

WHITE PAPER

Content Filtering: Multiple Layers of Threat Protection

Sponsored by: SurfControl

Tim Sheedy
September 2005

IDC OPINION

While viruses tend to be considered the major threat to organisations, spam and spyware are beginning to eat away at organisations productivity and efficiency, and in many respects could end up costing companies considerably more than they realise. To combat this, IDC advises that Australian businesses should:

- ☒ Introduce multiple layers of messaging and web filtering security to address the increasing number and sophistication of threats that are capable of infecting corporate networks.
- ☒ Implement solutions to scan email, instant messaging (IM), desktop applications and web traffic for confidential data, inappropriate content, intellectual property and unsolicited email — not only for viruses, but for spam, spyware and any other threat to an organisation.
- ☒ Ensure business communications comply with applicable government and industry regulations such as the Industrial Relations and Privacy Acts, various government mandates, and Australian Prudential Regulation Authority (APRA) and Australian Stock Exchange (ASX) regulations and guidelines.

IN THIS WHITE PAPER

In this IDC White Paper, we provide an overview of the trends driving the adoption of email and web filtering as well as antispymware software. A discussion of specific events noted in the press impacting Australian organisations to procure these security solutions, and the regulatory environment requiring such solutions, are included. IDC also provides recommendations for addressing the messaging and web security challenge in addition to thoughts on the future of the market as it may impact the long-term sustainability of certain providers and in turn customers' decisions about vendor selection.

METHODOLOGY

This White Paper leveraged worldwide research as the basis for a global understanding of the messaging security market, two key reports used specifically in this research were:

- ☒ *The Real Cost of Spam and Value of Antispam Solutions: What to Do About the Rising Cost of Spam* (IDC #TB20040902, August 2004).
- ☒ *Worldwide Spyware 2004–2008 Forecast and Analysis: Security and System Management Sharing Nightmares* (IDC #32229, November 2004).

A local study was also conducted, but as the respondent base was not statistically significant due to a small sample size, all research findings from those surveys were used for trend and discussion purposes only. The study consisted of interviews with 15 channel and 15 end-user organisations (total: 30). As SurfControl commissioned the study, some of the channel and end-user organisations were selected specifically for the purposes of analysing SurfControl's customer and partner base. To protect against a pro-SurfControl bias, no less than five interviews of non-SurfControl partners and customers were conducted to ensure a more representative view of market dynamics.

SITUATION OVERVIEW

Introduction

The challenge of controlling electronic communications as they flow into and out of an organisation is becoming increasingly critical. Virus infection remains an important concern around electronic communications, but other factors associated with employee productivity, regulatory compliance, resources and legal liability are driving the need to monitor Internet traffic of corporate IT users. Scanning email, IM, peer-to-peer (P2P), and other messaging applications for confidential data, inappropriate content, intellectual property, unsolicited email and inappropriate web browsing are now the norm for most Australian organisations. This responsibility entails wider operational complexity than traditional perimeter security. Web and messaging security products have assumed responsibility for ensuring that:

- ☒ Business communications comply with applicable government and industry regulations such as the Industrial Relations and Privacy Acts, various government mandates, and APRA and ASX regulations and guidelines. These regulatory and legislative pressures continue to put pressure on organisations to secure the use of electronic communications.
- ☒ Corporate concerns with employee productivity, legal liability and network resources continue to fuel the growth of the web filtering market. IDC believes 30–40% of Internet use in the workplace is not related to business.
- ☒ Offensive content, such as pornography or hate material, remains outside the organisation.
- ☒ Inadvertent or deliberate release of corporate confidential information and private customer data is detected and thwarted.
- ☒ Sensitive communications receive appropriate encryption and end-to-end protection.

Legislation and Corporate Governance Requirements

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.

Despite the serious nature of misuse of corporate email and Internet access there is limited federal and state legislation regulating this area. Current recommendations of legal counsel suggest best practice is to have strong Internet and email usage policies in place and to continue to inform and update employees of them. Organisations are currently not legally inhibited from surveillance of employee email or Internet usage under the Privacy or Industrial Relations Acts.

