CLEARSWIFT

Protecting against the leading causes of data breach

With content-aware gateway security

With the trend of large scale data breaches continuing, a 2008 Clearswift survey of over 1,000 IT and security professionals found that 94% of those polled agreed their data loss incentives was viewed as “important”, “very important” or “imperative” to their organization. Yet, the same poll found that since the introduction of data protection standards, 57.2 % of organizations could only increase their annual IT budget by a mere 10% or less to accommodate the demands of Data Loss Prevention (DLP). This whitepaper demonstrates how organizations can prevent the four leading causes of data breach.

Table of contents

Executive summary.

Odds are its happening right now. The confidential data that runs your business is hemorrhaging outside your organization and could be just minutes away from getting into the wrong hands.

Data leakage happens every day when confidential business information – customer or patient data, source code or design specifications, price lists, intellectual property and trade secrets, and forecasts and budgets in spreadsheets – leaves your company unprotected and goes outside the jurisdiction of your corporation. This uncontrolled data leakage puts your business in a vulnerable position. Once this data is no longer within your domain, your company is at serious risk. When cybercriminals "cash out" or sell this data for profit it costs your organization money, damages your competitive advantage, brand, reputation and destroys customer trust.

According to the Privacy Rights Clearinghouse, more than 234 million records have been compromised since 2005[1]. And, if you think that number sounds high consider this. A separate independent study conducted over a four year period touching 500 forensic investigations of companies who experienced data breach - a quarter of them publicly disclosed and the rest undisclosed- found more than 230 million compromised records[2]. We may only be witnessing the tip of the iceberg. Regardless of the number of records compromised, there is no doubting that data leakage is a serious threat to organizations – both large and small. A 2008 Clearswift survey found that 94% of those polled agreed that data loss was "important", "very important" or "imperative" to their organization.

But figuring out what to do to protect the organization has not always been simple or clear cut. Every day an organization postpones their decision to deploy data breach prevention strategy, they remain open to unnecessary and considerable compliance risks. The majority of organizations, those that must comply with the Payment Card Industry's Data Security Standard (PCI DSS) or the Healthcare Insurance Portability and Privacy Act (HIPPA), don't have the luxury of waiting. They need solutions to stop data loss today.

The recent data loss crisis we are experiencing is not because data loss is deemed unimportant to the organizations under attack; it is because many companies have been slow to adopt DLP solutions because they have been too expensive. In the Clearswift survey, 57.2 % of organizations revealed they could only increase their annual IT budget by a mere 10% or less to accommodate the demands of data protection standards. With DLP has been products ranging anywhere from a couple of hundred thousand dollars to millions of dollars, this option is not an affordable reality for most organizations who are under attack today.

This whitepaper was written for the organization that wants to focus on prevention of data loss and doesn't have millions to spend, but needs affordable solutions that can be implemented today to protect millions of sensitive records and dollars worth of intellectual property.

This whitepaper addresses:

- What organizations can do to prevent the four leading causes of data breaches.
- Why pure-play DLP solutions may not protect you from all four leading causes of data breaches.
- How to get prevent sensitive data leaving your organization with real-life case studies from companies who deployed a DLP strategy but didn't use a pure-play DLP product. Instead these organizations created DLP enforcement policies at the Clearswift content-aware gateway to leverage their investment by enforcing preventative measures where the majority of breaches occur.

1 Privacy Rights Clearinghouse: http://www.privacyrights.org/

2 Verizon Business Risk Team, 2008 Data Breach Investigations Report: A study conducted by the Verizon Business RISK Team

DLP: an over-hyped, confusing market.

Estimated to grow to a $3.2B market by 2011[3], DLP as a technology has been overhyped and misunderstood. Propped up only by market hype around the recent string of privacy breaches, DLP solutions have done very little to protect organizations from the millions of dollars in lost business, negative publicity and compliance fines that come with data breaches.

Pure-play DLP solutions, offer three types of data protection:

- Data-at-rest solutions: enforcing policies against data sitting in storage repositories.
- Data-in-motion solutions: enforcing policies over the content moving over the network.
- Data-in-use solutions: enforcing policies on users to block sensitive data from being misused on the desktop or transferred to USB devices.

