



The Security Division of EMC



RSA Solution Brief

RSA Solutions for Advanced Security Operations

How do you advance your security operations function?

Increasingly sophisticated security threats and the growing challenge of compliance mean that organizations must take a different view of security operations management. The traditional approach to security operations, centered almost exclusively on security information and event management (SIEM), is now being expanded. With SIEM at the core, advanced security operations programs also integrate data loss prevention, threat intelligence and key technologies from the IT operations function.

Together, these capabilities provide a comprehensive platform for the protection of critical resources and the achievement of compliance through comprehensive incident detection, response and remediation. With the appropriate enabling technologies in place, your security operations team is able to move quickly to identify suspicious activity or weaknesses in your security infrastructure; to respond to incidents swiftly and take steps to limit damage; and to analyze and report on events for the purposes of compliance and improving security across your organization.

Managing Advanced Security Operations Within Your Organization

To keep pace with the constant evolution of threats and compliance obligations, security operations teams need a comprehensive and sustainable framework for monitoring security events in real time and the delivering intelligence to both anticipate and respond to incidents. Traditionally this has meant security operations centered on SIEM. But for many organizations, a new view of security operations is emerging: one that sees SIEM as a security operations backbone and tied in with other key technologies and processes. By integrating capabilities from the broader security organization, and those found within the IT operations environment, security operations is able to establish a much more robust and sustainable program.

These organizations view security operations as effectively combining a set of core capabilities, both strategic and tactical, that are central to effective risk and IT compliance management. In addition, this 'next generation' of security operations requires coordination across numerous systems – many of which have not traditionally supported the security operations function. For example, by integrating IT operations capabilities, including change and configuration management and IT service desk, security operations is better able to detect and remediate security incidents.

By coordinating and integrating these functions, organizations have a better ability to handle incidents – the overriding priority of an advanced security operations function. And although it can be managed as an independent activity, integrating incident handling with other security and IT functions enables swifter responses and more accurate and complete intelligence. The result is better support given to other business functions, such as Legal, and more effective compliance.

So where do you turn for solutions that will facilitate this integrated approach and help you protect against the security threats to your business?

RSA can help you to create an advanced security operations function from the ground up, or evolve your existing operations.

RSA and EMC solutions for advanced security operations combine expertise within our consulting and advisory services team with our proven technology platforms to establish your next-generation security operations program. We equip you to effectively identify, manage and report on information risk, right across your organization, and give you the controls you need to adapt easily to the ever-changing landscape of IT compliance.

RSA solutions for advanced security operations combine the expertise of our consulting and advisory services with proven technologies to establish next-generation security operations programs.

RSA solutions for advanced security operations deliver essential services and technology capabilities that help you to:

■ Plan and develop your security systems and processes

- Define metrics for measuring and reporting
- Define team requirements
- Establish work flow processes
- Enact and test business continuity plans

■ Monitor and manage your infrastructure

- Identify hardware and software failures relevant to the security infrastructure
- Identify vulnerabilities affecting the IT infrastructure
- Ensure that IT infrastructure component configuration meets policy
- Correlate and analyze security inputs from multiple sources
- Manage changes in key elements of the security infrastructure
- Manage user access

■ Manage and respond to security incidents and events

- Identify potential security events in real time
- Provide immediate alerts regarding potential attacks
- Identify and execute basic remediation
- Drive more complex remediation through IT teams (such as the NOC)

- Monitor the effectiveness of security devices (e.g., IPS, IDS)
- Understand and manage emerging vulnerabilities
- Provide a real-time view into a network's security posture
- Identify hosts and resources affected by a security incident
- Integrate security events with incident response systems
- Identify and respond to both network and host-based attacks
- Ensure efficient and prioritized incident response
- Report on incident remediation status
- Enforce and validate compliance

■ Take a strategic view of security operations

- Investigate security incidents
- Identify trends to plan future remediation
- Drive internal awareness of security posture and policy
- Identify security areas needing improvement
- Create a sustainable framework for an advanced security operations program

Integrated Solutions for Advanced Security Operations

We bring together a comprehensive set of consulting and advisory services and IT security technologies to help you define, establish and manage an advanced security operations function. With RSA, you can take advantage of:

- Strategic consulting and design services that will identify requirements and help you develop a comprehensive security operations program
- Market-leading IT security technologies, including the RSA enVision® platform and the RSA® Data Loss Prevention Suite, that form your core security operations program
- Cutting-edge services, such as the RSA® FraudActionSM Threat Intelligence, that can help you stay ahead of emerging threats
- Integration with network operations technologies, such as change and configuration management and IT service desk, from EMC and other vendors to enhance the capabilities of the security operations function

RSA Consulting and Advisory Services

RSA offers a complete range of services that can be tailored to meet the needs of your organization, whether to address a specific situation or create an end-to-end security framework. The RSA Professional Services organization has the expertise to help you achieve measurable improvements in your security operations that align with your business objectives. We work closely with your stakeholders to devise the technology solutions and processes that will protect your information resources, enterprise-wide.

