

McAfee Network Security Platform

Az iparág leghaladóbb behatolás-megelőző megoldása

Gyorsabb védelem. Gyorsabb megoldás. Gyorsabb biztonság. A McAfee Network Security Platform (a korábbi McAfee IntruShield) integrált, automatizált és végrehajtható, tudásvezérelt biztonságot kínál. Kizárólag a Network Security Platform kombinálja a hálózati és a rendszerbiztonsági infrastruktúrát a vállalati szintű proaktív védelem érdekében. A telepítést követően azonnal megkezdheti a fenyegetések blokkolását. A fenyegetés blokkolását követően az adott tétel gyorsan és alaposan kivizsgálható. A kockázatok kezelése és a megfelelőség betartatása kisebb erőfeszítést igényel. Intelligens biztonsági és megbízható hálózati szintű platformjaink teljes biztonságot kínálnak vállalata számára.

Jellemzők

Vállalati szintű lefedettség

- Egyetlen, ágazati szinten bizonyított eszköz kínál átfogó, proaktív hálózat- és rendszerbiztonságot

Átláthatóbb és könnyebb kikényszeríthetőség az integrálásnak köszönhetően

- Integrálható a Vulnerability Manager és ePO megoldásokkal a kritikus hostok, fenyegetések és kockázatok fontosságának azonnali megtekintéséhez

Gyors, pontos döntések

- Valós idejű, nem csak automatikus, de végrehajtható biztonsága révén csökkenti a védelem elindításához és a biztonság eléréséhez szükséges időt

Megbízható, hálózati szintű platformok, következő generációs hálózatvédelem

- 100 Mbps-től 10 Gbps-ig terjedő teljesítmény
- A legnagyobb portsűrűség

Működési hatékonyság

- A McAfee hálózati, rendszer-, kockázati és menedzsment-termékei közötti együttműködés időt és erőforrásokat takarít meg

Könnyen telepíthető

- Az NSM-alkalmazás és a beépített telepítő varázsló segítségével az NSP telepítése csupán néhány percet vesz igénybe. Az alkalmazás portjainak alapértelmezés szerinti konfigurációja in-line bekötésű, jól beállított alapértelmezett irányelv alkalmazásával, ami rögtön kész a fenyegetések blokkolására.

Átfogó támogatás a beágyazáshoz

- IPv6, MPLS, GRE, Q-in-Q Double

Magas szintű rendelkezésre állás

- Layer 2 áthidalás (fail-open), Hardver-áthidalás, Feladatátvétel (fail-over)

Megbízható védelem valamennyi hálózatra kötött eszköz számára

Mennyire intelligens az Ön hálózati biztonsága? A hagyományos behatolás-megelőző rendszerek (IPS-ek) olyan végponti megoldások, amelyek rengeteg téves riasztást produkálnak és hihetetlen mennyiségű riasztási naplót tárolnak. A koordináltságuk hiánya azt eredményezheti, hogy a redundáns menedzsment folyamatok miatt értékes idő veszt el. A legtöbb PC-alapú megoldás nem skálázódik a támadások során, emellett kevés olyan program létezik, mely lehetőséget kínál a javítóprogramok telepítése által okozott nyomás enyhítésére.

Ezért választotta a legigényesebb vállalkozások és szolgáltatók közül több, mint 4 500 a McAfee Security Network Platformot hálózataik és hálózatra kötött eszközeik védelméhez.

Integrált hálózat- és rendszerbiztonság

A McAfee Network Security Platform tökéletes mindazon vállalkozások számára, amelyek a valós idejű biztonságot multi-gigabites teljesítménnyel és integrált, vállalati szintű hálózat- és rendszerbiztonsággal kombináló megoldást keresnek. A Network Security Platform által nyújtott tudásvezérelt biztonság lehetővé teszi a kockázatok automatikus kezelését és a megfelelőség automatikus teljesítését – mindeközben javítva a működési hatékonyságot és mérsékelve az információtechnológiai terhelést. A Network Security Platform együttműködik a McAfee Vulnerability Manager (a korábbi McAfee Foundstone), a McAfee ePolicy Orchestrator (ePO) és a Host Intrusion Prevention megoldásokkal, továbbá kulcsfontosságú összetevője a McAfee NAC megoldásának (hálózathozzáférés-szabályozó megoldás), a Unified Secure Access-nek. A program mindazt biztosítja, amire vállalkozásának szüksége lehet: védelem, átláthatóság, hatékonyság, kikényszeríthetőség és érték.

