



RSA[®]

The Security Division of EMC

RSA Solution Brief

RSA enVision[®] Platform: SIEM for All Sizes

No matter what the size of the organization, certain things will always hold true. There are never enough people to get everything done, demands on the IT team grow faster than the IT budget, and it's tough to get security dollars unless it:

- Averts or limits the impact of an inevitable catastrophe
- Gets the auditors in and out the door more quickly
- Gets the job done with fewer resources

Same problems, fewer people

Not all IT shops are matrix-managed behemoths. There are hundreds of thousands of companies worldwide which have a few hundred to a couple of thousand employees. These companies don't need all the flexibility of an enterprise solution but they're big enough to have complex needs. What's more, they're often subject to the same basic constraints of larger organizations when it comes to security and compliance.

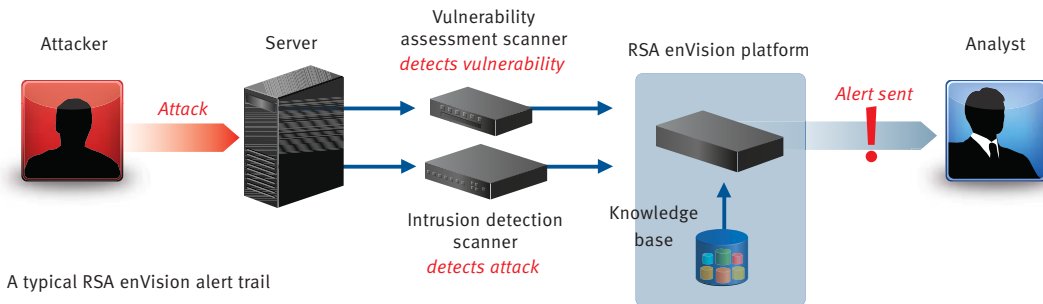
- **Compliance requirements can be extremely tough.** A large number of these companies are publicly traded and thus subject to securities rules. In the U.S. alone, thousands of companies have fewer than 1,000 employees yet are still subject to SOX compliance. Many of these companies operate in industries with stringent compliance requirements like financial services, healthcare, energy and retail. Also, big companies are increasingly passing on compliance obligations to their smaller suppliers, and asking tough questions about supplier internal controls, so compliance with frameworks like ISO27002 is becoming more important.
- **Security threats seldom differentiate between large and small organizations.** Smaller companies get just as hard hit by worms as larger organizations, and a smaller IT staff also means a lower likelihood of enforcing strict separation of duties that would prevent abuse by privileged employees.
- **IT budgets are often more stretched in smaller and mid-sized environments.** When it comes to IT security, smaller organizations aren't able to take advantage of the economies of scale that larger organizations can. Companies with fewer than 2,500 employees spend proportionally less on security – Forrester reckons that in 2008, companies with fewer than 1000 employees spent on average 9.1% of IT budget compared to 11.7% in larger organizations.

All in all it means any money being spent on IT, and security in particular, had better contribute to being able to do more with less.

A day in the life of an RSA enVision platform user

Bob is the security guy in the IT department of an insurance company. His company has about 1,200 employees, and an IT department of 60 people. He is the only person dedicated to security, but he gets help from some of the network and server folks. He also gets pulled into non-security issues as problems occur. Bob bought RSA enVision a year ago – he uses it extensively.

- *The auditor asks Bob for a report of all configuration changes in the last month.* The RSA enVision platform automatically collects and classifies all events, so it can recognize configuration changes without requiring intimate administrator familiarity with the system log format. This means that Bob can generate reports showing all configuration changes in just a few clicks. Without the RSA enVision platform, Bob would need to manually log in to each system to retrieve the logs – or worse still, get the system administrator for each system to do it for him. Bob would then need to pore over the logs and work out which events are configuration changes – a highly time consuming affair.
- *A vulnerable server is being attacked.* Bob deployed an intrusion detection system a few years ago. It produced so many alerts that he stopped paying attention to them – one time a web server was attacked, but the alert was buried since it was only one of hundreds triggered that day. Bob also has a vulnerability assessment tool, but he can't even hope to keep up with all the vulnerabilities it finds. With the RSA enVision platform, though, he can make both tools useful, since it can correlate IDS logs with vulnerabilities that his scanner has found – so he only gets alerted for a real attack on a vulnerable server.



A typical RSA enVision alert trail

– *A failure halts the customer portal.* This is one of those days when Bob needs to put on his non-security hat. The portal has just gone down for the third time in as many hours. Luckily, Bob is collecting events from the portal application, the Oracle® database, Linux OS and the Celerra® storage that holds the data. The application is producing multiple error messages, but Bob is quickly able to pull all the different logs to determine that this is the result of a schema change in the database that’s causing an hourly-running script to hang.

– **Real-time and Historical Log Analysis.** The RSA enVision platform provides a single point where users can configure real-time correlated alerts, generate reports for auditors or management, or perform ad-hoc queries to troubleshoot issues.

The platform may be deployed as a standalone, plug-and-play solution. It can also grow with you to become a scalable, high-availability distributed architecture. However you choose to deploy the RSA enVision platform, we include all the software, reports and correlations rules you’ll need at no extra cost.

How does the RSA enVision platform make life simpler?

