



McAfee Vulnerability Manager (Foundstone)

Określaj zagrożenia oraz przypadki naruszenia polityki bezpieczeństwa, ustalaj ważność zasobów oraz ograniczaj ryzyko do minimum

Szybko i skutecznie znajduj słabe punkty oraz przypadki naruszenia zasad obowiązującej polityki i określaj je pod względem ważności we wszystkich systemach podłączonych do sieci. Odpowiednio oceniaj wartość zasobów, stopień narażenia na ataki, skalę zagrożeń oraz dostępne środki zaradcze w celu zabezpieczenia najważniejszych zasobów firmy.

KLUCZOWE ZALETY

Podejmuj decyzje oparte na rzetelnych informacjach

- Połączone informacje na temat słabych punktów, zasobów i środków zaradczych
- Inteligentna analiza i korelacja zagrożeń
- Elastyczne raporty dostosowane do indywidualnych potrzeb oraz gotowe raporty audytowe

Efektywność operacyjna

- Audyty zgodności z obowiązującymi regulacjami i polityką bez wykorzystania programów typu agent
- Automatycznie wykrywaj słabe punkty i naruszenia zasad obowiązującej polityki oraz określaj je pod względem ważności
- Dokładne rozpoznanie słabych punktów oraz wersji systemu operacyjnego
- Eliminuj niepoprawne uaktualnienia

Skalowalne rozwiązanie zabezpieczające dla przedsiębiorstw

- Skanuj i chroń sieć o dowolnej wielkości
- Obsługa IPv6

Większe korzyści dzięki integracji

- Integracja z innymi produktami McAfee zapewniająca:
 - Zbieranie danych na temat słabych punktów z różnych źródeł
 - Zautomatyzowane wprowadzanie poprawek i środków naprawczych
 - Sieciowy system zapobiegania włamaniom (IPS)

Priorytetowe zarządzanie ryzykiem

Jak minimalizować ryzyko i chronić najważniejsze zasoby przedsiębiorstwa przed ciągle zmieniającymi się formami ataków i zagrożeń? Gdzie kierować działania związane z informatyką i bezpieczeństwem? Gdzie są one najbardziej potrzebne? Jak usprawnić pracę i wykazać zgodność z regulacjami w trakcie audytu?

Podejmuj decyzje na temat bezpieczeństwa na podstawie rzetelnych informacji za pomocą priorytetowego podejścia McAfee® Vulnerability Manager. Vulnerability Manager zwiększa dokładność i przydatność informacji na temat zagrożeń, słabych punktów, zasobów i krytyczności zagrożeń. To specjalistyczne, bezpieczne urządzenie zwiększa efektywność obecnych zasobów, zapewniając niskie koszty utrzymania. Można je integrować z pozostałymi produktami McAfee oraz technologiami innych firm w celu odpowiedniego wykorzystania poczynionych inwestycji oraz zwiększenia korzyści wynikających z zapewnienia ochrony i zgodności z przepisami, tak aby uzyskać system zabezpieczania przed włamaniami IPS, monitorowanie poziomu ryzyka, dostępność różnych środków zaradczych oraz szybsze rozwiązywanie problemów.

System umożliwia sprawdzanie zgodności z najważniejszymi przepisami krajowymi i branżowymi, wykorzystując do tego szablony dotyczące następujących regulacji: Sarbanes-Oxley Act (SOX), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), BS7799/ISO27002 oraz standard Payment Card Industry Data Security Standard (PCI DSS) i inne. Nasze szablony pomogą sprawdzić, które systemy nie są zgodne, zanim przybędą audytorzy.

Szeroki i dokładny zakres kontroli

Vulnerability Manager zapewnia szeroki zakres możliwej kontroli słabych punktów systemu informatycznego oraz przypadków naruszenia obowiązujących regulacji. System ten pozwala szybko i dokładnie określać wpływ powstających zagrożeń i słabych punktów na stopień ryzyka charakterystyczny dla firmy. Dzięki temu łatwiej i dokładniej będzie ona spełniać wymagania obowiązujących przepisów i polityki. W rzeczywistości Vulnerability Manager zapewnia użytkownikom narzędzia sprawdzania zgodności z obowiązującą polityką bez potrzeby wykorzystywania programów typu agent oraz dodatkowego oprogramowania lub konsoli zarządzania.

