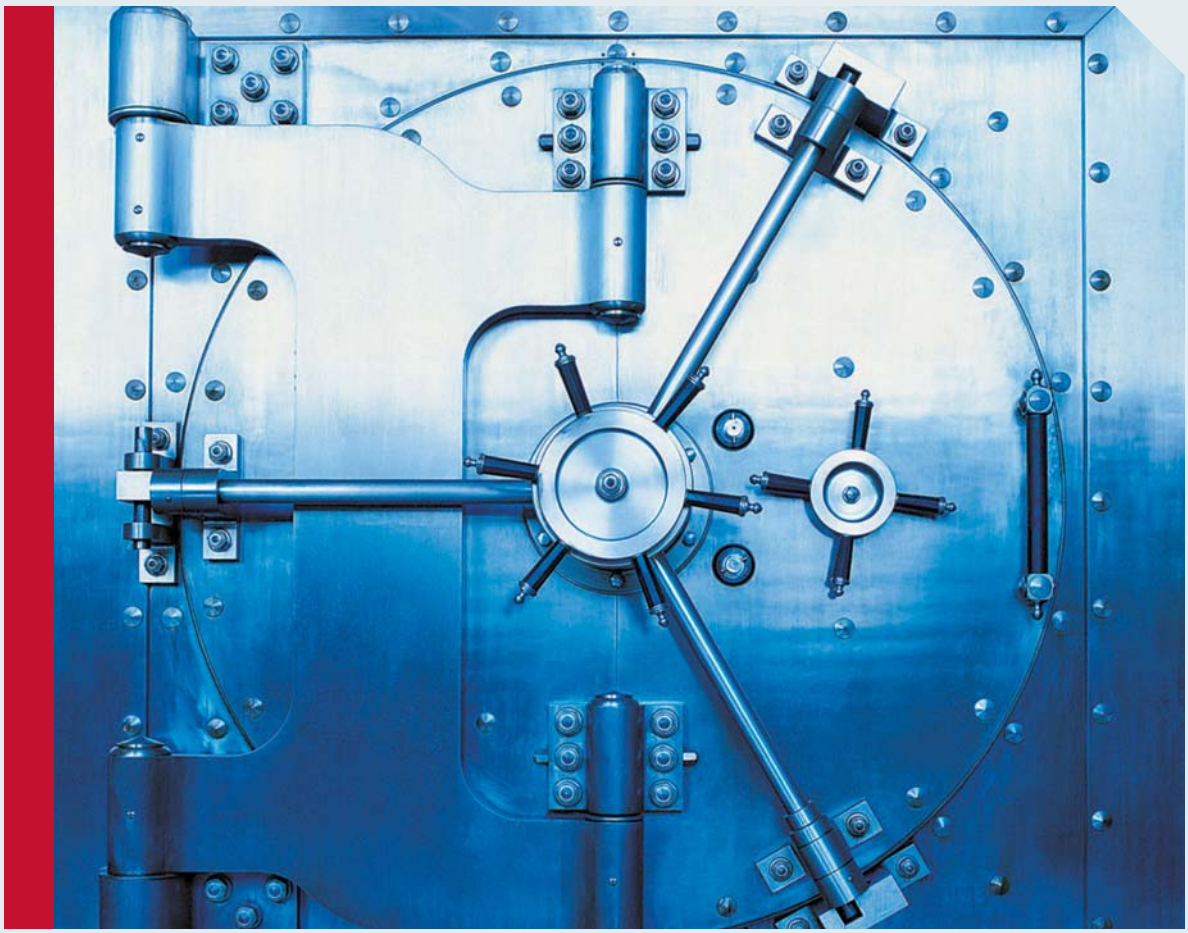
INTELLIGENS HÁLÓZATOK



INTELLIGENS HÁLÓZATOK

integrált hálózati biztonsággal

A hálózatokat érő minden eddiginél súlyosabb támadások csökkentik a hatékonyságot, hátráltatják az ügyfelek kiszolgálását, időkiesést okoznak, és így veszélyeztetik az egész üzletmenetet. A vállalat működésének és jó hírének szempontjából kiemelkedően fontos a támadásoknak ellenálló, integrált hálózatbiztonsági rendszer. Azonban ideje lenne túllépni a hálózat puszta védelmén, hiszen biztonsági és hálózati beruházásaikból a szervezetek stratégiai előnyt kovácsolhatnak.

