



Data Loss Prevention: Email and Web Gateway Best Practices

Abstract: This white paper explains some of the key concepts of data loss prevention (DLP), including the problems organizations encounter in implementing an effective DLP policy and how to alleviate them. The paper focuses on single-channel DLP at the email and Web gateways.

INTRODUCTION

Data is an important asset to every organization. With increasing reliance on electronic data transfer and storage as well as regulatory requirements, organizations strive to find the best ways in which to control access to sensitive information—for good reason. The independent website, <http://datalosdb.org/>, is updated all-too-frequently with reports of data loss incidents around the world. Each breach or loss can cost an organization up to US \$86 per record,² tarnish its reputation, and risk the consequences of non-compliance.

Data Loss Prevention tends to be split up into three categories: network, host-based and information identification.

Network-based DLP solutions usually provide a single-channeled approach to identifying and controlling data at one point on the network—either the email or internet gateways.

Host-based DLP solutions usually consist of an agent installed across all devices on a network and can be used to control access to hardware devices, such as memory sticks, and to the data itself.

Information identification usually refers to DLP products that use a number of technologies to identify and classify content across a network.

Data loss can occur at many levels within an organization:

- Outbound or internal emails can be sent to the wrong user by mistake. This is not uncommon given the “auto-completion of email addresses” feature present in many email clients, resulting in an accidental but potentially costly security breach.
- Web 2.0 sites make it easy to share information without thinking about the implications of posting sensitive data.
- Portable devices make it incredibly easy to remove data from a secure environment and lose it on the way home or to a meeting.

One of the major problems organizations face in implementing a DLP policy is the management of false positives. False positives occur when information is incorrectly identified as breaching policy. This can cause an important email to be blocked or denial of access to essential information. On the other hand, false negatives can be equally as serious, if not more so. False negatives can occur when sensitive information is not classified correctly and permitted to leave the secure environment. This is why many organizations spend a small fortune on DLP products, only to keep them in “monitor only” mode. The problem with “monitor only” mode is that by the time you detect a breach, it’s too late.

Another important problem, especially given the current economic climate, is that DLP solutions can be expensive, averaging approximately \$61 per user in 2007³. So organizations should identify what they want to protect and perform a risk analysis that compares the cost of data loss with the cost of protecting it.

IMPLEMENTING DLP

For the majority of organizations, DLP solutions can be simple to implement when using inexpensive, single-channel tools, but they should follow a few basic steps.

First, an organization must identify what information it is trying to control. For many, this will be dictated by industry regulations or local legislation. Other companies may wish to safeguard their own intellectual property. The ability to establish a core dictionary of key words, phrases or patterns is essential to an effective DLP policy. Whether it is credit card numbers, social security numbers, a list of medical complaints or financial terms, this information will be used to identify a potential data breach. Regular expressions, complex Boolean phrases, fingerprinting or even simple lists of words can be combined to great effect to identify content within traffic and permit remedial action.

However, this is often viewed as the most difficult aspect of establishing a DLP policy because it requires planning. Using gateway- or network-based tools to identify content within traffic can greatly diminish the size and scope of this task. Many organizations will need to identify and control data when it is moving around or leaving the corporate network, so initial monitoring of data-in-motion is the perfect place to start a DLP project.

Once an organization's managers and IT leaders identify the content they want to protect, they need to find ways to control it. Again, the simplest and most cost-effective manner of doing this is at the network or gateway level. Some of the more advanced email and Web gateway security products already provide this functionality—it just needs to be configured.

It helps to create content-filtering rules and apply them to groups and individuals, as required. Once sensitive content is identified, a number of actions can be taken, depending upon the content, the user, and in the case of email, the sender or the recipient.

Some examples of common DLP actions include:

Archive – the information is considered safe to access or to send but is archived for future analysis if required.

Block – access to the information is blocked or the email is not sent.

Quarantine – the identified data is held in a quarantine area for review. It can then be released, subject to inspection, or removed.

Monitor – information is identified and logged for reporting purposes. Commonly used at the beginning of a DLP project, this is used to identify trends in traffic or when data is not particularly sensitive. It can also be used to generate reports regarding permitted access to sensitive data to satisfy auditing requirements.

Alert/Notify – often used in conjunction with one of the other actions, alerts and notifications can be used to inform an administrator or data security officer about an attempted security breach. These attempts are often accidental, so notifications can help educate users about corporate policy regarding sensitive data.

Encrypt – in some cases, sharing the information is permitted, but only if the channel of communication or memory device is encrypted to avoid accidental loss or interception.

To be truly effective, DLP should be included as part of a broader acceptable use policy (AUP). Users should be told what is acceptable and what is unacceptable. It is unsafe to assume users know what data is sensitive and understand the potential pitfalls.

