

WHITE PAPER

Secure Content Management: Rebuilding the Foundation of Enterprise Security

Sponsored by: Computer Associates

Brian E. Burke

July 2003

IDC OPINION

Secure Content Management (SCM) is increasingly moving away from a focus on a single type of protection, such as antivirus software, toward a focus on broad protection against a wide range of emerging threats to enterprise content. Although antivirus software remains the foundation of enterprise security, emerging content security threats are forcing organizations to approach content security with multiple layers of protection. Concerns about spam, employee productivity, legal liability, and regulatory compliance are driving the need to scan email, instant messaging (IM), and Web traffic for inappropriate content, misuse of intellectual property, and unsolicited email. To make these tasks viable in large enterprises, customers require a unified way to manage multiple secure content technologies, including antivirus, spam protection, messaging security, and Web filtering.

This paper maps Computer Associates' eSCM solution against organizations' needs for Secure Content Management solutions. It seeks to address emerging risks associated with widespread misuse of the Web, IM, peer-to-peer (P2P) networks, and email applications. The paper details the following challenges associated with protecting organizations from an evolving array of threats to secure content. Management of multiple content risks must be balanced against the expense of increased IT management overhead. With IT staffing always a limited resource, enterprises look to make management of security products as simple as possible. By integrating the products at the client, consolidating IT administration with a single user interface and a common console, and delegating some management tasks to users, new SCM products reduce the strain on IT departments and help reduce overhead.

- ☒ New viruses continue to employ blended threat techniques, exploiting multiple weaknesses and attacking through multiple methods (e.g., email, file transfers, and Web browsers). This forces organizations to purchase additional layers of antivirus and content security products that must be deployed across the enterprise to be effective.
- ☒ Legal liability risks around employee file sharing (e.g., downloading copyrighted music and full-length movies) on corporate hard drives is drawing the attention of top-level executives. The Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and other groups 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.
- ☒ 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. More than 40% of the respondents to IDC's email retention survey, which recently surveyed 557 North American organizations, indicated that the number of spam emails received during an average day has risen 50–100% compared with the number they had received 12 months earlier.

- ☒ IM has entered the corporate world and has brought with it another layer of security concerns. Corporations that permit employees to run unsecured IM applications are putting enterprise systems at risk of virus infection, legal liability, and violation of privacy regulations. Moreover, IM applications can provide attack points for hackers seeking to gain entry into corporate systems by tunneling through firewalls.
- ☒ Corporate concerns with compliance with privacy regulations (e.g., Health Insurance Portability and Accountability Act of 1996 [HIPAA], Gramm-Leach-Bliley Act [GLBA], and Securities and Exchange Commission [SEC]) continue to fuel the explosive growth of content filtering and messaging security. As the use of email and IM increases, the need for solutions to secure, monitor, archive, and retrieve communications has become imperative for healthcare and financial services firms. Other industries, while not always as tightly regulated, are facing a growing array of new regulations in the United States and in other nations.

METHODOLOGY

IDC developed this White Paper using a combination of existing market forecasts and direct, in-depth primary research. To gain insights into the challenges facing enterprises and to learn more about how the CA eSCM solution helps address these challenges, IDC reviewed in-depth interviews it had conducted with IT executives at companies in several industry sectors. These organizations operate in healthcare, financial services, public services, manufacturing, and hospitality. In addition, IDC met with the CA team to review its goals and tactics. This report reflects all of these research perspectives.

IDC MARKET DEFINITION: SECURE CONTENT MANAGEMENT

Secure Content Management is a market that reflects corporate customers' need for a policy-based Internet management tool that manages Web content, messaging security, virus protection, and downloadable applications execution. SCM is a superset of the following product areas:

- ☒ **Antivirus software** identifies and/or eliminates harmful software and macros. Antivirus software scans hard drives, email attachments, floppy disks, Web pages, and other types of electronic traffic (including IM and SMS) for any known or potential viruses.
- ☒ **Web filtering software** denies users access to Web pages that are deemed objectionable or nonbusiness related. Web filtering is used by corporations to enforce corporate policy and by schools, libraries, and home computer owners to enforce parental or community-dictated controls.
- ☒ **Messaging security software** screens messaging applications such as email, IM, SMS, and P2P for spam or other objectionable content. The software is also used to enforce corporate policy by screening for confidential corporate information and to enforce compliance with privacy regulations (e.g., HIPAA, GLBA, and SEC). Messaging security also includes secure email.

