

# the Web Security report

A MESSAGING MEDIA PUBLICATION • DECEMBER 2007 EDITION • WWW.WEBSECURITYREPORT.COM

## ABOUT THIS PUBLICATION

The Web Security Report acts as a publishing partner for Internet security solutions providers, testing labs, research entities and trade organizations. Published by Messaging Media, LLC, the Web Security Report has an online and print audience of over 120,000 readers.

[publish@websecurityreport.com](mailto:publish@websecurityreport.com)

12 07

## Reinventing Data Loss Prevention

### TABLE OF CONTENTS

Reinventing Data Loss Prevention	1
Web Security News	8
Sponsor Profile	10
In This Edition	12

By Jeff Ubois

Data losses of thousands, even millions of customer records, inadvertent or accidental forwarding of sensitive email, and casual violations of corporate policies have become a daily occurrence – and are pushing data loss prevention to the top of the agenda at every company with an Internet connection.

Ensuring regulatory compliance, preventing loss or theft of intellectual property, and enforcing appropriate use policies on corporate networks are critical problems facing today's C-level executives. Simply put, the consequences of data loss – fines, negative publicity, loss

### Practice Makes Perfect

All too frequently, the industry is alerted to high-profile examples of confidential information being compromised. Organizations worldwide are losing data without even realizing it – and the effects can be devastating. The case for protecting business communications grows stronger with each misstep. Add in the always-changing regulatory environment, and security is a unique challenge.

Recently, IronPort Systems sponsored a report entitled, *Data Loss Prevention Best Practices*. With recommendations and discussion of technology solutions, this report outlines DLP strategies to help organizations take control and prevent data loss – before it's too late.

Free copies of this report are available at: [www.ironport.com/dlpbooklet](http://www.ironport.com/dlpbooklet)



> *continued on page 2*

### in the next issue

**2008: The Year of Web-based Threats** Spam, viruses, phishing, Trojans and malware have blended together, with one attack being used to propagate the platform to deliver another. Just as no organization today would consider running their email systems without multiple layers of defense, the Web Security Report explores how Web infrastructure must be similarly secured.

Regular features include: Web Security News, Company Spotlight and Sponsor Profile.

SPONSORED BY  
IRONPORT SYSTEMS



of trade secrets, alienation of strategic customers, reductions in company stock price, and legal action – can often be extreme.

The overall scope of the data loss problem has been framed in several different ways. The United States Trade Representative (USTR) reported in 2006 that U.S. businesses are losing approximately \$250 billion annually from trade secret theft, while the FBI estimated that the cost of all data breaches in 2006 to U.S. companies totaled \$62.7 billion.

Based on public reporting figures required by data breach notification laws, the Privacy Rights Clearinghouse determined that, “Over 167 million data records of U.S. residents have been exposed due to security breaches since January 2005.” According

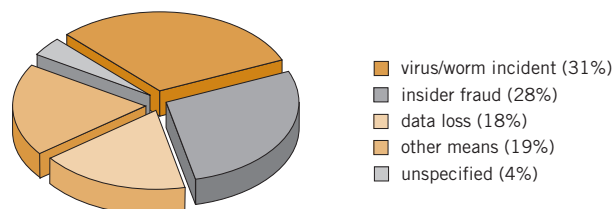
“The average information leak costs organizations approximately \$182 per record, averaging roughly \$4,800,000 per breach in total.”

*The Ponemon Institute*

to the Ponemon Institute, a research consortium dedicated to advancing privacy and data protection practices, “the average information leak costs organizations approximately \$182 per record, averaging roughly \$4,800,000 per breach in total.”

Even a casual glance at one list of data breaches, maintained at Attrition.org (<http://attrition.org/dataloss/>), shows that losses have reached epidemic proportions. And *Deloitte's 2006 Global Security Survey* reported that 49 percent of companies have experienced an internal security breach in the past year.

Unfortunately, getting a handle on the problem inside any particular organization is difficult because most companies don't know what is at risk. *The State of Information Security 2007*, a worldwide study by CIO, CSO and PricewaterhouseCoopers, notes that, “Only one-third (33 percent) of respondents keep an accurate inventory of user data or the locations and jurisdictions where data is stored. Similarly, only one-quarter (24 percent) keep inventory of all third parties using customer data.”



Nearly half of all companies surveyed have experienced an internal security breach in the past year.