Abszolút biztonság

A Network Security Platform az egymást átfedő, a védelmeket integráló behatolás-megelőző rendszer és belső tűzfal kombinációja révén védelmet biztosít minden hálózatra kötött eszköznek, kiterjesztve a védelmet a belső hálózatra is. Összeveti az aláírásokkal, a szolgáltatás-megtagadással (DoS) és a megosztott szolgáltatás-megtagadással (DDoS) járó támadásokkal kapcsolatos információkat, hogy a támadásokat pontosan blokkolhassa, még mielőtt azok elérhetnék kijelölt célpontjukat. Dinamikus fenyegetés- és sérülékenység-frissítések gondoskodnak a védelem folyamatosságáról.

Hálózati szintű platform multi-gigabites teljesítménnyel

A Network Security Platform célra szabott alkalmazásokból álló portfóliója költség hatékony, nagy teljesítményű megbízhatóságot nyújt minden helyszín számára, a leányvállalatoktól a hálózati központig. A Network Security Platform könnyen telepíthető és egyszerűen kezelhető. Percek alatt létrehozhatóak az irányelv-sablonok, amelyek hatékonyan kezelhetőek és frissíthetőek egy központositott, böngészőalapú felület segítségével. A Network Security Platform irigylésre méltó minősége és teljesítménye meghaladja a szolgáltató szintű (carrier-class) szabványok szintjét, aminek köszönhetően a McAfee megoldása az egyetlen behatolás-megelőzési megoldás, amely elnyerte az NSS Group Multi-Gigabit IPS tanúsítványát.

A programjavításokkal járó nehézségek mérséklése, valamint az Ön biztonsági irányelveinek kikényszerítése

Ön irányít. A Network Security Platform segítségével elszigetelheti rendszereit a kockázatoktól a programjavítások hitelesítése és telepítése során. Ellenőrizheti a forgalmat és egyedi irányelveket, védelmeket vezethet be egy adott hálózati szegmensre, egy gazdaszámítógép-csoportra, vagy akár egyetlen



Network Security Platform

Valós idejű védelem a vállalkozásnak

- Megakadályozza a támadásokat, miközben csökkenti a költségeket és az állásidőt
- Megvédi adatait és infrastruktúráját
- Teljesíti a megfelelőségi kezdeményezéseket

Megvédi rendszereit

- Proaktív védelem a nem javított rendszereknek
- Proaktív védelem a zero-day támadásokkal szemben
- Rendszerérzékelő behatolás-megelőző rendszer McAfee ePO-integrációval
- Megtekinthető host IPS-/vírus-/kémprogram-események

Megvédi hálózatát

- Következő generációs 10 Gigabites Ethernet
- IPv6 védelem
- Adaptív sebességkorlátozás
- Átfogó infrastruktúravédelem

Szabályozási és irányelvi megfelelés

- Valós idejű sérülékenység-észlelés és megfelelőség-jelentés
- Kockázat-észlelő IPS McAfee Vulnerability Manager-integrációval
- Viselkedés-szabályozott gazdaszámítógép-karantén
- Kikényszeríti a belső és a szabályozási politikát

rendszerre vonatkozóan. A megoldás emellett rugalmas is, így akkor telepítheti a javítóprogramokat, amikor készen áll rá, és olyan irányelv-kikényszerítést léptethet életbe, amely megfelel szervezete igényeinek.

Az opcionális NAC bővítő-szoftver hozzáadásával behatolás-megelőző megoldása hálózathozzáférés-szabályozó eszközzé alakítható, amely mind előzetes, mind pedig utólagos hozzáférés-szabályozást, identitásalapú hozzáférés-szabályozást, valamint gazdaszámítógép-karantént és kikényszeríthető hozzáférési irányelveket kínál.

Iparági szinten bizonyított hálózatbiztonsági eszköz

Védje meg vállalkozását a már bizonyított McAfee biztonsági eszközökkel, amelyeket a McAfee Avert Labs nonstop kutatása támogat. Méretezze védelmét szolgáltató szintű teljesítményre egyetlen integrált hálózatbiztonsági megoldás segítségével!

Pontos, vállalkozásszintű fenyegetés-megelőzés

- Védje meg vállalkozását az ismert és a zero-day támadásoktól, a DoS-, DDoS, SYN-flood és kódolt támadásoktól, valamint az olyan fenyegetésektől, mint a kémprogramok, a Voice over IP (VoIP) sérülékenységek, a bothálózatok, a rosszindulatú programok, a férgek, a trójaiak, az adathalászat és a peer-to-peer támadások
- Növelje a pontosságot többféle fejlett észlelési módszer alkalmazásával, beleértve az aláírás-, alkalmazás- és protokoll-anomáliák észlelését; a shellkód-észlelési algoritmusokat; valamint a következő generációs DoS- és DDoS-megelőzést
- Ellenőrizzen több, mint 100-féle protokollt és vizsgáljon át több, mint 3000 kiváló minőségű, több vezérjellel bíró (multi-token), multi-trigger aláírást az átmenő forgalom figyelése révén
- Szerezzen be proaktív blokkolást több száz támadással szemben, közvetlenül az előre konfigurált Ajánlott blokkolási irányelvekkel
- Folyamatos, nonstop fenyegetés-frissítéseket kap a McAfee Avert Labs globális kutatócsapatától

