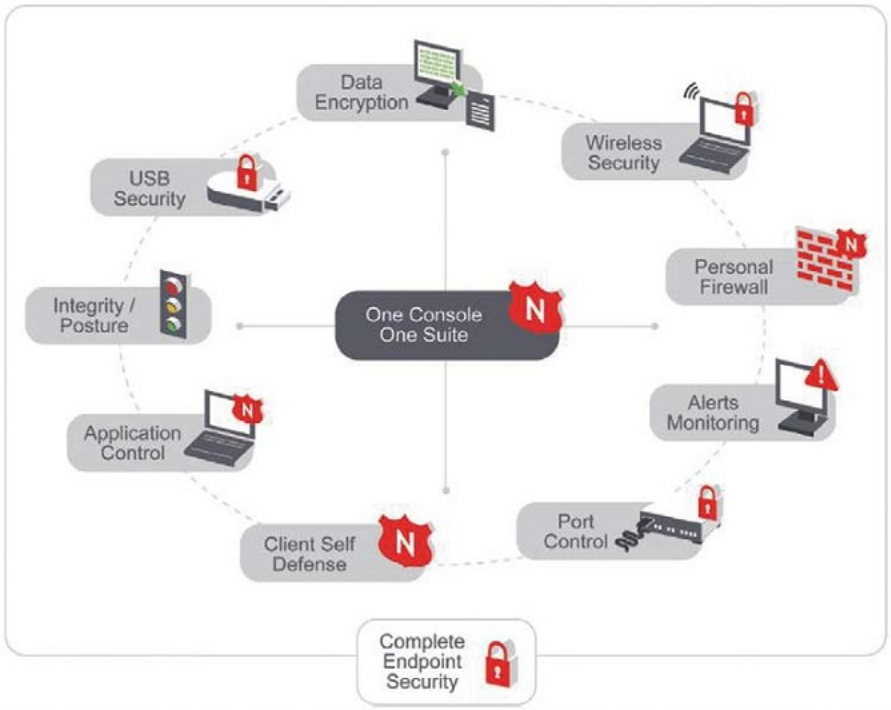
Termékismertető

Biztonsági megoldás hordozható és asztali munkaállomásokhoz



1. ábra: A központi irányítás megtartásával, a Novell ZENworks Endpoint Security Management biztonságossá teszi a hálózati végpontok használatát.

Novell megoldások

- Rendszerfelügyelet

Termékek

- ZENworks Endpoint Security Management

„A szállítók gyakran eltérő technológiák összességét használják a heterogén IT környezetek (beleértve a mobil és vezeték nélküli technológiákat is) végponti eszközeinek biztonságos használatát támogató megoldásaikban. A Novell ehelyett a piacra lépett egy egységes innovatív architektúrával, amely lehetővé teszi a hatékony és automatizált biztonsági eljárás kezelést az asztali és hordozható számítógépeken egyaránt."

Charles Kolody
IDC, kutatási igazgató

A végponti eszközök biztonságának megőrzése fontosabb annál, minthogy a végfelhasználókra lehetne bízni. Ennek ellenére, az IT infrastruktúra biztonsága sok esetben attól is függ hogy, az alkalmazottak hogyan állították be a számítógépükön a tűzfalat, lefuttatják-e a telepített vírusirtót, illetve hogyan használják az irodán kívül a VPN kapcsolatot. Ezekben az esetekben a végfelhasználók képzettsége és motiváltságuk hiánya nem nyújtja azt a biztos hátteret, ami a magas biztonsági szint megőrzéséhez kapcsolódó meglapozott döntésekhez szükséges lenne. Novell ZENworks Endpoint Security Management használatával a biztonság ellenőrzése a desktop eszközökre vonatkozóan a hozzáértő IT biztonsági szakemberek kezében összpontosul, ahova egyébként is ez való. Az alkalmazás kialakítása során lehetőség van az egyedi igényekből kiindulva csak bizonyos funkciók használatára, illetve arra is, hogy mint integrált megoldás nyújtson teljes védelmet az IT infrastruktúra végponti eszközeire vonatkozóan.

Beépített lokális tűzfal

A megoldás a világ leghatékonyabb tűzfalát kínálja a hacker, malware, protokoll és egyéb más támadásokkal szemben úgy, hogy használatával kapcsolatosan a végfelhasználóknak nem kell plusz ismeretet elsajátítania.

