



McAfee Host Intrusion Prevention for Desktops

Proaktywnie chroń punkty końcowe przez zaawansowanymi zagrożeniami

KLUCZOWE ZALETY

Ochrona przed nowymi, nie opisanymi do tej pory zagrożeniami

- Dzięki behawioralnemu systemowi zapobiegania włamaniom oraz wykrywania infekcji w oparciu o sygnaturę wirusa możesz zapobiegać nowym, wcześniej nieznanym zagrożeniom

Kontrola aplikacji

- Ochrona aplikacji przed wykorzystaniem ich w atakach wraz z możliwością określania, które aplikacje mogą być instalowane

Zapora sieciowa zintegrowana z systemem

- Ochrona i kontrola systemów w celu zapobiegania nowym niebezpieczeństwom, z którymi nie poradzi sobie sam program antywirusowy

Możliwość zarządzania systemem zabezpieczeń

- Dzięki pojedynczej zintegrowanej konsoli zarządzania bezpieczeństwem we wszystkich punktach końcowych możesz obniżyć koszty i zwiększać bezpieczeństwo

Wyzwanie

Zarządzanie ochroną oraz kontrolowanie łączności pomiędzy komputerami stacjonarnymi i laptopami w całej organizacji stanowi nie lada wyzwanie dla działu informatycznego. Poprzez swoje komputery pracownicy nieumyślnie wprowadzają do firmowej sieci robaki, programy szpiegujące oraz powodują inne zagrożenia. Systemy te często stanowią także cel hakerów wykradających informacje oraz atakujących inne wewnętrzne serwery, czy bazy danych. Może to doprowadzić do wycieku danych, narazić pracowników na niebezpieczeństwo oraz obniżyć wydajność całej firmy.

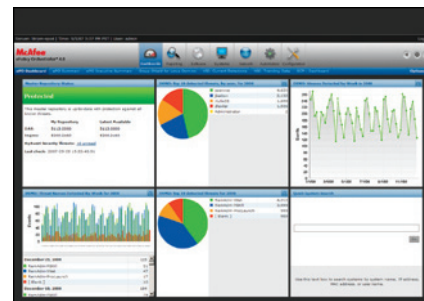
Jednym z największych wyzwań stojących przed szefem działu informatyki jest skuteczna ochrona stacji roboczych oraz zapobieganie znanym i nieznanym formom ataków, zanim staną się one powodem poważnych szkód. Jednakże ataki te są coraz bardziej agresywne i złożone. Najlepszym rozwiązaniem jest wdrożenie proaktywnej strategii bezpieczeństwa, która przede wszystkim zapobiega powstawaniu tych ataków. Stosując proaktywne podejście do zabezpieczania stacji komputerowych, możemy być pewni, że nasze poufne dane są odpowiednio chronione, a działalność firmy pozostaje niezakłócona.

McAfee Host Intrusion Prevention for Desktops

McAfee® Host Intrusion Prevention for Desktops (hostowa wersja IPS dla stacji roboczych) chroni zasoby za pomocą sprawdzonych metod obejmujących behawioralny system zapobiegania włamaniom oraz wykrywanie infekcji w oparciu o sygnaturę wirusa, kontrolę blokowania aplikacji oraz zaporę sieciową z kontrolą stanu połączeń (typu „stateful inspection”). Automatyczne aktualizacje sygnatur oraz ochrona przed nowymi, wcześniej nieznanymi zagrożeniami zapewniają wymaganą, zaawansowaną ochronę słabych punktów systemu. Częste wprowadzanie poprawek do systemów operacyjnych przestanie być już tak konieczne, a spełnianie wymagań prawnych, którym podlega organizacja stanie się o wiele łatwiejsze. Dzięki pojedynczemu programowi typu agent, zajmującemu się wykrywaniem intruzów na poziomie hosta oraz zapory sieciowej na komputerach, hostowa wersja IPS McAfee jest łatwa do wdrożenia, skonfigurowania i zarządzania.

