

# A McAfee FoundStone sérülékenységmentésment megoldása



Protect what you value

# Tartalomjegyzék

I. McAfee FoundStone appliances .....	3
Túl sok az adat.....	3
Fókuszáljunk a leginkább kritikus fenyegetésekre.....	3
Vizsgáljuk a teljes sérülékenység-menedzsment életciklust.....	3
Az Appliance megoldás előnyei.....	4
A sérülékenység-menedzsment prioritás-alapú megközelítése.....	5
II. A FoundStone Enterprise megoldás működés közben.....	6
McAfee Customer Care .....	8
Jövőkép .....	8

# I. McAfee FoundStone appliances

...Egy már sokat bizonyított, prioritás-alapú sérülékenység menedzsment megoldás...



1. ábra: A FoundStone Enterprise megoldás átforgó megoldást nyújt sérülékenység-menedzsment területen

## Túl sok az adat...

Minden szervezet a fenyegetésekről és sérülékenységekről szóló információáradattal néz szembe – s már maga a pusztá adattömeg is szinte lehetetlenné teheti annak a meghatározását, hogy mely fenyegetések számítanak kritikusnak, és melyek bírnak kevesebb jelentőséggel.

A sikeres sérülékenység menedzsment annak meghatározásával kezdődik, hogy mely tételek a legfontosabbak, az adott tételek sérülékenységének azonosításával, a fenyegetésekre adott válaszokkal és a rangsorolással. Egy hatékony, prioritás-alapú kockázat menedzsment nélkül egy szervezet mindig veszélyben van.

## Fókuszáljunk a leginkább kritikus fenyegetésekre

A McAfee® Foundstone® Enterprise egy díjnyertes prioritás-alapú sérülékenység-menedzsment megoldás. A Foundstone Enterprise lehetővé teszi a szervezetek számára, hogy a tétel értékének, a sérülékenység komolyságának és a fenyegetés kritikuságának a mérlegelésével csökkentsék a kockázatot. A szervezetek ezután oda irányíthatják erőforrásaikat, ahol a legnagyobb eredményt érhetik el, miközben javítják a szervezet biztonságát.

A Foundstone Enterprise egy zárt, nagyvállalati biztonsági megoldás, amelyet úgy terveztek, hogy kezelje és csökkentse a sérülékenységekkel társuló üzleti kockázatokat. A Foundstone az eszközök felderítésén, a leltár készítésén és súlyozáson keresztül a hálózati infrastruktúra védelmét kínálja, hogy biztosítsa az üzletmenet folytonosságát, felhasználva a fenyegetések és a közöttük levő kapcsolatok kikémlelését, és a kezelés nyomkövetését és a jelentéskészítést.

## Vizsgáljuk a teljes sérülékenység-menedzsment életciklust

A Foundstone Enterprise egy appliance (hardver megoldás, és szoftver) alapú komplett, plug-and-play megoldás a sérülékenység-menedzseléshez és a kockázatok csökkentéséhez. A Foundstone FS1000 Appliance percek alatt teljesen működésképes állapotba hozható és hozzáigazítható bármilyen informatikai környezethez. A menedzseléshez kizárólag egy web böngészőre van szükség. A Foundstone Enterprise lehetővé teszi a szervezetek számára, hogy azonnal ellenőrzésük alá vonhassák a sérülékenység menedzsment életciklusát:

- Felderíti és súlyozza az eszközöket, szervereket;
- Hajszálpontosan megállapítja a sérülékenységeket;
- Proaktív módon foglalkozik a kritikus fenyegetésekkel;
- Készlet-alapú orvoslás menedzselést folytat;
- Egyezteteti az intézkedéseket és a jelentéseket.

