

WHITE PAPER

Corporate Self Protection: Email Security Reduces Internal & External Risks

Sponsored by: Clearswift

Christian A. Christiansen
November 2006

IDC OPINION

Corporations are being assaulted by threats from all directions. Electronic communication opened many doors for misuse and abuse — and the rather unpleasant consequences of both. What can a company do to protect itself? Securing content is the answer. Whether emails are being screened for viruses or confidential information is blocked from being accidentally sent outside of an organization, properly securing an organization's data and information will drastically reduce the risk of problems caused by electronic communications such as email, instant messaging, and Web browsing. Moreover, customers are looking for understandable solutions that can be quickly implemented and easily managed.

IDC believes the secure content management (SCM) market grew to \$6.1 billion in 2005, up from \$4.9 billion in 2004, as companies are desperately trying to find ways to address these threats. This extraordinary 24% growth from 2004 to 2005 is only the tip of the iceberg as companies will continue to devise new strategies for reducing the negative impact and increasing the positive impact of electronic communications and the Internet.

METHODOLOGY

The opinions and quantitative data provided in this white paper on SCM stem from IDC's ongoing research into spam, spyware, viruses, outbound content compliance (OCC), Web filtering, and secure content. These sources of information include ongoing surveys, interviews with vendors providing the services and products, and systems integrators and VARs that provide these products to end users. IDC's forecast models are based on historical indicators of vendor performance and prevailing market trends.

IN THIS WHITE PAPER

This white paper provides a discussion on content security and how it affects the ability of corporations to protect their systems from external and internal abuse and infection. The document focuses on providing executives and senior decision makers with an understanding of how they might best protect their companies and their companies' interests from computer-related threats through the use of appliances, software, and services focused on SCM. We conclude with a discussion of

Clearswift's solution to securing content in small, medium-sized, and large enterprise organizations.

SITUATION OVERVIEW

Messaging security is growing in complexity. The simple filtering of emails for viruses or inappropriate Web browsing by employees is no longer sufficient to protect corporations and their representatives. Threats to the corporate environment can be:

- Legal (harassment or release of personally identifiable information)
- Corporate (release of confidential corporate materials and plans)
- Social (employee's misuse of corporate equipment and time)
- Digital (virus, spam, spyware)

These threats can come from practically every communication method and path imaginable and can be sent to, from, and even within a company. Often the bulk of this content is not exposed to security measures, potentially putting an organization at risk to a broad spectrum of threats.

Corporations need SCM to address the growing threats. SCM solutions include policy-based content security solutions designed to secure, monitor, filter, and block threats from messaging and Web traffic. Inbound threats include viruses, malicious code, spam, and unwanted content. Because employees can also be the origination point for problematic emails, SCM is also designed to protect against outbound threats, such as the inappropriate release of confidential data, customer records, intellectual property, and offensive content. All of these threats can have a wide range of impact, and corporations need to protect themselves from threats of all varieties.

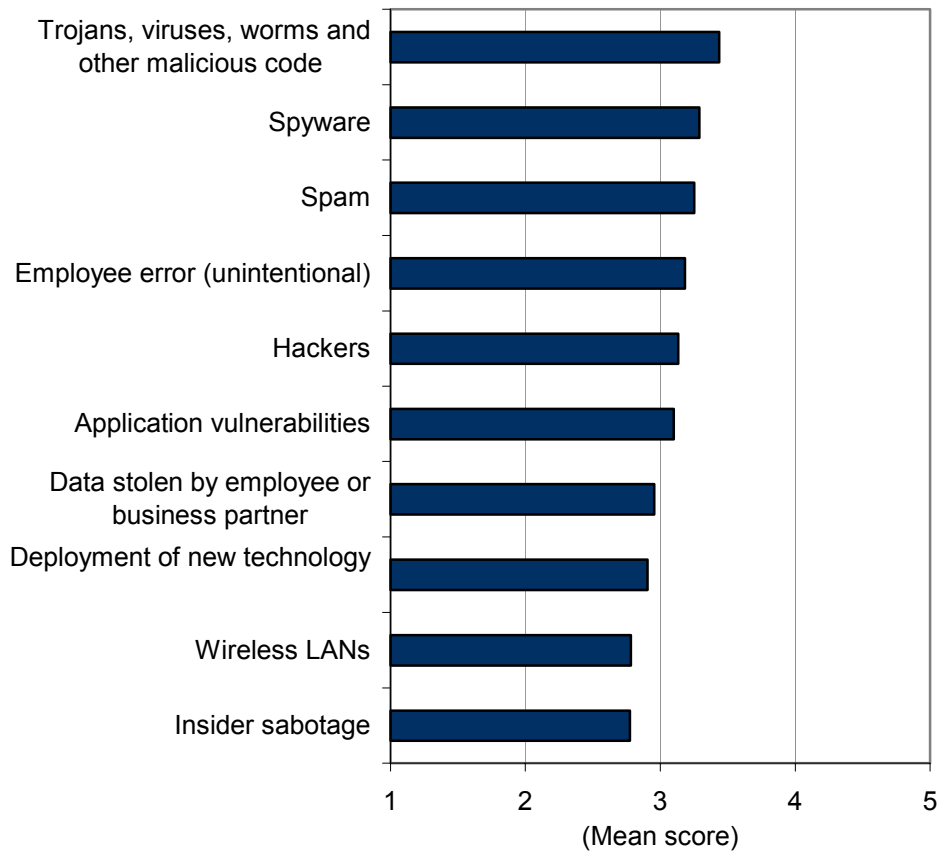
Malicious code, spyware, and spam continue to be the most serious threats facing corporations today, but internal threats are rapidly climbing the priority list of enterprise security threats and account for three of the top 10 most serious threats (see Figure 1). The demand for OCC solutions, a subset of SCM, has been fueled by the growing concern with the insider threat. Moreover, high-profile corporate scandals in which customer records, confidential information, and intellectual property were leaked are forcing organizations to take action. IDC believes the majority of internal security breaches often are not the result of malicious wrongdoing but rather of employees who unknowingly put their companies at risk. Such breaches may occur when employees unintentionally send email messages that contain confidential files or content. Another example is employees resending confidential files to their Web-based email boxes, or copying files to mobile devices, and thus exposing them to untrusted environments.

