

## McAfee Vulnerability Manager

Beazonosítja a fenyegetéseknek való kitettségeket és a biztonsági irányelvek megsértését, rangsorolja az erőforrásokat és csökkenti a kockázatot

A Vulnerability Manager gyorsan és pontosan megtalálja és rangsorolja a sérülékenységeket és az irányelvek megsértését valamennyi hálózatra kötött rendszerén. Az eszköz értékének, a sérülékenység súlyosságának, a fenyegetés kritikusságának és az ellenintézkedéseknek a mérlegelésével a védelmet a legfontosabb eszközökre összpontosítja.

### Jellemzők

#### Tájékozott döntéshozatal

- A sérülékenységekkel, eszközökkel és ellenintézkedésekkel kapcsolatos kombinált információk
- Fenyegetés-felderítés és -összevetés
- Személyre szabható jelentéskészítés és előre meghatározott ellenőrzés-jelentések

#### Hatékony működés

- Kliens program nélküli irányelv-megfelelőségi ellenőrzés
- A sérülékenységek és az irányelv-megsértések automatikus felderítése és rangsorolása
- A sérülékenységek és az operációs rendszerek pontos meghatározása
- A javítócsomagok nem megfelelő telepítésének kiküszöbölése

#### Integrálás egyéb McAfee-termékekkel

- Egységes IT-irányelv értékelés
- A javítócsomagok automatikus telepítése és automatikus helyreállítás
- Hálózatalapú behatolás-megelőzés

### Prioritásalapú kockázatkezelés

Hogyan tudja mérsékelni a kockázatokat és megvédeni legértékesebb eszközeit a változó sérülékenységekkel és fenyegetésekkel szemben? Hogyan irányítja az IT- és a biztonsági erőfeszítéseit, amikor és ahol azokra a leginkább szükség van? Hogyan javíthatja a munkafolyamatot és igazolhatja magabiztosan a megfelelőséget az ellenőrzéskor?

Hozzon tájékozottabb biztonsági döntéseket a McAfee Vulnerability Manager (korábban: McAfee Foundstone Enterprise) prioritásalapú megközelítését alkalmazva! A Vulnerability Manager a sérülékenységekkel, az eszközökkel és a fenyegetések kritikusságával kapcsolatos információk kombinálása révén javítja a biztonsági információk pontosságát és hasznosságát. Kipróbált alkalmazásaink növelik meglévő erőforrásainak hatékonyságát, ezáltal alacsony tulajdonlási költséget eredményeznek. A megoldás integrálható egyéb McAfee-termékekkel, valamint harmadik felek technológiájával is, megnövelve beruházásainak értékét, kibővítve a védelem nyújtotta előnyöket és a kockázat-érzékeny behatolás-megelőzésnek, az egységes IT-irányelv ellenőrzésnek, az ellenintézkedések tudatosságának, valamint a problémamegoldásnak való megfelelést.

Mérje fel az általános rendeleteknek és biztonsági szabványoknak való megfelelést a Sarbanes-Oxley törvényhez (SOX), a szövetségi információvédelem-kezelési törvényhez (Federal Information Security Management Act – FISMA), az egészségbiztosítási átvihetőség és elszámoltathatóság törvényéhez (Health Insurance Portability and Accountability Act – HIPAA), a Federal Desktop Core Configuration (FDCC) alapkonzfigurációhoz, a BS7799/ISO27002 szabványhoz, valamint a Fizetőkártya-üzletág adatbiztonsági szabványához (Payment Card Industry Data Security Standard – PCI DSS) készült sablonokkal. Sablonjaink segítségével még az ellenőrök érkezése előtt ellenőrizheti, hogy mely rendszerei nem teljesítik a megfelelőség követelményeit.

### A tartalom széleskörű és pontos lefedése

A Vulnerability Manager az IT-sérülékenységek és a biztonsági irányelvek megsértése ellenőrzésének széles választékát kínálja. Azonnal és pontosan meghatározza, hogy az újonnan felbukkanó fenyegetések és sérülékenységek hogyan hatnak az Ön biztonsági profiljára. Valójában a Vulnerability Manager kliens program nélküli, ún. agentless irányelv-megfelelőségi ellenőrzést kínál felhasználói számára, anélkül, hogy ehhez további szoftvereket vagy irányítókonsolekat kellene telepíteni. A megoldás a kezelt (agent) és a nem kezelt (agentless) rendszerek egyszerűsített ellenőrzése érdekében integrálható az ePO-val és a McAfee Policy Auditorral is.