## Az Appliance megoldás előnyei

A szűkös erőforrásokat maximálisan kihasználja azzal, hogy azokra a leginkább kritikus sérülékenységekre, eszközökre és fenyegetésekre fókuszál, amelyek a legnagyobb kockázatot jelentik:

- Minden részletre kiterjedően feltérképezi a teljes hálózatot, a vezeték nélküli hozzáférési pontokat is beleértve;
- A hírszerzési riasztások specifikus, cselekvésre felhasználható információt szállítanak a kitörő fenyegetések ellen (A szervezetek számára hatékony és könnyen érthető metrikájú mérési eszközöket nyújt a rendszer és a hálózati erőforrások biztonságát fenyegető kockázat mérésére és monitorozására: FoundScore, MyFoundScore és Risk Score néven. A szervezetek gyorsan felbecsülhetik biztonságuk állapotát, felmérhetik, összemérhetik üzleti egységeiket vagy régióikat és nyomon követhetik az implementált biztonsági házirendek és programok működését);
- Úttörő a fenyegetés-kikémlés riasztásainak, a fenyegetések közötti összefüggések kikémlésének és a teljesítmény megőrzésének érdekében megtett intézkedések integrálásában (nem is napra, hanem percre kész fenyegetés felderítési riasztások a McAfee Research-től, amely lehetővé teszi az azonnali reagálást a bekövetkező eseményekre, mint a milyenek a férgek és a támadások széles skálája, úttörő az egyes fenyegetések kockázatainak besorolásában a megfelelő eseményeknek az elemekhez és sérülékenységekhez való viszonyában; megfelelő mérési képességek);
- Belső biztonsági szabványokat és útmutatásokat hoz létre; ellenőrzi és méri a szabályzás teljesítményét;
- Automatikus frissítéssel és karbantartással alacsonyabb TCO-t ér el (a Foundstone Update Service automatikusan alkalmazza a legutolsó alkalmazásokat és operációs rendszer javításokat),



2. ábra: A FoundStone 1000 appliance megoldása (2 GB RAM, 2 x 2,8 GHz Intel Xeon P4 CPU, 140 GB SCSI HDD, 2 x 10/100/1000 NICs)

- Megerősített, skálázható appliance (minimális karbantartás, a legtöbb helyszínen lehetőség van aznapi vagy másnapi helyszíni javításra) ;
- Páratlan fenyegetés megjelenítés (az összes eszköz sérülékenységeinek és hibás konfigurálásának teljes spektrumát rendszeresen mélységben deríti fel és elemzi, beleértve ebbe az operációs rendszereket, a hálózati eszközöket, a kereskedelmi alkalmazásokat, adatbázisokat, vezeték nélküli eszközöket és az egyedi webes alkalmazásokat);
- Integrált gyógyítási menedzsment (zárt hurkot képező rendszer automatikusan jegyeket nyit és rendel hozzá az új sérülékenységek felfedezésékor, és automatikusan ellenőrzi és lezárja azokat a sikeres gyógyítás során);

- Flexibilis felhasználói fiók menedzsment (egy mindenre kiterjedő hierarchikus modell a szervezeteknek azt a rugalmasságot nyújtja, amelyre szükségük van ahhoz, hogy bármilyen méretű vállalkozásban hatékonyan menedzselje a biztonsági kockázatokat; az üzleti funkcióknak, a földrajzi régióknak, a technológiáknak vagy a szerepeknek megfelelően szervezze a felhasználói fiókokat).
- Zero day protection: A FoundStone képes nem csak a javítással rendelkező sérülékenységek felderítésére, de a már azonosított, javítással nem rendelkező sérülékenységek azonosítására is. Mellékeli a sérülékenységet felfedező cikket, valamint a szükséges konfiguráció változtatást is.