M86 Security recently published a step-by-step guide to approaching a DLP project. In it, M86 recommends the following:

Step 1: Do You Really Need a DLP Solution at the Moment?

The first question to ask is whether you really need a DLP solution. The reason for this question is that the technology and capability of DLP solutions is improving all the time, so the longer you can delay the implementation, the better the product, or so the theory goes. This doesn't advocate putting your organization at risk, but DLP is a strategy that needs careful planning.

Step 2: What Type of Solution Do You Require?

There are many types of products on the market such as hard drive encryption or endpoint port control solutions that promise to solve data loss issues. While they may address one of the ways that data loss occurs, they do not address the issue the way a content-aware DLP solution will. Content-aware DLP solutions focus on controlling the content or data itself.

There are two types of content aware solutions:

a. Single-channel solutions – Focus only on the data loss channel users want to address, such as email or Web.

b. Enterprise DLP solutions – Involve lengthy implementations and big budgets. They can also be disruptive to the organization, although they deliver more coverage.

However, all enterprises don't necessarily need an enterprise DLP solution. Don't automatically assume you'll need to buy a new product. Incumbent Web or email vendors might offer products that meet your current needs and a solid roadmap to ensure they will continue to meet your needs in the future.

Step 3: Identify What You Want to Protect

If you know exactly where all the content is that needs to be protected, then you are well on your way. If you don't, then you will need to consider using a data discovery solution to answer this question first. Then ensure you have control over where different types of content is saved. This will pay off in the future.

Step 4: Establish Why the Content Needs to Be Protected

Is it for compliance reasons or for protection of Intellectual Property? This could change not only how the content is identified but also how it is reported. For compliance, ensure you meet the data coverage required, like credit card numbers and other personally identifying information (PII) as required for PCI DSS compliance, but also the reporting requirements for the auditing process. For IP control, perhaps the solution has to recognize source code or CAD files? Ensure the solution you select has the coverage you need and is easy to teach for your required data types. Don't take the vendor's word for it. Try the solutions out against your data and compare them. This is a critical step in the success of your DLP solution, so you need to give it the time it deserves.

Step 5: Identify How Data is Currently Lost

This will help you determine the type of product to use. Is it through email? Is it being uploaded to websites such as Webmail or blog sites? Remember that what you are trying to stop is the accidental loss of data. If you are trying to stop the deliberate loss of data, then that is significantly more difficult and will seriously impact your business. If the user is resourceful and knowledgeable enough they will find ways to do it. Many companies forget about remote users and the devices they use offsite. Often, people take more risks when they are outside the office.

Step 6: Policy Creation

This is where implementation happens. M86's deep content inspection technology is effective in protecting data within email messages and attachments. Once this solution is installed, we determine how to create policy that recognizes the content we want to control and how it will be controlled. The previous steps will help you decide what to include in the policy and how to prevent the information from being leaked.

Step 7: Testing

Like any other IT implementation, testing is important for ensuring success. This requires a significant amount of testing. It's always better to run initially in monitoring-only mode to gauge the impact while you tune the controls. The testing will help you fine-tune the policy and determine how to enforce it in the future.

Step 8: Policy Communication

A step many miss. Employees need to be brought into the project to guarantee success. It will impact their day-to-day functions, so you need to be certain they understand why these controls are in place and support its use. This can be as simple as explaining why you are implementing the control and what could happen if you didn't. Obtain their feedback on the controls and how you might minimize the impact on their work.

Step 9: Policy Enforcement

After creating, testing and communicating the policy, it's time to move from monitoring controls to actively implementing them. Don't turn them all on at once. Prioritize them and release the most important and ones first. Ensure you have plenty of coverage to rectify any issues not found in testing as they arise, as this can impact employees. If you are not helpful or responsive, your employees' support will diminish.

Step 10: Future-proof Your Organization

Look for better ways to classify content or where different types of content are saved. When new applications or systems are installed, consider how you can implement them to simplify the required DLP controls. And continue to pay attention to the evolution of your DLP product. Update it as newer and better ways of implementing the controls you have in place will develop.

A. Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

While not completely relevant to a discussion of DLP, PCI-DSS's first requirement is to establish basic network security requiring the separation of the local network from the Internet and protecting the network from Internet-borne threats by using a firewall. It also requires organizations to secure this infrastructure by locking down access to integral systems—a good place to start.

B. Protect Cardholder Data

- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.

M86 MailMarshal SMTP, M86 MailMarshal Exchange and M86 WebMarshal can be configured to detect content within data streams using deep content inspection technology.