SITUATION OVERVIEW

Security continues to rank as a top technology concern for large enterprises. Although spending across numerous IT markets declined from 2001 to 2002, security spending remains a top priority in many organizations. In fact, in a recent IDC survey of almost

1,000 IT managers, security was rated the top priority for 2003. In addition, security was the only area in which the percentage of respondents who said spending had increased in the past six months was greater than the percentage of respondents who said it had decreased. Providing further evidence, a recent IDC study of IT decision makers indicates the security portion of many IT budgets will be increasing for 2003 and 2004. In fact, 54% said their security budgets were increasing, while 30% said they would remain the same as last year due to the prolonged economic situation and business performance.

The Secure Content Management market proved to be a primary area for security spending in 2002. In fact, the SCM market has performed extremely well over the past several years, experiencing very robust worldwide revenue growth that exceeded 29% in 2000, 22% in 2001, and an impressive 34% in 2002. IDC believes the robust growth in the Secure Content Management market has been driven by the factors described in the following sections.

ENTERPRISE EFFICIENCY

Nonbusiness-related Web surfing, personal emails and messages, and spam are time-consuming distractions that can hinder an employee's productivity. Personal emails containing jokes, chain letters, pictures, and games affect the productivity of the sender and recipient as well as the business productivity of other corporate users by clogging servers, workstations, and Internet links. Employees who visit pornographic Web sites from the workplace are still the biggest concern to an organization. However a myriad of Internet-based distractions now competes for employee time. Internet shopping, online stock trading, auction bidding and selling, online games, streaming media, music and video downloads, and job searches all tempt workers.

Content Security solutions were originally introduced to block and filter inappropriate and nonbusiness-related Internet use. Today, content security has evolved to provide both filtering and improved productivity within the corporate environment. This approach supports a broader, proactive, and knowledge-based environment for corporate users. The focus is a "productivity-enhancing" level of Internet use that optimizes individual employees' use of the Internet and better harnesses overall organizational intelligence. IDC believes content security solutions will continue to increase efficiency by reducing distractions and keeping workers focused.

SPAM

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. As stated previously, more than 40% of the respondents to IDC's email retention survey, which recently surveyed 557 North American organizations, indicated that the number of spam emails received during an average day has risen 50–100% compared with the number received 12 months earlier.

Spam not only drains worker productivity and consumes valuable IT resources such as disk storage, CPU cycles, and network bandwidth, but it can also expose the organization to legal liability due to the offensive nature of some messages. For example, Web-enabled mail clients automatically display pornographic images of some solicitations. There are many examples of lawsuits brought against corporations because an employee was offended. Spam is also another conduit for unknown viral applications into the corporation, links to pornographic or objectionable Web sites, and sensitive company information leaks.

In many cases, senders of unsolicited commercial email (spammers) are resorting to outright criminality in their efforts to conceal the source of their ill-sent missives. They often use Trojan horses to turn the computers of innocent consumers into secret spam zombies. The Trojan listens on a randomly chosen port and uses its own built-in mail client to dash off a message to a Hotmail account, putting the port number and victim's IP address in the subject line. The spammer then routes as much email as possible through the captured computer, knowing that any efforts to trace the source of the spam will end at the victim's Internet address. IDC believes worms and viruses will increasingly use spam techniques. These techniques include not just the exploitation of unprotected mail relays to maximize spread but also the use of social engineering to trick victims into opening malicious files. With the creativity of spammers likely to increase, companies must ensure that protective measures are widely deployed across all types of clients.

REGULATORY ISSUES

High-profile corporate accounting scandals and turmoil in certain vertical markets have driven a new set of federal regulations. Much of this legislation is aimed at ensuring greater accountability at public companies, providing oversight and review of equities research and sales, and safeguarding the security of consumer records in healthcare and financial settings.

As the use of email and IM increases, the need for solutions to secure, monitor, archive, and retrieve these communications has become imperative. This is especially true for financial services firms. Under SEC Rule 17a-4 and NASD rules 3010 and 3110, financial services firms are required to supervise and record all electronic communication between employees and clients. In addition, the GLBA requires financial services firms to ensure the security and confidentiality of customers' private records and information. Ongoing investigations and multimillion-dollar fines in these areas will continue to force organizations to reexamine their Web and email compliance efforts and look to SCM solutions to help solve this problem.

