

RSA enVision SMB vállalatok részére

Logelemző megoldások közepes méretű vállalatoknak

Áttekintés

Az RSA enVision Mid market platform egy speciálisan az EMEA régióknak kifejlesztett logelemző, analízáló, tároló megoldás (SIEM). Immáron ezekben a vállalatokban is elérhető a teljeskörű logelemző, compliance, kockázatelemző, riasztó, auditáló funkcionális.

Előnyök

Közepes méretű vállalkozások ugyanazokkal a biztonsági problémákkal küzdenek, mint a nagyvállalatok, de sok esetben kevesebb munkatárs és pénz áll rendelkezésre. Meg kell felelni iparági vonatkozó előírásoknak, riportokat kell készíteni, automatikusan kell lépni bizonyos fenyegetettségek esetén. Ez sajnos sok-sok órát elvesz az IT szakemberek munkaidejéből.

Azonban az RSA enVision megoldás minden IP alapú eszközről képes a logokat egy központi helyre gyűjteni (bármilyen változtatás nélkül), ezen adatokat tárolja a saját adatbázisában, képes valós időben feldolgozni azokat, és automatikus riasztások rendelkeznek egyes eseményekhez.

Az adminisztrátorok egyetlen központi konzol segítségével képesek korellációs szabályokat, analíziseket is készíteni, hogy az átláthatatlan, nem strukturált logok helyett egy könnyen kereshető, automatikus válaszlépésekkel operáló megoldást használjanak.

Az alkalmazás három nagy előnye:

Compliance – Az alkalmazás mindenfajta eszközről képes logot gyűjteni, akár alkalmazás szinten is, többfajta forrásból, melyek lényegesen megkönnyítik az előírásoknak való megfelelést. Közel 1.000 beépített riportjával (melyek természetesen tovább bővíthetők) képes megfelelni a manapság használt összes elvárásnak. A logok ráadásul éveken keresztül eltárolhatók és pillanatok alatt visszakereshetők.

Biztonság és kockázatelemzés – A valós idejű riasztásokkal, válaszlépésekkel, analízáló képességével az enVision nagyban segíti az adminisztrátorok munkáját. A szűrések és szabályok segítségével csak a lényeges adatok elemzésével kell időt tölteni, a nem releváns adatok (eltárolás után) nem igényelnek további erőforrást.

Optimalizált IT – A strukturált adatok könnyebben elemezhetők, feldolgozhatók, ezekből könnyebb riportot készíteni. Az enVision képes a kiszolgálók, hálózati eszközök, tárolórendszerek, alkalmazások eseményeinek begyűjtésére, és az eszközök prioritizálására is. Elemző képességével előre jelezhetők bizonyos IT problémák (szabad tárolóhely hiánya, hardverhibák, redundáns eszközök konfigurációs problémái, stb.), ezáltal is segítve a döntéshozók tervezési munkáját.

Működése

Az RSA enVision Mid Market platform akár 40 eszközről képes egyidőben logokat gyűjteni – többek között Windows, Check Point, Cisco eszközökről – Agent telepítése nélkül. Biztosítja, hogy az események, folyamatosan, valós időben kerüljenek egy központi adatbázisba, hogy a további elemzéseknek alapjául szolgáljanak. Mindezen funkciók grafikus felületen, szerepkör alapú felhasználók számára akár évekre visszamenőleg nyújtja.

A web alapú és az Event Explorer technológia egy intelligens analízáló eszköz, mellyel az adatok könnyedén szűrhetők, kereshetők.

Az RSA enVision Mid Market eszközök hardver alapú, standalone megoldások, nincs szükség további eszközök, alkalmazások beszerzésére a funkcionalitás eléréshez.
Amennyiben szükséges az adatok azonban nem csak a belső HDD-ken, de külső tárolórendszereken is elhelyezhetők.

Elérhető verziók

Ezen termékek csak és kizárólag EMEA régióban (és azon belül is Kelet-Európában) érhetők el.

A kiszolgálók az alábbi paraméterekkel rendelhetők:

enVision Mid Market ES Series	ES-160-PROMO	ES-260-PROMO
Megjegyzés	Standalone SIEM appliance	Standalone SIEM appliance
Maximum Events PS	100	200
Maximum eszközsám	20	40
Konkurens RSA enVision felhasználók	4	5
Konkurens Event Explorer felhasználók	5	
Alkalmazás	RSA enVision platform, featuring RSA enVision LogSmart IPDB real-time, inline correlation with automatic threat scoring; universal device support; over 1,100 standard reports with full report wizard; Event Explorer advanced visualization and forensic analysis tool; ILM protection, retention policy management, tiered storage support.	
Storage	300 GB internal	
Operációs rendszer	Security-hardened, embedded Microsoft Windows 2003 Server standard. ECC protected RAM. Redundant/hot-swappable fans, power supplies and RAID-1 protected disks	
Hálózati kártyák	2 x 10/100/1000TX Ethernet ports included, up to (6) via add-on network interfaces	
Tanúsítványok	ISO9002 certified, UL1950, CSA22.2 no 950, EN 60950, FCCPart15 - Class A, ICES-003 EN55024:1998, EIN55022:1998, EN50082-1, VCCI V-3/2000.4, AS/NZS3548	
Tápegység	Redundant, load-sharing 400-watt power supplies	
Méret	74.4 x 44.5 x 8.6 cm (DxWxH). Rack-mount slide rails included (requires 4-post rack).	

A rendelhető SKU számok:

SKU	Megjegyzés
ES-160 - PROMO	RSA enVision 160 Appliance
ES-260 - PROMO	RSA enVision 260 Appliance
U160P-260P-S	RSA enVision 160 to 260 Appliance Upgrade

SSP-160-12M	Basic Maintenance for RSA enVision ES-160 Appliance for 12 months
SSP-260-12M	Basic Maintenance for RSA enVision ES-260 Appliance for 12 months
PSP-160-12M	Enhanced Maintenance for RSA enVision ES-160 Appliance for 12 months
PSP-260-12M	Enhanced Maintenance for RSA enVision ES-260Appliance for 12 months

További információk: http://www.arrowecs.hu/products/rsa/rsa_products.php