RSA

The Security Division of EMC

RSA Solution Brief

RSA enVision® Platform

Real-time Actionable Security Information, Streamlined Incident Handling, Effective Security Measures

The job of Security Operations, whether a large organization with a dedicated staff and resources, or one person with multiple responsibilities, is to keep information assets secure by continually monitoring the organization's IT environment, anticipate and respond to immediate threats and long-term vulnerabilities, and provide advice and guidance on security matters to both senior management and business units. To be effective, security operations professionals must draw on tools that day in and day out turn a myriad of real time events into actionable data. They need an efficient closed-loop process for handling incidents and mitigating risk. They also need the visibility necessary to assess and fine-tune the effectiveness of security policies, processes and resources.

The RSA enVision platform collects, analyzes, correlates and alerts on log data from all event sources across the network and IT infrastructure. It also intelligently combines real-time threat, vulnerability, IT asset and environmental data. This enables organizations to respond quickly and thoroughly to high-risk security issues and pinpoint the places where problems are likely to appear. By automating manual processes and increasing productivity, the RSA enVision platform delivers increased security while reducing cost.

With over 1600 production customers world-wide across every industry, including 5 of the Fortune 10 and 40% of top global banks, the RSA enVision platform:

- Provides real-time, actionable security information for quick and accurate threat detection and alerting – by combining event data, asset and vulnerability information, and utilizing intelligent correlation capabilities, *security professionals prioritize and focus on the issues that support the business needs.*
- Improves analyst productivity by streamlining the incident handling process – by providing access to real, empirical data and offering a built-in workflow, from initial identification and prioritization of an incident, to investigation with contextual information, to escalation, resolution, closure and archiving, *security professionals efficiently and effectively accelerate problem resolution.*
- Increases the effectiveness of security measures and resources – by giving security professionals visibility into their enterprise, the status of an incident , the vulnerability and risk of high-priority assets and the use of security resources through comprehensive reporting and easy to use dash-boards, *security organizations can focus staff on high-risk issues and adapt and adjust policies, procedures and investments in order to mitigate risk.*

To be effective, security operations professionals must turn a myriad of real time events into actionable data.

The RSA enVision Platform – What Is It?

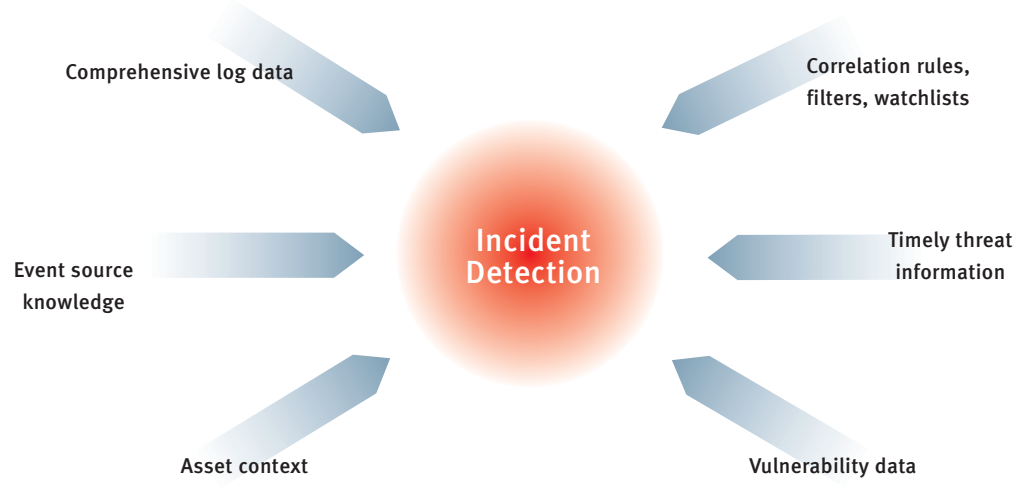
Analysts agree that the RSA enVision® platform is a market-leading solution for security information and event management (SIEM). It gives organizations a single, integrated 3-in-1 log management solution for simplifying compliance, enhancing security operations and risk mitigation and optimizing IT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

Simplify compliance.
Enhance security operations.
Optimize network operations.

