

IBM Internet Security Systems termékek és szolgáltatások

Fontos megjegyzések

- **Segít a kritikus eszközök védelmében és csökkenti a költségeket az on-line fenyegetések elleni megelőző lépésekkel.**
- **Segít a teljes informatikai infrastruktúra biztosításában, így az IT-munkatársak a központi üzleti folyamatokra koncentrálhatnak.**
- **Segít a rosszindulatú támadások blokkolásában, miközben védi a hálózati sávszélességet és az elérhetőséget.**
- **Támogatja az üzletmenet-folytonossági erőfeszítéseket azzal, hogy csökkenti a kiesések miatti állásidőt.**
- **Javítja az alkalmazottak hatékonyságát a vírusok és kéretlen levelek blokkolásával.**
- **Menedzseli, megfigyeli és méri a vállalati biztonságot a rendelkezések betartásának támogatásához.**

Védelem biztosítása még a fenyegetések előtt

A mai biztonsági fenyegetések kevés lehetőséget hagynak a hibázásra. Az intelligens és pusztító on-line ellenségek elleni folyamatos megelőző védelemhez a vállalati biztonságnak magában kell foglalnia a technológiák és műszaki alapelvek folyamatosan fejlődő halmazát. Ezek olyan fontos eszközök, amelyeknek saját fejlesztését és karbantartását csak kevés szervezet engedheti meg magának.

A hatékony biztonság érdekében sok problémát le kell küzdeni. Képzett munkatársakra van szükség, akiket csak drágán lehet megszerezni, alkalmazni és megtartani, akik ráadásul lekötik az amúgy is elégtelen informatikai erőforrásokat a cég termeléséhez és növekedéséhez szükséges központi tevékenységek támogatása elől. Az egyre bonyolultabb kormányzati előírások

további nyomást gyakorolnak a vállalatokra a kötelező biztonsági szintek fenntartásának tekintetében. A vállalati biztonság egyensúlyának megtartása nehéz dolog: ha nem jól menedzselik, akaratlanul is blokkolhatja a szabályszerű forgalmat, elvesző vagy elkéső tranzakciókat eredményezhet, ami alááshatja a vásárlók elégedettségét, és a bevételek visszaesését eredményezheti. Végül pedig a biztonság ciklikusan emelkedő és gyakran megjósolhatatlan költségei nagyon megnehezítik a cégek számára a pénzügyi tervezést és erőforrás-optimalizálást.

Azért, hogy segítsen megfelelni ennek a sokféle kihívásnak, az IBM Internet Security Systems (ISS) a központilag menedzselte, sérülékenységi kutatásokra és többrétegű biztonsági technikákra épülő megelőző termékek és szolgáltatások széles választékát kínálja.

A teljes informatikai infrastruktúra védelme

Az IBM ISS a meglévő üzleti folyamatokkal szorosan integrált megelőző védelmet kínál a teljes infrastruktúra megerősítésére – az átjárótól a középpontig vagy a legtávolabbi végpontokig. Ennek alapvető eleme az IBM Proventia termékcsalád. Ez a vírusvédő, tűzfal-, VPN-, behatolásvédelmi és -megelőzési, alkalmazásvédelmi, spamellenes és tartalomszűrési megoldásokat tartalmazó robusztus és mindenre kiterjedő védelmi platform az IBM X-Force kutatási és fejlesztési csapata által gyűjtött információkra épül.

A központilag felügyelt Proventia termékek családja a következőket tartalmazza:

IBM Proventia Network Intrusion Prevention System – automatikusan blokkolja a rosszindulatú támadásokat, miközben védi a hálózati sávszélességet és az elérhetőséget. Az X-Force csapat kutatásai alapján ez a biztonsági alkalmazás kivételes, mivel megelőző jellegű védelmet kínál az ismeretlen fenyegetésekkel szemben.