RSA enVision is a 3-in-1 Security Information and Event Management platform. It lowers the overhead of log analysis through:

- **Simpler Collection.** The RSA enVision platform can draw logs from hundreds, thousands or even tens of thousands of devices at once – including Windows® servers, Check Point® firewalls and Cisco® routers – without need for client-side software agents. If you have a home grown event source you need to collect from too, RSA enVision Universal Device Support allows you to integrate that event source easily, without additional coding.
- **Automated Log Management.** The RSA enVision platform provides end-to-end log lifecycle management. At collection, it compresses and tamper-proofs the log. Then throughout the log’s lifetime, the RSA enVision platform manages the storage of the data, whether it be on online or near-line storage, through to its archive and disposal in accordance with business requirements.

Why choose the RSA enVision platform?

RSA enVision technology is the industry-leading SIEM solution, and is an important component of the RSA and EMC product ecosystem. It should be a top choice for anyone considering a log management or SIEM solution for the following reasons:

- **Low TCO solution.** From its appliance form-factor to its agent-less architecture and ease of customization, the RSA enVision platform is designed to maximize time-to-value and minimize administrative costs.
- **Security knowledge you can build on.** The RSA enVision platform takes advantage of a broad partner eco-system of strategic technology partners and front-line security and compliance expertise. This provides users with a broad set of supported event sources, as well as built-in correlation rules and reports and regularly updated threat and vulnerability information. This knowledge augments security analysts’ expertise, making them more productive and effective.

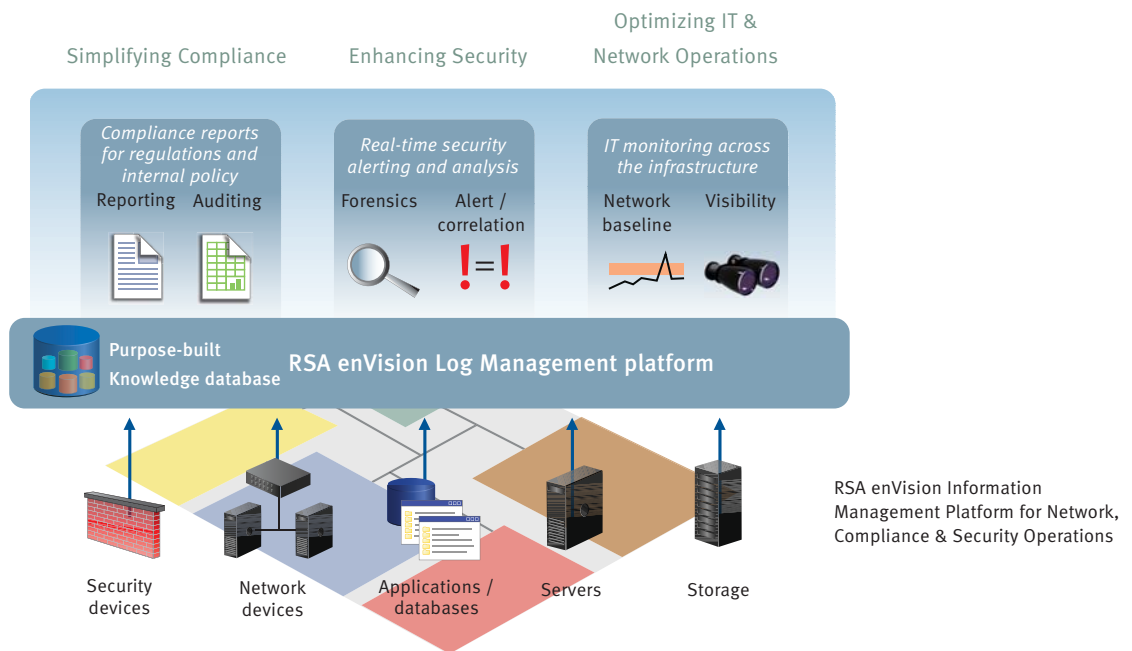
- **Proven solution with a large and active install base.** The RSA enVision platform has an unparalleled installed base of more than 1600 production customers across all industries and geographies. The online customer forum “Intelligence Community” is extremely active, and customers, product management and RSA professional services find it invaluable for sharing best practices as well as tips and tricks. This makes it a low risk purchase, since whatever you’re trying to do, you’re unlikely to be charting new territory.
- **Designed to grow with you.** The RSA enVision layered architecture allows deployments to be easily expanded. This means that users can start small and grow as SIEM needs evolve.
- **All from EMC and RSA.** The RSA enVision platform is a best-in-class product, supported by a strategic vendor with strong balance sheet. This provides customers with a single point of contact and global customer support. Moreover, it simplifies IT operations by integrating with a wide range of RSA and EMC solutions, including RSA Authentication

Manager, RSA Data Loss Prevention, EMC Voyence, EMC Celerra and EMC CLARiiON storage management solutions.

RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world’s leading organizations succeed by solving their most complex and sensitive security challenges. RSA’s information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, 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 Security Inc.
 RSA Security Ireland Limited
www.rsa.com

©2009 RSA Security Inc., all rights reserved. RSA, the RSA logo and enVision are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC, Voyence, Celerra and CLARiiON are registered trademarks of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.