OCC includes solutions that monitor, secure/encrypt, filter, and block outbound content contained in email, instant messaging, peer-to-peer messaging, file transfers, Web postings, and other types of messaging traffic. OCC solutions play a key role in enforcing corporate governance, which is defined by IDC as a combination of

complying with both external regulatory requirements and internal corporate policies and best practices.

FIGURE 1

Threats to Enterprise Security



n = 430

Note: Threat scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC's *Security Survey*, 2006

Governance Is of the First Order

Strong corporate governance is the foundation of successful protection from the wide variety of threats corporations face daily. Corporations need to establish, educate their workforces about, and enforce their policies effectively in order to ensure the protection they need. Yet the missing piece is often content security (see Figure 2).

FIGURE 2

The Missing Security Link: Secure Content



Source: Clearswift, 2006

Content security goes beyond the necessary antivirus and antispam measures for strictly email and Web content. Content security operates bidirectionally and works to analyze every email and Web interaction that enters, leaves, or circulates within a corporation. Such an SCM system would ideally identify breaches of policy and would take action on spam, viruses, spyware, and data such as credit card details and social security numbers. Corporations with a need for content security may be overwhelmed by the large numbers of vendors that are vying for attention with their products, which range from appliances to software and managed services.

Superior technology, however, is no longer enough. Customers are demanding SCM solutions that are simpler to understand, easier to implement, quicker to reconfigure for new threats and policies, and less onerous to administer. As the following utilities company case study illustrates, customers are building layered security solutions. They want to build granular implementations that selectively reduce the volume so as to make fine-grained filters for policy matters more efficient. As regulatory compliance and internal "acceptable usage" policies become more complicated, mail flows must be reduced to manageable levels so fine-grained filtering can work efficiently. This layered approach is critical to achieving a high level of enterprise content governance.

Customers are also looking for other features. Preconfigured security policies reduce implementation time, lower administrative overheads, and restrict legal liability from misinterpretation of critical regulations. They also eliminate various interpretations by centralizing the definition and enforcement of external and internal policies. With data retention regulations affecting a greater percentage of customers, email archiving is becoming a critical aspect of email security. It is not just a simple matter of archiving all emails; rather, administrators must be able to selectively restore only certain

emails so as to fully (but not excessively) comply with legal demands. Finally, email security systems must support a wide variety of messaging systems such as Microsoft Exchange and IBM Lotus Notes/Domino.

CASE STUDIES

Utilities Company: Building a Granular Email Security Solution

Background

In August 2006, IDC interviewed a large utilities company with approximately 15,000 employees. This customer considers its security a confidential matter and thus chose to remain anonymous. IDC has changed some incidental details to hide the company's identity.

Problem

This firm needed a granular mechanism for filtering mail and applying policy to handle the security threat's increasing volume, complexity, and sophistication. This process began in 2000 when the firm began receiving email-borne malware, but the threat situation was far less serious than it is today. However, the threat environment changed significantly with Netsky and Bagel signaling the beginning of a new, more serious onslaught. Mail problems increased as the utility was attacked with spoofed nondeliveries. The customer needed a solution to deal with massive quantities of unwanted emails.