Most DLP vendors struggle to offer solutions across all three areas and excel in only one area – either data in motion or data in use. Covering all three points is a multiple product sale that carries a lofty price tag – an expense that is unreasonable for most organizations at risk to afford. The majority of DLP companies are less than five years old and their products are even younger. Even though they may be on version seven or eight of their product it is not uncommon for the product to be less than that in real deployment years making it even more difficult to justify the expense. Regardless of the hype, organizations are at risk today and don't have the time to wait for DLP vendors' roadmaps to become reality or for a budget cycle to open. They need inexpensive solutions that can be applied today that leverage the existing security infrastructure and carry the most impact. To protect your organization, we suggest a different approach entirely. Instead of looking for the solution that covers the three data leakage points described by vendors, we suggested protecting your organization from the four leading causes of data breach happening today and being reported in the news. They include:

1 Accidental disclosure of information through the e-mail or Web gateway.

2 Large scale breaches caused by malware created by cyber criminals whose main intent is to steal data. Overwhelmingly they are using the Web gateway to distribute their malware and attack the client through the browser; not infected emails.

3 Large scale data breaches caused by hackers who look for a backdoor to steal valuable data from the corporate vault that can be sold on the black market.

4 Large scale data breaches caused by trusted insiders who profit by selling confidential or sensitive data to people on the outside. Most are opportunistic and not necessarily technically savvy and often try to sneak data out through the quickest and easiest method available. Its' estimate 80% of privacy data is leaked through the Web and e-mail gateway.

3 IDC May 2007, Information Protection and Control

Anatomy of a data breach: the four leading causes.

Until recently, corporations had more control over their data. The majority of enterprise content was locked under the controlled security of corporate applications and databases. Today, however, this data has been unleashed. Over eighty percent of content is unstructured – distributed in e-mails or webmail or stored as spreadsheets and confidential information sitting in database and application, file or SharePoint servers. This unstructured content travels freely into, within and outside most corporate entities unchecked.

The mobility of data increases the likelihood of data breaches delivering a serious or fatal blow to businesses. Consider some of the more newsworthy breaches that have been reported in recent years:

- 42 million credit and debit cards are leaked from a large retailer causing noncompliance with PCI DSS and costing the organization $256 million[4] and $130 million in settlement claims with banks and afflicted customers[5]
- 4.2 million credit and debit cards are leaked from a supermarket chain after malware is installed on more than 300 servers causing more than 1,800 reported cases of identity theft.
- A US software company's source code and design documents were stolen from an overseas R&D center.
- A hospital employee accidentally sent a list containing 4,500 AIDS patients and 2,000 HIV Positive patients putting patient privacy at risk and causing the hospital to be non-compliant with HIPAA.
- A Japanese nuclear power plant leaked sensitive information from virus-infected computers putting its citizens at risk.
- A British government agency exposed records of 25 million citizens.
- An international identity thief earns over $11 million in two years from cashing in on his trade of credit cards stolen from a number of US department stores.

[4] Ross Kerber, Cost of Data Breach at TJX Soars to $256m, Boston Globe, Aug. 15, 2007, available at: http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/

[5] Brad Stone, Global Trail of an Online Crime Ring, New York Times, Aug. 12, 2008 available at: http://www.nytimes.com/2008/08/12/technology/12therft.html

The first leading cause: accidental disclosure

We've all done it - accidentally hit the send button on an e-mail going to the wrong person. Quickly hit the forward button of an e-mail that had sensitive information buried below in a previous e-mail – information you didn't want the recipient to see. What about the employee with too much to do and not enough time? Chances are they are forwarding information to home computers to access confidential work data at home or on the road. In the process of doing business, employees make mistakes but when those mistakes involve confidential data or Personally Identifiable Information (PII), the results can be deadly.

How is your organization protecting itself from the following common mistakes?

- Someone in your sales organization accidentally e-mails the wrong price list – now the customer sees that their pricing is higher than their competitor's.

- An engineer at a R&D firm accidentally e-mails competitive intellectual property of one client to their competitor potentially compromising trade secrets.

- Someone in finance forwards PCI information buried in an e-mail to a third party supplier who should not see credit card and account data.

- An employee going on vacation wants to catch up on work over their break. They forward sensitive data using their free, personal webmail provider so they can access this data from their home computer or during their travel at a relative's house.