IBM Proventia Network Multi-Function Security – még kiterjedtebb védelem alacsonyabb költség mellett; kombinálja a behatolásvédelmet a tűzfal- és VPN-szolgáltatásokkal, a viselkedés és aláírás alapján azonosított vírusok elleni védekezést, a webes szűrést és a kéréstlen levelek kivédését. Ezt az egyesített fenyegetéskezelési (UTM) eszközt úgy tervezték, hogy automatikus védelmet nyújtson több mint ezer sérülési lehetőség, több mint 120 ezer vírus, az ismeretlen vírusok és egyéb vegyes fenyegetések több mint 93 százaléka és a kéréstlen levelek 95 százaléka ellen.

IBM Proventia Network Anomaly Detection System – bővíti a hálózati információkat és javítja a biztonságot a meglévő infrastruktúra-eszközökről származó hálózati forgalmi adatok auditálásával. A hálózati működés elemzésével a megoldás világos képet ad a hálózat gyenge pontjairól az aktív biztonsági fenyegetések, kockázatos felhasználói viselkedésformák, teljesítményproblémák és biztonsági előírások megsértésének automatikus érzékelésével.

IBM Proventia Network Enterprise Scanner – megvizsgálja a teljes hálózatot az eszközök és a gyenge pontok felderítésére, az eredményeket fontossági sorba rendezi, védelmi tevékenységeket rendel hozzájuk és jelenti. Az X-Force csapat mindenre kiterjedő, az iparágban nagy népszerűségnek örvendő sérülékenységi adatbázisát használó megoldás sérülékenységmenedzsmentet kínál a natív, a munkafolyamatok által támogatott hibajegykezelés használatával azért, hogy menedzsmenttevékenységeket biztosíthasson az infrastruktúra minden pontján.

IBM Proventia Web Filter – a szöveges és képes elemzést, valamint a világ egyik legnagyobb URL- és képadatbázisát ötvöző kifinomult technológia használatával blokkolja a nemkívánatos webes tartalmakat. Nagy teljesítményű és pontos. Javítja a hatékonyságot és az internethasználati irányelvek betartását.

IBM Proventia Mail Filter – figyeli az e-mail forgalom tartalmát, és automatikusan blokkolja a kéréstlen leveleket és más illegális tartalmakat. A kidolgozott elemzési technikákat egy több mint 200 ezer releváns spammintával és több mint 20 millió weboldalt tartalmazó adatbázissal kombináló megoldás azonosítja az ártalmatlan e-maileket és azonnal továbbítja azokat, miközben blokkolja a nemkívánatos e-maileket.

IBM Proventia Server Intrusion Prevention System – tűzfal és alkalmazásfelügyeleti funkciót kombinál olyan megelőző technológiákkal, mint a puffertúlcsoordulás elleni védelem és a behatolásvédelem. Ez a többrétegű megoldás automatikus biztonsági tartalomfrissítéseket fogadva védelmet nyújt a gyenge pontok ellen a szállítói javítások alkalmazása előtt, és biztonságot nyújt mind a Microsoft® Windows®, mind a Linux® operációs rendszerű szervereknek.

IBM Proventia Desktop Endpoint Security – megelőző jelleggel blokkolja a támadásokat, még mielőtt azok rendszerleállást vagy az alkalmazott munkaidejének kiesését okoznák, és drága help-desk hívásokat eredményeznének. Ez az ügynök egymagában személyi tűzfal, behatolásvédelem, puffertúlcsoordulás-védelem, alkalmazásvédelem és vírusvédelem is, hogy az asztali rendszerek védettek legyenek és megfelelhessenek a vállalati normáknak.

IBM Proventia Management

SiteProtector system – menedzseli, megfigyeli és méri a vállalati biztonságot, segít a szabályok betartásában a megfelelő gondosságot felmutató jelentésekkel, valamint átállási funkciókat biztosít az üzletmenet-folytonosság érdekében. Azzal, hogy egyetlen konzolt kínál a biztonsági termékek teljes skálájának menedzseléséhez, a SiteProtector rendszer csökkenti az informatikai és biztonsági munkatársak terhelését, és az egész vállalatra kiterjedő képet ad a biztonsági helyzetről.

