

# Tű a szénakazalban

## RSA enVision

....A következő dokumentum az RSA enVision termékét mutatja be.  
Ennek a dokumentumnak a segítségével a kívánt termékről alapszintű információ kapható, azonban a pontos specifikációhoz, kérjük keresse fel az Ön által preferált RSA viszonteladót.....

## Tartalomjegyzék

1.1 Előzmények .....	3
1.2 A megoldás.....	3
1.3 Loggyűjtés .....	5
1.4 Analízis .....	5
1.5 Menedzsment .....	5
1.6 Appliance .....	5
1.7 Független értékelés .....	6
1.8 Tesztelés .....	6

## Tű a szénakazalban

### 1.1 Előzmények

Mi történik akkor ha többszáz IP alapú eszköz, több ezer protokollt használva, jónéhány adatformátumban próbálja tárolni a működésével kapcsolatos logokat?

Néhány évvel ezelőtt még az volt a probléma, hogy képesek legyünk az eszközeinket „logolásra bírni”, ma már a gondjaink megsokasodtak, ugyanis az alkalmazások, eszközök, rendszerek elárasztanak minket tárolásra, elemzésre, konszolidációra váró eseményekkel.

Sokan természetesen úgy gondolhatják, hogy számukra nem fontos ez a megoldás, hiszen a cégük nem éri el azt a méretet, ahol erre a megoldásra már szükség lehet. De ha belegondolunk, hogy címtár szerver, levelezőszerver, webszerver, adatbázis szerver, tűzfal, aktív hálózati eszköz, nyomtató, munkaállomások, Wireless elérés már sok vállalatnál található, akkor már érdemes elgondolkodni azon, hogy ezeket a rendszereket manuálisan akarjuk-e felügyelni.

### 1.2 A megoldás

Az RSA enVision megoldás egy információ menedzsment rendszer, mely képes a különböző formátumú és struktúrájú adatok konszolidálására, rendezésére, szűrésére. Az RSA (EMC) egyik úttörője a security information and event management (SIEM) megoldásoknak, melyek egyre inkább terjednek, köszönhetően az infrastruktúra fejlesztéseknek és a törvényi előírásoknak.

Az RSA enVision megoldása (mely a Network Intelligence felvásárlásával került a portfólióba) nem csak a logok tárolása megoldott, hanem a következő funkciók is:

- Erőforrás osztályozás
- Trend analízis
- Anomália ellenőrzés
- Riportok
- Riasztások
- Előrejelzések
- Incidens menedzsment