Security Operations Strategy & Assessment: appropriate for customers with established security operations processes, or are establishing new security operations processes, and wish to advance their capabilities based on industry best practices and current state gap analysis,

RSA Consulting and Advisory Services

Service	Benefit
Security Operations Strategy & Assessment	Strategic assessment and recommendations based on security best practices
Security Operations Analysis and Design	Tailored plans for enhancement or implementation of an organization's security operations
Security Operations Management	Consultation centered around operational requirements

providing an actionable set of vendor and product agnostic recommendations.

Security Operations Analysis & Design: appropriate for customers that want a broad evaluation of security operations requirements providing a recommended solution design to meet the customer's objectives for security operations and incident management. It also includes an incident handling framework and next steps for the development of appropriate policies and procedures for security operations.

Security Operations Management: appropriate for customers seeking the development of more comprehensive policies, procedures, guidelines and documentation for an effective security operations function, including operational run-books and work flow that support the ability to run a security operations center / function or Incident Handling program on a day to day basis.

In addition to RSA Consulting and Advisory Services, the development of an advanced security operations function is supported by a combination of key technologies and solutions from RSA and EMC.

A comprehensive set of consulting and advisory services, and IT security technologies

RSA Advanced Security Operations Technology Solutions

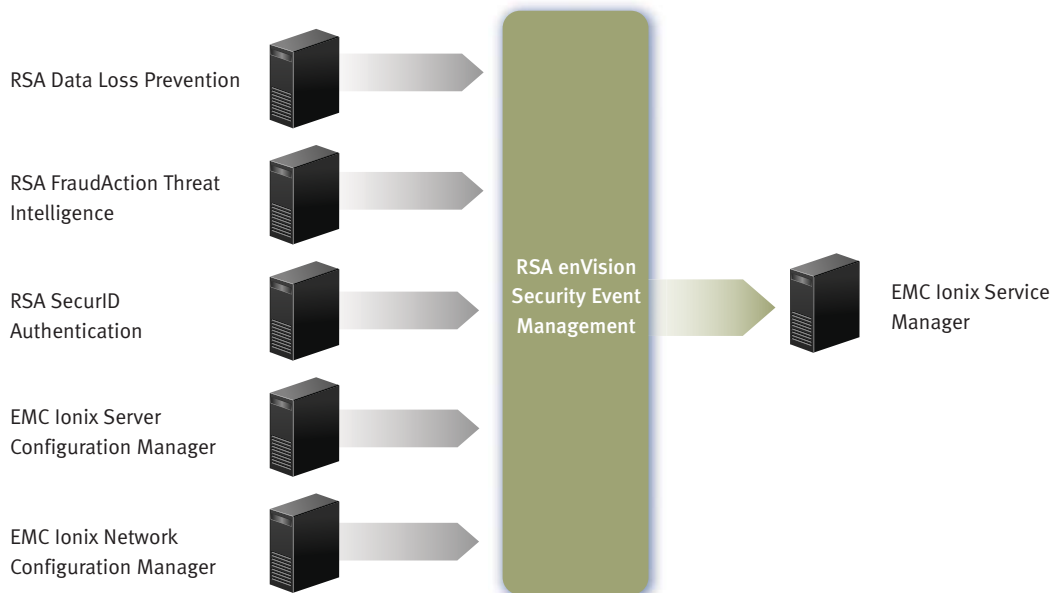
Solution	Function
RSA enVision® platform	Integrated SIEM that serves as the central platform for an advanced security operations program
RSA® Data Loss Prevention Suite	Provides a policy-based approach to securing data that integrates with RSA enVision to enable an information-centric approach to security operations
RSA FraudAction™ Threat Intelligence	Helps your security operations teams understand the current and emerging threat environment
RSA SecurID® authentication	Market-leading two-factor authentication technology to secure user access
EMC Ionix® Server Configuration Manager	Identifies vulnerabilities affecting your IT infrastructure and determines whether the associated security events are part of a broader attempt to compromise your business
EMC Ionix Network Configuration Manager	Provides a complete view of the configuration of systems such as firewall policy, IPS/IDS and VPN, enabling your business to deploy security updates to devices quickly
EMC Ionix Service Manager	Improves reporting on incident remediation status
EMC Ionix for IT Operations	Automates service and infrastructure monitoring, analysis and reporting
EMC Ionix Configuration Analytics Manager	Helps to ensure that network and server devices comply with security best-practice policies

RSA enVision® Platform

As the centerpiece of an advanced security operations program, the RSA enVision platform provides collection, alerting and analysis of log data to help your organization to simplify compliance and quickly respond to high-risk security events. RSA enVision technology is an effective SIEM and log management solution that collects and analyzes large amounts of data in real time, from any event source and in computing environments of any size.

