

EMC Security for Microsoft Exchange Solution: Data Loss Prevention and Secure Access Management

Applied Technology

Abstract

Securing a Microsoft Exchange e-mail environment presents a myriad of challenges and compliance issues for the enterprise. EMC is ideally positioned to help customers solve these challenges with proven RSA Security capabilities integrated into the solution architecture. This white paper will present the security architecture, capability, test cases, and results.

November 2008

Copyright © 2008 EMC Corporation. All rights reserved.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

Part Number h5850

Table of Contents

Executive summary	4
Introduction	5
Audience	5
About the author	5
Configuration	5
RSA Security.....	5
Exchange 2007/2003.....	6
Dell Mailbox Server	6
EMC CLARiiON	6
VMware.....	6
Architecture.....	7
Test cases and results	9
DLP SMTP e-mail protection	9
DLP Exchange public folders protection.....	10
DLP Datacenter Windows file system protection.....	11
DLP Endpoint file copy to a USB device.....	12
Secure Exchange management access	12
Secure Remote Outlook Access with a MS ISA server	13
Secure VMware SSH access to ESX Server 3.5.....	13
Conclusion	14

Executive summary

For many enterprises the Microsoft Exchange environment is the lifeblood of communications, information sharing, and knowledge exchange. Surveys have shown that a large percentage of employee time is spent answering e-mails, sending invites to meetings, and exchanging documents with both internal and external contacts. Security and compliance for the e-mail environment have proven especially difficult given the variation of threats, compliance objectives, policy requirements, and regulatory concerns.

There are three specific and important aspects of security that need to be considered for the Microsoft Exchange environment— governing your e-mail and information policy, controlling access to e-mail, and verifying that your information governance and compliance policies are being sustained.

This white paper will present EMC's proven approach to security and compliance for Microsoft Exchange. We will cover the following security and compliance topics in this white paper, from the point of view of deployment capabilities that support the above objectives:

- Data loss prevention
- Secure remote e-mail access
- Secure management access
- Information security policy enforcement

The EMC Security for Microsoft Exchange solution addresses these concerns with proven industry-leading RSA Security products. The new RSA® Data Loss Prevention (DLP) Suite discovers sensitive data in SMTP e-mail traffic, in Outlook files, and when saved to file systems. It also enforces policy by sequestering, encrypting, and alerting admins when policy violations occur. The RSA DLP Suite provides unified, seamless data policy orchestration across the Microsoft Exchange environment, allowing customers to discover and monitor sensitive data and apply the appropriate enforcement mechanisms to secure sensitive data across the solution stack. The integrated RSA DLP Enterprise Manager enables organizations to continuously monitor all incoming and outgoing e-mail messaging communications to help ensure that no data transfers take place that violate policy.

In addition, the RSA DLP Suite is engineered into the EMC solution both to regularly scan the environment to detect content that is out of compliance with defined policies and to notify administrators or take action – such as quarantining sensitive data – depending upon the rules established by the organization.

The implementation of RSA SecurID “two-factor” authentication on Microsoft's Internet Security and Acceleration Server 2006 (ISA 2006) for secure single sign-on (SSO) remote access to e-mail and privileged administrator access via Microsoft Terminal Services enforces access control at the mailbox and server level. Enhanced virtualization security restricts privileged user command line access to VMware ESX servers, implementing the supported RSA SecurID PAM module.

The EMC solution offers strong compliance capabilities with the inclusion of RSA enVision® technology, a market-leading log management solution for simplifying compliance, enhancing security operations, and optimizing IT and network operations. The RSA enVision platform provides the capabilities necessary to monitor solution components, correlate events, monitor network components for security incidents and events, manage and protect event logs, detect security events, and alert administrators when policy requires.

With these security capabilities, the EMC Security for Microsoft Exchange solution offers one of the most robust Exchange offerings to manage your corporate information risk, information governance policies, and compliance requirements.

Note: The scope of our white paper does not include anti-virus or spam protection, but our solution is interoperable with leading solutions in this area such as Cisco's IronPort appliance and other SMTP RFC compliant offerings.

Introduction

The purpose of this white paper is to document the configuration, architecture, use cases, and results from tests conducted at EMC labs. The first section of the white paper will describe the test configuration and deployment architecture in detail. Next we will discuss the use cases that formed the test plans. Then we will share our test results in the last section.