Az IBM ISS kiegészítő termékeket is kínál, amelyek szintén igazodnak a Proventia termékcsaládhoz, amely segít abban, hogy a védelem megelőzze a fenyegetéseket. Ezek az alábbiak:

IBM RealSecure Server Sensor – automatikus valós idejű behatolásvédelmet és -érzékelést kínál az események, gépnaplók, bejövő és kimenő hálózati tevékenységek elemzésével a kritikus fontosságú vállalati kiszolgálókon azért, hogy blokkolhatók legyenek a kritikus eszközöket károsító rosszindulatú tevékenységek. Ez a robusztus ajánlat érvényesíti a beépített aláírásokat és kifinomult protokollelemzést kínál viselkedésminta-halmazokkal és automatikus eseménymegfeleltetéssel az ismert és ismeretlen támadások kivédésére.

IBM RealSecure Network – hálózati behatolásvédelmi és kivédési funkciók,

amelyek figyelik a hálózati szegmenseket egy központosított műveleti és menedzsmenti keretrendszeren belül. A termék kivételes hálózati biztonsági teljesítmény elérését teszi lehetővé, valamint iparágvezető pontosságot kínál a rosszindulatú fenyegetések felderítésénél.

A kritikus üzleti eszközökre irányuló on-line fenyegetések mérséklése
Az IBM ISS világszínvonalú biztonsági szolgáltatásokkal egészíti ki termékcsaládját, amelyek segítenek a szilárd biztonsági stratégia kialakításában, megvalósításában és karbantartásában.

Az IBM Professional Security

Services szakértői biztonsági konzultációt biztosítva mindenféle méretű szervezetnek segítenek a kockázatok csökkentésében, a szabályozások betartásában, az üzletmenetfolytonosság fenntartásában és a biztonsági célok elérésében. Az IBM Professional Security Services tanácsadói százszázalékosan a biztonságot tartják szem előtt és bevált konzultációs módszereket használnak a globálisan elfogadott ISO 17799-es követendő biztonsági megoldások alapján. Ez a biztonsági szakértői csoport szabadalmaztatott eszközkészletek, a legfrissebb fenyegetési információk és fejlett ellenintézkedések használatával hatékony biztonsági programokat állít össze az üzleti folyamatok védelmére és javítására. A szolgáltatási ajánlatok:

IBM Penetration Testing – felderíti a hálózat gyenge pontjait, és méri a valós kockázatokat azzal, hogy egy biztonságos és felügyelt gyakorlat keretében demonstrálja a hálózati támadásokra jellemző rejtett és ellenséges tevékenységeket. A Penetration Testing több, mint egy szokásos eszköz- vagy hálózatvizsgálat; ez az iparág legátfogóbb megoldása. Szakértő tanácsadóink tapasztalataikat felhasználva a hacker szemével veszik szemügyre hálózatát, és ennek eredményeit fontossági sorba rendezett, jól alkalmazható kárenyhítési lépésekké foglalják össze a biztonsági helyzet javítására.

IBM Application Security Assessment – részletes áttekintést és az egyedi alkalmazások célzott kódelemzését nyújtja a biztonsági szempontból gyenge pontok feltérképezéséhez. Segít az értékes adatokat tároló alkalmazások biztosításában. Részletes eredményeket és megbízható ajánlásokat ad az alkalmazások biztonságosságának fokozásához.

IBM Information Security Assessment – kiértékeli az általános biztonsági állapotot, beleértve a biztonsági irányelveket, eljárásokat, vezérlőeszközöket és mechanizmusokat, valamint a fizikai biztonságot, a hálózatokat, szervereket, asztali gépeket és adatbázisokat. Ezzel a mindenre kiterjedő felméréssel azonosíthatók az informatikai infrastruktúra gyenge pontjai és a felügyelet, irányelvek és eljárások hiányosságai. Az iparág követendő eljárásaira épülő Information Security Assessment tervet ad az általános biztonsági helyzet javítására.