New South Wales is the first to consider employee surveillance legislation with the proposed NSW Workplace Surveillance Bill 2005. If passed, the bill will ensure that employees receive significant notification before email and Internet usage is monitored. This notice could be up to seven days ahead of commencement of surveillance and continued notification thereafter, most probably on a daily basis, of that email and Internet usage being monitored by the employer. The new bill is likely to force organisations to put their Internet and email usage policy on logon screens to ensure employees are fully aware and consistently reminded they are being monitored. Without such a bill, the law allows employers to look at employee email and Internet usage at their own discretion.

Another key legal requirement organisations should be aware of is "vicarious liability", which makes employers liable for all activities of employees. For example, if an employee sends pornographic emails to a colleague, the company is liable for sexual harassment. Employers are also liable for illegal usage of IT systems, for example if an employee uses corporate email servers to send spam emails. If an employee divulges customer details by putting addresses of recipients of a mass email in the "to:" header rather than the "bcc:" header the company is also liable. Such cases abound in Australia and abroad with rulings often not in the favour of the company liable for an employee's misconduct.

The following is a list of the current legislation driving Australian organisations to monitor and report on electronic communications and Internet usage more closely.

- Privacy Act (excludes employees — currently under review federally)
- Telecommunications (Interceptions) Act 2979
- New South Wales Workplace Surveillance Bill 2005 (not yet passed)
- Victorian Government in discussions (waiting on outcome of the NSW bill)
- Spam Act 2003
- Cybercrime Act
- Industrial Relations Acts

Technologies

There are a range of technologies broadly mapped into what IDC calls the secure content management (SCM) solutions that help organisations and consumers monitor and manage access to Internet resources and email communications. The following analysis will evaluate the market dynamics and drivers for adoption of three key technologies in this space:

- ☒ Email filtering
- ☒ Web filtering
- ☒ Antispyware

These technologies are essential for an organisation to secure its messaging and Internet environment.

Email Filtering

Email filtering has become critical for organisations for many reasons, such as ensuring optimal productivity of employees and decreasing the load on the network, email servers and storage environments clogged with unsolicited and even malicious email traffic. Another key reason why organisations require email filtering is the convergence of spam and malicious viruses designed to attack IT users for financial gain. With the possibility of financial gain we have seen a steady rise in the number of unsolicited and spam emails and IDC expects this to only continue increasing exponentially. As a result, email-filtering software is becoming a necessity.

In addition, organisations are under pressure from IT auditors, regulators, and legislative and corporate governance bodies to monitor and report on the usage of corporate systems to send and receive email. Not only are users capable of infecting IT systems with viruses or spreading unwanted or inappropriate email traffic throughout an organisation; they are also capable of sending, either deliberately or unintentionally, intellectual property and even violations of Privacy, Trade Practices and the Corporations Acts through email to competitors or recipients that are not meant to receive such information.

In short, email filtering is no longer a nice optional extra, it is essential for any organisation to ensure compliance with legal and corporate governance requirements.

Key trends in the antispam market include:

- ☒ Antispam will continue to converge with more comprehensive messaging security over the next year. IDC survey results from the Australian Security Survey show that two out of three executives view antispam as part of a larger network security solution.
- ☒ Content filtering tools put in place to identify spam will increasingly be used to filter outbound communications for policy enforcement, regulatory compliance, and inappropriate content.
- ☒ Spam will increasingly be viewed as a security threat. Viruses, malicious code and fraudulent solicitations for privacy information will continue to use spam as a delivery vehicle.

Table 1 represents key findings of a worldwide IDC study into the financial implications of spam and the cost savings that can be achieved by implementing an antispam solution. On average, an organisation with at least 500 email users will experience up to AU\$540,000 of cost savings with an antispam solution (based on the assumption that less than half of actual time saved is translated into financial savings, as users only dedicate a portion of freed-up time to productive use). The study revealed that antispam software could deliver 24 minutes a day in time savings

per IT staffer in their management of email servers. In short, the average annual cost saving to a firm from an antispam solution is AU\$1,720.

TABLE 1

Average Productivity Cost of Spam and Savings of Antispam Solutions

	Without Antispam Solution	With Antispam Solution
Email Users		
Daily time spent by each user	10 mins	5 mins
Average annual (cost)/savings to firm	(AU\$540,000)	AU\$103,000*
IT Staff		
Daily time spent by each IT staff	43 mins	19 mins
Average annual (cost)/savings to firm	(AU\$11,325)	AU\$1,720

Note: Based on an average firm with 500 email users looking only at productivity (time spent), not other factors.

