

I D C V E N D O R S P O T L I G H T

A Guide to Delivering Dynamic Protection in an Evolving Threat Environment

July 2007

Adapted from *Worldwide Information Protection and Control (IPC) 2007–2011 Forecast and Analysis: Securing the World's New Currency*, by Brian E. Burke and Rose Ryan, J.D. (IDC #206750, May 2007)

Sponsored by SonicWALL

Addressing information protection and control (IPC) is a complex challenge. The increasing use of corporate email, Web email, instant messaging (IM), peer to peer, and other channels for distributing data and the proliferation of mobile devices that allow employees to carry sensitive information outside the organization's boundaries make the control of information a substantial problem. This Vendor Spotlight examines the evolution of IPC solutions in their quest to discover, protect, and control information contained in data in motion, data at rest, and data in use to help organizations of all sizes and vertical industries. This Vendor Spotlight also contains a helpful checklist for selecting a security vendor and examines the role of SonicWALL in this strategically important market.

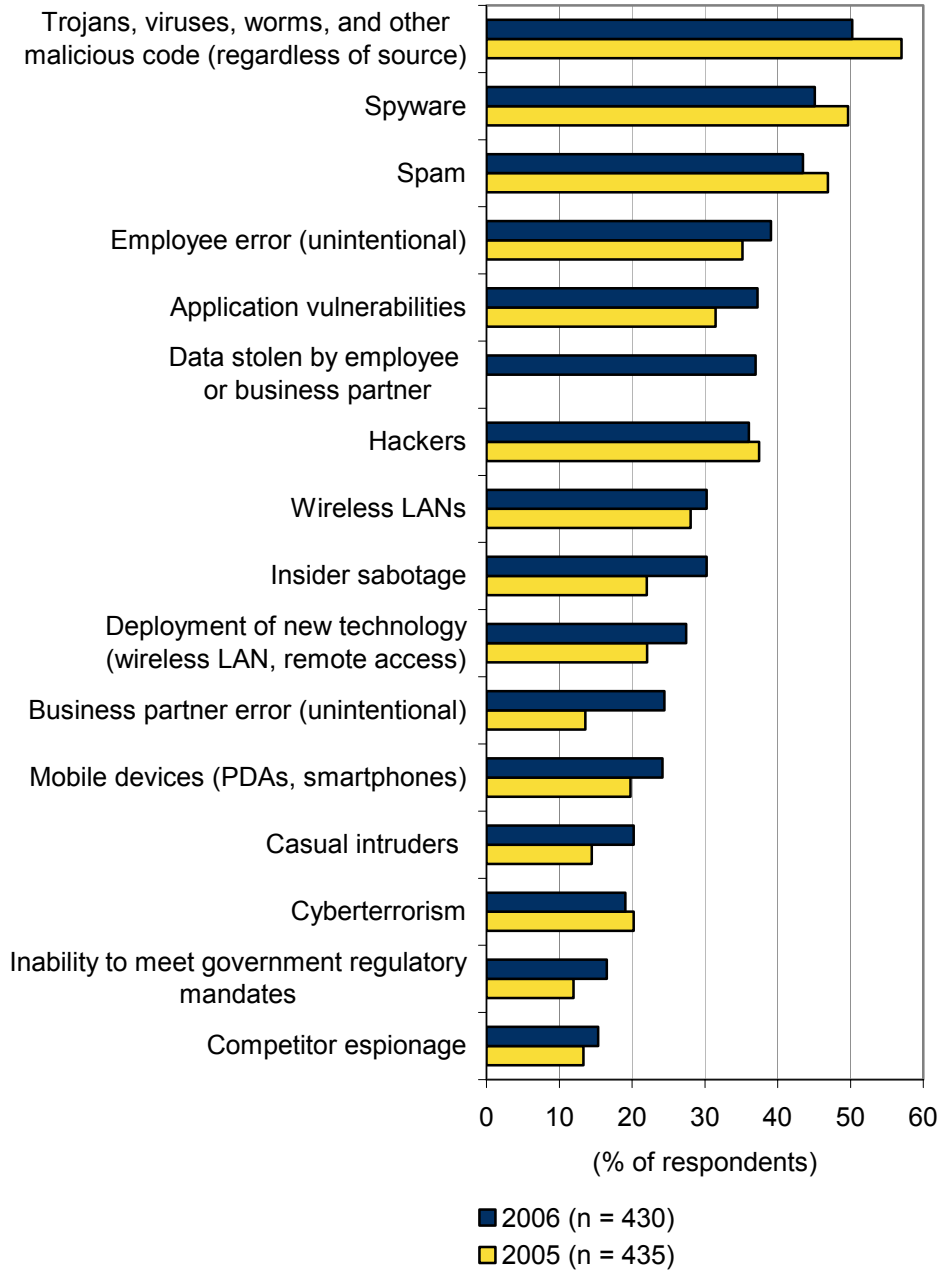
Enterprises Under Attack

Information is now a major business currency. The growing number of high-profile security breaches in which customer records, confidential information, and intellectual property were leaked, lost, or stolen has created an explosive demand for solutions that protect against the deliberate or inadvertent release of sensitive information. Moreover, numerous information-intensive government and industry regulations are requiring organizations to protect the integrity of customer and employee personal information and corporate digital assets. As a result, information protection and control are more important than ever.

Because workers can connect easily to Web sites that contain illegal or objectionable content, organizations are even more open to security breaches. Technologies such as peer-to-peer file sharing and instant messaging also make corporate networks vulnerable. Compounding the problem are internal threats, which have quickly become a major security concern in organizations of all sizes. According to IDC demand-side research, employee error, data stolen by an employee or business partner, and insider sabotage were each selected by users as among the top threats to enterprise security (see Figure 1).

Figure 1

The Top Threats to Enterprise Security



Source: IDC, 2006

Addressing the insider threat, however, is turning out to be a complex challenge. Enterprises must securely manage the aforementioned channels for distributing information — corporate email, Web email, instant messaging, and peer to peer — along with proliferating mobile devices that allow employees to carry sensitive information outside the organization.

On top of managing these threats, the increasingly complex environment of regulations and standards drives concerns about the accuracy and protection of an organization's data and information-rich messages, not only with employees but also with customers, partners, and contractors. Organizations are faced with addressing compliance issues surrounding Sarbanes-Oxley, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), FFIEC, PCI, and other federal regulations and guidelines, not only in the United States but globally.

