RSA Solution Brief

Streamlining Security Operations with RSA® Data Loss Prevention and RSA enVision® Solutions

Who is asking for this?
A Brief on the Security Operations Center user

The job of Security Operations team, whether in a large organization with dedicated staff and resources, or in a small company with one person assuming multiple responsibilities, is to keep information assets secure by continuously monitoring the organization's IT environment, anticipating and responding to immediate threats and long term vulnerabilities and providing 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 the effectiveness of security policies, processes and resources and the controls necessary to fine-tune them.

Drivers for Information Discovery

There is a growing shift in IT from perimeter-focused security measures to information-centric security. Information is the backbone of business and in an uncertain economy it is more important than ever to focus management efforts on securing this information. This is even more apparent when viewed in contrast with traditional perimeter security measures that have become ineffective and increasingly expensive to scale with the universal expansion of information across an enterprise.

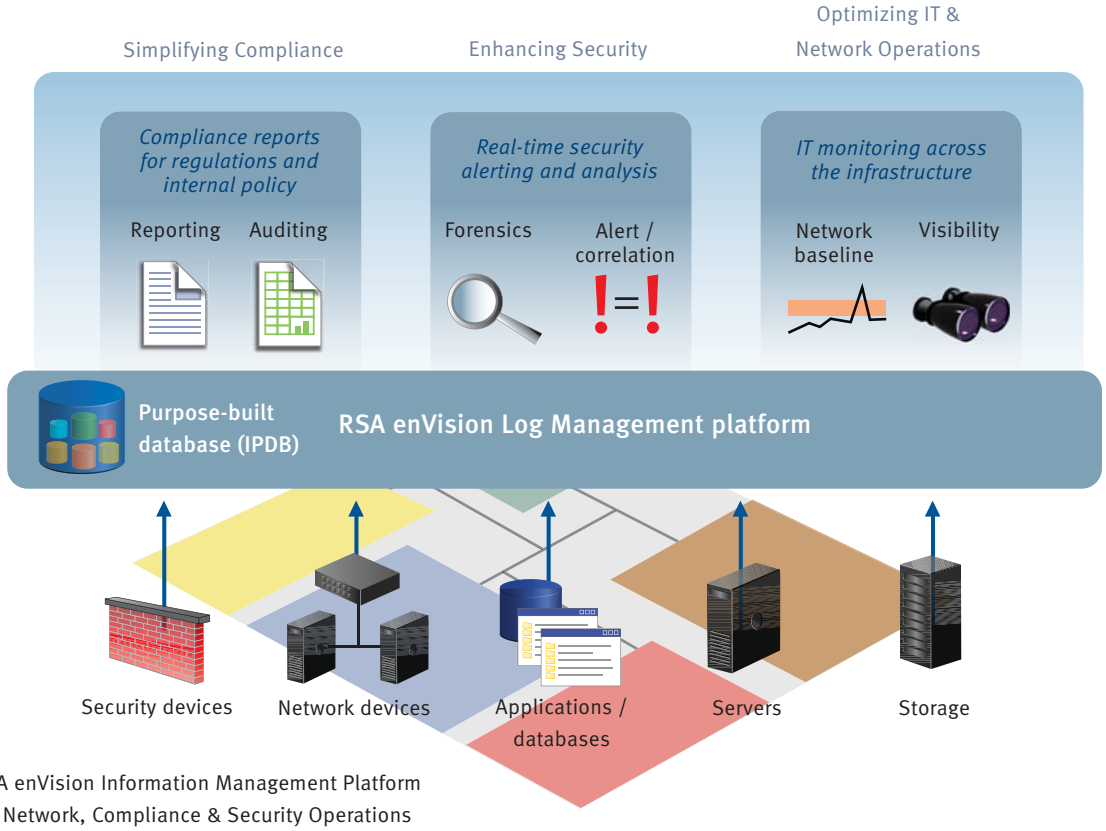
One of the key problems that security operations professionals face is the gap between business operations' use of information technology and corporate security policy. This gap and the resulting organizational barriers often make traditional security measures hard to implement. As a result, security operations professionals are increasingly turning to tools such as Data Loss Prevention (DLP) to identify critical information within the enterprise and Security Information and Events Management (SIEM) solutions to provide much-needed information risk discovery and management.-

What is the RSA enVision platform?

The RSA enVision platform collects, analyzes, correlates and alerts based 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 helps organizations to respond quickly and thoroughly to high-risk security issues and to 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. Utilizing intelligent correlation capabilities, security professionals can 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, escalation, resolution, closure and archiving. Security professionals can 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 dashboards, security organizations can focus staff on high-risk issues and adapt and adjust policies, procedures and investments in order to mitigate risk.



