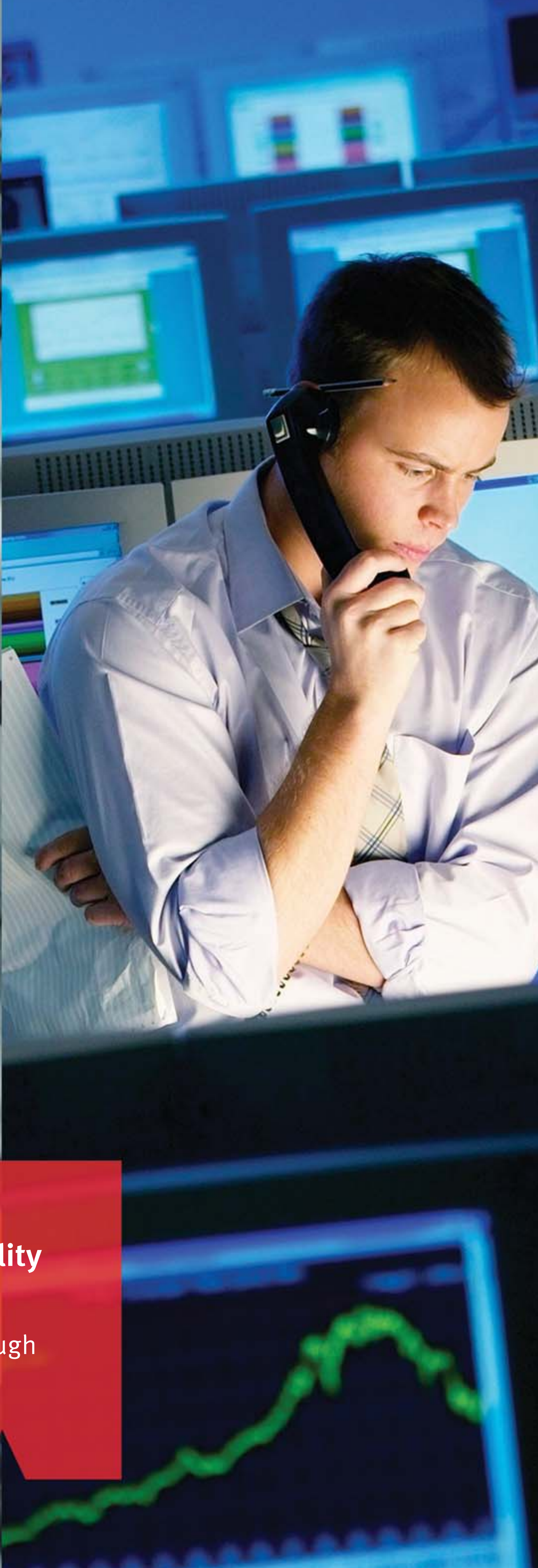


RSA

The Security Division of EMC

CISCO DEVELOPER

Preferred Solution

RSA Solution Brief

Extending Cisco® MARS Functionality with the RSA enVision® Platform

Enhance Security and Compliance through comprehensive forensics capabilities, auditing and reporting.

Cisco Security Monitoring, Analysis and Response (CS-MARS) empowers thousands of organizations to identify, manage and counter security threats. It works with existing Cisco network and security investments to identify, isolate and recommend precise removal of offending elements. Additional elements for enhancing security and compliance include enabling security investigations with network topology awareness and network behavior anomaly detections well as providing alerting, reporting and auditing across the entire Cisco IPS, firewall, routing, switching and end host infrastructure.

In order to extend CS-MARS alerting, reporting and auditing capabilities across a heterogeneous infrastructure, RSA, a Cisco Developer Network Partner, works closely with Cisco to support the integration of CS-MARS with the RSA enVision® platform, a market-leading solution for heterogeneous Security Information and Event Management (SIEM).

Key Benefits

- Leverages an investment in CS-MARS with the added value of enVision intelligence, analysis and long-term storage capabilities
- Enhances security operations by providing correlation across Cisco devices and other devices and applications
- Simplifies compliance with more than 1,300 reports tailored to specific compliance requirements
- Extends and accelerates forensics capabilities
- Automates archived log data searching
- Provides end-to-end log lifecycle management

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 analyze 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 into compliance status, user behavior and security anomalies, to help them in three key 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 1,300 included reports are tailored to today's specific compliance requirements, e.g., national laws (SOX, Basel II, JSOX, etc.), industry regulations (PCI, etc.) and best practices & standards (ISO27002, ITIL, etc.). The solution stores all log data without filtration or normalization and protects it from tampering, providing a verifiably authentic source of archived data.

