IDC
Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

Content Security: The Business Value of Blocking Unwanted Content

Sponsored by: SurfControl

Brian E. Burke

July 2003

IDC OPINION

Preventing unwanted content from entering the corporate network is an essential ebusiness necessity for organizations using the Internet, email, and the Web. Virus infection is still the number 1 concern regarding corporate security; however, other factors, such as policy enforcement, spam, legal liability, and regulatory compliance, are increasingly driving the need to scan email, instant messaging, and Web traffic for confidential data, inappropriate content, intellectual property, and unsolicited email.

This study presents SurfControl's Content Security solution as an example of how organizations are using content security technologies to address internal security risks associated with misuse of the Web, instant messaging, peer-to-peer networks, and email applications. This paper details the following risks associated with managing unwanted content. Highlights are as follows:

- Spam is no longer just a nuisance: It is quickly becoming both a potential legal liability and a major productivity drain on 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 received 12 months earlier.

- Instant messaging has entered the corporate world, bringing with it another layer of security concern. Unsecured instant messaging applications in corporations are putting enterprise systems at risk to virus infection, hackers, legal liability, and violation of privacy regulations. Moreover, instant messaging 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., HIPAA, GLBA, and SEC) continue to fuel the explosive growth of content filtering and messaging security. As the use of email and instant messaging increases, the need for solutions to secure, monitor, archive, and retrieve communications has become imperative for healthcare and financial services firms.

- Legal liability risks around employees downloading MP3s and full-length DVDs on corporate hard drives are drawing the attention of top-level executives. 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.

- A myriad of new Internet-based distractions are increasingly affecting employee productivity. Internet shopping, online stock trading, auction bidding and selling, online games, streaming media, MP3s, and even searching for outside employment all tempt workers. Personal emails, such as jokes, chain letters, pictures, and games, as well as spam, affect not only the productivity of the sender and recipient but also the business communications of other corporate users by clogging servers, workstations, and Internet links.

METHODOLOGY

IDC developed this White Paper using a combination of existing market forecasts and direct, in-depth, primary research. To gain insight into the challenges facing enterprises — and to learn more about how the SurfControl solution set helps address these challenges — IDC conducted in-depth interviews 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 SurfControl team to review their goals and tactics. This study reflects all of these research perspectives.

IDC MARKET DEFINITION: CONTENT SECURITY

Content security is a subset of the secure content management market. The content security market includes policy-based technologies that monitor Web and messaging applications for inappropriate content, spam, intellectual policy breach, non-compliance, and banned file types. The two key components of content security include:

- **Web filtering software.** Web filtering software is used to screen and exclude from access or availability Web pages that are deemed objectionable or non–business related. Web filtering is used by corporations (to enforce corporate policy), schools and universities, and home computer owners (via parental controls).

- **Messaging security software.** Messaging security software is used to screen messaging applications such as email, instant messaging, short messaging service (SMS), and peer-to-peer for spam or other objectionable content. The software is also used to enforce corporate policy by screening for company-confidential information and to enforce compliance with privacy regulations (e.g., HIPAA, GLBA, and SEC). Messaging security also includes secure email.

