

Novell Security Manager

www.novell.hu

TERMÉKISMERTETŐ

2005.05.27

Novell®

Tartalomjegyzék

Novell Security Manager	2
Áttekintés.....	2
Tűzfal.....	2
Virtuális magánhálózat.....	3
Védelem a behatolásokkal szemben.....	3
Vírusvédelem.....	3
Spam elleni védekezés.....	4
Barangolásvédelem (URL-szűrés).....	4
Funkciók.....	4
Előnyök.....	4

Novell Security Manager

A külső fenyegetésekkel szembeni védelemhez sokféle biztonsági alkalmazásra van szükség egy vállalatnál: tűzfalra, virtuális magánhálózatra, behatolásvédelemre, vírus- és spamszűrésre, valamint URL-szűrésre. Mindezen védelmi módszerek együttes telepítése általában drága, nem is szólva a felügyelet bonyolultságáról. Az Astaro technológiára épülő Novell Security Manager mindezeket egyben, egy kényelmesen felügyelhető, integrált csomagban kínálja - és mivel Linux alapokra épül, kihasználja a nyílt forráskódú közösség együttműködésének eredményeit. Nincs olyan kereskedelmi szoftver, ami ugyanezt kínálja. A Novell Security Manager elég nagy teljesítményű ahhoz, hogy az első vonalban küzdjön a biztonsági fenyegetésekkel szemben, de használható egy meglévő tűzfal mögötti hatékony kiegészítő szintként is.

Védje vállalati rendszereit hatékonyan és kényelmesen! A hat Linuxra épülő fontos biztonsági alkalmazással és a kényelmesen használható felülettel a Novell Security Manager erős védelmet jelent sokféle szintű biztonsági fenyegetéssel szemben.

Áttekintés

A kommunikáció létfontosságú - biztosnak kell lennie abban, hogy megkapja a fontos üzeneteket az ügyfelektől, az üzleti partnerektől és az alkalmazottaktól. De amikor crackerekről, spamküldőkről vagy vírusírókról van szó, akkor az egy másik történet.

Mostanra gyakorlatilag minden, az internetet használó szervezet ki van téve a támadásoknak, mégpedig egyre többféleképpen: vírusok, férgek, alkalmazások kihasználása, szolgáltatás-elfojtásos (denial-of-service) támadások, spam, információlopás és megannyi más veszély leselkedik rájuk. Ha meg szeretné védeni magát ezektől az egyre több irányból fenyegető veszélyektől, többféle védekezési módot kell használnia - a költségvetésen belül maradva.

A Novell Security Manager ezt a fajta biztonságot kínálja. Hatféle fontos alkalmazást és egy integrált felügyeleti platformot tartalmazó teljes hálózati biztonsági megoldásként a kiforrott szolgáltatások széles választékát kínálja, de rendkívül könnyű telepíteni és felügyelni. A védekezési mód kiválasztása mindezek ellenére csak egy kis része az erőforrások védelmének. Ezután még biztosítani kell, hogy az informatikai munkatársak képesek legyenek az egyes termékek telepítésére, használatuk megtanulására, integrálására a meglévő rendszerbe, beállítására és felügyeletére, valamint folyamatos frissítésére.

A Novell Security Manager minden más megoldásnál alacsonyabb költségeket kínál, mivel a Linuxra épül, amely nem csak költségtakarékossága, de páratlan biztonsága miatt is népszerű. Élvezheti a nyílt forráskódú közösség együttműködésének előnyeit, amelyek méretezhetővé és elég biztonságossá teszik a Novell Security Managert ahhoz, hogy a legszigorúbb követelményeknek is megfeleljen. Mivel mind a hat (az alábbiakban részletezett) biztonsági alkalmazás teljesen integráltan működik a Novell Security Managerben, a cég teljes kimenő és bejövő kommunikációs forgalma gyorsan, teljesen és hatékonyan védve van.

Tűzfal

A Novell Security Manager tűzfala a piacon kapható termékek közül az egyik legkifinomultabb és leghatékonyabb. Az összes, a hálózatról érkező kommunikációs csomag fejlődésének vizsgálata mellett egy szekcióban nyomon követi az eseményeket a kommunikációs folyamatok megsértésének felderítésére. 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 biztosít 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 szolgáltatáselfojtásos támadásokkal szembeni védelem.

Virtuális magánhálózat

Ha vannak olyan távoli felhasználói, akik az internetet használják kommunikációra, a Novell Security Managerben található virtuális magánhálózat (VPN) rendkívül nagy 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 azokkal, akik hotelszobákból vagy más nyilvános helyekről jelentkeznek be.