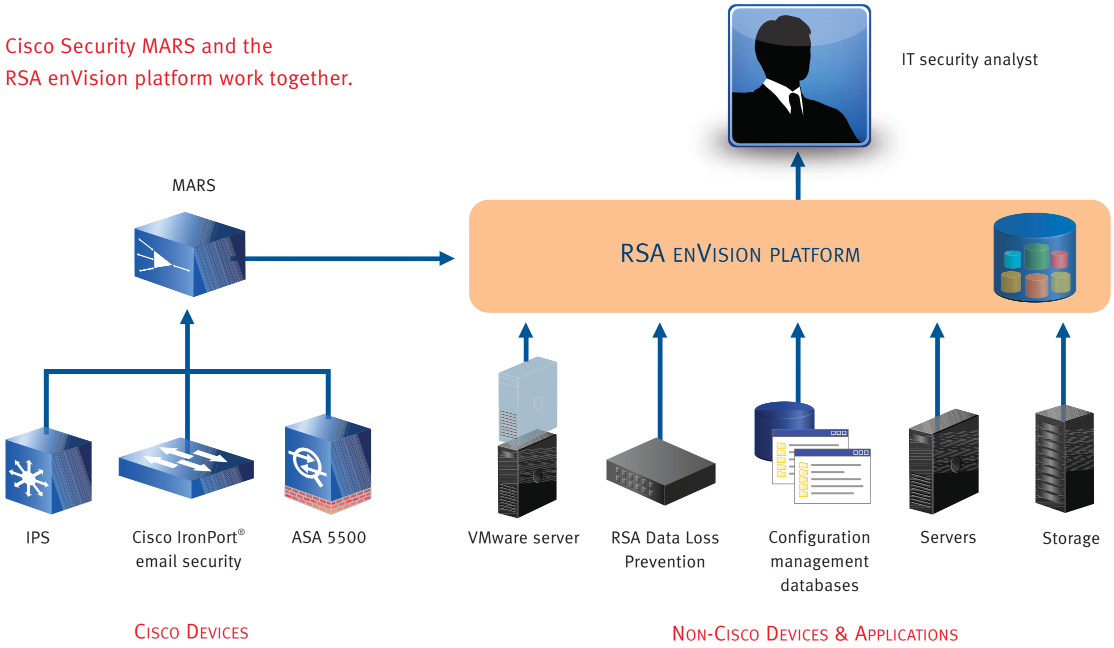
Enhancing Security and Risk Mitigation

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 to their Cisco network and the rest of their infrastructure and applications, they can take more effective actions to mitigate those risks. As an example, enVision technology integrates with RSA® Data Loss Prevention (DLP), which can discover the information of highest sensitivity throughout the environment. The RSA enVision platform can therefore correlate a CS-MARS alert for suspicious phone home activity from a botnet with an RSA DLP alert indicating sensitive data is leaving the network and thus fire a high priority alert for the security operations analyst to investigate.

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, it manages the storage of the data, whether online or nearline, through to its archive and disposal in accordance with business requirements.

Cisco Security MARS and the
RSA enVision platform work together.



Integration Details

The RSA enVision platform accepts all 100+ CS-MARS alerts, including those on botnets, client exploits, viruses, worms and more. These alerts can also be correlated with alerts from non-Cisco devices and applications to identify high priority issues that need immediate investigation. The Cisco MARS fired alerts can also be viewed in the enVision platform in multiple ways including dashboards, e-mail messages, SMS messages, etc.

By collecting and parsing CS-MARS archives, RSA enVision log management can also provide long-term storage and analysis of CS-MARS log and event data for compliance reporting and forensics investigations.

About RSA and Cisco

RSA and Cisco's long standing partnership provides customers with tightly integrated and certified solutions in the remote access, data loss prevention, web security, security management, wireless, core routing and IP telephony areas. RSA authentication and encryption products such as RSA® Digital Certificate Management Solutions, RSA SecurID® authentication and RSA BSAFE® encryption provide an integrated approach to the security of the Cisco Powered Network. RSA DLP and Cisco IronPort solutions are integrated to offer a built-in approach to data security. RSA enVision log management is integrated with Cisco Mobility Services Engine and CS MARS to increase the efficiency of security and compliance tasks and reporting.

In addition to Cisco Security MARS, the RSA enVision platform supports more than 20 Cisco devices including ASA, IronPort®, Pix® Firewall, IDS, UCS and WLC.

CISCO DEVELOPER
Preferred Solution

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.

CISCO DEVELOPER
Preferred Solution

MARS SB 0210

RSA®
The Security Division of EMC

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