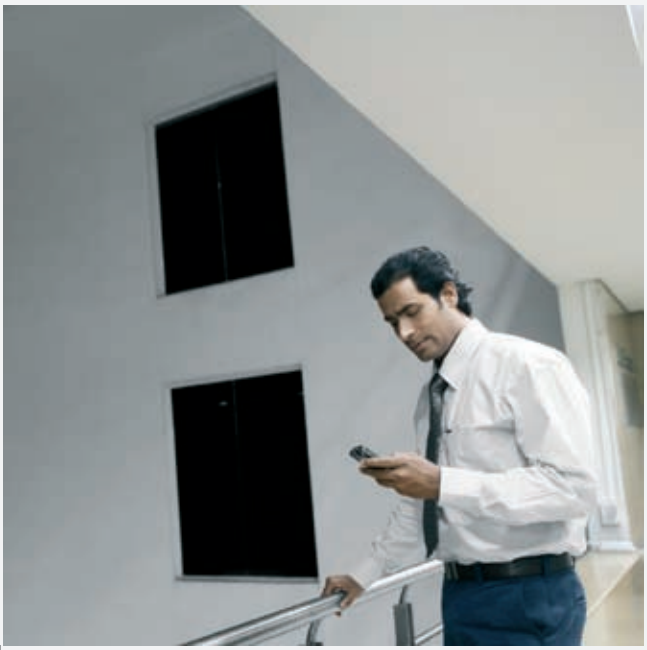
Integrált biztonság

a fenyegetések felszámolására

CISCO™

CISCO™

Fenyegetéskezelő és –elhárító megoldások



A Cisco Threat Control, vagyis fenyegetéskezelő megoldás teljes körű védelmet nyújt hálózatának a nagyobb rálátásnak, az egyszerűsített házirend alapú felügyeletnek és a proaktív rendszervédelemnek köszönhetően.

A Cisco Self-Defending Network, vagyis Cisco Önvédő hálózat részét képező megoldás a hálózatot, a szervereket, a végpontokat és az információt egyaránt védi. Szabályozza a hálózati hozzáférést, elkülöníti a fertőzött rendszereket, megelőzi a behatolásokat és védi az üzletkritikus értékeket. Már azelőtt szembeszáll az olyan kártékony forgalmakkal, mint a férgek, vírusok és malware, mielőtt azok kárt okozhatnának vállalkozásának, és teszi mindezt központosított házirenddel, konfigurálhatósággal és a biztonsági események kezelésével.

Miért van szükség fenyegetéskezelésre és –elhárításra?

A hálózattal szembeni biztonsági fenyegetések akár jelentősen visszavethetik a működési hatékonyságot, tönkretehetik az üzletmenetet és az üzleti műveleteket, és információvesztéssel járhatnak – amelyek viszont pénzügyi veszteséget és az előírásoknak való megfelelőség elmulasztását okozhatják. A hackerek folyamatosan új módszereket fejlesztenek ki, hogy saját pénzügyi érdekeik miatt információhoz férjenek hozzá, és ezeket a módszereket minden eddiginél nehezebb észrevenni. A vállalkozásoknak átfogó megoldásra van szükségük, amely rugalmasan kezelhető és bevethető az ezen fenyegetések elleni proaktív védelemben.

Milyen problémákat kell megoldani?

A vállalkozások biztonsági problémák ezreivel szembesülnek, például a következőkkel:

- Az alkalmazottak és az informatikai rendszerek hatékonyságának megőrzése vírusok és férgek kitörésekor
- Bizalmas információk védelme
- A cég és a márka hírnevének védelme
- Kommunikációs leállások és azok hatására a napi üzletmenetre
- E-üzleti alkalmazások folytonossága

Fenyegetéskezelő és –elhárító megoldás

A Cisco Threat Control and Containment, azaz Fenyegetéskezelő és –elhárító megoldás átfogó megközelítést kínál ügyfeleinknek a fenyegetések kezelésére és elhárítására, vállalatmérettől függetlenül páratlan védelmet nyújtva az internet-alapú és célzott támadásokkal, illetve behatolásokkal szemben.