(Source: *Deloitte's 2006 Global Security Survey*)

Moreover, many currently-available solutions don't address the most common problems. Instead, the majority of commercial offerings are built around threat models appropriate to movie plots, but without much relevance to how data is actually lost. An old-time security mindset (which holds that any solution not completely secure against any form of malice is worthless) still dominates inside many companies, and some vendors have obliged by offering solutions that are supposed to provide total control over corporate data.

That is not to say the threat of malicious insiders is unreal. But effective data loss prevention is about risk mitigation, not about unbreakable control of corporate data. The cause of data loss is often accidental. According to *IDC's Enterprise Security Survey*, “employee error is now the fourth largest security concern in the enterprise – behind malware, spyware and spam.”

The good news is that there are easy, effective solutions that can be implemented today to a variety of data loss problems. To do so requires separating out the various aspects of data loss.

## Understanding the Problems of Data Loss

While there are many ways of thinking about data loss prevention (DLP), there are two high level approaches that seem particularly useful. The first is to focus on the qualities of the data at risk; the second is to focus on the business objectives in the data loss prevention program.

## Data at Risk

For the purposes of security analysis, data is often categorized as 'at rest', 'in motion', and 'at the endpoints'.

- **Data at rest** is typically stored on disks in central facilities, in file systems and databases, and is not in continuous use. It may be accessible in various ways, and loss or leakage is likely to occur primarily as a result of intrusion – but it may also become public as a result of legal proceedings. Protection of data at rest has historically been a matter of good access control, though increasingly it has also involved protection from malware.
- **Data in motion** flows through the network, particularly to points outside the organization. Examples include email, instant messaging (IM), voice over IP (VoIP), and peer-to-peer (P2P) traffic. It may be lost to interception, and protected by encryption.
- **Data at the endpoints** is stored more or less temporarily by portable means such as laptops, cell phones, USB and other external drives, MP3 players, and other mobile devices. Data at the endpoints is at risk of loss or theft, and may be protected by encryption, or systems that use network connections to control access.

This framework may also be interwoven with the concept of an information life-cycle of creation, distribution, storage and eventual destruction. Evaluating how data moves through the life-cycle (and how each stage involves different moments of being at rest, in motion and at the end points) can illuminate the risks of data loss, and differentiate between possible solutions.

For example, a patient record may be at rest for years, then put in motion (in response to a physician's request) and land on one of the endpoints of the network. It may be lost via intrusion, misdirected email, interception, or laptop theft. Each of these potential losses requires a different technical approach.

The data at rest/data in motion/data at the endpoints framework is useful because it makes it possible to consider different threat models and different types of technical solutions. For example, accidental loss of data in motion through misdirected email requires a different solution than loss of data at rest to an intruder or malicious insider.

## Business Objectives

Three primary business needs – regulatory compliance, intellectual property protection and acceptable use policy enforcement – are driving the market for data loss prevention.

"All three areas are related but separate," says Nilesh Bhandari, product manager of the email security appliance platform at IronPort Systems (a Cisco business unit). "Though we are seeing more integrated solutions become available, it helps to consider each one separately.

Regulatory compliance is an issue for organizations of almost any size – largely because of the complex array of laws governing the collection and use of customer data and personally-identifiable information that could potentially be used to identify, contact, locate or impersonate an individual consumer, employee, student, patient, or taxpayer.

For example, California's SB 1386 requires businesses to report losses of personal data to their customers, and it applies to all companies with customers in California. More than 30 other states have passed similar data breach notification laws that require businesses to report when data has been lost.

In addition to data breach notification laws, there are the laws specific to particular industries or types of companies, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLB), Sarbanes-Oxley (SOX) and the European Union Data Protection Directive. There are also standards such as the Payment Card Industry Data Security Standard (PCI DSS) that contractually govern handling of corporate data.

————— > *continued on page 4*

Taken together, the regulations governing the collection, use, sharing, and disposal of data at rest, data in motion, and data at the endpoints can transform simple and routine actions into potential civil liabilities, and even criminal actions. Messages forwarded beyond the intended set of recipients, or containing unencrypted credit card information or patient records may be common, but it only takes one slip to create major damage.

Ensuring that an organization's intellectual property is protected is another key function of data loss prevention programs. Trade secrets, merger and acquisition discussions, and other confidential materials (such as salary data, personnel decisions and notes on negotiations with business partners) need to be simultaneously available to those who need them, and locked away from those who don't.