Audience

This white paper is intended for IT security professionals, CTOs, Exchange administrators and architects, systems administrators, systems architects, customers, and anyone involved in the design, implementation, and securing of an Exchange solution.

About the author

George L. Wrenn, CISSP, ISSEP, is a Consulting Product Security Manager at EMC and RSA Security. He has over 10 years of experience securing enterprise environments across many industries. In the past he has served as a director of security for a financial services company, a management consultant, researcher, and writer. He has published over 20 articles in major technology publications including *Search CIO*, *Information Security Magazine*, and *Search Financial Security*. He holds a bachelor's degree from Harvard University, attended MIT for five years as a graduate fellow, and was trained in cryptography at MIT as well. He is also an EMC Lean Six Sigma Black Belt.

Configuration

The major components involved in the configuration of this solution include:

- RSA DLP Suite 6.01
- RSA Authentication Manager 7.0
- RSA SecurID hardware authenticators
- RSA Authentication Manager agents for Windows and the PAM module
- RSA enVision ES-560 Appliance
- Microsoft Exchange 2007/2003 server
- VMware ESX Server 3.5 for virtualization
- EMC® CLARiiON® CX3-80 for storage

RSA Security

The RSA DLP Suite 6.01 Enterprise Manager and RSA Authentication Manager 7.0 servers were configured as follows:

- Dell 2950 server (32 GB RAM) with 250 GB internal storage
- Windows Server 2003 R2

The RSA DLP Network Interceptor and Network Coordinator were configured as follows:

- Dell 2950 server (32 GB RAM) with 250 GB internal storage
- VMware ESX Server 3.5
- RSA Authentication Manager PAM module
- RSA enVision ES-560 Appliance

Exchange 2007/2003

Exchange 2007/2003 Enterprise Edition was used in this solution. A detailed breakdown on the configuration of the servers and storage groups follows:

- Mailbox size: 350 MB mailbox limit with 15 days deleted item retention
- Number of Mailbox Servers: Eight, with 2,000 users per server
- Number of ESG per Mailbox Server: Four, with a total of eight LUNs – four for logs and four for DBs
- Database LUN size: 250 GB (500 users * 350 = 175 GB) plus 35% (White Space, DIR)
- Log LUN size: 30 GB, six-day retention
- Total production space: 8 TB for DB, 960 GB for logs
- HUB/CAS server configuration: Three HUB/CAS VMs (two CPU, 12 GB memory) and three domain controllers (two CPU, 8 GB memory), all on two ESX servers in a VMHA configuration

Dell Mailbox Server

A new Dell server was used to host the 16,000 Exchange users:

- Memory: 128 GB
- Server type: Dell PowerEdge R900
- CPUs: Four Quad-Core Intel Xeon 7350s
- HBA: Two QLogic QLE2462s
- Network connections: Eight 1 GB connections

EMC CLARiiON

A CLARiiON CX3-80 was used in the testing. A Cisco MDS 9509 was used as the SAN switch. Details on the CLARiiON configuration are as follows:

- Array type: CX3-80 and release 26
- Exchange production spindles: 64 300 GB 15k spindles for DB, and 22 146 GB 15k for logs
- Guest OS spindles: 10 300 GB 10k
- Replication Manager clone spindles: 48 300 GB 10k drives
- Additional array software used: SnapView™ release 26 (for clone creation)

VMware

VMware Infrastructure 3 simplifies IT environments so that you can leverage your storage, network, and computing resources to control costs and respond quickly to changing business needs. The VMware Infrastructure approach to IT management creates virtual services out of the physical infrastructure, enabling administrators to allocate these virtual resources quickly to the business units that need them most.

VMware Infrastructure 3 is the next generation of industry-leading infrastructure virtualization software. VMware Infrastructure 3 virtualizes servers, storage, and networking, allowing multiple unmodified operating systems and their applications to run independently in virtual machines while sharing physical resources. VMware Infrastructure 3 software components include VMware ESX Server and VMware Virtual Center.