Teljes körű rálátás és védelem: átfogó és proaktív hálózati megközelítés

- A teljes infrastruktúrára érvényes, a fenyegetésekkel szembeni intelligens védelem költséghatékony módon kiterjed minden rendszerre és eszközre
- A többtényezős fenyegetésazonosítás a házirend megszegését, a sebezhetőségek kiaknázását és a rendellenes viselkedést is kiszűri

Egyszerűsített szabályozás: a házirendek és azok kezelésének racionalizálása a teljes hálózaton

- Szabványosított házirend-kezelés a többféle hálózati elem között
- Teljes infrastruktúrára érvényes megvalósítás minden rendszerre és eszközre

Üzletmenet-folytonosság: a vállalkozás műveleteinek biztosítása

- Páratlan együttműködés és összhang a rendszerek, végpontok és a kezelés között
- Adaptív válaszadás lehetősége a valósidejű fenyegetésekre
- A Cisco Önvédő hálózat stratégia központi eleme

A Fenyegetéskezelő és –elhárító megoldás központi elemei

- **Cisco ASA 5500 sorozatú adaptív biztonsági berendezések**

  Moduláris platform, amely a biztonsági és VPN-szolgáltatások következő generációját kínálja a kis irodáktól a nagy vállalatokig mindenféle szervezet számára.
  http://www.cisco.com/go/asa

- **Cisco ASA 5500 Anti-X Edition**

  Az átjáró szinten veszi fel a harcot az olyan fenyegetések ellen, mint a spyware, a spam, a vírusok és az internetes tartalmakhoz kapcsolódó egyéb fenyegetések.
  http://www.cisco.com/go/asa

- **Cisco Security MARS**

  A nyers hálózati és biztonsági adatokat eseményekké alakítja és osztályozza, továbbá végrehajtható megelőző feladatokat fogalmaz meg.
  http://www.cisco.com/go/mars

- **Cisco Behatolásmegelőző (IPS) megoldások**

  Átjáró szinten nyújt védelmet a szervereknek, az alkalmazásoknak és más kritikus eszközöknek a hálózatok és alkalmazások elleni támadásoktól és férgektől, az adatközpontokban és a teljes LAN-hálózatban.
  http://www.cisco.com/go/ips

- **Cisco Security Agent**

  Célzott támadásoktól, spyware-től, root kitektől és nulladik napi támadásoktól védi a szervereket és asztali gépeket.
  http://www.cisco.com/go/csa

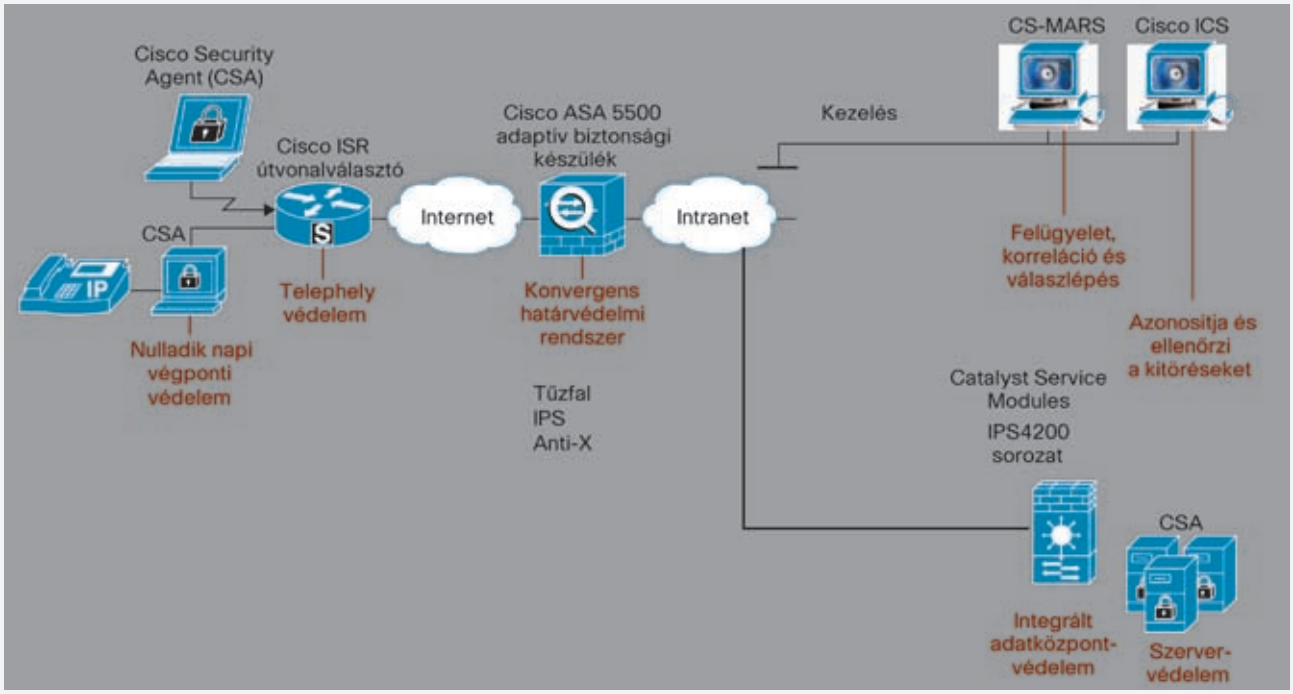
- **Cisco Hálózati hozzáférés-szabályozás (NAC)**

