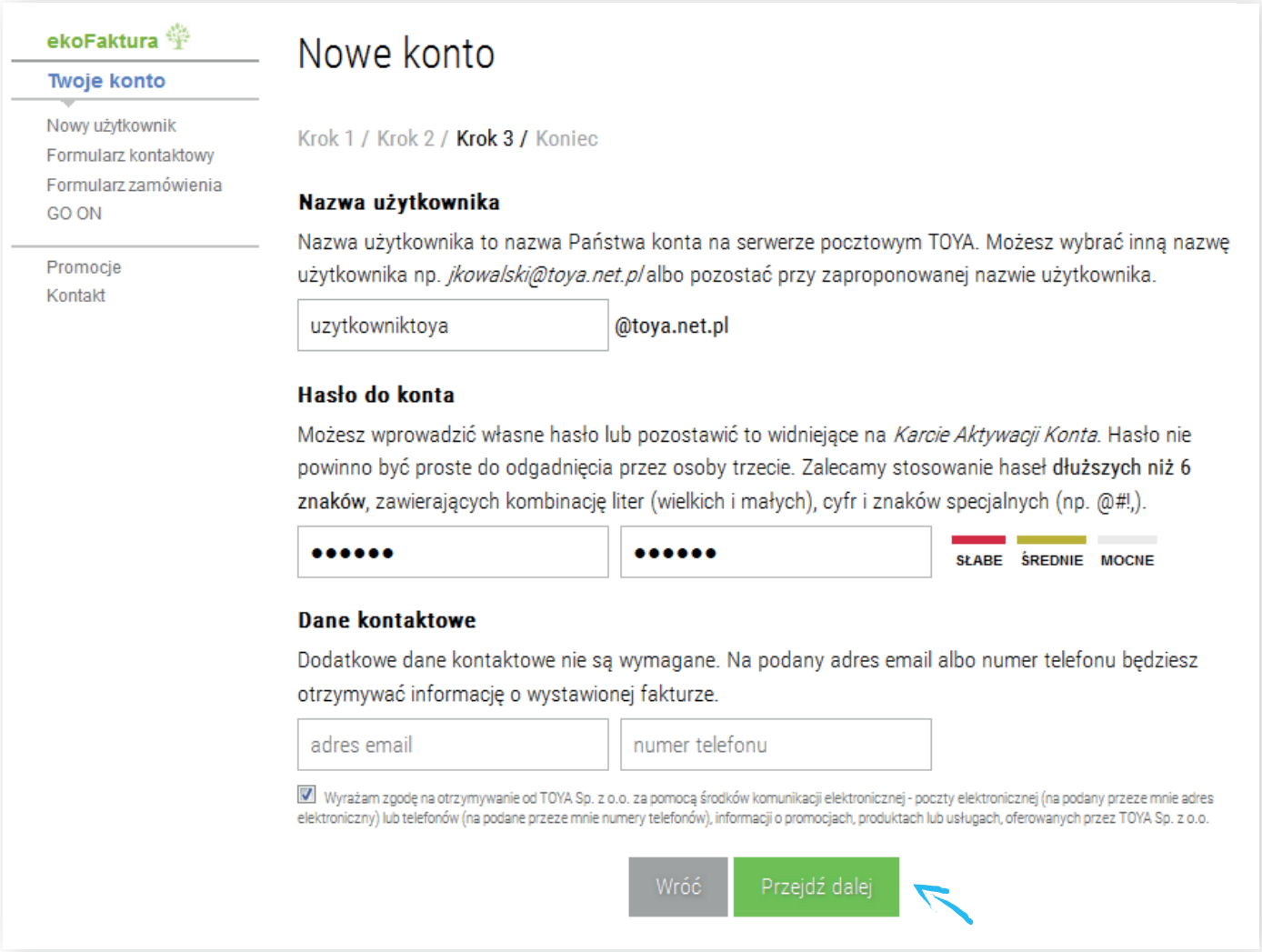


- W pierwszym kroku należy wpisać kod abonenta i hasło z Karty Aktywacji Konta i wcisnąć przycisk **„Przejdź dalej”** :

- W drugim kroku należy wybrać :
  - czy chcecie Państwo **zalogować się** na już istniejące konto, jeśli wcześniej było zakładane,
  - czy chcecie Państwo **utworzyć** zupełnie nowe konto,
  - czy chcecie Państwo **połączyć** swoje konto, jeśli wcześniej było zakładane, z kontem na portalu Facebook.

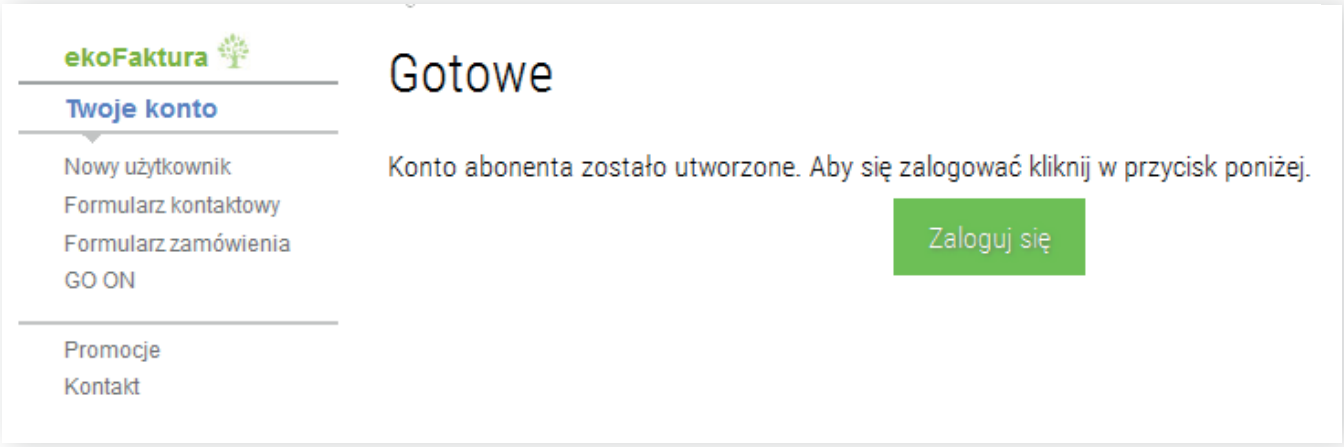


Jeśli wybiorą Państwo opcję założenia zupełnie nowego konta, to w trzecim kroku mogą Państwo jeszcze zmienić nazwę użytkownika i wprowadzić własne hasło przed zatwierdzeniem. Jeśli wszystkie dane wpisane przez Państwa się zgadzają, to należy wcisnąć przycisk **„Przejdź dalej”**:



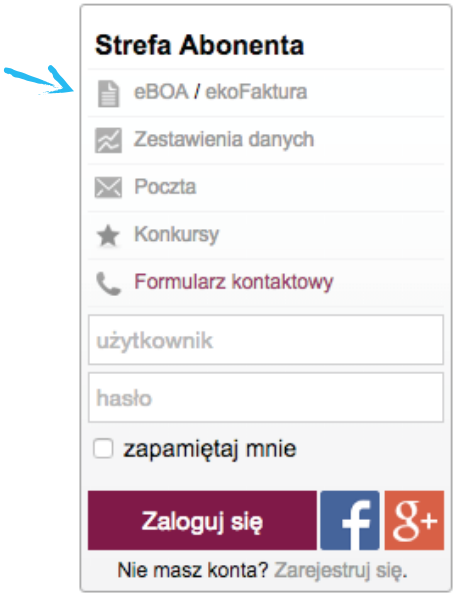
- W końcowym etapie zakładania konta należy upewnić się, że dane są poprawne. Jeżeli chcą Państwo dokonać jakichś poprawek, np. zmienić nazwę użytkownika lub hasło, należy wcisnąć przycisk **„Wróć”**. Jeśli jednak są Państwo pewni, że wpisane dane są poprawne, wówczas należy wcisnąć przycisk **„Tak, utwórz konto w TOYA”**:

- Po zatwierdzeniu Państwa konto już jest utworzone :

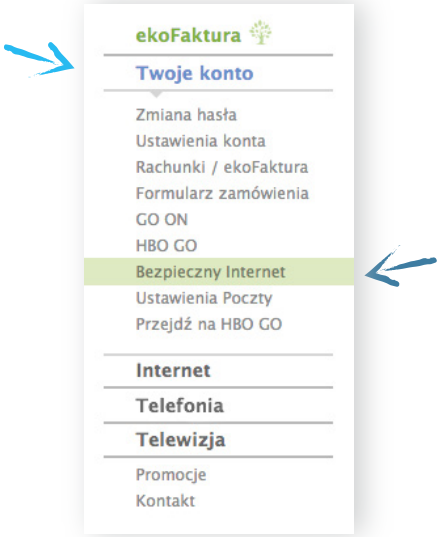


Instalacja programu Bezpieczny Internet TOYA

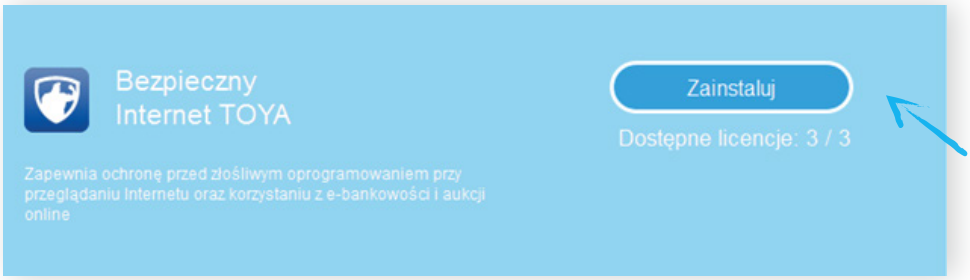
- Po zalogowaniu się w Portalu Abonenta należy w „Strefie Abonenta” kliknąć opcję **eBOA/ekoFaktura**:



- Następnie kliknąć po lewej stronie **„Twoje konto”**, a następnie poniżej wybrać opcję **Bezpieczny Internet**:

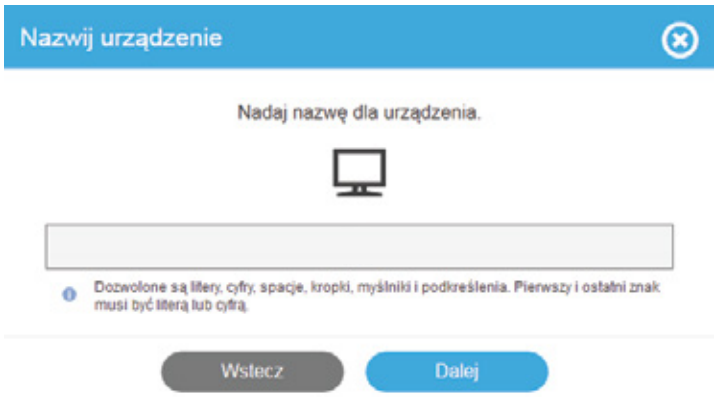


- W zależności od wykupionej opcji usługi, na ekranie pojawi się informacja o dostępnych licencjach. Po kliknięciu przycisku **„Zainstaluj”** pojawi się okienko z możliwością wyboru platformy:

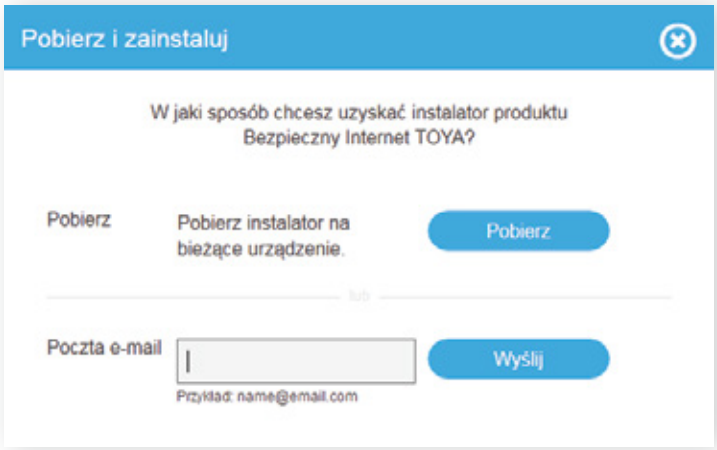


- Aby zainstalować Bezpieczny Internet na swoim urządzeniu z systemem Windows, należy wybrać opcję **Windows PC**:

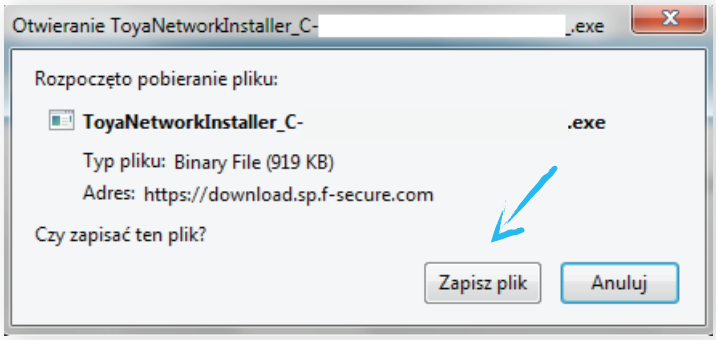
- Następnie należy nadać własną nazwę dla tego urządzenia:



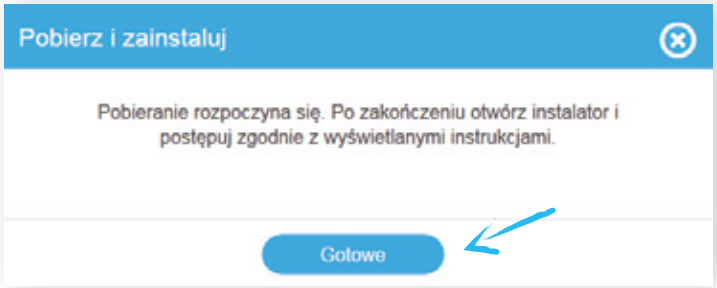
- Następnie należy wybrać w jaki sposób aplikacja Bezpieczny Internet TOYA ma zostać pobrana na Państwa urządzenie:



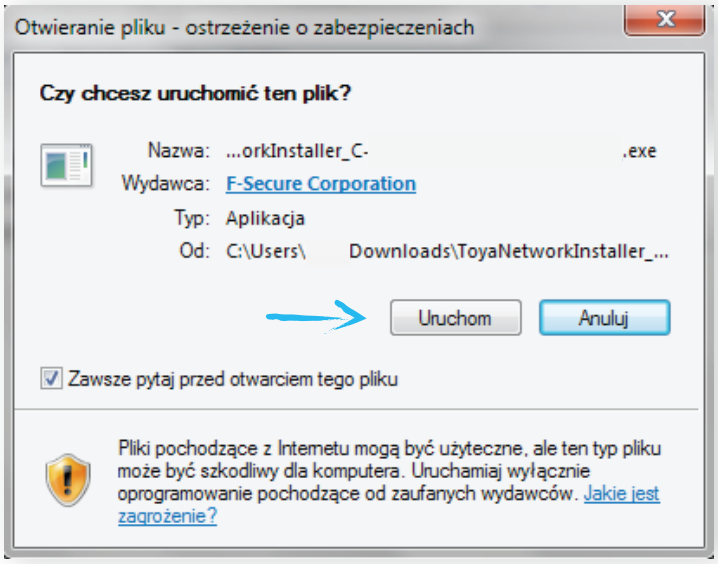
- Jeśli wybierzemy opcję **„Pobierz”**, to rozpocznie się proces pobierania pliku instalacyjnego na bieżące urządzenie.



- Plik instalatora należy zapisać. Jednocześnie na Portalu Abonenta pojawi się poniższy komunikat:



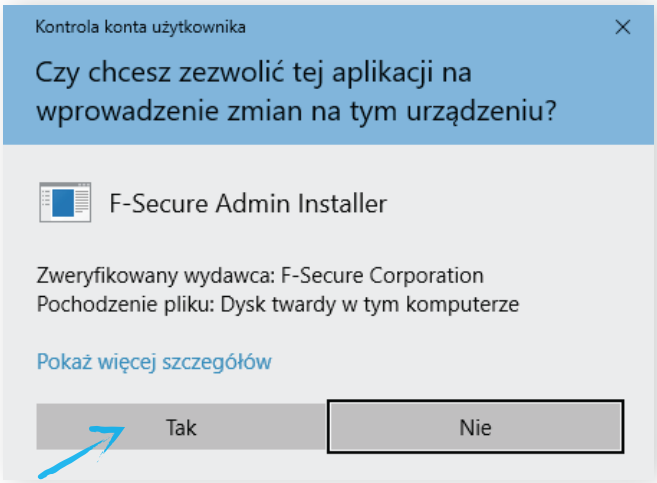
- Po jego pobraniu należy odnaleźć pobrany plik na swoim urządzeniu i uruchomić go aby rozpocząć instalację:



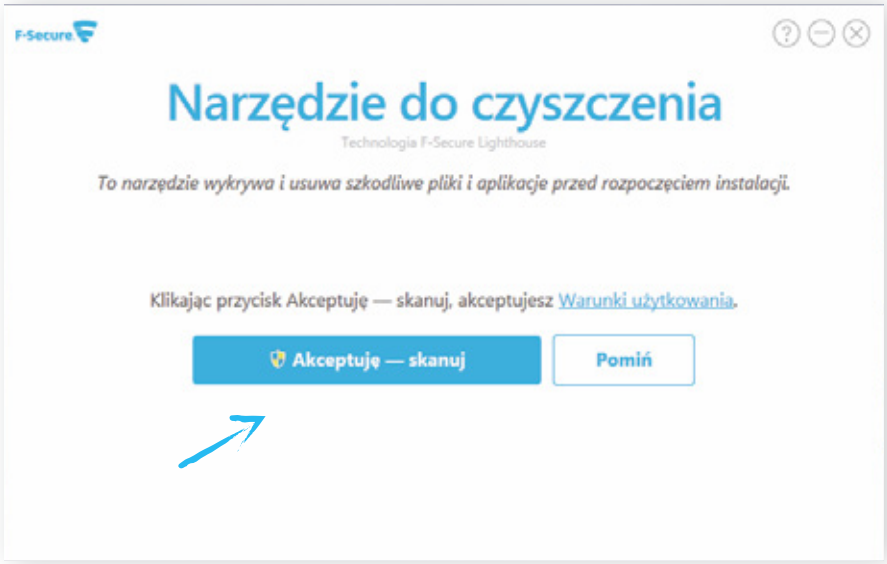
- W przypadku wyboru opcji wysłania pliku instalacyjnego na adres e-mail, otrzymamy na wskazany adres link, który po kliknięciu pozwoli na pobranie pliku instalacyjnego.

