

VENDOR NEEDS AND STRATEGIES

Clearswift: Securing Content

Thomas Raschke

IDC OPINION

Clearswift protects organizations with a variety of software, services, and appliances. IDC believes that the company will continue to answer market demands for easy-to-use, plug-and-play full content security with incorporated antivirus support and spam protection. Clearswift's road map is focused on helping organizations address issues created by unstructured content, and issues relating to digital threats, corporate and legal liability, and compliance to regulations. The company and its technology are well-positioned to address future challenges of the rapidly changing Internet, and secure content management (SCM), and email content security markets. The following outlines key market dynamics for these markets:

- ☒ In addition to revolutionizing the way that organizations conduct business, the Internet has raised serious challenges to content security by creating a variety of corporate, legal, social, and digital threats that expand as enterprise content grows. IDC believes that while most organizations have implemented protection against nuisances such as spam, and threats such as virus and network intrusion, disruptive intimidation posed by privacy and confidentiality leaks, IP theft, and internal threats, including pornography and harassment, continue to plague enterprises worldwide. SCM vendors like Clearswift help organizations understand the value of content by — when done right — offering a holistic enterprise content governance approach, which arms organization with policies and tools to ensure compliance with corporate and regulatory requirements.
- ☒ IDC believes that most organizations understand the value of protecting their information and have invested heavily in securing intellectual property and corporate networks. Unfortunately, they have failed to secure the majority of corporate data, which is contained in unstructured and unsecured environments on desktops, laptops, external storage devices, and network drives throughout the enterprise. This information continues to mount as employees create and share emails, documents, spreadsheets, presentations, and so on, which are then circulated freely in, out, and within the company. Through comprehensive enterprise content governance, organizations need to better understand the value of their unstructured data while implementing measures to protect the data against internal threats by controlling how it is used and distributed.
- ☒ Finally, IDC believes that the convenience and efficiency of electronic mail have been dramatically reduced due to the extremely rapid growth in the volume of unsolicited commercial electronic mail. Spam has become more than just a nuisance; it is quickly becoming both a major productivity drain and a potential legal liability in organizations across the globe. Spam fills networks, servers, and inboxes with unwanted and often offensive content. The business impact of spam only grows more serious as the volume of spam continues to rise.

IN THIS STUDY

Who is Clearswift? What does Clearswift bring to the security market, and how can this company gain competitive position in the rapidly emerging SCM and messaging security space? Additionally, this study takes a closer look at both the challenges and trends of the SCM market and its sub-market, the messaging security space.

SITUATION OVERVIEW

Greater Picture: Emerging Threats in the Secure Content Management Market

Outbound Content Compliance

The challenge of controlling electronic communications as they flow into and out of an organization is becoming increasingly more critical. Government and industry regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and SEC have placed unprecedented pressure on corporations to secure the use of their electronic communications. A wide range of communication channels available to employees, such as instant messaging, chat, Web mail, and peer-to-peer file sharing represent serious threats to customer information and can expose organizations to reputation, compliance, legal, and financial risk. Organizations that manage patient health information, social security numbers, and credit card numbers are being forced by government and industry regulations to implement minimal levels of security to address leakage of personal information. The loss of confidential personal information can materialize into compliance infractions, lawsuits from customers and/or patients, and potential identity theft. Identity theft has become a major issue for corporations and consumers alike.

Protecting a company's confidential information and intellectual property has also moved up the priority list of many IT departments. Gone are the days where intellectual property and corporate secrets were kept safe in locked cabinets behind guarded doors. Today, nearly all corporate information exists in electronic form, accessible to almost any employee. The risks of inadvertent or deliberate disclosure range from legal exposure to competitive disadvantage. Companies can risk losing serious money when design documents and source codes are posted to Internet message boards or emailed outside the organization.

Outbound content compliance (OCC) solutions have emerged to address the emerging internal threats. OCC solutions are playing a key role in helping organizations comply with both external regulatory requirements and internal corporate policies and best practices.

