

Outpost Network Security

Outpost Network Security oferowany przez firmę Agnitum to elastyczne rozwiązanie, doskonale zabezpieczające stacje robocze przed zagrożeniami z zewnątrz oraz wewnątrz sieci. Program oferuje szerokie możliwości dobrze znanego personal firewalla firmy Agnitum - Outpost Firewall Pro, zwycięzcy wielu testów w polskich i zagranicznych magazynach komputerowych. Outpost Network Security jako rozwiązanie korporacyjne posiada dodatkowo możliwość centralnej administracji, ułatwiającej zarządzanie ochroną w dużych firmach. Od wersji 2.0 Network Security został uzupełniony o moduł zabezpieczający stacje robocze przed zagrożeniami typu spyware.

Bezpieczeństwo

- doskonale zabezpiecza wszystkie stacje robocze w sieci
- chroni przed zagrożeniami zarówno z zewnątrz jak i wewnątrz sieci
- monitoruje na stacji roboczej wszystkie połączenia przychodzące i wychodzące
- zapewnia ochronę przed zagrożeniami typu spyware z użyciem regularnie aktualizowanej bazy sygnatur

Kontrola

- umożliwia utworzenie różnych profili konfiguracyjnych dla różnych grup użytkowników
- umożliwia centralną aktualizację komponentów programu
- pozwala zmieniać konfigurację zgodnie z wymaganiami polityki bezpieczeństwa firmy

Łatwość użytkowania

- umożliwia centralną instalację oprogramowania przy użyciu narzędzi do zdalnej instalacji
- pozwala na zainstalowanie konsoli do zdalnej administracji na standardowej stacji roboczej

Centralne zarządzanie z jednej konsoli

Agnitum Command Center jest centralnym narzędziem umożliwiającym zarządzanie programem Outpost Network Security Client na wszystkich stacjach roboczych w sieci. Program instalowany jest na serwerze lub dowolnej stacji roboczej zgodnej z wymaganiami systemowymi. Agnitum Command Center obejmuje trzy moduły:

Agnitum Client Computers - konfiguracja programu i reguł

Umożliwia centralną konfigurację oprogramowania na wszystkich stacjach roboczych w sieci z podziałem na różne grupy użytkowników. Plik konfiguracyjny jest udostępniany stacjom roboczym, które po uruchomieniu systemu Windows łączą się z Agnitum Command Center i pobierają plik z najnowszymi ustawieniami. Administrator w dowolnym momencie ma możliwość zmiany konfiguracji oprogramowania, udostępniając stacjom w sieci nowy plik konfiguracyjny.

Agnitum Publisher Service - dystrybucja plików konfiguracyjnych

Jest narzędziem umożliwiającym dystrybucję plików konfiguracyjnych programu Outpost Network Security Client w sieci przedsiębiorstwa.

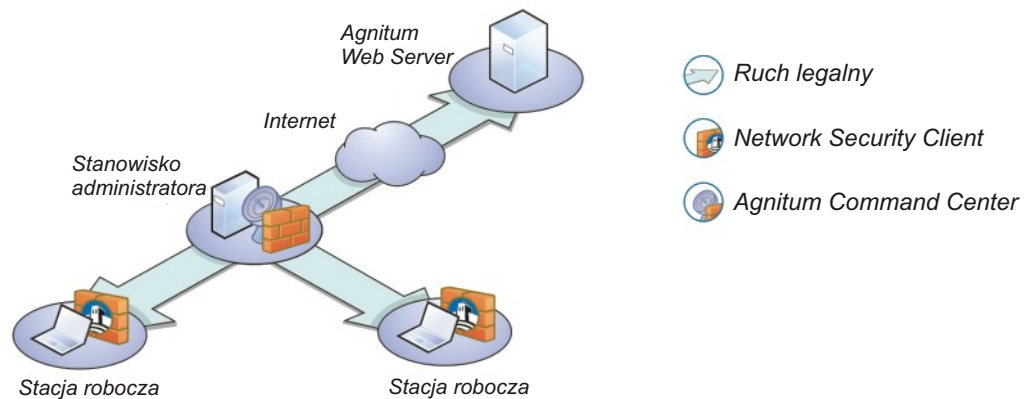
Agnitum Update Service - aktualizacja komponentów

