



The Security Division of EMC

RSA Solution Brief

A Comprehensive Approach to Regulatory Compliance

Securing Regulated Data

The regulatory landscape has shifted to such an extent in recent years that data security standards and disclosure laws now impact virtually every business across every industry. RSA is such a valuable partner for organizations facing industry or government regulations because our data loss prevention offerings are proven to be the most effective solutions for monitoring and protecting regulated data. RSA solutions enable even the largest global organizations to quickly discover their most sensitive information, remediate security issues, and effectively demonstrate and document compliance to auditors and regulators. Whether a retailer facing the Payment card Industry (PCI) Data Security Standard or a healthcare network that needs to comply with HIPAA, RSA has a data loss prevention solution to help you achieve your regulatory compliance goals.

The Most Comprehensive Solution for Regulatory Compliance

The RSA® Data Loss Prevention (DLP) Suite is comprised of three solutions that together can help companies protect their enterprise data—whether inside the Datacenter, traversing the Network, or out at the Endpoints—and demonstrate compliance with government and industry regulations.

RSA DLP Datacenter

Accurately identify all sensitive data at rest across the enterprise.

The only viable solution for discovering all of a company's sensitive data stored on thousands of laptops, desktops and servers in large corporate environments.

RSA DLP Network

Detect sensitive data in motion across your network.

The most precise network monitoring and blocking solution available on the market today makes it easy to screen network data traffic, create an audit trail and remediate incidents of violated policies.

RSA DLP Endpoint

Gain visibility and control over data in use on workstations.

RSA DLP Endpoint enables organizations to monitor data activity on user workstations for irregularities, alert users to at-risk processes and ultimately block the loss of specific, sensitive data before it happens.

Accuracy is Key

Effective monitoring and enforcement of compliance with regulations requires that data loss prevention systems attain the highest levels of accuracy in detecting regulated data. To achieve this goal, RSA employs a unique, modular policy structure that is both powerful and extremely easy to use. There are two key components to this system for achieving accuracy: Policies and Content Blades.

Content Blades

Content Blades encapsulate the logic and rules for detecting specific types of data, such as social security numbers, proper names or corporate financials, to name a few. Content Blades achieve extreme precision by employing a sophisticated set of data analysis capabilities. Designed to be built once and reused many times, Content Blades can easily be leveraged in multiple policies that may require the identification of similar sets of data. For example, a Social Security Number Content Blade could be used in policies for state privacy regulations, GLBA and HIPAA. Changes to Content Blades need only be made once, and are automatically reflected in all policies that use those Blades.

Policies

In addition to specifying which Content Blades to use, Policies also specify the usage and handling rules for each particular type of data. The Policy determines if there is a violation, and if so, how the data or transmission should be handled. Users can define a broad set of usage conditions and handling rules to ensure that the system acts in accordance with their specific data protection needs.

Knowledge Is Power

One key element that sets the RSA DLP suite ahead of all competing solutions when it comes to accuracy and regulatory compliance is the powerful set of One-Click Policies and Expert Content Blades. Over 50 pre-built policies are included in the system, designed around specific regulations and corporate data protection needs. Nearly 100 Expert Content Blades are also pre-built and included to precisely detect specific types of data. Not only does this speed implementation, but because both are pre-built by RSA's knowledge engineers, you get the expertise of a team of professionals who are certified in a range of data security regulations as well as trained in cognitive and library science, ensuring the most accurate data analysis results.

Achieving Compliance with Key Regulations

Payment Card Industry (PCI) Data Security Standard

The PCI Data Security Standard (DSS) is designed to protect the private information of account holders gathered throughout the transaction process. An

industry-based effort led by MasterCard® and Visa®, the PCI regulations impact any organization – retailers, merchants and payment processors – involved in receiving or processing payments.

RSA helps retailers and other organizations that need to protect PCI data and comply with the DSS in several ways:

- One-Click Policy for PCI-DSS is pre-built to identify and handle any located cardholder data.
- PCI-related Expert Content Blades leverage advanced detection capabilities to precisely identify specific data, including:
 - Primary account number (PAN)
 - Contact information
 - Address
 - Date
 - Proper person name
- Rapid data discovery enables organizations to prepare for PCI audits by scanning their entire network, in hours, to identify PCI compliance issues.

SSN Expert Content Blade

Detection Rules

Terms: SSN, social security, etc.
RegEX: formatted, unformatted number
Entities: proper person, etc.