The list of damaging and embarrassing leaks of confidential corporate data is growing longer every day. The common scenarios – price lists sent to incorrect addresses or forwarded to competitors, product plans leaked to the media, or proprietary information sent to

...companies are paying closer attention to ensuring that inadvertent or malicious forwarding of email containing sensitive data is brought under control, usually through a combination of content scanning and encryption.

webmail accounts by employees in the process of leaving – are all too familiar to readers of the business press. But, in the meantime, companies are paying closer attention

to ensuring that inadvertent or malicious forwarding of email containing sensitive data is brought under control, usually through a combination of content scanning and encryption.

Finally, there is the issue of creating, maintaining and monitoring acceptable or appropriate use policies for corporate data and information systems. While early appropriate use policies tended to focus on limiting liability, reducing time-wasting activities (e.g. limiting personal Internet use, access to webmail, or entertainment sites), and filtering content that could lead to lawsuits by employees (e.g. pornography, as

well as sexist, racist, or homophobic jokes), policies today are more complex, and rely on sophisticated rule sets intended to limit data loss. For example, it is common to automatically encrypt all mail sent to a corporate board, or containing social security numbers. Such rules are policy decisions, and the art is to create policies that improve security without slowing down or inconveniencing legitimate work. That makes selecting the right tools to support complex polices a critical task for CTOs, CIOs and other senior managers.

## Requirements for Effective DLP Solutions

Given the broad range of problems and business objectives related to data loss prevention, defining the needs of a given organization is a challenging and complex exercise. One approach is to separate the managerial, legal, and technical requirements that relate to compliance, intellectual property protection and use policies.

### Managerial and Legal Needs

Reporting should be at the top of nearly any list. No DLP solution can be effective unless it can provide detailed reports of all suspected violations. These reports should reveal patterns of behavior that can be acted on – for example, by adjusting corporate policies, focusing user education efforts and determining new rules to be enforced by the DLP solution. Reports should include details about message senders, intended recipients, message contents, attachments, policy violation and information about the violating content. Additionally, in the unfortunate case that a data breach occurs, the system must be able to quickly produce a report that will allow compliance with data breach notification laws.

“For the first time, managers have access to new levels of reporting based on fine grained scanning, and that can give them a real picture of their environment,” says IronPort's Bhandari. “Reporting makes it possible to see which users may be at risk, which types of content need more careful controls and

## DLP in Medical Environments

As part of a heavily-regulated industry, as custodians of some of the most sensitive data about individuals, and as organizations that must exchange vast quantities of information with outside organizations, health care organizations tend to be at the forefront of data loss prevention.

“To address the data loss problem, health care organizations should focus on content filtering and blocking of electronic communications leaving their networks, and not just email, but instant messaging, webmail, HTTP and FTP communications as well,” explains Bradley Hunter, director of technology solutions for the American Hospital Association Solutions, Inc. in Chicago, IL. “Across all key protocols, a high-performance, intelligent data loss prevention solution is important for health care organizations, and all other companies as well.”

The real challenge for most hospitals comes from meeting the complex array of use policies and regulatory requirements governing data. The comprehensive DLP solution to prevent confidential data loss in health care environments must:

- Monitor communications going outside of the organization
- Encrypt email containing confidential patient records and financial information
- Enable compliance with global healthcare data management mandates (e.g. HIPAA)
- Secure outsourcing and partner communications (e.g. with insurance companies)
- Protect intellectual property
- Prevent malware-related data harvesting
- Enforce acceptable use policies
- Enforce messaging policy (attachment size, no personal email, etc.)
- Add legal disclaimers to outgoing emails
- Deter malicious users (by creating the possibility of being caught)

There may also be upper-management apprehension about preventing embarrassing accidental disclosures of confidential data, providing support for partners' secure communications requirements, as well as liability concerns.

which recipients outside the organization may cause problems. For example, it's possible to note which email messages contain credit card or Social Security numbers, or which Microsoft Office documents have the word 'confidential' in the footer.”

Also near the top of the list should be transparency to end-users, who should not (typically) need to change the way they read, write, or send email. Ensuring that that is a minimal impact on work is the only way to be confident that the system will actually be used.

“Solutions to date have forced trade offs between security and convenience,” Bhandari continues.

“Employees will route around inconvenient systems to get their jobs done. To be effective, DLP systems must not interfere with legitimate work – yet support corporate policies.”