Because everybody makes mistakes and because not all employees understand disclosure policies, organizations are turning to Clearswift to prevent accidental disclosure at their content aware gateway by applying granular, content-aware policies for both the Web and e-mail gateways from one centralized policy management console. If you organization has not implemented enforcement policies at the gateway, your business is needlessly at risk from one of the most common forms of data breach.

Preventing accidental disclosure with the 3 E's

For many organizations, getting a handle around the prevention of accidental disclosure seems daunting. Clearswift has established a best practice that has been used to help many organizations – large and small - prevent accidental disclosure around the 3 E's:

1. Establish a policy.

2. Educate employees.

3. Enforce with policies at the content-aware gateway.

Step One: Establish a policy

Most organizations begin by establishing a few policies around the information they want to protect. In this phase, you will want to answer the following questions:

- What information do you want to protect?
- How should it be handled (sent through encryption server, sent in clear text...)?
- Who should not be permitted to receive (competitors, parts of the organization that are protected by "china walls")?
- How can the data be defined?

Step Two: Educate Employees

Once the policy is created, employees should be notified and educated. You should outline what data is to be protected, specifically where the data should not go and what will happen to them if the policy is violated. Also inform employees why not following policies subjects the organization to unnecessary risks. Your employees read the newspaper too. They understand the negative publicity of data breaches. The more they understand they are being part of the solution, the more likely they are to conform to policies. And remember, behavior modification takes time. Be prepared to repeat policies updates to employee frequently. Here, you can't over communicate enough.

Preventing accidental data breaches at the content-aware gateway: a case study.

A local police department in the United Kingdom must protect internal documents used in investigations. To prevent the accidental disclosure of this information getting out into the public domain, Clearswift was able to add a secret tag on all internal documents and prevent these documents from being sent outside the gateway – whether sent in e-mail, Web, or posted to a blog or Web server – accurately without interrupting the business.

Step Three: Enforce policies violations at the content-aware gateway

Once you have specifically defined what you want to protect and where the data should not go, it's time to define what enforcement action you want to take when a policy violation is detected. With Clearswift you can take a variety of action and you do not need to integrate with a DLP product to enforce actions.

With Clearswift you can take the following enforcement actions:

- Monitor for violations; archive and send to business manager
- Block by re-route back to employee
- Quarantine the e-mail for forensic review
- Block if going through a Web channel
- And more....

The most successful organizations are those that focus on the specific data they want to protect. They map out the scenarios they want to avoid. When you have sensitive data that must be protected and you can articulate where it should not go then you can easily implement these policies. Once the policy is defined on paper, organizations have created policy enforcement rules at the Clearswift content-aware gateway in less than 30 minutes.

The second leading cause: malware – the silent killer

The malware that will hurt your organization is no longer distributed by geeky adolescents trying to defame corporations. Malware is all grown up with a darkly emerging criminal component. The majority of malware being written today is after one thing – your corporation's valuable data.

A study by Verizon showed malware used to penetrate organizations was the contributing factor in nearly one-third of all data breaches under investigation[6]. Spyware, spam, phishing, viruses and malware are no longer written by fame seeking teenagers. This malware is going after valuable credit card, account data and passwords that is being stolen and traded on the underground by international criminals. And, it is not always attached in an e-mail. The new concern most organizations are not prepared for is the growing phenomenon of the "ghost in the browser" type of malware. A 2007 report found that 10 percent of the URLs surveyed (450,000 out of 4.5 million) contained malware that launched 'drive-by-downloads'[7]. This malware, once inside your organization, can sit silently for months, gather data and send out PII, credit card and account data to cyber criminals on the outside.

There would be little value in stealing credit and debit card or account data if a market for the stolen data did not exist. Unfortunately this underground is growing in size, scope and the speed with which criminals can flip this data for cash is surprisingly fast. Law enforcement agencies are seeing an increasing number of cybercriminals building this black market utilizing what can best be described as criminal social networking websites where they can anonymously buy, sell and trade stolen credit and debit card information as well as sell the tools – Trojans and malware – used to help leak this data. For the cyber criminal who can make up to $5.00 a card or up to $400 for bank account information, stealing data is a business[8]. And, for the cybercriminal who knows how to "cash in", utilizing this data can be worth millions. In July of 2007, the US Secret Service arrested Maksym Yastremskiy a 25 year old Ukrainian cybercriminal who managed to earn $11 million dollars in just two year for his effort in participating in an international online crime ring that is believed, cashed in on credit cards stolen from multiple US retailers including BJ Wholesale, Office Max, DSW and Barnes and Noble[9].