Vulnerability Manager to jedyny skaner sieciowy wykorzystujący technologię McAfee ePolicy Orchestrator® (ePO™) – naszą sprawdzoną, scentralizowaną konsolę zarządzania obsługującą ponad 50 milionów instalacji w przedsiębiorstwach na całym świecie. Jako że dane ePO zapewniają pełniejszy obraz systemu w celu wykonywania dokładniejszego badania, redukujemy pośpiech związanych z aktualizacjami i tylko najbardziej wrażliwe systemy wymagają szybkiego uaktualnienia.

OPCJE WDRAŻANIA

Dedykowane i bezpieczne urządzenia

- Vulnerability Manager 1000 i Vulnerability Manager 850
- Enterprise Manager
- Bazy danych na temat słabych punktów i zasobów
- Scan Engine
- Report Engine

Tylko oprogramowanie

- Zainstaluj na własnym sprzęcie; zestaw obejmuje aplikację Enterprise Manager, bazę danych na temat słabych punktów i zasobów oraz Scan Engine

Minimalne wymagania

Sprzęt

- Procesor: Dual Xeon 2 GHz, Dual Core Xeon 2,33 GHz lub wyższy
- RAM: 2 GB
- Wolne miejsce na dysku: partycja 80 GB
- Interfejs sieci Ethernet

System operacyjny

- Microsoft Windows 2000 Server z Service Pack 4
- Microsoft Windows 2003 Server Standard Edition z Service Pack 1

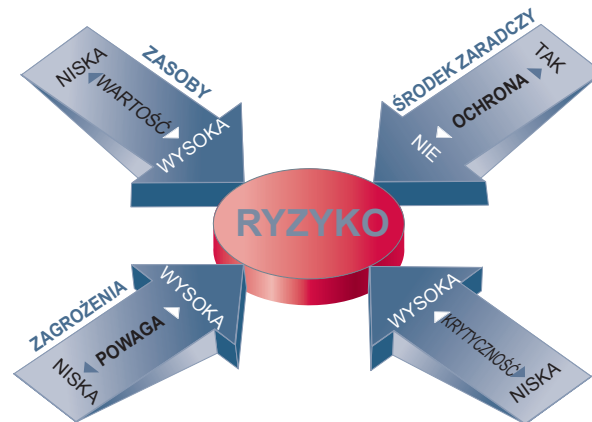
Baza danych

- Microsoft SQL Server 2005 z Service Pack 1 lub SQL Server 2000 z Service Pack 4
- Wszystkie poprawki hotfix i łatki SQL

Zintegrowany i kompleksowy mechanizm naprawczy

Potrzebujesz zainstalować aktualizacje? McAfee Remediation Manager automatycznie naprawia wszystkie słabe punkty i przypadki naruszenia polityki zidentyfikowane przez Vulnerability Manager. A może chcesz blokować zagrożenia na poziomie sieci? McAfee Network Security Platform (poprzednia nazwa IntruShield®) koreluje dane Vulnerability Manager i wykonuje skanowanie na żądanie, aby zsynchronizować ochronę sieci w zależności do aktualnego poziomu ryzyka.

Niezależnie od tego, jaki sposób działania Vulnerability Manager zostanie wybrany – bezobsługowe i bezpieczne urządzenie albo oprogramowanie umożliwiające korzystanie z własnych serwerów – nasze priorytetowe podejście zapewnia pełną kontrolę nad „cyklem życia” zarządzania ryzykiem. Co więcej, Vulnerability Manager dostosowuje się do największych i najbardziej złożonych sieci globalnych, dostarczając niezwykle elastycznych narzędzi do tworzenia raportów, które zadowolą każdego użytkownika.



Funkcje

Priorytetowe audyty i środki naprawcze

- Przeprowadzaj oceny w odniesieniu do wdrożonych polityk bezpieczeństwa, określaj najcenniejsze zasoby, wskazuj najważniejsze słabe punkty oraz stosuj środki naprawcze w celu ograniczenia najbardziej krytycznych zagrożeń.
- Importuj dane o zainstalowanej ochronie przed przepełnieniem bufora z zainstalowanej ochrony systemowej (ePO) w celu ograniczenia ilości natychmiastowych aktualizacji podczas kryzysu, które pozwala na skupienie się na najważniejszych słabych punktach.

