TECHNOLOGY

Overview

IRONPORT

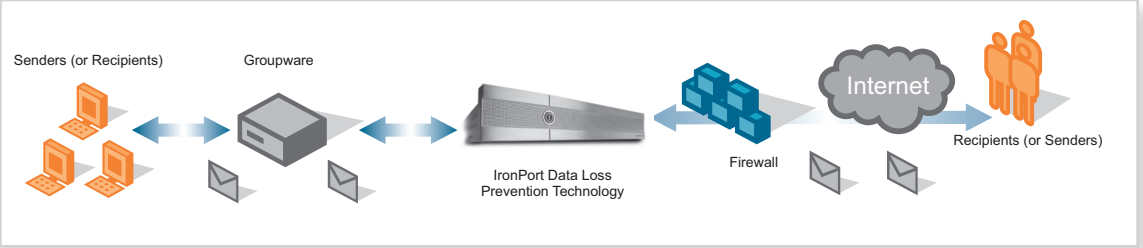
Data Loss Prevention Technology

INTEGRATED DLP SCANNING AND REMEDIATION FOR ORGANIZATIONS OF ALL SIZES.

OVERVIEW

Email has become the primary communication method for organizations of all sizes. Whether private information is deliberately or accidentally leaked, the ramifications of data loss are severe: violation of compliance regulations, erosion of customer trust and destruction of brand equity. As a result, executives are focused more than ever on rapidly deploying solutions to address data loss – and to do it in an easy-to-administer, unobtrusive manner.

As a leader in Internet gateway security, IronPort® Systems understands the complexities of creating a solution to address one of the most significant vectors for data loss: electronic communications. IronPort Data Loss Prevention technology gives corporate IT teams a single, fully-integrated solution that combines traditional email security functions (like spam and virus filtering) with work-flow based functions such as policy creation, content scanning, message encryption, quarantining and archiving.



Data Loss Prevention Made Easy: Corporations around the world are increasingly aware of the need to protect sensitive information. Whereas existing DLP solutions require additional hardware and new software to configure their monitoring solutions, IronPort customers can add DLP capabilities with the click of a mouse. The IronPort solution encompasses everything an enterprise IT team needs to start preventing data loss today.

INTEGRATED SCANNING

Compliance Dictionaries enable customers to address PCI, HIPAA, GLB, SOX and other regulatory compliance requirements. IronPort's compliance lexicons provide administrators with a pre-packaged set of key words and strings that make it easy to defend against outbound content compliance violations.

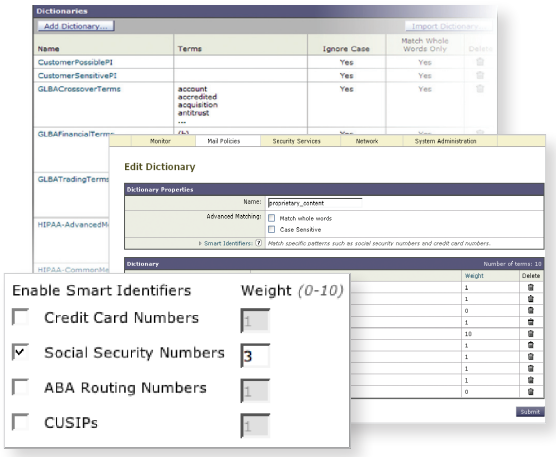
> "Email has become the de facto filing system for nearly all corporate information, making it even more critical to protect the outbound flow of messages."

— Brian Burke, Security Products Research Manager, IDC

INTEGRATED SCANNING (CONTINUED)

Smart Identifiers give administrators a simple way to configure and scan for sensitive patterns and strings that violate policy. With a simple point and click, administrators can configure filters that scan for:

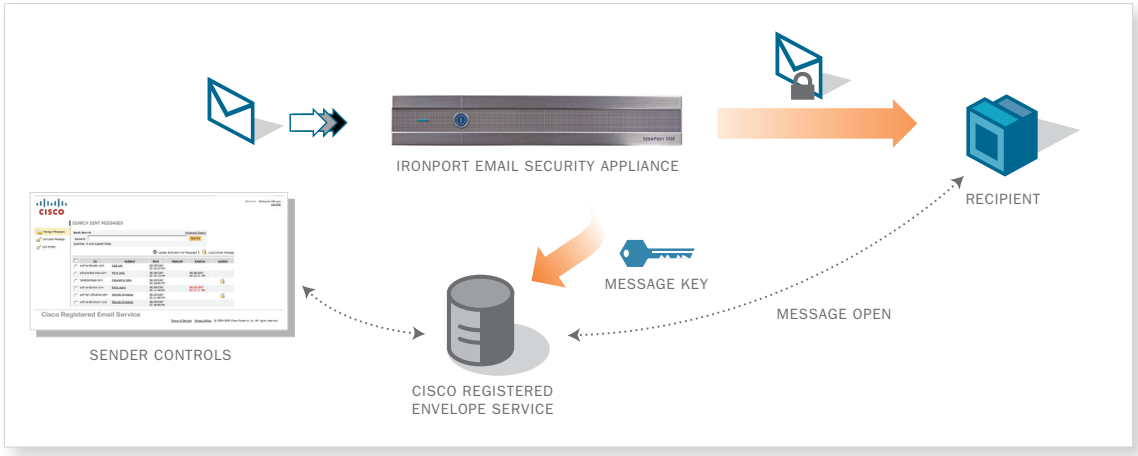
- Credit Card Numbers
- Social Security Numbers
- ABA Bank Routing Numbers
- CUSIPs



Content Filters and Attachment Scanning make it easy to create policies that are unique to your organization. IronPort's scanning engine can process over 300 different attachment types, and render the content for filtering purposes, to ensure DLP policy enforcement.

INTEGRATED REMEDIATION

Encryption is the cornerstone of an effective DLP solution. Automatic encryption is imperative as a remediation option for situations where sensitive information needs to be transmitted outside the organization. IronPort encryption capabilities use *IronPort PXE*™ encryption technology directly integrated on the IronPort appliance.



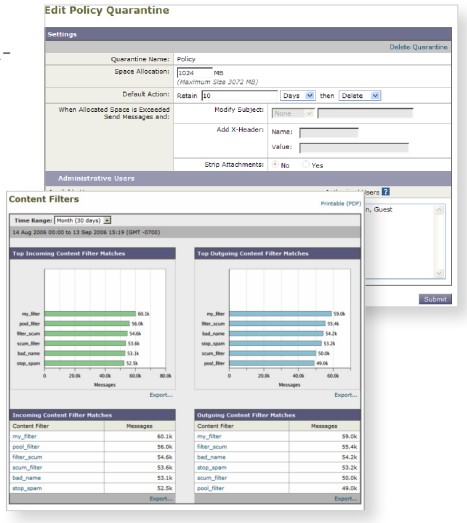
Encryption in Action: Using the Cisco Registered Envelope Service™ (CRES), IronPort email security appliances encrypt and decrypt messages to deliver the lowest TCO and highest service available.

Incoming and outgoing mail can now be encrypted and decrypted with no additional hardware required to filter, route and deliver messages securely. Based on an organization's policies, outbound messages are detected and automatically encrypted on the appliance.

INTEGRATED REMEDIATION (CONTINUED)

Compliance Quarantine provides Web-based access to review email that has been flagged by the content scanning engine. Multiple quarantines can be created and managed for your organization's unique policy and compliance requirements.

Compliance Reporting allows organizations to view the effectiveness of their DLP policies. The reporting engine provides a real-time view into the DLP rules being triggered and the summary list of policy violators. User-specific reports are also generated for identification, potential education and remediation.



DEPLOYMENT OPTIONS

IronPort Data Loss Prevention technology is fully-integrated on:

- *IronPort C-Series*™ appliances
- *IronPort X-Series*™ appliances
- The *IronPort Encryption Appliance*™

SUMMARY

IronPort 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. IronPort believes that a holistic solution for monitoring and data loss across all communication channels is vital to ensure the integrity of an organization's policies. Leadership within the Internet security market, together with its partnerships with industry-leading DLP vendors, puts IronPort in the unique position to offer a single vantage point to enterprises for this critical functionality.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

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

IRONPORT DATA LOSS PREVENTION 10/07 DOC RELEASE

IRONPORT

IronPort Systems, Inc.
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

P/N 435-0231-1 10/07

IronPort is now part of Cisco.

CISCO