To this end, cybercriminals, aided by malware will continue to contribute to the largest scale data breaches to date. The cybercriminal organizations collecting and trafficking this data on their websites just gets bigger and better at cashing in. Take for instance one of the more infamous groups – the "Shadow crew" – known to traffic at least 1.5 million stolen credit card numbers resulting in $4 million in actual losses to credit card companies and financial institutions until law enforcement was able to shut them down in 2004[10]. In the wake of their demise, they were easily and eagerly replaced by an even larger cybercrime forum boasting over 20,000 members where "business is usual" - the buying and selling stolen credit card data and new malware programs – continued allowing the harvesting of data on bigger and grander scales[11].

Preventing accidental data breaches at the content-aware gateway: a case study.

A video distribution company that supplies rival supermarket chains with videos has applied policies at the Clearswift Content Aware gateway that prohibits the sales department to send price lists intended for one customer to accidentally be sent to a rival store. Anytime a price list is sent, the Clearswift Content Aware gateway makes sure the list is going to the right domain, otherwise the e-mail is blocked and re-routed to the send at the gateway.

To protect themselves, organizations need to have a protection strategy in place at the gateway. On the inbound side, organizations must prevent new types of malware, Trojans and viruses from entering through the Web gateway before they enter the corporation. On the outbound side, organizations must look for leaking credit card, debit card and account information in the event that malware finds a backdoor into the organization and can begin sending sensitive data out. Unlike the leading DLP product, the Clearswift content-aware gateway does both and can lock down the organization from malware entering through the inbound Web gateway with the same centralized policy management console that is also searching for accidental or malicious disclosure of privacy data through the e-mail gateway.

[6] Verizon Business Risk Team, 2008 Data Breach Investigations Report: A study conducted by the Verizon Business RISK Team

[7] Google, "The Ghost in the Browser Analysis of Web-based Malware" 8 Peretti, Kimberly Kiefer, Data Breaches: What the Underground World of "Carding" Reveals, Volume 25 Santa Clara Computer and High Technology Journal.

[9] Brad Stone, Global Trail of an Online Crime Ring, New York Times, Aug. 12, 2008 available at: http://www.nytimes.com/2008/08/12/technology/12therft.html 10 Peretti, Kimberly Kiefer, Data Breaches:

[10] What the Underground World of "Carding" Reveals, Volume 25 Santa Clara Computer and High Technology Journal.

[11] Peretti, Kimberly Kiefer, Data Breaches: What the Underground World of "Carding" Reveals, Volume 25 Santa Clara Computer and High Technology Journal.

The third leading cause: "Inside Jobs"

The Brookings Institute estimates 80% of intellectual property is no longer represented as tangible products, but as intangible assets like source code, R&D strategies and engineering diagrams[12]. Sensitive data is no longer controlled under lock and key in datacenters or file cabinets. It's everywhere. To stay competitive, businesses have adopted Web and e-mail friendly cultures and business models allowing employees to transmit just about every type of sensitive corporate secret electronically, instantaneously. This accessibility means trusted employees have inside access to valuable data like account information and intellectual property. When the opportunity is there, it becomes more probable that trusted insiders cash in on this data either working or alone or with friends on the outside who are helpful in aiding large scale data breach attacks.

[12] Baruch Lev, Intangibles: Management, Measurement and Reporting, Brookings Institute, Washington DC.

The fourth leading cause: Hackers Incorporated.

It almost seems passé to talk about, but hacking into corporate networks is alive and well even though networks are much more fortressed than ever before causing hackers to look to lower hanging fruit like attacking PCs with key logging malware through browsers or working with insiders who can turn over credentials allowing hackers to gain easy access to the digital identities sitting in databases, servers and Point of Sale (PoS) devices.

