RSA®

The Security Division of EMC

RSA Solution Brief

RSA enVision™ Platform

Compliance and Security Information Management

Actionable Compliance and Security Intelligence

RSA enVision™ technology is an information management platform for comprehensive and efficient transformation of event data into actionable compliance and security intelligence. RSA – The Security Division of EMC – pioneered security information and event management (SIEM), which has become a necessity for any company with operation-critical IT infrastructure and accountability to compliance standards. The most accurate analysis and verifiable compliance requires thorough data gathering. The RSA enVision Platform has been proven to efficiently collect and protect *All the Data*™ from any IP device, in computing environments of any size, without filtering and without the need to deploy agents.

Based on the LogSmart Internet Protocol Database (IPDB), RSA enVision appliances capture and store up to hundreds of thousands of data events per second, providing an enterprise-view of activity from any number of sources, including perimeter and network devices, operating systems and even proprietary applications. That's why over 800 customers – including some of the largest global Fortune 100 enterprises – have selected RSA enVision technology as the optimal platform to acquire and leverage security and compliance intelligence.

RSA enVision Platform:

- View real-time events, correlate events across device types
- Alert against baseline anomalies
- Alert on unusual privileged user activity
- Maintain digital chain of custody with unaltered log data for data retention and forensic requirements
- Automate compliance reports
- Provide inbound and outbound IP traffic summaries

A Platform for Enterprise Log Management, Compliance and Security

The RSA enVision platform eliminates redundant business data silos that can be created in many organizations. By collecting and managing *All the Data*™, the platform helps inform virtually anyone in your organization. Everyone from desktop operations, to the help desk, to applications and network management professionals can get the information they need from a single platform for enterprise log management, compliance and security. Capturing every event on the network ensures effective enterprise SIEM and eliminates uncertainty. Compliance auditors have a complete set of data to meet reporting requirements. Risk management staff and security operations have complete picture to evaluate security alerts in real time. Thanks to powerful RSA enVision collection, management and analysis tools, compliance and security objectives are easily achieved.

Stakeholder Value

Stakeholders	What is needed?	The RSA enVision Platform Answer
Network Administrator	What systems are in place to monitor access control, privileged user monitoring and configuration controls?	By capturing *All the Data*™, RSA enVision technology analyzes hundreds of disparate security events and provides alerts on changes and unauthorized use of systems in real-time, making managing security more streamlined.
Security Administrator	How will your organization create a compliance program in a cost-effective manner?	Prove compliance with packaged reporting templates formatted specifically for Sarbanes-Oxley, GLBA, PCI, HIPAA, FISMA, NERC, Basel II, and NISPOM.
Server Administrator	How can you keep up with real-time monitoring, threat detection and malicious code detection without being flooded by false positives?	RSA enVision technology reduces false positives by correlating data against other network and security devices and helps you to rank threats to your most critical assets and brings those threats to your immediate attention.
Database Administrator	When a security threat is identified, how can I cross-reference that with the rest of the network?	With RSA enVision Event Explorer, you can look across applications, firewall, IDS and other types of data and zoom in on the data from different perspectives.
Application Administrator	How do I add my proprietary application to the mix?	In addition to hundreds of supported devices, the RSA enVision platform's open architecture provides all the tools required to add new source devices at will.