Integrálás a McAfee ePolicy Orchestrator (ePO) megoldással

- Kövesse nyomon valós időben a kivitelezhető rendszer- gazdaszámítógép részleteit, beleértve a host nevét, a felhasználó nevét, az operációs rendszert, a patch-szintet, a MAC-címet, az utolsó keresés dátumát, a védelem részleteit, és a top gazdaszámítógép IPS-t, az antivírus- és antispyware-eseményeket
- Szintetizálja és szűrje több eszköz adatait testre szabott jelentések készítéséhez

Valós idejű kockázatérzékelő hálózatbiztonsági platform

- A McAfee Vulnerability Manager-rel történő integrálás révén többszörös sérülékenységi-adat pontot importálhat automatikusan; a rendszeres vagy kézzel indított keresések pontosan meghatározzák a fenyegetés jelentőségét

Adaptív sebességkorlátozás (rate limiting)

- A Network Security Platform valós idejű, protokoll-alapú sebességkorlátozást használ az alkalmazás-, protokolltípus- és port-alapú sáv szélesség-szabályozáshoz és a szolgáltatás minőségének javítása érdekében
- Rangsorolja a vállalkozás szempontjából kritikus forgalmat és blokkolja a nem kívánt és kockázatos alkalmazásokat

Az NSS Group tanúsítványa

- A Network Security Platform az egyetlen behatolás-megelőzési megoldás, amely elnyerte az NSS Group Multi-Gigabit IPS tanúsítványát

Igazolt kezelhetőség és rendelkezésre állás

A Network Security Platform alkalmazások és irányelvek egyszerű, központosított webalapú kezelése az alábbiakat tartalmazza:

- Tizennégy azonnal használható, előre meghatározott biztonságiirányelv-szabályozási sablon
- Integrált felhasználó-hitelesítési támogatás a külső adatbázisokhoz, beleértve a Radius-t, az LDAP-t és a TACACS-ot
- A McAfee Network Security Manager (a korábbi McAfee IntruShield Security Manager) folyamatosan működő kezelést, automatikus feladatátvételt (failover) és visszaköltöztetést (fail-back), valamint a kritikus konfigurációs adatok visszaállítását kínálja
- A Network Security Manager szoftver ingyenesen áll rendelkezésre akár két Network Security Platform alkalmazás kezeléséhez
- A Network Security Central Manager (a korábbi McAfee IntruShield Command Center) hierarchikus kezelést kínál az irányelvek megtekintésének, módosításának és disztribúciójának központosított szabályozásához a nagyméretű és földrajzilag szétszórott szenzortelepítések támogatása érdekében
- A nagy rendelkezésre állású konfiguráció átlátható, 7-es szintű állapotkövető feladatátvételt tesz lehetővé, amellyel elkerülhető az egyetlen meghibásodási pontból eredő leállás