**“Employees will route around inconvenient systems to get their jobs done. To be effective, DLP systems must not interfere with legitimate work – yet support corporate policies.”**

*Nilesh Bhandari, IronPort Systems*

While some legal requirements are nearly universal (e.g. any data loss prevention system should enable compliance with data breach notification laws), many others are specific to particular industries and organizations. Consequently, defining the legal requirements for DLP must involve not just the IT department, but typically legal and accounting departments as well.

Companies on the verge of purchasing a DLP solution should check to see if their prospective vendor has template policies that match existing legal needs, and if these templates can be easily adjusted. A good clue is whether other companies in the same industry have adopted the solution.

Ultimately, any system must be able to flexibly adapt to support a wide and changing set of policies as circumstances, regulations, business partners and technical systems evolve. That means having an effective set of rule definitions, and an easy way of changing them.

### Technical Requirements, Content Scanning and Encryption

Again, there is no one-size-fits-all set of technical requirements, but for most companies, a few issues are critical.

—> *continued on page 6*

The first is effectiveness, not just in halting outbound leakage of sensitive data, but also in avoiding false positives – that is, preventing legitimate messages from leaving the enterprise.

Another necessity is support for other communications channels (data in motion) such as instant messaging, FTP, peer-to-peer, and data at the end points, especially on laptops and other portable storage devices. “Email is still the number one source of outbound leaks, whether those are intentional or accidental, but other media are also a problem,” notes Bhandari. “Laptop theft has been responsible for some of the worst data breaches involving customer and patient records.”

A third requirement that is becoming increasingly important is the ability to interoperate with the DLP systems at partners and customers. Though standards are still emerging, it’s important that the burden of DLP doesn’t fall too heavily on those outside the company. “It’s clear that dedicated DLP vendors will need to interoperate,” Bhandari adds.

Technical requirements are often inseparable from technical possibilities, so it’s worth taking a somewhat deeper look at new approaches to content scanning and encryption.

Content monitoring tools examine outbound traffic, scanning for and detecting sensitive data, and then based on corporate policies, automatically block or encrypt the traffic. For this to be acceptable, both high accuracy and high performance are essential. Without high accuracy, data that should not go through, may, and data that should, may not. Policies that are too restrictive prevent users from working effectively, and drive them to use alternatives (such as free webmail services).

Over the last several years, content scanning technologies have improved dramatically, offering

much better visibility into outbound messages, and particularly into attachments. As a result, the options for policy enforcement have expanded. Based on the results of content scans, DLP systems can drop, bounce, alter, archive, or encrypt a message, generate a notification, and/or blind carbon-copy the message to an archive or compliance officer. These content scanning options can also be applied to other channels such as IM, FTP, and peer-to-peer.

“There are two key capabilities required for content filtering: high performance and the ability to accurately scan nearly anything,” explains Bradley Hunter, director of technology solutions, for the American Hospital Association Solutions, Inc. “High performance is important, because anything short of line speed introduces a noticeable delay for end-users – while detection accuracy and the ability to define granular policies are what content scanning tools require to both avoid letting leaks through and generating too many false positives.”

In addition, content scanning systems have become much more tightly integrated with Lightweight Directory Access Protocol (LDAP) directory services, allowing selective application of particular rules. For example, by integrating content scanning with LDAP directories, it is possible to set policies like ‘encrypt email sent by the financial officers to business partners or to the board’, ‘append disclaimers to all outgoing emails sent by the legal department’, or ‘archive messages containing Social Security numbers sent by HR’.

At the same time, the encryption technology fundamental to DLP has improved, primarily by becoming more much transparent to end-users, and much easier to manage for system administrators. Improvements in ease of use have come through tighter integration with mail systems, and a move away from more complex public key infrastructure (which has also lightened administrative burdens). As result, modern encryption systems require no special client software, and no pre-enrollment to receive messages.

Though standards are still emerging, it's important that the burden of DLP doesn't fall too heavily on those outside the company.

“Encryption is a fundamental piece of the data loss prevention puzzle. IronPort’s encryption technology (which was strengthened by our acquisition of PostX earlier this year) is special because it is easy and transparent to both sender and recipient,” states Bhandari.

For buyers of DLP systems, the crucial point is that encryption systems used for DLP should not add extra steps in the composition of messages, or inhibit intended recipients from reading their mail.

## DLP, Culture and Management – Implementing Solutions

Implementation of DLP solutions involves changes to corporate processes, engagement with different stakeholders, and sometimes even cultural changes within an organization.

