FAQ: Cisco DLP: Email, Network and Beyond

Cisco enables a world of many clouds—private, public, and hybrid. Our broad cloud security portfolio includes email security, email encryption, and web security solutions, available through 17 global data center locations. We provide a compelling and assured cloud experience, with applications and services delivered anywhere, anytime, and on any device.

Traditional security "borders" do not apply in the cloud. Enterprises need effective data security solutions that help prevent leakage of intellectual property and other confidential data via email and the web; that meet security-related compliance demands of regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and other worldwide privacy regulations; and that enforce acceptable use policies for governance.

To help customers meet these challenges, Cisco is working with partners like RSA to form a leading data loss prevention (DLP) ecosystem that establishes a common classification and policy management platform across the enterprise for customers.

Q. How are Cisco and RSA specifically collaborating on DLP?

A. In 2009, Cisco integrated RSA DLP technology into its email security solutions to provide customers with comprehensive global regulatory compliance coverage; best-in-class accuracy for identifying sensitive, data-comprehensive remediation options including universal, message-based encryption; and ease of deployment and management.

The ongoing collaboration between Cisco and RSA has resulted in development of a powerful but simple approach to DLP: the Cisco IronPort® RSA Email DLP solution. Organizations can now secure sensitive data with a holistic, systems-based approach that builds information security into the infrastructure.

Q. What benefits does the Cisco IronPort RSA Email DLP solution provide?

A. With Cisco IronPort RSA Email DLP, customers can easily extend DLP enforcement from Cisco IronPort Email Security solutions with RSA's DLP Suite, enabling a complete end-to-end DLP solution with a common information classification and policy framework that protects data in motion, at rest, and in use.

Integration between Cisco IronPort Email Security solutions and RSA DLP Enterprise Manager provides customers with easy expansion of DLP to the web, data centers, and endpoints; enhanced diversity of predefined policies and additional content analysis techniques, including fingerprinting capabilities; and reduced hardware costs, with the ability to use existing Cisco IronPort Email Security solutions.

Q. How does the solution simplify DLP management for organizations?

A. Many DLP point solutions require multiple management consoles for policies and remediation. Cisco IronPort RSA Email DLP offers centralized policy management: A single universal policy can be applied across the RSA infrastructure and Cisco IronPort Email Security solutions. Comprehensive visibility into the risk of sensitive data loss across the enterprise with all incident investigation, remediation, and reporting is accomplished through a single console.

Q. In what other ways does Cisco IronPort RSA Email DLP differ from competing solutions?

A. First and foremost: accuracy. The solution provides the best accuracy in identifying sensitive data. The RSA content classification engine conducts sophisticated analysis on keywords, phrases, patterns, and many other parameters to achieve industry-best accuracy in detecting sensitive data.

Other features include:

- An extensive policy library. More than 100 expert policies that address worldwide industry and regional regulations are available “out of the box.”
- Expandability. Customers can easily extend DLP to their data centers, endpoints, and web infrastructures.
- Comprehensive remediation and management, including severity-based quarantine and message-based encryption options. The Cisco IronPort RSA Email DLP solution also offers “a single pane of glass” for managing both outbound control (DLP policies, violations, and remediation) and inbound security (antispam, antivirus, and targeted attack prevention).

Q. How can I learn more?

A. For more information about the Cisco IronPort RSA Email DLP solution and Cisco’s Cloud Email Security Portfolio, go to: http://www.cisco.com/en/US/prod/vpndevc/ps10128/ps10154/dlp_overview.html

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.**

Printed in USA C67-703227-00 03/12