* Please note that less than half of actual time saved is translated into financial savings to adjust for a standard ROI assumption that users typically make productive use of only a portion of freed up time.

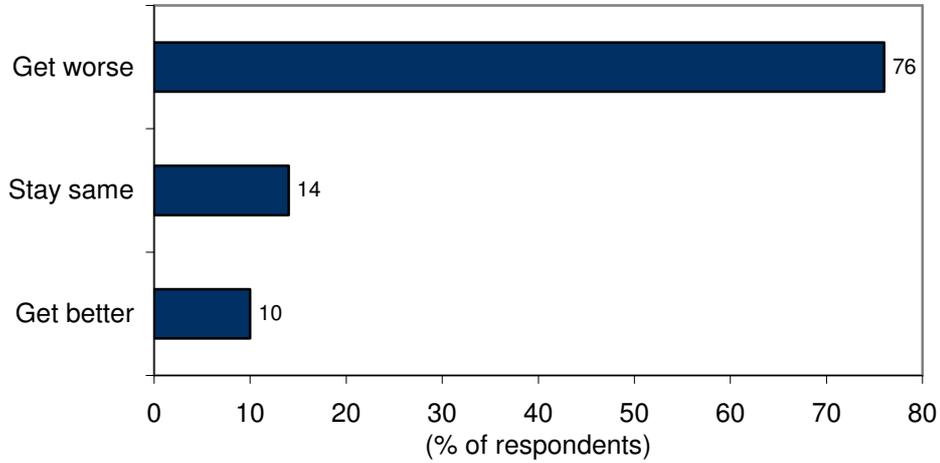
Source: *The Real Cost of Spam & Value of Antispam Solutions: What to Do About the Rising Cost of Spam* (IDC Doc #TB20040902, August 2004; revised July 2005).

In a worldwide IDC survey, 76% of respondents indicated they expect the spam problem to get worse over the next two years (Figure 1). In the same survey, 69% of respondents indicated they had an antispam solution in place (Figure 2).

FIGURE 1

Expectations of the Spam Problem

Q: In the next two years, do you expect the spam problem to get better, stay the same or get worse?

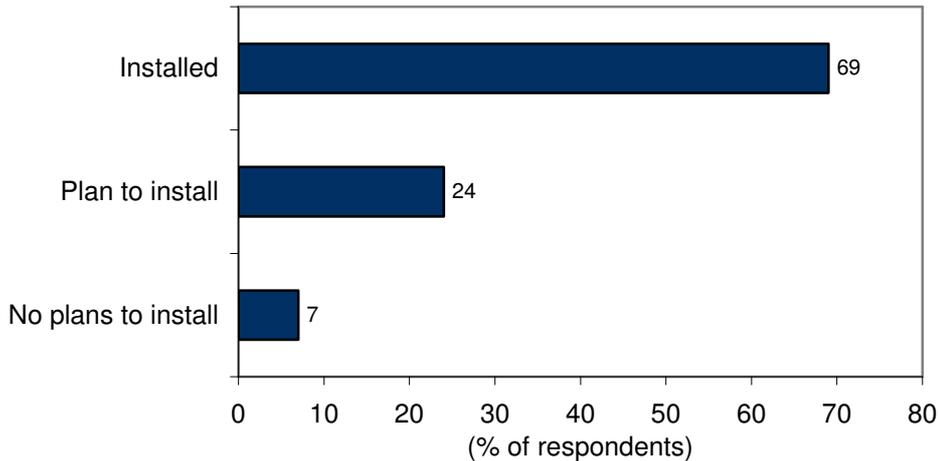


Source: *The Real Cost of Spam & Value of Antispam Solutions: What to Do About the Rising Cost of Spam* (IDC Doc #TB20040902, August 2004).

FIGURE 2

Status of Antispam Solutions

Q: Which of the following best describes your organisation's status in terms of having an antispam solution in place:



Source: *The Real Cost of Spam & Value of Antispam Solutions: What to Do About the Rising Cost of Spam* (IDC Doc #TB20040902, August 2004).