M86 MailMarshal (SMTP and Exchange) is configured to use regular expressions that can detect credit card numbers and data associated with credit cards. Rules can be created quickly and easily to ensure that any content that contains credit card information will be dealt with accordingly. M86 WebMarshal can also identify phrases and expressions and block data being uploaded to websites, forums or blogs or prevent that data from being sent via Webmail accounts such as Hotmail or Gmail. M86 WebMarshal and M86 MailMarshal SMTP can also use a number of other techniques to help protect against malicious code, phishing attacks, bad websites, dangerous file types and other threats that can occur at the Web or email gateway, helping further protect cardholder data.

M86 MailMarshal Secure Email Server and M86 MailMarshal SendSecure can be used with M86 MailMarshal SMTP to ensure that any emails containing credit card or personal information are only allowed to leave the email gateway in an encrypted fashion. M86 WebMarshal can block sensitive content that is being uploaded to an unencrypted site, ensuring that sensitive cardholder data is not being sent over the Internet unsecured.

C. Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software on all systems commonly affected by malware.
- Develop and maintain secure systems and applications.

M86 MailMarshal (SMTP and Exchange) and M86 WebMarshal use multiple anti-virus engines and file detection techniques as well as zero-day protection tools to ensure malware is blocked. The M86 Web Filter and Reporter (M86 WFR) is also able to identify attempts by malware to "call home" for updates and instructions.

D. Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.

M86 MailMarshal (SMTP and Exchange) and M86 WebMarshal ensure confidential data is not transmitted beyond authorized users. M86 MailMarshal for Exchange can enforce "ethical" walls within a company's internal email system, while M86 MailMarshal SMTP ensures this data is not sent outside the organization (or if it is, then only to specific recipients. Even then you can choose to enforce encryption). M86 WebMarshal can prevent users from uploading confidential information to Webmail, blogs, forums or other sites.

E. Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.

Alerts can be generated whenever M86 MailMarshal or M86 WebMarshal identifies credit card information in an email or HTTP traffic, allowing for prompt action to be taken. Likewise, a range of reports can be created to identify trends and perform in-depth forensic analysis.

F. Maintain an Information Security Policy

- Maintain a policy that addresses information security.

M86 WebMarshal and M86 MailMarshal include a default security policy that can be adapted quickly and easily to suit the needs of any environment. An important part of maintaining an AUP is to ensure users know about it. M86's suite of security products use email notifications and Web-based warning pages to notify users when an AUP is in place and educate them when they have contravened that policy.

M86 SOLUTIONS FOR DATA LEAKAGE

M86 provides proactive tools to protect against data leakage. These tools work in a policy-based framework to enforce security and prevent attempts to leak information. M86 products can be adapted to identify data specific to your business and manage this data according to your unique policy requirements.

These tools include:

- **Deep Content Inspection** – uses Lexical Analysis, or the ability to control email based on the presence of certain keywords and phrases. M86 solutions identify passages of confidential text either in the message body or buried within an attachment.

With respect to Web browsing, M86 can detect attempts to upload confidential text to websites. For example, attempts to use Webmail (like Yahoo or Gmail) to send confidential information or to post it in a blog or message board can be prevented.

- **User Management** – the ability to restrict rights for distributing confidential information to authorized persons only. Examples are financial reports that can only be emailed externally by the CFO, or product designs that can only be emailed by members of the executive team. If another user tries to email a confidential document to an external email address, the message can be blocked, and a notification can be sent to your security officer, a supervisor or other appropriate email address.

User Management can restrict the ability to upload certain attachment types to websites. This prevents unauthorized users from uploading Excel spreadsheets or CAD files to the Internet without permission.

- **File Management** – M86 products allow you to control more than 175 different file types. This control includes file type, sender and recipient, the presence of key words and other elements. These products identify files by the characteristic code signatures of the file type, rather than relying on the name of the file or the file extension for identification.

Using the file extension for identification is an unreliable method which allows a user to easily circumvent security by renaming the file extension. There are several file management options available to protect against data leakage. For instance:

- **Embedded Signatures** – you can embed code words or alphanumeric markers in confidential documents such as “CODEWORD123,”. These markers can be made invisible to the reader, but M86 MailMarshal still detects the code word and blocks any document featuring the code word that is being sent by an unauthorized user.
- **Fingerprinting** – you can save a copy of any confidential document or file into M86 MailMarshal's “fingerprint” folder. Any email with a file attachment saved in the “fingerprint” folder can then be detected. Any attempt to email or access a restricted file can be blocked and reported.
- **File Type** – specific file types such as CAD, Microsoft Project plans or password protected ZIP files can be automatically restricted to authorized users. This prevents other users from emailing files that are not related to their job functions. M86 MailMarshal detects files embedded within other files, such as a Word file inside of an Excel spreadsheet or a database file in a ZIP compressed archive file.
- **Recipient Blacklisting** – this allows users to define specific email addresses or domains and control email communication to those addresses. For example, with M86MailMarshal, you can set a wildcard rule that states “block all emails to *@mycompetitor.com unless from the Authorized Users group.” This rule would block any email going to your competitor's email domain that comes from an unauthorized email address.
- **Webmail Blocking** – M86 WebMarshal can completely block access to blacklisted Webmail accounts. However, if you wish to allow users restricted access to Webmail for limited personal use, you can block users from uploading certain file types or even adding confidential text.
- **Anti-virus and Anti-spyware** – M86 products support the use of many third-party anti-virus and antispyware scanners. These block Trojans and malicious spyware that enter an organization via email or the Web—at the gateway. Viruses and spyware are the most common tools employed by hackers who want access to confidential information. By employing a layered approach to virus and spyware protection at the server level, M86 products also help to prevent data leakage by external parties.