The RSA and Exchange Mailbox VM configuration details are as follows:

- Number of VM clients used to support 16,000 mailboxes: Eight
- Number of ESX Servers to support the eight Mailbox Server VMs: One
- Mailbox ESX Server details: Dell R900, four quad cores, 128 GB memory, two QLogic OLE2462s

- Mailbox Server VM configuration: two cores, 12 GB memory (supports 2,000 users)
- OS Swap space: 20 GB

Architecture

The solution architecture is presented in Figure 1.

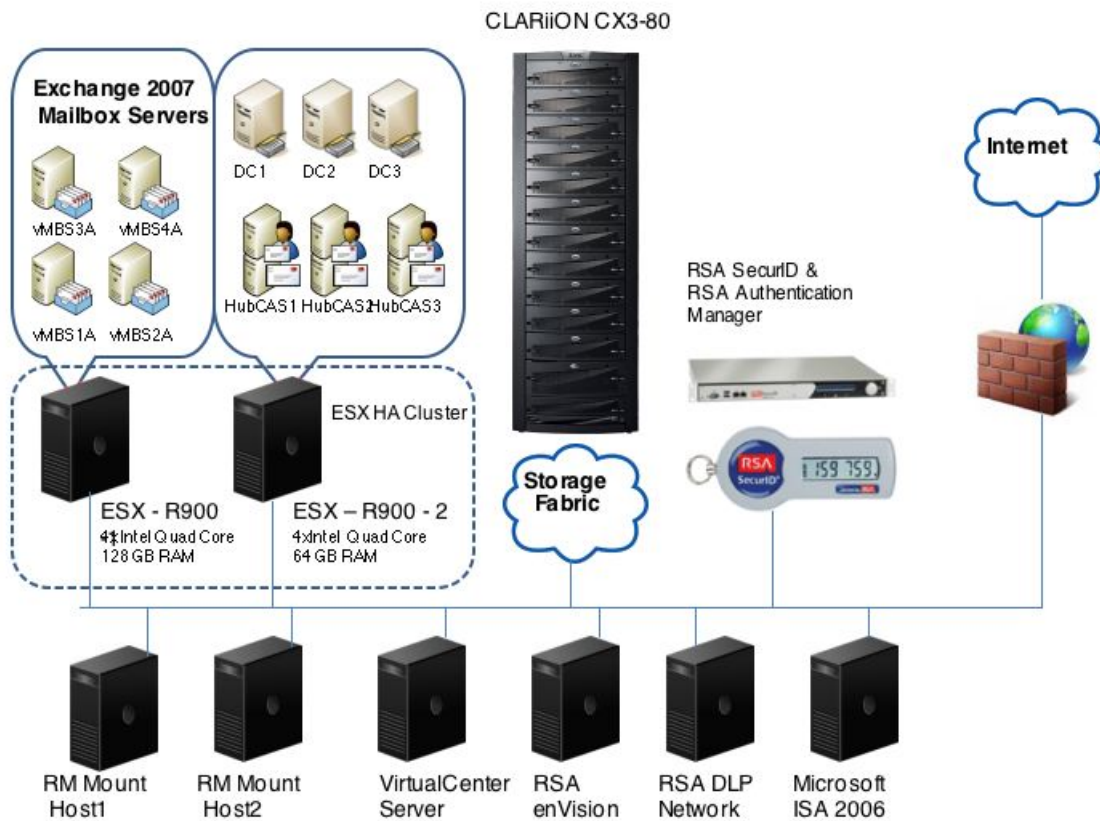


Figure 1. EMC Security for Microsoft Exchange Solution architecture

The RSA DLP components consisted of the following servers and configuration:

- RSA DLP Enterprise Manager hosted on a Dell server running the Windows 2003 R2 server
- RSA DLP Network Interceptor (SMTP gateway) with a proprietary appliance OS
- RSA DLP Network Coordinator (for Interceptor communications to Enterprise Manager) running on a Dell 2950 server as a VM
- RSA DLP Data Center and Endpoint agents installed on Windows 2003 R2 servers and a Windows XP desktop
- RSA DLP Enterprise Coordinator hosted on a Dell server running a Windows 2003 R2 server
- RSA SecurID/Authentication Manager on dedicated hardware
- RSA enVision appliance on dedicated hardware
- RSA Authentication Manager agents installed on Windows 2003 R2
- RSA Authentication Manager PAM module on VMware ESX Server 3.5
- Microsoft ISA 2006 server with embedded RSA SecurID DLL

The primary architectural design element of our e-mail DLP configuration relies on the DLP Network Interceptor acting as a SMTP gateway between the core Exchange HUB CAS and Exchange Edge servers. By intercepting all SMTP outbound traffic, strict policy enforcement is possible. The network interceptor required the presence of a network coordinator to orchestrate policy configuration and data transfer between the interceptor and the DLP Enterprise Manager component.

