




Data Loss Prevention Best Practices

Managing Sensitive Data in the Enterprise

A REPORT FROM
IRONPORT SYSTEMS

WITH A FOREWORD BY BRADLEY R. HUNTER



A MESSAGING MEDIA PUBLICATION

Table of Contents

Foreword by Bradley R. Hunter	5
Introduction.	9
Defining the Data Loss Problem.	11
What Data is Sensitive?	12
Regulatory Compliance	12
Intellectual Property Protection	12
Why is Data Loss So Prevalent?	14
Sizing Up the Data Loss Problem.	15
Getting to the Heart of the Matter: Uncontrolled Communications	17
Putting Teeth in Corporate Policy: The DLP Traffic Cop	18
Appropriate Use Enforcement	19
Best Practice #1: Take Time to Define DLP Needs.	21
Best Practice #2: Prioritize the DLP Focus	23
Best Practice #3: Ensure Effective, Comprehensive Coverage	24
Best Practice #4: Make the Solution Unobtrusive	25
Best Practice #5: Look for Work Flow, Administration and Reporting. . .	26
Best Practice #6: Combine Best-of-Breed Solutions.	27
Conclusion.	29
Appendix: Regulatory Compliance	30
Special Section: IronPort Stops Data Loss in its Tracks	35

DISCLAIMER: The law in this area changes rapidly and is subject to differing interpretations. It is up to the reader to review the current state of the law with a qualified attorney and other professionals before relying on it. Neither the authors nor IronPort make any guarantees or warranties regarding the outcome of the uses to which this material is put. This paper is provided with the understanding that the authors and IronPort are not engaged in rendering legal or professional services to the reader.

Copyright © 2000-2007 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

“As your network traffic increases...your chosen solution must scale to keep pace, with both volume and network bandwidth.”

BRADLEY R. HUNTER
Director of Technology Solutions, AHA Solutions, Inc.

Foreword

by Bradley R. Hunter

Consider the Herculean efforts today to protect the network from threats: intrusion prevention systems scan packets for potentially damaging content; email security systems check for viruses in email content and firewalls block unsolicited connections. To stop the onslaught of threats to corporate and government networks, a host of software and appliances are being deployed daily. In general, these border police applications are doing a fairly decent job of stopping unauthorized intrusion at the door to your network.

But what about organizational insiders? Which applications or appliances are scrutinizing the information being passed out of the network? Intrusion



IronPort's email security products have the exclusive endorsement of the American Hospital Association (AHA).

prevention systems and firewalls aren't looking for intellectual property sliding out the door right under their virtual noses. Specifically in health care organizations, what about patient information sent unprotected over the Internet to another provider? Add in the always-changing regulatory environment, and security is a unique challenge. All it takes is one misstep to compromise sensitive information. These are legitimate, authorized users communicating in an above-board way – but potentially exposing sensitive data in the process. This is the core of the immensely complex problem of data loss.

To address the data loss problem, organizations need to focus now on content filtering and blocking of electronic communications leaving the network – and not just email, but instant messaging (IM), webmail, HTTP and FTP communications as well. All avenues of electronic communication need to be policed to prevent intellectual property, financial information, patient information, personal credit card data, and a variety of sensitive information (depending on the business and the industry) from falling into the wrong hands.

There are two key capabilities required for content filtering: high performance and the ability to accurately scan nearly anything. Let's begin with the former. With today's ever-increasing bandwidth requirements, high performance is a must. Anything short of line speed would introduce a noticeable delay to end-users. And it must be scalable. As your network traffic increases, which it surely will (and at a rate even faster than you anticipate), your chosen solution must scale to keep pace with both volume and network bandwidth.

The ability to accurately scan nearly anything is a critical competency. Content monitoring tools look at the content, scan and detect sensitive data, and mitigate risk through automated blocking or encryption of outgoing messages – based on policy requirements.

But the trick is to get the accuracy right. Detection accuracy and the ability to define granular policies are what content scanning tools require to both avoid letting leaks through or generating too many false positives.

Across all key protocols, a high-performance, intelligent data loss prevention (DLP) solution is a must-have for today's organizations. Decision-makers should look to vendors with deep expertise in content scanning and select a best-of-breed DLP solution.



Bradley R. Hunter

Director, Technology Solutions
American Hospital Association Solutions, Inc.

“The average information leak costs organizations approximately \$182 per record, averaging roughly \$4,800,000 per breach in total.”

SOURCE:
THE PONEMON INSTITUTE

Introduction

While a great deal of attention has been given to protecting companies' electronic assets from outside threats – from intrusion prevention systems to firewalls to vulnerability management – organizations must now turn their attention to an equally dangerous situation: the problem of data loss from the inside.