Uruchomienie programu Bezpieczny Internet TOYA

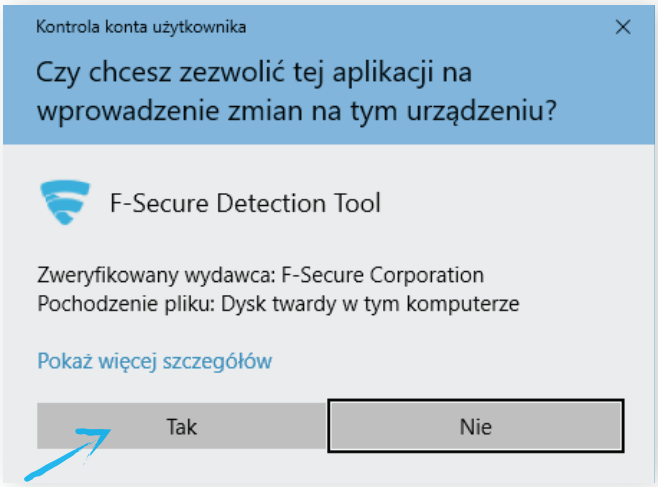
- Po uruchomieniu program poprosi wprowadzenie zmian w systemie niezbędnych dla wykonania instalacji oprogramowania. Ich przyznanie potwierdzamy przyciskiem **„Tak”**.



- W przypadku wykrycia przez program konieczności weryfikacji stanu bezpieczeństwa systemu operacyjnego, program uruchomi okno, w którym przyciskiem **„Akceptuję - skanuj”** potwierdzamy zgodę na usunięcie z systemu szkodliwych plików, które mogą uniemożliwić instalację programu.

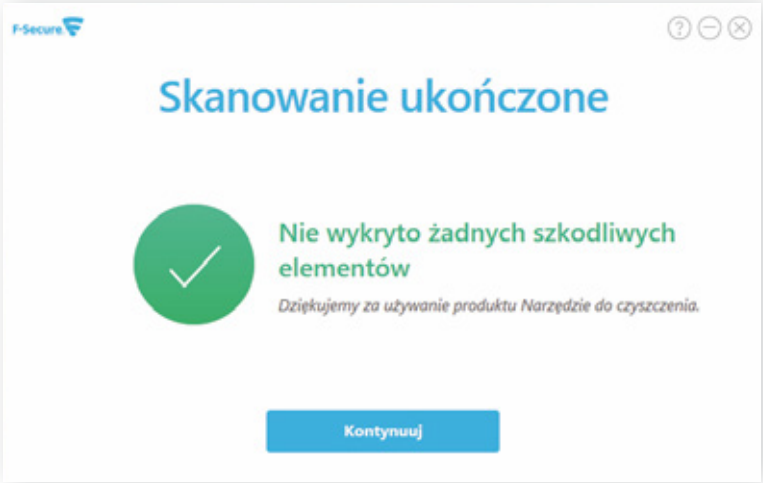


- Aby program mógł dokonać niezbędnych czynności potwierdzamy przyciskiem **„Tak”** zgodę na jego uruchomienie.

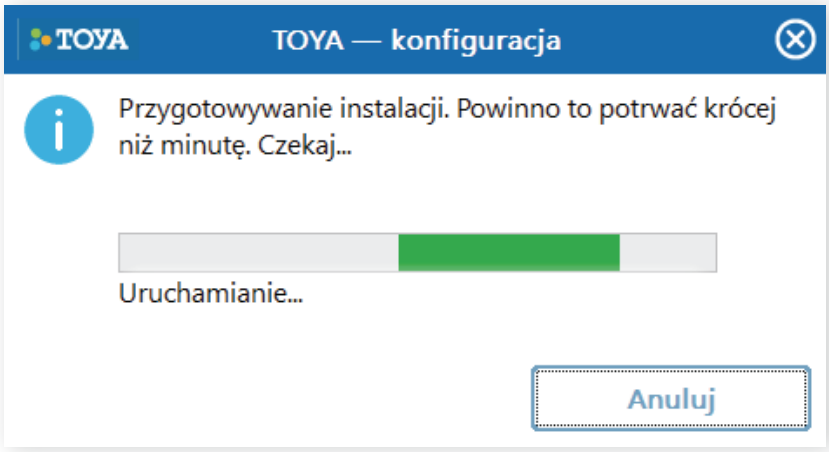


- W przypadku, gdy program wykryje w systemie pliki mogące powodować zagrożenie należy zastosować się do wskazówek, zmierzających do ich usunięcia.

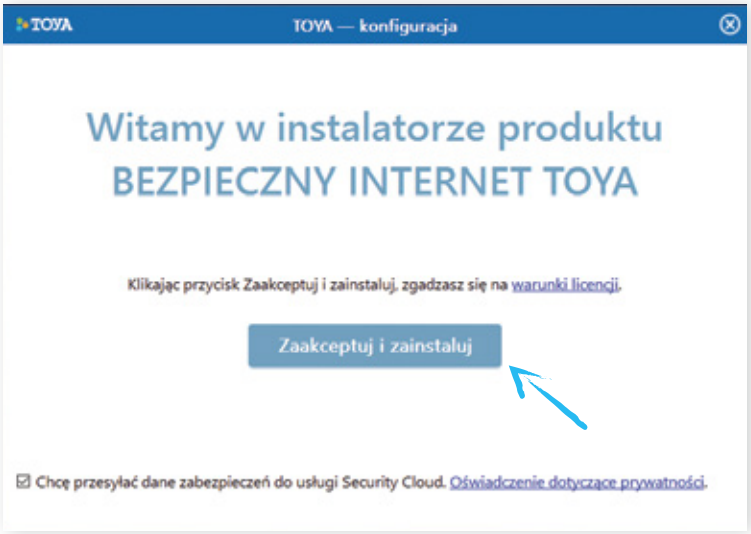
- Po przeskanowaniu systemu i usunięciu istniejących zagrożeń program pokaże poniższe okno, potwierdzające brak w systemie szkodliwych elementów.

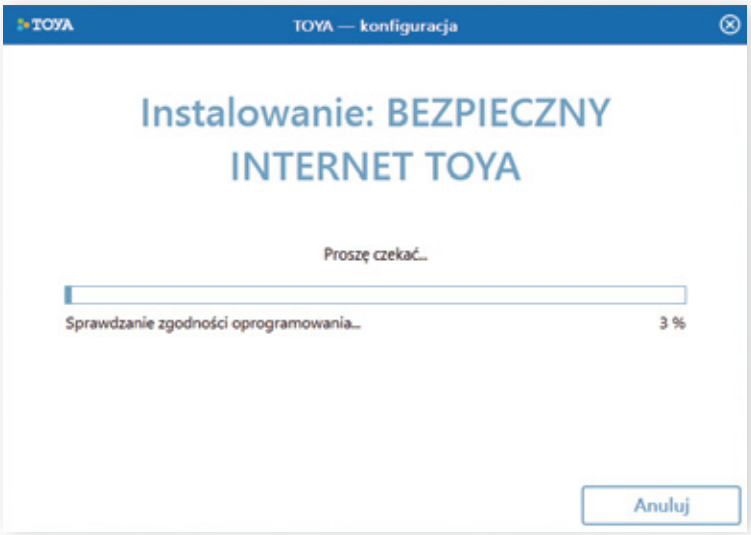


- W kolejnym kroku zostanie automatycznie uruchomiony instalator programu Bezpieczny Internet TOYA.

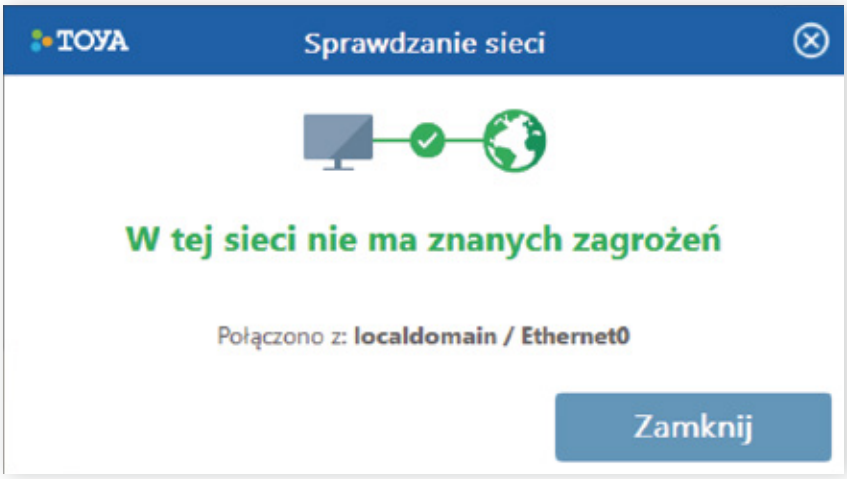


- Następnie należy potwierdzić zaakceptowanie warunków licencji i zgodę na instalację poprzez naciśnięcie przycisku **„Zaakceptuj i zainstaluj”**.

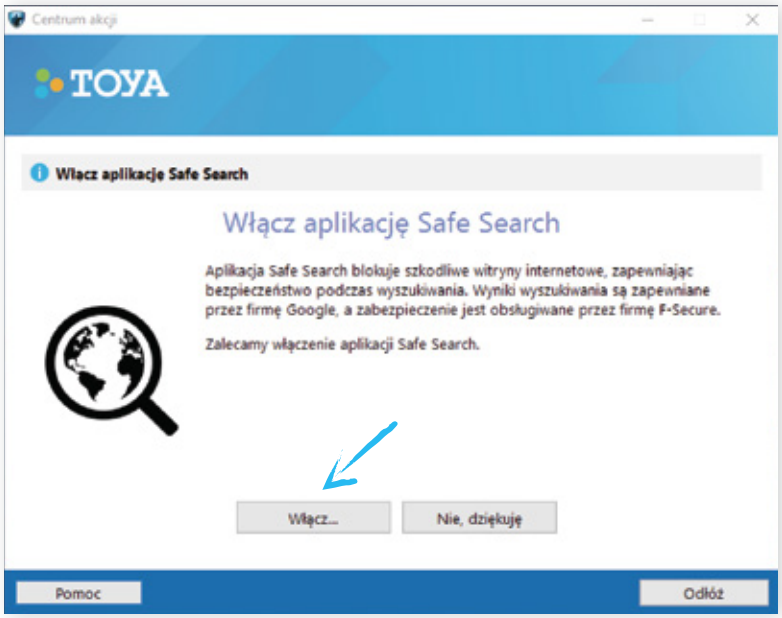




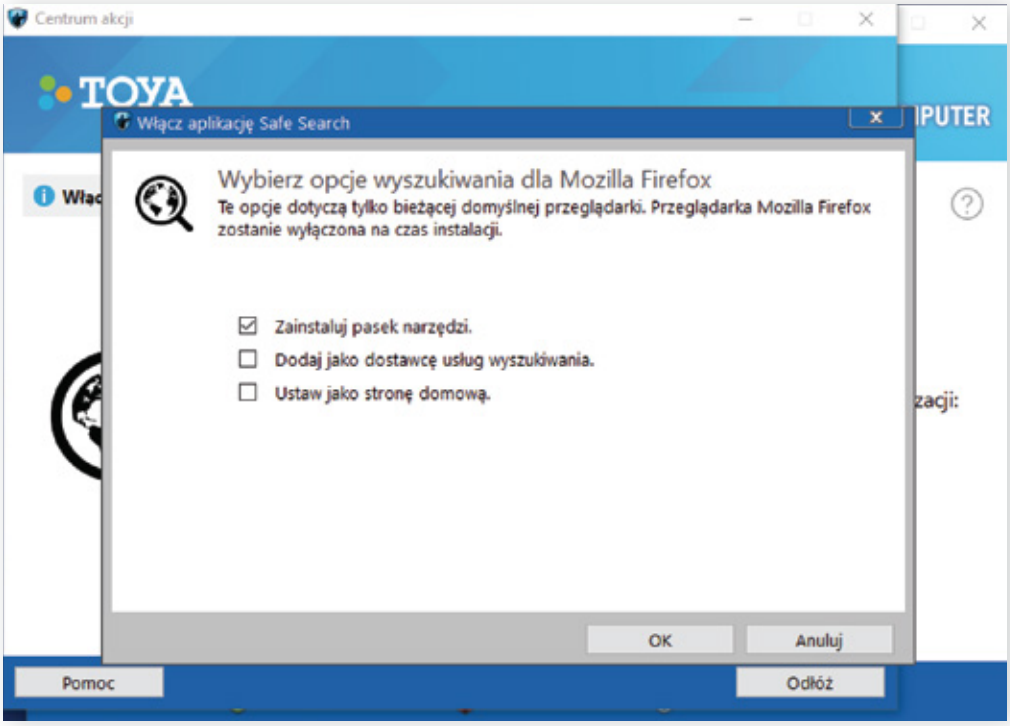
- Po zakończeniu instalacji program zweryfikuje bezpieczeństwo sieci z jakich Państwo korzystają, co potwierdzone zostanie poniższym komunikatem.



- Program zapyta również o zgodę na zainstalowanie dodatku do przeglądarki pozwalającego na kategoryzowanie wyników wyszukiwania pod kątem bezpieczeństwa informacji. Zalecanym ustawieniem jest **„Włącz”**.

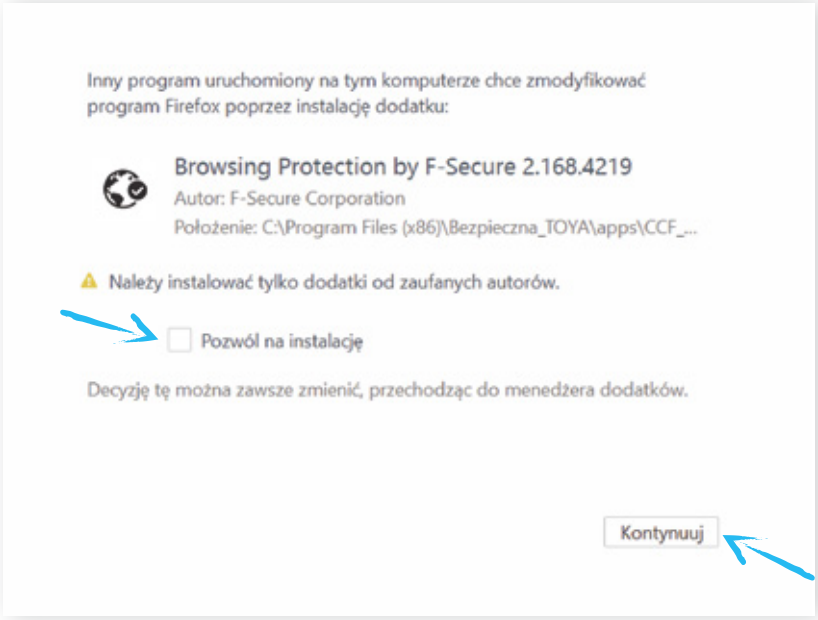


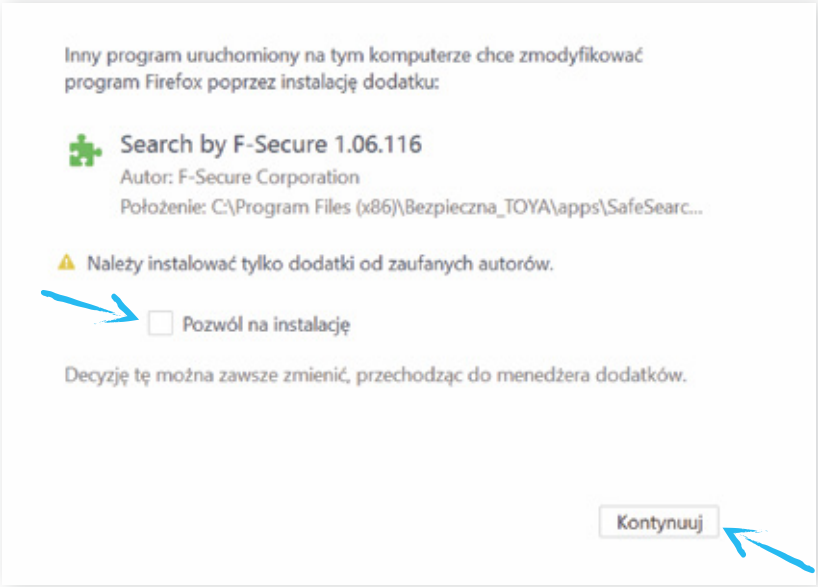
- Po włączeniu program poprosi o zaakceptowanie ustawień zaawansowanych funkcji wyszukiwania.



- Pierwsze uruchomienie przeglądarki będzie również wymagało potwierdzenia zgody na zainstalowanie dodatków w systemie.

- Zalecanym ustawieniem jest zaznaczenie opcji **„Pozwól na instalację”** oraz potwierdzenie przyciskiem **„Kontynuuj”**.





TOYA

APLIKACJA BEZPIECZNY INTERNET TOYA
dla komputerów z systemem Windows - instrukcja obsługi

Telewizja Internet Telefonia Mobilna VOD TV 3G GO

Spis treści

Pierwsze kroki w produkcie Bezpieczny Internet TOYA

Tematy:

W tej sekcji opisano, jak skonfigurować produkt, aby ręcznie lub automatycznie skanował urządzenie, jak wyświetlić i zmienić ustawienia zaawansowane kontrolujące działanie produktu oraz jak wyświetlić statystyki pokazujące działania produktu od momentu zainstalowania.