A Vulnerability Manager az egyetlen olyan hálózati letapogató eszköz, amely felhasználja a világszerte több mint 58 millió telepítéssel rendelkező, a már bizonyított központosított menedzsmentkonzol, a McAfee ePolicy Orchestrator (ePO) eszközinformációit is. Az ePO adatai jóval teljesebb képet nyújtanak a rendszerről a pontosabb értékeléshez, ezáltal csökkentve a sürgős beavatkozás szükségességét, így elegendő, ha csak a legsérülékenyebb rendszerek hibáit javítja ki.

### Integrált és átfogó helyreállítás

Javítócsomagra van szüksége? A McAfee Remediation Manager automatikusan kijavítja a Vulnerability Manager által azonosított sérülékenységeket és irányelv-megsértéseket. Vagy hálózati szinten szeretné blokkolni a fenyegetéseket? A McAfee Network Security Platform (a korábbi McAfee IntruShield) összeveti a Vulnerability Manager adatait és on-demand ellenőrzéseket futtat, így az Ön hálózati biztonsága megfelel a már frissített kockázati helyzetnek.

### Hozzáadott segítség PCI DSS megfeleléssel

A Vulnerability Manager segíti a felhasználót a PCI DSS-ben meghatározott specifikus rendelkezések betartásában. A biztonsági javítócsomagok telepítésének hitelesítése, az új

## Telepítési lehetőségek

### Alkalmazások – célra szabott, már bizonyított alkalmazások

Vulnerability Manager 1000 és Vulnerability Manager 850

- Enterprise Manager
- Sérülékenység- és eszköztárak
- Keresőmotor
- Jelentéskészítő motor

### Csak szoftver

Saját hardverére telepíti; az

Enterprise Manager-t, sérülékenység- és eszköztárakat, keresőmotort, valamint egy az operációs rendszer keményítésére szolgáló eszközt tartalmaz

### Minimális követelmények

Hardver:

- CPU: Dual Xeon 2 Ghz, Dual Core Xeon 2.33 Ghz, vagy jobb
- RAM: 2 GB
- Lemezterület: 80 GB-os partíció
- Ethernet hálózati interfész

Operációs rendszer:

- Microsoft Windows 2003 Server Standard Edition (x86), 2-es szervizcsomaggal

Adatbázis:

- Microsoft SQL Server 2005, 2-es szervizcsomaggal vagy SQL Server 2000, 4-es szervizcsomaggal
- Valamennyi SQL hotfix és patch

Virtualizálás

- VMware Virtual Infrastructure 3 (VMware ESX 3.x)

### Kiegészítő alkalmazások

A Vulnerability Manager a következő alkalmazásokat támogatja:

- FSDBUTIL
- Nyílt alkalmazásprogramozási interfész és szoftverfejlesztési készlet (API/SDK)
- Hitelesítő eszközök
- FSUpdate
- Vállalati kockázatkezelő rendszerek (ERM)

sérülékenységek azonosítása és a sérülékenységek frissítése révén a Vulnerability Manager segíti a vállalatokat a 6.1-es, 6.2-es és 11.2-es követelmények teljesítésében. A McAfee PCI Certification Service (tanúsítási szolgáltatás) kiterjeszti ezt az értéket, azáltal, hogy egy további követelménynek felel meg – a minősített, a megfelelés igazolására jogosított gyártó által végzett negyedéves külső ellenőrzés követelményét.

A McAfee elismert, a megfelelés igazolására jóváhagyott gyártó (Approved Scan Vendor – ASV). PCI Certification Service külső ellenőrzésünk kiegészíti a Vulnerability Manager által végzett sérülékenység- és irányelv-ellenőrzési értékeléseket.