In fact, in many organizations there's a gaping hole in the controlled, secure environment created to protect electronic assets. This hole is the now ubiquitous way businesses and individuals communicate with each other – over the Internet.

Whether it's email, instant messaging, webmail, a form on a website, or file transfer, electronic communications exiting the company still go largely uncontrolled and unmonitored on their way to their destinations – with the ever-present potential for confidential information to fall into the wrong hands. Should sensitive information be exposed, it can wreak havoc on the organization's bottom line through fines, bad publicity, loss of strategic customers, loss of competitive intelligence and legal action.

Given today's strict regulatory and ultra-competitive environment, data loss prevention (DLP) is one of the most critical issues facing CIOs, CSOs and CISOs. For those creating and implementing a DLP strategy, the task can seem daunting. Fortunately, effective technical solutions are available. This report presents best practices that organizations can leverage as they seek solutions for preventing leaks, enforcing compliance, and protecting the company's brand value and reputation.

“You have to understand what kind of sensitive data you have, and do a risk evaluation of what happens if data is exposed or gets in the wrong hands.”

THOMAS RASCHKE
Senior Analyst, Forrester Research, Inc.

“Employee error is now the fourth largest security concern in the enterprise – behind malware, spyware and spam.”

IDC ENTERPRISE SECURITY SURVEY, 2006

Defining the Data Loss Problem

The issue of data loss encompasses everything from confidential information about one customer being exposed, to thousands of source code files for a company’s product being sent to a competitor. Whether deliberate or accidental, data loss occurs any time employees, consultants, or other insiders release sensitive data about customers, finances, intellectual property, or other confidential information (in violation of company policies and regulatory requirements).

Consider the following high-profile examples: AOL posts search engine data containing personal information about its members, a DuPont employee leaks \$400 million in intellectual property, the CEO of Whole Foods bashes the competition via industry blogs, a former Ceridian employee accidentally posts ID and bank account data for 150 employees of an advertising firm on a website. The list goes on and on.

With all the avenues available to employees today to electronically expose sensitive data, the scope of the data loss problem is an order of magnitude greater than threat protection from outsiders.

Consider the extent of the effort required to cover all the loss vectors an organization has the potential to encounter:

- **Data in motion** – Any data that is moving through the network to the outside via the Internet
- **Data at rest** – Data that resides in files systems, databases and other storage methods
- **Data at the endpoint** – Data at the endpoints of the network (e.g. data on USB devices, external drives, MP3 players, laptops, and other highly-mobile devices)

To avoid getting broadsided by a data loss, companies must evaluate their specific vulnerabilities for each loss vector and respond appropriately.

What Data is Sensitive?

There are two main concerns driving data loss prevention efforts: regulatory compliance and protection of intellectual property.

Regulatory Compliance

Nearly every organization falls under one or more local, federal, or international regulatory mandates. Whether it's the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLB), Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI DSS), European Union Data Protection Directive, or other regulations, companies are required to take measures to protect private and personally-identifiable information. Personally-identifiable information is defined as any piece of information which can potentially be used to uniquely identify, contact, or locate a single person – whether a consumer, employee, student, patient, or taxpayer. In the U.S., thirty-five states currently mandate the notification of individuals by the company suffering a data loss in the event that their personally identifiable information is breached.

Data loss is not only a significant problem for companies in data-sensitive industries such as health care and finance, but for nearly any organization conducting business worldwide.

Unfortunately, the road to compliance is filled with regulatory pitfalls. Simple missteps, such as sending a legitimate email (containing unencrypted credit card information) or sharing a report (including employee medical data) with an unauthorized person, can constitute regulatory violations.

Intellectual Property Protection

In today's hyper-competitive environment, intellectual property (IP) protection is a major concern for organizations of all sizes. From industrial espionage to employees defecting to a competitor and taking sensitive information with them, protecting one of the most important assets of the business is a key driver of data loss prevention efforts.

According to a 2006 report from the office of the United States Trade Representative (USTR), U.S. businesses are losing approximately \$250 billion annually from trade secret theft. For example, Apple Computer filed a lawsuit against an employee who posted images of two new products on the Web prior to release. The fact that these images appeared on the Web, before the products were launched, was reported to cause a drop in Apple's share value.

Trade secrets, according to the Uniform Trade Secrets Act (UTSA), include formulas, patterns, compilations, program devices, methods, techniques, or processes. They also can be diagrams and flow charts, supplier data, pricing data and strategies, source code, marketing plans and customer information. With so much that could be considered a trade secret, chances are good that employees may not even know they are handling IP.