1.1 Jak sprawdzić, czy urządzenie jest chronione?

Aby upewnić się, że urządzenie jest chronione, sprawdź informacje o stanie produktu dostępne na stronie **Stan**.

Na stronie **Stan** wyświetlane są informacje o stanie ochrony i terminie ważności subskrypcji.

1.1.1 Ikony stanu zabezpieczeń

Ikony na stronie **Stan** przedstawiają ogólny stan produktu i jego funkcji zabezpieczeń.

Następujące ikony przedstawiają stan produktu i jego funkcji zabezpieczeń.

Ikona stanu	Nazwa stanu	Opis
	OK	Urządzenie jest chronione. Funkcja jest włączona i działa poprawnie.
	Informacja	Produkt informuje o specjalnym stanie funkcji. Wszystkie funkcje działają poprawnie, ale na przykład pobierane są aktualizacje.
	Ostrzeżenie	Urządzenie nie jest w pełni chronione. Produkt wymaga uwagi, na przykład od dłuższego czasu nie został zaktualizowany.
	Błąd	Urządzenie nie jest chronione. Na przykład wygasła ważność subskrypcji lub jest wyłączona krytyczna funkcja.
	Wyłączone	Niekrytyczna funkcja jest wyłączona.

1.2 Wyświetl narzędzia produktu

Na stronie **Narzędzia** są wyświetlane informacje na temat korzystania z narzędzi produktu.

1.2.1 Skanowanie zaawansowane

Zaawansowane ustawienia skanowania umożliwiają dostosowanie sposobu, w jaki produkt skanuje w poszukiwaniu wirusów.

Możesz wybrać **pełne skanowanie komputera**, szybsze **skanowanie w poszukiwaniu wirusów** lub **wybrać obszar skanowania**. Możesz też **zmienić ustawienia skanowania** zarówno w przypadku skanowania ręcznego, jak i zaplanowanego, oraz **wyświetlić raport z ostatniego skanowania**.

Informacje: Do zmiany ustawień skanowania wymagane są uprawnienia administratora.

1.2.2 Narzędzie do czyszczenia

Za pomocą narzędzia do czyszczenia możesz usunąć szkodliwe pliki, których nie można usunąć przez ręczne skanowanie.

1.2.3 Uprawnienia aplikacji

Na tej stronie widoczne są wszystkie aplikacje monitorowane przez funkcję DeepGuard.

Informacje: Aby otworzyć tę stronę, musisz mieć prawa administratora.

1.2.4 Kwarantanna

Kwarantanna to bezpieczne repozytorium dla plików, które mogą być szkodliwe. Pliki poddane kwarantannie można przywrócić lub, jeśli użytkownik tak zdecyduje, usunąć.

Informacje: Aby otworzyć tę stronę, musisz mieć prawa administratora.

1.2.5 Ustawienia Zapory systemu Windows

To narzędzie otwiera stronę ustawień zapory systemu Windows, na której możesz edytować ustawienia zapory systemu Windows.

1.2.6 Sprawdź dostępność aktualizacji

Za pomocą tego narzędzia możesz ręcznie sprawdzić dostępność najnowszych aktualizacji.

Zwykle produkt automatycznie sprawdza dostępność aktualizacji kilka razy dziennie. Możesz jednak zrobić to ręcznie, aby sprawdzić, czy od ostatniego sprawdzenia automatycznego nie pojawiła się nowsza aktualizacja.

1.2.7 Wyłącz wszystkie funkcje zabezpieczeń

Możesz wyłączyć wszystkie funkcje zabezpieczeń, takie jak skanowanie w poszukiwaniu wirusów, jeśli chcesz zwolnić zasoby systemowe. Te funkcje zostaną włączone po następnym uruchomieniu programu lub ponownym uruchomieniu komputera.

Informacje: Do wyłączenia funkcji zabezpieczeń wymagane są uprawnienia administratora.

Informacje: Po wyłączeniu funkcji zabezpieczeń komputer nie jest w pełni chroniony.

1.3 Jak wyświetlić działania podjęte przez produkt

Strona **Statystyka** umożliwia wyświetlanie historii działań produktu.

1.3.1 Wyświetlanie statystyki produktu

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

Aby otworzyć stronę **Statystyka**:

Kliknij opcję **Statystyka**.

Na stronie **Statystyka** są wyświetlane następujące informacje:

- **Skanowanie w poszukiwaniu wirusów** zawiera informacje o liczbach plików przeskanowanych i oczyszczonych przez produkt od momentu zainstalowania.
- **Aplikacje** wskazuje liczbę programów, którym technologia DeepGuard umożliwiła działanie lub które zablokowała od momentu zainstalowania produktu.

1.3.2 Wyświetl oś czasu produktu

Zobacz listę czynności wykonanych przez produkt w celu ochrony komputera lub urządzenia.

Aby wyświetlić stronę osi czasu produktu:

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu.
   Zostanie wyświetlone menu podręczne.
2. Wybierz pozycję **Otwórz oś czasu produktu**
   Zostanie wyświetlona strona osi czasu produktu.

1.4 Jak zmienić ustawienia zabezpieczeń

Na stronie **Ustawienia** możesz dostosować działanie produktu.

Możesz zmienić ustawienia ochrony antywirusowej, zapory, filtrowania spamu oraz ręcznego i planowanego skanowania.

Informacje: Aby otworzyć tę stronę, musisz mieć prawa administratora.

1.4.1 Otwieranie ustawień

Edytując ustawienia zaawansowane, można zmienić sposób działania produktu.

Aby otworzyć ustawienia zaawansowane:

Na stronie Stan kliknij opcję **Ustawienia**.

Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

Zostanie wyświetlone okno **Ustawienia**.

W okienku z lewej strony są wyświetlane składniki produktu pogrupowane według funkcji. W prawym okienku można zmieniać ustawienia.

Szybki dostęp do ustawień produktu

Tematy:

Na komputerze dostęp do wielu ustawień produktu można wygodnie uzyskać z menu kontekstowego ikony na pasku zadań, która jest dostępna podczas działania produktu.

Menu kontekstowe obejmuje następujące pozycje:

- Łącze do internetowego Portalu Abonenta TOYA
- Ustawienia subskrypcji, gdzie możesz sprawdzić informacje o subskrypcji oraz identyfikator konta
- Tryb gier, za pomocą którego można uwolnić zasoby systemowe
- Centrum akcji, gdzie są wyświetlane ważne powiadomienia dotyczące spraw wymagających uwagi użytkownika.
- Oś czasu produktu, gdzie możesz zobaczyć listę czynności wykonanych przez produkt w celu ochrony komputera
- Typowe ustawienia, gdzie możesz zobaczyć najnowsze pobrane aktualizacje i zmienić ustawienia połączeń i prywatności
- Sprawdzanie dostępności aktualizacji, gdzie możesz ręcznie pobrać najnowsze aktualizacje, jeśli są dostępne

2.1 Tryb gier

Włączając *tryb gier*, możesz zwolnić niektóre zasoby systemowe, aby zwiększyć wydajność gier komputerowych.

Gry komputerowe często potrzebują dużo zasobów systemowych do płynnego działania. Jeśli podczas gry na komputerze są uruchomione inne aplikacje działające w tle i zużywające zasoby systemowe oraz korzystające z sieci, może to obniżać wydajność gry.

W *trybie gier* produkt ogranicza swój wpływ na działanie komputera i zmniejsza użycie sieci. Dzięki temu zwalnia niektóre zasoby systemowe dla gier, jednocześnie zapewniając podstawowe funkcje zabezpieczające. W trybie gier wstrzymywane są na przykład aktualizacje automatyczne, zaplanowane skanowania i inne operacje, które potrzebują dużo zasobów systemowych lub przepustowości sieci.

Gdy korzystasz z dowolnej aplikacji pełnoekranowej, na przykład podczas wyświetlania prezentacji, pokazu slajdów lub filmu albo grania w grę w trybie pełnoekranowym, pokazywane są tylko krytyczne powiadomienia, które wymagają natychmiastowej reakcji. Inne powiadomienia są wyświetlane dopiero po wyjściu z trybu pełnoekranowego lub wyłączeniu *trybu gier*.

2.1.1 Włącz tryb gier

Włącz *tryb gier*, aby zwiększyć wydajność gier na komputerze.

Aby włączyć *tryb gier*:

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu.
   Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Tryb gier**.
   Użycie zasobów systemowych przez produkt jest teraz zoptymalizowane, aby gry działały płynnie na komputerze.

Pamiętaj o wyłączeniu *trybu gier* po zakończeniu grania. *Tryb gier* jest automatycznie wyłączany po ponownym uruchomieniu komputera lub wybudzeniu go z uśpienia.

2.2 Jak korzystać z centrum akcji

W centrum akcji są wyświetlane ważne powiadomienia dotyczące spraw wymagających uwagi użytkownika.

Jeśli w centrum akcji występują jakieś oczekujące akcje, centrum powiadamia o tym okresowo.

2.2.1 Otwieranie centrum akcji

Aby wyświetlić wszystkie powiadomienia wymagające uwagi, otwórz centrum akcji.

Aby otworzyć centrum akcji, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu.
   Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz centrum akcji**.
   W centrum akcji wyświetlana jest lista pozycji wymagających uwagi.
3. Kliknij pozycję na liście, aby wyświetlić więcej informacji na jej temat.
4. Jeśli na razie nie chcesz nic robić z powiadomieniem, kliknij przycisk **Odłóż**, aby zająć się nim później.

Wskazówka: Jeśli chcesz zamknąć centrum akcji i rozwiązać problemy później, kliknij opcję **Odłóż wszystko**.

2.2.2 Instalowanie uaktualnienia produktu

Jeśli do zainstalowanego produktu zostanie udostępnione bezpłatne uaktualnienie, możesz je zainstalować i korzystać w nowej wersji.

Aby uaktualnić produkt, wykonaj następujące czynności:

1. Otwórz centrum akcji.
   W centrum akcji jest wyświetlana pozycja **Uaktualnienie produktu jest dostępne**. Jeśli centrum akcji zawiera kilka pozycji, kliknij pozycję, aby ją otworzyć.
2. Kliknij przycisk **Uaktualnij**.

   Informacje: Jeśli warunki licencji uległy zmianie, musisz zaakceptować nowe warunki, aby uaktualnić produkt.

Po ukończeniu uaktualnienia konieczne może być ponowne uruchomienie komputera.

2.2.3 Instalowanie nowego produktu

Jeśli do Twojej subskrypcji zostanie dodany nowy produkt, możesz go zainstalować i z niego korzystać.

Nowe produkty mogą być dodawane do subskrypcji w okresie jej ważności.

Aby zainstalować nowy produkt, wykonaj następujące czynności:

1. Otwórz centrum akcji.
   W centrum akcji jest wyświetlana pozycja **Zainstaluj nowy produkt**. Jeśli centrum akcji zawiera kilka pozycji, kliknij pozycję, aby ją otworzyć.
2. Kliknij przycisk **Zainstaluj**.

   Informacje: Jeśli nie chcesz instalować produktu, możesz kliknąć ikonę kosza w prawym górnym rogu, aby zamknąć przypomnienie i usunąć je z centrum akcji.

3. Wykonaj instrukcje kreatora, aby zainstalować produkt.

Po ukończeniu instalacji konieczne może być ponowne uruchomienie komputera.

2.2.4 Zastąp wygasający produkt

Jeśli ważność Twojej subskrypcji wygasa i aktualnie zainstalowany produkt nie jest już dostępny, nie możesz kontynuować swojej subskrypcji, ale możesz bezpłatnie uaktualnić ją do nowego produktu.

Aby uaktualnić produkt, wykonaj następujące czynności:

1. Otwórz centrum akcji.
   W centrum akcji jest wyświetlana pozycja **Uaktualnij produkt**. Jeśli centrum akcji zawiera kilka pozycji, kliknij pozycję, aby ją otworzyć.
2. Kliknij przycisk **Uaktualnij**.

Po ukończeniu uaktualnienia konieczne może być ponowne uruchomienie komputera.

2.2.5 Co to są powiadomienia

Powiadomienia to niewielkie komunikaty wyświetlane w prawym dolnym rogu ekranu komputera.

Powiadomienia informują o czynnościach wykonywanych przez produkt w celu zapewnienia ochrony komputera. Produkt wyświetla informacje za pomocą powiadomień na przykład wtedy, gdy uniemożliwi uruchomienie potencjalnie szkodliwego programu. Te powiadomienia mają na celu informowanie użytkownika i nie wymagają podejmowania jakichkolwiek działań.

2.3 Zmienianie typowych ustawień produktu

W tej sekcji opisano sposób zmieniania typowych ustawień produktu.

Ustawienia obejmują następujące opcje:

- Pobrane pliki udostępniające informacje o pobranych aktualizacjach i umożliwiające ręczne sprawdzanie dostępności aktualizacji.
- Ustawienia połączeń służące do zmieniania sposobu nawiązywania połączenia internetowego przez komputer.
- Ustawienia prywatności, gdzie możesz zdecydować się na korzystanie z usługi Security Cloud.

2.3.1 Otwórz typowe ustawienia

Edytując typowe ustawienia, można zmienić sposób działania produktu.

Aby otworzyć stronę typowych ustawień:

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu.
   Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
   Zostanie wyświetlona strona **Typowe ustawienia**.

2.3.2 Sprawdź dostępność aktualizacji

Możliwe jest wyświetlenie daty i godziny ostatniej aktualizacji.

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

Aby sprawdzić dostępność aktualizacji dla zainstalowanych produktów:

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu.
   Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
   Zostanie wyświetlona strona **Typowe ustawienia**.
3. Wybierz opcję **Pobrane pliki**.
   Zostaną wyświetlone informacje o ostatnio pobranych aktualizacjach do produktów.
4. Aby ręcznie sprawdzić dostępność aktualizacji, wybierz opcję **Sprawdź teraz**.
   Produkt sprawdzi, czy są dostępne nowsze aktualizacje.

   Informacje: Aby móc sprawdzić dostępność aktualizacji, połączenie internetowe musi być aktywne.

2.3.3 Zmień ustawienia połączenia

Instrukcje dotyczące wybierania, jak Twój komputer łączy się z Internetem i jak traktować aktualizacje podczas korzystania z sieci komórkowej.

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu.
   Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Otwórz typowe ustawienia**.
3. Wybierz pozycję **Połączenie**.
4. Za pomocą listy Serwer proxy HTTP określ, czy komputer korzysta z serwera proxy do nawiązywania połączenia z Internetem.
   - Wybierz opcję **Nie używaj**, jeśli komputer jest połączony z Internetem bezpośrednio
   - Wybierz opcję **Użyj ustawień przeglądarki**, aby zastosować ustawienia serwera proxy HTTP skonfigurowane w przeglądarce internetowej.
   - Wybierz opcję **Ustawienia niestandardowe**, aby ręcznie skonfigurować ustawienia serwera proxy HTTP
5. Na liście Komórkowa transmisja danych wybierz preferowaną opcję aktualizacji dla połączeń na urządzeniu przenośnym
   - Wybierz opcję **Nigdy**, jeśli nie chcesz, aby aktualizacje były pobierane podczas używania szerokopasmowego połączenia na urządzeniu przenośnym
   - Wybierz opcję **Tylko w sieci mojego operatora**, jeśli chcesz, aby aktualizacje były zawsze pobierane, gdy urządzenie znajduje się w zasięgu sieci głównego operatora. Jeśli natomiast sieć głównego operatora jest niedostępna, aktualizacje zostają wstrzymane. Wybranie tej opcji jest zalecane. Pozwala to utrzymywać aktualny stan produktu zabezpieczającego bez nieoczekiwanych kosztów.

- Wybierz opcję **Zawsze**, jeśli chcesz, aby aktualizacje były zawsze pobierane, niezależnie od używanej sieci. Wybierając tę opcję, można upewnić się, że zabezpieczenia komputera są zawsze aktualne, bez względu na koszty.

  Informacje: Aby decydować oddzielnie za każdym razem, gdy nawiązywane jest połączenie z inną siecią, wybierz opcję **Zapytaj przed skorzystaniem z roamingu w innej sieci**.

2.4 Sprawdź dostępność aktualizacji

Ręcznie sprawdź dostępność najnowszych aktualizacji.

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

Aby upewnić się, że najnowsze aktualizacje zostały zainstalowane:

1. Kliknij prawym przyciskiem myszy ikonę produktu na pasku zadań systemu.
   Zostanie wyświetlone menu podręczne.
2. Wybierz opcję **Sprawdź dostępność aktualizacji**.
   Produkt nawiąże połączenie z Internetem i sprawdzi dostępność najnowszych aktualizacji. Jeśli ochrona nie jest aktualna, zostaną pobrane najnowsze aktualizacje.
3. Kliknij przycisk **Zamknij**.

Skanowanie komputera w poszukiwaniu szkodliwych plików

Tematy:

Ochrona antywirusowa chroni komputer przed programami, które mogą wykraść przechowywane na nim informacje osobiste, uszkodzić go lub użyć w niedozwolonych celach.

Domyślnie produkt zajmuje się szkodliwymi plikami natychmiast po ich wykryciu, aby nie wyrządziły żadnych szkód.

Domyślnie produkt automatycznie skanuje lokalne dyski twarde, nośniki wymienne, takie jak pamięci przenośne i dyski DVD, oraz pobieraną zawartość.

Dodatkowo możesz włączyć w produkcie automatyczne skanowanie poczty e-mail.

Produkt obserwuje też działanie komputera w poszukiwaniu zmian sugerujących obecność szkodliwych plików. Gdy produkt wykryje niebezpieczne zmiany w systemie, na przykład zmiany ustawień systemowych lub próby zmiany ważnych procesów systemowych, składnik DeepGuard zatrzyma aplikację, aby nie wyrządziła szkód.

