



The Security Division of EMC

RSA Solution Brief

RSA® Data Loss Prevention Suite

Uncover your risk, establish control.

Executive Summary

RSA Data Loss Prevention (DLP) helps uncover business risk associated with sensitive data loss and dynamically lowers that risk through policy based remediation and enforcement mechanisms based on the business driver. RSA DLP is designed to help mitigate this risk regardless of whether the data is at rest in a datacenter, moving as network traffic, or driven by an end user out at an endpoint. RSA DLP leverages unified policy management across all three products - RSA DLP Datacenter, RSA DLP Network and RSA DLP Endpoint - to simplify deployment and provide consistent ongoing management of all sensitive data in the enterprise.

A Shift in Enterprise Risk Management

The information landscape is changing. Over the last several years, there has been a noticeable shift in attention and investment from securing the network, to securing systems within the network, to securing the data itself. Several factors seem to be driving the paradigm shift in the way businesses protect their sensitive data and lower their risk:

- The threat of data loss from insiders is on the rise
- Companies are storing more sensitive data of all types
- A growing need to share more data internally and with partners
- New markets are emerging for stolen data
- The Regulatory environment is expanding and becoming more complex

Compounding this paradigm shift, traditional security technologies focused on hackers and perimeter protection do not help mitigate internal risks in a meaningful way. A renewed focus is needed to address threats that are being propagated by insiders with malicious intent or who unknowingly put data at risk via broken business and security processes. Over time, risks from sensitive data loss ultimately result in increased financial exposure to the business in terms of breach remediation, compliance costs, customer churn, and brand erosion.

RSA DLP Suite At a Glance:

- Uncover and mitigate risks posed by sensitive data by discovering, monitoring, enforcing, auditing, and reporting on it everywhere it resides.
- Achieve enterprise scalability through distributed architecture so that sensitive data is discovered as quickly as it is created.
- Lower the TCO of the solution through a highly accurate data analysis engine and effective centralized policy management.
- Remediate risk by mapping the severity and nature of the risk to the appropriate workflow and remediation level required.

"The RSA DLP Suite (formerly Tablus) should be on the short lists of organizations that are focused on data in motion and that have large file repositories and lack clarity about their sensitive data. It is also a good choice to address requirements for detection of data at rest in large distributed environments."

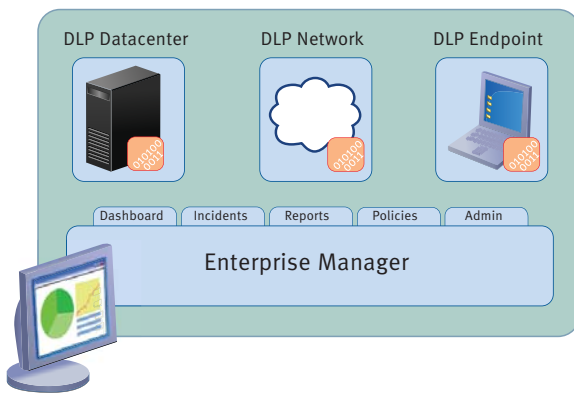
*Gartner Magic Quadrant
for Content Monitoring and Filtering
and Data Loss Prevention
2Q 07, April 13, 2007*

RSA DLP: A Proactive Approach to Developing Data Security Policy

The RSA DLP Suite is an integrated suite of products that provides a proactive approach to managing the business risk associated with enterprise data loss. The RSA DLP Suite is made up of three products: RSA DLP Datacenter, RSA DLP Network, and RSA DLP Endpoint that are sold separately or as a package based on the customer requirements for protecting sensitive data. This approach is predicated on centralized policy management via the Enterprise Manager to help

thwart data loss anywhere sensitive data resides. This novel approach helps businesses itemize and prioritize their risk and then systematically remediate it as per a particular data security policy.

Customers typically start by creating and developing information-centric security policies and use RSA DLP to identify sensitive data at the source through precise discovery and classification techniques. Once the sensitive data is identified, RSA DLP helps establish control by mapping the appropriate enforcement mechanisms to the data based on one or more of the specific security drivers cited in the table. Sophisticated workflow, notification, audit,



RSA DLP 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 end points.

