Novell Security Manager – Védelem egy egész hadsereg erejével

A Novell Security Manager egy kényelmesen felügyelhető, integrált csomag a vállalatok és intézmények biztonságos működésének megteremtéséhez.

© Kiskapu Kft. Minden jog fenntartva

Informatikai rendszerünk stabil működésének elengedhetetlen feltétele a biztonság megteremtése. A külső fenyegetésekkel szembeni védelem megvalósításához azonban sokféle biztonsági eszközre és alkalmazásra van szükség egy vállalatnál: tűzfalra, virtuális magánhálózatra, behatolásvédelemre, vírus- és spamszűrésre, valamint ***URL***-szűrésre. Mindezen védelmi módszerek különféle gyártóktól való beszerzése és telepítése költségigényes, és a rendszer felügyeletét is jelentősen megnehezíti. A ***Novell Security Manager*** mindezeket egyben, egy kényelmesen felügyelhető, integrált csomagban kínálja.

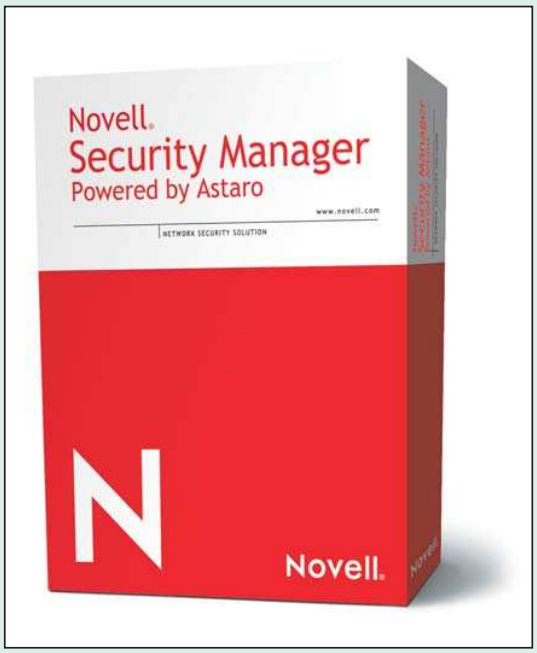
A ***Novell*** a ***Linux*** és a személyazonosság alapú biztonság területén piacvezető technológiáját és az ***Astaro*** hálózati biztonsági szoftverek és berendezések terén szerzett tapasztalatát ötvözve fejlesztette ki a ***Novell Security Manager*** legújabb verzióját. A ***Linux*** alapokra épülő biztonsági megoldás kihasználja a nyílt forráskódú közösség együttműködésének eredményeit; egyetlen kereskedelmi szoftver sem kínálja ugyanezeket a funkciókat.

A ***Novell Security Manager*** nagy teljesítménye miatt hatékony védelmet nyújt az első vonalban felmerülő biztonsági fenyegetésekkel szemben, de használható egy meglévő tűzfal mögötti kiegészítő szintként is.

Áttekintés

A folyamatos, zökkenőmentes kommunikáció az ügyfelek, az üzleti partnerek és az alkalmazottak között létfontosságú egy vállalat működéséhez. Az internetet használó szervezetek fokozottan ki vannak téve a különféle rosszindulatú támadásoknak: vírusok, férgek, alkalmazások kihasználása, ***szolgáltatásmegtagadási támadások (denial-of-service; DoS)***, spam, információlopás és még sorolhatnánk.

Az egyre több irányból fenyegető veszélyek ellen többféle védekezési módszert is kell használni – a rendelkezésre álló költségkereten belül. A ***Novell Security Manager*** minden más megoldásnál alacsonyabb költségszinten képes mindezt megvalósítani. Mivel ***Linuxra*** épül, nem csak költséghatékonysága, de páratlan biztonsága miatt is népszerű.



Könnyen telepíthető és felügyelhető, méretezhető és mégis biztonságos. Használatával a cég teljes kimenő és bejövő kommunikációs forgalma gyorsan, teljesen és hatékonyan biztosítható.