IBM Payment Card Industry Assessment – segít a Payment Card Industry (PCI) adatbiztonsági szabvány betartásában. Az IBM ISS-t a PCI Security Standards Council által nyilvántartott Qualified Security Assessor (QSA) és Approved Scanning Vendor (ASV). A felméréseket a PCI-felmérések vezetésére feljogosított konzultánsok vezetik. A fizetési alkalmazások felmérésére is van mód, ezeket Qualified Payment Application Security Professional (QPASP) minősítéssel rendelkező konzultánsok végzik.

IBM Emergency Response Services – incidensválaszokat, felkészültségi tervezést és igazságügyi elemzéseket tartalmaz, amelyeket biztonsági szakértőink végeznek. Az előfizetéses szolgáltatásként és igény szerinti szolgáltatásként is elérhető termék esetében az Emergency Response (vészhelyzeti) csapat gyorsan reagál a folyamatban lévő támadásokra, illetve a szervezettel együtt dolgozva egyéni reagálási terveket készítenek a jövőbeli támadások hatásának csökkentésére. Emellett a biztonsági szakértők közreműködhetnek egy számítástechnikai igazságügyi vizsgálat, feltérképezés vagy per során az információs biztonsági réseket kihasználó elkövetők megtalálásában és bíróság elé állításában.

IBM Policy Development – meghatározza a kritikus folyamatokkal, technológiákkal, menedzsmenttel és adminisztrációval kapcsolatos döntéseket irányító stratégiákat és irányelveket az informatikai eszközök védelmére és a rendelkezések betartására.

IBM Network Architecture Design Services – kiértékeli a meglévő hálózati architektúrát és együttműködik az Ön munkatársaival egy részletes biztonsági architektúra-felépítés kidolgozásában az informatikai környezet védelme érdekében.

IBM Technology Implementation Planning – a hálózati műveleteket a lehető legkisebb mértékben érintő biztonsági megoldási terv elkészítésével segít abban, hogy a legjobban kihasználhassa biztonságtechnológiai adottságait. Segít a biztonsági megoldások folyamatos menedzselésének és karbantartásának megtervezésében.

IBM Deployment Consulting – segíti az IBM ISS megoldásokba fektetett beruházások megtérülési értékének maximalizálásában. Az IBM ISS biztonsági szakértői közreműködnek a telepítés, beállítás és finomhangolás műveletében, és segíthetnek az új ISS megoldásokra való átállás során is.

IBM Staff Augmentation – IBM ISS biztonsági szakértőkkel bővíti a belső erőforrásokat. A házon belüli csapat kibővítéseként működő IBM ISS tanácsadók költséghatékony biztonsági módszertant bocsátanak rendelkezésére és lehetőséget hagynak a belső munkatársaknak arra, hogy a normál üzleti folyamatok fenntartására koncentráljanak.

IBM Vertical & Regulatory QuickStart Programs – felbecsüli a meglévő biztonsági rendszer, valamint az ipari és kormányzati szabályok a Supervisory Control and Data Acquisition (SCADA), a Sarbanes-Oxley, a Health Insurance Portability and Accountability Act (HIPAA), a Gramm-Leach-Bliley Act és a Federal Information Security Management Act (FISMA) betartásának hiányosságait. Részletes ajánlásokat fogalmaz meg a megfelelés elérésével és a biztonsági helyzet javításával kapcsolatban.

IBM Security Awareness Training – egy on-line oktatási program használatával segíti az alkalmazottak kiképzését a követendő biztonsági eljárások és irányelvek tekintetében. Az Awareness Training mellett az IBM ISS sokféle egyéb, az ügyfeleknél vagy külső helyszíneken biztosított oktatással segít abban, hogy a lehető legtöbbet hozhassa ki az IBM ISS megoldásokra fordított befektetésekből.