## Tulajdonságok

### Prioritásalapú ellenőrzés és helyreállítás

- Értékelést végez el a biztonsági irányelvek alapján, meghatározza a legértékesebb eszközöket, a legkockázatosabb sérülékenységeket célozza meg, valamint a legkritikusabb fenyegetések esetében végez el helyreállítást
- Importálja a rendszervédelemből (ePO) a puffer-túlcsordulás (buffer overflow) elleni védelem adatait a sürgősségi javítócsomag-telepítések csökkentése érdekében, lehetővé téve, hogy a vészhelyzetek során a kritikus sérülékenységekre összpontosítsuk a védelmet

### Átfogó sérülékenység- és irányelv-ellenőrzések

- A személyre szabható sablonok mérik a SOX, a PCI DSS, a HIPAA, az ISO27002, a FISMA, és a Federal Desktop Core Configuration (FDCC) alapkonfigurációinak való megfelelést
- Felfedi a nem kezelt eszközöket, például az idegen (rogue) vezeték nélküli hozzáférési pontokat vagy hálózatának elfelejtett virtualizált VMware host-jait
- A Vulnerability Manager FASL szkriptjei lehetővé teszik a biztonsági szakemberek számára, hogy személyre szabott sérülékenység-ellenőrzéseket írjanak a szellemi tulajdont képező (proprietary) és az örökölt (legacy) programok vizsgálatához

- A Vulnerability Manager értékelő képessége magában foglalja a XCCDF, OVAL és egyéb, a Security Content Automation Protocol-ban (SCAP) szereplő nyílt szabványokat követő, harmadik felek által kidolgozott tartalmakat is

### Egyszerűbb az irányelveknek való megfelelés

- Használjon előre meghatározott irányelv-ellenőrzéseket a kiterjesztett szkenneléshez; a program az eredményeket rögzíti, tárolja, és jelentést készít róluk
- Az új irányelv-ellenőrzések specifikus paramétereit könnyen kezelhető, varázslóalapú felületen határozhatja meg
- A program irányelvek alapkonfigurációját egy referencia-rendszerellenőrzés alapján határozza meg, majd értékeli a többi rendszer megfelelését

### Konfigurálható szabályalapú eszköz-meghatározás

- Konfigurálható sérülékenység-ellenőrzések egyedi eszközök vagy eszközcsoportok alapján, anélkül, hogy IP-tartományokat kellene megadni
- Automatikus eszközcsoportosítás és az eszközök nyomon követése a berendezés típusa (webszerverek, munkaállomások, levelezőszerverek), az operációs rendszer, az IP-cím tartomány, a gazdaszámitógépek, a DNS-nevek vagy a személyre szabott szabályok szerint

### Rugalmas jelentéskészítés

- Tekintse meg a sérülékenységgel kapcsolatos információkat és a biztonságvédelmi adatokat McAfee ePO jelentéseiben
- Készítsen jelentéseket platformok, üzleti egységek, földrajzi hely vagy IP-tartomány szerint, hogy bepillantást nyerhessen az irányelvek megsértésébe, a sérülékenységekbe, a helyreállítási intézkedésekbe és a változó kockázati profilokba
- Tekintse meg a Windows- és Unix-rendszerek kliens program nélküli irányelv-ellenőrzéseinek eredményeit a rugalmas és részletes jelentéskészítési opciók segítségével
- Tekintse meg az ePO-konzolon belül a kliensalapú, valamint a kliens program nélküli ellenőrzések összesített eredményeit
- Továbbítsa a sérülékenység-értékeléseket XCCDF-jelentés formátumban

### Skálázható nyílt architektúra

- A Vulnerability Manager többretegű keresése, irányítása és adatbázisa úgy lett megalkotva, hogy illeszkedjen infrastrukturális igényeihez

„Azzal, hogy lehetővé tette hálózatunk biztonsági kockázatainak prioritásalapú megközelítéssel történő kezelését, a McAfee Vulnerability Manager elősegítette a CSU, Chico számára a kockázatok jelentős mérséklését, valamint általános biztonságkockázati helyzetünk javítását.”

Jason Musselman,  
információbiztonsági elemző, CSU,  
Chico

További információért látogasson el a [www.mcafee.com](http://www.mcafee.com) weboldalra!