SITUATION OVERVIEW

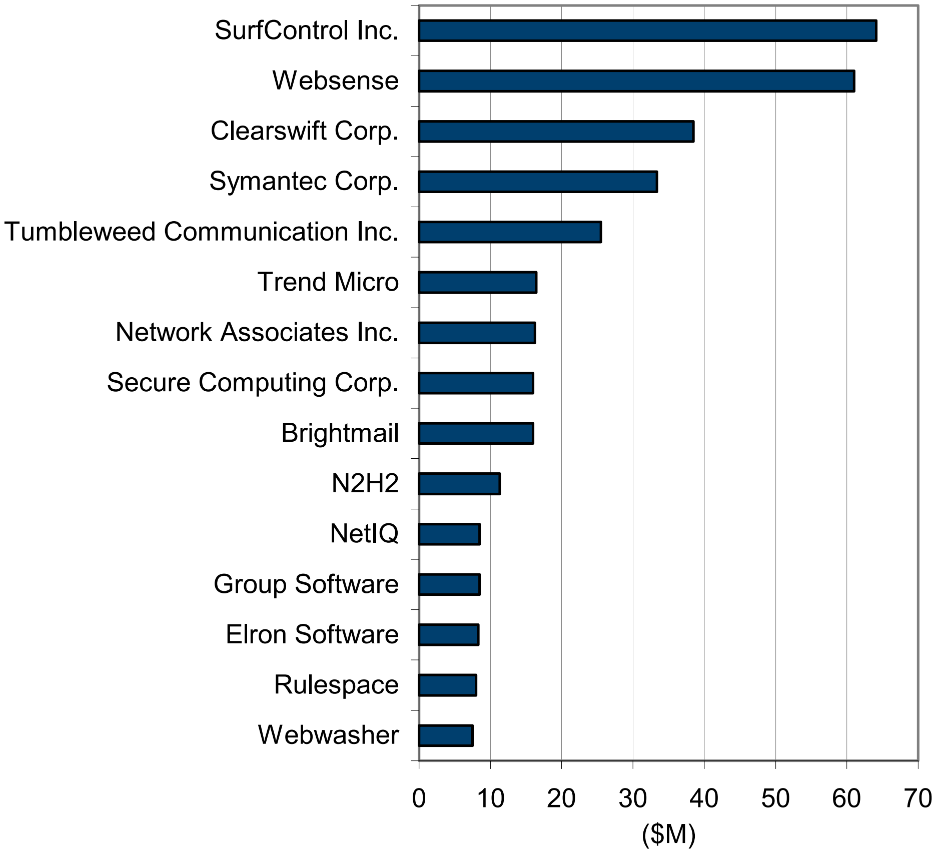
2002 CONTENT SECURITY MARKET

Worldwide revenue for content security software reached $506 million in 2002, representing 49% growth over 2001. SurfControl led the content security market in 2002 with $64.1 million in revenue, as shown in Figure 1. The impressive growth in the content security market in 2002 was largely driven by the adoption of messaging security solutions to prevent spam, comply with privacy regulations, and reduce legal liability.

Worldwide revenue for content security software reached $506 million in 2002, representing 49% growth over 2001. SurfControl led the content security market in 2002 with $64.1 million in revenue.

FIGURE 1

WORLDWIDE CONTENT SECURITY REVENUE BY VENDOR, 2002



Source: IDC, 2003

BUSINESS VALUE OF BLOCKING UNWANTED CONTENT

Unmonitored use of the Internet, instant messaging, peer-to-peer, and email hits corporations on many levels. First, there are wasted investments in Internet infrastructure. Next, there are productivity drains on distracted staff and on help desks whose time is drained by having to support both work-related and non–work-related Internet use. Finally, unregulated use sets up an environment where private or confidential data can be misused or mishandled and where regulatory breaches are likely. These issues are discussed in detail below.

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. 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, 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. 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, using 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. Spammers take it from there, routing as much email as they like 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 (not just the exploitation of unprotected mail relays to maximize spread), using social engineering to trick victims into opening malicious files.

IDC believes worms and viruses will increasingly use spam techniques (not just the exploitation of unprotected mail relays to maximize spread), using social engineering to trick victims into opening malicious files.

- While spam is a newer problem for IT to solve, IDC believes first- and second-generation anti-spam capabilities are already integrated into existing "messaging security" infrastructure. We believe spam will become a feature of a total messaging security solution that prevents leaks of private or confidential data, inappropriate emails, large files, viruses, and other messages that violate corporate policy. IDC believes the problem is broader than just spam, and the solution needs to be broader as well, not just a spam filter.

INSTANT MESSAGING AND PEER-TO-PEER COMMUNICATIONS

- Instant messaging has entered the corporate world, bringing with it another layer of security concerns. Instant messaging 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 that system via insecure instant messaging applications. Viruses can also enter via file transfers between users, threatening 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 peer-to-peer 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 a target for back doors and Trojans.

