

## WHITE PAPER

# Trend Micro: Gateway Antivirus Leader Tackles Spyware with a Unique Multilayered Approach

Sponsored by: Trend Micro

Brian E. Burke

April 2005

## IDC OPINION

No longer an annoying pest swarming over home PCs, spyware recently mutated into a serious enterprise security threat. It quickly ascended the priority list of corporate security departments. Rising threats and the resulting demand for spyware protection drove many corporations to purchase first-generation point products typically designed for consumers. However, corporate customers increasingly demand antispymware from established antivirus vendors as part of an integrated solution. Along these lines, IDC believes that antispymware is most effective as part of a comprehensive layered security solution, not as a standalone antispymware point product.

This white paper discusses Trend Micro's integrated, multilayered gateway and client security solutions that secure spyware, viruses, worms, and other malicious code.

Overall, corporate customers increasingly find that spyware:

- ☒ **Threatens network security.** A 2004 IDC survey of 600 North American organizations showed that spyware is a serious threat to network security. Spyware ranked as the fourth greatest threat to network security ahead of spam and hackers. IDC estimates that spyware infects 67% of all computers (including consumer PCs). In most cases, the average PC is riddled with multiple spyware programs. Many machines swarm with hundreds of spyware programs.
- ☒ **Increases costs and reduces productivity.** Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number of help desk calls and support costs related to spyware are creating a heavy burden on corporate resources.
- ☒ **Overpowers point products.** Security and IT departments are moving away from a focus on a single type of protection, such as antispymware, toward a focus on broad protection from a wide range of emerging threats to enterprise security. Antispymware is increasingly becoming a feature of integrated gateway and client security solutions.
- ☒ **Enriches marketing firms and criminals.** Spyware is not going away; it's not a serious hacking challenge for most programmers. Moreover, spyware is a profitable revenue source for legitimate corporations (online marketing firms and advertising firms) and criminal enterprises (identity theft using keyloggers).

## METHODOLOGY

IDC developed this white paper using a combination of existing market forecasts and direct, in-depth primary research. To gain insights into the impact of spyware challenges organizations face in managing multiple security technologies, and to learn more about how Trend Micro's multilayered approach helps address these challenges, IDC conducted in-depth interviews with IT executives in various vertical industries. In addition, IDC met with the Trend Micro team to review its goals and tactics. This document reflects all of these research perspectives.

## SITUATION OVERVIEW

### Spies Among Us

According to a 2004 IDC survey, spyware was ranked as the fourth greatest threat to network security ahead of spam, hackers, and even cyberterrorism. Spyware fuels consumer and corporate users' privacy concerns.

When it comes to spyware, the boundary between legal and criminal activity is very vague. Ambiguous End User License Agreements (EULAs) speciously obtain users' consent to download spyware. In exchange for free programs, users unknowingly forgo their right to privacy. Commonly, free software hides these disclosures within the EULA's convoluted language. Most users never read the EULA and simply click the "I Accept" button. If they read the endless EULA text, the wording is so confusing that they do not realize they are giving the vendor permission to download not only the desired software but also the added spyware.

Increasingly, more malicious types of spyware are installed without users' consent, as a drive-by download or as the result of clicking some option in a deceptive pop-up window. A drive-by download is the delivery practice of automatically downloading and installing software, usually malicious, on a user's machine without the consent or knowledge of the user. Unlike a pop-up download, which asks a user for consent, a drive-by download is carried out invisibly to the user: it can be initiated by simply visiting a Web site or viewing an HTML email message. What concerns corporate security departments is that the more sophisticated types of spyware can be used to log keystrokes, scan files, install additional spyware, reconfigure Web browsers, and snoop email and other applications. In some cases, spyware can even capture screenshots, account names, passwords, and sensitive personal information as well as turn on Webcams.

According to a 2004 IDC survey, spyware was ranked as the fourth greatest threat to network security ahead of spam, hackers, and even cyberterrorism.

### Impact on Corporate Resources

Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number of help desk calls related to spyware are forcing corporations of all sizes to take action.

Spyware is both a security and system management nightmare. Today, malicious spyware easily infiltrates corporate firewalls under the guise of less suspect network traffic. Once resident within the corporate intranet, spyware begins to realize its inventor's purpose. It may monitor activity, search files, and steal data, all the while

Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number of help desk calls related to spyware are forcing corporations of all sizes to take action.

relaying sensitive information back to its creator. Thus, valuable trade secrets are lost to some clever software. In addition to compromising security, spyware also places a burden on system management. Even nonmalicious spyware causes significant productivity losses within a company. Corporate productivity suffers from the sheer distraction of these annoying ads. Many employees struggle with annoying pop-up ads on a daily basis, spending hours trying to stop the ads from recurring. Employees often install unauthorized pop-up blockers that may carry new spyware executables in attempts to prevent these annoyances.