Companies need to take steps to better protect valuable IP property from situations such as:

- Inadvertent forwarding of email containing product development or business plans to another email recipient
- Sending unreleased pricing information to the wrong email address
- Customer or competitive information sent by an employee to a third-party for financial gain
- Proprietary information sent to a distributor, who might then forward it on to competitors

Data loss is not only a significant problem for companies in data-sensitive industries...but for nearly any company conducting business worldwide.

Why is Data Loss So Prevalent?

We're all electronically connected in numerous ways. Whether on the road, in the office or at home – we're never far away from an electronic device capable of linking us to others nearby or halfway around the globe. Instant access to electronic data has become more crucial in day-to-day business.

Take worldwide collaboration, for instance: many companies have offshore development offices, outsourced service providers, and/or international offices – all of which exponentially increase the opportunity for data loss. With a simple email communication, confidential information can instantaneously travel to the far corners of the earth.

Closer to home, the environment is also ripe with opportunity for data loss. Workers today experience a far greater amount of flexibility in their work location and hours than previous generations. For instance, a May 2006 U.S. Chamber of Commerce report stated that 20 million Americans now telecommute – meaning that electronic communications become the lifeline to the office with important and possibly sensitive company data traveling back and forth in cyberspace – a prime target for criminals to hijack.

Over the years, organizations have spent a tremendous number of resources in hopes of protecting their information. However, the majority of their efforts have been focused on preventing outsiders from hacking into the organization. According to leading analyst firms, the majority of all leaks are the result of unintentional information loss from employees and partners. Some research indicates that more than half (and as much as 80 percent) of security breaches are caused by insiders, with actions originating behind the firewall. An organization doesn't need far-flung offices or telecommuting staff to be a fertile ground for data loss – whether intentional, or (more often than not) accidental, employees can cause a catastrophe for their company with the simple click of a mouse.

Sizing Up the Data Loss Problem

It's a mobile, connected world – and companies are paying the price for not monitoring and controlling electronic communications as they exit the safety of the company. While most organizations scan inbound email for unsolicited or dangerous content, most fail to check their outgoing email, IM and other Internet-based communications, essentially allowing the unauthorized or unintentional transfer of sensitive information outside of the organization.

Deloitte's 2006 Global Security Survey reported that 49 percent of companies have experienced an internal security breach in the past year. Of those, 31 percent experienced a breach from a virus/worm incident, 28 percent through insider fraud and 18 percent by means of data leakage (19 percent experienced the breach through other means and 4 percent choose not to specify). It's also significant that fully 96 percent of respondents reported that they are, "concerned about employee misconduct involving their information systems."

Most Common Internal Security Breach Causes

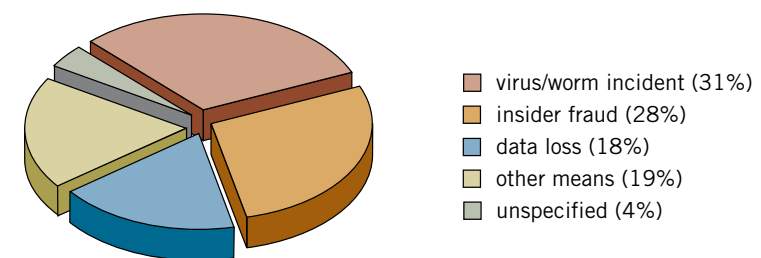


FIGURE 1: Nearly half of all companies surveyed have experienced an internal security breach in the past year. The most common breach causes are outlined in the chart above. (Source: Deloitte's 2006 Global Security Survey)

According to the Privacy Rights Clearinghouse, more than 100 million data records of U.S. residents have been exposed due to security breaches since February 2005. While the FBI estimates that the total cost of all data breaches in 2006, including corporate data, cost companies a total of \$62.7 billion, experts add that the average cost of one incident of data loss or leakage for large organizations is estimated at \$4.8 million.

Data loss can compromise intellectual property or cause an organization to violate compliance regulations. It can be an all-out threat to the considerable brand value a company has built. To protect its investment in its brand, products, partnerships and employees, a company can no longer afford to ignore this hole in the corporate armor.

“...more than 100 million data records of U.S. residents have been exposed due to security breaches since February 2005.”

SOURCE:
THE PRIVACY RIGHTS CLEARINGHOUSE

Getting to the Heart of the Matter: Uncontrolled Communications

Given the prevalence of electronic communications, data in motion (i.e., data that is traveling through and out of the network) is one of the most significant data loss vectors to address today. For example, an employee sends documents to a personal email address so he or she can work from home. Or a hospital employee accidentally sends patient information to the wrong person. A summer intern unknowingly cuts and pastes confidential product information into a blog entry.

