RSA DATA LOSS PREVENTION

Helping organizations address the challenges of securing data at rest, in motion and in use

AT-A-GLANCE

- Comprehensive coverage across threat vectors including email, webmail, HTTP/S web traffic, virtual machines, smartphones, tablets, Microsoft SharePoint, file shares and much more
- Industry-best accuracy in identifying and classifying sensitive data
- Unique workflow processes to involve key business stakeholders in policy and incident management
- Educate employees in real time about corporate policy violations and drastically reduce the risk of sensitive data loss

OVERVIEW

Data loss prevention is about more than just discovering data and preventing information from being lost, stolen or misused. A good strategy is capable of helping organizations solve the complex business problems they face every day, including the need to simplify compliance, streamline business processes and protect intellectual property and brand value.

RSA Data Loss Prevention helps organizations address these challenges for data at rest, data in motion, and data in use:

- RSA DLP Datacenter identifies and enforces policies for sensitive data residing in file shares, databases, storage systems (SAN/NAS), Microsoft SharePoint® sites, other data repositories, and cloud-based repositories, such as Microsoft SharePoint Online.
- RSA DLP Network monitors and enforces policies for sensitive data sent through corporate email, webmail, instant messaging, FTP, social media, blogs, and other web traffic.
- RSA DLP Endpoint identifies and enforces policies for sensitive data stored or in use on laptops, desktops, virtual applications, and virtual desktops.

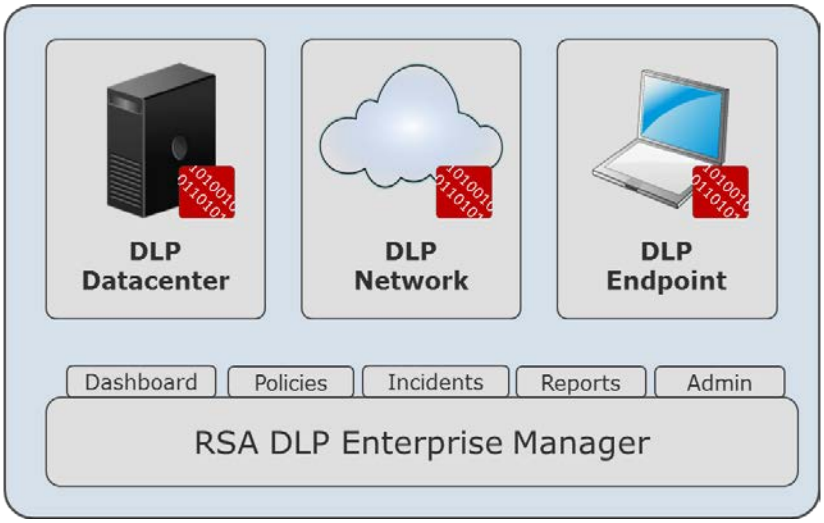
CENTRALIZED MANAGEMENT

Each DLP module is centrally managed by the RSA DLP Enterprise Manager, a single browser-based management console. The RSA DLP Enterprise Manager offers five key functions:

- Dashboard: Monitor incident trends and identify emerging data security risks in a single view.
- Incident Workflow: Search, filter, and drill down into incidents and view all relevant information including owner/sender, recipient, policy violation, and matched content. Numerous remediation and workflow options enable quick resolution of incidents.
- Reporting: Create, view, and save presentation-ready reports that summarize incidents across a number of fields and automatically send to key stakeholders.
- Policy Administration: Choose from over 170 existing out-of-box, expert-built policies or easily create your own. All tools are GUI-based and do not require manual configuration.
- System Administration: Centrally deploy, manage, and monitor the status and progress of all agents and scan groups. Configure nearly everything using GUI controls.

RSA Data Loss Prevention

RSA DLP gives insight into the risk status and trends of sensitive data in your enterprise – based on policies – regardless of whether the data resides in a datacenter, traverses the network or is in use on endpoints.