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. Spyware opens unchecked communication gateways for the exchange of information. By broadcasting monitored behavior back to its source, often referred to as "phoning home," spyware exposes organizations to a possible back-channel security breach compromising not only the host PC but also, potentially, the entire network. This exposure could allow future automatic installation of other spyware programs, and it provides opportunities for more advanced programs to inflict even greater damage.

Today, employees file hundreds of tickets for unexplained machine slowdowns.

## BEST PRACTICES

IDC believes corporations should consider spyware's detection/removal as part of a comprehensive multilayered strategy, not just as a standalone antispyspyware client. Corporate client software is important, but a complete solution should include gateways that prevent infections before the malicious code reaches the client.

In addition to inbound protection, gateways also need outbound capabilities to:

- ☒ Stop users from going to known spyware sites
- ☒ Prevent desktops infected with spyware from phoning home

Simple blocking, however, is not enough. A granular approach is needed. Organizations should prioritize their spending to ensure that the most malicious spyware is blocked/cleaned. For example, the detection of nonmalicious cookies is obviously a lower priority than the detection of keyloggers. This calls for a taxonomy of definitions and threat levels for different spyware programs, as shown below:

- ☒ **Grayware** is an industry term used to describe a broad range of spyware and other (mostly legitimate but) potentially unwanted applications, such as adware, dialers, joke programs, remote access programs, hacking tools, browser hijackers, password crackers, and so forth.
- ☒ **Spyware** refers to programs that gather information about a person or organization and relay the information to advertisers or other interested parties. Installation, tracking, and relaying typically are done without user consent or knowledge. Spyware can be legitimate or malicious in intent, and it includes keyloggers, screen captors, event loggers, and data miners.

- ☒ **Screen captors** are programs that capture information as a still or video image and either relay it to a defined third party or store it on the system for future viewing.
- ☒ **Event loggers** are programs that log "system events" for future viewing or relay to third parties. Events often contain users' computing habits (versus browsing habits).
- ☒ **Keyloggers** can record every keystroke on a PC and steal passwords and other confidential information.
- ☒ **Cookies** are text files, created on computers when visiting Web sites, that contain information on user browsing habits and allow Web sites to more precisely target advertisements or display customized information. In the spectrum of grayware, cookies are typically among the programs of least concern, particularly those that have expiration dates, are tied to only one domain, track less sensitive information, and store information in encrypted form.
- ☒ **Data miners (tracking cookies)** track more extensive amounts of information about users and are usually accessed by multiple domains. While typically used to more accurately target advertising, these cookies build a more complete demographic and psychographic profile of the user, creating a potential privacy concern and giving the ill-intentioned spyware writer a rich source of potentially exploitable personal or corporate information.
- ☒ **Browser hijackers** can reset a user's default home page and search results. Some may prevent a user from changing the browser's home page back to its original default setting.

Effective solutions allow for administrative and policy flexibility that allows/disallows certain types of grayware by individual user or workgroup. For example, IT departments often need to download remote access tools, whereas average employees do not.

IDC believes there are many benefits of implementing integrated security solutions. For example, these solutions can help lower the total cost of ownership. A single vendor can typically offer a lower total price for an integrated solution than the sum of list prices for each component purchased from multiple vendors. Moreover, integrated security solutions provide central consoles to manage multiple security products across a network. This eliminates the need for administrators to use multiple consoles to manage and update their security products. IDC believes that existing antivirus vendors with integrated gateway and desktop offerings are well positioned to provide integrated antispysware functionality.

IDC believes there are many benefits of implementing integrated security solutions.

# TREND MICRO: MULTILAYERED PROTECTION

## Corporate Overview

Founded in 1988, Trend Micro is headquartered in Tokyo, Japan. Its 25 business units employ more than 2,500 people across Asia, Europe, North America, and South America. Trend Micro focuses on outbreak prevention. It provides customers with a comprehensive approach to managing an outbreak's life cycle, reducing the impact of network worms and virus threats, and improving productivity and information retrieval. According to IDC, Trend Micro is a worldwide leader in the gateway and server antivirus market.