Web Filtering

The demand and interest in web filtering solutions remains strong, with corporate concerns about web security, employee productivity, legal liability and network resources on the rise. Web filtering has evolved from addressing a single class of employee distractions — access to URLs — to more robust, scalable and flexible

filtering solutions that address the complex security needs of a networked business world. Current web filtering solutions offer more mature architectures and finer-grained categorisation, as well as filtering options beyond simple “permit” and “deny”. IDC believes organisations will demand more robust, scalable and flexible filtering solutions to address the complex security needs of networked businesses. As the next generation of web filtering solutions begins to take shape, employees and employers face an ever-growing set of distractions and challenges beyond non-business-related web sites. These include:

- ☒ Web security concerns, due to the wave of web-based viruses and malicious mobile code (MMC) (e.g., NIMDA, Code Red and Bugbear) that have escaped traditional signature-based antivirus software.
- ☒ More users relying on protocols such as streaming media, IM and P2P.
- ☒ The growing number of “phishing attacks”, which has opened corporate eyes to the threat spyware poses to information security. Spyware has been known to target employees and trick them into providing corporate passwords.
- ☒ Employees installing commercially available software, rogue malware, unlicensed software and freeware/shareware.

Antispyware

Spyware is no longer just a consumer nuisance; it is quickly becoming a major security and productivity concern in the corporate environment. A recent IDC global survey of over 600 organisations listed spyware as the fourth-greatest threat to a company’s enterprise network security. IDC estimates that 67% of all computers (mostly consumer) have some form of spyware — in most cases, there are multiple spyware programs, even hundreds. The pains of spyware go beyond annoying pop-ups and are felt by both help desk and system management.

Spyware is not going away. It is not a malicious hacking challenge for programmers; rather, it is a revenue source for legitimate corporations. Table 2 represents IDC’s assessment of the historical spyware market and the expected future direction of the market over the next couple of years.

TABLE 2

IDC’s Spyware Time Line

Year	Description
2003	The majority of antispyware sales are standalone solutions sold to consumers. Spyware is just starting to become a topic of discussion in corporate security departments.
2004	Enterprises start to become concerned with Spyware. System management and help desk calls related to spyware rise at a rapid pace. Standalone antispyware vendors start to market their solutions to the corporate market in early 2004. Antivirus vendors begin to build/buy spyware solutions in mid-2004.
2005	Spyware is now a major problem in the corporate environment. All antivirus vendors now offer antispyware features in both consumer suites and enterprise desktop security solutions. Corporate customers who bought standalone solutions in 2004 are now expecting the problem to be solved by their antivirus vendors. The shift from antispyware sold as a standalone product to a feature of a more comprehensive solutions happens in mid-

TABLE 2

IDC's Spyware Time Line

Year	Description
	2005.
2006	All desktop antivirus solutions now contain antispymware features. Antispymware is considered a feature and spyware is treated like any another type of malware (e.g., viruses, Trojans, zombies, worms). Standalone antispymware solutions see very few new corporate sales and low renewals. Consumers are still buying some standalone solutions on an as-needed basis.
2007	Standalone antispymware sales begin to decline rapidly in late 2006 and this will continue through 2007. Consumers are still buying some standalone solutions on an as-needed basis. There are virtually no enterprise sales of standalone antispymware products.
2008	Standalone antispymware sales continue to decline in 2008. Very few standalone antispymware vendors remain, and all are consumer-only solutions.

Source: *Worldwide Spyware 2004–2008 Forecast and Analysis: Security and System Management Sharing Nightmares* (IDC Doc #32229, November 2004).

There are both legal and illegal forms of spyware. Spyware is an executable program that is covertly installed (with or without any action on the part of the user) and monitors a person or organisation, broadcasting the information back to an outside party controlling the program. Spyware is often installed without the user's consent, as a drive-by download or as the result of clicking some option in a deceptive pop-up window. What concerns corporate security departments is that spyware can also be used to monitor keystrokes, scan files, install additional spyware, reconfigure web browsers, and snoop email and other applications. Some of the more sophisticated spyware can even capture screenshots or turn on webcams. Although some spyware is installed with the user's knowledge, most programs have been slyly bundled with some other free download.

