

RSA enVision™ Platform at a Glance

3-in-1 Log Management Solution

What is it?

Analysts including Gartner agree that the RSA enVision™ platform is the market-leading solution for Security Information and Event Management (SIEM). It gives organizations a single, integrated 3-in-1 log management solution for simplifying compliance, enhancing security and risk mitigation, and optimizing IT and network operations through the automated collection, analysis, alerting, auditing, reporting and security storage of all logs.

What does it do?

The RSA enVision platform collects all the event logs generated by IP devices within your network, permanently archives copies of the data, processes the logs in real-time and generates alerts when it observes suspicious patterns of behavior. Administrators can interrogate the full volume of stored data through an intuitive dashboard, and advanced analytical software turns the complex, unstructured mass of raw data into structured information, giving administrators actionable insights to help them in three main areas:

Simplifying Compliance. Administrators can automatically collect log data about network, file, application and user activity that can significantly help simplify the compliance process. Over 1,100 included reports are tailored to today's specific compliance requirements. And the solution also simplifies compliance with whatever legislation emerges in years to come, because it stores all log data without filtration or normalization and protects it from tampering, providing a verifiably authentic source of archived data.

Enhancing Security and Risk Mitigation. With real-time security event alerts, monitoring and drill-down forensic functionality, the platform gives administrators a clear view of important information. Because they can see and understand the threats and risks, they can take more effective actions to mitigate those risks.

Optimizing IT and Network Operations. Managed log data is the best source of information about infrastructure performance and user behavior. IT support staff can leverage the RSA enVision platform to track and manage activity logs for servers, networking equipment and storage platforms, as well as monitor network assets, the availability and status of people, hardware and business applications. It provides an intelligent forensic tool for troubleshooting infrastructure problems and protecting infrastructure resources, and it assists IT managers in help desk operations and provides granular visibility into specific behaviors by end-users.

How does it work?

The RSA enVision platform can draw logs from tens of thousands of devices at once – including Windows® servers, Check Point® firewalls and Cisco® routers – without need for client-side software agents. This ensures that *All the Data™* is collected continuously, all of the time. RSA enVision baselining, trending and reporting functionality gives IT and network administrators a long-term graphical overview of performance and security events, improving planning effectiveness while reducing workload. The platform may be deployed either as a standalone, plug-and-play solution or as part of a scalable, high-availability distributed architecture to cope with the demands of the largest enterprise networks. Whichever option you choose, we include all the software you'll need at no extra cost.

Web-based management and RSA enVision Event Explorer™ technology, our highly intelligent analytical tool, provide intuitive control and enhanced, detailed deep-dive and forensic analysis. When deployed as a standalone solution (using the ES range), one self-contained, security-hardened appliance does it all, including data collection, management, analysis and storage. When deployed in a distributed architecture (using the LS range), multiple dedicated appliances are deployed where required to perform key roles. Local and remote collectors perform data collection. Data servers manage the data. Application servers perform analysis and reporting. Data itself can be stored using direct attached, online, near-line or offline storage from the full EMC storage portfolio.





What options are available?

A range of ES and LS appliances are available, and all are based on the same hardware platform with licensing to suit your specific business requirements. To choose the product that's most appropriate for you, look at the number of network devices you have to monitor and the number of events per second you'll need to process.

| ES Series | | ES 560 | ES 1060 | ES 2560 | ES 5060 | ES 7560 |
|--|--|---------------------------|---------------------------|---------------------------|---------------------------|---------------------------|
| Description | | Standalone SIEM appliance | Standalone SIEM appliance | Standalone SIEM appliance | Standalone SIEM appliance | Standalone SIEM appliance |
| Sustained events PS | | 500 EPS | 1,000 EPS | 2,500 EPS | 5,000 EPS | 7,500 EPS |
| Maximum devices per appliance | | 100 | 200 | 400 | 750 | 1,250 |
| Simultaneous RSA enVision users | | 6 | 8 | 10 | 12 | 14 |
| Simultaneous Event Explorer users included/maximum | | 1/5 | 2/5 | 3/5 | 4/5 | 5/5 |
| Storage | | 300 GB internal | 300 GB internal | 300 GB internal | External storage required | External storage required |

| LS Series | LS A60 | LS D60 | LS L605 | LS L610 | LS R601 | LS R602 |
|--|------------------------------|---------------------------|---------------------------|---------------------------|----------------------------|----------------------------|
| Description | Application server appliance | Database server appliance | Local collector appliance | Local collector appliance | Remote collector appliance | Remote collector appliance |
| Sustained events PS | NA | 30,000 EPS | 5,000 EPS | 10,000 EPS | 1,000 EPS | 2,000 EPS |
| Maximum devices per appliance | NA | 3,072/6144* | 1,500 | 2,048 | 512 | 1024 |
| Simultaneous RSA enVision users | 16 | NA | NA | NA | NA | NA |
| Simultaneous Event Explorer users included/maximum | 5/15 | NA | NA | NA | NA | NA |
| Storage | RSA enVision NAS3500 | | | | | |

Product Specifications

OPERATING ENVIRONMENT

Security-hardened, embedded Microsoft Windows 2003 Server standard.
 Hardware Redundancy
 ES: ECC protected RAM.
 LS: 8 GB fully buffered RAM.
 ES/LS: redundant/hot-swappable fans, power supplies and RAID-1 protected disks.

ENVIRONMENTAL MONITORING & MANAGEMENT

IPMI 2.0 out-of-band management. 100% "headless" remote appliance mgmt.

NETWORKING

ES: (2) 10/100/1000TX Ethernet ports included, up to (6) via add-on network interfaces
 LS: (6) 10/100/1000TX Ethernet ports

STORAGE OPTIONS

Direct-attach 2.75 TB usable (see the RSA enVision DAS2000 data sheet)
 Network-attach 3.5 TB to 7 TB usable (see the RSA enVision NAS3500 data sheet)

REGULATORY AND AGENCY APPROVAL

ISO9002 certified, UL1950, CSA22.2 no 950, EN 60950, FCCPart15
 - Class A, ICES-003 EN55024:1998, ENEC55022:1998, EN50082-1,
 VCCI V-3/2000.4, AS/NZS3548.

APPLICATION SOFTWARE

The 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.

POWER OPTIONS

Redundant, load-sharing 400-watt power supplies. 120/240 volt auto-switching.

PHYSICAL

29.3 x 17.5 x 3.4 inches, 74.4 x 44.5 x 8.6 cm (DxWxH).
 Rack-mount slide rails included (requires 4-post rack).
 Weight: 59 lbs, 24.5 kg.

WARRANTY

90-day hardware warranty extendable to 5 years with active maintenance contract.



RSA Security Inc.
 RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2008 RSA Security Inc. All Rights Reserved.
 RSA, enVision, All the Data, Event Explorer and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.