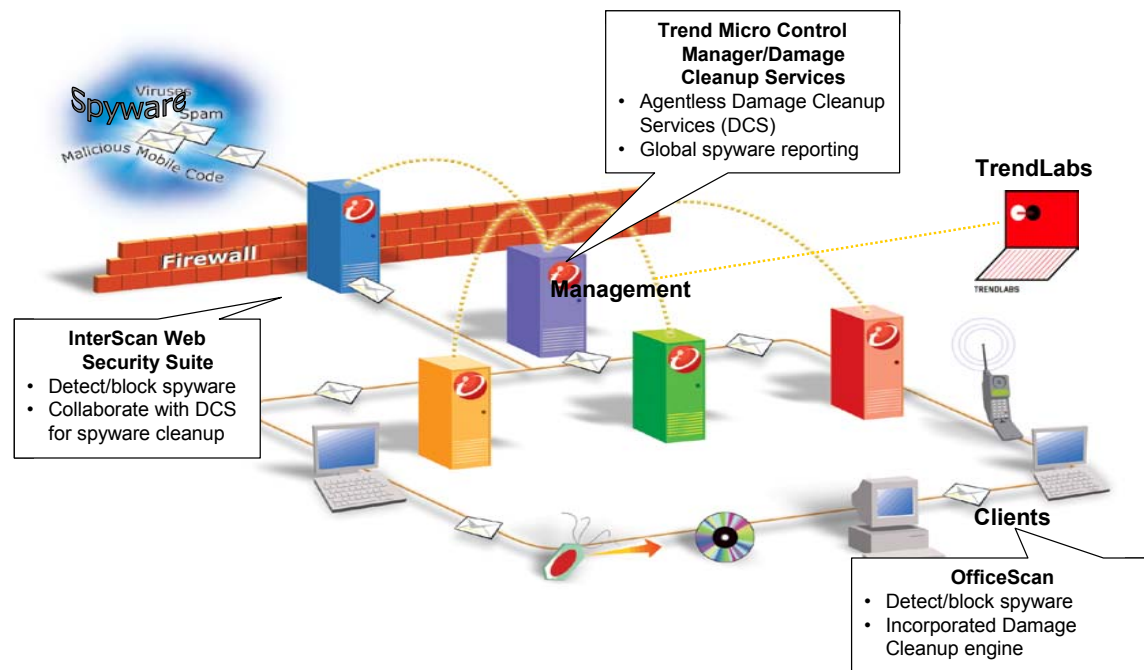
### *Multilayered Antispyware*

Trend Micro provides spyware prevention, detection, and removal. To provide optimal protection, the company designed its solution to be deployed at both the corporate gateway and on corporate desktops, as shown in Figure 1. The Trend Micro management infrastructure provides:

- ☒ Integrated policy management
- ☒ Global and local spyware event logging and reporting
- ☒ Timely pattern and threat management service core competencies

**FIGURE 1**

Trend Micro's Multilayered Antispyware Solution



Source: Trend Micro, 2005

### **Gateway Protection: InterScan Web Security Suite (IWSS)**

Trend Micro InterScan Web Security Suite delivers high-performance security for HTTP and FTP traffic at the Internet gateway. The suite integrates antivirus, antiphishing, antispymware, malicious mobile code protection (optional), and URL filtering capabilities. This comprehensive solution scans Web content and blocks malicious threats — without sacrificing Web performance. It is also highly flexible and scalable, even on large, complex networks. With a centralized management console, IT managers can deploy a rapid, coordinated defense against emerging threats. IWSS includes flexible policy management with LDAP integration that allows for selective spyware blocking based on user or group roles.

### **Desktop Protection: OfficeScan**

Trend Micro OfficeScan is a client/server security solution that integrates the core capabilities of multiple security technologies. Its Web-based management console gives administrators transparent access to desktop and mobile clients to coordinate automatic deployment of security policies and software updates. OfficeScan helps enforce security policies with Cisco network access devices that support Network Admission Control (NAC) or through Network VirusWall. It also mitigates the daily threat of file-based and network viruses and intruders, and it prevents spyware from installing/loading on client machines.

### **Damage Cleanup Services**

Trend Micro Damage Cleanup Services assess damage and remove worms, virus remnants, Trojans, spyware, and memory registries on clients — regardless of the brand of antivirus or antispymware deployed. This helps prevent reinfection and decreases the labor and costs of manual cleanup.

Damage Cleanup Services enable IT managers to do the following tasks:

- Automate cleanup of virus remnants, Trojans, spyware, and memory registries, including agentless remote cleanup
- Generate detailed reports that identify infected and cleaned machines

When used in conjunction with Trend Micro Damage Cleanup Services, OfficeScan and InterScan Web Security Suite provide automated cleanup of spyware and viruses, including removal of unwanted programs and cleaning of remnants such as dropped files and system registry changes.