  A felhasználót és a rendszerkörnyezetet ellenőrizve meggátolja a hálózat és az infrastruktúra megfertőzését.
  http://www.cisco.com/go/nac

A Cisco Security Center webes portál egyedülálló, integrált információforrás a friss biztonsági eseményekről, amely arra vonatkozóan is segítséget nyújt, hogyan lehet a Cisco termékeket és szolgáltatásokat az új fenyegetések mérséklésére használni.
http://tools.cisco.com/security/center/home.x

CISCO™

Dolgozzon ki átfogó és felügyelhető fenyegetéskezelő stratégiát



Életciklus alapú biztonsági szolgáltatások a Fenyegetéskezelő és –elhárító megoldásokhoz

- A Cisco Security Center portál egyedülálló, integrált információforrás a friss biztonsági eseményekről, amely arra vonatkozóan is segítséget nyújt, hogyan lehet a Cisco termékeket és szolgáltatásokat az új fenyegetések enyhítésére használni.
- A Cisco IPS Signature Subscription szolgáltatás előfizetői hozzáférést kapnak a Cisco Security IntelliShield Alert Manager adatbázishoz, amely nem csupán teljes körű hírforrás az IPS eseményekről, hanem az IPS támadásmintákat az IntelliShield riasztásokkal összefüggésbe hozva a potenciális támadások gyors orvoslására is képes.
- A Cisco IPS, a Cisco Security MARS, a Cisco NAC és a Cisco Security Agent alkalmazási tanácsadási szolgáltatásokkal egyszerűbbé válik az új megoldások használata, mivel a Cisco szakértők bevált biztonsági tervezési elvekkel és hálózatintegrációs szakértelmükkel segítik a folyamatot.
- A Cisco IPS Remote Update and Tuning Service az IPS eszközök mindennapi működtetését egyszerűsíti azáltal, hogy a signature frissítések megjelenésekor alkalmazza és finomhangolja azokat.

Hogyan fogjon hozzá?

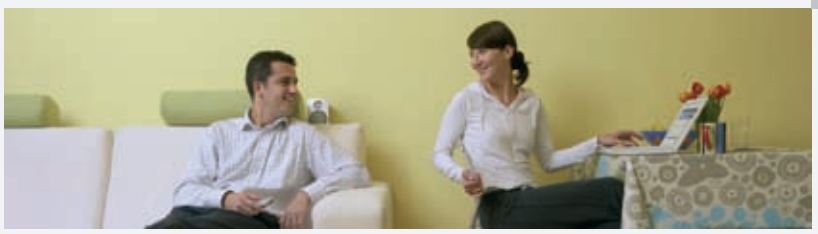
Egy teljes körű, proaktív biztonsági stratégia kialakítása állandóan változásban levő folyamat, amelynek fontos kezdőlépése a kritikus pontok azonosítása. Ha szeretné részletesen megtudni, hogyan építse ki biztonsági megoldását, olvassa el a Cisco Fenyegetéskezelés és –elhárítás című fehér könyvét (amit **Cisco értékesítés menedzser**étől szerezhet be).

