

# McAfee Endpoint Security termékcsaládok

Erősebb biztonság kisebb működési költségekkel és egyszerűsített megfeleléssel

A biztonságos végponti környezet biztosítása a vállalkozás számára összetett feladat lehet. A kifinomult kártevő programok és a határok nélküli munkahely megkönnyíti a cyberbűnözőknek az információ- és eszközlopást. A szabályok az adatvédelem növelésére és a megfelelés ellenőrzésére kényszerítenek. A biztonságipont-termékek emelkedő száma pedig növeli a kezelési költségeket és bonyolítja a választ. A McAfee® Endpoint Security termékcsalád egyesíti az iparág vezető végponti biztonságot és adatvédelmet a páncélozott biztonság központi kezelésével, ami korszerűsíti a működést és megkönnyíti a megfelelést.

## Kulcsfontosságú előnyök

- Páncélozott védelem az összes végpont számára
- Alacsonyabb működési költségek központi kezeléssel
- A megfelelés egyszerűbb a hagyományos sablonokkal

„Az NSS Labs létrehozta az Operation Aurora támadás variánsait, és letesztelte a kártevők elleni szoftvert, hogy lássák, a hét termék közül melyik állítja meg a biztonsági réseket kihasználó és veszélyes rakománykódokat. A támadás láthatósági szintjének és az első felfedezés óta eltelt idő ismeretében úgy gondoltuk, hogy a legtöbb – ha nem az összes – termék kijávitáná a biztonsági rést. Azonban a hét tesztelt termék közül mindössze egy akadályozta meg megfelelően a biztonsági rés többszörös kihasználására irányuló támadásokat, demonstrálva ezzel a biztonsági résen alapuló védelmet (McAfee).”

— Az NSS Labs vizsgálata szerint a legtöbb végponti biztonsági termék nem rendelkezik „Biztonsági résen alapuló védelemmel”  
<http://nsslabs.com/nss-labs-in-the-news/nss-labs-finds-most-endpoint-security-products-lack-vulnerability-based-protection.html>

Már elmúltak azok a napok, amikor elegendő volt egy vírusirtó program. A mai veszélyforrások között folyamatos, állandóan változó férgek, kémprogramok, trójaiak, botok, rootkitek, hackerek, azonosságlopók és célzott támadások találhatók. A szakértők ezekkel dolgoznak, és hozzáférnek az alkalmazásokhoz bárhol, de a mobil eszközeik és laptopjaik – a Mac gépek is – veszélyeztethetik a hálózatot és a rendszereket, mikor visszatérnek az irodába. Az adatok megvédésére irányuló szigorú követelményekkel, valamint a szabályozásnak való megfelelés ellenőrzésével és jelentésével a kockázatok még nagyobbak, mint eddig. Az anyagi lehetőségek azonban takarékoságra intenek.

Összerakhatna egy gyűjteményt különálló termékekből, de soha nem érné el a McAfee Endpoint Security termékcsalád hatékonyságát. Ez azért van, mert mi integráljuk a technológiákat a koordinált, teljes megoldásokhoz, amelyek a legjobb védelmet nyújtják a mai többvektoros veszélyforrásokkal szemben. Az Endpoint Security termékcsalád megvédi Önt mind az öt veszélyforrástól – rendszer, e-mail, web, adat és hálózat.

Az integrált biztonság páncélszerű védelmet nyújt, de telepítése és kezelése könnyű. A McAfee Endpoint Security termékcsalád megerősíti a kártevő programokkal és az adatvesztéssel szembeni védelem rétegeit az iparág egyedüli nyílt biztonsági és megfeleléskezelési platformjával. A termékcsalád erős alapot ad a felhasználók, rendszerek és adatok biztonságossá tételéhez, s emellett a működtetési hatékonyság megkönnyíti a hatékony biztonság fenntartását.

## McAfee Total Protection for Endpoint – Enterprise Edition termékcsalád

Vezető megoldásunk páncélszerű védelmet nyújt az összes végpont, többek között Windows, Mac, Unix és Linux rendszerek, valamint a mobil eszközök számára. A zökkenőmentes integráció biztonságossá teszi a rendszereket és az adatokat a kifinomult kártevő programokkal szemben, mint amilyenek a botok vagy a „nulladik” napos támadások. Megvédi Önt, ha a készülék elveszik vagy ellopják, és blokkolja a nem megfelelő rendszereket, illetve az illetéktelen eszközöket, amelyek megpróbálnak hozzáférni a fontos üzleti rendszerekhez és az érzékeny adatokhoz.