Regulatory Compliance

The challenge of controlling electronic communications as they flow into and out of an organization is becoming increasingly more critical. Government and industry regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, SEC, and Basel II have placed unprecedented pressure on corporations to secure the use of their electronic communications. In many cases in which the original intent was to address a regulatory issue, the security aspect represents part of the solution. Organizations are faced with the complex task of complying with various regulations and making sure that employees do not inadvertently, or deliberately, break the law. Each of these regulations can carry criminal penalties and/or civil penalties. Criminal means criminal prosecution of individuals as well as substantial fines. Successful criminal convictions generally lead to civil lawsuits. Civil lawsuits (especially in class action situations) can carry substantial financial penalties and damage a company's reputation with its customers. Although many regulations only fall into the civil area and would seem "toothless," the fact that they permit class action suits creates major opportunities for the legal community, especially in today's litigious society.

Spam Not Slowing Down

IDC estimates the amount of spam being sent on an average day worldwide has jumped from 4 billion in 2001 to 17 billion in 2004. Spam is quickly becoming both a potential legal liability and a major productivity and resource drain for corporate IT departments and corporate users alike. Moreover, spam is viewed as a security threat because it can carry viruses, malicious code, and fraudulent solicitations for privacy information. Nearly 70% of organizations surveyed have already deployed antispam solutions to address this growing threat. Organizations without such solutions are behind the times and putting themselves at unnecessary risk. More than two-thirds of IT respondents feel the spam problem will get worse in the next two years. Moreover, IT executives feel strongly that government legislation will have little to no effect on it. Most email users surveyed (70%) without antispam solutions reported increases in the number of spam messages received in 2003 over the prior year. IDC estimates that the number of spam messages sent daily will continue to grow, reaching 23 billion worldwide in 2007. With the help of antispam solutions, spam is expected to become a problem that is more manageable, often as part of comprehensive messaging security solutions.

In the past, spammers traditionally sent spam from their own ISP account. When corporate IT departments and antispam solutions first started to block messages from certain domains and ISP accounts, spammers turned to new methods to conceal their identity. IDC believes spammers are starting to resort to outright criminality in their efforts to conceal the sources of their spam messages, using Trojan horses to turn the computers of innocent consumers and corporate users into secret spam engines. The explosive growth of cable modems and broadband connections have left consumers and remote employees open to attack. In many cases, their computers are being used as a relay for sending spam to thousands of other people. There is also very little chance that the PC's owner will have any idea that their system is being used by a third party. The SoBig virus is a good example of the convergence of spam and viruses.

Gone Phishing

The recent incidents of phishing attacks on banks and their online customers have opened both consumer and corporate eyes to the increasing dangers of corporate

identity theft. Phishing is clearly motivated by financial fraud and gain, and thus criminals are most often behind these attacks, rather than teenagers just trying to cause havoc. Phishing attacks use spoofed emails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, and social security numbers.

IDC believes more sophisticated attackers, often from organized crime, will increasingly use phishing techniques to obtain credit card numbers, bank account information, and other personal information to perpetrate identity theft. We believe the sophistication and scale of online frauds and identity thefts will continue to increase at a rapid pace.

Context: The Messaging Security Market

Definition

Messaging security software is a subset of the SCM market and is used to monitor, filter, and/or block messages from different messaging applications (e.g., email, IM, SMS, and peer to peer) containing spam, company confidential information, and objectionable content. Messaging security is also used by certain industries to enforce compliance with privacy regulations (e.g., HIPAA, Gramm-Leach-Bliley, and SEC) by monitoring electronic messages for compliance violations. This market also includes secure [encrypted] email.