Mapping Today's Data Loss Challenges

The risk associated with sensitive data loss manifests itself in regulatory and non regulatory areas. To mitigate these types of risks organizations must turn to next-generation solutions, such as the RSA DLP Suite, that focus on securing the data itself, whether the data is at rest in a data center, moving as network traffic or driven by an end user out at an end point

BUSINESS RISK	SECURITY DRIVERS	DATA AT RISK (EXAMPLES)	CONSEQUENCES OF DATA BREACH
Regulatory	Maintain compliance	Financial information: specific data tagged for international and U.S. regulations such as Sarbanes Oxley (SOX) and Gramm-Leach-Bliley Act (GLBA)	Fines, loss of consumer confidence, and the cost of breach disclosure
		Personally identifiable information (PII): employee and customer data tagged for regulations such as payment card industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) and California SB 1386	
Non-regulatory	Protect business strategy and operations info.	Pricing, M&A, sales and marketing information	Loss of competitive advantage, customer churn, loss of revenue, damage to brand equity and low employee morale
	Protect intellectual property	Source code, patent, blueprints or engineering documents	



and reporting mechanisms work together to uncover and define broken business processes which are often at the root cause of a data breach. RSA DLP notification and enforcement mechanisms are flexible enough to meet the specific needs of the lines of business, the compliance and legal department, or other stakeholders such as human resources.

RSA DLP customers have a substantially lower risk profile regarding data loss than their counterparts, leading to a better security posture and healthier business prospects. The ability to maintain regulatory compliance and limit intellectual property and strategy and operations data exposure translates into gains in consumer confidence, lower customer turnover, a reduction in fines and penalties, and delivers better overall protection to the business. The RSA DLP Suite is all about uncovering risk and establishing control of your most sensitive information through data security policy creation and enforcement.

Key Advantages of the DLP Suite

Centralized Policy Management

Centralized policy management for sensitive data residing anywhere in a data center, on a network or out at the end points provides consistent discovery, remediation and control depending on the business risk and security drivers.

Enterprise Performance & Scalability

An enterprise-level distributed architecture powers the fastest scanning across end points and data center targets to discover and analyze sensitive data as it is created.

Highest levels of Accuracy

Market-leading accuracy in identifying sensitive data is achieved through the deployment of sophisticated data detection algorithms and policy templates that discover sensitive information based on both content analysis and contextual placement of keywords within a file.

Flexible Incident Workflow, Audit & Reporting

Sophisticated and flexible workflow, notification, audit and reporting mechanisms work together to uncover and define broken business processes that are often at the root cause of a data breach.

RSA® DLP Datacenter

Discover and Remediate Sensitive Data at the Source

The main purpose of a data center is to run and support the applications used by business groups within an organization; as a result a large amount of data is stored in data centers. Some of it is sensitive and this sensitive data is typically scattered across file systems, databases, e-mail systems, content management systems or large SAN/NAS environments. This is often the root cause of data loss because these systems have large volumes of users accessing the data and many of these users do not require all the current access rights in order to do their jobs. This unneeded access poses an internal security risk to the business. RSA DLP Datacenter discovers sensitive data through detailed analysis and provides an overview of the risk to that data in a data center.

For example, users might accidentally or intentionally download a sensitive file from a file system or a database and share it with unauthorized users outside the company. This loss of sensitive data introduces a business risk; RSA DLP Datacenter mitigates this risk at the source by quickly and accurately discovering all the sensitive data resident in the data center. RSA DLP Datacenter can remediate the risk by executing actions such as quarantine and delete on the sensitive data or move it off to a secure system.



RSA DLP Datacenter discovers sensitive data no matter where it resides in the data center.

Data Source	Actions
file shares	quarantine
NAS/SAN	delete
database files	notify
SharePoint sites	move to a secured location
content management systems	



Use Cases

- Discover and prioritize sensitive data, and remediate based on policy
- Report and audit sensitive data in the data center
- Uncover and lower the risk of inappropriate or unwanted data access controls

RSA® DLP Network

Monitor Sensitive Data Leaving Your Network and Enforce Actions

Collaboration, both internally and externally, is critical to the success of any business. Collaboration in the current economy requires flow of information in the form of e-mails, instant messages and other forms of network communication. This flow of data is the life blood of companies and is essential to keep the company nimble and increase productivity. The downside is that often times it opens avenues for sensitive data to leak out to unauthorized entities. Either intentionally or accidentally, a sensitive file may be sent as an attachment with an e-mail or a trade secret may be transmitted via instant messaging.

Furthermore, the sensitive data in these transmissions can be intercepted over the wire, unintentionally leaked to a wrong address or simply be outside of regulatory compliance guidelines. Any of these types of unauthorized transmissions can put the business at risk.