Választhat a legfejlettebb titkosítási algoritmusok és a hitelesítési módszerek közül, valamint a VPN-kliensek széles köréből. A Novell Security Manager saját tanúsítványhatósággal rendelkezik a digitális aláírások használatának egyszerűsítésére a magas biztonsági fokozatú kommunikáció érdekében, valamint 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. A Novell Security Manager érzékeli a behatolást és védekezik is ellene, más szavakkal, ha gyanús tevékenységet észlel, vagy e-mailben értesíti a rendszergazdát vagy megmondja a tűzfalnak, hogy azonnal blokkolja a gyanús forgalmat. Ennek felügyeletét az egyedi szabályok vagy a teljes kategóriák szintjén is végezheti. A szabályokat a Novell Up2Date szolgáltatás folyamatosan frissíti; Ön új szabályokat adhat hozzá vagy testre szabhatja a meglévőket.

Leállíthatja vagy korlátozhatja az újabb kommunikációs médiákkal - például az azonnali üzenetküldéssel, a csevegéssel vagy a peer-to-peer hálózatokkal - kapcsolatos tevékenységeket. Ez kritikus fontosságú kiegészítője lehet a biztonságának, különösen, mivel egyelőre kevés védekezési mód létezik az ezekkel a technológiákkal összefüggő 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. Egyike annak a kevés megoldásnak, amely 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. Ellenőrzi a gyanús kódokat a Kaspersky Lab adatbázisában, amely a világ 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 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, visszautasítja azokat a küldőnek szóló üzenettel, 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 beállítása 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 is, így felismerhetővé válnak a mintázatok és a trendek is.

Barangolásvédelem (URL-szűrés)

Az Internet egy rendkívül fontos eszköz a mai cégek számára, de ha a munkatársak túl sok idő töltenek a weben barangolva, a termelékenység csökkenhet, illetve ha nem helyénvaló vagy jogvédett anyagokat töltenek le, törvényes felelősségi problémák is felvetődhetnek. A barangolásvédelem lehetővé teszi a webes tevékenységek védelmét a webhasználati irányelvek kidolgozására, majd az irányelveket sértő webhelyek meglátogatásának blokkolására. 58 különféle kategória használatával határozhatja meg a webhasználati irányelveket, például meztelenség, szerencsejátékok, bűnös tevékenységek, illetve törvényes, de nem helyénvaló dolgok, mint például vásárlás, árverések látogatása, szórakozás vagy munkakeresés. 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 webcíment tartalmazó adatbázist használ - ez a kereskedelmi forgalomban kapható legnagyobb lista. Ez saját fekete- és fehérlistákkal bővíthető. A felhasználók különféle csoportjai számára külön fekete- és fehérlisták is létrehozhatók.

Funkciók

A hat integrált peremhálózati biztonsági alkalmazás a következő szolgáltatásokat nyújtja:

- Mindenre kiterjedő biztonsági infrastruktúra, amely védelmet jelent a crackerekkel, vírusokkal, férgekkel, levélszeméttel, behatolásokkal és egy sor másfajta biztonsági fenyegetéssel szemben
- Linuxos alap, amely minden más platformon futó ajánlatnál nagyobb teljesítményt kínál
- URL-szűrés a helytelen weboldalak látogatásának felügyeletére
- Kényelmesen megtanulható és telepíthető szoftverek
- Kényelmesen megtanulható és telepíthető integrált alkalmazások
- Számos különféle VPN-architektúra támogatása az ágazati kirendeltségek, otthoni felhasználók és mások igényeihez illeszkedve (mindenféle típusú hálózatok és számítógépek összekapcsolása)
- Az Astaro díjnyertes technológiájára épülő szoftver, amely hatvan ország több mint 20 ezer hálózatát védi

Előnyök

Sok érv szól a Novell Security Manager mellett:

- Többféle fenyegetéssel szemben többféle védelmi módszert kínál egyetlen integrált alkalmazásban

- Felhasználja a nyílt forráskódú közösség együttműködését a megoldás nagy teljesítményének és biztonságosságának fenntartásában
- Csökkenti annak lehetőségét, hogy emberi mulasztásból sérülékennyé váljon a rendszer
- Gyorsan felel az újfajta fenyegetésekre azzal, hogy automatikusan, gyorsan és folyamatosan frissíti az összes biztonsági alkalmazást
- Napról napra fokozza az alkalmazottak teljesítményét a biztonsági infrastruktúra spamszűréssel és barangolásvédelemmel történő kiegészítésével
- Javítja az informatikai munkatársak eredményességét is a kényelmesen telepíthető, felügyelhető és frissíthető, teljes biztonsági infrastruktúra révén
- Mindenütt ugyanazokat a szoftvereket és felügyeleti eszközöket alkalmazza
- Használható a teljes vállalat elsődleges hálózati biztonsági infrastruktúrájaként, de a kirendeltségek vagy az egyes részlegek kényelmesen felügyelhető külön biztonsági szintjeként is

Csak a Novell Security Manager képes Linuxra építve hat különböző szinten védeni rendszerét a károsodásokkal és a rosszindulatú támadásokkal szemben, miközben egyszerű, egy felületről végezhető felügyeletet és kényelmes telepítést kínál.

