



McAfee Enterccept Standard Multi-Platform Server Agent

Ochrona krytycznych systemów przed włamaniami

Wyzwanie

Z roku na rok wykrywanych jest coraz więcej luk w zabezpieczeniach, wzrasta również szybkość, z jaką atakujący mogą łamać zabezpieczenia systemów o znaczeniu krytycznym. Dostępność i integralność systemów oraz poufność danych są coraz bardziej zagrożone. Konwencjonalne programy antywirusowe i systemy wykrywania włamań działają w sposób interwencyjny i nie chronią przed atakami nieznanymi (klasy „zero-day”), wykorzystującymi nowo odkryte luki w zabezpieczeniach. Ponadto wszystkie firmy, niezależnie od wielkości, muszą przestrzegać przepisów mówiących o konieczności ochrony poufnych danych i kontrolowania dostępu do systemów i aplikacji.

Aby prewencyjnie chronić systemy przed dzisiejszymi zaawansowanymi atakami, przedsiębiorstwa powinny wdrażać wielowarstwowe zabezpieczenia przed włamaniami. System McAfee® Enterccept® zapewnia najbardziej kompleksową, najdokładniejszą i najbardziej rozszerzalną ochronę przed włamaniami spośród wszystkich rozwiązań dostępnych na rynku. Pozwala przedsiębiorstwom zmniejszyć ryzyko, zapewnić ciągłość działania firmy i obniżyć całkowity koszt posiadania.

Rozwiązanie McAfee Enterccept

Wieloplatformowe agenty systemu Enterccept Standard wykorzystują opatentowaną, wyróżnianą technologię do zabezpieczania systemów przed atakami nieznanymi (klasy „zero-day”) oraz przed zagrożeniami znanymi. Każdy z tych centralnie zarządzanych agentów skutecznie blokuje ataki, wykorzystując rozbudowany zestaw technologii ochrony przed włamaniami.

- Reguły zachowań chronią przed atakami klasy „zero-day” wykorzystującymi nowo wykryte luki w zabezpieczeniach. Nie wymagają uaktualnień.
- Sygnatury zabezpieczają hosty, dokładnie identyfikując niebezpieczny ruch znanych typów, co znacznie zmniejsza liczbę przypadków błędnego rozpoznania zagrożeń.
- Zapora systemowa (tylko w wersjach do systemu Windows®) kontroluje dostęp do systemu i aplikacji, blokując ruch przychodzący i wychodzący na podstawie kontroli adresu IP, protokołu lub portu.

Korzyści

Kompleksowa ochrona

- Blokuje ataki klasy „zero-day” nie wymagając uaktualnień, co znacznie zmniejsza potrzebę szybkiego wdrażania programów korygujących (tzw. poprawek) w przypadku wykrycia nowych zagrożeń.
- Uzupełniające się technologie zapewniają dostępność, integralność oraz poufność danych i serwerów.
- System zapobiegania włamaniom i zapora systemowa chronią przed atakami aplikacje o znaczeniu krytycznym.



System McAfee Enterccept zapobiega atakom znanym i nieznanym wykorzystując reguły zachowań, sygnatury i zaporę systemową.

Dokładność

- Definiując „zaufane oprogramowanie”, firmy unikają błędnego rozpoznawania zagrożeń w aplikacjach o znaczeniu krytycznym.
- Sygnatury umożliwiają szczegółowe opisanie zdarzeń wraz z informacjami o szczegółach ataku.
- Wstępnie skonfigurowane, dostosowywane reguły zmniejszają liczbę przypadków błędnego rozpoznawania zagrożeń i umożliwiają wykorzystanie cennych umiejętności specjalistów ds. zabezpieczeń do innych zadań.

Rozszerzalność

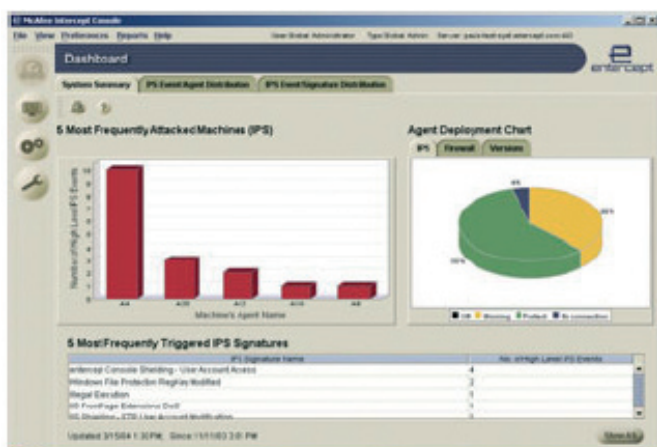
- Jeden system umożliwia zarządzanie nawet 10 tys. agentów.
- Możliwość opcjonalnego zarządzania za pośrednictwem programu McAfee ePolicy Orchestrator® 3.x.
- Niewidoczna instalacja i uaktualnianie bez restartu systemu gwarantują nieprzerwaną ochronę.
- Poziomy ochrony można dostosowywać — od rejestrowania po blokowanie ruchu.