Mivel a hálózat működése mindenre kihat, az infrastruktúra összes fontosabb pontján beépített, automatikus funkciókkal kell gondoskodni a védelemről. Az integrált biztonsági megoldással kiküszöbölhetők a felesleges átfedések, és csökkenthető az informatikai szakemberek terhelése. Az így létrejövő hatékony és az egész hálózatra kiterjedő védelem további előnye, hogy miközben kívül tartja a támadókat, lehetővé teszi a hálózat egyes részeinek biztonságos megnyitását az ügyfelek, beszállítók és üzleti partnerek számára. A megbízható felhasználóknak nyújtott, főbb rendszerekre kiterjedő biztonságos kapcsolat olyan hatékony együttműködést tesz lehetővé, amelynek pénzben is kifejezhető haszna biztosítja a beruházás folyamatos megtérülését.

INTELLIGENS HÁLÓZATOK
integrált hálózati biztonsággal

A Cisco „önvédő hálózatában” a biztonsági funkciók az infrastruktúra valamennyi eszközére kiterjednek. A Cisco intelligens hálózati koncepciója egy sor irányelvet határoz meg az infrastruktúra komponenseinek rendszerszemléletű integrálására. A hibákkal szemben ellenállóbb, egységes hálózat könnyebben hozzáigazítható a szervezet mindenkori igényeihez.

VALÓBAN BIZTONSÁGOS VÁLLALATÁNAK, INTÉZMÉNYÉNEK INFORMATIKAI HÁLÓZATA?

A hálózatokat veszélyeztető támadók nemcsak különösen találékonyak, de rendkívül hatékonyak is. Egyre újabb fejlesztéseikkel a biztonsági termékek és a hálózatra csatlakozó eszközök gyenge pontjain ütnek rést. Ezért a hálózatbiztonsági szakembereknek folyamatos készenlétben kell állniuk, hogy ellenintézkedéseket tegyenek. Amikor 2004. áprilisában a nagy pusztítást okozó Sasser vírus lecsapott, az egyetlen hatásos ellenszer egy mindössze tizennyolc napja elérhető hibajavítás volt. A hibajavítások telepítése az összes rendszerre és az új biztonsági technológiák gyors bevezetése azonban jelentős kihívás. A személyi számítógépek és szerverek védelmén kívül a rendszergazdák feladata biztonságosan üzemeltetni az értékesítési pontokon működő terminálokat, a hardveres riasztórendszereket, sőt a vírustámadásokkal fenyegetett, Microsoft Windows alapokra épülő létesítményfelügyeleti rendszereket is. Mivel számos eszköz és az azokon futó alkalmazások közvetlenül kapcsolódnak a hálózathoz, a támadásoknak kitett hálózat üzleti szempontból veszélyes környezet.

A veszélyforrások és a támadások száma immár oly nagy, hogy nem érdemes velük egyenként fölvenni a harcot. Az eredményesebb és hatékonyabb védelem érdekében a szakembereknek automatikus hálózati veszélyfelismerő és elhárító megoldásokat kell bevetniük.

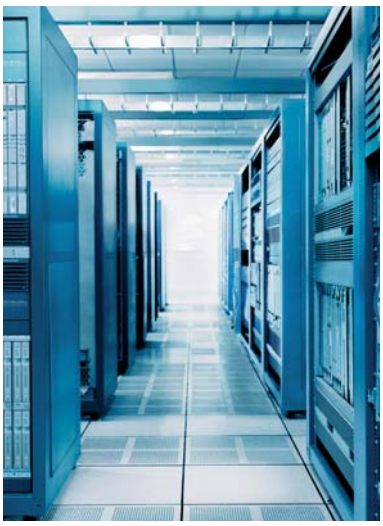
A Cisco intelligens hálózati szolgáltatásaival fölvértezett infrastruktúrában a hálózat hatékonyabban védekezik az ismert vírusok ellen, és alkalmazkodik az új veszélyforrásokhoz a megadott szabályok alapján. Mindez egy gyors, minden részletre kiterjedő és a körülményekhez rugalmasan illeszkedő védelmi rendszerben zajlik. A hálózati események pontos követése kulcskérdés az üzleti prioritásokat is figyelembe vevő, összehangolt védekezés szempontjából.