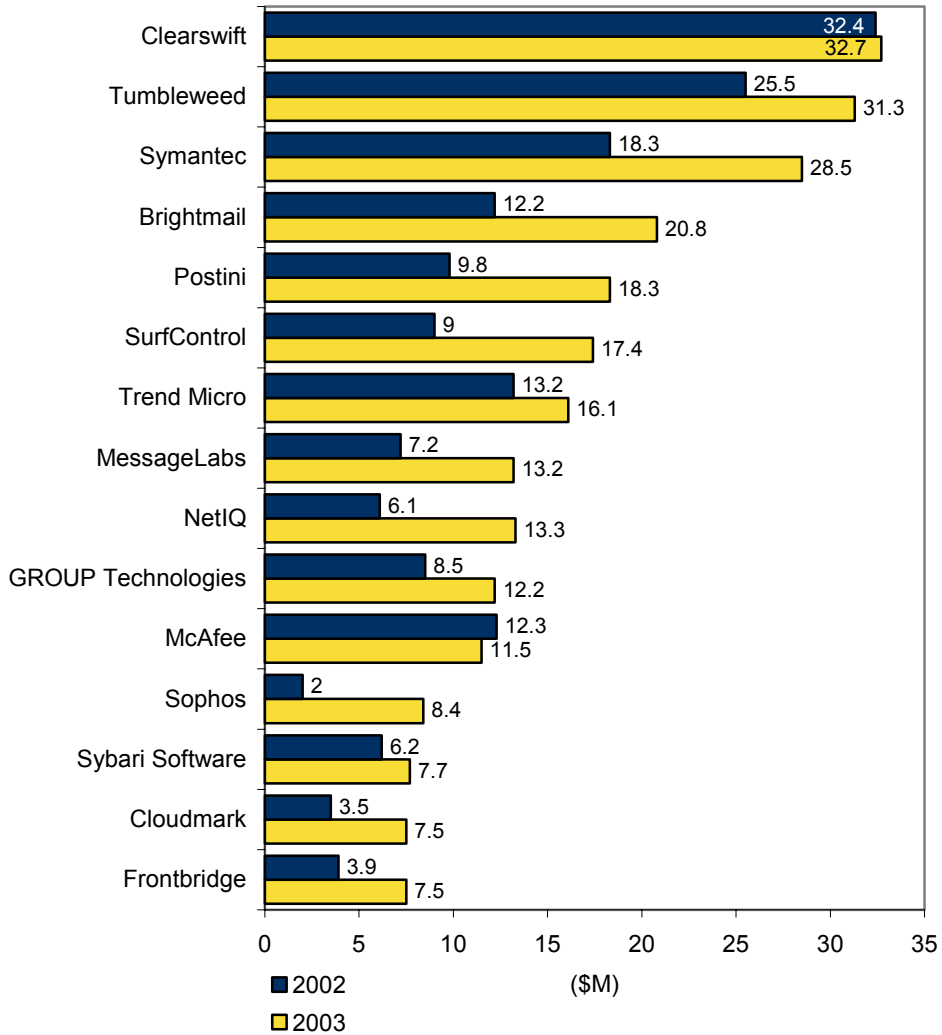
The Messaging Security Market by Vendors

Clearswift, a privately-held U.K. SCM software company, acquired the Content Technologies subsidiary of Baltimore Technologies on January 24, 2002. Already in 2001, the combined revenue of Clearswift and the Content Technologies subsidiary made Clearswift the worldwide leader in the then-called email scanning software market. In 2002 and 2003, the company continued to lead the — now called — messaging security market with 13% and 8% worldwide share respectively. Early estimates for 2004 show a similar picture.

Clearswift leads the worldwide messaging security software market with \$32.7 million in 2003, as shown in Figure 1. This model shows the 2002 and 2003 market development for the worldwide messaging security market.