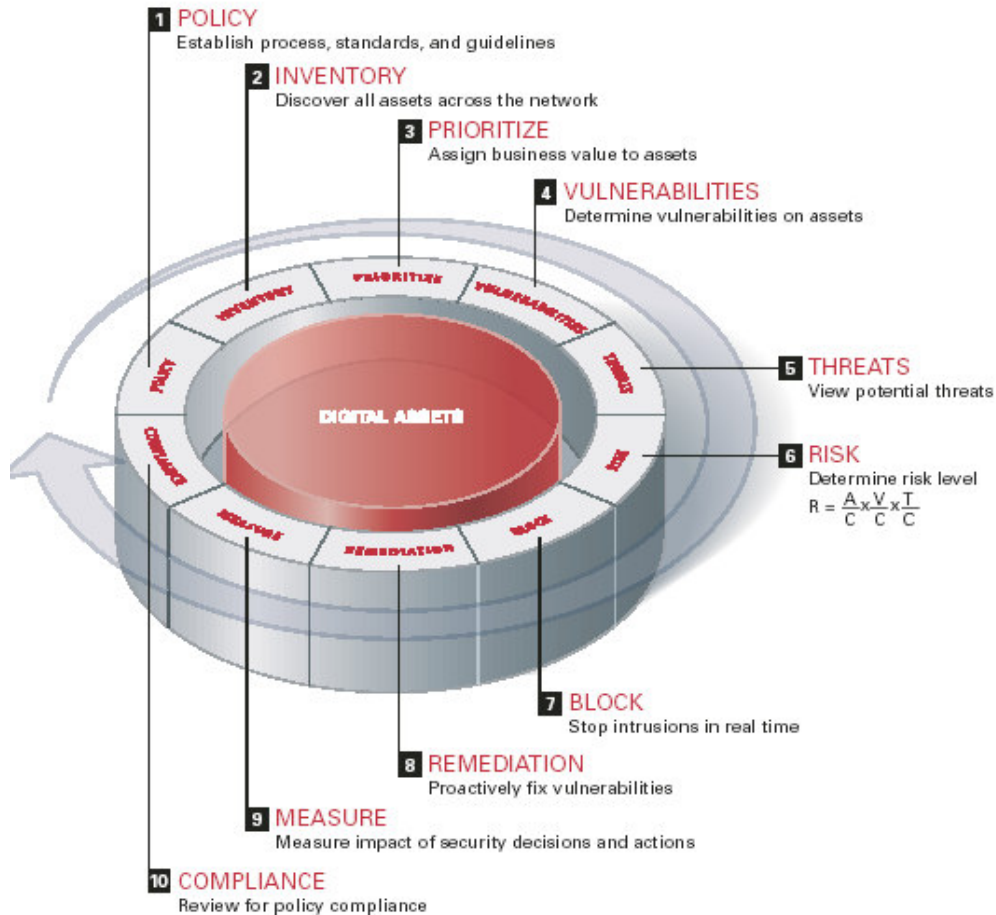
## A sérülékenység-menedzsment prioritás-alapú megközelítése

Azokra a legkritikusabb sérülékenységekre, elemekre és fenyegetésekre fókuszál, amelyek a legnagyobb kockázatokat jelentik;

Hatékonyan hasznosítja a korlátozott pénzügyi és humán erőforrásokat;

Egy alapszintet hoz létre és felméri a fejlődést a megfelelő szabványokhoz képest;

Stratégiaileg védi a ránk törő fenyegetésekkel szemben az üzleti szempontból kritikus elemeket.



3. ábra: A FoundStone komplett megoldást nyújt a teljes sérülékenység-menedzsment életciklusra

#	ELEM	MEGJEGYZÉS
1	Házirend	Létrehozza a folyamatot, a szabványokat és az útmutatásokat
2	Leltár	Felderíti a hálózaton keresztül az összes elemet

3	Priorizálás	Üzleti értéket rendel az egyes elemekhez
4	Sérülékenységek	Meghatározza a sérülékenységeket az egyes elemeken
5	Fenyegetések	Meghatározza a potenciális fenyegetéseket
6	Kockázat	Meghatározza a kockázat szintjét az alábbi képlet alapján $R = \frac{A}{C} \times \frac{V}{C} \times \frac{T}{C}$
7	Blokkolás	Valós idejű blokkolást végez rosszindulatú behatolás esetén
8	Javítás	Proaktív módon javítja a sérülékenységeket
9	Monitorozás	Méri a biztonsági döntések és intézkedések hatását
10	Megfelelőség	A házirend megfelelőségének áttekintése

4. ábra: A teljes sérülékenység-menedzsment életciklus

## II. A FoundStone Enterprise megoldás működés közben

A kulcsrakészen kapott megoldás a – sajnos elkerülhetetlen – szerelési munkák után (rack szerelés, IP cím beállítás, DNS konfiguráció, license file importálás) azonnal működésre készen áll.