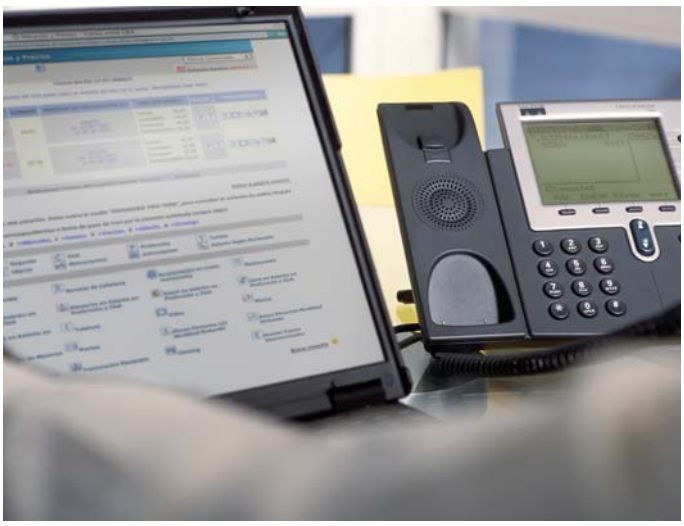
INTELLIGENS HÁLÓZAT ÉS BIZTONSÁG

A Cisco intelligens hálózati megoldása szisztematikus megközelítésmódjával integráltan kezeli a hálózatot és az azon futó alkalmazásokat. A rugalmas szabályokkal a rendszer az üzleti folyamatokhoz igazítható. A biztonságot, felügyeletet vagy kommunikációt érintő szabályok bármikor gyorsan módosíthatók, és a változtatások automatikusan tükröződnek a hálózat egészében.

A Cisco Systems biztonsági koncepciójának fontos ismérve, hogy a védelmi funkciókat az infrastruktúra elemeibe (pl. kapcsolók, útválasztók, végpontok) integrálja, és így rendszerszemléletű felügyeletet biztosít. Ezáltal a biztonság a hálózat szerves részévé válik. Az integrált biztonsági funkciók a hálózatvédelmi alkalmazásokkal együttműködve kiküszöbölik az egymástól elkülönülő rendszerekre jellemző biztonsági réseket, miközben több és áttekinthetőbb információt szolgáltatnak a szervezet egészét érintő biztonsági problémákról, így a szakemberek felkészültebben szállhatnak szembe a hálózat ellen irányuló támadásokkal.

A rendszergazdák által beállított szabályok érvényesítéséről automatikus munkafolyamatok gondoskodnak. Az egyes szabályok a különböző üzleti célkitűzéseknek megfelelő kockázatmérséklési stratégiákat fordítják le konkrét informatikai és hálózati követelményekre. A rendszergazdák a mindenkori helyzethez igazodva módosíthatják a biztonsági szabályrendszert. Ezzel biztosítható, hogy a védelmi intézkedések pontos és helyes információkon alapuljanak, és megfeleljenek a helyi és nemzetközi előírásoknak.





A Cisco biztonsági megoldásai szabályközpontú felügyelettel gondoskodnak az alapvető üzleti folyamatok és értékes adatok védelméről. A hálózati intelligencia, a biztonsági alkalmazások, a szabályközpontú felügyelet, valamint az automatikus munkafolyamatok ötvözete kellően hatékony, rugalmas és önmagát védő infrastruktúrát eredményez.

MINDENRE KITERJEDŐ VÉDELEM, NAGYOBB HATÉKONYSÁG

Napjaink biztonsági környezetének nélkülözhetetlen része az átfogó megközelítési módot alkalmazó, intelligens hálózat. A rendszergazdák korábban a hálózatot kívülről fenyegető veszélyek elhárítására helyezték a hangsúlyt. Ma már azonban számos veszélyforrás a rendszeren belül jelentkezik. Emögött állhat az alkalmazottak szándékossága, de véletlenül is előfordulhat, hogy valaki megfelelő védelem nélkül, távoli eléréssel csatlakozik a hálózathoz, és akaratlanul vírussal fertőzi meg a rendszert.