A Novell teljes hálózati biztonsági megoldása összesen hat határbiztonsági alkalmazást és integrált felügyeleti platformot biztosít. A ***SUSE LINUX*** alapú alkalmazás átfogó biztonsági infrastruktúrája a betörők, vírusok, férgek, levélszemét és betörések jelentette biztonsági fenyegetések ellen is védelmezi a vállalatokat.

Tűzfal

A ***Novell Security Manager*** tűzfala az összes hálózatról érkező kommunikációs csomag fejlécét átvizsgálja, és a kommunikációs folyamatok megsértésének felderítése végett nyomon követi az eseményeket.

Blokkolja a kommunikációs forgalmat, ha az nem felel meg a portokra, protokollokra, valamint a várt forrásokra és célhelyekre beállított szabályoknak (állapotfigyelő csomagvizsgálat és alkalmazásszintű szűrés). Képes megvédeni a forgalmat a vezeték nélküli eszközöktől is.

A számos hálózati kapcsolat felügyeletének egyszerűsítésére és a teljesítmény növelésére az ***Astaro*** biztonsági proxykat alkalmazza a legfontosabb protokollokhoz (például a ***HTTP***, ***DNS***, ***SOCKS***, ***POP3***, ***Ident*** és ***SMTP*** esetében). A fontos tűzfalfunkciók közé tartozik még a hálózati címfordítás,

a maszkolás, valamint a szolgáltatmegtagadási támadásokkal szembeni védelem.

Virtuális magánhálózat

A távoli felhasználók számára, akik az internetet használják kommunikációra, a *Novell Security Managerben* található ***virtuális magánhálózat (VPN)*** rendkívüli mértékben képes csökkenteni a kommunikációs költségeket azzal, hogy megszünteti a drága bérelt vonalak szükségességét. Mivel a *VPN*-átjáró rendkívül rugalmas – sokféle architektúrát támogat –, *VPN* kapcsolat teremthető a távoli irodákkal, az otthoni munkahelyekkel és egyéb nyilvános helyekkel (például szállodák konferenciatermeivel). A legfejlettebb titkosítási algoritmusok és a hitelesítési módszerek, valamint a *VPN*-kliensek széles köre áll rendelkezésre.
A *Novell Security Manager* saját tanúsítványhatósággal rendelkezik a digitális aláírások egyszerű és biztonságos kezelésére, és teljes mértékben támogatja a nyilvános kulcsú titkosítás használatát.

Védelem a behatolásokkal szemben

A *Novell Security Manager* behatolásvédelmi összetevője egy több mint 2000 mintát és szabályt tartalmazó adatbázis alapján (amelynek karbantartását a vezető nyílt forráskódú ***Intrusion Detection Snort***™ behatolásvédelmi projekt végzi) felderíti és blokkolja az alkalmazás- és protokollspecifikus támadásokat. Beállítható, hogy gyanús tevékenység észlelése esetén e-mailben értesítse a rendszergazdát, vagy azonnal blokkolja a gyanús forgalmat a tűzfalon keresztül. Ennek felügyeletét az egyedi szabályok vagy a teljes kategóriák szintjén is végezheti. A szabályokat a *Novell Up2Date* szolgáltatás folyamatosan frissíti; ezekhez új szabályok adhatóak, vagy a meglévők testre szabhatóak. Leállítható, vagy korlátozható a legújabb kommunikációs formákkal kapcsolatos tevékenység: például az azonnali üzenetküldés, a csevegés vagy az ***egyenrangú (peer-to-peer) hálózatok***. Ez kritikus fontosságú kiegészítője lehet a biztonságnak, különösen, mivel egyelőre kevés védekezési mód létezik az ilyen típusú visszaélésekkel szemben.

