

## Termékismertető

# Novell Sentinel

A Sentinel terméket a Novell a biztonsági előírások és a megfelelési szabályok betartásának hatékony követésére és ellenőrzésére fejlesztette ki. A kézzel végzett megfigyelés és kockázatelemzés már kis számú megfigyelt eszköz esetén is óriási teher, a Sentinel automatizálási képességeinek segítségével azonban akár több ezer szerver, hálózati eszköz, vagy szoftvertermék is hatékonyan megfigyelhető. A megfelelési követelmények többé nem szabhatnak határt cége növekedésének és nem vágnak részt a költségvetésén sem.

### A Novell Sentinel az informatikai rendszerek őrangyala

Egy cég informatikai infrastruktúráját alkotó szerverek, adatbázisok, tűzfalak, switchek, betörésvédelmi, vírusirtó, és más szoftverrendszerek nap mint nap rengeteg eseményt, értesítést, naplófájlt generálnak. Ezek rengeteg információt tartalmaznak, de ez részletes kiértékelés nélkül mit sem ér. Napjainkban a növekvő IT biztonsági fenyegetés hatására egyre bonyolultabb és egyre szigorúbb szabályozások és megfelelési elvárások lépnek életbe, miközben az online ügyfelek száma és ezzel párhuzamosan a cégen belüli IT környezet mérete és bonyolultsága is dinamikusan növekszik. Hamar elérkezhet az a kritikus pont, ahol már a kézi naplóelemzést képtelenség megfelelő idő alatt, az elvárt minőségben, és kigazdálkodható költséggel elvégezni. A Novell ezért kifejlesztett egy megoldást, mellyel ez a bonyolult és időigényes feladat automatizálható.

### A kézi feldolgozás egyszerűen nem kielégítő megoldás a biztonsághoz

A naplófájlok kéző összegyűjtése és elemzése, az események összevetése a megfelelési szabályokkal rendkívül munka- és időigényes folyamat. Miközben ez a munka zajlik, az események előrehaladnak, ily módon újabb, időbeni biztonsági lyuk keletkezik.

A Novell Sentinel biztonsági információ és esemény kezelő (SIEM) rendszer a piacon egyedülálló teljesítménnyel és skálázhatósággal bír. Képes a legnagyobb, legbonyolultabb IT környezetek valós idejű megfigyelésére, lehetővé teszi a biztonsági események és megfelelési kihágások gyors és hatékony kezelését. Automatikusan felismeri a szabályok megszegését és azonnal megteszi a szükséges válaszlépéseket, eközben pedig mérhetővé és bizonyíthatóvá teszi az előírásoknak való megfelelés paramétereit.

A Sentinel másodpercenkénti több ezer esemény adatainak valós idejű begyűjtését, korrelálását, megfigyelését, és megjelenítését végzi el az alábbi modulok segítségével:

- Sentinel Control Center
- Sentinel Reports
- Sentinel Collector Manager
- Sentinel Advisor (opcionális)
- Mainframe Collector (opcionális)
- PCI Solution Pack (opcionális)
- Identity Tracking Solution Pack (opcionális)

A Sentinel Control Center egy központi, integrált, grafikus kezelőfelület, mely lehetővé teszi a valós idejű megfigyelést, korrelációt, és riportkészítést.

### ■ Megoldás

■ Személyazonosság-kezelés és biztonság

■ Biztonsági események kezelése (SIEM – Security Information and Event Management)

### ■ Termékek

■ Sentinel

■ Sentinel RD

### Fontosabb képességek:

- folyamatos, 24 órás megfigyelés
- naplófájlok és események automatikus összegyűjtése, normalizálása, korrelálása
- rendellenességek, trendek, behatolási kísérletek automatikus felismerése
- azonnali automatikus válaszlépések az incidensekre a gyors elhárítás érdekében
- integráció a személyazonosság-kezelő megoldásokkal, az események felhasználókhöz rendelése
- grafikus kezelőfelület, az események grafikonok segítségével történő áttekintése
- valós idejű riportkészítés az előírásoknak való megfelelés dokumentált bizonyításához
- beépített hibajegykezelés, illetve együttműködés külső rendszerekkel

### Fontosabb előnyök:

- robusztus, jól skálázható SIEM megoldás vállalati vagy kormányzati felhasználók számára
- a ma piacon lévő legerősebb monitorozó rendszer a PCI-DSS szabványoknak történő megfeleléshez
- kiválóan illeszkedik a Novell piacvezető személyazonosság-kezelési és hozzáférés-kezelési megoldásaihoz



**"A Novell Sentinel minden szükséges eszközt a rendelkezésünkre bocsájt ahhoz, hogy felismerjük az anomáliákat, észrevegyük a betörési kísérleteket, és teljesítsük a PCI-DSS által előírt naplómegfigyelési és auditálási követelményeket."**

*Oliver Eckel, Vállalati Biztonsági Főnök, bwin International Ltd.*

[www.novell.hu](http://www.novell.hu)