Jak działa system McAfee Enterccept

Każdy agent systemu Enterccept ma w pełni skonfigurowany domyślny szablon reguł ochrony, co zapewnia bezpieczeństwo od razu po uruchomieniu systemu. Ponadto agenty mają rozbudowane funkcje konfiguracyjne, które umożliwiają specjalistom ds. zabezpieczeń tworzenie i dostrajanie reguł odpowiadających wymaganiom konkretnego środowiska. Zmniejsza to liczbę przypadków błędnego rozpoznawania zagrożeń.

McAfee®

Agent bada określone odwołania do systemu operacyjnego i interfejsu programowania API wykorzystywane przez wszystkie aplikacje do zgłaszania żądania obsługi do systemu operacyjnego. Szybko i efektywnie porównuje swoje reguły zachowań i sygnatury znanych ataków z informacjami o każdym odwołaniu (takimi jak proces zgłaszający odwołanie, kontekst zabezpieczeń tego procesu, zasoby, do których żąda dostępu, itd.). Następnie blokuje wszystkie odwołania związane z podejrzanym zachowaniem lub szkodliwym kodem.



Konsola zarządzania systemu *Entercept* przedstawia w czytelnej i zwężonej formie zagrożenia oraz status systemu.

Najważniejsze funkcje

Zapobieganie nieznanym atakom (klasy „zero-day”) — *Entercept* zapobiega nowym, wcześniej nieznanym atakom, wykorzystując efektywne reguły zachowań. Pozwalają one bez uaktualnień egzekwować prawidłowe zachowanie systemu operacyjnego i aplikacji oraz blokować nowe ataki naruszające reguły.

Zapobieganie przepełnieniu bufora — Opatentowana technologia uniemożliwia wykonanie kodu w wyniku przepełnienia bufora. Agenty chronią najważniejsze serwery przed atakami wykorzystującymi tę technikę, które są najczęstszym źródłem zagrożeń dla serwerów.

Zapobieganie znanym atakom — Blokuje znane zagrożenia oraz zapobiega powstaniu szkód w systemie, porównując jego aktywność z informacjami o znanych atakach pochodzącymi z obszernej bazy danych. Agenty automatycznie wyszukują uaktualnienia z sygnaturami nowych ataków.

Ochrona zasobów — Chroni dostępność, integralność i poufność systemu, blokując dostęp do najważniejszych zasobów (plików, ustawień, kluczy rejestru, usług itd.).

Zapora systemowa (tylko w wersjach do systemu Windows) — Blokuje ruch przychodzący i wychodzący za pomocą drobnoziarnistego filtra pakietów oraz zapory. Blokowanie może następować na podstawie analizy portów, protokołów i adresu IP.

Ochrona serwera WWW i serwera bazy danych osłonami i otoczkami — Technologia ta zapobiega penetracji z zewnątrz i niewłaściwemu wykorzystaniu zasobów aplikacji o znaczeniu krytycznym (plików, użytkowników, rejestru itd.). Otoczka uniemożliwia chronionym aplikacjom szkodliwą aktywność, wykraczającą poza normalne zachowanie (np. dostęp do danych innych aplikacji).

Ochrona HTTP i SQL — Ochrona HTTP blokuje ataki na serwery WWW firm Apache, Sun lub Microsoft®, wykorzystując unikatowy mechanizm analizy składniowej protokołu http. Ochrona SQL zabezpiecza serwery SQL 2000 przed atakami typu SQL Injection (wstrzykiwanie kodu SQL), wykorzystując unikatowy mechanizm zapytań SQL.

Wdrażanie i monitorowanie za pośrednictwem systemu McAfee ePO™ 3.x — Opcje instalowania, uaktualniania i monitorowania agentów.

Wymagania systemowe

Windows (tylko wersje angielska, francuska i niemiecka)
Wersja dla Polskich systemów operacyjnych dostępna w 2006.

- Windows 2003 Server
- Windows XP SP2
- Windows 2000 Server i Advanced Server
- Windows NT 4 Server lub Enterprise Server, SP 6a
- Microsoft SQL Server 2000
- Microsoft IIS 4, 5 i 6

Sun

- Solaris 7, 8 i 9 (jądro 32-bitowe i 64-bitowe)
- Sun ONE/iPlanet 3.6, 4.0, 4.1 i 6.0

HP-UX

- HP-UX II.0, Ili (64-bitowy procesor PA-RISC)

Apache

- Apache 1.3.6 lub nowszy, 2.0.42 lub nowszy

McAfee PrimeSupport

Program McAfee PrimeSupport® jest elementem niezbędnym do maksymalnego wykorzystania inwestycji w rozwiązania do ochrony systemów i sieci firmy McAfee. Zespół PrimeSupport dysponuje wszelkimi niezbędnymi zasobami i jest gotowy do świadczenia usług wymaganych przez klienta. W ramach programu PrimeSupport można korzystać m.in. z dostępu do wszystkich wersji serwisowych i uaktualnień produktów oraz do kompleksowego zestawu dodatkowych internetowych mechanizmów samopomocy, telefonicznej pomocy technicznej dostępnej przez 24 godziny na dobę i 7 dni w tygodniu, pomocy wyznaczonych opiekunów klienta ds. pomocy technicznej oraz szeregu innych usług pomocy technicznej w zakresie sprzętu i oprogramowania, które można dostosować do potrzeb klienta.