### **TrendLabs**

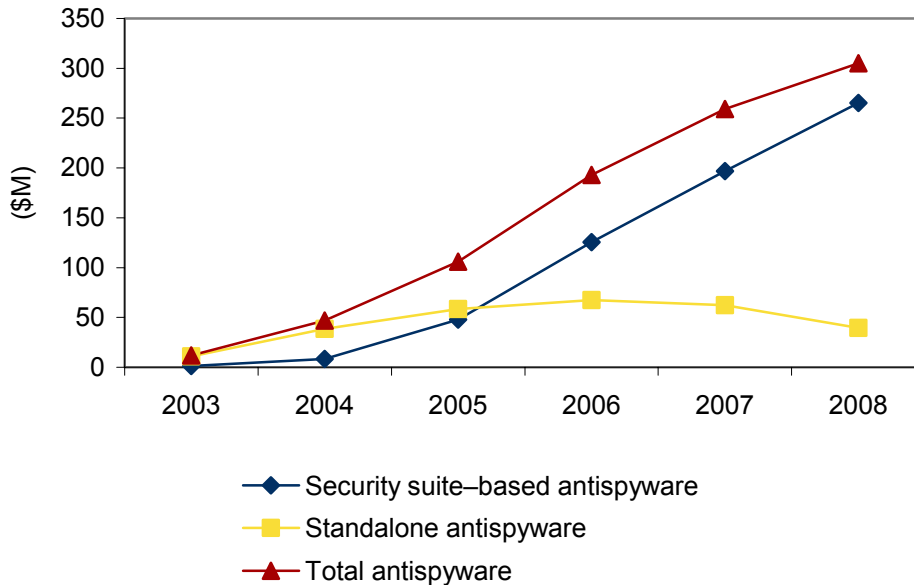
Increasingly, spyware is a very labor-intensive issue. Remediating spyware requires a comprehensive research and support infrastructure from vendors offering effective antispymware solutions. TrendLabs is a global network of threat research and product support centers that serve as the backbone of Trend Micro's service infrastructure for providing continuous round-the-clock coverage to Trend Micro customers around the world. With more than 300 engineers, researchers, and support personnel spread across its dedicated service centers in Manila; Tokyo; Paris; Munich; Taipei; and Lake Forest, California, TrendLabs can monitor potential security threats and mount a rapid response to major virus incidents, new spam tactics, and spyware and other grayware.

## MARKET OVERVIEW AND FUTURE OUTLOOK

The antispymware market grew explosively from 2003 to 2004. Worldwide revenue for antispymware solutions grew from \$12 million in 2003 to \$47 million in 2004, representing a 283% growth rate (see Figure 2). With the growing concerns over the spyware threat, IDC believes that enterprise customers will demand that antivirus vendors incorporate antispymware features into their larger suites. IDC believes that antivirus vendors will continue to focus on either developing better-performing solutions or buying antispymware technology from the standalone vendors that have gained credibility within the consumer market.

**FIGURE 2**

Worldwide Antispymware Software Revenue by Segment, 2003–2008



Source: IDC, 2005

## CHALLENGES/OPPORTUNITIES

Trend Micro's dominance in the gateway and server antivirus market could present an obstacle for desktop deployments because some organizations prefer to use more than one vendor for antivirus protection.

Trend Micro can overcome this obstacle by positioning its solution set as a comprehensive integrated solution that will not only improve security but also reduce the time and cost associated with managing multiple point solutions. For instance, using one vendor's products will result in lowered internal support and training costs because staff need to be trained on only one product.

IDC believes corporations will increasingly look for security solutions that provide a high degree of integration and address both administrative costs and security concerns to an equal degree.

Another challenge for Trend Micro is to move customers away from a best-of-breed "product" mentality to a best-of-breed "solution" mentality. The company can overcome this challenge by positioning its antispyware solution not as a point solution but as a key feature of its enterprise protection strategy, which includes protection against hackers, viruses, worms, trojans, and other types of malicious code.

## **CONCLUSION**

Enterprise security is increasingly moving away from a focus on a single type of protection, such as antispyware, toward a focus on broad protection from a wide range of emerging threats. Viruses, spyware, adware, trojans, worms, and other types of malicious code are forcing organizations to approach security with a more comprehensive solution, not with point solutions. Moreover, there is an increasing need for integration between individual security technologies in order to reduce the cost and time associated with managing point products.

Trend Micro's ability to detect, block, and clean spyware at both the gateway and desktop provides organizations with a unified framework for enterprisewide spyware protection. Overall, IDC believes the multilayered solution set from Trend Micro is well positioned to address the complex spyware threats of the future.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2005 IDC. Reproduction without written permission is completely forbidden.