A működés megértéséhez először tisztázni kell a legfontosabb fogalmakat.

Organization: adott cég / cégcsoport / osztály, ahol a FoundStone Enterprise működni fog. Ez az Organization egy infrastruktúra csoportot definiál.

User: felhasználók, role-based jogosultsággal.

Scan: adott infrastruktúra környezetben folyó sérülékenység-menedzsment vizsgálat, melynek során a FoundStone meghatározza az adott Subnet-ben található eszközök hardvergyártóját, operációs rendszerét, verzióját, a telepített patch-eket, a telepített alkalmazásokat, a hálózati beállításokat, valamint a sérülékenységeket (és amennyiben létezik a hozzájuk tartozó javításokat is).

Scan Template: A FoundStone Enterprise segítséget nyújt azoknak az ügyfeleknek, akik számára fontos a SOX, vagy a Basel-i előírások megfelelőségének ellenőrzése. Ezt támogatja a beépített template készlet. Akár néhány kattintással ellenőrizni tudjuk, hogy eszközeink megfelelnek-e ezen előírásoknak.

Device: olyan eszköz, mely a Scan-elés során felderítésre kerül. Ez lehet szerver, kliens, nyomtató, switch, router, gyakorlatilag bármilyen olyan eszköz, aminek IP címe van.

Subnet: adott Subnet, amelyen belül a scan-elés folyik.

Vulnerability: adott operációs rendszeren, adott verzión, adott konfigurációs beállítások esetén fennálló olyan bug, melynek kihasználásával az eszköz működése megváltoztatható.

Riport: A Scan-elés eredményének rövid összefoglalója .html, .pdf, .csv formátumban. Ez akár e-mail-ben is továbbítható automatikusan.

Schedule: A FoundStone működése közben a Scan-elés időzíthető, így elkerülhető a sávszélesség napközbeni túlzott kihasználása.

Vulnerability group: a FoundStone által ismert sérülékenységek csoportosítva vannak (pl.: IIS vulnerabilities, Apache vulnerabilities, Wireless vulnerabilities, Windows vulnerabilities, stb.). Ezekkel a csoportokkal tudjuk pontosítani, hogy a Scan-elés során milyen típusokat ellenőrizzen a FoundStone.

Credentials: A Windows-os gépek ellenőrzése során megadható olyan felhasználó, akinek a jogosultságával próbáljon meg a FoundStone plusz ellenőrzéseket végezni.

Patch: a sérülékenységekre megjelent javítás, melynek telepítésével elkerülhető a nem üzemszerű működés.

Operating System: azon operációs rendszerek, melyek a FoundStone Enterprise ismer, azaz ezeken képes a sérülékenységeket ellenőrizni. A támogatott operációs rendszerek listája több mint 700 operációs rendszert ismer, és folyamatosan bővül.