Enhancing Security Operations

Security Operations Role	Responsibilities	Data/Tools Needed	RSA enVision Solution
CISO	Interface between the business and Security Operations; set direction; justify budget	Security status "at a glance"; security metrics	Graphical and tabular executive dashboards; extensive out-of-the-box reports
Security Architect	Design & maintain Security Policy and controls; general understanding of state of security and compliance	Metrics to track effectiveness of policies and controls	Extensive reports (security and compliance); out-of-the-box and easy to customize dashboards; historical and trend reports
Security Manager	Oversee Security Operations resources and budgets; incident response oversight	Resource and security metrics, including incident response statistics	Security status and productivity dashboards including: team workload, incident rate, tasks by priority for workload management; and vulnerability dashboards including most vulnerable assets ranked by severity or by business rating
Security Analyst	Monitor consoles, device configuration & vulnerability management, detect incidents, respond to alerts, conduct investigations, manage incident resolution; provide technical advice	Asset & vulnerability status, threat information, real-time and long-term event data, baseline, policy and identity information. Need collaborative incident handling process; tools to focus on high-risk incidents	Baseline, event, asset and vulnerability data to reduce false positives and alert, in real-time, on high security-risk incidents; extensive content-rich correlation rules (e.g. SANS Top 20); automated Watchlists (e.g. Privileged User Monitoring); collaborative closed-loop incident handling process, from incident identification and research through resolution, closing and archiving

Real-time Incident Detection



Real-Time, Actionable Information for Quick and Accurate Threat Detection and Alerting

The RSA enVision platform examines and analyzes events in real-time to detect and alert on high priority incidents. It combines best-of-breed log management capabilities, advanced correlation functions and comprehensive knowledge of threats and vulnerabilities to provide security organizations the ability to efficiently and accurately "find the needle in the haystack."

Event Data Collection – The RSA enVision platform was purpose-built to collect event data from any and every event source, including network, security, host and storage devices as well as applications and databases. With its LogSmart IPDB (Internet Protocol Data Base) architecture, RSA enVision software collects events without agents, allowing for faster deployment and reduced ongoing management. It does not filter, reduce, normalize or alter the raw event information, allowing organizations to access complete data and therefore to identify an incident in real-time, investigate it, anticipate problems and conduct complete forensic analysis for internal or external auditors. Secure, scalable storage and industry-leading compression rates deliver a cost-effective solution.

Vulnerability and Asset Management – The RSA enVision platform gives event data additional context by combining it with data from vulnerability assessment tools and configuration management systems. This allows it to alert administrators when vulnerabilities appear on critical systems and prioritize security alerts based upon the value of the asset being attacked and its vulnerabilities. It also makes a rich set of contextual data available to analysts investigating security incidents so that they can make better decisions about how to respond.

Advanced Correlation Rules & Watchlists – The RSA enVision platform provides a wide set of content-rich correlation rules that define the conditions under which an alert or notification should be automatically triggered. These correlation rules can be easily enhanced with new content, and can be tailored to create environment-specific conditions that will detect risk and eliminate or reduce the window of exposure. With watchlists, organizations can easily create and update lists of mission critical assets, or of accepted (or forbidden) assets so that, for example, core business applications, privileged users, former employees, spammers, known hackers, or bot-net servers can be automatically monitored. The SANS Top 20 Watchlist, for instance, monitors for any exploit related to the SANS Top 20 list.

Timely Threat Information – The RSA enVision platform imports information from IDS/IPS devices commonly used by enterprises. These devices continually scan the network to detect occurring threats such as hackers attacking systems or gathering information from them. It also contains an embedded vulnerability repository derived from the Department of Homeland Security's National Vulnerability Database; it contains detailed descriptions about current vulnerabilities such as an explanation of its potential impact, the type of loss it can cause and an indication of how an exploit may result in a confidentiality breach.