Kompleksowe kontrole słabych punktów i reguł

- Lokalizuj niezarządzane urządzenia, takie jak obce bezprzewodowe punkty dostępu lub zapomniane wirtualne systemy VMware w swojej sieci.
- Szablony dostosowywane do indywidualnych potrzeb sprawdzają zgodność z SOX, PCI DSS, HIPAA, ISO27002, FISMA oraz przepisami Federal Desktop Core Configuration (FDCC).
- Foundstone Scripting Language (FSL) umożliwia specjalistom programowanie niestandardowych kontroli bezpieczeństwa w celu przetestowania własnych programów.
- Otrzymuj kompleksowe, natychmiastowe i nieprzerwane wsparcie dotyczące pojawiających się słabych punktów od McAfee Avert® Labs – najbardziej szanowanego na świecie centrum badań nad zagrożeniami w sieci.

Łatwiejsze zapewnianie zgodności z polityką bezpieczeństwa

- Udostępniaj użytkownikom rozszerzone opcje skanowania poprzez gotowe sprawdzenia reguł polityki bezpieczeństwa, których wyniki są zapisywane i przedstawiane w formie raportów.
- Określaj specyficzne parametry nowych sprawdzeń polityki za pomocą łatwego w użyciu interfejsu w formie kreatora.

Konfigurowana identyfikacja zasobów w oparciu o określone charakterystyki

- Automatycznie grupuj i lokalizuj zasoby w odniesieniu do rodzaju urządzeń (serwer WWW, stacja robocza, serwer pocztowy), typu systemu operacyjnego, zakresu adresu IP, nazw hosta, nazw DNS lub innych zasad.

Elastyczne raportowanie

- Otrzymuj raporty z podziałem na dane platformy, jednostki biznesowe, lokalizację geograficzną i zakres IP w celu uzyskania informacji na temat łamania zasad danej polityki, słabych punktów, stosowania środków naprawczych oraz zmian stanu ryzyka.
- Gotowe szablony dotyczące przepisów, standardów oraz regulacji krajowych i branżowych znacznie ułatwiają proces zapewniania zgodności.

**OPCJE
WDRAŻANIA
(ciąg dalszy)**

Aplikacje dodatkowe

- Vulnerability Manager obsługuje następujące aplikacje:
 - FSDBUTIL
 - Otwarte API/SDK
 - Narzędzia certyfikacji
 - FSUpdate
 - ERM

„Rozwiązanie Vulnerability Manager, wprowadzające priorytetowe podejście do zarządzania ryzykiem w naszej sieci, umożliwiło firmie CSU w Chico znacznie ograniczyć ryzyko oraz zwiększyć ogólny poziom bezpieczeństwa firmy.”

*Jason Musselman,
analityk ds. bezpieczeństwa danych,
CSU, Chico*

Więcej informacji na ten temat znajduje się na stronie www.mcafee.com.

- Przeglądanie wyników audytów przeprowadzanych bez programów zainstalowanych na urządzeniach końcowych, dotyczących zgodności z polityką bezpieczeństwa dla systemów Windows® i Unix z elastycznymi i szczegółowymi opcjami raportowania.
- Tworzy szczegółowe sprawozdania dotyczące zgodności z przepisami, np. ogólny stan zgodności, stan zgodności pojedynczego hosta oraz stan zgodności dla danej polityki.
- Wskaźnik FoundScore pomaga zrozumieć, przeanalizować profil ryzyka w danym czasie i stworzyć sprawozdanie na jego temat, pokazując zmiany w odniesieniu do skanowania, poziomu ryzyka, słabych punktów i platformy.