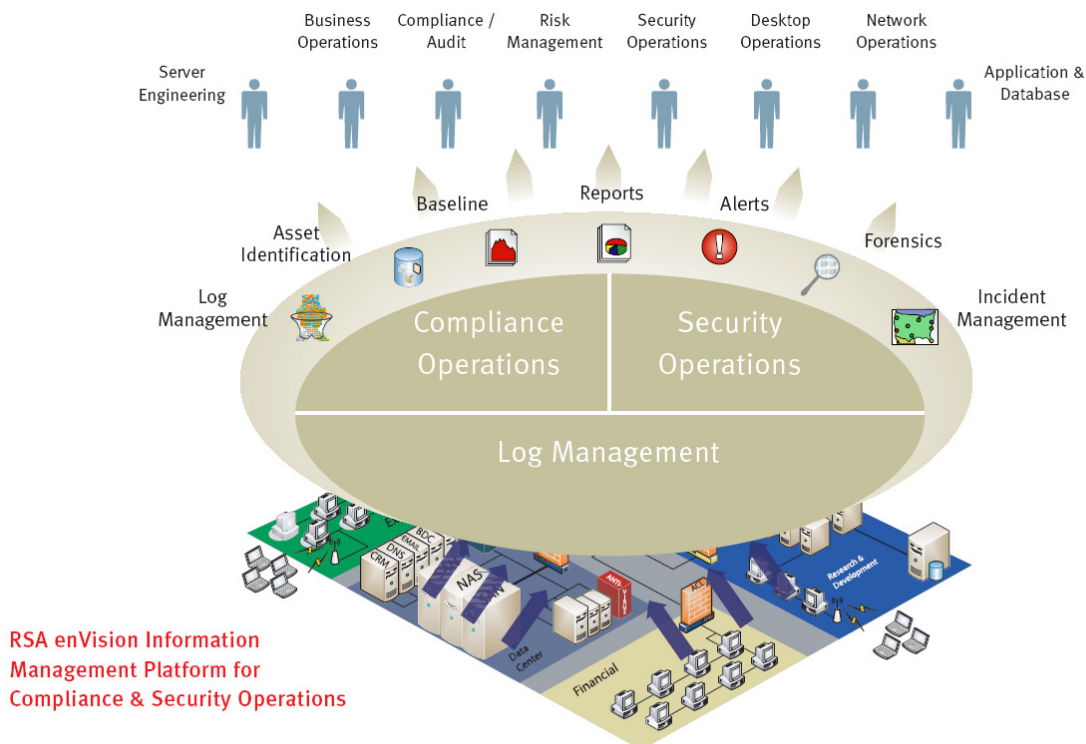
1. ábra: RSA enVision modulok

Ezen funkciók minden felhasználói igényt képesek kielégíteni, ám emellett nagyon lényeges szempont az is, hogy milyen eszközöket képes az enVision támogatni, azaz honnan képes logokat gyűjteni. A teljesség igénye nélkül, a következő gyártók támogatottak: Apple, Blue Coat, Check Point, Cisco, CA, EMC, ISS, Juniper, McAfee, Microsoft, Novell, Red Hat, Symantec.

A teljes lista itt megtalálható:

[http://rsasecurity.agora.com/rsasecured/results.asp?product\\_program=116](http://rsasecurity.agora.com/rsasecured/results.asp?product_program=116)

A megoldás további előnye, hogy nem csak egy üzleti részlegnek képes segítséget nyújtani, hanem szinte az összes osztály érezheti az előnyét (az ábrán láthatóak az érintett osztályok).



2. ábra: Az RSA enVision megoldásában érintett divíziók

A termék legfrissebb verziójának újdonságai:

- Az állandóan fennálló tárhelyhiány probléma megoldásában a még jobb tömörítési algoritmus segíthet
- Az új Event Explorer konzol segítségével a felügyelt eszközök analizálása, ellenőrzése még egyszerűbben történhet meg. Az Event Explorer valós idejű grafikus felületet nyújt a riportok finomhangolására, időzítésére, előrejelzésekre, statisztikák készítésére. Az eredmény akár grafikus akár record alapú is lehet (támogatott a html, pdf, csv formátum is).
- A 3.5-ös verzió már tartalmaz Vulnerability and Asset Management modult (VAM) is.
- Képes együttműködni független gyártók ezen megoldásaival.

### 1.3 Loggyűjtés

Ahhoz, hogy egy vállalat biztonságosan, és megbízhatóan működjön tudni kell mindenről ami az infrastruktúránkban történik. Az enVision képes többszáz eszközzel, alkalmazással, rendszerrel együttműködni. A megoldáshoz nem szükséges semmilyen Agent telepítése kliens oldalon, hiszen API-k, snmp trap-ek, syslog események, Windows Event Log-ok gyűjtését is alapértelmezetten támogatja. Amennyiben olyan eszközzel van szó, ahol a logok formátuma ismeretlen, úgy az Universal Device Support modul lehet a megoldás.

### 1.4 Analízis

Az analízisek, riportok, előrejelzések készítése sok időt emészt el, amit most akár meg is spórolhatunk. Hiszen a több mint 800 beépített riport – amelyek bővíthetők – minden kérdésre választ adhat. Mivel egyre több cég kötelessége a különböző biztonsági előírásoknak való megfelelés (SOX, HIPPA, Basel regulations) így ezek ellenőrzésére is sor kerülhet a logok összegyűjtése után.

Az enVision automatikusan térképezi fel a log események alapján a hálózatot, és egy tanulási ciklus után képes az anomáliákat is értelmezni. Természetesen ezek a szabályok finomhangolhatóak korrelációs házirendekkel.