The following is an overview of the different types of spyware:

- ☒ **Malicious Spyware.** Malicious spyware may come by more stealthy methods. It can come packaged with spam, adult entertainment web sites with disguised links and as a supplemental payload in worms. Generally, these spyware programs contain additional malicious code such as zombies, key loggers, and worms. The intent can range from controlling a user's PC, to launching denial of service attacks against other users, to identity theft.
- ☒ **Legitimate Spyware — An Oxymoron?** When it comes to spyware, the boundary between legal and criminal activity is very vague. Ambiguous End-User Licence Agreements (EULAs) speciously attain user consent for downloading spyware. In exchange for free programs, users unknowingly forgo their right to privacy. Legislation provides general guidelines for consumer rights, requiring spyware programs to inform the user of their practices. Most often, these disclosures are written within the convoluted language of the EULA of a free program. Most people never read the EULA and, if they do, the wording is so confusing that they do not realise they are giving the vendor permission to install not only the desired download, but also the added spyware. With the lines between legal and criminal so vague, legislation's ability to protect users is, at best, insufficient.

Although the consequences of spyware may be as minor as annoying advertising pop-ups, it has the potential to do significant damage to the machine and also to the entire network. Spyware has the ability to capture virtually all online activity. From monitoring all keystrokes, to email snooping, to scanning files on the hard drive, to changing system or registry settings — spyware is a great personal and enterprise security threat. Such activities can lead to identity theft, data corruption and even theft of company trade secrets. At the very least, spyware can slow down individual machines and congest network traffic. Such performance issues then lead to increased help desk calls, again taking up valuable company resources. Spyware is both a security and system management problem. To IT departments and users, spyware's pain is often felt by the help desk and/or the desktop management administrators.

From a system administrator's point of view, spyware poses an exhaustive challenge. Today, employees file hundreds of tickets for unexplained machine slowdowns. Networks fall victim to the communication overhead generated by these malicious programs. This can spell disaster for an already-overloaded help desk. Without effective early detection and blocking software, the total cost of spyware will continue to rise.

From a corporate perspective, both security and system management teams feel the burden. Today, malicious spyware easily infiltrates corporate firewalls under the guise of less-suspect network traffic. Once resident within the corporate intranet, spyware begins to realise its inventor's purpose. It may monitor activity, search files and corrupt data, all the while relaying sensitive information back to its creator. Thus, valuable trade secrets are lost. In addition to compromising security, spyware also places a burden on system management. Even non-malicious spyware causes significant productivity losses within a company.

When looking to address how to prevent spyware, it is important to look at the technology available to protect organisations from it. Spyware prevention is a difficult challenge. Current firewalls and antivirus software are ineffective against spyware. Given that it is often bundled with legitimate programs, it can easily pass through firewalls uncontested, and spyware programs do not behave in normal viral patterns that can be detected by antivirus software.

There are three strategies of spyware protection:

- ☒ **Prevention.** Blocking spyware programs from entering the system.
- ☒ **Entrapment.** Barricading downloaded programs and inhibiting them from sending messages out.
- ☒ **Disinfection.** Cleaning the system of the spyware — complete removal.

Spyware removal is a difficult task. Given that many spyware programs are bundled with free programs, the free program may cease to function without the spyware component. Moreover, spyware programs often include many additional tracing mechanisms that are left behind even after the spyware is removed. Simply uninstalling the program does not necessarily solve the problem. To cleanse the system thoroughly requires a deep understanding of the spyware program and all its idiosyncrasies, codedependencies and application relationships.

That said, IDC anticipates continued improvement and activity on the part of antispymware and secure content management vendors to address the significant technical challenge of combating spyware. This sector is becoming more important and presenting significant growth opportunities.

Events in the Press

More than 300 Australian workers have either been sacked or disciplined for Internet or email abuse over the past 12 months. Serious breaches of workplace policy on Internet and email usage are occurring with greater and greater frequency. The number of reported cases almost tripled, from five to 14, between 2002 and 2003. In 2004 there were 27 reported cases.

Since 1998 more than 200 workers have lost their jobs and 900 suspended or investigated. Recent cases reveal the serious implications for workers at the receiving end, for the alleged perpetrators, for HR professionals and for company reputations.