Solution

Today, virus detection remains a key issue. Anything that looks like malware is deleted. However, this solution is not enough. The company realized that it also needs a granular filtering approach to reduce the volume of mail so that more intensive policy control can be selectively applied.

To deal with these requirements, the utility has implemented a granular approach to email security using appliance and software products from Clearswift. The utility uses four appliances. Two run in tandem for load balancing. One is a standby for unexpected surges in mail volume. The fourth box is an onsite spare and test machine.

As shown in Figure 3, appliances function as coarse-grained filters (largely for spam and malware). The software concentrates on finer-grained, policy-based mail filtering of unauthorized content and unwanted graphics as well as more selective spam detection. To maintain high data flows and reduce IT administration, the appliances do not quarantine. (Although managed email security service could be the initial stage in reducing mail volume, this customer has not implemented managed services.)

The appliances' goal was to delete roughly 17% of incoming mail. However, the appliances actually delete 25% of the mail. The utility receives 5 million emails per month — 50% of which are spam — and the appliances have reduced mail volume by

roughly 1 million pieces. Moreover, the customer mentioned that "training for appliances is much less when people are already familiar with Clearswift software products."

After the appliances finish their impressive reduction in volume, the software is used for more discriminate filtering. If there is a question from the appliances, they just pass this mail to the Clearswift software. There are two software levels of filtering. The first level makes a final determination on spam. The second level checks email against corporate policy (e.g., inappropriate language, unwanted content, unauthorized graphics or attachments, and customer privacy violations).

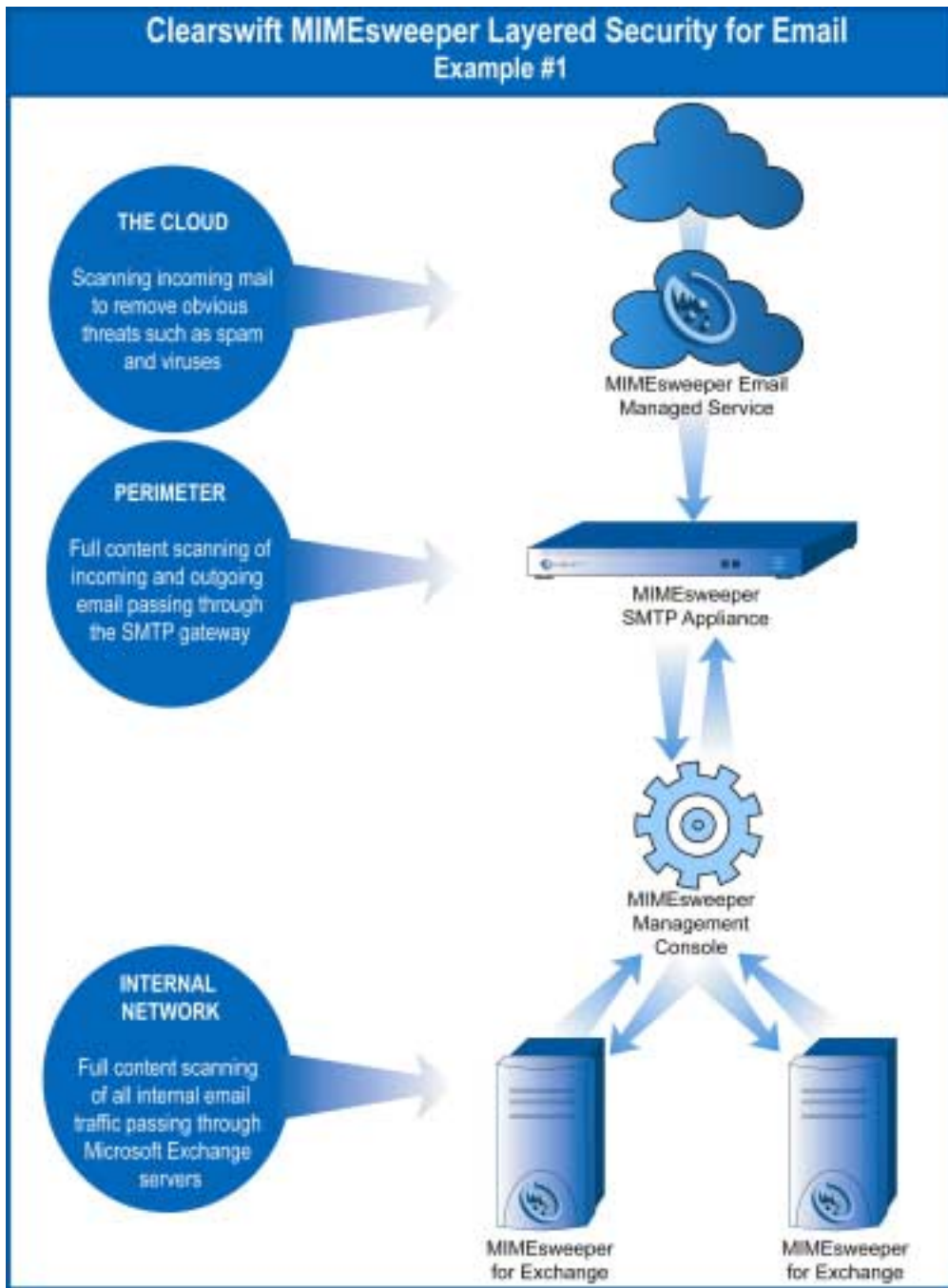
The customer has been very impressed. It estimated that over a month's time, this granular solution eliminated over 1 million messages, saved 10% in bandwidth, reduced email archiving by 6GB, and shortened backup times by 20%. Plus, it stopped roughly 18,000 malware threats. The customer said that the majority of the threats were very serious. As for overall productivity, the customer believes that employees gained five seconds of time for each message that they didn't have to manually delete. This translates into almost 1,400 hours per month of additional productivity. In terms of reduced IT administration, the customer estimated that it saves two to three man-days per month. After only a few months of operation, the customer commented that "[the Clearswift solution] has nearly paid for itself."