### **Ha az aktív megfigyelés hasznos, az aktív riportkészítés felbecsülhetetlen**

A Sentinel Reports a Sentinel kulcsfontosságú összetevője. Riportjai segítségével könnyedén bizonyítható, hogy a cég folyamatosan megfigyeli a felhasználók tevékenységét a kritikus, SOX, HIPAA, FISMA, PCI, és más előírások által érintett rendszereken. A biztonsági és megfelelőségi incidensek felismerésre, követésre, és megoldásra kerülnek, és a riportok remek áttekintést nyújtanak a cégvezetés, valamint a külső és belső auditorok számára a felhasználók tevékenységéről. Olyan trendekre és rendellenességekre derülhet fény, amelyek kézi feldolgozás mellett rejtve maradnának. A riportkészítő alkalmazás képes testre szabott, cégspecifikus riportok készítésére, és nagy erőssége, hogy a létrehozott riportok a legkülönbözőbb formátumokban publikálhatók, beleértve a Crystal Reports-t, vagy akár belső vállalati portálon történő automatikus, előre időzített közzétételt is.

### **Sokszor nagy mennyiségű adat áll rendelkezésre, de kiértékelés és megértés nélkül ez hasznavehetetlen**

A Sentinel segít értelmezni a cége informatikai infrastruktúrája által termelt hatalmas mennyiségű adatot. Rendkívül kifinomult elemzési technológiájával gyorsan felismerhetővé teszi az új trendeket, támadásokat, és szabályszerűségeket. A címtár-integráció révén egyszerű IP címek helyett a felhasználói személyazonosságokhoz köthetők a különböző események. A Sentinel Active Views valós időben frissülő, testreszabható grafikonokkal és ábrákkal remek áttekintést nyújt, de szükség esetén lehetőség van akár több órára visszamenőleg leásni a részletes információkba, mely egy valóságos bűnügyi nyomrögzítő készlettel ér fel.

### **Nem csak jelent, érvényt is szerez**

A Sentinel képes automatikusan, valós időben válaszlépéseket tenni a bekövetkező eseményekre. Az iTRAC Workflow automatizálja az eseményazonosítási és eseménykezelési munkafolyamatokat, a szabályok érvényre juttatását, és lehetőséget biztosít a testreszabásra.

### **Naplózással kapcsolatos ipari szabvány hiányában rugalmas, adaptív technológia segíti az adatforrások egyesítését**

Az Event Source Management (ESM) keretrendszer adatgyűjtő ügynökprogramok (Collector) segítségével a különböző rendszerekről összegyűjti, szűri és átalakítja, egységesíti a napló- és eseményadatokat, majd rendelkezésre bocsájtja azokat későbbi kiértékelés, megjelenítés, és riportkészítés céljából. Lehetővé teszi, hogy vizuális formában kezelje és figyelje a Sentinel és az adatforrások közti kapcsolatokat. Képes felismerni a téves riasztási eseményeket, ennek köszönhetően a védekezési erőforrások a megfelelő helyen és időben összpontosíthatók. Az incidenskezelő modul kétirányú kommunikációt folytathat a legelterjedtebb hibajegykezelő rendszerekkel, így akár teljes, automatizált incidenskezelési eljárásrend alakítható ki. A Collector Manager nem csak kihelyezi, konfigurálja, és monitorozza a Collector-okat, hanem lehetővé teszi újak kifejlesztését, azaz bármilyen informatikai rendszer elem becsatornázását a Sentinel Control Center-be.

### **Változatok és rendszerkövetelmények**

#### **■ Sentinel 6.1**

Támogatott szerverplatform: SLES 10 (32/64 bit), RHEL 4 (64 bit), Solaris 10 (SPARC64), Windows 2003 (32 bit) és Windows 2008. Támogatott adatbázisok: Oracle 10g EE, MS-SQL Server 2005SP1 és 2008. Kezelőfelületi alkalmazások platformja: SLED 10 vagy Windows XP-Vista, kivéve a Collector Builder-t (csak Windows).

#### **■ Sentinel 6.1 RD**

A Sentinel Rapid Deployment változata, mely beépített adatbázist tartalmaz, így gyorsan üzembe helyezhető. Támogatott szerverplatform: SLES 10 SP2 (64 bit) ext3 fájlrendszerrel.

### **Hardverkövetelmények**

Terheléstől függően változó, de egy középkategóriás x86 szerverrel (2x Xeon QC E5310, 16GB RAM, 1TB RAID10 min. 4db 15k SAS HDD-ből, Gigabit Ethernet) akár 3000 EPS fölötti feldolgozási teljesítmény is elérhető.

Keresse meg a Novell helyi megoldásszállítóját, vagy hívja a Novell helyi képviselőjét az alábbi számon:

#### **Novell Kft.**

MOM Park, SAS torony  
1124 Budapest, Csörsz u. 45.

Tel: +36 (1) 489-4600

Fax: +36 (1) 489-4601

[iroda@novell.hu](mailto:iroda@novell.hu)

[www.novell.hu](http://www.novell.hu)