Q & A

Cisco IronPort Email Data Loss Prevention

Data security and data loss prevention (DLP) are serious issues for companies, as the number of incidents – and the cost to those experiencing them – continues to increase. The RSA Email DLP feature for Cisco IronPort email security appliances provides accurate and easy-to-use content-level filtering to detect sensitive data before it leaves the organization. With more than 100 predefined DLP policies, numerous methods to handle DLP violations, and reporting and auditing capabilities, RSA Email DLP is a complete data loss prevention solution for email.

GENERAL INFORMATION ON DATA LOSS PREVENTION FOR EMAIL

What is data loss prevention (DLP) for email?

Data loss prevention for email is content-level scanning of email messages and attachments to detect inappropriate transport of sensitive information. Examples of sensitive content are personal identifiers (e.g., credit card or Social Security numbers) or corporate intellectual property (e.g., internal or confidential documents).

Why is DLP for email important now?

With more and more sensitive information being transported electronically, there is greater potential for inadvertent (or malicious) disclosure of private information. Governments are seeking to contain this risk by imposing regulations on the handling of sensitive personal information. One of the methods of containment is proactive detection of sensitive content before it leaves an organization's boundaries.

Is my company required to use DLP for email?

The healthcare and financial services industries have the largest number of regulations around data loss. However, as a majority of U.S. states have enacted personal identity breach laws (that require public notification if sensitive personal information is leaked), nearly all companies can reduce their risk by applying DLP best practices.

RSA EMAIL DLP LICENSE FOR CISCO IRONPORT EMAIL SECURITY APPLIANCES

What is the RSA Email DLP?

Cisco has partnered with RSA, a leading DLP solution provider, to provide integrated DLP technology on Cisco IronPort email security appliances. The RSA Email DLP license is a software feature for these appliances.

What are the benefits of the RSA Email DLP license?

Benefits of RSA Email DLP include:

- Accurate data loss detection with low false positives
- Robust DLP capability integrated directly into Cisco IronPort email security appliances
- Simple implementation with many predefined policies

What elements of a DLP solution are provided by Cisco IronPort email security appliances with RSA Email DLP?

RSA Email DLP is a complete solution for email data loss prevention. All DLP solution elements, such as policy creation, incident handling, quarantine, encryption and other remediation actions are included.

Do I need to understand compliance laws to implement this solution?

The most widely used DLP policies (e.g., HIPAA, PCI, SOX, GLB) are predefined. They need little to no additional configuration and do not require in-depth regulatory knowledge.

Can I create my own DLP policies?

Yes. Customized DLP policies can be created if the existing predefined DLP policy templates are not sufficient.

What type of reporting and tracking features are available?

On the Cisco email security appliances, DLP reporting ranges from high-level incident trending over time to granular information, including a per-message audit capability that details the matches found.

Does the RSA Email DLP feature support data loss prevention requirements for countries other than the United States?

Yes. In addition to U.S.-specific requirements, RSA Email DLP helps detect the following non-U.S. personal identification numbers:

- Australia (Bank, Business and Company, Medicare Card, and Tax File)
- Canada (Drivers License, Social Insurance)
- European Union (Debit Card)
- France (BIC, Drivers License, IBAN, National Identification, and VAT)
- Germany (BIC, Drivers License, IBAN, National Identification, and Passport)
- Italy (Drivers License, IBAN, and National Identification)
- Netherlands (Drivers License, IBAN, National Identification, and Passport)
- New Zealand (Ministry of Health)
- Spain (National Identification, Passport and Social Security)
- Sweden (IBAN, National Identification, and Passport)
- United Kingdom (BIC, Drivers License, IBAN, National Health Services, National Insurance, Passport, Tax, and VAT)

How are message encryption requirements addressed?

If a sensitive message requires encryption, the message can be automatically encrypted using the Cisco IronPort Email Encryption feature – an agentless encryption mechanism that does not require PKI certificates, key management, or any recipient training. Like the RSA Email DLP feature, this is a software license available on Cisco IronPort email security appliances.

How much does the RSA Email DLP license cost?

RSA Email DLP is a per-user license. The exact cost is dependent upon the deployment specifications selected by the customer.

Can I evaluate RSA Email DLP before I purchase?

Yes. Cisco offers a free evaluation program for Cisco IronPort email security appliances and associated features.

SUMMARY

Cisco IronPort Email Data Loss Prevention delivers high-performance, comprehensive data loss prevention for data in motion – helping organizations both large and small prevent leaks, enforce compliance, and protect their brand and reputation.

TRY BEFORE YOU BUY

Through a global salesforce and reseller network, Cisco offers a free "Try Before You Buy" program for Cisco IronPort email security appliances. For additional information, please contact your local Cisco sales representative or visit: www.ironport.com/try.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at **www.cisco.com/go/offices**.

P/N 435-0258-1 6/09