LEGAL LIABILITY

- Legal liability risks around employees downloading MP3s and full-length DVDs on corporate hard drives are becoming major concerns. The Recording Industry Association of America (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 Motion Picture Association of America, 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.

- The fact that messages sent by the employees of an organization is done so on behalf of that company presents a major concern for 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 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, 70% of all Internet porn traffic occurs during the 9-to-5 workday (SexTracker). This is clear evidence that employees visiting inappropriate Web sites from the office still represent a risk to organizations.

PRIVACY REGULATIONS

- High-profile corporate accounting scandals and turmoil in certain vertical markets have driven a new set of federal regulations 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 instant messaging increases, the need for content security solutions to secure, monitor, archive, and retrieve these communications has become imperative 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 Gramm-Leach-Bliley Act requires financial services firms to ensure the security and confidentiality of customer 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 content security solutions to help solve this problem.

As the use of email and instant messaging increases, the need for content security solutions to secure, monitor, archive, and retrieve these communications has become imperative for financial services firms.

- The mandate to ensure compliance with the Health Insurance Portability and Accountability Act of 1996 — which requires that all patient healthcare information be protected to ensure privacy and confidentiality when electronically stored, maintained, or transmitted — 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 it inherently insecure, opening the door to security breaches, information interception, and potentially devastating liabilities. HIPAA became effective April 14 and carries penalties of up to $250,000 in fines and jail time of up to 10 years.

- A new California law, SB 1386, meant to protect consumer information from fraud, could be a sign of things to come from other states and possibly other regions across the world. 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, those who fail to disclose that a security breach has occurred could be liable for civil damages or face class actions.

CONFIDENTIAL INFORMATION

- For many companies, preventing leaks of confidential information is key to the success of their business. The Web, email, instant messaging, and peer-to-peer applications are an easy outlet 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 hard evidence (such as a paper trail or floppy disk) to show for it. As instant messaging use grows in the corporate world, corporations will have another vulnerability to contend with.

The Web, email, instant messaging, and peer-to-peer applications are an easy outlet for accidental or deliberate leaks of confidential information.

VIRUSES AND MALICIOUS CODE

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

- 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 clearly a threat to financial institutions across the world. The virus also contains back-door capabilities and can shut down antivirus and firewall programs.

- 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 these two types of virus incidents are added together, results show that an alarming 43.5% of companies are at risk from viruses.

According to a recent IDC survey of 325 firms across the United States, 82% of respondents said that they had experienced a virus attack.

EMPLOYEE PRODUCTIVITY

- Pornographic sites are still commonly visited from the workplace; however, a myriad of new Internet-based distractions now compete for employee time. Internet shopping, online stock trading, auction bidding and selling, online games, streaming media, MP3s, and even searching for outside employment all tempt workers. Personal emails, such as jokes, chain letters, pictures, and games, affect not only the productivity of the sender and recipient but also the business communications of other corporate users by clogging servers, workstations, and Internet links.

- Although the Internet is a superb research tool, distractions are only a click away. Web sites that offer vacation travel, entertainment, sports, news, pornography, and politics result from even the most benign, business-oriented searches. Banner advertisements are also powerful lures for even the most focused user. Employees accessing inappropriate Web sites, along with the drain on employee time and corporate resources that results from excessive personal use of the Web and email, will continue to be concerns that corporations must manage.

BEST PRACTICES: HOW TO RESOLVE THE CHALLENGES

IDC's interviews provide the "voice of the user" to describe what is most important to IT executives across a range of industries and how they approach resolving the challenges of blocking unwanted content.

MAXIMIZE CORPORATE RESOURCES AND USER PRODUCTIVITY

Employees are undoubtedly an organization's most important resource — and again, although the Internet is a superb research tool, distractions are only a click away. One executive we spoke with said:

> Our main reason for implementing this technology was employee productivity. Our main concern was cutting down non–business-related Web surfing during work hours. With the SurfControl solution, we were able to set up a list of job-related sites for employees to access, while at the same time limit the non–work-related sites. We obviously blocked all sites related to pornography.