Context Rules

Weights: apply weights/maximum weight to matches
Proximity: matches must occur within a certain number of characters
Required: require certain matches
Threshold: trigger incident if weight exceeds threshold

Usage

File type: all, type, extension, size, encrypted
Protocol: all, e-mail, web, IM/chat, HTTP/S, FTP
Transmission: all, recipient, sender, IP address

Handling

Action: allow, audit, block, quarantine, encrypt
Notification: owner, sender, group

One-Click Policy: CA SB-1386

SSN Blade

CCN Blade

CDL Blade

Policy Rules

Usage: all transactions
Handling: audit

Policy Rules

Content Blades are the definitions that specify the detection and context rules needed to accurately classify sensitive data. Policies are the framework for Content Blades and also define usage and handling rules to ensure data compliance and protection.



Payment Card Industry Data Security Standard (PCI-DSS)	
Industry	Retailers, merchants, payment processors, acquirers
Data Example	Cardholder data and sensitive information, including: primary account number, name, service code and expiration date
Penalty Estimates	\$500,000 per incident for non-compliance; loss of certification, business and consumer confidence; cessation of ability to process transactions — a virtual death penalty for retailers.

RSA DLP in Action At Digital Insight

One of the largest on-demand providers of online banking in the U.S., with more than 1,750 client banks and credit unions, works with RSA to:

- Gain a better understanding of the location of sensitive information.
- Guard against data proliferation, and measure and enforce policies including PCI-DSS, state-level privacy statutes and GLBA.
- Demonstrate their implementation of the highest possible security standards to auditors

State Data Privacy & Notification Laws	
Industry	Any organization with customers in a covered state
Data example	Name, social security number, driver's license number, primary account number and password (varies by state)
Penalty estimates	Cost of notification: approximately \$10-\$35 per customer; brand damage; shareholder and consumer confidence loss

State-Level Data Privacy & Notification Laws

In light of continuing identity theft and data breach incidents across the U.S., many states have enacted data privacy laws that require businesses and organizations to notify individual customers and members in the event that their personally identifiable information (PII) is lost, stolen or inadvertently released.

RSA protects personally identifiable information and helps companies comply with state-level data breach laws with:

- One-Click policies for privacy protection are pre-built to identify and handle PII in compliance with state privacy regulations, including California SB-1386.

- PII-related Expert Content Blades are pre-built to precisely detect:

- Social security numbers (SSN)
- Credit card numbers (CCN)
- Drivers license numbers (all U.S. states)
- Contact information
- Address
- Password

Gramm-Leach-Bliley Act

A far-reaching effort by the federal government to modernize and deregulate the U.S. financial industry, the Gramm-Leach-Bliley Financial Modernization Act (GLBA) also represents the government's most concerted effort to respond to growing public concerns over the privacy of personal information. Specifically, GLBA states that "each financial institution has an affirmative continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information (NPPI)."

RSA helps organizations to protect non-public personal information and to comply with GLBA in several unique ways:

- One-Click policy for GLBA is pre-built to identify and handle any located non-public personal information, including credit card numbers, social security numbers and custom account numbers.



Gramm-Leach Bliley Act	
Industry	Banks, financial Institutions, insurers, securities brokers
Data Example	Names, addresses, phone numbers, bank and credit card account numbers and social security number
Penalty Estimates	Up to \$100,000 per violation

- GLBA-related Expert Content Blades are pre-built to detect specific data including:
 - Social security numbers (SSN)
 - Credit card numbers (CCN)
 - ABA routing numbers
 - Contact information
 - Address
 - Password
- New Content Blades can be created to specify an organizations particular account number format, and more.
- Rapid data discovery enables organizations to prepare for GLBA audits by scanning their entire network, in hours, to create a full data inventory and to identify GLBA compliance issues.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA privacy regulations establish standards for securing protected health information against misuse or disclosure. Protected health information (PHI) is confidential, personal, identifiable information concerning an individual's health and well being that is created or received by a health plan, provider or healthcare clearinghouse, and is transmitted or maintained in any form.

For organizations needing to comply with HIPAA, RSA helps to secure PHI in several ways:

- One-Click policy for HIPAA is pre-built to identify and handle PHI from a variety of angles: account numbers, social security numbers and disease codes
- HIPAA-related Expert Content Blades are pre-built to detect specific data, including:
 - Social security number
 - Contact information
 - Address
 - Healthcare terms for diseases, procedures, etc.
 - HIPAA terms for diagnosis codes and common procedure terms
- New Content Blades can be easily created to define custom patient ID formats, and more.