A szűrési feltételeknek köszönhetően a logok csoportosíthatóak IP cím, port, host, felhasználó, protokoll alapján is, ezzel is növelve a kimutatások használhatóságát. Természetesen akár vállalat specifikusan testre is szabhatóak.

Az Event Explorer pedig további funkciókat nyújt, hiszen képes divízió specifikus kimutatásokra, riport-a-riportban funkcióra, és a különböző előírásoknak megfelelő teploték használatára.

### 1.5 Menedzsment

A redundandáns loggyűjtéstől, feldolgozástól kezdve a házirendek kialakításáig, a háttértárolók optimalizálásáig többfajta eszközzel képes segíteni az ügyfeleknek. Az új verziójú Event Explorer , a már kiforrott és web alapú menedzsment konzol is az egyszerűsített adminisztrációt támogatja.

### 1.6 Appliance

Minden vállalat egyedi. Ezért nem lehetséges egyetlen típussal minden erőforrás igény kielégítése. Az RSA ezért 11 különböző paraméterű szervert tervezett, melyek már 100 rendszertől akár 10.000 rendszerig képesek optimálisan működni (a termék megvásárlásával jogosultak vagyunk a szerver, az operációs rendszer, az alkalmazás és az összes modul használatára a license-ben definiált eszközszámig).

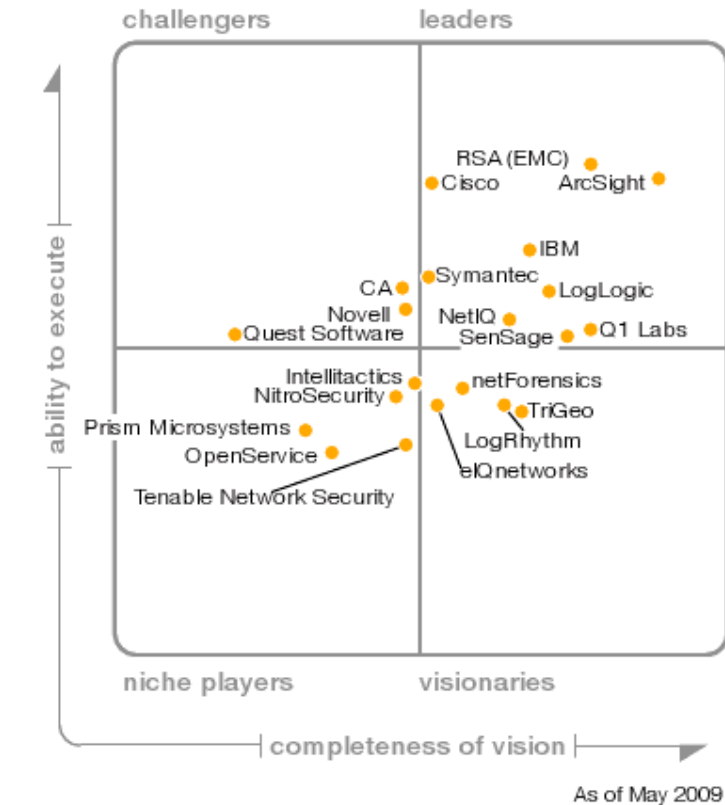


3. ábra: Az RSA enVision appliance megoldása

Az appliance másik nagy előnye a logtárolási módszer (LogSmart Internet Protocol Database – IPDB), mellyel akár többszáz ezer logesemény dolgozható fel másodpercenként. Az IPDB tömörítési aránya is nagyon jó, képes – a duplikációk kiszűrésével – akár 50-60%-os tömörítési arányt is elérni.

### 1.7 Független értékelés

A gartner értékelése szerint jelenleg az enVision rendszer a Security Information and Event Management kategóriában a technológiavezető márka.



Source: Gartner (May 2009)

4. ábra: Gartner értékelés eredménye

### 1.8 Tesztelés

Amennyiben szándékában áll hasonló megoldást vásárolni, az Arrow ECS Kft., az RSA magyarországi disztribútora – demo szerverrel felvértezve – segítséget tud nyújtani a helyes döntés meghozásában. A tesztelés ingyenes, és sok kérdésre választ adhat, ha lehetséges próbálja ki a különböző megoldásokat vásárlás előtt.