FIGURE 1

Worldwide Messaging Security Software Revenue by Top 20 Vendors, 2002 and 2003 (\$M)



Source: IDC, 2005

Clearswift: A Closer Look

Clearswift provides solutions that assist in protecting organizations from the threats posed by electronic communication. Clearswift products secure content and protect against digital attacks by enforcing policies that increase productivity, reduce IT costs, and create a safer business environment. Clearswift is the worldwide leader in messaging security and accounted for \$32.7 million in revenue and an 8.2% share of the total worldwide messaging security market in 2003. The company delivers the capabilities for organizations to protect themselves against email- and Web-based threats, meet legal and regulatory requirements, implement productivity-saving policies, and manage intellectual property passing through the network. The company's expertise is in threat prevention and risk reduction, through the definition and deployment of policy on multiple types of content. Content security threats include:

- Circulation of inappropriate images and text
- Spam and oversized files that cause network degradation
- Loss and corruption of business critical data
- Breaches of confidentiality
- Infection of viruses and malicious code
- Compliance with privacy regulation

Product Overview

Clearswift is present in 15 countries worldwide with headquarters both in the U.K and U.S. and sales offices in Germany, Sweden, Japan, and Australia. MIMESweeper is the leading family of content security solutions with over 15,000 customers worldwide and over 20 million users.

Clearswift MIMESweeper is a family of policy-based content security solutions that enable organizations to protect themselves against email and Web-based threats, meet legal and regulatory requirements, implement productivity-saving policies and manage intellectual property passing through their network. All MIMESweeper products have the following in common:

- Policy-based — so security is reflected in the way business is conducted
- Integrated — to deliver total content security with a single approach
- Covers all boundaries — SMTP, HTTP, Web mail, and internal messaging

Detailed Product Portfolio

The MIMESweeper family includes a comprehensive set of products for external email (everything that enters or leaves through the SMTP gateway), internal email (for Exchange and Domino), the Web (securing a company's Web use), and specialist solutions (addressing specific security challenges). Clearswift also offers a managed service called e-Sweeper.

External Email: Everything that Enters or Leaves through the SMTP Gateway

MIMESweeper for SMTP addresses all the content security threats and provides protection against isolated threats such as viruses and spam.

IMAGEmanager examines and compares detected images with the characteristics of those held in an extensive database of previously analyzed images.

SECRETsweeper is an encryption/decryption and digital signature gateway that provides gateway signing, encryption/decryption, and policy-based management of the threats associated with encrypted email.

Archiving solutions based on MIMESweeper technology provide policy-based email archiving software that allows intelligent search and retrieval of email for legal and regulatory compliance.

MIMESweeper SMTP Appliance is a content security box offering "plug and play" deployment, automated updates, and easy, intuitive management. The product comes pre-loaded with bi-directional deep content filtering and antivirus/spam protection in an easy-to-integrate and -manage policy engine.

Internal Email: For Exchange and Domino

MIMESweeper for Domino is a policy-based solution that manages internal content security threats in Lotus Domino environments, for example Domino mail and databases.

MIMESweeper for Exchange allows organizations to protect against digital threats coming from internal email communication, e.g. employees sending round jokes, MP3 files, or defamatory emails.

The Web: Securing a Company's Web Use

MIMESweeper for Web analyzes Web content and blocks pages or files that are prohibited by a security policy but are not yet listed on any URL filter.

MIMESweeper URL Filter is an optional plug-in to the MIMESweeper for Web solution that blocks Web access to Web sites blacklisted by a security policy.

Specialist Products: Addressing Specific Security Challenges

This is a range of specialized security solutions for the most security conscious environments such as government and defense organizations. They deliver the policy infrastructure and the enforcement technology required to deploy a comprehensive management and security solution.

Specialist products: Government and military messaging infrastructure products designed to protect the most complex environments. Products include X.400 Filter, Bastion II, FlashPoint, and DeepSecure.

Managed Service e-Sweeper

Clearswift also offers a managed service called e-Sweeper, which is an email content security solution provided by service providers to their clients. This means that security professionals handle protection from content threats at customers' email gateways. This frees organizations from the cost of implementing the hardware, software, and administration expertise necessary to effectively stop the myriad of content security threats.