Similarly, the DLP Datacenter and Endpoint agents required an Enterprise Coordinator server to communicate with the DLP Enterprise Manager for event reporting and policy enforcement.

RSA SecurID agents for Microsoft Windows were installed on the Windows 2003 R2 servers to enforce strong authentication for Terminal Services access to management functions. The RSA SecurID PAM module was installed on VMware ESX Server to force strong authentication for command-line management access.

Remote access to the Outlook Web Access (OWA) for end users is secured with forms-based firewall authentication implemented on a Microsoft ISA 2006 server. Microsoft includes the RSA SecurID DLL on an ISA 2006 server to allow for the option to enable the SecurID authentication method. In our architecture the ISA server acts primarily as a secure http proxy for all remote traffic to Outlook Web Access. All Microsoft servers were configured as members of the same Windows domain.

RSA enVision was configured to log Windows events centrally to enable centralized log management and compliance reporting for the entire environment.

RSA DLP Enterprise Manager was configured with HIPAA and PCI-DSS policies enabled. Figure 2 shows the policy configuration.

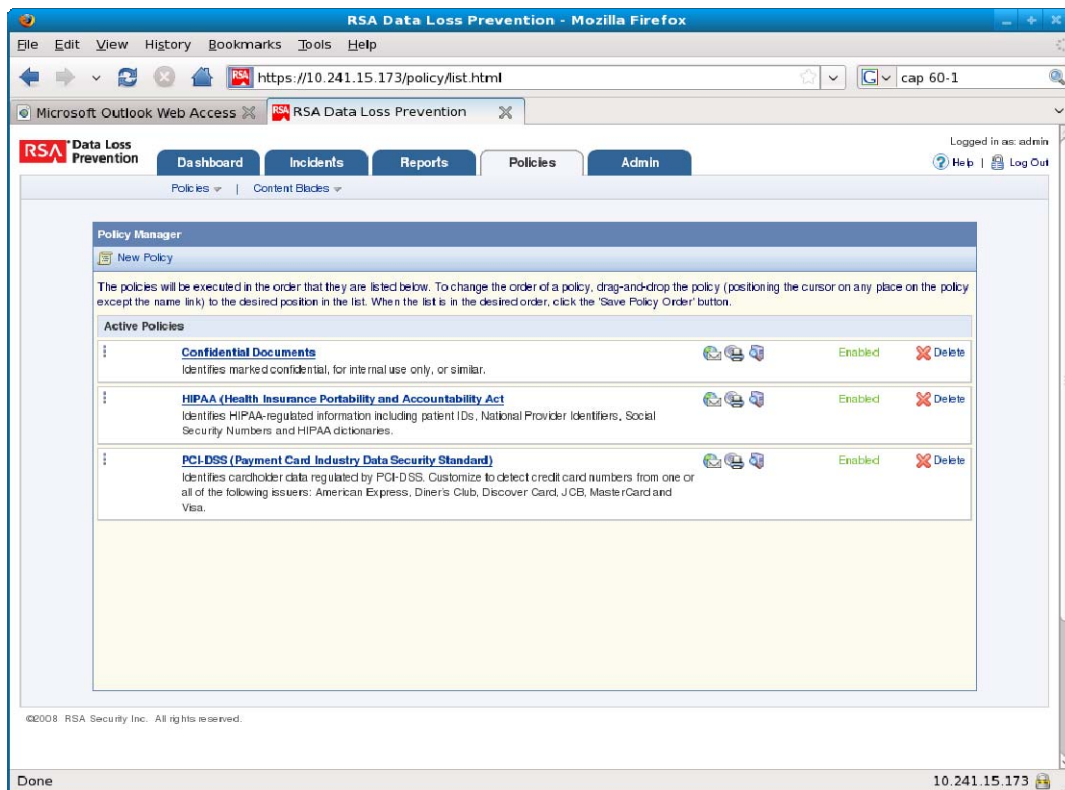


Figure 2. HIPAA and PCI-DSS policies enabled in RSA DLP Enterprise Manager

Test cases and results

DLP SMTP e-mail protection

PCI subcase

The sender attempts to e-mail a message with credit card numbers in the body and a Microsoft Exchange file attachment.

