



# McAfee Host Intrusion Prevention for Servers

## Proaktywnie zabezpieczaj swoje serwery i aplikacje

### KLUCZOWE ZALETY

**Behawioralny system zapobiegania włamaniom (IPS) oraz wykrywanie ataku w oparciu o sygnaturę wirusa**

- Chroni systemy przed nowymi, nieopisanymi wcześniej atakami (Zero Day Attack) oraz dokładnie określa znane zagrożenia

**Zapora sieciowa zintegrowana z systemem**

- Chroni i kontroluje systemy w celu zapobiegania nowym niebezpieczeństwom, z którymi nie poradzi sobie sam program antywirusowy

**Kontrola aplikacji**

- Chroni aplikacje przed wykorzystaniem ich w atakach oraz określa, które aplikacje mogą być instalowane

**Możliwość zarządzania systemem zabezpieczeń**

- Obniżyć koszty oraz podnieść bezpieczeństwo za pomocą pojedynczego zintegrowanego systemu zarządzania bezpieczeństwem na wszystkich stacjach roboczych

### Wyzwanie

Dla działalności firmy kluczowe znaczenie mają serwery. To na nich znajdują się najcenniejsze informacje i to one pozwalają utrzymać ciągłość działania przedsiębiorstwa. Jednym z największych wyzwań stojących przed dyrektorem ds. informatyki jest skuteczna ochrona tych serwerów i aplikacji przed znanymi i nieznanymi formami ataków mogących zakłócić funkcjonowanie całej firmy. Aby zapewnić odpowiednie bezpieczeństwo, należy podejmować szereg działań dla ochrony całej sieci z wykorzystaniem technologii zabezpieczających.

Ataki na słabe punkty serwerów i aplikacji są jednak coraz bardziej złożone i przeprowadzane w agresywny sposób. Stosowane środki zdają się rozwiązywać dany problem tylko na krótki czas. Kluczem do zwycięstwa w tej grze jest wdrożenie proaktywnej strategii bezpieczeństwa, która przede wszystkim zapobiega powstawaniu tych ataków. Stosując proaktywne podejście do zabezpieczania serwerów i aplikacji, możemy być pewni, że nasze poufne dane są odpowiednio chronione, a działalność firmy pozostaje niezakłócona.

### McAfee Host Intrusion Prevention for Servers

Rozwiązanie McAfee Host Intrusion Prevention for Servers (hostowa wersja rozwiązania IPS dla serwerów) monitoruje i blokuje niepożądane działania oraz zapobiega zagrożeniom. Zapewnia ono pracę serwerów bez przestoju oraz chroni takie zasoby firmy, jak aplikacje i bazy danych. Zabezpieczenie to wykorzystuje wiele sprawdzonych metod, łącznie z behawioralnym systemem zapobiegania włamaniom oraz wykrywanie ataków w oparciu o sygnaturę wirusa, systemową zaporę sieciową i kontrolę czy blokowanie aplikacji. Automatycznie aktywowane osłony słabych punktów systemu operacyjnego i poufnych informacji proaktywnie chronią te elementy. Natychmiastowe wprowadzanie poprawek do systemów operacyjnych przestanie być już tak konieczne, a spełnianie wymagań prawnych, którym podlega firma stanie się o wiele łatwiejsze. Hostowa wersja IPS jest łatwa we wdrożeniu, konfiguracji i zarządzaniu.

### Centralne zarządzanie systemami zabezpieczeń

McAfee ePolicy Orchestrator® (ePO™) to wiodące w branży rozwiązanie służące do zarządzania bezpieczeństwem, zapewniające skoordynowaną i proaktywną ochronę firmy przed złośliwymi zagrożeniami i atakami. Przy wykorzystaniu tej centralnej platformy zarządzania McAfee, administratorzy mogą neutralizować zagrożenia pochodzące z niedozwolonych i niezgodnych z polityką systemów, stale aktualizować ochronę, konfigurować i wdrażać politykę bezpieczeństwa oraz monitorować stan zabezpieczeń, 24 godziny na dobę i 7 dni w tygodniu. Wykorzystaj ePO do zarządzania wszystkimi nowymi rozwiązaniami zabezpieczającymi, w tym hostową wersję IPS.