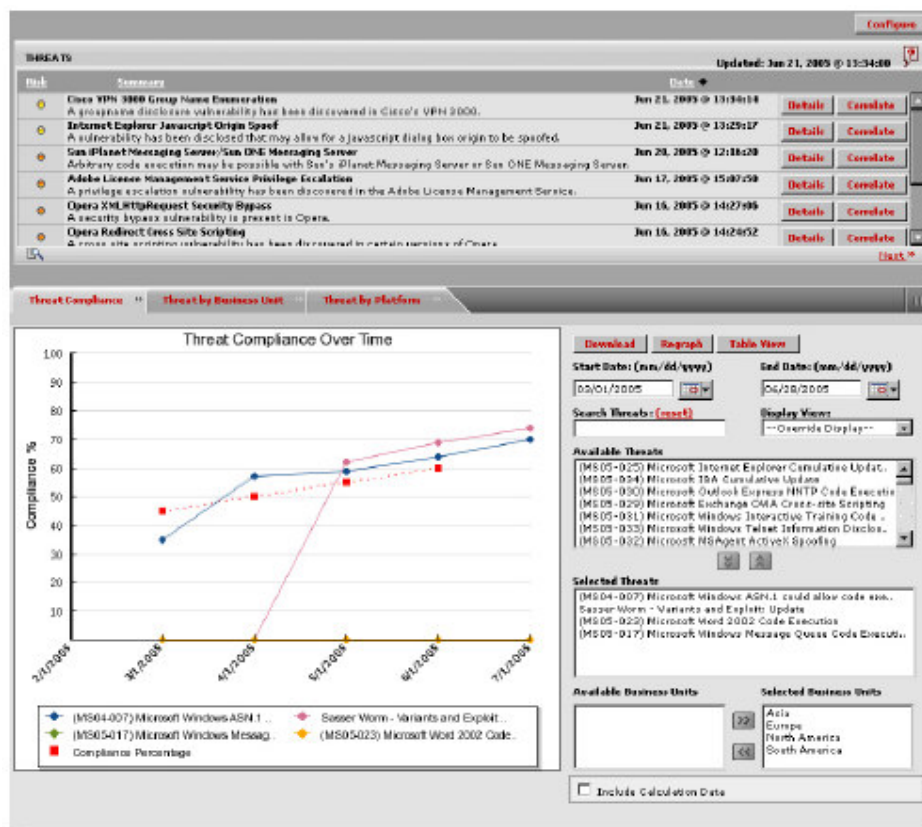
A rendszerre törtnő belépés után a FoundStone számára definiálni kell a következőket:

- Organization
- Subnet
- User
- Vulnerability group
- Scan template
- Schedule

Ezek után a rendszer automatikusan megvizsgálja az adott Subnet-et, azaz ellenőrzi többek között a Default Share-eket, a nyitott portokat, WMI eléréseket, alkalmazásokat, Credentials megadása esetén plusz ellenőrzéseket is végez.

Megjegyzés: Nem hacker eszközökkel végzi az ellenőrzést, nincs rosszindulatú betörés, nincs ellenőrizetlen tevékenység, az alkalmazás csupán monitoroz, semmilyen módosítást nem végez a Scan-elés során.

A Scan-elés lezárásaként elkészíti a riport file-okat, illetve amennyiben konfigurálva van ezeket automatikusan el is küldi e-mail-ben, vagy akár továbbítja Remediation Ticket-ként a rendszerfelügyeleti megoldásnak a talált sérülékenységeket.



5. ábra: A Threat Compliance View lehetővé teszi a szervezetek számára, hogy percrekészt riasztásokat kaphassanak a közelgő fenyegetésekről és mérjék a teljesítményt a fenyegetés, az üzleti egység és platform alapján.

A riportok nagy előnye, hogy többretegű, azaz IP címek, sérülékenységek, prioritás szerint is csoportosítva van, és ezen riportok át is járhatók egy kattintással.

## **McAfee Customer Care**

A McAfee Gold Support gyors hozzáférést biztosít a mi gyakorlott és magasan képzett IT-security tanácsadó csapatunkhoz. A McAfee díjnyertes ServicePortal-jához való hozzáféréssel, és a frissítések és javítások korlátlan letöltése mellett 24/7/365 hozzáférést kap telefonon és online chat programokon keresztül a McAfee biztonsági vizsgákat tett technikusaihoz.

A McAfee Platinum Support azok számára az ügyfelek számára áll rendelkezésre, akik értékelik egy kijelölt Technical Account Manager (TAM) személyes 24/7 proaktív tanácsadását. Az Platinum TAM-ja ismeri az ügyfél telepített McAfee rendszereit és a tanácsadás történetét, és proaktív módon áll kapcsolatban az ügyféllel, ha szükséges a megvásárolt termék teljesítményét optimalizálni és maximalizálni kell az ügyfél vállalkozásánál az üzemidőt.

## **Jövőkép**

A McAfee célja, és stratégiája, hogy a továbbiakban bővítse a FoundStone sérülékenység-menedzsment megoldását. Felvásárlásokkal, saját fejlesztésekkel bővíti a funkcionalitást, melynek a célja, hogy nem csak a Scan-elés, riportgenerálás legyen teljesen automatikus, de a prioritizálás, központosított házirend template-k ellenőrzése, és a központi patch telepítés is.