Future

The customer is very satisfied with the current Clearswift solution, but it recognizes that complacency is just another impending security vulnerability. The company continues to worry about worms, email-oriented denial-of-service (DoS) attacks, and phishing. Because certain enterprise applications need emails to be presented in a certain way, the company is considering utilizing Clearswift's ability for routing and remapping of email addresses to improve mail flow, increase privacy, and reduce administrative overhead. As for phishing, this company feels that phishing protection "is an important part of offering employees a safe place to work."

FIGURE 3

Building a Granular Email Filtering Strategy



Source: Clearswift, 2006

Multinational Retailer Goes Beyond Regulatory Compliance Toward Internal Policy Enforcement

Background

Even though global trends influence fashion, retail buying behavior remains regional. However, global supply chains are a necessity in order to remain cost competitive. Secure messaging is a critical component in timely communications with retail stores, affiliates, partners, and suppliers.

Satisfying international compliance regulations provides guidance for some security best practices. However, this retailer needed greater security than was afforded by compliance with regulations. It wanted to use messaging security to ensure adherence to internal policies as well. It believed that rigorous enforcement would increase efficiency and improve productivity.

IDC interviewed this customer in late August. To satisfy the company's request to remain anonymous, IDC changed some details of this case study.

Problem

This large multinational retailer has stores, partners, and suppliers in Europe, Asia, and North America. It needed a comprehensive messaging security system that could provide a consolidated infrastructure for both regulatory and even more stringent internal policies. The retailer's top 3 priorities were eliminating offensive content, stopping dangerous file types, and controlling confidential information.

Eliminate Offensive Content

Offensive (and inappropriate) content includes material concerning race, hate, sex, and harassment, as well as spam. The retailer was the subject of harassing emails from both groups (e.g., activist group protesting foreign products) and individuals (e.g., lovelorn employees making unwelcome advances toward one another). It was not just a matter of internal parties (e.g., employees) sending unwanted content to external customers and suppliers. The retailer also wanted to enforce corporate policies that forbade external sources from sending unwanted content to internal recipients. Moreover, the retailer also wanted to eliminate internal-to-internal mailing of banned materials. The legal and regulatory issues were a significant factor, but senior management felt that even casual dissemination of somewhat questionable materials caused unproductive behavior among employees and reflected poorly on the retailer's reputation from an external perspective.

Stop Dangerous File Types

In addition to malware (e.g., viruses, worms, trojans, and spyware), the retailer was concerned about all executable files attached to an email. The customer wanted to know if the file was safe, and more importantly, if it was unwanted and subject to deletion. Even legitimate executable software that failed compliance with the retailer's internal policies was quarantined and/or deleted. The retailer felt that any executable could damage the corporate system image on clients and servers. By maintaining

homogeneous system images, the retailer strongly believes that help desk calls and downtime are minimized.

Control Confidential Information

In the past, the retailer experienced an embarrassing compliance violation following an unauthorized release of its financial statements. As a result, the retailer needed to track confidential information. This situation was complicated because the retailer frequently used encryption for legitimate mail and file transfers. The customer needed a solution that could decrypt, inspect, re-encrypt, or quarantine mail and attachments, as dictated by policy. Controlling encrypted messages was a constant problem for the customer because these emails contained both legitimate and illegitimate content. Distinguishing between the two was critical because legitimate suppliers used encryption.