RSA enVision Information Management Platform for Network, Compliance & Security Operations

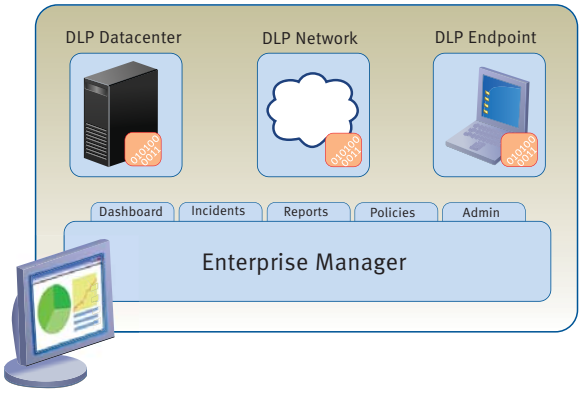
What is RSA Data Loss Prevention?

The RSA Data Loss Prevention (DLP) Suite is an integrated suite of data security products that provides a proactive approach to managing your business risk associated with the loss of sensitive data. Together, the RSA DLP Datacenter, Network and Endpoint modules, which comprise the DLP Suite, create a comprehensive data loss prevention solution that:

- Discovers and protects sensitive data in the data center, on the network and on the end points while leveraging common policies across the infrastructure. DLP helps locate sensitive data no matter where it resides, including file systems, databases, e-mail systems, large SAN/NAS environments, and end points.
- Mitigates risk through identity aware policy based remediation and enforcement. RSA DLP leverages Active Directory Groups on the network and at the end point. Integration with Microsoft Rights Management Service® (RMS) provides group-specific controls and enables protection beyond the company's boundaries.
- Reduces total cost of ownership with industry-leading scalability, incident handling and workflow, and a comprehensive policy library. A dedicated information classification and policy research team provides finely-tuned policies, content types and classification modules, resulting in very high accuracy ratings. The result is less time required to set up and tune policies and faster value delivery from the DLP system. RSA DLP scales across the enterprise and offers great flexibility, including optional temporary agents and grid scanning. The lowest possible TCO is achieved by leveraging existing customer hardware for DLP and requiring fewer hours for set-up and ongoing maintenance.

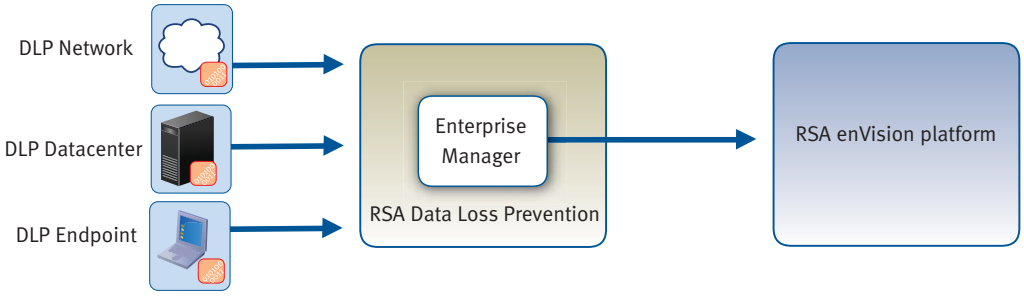
Combined Data Loss Prevention and enVision Deployment Scenario

In order to initially detect and audit sensitive data, the customer first configures policies and content detection modules in RSA DLP. The Enterprise Manager module receives events from the DLP components whenever a policy violation is detected. As events are generated, the Enterprise Manager forwards the relevant event and user information to the enVision platform. The customer uses the enVision platform to collect, correlate, analyze and alert on this information in combination with asset and user information from other sources. The feedback from that analysis is used to fine-tune DLP policies to ensure sensitive data is stored and used appropriately.



RSA Data Loss Prevention Suite

The RSA DLP Suite gives you insight into the risk status and trends of sensitive data in your enterprise – based on policies – regardless of whether the data resides in a data center, on a network or out at the endpoints.



Combined deployment applies the powerful analysis and correlation features of the RSA enVision platform to the content-aware information discovery provided by RSA Data Loss Prevention. The integration brings enVision log parsing and reporting to all DLP events, which are forwarded to enVision via syslog by the DLP Enterprise Manager. Beginning with RSA enVision 4.0 and RSA Data Loss Prevention 7.0, this capability is offered out-of-the-box, with no complex setup required in either product. This feature will be offered to all RSA enVision platform customers via the monthly content update package.

Use Cases

Use Case: Security Incident Impact Classification

A security operations center (SOC) professional has to monitor and respond to many different types of security incidents such as malware attacks, vulnerability exploits and access spoofing. Via an integrated enVision and DLP solution, efficient correlation of security and DLP event logs can help the analyst quickly determine the severity and impact of a potentially urgent incident. By providing insight into the type and sensitivity of information involved in the incident, DLP can help the SOC analyst decide when and how to remediate it and assess what damage has been done.

Use Case: Watchlisting

The SOC user may receive an alert from the enVision platform that indicates suspicious user activity but does not in itself represent a security breach. In this case, the analyst may want to correlate the suspicious activity with all of the other activity by the same user. Using the RSA enVision platform with event input from DLP, the SOC user can quickly gather all of that user's information and find a pattern of actions that, when taken as a whole, could represent a much more severe incident than the original alert. For instance, a user sending a financial spreadsheet to a personal e-mail account may generate an alert, but it may become much more serious if the analyst discovers that same user has also been copying numerous other sensitive documents to a personal thumb drive.