A vezérlések ezen kombinációja ideális a modern vállalatok számára, ahol a felhasználók szabadságra vágyanak – valamint a mobilitásukkal és a rugalmasságukkal járó kockázatok elleni védelemre. A többplatformos támogatás, a hálózati hozzáférés vezérlése, a szabályzatauditálás, a webszűrés és a végponttitkosítás lehetővé teszi az igényeknek való megfelelést, miközben biztosítja a cégvezetők és a könyvelők által megkövetelt adatvédelmet és felelősséget.



#### McAfee Endpoint Protection – Advanced termékcsalád

A fejlett védelem megóvja a mai, határok nélküli munkaerőt a Windows-rendszereket fenyegető kifinomult kártevő programok és „nulladik” napos támadások ellen biztonságot nyújtó integrált, proaktív védelemmel. A központi szabályozásalapú kezelés, a hozzáférés-vezérlés és az auditálás segít az erőforrások biztonságának és megfelelésének megőrzésében.

#### McAfee Endpoint Protection termékcsalád

Legalapvetőbb védelmünk integrálva van a McAfee ePO szoftverrel, és megvédi a Windows-rendszereket a kifinomult kártevő programoktól és az illetéktelen eszközöktől. A kártevők elleni védelem, az eszközvezérlés és az alapvető e-mail- és webvédelem segítségével remekül megóvhatja hagyományos asztali számítógépeit és fix rendszereit, amelyek csak korlátozottan vannak kitéve az internetről érkező fenyegetéseknek.

#### A vezetés, mely csökkenti a működési költségeket

A McAfee ePolicy Orchestrator® (ePO™) szoftver egy egyszerű, központi platform, ami kezeli a biztonságot, védelmet nyújt, és csökkenti a biztonsági műveletek költségeit. Webalapú tulajdonsága révén bárhol könnyen elérhető, intelligens biztonságot nyújt, amely automatizált és aktív a gyors és hatékony döntések és a jobb vezérlés érdekében. Biztosítja a rendszer biztonsági szabályzatának való megfelelést – elhelyezkedéstől függetlenül –, és segít megakadályozni a mai kifinomult támadások által előidézett költséges üzleti összeomlásokat.

Ez a nyílt kezelési szerkezet kihasználja az egyetlen ügynök-egyetlen konzol kialakítás előnyeit. A régi stílusú pontmegoldásokhoz képest a mi korszerű szemléletünk lényegesen egyszerűsíti a védelmek és a hozzá kapcsolódó szabályok és szabályzatok telepítését és karbantartását. Kiküszöböli a több ügynök rendszerhatását és a több konzol döntéshozatali eredménytelenségét. Amikor a veszélyforrások és a szabályok változásakor a szabályzatokat át kell nézni, a frissítések gyorsan, pontosan és egyenletesen zajlanak le.

Ha a McAfee ePO platformot használja a végpontok, a hálózat, valamint a kockázati és megfelelési folyamatok összekötéséhez, teljes körű rálátást nyer az egész biztonsági és megfelelési környezetre, így az IT munkatársak teljes mértékben hasznosíthatják a vállalat minden pontjából származó biztonsági adatokat, és nem a több forrásból származó elszigetelt adatokra alapoznak. Összehasonlíthatja a végpontból, a hálózatból és az adatbiztonságból származó fenyegetéseket, támadásokat és eseményeket, valamint a megfelelési auditálásokat, hogy javítsa a biztonsági intézkedések és a megfelelési jelentések fontosságát

és hatékonyságát. Más kereskedő nem rendelkezik ezen biztonsági területeket átfedő, egységes integrált kezelési platformmal. A McAfee ePolicy Orchestrator leegyszerűsíti a biztonság kezelését, és csökkentheti az IT biztonsági és a megfelelés kezelési költségeit több mint 60 %-kal (forrás: MSI International 488 közepes és nagyméretű vállalat felmérése). És hogy még többet megspórolhasson a működési költségeken, nyílt szerkezetünk összeköti Önt a McAfee Security Innovation Alliance több mint 90 partnerének termékeivel.

#### Folyamatos teljesítmény-titkosítás

Az érzékeny adatok páratlan védelmével a vállalkozások megelőzhetik az információ elvesztését, és fenntarthatják az üzleti folytonosságot. Folyamatos teljesítmény-titkosítást nyújt a laptopok és a mobil eszközök számára, hogy megakadályozzák az érzékeny adatok elvesztését, különösen az elveszett vagy ellopott készülékeknél. A végponttitkosítással a szervezetek bármikor hatékonyan titkosíthatják és dekódolhatják készülékeiket a felhasználók vagy a rendszer teljesítményének megzavarása nélkül. Jelenléte biztosítja a biztonsági szabályzatok végrehajtását és a szabályozási megfelelés elérését.

