

RSA® Data Loss Prevention Datacenter

Complete data loss prevention for sensitive information residing in data centers

At a Glance

- Understand the risk profile by discovering and analyzing sensitive data in file shares, SAN/NAS, database files and other data repositories
- Attain high levels of accuracy and precision in identifying sensitive data
- Manage sensitive data through actions such as quarantine and delete
- Leverage unified policy management to simplify deployment and ongoing management

Overview

The amount of digital data stored at enterprise data centers is almost doubling every year and the major part of it is in the form of unstructured data – files in file shares and repositories. Some is highly sensitive to government regulation in nature, such as customer social security numbers. Some is not subject to regulation but nonetheless sensitive: intellectual property or business confidential information. Traditional methodologies involving the manual identification of sensitive data are very ineffective, time-consuming and expensive given the diverse nature of the data and the amount to be analyzed.

RSA® Data Loss Prevention (DLP) Datacenter, which is a part of the RSA DLP Suite, is a comprehensive data loss prevention solution for information residing in file shares, SAN/NAS, SharePoint® sites and other data repositories. It scans data sources with advanced grid scanning technology, delivering unprecedented efficiencies in uncovering the risk profile of the data center.

Discover and Manage Sensitive Data

RSA DLP Datacenter has a revolutionary architecture that brings the software to the data rather than the data to the software. Contrary to typical discovery technologies, where data from multiple locations is pulled to a central location for analysis, RSA DLP Datacenter scans and analyzes the data close to where it resides. Its unique on-the-spot grid-based architecture and distributed scanning capabilities enable enterprises to scan all the sensitive data stored across file shares, databases, SharePoint sites and other repositories without generating any significant network traffic. This allows organizations to scan thousands of file servers simultaneously and cut scan times from months to hours.



Enterprise Incident Management & Reporting

Once sensitive data is discovered, RSA DLP Datacenter initiates an incident tracking workflow process to log and monitor the data at risk. It maintains an audit trail of incidents and can alert a pre-defined set of stakeholders through e-mail, RSS feeds or IM.

ID	Date	Type	Severity	Status	Assignee	Sender/User/Owner	Protocol/ User Action	Policy	Policy Action
18698	4/26/2007, 4:54 PM	✉	Critical	Open	bsmith	jgraves@acme.com	Email	California SB-1386	Quarantine & Audit
18696	4/26/2007, 2:05 PM	📁	High	Open	bsmith	jgraves	Copy to USB	California SB-1386	Block & Audit
18690	4/25/2007, 5:43 AM	📁	Critical	Open	bsmith	jgraves		California SB-1386	Audit
18504	4/25/2007, 11:32 AM	📁	Medium	Open	bsmith	kpeters@acme.com	Copy	PII Violation	Justify & Audit
18001	4/22/2007, 2:30 AM	📁	Low	Open	bsmith	tomlee@acme.com	Web	Social Security	Block & Audit
17503	4/22/2007, 1:59 AM	📁	High	Open	bsmith	msriniva@acme.com		HIPAA Events	Encrypt & Audit
17448	4/22/2007, 11:05 AM	📁	Low	Open	bsmith	lnavier@acme.com		PII Violation	Audit
17440	4/22/2007, 10:43 AM	✉	Medium	Open	bsmith	mchan@acme.com	Email	HIPAA Events	Audit
17643	4/21/2007, 9:08 AM	📁	Low	Open	bsmith	thapers@acme.com	Copy	GLBA (CC Number)	Notify & Audit
17600	4/21/2007, 8:32 AM	✉	Low	Open	bsmith	lnavier@acme.com	Email	PII Violation	Audit

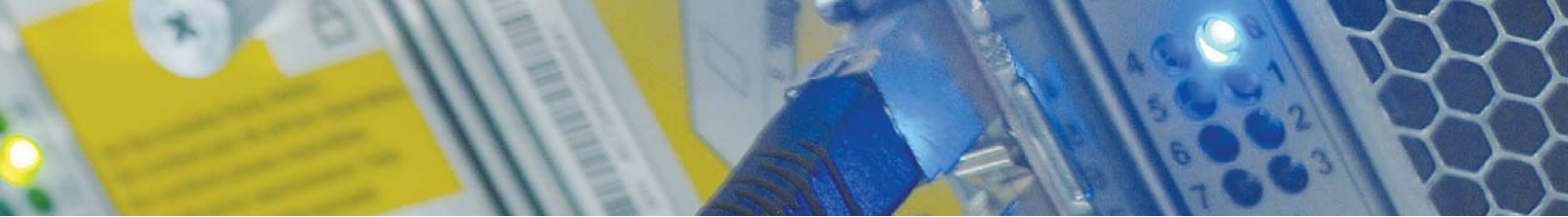
High Levels of Accuracy

Every sensitive file identified as a policy violation needs to be addressed as a security threat and remediated. Conventional solutions without high levels of accuracy identify significant numbers of non-sensitive files as sensitive files (e.g., confusing a random fifteen digit number with a credit card number) resulting in false positives. This inaccurate risk profile information not only increases the total cost of ownership, but also decreases the credibility of the system over time. These false alarms force organizations to spend cycles remediating risks that do not exist, resulting in the waste of valuable security and IT resources.