- ☒ **EDS Australia.** IT Staff of Commonwealth Bank IT contractor EDS Australia were asked to step away from their desks during raids of a suspected pornography piracy ring operating out of EDS's Sydney CBD offices. **Source:** *"EDS caught out in porn piracy scandal", Crickey.com.au, 15 July, 2004.*
- ☒ **Woolworths.** Dozens of managers were reportedly dismissed or disciplined — amid denials that up to 150 managers were involved — in an Internet pornography scandal. **Source:** *Matthew Denholm, "Jobs go in porn scandal", Herald Sun, 27 February 2004.*
- ☒ **Department of Defence.** Two naval officers were charged in October 2004 with possession of child pornography downloaded from the Internet onto a computer onboard their vessel. **Source:** *Les Kennedy, "Tougher child porn laws flagged as sailors charged", Sydney Morning Herald, 4 October 2004, p.2.*
- ☒ **CityRail.** Up to 80 CityRail workers were allegedly involved in the circulation of as many as 200 inappropriate images. Two senior transit officers resigned. A CityRail source said: "Those doing it thought it was so funny they sent it to female colleagues to shock or upset them". **Source:** *John Kidman, "CityRail workers quit over email porn", The Sun-Herald, 26 September 2004.*
- ☒ **Australia Post.** Up to 50 Australia Post managers and staff were caught sending pornographic emails from their work computers, some depicting children engaged in sex acts. At least four people resigned, two were dismissed and dozens suspended pending further inquiries. **Source:** *"Post office in porn probe", Launceston Examiner, 5 December 2003, p.5.*
- ☒ **Williams and Centrelink.** A 2004 case involving a male Centrelink employee who sent a pornographic email to a female colleague. Despite the fact that the female employee did not report this offence, the company caught it with email monitoring software and took action against the sender. **Source:** *Stefanie Balogh, "Let the voyeur beware", The Australia, 17 March 2004, p.13.*

IDC believes that if email monitoring had not been in place and action taken against the offender, the company would have been liable for sexual harassment via "vicarious liability". *Please note, this article outlines only the incident and does not make qualitative statements concerning filtering or what the company could*

have been sued for (hence the amendment to clarify what was reported and what are IDC's own conclusions).

Making Spyware Illegal

In May 2005, the Australian Democrats issued the Spyware Bill 2005, which has yet to be signed. The law is intended to make it unlawful to engage in deceptive acts or practices using spyware software, including causing unsolicited pop-up ads to be shown on a person's computer screen. The law makes it illegal unless the web site owner authorised the pop-up advertisement. The Bill proposed charges of up to two years in prison for installing spyware and cookies on a computer without user permission.

The government defines spyware as software that is "secretly installed on a computer and takes things from it without the permission or knowledge of the user". If introduced, the proposed law would differentiate between different types of spyware, targeting spyware that is the most malicious and economically costly to the user. The aim of the law is to address issues such as deceptive conduct, Internet banking fraud, unauthorised access and content modification.

Due to the covert nature of spyware, installation enforcement is difficult. The government is investigating all possible technical measures to thwart the proliferation of spyware and enforcement of the Spyware Bill if and when it's introduced.

FUTURE OUTLOOK

In order to protect against malicious content traversing corporate networks, either deliberately or illegitimately introduced into systems and the network, IDC recommends implementing a comprehensive threat protection strategy. While IDC is not advocating one vendor over another, an analysis of the key pure-play vendors (i.e., vendors who do not also provide antivirus software) in the messaging and web security space has shown SurfControl to be a market leader for these solutions in Australia. The following analysis is IDC's view of the benefits of SurfControl's solutions based on an in-depth study of the Australian messaging and web security market in July and August 2005, and the challenges that the company may face going forward.

Managing the Challenge — SurfControl

SurfControl is one of the global leaders in the secure content management market as evidenced by its installed base of 20,000 customers worldwide. SurfControl protects organisations with multiple layers of threat protection, which continuously filter inbound, outbound and internal Internet traffic to stop known, emerging and customer-specific threats.