#### Átfogó eszközkezelés

Akadályozza meg, hogy a kritikus adatok elhagyják a céget a kivehető adathordozókon, mint pl. USB-meghajtókon, iPodokon, Bluetooth eszközökön, írható CD-ken és DVD-ken. Eszközeinkkel figyelemmel kísérheti és vezérelheti az összes asztali és hordozható számítógép adatátvitelét – függetlenül attól, hogy a felhasználók és a bizalmas adatok hová mennek, még akkor is, amikor nem csatlakoznak a vállalati hálózathoz.

	McAfee Total Protection for Endpoint – Enterprise Edition termékcsalád	McAfee Endpoint Security – Advanced termékcsalád	McAfee Endpoint Protection termékcsalád
Egyetlen kezelési konzol	•	•	•
Valós idejű vírusvédelem és kémprogram elleni védelem	•	•	•
McAfee SiteAdvisor Enterprise Plus	•	•	•
Eszközvezérlés	•	•	•
E-mail szerver vírusvédelme és levélszemét elleni védelme	•	•	•
Asztali tűzfal	•	•	
Host Intrusion Prevention (Host IPS)	•	•	
Alkalmazások blokkolása	•	•	
Hálózati hozzáférés-vezérlés	•	•	
Asztali szabályozás auditálása	•	•	
Webszűrés – Állomás	•	•	
Végponttitkosítás	•		
Többplatformos és mobileszköz-támogatás	•		

**A McAfee létrehozta az iparág szabványát**

- A Gartner négy egymást követő évben a végpontbiztonság és a mobil adatvédelem vezetőjeként nevezte meg
- Elsőként kínál együgyenökös és egykonzolos megoldást a végpontbiztonsághoz
- Az első alkalmazás, amely a biztonsági termékek széles körét kezeli; egyetlen konzol nyújt biztonságot a végpont, a hálózat, az adatok, a web és az e-mail számára
- Az első termék, amely egyesítette a kezelési platformot a végpontbiztonsághoz és a megfeleléskezeléshez
- Az első termék, amely kezeli a McAfee és a harmadik fél által készített biztonsági eszközöket is
- Az első, amely kombinálja a szabályozásauditálást és a szabályozás kényszerítését egyetlen motorban
- Az első, amely kombinálja a végpontbiztonságot és az adatvédelmet egyetlen valóban integrált termékcsaládban

**„Nulladik” napos védelem és a biztonsági rés védelme**

Búcsúzzon el a vészhelyzeti javításoktól! Az állomásbehatalás megelőzése megóvja a végpontokat a kártevő programoktól, automatikusan frissülő aláírásai pedig megvédik az asztali számítógépeket és a szervereket a támadástól, miközben Ön az ütemezés szerint telepíti és teszteli a javítófájlokat. Szabadalmaztatott viselkedésalapú védelmünkkel kombinálva, amely megelőzi a buffer overflow támadásokat, a piacon elérhető legfejlettebb technológiát kapja a rendszer a biztonsági résék védelméhez. A McAfee Host IPS „nulladik” napos védelmet nyújtott a Microsoft kritikus biztonsági réseinek közel összes (90%) esetében.

**Hatékony szabályzatmegfelelés**

A McAfee ePO szoftver egyetlen platformot kínál a végpontbiztonság és a megfelelésauditálás kezeléséhez, megnyitva ezzel az utat a hatékonyság új szintjei előtt. A szervezetek megmérhetik a megfelelést a legjobb eljárás szabályzatoknak – ISO 27001 és CoBIT –, valamint a kulcsfontosságú ipari szabályzásoknak megfelelően, melyben megtalálható a Payment Card Industry Data Security Standard (PCI DSS), a Gramm-Leach-Bliley Act (GLBA), a Health Insurance Portability and Accountability Act of 1996 (HIPAA), a Sarbanes-Oxley Act of 2002 (SOX) és ezek nemzetközi változatai. A szabályozás auditálási funkcióját a Secure Content Automation Protocol (SCAP) érvényesíti, és lehetővé teszi az USA szövetségi ügynökségeinek, hogy könnyen megfeleljenek a Federal Desktop Core Configuration (FDCC) szabványnak.

**Fejlett e-mail vírus és levélszemét elleni védelem**

Az alkalmazás megvizsgálja a bejövő és kimenő e-maileknél a levélszemét-tartalmat, a nem megfelelő tartalmat és a káros vírusokat. A gyanús e-mailek karanténba kerülnek, így az e-mailes fenyegetések nem terjednek el, és nem érintik a hálózatot, illetve a felhasználókat. A vírusvédelmi réteg megvédi az e-mail szervereket, és elfogja a kártevő programokat, mielőtt azok elérnék a felhasználó beérkezett üzeneteit.