Dużym ułatwieniem dla administratora jest również możliwość centralnej aktualizacji komponentów programu na wszystkich stacjach roboczych w sieci. Pliki aktualizacyjne pobierane są przez Agnitum Update Service do wybranego katalogu, z którego następnie aktualizują się stacje robocze. Ponadto administrator ma możliwość skonfigurowania automatycznej aktualizacji komponentów według harmonogramu. Dostępne są dwie opcje: aktualizacja dzienna oraz tygodniowa. Dodatkowo dostępna jest również opcja aktualizowania komponentów programu ręcznie, na żądanie administratora.

Wymagania systemowe:

Stacje robocze:
Windows
98/ME/2000/XP

Konsola zarządzająca:
Windows
NT/2000/XP/2003



Outpost Network Security Client

Outpost Network Security Client pracujący na stacjach roboczych oferuje poziom ochrony znany z wielokrotnie nagradzanego Outpost Firewalla Pro. Program monitoruje cały ruch przychodzący i wychodzący, kontrolując wszystkie połączenia nawiązywane przez system oraz poszczególne aplikacje i blokując nieużywane porty. Dodatkowo dzięki opcji „Ochrona prywatnych informacji” Outpost blokuje wysłanie poufnych danych (np. haseł dostępu), wysyłając zamiast hasła, nieczytelny tekst w postaci gwiazdek. Firewall oferuje możliwość pracy w trybie ukrytym (stealth mode), a filtrowanie ARP (Address Resolution Protocol) chroni przed podszyciem się intruza pod inne adresy IP w sieci lokalnej, zapewniając także ochronę przed nieautoryzowanymi próbami połączeń w sieciach Wi-Fi.

Ochrona przed spyware

Wtyczka antyspyware zapewnia ochronę przed programami szpiegowskimi wykrywając je na podstawie baz sygnatur spyware, jak również poprzez monitorowanie połączeń. Każde nowe połączenie jest sprawdzane pod kątem legalności i jeżeli zostanie rozpoznane jako spyware jest automatycznie blokowane przez program. Użytkownik dysponuje skanerem rezydentnym oraz skanerem na żądanie. Wykryte programy szpiegowskie są automatycznie blokowane i usuwane, zapewniając bezpieczne surfowanie w sieci.

Inne wtyczki rozszerzające

Outpost Firewall Client oferuje użytkownikom szereg wtyczek (plug-in), podnoszących poziom bezpieczeństwa oferowany przez program oraz wpływających na poprawę jakości pracy podczas korzystania z Internetu. Obecnie dostępne są dodatkowe wtyczki:

- Blokowanie reklam - pozwala blokować irytujące reklamy w Internecie zarówno po ciągu znaków jak również po rozmiarze obrazka reklamowego.
- Filtrowanie aktywnej zawartości - skutecznie blokuje niebezpieczną zawartość stron internetowych jak skrypty Java czy Active X.
- Filtrowanie załączników poczty elektronicznej - wspomaga działanie programu antywirusowego dodatkowo ostrzegając użytkownika przed otwarciem potencjalnie niebezpiecznego załącznika poczty.
- Filtrowanie zawartości - blokuje dostęp do stron internetowych na podstawie adresu (np. www.sex.pl) lub poszczególnych słów w treści strony.
- Pamięć DNS - przechowuje w pamięci adresy ostatnio otwieranych stron WWW wraz z odpowiadającymi im numerami IP.
- Wykrywanie ataków - obejmuje system wizualnych komunikatów o atakach, które są również rejestrowane w Dziennikach zdarzeń, a także umożliwiała blokowanie adresu IP intruza zapobiegając atakom z danego adresu IP w przyszłości.