Further impetus for executives to push their organizations to comply with these regulations includes personal liability and the threat of criminal and/or civil penalties. Civil prosecution can carry substantial financial penalties and damage a company's reputation with its customers.

Regulations governing privacy have been passed worldwide but vary from country to country. Organizations doing business internationally are struggling to cope with the effort to comply across borders. In the United States, complying with federal regulations that have recently come into effect is not as straightforward as executives would have hoped. Many of the laws are written with vague directives and haven't kept up with messaging technology.

The process of building best practices and industry standards is ongoing. The interpretation of federal regulations and the gradual building of industry standards is providing a framework from which companies can begin addressing both the concerns around sufficient security processes and the need for regulatory compliance. This has been a slow and often painful process for many organizations that find themselves learning from the financial loss and public humiliation typically accompanying noncompliance.

An Evolving Threat Environment

As companies depend more on messaging systems to conduct business, the threats continue to grow. Organizations are still battling to defend against the increasing volume and sophistication of spam, spyware, and malicious code. And the threat environment continues to evolve from a mischievous hobby to a money-making criminal venture that has attracted a new breed of sophisticated hackers.

The sophisticated hackers of today are less concerned with destroying systems and knocking out Web sites. They realize that they can generate money from stealing confidential personal information and corporate data and selling it to spammers or those involved in organized crime and fraud. IDC believes that this profit-driven motivation will cause the number of attacks to increase in sophistication, frequency, and severity. For example, email phishing attacks are now daily occurrences for many organizations, especially for the largest financial institutions and their customers. It has also become common practice for cybercriminals to share each other's technology and skills in order to increase the sophistication of malicious code. With the cybercriminal ecosystem becoming so well interconnected, IDC believes it's important to select a security vendor that has its own threat ecosystem. This provides a good counterpart to hackers' and spammers' ecosystems. The ability for a vendor to provide real-time analysis on threats to a corporate network, the Web, and email will be critical in combating the sophisticated blended-threat environment.

Meanwhile, the pure volume of spam continues to rise at a rapid pace. 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. An increasing amount of spam is being sent by a robot network

(botnet) of zombie machines. These are computers attached to the Internet that have been compromised by a security cracker, a computer virus, or a Trojan horse. Generally, a compromised machine is only one of many in a botnet and will be used to perform malicious tasks of one sort or another under remote direction.