Solution

For messaging security management, the retailer is using Clearswift's MIMESweeper software. The customer reports that MIMESweeper is very reliable and configurable. MIMESweeper's policies are the key to granular policy enforcement.

Eliminate Offensive Content

This retailer characterizes spam as offensive content. The retailer used MIMESweeper's anti-spam capabilities to reduce unwanted mail. It also changed the domain name for email so the retailer's email addresses are not visible from an external perspective. With a strict prohibition on personal emails, the retailer sees very little spam because its email addresses are never published. Moreover, the heavy scanning of all attachments almost eliminates malicious code that harvests personal email addresses for the purpose of spoofing spam. (This avoids a common attack that uses email addresses from personal email directories so the spam looks like it came from someone that the recipient already knows.) As a result of Clearswift's flexible configuration and customer policies, the retailer stops 80,000 spam per week.

The customer also uses Clearswift's flexibility for other benefits. It eliminates the circulation of unwanted content such as jokes and multimedia files. This protects the company's reputation, eliminates foul language, and reduces offensive content. It also provides a second level of virus protection by stopping viruses without signatures. (This malicious code is also known as zero day attacks because the vulnerability is unknown.)

Actively filtering mail also reduces the harassment and/or bullying of employees. Typically, attackers use anonymous (or spoofed) Web mail accounts for harassment. Clearswift can reduce or eliminate Web mail traffic, but it can also help discover perpetrators. In a recent incident, a secret (and unwanted) admirer used an anonymous Hotmail account to harass another employee. This attention was clearly unwanted and frightening. The customer used MIMESweeper to show who logged into Hotmail at the same time that the victim received the emails. MIMESweeper's logs were used to discipline the harasser, but the customer wants to prevent these situations in the first place. It believes that proactive policies are better than retribution because it is expensive to hire, train, and then investigate a person after the act has

occurred. It is better to prevent this behavior by informing employees of the company's email policies, eliminating Web mail, and curtailing personal emails.

Stop Dangerous File Types

Because the customer has strict policies for all attachments, it has almost eliminated email-borne malicious code. These same policies apply to all executables contained within emails. By treating all attachments and executables as potentially damaging to the firm's clients and servers, the retailer can maintain consistent client and server system images. This reduces help desk calls by 30% to 50%, cuts unscheduled downtime, makes upgrades less likely to fail, and improves productivity. It also ensures that the retailer does not pass along malicious code or unwanted executables (e.g., electronic greeting cards) to its external partners.

Control Confidential Information

To meet compliance regulations and satisfy external customers' needs for privacy, the company uses encrypted emails for confidential information. On a daily basis, the company receives a total of 75 messages. Controlling encrypted messages is a constant problem for the company. It used encrypted mail services from a third party to encrypt and de-encrypt mail from trusted partners. Every encrypted message that cannot be automatically checked is quarantined and then manually reviewed. Because routing these messages is also critical, MIMESweeper enables the execution of very specific rules for passing this traffic along to other departments and enterprise applications. Because encrypted messages are often compressed before encrypting, zip files are considered dangerous as well. MIMESweeper opens a zip file and reconciles the file extension against file structure signatures to prevent exposure to malicious code.

Benefits of Comprehensive Email Policies

Even though restrictive email policies are the subject of employee complaints, the company's IT organization feels the benefits are worth the effort. It receives 100,000 emails per day, but 70% is spam. Because this traffic is stopped at the gateway, over 80% of employees do not receive any spam. The low percentage of employees who receive spam is directly attributed to the company's internal policies. The efficiency of the company's messaging security is highlighted by the fact that 4,500 email accounts (includes employees and partners) are supported by one-third of a full-time equivalent (FTE) dedicated to email security and another one-third of an FTE on the technical side. The customer also cited reduced storage space (eliminating 80,000 spam mails and most multimedia files) was a large savings. Overall, the customer believes that due diligence and protection are the more important benefits.

As for senior management's recognition of IT efforts, the directors are aware that the company's stringent email policies and MIMESweeper's enforcement are saving the company from virus attacks, giving senior people confidence with regard to confidential information, and largely eliminating external harassment.