RSA DLP Network helps mitigate these risks by quickly and accurately discovering and analyzing data leaving the network and enforcing data security policies based on the line of business and security drivers.



RSA DLP Network discovers and monitors sensitive data as it moves on your network and enforces actions such as blocking.

Supported Transmissions	Enforce Action
e-mail (SMTP, IMAP, etc.)	allow block
IM/chat	encrypt
HTTP/S	notify
FTP	
generic TCP	

RSA DLP Network can provide data loss prevention in one of two ways. First, it can provide value in a passive monitoring mode to help understand specific risks to the business and help uncover broken business processes. In this mode RSA DLP Network sends notifications and alerts to appropriate parties to help audit and educate users about risky transmissions or business practices. It also provides the ability to operate in an active enforcement mode to provide additional enforcement mechanisms such as native e-mail blocking capabilities or encryption through partners. Regardless of which method fits the company's risk profile, RSA DLP Network reduces the probability of these sensitive transmissions impacting the business and the bottom line.

Use Cases

- Passively monitor sensitive data flowing out of a network
- Actively block and remediate data in motion based on policy
- Deliver alert notifications via workflow and audit or report on data security violations

RSA® DLP Endpoint

Discover and Control Sensitive Data on End Points

End points such as laptops or desktops have revolutionized the way we do business. Most of our day-to-day activities are done at these end points and they are a critical component of a successful business to support a highly mobile and productive workforce. Since most employees spend a majority of their time working at these endpoints it is not hard to imagine that a tremendous amount of sensitive information ultimately ends up residing on laptops and desktops. And statistics show that over 50% of the data lost in today's IT environments is from the end points through transmission off to mobile devices.

Sensitive data might ultimately get to the end point via a file download from a file system or a database, as a remnant of an archived email transmission, or even as manual data entry created at a workstation and downloaded to a hard drive. The only way to ensure that this sensitive data on the endpoint is protected is by quickly and accurately discovering and analyzing where the data resides, monitoring its movement and then enforcing actions such as blocking to prevent unauthorized usage.

"The RSA DLP Suite (Tablus Content Sentinel) helps you gauge gaps in your data security by identifying content at risk on laptops, desktops and servers. You can then take measures to protect this information before it moves or is misused. This alone can help demonstrate to auditors that you're taking proactive security measures. Similarly, protecting confidential data reduces the risk of it getting into the hands of competitors. As such, this solution plays an important role within an overall strategy to enforce compliance with corporate and regulatory policies."

*Infoworld
Quickly discover sensitive content
June 26th, 2007
Mike Heck*

RSA DLP Endpoint has two distinct capabilities that work in conjunction to help lower the risk of sensitive data loss on laptops and desktops. First, based on the centralized policies, RSA DLP Endpoint helps discover and analyze the sensitive data on laptops and desktops. Secondly, RSA DLP Endpoint enhances security by blocking the transmission of sensitive data off to mobile devices such as USB drives or CD/DVDs and by providing additional file control capabilities around printing.

Use Cases

- Discover, monitor and analyze sensitive data at the end points.
- Prevent and control unauthorized movement of data off of corporate workstations and limit other users' actions, based on policy.
- In the event of laptop theft, report on the details of sensitive data as per regulations



RSA DLP Endpoint discovers and monitors sensitive data and enforces actions on endpoints such as laptops and desktops.

Endpoint supports policy action based on network connection status.

Supported End Points

laptops and desktops with Windows OS 2000 SP4 or higher (note: deferred support for Vista)

Enforce Actions:

Allow or Block
print
save/save as
burn to CD/DVD
export through USB



Take the Next Step. Snapshot Your Risk Today

The RSA DLP RiskAdvisor service is a professional services led engagement using the RSA DLP Suite to help organizations transform their data security posture from reactive to proactive. By defining sensitive data and determining where that data resides, this service provides a basis for identifying broken business processes and helps companies formulate a data loss prevention strategy. The service provides a detailed risk report with recommendations on process improvement and better management of regulatory or non-regulatory exposure.

RSA DLP RiskAdvisor Services include:

- Focused inventory of sensitive data
- Scan desktops and laptops
- Scan file shares
- Executive summary report on current risk profile and recommendations



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, 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.

©2007 RSA Security Inc. All Rights Reserved.

RSA, 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 is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

DLPST SB 1207



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

The Security Division of EMC