RSA DLP Datacenter achieves exceptionally high accuracy in identifying sensitive data such as personally identifiable information (PII), payment card industry (PCI) data and confidential business data. High levels of accuracy are achieved through the deployment of sophisticated detection algorithms that follow precise rules on how to identify sensitive data. These precision rules help the algorithms not only to analyze keywords and patterns but also to investigate the contextual placement of the keywords within a file. Organizations can either enable pre-built data detection templates (for data related to PCI, PII, HIPAA, GLBA, SOX) or build their own rules to achieve high levels of accuracy in discovering sensitive data and preventing data loss.

“Grid processing and incremental scanning were essential for Microsoft given the volume of data that we store. Also, RSA DLP Datacenter (formerly Content Sentinel) generates matched files with an accuracy rate consistently at or above 98%.”

*Olav Opedal
Security Program, Microsoft*



Scalability and Centralized Management

Enterprises having thousands of file servers and repositories demand an efficient and scalable methodology not only to discover and analyze sensitive data but also to take actions for security such as delete and quarantine. RSA DLP Datacenter, as part of the RSA Data Loss Prevention Suite, with a unified policy management architecture, allows easy deployment and management regardless of where the data resides. From a centralized location, administrators can configure data detection templates and enforce policies across all data sources in the enterprise, reducing deployment times and the total cost of ownership.

"As I've found in a previous RSA DLP Datacenter (Tablus Content Sentinel) evaluation, the company's content detection is precise. The pre-built Expert Content Blades produced minimal false positives. After registering my custom client lists and source code, RSA Datacenter 3.0 found all instances of sensitive data."

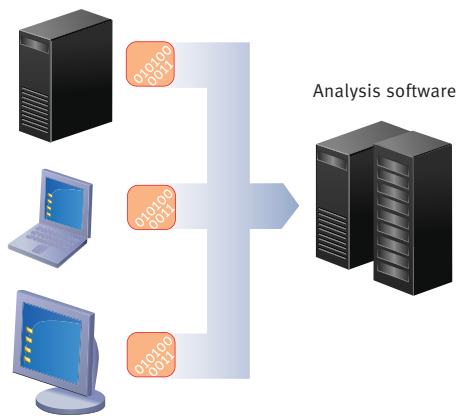
Mike Heck

"Quickly Discover Sensitive Content"

InfoWorld, June 26, 2007

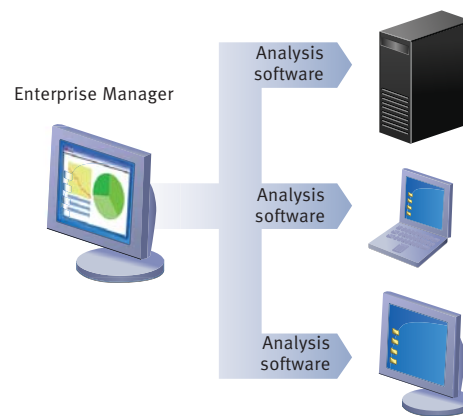
Scan and Analyze Sensitive Data Where it Resides

Discover and analyze sensitive data with exceptionally high efficiencies using revolutionary distributed on-the-spot scanning architecture.



Traditional single-point scanning approach

Move all data to the analysis software.



RSA DLP Datacenter distributed approach

Send the analysis software to the data.



RSA DLP Datacenter Features and Benefits

DESCRIPTION	SUPPORTED SYSTEMS	BENEFITS
Discovery targets	<ul style="list-style-type: none"> - Windows, AIX, HP-UX, Solaris file shares - SharePoint®, Documentum and other repositories 	<ul style="list-style-type: none"> - Support for many enterprise data sources
Regulatory data supported	<ul style="list-style-type: none"> - Payment card industry (PCI) - Personally identifiable information (PII) - Health Insurance Portability and Accountability Act (HIPAA) - Gramm-Leach-Bliley Act (GLBA) - Sarbanes Oxley (SOX) - CA SB 1386 	<ul style="list-style-type: none"> - Help to comply with regulations - Mitigate the risk of legal fines - Preserve customer confidence - Help prevent costs associated with data breaches
Non-regulatory data supported	<ul style="list-style-type: none"> - Intellectual property such as source code, blue prints, etc. - Business strategy and operations data such as pricing, competitive analysis, mergers and acquisitions information 	<ul style="list-style-type: none"> - Help prevent class action lawsuits - Mitigate the risk of losing competitive advantage - Help prevent loss of revenue - Protect brand equity - Protect intellectual property

Comprehensive Data Loss Prevention

The RSA DLP Suite (Network, Datacenter and Endpoint modules) comprises a comprehensive data loss prevention solution that discovers, monitors and protects sensitive data from loss or misuse whether in a data center, on the network or at the end points.

About RSA

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.