Malicious attacks are becoming more sophisticated, for example, with the use of "blended" threats, combining spam, spyware, viruses, and other malware in one attack. Attackers, too, are becoming increasingly focused and targeted in their attacks. Moreover, financial gain, fraud, and identity theft continue to be the leading drivers behind the increasing sophistication and volume of attacks. IDC believes these are the primary reasons for the resurgence of spam as a major threat to enterprise security.

Also, the need to protect against leakage of intellectual property and violations of government and industry regulations is compelling organizations to take insider threats more seriously. Demand for outbound message security is increasing to meet compliance and privacy issues.

As organizations increasingly use the Internet for messaging and communications, it has become a more popular threat vector for hackers, spyware, and virus writers. Until recently, for instance, email-borne viruses were the most attractive weapon of hackers who sought to damage or disrupt business operations. Now, the new vector of malware attack is the Web. A growing number of malicious programs are exploiting patched and unpatched security weaknesses in Internet browsers.

An infected Web page, for example, can exploit a site visitor's computer remotely without the visitor even having to physically click on any links. Web-based malware programs can attack automatically and in real time, not only from the infected pages of site but also through email that's downloaded from a Web-based mailbox and even from worms imbedded in images.

The result is that Web security concerns are at an all-time high among organizations seeking protection from a rash of spyware, Trojan horses, worms, and other Web-traffic-borne menaces. The number of Web sites distributing spyware has increased explosively as spyware creators continue to extend their distribution channels. Indeed, spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC demand-side research.

IDC believes that as Web-based attacks continue to become more malicious and sophisticated, Web security solutions will play an increasingly valuable role as a security enhancement to traditional antivirus and firewall deployments. Given the real-time nature of HTTP, POP3, FTP, and HTTPS protocols and their data streams, more sophisticated real-time scanning capabilities are needed to ensure that traffic within these Web-based paths remains free from successful attacks through these vectors.

The demand for Web security solutions has also been fueled by concerns with employee productivity and network resources. The benefit of unclogging valuable bandwidth resources in organizations is becoming increasingly important as more Web sites offer access to streaming audio, video, FTP, and chat. Many corporate users, for example, are unaware of the network-bandwidth consumption associated with listening to online music or downloading MP3 files. This type of activity not only affects the network performance of the responsible party but also degrades network performance for all users in the organization.

Messaging security solutions must evolve to discover, protect, and secure information in three classifications

- Data in motion
- Data at rest
- Data in use

In other words, instead of focusing on inbound threats only, security must consider inbound and outbound messaging, plus the "live" messaging of Web site interactions. In addition, encryption will play an increasingly important role in messaging. Regulatory compliance, as well as the growing list of embarrassing losses of data by companies, will drive stronger protection for specific information.

In short, the changing nature of threats to corporate information and messaging will force organizations to look for new approaches to enterprise message security.

Considering SonicWALL

Founded in 1991, SonicWALL Inc. designs, develops, and manufactures network security, secure remote access, Web and email security, continuous data protection, and policy and management solutions. The Sunnyvale, California, company offers appliance-based products as well as value-added subscription services for enterprise-class Internet and data protection.

In early 2006, SonicWALL acquired email security company MailFrontier Inc. to include powerful email security as part of its end-to-end suite of secure content management (SCM) and unified threat management (UTM). This acquisition has provided MailFrontier's customers with SonicWALL's secure content management and unified threat management capabilities, while SonicWALL's distributed enterprise customers are gaining access to a further range of offerings for midmarket companies.

SonicWALL's family of network security appliances combines robust security services with high-speed deep packet inspection to provide protection for organizations of all sizes. SonicWALL offers the following products/solutions that can be combined to provide scalable enterprise security:

- SonicWALL Email Security solution offers network protection from all inbound and outbound email threats by leveraging a global end-to-end attack monitoring network. Protections include antispam, antiphishing, antivirus, and Time-Zero technology; policy management; connection management; zombie detection; compliance; and content filtering. This appliance features quick configuration, end-user spam management, seamless LDAP integration, administrative quarantine, robust reporting, and automatic updating. SonicWALL Email Security protects inbound and outbound email for organizations of fewer than 25 to more than 100,000 users.
- SonicWALL Content Security Manager Series (CSM) is an appliance-based gateway security and content filtering solution that integrates real-time gateway antivirus, antispypware, and intrusion prevention to deliver maximum network protection from today's sophisticated Internet threats. This appliance integrates seamlessly behind any firewall, making it easy to install. The CSM appliances protect networks from a wide range of Internet threats, such as viruses, worms, trojans, spyware, email-based fraud attempts, and illicit or unproductive Web content. All incoming data is scanned in real time at the gateway to block threats before they can do any damage. The CSM 2200 and 3200 receive up-to-the-minute signatures about the latest Internet security risks via a continuous, real-time connection to SonicWALL's dynamically updated database.