Wysoce skalowalna, otwarta architektura

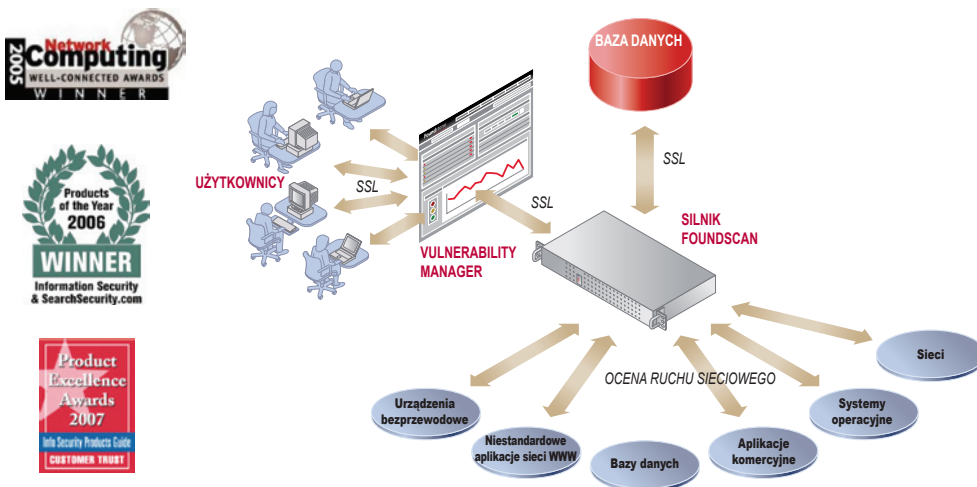
- Rozproszona architektura Vulnerability Manager: skaner, system zarządzania oraz baza danych Vulnerability Manager są zaprojektowane z myślą o środowisku Twojej firmy.
- Funkcje tego systemu obejmują wykrywanie zasobów, zarządzanie, skanowanie i raportowanie.

Dokładna identyfikacja systemu operacyjnego i słabych punktów oraz natychmiastowa ocena zagrożeń

- Importuj dane na temat zasobów i systemu operacyjnego z ePO do bazy danych Vulnerability Manager w celu zapewnienia lepszej ochrony i 100% dokładności, co umożliwia poprawne wprowadzanie uaktualnień.
- Identyfikuj zasoby chronione już za pomocą innych mechanizmów, aby skupić działania naprawcze na zasobach bardziej narażonych na atak oraz ograniczyć ilość koniecznych natychmiastowych uaktualnień.
- Bez wykonywania ponownego skanowania całej sieci, Vulnerability Manager w ciągu kilku minut może przeprowadzić wizualizację i sklasyfikować potencjalne zagrożenia, korelując informacje o najnowszych zagrożeniach z istniejącymi danymi na temat zasobów i słabych punktów systemów.
- Skanowanie platform Microsoft® Windows, UNIX, Cisco IOS i VMware za pomocą podanych uprawnień lokalnych wykazuje słabe punkty oraz przypadku naruszenia obowiązującej polityki z największą dokładnością w całej branży.

Efektywność operacyjna

- Scentralizowane zarządzanie skanowaniem umożliwia przyspieszenie procesu skanowania, eliminując konieczność wyboru określonego silnika skanującego dla danego zadania skanowania.
- Poprzez synchronizację zasobów z Lightweight Directory Access Protocol (LDAP) i Active Directory (AD), można skonfigurować wiele serwerów LDAP dla Vulnerability Manager w celu importowania informacji na temat zasobów, aby ograniczyć czas wykorzystywany przez administratorów na tworzenie struktur zasobów przeznaczonych do skanowania.
- Uaktualniaj, konfiguruj i monitoruj i zarządzaj całym procesem wdrażania rozwiązania Vulnerability Manager w scentralizowany i jednolity sposób za pomocą Configuration Manager.
- Otrzymuj automatyczne aktualizacje oprogramowania i konfiguracji, dane dotyczące stanu systemu oraz powiadomienia poprzez pocztę e-mail.
- Zarządzaj certyfikatami za pomocą pojedynczej konsoli zarządzania.





McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee i/lub inne powiązane produkty McAfee opisane w niniejszym dokumencie są zastrzeżonymi znakami towarowymi lub znakami towarowymi McAfee Inc. i/lub jej podmiotów zależnych w Stanach Zjednoczonych i/lub w innych krajach. Kolor czerwony w połączeniu z zabezpieczeniami jest wyróżniającą cechą produktów marki McAfee. Pozostałe produkty niezwiązane z McAfee i/lub zastrzeżone i niezastrzeżone znaki towarowe zostały wymienione w niniejszej publikacji tylko w celach referencyjnych i są wyłączną własnością odpowiednich podmiotów.
© 2008 McAfee, Inc. Wszelkie prawa zastrzeżone.

1-cor-fs-ent-virt-002-0108