Companies involved in delivery of healthcare services or handling of claims must ensure compliance with HIPAA, which requires all patient healthcare information be protected to ensure privacy and confidentiality when electronically stored, maintained, or transmitted. These requirements will be a critical force behind the implementation of security technologies not only in the healthcare services industry but across all healthcare entities, including insurance, government, and education. The very openness of the Internet and email makes them inherently insecure, opening the door to security breaches, information interception, and potentially devastating liabilities. HIPAA became effective April 14, 2003, and carries penalties of up to \$250,000 in fines and jail time of up to 10 years.

In addition to the regulations in the financial services and healthcare markets, a new California law, SB 1386, which protects consumer information from fraud, could be a sign of things to come from other jurisdictions in the United States and in other countries. The law mandates public disclosure of computer security breaches in which confidential information of any California resident may have been compromised. The law covers every enterprise, public or private, doing business with California residents. Starting July 1, 2003, companies that fail to disclose that a security breach has occurred could be liable for civil damages or face class actions.

In all these cases, penalties for privacy legislation noncompliance can be severe and include government fines, litigation costs, marketing sanctions, and brand reputation damage.

C O R P O R A T E C O N F I D E N T I A L I T Y

For many companies, preventing leaks of confidential information is key to the success of their business. The Web, email, IM, and P2P applications are easy outlets for accidental or deliberate leaks of confidential information. Alarming amounts of confidential corporate data can easily be sent out of the company email system at the stroke of a key, with no permanent audit trail. As IM use grows in the corporate world, corporations will have to contend with yet another vulnerability.

N E W T H R E A T E N V I R O N M E N T

Viruses continue to be, by a wide margin, the most common threat facing corporations today. According to a recent IDC survey of 325 firms across the United States, 82% of respondents said that they had experienced a virus attack. Of the organizations that experienced a virus attack, 30% reported that the virus was detected but not immediately repelled. This response indicates that even virus attacks that are detected can still cause harm. The rate at which virus attacks were not detected at all was 13.5% — obviously high enough to be a major concern to IT organizations. When both undetected and unrepelled types of virus incidents are added together, results show that an alarming 43.5% of viruses pose risks to organizations.

Although viruses and malicious code remain constant, hybrid threats such as Nimda and Code Red are now the most significant online threats to companies. A hybrid threat spreads in multiple ways including as an email attachment and by exploiting vulnerabilities in Web servers.

Because hybrid and blended threats are designed to get past point-solution security systems, there will be a strong push toward a "layered security" approach that will be better able to combat blended threats. It is clear that antivirus alone is not the answer to these more sophisticated threats. The layered security approach combines solutions such as desktop antivirus, server and gateway antivirus, and content filtering for Web and email to combat the new threat environment.

Moreover, it is now common for viruses to have a specific target. The latest variant of the Bugbear computer virus is being investigated by the FBI after the virus was found to be specifically targeting banks among its many potential victims. Bugbear is a mass-mailing worm that also spreads through networks and is particularly dangerous because it can log keystrokes on a user's computer, potentially giving personal information and account numbers to an attacker. This is not just a threat to financial institutions across the world; it is also a threat to anyone conducting financial transactions over the Internet. The virus also contains backdoor capabilities and can shut down antivirus and firewall programs.

The corporate network is no longer contained within the walls of the company. Clients are now highly mobile. Mobile phones and smart handheld devices are also becoming more tempting targets for virus writers. To date, there have been several examples of viruses specifically developed to exploit vulnerabilities in mobile phones and handheld computers. The majority of these viruses have been harmless, but they have laid the "proof of concept" groundwork for others to follow. Attacks on corporate computer systems, both wired and wireless, will continue to become more sophisticated and will target multiple vulnerabilities in the network.

L E G A L L I A B I L I T Y

Legal liability risks around employees downloading MP3s and full-length DVDs on corporate hard drives is becoming a major concern for corporate executives and legal departments. The RIAA recently collected a \$1 million fine from an organization found

to have copyrighted music files on the corporate network. In addition, the RIAA, the MPAA, and other groups 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. Employees who use the Web and P2P networks to download copyrighted material are clearly becoming a potentially very expensive liability.

In addition, the fact that emails sent by employees are done so on behalf of a company impacts the corporate image. Anything sent from a corporate email address is effectively written on electronic company letterhead. As a result, any views, quotes, or discussions made via company email can be representative of the company and legally binding. There are also many examples of lawsuits filed against companies whose employees have made racist or sexist remarks transmitted by email.

Employees who visit pornographic or racist/hate sites also represent a major legal liability concern for many organizations. In fact, according to SexTracker, 70% of all Internet pornography traffic occurs during the 9:00 to 5:00 workday. This is clear evidence that employees visiting inappropriate Web sites from the office are still a risk to their employers. IDC believes SCM solutions will continue to have success in addressing these issues.