As the latter example shows, it's not only outbound email that must be addressed. There are many avenues in which confidential data or proprietary secrets can leave an organization via the Internet:

- Email
- Webmail
- HTTP (message boards, blogs and other websites)
- Instant Messaging
- Peer-to-peer sites and sessions
- FTP

Current firewall and other network security solutions do not include data loss prevention capabilities to secure data in motion. Missing are such important controls as content scanning, blocking of communications containing sensitive data and encryption. While companies have attempted to address the data loss problem through corporate policies and employee education, without appropriate controls in place, employees can (either through ignorance or malicious disregard) still leak confidential company information.

While data loss solutions must address the risks inherent in data at rest and data at the end-point, given the extent to which data in motion can impact

the health and longevity of an organization, companies must begin implementing comprehensive data loss prevention solutions specifically to prevent employees, consultants, vendors and any other authorized user from transmitting sensitive information outside the organization. Further, they must embrace multiple solution layers – including email, Web, instant messaging and more.

Putting Teeth in Corporate Policy: The DLP Traffic Cop

To tackle the vulnerability of data in motion, and police the various electronic communication avenues for data loss, companies need a traffic cop – monitoring and controlling each and every communication that leaves the company, regardless of the manner of transport.

A comprehensive DLP solution prevents confidential data loss by:

- Monitoring communications going outside of the organization
- Encrypting email containing confidential content
- Enabling compliance with global privacy and data security mandates
- Securing outsourcing and partner communications
- Protecting intellectual property
- Preventing malware-related data harvesting
- Enforcing acceptable use policies
- Providing a deterrent for malicious users (by creating the possibility of being caught)

In addition to blocking communications with sensitive data from being sent outside the organization, a DLP solution can also be instrumental in helping companies comply with regulations. Outbound email containing personally-identifying patient information can be encrypted automatically, as can any mail attachments containing proprietary or personal information.

As organizations seek out a solution to the data loss problem, keeping DLP best practices in mind can help determine the right solution for a company's specific requirements.

Appropriate Use Enforcement

A critical component of data loss prevention (which also protects the organization from litigation and potential criminal misconduct) is the definition and enforcement of appropriate/acceptable use policies for electronic communications. Typical appropriate use areas include policies against illegal or discriminatory activities, large attachments, or sending of communications to certain parties without legal disclaimers.

To enforce appropriate use policies, organizations may require a DLP solution with the following capabilities:

- Block (or alert about) illicit activity, such as pornography
- Prohibit distribution of copyrighted music and video files through P2P file sharing programs
- Prevent use of gambling websites
- Enforce messaging policy (attachment size, no personal email, etc.)
- Add legal disclaimers to outgoing emails

While the problem of data loss can appear overwhelming, best practices are being formulated as organizations begin to implement the DLP traffic cop in a variety of infrastructure settings.

“Current policies designed to protect organizations against the leakage of sensitive information are not considered effective by the majority of organizations.”

OSTERMAN RESEARCH

Messaging Policy Management Trends Report, 2007-2010

BEST PRACTICE #1:

Take Time to Define DLP Needs

The critical first step towards solving the data loss problem is to develop a comprehensive understanding and inventory of the types of sensitive data that exist within the organization and what policies are needed to control and enforce how that data can be shared. To do this, organizations need to review the extent to which their companies or agencies are impacted by regulatory compliance, intellectual property protection and appropriate use enforcement.

For instance, it's critical to understand exactly how regulations apply to the overall organization, as well as to individual users, departments and remote offices. A particular company may need a solution where content is scanned and automatically encrypted to protect private information, for example. Taking a more granular view of compliance areas makes it easier to define requirements, manage compliance and demonstrate effectiveness of compliance solutions.

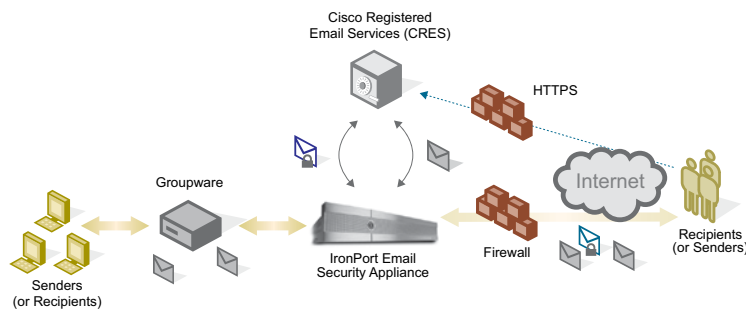
After determining relevant areas where sensitive data need to be protected, organizations should also consider the impact of data loss prevention on workflow, ensuring that any solution implemented is designed to be dynamic and flexible as workflow and processes change.