*Konsola ePO ułatwia przeglądanie danych hostowej wersji IPS.*



## WYMAGANIA SYSTEMOWE

### Microsoft Windows (wersja 32-bitowa)

- Windows 2000 Server
- Windows 2000 Professional Server
- Windows 2000 Datacenter Server
- Windows 2000 Advanced Server z dodatkiem SP2 lub późniejszym

### Microsoft Windows (wersja 64-bitowa)

- Windows Server 2003
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Standard Edition
- Windows 2003 Server Web Edition z dodatkiem SP2 lub późniejszym

### Red Hat Linux

- Red Hat Enterprise Linux 4.0
- 32-bitowy system operacyjny Intel i686

### Sun Solaris

- Solaris 8, sun4u (jądro 32-bitowe lub 64-bitowe)
- Solaris 9, sun4u (jądro 32-bitowe lub 64-bitowe)
- Solaris 10, sun4u (tylko wersja 64-bitowa)

### Obsługiwane platformy serwerów WWW:

- Serwer WWW Apache 1.3.6 i wersje późniejsze
- Serwer WWW Apache 2.0.42 i wersje późniejsze
- Sun ONE Web Server 6.0
- Sun Java Web Server 6.1
- IIS 4.0, 5.0 i 6.0 (Windows)

### Obsługiwane platformy serwerów baz danych:

- Microsoft SQL Server 2000 (Windows) SP3a, SP4

## Funkcje i zalety

### Trzy poziomy ochrony

Hostowa wersja IPS stanowi najbardziej kompleksowe rozwiązanie chroniące firmy przed atakami. Behawioralny system ochrony blokuje nowe, nie opisane wcześniej ataki (Zero Day Attack) oraz wymusza odpowiednie zachowanie systemu operacyjnego i aplikacji; sygnatury blokują znane formy ataków i zapewniają administratorom pełną ochronę słabych punktów ich systemów; kontrola aplikacji umożliwia monitorowanie i kontrolowanie dowolnie wybranych aplikacji na serwerach, a zapora sieciowa zapewnia zgodność z politykami dostępu do aplikacji i systemu.

### Behawioralny system zapobiegania włamaniom (IPS) oraz wykrywanie ataków w oparciu o sygnaturę wirusa

Behawioralny system zapobiegania włamaniom zaimplementowany w hostowej wersji IPS, który nie wymaga aktualizacji sygnatur, chroni systemy przed nowymi atakami (Zero Day Attack) skierowanymi w nowe słabe punkty systemów. Funkcje produktu:

- **Uniemożliwienie wykorzystania przepełnienia bufora** – opatentowana technologia wykorzystana w hostowej wersji IPS McAfee zapobiega wykonaniu kodu w wyniku ataków polegających na przepełnieniu bufora (buffer overflow), będących jedną z najczęściej stosowanych metod ataku na serwery.
- **Ochrona słabych punktów** – automatycznie aktualizowana ochrona słabych punktów serwerów zabezpieczająca przed atakami na oprogramowanie i umożliwiająca przetestowanie uaktualnień systemu operacyjnego i aplikacji przed ich wdrożeniem.
- **Ochrona serwerów WWW i serwerów baz danych** – hostowa wersja IPS dla serwerów zawiera unikalne rozwiązania stworzone specjalnie do ochrony serwerów WWW i serwerów baz danych przed takimi atakami, jak ujawnienie plików źródłowych i innych zasobów składowanych lokalnie na serwerze (tzw. „directory traversal”) oraz wykorzystanie luk typu SQL Injection.

### Kontrola aplikacji

Hostowa wersja IPS zapewnia możliwość kontrolowania i monitorowania aplikacji działających na serwerze. Funkcje produktu:

- **Ochrona aplikacji** – uniemożliwia przeniknięcie do aplikacji oraz ich danych lub użycia ich do zaatakowania innych aplikacji, nawet przez użytkownika o uprawnieniach administratora.
- **Blokowanie aplikacji** – hostowa wersja IPS może nie dopuszczać do instalowania aplikacji na serwerach, dzięki czemu można ograniczyć liczbę nieautoryzowanych instalacji. Dzięki funkcji blokowania aplikacji użytkownik jest powiadamiany o nowym oprogramowaniu (niezależnie od tego, czy jest ono dopuszczalne, czy zabronione), dzięki czemu może on śledzić i uniemożliwiać instalowanie nowych aplikacji w otoczeniu serwerowym.

### Zapora sieciowa

Zapora sieciowa z kontrola stanu połączeń (typu „stateful inspection”) dla serwerów Windows® proaktywnie chroni i kontroluje serwery, zapobiegając nowym zagrożeniom, z którymi nie poradzi sobie samo oprogramowanie antywirusowe. Chroni ona serwery w sieci przed atakami skierowanymi na dane, aplikacje lub system operacyjny, wykorzystując kilka poziomów architektury sieciowej i stosując różne kryteria ograniczania ruchu w sieci.