Critical Activity Detection	Example
Critical Administrative Activity	Detect high-risk administrative actions on critical assets, like out-of-policy configuration changes to high- risk assets, or unusual privilege delegation
Suspicious User Activity	Detect unusual authentication or access control issues, like multiple failed logons, or unauthorized system accesses
High Risk Vulnerabilities	Detect new high risk vulnerabilities on critical assets, or likely attacks on vulnerable hosts
Suspicious Network Activity	Detect unusual deviations in network behavior, or network activity that violates policy
Critical System Errors	Detect critical errors on high-priority systems that might result in a system outage

The RSA enVision platform thus performs the automatic correlation of security events with what is known about an IT asset, its priority to the business and its relative vulnerability. In this way, it dramatically reduces false positives and alerts on high-risk events, enabling the security operations team to take immediate action on prioritized incidents.

A large global post-trade processing infrastructure company looking for multiple logging protocols, event aggregation and correlation, real-time alerts, privileged user monitoring and focused threat detection found that enVision helped them "…find the needle in the haystack. [It] points us to the area to look for the needle and sometimes it puts the needle right on top of the haystack."

Security Analyst

Security Manager

Streamlined Incident Handling Process

RSA enVision software provides real-time notification of high-risk security issues that need to be handled by security analysts and specialists. Whether in an e-mail, a console alert, or a blackberry message, a notification begins the incident handling process where the goal is to quickly reach effective resolution and closure.

A closed-loop, collaborative process

Examine all available information & supporting evidence with easy to use UI, broad search capabilities with contextual information including powerful asset and vulnerability lookup

Sort, categorize & prioritize incoming incidents

Analysis

Gather, document and preserve information and analysis of evidence; audit trail of complete investigation

Triage

Forensics

Reports on incident status

Notification

Track & Trace

Trace views to monitor activity by user, IP address, etc.

Close

Escalate and/or Remediate

Accept status change from downstream ticketing system for complete closed-loop process

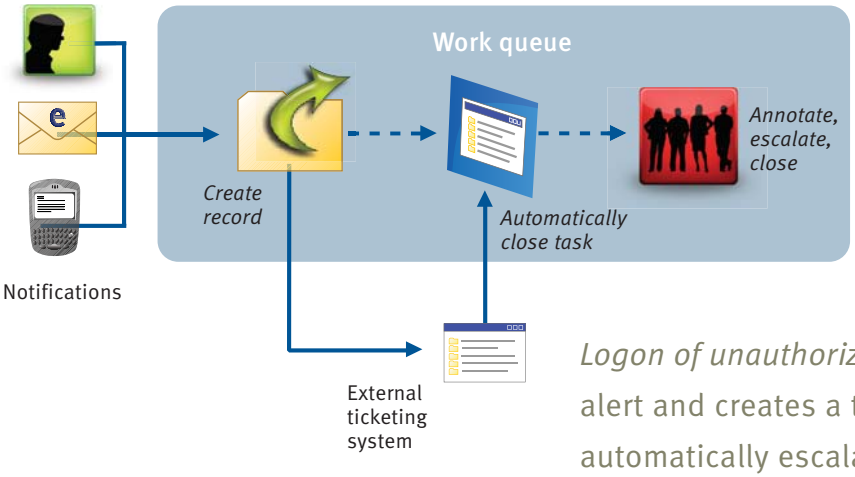
Automatically escalate to downstream systems (e.g. ticketing, configuration management) or to domain expert, and include all relevant annotations and log records

Remediate: Track and document incident resolution/remediation

With an intuitive interface that supports the processes, workflows and procedures required by security operations organizations, the RSA enVision platform provides a closed-loop, collaborative workflow that

- efficiently triages the incident to the appropriate security analyst/specialist;
- enables detailed analysis and forensics with access to comprehensive event, asset and vulnerability information;
- provides track and trace capabilities to monitor activity by user, IP address, etc.,
- offers the ability to escalate incidents within security operations or to downstream systems (e.g. ticketing systems);
- accepts updates from downstream systems and monitors incident resolution through closure, and
- creates incident reports and dashboards.