3.1 Jak przeskanować komputer

Jeśli ochrona antywirusowa jest włączona, automatycznie wyszukuje szkodliwe pliki na komputerze.

Zalecamy, aby ochrona przed wirusami była włączona przez cały czas. Możesz też skanować pliki ręcznie i konfigurować zaplanowane operacje skanowania, aby upewnić się, że na komputerze nie ma szkodliwych plików, albo skanować pliki wyłączone ze skanowania w czasie rzeczywistym. Skonfiguruj zaplanowane skanowanie, aby skanować komputer regularnie (codziennie lub co tydzień).

3.1.1 Automatyczne skanowanie plików

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

Gdy komputer uzyskuje dostęp do pliku, funkcja skanowania w czasie rzeczywistym analizuje ten plik pod kątem obecności złośliwego oprogramowania, zanim zezwoli komputerowi na dostęp.

Jeśli skanowanie w czasie rzeczywistym wykryje szkodliwą zawartość, zainfekowany plik zostanie umieszczony w kwarantannie, zanim będzie mógł wyrządzić jakiekolwiek szkody.

Czy skanowanie w czasie rzeczywistym ma wpływ na wydajność komputera?

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

Pliki, których skanowanie trwa dłużej:

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

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

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

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

Włączanie lub wyłączanie skanowania w czasie rzeczywistym

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

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

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

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

2. Włączanie i wyłączanie **Ochrony antywirusowej**.
3. Kliknij przycisk **OK**.

Automatyczne przetwarzanie szkodliwych plików

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

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

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

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

2. Wybierz pozycję **Ochrona antywirusowa**.

3. Wybierz opcję **Przetwarzaj szkodliwe pliki automatycznie**.

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

Przetwarzanie oprogramowania szpiegującego

Ochrona antywirusowa natychmiast blokuje oprogramowanie szpiegujące przy próbie uruchomienia.

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

Po wykryciu oprogramowania szpiegującego należy wybrać jedną z następujących czynności:

Czynność do wykonania	Co dzieje się z oprogramowaniem szpiegującym
Przetwórz automatycznie	Pozwól programowi wybrać najlepsze działanie w zależności od wykrytego oprogramowania szpiegującego.
Poddaj aplikację kwarantannie	Przenieś potencjalnie niechcianą aplikację do kwarantanny, skąd nie może uszkodzić komputera.
Usuń aplikację	Trwale usuń aplikację z komputera.
Tymczasowo zablokuj aplikację	Zablokuj dostęp do aplikacji, ale pozostaw ją na komputerze.
Nie blokuj aplikacji	Zezwól na uruchomienie aplikacji i wyklucz ją ze skanowania w przyszłości.

Obsługa potencjalnie niechcianych aplikacji

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

Po wykryciu potencjalnie niechcianej aplikacji należy wybrać jedną z następujących czynności:

Czynność do wykonania	Co dzieje się z aplikacją
Poddaj aplikację kwarantannie	Przenieś potencjalnie niechcianą aplikację do kwarantanny, skąd nie może uszkodzić komputera.
Usuń aplikację	Trwale usuń aplikację z komputera.
Tymczasowo zablokuj aplikację	Zablokuj dostęp do aplikacji, ale pozostaw ją na komputerze.
Nie blokuj aplikacji	Zezwól na uruchomienie aplikacji i wyklucz ją ze skanowania w przyszłości.

3.1.2 Ręczne skanowanie plików

Możesz przeskanować cały komputer, aby upewnić się, że nie zawiera szkodliwych plików ani niechcianych aplikacji.

Pełne skanowanie komputera sprawdza wszystkie wewnętrzne i zewnętrzne dyski twarde w poszukiwaniu wirusów, oprogramowania szpiegującego i potencjalnie niechcianych aplikacji. Ta funkcja przeprowadza również sprawdzanie pod kątem plików ukrytych przez programy typu „rootkit”. Pełne skanowanie komputera może potrwać dłuższy czas. Możesz też przeskanować tylko obszary systemu zawierające zainstalowane aplikacje, aby bardziej wydajnie znaleźć i usunąć niechciane aplikacje i szkodliwe elementy z komputera.

Skanowanie plików i folderów

Jeśli określone pliki na komputerze budzą podejrzenia, można przeskanować tylko te pliki lub foldery. Takie skanowanie będzie trwać znacznie krócej niż skanowanie całego komputera. Na przykład po podłączeniu do komputera zewnętrznego dysku twardego lub pamięci USB możesz je przeskanować, aby upewnić się, że nie zawierają szkodliwych plików.

Przeprowadzanie skanowania ręcznego

Możesz przeskanować cały komputer lub przeprowadzić bardziej wydajne skanowanie w poszukiwaniu wirusów, które sprawdza określone obszary systemu bardziej narażone na szkodliwe pliki i niechciane aplikacje.

Aby przeskanować komputer:

1. Wybierz typ skanowania, które chcesz uruchomić.
   - Jeśli chcesz szybko przeskanować komputer, kliknij opcję **Skanuj w poszukiwaniu wirusów** na stronie **Stan**.
   - Aby w pełni przeskanować komputer, wybierz kolejno opcje **Narzędzia** > **Opcje skanowania w poszukiwaniu wirusów** > **Pełne skanowanie komputera**.

   Informacje: Wybierz kolejno opcje **Narzędzia** > **Opcje skanowania w poszukiwaniu wirusów** > **Zmień ustawienia skanowania**, aby zoptymalizować sposób ręcznego skanowania komputera w poszukiwaniu wirusów i innych szkodliwych aplikacji.

   Rozpocznie się skanowanie ręczne.
2. Jeśli skanowanie ręczne wykryje szkodliwe elementy, wyświetli ich listę.
3. Kliknij wykryty szkodliwy element, aby wybrać, co z nim zrobić.

Opcja	Opis
Wyczyść	Wyczyść pliki automatycznie. Pliki, których nie można wyczyścić, zostaną umieszczone w kwarantannie.
Kwarantanna	Umieść pliki w bezpiecznym miejscu, gdzie nie mogą się rozprzestrzeniać, ani uszkodzić komputera.
Usuń	Trwale usuń pliki z komputera.
Pomiń	Nic nie rób i pozostaw pliki na komputerze.
Wyklucz	Zezwól na uruchomienie aplikacji i wyklucz ją ze skanowania w przyszłości.

   Informacje: Niektóre opcje są niedostępne w przypadku pewnych typów szkodliwych elementów.

4. Kliknij opcję **Przetwórz wszystkie**, aby uruchomić proces czyszczenia.
5. Skanowanie ręczne wyświetla wyniki obejmujące liczbę szkodliwych elementów, które zostały wyczyszczone.

   Informacje: Skanowanie ręczne może wymagać ponownego uruchomienia komputera w celu ukończenia procesu czyszczenia. Jeśli tak jest, kliknij opcję **Uruchom ponownie**.

W niektórych przypadkach skanowanie ręczne nie może usunąć wykrytego szkodliwego elementu. Aby usunąć takie elementy, użyj *Narzędzia do czyszczenia*.

Typy skanowania

Skanowanie może obejmować cały komputer lub dotyczyć tylko określonego typu złośliwego oprogramowania albo określonej lokalizacji.
Poniżej wymieniono różne typy skanowania:

Typ skanowania	Skanowane elementy	Zalecane użycie
Skanowanie w poszukiwaniu wirusów i oprogramowania szpiegującego	Określone obszary komputera w poszukiwaniu wirusów, oprogramowania szpiegującego i potencjalnie niechcianych aplikacji	Skanowanie tego typu jest dużo szybsze niż pełne skanowanie. Przeszukiwane są tylko obszary systemu zawierające zainstalowane pliki programów. Skanowanie tego typu jest zalecane, gdy trzeba szybko sprawdzić, czy komputer nie jest zainfekowany, ponieważ umożliwia ono wydajne wyszukiwanie i usuwanie wszelkiego aktywnego

Typ skanowania	Skanowane elementy	Zalecane użycie
		złośliwego oprogramowania znajdującego się na komputerze.
Pełne skanowanie komputera	Cały komputer (wewnętrzne i zewnętrzne dyski twarde) w poszukiwaniu wirusów, oprogramowania szpiegującego i potencjalnie niechcianych aplikacji	W celu uzyskania całkowitej pewności, że na komputerze nie ma szkodliwego oprogramowania ani niechcianych aplikacji. Skanowanie tego typu zajmuje najwięcej czasu. Stanowi połączenie funkcji szybkiego skanowania w poszukiwaniu złośliwego oprogramowania i funkcji skanowania dysku twardego. Ta funkcja przeprowadza również sprawdzanie pod kątem plików ukrytych przez programy typu „rootkit”.
Wybierz elementy do przeskanowania	Określony folder lub dysk w poszukiwaniu wirusów, oprogramowania szpiegującego i potencjalnie niechcianych aplikacji	Użyj tej opcji skanowania, jeśli podejrzewasz, że określona lokalizacja na komputerze zawiera szkodliwe pliki — na przykład pliki pobrane z potencjalnie niebezpiecznych źródeł, takich jak sieci udostępniania plików typu „peer-to-peer”. Skanowanie może trwać krótko lub długo w zależności od rozmiaru i liczby skanowanych plików. Jeśli na przykład przeskanujesz folder, który zawiera tylko kilka małych plików, skanowanie zostanie szybko ukończone.

Skanowanie w Eksploratorze Windows

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

Aby przeskanować dysk, folder lub plik:

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

Kreator skanowania przeprowadzi użytkownika przez proces oczyszczania, jeśli wykryje podejrzane elementy podczas skanowania.

Wybieranie plików do skanowania

Możesz wybrać typy plików, które mają być skanowane w poszukiwaniu *wirusów* i innych szkodliwych elementów podczas skanowania ręcznego i zaplanowanego.

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Skanowanie ręczne**.
3. W obszarze **Opcje skanowania** określ następujące ustawienia:

Skanuj tylko znane typy plików — Skanowanie tylko plików, w przypadku których istnieje największe prawdopodobieństwo infekcji, na przykład plików wykonywalnych. Wybranie tej opcji zapewnia szybsze skanowanie. Takie skanowanie obejmuje pliki z następującymi rozszerzeniami: `ani, asp, ax, bat, bin, boo, chm, cmd, com, cpl, dll, doc, dot, drv, eml, exe, hlp, hta, htm, html, htt, inf, ini, job, js, jse, lnk, lsp, mdb, mht, mpp, mpt, msg, ocx, pdf, php, pif, pot, ppt, rtf, scr, shs, swf, sys, td0, vbe, vbs, vxd, wbk, wma, wmv, wmf, wsc, wsf, wsh, wri, xls, xlt, xml, zip, jar, arj, lzh, tar, tgz, gz, cab, rar, bz2, hqx`.

Skanuj wewnątrz plików skompresowanych	Skanowanie zarchiwizowanych plików i folderów.
Użyj zaawansowanej heurystyki	Podczas skanowania zostaną użyte wszystkie dostępne zasoby heurystyki w celu skuteczniejszego wykrywania nowego i nieznanego złośliwego oprogramowania. **Informacje:** Zaznaczenie tej opcji wydłuża czas skanowania i może powodować zwiększenie liczby zgłoszeń programów niepoprawnie uznanych za niebezpieczne (nieszkodliwych plików zgłoszonych jako podejrzane).

4. Kliknij przycisk **OK**.

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

Co zrobić w przypadku wykrycia szkodliwych plików

Sposób postępowania z wykrytymi szkodliwymi plikami można wybrać.

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

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Skanowanie ręczne**.
3. W sekcji **W przypadku wykrycia szkodliwego elementu** wybierz jedną z tych opcji:

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

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

Planowanie skanowania

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

Aby zaplanować skanowanie:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Skanowanie zaplanowane**.
3. Włącz opcję **Skanowanie zaplanowane**.
4. Wybierz pozycję **Skanowanie zaplanowane**.
5. Wybierz czas rozpoczęcia skanowania.

Opcja	Opis
Codziennie	Komputer będzie skanowany codziennie.
Co tydzień	Komputer będzie skanowany w wybrane dni tygodnia. Wybierz dni z listy.
Co miesiąc	Komputer będzie skanowany w wybrane dni miesiąca. Aby wybrać dni: 1. Wybierz jedną z opcji w polu **Dzień**. 2. Wybierz dzień miesiąca z listy znajdującej się obok wybranego dnia.

6. Określ czas rozpoczęcia skanowania w wybrane dni.

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

7. Kliknij przycisk **Zastosuj**.

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

Informacje: Zaplanowane skanowanie jest wstrzymywane, gdy *tryb gier* jest włączony. Po wyłączeniu tego trybu wstrzymane skanowanie jest automatycznie kontynuowane.

3.1.3 Skanowanie poczty e-mail

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

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

Aby włączyć skanowanie poczty e-mail:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Ochrona antywirusowa**.
3. Wybierz opcję **Usuń szkodliwe załączniki wiadomości e-mail**.
4. Kliknij przycisk **OK**.

Kiedy są skanowane wiadomości e-mail i załączniki?

Ochrona antywirusowa usuwa szkodliwe obiekty z otrzymywanych wiadomości e-mail.

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

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

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

3.1.4 Sprawdzanie czynności wykonanych przez produkt

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

Czasami po wykryciu szkodliwego obiektu produkt nie może wykonać akcji wybranej przez użytkownika. Jeśli na przykład zostanie wybrana opcja wyczyszczenia plików, a plików nie można wyczyścić, produkt przeniesie je do kwarantanny. Tę informację można wyświetlić w historii wydarzeń.

Aby wyświetlić historię wydarzeń, wybierz opcje **Narzędzia** > **Ostatnie wydarzenia**.

W historii wydarzeń wyświetlane są następujące informacje na temat szkodliwych plików:

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

3.1.5 Używanie narzędzia do czyszczenia

Za pomocą narzędzia do czyszczenia możesz usunąć szkodliwe pliki, których nie można usunąć przez ręczne skanowanie.

Informacje: Ta funkcja jest niedostępna w niektórych wersjach produktu.

Narzędzie do czyszczenia wymaga połączenia z Internetem.

Aby uruchomić narzędzie do czyszczenia:

1. Na stronie **Narzędzia** wybierz kolejno opcje **Opcje skanowania w poszukiwaniu wirusów** > **Narzędzie do czyszczenia**.
2. Produkt sprawdza i pobiera najnowszą wersję narzędzia do czyszczenia z Internetu.
   Narzędzie do czyszczenia jest uruchamiane automatycznie po zaktualizowaniu do najnowszej wersji.
3. W oknie narzędzia do czyszczenia kliknij opcję **Rozpocznij skanowanie**, aby przeskanować komputer.
   - Jeśli zostanie wyświetlona umowa licencyjna, przeczytaj ją i kliknij **Akceptuję**, aby kontynuować.

   Narzędzie do czyszczenia skanuje komputer i usuwa znalezione szkodliwe pliki. Jeśli to konieczne, narzędzie do czyszczenia ponownie uruchomi komputer, aby usunąć szkodliwe pliki.

3.1.6 Jak wykluczyć pliki ze skanowania

Czasami trzeba wykluczyć niektóre pliki lub aplikacje ze skanowania. Wykluczone elementy nie są skanowane, dopóki nie zostaną usnięte z listy wykluczonych elementów.

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

Wykluczanie typów plików

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

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

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz, czy chcesz wykluczyć typ pliku ze skanowania w czasie rzeczywistym, czy skanowania ręcznego:
   - Aby wykluczyć typ plików ze skanowania w czasie rzeczywistym, wybierz opcję **Ochrona antywirusowa**.
   - Aby wykluczyć typ plików ze skanowania ręcznego, wybierz opcję **Skanowanie ręczne**.
3. Kliknij łącze **Wyklucz pliki ze skanowania**.
   Zostanie otwarta strona **Wykluczanie ze skanowania**
4. Aby wykluczyć typ pliku:
   a) Wybierz kartę **Typy plików**.
   b) Wybierz opcję **Wyklucz pliki z tymi rozszerzeniami**.
   c) W polu obok przycisku **Dodaj** wpisz rozszerzenie pliku określające typ plików, które chcesz wykluczyć.

      Aby uwzględnić pliki, które nie mają rozszerzenia, należy użyć znaku „.”. Można też zastosować symbol wieloznaczny „?” reprezentujący dowolny znak lub „*” reprezentujący dowolną liczbę znaków.

      Aby na przykład wykluczyć pliki wykonywalne, wpisz w tym polu wartość `exe`.
   d) Kliknij przycisk **Dodaj**.
5. Powtórz poprzedni krok dla każdego rozszerzenia, które ma zostać wykluczone ze skanowania w poszukiwaniu wirusów.
6. Kliknij przycisk **OK**, aby zastosować nowe ustawienia i zamknąć okno **Wykluczanie ze skanowania**.

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

Wykluczanie plików według lokalizacji

Po wykluczeniu plików według lokalizacji pliki znajdujące się na określonych dyskach lub w określonych folderach nie są skanowane w poszukiwaniu szkodliwej zawartości.

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

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz, czy chcesz wykluczyć lokalizację ze skanowania w czasie rzeczywistym, czy skanowania ręcznego:
   - Aby wykluczyć lokalizację ze skanowania w czasie rzeczywistym, wybierz opcję **Ochrona antywirusowa**.
   - Aby wykluczyć lokalizację ze skanowania ręcznego, wybierz opcję **Skanowanie ręczne**.
3. Kliknij opcję **Wyklucz pliki ze skanowania**.
4. Aby wykluczyć plik, dysk lub folder:
   a) Wybierz kartę **Obiekty**.
   b) Wybierz opcję **Wyklucz obiekty (pliki, foldery itd.)**.
   c) Kliknij przycisk **Dodaj**.
   d) Wybierz plik, folder lub dysk, który chcesz wykluczyć ze skanowania antywirusowego.

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

e) Kliknij przycisk **OK**.

