



Securing Healthcare Organizations with Cisco IronPort Data Loss Prevention

Protecting sensitive data and complying with the Health Insurance Portability and Accountability Act (HIPAA) are of critical importance to healthcare professionals. Cisco® IronPort Email Security Appliances counteract incoming threats, such as spam and malware, which could expose sensitive data causing a security breach. Cisco IronPort® products also provide outbound control, enforced by email data loss prevention (DLP), to help ensure that patient health information (PHI) does not leave the network unprotected. Cisco offers built-in encryption as a remediation option for secure message delivery and maintaining compliance with regulations. These benefits also mean cost savings that include avoiding fines for compliance breaches and safeguarding the email infrastructure with a single, integrated solution.

Protect Patient Information and Medical Records

As electronic means of communication gain ground with healthcare providers, they provide many new ways for data to leave an organization: USB backups, bulk data transfers onto another machine (FTP), lost or stolen laptops and hard drives, misplaced mobile devices, and printouts. However, email is the foremost collaboration tool, making it a fertile medium for data loss and the most common vector for malicious activity. Stolen PHI can be used to blackmail high-profile individuals and celebrities or to steal medical identities and commit insurance fraud. Organizations that are seriously considering a well-reasoned strategy for mitigating the effects of data loss within the enterprise should first understand and protect the data leaving the network via email.

Email is also the most common vector for spam or phishing attacks and the first step in the delivery of malicious software such as keystroke loggers, Trojans, or viruses. However, not all data leaves through malware. Malicious intent for personal gain, or an inadvertent mistake, may also result in data loss. Technological safeguards must take into account all of these situations, which can mean a major deployment and rollout challenge for any healthcare IT professional.

How Cisco IronPort Email Data Loss Prevention Can Help

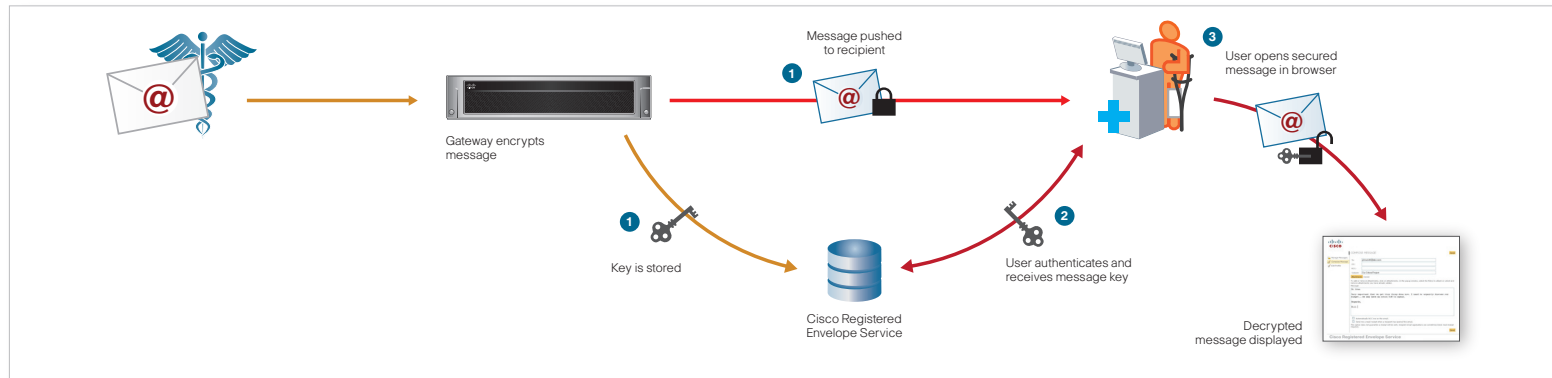
The Cisco IronPort C-Series email security appliance offers advanced DLP capabilities. In partnership with RSA, the leading vendor for data loss prevention solutions, Cisco has developed a DLP detection and enforcement engine that is fully integrated into the appliance. Securing medical data while it is being exchanged among different stakeholders involves making sure:

1. Data is scanned while in motion
2. Any potential flags are raised
3. Electronic or human mitigations are put into place if deemed necessary
4. The data is transmitted securely

The integrated solution has predefined policies that can detect issues regarding HIPAA requirements, state privacy laws, and Sarbanes-Oxley (SOX) regulations—providing organizations with a simple way to meet compliance mandates and protect confidential information. Furthermore, data that needs to be shared with outside parties can be encrypted to ensure that it reaches the intended recipient securely.