Test results

The DLP Network Interceptor detected a PCI-DSS policy violation and reported the event to the DLP Manager as shown in Figure 3.

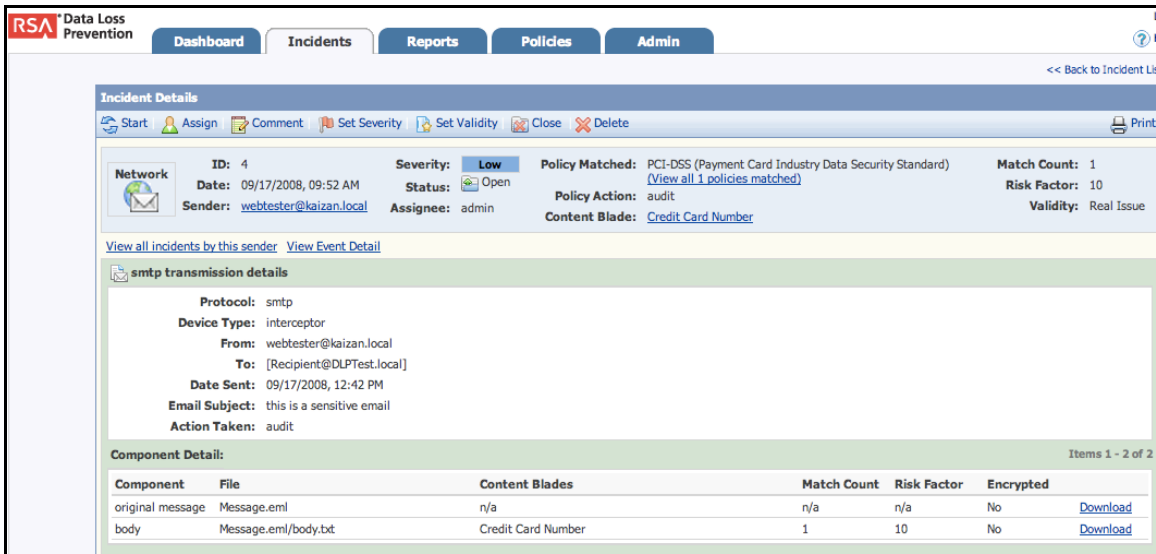


Figure 3. Policy violation detected by DLP Network Interceptor

HIPAA subcase

The sender attempts to e-mail a message with Social Security numbers in the body and a Microsoft Exchange file attachment.

Test results

The DLP Network Interceptor detected the HIPAA policy violation and reported the event to the DLP Manager as shown in Figure 4.

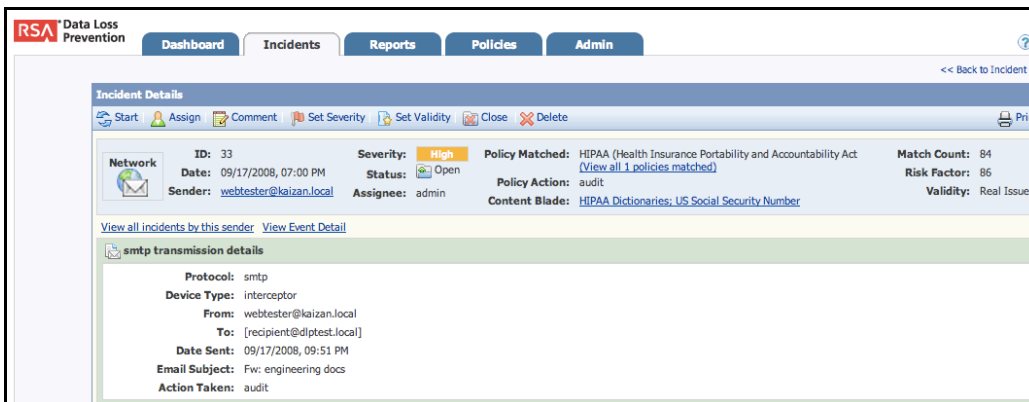


Figure 4. Policy violation detected by DLP Network Interceptor

DLP Exchange public folders protection

PCI subcase

The end user attempts to post a file with credit card numbers in the body to a public folder.