5. Powtórz poprzedni krok w celu wykluczenia innych plików, folderów lub dysków ze skanowania antywirusowego.
6. Kliknij przycisk **OK**, aby zamknąć okno dialogowe **Wykluczanie ze skanowania**.
7. Kliknij przycisk **OK**, aby zastosować nowe ustawienia.

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

Wyświetlanie aplikacji wykluczonych

Aplikacje wykluczone ze skanowania można wyświetlać i usuwać z listy elementów wykluczonych, aby w przyszłości były uwzględniane podczas skanowania.

Jeśli produkt wykryje potencjalnie niechcianą aplikację, ale wiesz, że jest ona bezpieczna, lub jest to oprogramowanie szpiegujące niezbędne do używania innej aplikacji, możesz wykluczyć ją ze skanowania, aby produkt nie wyświetlał więcej ostrzeżeń dotyczących tej aplikacji.

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

Aby wyświetlić aplikacje wykluczone ze skanowania:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz, czy chcesz wyświetlić aplikacje wykluczone ze skanowania w czasie rzeczywistym, czy ze skanowania ręcznego:
   - Aby wyświetlić aplikacje wykluczone ze skanowania w czasie rzeczywistym, wybierz opcję **Ochrona antywirusowa**.
   - Aby wyświetlić aplikacje wykluczone ze skanowania ręcznego, wybierz opcję **Skanowanie ręczne**.
3. Kliknij opcję **Wyklucz pliki ze skanowania**.
   Zostanie otwarta strona **Wykluczanie ze skanowania**
4. Wybierz kartę **Aplikacje**.
5. Aby ponownie przeskanować wykluczone aplikacje, wykonaj następujące czynności:
   a) Wybierz aplikację, którą chcesz uwzględnić podczas skanowania.
   b) Kliknij przycisk **Usuń**.
6. Kliknij przycisk **OK**, aby zamknąć okno dialogowe **Wykluczanie ze skanowania**.
7. Kliknij przycisk **OK**, aby zamknąć okno.

Nowe aplikacje pojawiają się na liście wykluczeń dopiero po dodaniu ich podczas skanowania i nie można dodać ich bezpośrednio do listy wykluczeń.

3.1.7 Jak korzystać z funkcji kwarantanny?

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

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

Kwarantannie można poddać szkodliwe oprogramowanie oraz potencjalnie niechciane aplikacje w celu ich unieszkodliwienia. W razie potrzeby aplikacje i pliki można później przywrócić z kwarantanny.

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

- Zazwyczaj użytkownik może usuwać wirusy i inne szkodliwe oprogramowanie poddane kwarantannie.
- Zazwyczaj użytkownik może usuwać *oprogramowanie szpiegujące* poddane kwarantannie.

  Czasami *oprogramowanie szpiegujące* umieszczone w kwarantannie może być częścią innej aplikacji i *jego* usunięcie powoduje, że dana aplikacja nie działa poprawnie. Jeśli chcesz nadal korzystać z tej aplikacji, przywróć *oprogramowanie szpiegujące* z kwarantanny.

- Potencjalnie niechciane aplikacje mogą być szkodliwe dla komputera lub innych używanych aplikacji.

  Jeśli aplikacja została umyślnie zainstalowana i prawidłowo skonfigurowana, jest mniejsza szansa, że będzie ona szkodliwa. Jeśli aplikacja została zainstalowana bez wiedzy użytkownika, prawdopodobnie jest ona złośliwa i należy ją usunąć.

Wyświetlanie elementów poddanych kwarantannie

Na temat elementów poddanych kwarantannie można wyświetlać więcej informacji.

Aby wyświetlić szczegółowe informacje na temat elementów poddanych kwarantannie:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Ochrona antywirusowa**.
3. Na stronie **Narzędzia** wybierz opcję **Kwarantanna**.
   Na stronie **Kwarantanna** dostępne są informacje o łącznej liczbie elementów w kwarantannie.
4. Aby wyświetlić szczegółowe informacje na temat wybranego elementu poddanego kwarantannie, kliknij przycisk **Szczegóły**.
5. Aby wyświetlić dodatkowe informacje na temat elementu poddanego kwarantannie, kliknij ikonę obok tego elementu.

Przywracanie elementów poddanych kwarantannie

Potrzebne elementy można przywracać z kwarantanny.

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

Przywracanie elementów poddanych kwarantannie

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Ochrona antywirusowa**.
3. Kliknij opcję **Wyświetl kwarantannę**.
4. Zaznacz elementy w kwarantannie do przywrócenia.
5. Kliknij przycisk **Przywróć**.

Co to jest technologia DeepGuard?

Tematy:

Funkcja DeepGuard monitoruje aplikacje w celu wykrycia potencjalnie szkodliwych zmian w systemie.

Funkcja DeepGuard zapewnia, że używasz tylko bezpiecznych aplikacji. Bezpieczeństwo aplikacji jest weryfikowane na podstawie informacji z zaufanej usługi zewnętrznej. Jeśli nie można zweryfikować bezpieczeństwa aplikacji, funkcja DeepGuard zaczyna monitorować jej działanie.

Technologia DeepGuard blokuje nowe i dotychczas niewykryte *konie trojańskie*, *robaki*, *luki w oprogramowaniu* i inne szkodliwe aplikacje, które próbują wprowadzać zmiany na komputerze, a także uniemożliwia podejrzanym aplikacjom dostęp do Internetu.

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

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

4.1 Wybierz, co monitoruje funkcja DeepGuard

Funkcja DeepGuard monitoruje ważne ustawienia i pliki systemowe oraz próby wyłączenia ważnych aplikacji, takich jak ten produkt zabezpieczający.

Aby wybrać, co monitoruje funkcja DeepGuard:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz przełącznik w prawym górnym rogu, aby upewnić się, że funkcja **DeepGuard** jest włączona.
3. Wybierz ustawienia funkcji DeepGuard:

Ostrzegaj o podejrzanych działaniach	Pozostaw tę opcję włączoną, aby otrzymywać ostrzeżenia o podejrzanych działaniach aplikacji. Jeśli ją wyłączysz, funkcja DeepGuard przestanie monitorować podejrzane działania, co zmniejsza poziom zabezpieczeń.
Ostrzegaj o lukach w zabezpieczeniach aplikacji	Pozostaw tę opcję włączoną, aby otrzymywać ostrzeżenia o potencjalnych próbach wykorzystania luk w zabezpieczeniach. Jeśli ją wyłączysz, szkodliwe strony internetowe i dokumenty będą mogły wykorzystywać luki w zabezpieczeniach aplikacji, co zmniejsza poziom zabezpieczeń. Nie zalecamy wyłączania tej opcji.
Pytaj o pozwolenie na nawiązanie połączenia internetowego	Pozostaw tę opcję włączoną, aby otrzymywać powiadomienia od funkcji DeepGuard, gdy nieznane aplikacje próbują nawiązać połączenie z Internetem.
Użyj trybu zgodności (zmniejsza poziom zabezpieczeń)	W celu zapewnienia maksymalnej ochrony funkcja DeepGuard tymczasowo modyfikuje uruchomione programy. Niektóre programy sprawdzają, czy nie zostały uszkodzone lub zmodyfikowane, i mogą nie być zgodne z tą funkcją. Na przykład gry internetowe zawierające narzędzia zapobiegające oszukiwaniu po uruchomieniu stale sprawdzają, czy nie zostały w jakikolwiek sposób zmodyfikowane. W takich przypadkach można włączyć tryb zgodności.

4. Kliknij przycisk **OK**.

4.1.1 Zezwalanie na aplikacje zablokowane przez funkcję DeepGuard

Aplikacje akceptowane i blokowane przez funkcję DeepGuard można kontrolować.

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

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

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **DeepGuard**.
3. Kliknij pozycję **Zmień uprawnienia aplikacji**.
   Zostanie wyświetlona lista **Aplikacje monitorowane**.
4. Znajdź aplikację, na uruchomienie której chcesz zezwolić, i kliknij przycisk **Szczegóły**.

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

5. Wybierz opcję **Zezwalaj**.
6. Kliknij przycisk **OK**.

7. Kliknij przycisk **Zamknij**.

Funkcja DeepGuard umożliwi aplikacji ponowne wprowadzanie zmian w systemie.

4.2 Co robić w przypadku ostrzeżeń o podejrzanych działaniach

Funkcja DeepGuard blokuje monitorowane aplikacje, gdy wykonują podejrzane działania lub próbują nawiązać połączenie z Internetem.

Możesz zdecydować, czy pozwolić aplikacji na dalsze działanie na podstawie tego, co się stało.

4.2.1 Funkcja DeepGuard zablokowała szkodliwą aplikację

Funkcja DeepGuard wyświetla powiadomienie, gdy wykryje i zablokuje szkodliwą aplikację.

Po otwarciu powiadomienia:

Kliknij opcję **Szczegóły**, aby wyświetlić więcej informacji o danej aplikacji.
Szczegóły zawierają następujące dane:

- lokalizacja aplikacji,
- reputację aplikacji w chmurze zabezpieczeń,
- stopień powszechności aplikacji, a także
- nazwę wykrytego złośliwego oprogramowania.

Możesz przesłać próbkę aplikacji do analizy.

4.2.2 Funkcja DeepGuard zablokowała podejrzaną aplikację

Jeśli opcja **Ostrzegaj o podejrzanych działaniach** jest włączona w ustawieniach funkcji DeepGuard, otrzymasz powiadomienie, gdy zostanie wykryta aplikacja wykonująca podejrzane działania. Jeśli ta aplikacja jest zaufana, możesz zezwolić na jej działanie.

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

1. Kliknij opcję **Szczegóły**, aby wyświetlić więcej informacji o danej aplikacji.
   W sekcji szczegółów są wyświetlane następujące dane:
   - lokalizacja aplikacji,
   - reputacja aplikacji w chmurze zabezpieczeń,
   - stopień powszechności aplikacji, a także
   - nazwę złośliwego oprogramowania.
2. Wybierz, czy aplikacja zablokowana przez funkcję DeepGuard jest zaufana:
   - Wybierz opcję **Ta aplikacja jest zaufana — kontynuuj**, jeśli nie chcesz blokować aplikacji.

     Aplikacja jest prawdopodobnie bezpieczna, jeśli:
     - funkcja DeepGuard zablokowała tę aplikację w wyniku czynności wykonanej przez użytkownika,
     - użytkownik rozpoznaję aplikację,
     - aplikacja pochodzi z zaufanego źródła.
   - Wybierz opcję **Ta aplikacja nie jest zaufana. Zablokuj.**, jeśli aplikacja ma pozostać zablokowana.

     Aplikacja jest prawdopodobnie niebezpieczna, jeśli:
     - aplikacja nie jest powszechna,
     - aplikacja ma nieznaną reputację,
     - użytkownik nie zna aplikacji.

Możesz przesłać próbkę podejrzanej aplikacji do analizy.

4.2.3 Nieznana aplikacja próbuje nawiązać połączenie z Internetem

Jeśli opcja **Pytaj o pozwolenie na nawiązanie połączenia internetowego** jest włączona w ustawieniach funkcji DeepGuard, otrzymasz powiadomienie, gdy nieznana aplikacja spróbuje nawiązać połączenie z Internetem. Jeśli ta aplikacja jest zaufana, możesz zezwolić na jej działanie.

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

1. Kliknij opcję **Szczegóły**, aby wyświetlić więcej informacji o danej aplikacji.
   W sekcji szczegółów są wyświetlane następujące dane:
   - lokalizacja aplikacji,
   - reputację aplikacji w chmurze zabezpieczeń,
   - stopień powszechności aplikacji,
   - jakie działanie próbowała wykonać aplikacja, a także
   - z jakim adresem aplikacja próbowała się połączyć.
2. Wybierz, czy aplikacja zablokowana przez funkcję DeepGuard jest zaufana:
   - Wybierz opcję **Ta aplikacja jest zaufana — kontynuuj**, jeśli nie chcesz blokować aplikacji.

     Aplikacja jest prawdopodobnie bezpieczna, jeśli:
     - funkcja DeepGuard zablokowała tę aplikację w wyniku czynności wykonanej przez użytkownika,
     - użytkownik rozpoznaję aplikację,
     - aplikacja pochodzi z zaufanego źródła.
   - Wybierz opcję **Ta aplikacja nie jest zaufana — zablokuj ją.**, jeśli aplikacja ma pozostać zablokowana.

     Aplikacja jest prawdopodobnie niebezpieczna, jeśli:
     - aplikacja nie jest powszechna,
     - aplikacja ma nieznaną reputację,
     - użytkownik nie zna aplikacji.

Gdy *tryb gier* jest włączony, funkcja DeepGuard zezwala każdej nieznanej aplikacji na łączenie się z Internetem. Jednocześnie szkodliwe aplikacje próbujące nawiązać połączenie z Internetem są blokowane przez tę funkcję nawet w *trybie gier*.

Możesz przesłać próbkę podejrzanej aplikacji do analizy.

4.2.4 Funkcja DeepGuard wykryła możliwą lukę w zabezpieczeniach

Jeśli opcja **Ostrzegaj o lukach w zabezpieczeniach aplikacji** jest włączona w ustawieniach funkcji DeepGuard, otrzymasz powiadomienie, gdy zostanie wykryte podejrzane działanie aplikacji po otwarciu szkodliwej strony internetowej lub szkodliwego dokumentu.

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

1. Kliknij opcję **Szczegóły**, aby wyświetlić więcej informacji o danej aplikacji.
   W sekcji szczegółów są wyświetlane następujące dane:
   - nazwę złośliwego oprogramowania, a także
   - źródło luki w zabezpieczeniach (szkodliwa strona internetowa lub szkodliwy dokument), jeśli jest znane.
2. Wybierz, czy aplikacja zablokowana przez funkcję DeepGuard jest zaufana:
   - Wybierz opcję **Pozostaw aplikację uruchomioną (może to stanowić ryzyko dla urządzenia)**, jeśli nie chcesz zamykać aplikacji.

     Możesz chcieć zostawić aplikację otwartą, jeśli jej zamknięcie bez zapisania danych jest nie do zaakceptowania w tym momencie.

- Wybierz opcję **Zamknij aplikację, aby zapobiec próbie wykorzystania tej luki**, jeśli chcesz zamknąć aplikację i zapewnić bezpieczeństwo urządzenia.

  Zalecamy zamknięcie aplikacji w celu zapewnienia bezpieczeństwa urządzenia.

Jeśli źródło luki zostało zidentyfikowane, możesz przesłać próbkę do analizy.

4.3 Przesyłanie podejrzanych aplikacji do analizy

Możesz pomóc nam wzmocnić zabezpieczenia, przesyłając podejrzane aplikacje do analizy.

Gdy funkcja DeepGuard zablokuje aplikację, bo na przykład stanowi ona potencjalne zagrożenie dla bezpieczeństwa komputera lub aplikacja próbowała wykonać szkodliwą operację, możesz przesłać próbkę aplikacji do analizy.

Możesz to zrobić, jeśli wiesz, że aplikacja zablokowana przez funkcję DeepGuard jest bezpieczna, lub jeśli spodziewasz się, że może być szkodliwa.

Aby przesłać próbkę do analizy:

1. Gdy funkcja DeepGuard zablokuje aplikację, wybierz, czy chcesz aby pozostała zablokowana czy zezwolić na jej działanie.
2. Funkcja DeepGuard może zapytać, czy chcesz przesłać próbkę aplikacji do analizy. Kliknij **Prześlij**, aby przesłać próbkę.

   Informacje: Funkcja DeepGuard nie zawsze prosi o przesłanie próbki. Czasami mamy już informacje o zablokowanej aplikacji.

Blokowanie spamu

Tematy:

Przy użyciu funkcji filtrowania spamu można wykrywać wiadomości zawierające spam i phishing, a następnie usuwać je ze skrzynki odbiorczej.

Wiadomości zawierające *spam* i *phishing* często przesłaniają swoją liczbą pożądane wiadomości e-mail.

Wiadomość e-mail jest uznawana za *spam*, jeśli została wysłana w ramach dużego zbioru wiadomości o podobnej treści i bez uzyskania od Ciebie pozwolenia na wysyłkę.

Wiadomości stanowiące próbę *phishingu* mają na celu wykradzenie informacji osobistych. Te wyglądające autentycznie wiadomości są podobne do wiadomości wysyłanych przez prawdziwe firmy i mają oszukać użytkowników komputerów w celu wyłudzenia od nich informacji osobistych, takich jak numery kont, hasła, numery kart kredytowych oraz numery identyfikacyjne. Nie należy ufać zawartości żadnych wiadomości e-mail wykrytych przez funkcję filtrowania spamu i wiadomości typu phishing.

5.1 Włączanie i wyłączanie filtrowania spamu

Aby wiadomości zawierające spam i phishing były usuwane ze skrzynki odbiorczej, funkcja filtrowania spamu powinna być stale włączona.

Aby włączyć lub wyłączyć filtrowanie spamu, wykonaj następujące czynności:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Włącz lub wyłącz opcję **Filtrowanie spamu**.
3. Kliknij przycisk **OK**.

Wskazówka: Utworzenie reguły filtrowania spamu w programie do obsługi poczty e-mail umożliwia automatyczne przenoszenie masowo wysyłanych reklam i oszukańczych wiadomości e-mail do folderu spamu.

5.2 Oznaczanie spamu etykietą

Funkcja filtrowania spamu umożliwia oznaczanie etykietą pola tematu wiadomości zawierających spam.

Aby tekst [SPAM] był dodawany do spamu i wiadomości typu phishing:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Filtrowanie spamu**.
3. Wybierz opcję **Oznacz spam etykietą [SPAM] w wierszu tematu wiadomości e-mail**.
4. Kliknij przycisk **OK**.

Po otrzymaniu wiadomości e-mail zawierającej spam lub phishing, funkcja filtrowania spamu doda tekst `[SPAM]` w polu tematu wiadomości e-mail.

5.3 Konfigurowanie programów poczty e-mail do filtrowania spamu

W programie do obsługi poczty e-mail można utworzyć reguły filtrowania *spamu* oraz *phishingu* w celu automatycznego przenoszenia niechcianych wiadomości do oddzielnego folderu.