Companies can customize lists of work-related sites, often called a "white list," to help maintain and optimize employee, workgroup-, corporate-, and industry-level libraries of information and useful information sites. This productivity-enhancing level of Internet use will both optimize individual employees' use of the Internet and better harness overall organizational intelligence.

In addition, organizations that monitor email and Web usage patterns can create usage policies that can help unclog valuable bandwidth resources. Many corporate users may not be aware of the network bandwidth consumption associated with emailing or downloading large files (i.e., MP3s, video clips, and streaming media). This type of activity not only affects the network performance of the responsible party, it also degrades network performance for all corporate employees. One company executive said: "We had employees using Kazaa to download music during the day. The president of the company actually noticed a change in the performance of the Internet."

MINIMIZE LIABILITY

Like any law, reinforcements have been established in the form of penalties for those companies that do not comply with privacy regulations. Penalties for privacy legislation noncompliance can be severe and include government fines, litigation costs, marketing sanctions, and brand reputation damage. An organization's damaged brand reputation can often be more harmful than any fine associated with violating privacy regulations. IDC believes content security solutions can help organizations minimize the risk of noncompliance and also reduce the risk of bad publicity for firms that violate customer privacy regulations either intentionally or accidentally. The offending firms are often faced with customers and consumers who are likely to choose another establishment for future business dealings. As one executive put it: "You certainly don't want your employees sending out confidential data or dirty jokes and subjecting the company to liability or damage to reputation." Another executive pointed out: "The legal liability issue really jump-started the decision to implement. I read a lot of stories about other companies being sued because an employee was offended. We didn't want to take that chance."

PROTECT PROPRIETARY DATA

The inadvertent or deliberate leakage of corporate confidential data can be very costly to an organization. An executive at a pharmaceutical research firm told IDC:

> If I look at my own industry, we have an environment where we have a very, very big research and development operation, and clearly anything to do with that is sensitive in many respects. First of all, simply the commercial sensitivity of any information you are developing, because that information is very, very expensive. Classically, it takes about 10 to 12 years from developing a pattern in a compound to actually getting it to market, and very few of your patterns ever end up as a commercial product. Once you have got it in the market, you then only have another 8 to 10 years maximum to effectively actually recover the enormous research and development cost you have on it. So we always have a very, very kind of quiet focus on that importance of that data.

IDC believes this case holds true for almost any organization whose employees have access to the Web and email. The risk of proprietary information leakage out of an organization is clearly something that cannot be ignored in today's business environment.

IMPLEMENT LAYERS OF SECURITY

IDC believes content security solutions offer a very effective complement to antivirus technologies by filtering or blocking certain emails based on corporate policy. IDC believes that this layered approach can enhance an organization's overall security architecture. An IT manager we spoke with told us:

> We realized that virus protection software generally arrives two days after the virus hits. And if we were smart, we would be able to identify the kinds of files or the names of files that are coming in and be able to quarantine and block those before they even made it into our networks, giving us some advance ability to protect ourselves without ever having the virus protection there. So with all of that in mind, that is one of the reasons that we have deployed the content filtering.

PREVENT FALSE POSITIVES

In many organizations, the concern about false positives, or blocking legitimate email, has been the main barrier to anti-spam implementation. An executive at a banking consulting firm commented to IDC that:

> We were getting so much spam, I can't even begin to tell you. Our main concern with implementing an anti-spam product was the chance of accidentally blocking non-spam messages. With the SurfControl product, I was able to use their rule set to customize my own set of rules and minimize the chance of over blocking. With their rule set, you can do almost anything.

THE SURFCONTROL SOLUTION

COMPANY OVERVIEW

Since the initial launch of its first Web filtering software in 1998, SurfControl has expanded from a small engineering team into the worldwide leader for content security solutions. SurfControl employs nearly 450 people and has more than 20,000 customers worldwide. SurfControl has nine offices worldwide: California and Massachusetts in the United States; Manchester and London in the United Kingdom; Rotterdam, Holland; Vienna, Austria; Frankfurt, Germany; Singapore; and Sydney, Australia.