FUTURE OUTLOOK

The Messaging Security Market

Spam

Spam became the primary driver for messaging security implementation in 2004. In fact, this is the first time in history that antivirus technologies have taken a backseat to any other security technology. Almost every vendor in the messaging security market has developed, partnered with, or acquired an antispam technology. The main reason for this is not just the fact that spam has overwhelmed most corporate users; the more important reason is money. Spam is no longer just a nuisance; it is quickly becoming both a potential legal liability and a major productivity drain for corporate IT departments and corporate users alike. Because of this, many organizations have set aside specific funds to solve the spam problem. Internet service providers (ISPs) and antispam solution vendors report that spam currently represents 45%–80% of all inbound Internet email.

Secure Email

There has always been a need for secure email, and there have been many good products to provide the confidentiality and integrity email should require. However, the market for these solutions never really took off until now. The questions asked when managers wanted to deploy secure email are, why, and, how much?

The answer to the first question is that enterprises require secure email to meet government regulatory requirements such as HIPAA and Sarbanes-Oxley. The need to secure communications to comply with regulations was the main driver of this market for most of 2003. Many healthcare organizations are looking toward email as a way to comply with HIPAA. Public companies are concerned about Sarbanes-Oxley and how it will impact them, so they are also looking at secure email.

When companies deploy for regulatory compliance, cost does not top the list of considerations, but many companies see secure email as a way of reducing costs. By using a one-to-many secure email delivery system, companies can use secure email to reduce costs by replacing the mailing of statements to customers. It is also a better solution than a Web portal because customers receive the statement so they can view it offline and do not always need to contact the Web portal to view.

With the need for privacy protection and regulatory compliance, along with real cost savings for secure email replacing standard paper mailings and the ability to tie to email content security, email security companies like Sigaba, Tumbleweed, PKWare, and ZixCorp, along with the PKI-enabled email applications from Entrust, RSA Security, and VeriSign are having considerable success and should continue to do so in the future.

Instant Messaging

Instant messaging has entered the corporate world and has brought with it another layer of security concerns. Such applications can provide attack points for hackers seeking to gain entry into corporate systems by tunneling through firewalls. This vulnerability leaves corporate information at risk because any data a trusted employee can see is potentially viewable by hackers gaining access to the system via insecure instant messaging applications. Viruses can also enter via file transfers between users and threaten productivity and data. Moreover, instant messaging represents an "instant distraction" for employees, with addictive implications regarding productivity.

IDC believes the number of attacks on users of Internet relay chat (IRC) and instant messaging will continue to rise. These attacks consist of attempts to trick the unknowing user into downloading and executing automated agent software that allows remote systems to use target systems as attack platforms for DDoS attacks against other systems or as targets for backdoors and Trojans.

Proprietary Information and Privacy Protection

The inadvertent or deliberate release of sensitive customer information is another major problem facing organizations using electronic communications. A perfect example of this was the Prozac incident a few years ago. On June 27, 2001, an Eli Lilly employee sent an email message to Medi-messenger subscribers announcing the termination of the Medi-messenger service. To do this, the employee created a new computer program to access subscribers' email addresses and send them the email. The June 27 email disclosed the email addresses of all 669 Medi-messenger subscribers to each individual subscriber by including all of the recipients' email addresses within the "To:" line of the message. By including the email addresses of all Medi-messenger subscribers within the June 27 email message, Eli Lilly unintentionally disclosed personal information provided to it by consumers in connection with their use of the Prozac.com Web site. The frustrating part for Eli Lilly was that were policies in place to protect against just this sort of thing happening. This case clearly shows that policies alone are not enough. Organizations must adopt security technologies to ensure that their corporate policies are enforced and that consumer privacy regulations are not violated.

PECS

IDC has coined a new term, "policy-enforced client security (PECS)," for products that will eventually address the security concerns regarding transitory users (e.g., laptop, PDA, and mobile users). PECS will provide a platform for client security solutions, such as antivirus and messaging security. The growing number of users logging into corporate networks from home and other relatively insecure remote locations is proving to be a major challenge for companies to enforce corporate policies and comply with government regulations. In addition, workers who log into corporate networks from home or other remote locations often do not have the same defenses and are increasingly vulnerable to having their systems infected by viruses and hackers.