Security Incident Management Workflow



Logon of unauthorized user triggers an alert and creates a task. The task is automatically escalated to the external ticketing system. IT Operations disables the account and the task is closed via 2-way integration. Security Operations validates the remediation, updates the report. The closed task is saved.

Increased Visibility into the Effectiveness of Threat Detection & Security Measures and Resources

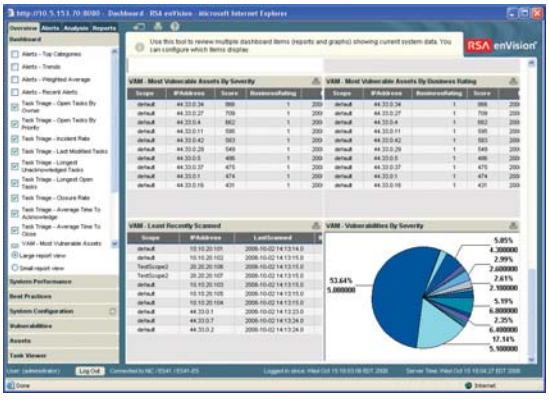
Whether to get a snapshot of the overall state of security of the organization, to understand the vulnerability of key IT assets, or to assess the effectiveness of the security operations team, the security operations team needs quick access to information that will enable timely and accurate communication, decision-making and resource optimization.

The RSA enVision platform provides the complete range of monitoring and measurement information: from high-level graphical dashboards to detailed scheduled or on-demand reporting capabilities that can display essential data graphically or in tabular format.

Vulnerability Management Metrics and Dashboards

Security operations management needs accurate, timely risk and vulnerability information that enable effective communication to the executive team and to the business. The RSA enVision platform presents managers graphical dashboards and detailed reports that include:

- summarized asset risk (vulnerabilities, patches, etc)
- most vulnerable assets by severity
- most vulnerable assets by business rating
- incident trends

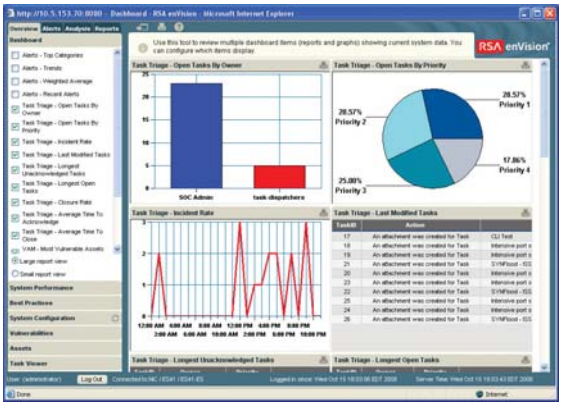


Security Operations Dashboard for Vulnerability Management

Incident Management Metrics and Dashboards

Security operations management also needs easy Incident Management metrics and dashboards. With RSA enVision software, managers can quickly assess the effectiveness of the security organization with pre-defined or customizable dashboards that present incident handling metrics such as:

- team workload including open incidents by owner
- incident rate
- recent activity
- closure rate
- average time to closure
- unacknowledged tasks