SurfControl — Strengths

SurfControl offers a number of differentiators in the messaging security market from a customer's point of view, including:

- ☒ SurfControl Enterprise Protection Suite integrates Web, e-mail, and endpoint security solutions to protect against the growing number of threats that exploit multiple vulnerabilities. Its Adaptive Threat Intelligence Service provides the entire suite with continuous updates and serves as the technical architecture allowing for the sharing of threat signatures between all Protection Suite components.
- ☒ SurfControl has over 60 Global Threat Experts, located in more than 20 countries worldwide, providing continuous monitoring of all Internet threats. The Experts supply multilingual and multicultural understanding to address the global nature of attacks. SurfControl promises extensive human review of all signatures and updates to avoid any miscategorisation or “false positives” in its messaging and web security solutions.
- ☒ SurfControl has eight multilingual databases that are continuously updated and checked for accuracy. An additional layer of protection is added by integrating these databases to target blended threats that propagate over multiple entry points (e.g., web, email, IM, P2P).
- ☒ Signature-driven threat identification at the component level identifies malicious applications and files, even if disguised through renaming, relocation or compression.
- ☒ Antispam protection incorporates the powerful technologies of digital fingerprints, heuristics and SurfControl's own LexiRules.
- ☒ SurfControl Email Filter comes with a collection of keyword email dictionaries covering 10 languages — each with 16 categories of email content. SurfControl's Email Filter Learning Agent offers a solution to protect companies' confidential information.
- ☒ SurfControl offers web-based, secure logon reporting with “Report Central”. SurfControl can also help organisations with compliance through monitoring and reporting on all electronic communications based on customised corporate policies.
- ☒ Protection against spyware and other malicious applications is centrally managed and easily deployed via directory services.
- ☒ SurfControl offers pass-by or pass-through web filtering, including to mobile computer users.
- ☒ SurfControl offers policy-based administration, including automatic enforcement of end user time and bandwidth thresholds, through a graphical interface with drag and drop, real time monitoring of messages, policies and remote access.
- ☒ Proactive support is provided by Customer Care contacting customers after the sale to ensure products are working satisfactorily. Technical support is offered locally.

IDC's in-depth analysis of the email and web security software vendors in Australia concluded that SurfControl currently holds the market-leader position in the pure-play messaging and web security market (i.e., excluding antivirus vendors).

SurfControl — Challenges

All the major antivirus vendors (e.g., Symantec, McAfee, Trend Micro, Computer Associates, Sophos) have introduced antispam and antispymware software. Many are putting more emphasis into their desktop firewall offerings as well. The reason for the antivirus vendors' expansion of technology focus is to respond to customers' requirements for more complete solutions. As a result, antispam, antispymware and desktop firewall components are being sold primarily as 'add-ons' by the antivirus vendors, with the aim more to differentiate their antivirus offerings than to grow bottom line revenues with these technologies. Customers (and this is reinforced by channel partners) expect these technologies to be 'cheap' or 'add-ons' to an existing antivirus software licence. This has serious downward pricing pressure implications for the pure-play messaging and web filtering security vendors. To counter this trend, SurfControl provides an Enterprise licence that includes the software for all their technologies — called the Enterprise Protection Suite — and customers select, which piece they need as an 'add-on' whether its web, email, spyware protection, antivirus or image scanning. This is one of the few truly integrated security solutions in the market.

IDC expects downward pricing pressure to grow, particularly in the antispam market. In fact, IDC does not expect the antispam or antispymware markets to exist as standalone markets for very long, as the majority of customers simply expect these technologies to be bundled with antivirus software solutions. That said, there will continue to be large lucrative deals with major corporates, managed service providers and Internet service providers, who need robust, scalable and specialised antispam software.

The content and web filtering markets are not expected to suffer such drastic consequences, mainly because the antivirus vendors are not aggressively targeting this space. Customers can understand the need to invest in specialty software for web filtering because this software needs to be highly scalable and non-disruptive when integrated into the web infrastructure. Content filtering software often requires more sophisticated research and development, so best-of-breed vendors can often differentiate with cutting edge technology.

For SurfControl, there are significant threats to the long-term growth prospects of the market it makes significant revenues from, namely antispam. This may have implications on SurfControl's ability to grow and to fund new research and development (R&D) efforts. That said, all of SurfControl's customers interviewed in the July/August 2005 survey indicated no plans to displace SurfControl products and were happy with their investment. In fact, many respondents were displacing other products to implement SurfControl solutions.