HIPAA subcase

The end user attempts to post a file with Social Security numbers in the body to a public folder.

Test results

The DLP Datacenter agent detects a policy violation and reports the event to the DLP Manager as shown in Figure 5.

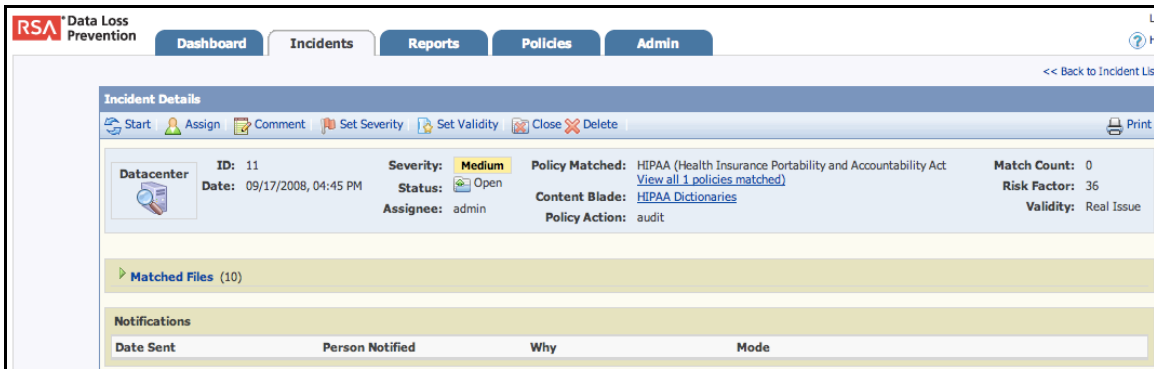


Figure 5. Policy violation detected by the DLP Datacenter agent

DLP Datacenter Windows file system protection

PCI subcase

The administrator copies unencrypted files to the local hard drive on a Windows server with credit card numbers.

HIPAA subcase

The administrator copies unencrypted files to the local hard drive on the Windows server with Social Security numbers.

Test results

The DLP Datacenter agent detects a policy violation and reports the event to the DLP Manager as shown in Figure 6.

The screenshot displays the RSA Data Loss Prevention (DLP) Datacenter interface. The top navigation bar includes 'Dashboard', 'Incidents', 'Reports', 'Policies', and 'Admin'. The 'Incident Details' section shows the following information:

- Incident ID:** 43
- Date:** 09/22/2008, 04:17 PM
- Severity:** Low
- Status:** Open
- Policy Matched:** PCI-DSS (Payment Card Industry Data Security Standard)
- Match Count:** 6
- Risk Factor:** 10
- Assignee:** admin
- Content Blade:** Credit Card Number
- Policy Action:** audit
- Validity:** Real Issue

Below the incident details, a section titled 'Matched Files (6)' shows a table of files that triggered the incident. The table has the following columns: Event ID, Filename (path), File Owner, Manual Action, Content Blade, Severity, Risk Factor, Last Modified, First Found, Last Seen, and Copies. The table lists six files, all with a severity of Low and a risk factor of 10.

Event ID	Filename (path)	File Owner	Manual Action	Content Blade	Severity	Risk Factor	Last Modified	First Found	Last Seen	Copies
1212	\\192.168.165.180\C\$\Documents and Settings\dbadmin.IIM\Desktop\COPY (5) of tax info.txt	BUILTIN\Administrators		Credit Card Number	Low	10	09/22/2008, 03:17 PM	09/22/2008, 04:07 PM	09/22/2008, 04:07 PM	Find Copies
1213	\\192.168.165.180\C\$\Documents and Settings\dbadmin.IIM\Desktop\COPY (6) of tax info.txt	BUILTIN\Administrators		Credit Card Number	Low	10	09/22/2008, 03:17 PM	09/22/2008, 04:07 PM	09/22/2008, 04:07 PM	Find Copies
1214	\\192.168.165.180\C\$\Documents and Settings\dbadmin.IIM\Desktop\credit.txt	BUILTIN\Administrators		Credit Card Number	Low	10	09/22/2008, 03:17 PM	09/22/2008, 04:07 PM	09/22/2008, 04:07 PM	Find Copies
1215	\\192.168.165.180\C\$\Documents and Settings\dbadmin.IIM\Desktop\credit card number.txt	BUILTIN\Administrators		Credit Card Number	Low	10	09/22/2008, 03:17 PM	09/22/2008, 04:07 PM	09/22/2008, 04:07 PM	Find Copies
1216	\\192.168.165.180\C\$\Documents and Settings\dbadmin.IIM\Desktop\MyInfo.xls	BUILTIN\Administrators		Credit Card Number	Low	10	09/22/2008, 03:17 PM	09/22/2008, 04:07 PM	09/22/2008, 04:07 PM	Find Copies