Valós idejű, nonstop biztonsági menedzsment
Nagyon kevés szervezet rendelkezik olyan erőforrásokkal, amely lépést tud tartani az örökké változó, a vállalat működését és a profitot veszélyeztető internetes fenyegetésekkel. A vállalati biztonság heti 7x24 órás feladat, amelynek része a javítások menedzselése a változatos informatikai rendszerekben, valamint az alkalmazottakat, szállítókat és vásárlókat érintő biztonsági irányelvek betartatása.

Az IBM Managed Security Services mindenre kiterjedő kiszervezett megoldásokat kínál a valós idejű biztonsági menedzsmentre, beleértve a rendszerfigyelést, a sürgősségi válaszlépéseket és a folyamatos, 24 órás védelmet – mindezt a házon belüli biztonsági erőforrások költségének töredékéért. Ezek a következők:

IBM Managed Protection Services – az iparágvezető, teljesítményalapú szolgáltatásszint-szerződését kínálva kényelmes és megbízható átmenetet kínál a hálózati védelem átadására egy megbízható biztonsági partnernek. Ezek a védelmi megoldások jóval többet kínálnak, mint a sima eseménymegfigyelést és eszközmenedzsmentet: teljesítményalapú szolgáltatásszint-szerződéseket, amelyek 50 ezer USD értékű pénzvisszafizetést nyújtanak az ügyfél számára egy biztonsági rés esetén.* A Managed Protection Services valós idejű, napi 24 órás megfigyelést, menedzsmentet és kiterjesztést biztosít a többféle platformon és operációs rendszerrel működő hálózatok, szerverek, asztali rendszerek és vezeték nélküli alkalmazások számára.

IBM Managed and Monitored Firewall Services – a tűzfalnaplók mindenre kiterjedő nonstop szakértői megfigyelése, menedzselése és elemzése a folyamatosan változó fenyegetések észlelésére, megelőzésére és visszaverésére. A szolgáltatás többféle módon vehető igénybe a meglévő biztonsági beruházások értékének maximalizálására, a házon belüli megoldások költségének töredékéért.

IBM Managed IDS & IPS Services – a házon belüli behatolásvédelmi (IPS-) és behatolásészlelési (IDS-) megoldásoknál jelentősen olcsóbban segíti a hálózat és a szerverek védelmét a hálózaton belülről és kívülről érkező támadások ellen. A szolgáltatás az IDS-események átfogó, heti 7x24 órás megfigyelését, menedzselését és elemzését biztosítja, valós idejű válaszlépésekre és kiterjesztésre adva módot, de segít a törvényszéki vizsgálatok és a helyreállítás során is.

IBM Security Event and Log Management Services – segít abban, hogy a szervezetek egyetlen hézagmentesen illeszkedő platformot alakítsanak ki a különféle biztonsági technológiákról szóló információk összegyűjtésével a biztonsági és hálózati események trendjeinek archiválására, összevetésére és nyomon követésére a válaszlépések és a kárenyhítési munkafolyamatok egyidejű menedzselése mellett. Az ügyfelek lehetőséget kapnak a sokféle eszköztípuson működő operációs rendszerek és alkalmazások naplójának lekérdezésére egyetlen közös felületen. Ezzel drámai mértékben felgyorsítható a nagyszámú eszközön végrehajtott biztonsági vizsgálatok időtartama. Az IBM ISS archiválja is ezeket a naplóadatokat, rendkívül hatékonyan korszerűsítve a megfelelési műveleteket.

IBM Vulnerability Management Service – automatizálja a sérülékenységmenedzsment életciklusát, miközben láthatóvá teszi az összes potenciális kockázatot hordozó területet. Ez a kulcsrakész szolgáltatás fenntarthatóvá teszi az üzleti folyamatokat a szerverek, tűzfalak, kapcsolók és más eszközök valós idejű menedzselésével és elemzésével. Egyesítve a menedzselte szkenelési szolgáltatásokat a munkafolyamat- és esetkezeléssel, védelmezi a hálózati infrastruktúrát a potenciális üzleti veszélyt jelentő behatolásoktól.