- SonicWALL TZ and PRO Series appliances are designed to reduce cost, risk, and complexity by integrating automated and dynamic security capabilities for comprehensive protection and maximum performance. Working in conjunction with SonicWALL network security appliances, the company's Enforced Client service guarantees that all endpoints have the latest versions of antivirus and antispymware software installed and active. Along with SonicWALL's gateway and server protection, SonicWALL endpoint security is designed to keep an enterprise network free from viruses and spyware.
- SonicWALL SSL-VPN solutions provide users with secure and clientless remote access using a standard Web browser to a broad range of resources on a corporate network, such as files and file systems, Web-based applications, Web-enabled applications, HTTP, and HTTPS intranets. In addition, these solutions enable access to applications installed on desktop computers and application servers.
- SonicWALL Backup & Recovery solutions provide automatic, real-time data backup for servers, laptops, and PCs. The solution backs up files first locally to ensure data can be recovered instantly from any previous point in time. It also includes hands-free, automatic offsite capabilities to protect businesses against disasters. The CDP series of products back up only block-level differences within each file, and then compresses them so the network is not impacted or compromised.

All these solutions provide central management and remote administration features.

Challenges and Opportunities

SonicWall has a broad range of solutions, but they do face market challenges. As companies demand integrated solutions, first- and second-generation security providers will jump on the bandwagon, creating increased competition for SonicWALL. In addition, many vendors of enterprise network software view security as a profitable add-on to their existing solutions. As a result, SonicWALL must continue to clearly differentiate itself and/or look to partner to compete against major technology suppliers.

Needless to say, SonicWALL must continue its technology leadership to maintain any advantage in the market — no small task given how rapidly malware, spam, trojans, and so forth are changing.

Conclusion and Essential Guidance

IDC believes that secure content management is rapidly converging with threat management and must be addressed at multiple points and layers in a network. This convergence is currently in various stages throughout corporate networks. Organizations are increasingly buying messaging security solutions that address multiple threats and deliver integrated antivirus, antispam, and content filtering in a single solution. Security appliances are quickly becoming the platform of choice for integrating multiple messaging security technologies.

Unified threat management appliances are another area where secure content management is quickly becoming a feature. UTM products include multiple security features integrated into one box. The need to coordinate and manage multiple client-security technologies across the enterprise is driving convergence on the endpoint (desktops, laptops, etc.). Organizations are increasingly looking for endpoint security solutions that integrate antivirus, antispymware, and personal firewall into a single solution that offers centrally managed consoles for alerts and updates, aggregated logs, and common policy engines.

Recent IDC surveys of user organizations show that the complexity of managing security technologies is the third-highest challenge organizations will face. IDC believes this is clear evidence of the need for more integrated solutions, and organizations should use the following checklist of questions when selecting a vendor to help them keep secure:

- Does the vendor provide a single type of protection, such as antivirus only, or does the vendor offer a diverse range of protection for a variety of emerging threats to enterprise security?
- Is the vendor's technology based on a real-time threat ecosystem?
- How does the company offer protection at multiple locations across the enterprise network, including protection for remote access?
- Does the company offer solutions to help monitor and document protection of sensitive information to ensure compliance?
- Does the company offer real-time feedback from multiple resources as a key to effective dynamic threat management?
- Does the company offer a mix of solutions that include hardware, software, and services to meet messaging security needs?
- How can the vendors' products/solutions scale to grow with enterprise message security needs?
- How rapidly can protections against new and emerging threats be added to the network?
- How do the company's solutions work with other installed products, such as firewalls, etc.?
- How do the company's solutions protect outbound, as well as inbound, traffic?
- How does the company integrate encryption into its solutions?

IDC believes the market for information protection and control will continue to be important and grow. To the extent that SonicWALL can address the challenges described in this Vendor Spotlight, the company has a significant opportunity for success.

A B O U T T H I S P U B L I C A T I O N

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.

C O P Y R I G H T A N D R E S T R I C T I O N S

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 GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

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