RESOLVING THE PROBLEM

Secure Content Management requires multiple tools and staffing resources, yet its value isn't always clear. In many cases, Secure Content Management is a lose-lose situation for IT departments. If they do their job perfectly, they are looked upon as just "doing their job." If something does get through, such as a virus, malicious code, spam, or inappropriate content, then the IT department has clearly failed.

How should organizations deal with this challenge? IDC believes that three critical elements provide the most effective help for building the best defense with the least impact on IT resources:

☒ **Consolidated client.** The ability to install and configure one product that performs multiple functions reduces the time of installation and, more important, the long-term support costs. With a consolidated client, the integration between the different security functions is built in. In addition, the chance of conflicts with other applications is reduced because the security functions are delivered in a complete integrated solution. Additionally, an integrated solution will result in lowered internal support and training costs because the IT staff needs to be trained on only one product.

Many customers have told us of the importance of an integrated client with respect to their remote access solutions. In fact, a large financial institution recently told us that client-less virtual private networks (VPNs) were scheduled for a massive deployment, but the IT department was concerned that a secure connection without a secure client was worthless. Moreover, a corrupted client represents a severe security threat because malicious code could traverse the VPN and gain trusted access to internal corporate resources. Therefore, this bank delayed the client-less VPN solution until it found a consolidated client.

☒ **Unified management interface.** Customers want a consolidated console for managing all the SCM applications along with aggregated reporting, analysis, and control functions so that they can reduce IT administration chores and costs as well as personnel costs. They also benefit from a single management interface across many applications because of the economies of scale when installing software updates and providing enterprisewide managed security services.

Senior management continually demands that IT do more with less. A consolidated console means that less time is spent on repetitive administrative tasks, educating operators on various product interfaces, and reviewing overlapping logs. In large distributed environments where direct IT support is financially impossible, the ability to manage large numbers of individuals working at home, work sites, and large remote facilities is critical.

- ☒ **Delegated administration.** Anytime you can move a task from IT to users, you have reduced the level of IT administrative cost. Delegated administration can increase enterprise productivity with the decentralization of activities across organizations. The process simplifies the management of users for immediate creation, maintenance, and termination of user access rights. In the SCM area, users can help manage false positives (e.g., legitimate emails that were blocked by spam filters), identify new spam sources, and categorize Web sites that are potentially harmful.

THE CA SOLUTION: eTRUST SECURE CONTENT MANAGEMENT

C O R P O R A T E O V E R V I E W

Computer Associates International Inc. (CA), one of the world's largest software companies, delivers software and services that enable organizations to manage their IT environments. Focus areas include network and systems management, storage and security management, portal and business intelligence, and application life cycle management. Founded in 1976, CA is headquartered in Islandia, New York, and operates in more than 100 countries. CA's core strength lies in its expertise in systems, network, and security management as well as its long history in the antivirus market. CA's eTrust Secure Content Management builds upon the preventative capabilities of antivirus software and integrates with eTrust Security Command Center for security management.

e T R U S T S E C U R E C O N T E N T M A N A G E M E N T

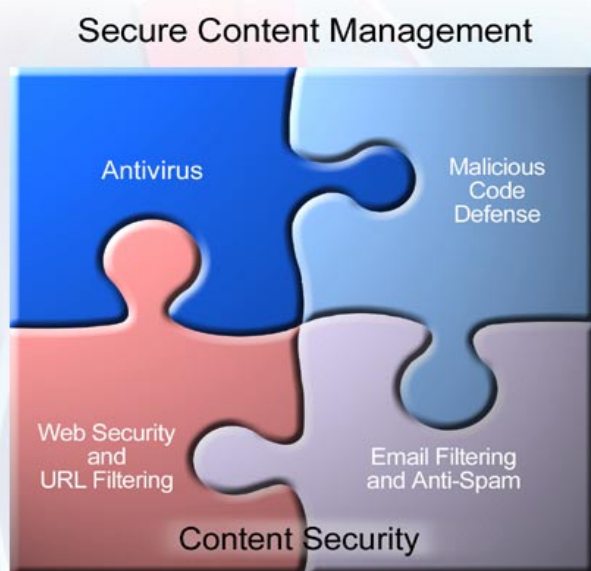
eTrust Secure Content Management is built on the foundation of CA's antivirus business and addresses the evolution of the threat environment that requires a more comprehensive view and a larger set of solutions (see Figure 1). eTrust Secure Content Management utilizes an adaptive approach that is built around:

- ☒ **Antivirus.** CA offers antivirus double protection by using two separate virus scanning engines built into the product, designed to catch more threats than a single scan engine. This allows for a much higher degree of accuracy in detecting both known and unknown threats.
- ☒ **Email and content security.** CA uses keyword identification to safeguard against the transmission of proprietary information via email. The keyword filter can also be used to enforce compliance with privacy regulations (e.g., HIPAA, GLBA, and SEC) by scanning messages for words or phrases that may contain private information. In addition, the filter can minimize legal liability risks by blocking offensive emails from leaving or entering the organization.
- ☒ **Spam filtering.** With CA's spam filter, individual users are able to define what they consider to be spam. This allows for a much higher degree of accuracy in blocking spam and reduces the chance of false positives by allowing the user to define what he or she considers spam. This type of self-administration helps offload spam management tasks from overburdened IT departments to users.

- ☒ **Web security.** CA's Web security can help organization increase employee productivity, reduce legal liability, and maximize corporate resources by preventing misuse of Web surfing by corporate users. By using a comprehensive filter of URLs, CA can prevent users from visiting inappropriate Web sites, downloading music and video files, and other types of nonbusiness-related Web activities.
- ☒ **Malicious code.** CA offers proactive identification to block malicious code from entering the organization. With an ever-escalating number of employees accessing the Internet to perform their everyday business activities, virus writers are increasingly targeting Java and ActiveX code in Web sites as another means of distribution. CA's malicious code detection provides an added layer of security that addresses the growing mobile code threats.

FIGURE 1

SECURE CONTENT MANAGEMENT COMPONENTS



Source: IDC, 2003

CHALLENGES/OPPORTUNITIES

With eTrust Secure Content Management, CA is making a bold move in tackling the complex challenges inherent in content security. The customers IDC spoke with agree and are eager to gain more centralized control with Secure Content Management. They want centralized control over intellectual property and confidential data, such as product plans and discount schedules, whether the information is warehoused in the corporate database or on an employee's mobile device. Corporate IT departments want corporatewide enforcement of data usage policies so that unauthorized or inadvertent releases of confidential information are reduced or eliminated. We believe that CA's

strength in management products (network, systems, and security) brings integrated administration to the SCM space at a critical time when the challenges of securing content are threatening to overwhelm many IT departments. eSCM is a valuable solution for many customers that need a unified environment to reduce the complexity of purchasing, installing, and managing this challenging environment.

To meet future customer demands, CA's eSCM solution must be not only complete but also nonintrusive. Customers believe that by combining content management and security they can address the business aspects of the problem and improve end-point security compliance with a largely user-transparent implementation. In this respect, IDC believes CA must develop a unified management console for the eTrust Secure Content Management solution. Moreover, customers will expect tight integration between Secure Content Management and remote access solutions, especially clientless or SSL VPN. An integrated Secure Content Management solution would check the security of the client before allowing access to the VPN. IT managers realize that "trusted" users gaining access through fully authenticated VPN connections represent a potential new source of worms, Trojans, and other malicious code.

While these concerns may look like daunting challenges for CA's eTrust Secure Content Management, we believe that most of the essential capabilities are currently under development by CA. We fully expect that CA's solutions in this area will meet or exceed most customers' expectations.

CONCLUSION

Management is essential to helping secure content and users' end-point systems. It also addresses the lose-lose situation that many IT organizations face as they see the rising onslaught of new content-oriented threats. Strong management can make it easier for IT departments to secure content against emerging new threats while not interfering with ongoing business.

A unified approach is needed to deal with this situation. Antivirus software works well to block viruses. However, the increased complexity of threats, including hybrid viruses and spam, requires a new security approach. Content security is much more complex, focusing on "what" information is being sent to "which" Web site/email address. A strong policy engine that is centrally managed and efficiently distributed to remote sites and users is essential to returning control to the IT organization.

CA's eSCM solution provides the framework for an enterprisewide integrated solution. It builds the company's antivirus foundation and addresses evolving threat environment. Moreover, Computer Associates' core strength is in systems, network, and security management. This alliance of deep IT management knowledge with secure content control is a robust combination of business priorities with intelligent security management. In eSCM, CA leverages its management expertise to provide a valuable, integrated, enterprisewide SCM solution that customers should investigate. Overall, IDC believes CA's eSCM is well positioned to serve the broad base of market demand for an integrated content security solution.

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 2003 IDC. Reproduction without written permission is completely forbidden.