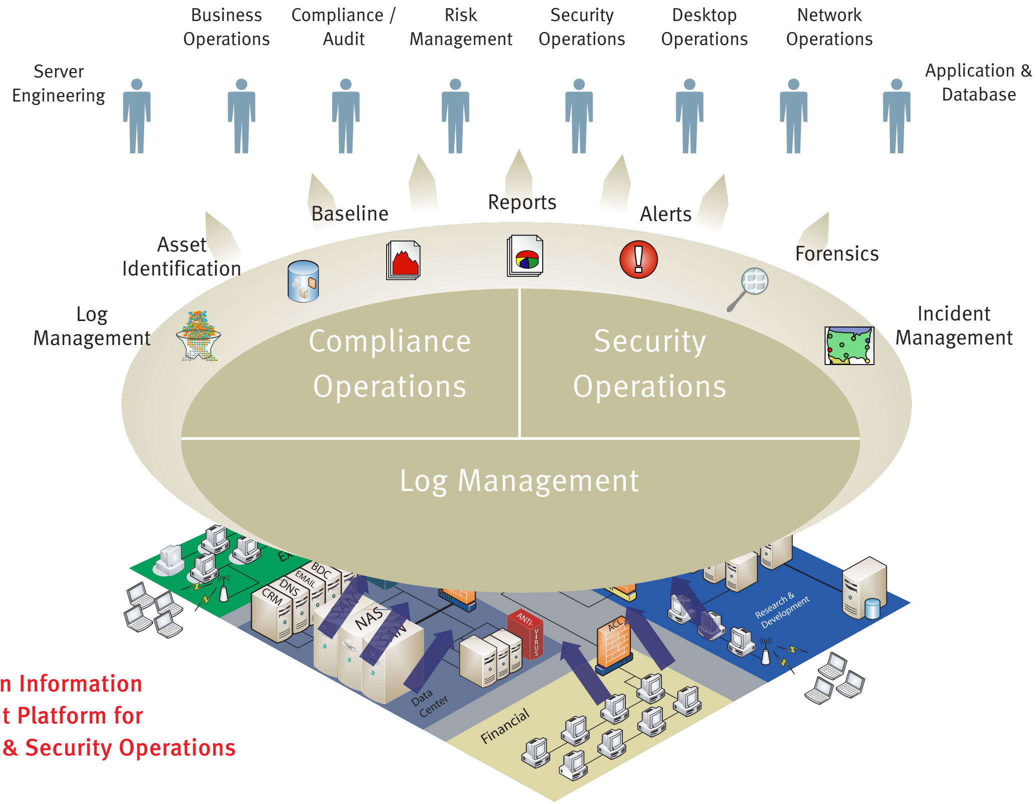
A Platform for Information Management

Meeting compliance mandates and providing for accurate forensic analysis means that ever-increasing amounts of log data must be retained. The ability to store and manage this data over its lifecycle is now imperative for successful SIEM deployment. From high-availability collection and protection to tiered storage optimization, RSA enVision technology provides a platform for enterprises of all sizes to manage growing volumes of information economically, according to its changing value to the business. The RSA enVision Information Lifecycle Management (ILM) solution set ensures long-term SIEM success with information lifecycle management abilities ranging from flexible retention policies to integrations with leading storage vendors to available pre-configured storage options.

A Platform for Success

Proven performance, collection and analysis of *All the Data*, best-in-class scalability, and the most complete information lifecycle management means that RSA enVision technology continues to be a leading platform for compliance and security operations success. Moreover, the open architecture of RSA enVision can fit your security and compliance strategy by supporting interoperation with other SIEM components and analysis tools, handling any device type, and integrating with EMC and leading third party storage solutions. It all adds up to better overall return on investment, which is why RSA enVision technology continues to be a leader in SIEM solutions.

a leader in security information and event management solutions



RSA enVision Information Management Platform for Compliance & Security Operations

Collection

To truly secure the information infrastructure, organizations need to know exactly what is happening across the entire network and IT infrastructure – all of the time. Complete collection of all event data, including employee activities, access to customer and financial information, and suspect or denied access attempts from outside the network is key to full security and compliance regulation coverage. The RSA enVision platform allows organizations to capture data in real time from thousands of disparate devices and applications across the enterprise. Whereas other solutions reduce or pre-filter the data coming from source devices, RSA enVision appliances leverage the advanced LogSmart IPDB architecture to capture *All the Data* from network, security, host, application and storage layers across the enterprise. Data is immediately and efficiently written and read back for swift analysis.

Agent-free collection means faster deployment, no ongoing management of agents spread throughout the network, no risk or impact to the network infrastructure and reduced total cost of ownership due to the ease of configuration and deployment.

Universal Device Support provides the ability to add message collection from devices and applications in an ad-hoc manner. The RSA enVision open architecture provides all the tools required to add new source devices on-the-fly. Ideal for auditing applications built in-house and for second-tier devices, universal device support gives the user an easy to use platform to collect, analyze and manage log data for new devices and it offers:

- A graphical user interface to add new messages.
- Control over device and message classification.
- Simple definition of message IDs and payload data.
- Support for multiple applications running on the same host.

Analysis

RSA enVision technology radically simplifies security and compliance by consolidating and analyzing data from complex enterprise infrastructure. This powerful capability allows organizations to respond faster to external threats and discern internal ones by gaining unified and comprehensive visibility over their networks.

Baselines

The RSA enVision platform is built on top of a knowledge base encompassing tens-of-thousands of known log messages and an open classification taxonomy that learns network patterns to establish baselines.

- Baselines are created automatically – with no configuration required.
- Baselines are available for any user-defined time frame.
- Correlation rules can be built to detect baseline anomalies based on percentage change.
- Dynamic baselines can be created to track specific groups of devices and events.

Correlated Alerts & Security Reports

With its scalable data collection and vast view of all logs, the RSA enVision reporting engine provides quick and easy access to compliance-sensitive data. Built-in reports are available for specific compliance regulations, and administrators can create reports based on their organization's specific compliance policies. With over 700 built-in reports, RSA enVision technology provides information on a wide variety of user-defined issues.

- All reports can be modified to meet specific needs.
- Reports can span any time period, from minutes to months of data.
- Reports can run ad hoc or can be scheduled to run automatically.
- Multiple tabular and graph outputs are supported.
- Multiple export formats supported, including .csv, .pdf and more.