IDC's view is that if the company develops or acquires new technology beyond messaging and web security, SurfControl will be in a much better position to overcome the threats to the antispam and antispymware markets posed by the antivirus vendors. SurfControl can also focus growth efforts on the still healthy and growing web and content filtering markets. In short, the future is not dire for SurfControl, nor any other best-of-breed vendor in the messaging security space. In fact, the email filtering market provides significant growth opportunities, especially for vendors developing new technologies to address the security risks associated with outbound email traffic.

With Enterprise Protection Suite, SurfControl is making a bold move in tackling the complex challenges inherent in content filtering. The customers IDC spoke with agree

and are eager to gain more integrated control with security technologies. To meet future customer demands, SurfControl's solution must be not only complete but also nonintrusive. In this respect, IDC believes SurfControl must develop a unified management console for the Enterprise Protection Suite. Although these concerns may look like daunting challenges for SurfControl, we believe that most of the essential capabilities are currently under development. We fully expect that SurfControl's Enterprise Protection Suite solutions will meet or exceed most customers' expectations.

CONCLUSION

The harm potential and sophistication of attacks — often referred to as blended threats, hitting corporate networks through multiple vectors including email, web traffic, IM and P2P networks — continues to escalate. Organisations must have an effective and up-to-date enterprise security strategy as a minimum requirement for email and Internet usage to function properly. IDC offers the following recommendations to end users in order to manage electronic communications more effectively:

- ☒ **Protect the pipeline.** Email pipelines continue to be a favourite target for malicious attacks, including worms, viruses, hackers, blended threats and the like. Moreover, recent incidents have achieved widespread propagation at rates significantly faster than those of many previous viruses. Today's propagation times have dropped from hours to minutes.
- ☒ **Look at spyware.** Spyware has quickly moved to the top of the priority list of corporate security concerns. Spyware has the ability to monitor keystrokes, scan files on a hard drive, monitor other applications, install other spyware programs, read cookies and change the default home page on a web browser.
- ☒ **Stop Spam.** Spam continues to clog networks, servers, and inboxes with unwanted and often offensive content. The convenience and efficiency of email have been dramatically reduced by the extremely rapid growth in the volume of unsolicited commercial email. Based on an IDC global study, the cost of spam for an organisation with 500 employees, on average, equates to AU\$540,000 a year in lost productivity. With an antispam solution, an organisation can save up to AU\$103,000 a year in improved productivity.
- ☒ **Monitor web usage.** Monitoring the usage of the Internet by employees has become a necessity for all organisations, not just as part of maintaining an effective IT security policy and managing bandwidth usage, but also to protect against the ramifications of "vicarious liability". If "adequate and sufficient" measures are not taken to monitor employees and inhibit misuse of Internet resources, the company can be liable for employees' misconduct. Web filtering and monitoring software has been considered by the court in cases involving misuse of Internet resources as "adequate and sufficient". As such Australian organisations would be advised to have some sort of web filtering software in place to protect an organisation from "vicarious liability".

It is IDC's recommendation that organisations seek out messaging and web filtering solutions that deliver:

- ☒ **Greater effectiveness over time.** As the amount of unwanted email and web traffic continues to rise, the percentage of daily worldwide messages sent that are spam will nearly equal legitimate email by 2006, according to IDC's global spam study. As such, organisations will need to take measures to protect corporate networks from the onslaught of spam emails. The key to staying ahead of the rapidly changing dynamics of ensuring that the usage of electronic communications is done in a secure and legal manner is by leveraging end-to-end integrated solutions that provide frequent technology updates.
- ☒ **Lower administration.** Focus on selecting content filtering solutions that make management easy. The use of automatic updates and shared management platforms are examples of ways software packages can help to keep the costs of maintaining email and web security at an acceptable level.
- ☒ **Greater flexibility.** Unlike viruses, there can be legitimate disagreements about what constitutes "unwanted" email and web traffic. Web and email content filtering solutions should have extensive policy creation and user self-management mechanisms in order to allow for the greatest flexibility possible for each organisation's unique requirements.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Consulting Asia/Pacific team at +61-2-9925-2236 or bjohnson@idc.com. Translation and/or localization of this document requires an additional license from IDC. For more information on IDC visit www.idc.com.au. For more information on IDC Australia GMS visit www.idc.com.au/products/gms

IDC Australia: Level 3, 157 Walker Street, North Sydney, NSW 2060, Australia
P.61.2.9922.5300 F.61.2.9957.2330

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