A McAfee Network Security Platform tulajdonságai

10 Gigabit Ethernet kapcsolat									
Hardverösszetevők	M-8000	M-6050	M-4050	M-3050	I-4010 I-4000	I-3000	I-2700	I-1400	I-1200
Hálózat elhelyezkedés	Core	Core	Core	Core	Core	Core	Perimeter	Branch office / Perimeter	Branch office
Teljesítmény	10 Gbps	5 Gbps	3 Gbps	1.5 Gbps	2 Gbps	1 Gbps	600 Mbps	200 Mbps	100 Mbps
Maximális egyidejű kapcsolatok	4,000,000	2,000,000	1,000,000	750,000	1,000,000	500,000	250,000	80,000	40,000
Portok									
Gigabit Ethernet érzékelő portok	16	8	8	8	12/4	12	2	-	-
10 Gigabit Ethernet	12	8	4	4	-	-	-	-	-
Gyors Ethernet (FE) érzékelő portok	-	-	-	-	-	-	6	4	2
Dedikált válaszportok	1 GigE	1 GigE	1 GigE	1 GigE	2 FE	2 FE	3 FE	1 FE	1 FE
Dedikált menedzsment portok	1 GigE	1 GigE	1 GigE	1 GigE	1 FE	1 FE	1 FE	1 FE	1 FE
Külső fail-open irányító portok	14	8	6	6	6/2	6	1	-	-
Console és aux portok	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Beépített hálózati kivezetések	Nem	Nem	Nem	Nem	Nem	Nem	Igen (FE portoknak)	Igen	Igen
Fail-open	Opcionális	Opcionális	Opcionális	Opcionális	Opcionális	Opcionális	Igen (FE portoknak)	Igen	Igen
Fail-close	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Működés módja									
Span port monitor	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Kivezetés módja	Opcionális	Opcionális	Opcionális	Opcionális	Opcionális	Opcionális	Igen (FE portoknak)	Igen	Igen
In-line mód	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Port csoportosítás	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
10Gbps-plus megoldás	Igen	Igen	-	-	-	-	-	-	-
Virtuális IPS rendszerek száma	1 000	1 000	1 000	1 000	1 000	1 000	100	32	16
Forgalom monitor az aktív - aktív linkeken	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Forgalom monitor az aktív - passzív linkeken	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Aszimmetrikus forgalom irány monitorozása	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Rendelkezésre állás									
Redundáns energia	Igen (opcionális)	Igen (opcionális)	Igen (opcionális)	Igen (opcionális)	Igen (opcionális)	Igen (opcionális)	Igen (opcionális)	Nem	Nem
Eszközhíány észlelés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Link hiány észlelés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Fizikai									
Méret	2x 2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D) each	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 16.75(W) x 3.05(H) x 30.00(D)	2RU Rack mountable 17.44(W) x 3.44(H) x 23.00(D)	2RU Rack mountable 17.44(W) x 3.44(H) x 23.00(D)	2RU Rack mountable 17.44(W) x 3.44(H) x 23.00(D)	1RU Rack mountable 17.32(W) x 1.65(H) x 10.5 (D)	1RU Rack mountable 17.32(W) x 1.65(H) x 10.5(D)
Súly	94 lbs. (2x47)	47 lbs.	47 lbs.	47 lbs.	47 lbs.	47 lbs.	47 lbs.	17 lbs.	15 lbs.
Energia	100-240VAC (50/60Hz)								
Energiafogyasztás	900w (2x450w)	450w	350w	350w	350w	350w	250w	100w	100w
Hőmérséklet	0° to 35° C (működési) -40° to 70° C (kikapcsolt állapotban)				0° to 40° C (működési) -40° to 70° C (kikapcsolt állapotban)				
Relatív pára-tartalom (nem sűrűsödő)	Működési: 10% - 90 % kikapcsolt állapotban: 5% - 95 %								
Magasság	0-tól 10,000 lábíg								
Biztonsági tanúsítvány	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, IEC 60825, 21CFR1040 CB license and report covering all national country deviations.								
EMI tanúsítvány	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)								

A McAfee Network Security Platform tulajdonságai

Szoftverösszetevők		M-8000	M-6050	M-4050	M-3050	I-4010 I-4000	I-3000	I-2700	I-1400	I-1200
Átfogó forgalom-vizsgálat	IP töredezettség-mentesítés és TCP stream újraszervezés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Részletes protokoll analízis	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Aszimmetrikus forgalom-monitorozás	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Protokoll-normalizálás	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Fejlett kikerülési védelem	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Törvényszéki adatgyűjtés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Protokoll alagutak	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Protokoll felfedezés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Aláírás érzékelés	Felhasználói aláírások	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Valós idejű aláírás frissítés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Rendellenesség érzékelés	Statisztikai rendellenesség	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Protokoll rendellenesség	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Alkalmazás rendellenesség	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
DoS érzékelés	Érték alapú észlelés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Önképző profil alapú érzékelés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Maximum DoS profilok	5000	5000	5000	5000	5000	5000	300	120	100
Behatolás-megelőzés	Támadások valós idejű megállítása	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Drop támadás csomagok/folyamatok	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Host karantén	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	TCP helyreállítás, el nem érhető ICMP	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Csomag loggolás	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Automatikus és felhasználói megelőzés	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Titkosított védelem	Titkosított támadások valós idejű megállítása	Nem	Nem	Nem	Nem	Igen	Igen	Igen	Nem	Nem
Belső tűzfal	Nem kívánt és kellemetlen forgalom blokkolása	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Biztonsági stratégia végrehajtás	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Rendelkezésre állás	Alapos failover	Igen	Igen	Igen	Igen	Igen	Igen	Igen (FE port)	Igen	Igen
Vezérlés	Parancs interfész (konzol)	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
	Vezetői kommunikáció	Védett csatorna	Védett csatorna	Védett csatorna	Védett csatorna	Ugyanaz minden modellhez	Ugyanaz minden modellhez	Ugyanaz minden modellhez	Ugyanaz minden modellhez	Ugyanaz minden modellhez