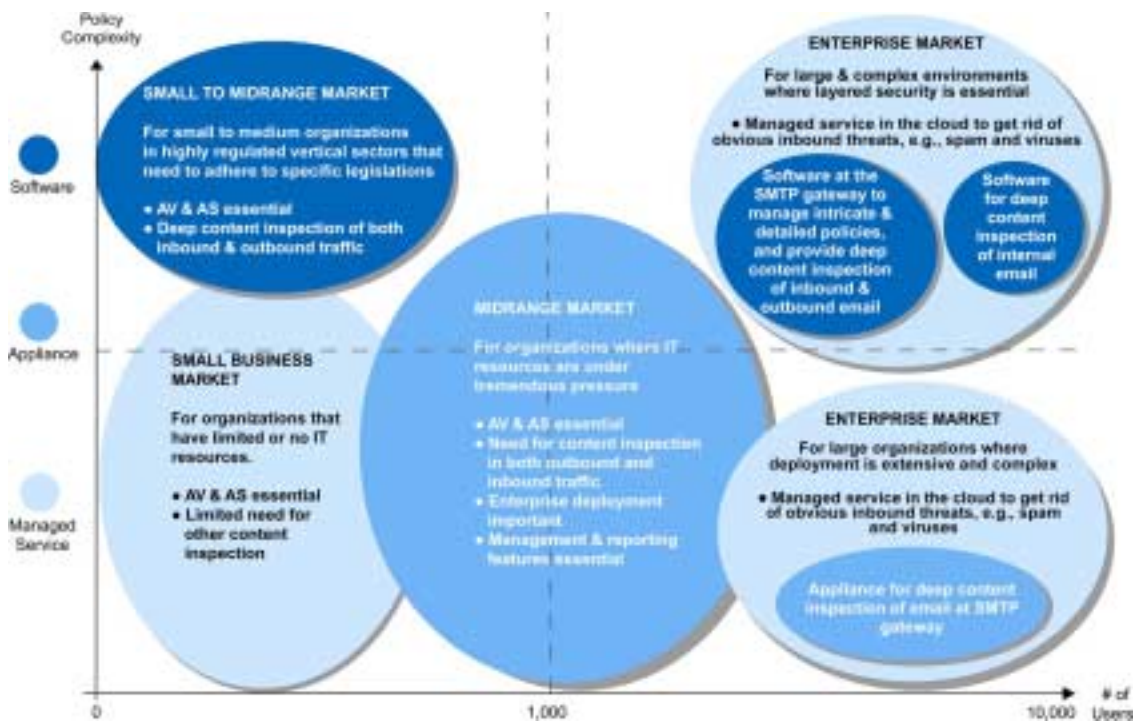
As for Clearswift's continued use, the utility said, "They were selected and remain in use because their products are very good." However, the customer has no brand loyalty and commented, "If they don't remain good, we will buy something else. Clearswift's reputation is only as good as their continuing performance." However, the customer does not expect to replace Clearswift anytime soon, saying that "Clearswift continually has churned out a high-quality product for the past eight years."

APPLIANCES, SOFTWARE, AND SERVICES — OH MY!

Amid the clamoring of SCM vendors, it is often difficult to understand which product might best fit an organization's needs. A corporation can choose from appliance-based solutions, software-based solutions, and managed services. Each of these solutions provides a different level of protection for a corporation, and combined they can provide a very strong defense for a larger organization. Figure 4 shows where each solution is best suited, depending on the size of an organization and the complexity of its policies.

FIGURE 4

Secure Content Products: Which One Is Right for You?



Source: Clearswift, 2006

Appliances

Secure content appliances are good for rapid and straightforward deployment. They secure against very specific threats, and companies with time and resource pressures will be most interested in the utilization of appliances. Appliances can work best for midsize companies or as part of a broader solution for larger enterprises.