CONCLUSION

In summary, information is important, and organizations need to protect it. The problem many organizations face today, however, is that it has never been easier to access or move data, and the costs have never been so high. Email and Web access provide easy to distribute or lose sensitive data. Users can intentionally or accidentally share information with third parties with just a few mouse clicks. And with regulators ready to impose large fines and, in some cases, prison sentences, data leakage is something that people can ill-afford to ignore.

As such, it is essential that organizations identify their sensitive information and protect access to it. Whether it is intellectual property, personal information, data subject to regulatory requirements or “top Secret” military documents, organizations need to know what it is, where it is going and how to protect it.

Organizations need to deploy content-aware security products to back up an Acceptable Use Policy combined with staff training that clearly states what information should be treated as confidential and any actions to take when sharing it.

Currently, the easiest and most cost-effective method of achieving this is to use the single-channeled network and gateway tools that provide easy-to-use, effective data loss prevention techniques that address the needs of most organizations. In many cases this means looking at gateway security products that are already in place and configuring them to meet new DLP requirements.

All M86 products have been designed to secure unsecure protocols and methods of communication. From DoS and DHA attacks to blocking offensive language, M86 products allow administrator to protect their email and Web gateways from all kinds of threats and vulnerabilities.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry’s leading Secure Web Gateway provider. The company’s appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

REFERENCES

1. Gartner Magic Quadrant for Content-Aware Data Loss Prevention, July 2009.
2. http://www.theregister.co.uk/2009/02/04/data_breach_cost_guesstimate/
3. Frost & Sullivan's 2008 World Data Leakage Prevention Market Report.
4. http://searchsoftwarequality.techtarget.com/news/column/0,294698,sid92_gci1335662,00.html#

M86 DLP SOLUTIONS

M86 MailMarshal SMTP - an email security solution that combines email threat protection, content security, policy enforcement, compliance and data leakage prevention into a highly scalable, flexible, easy-to-manage solution. M86 MailMarshal acts as an email gateway, powered by an unrivalled Defense-in-Depth Anti-Spam Engine, filtering all incoming and outgoing email at the network perimeter.

M86 MailMarshal Exchange - one of the few solutions available in the market today to provide email management that filters and manages internal inbox-to-inbox email for educational organizations. It monitors and controls internal office email content that travels within a school, college or university to ensure a safe, productive working environment and compliance with acceptable use policies.

M86 MailMarshal Secure Email Server - a dedicated policy-based secure email solution that provides encryption, digital signing and deep content inspection of inbound and outbound email messages. It operates with any email gateway that can recognize S/Mime encrypted email, and automatically updates contact details and secure certificate credentials for encryption contact via a centralized server.

M86 MailMarshal SendSecure - a hosted service that allows easy encryption of email messages via a secure Web portal, thus users to send secure messages to any email recipient in the world, without requiring the exchange of any keys or certificates. Secure email recipients do not require any special software to receive these messages — just an Internet connection and a Web browser.

M86 MailMarshal Service Provider Edition - a SaaS security solution enabling Managed Service Providers and Internet Service Providers to offer hosted email content security services to any size of school and small office/home office (SOHO) customers. It combines email filtering, anti-spam, anti-virus, anti-pornography, anti-phishing, policy compliance, email archiving and reporting into a centrally managed, highly scalable architecture.

M86 Secure Web Gateway - a comprehensive Web security solution that uses Real-time Code Analysis. It enables productivity, compliance, liability and bandwidth control as well as multi-layered Web security. For DLP, it scans all inbound and outbound Web traffic (HTTP and HTTPS); scans within uploaded files and posted text; and looks for file types and lexical content based on dictionaries and logic rules.

M86 WebMarshal - the most complete secure Web gateway solution on the market today. It goes beyond URL filtering to provide comprehensive Web access control and management, complete threat protection (URL, AV and malware filtering) and data leakage prevention in a single, policy-based, easy-to-manage and highly scalable solution.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads.



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Suite 3, Level 7, 100 Walker St
North Sydney NSW 2060
Australia
Phone: +61 (0)2 9466 5800
Fax: +61 (0)2 9466 5899

Version 08/12/10