Finally, a critical success factor for implementing a DLP solution is to ensure executive involvement. Identify a champion within the “C-suite” (e.g., the CIO, CSO, CISO or CTO) who can provide the credibility and support needed to implement an enterprise-wide program.

CASE IN POINT**Data Loss Prevention Ensures Regulatory Compliance**

A leading provider of insurance brokerage and specialty insurance underwriting services needed to ensure compliance with HIPAA and GLB mandates. It sought a solution that would enable the company to easily and thoroughly demonstrate compliance during audits. Critical requirements were that the solution be easy-to-use, automatically identify sensitive data, secure the data automatically and cover the user population – without the necessity of client software.

The company chose IronPort C-Series™ email security appliances, with integrated encryption for data loss prevention. With this comprehensive solution, not only is the company ensuring compliance with regulations, it's also enforcing appropriate use policies.



Based on DLP policies, IronPort email security appliances encrypt and decrypt messages using the Cisco Registered Email Service™ (CRES) to deliver the lowest TCO and highest service availability.

BEST PRACTICE #2:**Prioritize the DLP Focus**

Organizations rely on email, instant messaging, and Web-based communications to maintain efficient communications internally, with suppliers and partners, and most importantly with customers. While electronic communications have revolutionized the efficiency of communication, they have also introduced additional risks particularly with regards to policy compliance and data privacy. An off color joke told between two friends out of the office can quickly become an HR policy violation incident when sent and resent through corporate email. Disgruntled employees can forward key documents to third parties, thus risking loss of critical intellectual property. The inadvertent slip of a mouse click can send a customer's personal information to a mailing list causing not only an embarrassing event in the news, but one that results in costly fines and remediation activity.

Data loss prevention is a complex problem that requires blending best-of-breed solutions to address all relevant aspects for a particular organization. This means first identifying all the potential vectors for data loss in your organization (data at rest, data in motion and data at the endpoint) and then prioritizing them – based on criteria such as past breaches, volume of communications, volume of data, the likelihood of a breach and the number of users with access to those vectors.

Focusing first on the most significant DLP areas – those that represent the greatest potential loss vectors – makes it easier to justify solutions and get started on plugging the leaks. For instance, given their ubiquitous usage, the accidental leakage of sensitive information via email and Web communications is likely to be a primary area of focus for the majority of companies.

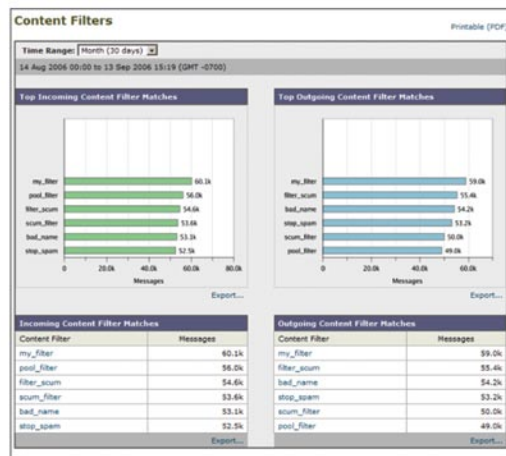
BEST PRACTICE #3:

Ensure Effective, Comprehensive Coverage

Based on the first two best practices, organizations have identified information to be protected and the avenues of data loss that are most probable. Now it's time to begin researching a data in motion DLP solution that best meets the company's particular requirements.

Overall, a DLP solution must be able to effectively and comprehensively detect attempted policy violations. This includes:

- Multi-protocol monitoring and prevention
- Content-level analysis of all major file and attachment types
- Selective blocking and/or quarantining of messages
- Automatic enforcement of corporate encryption policies



Reporting and remediation are central elements of an effective DLP solution.

BEST PRACTICE #4:

Make the Solution Unobtrusive

The next important aspect for a DLP solution is that it's non-intrusive. Overcoming the challenges of maintaining effective communications (while ensuring management and control of customer and sensitive information) requires both well thought out policies, and processes for monitoring communications content. Breaches must be prevented with negligible impact on end-users. Any perceptible delay in email communications or Internet page loads can inhibit the flow of business and the productivity of employees.

This means that the DLP solution must run at line-speed – scaling to gigabit network rates as required. Further, it must continue to run consistently – despite traffic volume increases (hence the need for a solution to continue scaling as companies and networks grow).

Organizations should select a DLP solution for email and Web that can manage ever-increasing message volumes and handle future bandwidth requirements. While this may seem like a daunting endeavor, the good news is that there are solutions which are optimized for scalability, performance and security.

A DLP solution must run at line-speed – scaling to gigabit network rates if required.

BEST PRACTICE #5:

Look for Work Flow, Administration and Reporting

When choosing a DLP solution, organizations should also keep deployment, management, and reporting in mind. To help keep total cost of ownership low, the selected product should be simple and fast to implement effectively within the organization's infrastructure – leveraging plug-and-play capabilities to minimize integration requirements.