Miért a Ciscót válassza?

A Cisco világszinten vezető szerepet játszik a hálózatbiztonsági megoldások területén. A Cisco kínálja a legátfogóbb megoldást az informatikai infrastruktúrát érő fenyegetések elleni védekezésre. A Cisco integrált, együttműködő és alkalmazkodó biztonsági megoldása teljes körűen kezeli mindazokat a fenyegetéseket, amelyekkel napjainkban a szervezetek kénytelenek szembenézni, ezzel biztosítva az informatikai rendszerek és az alkalmazottak hatékonyságát, illetve legfontosabb információs értékeik védelmét. Akár internetes fenyegetésekről, akár célzott támadásokról és behatolásokról van szó, a Cisco megoldások olyan eszközöket kínálnak az IT és biztonsági szakembereknek, amelyekre az információs biztonsági fenyegetések ellen egyre összetettebbé váló küzdelem idején a szervezeteik védelme érdekében szükségük van.

Ismerje meg, hogyan védik a Cisco integrált biztonsági megoldásai a teljes szervezetét az egyre fejlődő fenyegetések ellen!

Ismerje meg, hogyan védenek a Cisco Fenyegetéskezelő megoldások a fenyegetések következő generációval szemben.
Látogasson el a http://www.cisco.com/offer/syg/security oldalra, tudjon meg többet a Cisco Fenyegetéskezelő megoldásokról, és megkapja ingyenes üzleti kockázati értékelésünket.



A biztonsági fenyegetések a hálózat bármely pontján megjelenhetnek.

Pontosan ezért lényeges, hogy biztonsági megoldásai mindenhol védelmet nyújtsanak. A válasz: a Cisco Önvédő hálózat. Az egymástól függetlenül működő és csak az infrastruktúra egy-egy részét védő termékekkel ellentétben a Cisco megoldásai garantálják, hogy az infrastruktúra minden egyes apró eleme védelmi pontként szolgáljon. A rendszerszintű megközelítés kevesebb alkotóelemből álló szabványosított platformot használ – egyedülálló felügyeletet biztosítva ezzel a következő generációs fenyegetések, illetve azok visszaszorítása felett. Valamint lehetővé teszi az Ön számára, hogy figyelmét a valóban fontos üzleti kérdésekre fordítsa.

Ha az idő pénz, a leállással töltött idő még inkább az

Egy teljesen integrált biztonsági rendszer fenntartásának költsége elenyésző ahhoz képest, amennyibe egy ilyen rendszer hiánya kerül. A Cisco proaktív biztonsági megközelítésének köszönhetően kevesebb leállással működtetheti vállalkozását, megőrizheti ügyfelei elégedettségét, és mindenek felett biztosíthatja hálózata sértetlenségét és biztonságát. És ha mégis probléma jelentkezne, a Cisco a nap 24 órájában kínál támogatási szolgáltatásokat.

Vállalkozása úton van. Mi abban segítünk, hogy célba érjen

Egy vállalkozás jövőjének megtervezéséhez komoly gondolkodásra van szükség. Vagy egy útmutatóra. A Cisco Smart Business útmutató pontosan azokat a biztonsági megoldásokat kínálja, amelyekre ma van szüksége a holnap kihívásainak kezeléséhez. Ráadásul a Cisco díjnyertes partnerhálózatával olyan minősített partnerek, rendszerintegrátorok és szolgáltatók segítségéhez fér hozzá, amivel beazonosíthatja és alkalmazhatja a legújabb technológiájú megoldásokat.

Különleges ajánlat: Használja ki a kedvező árú, csomagban kínált Cisco Fenyegetéskezelő és –elhárító megoldások előnyeit. A részletekért lépjen kapcsolatban Cisco értékesítési menedzserével vagy helyi partnerével.

Cisco Systems Magyarország Kft.
1123 Budapest, Csörsz u. 45.
Telefon: (1) 225 4600
Fax: (1) 225 4611
www.cisco.hu