Figure 6. Policy violation detected by the DLP Datacenter agent

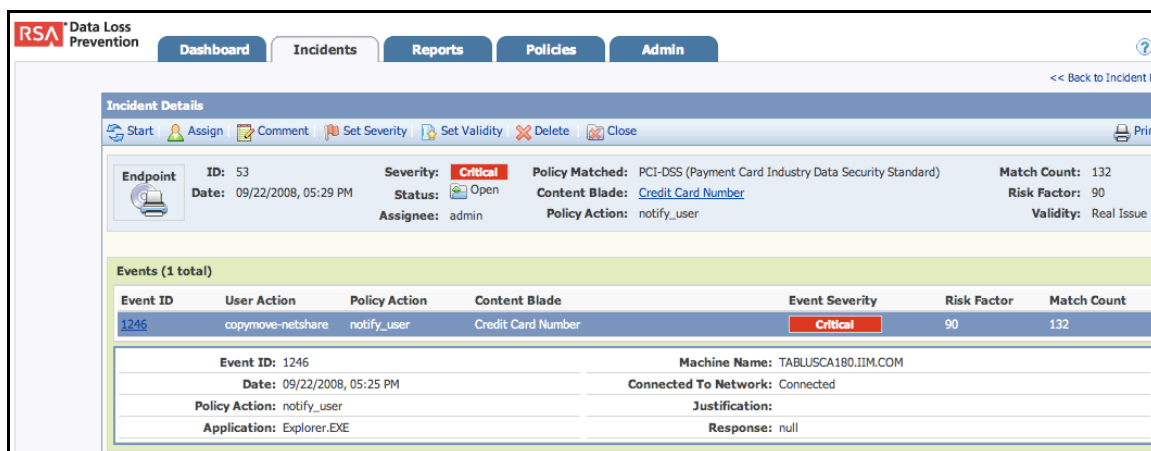
DLP Endpoint file copy to a USB device

PCI subcase

A company employee attempts to copy unencrypted files from the local hard drive on a Windows workstation with credit card numbers to a portable USB storage device.

Test results

The DLP Endpoint agent detects a policy violation and reports the event to the DLP Manager as shown in Figure 7.



The screenshot displays the RSA Data Loss Prevention (DLP) Manager interface. The top navigation bar includes 'Dashboard', 'Incidents', 'Reports', 'Policies', and 'Admin'. The 'Incident Details' section shows the following information:

- Endpoint ID:** 53
- Date:** 09/22/2008, 05:29 PM
- Severity:** Critical
- Status:** Open
- Assignee:** admin
- Policy Matched:** PCI-DSS (Payment Card Industry Data Security Standard)
- Content Blade:** Credit Card Number
- Policy Action:** notify_user
- Match Count:** 132
- Risk Factor:** 90
- Validity:** Real Issue

Below the incident details, there is a table for 'Events (1 total)':

Event ID	User Action	Policy Action	Content Blade	Event Severity	Risk Factor	Match Count
1246	copymove-netshare	notify_user	Credit Card Number	Critical	90	132

Additional details for Event ID 1246 are shown below the table:

- Event ID:** 1246
- Date:** 09/22/2008, 05:25 PM
- Policy Action:** notify_user
- Application:** Explorer.EXE
- Machine Name:** TABLUSCA180.IIM.COM
- Connected To Network:** Connected
- Justification:**
- Response:** null

Figure 7. A policy violation is reported to the DLP Manager

Secure Exchange management access

Terminal server subcase

An administrator attempts to authenticate to a terminal server to access the Exchange management console. The system responds with an authentication prompt. The administrator enters a username, PIN, and token code. Access is granted with the correct code. Figure 8 depicts the login prompt for SecurID for Microsoft Windows.