Funkcja filtrowania spamu oznacza wszystkie wykryte wiadomości e-mail zawierające spam i phishing przedrostkiem [SPAM] w polu tematu wiadomości e-mail. Aby te wiadomości były automatycznie przenoszone ze skrzynki odbiorczej, należy utworzyć folder spamu oraz reguły filtrowania w programie poczty e-mail. W przypadku używania kilku kont poczty e-mail należy utworzyć osobne reguły filtrowania dla każdego z nich.

W tej sekcji znajdują się instrukcje dotyczące tworzenia folderu spamu oraz reguły filtrowania w programach Poczta systemu Windows, Microsoft Outlook, Mozilla Thunderbird, Eudora i Opera. Postępując według tych instrukcji, możesz także utworzyć podobne reguły filtrowania w innych programach do obsługi poczty e-mail.

Informacje: Filtrowanie *spamu* jest obsługiwane tylko dla protokołu POP3. Nie są obsługiwane programy poczty e-mail oparte na sieci Web ani inne protokoły.

5.3.1 Blokowanie spamu w programie Poczta systemu Windows

Aby filtrować wiadomości zawierające *spam* i phishing, musisz utworzyć odpowiedni folder i regułę filtrowania.

Aby korzystać z funkcji filtrowania spamu i wiadomości typu phishing w programie Poczta systemu Windows, upewnij się, że włączono opcję **Oznacz spam etykietą [SPAM] w wierszu tematu wiadomości e-mail** w oknie ustawień **Filtrowanie spamu**.

Aby utworzyć regułę filtrowania *spamu*:

1. W menu **Poczta systemu Windows** wybierz kolejno pozycje **Foldery** > **Reguły wiadomości**.

   Informacje: Jeśli okno **Nowa reguła poczty** nie zostanie wyświetlone automatycznie, na karcie **Reguły poczty e-mail** kliknij pozycję **Nowa**.

2. W oknie **Nowa reguła poczty** utwórz regułę powodującą przenoszenie wiadomości e-mail do folderu *spamu*:
   a) W polu warunków wybierz opcję **Kiedy w polu Temat znajdują się określone wyrazy**.
   b) W polu akcji wybierz opcję **Przenieś ją do folderu**.
3. W polu opisu reguły kliknij łącze **znajdują się określone wyrazy**.
   a) W oknie **Wpisywanie określonych wyrazów** wprowadź tekst `[SPAM]` i kliknij przycisk **Dodaj**.
   b) Kliknij przycisk **OK**, aby zamknąć okno **Wpisywanie określonych wyrazów**.
4. W polu opisu reguły kliknij łącze **folderu**.
   a) W oknie **Przenoszenie** kliknij pozycję **Nowy folder**.
   b) Wpisz `spam` jako nazwę nowego folderu i kliknij przycisk **OK**.
   c) Kliknij przycisk **OK**, aby zamknąć okno **Przenoszenie**.
5. W polu nazwy reguły wpisz `Spam`.
6. Kliknij przycisk **Zapisz regułę**, aby zamknąć okno **Nowa reguła poczty**.
   Zostanie otwarte okno **Reguły**.
7. Kliknij przycisk OK, aby zamknąć okno **Reguły**.
   Jeśli chcesz zastosować nową regułę do wiadomości e-mail istniejących już w skrzynce odbiorczej, wybierz regułę **spam** i kliknij przycisk **Zastosuj teraz**.

Reguła filtrowania *spamu* została utworzona. Od tej chwili *spam* będzie filtrowany do folderu *spamu*.

5.3.2 Blokowanie spamu w programie Microsoft Outlook

Aby filtrować wiadomości zawierające *spam* i phishing, musisz utworzyć odpowiedni folder i regułę filtrowania.

Aby korzystać z funkcji filtrowania spamu i wiadomości typu phishing w programie Microsoft Outlook, upewnij się, że włączono opcję **Oznacz spam etykietą [SPAM] w wierszu tematu wiadomości e-mail** w oknie ustawień **Filtrowanie spamu**.

Informacje: Podane czynności mają zastosowanie do programu Microsoft Outlook 2007. Czynności dla innych wersji mogą się nieznacznie różnić.

Aby utworzyć regułę filtrowania *spamu*:

1. W menu **Narzędzia** wybierz polecenie **Reguły i alerty**.
2. Na karcie **Reguły wiadomości e-mail** kliknij przycisk **Nowa reguła**.
3. Na liście **Zorganizuj swoją pracę** wybierz szablon **Przenieś wiadomości z określonymi wyrazami w temacie do folderu**.
4. Kliknij przycisk **Dalej**.
5. W okienku **Krok 2: Edytuj opis reguły** kliknij łącze **określonych wyrazów**.
   a) W polu **Podaj wyrazy lub frazy do wyszukiwania w temacie** wpisz `[SPAM]` i kliknij przycisk **Dodaj**.
   b) Kliknij przycisk **OK**, aby zamknąć okno **Wpisywanie określonych wyrazów**.
6. W okienku **Krok 2: Edytuj opis reguły** kliknij łącze **folderu**.
   a) W oknie **Reguły i alerty** kliknij opcję **Nowe**.
   b) Wpisz `spam` jako nazwę nowego folderu i kliknij przycisk **OK**.
   c) Kliknij przycisk **OK**, aby zamknąć okno **Reguły i alerty**.
7. Kliknij przycisk **Zakończ**.
8. Kliknij przycisk **OK**.

Jeśli chcesz zastosować nową regułę do wiadomości e-mail istniejących już w skrzynce odbiorczej, przed zamknięciem okna Reguły i alerty kliknij opcję **Uruchom reguły teraz**.

Reguła filtrowania *spamu* została utworzona. Od tej chwili *spam* będzie filtrowany do folderu *spamu*.

5.3.3 Blokowanie spamu w programach Mozilla Thunderbird i Eudora OSE

Aby filtrować wiadomości zawierające *spam* i phishing, musisz utworzyć odpowiedni folder i regułę filtrowania.

Aby utworzyć regułę filtrowania *spamu*:

1. Utwórz nowy folder na spam i wiadomości typu phishing:
   a) Kliknij prawym przyciskiem myszy nazwę swojego konta e-mail i wybierz polecenie **Nowy folder**.
   b) Wprowadź `spam` jako nazwę nowego folderu.
   c) Kliknij **Utwórz folder**.
2. Upewnij się, że Twoja nazwa konta jest wybrana i kliknij pozycję **Zarządzaj filtrami wiadomości** na liście **Funkcje zaawansowane**.
3. Kliknij przycisk **Nowe**.
4. W polu **Filter name** (Nazwa filtru) wprowadź nazwę `spam`.
5. Utwórz niestandardowy wpis nagłówka:
   a) Na liście **Dopasuj wszystkie poniższe** otwórz pierwsze menu rozwijane, w którym jest domyślnie wybrana pozycja **Temat**.
   b) Z pierwszej listy rozwijanej wybierz pozycję **Customize (Dostosuj)**.
   c) W oknie dialogowym **Customize Headers (Dostosowywanie nagłówków)** wprowadź wartość `X-Spam-Flag` jako nagłówek nowej wiadomości, a następnie kliknij przycisk **Add (Dodaj).**
   d) Kliknij przycisk **OK**, aby zamknąć okno dialogowe **Customize Headers (Dostosowywanie nagłówków)**.
6. Utwórz regułę filtrowania spamu:
   a) Na liście **Dopasuj wszystkie poniższe** otwórz pierwsze menu rozwijane i wybierz pozycję **X-Spam-Flag**, która została utworzona w poprzednim kroku.
   b) W drugim menu rozwijanym wybierz pozycję **zawiera**.
   c) W ostatnim polu w wierszu wpisz `Tak` jako tekst, który ma być dopasowany.
7. Utwórz akcję przenoszącą spam do folderu spamu:
   a) Na liście **Wykonaj te czynności** wybierz pozycję **Przenieś wiadomości do**.
   b) Na drugiej liście rozwijanej wybierz folder `spamu`.
8. Kliknij przycisk **OK**, aby zapisać zmiany.
9. Zamknij okno dialogowe **Message Filters** (Filtry wiadomości).

Reguła filtrowania *spamu* została utworzona. Od tej chwili *spam* będzie filtrowany do folderu *spamu*.

5.3.4 Blokowanie spamu w programie Opera

Aby filtrować wiadomości zawierające *spam* i phishing, musisz utworzyć odpowiedni folder i regułę filtrowania.

Informacje: Podane czynności mają zastosowanie do programu Opera 12. Czynności dla innych wersji mogą się nieznacznie różnić.

Aby utworzyć regułę filtrowania *spamu*:

1. Otwórz widok **Opera Mail**.
2. Kliknij prawym przyciskiem myszy domyślny folder *Spam* i wybierz polecenie **Properties** (Właściwości).
3. Kliknij przycisk **Add Rule** (Dodaj regułę).
4. Utwórz regułę powodującą przenoszenie wiadomości e-mail do filtru *spamu*:
   a) Z pierwszej listy wybierz pozycję **Any header (Dowolny nagłówek)**.
   b) Z drugiej listy wybierz pozycję **contains (zawiera)**.

c) W polu tekstowym wpisz wartość `X-Spam-Flag: Yes` jako tekst, który ma być dopasowywany. Między dwukropkiem a słowem `Yes (Tak)` pozostaw spację.

5. Kliknij przycisk **Close** (Zamknij), aby zatwierdzić nową regułę filtrowania *spamu*.

Reguła filtrowania *spamu* została utworzona. Od tej chwili *spam* będzie filtrowany do folderu *spamu*.

Co to jest zapora

Tematy:

Zapora uniemożliwia intruzom i szkodliwym aplikacjom dostęp do komputera z Internetu.

Zapora umożliwia nawiązywanie tylko bezpiecznych połączeń internetowych z komputera i blokuje włamania z Internetu.

6.1 Włączanie i wyłączanie zapory

Zapora blokuje intruzom dostęp do komputera, dlatego nie należy jej wyłączać.

Aby włączyć lub wyłączyć zaporę, wykonaj następujące czynności:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Włącz lub wyłącz opcję **Zapora**.

   Informacje: Po wyłączeniu funkcji zabezpieczeń komputer nie jest w pełni chroniony.

3. Kliknij przycisk **OK**.

Wyłączanie *zapory* nie jest zalecane. Wyłączenie zapory powoduje narażenie komputera na ataki sieciowe. Jeśli aplikacja przestanie działać, bo nie może nawiązać połączenia z Internetem, to zamiast wyłączać *zaporę* należy zmienić *ustawienia zapory*.

6.2 Zmień ustawienia zapory

Gdy zapora jest włączona, ogranicza dostęp do i z komputera. Niektóre aplikacje do prawidłowego działania mogą wymagać zezwolenia na dostęp przez zaporę.

W celu ochrony komputera produkt korzysta z Zapory systemu Windows.

Aby zmienić ustawienia zapory systemu Windows, wykonaj następujące czynności:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Zapora**.
3. Kliknij opcję **Zmień ustawienia zapory systemu Windows**.

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

Więcej informacji na temat Zapory systemu Windows znajduje się w dokumentacji systemu Microsoft Windows.

6.3 Zapobieganie pobieraniu szkodliwych plików przez aplikacje

Możesz zapobiec pobieraniu przez aplikacje szkodliwych plików z Internetu.

Niektóre witryny internetowe zawierają programy wykorzystujące luki w zabezpieczeniach i inne szkodliwe pliki, które mogą wyrządzić szkody na komputerze. Zaawansowane zabezpieczenia sieciowe umożliwiają zapobieganie pobieraniu szkodliwych plików przez aplikacje, zanim takie pliki dotrą na komputer.

Aby zablokować aplikacjom możliwość pobierania szkodliwych plików, wykonaj następujące czynności:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Zapora**.
3. Wybierz opcję **Nie zezwalaj aplikacjom na pobieranie szkodliwych plików**.

Informacje: To ustawienie działa nawet po wyłączeniu zapory.

6.4 Blokowanie połączeń z fałszywymi witrynami internetowymi

Możesz otrzymywać powiadomienia, gdy w używanej sieci wystąpi próba przekierowania połączenia na fałszywą witrynę internetową.

System nazw domen (DNS — Domain Name System) przekształca adresy sieciowe wpisywane w przeglądarce na odpowiednie adresy IP. Zwykle router jest połączony z serwerem DNS obsługiwanym przez usługodawcę internetowego. Jeśli haker lub szkodliwe oprogramowanie uzyska dostęp do routera, może zmienić jego ustawienia w celu korzystania z innego serwera DNS.

W przypadku takiego ataku na router zamiast otwieranych witryn internetowych mogą być wyświetlane ich fałszywe wersje.

Aby otrzymywać powiadomienia o przejęciu używanej sieci:

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

   Informacje: Do zmiany tych ustawień wymagane są uprawnienia administratora.

2. Wybierz pozycję **Zapora**.
3. Wybierz opcję **Ostrzegaj mnie, jeśli bezpieczeństwo używanej sieci jest naruszone**.

Informacje: To ustawienie działa nawet po wyłączeniu zapory.

6.5 Używanie zapór osobistych

Ten produkt został zaprojektowany do współpracy z zaporą systemu Windows. Aby inne zapory osobiste współpracowały z produktem, należy je odpowiednio skonfigurować.

Produkt korzysta z podstawowych funkcji zapory systemu Windows, takich jak kontrolowanie ruchu sieciowego i oddzielanie sieci wewnętrznej od publicznego Internetu. Ponadto technologia DeepGuard monitoruje zainstalowane aplikacje i uniemożliwia podejrzanym aplikacjom dostęp do Internetu bez pozwolenia.

Jeśli zastąpisz zaporę systemu Windows zaporą osobistą, upewnij się, że przepuszcza ona ruch sieciowy dla wszystkich procesów F-Secure. Należy zezwolić na dostęp do sieci wszystkich procesów F-Secure, jeśli zostanie wyświetlony odpowiedni monit.

Wskazówka: Jeśli używana zapora osobista ma ręczny tryb filtrowania, zezwól za jego pomocą na dostęp do sieci wszystkich procesów F-Secure.

Bezpieczne korzystanie z Internetu

Tematy:

Ochrona przeglądania ułatwia bezpieczne korzystanie z Internetu, podając klasyfikacje bezpieczeństwa stron internetowych w przeglądarce i blokując dostęp do stron oznaczonych jako szkodliwe.

Produkt zapewnia też ochronę przed oszustwami finansowymi podczas korzystania z usług bankowości internetowej. Otwarcie sesji usług bankowości online powoduje, że funkcja ochrony bankowości automatycznie dodaje specjalną warstwę zabezpieczeń, która uniemożliwia ingerowanie w poufne transakcje.

Informacje: Na smartfonach i tabletach funkcje Ochrona przeglądania i Ochrona bankowości są połączone w jednej funkcji o nazwie **Bezpieczne przeglądanie**.

7.1 Jak włączyć ochronę przeglądania

Włączona funkcja ochrony przeglądania blokuje dostęp do szkodliwych stron internetowych.

Aby włączyć funkcję ochrony przeglądania:

1. Na stronie głównej wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij przycisk **Ustawienia**.
   Zostanie wyświetlone okno dialogowe **Ustawienia**.
2. Wybierz pozycję **Ochrona przeglądania**.
3. Kliknij przełącznik w prawym górnym rogu.
4. Jeśli chcesz wyświetlać klasyfikację bezpieczeństwa stron internetowych w wynikach wyszukiwania (Google, Yahoo i Bing), wybierz opcję **Pokazuj klasyfikację reputacji witryn w wynikach wyszukiwania**.
5. Jeśli przeglądarka jest otwarta, uruchom ją ponownie w celu zastosowania zmienionych ustawień.

7.2 Ręczne instalowanie funkcji Ochrona przeglądania

W przypadku obsługiwanych przeglądarek może być konieczne ponowne zainstalowanie rozszerzeń Ochrona przeglądania lub włączenie ich ręcznie.

Strona główna produktu zawiera informacje o niezainstalowanych lub niewłączonych rozszerzeniach przeglądarki domyślnej.

Informacje: Niektóre przeglądarki, na przykład Microsoft Edge, nie obsługują rozszerzeń.

Aby ponownie zainstalować rozszerzenia przeglądarki:

1. Na głównej stronie **Stan** wybierz opcję **Ochrona przeglądania** u dołu.
   Pojawi się strona funkcji Ochrona przeglądania.
2. Wskaż konto użytkownika systemu Windows i wybierz opcję **Ustawienia**.

   Informacje: Aby otworzyć tę stronę, musisz mieć uprawnienia administratora.

   Pojawi się strona Ustawienia zabezpieczeń.
3. W sekcji **Inne** wybierz opcję **Rozszerzenia przeglądarki**.
4. Wybierz pozycję **Zainstaluj rozszerzenia ponownie**.
   Powoduje to ponowne zainstalowanie rozszerzeń produktu na wszystkich obecnie zainstalowanych przeglądarkach.
5. Wybierz przycisk **OK**.
   Strona Ustawienia zabezpieczeń zostanie zamknięta.

Jeśli chcesz ręcznie włączyć rozszerzenia przeglądarki, musisz edytować ustawienia przeglądarki:

- W przeglądarce Firefox w menu wybierz opcję **Narzędzia** > **Dodatki** i kliknij przycisk **Włącz** obok rozszerzenia.
- W przeglądarce Chrome w menu wybierz opcję **Ustawienia**, wybierz pozycję **Rozszerzenia** i kliknij przycisk **Włącz** obok rozszerzenia.
- W przeglądarce Internet Explorer wybierz opcję **Narzędzia** > **Zarządzaj dodatkami**, wybierz rozszerzenie przeglądarki i kliknij przycisk **Włącz**.
- Przeglądarka Microsoft Edge nie obsługuje rozszerzeń.

Informacje: Jeśli trzeba ręcznie włączyć rozszerzenia, należy to zrobić oddzielnie na każdym koncie użytkownika komputera.