Use Case: Data Movement Forensics

As the SOC analyst uses the event data from DLP to make real-time decisions about security breaches, the forensic analyst uses the same data to strengthen an internal investigation. Incorporating DLP events into the enVision platform allows an analyst to look beyond what data repositories a user had access to. The analyst can now see exactly what types of data the user could access, how sensitive that data was, and what actions the user took or attempted with that information.

Whereas previously the analyst could only determine that a user under investigation had access to a given SharePoint® site, he can now prove that the SharePoint site contained a sensitive customer list that the user then copied to a USB thumb drive and also e-mailed to a competitor – all within the same enVision interface. This level of detailed information gives the SOC user an unparalleled ability to investigate security incidents.

Use Case: Critical Business Information Discovery

Discovery of where sensitive data resides and how it is protected is the first step in securing that data. Through the integration between DLP and the enVision platform, all information about critical security assets and sensitive corporate data can be stored and analyzed in one place. Now, the enVision platform can become the centralized tool for monitoring the vulnerability status of various IT assets and correlating it with the critical business information they contain.

There are numerous benefits to creating this centralized information store, ranging from a simplified report generation process – the result of a single interface – to an improved feedback loop, allowing for precise tuning of existing security measures. A firewall, for instance, may be modified to be more restrictive once the data that it protects is learned to be extremely sensitive. It is the combination of DLP and the enVision platform that makes this type of holistic analysis feasible.

Use Case: Privileged User Reporting

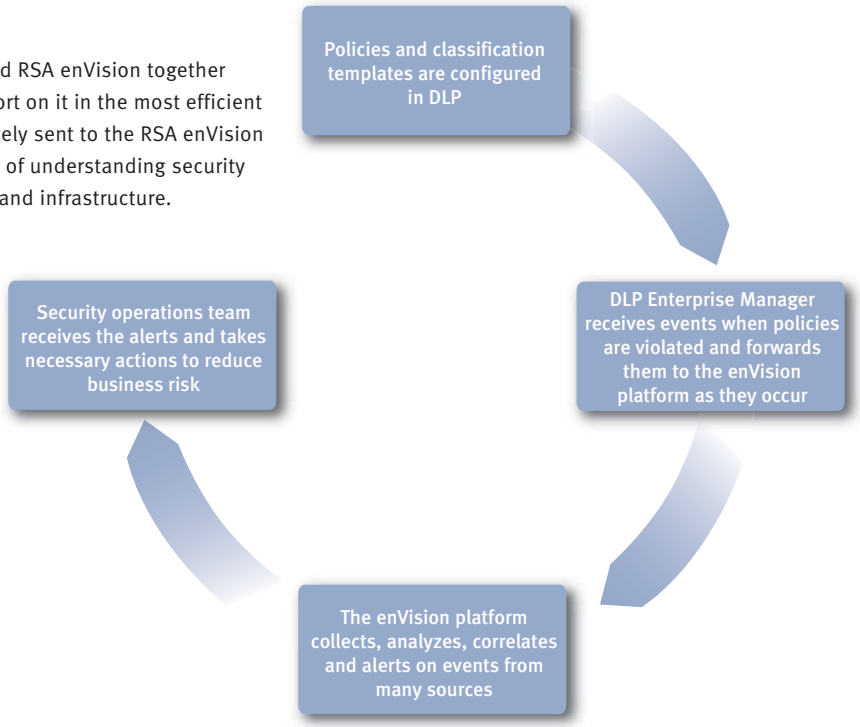
Information and its users change frequently, which requires compliance reporting to be an ongoing pursuit. On its own, the RSA enVision platform offers per-user alerting and reporting regarding what data was accessed. With the addition of DLP events into the enVision platform, the security specialist can add a new layer of reporting that indicates not only what data was accessed but also what the sensitivity or confidentiality of that data was. The analyst can now generate compliance reports to show what types of data privileged users can access, as well as what data is actually being accessed and which movements of that data are affecting compliance.

Feature	Benefit
Out-of-the-box integration of RSA Data Loss Prevention with the enVision event stream	– Enrich SOC environment in real time with business sensitivity metrics.
Report security violations by user, department, information and infrastructure	– Discover sensitive data and all related information to enable action on faulty business processes
Query user or asset incident by information sensitivity	– Prioritize and remediate security incidents by information sensitivity – Execute data movement forensics including user access activity, data movement, asset & information criticality.

Conclusion

The integration of RSA Data Loss Prevention and the RSA enVision platform combines the powerful analysis, correlation, and reporting features of the enVision platform with the comprehensive information discovery capabilities of RSA DLP. Together, RSA DLP & the RSA enVision platform become part of a compelling solution to deliver business-centric information security. By enhancing traditional auditing methods with content-aware information discovery, customers can gain critical insight into where their sensitive data lives and how well it is being protected, allowing them to fine-tune controls and report on access more effectively than ever before.

RSA Data Loss Prevention Suite and RSA enVision together can identify business risk and report on it in the most efficient way possible. DLP events are natively sent to the RSA enVision platform to streamline the process of understanding security risk across information, identities and infrastructure.



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.

DLPENV SB 0409

RSA®
The Security Division of EMC

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