IDC envisages PECS involving modules that could include firewalling, intrusion detection, VPN, antivirus, content security, and authentication. Wrapping all of this together would be a centralized policy-management capability. The benefits to implementing a PECS strategy include reducing malicious threats from alternative Internet service providers (ISPs) and enforcing policy at an individual level as well as transparent security policies for the user, user inability to disable security, and lower administration costs. IDC believe that PECS will enhance, not replace, server-based security. IDC believes the biggest security threat today is remote users. VPN access is proliferating, and with the onset of wireless home networking, it's becoming increasingly easy to gain access to a corporate network. We believe PECS will be the foundation for organizations to ensure that remote workers are covered by the same security polices that govern the corporate network.

Copyright Violations

Legal liability risks around employees downloading MP3s and full-length DVDs on corporate hard drives will become another concern in many organizations. The Recording Industry Association of America (RIAA) and the Motion Picture Association of America recently warned CEOs of Fortune 1000 companies that their corporations will be held liable for breaking copyright laws if employees use company networks to download, store, or distribute music or movies illegally.

Clearswift: Strategic Direction

Clearswift enables organizations to protect themselves against digital attacks, meet legal and regulatory requirements, implement productivity-saving policies, and manage intellectual property passing through their network.

To address the gaps that exist in the current layered security infrastructure, Clearswift announced enhancements to its current product line that will allow Clearswift customers to meet the demands of the market to address regulatory and legal issues brought on by regulatory statutes and compliance laws worldwide.

Underpinning the strategic road map, Clearswift will provide content security solutions to the market on a range of platforms — software, managed services, and appliances. Consequently, the latest addition to the MIMESweeper family is an SMTP appliance offering "plug and play" deployment, automated updates and easy, intuitive management. The product comes pre-loaded with bi-directional deep content filtering and antivirus/spam protection in an easy-to-integrate and -manage policy engine.

Only recently, Clearswift announced a new CEO following the departure of former CEO David Guyatt, who was replaced by Jon Lee (formerly CEO of London Bridge Software). Lee, along with Clearswift Chairman Carl Symon, is expected to continue the company's road map, which is focused on helping organizations address the future of the rapidly changing Internet and email content security market.

Finally, as spyware is at the forefront of customer's minds, Clearswift will have to offer a solution to address this particular pain point.

ESSENTIAL GUIDANCE

Corporate concerns regarding compliance with privacy regulations will continue to fuel the growth of messaging security solutions. High-profile corporate accounting scandals and turmoil in certain vertical markets will create additional federal and industry regulations aimed at ensuring greater accountability of public companies, providing oversight and review of equities research and sales, and safeguarding the security of consumer records not just in healthcare and financial settings but in all verticals that manage, store, or transmit customer information.

IDC also believes customers will continue to buy point solutions to solve the spam problem, but this will be the exception, not the rule. Antispam will continue to be an important adoption driver in the messaging security section; however, IDC believes it will become a feature of messaging security and not a distinct market. IDC recommends that vendors continue to develop, acquire, or tightly integrate with partners to offer a complete messaging security solution.

IDC believes that outbound content compliance will be a strong growth area over the next five years. There are many different items converging, which leads IDC to this conclusion. The bottom line is that OCC is needed and because of government and industry standards and regulations, enterprises must deploy and use such solutions. This market will develop in a consistent manner. There are many other security issues enterprises are working on, so the deployment of OCC will be done over time as companies deal with varying security initiatives.

One factor that will expand the use of OCC will be the expanded usage of email on handheld devices like BlackBerrys, smart phones, and PDAs. Another important growth area will be instant messaging. Security for this growing communications channel will be important as more enterprises adopt the technology. Vendors who can meet these developing areas in addition to traditional email will have a considerable competitive advantage.