Akár belülről ered a fenyegetés, akár kívülről, ma már a mobil számítógépektől a nagy teljesítményű útválasztókig minden eszköz potenciális támadási felületet jelent. Ezért a hálózat minden egyes pontjának egyben védelmi állásként is kell szolgálnia. A biztonsági szabályrendszer bevezetésére és a hálózati pontok ellenőrzésére maga a hálózat a legalkalmasabb, hiszen minden eszközzel, rendszerrel, adattal és felhasználóval kapcsolatban áll. A hálózati biztonsági rendszer további előnyei közé sorolhatók még az alábbi szempontok:

- **Költségmegtakarítás –** A teljes hálózati infrastruktúrát lefedő, rendszerszintű biztonsági megközelítés jól hasznosítja az addigi beruházásokat, mivel kiterjeszti a meglévő és új hálózatvédelmi mechanizmusok funkcióit.
- **Dinamizmus –** A biztonsági szabályrendszer módosításai egy helyről, egyszerre és gyorsan végrehajthatók akár egy világcég teljes rendszerében is, ami automatikus, azonnali és a hálózat egészére kiterjedő védelmet biztosít.
- **Integráció –** A Cisco biztonsági alkalmazásai maximálisan kihasználják a Cisco hálózati eszközeiben, hálózati szoftvereiben, illetve az infrastruktúra hardvereszközeiben rejlő intelligens hálózati szolgáltatásokat.
- **Automatizálás –** A rendszergazda által beállított szabályok alapján a hálózat azonnal, automatikus ellenintézkedésekkel reagál a biztonsági eseményekre.

Az átfogó – belső vagy külső, rosszindulatú avagy nem szándékos eredetű – veszélyeket egyaránt kizáró védelem biztonságos együttműködést tesz lehetővé a hálózaton, és egyben fokozza a hatékonyságot is. Az ügyfelek és a látogatók anélkül csatlakoztathatják saját mobil számítógépeiket a világhálóhoz a vezeték nélküli hálózaton keresztül, hogy azzal bármilyen módon veszélyeztetnék a hálózat biztonságát. A szállítók és a partnerek is biztonságosan kapcsolódhatnak a vállalati hálózathoz úgy, hogy csak a számukra engedélyezett adatokhoz férhetnek hozzá. Az alkalmazottak otthonukból vagy üzleti útjuk során bárhonnan azzal a megnyugtató érzéssel léphetnek be a hálózatba, hogy véletlenül sem kerülhet tőlük vírus a rendszerbe. A hatékonyabb együttműködés a belső munkacsoportok, a beszállítói lánc különböző szereplői, illetve az egyes részlegek között pénzben is kifejezhető hasznot hoz.

AZ INTELLIGENS HÁLÓZAT MŰKÖDÉS KÖZBEN

A hálózati hozzáférés-szabályozás (Network Admission Control – NAC) olyan rendszerszintű biztonsági megoldást kínál, amely automatikusan megakadályozza, hogy a vírusok bejussanak a vállalati – intézményi hálózatba. Az átfogó hálózati és biztonsági szolgáltatásokkal rendelkező NAC iskolapéldája a Cisco intelligens hálózati megoldásainak.

Ha egy felhasználó – közvetlen vagy vezeték nélküli kapcsolaton keresztül – be akar lépni a hálózatba, akkor a NAC-ot futtató útválasztó először ellenőrzi, hogy a felhasználó rendszere rendelkezik-e biztonsági tanúsítványokkal (pl. vírusvédelmi szoftver vagy az operációs rendszer hibajavításai). Ha igen, akkor az útválasztó lekérdezi a megfelelő jogosultságellenőrző szabályt tároló kiszolgálót, amely ellenőrzi, hogy a megadott tanúsítványok megfelelnek-e a biztonsági előírásoknak. Amennyiben a NAC mindent rendben talál, engedélyezi a kapcsolódást a rendszerhez.

Ha azonban a felhasználó rendszere nem felel meg az előírásoknak, a NAC automatikusan gondoskodik annak frissítéséről. Ha például egy személyi számítógép csatlakozni próbál a hálózathoz, de nem rendelkezik a vírusvédelmi szoftver legújabb változatával, akkor azt a NAC a karantén zónába irányítja át. Itt található a legújabb vírusvédelmi szoftverrel rendelkező szerver, amely pótolja a karanténba zárt rendszer hiányosságait. Ebben az esetben a szerver automatikusan telepíti a hiányzó szoftvert, és ezután a felhasználó már csatlakozhat is a hálózathoz. Ha a távoli rendszer vírussal is fertőzött, akkor a NAC nemcsak feltelepíti a legújabb vírusvédelmi szoftvert, hanem megkeresi és el is távolítja a vírust, mielőtt engedélyezi a felhasználó csatlakozását a hálózathoz.