Further, a DLP solution should be optimized for easy maintenance and management. Automatic updates are one area where the ideal choice would simplify these functions.

A DLP solution cannot be effective without detailed reports of all suspected violations. Administrators and policy officers should have the ability to receive reports outlining detected violations, with in-depth information that enables them to take action. These details include: the message sender, contents, attachments, intended recipients and information about the violating content.

Robust reporting capabilities allow policy officers to readily access information to:

- Analyze and improve the organization's DLP capabilities
- Automatically deliver decision-making information in a timely manner
- Easily generate instant reports for executives

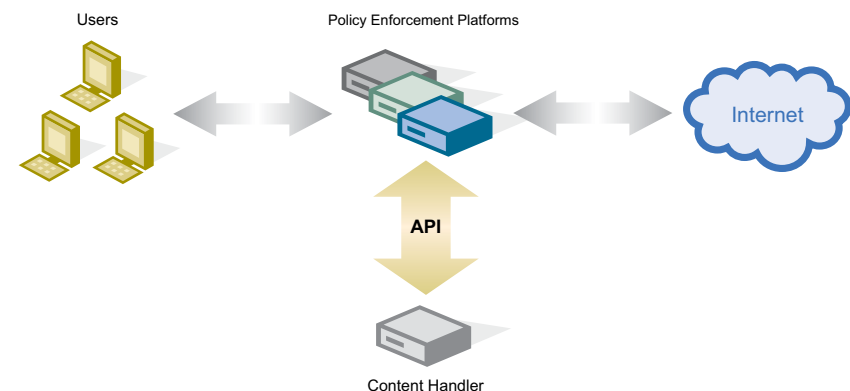
BEST PRACTICE #6:

Combine Best-of-Breed Solutions

Solutions for data loss prevention are still evolving, with no single one providing all the in-depth capabilities most organizations require. For instance, managing security across both data in motion and data at rest vectors is a challenge – with each vulnerability requiring a different set of capabilities.

Looking across the entire data flow, companies need to address the data loss problem by creating an end-to-end solution, using best-of-breed products. The best answer is to leverage solutions from dedicated vendors for data in motion and data at rest to gain the most comprehensive, effective prevention across the board.

The hallmark of best-of-breed solutions is the ability to extend and enhance their effectiveness through integration with other best-of-breed tools. Companies should avoid selecting a DLP solution that inhibits them from integration in the future. As the industry evolves, it will be crucial to have the flexibility and support to take full advantage of future third-party solutions through connectivity and data sharing.



Looking Forward: In the future, open, high-performance Application Programming Interfaces (APIs) will enable unified DLP management.

“...we seem to be in the midst of a ‘data loss epidemic’, with tens of millions of individuals receiving data loss notification letters this year.”

RICH MOGULL
Research Vice President, Gartner, Inc.

Conclusion

Data loss prevention is a serious issue for companies, as the number of incidents (and the cost to those experiencing them) continues to increase. Whether it's a malicious attempt, or an inadvertent mistake, data loss can diminish a company's brand, reduce shareholder value, and damage the company's goodwill and reputation.

By leveraging best practices, companies can seek out a data loss prevention solution that best suits their particular needs. For compliance with regulations such as HIPAA and PCI, protection of intellectual property, and enforcement of appropriate use policies, a best-of-breed DLP solution for data in motion will help address one of the most significant vectors for data loss: electronic communications.

Combined with data at rest and data at endpoint solutions (which protect file systems, databases and data on various portable devices), a data in motion solution helps protect companies across the board from the risk of data loss. Organizations that proactively embrace this challenge will reap the benefit of deeper compliance with regulatory policies and greater protection for valuable intellectual assets.

APPENDIX:

Regulatory Compliance

In this section we outline the legal requirements of some of the most important laws affecting messaging. Each of these regulations is complex, and none have been written with an eye to the real capabilities of current messaging technologies, or the typical corporate practices that have evolved to meet the demands of business and other practical requirements.

As with any compliance-related activity, your business must consult its professionals (e.g. lawyers, accountants, and consultants) to assess the measures it must take to comply with the specific laws and regulations applicable to its activities.

Gramm-Leach-Bliley (GLB)

The Gramm-Leach-Bliley Act of 1999 (sometimes called the Financial Modernization Act, and frequently shortened to GLB) is intended to ensure protection of consumers' private financial data, which the Act refers to as Nonpublic Personal Information (NPI). GLB applies to a wide range of financial institutions and other organizations that maintain NPI related to their customers.