Hacking into insecure wireless networks of popular US restaurants and department stores in Miami was the method by which hacker Albert Gonzalez stolen millions of credit card numbers. Gonzalez working with 10 other people in an international online crime ring, was able to harvest and store this credit and debit card data on servers in the Latvia and the Ukraine. Fake credit cards created with the stolen data and purchased from China was then able to allow the criminals to cash-out by withdrawing money from ATM machines. Taking many years, this group was the largest hacking and data theft case ever successfully investigated and prosecuted within the United States going well beyond US boundaries to arrest individuals in Eastern Europe and China[13]. When the damage is done, organizations don't have the luxury to wait years for law enforcement to track down and arrest hackers. Increasingly, these hackers are more difficult to find and is taking up more investigative resources. Organizations must learn to protect themselves. Here the best method of defense is to monitor for credit, debit and account data leaving the corporate network. For many organizations, there is never any reason for this data to leave unless it is going to designated, predefined partners in encrypted format. By monitoring and/or blocking this data at the Clearswift content-aware gateway, organizations can be protected from data breach and also gather the forensic data so desperately needed by law enforcement to gather evidence to convict cybercriminals and hackers.

[13] Brad Stone, Global Trail of an Online Crime Ring, New York Times, Aug. 12, 2008 available at: http://www.nytimes.com/2008/08/12/technology/12therft.html

Financial institution protects from data breach with content aware gateway: a case study.

To lock down credit card and bank account information, a financial services institution enacted an internal policy requiring this information to only be transmitted between specific third party processors through a Virtual Private Network (VPN). No credit card information was allowed to leave the financial institution. This allows the bank to monitor the outbound gateway block unauthorized PII, credit card information and bank account information protecting the organization from compliance violations and its customers from identity theft. To avoid a situation where malware leaks encrypted credit and debit card account information outside, the financial institution also blocks encrypted information that is not originated with the VPN from leaving the bank. This encrypted data is quarantined and forensically reviewed.

Data breach: 4.2 Million accounts compromised in malware attack at US grocery store.

In 2008, Boston-based Hannaford Brothers grocery store was the first victim to fall prey to a malware attack that leaked 4.2 million credit cards from each of the servers operating in roughly 300 stores.

What is a content-aware gateway?

If you are running e-mail and web with URL filtering, Anti-Virus, Malware or Spam protection in your organization, the chances are you have the early foundation of a content-aware gateway already in place. This gateway consists of two important products: your e-mail Mail Transfer Agent (MTA) and your Web proxy. The MTA applies policies against e-mail entering and leaving your organization. Most organizations MTAs have AV, AS, or Malware detection engines to prevent bad e-mails from entering the corporation. On the Web side, organizations have Web proxies that can terminate inappropriate Web sessions that violate your corporation policy such as surfing the Web, or trying to download inappropriate materials from Web servers.

What very few have, is the ability to tie these solutions together into a unified soliution for web and mail together with one set of centralized data loss prevention policies, combined, with a solution that also prevents malware.

The Clearswift content-aware solution ties both of these gateways together and conducts deep content analysis against data entering and leaving the corporation from one centralized policy console. It prevents the malware entering the organization and prevents inappropriate or sensitive information from leaving.

Clearswift – a company with 20 years of building proven content inspection and malware prevention Anti-Virus Spam and Malware products – provides the only content-aware solution at both gateways allowing organizations to apply one set of policy standards against both types of traffic from a centralized console.

Helping a leading department store chain complying with PCI DSS: a case study.

A retail chain of department stores based in the UK with less than 10,000 employees recently used Clearswift content monitoring to comply with PCI and protect credit and debit card information. The department store had been a long time user of Clearswift's inbound mail gateway product to protect the organizations from malware, spam, and viruses. With the growing concerns around the protection of PII and compliance with PCI, they began content filtering on the outbound gateway to ensure that under no circumstances would credit cards leave the organization (regardless of whether this information was contained in e-mail or over the Web). Within 30 minutes, the security team installed the PCI template and configured the appropriate policies for the department chain. Weeks later, the value of the solution proved itself when an e-mail with credit card and account data secretly embedded in a file, which was then embedded in two more files was accurately detected, quarantined and blocked. A forensic review of the information revealed the source of the insider attack allowing the department store chain from avoiding brand damage and negative publicity.

Solutions: pure-play DLP versus the Clearswift content-aware gateway.