From an inbound perspective, Cisco IronPort Email Security Appliances defend against email-borne malware with a multi-layer approach for anti-spam and anti-virus protection. Reputation filtering is the first layer of protection, giving email messages a reputation score of good, bad, or neutral (based on the IP address the sender). Ninety percent of all spam is stopped by reputation filtering before it enters the network. Cisco IronPort Anti-Spam is the second layer of protection, using the Cisco IronPort Context Adaptive Scanning Engine (CASE). This engine examines the complete context of a message, including “What” content the message contains, “How” the message is constructed, “Who” is sending the message, and “Where” the call to action of the message takes the user. By combining these elements, Cisco IronPort Anti-Spam accurately stops a broad range of threats. Cisco IronPort Virus Outbreak Filters are another critical layer of preventive defense against new outbreaks—detecting and stopping viruses an average of 13 hours before traditional virus signatures are available. Traditional anti-virus technology is also fully integrated to enable multiple virus detection methods and ensure strong protection against even the most complex attacks. Cisco uses multiple methods, incorporating preventive and reactive measures, to provide a comprehensive email security defense.





Regardless of the healthcare entity, messages are always secure with Cisco IronPort Email Encryption technology.

Solution Features and Benefits

The RSA Email DLP and Email Encryption features on Cisco IronPort appliances enable healthcare organizations to protect patient information and other sensitive data.

Form Factor Flexibility: Email DLP and encryption are available regardless of whether an organization chooses cloud, hybrid, or on-premises. This gives healthcare providers more flexibility in selecting an email security infrastructure that best meets their growing business needs.

Addressing HIPAA Compliance: RSA Email DLP detects HIPAA infractions with dictionaries and proprietary code sets, U.S. Social Security numbers, and U.S. National Provider Identifiers. These may also be customized to detect patient identification numbers.

Over 100 Predefined Policy Templates: RSA Email DLP offers policies for healthcare providers including:

- Regulatory compliance
- U.S. state regulatory compliance
- Acceptable use policies
- Privacy protection
- Company confidential information
- Built-in classifiers
- Intellectual property protection

Protecting Patient Information: The RSA Email DLP scanning engine helps enable Cisco to provide customers with a spam efficacy rate of 99 percent and a false-positive rate of less than 1 in 1 million. In-depth scanning is accomplished by analyzing different data sets, matches and the proximity of data sets, in the body of the email message as well as attachments.

Powerful Email Encryption, Easy to Use: Healthcare IT can select from several options for secure delivery. Sensitive email messages can be set to be automatically encrypted, to be subject to recall, and to provide a read receipt without the burden resting on the recipient.

Severity-Based Remediation: Flexible remediation options may be automated based on the severity of the infraction. For example, the communication between two physicians who are collaborating on a patient can be auto-encrypted to ensure their seamless and secure communication. Or a message with a confidential spreadsheet, containing patients' procedural data that occurred in the last month, can be automatically quarantined.

In-Depth HIPAA and DLP Policy Reports: Actionable DLP reports are available on a system and individual user level. Reports contain in-depth information about who committed the violation, details of each violation, and the remediation action.

Summary

Deploying a data loss prevention solution does not require that the entire email infrastructure be re-architected. To protect organizations from inbound threats, as well as to safeguard PHI, the Cisco IronPort Email Security portfolio provides integrated features for an organization's existing infrastructure. Cisco provides a comprehensive, easy-to-manage, and accurate DLP solution to protect healthcare organizations from sensitive data loss.

Contact Us

Cisco sales representatives, channel partners, and system engineers are ready to help you evaluate how Cisco IronPort products can make your corporate network infrastructure secure, reliable, and easier to manage. If you believe that your organization could benefit from these industry-leading products, please call 650-989-6530 or visit us on the web at www.ironport.com/leader.