- Eszközalapú felderítés, menedzsment, keresés és jelentéskészítés szerint konfigurálható, ePO, AD vagy LDAP csoportosítások alapján
- Támogatja a virtualizált VMware-környezetben történő telepítést

#### Azonnali fenyegetés-értékelés

Összeveti a fenyegetéssel kapcsolatos információkat az eszközök értékével és a sérülékenységekkel, segítséget nyújtva Önnek ahhoz, hogy a legsérülékenyebb eszközökön végezhesse el a helyreállítást, és csökkentse a javítóprogramok telepítését vészhelyzetek esetén

A Vulnerability Manager a fenyegetésekkel kapcsolatosan automatikusan biztosított útmutató információk felhasználásával, a teljes hálózat ismételt átnézése nélkül képes percek alatt megjeleníteni és rangsorolni az új fenyegetések nyújtotta potenciális kockázatokat

A Microsoft Windows, a UNIX, a Cisco IOS és a VMware platformok bizonyítvány-alapú keresései az ágazat legpontosabb találatait biztosítják a sérülékenységek és a biztonsági irányelvek megszegése tekintetében

#### Működési hatékonyság

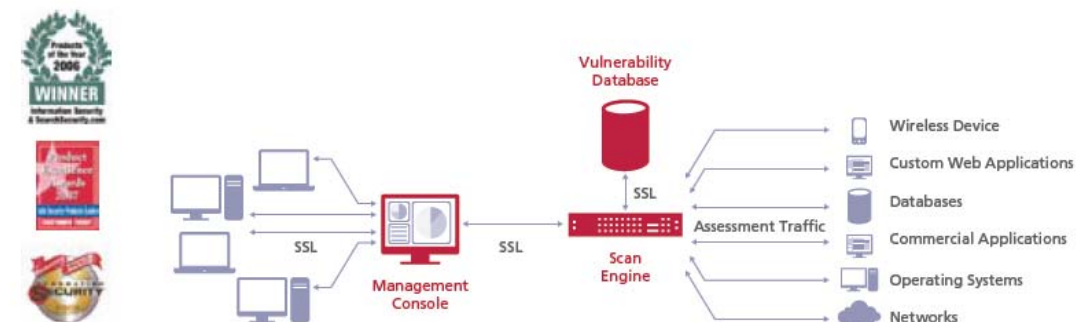
- A központosított keresés-kezelés lehetővé teszi, hogy a nélkül javítsa az ellenőrzések sebességét, hogy ki kellene választani a specifikus keresőmotort a futtatáshoz
- A Lightweight Directory Access Protocol-lal (LDAP) és az Active Directory-val (AD) történő eszközszinkronizálás révén

többszörös LDAP-szervert konfigurálhat a Vulnerability Manager-hez az eszközinformáció importálása céljából; az adminisztrátornak így kevesebb időt kell töltenie a keresendő IT-eszközök létrehozásával és csoportosításával

- A Configuration Manager segítségével a teljes Vulnerability Manager-telepítést központosított, egységes módon tudja javítani, konfigurálni, ellenőrizni és kezelni
- A tanúsítványokat egységes kezelőfelületen tudja kezelni

#### Integrálás az ePO-val a biztonságirányítási infrastruktúra beruházásainak optimalizálása érdekében

- A Vulnerability Manager információval látja el az ePO-t a nem kezelt eszközökkel kapcsolatban
- A Vulnerability Manager kereséseit nem pusztán IP-tartományokban, hanem eszközcsoportokon is végzi
- A McAfee Threat Information Service (MTIS – fenyegetésekkel kapcsolatos információs szolgáltatás) adatai bekerülnek az ePO-ba, és összevetésre kerülnek az egyéb McAfee-termékek által biztosított sérülékenységekkel kapcsolatos információkkal és biztonságvédelemmel
- A kvantitatív kockázati értékek az ePO-ban kerülnek kiszámításra és tárolásra (a Vulnerability Manager eredményeit felhasználva)
- Az egységesített irányelv-értékelési sablonok egyszerre végeznek ágensalapú és kliens program nélküli értékeléseket



A McAfee Vulnerability Manager többretegű architektúrát használ a skálázhatóság maximalizálása és a telepítés rugalmassága érdekében.