When protecting your organization from the leading causes of data breach, most organizations consider deploying some type of content aware solution that can provide deep content analysis to identify “at risk” content and take the right enforcement actions to protect the organization. Here, many organizations think they need an expensive DLP product. However, applying a content aware strategy at the gateway without ever buying a DLP product is proving to be a more practical and affordable alternative for the large majority of organizations who need DLP products today. When it comes to protecting your organization from the four leading causes of data breach, both DLP solutions and the Clearswift content-aware gateway can:

- Accurately detect when confidential data is leaving the organization (data-in-motion)
- Provide important forensic information in the event of a data breach
- Create centralized policy management around the use of data leaving the organization
- Provide centralized dashboards to report on data usage trends and policy violations

But the Clearswift content-aware gateways actually goes one step further by:

- Preventing malware from coming through the e-mail and Web gateway (not available in pure-play DLP solutions)
- Preventing confidential data from leaving through the outbound gateway. (DLP solutions only attach message headers to e-mails in violation of policy, they don’t take actually take the enforcement action.)
- Preventing internal employees communicating within the Exchange environment where it is not appropriate (not available in pure-play DLP solutions)

CLEAR SWIFT

Table 1: The Clearswift content aware gateway and the leading pure-play DLP solution.

	Clearswift	Leading DLP Solution
Content Awareness and Policy Creation		
Granular policy management – ability to apply rules enterprise wide or department, region or individual.	YES	YES
Can apply policy enforcement around context (source, destination, size, recipients, sender, header, metadata, time, location, format) as well as content.	YES	YES
Provides deep content inspection based on rule-based/regular expression and lexical techniques that include check sums for credit cards.	YES	YES
Fingerprinting techniques for exact matching of structured content like database content and unstructured data like intellectual property.	YES	YES
Partial document matching where unstructured, sensitive data can be matched based on a series of overlapping hash values.	YES	YES
Statistical analysis – use of Bayesian analysis and machine learning to find policy violations in content that resembles the protected content.	YES	YES
Conceptual/Lexicon allowing combination of dictionaries, rules to protect content that can be defined by a situation like insider trading or inappropriate workplace behavior.	YES	YES
Conceptual/Lexicon allowing combination of dictionaries, rules to protect content that can be defined by a situation like insider trading or inappropriate workplace behavior.	YES	YES
Easy to use, intuitive management interface, rich clear reporting and workflow.	YES	YES
Seamless integration with Active Directory	YES	YES
Policy Enforcement – E-mail Outbound (prevent accidental and malicious attacks from insiders or hackers)		
Is a full-functioning MTA capable of preventing e-mail that fails a policy from leaving the organization.	YES	NO
Is a full-functioning MTA capable of applying policy on internal e-mail systems.	YES	NO
Policy Enforcement – Web Traf fic and Web 2.0 (prevents accidental and malicious attacks from insiders or hackers)		
Is a full functioning Web proxy capable of blocking sensitive content from leaving via webmail, IM or Web protocols.	YES	NO
Web 2.0 – protect sensitive data moving from or to SharePoint, Blogs or Wikis.	YES	NO
Is a full functioning Web proxy capable of reading encrypted SSL traffic.	YES	NO
Policy Enforcement – Malware (prevents attacks from malicious code at the Web or e-mail gateway)		
Anti-spam and malware integration.	YES	NO
Protection for Zero-day threats.	YES	NO
Anti-virus protection.	YES	NO
Policy Enforcement – Internal E-mail (prevents e-mails from being sent with disregard for internal compliance policies)		
Internal e-mail compliance policy enforcement on Exchange.	YES	NO
Policy Enforcement – Data at Rest (finds sensitive data stored within the enterprise)		
Desktops or clients.	NO	YES
Fileservers.	NO	YES
Fingerprints sensitive data.	YES	YES

Helping a US hospital comply with HIPAA: a case study .

Helping a US hospital comply with HIPAA: a case study . A leading hospital in the US evaluating spam solutions put the Clearswift appliance to the test. In addition to spam, it was discovered that the CIO was also struggling with outbound data compliance issues to protect sensitive patient information in accordance with HIPAA. The hospital CIO was unaware that one Clearswift appliance allowed them to do both. When the hospital conducted a 24 hour evaluation of their inbound and outbound gateways they received some disturbing news. Confidential patient information was leaving the hospital in e-mails being sent by two emergency room nurses. A forensic evaluation of the outbound e-mails sent by the nurses and the inbound e-mails received from their correspondents on the outside revealed they were sending patient PII information, insurance information and diagnoses to a local prominent attorney who paid the nurses for this valuable data. The attorney used this information to target former patients and file malpractice lawsuits against the hospital. The CIO was able to conduct an internal investigation and create the legally binding evidence to terminate the nurses and go after the law firm for damages. Future policies were designed to alert the CIO when confidential information was being sent out of the hospital. This policy was created in under 30 seconds and the hospital continues to use Clearswift content filtering to protect sensitive data from leaving as well as spam and malware from coming in for a fraction of what they thought they would have to spend on DLP solution.