RSA DLP in Action at Meridian Health

The premier healthcare provider in central New Jersey, Meridian Health offers a broad continuum of care through its four hospitals, providing top-quality care to more than 250,000 people each year. Meridian relies on RSA to:

- Identify and secure PHI subject to the Health Insurance Portability and Accountability Act.
- Monitor for and secure PII, as well as data governed by the PCI standard flowing across the company's network.
- Maintain adherence to strict internal privacy standards.



Health Insurance Portability and Accountability Act (HIPAA)	
Industry	Providers, healthcare clearinghouses, health plans and employers who self-insure
Data Example	Names, addresses, phone numbers, e-mail, date of birth, social security number, medical record number, insurance benefit number.
Penalty Estimates	Failure to comply: up to \$25,000. Wrongful disclosure: up to \$250,000, depending on pretense and intent, plus prison time.

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act was passed to reinforce confidence and protect investors by bringing accountability, transparency and responsibility to the accounting and reporting practices of publicly traded companies. It requires companies to comply with SEC regulations requiring stringent disclosure and proper valuation of intellectual property (IP) and intangible assets.

The type of company confidential information and intellectual property assets regulated by SOX can be the most difficult data to accurately identify and protect. RSA brings extreme precision to the identification of this type of data.

Sarbanes-Oxley (SOX)	
Industry	All publicly traded companies in the U.S.
Data Example	Un-announced financial data, trade secrets
Penalty Estimates	Up to \$5M plus prison time, depending on intent.

RSA helps organizations that need to comply with SOX in several ways:

- One-Click policy for SOX identifies and handles several categories of sensitive corporate information, including company financial information, contracts, source code and more.
- SOX-related Expert Content Blades are pre-built to detect specific data, including:
 - Company financials
 - Contracts
 - Source code
 - Patents
- New Content Blades can be easily created to define any type of custom corporate information you need to protect.

RSA DLP in Action at Microsoft®

To protect its regulated data and sensitive intellectual property, Microsoft® first had to tame their data sprawl. With RSA, Microsoft was able to:

- Use grid-processing capabilities to locate and remediate sensitive information across 30,000 file shares and more than 120,000 SharePoint® servers
 - more than 12 terabytes of data in total.
- Protect sensitive data – and compile an audit trail-in compliance with Sarbanes-Oxley and the PCI Data Security Standards.
- Keep total cost of ownership as low as possible, relying on industry-leading accuracy to eliminate false positives.

RSA Data Loss Prevention Suite

Complete Visibility and Control	
Locate All Sensitive Data	RSA DLP provides a viable way to discover and inventory sensitive data stored across your network – key for ensuring compliance with GLBA and PCI-DSS.
Monitor Data Activity	DLP precisely monitors sensitive data in motion on the network and in use on desktops to understand how it moves and multiplies, and how to best protect it.
Automate Policy Enforcement	With its high precision, RSA DLP helps you confidently automate policies to ensure that they're followed and that breaches are averted.
Assess Risk	DLP leverages reports to help you to benchmark your risk, prioritize proactive mitigation activities and measure your risk score over time.
Maintain Audit Readiness	RSA DLP delivers a fast path to visibility and control with expert policies that quickly help you obtain regulatory compliance – so you'll be ready when the auditors arrive.
Key Capabilities	
Precision Data Detection	RSA DLP ensures high accuracy levels in detection right out of the box.
One-click Policy Library	Pre-built policies specify handling rules to protect all types of confidential information in accordance with key regulations and corporate policies includes: GLBA HIPAA Payment Card Industry (PCI-DSS) Sarbanes-Oxley (SOX) State Data Privacy Regulations (including California SB-1386)
Expert Content Blades	100+ sophisticated, pre-built data definitions encapsulate rules and logic for precisely detecting sensitive data in key regulatory policies, including: Credit card numbers (one, comprehensive) Credit card numbers (multiple, by issuer) Contact information Primary account number Driver's license numbers Healthcare and HIPAA Terms Source code Corporate financials
Automated Policy Enforcement	The RSA DLP solution includes a broad range of policy enforcement capabilities: Allow Audit Block Move to secure location Quarantine Delete Encrypt
Incident Workflow	Easy-to-use incident workflow helps users to review open incidents – meeting wide-ranging and detailed criteria; quickly assess or review specific areas of concern and track remediation efforts.
Pre-Built Reporting	Concise dashboards and pre-built reporting help keep appropriate team members informed.
Selective Encryption of E-mail Transmissions	DLP automatically routes e-mails containing sensitive data to an encryption server to secure messages and attachments on-the-fly in accordance with data protection policies.



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.

©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. Microsoft and SharePoint are registered trademarks of Microsoft Corporation in the U.S. and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

DLPRC SB 1107



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

The Security Division of EMC