LEARN MORE

Related Research

- ☒ *Trend Micro Acquires Spyware Company InterMute: A Trend?* (Doc #IS53M, May 2005)
- ☒ *Western Europe Security Appliance 2005–2009 Forecast and 2004 Competitive Vendor Shares* (Doc #IS04M, May 2005)
- ☒ *Western European Security Software 2005–2009 Forecast* (Doc #IS02M, April 2005)
- ☒ *CeBIT 2005: One Hall to Secure Them All* (Doc #IS52M, Mar 2005)
- ☒ *European End-User Survey: 2005 Spending Priorities, Outsourcing, Open Source, and Impact of Compliance* (Doc #LC01M, Mar 2005)
- ☒ *European Mobile Security Software Forecast, 2004–2009* (Doc #WL01M, Mar 2005)
- ☒ *Microsoft Security 2005: Raising the Bar?* (Doc #IS01M, Mar 2005)
- ☒ *Oracle Obtains Oblix, Secures Solutions* (Doc #33184, Mar 2005)
- ☒ *IDC's Software Taxonomy, 2005* (Doc #32884, Feb 2005)
- ☒ *Consolidation Trend Continues for Identity and Access Management as BMC Software Acquires Calendra* (Doc #32756, January 2005)
- ☒ *Western European Security Appliance Market, 3Q04: ID&P and UTM Security Appliances Continue to Thrive* (Doc #SB01M, Jan 2005)
- ☒ *EMEA Currency Issues In Global Business Planning* (Doc #RAT01L, Dec 2004)
- ☒ *European End-User Survey: How Secure is Europe?* (Doc #IS04L, November 2004)
- ☒ *Novell BrainShare Europe 2004: What's the Identity of the Penguin?* (Doc #IS51L, October 2004)

Definitions

Security Software

Security software covers a wide range of technologies used to improve the security of computers, information systems, Internet communications, networks, and transactions. It is used for confidentiality, integrity, privacy, and assurance. Through the use of security applications, organizations can provide security management, access control, authentication, virus protection, encryption, intrusion detection and prevention, vulnerability assessment, and perimeter defense. All these tools are designed to improve the security of an organization's networking infrastructure and help advance value-added services and capabilities.

Secure Content Management (SCM)

SCM includes policy-based content security solutions designed to secure, monitor, filter, and block threats from messaging and Web traffic. SCM protects against inbound threats such as spam, fraudulent emails, viruses, worms, Trojans, spyware, and offensive material. SCM solutions are also designed to protect against outbound threats such as confidential data, customer records, intellectual property, and offensive content leaving an organization. SCM solutions play a key role in complying with government and industry regulations as well as enforcing corporate policies. SCM is a superset of three specific product areas:

Antivirus software scans hard drives, networks, email, floppy disks, Web traffic, and other types of electronic traffic (e.g., instant messages and mobile messaging) for any known or potential viruses, worms, Trojans, spyware, or other types of malware.

Web filtering software is used to screen and exclude from access or availability Web content that is deemed objectionable or non-business related or poses a security threat. Web filtering is used by corporations to enforce corporate Internet use policy as well as by schools and universities and home computer owners (for parental controls).

Messaging security software is used to monitor, filter, block, secure, and encrypt both inbound and outbound messaging traffic (e.g., email, instant messaging, SMS, and peer to peer). Messaging security solutions are used to detect spam, company confidential information, violations of government and industry regulations, and objectionable content. Messaging security also includes encrypted email and enterprise digital rights management (DRM). The following are representative vendors and products in the SCM market:

- Computer Associates (eTrust Secure Content Management and Antivirus)
- McAfee (McAfee Anti-Virus)
- Sophos (PureMessage and MailMonitor)
- SurfControl (SurfControl Web Filter and SurfControl E-Mail Filter)
- Symantec (Symantec AntiVirus, Norton Antivirus, and Brightmail)
- Trend Micro (InterScan, ScanMail, and PC-cillin)
- Websense (Websense Enterprise)

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at +44 (0) 20 8987 7107 or mheath@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2005 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Published Under Services: European Security Products and Strategies