Forensics

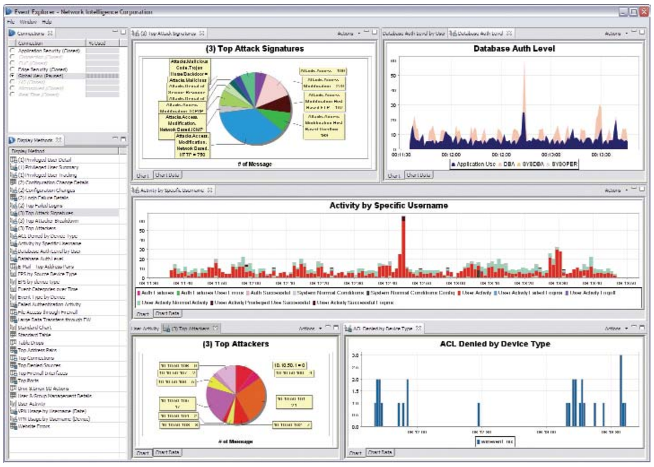
The RSA enVision platform provides a detailed view of the events that trigger security threats thanks to extensive drill-down capabilities. Security administrators can see exactly what patterns are forming on their networks and the specific IP addresses, ports, hosts, users and protocols involved in these patterns. Extensive querying and filtering capabilities and robust user interface tools all help users to search for data by any user-defined attribute.

Visually Analyze *All the Data*

Event Explorer is an advanced analytics module for the RSA enVision platform. You can rely on the Platform to capture *All the Data* and Event Explorer to dynamically view it. With the ability to zoom into selected perspectives, Event Explorer widens the range of issues that can be investigated simultaneously. Event Explorer provides a flexible window into compliance, security and business operations so you can analyze *All the Data* and benefit from 100 percent visibility into the security and compliance infrastructure.

Event Explorer

Powerful real-time event information analysis and visualization


Event Explorer – Network Intelligence Corporation
File Window Help
Connections
Display Methods
(3) Top Attack Signatures
# of Message
Database Auth Level
Application Use DBA SYSDBA SYSOPER
Activity by Specific Username
(3) Top Attackers
# of Message
ACL Denied by Device Type
Chart Chart Data
Actions

Management

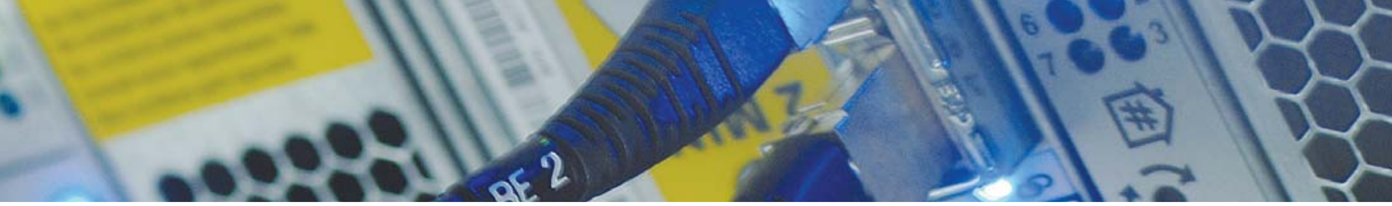
From high availability collection and protection to policy-based retention to tiered storage optimization, RSA enVision technology provides the most complete platform for enterprises of all sizes to manage growing volumes of information according to its changing value to the business. The RSA enVision ILM solution set encompasses processes, tools, and configurations that meet the critical need to optimize, protect, store and intelligently manage large volumes of information over the security and compliance information lifecycle. RSA enVision ILM technology encompasses

RSA enVision Appliances

Every enterprise is unique. That's why RSA offers a range of solutions that are scalable to any size. As you grow, your SIEM solution can easily grow with you. Please contact RSA to find out about an appliance solution that will meet your exact needs.

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	LC 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	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					



The expertise of RSA – and EMC – can help your organization identify the best solution quickly.

data optimization and protection, flexible retention policy settings, integrations with leading storage vendors and easy to implement pre-configured storage package options. For instance, log retention policies defined in the Platform can be automatically executed through EMC's storage solution portfolio, enabling complete collection-to-retirement management for all security information.

Powerful Professional Services

RSA offers a full suite of professional services expertise to help you get the most from your security and compliance solution. Our consultants are fully qualified to apply a deep knowledge of networks, storage, applications and industry-specific security issues to your high-level business challenges. The expertise of RSA – and EMC – can help your organization identify the best solution quickly, implement the right solution efficiently and seamlessly integrate our technology with your existing infrastructure. You can benefit from the security expertise of RSA and the breadth of enterprise management and storage expertise of EMC to help you deploy the leading SIEM enterprise platform for compliance and security operations with an aggressive ROI and immediate results.

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 management.

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 (refer to RSA enVision DAS2000 data sheet)

Network-attach 3.5 TB to 7 TB usable (refer to RSA enVision NAS3500 data sheet)

REGULATORY AND AGENCY APPROVAL

ISO9002 certified, UL1950, CSA22.2 no 950, EN 60950, FCC Part 15 – Class A, ICES-003 EN55024:1998, EIN55022:1998, EN50082-1, VCCI V-3/2000.4, AS/NZS 3548.

APPLICATION SOFTWARE

RSA enVision, featuring LogSmart IPDB; real-time, inline correlation with automatic threat scoring; universal device support; over 800 standard reports with full report wizard; Event Explorer advanced visualization and forensic analysis tool; RSA enVision 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 is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA®
The Security Division of EMC

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