SurfControl delivers on its promise to help companies "Stop Unwanted Content" in the workplace by continuing to expand its product offering for filtering to address new content risks as they emerge. The product set in the SurfControl total filtering solution — Web, E-mail (including Anti-Spam and Anti-Virus), and Instant Message — offers a complete Web and messaging security solution that addresses Internet, email, instant messaging, and peer-to-peer applications. The content security solutions can be managed from a single workstation with SurfControl's remote management capabilities.

SurfControl offers a total content security solution addressing the Internet, email, instant messaging, and peer-to-peer applications.

PRODUCT OVERVIEW

SURFCONTROL WEB FILTER™

SurfControl Web Filter serves as a line of defense between employees and the Internet by examining requests and allowing or denying them based on company-specific rules. By providing both platform-independent and platform-integrated solutions, SurfControl Web Filter requires no change to an organization's architecture. SurfControl Web Filter incorporates quality content, artificial intelligence, multiple deployment options, and comprehensive reporting and analysis. Flexible rule creation gives organizations the ability to restrict access to sites they deem inappropriate, as well as create threshold rules that set time or size limits to manage access. These options protect users from excessive non–business-critical surfing, security threats, and potentially inappropriate material.

SurfControl offers both pass-by and pass-through filtering technology that watches Internet and email traffic as it crosses ports, determining how to handle each request as defined by corporate policy. This gives organizations the ability to not only secure the network and protect the organization but also to completely stop unwanted information before it enters the corporate network.

SURFCONTROL E-MAIL FILTER™

SurfControl E-mail Filter defends users and mission-critical email from risks by automatically and intelligently identifying threats, as defined by corporate policy. Developed as a safeguard, SurfControl E-mail Filter uses an industry-leading anti-spam database and advanced lexical analysis. Through the use of artificial intelligence and a multitude of anti-spam techniques, email is reviewed before it reaches the corporate mail server, giving an organization protection from harmful email content and spam, as well as the possible disclosure of confidential data.

INSTANT MESSAGING AND PEER-TO-PEER NETWORKING

Up until now, the content risks delivered via "port-agile" public instant messaging and peer-to-peer applications have been greatly underestimated. SurfControl Instant Message Filter™ is designed to give organizations control over the use of instant messaging and peer-to-peer applications inside their network. By combining comprehensive instant messaging and peer-to-peer signature-recognition technology with the ability to block access to these applications down to a unique IP address or subnetwork, organizations have an easy and effective way to protect their network and business from predefined security risks.

ARTIFICIAL INTELLIGENCE

As an extra layer in the fight against ever-changing content risks, SurfControl uses a set of artificial intelligence tools and techniques, collectively called Adaptive Reasoning Technology, to cover objectionable content that most often emerges quickly and without warning. SurfControl's "V" product range (including Virtual Control Agent™, Virtual Image Agent™, and Virtual Learning Agent™) uses artificial intelligence to dynamically recognize and update filtering tools as new inappropriate or high-risk information appears.

PRODUCT ARCHITECTURE

The SurfControl content security solution is built on the technologies detailed below.

URL CATEGORY LIST

The URL category list consists of 40 categories containing millions of "human-reviewed" Web sites. The SurfControl global content team researches, reviews, and categorizes Web sites in more than 65 languages covering more than 200 countries. Customers receive daily updates, representing more than 35,000 sites a week.

EMAIL DICTIONARIES

SurfControl E-mail Filter comes equipped with 15 dictionary categories covering multiple languages, including Dutch, English, French, German, Italian, and Spanish. Each dictionary contains a list of category-specific words and phrases that are each assigned a point value. Both the words and values are completely customizable. Users can also add or delete words and phrases to create dictionaries that serve specific company needs.

ANTI-SPAM AGENT™

A constantly updated database of electronic signatures of spam and junk email gives organizations the ability to stop spam by deciding which emails to restrict or allow and how to handle them. The email-filtering content database classifies each message by type, such as "Adult," "Hoax/Rumor," "Illegal Material," and "Chain Letter," as well as by media type, such as text, graphics, and executable.