7.3 Co zrobić, gdy witryna sieci Web jest zablokowana

Przy próbie uzyskania dostępu do witryny sklasyfikowanej jako szkodliwa jest wyświetlana strona blokowania funkcji ochrony przeglądania.

Gdy pojawi się strona blokowania funkcji ochrony przeglądania:

1. Jeśli mimo wszystko chcesz przejść do tej witryny, kliknij opcję **Zezwalaj na dostęp do witryn**. Kontrola konta użytkownika systemu Windows poprosi o potwierdzenie tej czynności.
2. Jeśli to konieczne, wprowadź dane konta administratora, a następnie potwierdź zmiany.

7.4 Bezpieczne korzystanie z bankowości internetowej

Funkcja ochrony bankowości blokuje szkodliwe działaniami w czasie korzystania z banku internetowego lub wykonywania transakcji w trybie online.

Funkcja ochrony bankowości automatycznie wykrywa bezpieczne połączenia z witrynami bankowości internetowej i blokuje wszelkie połączenia, które nie prowadzą do witryn tego typu. Po otwarciu witryny bankowości internetowej dozwolone są tylko połączenia z witrynami bankowości internetowej oraz witrynami, które są określone jako bezpieczne do użytku podczas korzystania z bankowości internetowej.

Funkcja Ochrona bankowości obsługuje obecnie następujące przeglądarki:

- Internet Explorer 9 lub nowsza
- Microsoft Edge
- Firefox 13 lub nowsza
- Google Chrome

Na smartfonach i tabletach funkcja ochrony bankowości stanowi część funkcji Bezpieczne przeglądanie. Włączenie funkcji Bezpieczne przeglądanie automatycznie aktywuje ochronę bankowości.

7.4.1 Włączanie funkcji Ochrona bankowości

Po włączeniu funkcji Ochrona bankowości wszystkie sesje i transakcje bankowe zostają zabezpieczone.

Aby włączyć funkcję Ochrona bankowości:

1. Na stronie głównej wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij przycisk **Ustawienia**.
   Zostanie wyświetlone okno dialogowe **Ustawienia**.
2. Wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij pozycję **Ustawienia**.
   Zostanie otwarta strona **Ustawienia**.

   Informacje: Aby otworzyć tę stronę, musisz mieć prawa administratora.

3. Wybierz pozycję **Ochrona bankowości**.
4. Kliknij przełącznik w prawym górnym rogu okna, aby włączyć lub wyłączyć funkcję Ochrona bankowości.
5. Wybierz przycisk **OK**.
   Funkcja Ochrona bankowości jest teraz włączona na wybranym koncie użytkownika.
6. Jeśli chcesz, aby aktualne połączenia pozostały otwarte, wybierz opcję **Nie przerywaj moich aktywnych połączeń internetowych**.

   Podczas korzystania z witryny internetowej banku lub realizowania płatności online, funkcja Ochrona bankowości blokuje wszystkie połączenia, które nie są niezbędne do przeprowadzenia operacji bankowych. Oznacza to, że o ile nie wybierzesz tego ustawienia, wszystkie aktywne połączenia internetowe zostaną zamknięte.

7.4.2 Używanie ochrony bankowości

Po włączeniu funkcja Ochrona bankowości automatycznie wykrywa dostęp do witryny bankowości internetowej.

Gdy w przeglądarce zostanie otwarta witryna bankowości internetowej, u góry ekranu pojawia się powiadomienie funkcji **Ochrona bankowości**. W trakcie sesji ochrony bankowości wszystkie inne połączenia są blokowane.

Wskazówka: Jeśli nie chcesz, aby aktywne połączenia były przerywane przez funkcję Ochrona bankowości, kliknij opcję **Zmień ustawienia** w powiadomieniu w celu edytowania ustawień produktu dla swojego konta użytkownika.

Aby zakończyć sesję ochrony bankowości i przywrócić możliwość nawiązywania innych połączeń:

Kliknij przycisk **Zakończ** w powiadomieniu **Ochrona bankowości**.

Co to jest *Search by F-Secure*

Tematy:

Program *Search by F-Secure* udostępnia ocenę bezpieczeństwa odwiedzanych witryn internetowych i zapobiega przypadkowemu uzyskiwaniu dostępu do szkodliwych stron.

Program *Search by F-Secure* wykrywa witryny internetowe zawierające zagrożenia, takie jak złośliwe oprogramowanie (wirusy, robaki, konie trojańskie), lub usiłujące wykradać poufne informacje, na przykład nazwy użytkowników i hasła.

8.1 Co to jest klasyfikacja bezpieczeństwa

Klasyfikacja bezpieczeństwa udostępniana w wynikach wyszukiwania ułatwia unikanie internetowych zagrożeń.

Klasyfikacja bezpieczeństwa jest oparta na informacjach z kilku źródeł, takich jak analitycy złośliwego oprogramowania i partnerzy firmy F-Secure.

	Według naszych informacji dana strona internetowa jest bezpieczna. Nie wykryliśmy na niej żadnych podejrzanych elementów.
	Ta strona jest podejrzana. Zalecamy zachowanie ostrożności podczas jej odwiedzania. Unikaj pobierania jakichkolwiek plików i podawania danych osobowych.
	Ta strona jest szkodliwa. Zalecamy unikanie jej odwiedzania.
	Nie przeanalizowaliśmy jeszcze tej strony internetowej lub obecnie nie są dostępne żadne informacje na jej temat.
	Administrator pozwolił Ci na otwarcie tej strony internetowej.
	Administrator zablokował tę stronę internetową, dlatego nie możesz jej otworzyć.

8.2 Konfigurowanie programu *Search by F-Secure* w przeglądarce internetowej

Program *Search by F-Secure* obsługuje następujące przeglądarki internetowe:

- Internet Explorer 8 dla systemu Windows XP SP3
- Internet Explorer, dwie najnowsze wersje wydane dla systemów Windows Vista, Windows 7 i Windows 8
- Firefox, dwie najnowsze wersje
- Google Chrome, dwie najnowsze wersje

8.2.1 Używanie programu *Search by F-Secure* w przeglądarce Internet Explorer

Możesz ustawić program *Search by F-Secure* jako domyślną stronę główną, dostawcę usług wyszukiwania i zainstalować pasek narzędzi wyszukiwania w przeglądarce Internet Explorer.

Postępuj zgodnie z tymi instrukcjami, aby korzystać z programu *Search by F-Secure* w przeglądarce Internet Explorer:

1. Otwórz program Internet Explorer.
2. Gdy w przeglądarce Internet Explorer zostanie wyświetlona wiadomość, że dodatek paska narzędzi jest gotowy do użycia, kliknij przycisk **Włącz**. Jeśli zamiast tego zostanie wyświetlone okno dialogowe **Kilka dodatków jest gotowych do użycia**, najpierw kliknij przycisk **Wybierz dodatki**.

   Informacje: W przeglądarce Internet Explorer 8 pasek narzędzi jest gotowy do użycia automatycznie.

   Informacje: Ten komunikat nie zostanie wyświetlony, jeśli podczas instalacji produktu nie został zainstalowany pasek narzędzi wyszukiwania.

3. Aby ustawić *Search by F-Secure* jako domyślnego dostawcę usług wyszukiwania:
   a) Wybierz opcje **Narzędzia** > **Opcje internetowe**.
   b) W sekcji **Wyszukiwanie** kliknij pozycję **Ustawienia**.
   c) Na liście **Dostawcy usług wyszukiwania** kliknij prawym przyciskiem myszy pozycję *Search by F-Secure* i wybierz opcję **Ustaw jako domyślną**.

8.2.2 Używanie programu *Search by F-Secure* w przeglądarce Firefox

Możesz ustawić program *Search by F-Secure* jako domyślną stronę główną, dostawcę usług wyszukiwania i zainstalować pasek narzędzi wyszukiwania w przeglądarce Firefox.

Informacje: Jeśli konfiguracja programu Firefox uniemożliwia zmienianie strony głównej i dostawcy usług wyszukiwania, program *Search by F-Secure* nie może zmodyfikować tych ustawień.

Wykonaj poniższe czynności, aby włączyć pasek narzędzi *Search by F-Secure* w przeglądarce Firefox po zainstalowaniu produktu:

1. Otwórz program Firefox.
2. Otwórz kartę **Instalacja dodatków**.
3. Upewnij się, że wymienionym dodatkiem jest program *Search by F-Secure*.
4. Zaznacz pole wyboru **Zezwalaj na tę instalację**.
5. Kliknij przycisk **Kontynuuj**.
6. Kliknij opcję **Uruchom program Firefox ponownie**.

8.2.3 Używanie programu *Search by F-Secure* w przeglądarce Chrome

Możesz ustawić program *Search by F-Secure* jako domyślnego dostawcę usług wyszukiwania i zainstalować pasek narzędzi wyszukiwania w przeglądarce Chrome.

Jeśli domyślną przeglądarką jest Chrome, instalacja produktu może automatycznie zainstalować pasek narzędzi wyszukiwania i dodać *Search by F-Secure* jako dostawcę usług wyszukiwania.

Aby ustawić *Search by F-Secure* jako domyślnego dostawcę usług wyszukiwania:

1. W menu przeglądarki Chrome wybierz polecenie **Ustawienia**.
2. Znajdź ustawienia **Wyszukiwanie**.
3. Kliknij opcję **Zarządzaj wyszukiwarkami**.
4. W wierszu *Search by F-Secure* kliknij pozycję **Ustaw jako domyślną**.

8.3 Usuwanie aplikacji *Search by F-Secure*

8.3.1 Usuwanie programu *Search by F-Secure* z przeglądarki Internet Explorer

Postępuj zgodnie z tymi instrukcjami, jeśli chcesz wyłączyć program *Search by F-Secure* w przeglądarce Internet Explorer.

1. Otwórz Panel sterowania systemu Windows.
2. Otwórz **Sieć i Internet** > **Opcje internetowe**.
   Zostanie wyświetlone okno **Właściwości internetowe.**
3. Aby domyślną stroną główną nie była już witryna produktu *Search by F-Secure*, wykonaj te czynności:
   a) W oknie **Właściwości internetowe** otwórz kartę **Ogólne**.
   b) W sekcji **Strona główna** kliknij opcję **Użyj domyślnej**.
4. W oknie **Właściwości internetowe** otwórz kartę **Programy**.
5. Kliknij opcję **Zarządzaj dodatkami**.
   Zostanie otwarte okno **Zarządzaj dodatkami**.
6. Aby dostawcą wyszukiwania nie był już produkt *Search by F-Secure*, wykonaj te czynności:
   a) W sekcji **Zarządzaj dodatkami** wybierz opcję **Dostawcy wyszukiwania**.
   b) Wybierz opcję *Search by F-Secure*.
   c) Kliknij przycisk **Usuń**.
7. Aby usunąć pasek narzędzi *Search by F-Secure*, wykonaj te czynności:
   a) W sekcji **Zarządzaj dodatkami** wybierz opcję **Paski narzędzi i rozszerzenia**.
   b) Wybierz opcję *Search by F-Secure*.

c) Kliknij przycisk **Wyłącz**.

Informacje: Odinstaluj program *Search by F-Secure*, aby całkowicie usunąć wyszukiwarkę i pasek narzędzi *Search by F-Secure*.

8.3.2 Usuwanie funkcji *Search by F-Secure* z przeglądarki Firefox

Postępuj zgodnie z tymi instrukcjami, jeśli chcesz wyłączyć program *Search by F-Secure* w przeglądarce Firefox.

1. Aby domyślną stroną główną nie była już witryna produktu *Search by F-Secure*, wykonaj te czynności:
   a) Otwórz **Narzędzia** > **Opcje**.
   a) W oknie **Opcje** otwórz kartę **Ogólne**.
   b) Kliknij przycisk **Przywróć domyślną** pod polem **Strona startowa**.
2. Aby dostawcą wyszukiwania nie był już produkt *Search by F-Secure*, wykonaj te czynności:
   a) Kliknij opcję dostawcy wyszukiwania w polu wyszukiwania, aby otworzyć menu wyszukiwarki.
   b) Kliknij opcję **Zarządzaj wyszukiwarkami**.
   c) Wybierz na liście produkt *Search by F-Secure* i kliknij przycisk **Usuń**.
   d) Kliknij przycisk **OK**.
3. Aby usunąć pasek narzędzi *Search by F-Secure*, wykonaj te czynności:
   a) Otwórz **Narzędzia** > **Dodatki**.
   b) W oknie **Menedżer dodatków** otwórz kartę **Rozszerzenia**.
   c) Kliknij opcję **Wyłącz** w wierszu rozszerzenia *Search by F-Secure*.
   d) Uruchom ponownie przeglądarkę, aby usunąć pasek narzędzi.

Informacje: Odinstaluj program *Search by F-Secure*, aby całkowicie usunąć wyszukiwarkę i pasek narzędzi *Search by F-Secure*.

8.3.3 Usuwanie programu *Search by F-Secure* z przeglądarki Chrome

Postępuj zgodnie z tymi instrukcjami, jeśli chcesz wyłączyć program *Search by F-Secure* w przeglądarce Chrome.

1. Aby zmienić dostawcę wyszukiwania z programu *Search by F-Secure*, wykonaj te czynności:
   a) W menu przeglądarki Chrome wybierz polecenie **Ustawienia**.
   b) Znajdź ustawienia **Wyszukiwanie**.
   c) Kliknij opcję **Zarządzaj wyszukiwarkami**.
   d) Kliknij znak **X** na końcu wiersza programu *Search by F-Secure*.
2. Aby usunąć pasek narzędzi *Search by F-Secure*, wykonaj te czynności:
   a) Kliknij prawym przyciskiem myszy ikonę programu *Search by F-Secure* na pasku narzędzi.
   b) Wybierz opcję **Usuń z przeglądarki Chrome**.

Informacje: Odinstaluj program *Search by F-Secure*, aby całkowicie usunąć wyszukiwarkę i pasek narzędzi *Search by F-Secure*.

Ograniczanie dostępu do zawartości internetowej

Tematy:

Możesz chronić siebie i swoich bliskich przed oglądaniem nieodpowiednich materiałów w Internecie przez ograniczenie dostępu do szkodliwych i niechcianych treści.

Internet zawiera mnóstwo interesujących witryn. Niestety nie wszystkie z nich zawierają materiały, które można uznać za odpowiednie lub pożądane — zwłaszcza dla dzieci.

Funkcja Blokowanie zawartości pozwala upewnić się, że zarówno Ty, jak i Twoi bliscy, nie wyświetlicie nieodpowiednich treści na komputerach. Dzięki tej funkcji możesz ograniczyć strony internetowe dostępne do przeglądania i określić harmonogram dozwolonego korzystania z trybu online. Możesz też ukryć w wynikach wyszukiwania łącza do treści przeznaczonych dla osób dorosłych.

Na smartfonach i tabletach możesz użyć funkcji Kontrola rodzicielska, aby zablokować dostęp do witryn internetowych zawierających nieodpowiednie treści. Możesz też użyć funkcji Kontrola aplikacji w celu kontrolowania aplikacji, z których dzieci mogą korzystać.

9.1 Blokowanie zawartości internetowej na komputerze

Możesz chronić siebie i swoich bliskich przed wieloma różnymi zagrożeniami internetowymi przez ograniczenie dostępu do określonych rodzajów treści, które użytkownicy mogą wyświetlać na komputerze.

Te ograniczenia są stosowane do kont użytkowników systemu Windows, więc obowiązują natychmiast po zalogowaniu się na konto przez użytkownika.

Informacje: Ograniczenie dostępu do określonych zawartości w trybie online pozwala chronić konta użytkowników przed programami czatu i poczty e-mail, które są uruchamiane w przeglądarce.

9.1.1 Zezwalanie na dostęp do stron sieci Web

Aby zezwolić na dostęp tylko do zaufanych witryn i stron internetowych, można dodać te witryny i strony do listy dozwolonych witryn.

Aby zezwolić na dostęp do określonych stron internetowych, wykonaj następujące czynności:

1. Na stronie Stan wybierz opcję **Ochrona przeglądania**.
   Zostanie otwarta strona **Ochrona przeglądania**.
2. Wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij pozycję **Ustawienia**.
   Zostanie otwarta strona **Ustawienia**.

   Informacje: Aby otworzyć tę stronę, musisz mieć prawa administratora.
3. Wybierz pozycję **Blokowanie zawartości**.
4. Kliknij przełącznik w prawym górnym rogu okna, aby włączyć lub wyłączyć funkcję Blokowanie zawartości.
5. Wybierz opcję **Zezwalaj tylko na wybrane witryny**.
6. Kliknij przycisk **Dodaj**, aby dodać witryny internetowe do listy **Witryny dozwolone**.
7. Po dodaniu wszystkich witryn, które mają być dostępne, kliknij przycisk **OK**.

Po zalogowaniu się użytkownik korzystający z edytowanego konta systemu Windows będzie miał dostęp tylko do witryn internetowych dodanych do listy dozwolonych witryn.

9.1.2 Blokowanie stron sieci Web w zależności od typu ich zawartości

Możesz zablokować dostęp do witryn i stron zawierających nieodpowiednie treści.

Aby wybrać typy blokowanej zawartości internetowej, wykonaj następujące czynności:

1. Na stronie Stan wybierz opcję **Ochrona przeglądania**.
   Zostanie otwarta strona **Ochrona przeglądania**.
2. Wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij pozycję **Ustawienia**.
   Zostanie otwarta strona **Ustawienia**.

   Informacje: Aby otworzyć tę stronę, musisz mieć prawa administratora.
3. Wybierz pozycję **Blokowanie zawartości**.
4. Kliknij przełącznik w prawym górnym rogu okna, aby włączyć lub wyłączyć funkcję Blokowanie zawartości.
5. Wybierz opcję **Zablokuj zawartość internetową**.
6. Zaznacz zawartość, którą chcesz zablokować.
7. Po wybraniu wszystkich typów zawartości, które chcesz zablokować, kliknij przycisk **OK**.