Figure 8. SecurID login

Secure Remote Outlook Access with a MS ISA server

SSO subcase

A user attempts to access Outlook Web Access via a web browser with SecurID.

System response

The ISA Server intercepts the request and prompts the user for a SecurID PIN and token code.

The user enters the code and is granted access to the mailbox. Figure 9 depicts the form-based method login prompt from ISA Server 2006.



Figure 9. Login prompt

Secure VMware SSH access to ESX Server 3.5

SSH subcase

A user attempts to access ESX Server via SSH to authenticate with SecurID.

System response

ESX Server, using the RSA PAM module, intercepts the request and prompts the user for a SecurID PIN and token code.

The user enters the code and is granted access to ESX Server as depicted in Figure 10. The `Uname -a` output displays the VMware ELVMnix version.

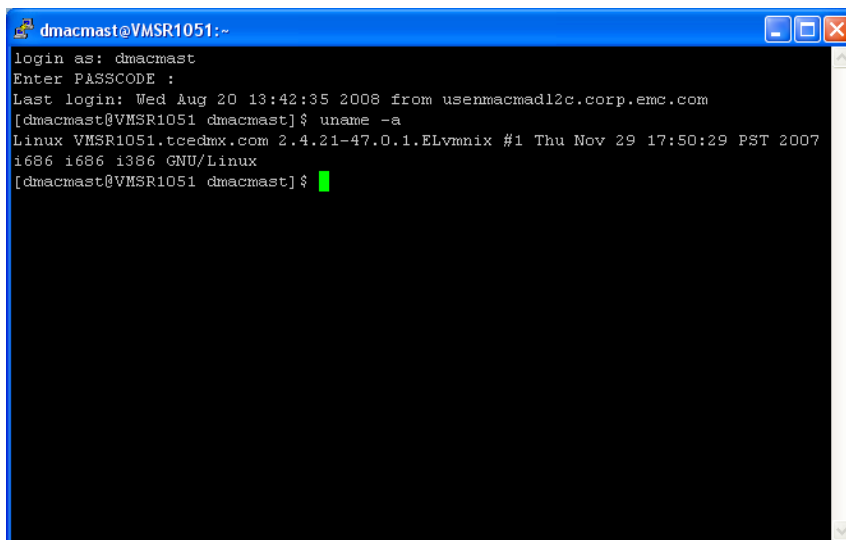


Figure 10. Uname – a output

Conclusion

The EMC Security for Microsoft Exchange solution provides comprehensive data loss prevention that enables enterprise-wide data security policy enforcement for Microsoft Exchange messaging environments. The RSA DLP Network inspects all outgoing SMTP traffic for potential security policy and regulatory violations, stopping data leaks before they can succeed. Integrated DLP Datacenter agents on all domain servers scan files to discover potential policy violations on e-mail “data at rest.” Lastly, RSA DLP Endpoint agents on enterprise PCs protect sensitive information from leaking to USB drives and other media, report policy violations as they happen, and protect data with endpoint policy enforcement.

Built-in RSA SecurID and RSA Authentication Manager strong two-factor authentication protects privileged user access to VMware ESX Server, Microsoft Exchange, and Microsoft Windows environments, ensuring all actions taken by administrators are strongly authenticated and tracked. The option to perform secure remote management of the Exchange environment is critical to meet today’s high availability goals set for e-mail systems. By leveraging proven RSA SecurID technology organizations can safely allow remote management access via Microsoft Terminal Services without compromising security.

Highly scalable, single sign-on (SSO), and secure remote user access to Microsoft Outlook Web Access (OWA) services are now easier to implement with the advent of Microsoft Internet Security and Acceleration Server 2006. The ISA 2006 server offers built-in RSA SecurID capability for form-based SSO access to OWA, enabling organizations to meet remote user access requirements without sacrificing security.

The EMC Security for Microsoft Exchange proven solution leverages best-of-breed RSA Security technology to secure messaging environments and meet policy compliance objectives.