A NAC két további szolgáltatást is hasznosít: a Cisco Security Agentet (CSA), amely kivédi az ismeretlen támadásokat, és megakadályozza, hogy azok a hálózaton belül rendellenes viselkedést okozzanak, valamint a Cisco Trust Agentet, amellyel a NAC például ellenőrizheti, hogy a rendszeren telepítve van-e a CSA vagy a vírusvédelmi szoftver legújabb verziója. A NAC 2-es fázisa Ethernet kapcsolókat és vezeték nélküli hozzáférési pontokat is támogat, és ezáltal a szolgáltatás szinte valamennyi hálózati eszközfajtán elérhetővé válik.

ÖSSZEGZÉS

Az intelligens hálózat a hagyományos biztonsági eszközök képességeinek megsokszorozása révén az egész szervezetre kiterjedő integrált és egységes biztonsági megoldást kínál. Egyedi eszközökkel ugyan elhárítható a támadások egy része, de a hálózat egészére kiterjedő rendszerintegráció sokkal hatékonyabb, átfogóbb és proaktív megközelítési módot kínál, amely azonnal alkalmazkodik az új támadásokhoz. Ez a dinamizmus kulcsfontosságú az adatok megfelelő szintű védelméhez és az üzletmenet folytonosságának biztosításához.

A Cisco rendszerszemléletű biztonsági megoldásainak hármas alapja: a készülékek beépített intelligens funkciói, az ezeket hasznosító automatikus szoftvereszközök és a szabály alapú felügyelet. Ezek együttműködése garantálja a maximális biztonságot, a rendszergazdának pedig csak a szabályok beállításával és a stratégiai szempontokkal kell törődnie. Ez az alaposan körülbástyázott informatikai környezet a megbízható felhasználók számára biztonságos kapcsolatot kínál, és ezzel elősegíti a hatékony együttműködést.

A Cisco intelligens hálózata és hálózatbiztonsági megoldásai együttesen alkotják az önmagát védő hálózat alapját. Ez nemcsak elősegíti a védelem automatizálását, de csökkenti a működési költségeket, és növeli a működés hatékonyságát.

A Cisco intelligens hálózati megoldásairól további tájékoztatást a **http://www.cisco.com/go/intelligentnetworking** webhelyen találhat.

Vállalati központ
Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Egyesült Államok
www.cisco.com
Tel.: +1 (408) 526-4000
+1 (800) 553-NETS (6387)
Fax: +1 (408) 526-4100

Európai központ
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
Hollandia
www-europe.cisco.com
Tel.: +(31) 020-357-1000
Fax: +(31) 020-357-1100

Amerikai központ
Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Egyesült Államok
www.cisco.com
Tel.: +1 (408) 526-7660
Fax: +1 (408) 527-0883

Ázsiai és csendes-óceáni központ
Cisco Systems Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel.: +(65) 631-777-77
Fax: +(65) 631-777-99

A Cisco Systems cégnek több mint 200 irodája működik az alábbi országokban és térségekben. Ezek címei, telefonszámai és faxszámai megtalálhatók a **Cisco.com webhelyen a www.cisco.com/go/offices címen.**

Argentína • Ausztrália • Ausztria • Belgium • Brazília • Bulgária • Chile • Costa Rica • Ciprus • Cseh Köztársaság • Dánia • Dél-Afrika Dubai, Egyesült Arab Emirátusok • Egyesült Államok • Egyesült Királyság • Finnország • Franciaország • Fülöp-szigetek • Görögország • Hollandia • Hongkong Horvátország • India • Indonézia • Írország • Izrael • Japán • Kanada • Kína • Kolumbia • Korea • Lengyelország • Luxemburg • Magyarország • Malajzia Mexikó • Németország • Norvégia • Olaszország • Oroszország • Peru • Portugália • Puerto Rico • Románia • Skócia • Spanyolország • Svájc Svédország • Szaúd-Arábia • Szingapúr • Szlovákia • Szlovénia • Tajvan • Thaiföld • Törökország • Új-Zéland • Ukrajna • Venezuela • Vietnam • Zimbabwe