Po zalogowaniu się użytkownik korzystający z edytowanego konta systemu Windows nie będzie miał dostępu do witryn internetowych z zablokowaną zawartością.

9.1.3 Edytowanie listy dozwolonych/zablokowanych witryn

Istnieje możliwość zezwolenia na dostęp do określonych zablokowanych witryn, a także zablokowania witryn, których nie uwzględniono w żadnym z typów zawartości.

Informacje: W zależności od używanej wersji produktu, może być dostępne tylko zezwalanie lub blokowanie witryn, ale nie obie opcje naraz.

Można na przykład uznać określoną witrynę za bezpieczną, mimo że inne witryny z danym typem zawartości mają być zablokowane. Można również zablokować konkretną witrynę, mimo że inne witryny z tym typem zawartości mają być dozwolone.

Aby zezwolić na dostęp do witryny lub ją zablokować:

1. Na stronie głównej wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij przycisk **Ustawienia**.
   Zostanie wyświetlone okno dialogowe **Ustawienia**.
2. Wybierz pozycję **Blokowanie zawartości**.
3. Kliknij pozycję **Wyświetl wyjątki związane z witrynami**.
   Jeśli witryna, która ma zostać poddana edycji, jest wyświetlana jako dozwolona lub zabroniona i ma zostać przeniesiona z jednej listy na drugą:
   a) W zależności od tego, która lista witryn ma być edytowana, kliknij kartę **Dozwolone** lub **Zabronione**.
   b) Kliknij prawym przyciskiem myszy witrynę na liście i wybierz opcję **Zezwalaj** lub **Nie zezwalaj**.
   Jeśli witryny nie ma na żadnej z list:
   a) Kliknij kartę **Dozwolone**, jeśli chcesz zezwolić na dostęp do witryny, lub kartę **Zabronione**, jeśli chcesz zablokować witrynę.
   b) Kliknij przycisk **Dodaj**, aby dodać nową witrynę do listy.
   c) Wpisz adres witryny internetowej, którą chcesz dodać, i kliknij przycisk **OK**.
   d) W oknie **Wyjątki związane z witrynami** kliknij przycisk **Zamknij**.
4. Kliknij przycisk **OK**, aby wrócić na stronę główną.

Aby zmienić adres dozwolonej lub zablokowanej witryny, kliknij prawym przyciskiem myszy witrynę i wybierz opcję **Edytuj**.

Aby usunąć dozwoloną lub zablokowaną witrynę z listy, zaznacz witrynę i kliknij przycisk **Usuń**.

9.1.4 Korzystanie z filtra wyników wyszukiwania

Możesz włączyć filtr wyników wyszukiwania, aby zablokować nieodpowiednie treści w wynikach wyszukiwania.

Filtr wyników wyszukiwania ukrywa treść tylko dla dorosłych, ustawiając poziom „rygorystyczny” funkcji SafeSearch w wyszukiwarkach Google, Yahoo i Bing. Ta funkcja nie jest w stanie zablokować wszystkich nieodpowiednich i niedozwolonych treści w wynikach wyszukiwania, ale pozwala uniknąć znacznej większości z nich.

Aby włączyć filtr wyników wyszukiwania:

1. Na stronie głównej wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij przycisk **Ustawienia**.
   Zostanie wyświetlone okno dialogowe **Ustawienia**.
2. Wybierz kolejno opcje **Kontrola rodzicielska** > **Filtr wyników wyszukiwania**.
3. Kliknij przełącznik w prawym górnym rogu.

Po włączeniu filtra wyników wyszukiwania zastąpi on ustawienia funkcji SafeSearch w witrynach internetowych dla danego konta użytkownika systemu Windows.

9.1.5 Ustawianie ograniczeń czasowych

Możesz kontrolować, kiedy i jak długo można używać tego komputera.

Ustawiając różne ograniczenia dla poszczególnych kont użytkowników systemu Windows, można kontrolować następujące aspekty:

- Kiedy dana osoba może przeglądać Internet na komputerze — można na przykład zezwolić na przeglądanie Internetu tylko przed godziną 20:00.
- Jak długo użytkownik może przeglądać Internet na komputerze. Można na przykład zezwolić na przeglądanie Internetu tylko przez jedną godzinę dziennie.

Informacje: Jeśli usuniesz ograniczenia czasowe dla użytkownika, będzie on mógł używać komputera i przeglądać Internet w dowolnej chwili.

Ustawianie ograniczeń czasowych

Możesz kontrolować, kiedy i jak długo można używać tego komputera.

Ustawiając różne ograniczenia dla poszczególnych kont użytkowników systemu Windows, można kontrolować następujące aspekty:

- Kiedy dana osoba może przeglądać Internet na komputerze — można na przykład zezwolić na przeglądanie Internetu tylko przed godziną 20:00.
- Jak długo użytkownik może przeglądać Internet na komputerze. Można na przykład zezwolić na przeglądanie Internetu tylko przez jedną godzinę dziennie.

Informacje: Jeśli usuniesz ograniczenia czasowe dla użytkownika, będzie on mógł używać komputera i przeglądać Internet w dowolnej chwili.

Aby ustawić dozwolone godziny:

1. Na stronie głównej wybierz konto użytkownika systemu Windows, które chcesz edytować, i kliknij przycisk **Ustawienia**.
   Zostanie wyświetlone okno dialogowe **Ustawienia**.
2. Wybierz pozycję **Ograniczenia czasowe**.
3. Kliknij przełącznik w prawym górnym rogu.
4. Wybierz typ dostępu, jaki chcesz ograniczyć:
   - Aby ograniczyć ogólny dostęp do komputera, wybierz pozycję **Zablokuj komputer**.
   - Aby ograniczyć przeglądanie Internetu, wybierz pozycję **Zablokuj tylko przeglądanie Internetu**.
5. W tabeli *dozwolonych godzin* ustaw godziny dla każdego dnia tygodnia.
   Jeśli nie chcesz ograniczać dostępu do określonych godzin, upewnij się, że wszystkie komórki w tabeli są wybrane.
6. Wybierz maksymalną liczbę dozwolonych godzin dziennie.
   Jeśli nie chcesz ograniczać dozwolonego czasu korzystania z komputera, upewnij się, że czas przeglądania jest ustawiony na **Maks**.
7. Kliknij przycisk **OK**.

Te ograniczenia czasowe będą stosowane dla każdego, kto używa wybranego konta użytkownika systemu Windows.

Security Cloud

Tematy:

Funkcja *Security Cloud* (znana wcześniej jako Sieć ochrony w czasie rzeczywistym) to usługa internetowa firmy F-Secure Corporation służącą do identyfikowania bezpiecznych aplikacji i witryn internetowych oraz zabezpieczania przed złośliwym oprogramowaniem i witrynami wykorzystującymi luki w zabezpieczeniach.

10.1 Co to jest funkcja *Security Cloud*?

Funkcja *Security Cloud* to usługa online zapewniającą błyskawiczne reakcje na nowe zagrożenia internetowe.

Korzystając z funkcji *Security Cloud*, zezwalasz jej na gromadzenie danych zabezpieczeń, które pomagają nam wzmocnić nasze zabezpieczenia przed nowymi i powstającymi zagrożeniami. Funkcja *Security Cloud* gromadzi dane zabezpieczeń dotyczące nieznanych, złośliwych i podejrzanych aplikacji oraz niesklasyfikowanych witryn internetowych. Te informacje mają charakter anonimowy i są wysyłane do analizy zbiorczej w firmie F-Secure Corporation. Korzystając z wyników takich analiz, udoskonalamy zabezpieczenia przed najnowszymi zagrożeniami i złośliwymi plikami.

Jak działa funkcja *Security Cloud*?

Funkcja *Security Cloud* gromadzi dane zabezpieczeń dotyczące nieznanych aplikacji i witryn internetowych oraz złośliwych programów i witryn zawierających próby wykorzystania luk w zabezpieczeniach. Zbieramy dane zabezpieczeń, aby udostępniać Ci usługi zabezpieczeń, które subskrybujesz, oraz zwiększać bezpieczeństwo innych naszych usług. Musimy zbierać dane zabezpieczeń dotyczące nieznanych plików, podejrzanego zachowania urządzeń czy odwiedzanych adresów URL. Te dane są niezbędne do działania naszych usług.

Usługa *Security Cloud* nie śledzi działań użytkowników w Internecie, nie gromadzi informacji na temat witryn, które zostały już przeanalizowane, ani nie zbiera informacji o bezpiecznych aplikacjach zainstalowanych na komputerze. Dane zabezpieczeń nie są używane w celach marketingowych.

10.2 Zalety funkcji *Security Cloud*

Funkcja *Security Cloud* zapewnia szybszą i dokładniejszą ochronę przed najnowszymi zagrożeniami — bez niepotrzebnych alertów dotyczących podejrzanych aplikacji, które nie są złośliwe.

Korzystając z funkcji *Security Cloud*, możesz pomóc nam w wykrywaniu nowych i nieznanych form złośliwego oprogramowania oraz określaniu obiektów niepoprawnie uznanych za niebezpieczne.

Wszyscy użytkownicy funkcji *Security Cloud* pomagają sobie wzajemnie. W przypadku wykrycia podejrzanej aplikacji funkcja *Security Cloud* używa wyników analizy tej aplikacji wykrytej wcześniej u innych użytkowników. Funkcja *Security Cloud* zwiększa ogólną wydajność, ponieważ zainstalowany produkt zabezpieczający nie musi skanować aplikacji przeanalizowanych i uznanych za bezpieczne przez funkcję *Security Cloud*. Podobnie informacje dotyczące złośliwych witryn internetowych i niechcianych wiadomości zbiorczych są udostępniane za pomocą funkcji *Security Cloud*, umożliwiając zapewnianie dokładniejszej ochrony przed witrynami wykorzystującymi luki w zabezpieczeniach i spamem.

Im więcej osób korzysta z funkcji *Security Cloud*, tym indywidualna ochrona użytkowników staje się lepsza.

10.3 Jakie dane są przesyłane

Korzystając z funkcji *Security Cloud*, zezwalasz jej na gromadzenie danych zabezpieczeń dotyczących instalowanych aplikacji i odwiedzanych witryn internetowych. Te dane umożliwiają funkcji *Security Cloud* zapewnianie ochrony przed najnowszymi złośliwymi aplikacjami i podejrzanymi witrynami internetowymi.

Analizowanie reputacji plików

Funkcja *Security Cloud* gromadzi dane zabezpieczeń dotyczące tylko aplikacji bez określonej reputacji i znanych plików, które są podejrzane lub zawierają złośliwe oprogramowanie.

Gromadzone są informacje tylko na temat plików aplikacji (plików wykonywalnych). Inne typy plików nie są uwzględniane.

W zależności od produktu gromadzone dane zabezpieczeń mogą obejmować:

- ścieżkę do pliku aplikacji (bez jakichkolwiek informacji identyfikujących użytkownika),
- rozmiar oraz datę utworzenia lub zmodyfikowania pliku;
- atrybuty i uprawnienia pliku;

- informacje o sygnaturze pliku;
- bieżącą wersję pliku i nazwę firmy, w której został utworzony;
- źródło pliku lub adres URL jego pobierania (bez jakichkolwiek informacji identyfikujących użytkownika),
- wyniki skanowania plików przy użyciu technologii F-Secure DeepGuard i mechanizmów antywirusowych;
- inne podobne informacje.

Analizowanie reputacji witryn internetowych

Funkcja *Security Cloud* nie śledzi działań użytkowników w Internecie, a jedynie sprawdza bezpieczeństwo odwiedzanych witryn podczas przeglądania Internetu. Po otwarciu witryny funkcja *Security Cloud* sprawdza, czy jest ona bezpieczna, a następnie powiadamia o poziomie ewentualnego zagrożenia (w przypadku podejrzanych lub szkodliwych witryn).

Aby zwiększyć jakość usługi i zachować wysoką dokładność analizy, funkcja *Security Cloud* może gromadzić informacje o odwiedzanych witrynach internetowych. Takie informacje są zbierane, gdy odwiedzana witryna zawiera złośliwe lub podejrzane elementy albo próby wykorzystania znanych luk w zabezpieczeniach bądź jeśli zawartość witryny nie została jeszcze sprawdzona i skategoryzowana. Gromadzone informacje obejmują adres URL i metadane powiązane z witryną i wizytą w niej.

Funkcja *Security Cloud* korzysta z rygorystycznych zabezpieczeń uniemożliwiających wysyłanie prywatnych danych użytkowników. Dodatkowo liczba gromadzonych adresów URL jest ograniczona. Przed wysłaniem wszystkie gromadzone dane są filtrowane pod kątem informacji związanych z prywatnością i wszystkie pola, które mogą zawierać dane dotyczące użytkownika i pozwalać na jego identyfikację, są usuwane. Funkcja *Security Cloud* nie ocenia ani nie analizuje stron w prywatnych sieciach ani nie gromadzi żadnych informacji o prywatnych adresach sieciowych i aliasach.

Analizowanie informacji systemowych

W ramach działania funkcji *Security Cloud* gromadzone są informacje o nazwie i wersji systemu operacyjnego, połączeniu internetowym oraz dane statystyczne dotyczące użytkowania funkcji *Security Cloud*, takie jak liczba zapytań o reputację witryny i średni czas uzyskiwania wyników zapytania, na potrzeby monitorowania i ulepszania naszej usługi.

10.4 W jaki sposób chronimy Twoją prywatność

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

Zgromadzone dane zabezpieczeń nie są przetwarzane indywidualnie, ale w zbiorowej postaci obejmującej informacje uzyskane od innych użytkowników funkcji *Security Cloud*. Wszystkie dane są anonimowo analizowane pod kątem statystycznym, co oznacza, że nie można ich skojarzyć z poszczególnymi użytkownikami.

Żadne informacje umożliwiające identyfikowanie tożsamości użytkowników nie są uwzględniane w gromadzonych danych. Funkcja *Security Cloud* nie gromadzi prywatnych adresów IP ani innych danych osobowych, takich jak adresy e-mail, nazwy użytkowników i hasła. Mimo że podejmujemy wszelkie starania w celu usunięcia wszystkich identyfikujących danych osobistych, istnieje możliwość pozostania identyfikujących danych w gromadzonych informacjach. W takich sytuacjach nie będziemy używać tych przypadkowo uzyskanych danych w celu określania tożsamości użytkowników.

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

Zbieranie danych zabezpieczeń

Naszą główną regułą jest to, że dane, które identyfikują Twoją tożsamość lub w jakiś sposób łączą Cię z danymi zabezpieczeń zbieranymi na urządzeniu, są usuwane lub ukrywane w celu ochrony Twojej prywatności. Możemy dalej przekazywać takie dane zabezpieczeń do naszych oddziałów, podwykonawców, zespołów pomocy komputerowej i innych firm — z zachowaniem anonimowości danych.

Będziemy przetwarzać dane zabezpieczeń — lub wynikające z nich metadane — w formie umożliwiającej określenie tożsamości tylko w wyjątkowych przypadkach, gdy nie możemy świadczyć usług w inny sposób, na przykład w czasie rozwiązywania zgłoszonego przez Ciebie problemu — za Twoją zgodą. Innym przykładem jest pokazywanie złośliwego oprogramowania na zainfekowanych urządzeniach w firmowym portalu zarządzania produktami. Jeśli to konieczne, możemy udostępniać takie dane zabezpieczeń umożliwiające zidentyfikowanie naszym oddziałom, podwykonawcom i dystrybutorom. Szczegółowe dane dotyczące oglądanych przez Ciebie stron internetowych są zawsze anonimowe i nigdy nie mogą być z Tobą powiązane.

10.5 Skanowanie treści za pomocą usługi Security Cloud

Usługa Security Cloud skanuje pliki aplikacji w chmurze, aby sprawdzić, czy można ich bezpiecznie używać.

W naszych produktach komputerowych pojedyncze podejrzane aplikacje można przesyłać ręcznie do *Security Cloud* po wyświetleniu odpowiedniego monitu produktu. Funkcja *Security Cloud* nigdy nie przesyła osobistych dokumentów.

10.6 Włączanie funkcji *Security Cloud*

Udostępniając dane zabezpieczeń dotyczące złośliwych programów i witryn internetowych, możesz pomóc nam w ulepszaniu zabezpieczeń oferowanych w ramach działania funkcji *Security Cloud*.

Korzystanie z usługi *Security Cloud* możesz włączyć i wyłączyć w dowolnej chwili w ustawieniach produktu. Nawet jeśli nie chcesz korzystać z usługi Security Cloud, niektóre funkcje produktu muszą się z nią komunikować, aby umożliwić działanie zasubskrybowanej usługi zabezpieczeń. Dane telemetryczne, na przykład częstotliwość korzystania z usługi Security Cloud, sygnatury czasowe i numery wersji bazy danych wirusów będą przesyłane do usługi Security Cloud, nawet jeśli nie chcesz jej używać.

Rezygnacja

Jeśli nie chcesz udostępniać takich danych, funkcja *Security Cloud* nie będzie gromadzić żadnych informacji dotyczących zainstalowanych aplikacji i odwiedzanych witryn. Jednak produkt musi wysyłać do serwerów firmy F-Secure zapytania dotyczące reputacji aplikacji, witryn internetowych, wiadomości i innych obiektów. Zapytania są przeprowadzane przy użyciu kryptograficznej sumy kontrolnej, gdzie sam obiekt, którego zapytanie dotyczy, nie jest wysyłany do firmy F-Secure. Nie śledzimy danych dla poszczególnych użytkowników — tylko liczba zapytań dla pliku lub witryny jest zwiększana.

Całkowite zatrzymanie komunikacji z funkcją *Security Cloud* nie jest możliwe, ponieważ stanowi ona integralną część ochrony zapewnianej przez produkt.

10.7 Pytania dotyczące funkcji *Security Cloud*

Informacje kontaktowe w przypadku jakichkolwiek pytań dotyczących funkcji *Security Cloud*.

Jeśli masz jakiekolwiek inne pytania dotyczące funkcji *Security Cloud*, skontaktuj się z nami:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

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

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