Vezeték nélküli eszközök hatékony biztonsági felügyelete

Megfelelő felhatalmazással rendelkező szakemberek számára lehetőség nyílik központilag meghatározni, hol, mikor és hogyan képesek a felhasználók kapcsolódni a számítógépük által azonosított vezeték nélküli belépési pontokon keresztül. Továbbá megszabható a szükséges titkosítási eljárás minimális szintje vagy akár teljesen letiltható a vezeték nélküli hálózatok használata. A végfelhasználóktól automatikusan kikényszeríthető a VPN használat az irodán kívüli helyszíneken is, mint pl. egy hotelszoba, kávézó, vagy hot spot.

Ponemon Egyetem 2006-os Cost of Data Breach tanulmánya alapján a vállalatok átlagosan 5 millió dollárt költenek az elveszett vagy ellopott adatokkal kapcsolatosan az eredeti állapot helyreállítására, átlagosan 182 dollárba kerül minden rendbe hozott felhasználói rekord. Az esetek 49%-ában az adatok elvesztése ellopott vagy elhagyott laptop-ok, desktopok, PDA-k vagy USB drive-ok miatt történik.

www.novell.hu

Portok felügyelete

ZENworks Endpoint Security Management beépített, a vezeték nélküli kapcsolatra vonatkozó funkciói biztosítják az összes olyan végponti kommunikációs csatorna (port és adapter) teljes felügyeletét, mint a:

- Hálózati adapter,
- Modem,
- Infravörös port,
- 1394 (Firewall),
- Soros és párhuzamos portok

Adatok titkosítása

A rendszerben lévő, központilag, rugalmasan kialakítható szabályrendszer képes biztosítani többek között a titkosítás kialakításának lehetőségét fájl típusra, a tárolás helyére, eszköz típusra vonatkozóan anélkül, hogy a felhasználónak szüksége lenne a saját biztonsági beállításainak kezelésére.

USB eszközök biztonságának felügyelete

Ha nincsenek megfelelően kezelve, az új generációs hordozható adatok tárolására alkalmas eszközök használata komoly gondot jelenthet a biztonság megőrzése és az előírások betartása szempontjából. A Novell megoldásának felhasználói beavatkozás nélkül automatikusan terjesztésre és betartatásra kerülő, USB eszközök felügyeletére vonatkozó funkciója lehetővé teszi a legmagasabb szintű, testre szabható, tárolóeszközökre vonatkozó biztonsági előírás betartását. A funkció használata biztosítja az ellenőrzést az összes olyan, úgynevezett optikai és hordozható tároló eszköz felett, mint például:

- CD, DVD,
- USB diszk,
- Flash memória,
- Pendrive
- Floppy, ZIP meghajtó,
- Zenei lejátszók, telefonok és más olyan eszközök, amelyek memóriával rendelkeznek.

Az engedélyezési eljárásokat úgy lehet kialakítani, hogy azokat rugalmasan, az igényeknek megfelelően, automatikus módszeren keresztül lehessen érvényre juttatni, a végrehajtás során pedig figyelembe lehet például venni a felhasználó tartózkodási helyét és az eszköz sorozatszámát is. Például, ha engedélyt adunk a hordozható eszközökre történő íráshoz, létre lehet hozni olyan automatikusan előálló figyelmeztetést, jelentést, amely rögzíti az összes eszközre kiírt fájlt.

Alkalmazások felügyelete

Abban az esetben, amikor – tudatosan vagy tudatlanul – nem engedélyezett alkalmazások futnak a szervezet számítógépein, szembe kell nézni a fertőzésekből származó kockázatokkal, illetve, az illegális szoftverhasználat veszélyeivel. A Novell Endpoint Security Management segítségével a szervezet IT infrastruktúráján futó alkalmazások teljes felügyeletét meg lehet megvalósítani a következő tulajdonságok kihasználásával:

- Alkalmazások feketelistája,
- Alkalmazás felügyelet helyszín szerint,
- Vírusirtók/spyware programok sértetlensége,
- VPN-re vonatkozó szabályok hatályba léptetése,
- Haladó script készítése.

Figyelmeztetések, riasztások

A funkció lehetővé teszi, hogy a biztonsági előírások megsértésével kapcsolatos bármilyen kísérlet jelentésre kerüljön ahhoz, hogy azonnal kezelni lehessen az ezzel kapcsolatban felmerülő kockázatokat.

Keresse meg helyi megoldásszállítóját, vagy vegye fel a kapcsolatot a Novell magyarországi képviseleti irodájával az alábbi elérhetőségek valamelyikén:

MOM Park, SAS torony
1124 Budapest, Csörsz u. 45.
Tel: +36 (1) 489-4600
Fax: +36 (1) 489-4601
info@novell.hu
www.novell.hu

NetIQ | Novell | SUSE

Novell®