Software

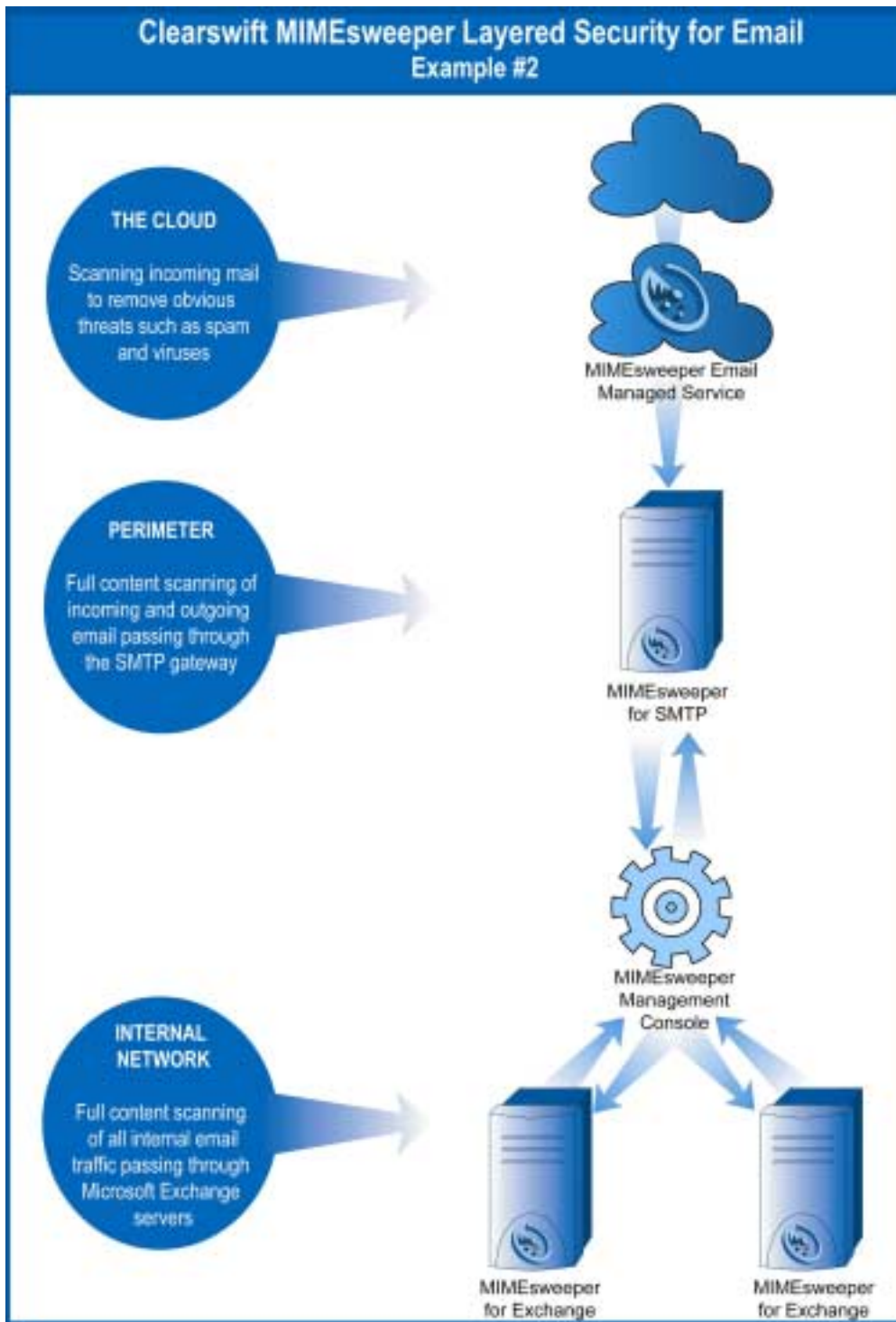
Software-based SCM allows for complete and finite control over a company's policies supporting very specific industry requirements. Software allows for a highly customized and tailored environment suitable for meeting regulatory requirements. It also does very well with larger storage subsystems. While software is an excellent solution for all, it is often expensive for small and medium-sized businesses (SMBs). It works best for large enterprises and the upper end of the midsize company segment.

Managed Services

Secure content managed services are an excellent method for SMBs to acquire content security without the expense of hardware or software applications. For larger enterprises, managed services can be the front-line filter, stripping out most content annoyances before they reach the network and are filtered more specifically. Figure 5 illustrates how "The Cloud" (or a managed service) to reduce mail traffic by 50% to 70% before it hits the "Perimeter" (or a company's mail servers so fine-grained filtering can run more efficiently against low email volumes.

FIGURE 5

Combining Appliances, Software, and Managed Services



Source: Clearswift, 2006

Building Granular Email Security Strategies

At first glance, the tendency is to look at appliances, software, and managed services as mutually exclusive solutions. However, these solutions can work in concert to build a layered email security strategy that provides coarse to fine grained filtering and policy enforcement. Layering security tools such as appliances, software, and managed services on one network can produce these granular filtering solutions.

As mentioned in the case studies, appliances can reduce spam and other unwanted email by 50% to 80%, depending on the filtering rules. (As shown in Figure 5, managed services in "The Cloud" can reduce unwanted traffic such as malicious code, and spam.) This allows finer-grained filtering on software-based servers. This filtering means that existing infrastructure can be used to efficiently enforce sophisticated internal and external compliance policies. Reducing traffic and implementing detailed categorization lead to more efficient archiving. With most litigation demanding email records, smaller and well archives enables IT to more quickly satisfy subpoenas and compliance requirements with less administrative overhead.