The two areas of greatest concern to most companies are the Financial Privacy Rule, which covers the collection, use and disclosure of NPI, and the Safeguards Rule, which describes the processes companies must take to protect NPI.

While GLB doesn't make reference to specific technologies (i.e., the law is "technology neutral"), in practice, the Safeguards Rule means that companies should implement policy enforcement tools that can encrypt or block email traffic, as appropriate, based on message sender, recipient and content. In addition, companies must implement systems that provide logging and reporting – allowing them to demonstrate compliance.

Section 302, which assigns responsibility for financial reports, and Section 404, which describes required internal controls, are the two sections most relevant to electronic data loss. These provisions outline several conditions directly relevant to email policies and practices as they relate to loss of financial data, including requirements for:

- Identification and handling of information that must be kept confidential
- Identification of individual message senders
- Confidential transmission of email
- Hardening email and other servers that store confidential information
- Tracking and logging message traffic
- Auditing capabilities
- Message indexing, archiving and retention

As with GLB, SOX isn't specific about the precise policies or technical means companies should use to implement these requirements. However, there is no question that SOX compliance requires a data loss prevention capability for a public company's messaging architecture.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) places a number of requirements on the health care industry's information handling practices, and has direct impact on the operation of messaging systems.

Under HIPAA, organizations must ensure that email messages containing protected health information are secured, even when transmitted via unencrypted links, that senders and recipients are properly verified (technically, HIPAA's "person or entity authentication" standard applies only to "a person seeking access to electronic protected health information," not to the sender of that information) and authenticated, and that email servers and the messages they contain are protected. In other words, HIPAA affects both information in transit, and information at rest.

HIPAA does not specify particular technologies that should be used to implement these rules. Rather, the rules can be seen as an attempt to mandate best practices of information security. There is a broad consensus in the technology community that technical approaches such as authentication, encryption, content filtering, hardened message server software and archiving are appropriate means for meeting HIPAA requirements.

California 1386

Effective since July 2003, this mandate requires public disclosure of computer security breaches in which confidential information of California residents may have been compromised.

ISO/IEC 27002:2005 (formerly ISO 17799)

A generic set of best practices in information security that is rapidly gaining acceptance worldwide. It provides recommendations for use by those who are responsible for initiating, implementing or maintaining information security systems.

Family Educational Rights and Privacy Act (FERPA)

FERPA governs the privacy of student records in any medium, including email, and applies to any institution that receives funds from the Department of Education.

California AB 1350

This California Assembly bill affects businesses that own or license personal information about California residents – mandating that such businesses implement “reasonable security procedures” to protect that information.

Title 21 CFR Part 11

Primarily focused on pharmaceutical and other industries controlled by the Food and Drug Administration (FDA), this regulation defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.

European Union Data Protection Directive of 2002

This regulation updates legal standards for the processing of personal data and the protection of privacy. The law sets stringent restrictions on which personal information can be collected and stored. It also dictates rules for passing personal data to non-EU countries.

“After a thorough evaluation of alternatives, IronPort Systems proved to have the most accurate, and easiest to manage, DLP solution – by far.”

SANTOSH GOVINDARAJU
CEO, Paragon Mortgage, Inc.

SPECIAL SECTION:

IronPort Stops Data Loss in its Tracks

IronPort® Systems, a Cisco business unit, offers an excellent example of a DLP solution. Built on industry best practices to deliver powerful and effective data loss prevention for data in motion, IronPort’s state-of-the-art content scanning engine acts as traffic cop to deliver unparalleled data protection across email, Web, IM and other Internet-based communications.

In production at more than 20 percent of the world's largest enterprises, IronPort is a leading provider of email and Web security appliances. IronPort’s high-performance, easy-to-use and technically-innovative products provide the critical tools organizations need for data loss prevention.

Next Generation Compliance Filters

IronPort’s pre-defined content filters for HIPAA, GLB, SOX and other regulations automatically scan emails for protected financial and health information. Easily extensible lexicons allow companies to customize these rules to meet specific requirements. IronPort also has an extensive ‘best practices’ database of content filters deployed for customers in the health care, financial, legal, technology and other industry verticals. IronPort’s easily deployed solution defends organizations against outbound content compliance violations.