For starters, businesses new to DLP will need to first identify the types of information that are most at risk. These may be core assets (like the formula for Coca-Cola), business data (like price lists), and third-party data (like patient records). The next step is determining who should have access to that information. Often, it turns out that information is more accessible than it needs to be, or that it is possible to restrict information access (based on business functions, group membership, or job roles), or that external partners have special needs that must be taken into account.

Having identified sensitive information, and the users of that information, organizations can then examine how that information is stored (at rest), transmitted (in motion), and used (at the end points). While improving the email system often offers the quickest and greatest payoff, regulatory requirements – and good business sense – require that other channels also be kept in mind during the analysis. These might include instant messaging, file transfer (particularly services that bypass the firewall by using Port 80), printing and portable storage devices.

Getting a sense of these realities – what information is sensitive, who has access to it and how it is typically transmitted – is far from trivial. But it is fundamental to the creation of meaningful corporate information policies, which must also take account of regulatory requirements and strategies to minimize risks of litigation. Given the breadth of choices supported by modern DLP solutions, expect the (re)design of information policies to take some time. Though many DLP solutions provide policy templates, some customization is likely to be required, and that will involve discussions with many different stakeholders within the organization.

## Conclusion

Ultimately, data loss prevention is about risk mitigation, and that means understanding what the true threats and typical patterns of loss really are.

Bhandari sums up, “The reality is that the vast majority of data losses are accidental. Our solutions prevent that from occurring, and do it in a simple way – which is critical because an environment that is too locked down can prevent a business from growing.”

The answer, it seems, is to implement policies that strike the right balance between openness and control – using security technologies that provide deep management insight into the environment, high performance and reliability, and yet remain transparent to end-users. ■

### About the Author

Jeff Ubois is a technology analyst specializing in collaboration and archiving technology. He is the former editor of the Messaging News website and co-founded Omniva Policy Systems, an early DLP vendor purchased by Liquid Machines. His writing has been published in First Monday, Release 1.0, Computerworld, and the publications of Ferris Research – a San Francisco-based consultancy specializing in messaging and collaboration.

## Spyware Purveyor Closes Doors

DirectRevenue, a company that made tens of millions of dollars pushing ads onto compromised computers, closed down this week – nearly four months after the Federal Trade Commission (FTC) levied a \$1.5 million fine against the firm. The light shed on the operations of Direct Revenue and other spyware and adware firms gave security researchers enough data to estimate that each consumer infected by the software nets a firm nearly \$3 in revenue per year.

According to a message posted to its website, DirectRevenue and its subsidiary Best Offers “have ceased operations.” The company left behind a single page of instructions to allow victims to uninstall its software and an email address, which appeared to be invalid. The company gave no reason for its closure.

More information on this story is available at: <http://www.securityfocus.com/brief/615>

## Trojan Targets Skype

Security analysts are warning of another malicious software program masquerading as an installer file for Skype. A password-stealing Trojan is targeting the popular, eBay-owned VoIP (Voice over Internet Protocol) and IM service – posing as a security plug-in and displaying a fake log-in screen that’s almost identical to the real thing. Skype is frequently targeted by malware writers because it is so widely used. Other attacks have focused on sending links to malware, via the program’s chat function, as well as worms. Those who worry about network security tend to dislike

Skype due to the service’s ability to embed things into a protocol, its disruption of calling services and the fact that it uses supernodes. It is also said that Skype’s encryption makes it difficult to determine what malware it is allowing onto an enterprise network. Skype is recommending that users update their anti-virus detections to avoid infection.

To learn more, visit: <http://www.eweek.com/article2/0,1895,2200670,00.asp>

## Privacy Groups Call for Web Tracking Opt Out

A coalition of nine privacy and consumer groups have proposed a “do-not-track list” that would allow consumers to opt out of advertising efforts that track their online movements. The groups, including the Center for Democracy and Technology (CDT), the Consumer Federation of America and the Privacy Rights Clearinghouse, called for the Federal Trade Commission to create a list of servers that track users online. Consumers could then download the list, and use security software, to block sites that they don’t want tracking them. Similar in some ways to the do-not-call telemarketing list (currently maintained by

the FTC), this new list would allow consumers to take control of their personal information online. While they would originally have to download the list and manually enter sites to block into security software, the privacy coalition expects that browser developers would create tools to automate that process.