SIMPLIFY COMPLIANCE

Today, organizations are spending more time addressing compliance requirements – a process that has become burdensome and taxing on it resources. Not only must organizations comply with governmental regulations, they may also be expected to address industry and international regulations depending on the markets and regions in which they operate.

RSA DLP can simplify compliance through the following key features:

- Over 170 out-of-the-box, expert-built polices cover a comprehensive range of international regulations and are applied consistently across DLP Datacenter, DLP Network, and DLP Endpoint. RSA's dedicated Knowledge Engineering team stays abreast of the latest changes in regulations and applies that knowledge to fine-tune polices, saving time and allowing organizations to quickly realize the value of their investment.
- Fast, scalable, and accurate Datacenter and Endpoint discovery scans allow you to quickly map out your organization's risk profile and prioritize activities necessary to meet compliance objectives.
- Quickly remediate files containing regulatory data found by DLP Datacenter with RSA DLP Risk Remediation Manager, a dedicated workflow module to help connect IT with business file owners
- Compliance reporting is made easy through an incident tracking workflow process that logs and monitors policy violations and maintains an audit trail of incidents.

STREAMLINE BUSINESS PROCESSES

Data loss prevention is often associated with many negative connotations such as complex and onerous operations and annoyed end users. This leaves organizations concerned with the impact that a DLP solution might have on their business operations.

RSA DLP is designed to help organizations identify the broken policies or procedures that are often at the root of most data breaches. For example, an HR representative might be sending out sensitive employee information to an external benefits vendor, unaware that this activity is in violation of a regulation or corporate policy. RSA DLP enables organizations to identify broken business processes and monitor ongoing efforts to educate employees on security policies in the following ways:

"We've been very impressed with RSA Data Loss Prevention. it helps educate users on correct e-mail practices while flagging potential risks to our administrators. the dual approach has accelerated our journey to compliance, reducing risk exposure 75% in the first year."

Senior Technical Security Manager
Large Telecommunications Provider

- Employees can be notified of policy violations at the network or the endpoint and be given the option to continue with the action or to cancel it. This empowers employees to make informed decisions without affecting their ability to do their job.
- Each business unit within an organization has different security needs. Through role-based access and granular policy customization, RSA DLP Enterprise Manager makes it easy to customize policy responses by internal functional groups and distribute remediation tasks to business managers or end users.
- A rich set of reports can be automatically generated and e-mailed to executives, administrators, and business managers - making the value of DLP more visible across the organization.

PROTECT INTELLECTUAL PROPERTY AND BRAND VALUE

Trade secrets, which exist everywhere including engineering, marketing, business development, and finance, comprise two-thirds of a company's information value but companies are still spending more time and resources on meeting compliance requirements.

RSA DLP allows organizations to protect intellectual property, maintain brand value, retain talented employees, and increase customer loyalty through several key features:

- RSA DLP offers numerous policy templates thereby helping organizations save time and money by eliminating the need to develop polices from scratch.
- RSA DLP Policy Workflow Manager is a workflow module that enables business managers to efficiently define and protect confidential data such as intellectual property, blueprints, and financial statements.
- RSA DLP Network analyzes all outbound content in a port-agnostic way so that no confidential or embarrassing information is e-mailed out of the company or posted to rumor websites.
- RSA DLP Endpoint offers full protection for mobile employees through fingerprint and described-content policies both on and off the corporate network.

THE RSA INFORMATION SECURITY VISION

RSA's focus is on providing our customers the insight they need protect their most critical information and assets. In addition to solving the standard data loss use cases, RSA is also focused on solving more advanced data loss scenarios, including the threat of data loss from malicious insiders and external attacks, and enabling more proactive information risk management. To address these areas, RSA is taking a layered approach, leveraging agile and integrated technologies. With integrations between RSA DLP, RSA Archer GRC (Governance, Risk and Compliance), and RSA Security Analytics, which combines full packet capture, log collection and analytic capabilities, organizations can better detect and prevent the loss of sensitive data with these evolving threats.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

Published in the USA. 08/13 Solution Overview.

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice. H12223

www.EMC.com/rsa