ANTI-VIRUS AGENT™

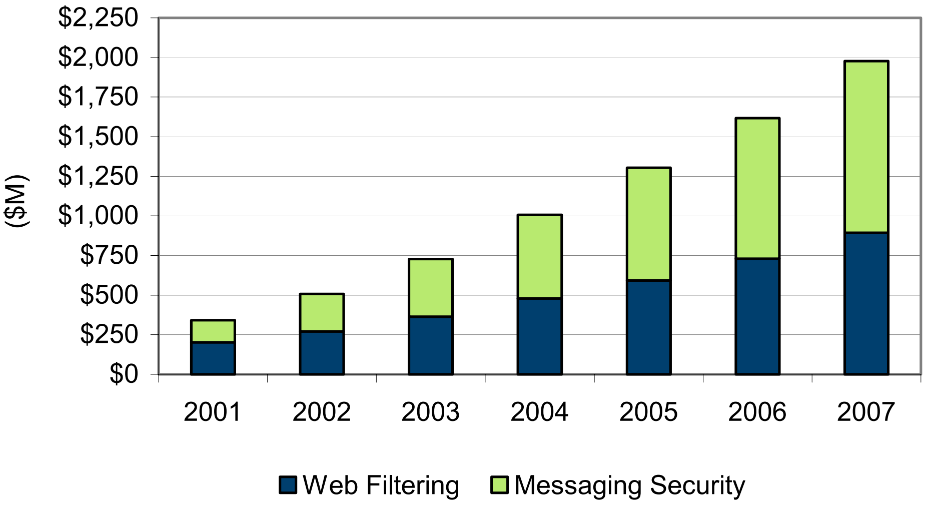
Powered by McAfee, SurfControl's Anti-Virus Agent (AVA) offers complete virus cleansing, scanning, and blocking, as well as automatic updates of new virus signature files, giving organizations immediate protection against new risks.

FUTURE OUTLOOK

As Figure 2 shows, IDC believes the market for content security solutions will grow from $506 million in 2002 to almost $2 billion by 2007, representing a 31% compound annual growth rate (CAGR). IDC believes customers will continue to buy point solutions, but this will be the exception, not the rule. Anti-spam will continue to be an important driver in adoption of content security; however, we believe it will become a feature of messaging security, not a distinct market.

FIGURE 2

WORLDWIDE CONTENT SECURITY REVENUE BY SEGMENT, 2001–2007 ($M)



Source: IDC, 2003

CHALLENGES AND OPPORTUNITIES

With so much media coverage of hacking and viruses, enterprises may require education on the value of enhanced content security and management of Web, instant messaging, peer-to-peer, and email usage. Many executives are still struggling to understand the business value of the many types of IT security technologies. The challenge is to make organizations understand the risk of Internet content — an information risk that may, in fact, be as or more damaging than the damage from infrastructure threats. As discussed earlier, a key role of message security is protecting confidential information. For SurfControl to widen its customer base, executives need to understand the value of technologies that prevent waste and misuse, protect against legal liability, and prevent leakage of confidential data as well as they now understand the value of technologies that detect viruses and attempted break-ins.

The challenge of protecting remote employees is another area SurfControl can address in the near future. As the corporate network continues to expand beyond the firewall, the challenge of protecting an increasing number of remote clients and types of clients will be essential to ebusiness enablement. IDC 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 who move around). PECS will provide a platform for client security solutions such as antivirus and content filtering. As mobile text messaging becomes more widespread, SurfControl will need to cover that communication sphere as well, either directly or through close partnerships.

CONCLUSION

Unlike traditional security products, content security's business value is easily understood. Protection from legal action, increased productivity, compliance with privacy regulations, and the maximization of corporate assets are demonstrable benefits. IDC believes this market will continue to become a major element in most customers' security architectures.

The solution set from SurfControl can play a key business role in intelligently filtering unwanted content from entering an organization. By taking a multilayered approach and providing stronger controls on Web, instant messaging, and email usage under a common user interface, these products provide a critical enhancement to traditional IT perimeter security products. SurfControl, a well-known leader in Web filtering, has clearly established itself as a major player in the messaging security market as well, growing 387% from 2001 to 2002. IDC believes SurfControl is well positioned for continued success in the content security market.