For distributed environments, managed services can be layered onto distributed sites for reduced IT administration. MIMESweeper Managed Service offers easily managed messaging security and archiving capabilities for SMB and enterprises. For enterprises, it can be used as a coarse filter to reduce traffic. This traffic reduction increases the effectiveness of existing fine-grained mail filters and reduces the mail volume that must be archived. For remote office/branch office (ROBO) settings, managed services can eliminate the need for local support staff, ensure uniform compliance, and cut security costs for distributed environments. For SMBs, managed services offer the often lacking security expertise, provide a predictable messaging security cost structure, and enable compliance with corporate partners' privacy policies.

FUTURE OUTLOOK

IDC believes that as threats continue to expand, and criminals and technology continue to advance at a rapid pace, almost all companies will invest in content security as basic table stakes to doing business electronically. As SCM technology develops, it will evolve as a core part of how most companies will function electronically. Companies will need to select vendors that have both the flexibility and the capability to best meet their needs, and vendors such as Clearswift are ready to offer their services and solutions.

Clearswift's Solutions Address Content Security

Clearswift's solutions provide corporations with a simplified and flexible way to address their content security concerns. Increasingly, corporations need a comprehensive, intuitive approach to SCM that does not increase the workload or number of personnel required to do the job. By deploying solutions such as those that Clearswift offers, corporations are able to act upon plans to fulfill the necessary

requirements of all levels of their organizations: from the IT staff that needs to implement and manage the solution to the C-level executive who wants it to work and never have to hear of it beyond knowledge that it exists.

Clearswift evolved its successful software product into both an appliance and a managed service. As a result, enterprises of all shapes and sizes have the flexibility to select the type of SCM that is most appropriate for their needs. Table 1 shows Clearswift's product set.

TABLE 1	
Clearswift's MIMESweeper Content Security Solutions	
Solution	Description
MIMESweeper SMTP Appliance	This appliance is complete email security in a box. It incorporates Kaspersky, Clearswift SpamLogic™ antispam, and Clearswift intelligent MIMESweeper content filtering. It blocks all incoming and outgoing email threats and requires no special knowledge to install and use.
MIMESweeper Software	For SMTP, Domino, and Exchange, MIMESweeper is designed to be the intuitive answer to most complex and intricate IT security needs. Regardless of company size, when business demands the highest level of industry-specific content security, MIMESweeper software provides the solution. The software offers a combination of total policy control, performance, and versatility to allow for specific tailoring to meet business needs.
MIMESweeper Managed Services	Managed services are the simplest way to secure email systems. There is no software or hardware to install or update. Every email sent or received is checked by Clearswift's antispam, antivirus, and content security technologies before leaving or entering the company's systems. MIMESweeper Email Managed Service also helps enforce email policies with full archiving to ensure regulatory compliance. All inbound, outbound, and internal emails are archived; no onsite hardware or software is needed.

Source: IDC and Clearswift, 2006

CHALLENGES/OPPORTUNITIES

Despite the advances in secure content technologies, many challenges are ahead. The advancement of networking, mobile devices, and small form factor USB drives — along with the continual evolution in the ability to transfer data quickly and unobtrusively from one point to another — creates enormous challenges for all makers of SCM technologies.

Specifically, while Clearswift provides very strong and flexible solutions, it still needs to further develop certain areas such as secure instant messaging, Web filtering managed services, encryption, and archiving. Its customers would benefit from the option of both an appliance and a managed service for Web-based threats. In answer to this need, the company has just released an appliance version. We expect a managed service in 2007. Therefore, its customers shouldn't have to wait too long for a broader range of email security solutions.

The opportunities for Clearswift lie in its ability to bring all these solutions together to offer a very comprehensive, yet flexible solution for corporations to address their challenges in securely managing their content. As Clearswift fleshes out its product portfolio completely, its breadth of product will enable it to have a broader customer base than any one product option (software, appliance, managed service) would alone.

CONCLUSION

It is clear to IDC that the threat environment around electronic communications will only increase in complexity for the corporations using such communications extensively. Customers still need the basics (anti-spam and anti-virus), but they recognize that risk comes from many different sources (employees, business partners, contractors, consultants, criminals, government regulations, and industry recommendations). Failure to address these interwoven vulnerabilities can disrupt operations, generate negative publicity, and result in onerous legal issues.

- ☒ Policy enforcement is the key to dealing with this increasingly complex risk environment. A solid solutions must deal with:
 - ☒ Inbound content that is either malicious or simply unwanted
 - ☒ Outbound content that might leak company-confidential information, cause harm/offense to customers and/or violate regulations
 - ☒ Content in transit so it is protected while still being subject to administrative review
 - ☒ Management that is granular and flexible enough to handle large changes in traffic volumes, comprehensive messaging security policies, international compliance regulations, and individual corporate policies without needlessly burdening the IT staff.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.