Możliwość zarządzania systemem zabezpieczeń organizacji

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



Konsola ePO ułatwiająca przeglądanie danych hostowej wersji IPS dla stacji roboczych

WYMAGANIA SYSTEMOWE

Microsoft Windows®
(w języku angielskim, francuskim, niemieckim, hiszpańskim, japońskim, koreańskim i chińskim tradycyjnym)

- Windows XP Home z dodatkiem Service Pack 2
- Windows XP Professional z dodatkiem Service Pack 2
- Windows XP Tablet PC
- Windows Vista, wersja 32-bitowa i 64-bitowa

Funkcje i zalety

Proaktywna ochrona

Hostowa wersja IPS dla stacji roboczych zapewnia najbardziej kompleksowe rozwiązanie chroniące firmy przed atakami.

Behawioralny system ochrony

Behawioralny system ochrony blokuje ataki z wykorzystaniem nowych, wcześniej nieznanymi luk (tzw. Zero Day Attacks) oraz wymusza odpowiednie zachowanie systemu operacyjnego i aplikacji; sygnatury blokują znane formy ataków i zapewniają administratorom pełną informację na temat słabych punktów ich systemów oraz możliwych zagrożeń, a zapora sieciowa zapewnia zgodność z polityką dostępu do aplikacji i systemu.

- **Uniemożliwienie wykorzystania przepełnienia bufora** – opatentowana technologia hostowej wersji IPS McAfee zapobiega wykonaniu kodu na skutek ataków polegających na przepełnieniu bufora (buffer overflow).
- **Ochrona aplikacji** – uniemożliwia przeniknięcie do aplikacji oraz ich danych lub użycia ich do zaatakowania innych aplikacji, nawet przez użytkownika o uprawnieniach administratora.

Ochrona w oparciu o sygnaturę wirusa

Ochrona realizowana przez hostową wersję IPS w oparciu o sygnaturę wirusa dokładnie określa i blokuje znane formy ataku oraz znacznie zmniejsza liczbę błędnych klasyfikacji potencjalnych zagrożeń. Funkcje produktu:

- **Ochrona słabych punktów** – automatycznie aktualizowana ochrona słabych punktów na komputerach zabezpieczająca przed atakami i umożliwiająca przetestowanie uaktualnień przed ich wdrożeniem.
- **Ochrona aplikacji na komputerach stacjonarnych** – programy typu agent na komputerach stacjonarnych zawierają unikalne funkcje ochrony dla często używanych aplikacji, tj. Internet Explorer i Microsoft® Outlook.

Zapora sieciowa na komputerach stacjonarnych

Zapora sieciowa z kontrolą stanu połączeń (typu „stateful inspection”) zawarta w hostowej wersji IPS proaktywnie chroni i kontroluje komputery stacjonarne i laptopy, zapobiegając nowym zagrożeniom, z którymi nie poradzi sobie samo oprogramowanie antywirusowe. Funkcje produktu:

- **Rozróżnianie rodzajów połączenia** – możliwość stosowania różnych poziomów ochrony w zależności od tego, gdzie i jak system jest podłączony do sieci. Przykładowo, można określić bardzo rygorystyczne zasady dla użytkowników podłączających się bezpośrednio do Internetu i mniej rygorystyczne dla tych, którzy są podłączeni do domeny firmowej.
- **Izolacja połączenia** – możliwość blokowania całego ruchu do i z niezabezpieczonych sieci, podczas gdy użytkownicy podłączają się do krytycznych sieci, np. do firmowej sieci LAN.
- **Tryb kwarantanny** – zapobiega zainfekowaniu sieci przez słabo zabezpieczone stacje komputerowe. Przy współpracy z McAfee Agent, hostowa wersja IPS porównuje lokalne zasady polityki z obecnie przypisanymi przez ePO i ogranicza dostęp do sieci, jeśli dany użytkownik korzysta ze starych lub nieaktualnych zasad polityki.
- **Obsługa IPv6** – zapora sieciowa obecnie obsługuje protokół IP v6 „nowej generacji” będący integralną częścią systemu Windows Vista.

Kontrola aplikacji

Jako dodatkowy poziom ochrony hostowa wersja IPS dla stacji roboczych zapewnia możliwość kontrolowania, które aplikacje mogą pracować, a które nigdy nie powinny działać na danym komputerze. Jako, że tego rodzaju ochrona tworząca „białe i czarne listy aplikacji” jest czuła na działanie automatycznych uaktualnień (łatek) i aktualizacji, blokowanie aplikacji jest najlepszym rozwiązaniem dla systemów wymagających nadzwyczajnej ochrony oraz tych, które są użytkowane w bardzo ukierunkowany i stabilny sposób, np. kioski informacyjne.