IBM ISS X-Force Threat Analysis Service – személyre szóló információkat ad a hálózati biztonságot befolyásolni képes fenyegetések széles skálájáról. Az IBM ISS biztonsági műveleti központok belső hálózatáról származó kiemelkedő minőségű, valós idejű kockázati információkat és a megújult X-Force kutatási és fejlesztési csapattól származó biztonsági információkat egyesítő szolgáltatás a globális on-line fenyegetési helyzet részletes és személyre szabott elemzését kínálja.

A biztonsági műveletek figyelése egy központosított irányítóközpontból
Az IBM ISS Virtual-Security Operations Center (Virtual-SOC) nevű terméke lehetőséget ad a (menedzselte vagy nem menedzselte, az IBM ISS-től vagy más szállítótól származó) biztonsági műveletek figyelemmel kísérésére és menedzselésére a Virtual-SOC portálon, egyetlen webes konzolon keresztül. A Virtual-SOC valójában az IBM Internet Security Systems saját hat globális műveleti központjának teljesítményét biztosítja az ügyfelek Virtual-SOC portáljainak, teljes hozzáférést nyújtva a következőkhöz:

- *A megújult X-Force csapat biztonsági információi*
- *Nonstop megfigyelés és menedzsment az év minden napján*
- *Mindenre kiterjedő IBM ISS tanácsadási szolgáltatások*
- *Hibajegykezelés, nyomkövetés, riasztás, kiterjesztés és válasz*
- *Jelentések, archiválás és visszaállítás*
- *Élő együttműködést az IBM ISS biztonsági szakértőivel*

Miért éppen az IBM Internet Security Systems?
A megelőző jellegű biztonsági funkciókhoz iparágvezető kutatásra, a támadási trendeket és technikákat felmérni képes éles szemre, valamint korszerű és megfizethető platformra van szükség – csak így biztosíthatók tudásalapú speciális biztonsági megoldások. Az IBM ISS biztosítja a megelőző jellegű biztonsági szolgáltatásokhoz szükséges kiterjedt tudást, innovatív kutatási módszereket és összetett technológiákat. Gyakorlott és hivatalos minősítéssel rendelkező tanácsadóink, tervezőink, projektmenedzsereink és a tárgyhoz értő szakértőink felkészültek arra, hogy a teljes informatikai infrastruktúra (a hálózati újtárhoztól az asztali rendszerekig) védelmére készített megelőző jellegű biztonsági termékek és szolgáltatások átfogó platformját biztosítsák szervezete számára.

További információk
Ha többet szeretne megtudni az IBM Internet Security Systems termékeiről és szolgáltatásairól, kérjen konzultációs időpontot az IBM szakértőtől. Hívja az (1) 382-5500 telefonszámot, küldjön egy e-mailt az info@hu.ibm.com címre, vagy látogasson el a következő weboldalra:

ibm.com/hu/services



IBM Magyarországi Kft.

H-1117 Budapest,
Neumann János u. 1.
Hungary

Az IBM Magyarország honlapjának címe:

ibm.com/hu

Az IBM, az IBM logó, az ibm.com, a Proventia, a RealSecure, a SiteProtector és az X-Force az International Business Machines Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A Linux Linus Torvalds védjegye az Egyesült Államokban és/vagy más országokban.

A Microsoft és a Windows a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

Más vállalatok, termékek vagy szolgáltatások nevei mások védjegyei, szolgáltatásvédjegyei vagy más jogcímű tulajdonai lehetnek.

Az IBM-termékekre és -szolgáltatásokra történő hivatkozás nem jelenti azt, hogy az IBM ezeket más országokban is forgalmazni akarja.

- * Pénzvisszafizetés (csak az IBM Managed Protection Services Premium szintjénél):
Ha az Level IBM Internet Security Systems nem felel meg a Security Incidents Prevention garanciában megfogalmazottaknak, akkor minden nem megfelelés esetén 50 ezer USD jár az ügyfélnek. További részletekért olvassa el az IBM Internet Security Systems SLA-kat.

Készült az Egyesült Államokban.
02-07

© Copyright IBM Corporation 2007
Minden jog fenntartva.