DLP products – a redundant technology?

Unless they are running a full Web proxy and MTA inside, most "pure-play" DLP technologies are designed to provide passive network monitoring, not active enforcement. Content leaving the organization is run against a policy rule set to look for breaches of confidential or sensitive data. When policies fail, the data is flagged for action further in at the e-mail or Web gateway.

When violations are found in e-mail, this information is reported in the DLP centralized policy management and reporting console but enforcement actions – quarantine, block, encrypt, reroute, copy – are not conducted within the DLP solution. For enforcement to work, the DLP product reroutes outbound messages to an MTA or the Clearswift content-aware gateway for action. The DLP solution does not take the enforcement action – they enable it to happen further down the e-mail stream, but the action is taken by the MTA or Clearswift content-aware gateway.

When violations are found in Web traffic, the DLP solution sends an iCAP message to a Web proxy or the Clearswift content-aware Web Gateway. Again, the DLP product does not actually enforce policy but sends a message for content enforcement to take place later in the Web stream. While DLP products perform full packet capture and can reconstruct sessions in real time, they are not the enforcing agent (unless they are running a full proxy).

At the height of the data leakage hype curve, content reconstruction and passive monitoring was useful from the perspective of helping organizations understand where they were truly at risk. Unfortunately the products did nothing to protect the organization from preventing data breaches as the enforcement agent themselves. The data was already out the door. Ironically, the enforcement action that made DLP tools attractive to prevent data breaches is not being conducted by the DLP product, but by the preexisting products – MTAs and Web proxies - already in use on organizations' networks today.

Despite the hype, many organizations are realizing DLP products are a redundant technology because you can turn on the same data-in-motion DLP features plus protect the organization from incoming malware with the Clearswift content-aware gateway – a solution with a 20 year track record.

Conclusion

The question many organizations need to ask is why add pure-play DLP products as an extra hop in the e-mail stream when content-aware gateways like the Clearswift solutions already provide this functionality today with added malware protection. The Clearswift content-aware gateway simplifies content security. Clearwift's content-aware Gateway solution is designed to take the hassle and cost of DLP by securing your brand, reputation and preserving customer trust and a 20 year commitment to content security that has already helped 17,000 of the world's most successful and security conscious organizations in the world.

By centralizing policy management through one console that addresses the threats at both the Web and e-mail gateways as well as the internal e-mail system, you won't need to add expensive DLP products. The Clearswift content-aware gateway makes data-in-motion DLP solutions redundant, while reducing cost through consolidation of web and mail security, together with malware and data loss prevention, with solutions available for virtualization to further reduce cost.. This approach allows both large and small organizations achieve their data protection and compliance needs with a much more affordable, realistically deployable and price sensitive solution. Best, you are not giving any policy management customization or flexibility up when you go with the Clearswift content-aware solutions. Every customer has been able to take a customized approach to achieving their data protection needs quickly in minutes – not weeks as with the leading DLP solution.

CLEAR
SWIFT

Contact Clearswift

United States

Clearswift Corporation
161 Gaither Drive
Centerpointe Suite
101Mt. Laurel,
NJ 08054

Tel: +1 800 982 6109
Fax : +1 888-888-6884

Spain

Cerro de los Gamos 1,
Edif. 1
28224 Pozuelo de Alarcón,
Madrid

Tel: +34 91 7901219 / +34 91 7901220
Fax: +34 91 7901112

United Kingdom

1310 Waterside,
Arlington Business Park,
Theale,
Reading,
Berkshire, RG7 4SA

Tel: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Germany

Amsinckstrasse 67,
20097 Hamburg

Tel: +49 40 23 999 0
Fax: +49 40 23 999 100

Australia

Level 5, Suite 504,
165 Walker Street,
North Sydney,
New South Wales, 2060

Tel : +61 2 9424 1200
Fax : +61 2 9424 1201

Japan

Hanai Bldg. 7F, 1-2-9,
Shiba Kouen Minato-ku
Tokyo 105-0011

Tel : +81 (3) 5777 2248
Fax : +81 (3) 5777 2249