Vírusvédelem

A *Novell Security Manager* szűrő keretrendszere átvizsgálja az e-mail üzeneteket, fájlokat és a webes forgalmat a vírusok, férgek, trójai programok és egyéb rosszindulatú szoftverek után kutatva. A *Novell Security Manager* kétféle típusú vírusvédelmet kínál: a hagyományos e-mailekhez és fájlokhoz, valamint a webböngészőben letöltött e-mailekhez és fájlokhoz is.
A *Novell Security Manager* sokféle vírusellenőrző módszert használ annak érdekében, hogy a lehető legtöbb vírust megfogja: elemzi az e-maileket és a csatolmányokat az ismert, vírusokhoz társítható kódok megkeresésére, heurisztikus módszerekkel keres az ismert vírusmintázatokhoz hasonló kódokat és ezeket hagyja végrehajtódni egy védett környezetben, ahol a problémák a megfertőződés veszélye nélkül felismerhetők.
A gyanús kódokat összeveti a *Kaspersky Lab* adatbázisával, amely a világ egyik legnagyobb, 100 ezer vírusjellemzőt tartalmazó listája. Az átjáróban történő vírusellenőrzés lehetővé teszi az új vírusokra való gyors reagálást, mielőtt azok elérnék a belső rendszereket. Ez a szolgáltatás az asztali vírusellenőrzők kritikus fontosságú kiegészítője, mert azokat gyakran bonyolult a teljes szervezetben frissíteni. Megadható, hogy el kívánja-e dobni a gyanús leveleket és csatolmányokat, vagy visszautasítja azokat a küldőnek szóló üzenettel, illetve figyelmeztetéssel átengedi a felhasználó felé vagy karanténba zárja őket, hogy az adminisztrátor megvizsgálhassa azokat és megtehesse a szükséges intézkedéseket.

Spam elleni védekezés

A *Novell Security Manager* számos spamfelismerő módszert használ a kéretlen levelek azonosítására és blokkolására. Ellenőrzi a levelek forrását az ismert spamküldők listájával összehasonlítva, saját fekete- és fehérlistákat hoz létre, szabályokat és mintázatokat használ a levelek szövegének elemzésére és hozzájuk rendel egy „spam pontszámot". A kívánt küszöbérték beállításával a gyanús levelek eldobhatók, visszautasíthatók egy küldőnek szóló üzenettel, figyelmeztetéssel átengedhetők a felhasználó felé, illetve karanténba zárhatók, ahol a rendszergazda megvizsgálhatja őket és megteheti a megfelelő intézkedéseket. Ez a rugalmasság lehetővé teszi a finom egyensúly megteremtését a spamszűrés és jó levelek véletlen blokkolásának elkerülése között. A *Novell Security Manager* jelentést készít a spamüzenetek számáról és méretéről, így felismerhetőkké válnak a mintázatok és a trendek is.

Barangolásvédelem (URL-szűrés)

Az internet rendkívül fontos eszköz a cégek számára, de ha a munkatársak túl sok időt töltenek a weben barangolva, a termelékenység csökkenhet, illetve ha nem helyénvaló vagy jogvédett anyagokat töltenek le, akkor jogi problémák is felvetődhetnek. A barangolásvédelem lehetővé teszi a webes tevékenységek védelmét a webhasználati irányelvek kidolgozásával.
A *Novell Security Manager* segítségével a cég vezetése 58 különféle kategória használatával határozhatja meg a webhasználati irányelveket, ilyenek például a szex, a szerencsejátékok, a törvénytelen tevékenységek, illetve az amúgy törvényes, de a munkához nem szükséges tevékenységek mint például a vásárlás, az árverések látogatása, a szórakozás vagy a munkakeresés. Az üzemeltetést végző osztály egyszerűen mérheti a webes tevékenységeket és jelentéseket készíthet ezekről a problémák azonosítására és a prioritások megadására, vagy blokkolhatja bizonyos ***URL*** kategóriák elérését, így azok hozzáférhetetlenek lesznek a felhasználók számára.
A *Novell Security Manager* egy (a *Cobiontól* származó) 20 millió kategorizált webcímet tartalmazó adatbázist használ, ami jelenleg a kereskedelmi forgalomban kapható legnagyobb lista. Ez a lista természetesen további saját fekete- és fehérlistákkal bővíthető. A felhasználók különféle csoportjai számára pedig külön fekete- és fehérlisták is létrehozhatók. ■

© Kiskapu Kft. Minden jog fenntartva