By delivering the ability to integrate with a wide range of security (e.g., IDS, IPS, authentication, DLP) and IT service management technologies (e.g., service desk, incident management, change and configuration management) from many leading vendors as well as EMC, and support for standards and frameworks such as ISO 27002 and ITIL, RSA enVision event management helps you to better leverage capabilities across your security and IT operations environments.

The RSA enVision platform significantly reduces security operations workloads by using industry-standard vulnerability assessment systems to analyze and rate events based on actual risk versus potential



risk. Your organization can gain a real-time view of its security posture across the enterprise, with the ability to see, respond to and report on security events and attacks quickly and more efficiently.

RSA Data Loss Prevention Suite

RSA DLP technology provides a policy-based approach to securing data. It also integrates with the RSA enVision platform, providing the ability to identify where sensitive data exists across the enterprise, enforce controls, actively monitor data, alert administrators to any suspicious activity, and report on and audit events to ensure compliance with policy.

By monitoring and reacting to suspicious activity that's tied to sensitive data, RSA DLP solutions identify potential non-compliance events in real time and generate immediate alerts. They also control the transmission of sensitive data across your IT infrastructure: quarantining, deleting, moving or applying rights management to documents that contain private information.

RSA® FraudAction™ Threat Intelligence

RSA FraudAction Threat Intelligence helps security operations teams understand current and emerging threats. It monitors fraudster communications and identifies hosts and resources that may be under attack, and then takes steps to protect them. Offered as an outsourced service, RSA FraudAction Threat Intelligence helps your organization to support its security operations function and deliver even greater value to the business by minimizing resource investment while deploying a solution quickly.

RSA SecurID® Authentication

RSA SecurID technology is the most widely deployed, relied-upon two-factor authentication solution on the market today. Businesses globally trust RSA SecurID strong authentication to ensure that the right people get secure access to the data they need. Within an advanced security operations function, RSA SecurID technology helps you to better control access through strong authentication, particularly for privileged users.



EMC Ionix Server Configuration Manager

Working together with the RSA enVision platform, EMC Ionix Server Configuration Manager (SCM) identifies vulnerabilities affecting your IT infrastructure and determines whether the associated security events are part of a broader attempt to compromise your business. SCM also helps security teams to ensure that IT configurations meet policy guidelines and can identify and remediate violations. By enforcing access controls SCM helps to manage user access and also provides an efficient and prioritized event and incident response, accelerating root cause analysis.

EMC Ionix Network Configuration Manager

In addition to the comprehensive protection offered by SCM, EMC Ionix Network Configuration Manager (NCM) helps security teams to manage changes to key elements of the IT security infrastructure such as firewall policy, IPS/IDS and VPN. NCM provides a complete view of these systems' configurations, helping your business to roll out security updates to devices quickly. NCM also helps security staff see which devices are affecting service levels.

EMC Ionix Service Manager

EMC Ionix Service Manager supports the development of an advanced security operations function by helping you to more easily report on incident remediation status. Through integration with IT monitoring tools, Ionix Service Manager automates service management and proactively reports on potential service-affecting problems related to availability or performance.

EMC Ionix for IT Ops

EMC Ionix for IT Ops automates service and infrastructure monitoring, analysis and reporting, helping security teams to work more efficiently. It can quickly pinpoint the root cause of service performance and availability issues across the data center operations infrastructure, including the network, servers, storage and applications. EMC Ionix for IT Ops also supports collaboration with third-party response systems, integrating security events with incident response systems to better streamline advanced security operations.

EMC Ionix Configuration Analytics Manager

EMC Ionix Configuration Analytics Manager (CAM) monitors user-defined key performance indicators, helping to ensure that network and server devices comply with security best-practice policies. Armed with the data CAM provides, your security teams can make more effective decisions about aligning IT resources with business objectives.

Why Choose RSA Solutions for Advanced Security Operations

RSA offers the broadest range of services and technologies necessary to develop a truly advanced security operations function. Ranging from consultative professional services to SIEM, data loss prevention, and threat intelligence, RSA's expertise and proven technology can help your organization build the advanced security operations capabilities you require.

By blending capabilities from EMC and RSA, we are able to deliver comprehensive, integrated solutions that completely address the functional requirements of today's advanced security operations teams, expanding beyond security management to include service desk, server and network configuration, and change management.

Gain a real-time view of security posture across the enterprise, with the ability to see, respond to, and report on security events and attacks quickly and efficiently.



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, SecurID, enVision, FraudAction, RSA Security and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC and Ionix are registered trademarks of EMC Corporation. All other products or services mentioned are trademarks of their respective companies.



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