The full proposal can be viewed at: [http://www.worldprivacyforum.org/pdf/ConsumerProtections\\_FTC\\_ConsensusDoc\\_Final\\_s.pdf](http://www.worldprivacyforum.org/pdf/ConsumerProtections_FTC_ConsensusDoc_Final_s.pdf)

## Phish Fighters Floored by DDoS Assault

Castlecops, the volunteer security community that runs a well-known phishing website investigation service, has been hit by a distributed denial of service (DDoS) attack. Founded five years ago, CastleCops is best known for its Phish Incident Reporting and Termination (PIRT) taskforce. Surfers are able to report fraudulent sites to Castlecops volunteers, who investigate these reports. Castlecops volunteers do the leg work and carry out the sometimes tricky process of having bogus sites removed from the

Internet. The organization also assists in educating users about malware risks. The motives of the attack are unclear, though it's reasonable to assume that phishing fraudsters or malware authors (who have most to gain from the unavailability of Castecop's website) are the likely perpetrators.

Additional details can be found at: [http://www.theregister.co.uk/2007/02/20/castlecops\\_ddos/](http://www.theregister.co.uk/2007/02/20/castlecops_ddos/)

## The Web has an Evil Side

It's getting harder to know who to trust on the Web, according to online safety advocates StopBadware.org. Recently, the group released its *2007 Trends in Badware* report, saying the bad guys are finding new ways to place their malicious software on our computers. StopBadware maintains a list of 200,000 websites that are known to be associated with malicious downloads. More than half of these sites have been hacked and don't even realize it. This move to delivering malicious software on legitimate sites has been a disturbing trend over the past year.

So, with all this badware, is the Internet a more dangerous place to be? Max Weinstein, a project manager with StopBadware believes things are getting better. "I think the bad guys are always trying to stay a step ahead of the average users," he said. However, "people are learning, and I think that is having an effect."

The complete report is available at: <http://www.stopbadware.org/home/consumerreport>

## company spotlight

### Orchestra Corporation

Can you prevent the loss of significant, confidential data within your company? You can, if you use Orchestra. The company helps organizations eliminate the risks in uncontrolled electronic actions by securing confidential data, ensuring message compliance, instituting proper legal hold and ensuring robust records management. Orchestra's



software layers in monitoring, detection and policy enforcement provide control mechanisms – enforcing rules on access to proprietary data and intellectual property. Founded in 2000, Orchestra is headquartered in New York with additional sales offices in Boston, London and Toronto. [www.orchestria.com](http://www.orchestria.com)

**IRONPORT SYSTEMS, a Cisco business unit, is a leading provider of enterprise spam, virus and spyware protection. IronPort offers an excellent example of a data loss prevention (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 delivers 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'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.



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

### 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 as 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.

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



### Iron Port Email and Web Security Appliances

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

Get started on your DLP plan with IronPort technology.

### 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.

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.

### The IronPort Advantage

IronPort email and Web security appliances are in production at more than half of Fortune 100 companies and eight of the ten largest ISPs. IronPort simplifies data loss prevention with an integrated, inline solution to ensure regulatory compliance, protect intellectual property, enforce acceptable use policies and more. IronPort's industry-leading systems vastly improve the administration of corporate infrastructure, reduce the burden on technical staff and have a demonstrated record of unparalleled performance, accuracy and reliability.

To secure greater protection for your company's Web or email messaging system, visit [www.ironport.com/dlp](http://www.ironport.com/dlp) or call 650-989-6530.

IronPort is now  
part of Cisco.



[www.ironport.com](http://www.ironport.com)

**PAGE 1 Reinventing Data Loss Prevention**

Organizations are losing confidential data and intellectual property. Whether data loss happens accidentally, or as a result of malicious activity, the effect on the organization can be severe. With discussion of technology solutions and best practices, the Web Security Report outlines DLP strategies to help round out a successful risk management portfolio.

**PAGE 8 Web Security News**

Your source for short takes on Web security tales, tools, tips and trends.

**PAGE 10 Sponsor Profile**

Web Security Report sponsor, IronPort Systems, is developing revolutionary technologies to help make the Internet safe.

### THE WEB SECURITY REPORT

A Messaging Media Publication

#### BUSINESS OFFICES

Messaging Media, LLC  
10536 Putney Road  
Los Angeles, CA 90064  
Phone: 866-808-4200  
Fax: 310-836-4067

#### ADVERTISING/SPONSORSHIP INFORMATION

Managing Partner: Tim Matteson  
publish@websecurityreport.com  
866-808-4200 (ext. 361)

the Web Security report

Messaging Media, LLC  
10536 Putney Road  
Los Angeles, CA 90064