Security Operations Dashboard for Incident Management

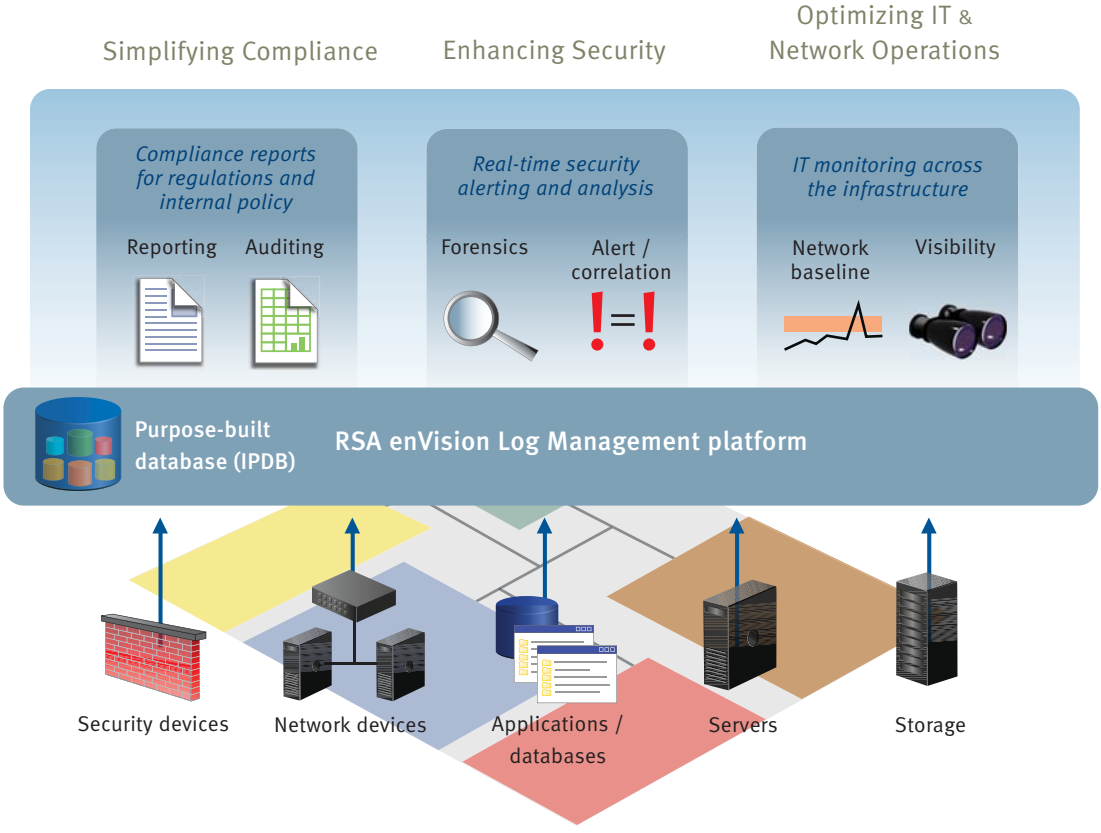
Conclusion

The RSA enVision platform dramatically enhances the effectiveness and efficiency of security operations teams. By providing complete, in-depth data on events, assets, vulnerabilities and business priorities, and offering powerful correlation capabilities, organizations are alleviated from chasing false positives and can focus on the organization's high priority issues. By offering a collaborative, closed-loop incident handling process supported by rich content, comprehensive search function and drill-down forensic capability, organizations accelerate closure rates. By presenting informative, easy-to-use dashboards and reports, security management gets an accurate view of the state of security and can assess the effectiveness and efficiency of its security measures and organization.

An end-to-end SIEM solution

RSA enVision 3-in-1 SIEM Platform

The RSA enVision platform offers an end-to-end SIEM solution that enables the transformation of security operations: it increases analyst productivity, provides security managers timely insight into their operations, enhances integration with enterprise systems – all supported with rich content that evolves with business requirements and emerging threats. Its powerful 3-in-1 platform also dramatically simplifies compliance and provides essential information to IT & network operations teams. All within a single product.



Getting Started

The RSA enVision platform is designed for easy deployment and management. However, many organizations look for guidance and assistance to expedite time-to-value, facilitate the integration with existing systems and processes, establish best practices and to ensure the alignment of technologies with security goals…or simply to complement in-house resources.

With RSA Professional Services you get world-class expertise to guide solution planning, design and deployment. Smart, experienced, skilled and committed to your success, the people of RSA Professional Services can help you quickly achieve the benefits of proven RSA enVision technology while reducing the risks often associated with new technology initiatives.

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.

ENVSO SB 0209

RSA®
The Security Division of EMC

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