**Proaktív webbiztonság**

Számos webes fenyegetés csendes és láthatatlan a weben szörfözők számára. A megfelelés biztosításához és a webböngészés kockázatainak csökkentéséhez figyelmeztesse a felhasználókat az előforduló kártevő weboldalakra azok használata előtt. Engedélyezheti és blokkolhatja a weboldalakkal való hozzáférést, vezérelheti, hogy a felhasználók a vállalati hálózaton vagy azon kívül használják az internetet. A kifinomult

vezérlésben megtalálható a tartalomszűrés, valamint a felhasználók és a csoportok weboldal-hozzáféréseinek kényszerítése, teljes kezeléssel és jelentéssel.

**Rugalmas hálózathozzáférés-vezérlés**

A vállalati hálózatokhoz való hozzáférés vezérlése, a végpont biztonsági szabályzatának kényszerítése, és a végpontvezérlés integrálása a meglévő infrastruktúrákkal. Függetlenül attól, hogy a végpontok hogyan csatlakoznak a hálózathoz, a hálózathozzáférés-vezérlés felderíti és kiértékeli a végpont megfelelési állapotát, meghatározza a megfelelő hálózati hozzáférési szabályzatokat, és automatizált szervizelést kínál.

**A virtuális környezetek védelme**

A virtuális gépek azonos vagy nagyobb biztonsági nyomás alatt vannak, mint a fizikai rendszerek, és teljes védelmet igényelnek. A McAfee Endpoint Security termékcsalád támogatja a virtuális környezetek központi telepítését, így biztosítva azt, hogy ezen erőforrások mentesek legyenek a kártevő programoktól és az egyéb biztonsági kockázatot jelentő elemektől. Többet megtudhat a virtuális környezetekhez készült McAfee-megoldásokról, ha ellátogat ide: [www.mcafee.com/virtualization](http://www.mcafee.com/virtualization).

**McAfee Artemis Technology – mindig bekapcsolva, kártevő programok elleni valós idejű védelem**

A fejlett és folyamatos fenyegetések példa nélküli növekedésével a vállalkozások nem függhetnek azoktól a megoldásoktól, amelyek a végpontvédelemhez kizárólag aláírás-elemzést használnak. A fenyegetés felfedezésének időpontja és az aláírás végpontokon történő alkalmazásának ideje között egy 24–72 órás időrés található. Ez idő alatt az adatok és a rendszer ki vannak téve a fertőzésnek. A McAfee Artemis Technology eltünteti ezt az időrést, mert a McAfee Labs™ által összegyűjtött globális fenyegetések felismerésére alapozva valós idejű, mindig bekapcsolt védelmet nyújt. Az Artemis Technology karanténba helyezi vagy blokkolja a fenyegetést még az előtt, hogy az aláírás bármikor, bárhol kifejlődné.

**Védelem a McAfee Labs által**

A globális kutatás lábnyomával a McAfee Labs a legátfogóbb globálisfenyegetés-felismerést kínálja a piacon. Háttérben a több mint 400 szabadalommal, az internetet pásztázó szenzorok milliós nagyságrendű hálózatával és az összes lényeges fenyegetésvektor láthatóságával a McAfee Labs páratlan védelmet nyújt az ismert és a felbukkanó fenyegetésekkel szemben.

**Bizonyított és erőteljes technológia**

A McAfee világszerte közel 120 millió végpontot véd, köztük a világ legnagyobb vállalatának és kormányainak hálózatait. A McAfee folyamatosan az egyik legmagasabb észlelési aránnyal rendelkezik az AV-Comparatives szerint, megelőzve a Symantecet, a Kasperskyt, a Sophost, a Microsoftot és minden nagyobb vetélytársat az összes észlelés százalékos arányaiban. (Forrás: <http://www.av-comparatives.org/>)

**McAfee megoldásslolgáltatások**

McAfee SecurityAlliance™ partnereivel együtt a McAfee szolgáltatások széles körét nyújtja a biztonsággal összefüggő feladatok felmérése, megtervezése, végrehajtása, beállítása és kezelése érdekében. Bővebben itt olvashat: [www.mcafee.com/us/enterprise/services/product\\_consulting/](http://www.mcafee.com/us/enterprise/services/product_consulting/).

**McAfee műszaki támogatás**

A McAfee műszaki támogatástól származó programokkal minden gördülékenyen megy a telepítés közben, és azt követően is. Magasan képzett és tanúsítvánnyal rendelkező biztonsági szakértőink gazdag tudással és erőforrásokkal rendelkeznek, és biztosítják a biztonsági termékek folyamatos működését. Többet megtudhat itt: [mysupport.mcafee.com](http://mysupport.mcafee.com).

**További tudnivalók**

Menjen a [www.mcafee.com/us/enterprise/products/system\\_security/index.html](http://www.mcafee.com/us/enterprise/products/system_security/index.html) oldalra, vagy hívjon minket a 888-847-8766 számon a nap 24 órájában, a hét minden napján.