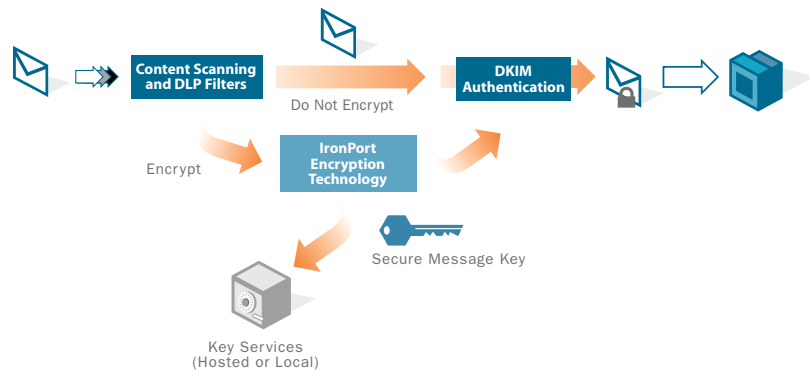
IronPort Email Encryption

Industry-leading encryption technology enables IronPort users to comply with regulatory requirements related to the securing of health and financial information. The company’s secure email delivery solution seamlessly encrypts, decrypts and digitally signs confidential email messages. IronPort provides a unified solution for enforcing granular encryption policies, and guarantees message signing (sender and recipient verification) and integrity while protecting messages stored on servers.

High-Performance, Multi-Protocol Content Scanning

IronPort's high-performance content scanning engine provides flexibility and fine-grained controls for effective monitoring of outbound messages for sensitive information. Organizations can scan and filter virtually any portion of an outbound message (message headers, subject, sender, recipient, attachment type or content, and message body content) for specific keywords, regular expressions, as well the contents of pre-defined or customizable dictionaries. These capabilities allow for a wide variety of policy enforcement options – drop, bounce, alter, archive, or encrypt a message, generate a notification, and/or blind carbon-copy the message to an archive or compliance officer.

Outbound Email Pipeline with IronPort Encryption Technology



DLP filters on IronPort C-Series appliances identify messages to be encrypted, based on compliance and business considerations. Once encrypted, messages continue through the mail pipeline for DKIM authentication and delivery.

IronPort's content scanning system integrates with industry standard LDAP servers to test users' existence within a company group, or their permissions to send a specific type of message. Integration with LDAP servers allows organizations to incorporate email rules into the overall company workflow policies. Using a point-and-click interface, IronPort customers can define and enforce specific mail policies based on whether a sender or recipient

is member of a particular LDAP group. For example, you can encrypt all emails sent by the accounting group to a business partner, or add a disclaimer to all outgoing emails sent by the legal team.

Web and Instant Messaging Protection

Not limited to email messaging, IronPort delivers state-of-the-art functionality to detect and block the loss of sensitive data via Web and instant messaging. Based on its advanced content filtering capabilities, IronPort can stop: FTP sessions and uploads, IM sessions (including HTTP-tunneled IM sessions, native IM sessions and access to IM sites), access to peer-to-peer file sharing sites (including HTTP-tunneled and native P2P sessions) as well as spyware "phone home" activity. IronPort technology also prevents keyloggers and system monitors from entering the network.

Enterprise Management Tools

Detailed logs and reports identify messages that trigger specific policy rules and track the actions taken on these messages. For example, an email administrator can verify whether outgoing messages to a particular recipient were encrypted. This enables administrators to effectively meet the logging and reporting requirements of even the most stringent regulatory requirements. Additionally, this information is maintained under change control, which provides the kind of auditability called for in email-related regulations.

A Key Component of an End-to-End DLP Solution

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.

More information about IronPort can be found at: www.ironport.com/dlp.

IRONPORT EMAIL AND WEB SECURITY APPLIANCES

- IronPort C-Series
- IronPort X-Series
- IronPort S-Series



IRONPORT. ENFORCING DATA LOSS PREVENTION.

IronPort email and Web security appliances are in production at more than half of Fortune 100 companies and eight of the ten largest ISP's. These industry-leading systems have a demonstrated record of unparalleled performance, accuracy and reliability.

The same technology that powers and protects IronPort's most sophisticated customers is available for companies of all sizes, starting with IronPort's entry-level appliances.

By enforcing Data Loss Prevention – including Regulatory Compliance, Intellectual Property Protection and Acceptable Use Policy Enforcement – IronPort email and Web security appliances vastly improve the administration of corporate infrastructure, reduce the burden on technical staff and provide state-of-the-art protection.

Get started
on your
DLP plan
with IronPort
technology.



MAKING THE INTERNET SAFE.™

BRADLEY R. HUNTER is Director of Technology Solutions for American Hospital Association Solutions, Inc. In this capacity, he is responsible for the strategic planning, marketing, business development and adoption of technology solutions exclusively endorsed by the American Hospital Association. A graduate of Purdue University and the University of Illinois – Urbana Champaign, he has over 10 years of experience in the health care and information technology field, specializing in administration/management, business development, executing product rollout and marketing campaigns, and customer retention strategies. Bradley is an active member of numerous associations focused on improving the adoption of healthcare information technologies to improve the quality, patient safety, patient experience and financial stability of hospitals.

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.