

WHITE PAPER

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

Sponsored by: Trend Micro

Brian E. Burke
June 2006

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 are increasingly demanding enterprise-class spyware solutions from their established security vendors.

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

Overall, corporate customers increasingly find that spyware:

- ☒ **Threatens network security.** Spyware continues to move up the priority list of corporate security threats. Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC's 2005 *Enterprise Security Survey*. IDC believes more than three-quarters of all corporate machines are infected with various forms of spyware. In most cases, the average PC is riddled with multiple spyware programs and, in some cases, hundreds of spyware programs.
- ☒ **Increases cost 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 cost related to spyware are creating a heavy burden on corporate resources.
- ☒ **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 key loggers).

METHODOLOGY

IDC developed this white paper using a combination of existing market forecasts and direct, in-depth primary research. To gain insight 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 their goals and tactics. This report reflects all of these research perspectives.

SITUATION OVERVIEW

Spies Among Us

Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC's 2005 *Enterprise Security Survey*, up from fourth in 2004. When it comes to spyware, the boundary between legal and criminal activity is very vague. Ambiguous end user license agreements (EULA) 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 EULA's endless 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.

Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC's 2005 *Enterprise Security Survey*, up from fourth in 2004.

Increasingly, more malicious types of spyware are 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. 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 users 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, sensitive personal information, and turn on Webcams.

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, steal data, and all the while 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 non-malicious spyware causes significant productivity losses within a company. Corporate productivity suffers by 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 in fact carry new spyware executables in attempts to prevent these annoyances. From a system

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.

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 could allow future automatic installation of other spyware programs and even provide opportunities for more advanced programs to inflict 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. Client-based antispymware software is important, but a complete solution should also include perimeter protection at the corporate gateway that prevents infection before spyware can reach the end user.

In addition to inbound protection, gateway solutions 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, detection for non-malicious 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.** 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, etc.
- ☒ **Spyware.** Programs that gather information about a person or organization and relay the information to advertisers or other interested parties. Installation, tracking, and relaying are all done typically without user consent or knowledge. The programs can be legitimate or malicious in intent and include keyloggers, screen captors, event loggers, and data miners.
- ☒ **Screen captors.** 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.** 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.** 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 your default homepage and search results. Some may prevent you from changing your browsers homepage back to its original default setting.

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

Integrated Suite Versus Best-of-Breed

There is no "one size fits all" offering when it comes to corporate security. This is especially true with antispymware solutions where organizations of various sizes and vertical industries can have completely different needs. IDC believes there are benefits for implementing an integrated security suite as well as best-of-breed point solutions:

- ☒ Integrated security 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.
- ☒ Best-of-breed security solutions focus on providing higher levels of effectiveness, accuracy, and performance. Best-of-breed solutions typically focus on solving a very specific business need or pain point. In the case of spyware, there is a very clear and immediate pain point to solve. Best-of-breed can also minimize risk by allowing organizations to purchase solutions in a modular way so they pay only for what they need.

IDC believes there are many benefits for implementing an integrated security solution.

IDC believes customers who prefer best-of-breed solutions look for solutions from established security vendors that can offer investment protection and a migration path to a more comprehensive solution in the future. Moreover, we believe customers will increasingly look for best-of-breed solutions that come with a central management console to manage multiple security products. True "enterprise-class" standalone solutions will need this level of central management in order to be considered best-of-breed for the enterprise.

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 the worldwide leader in gateway and server antivirus.

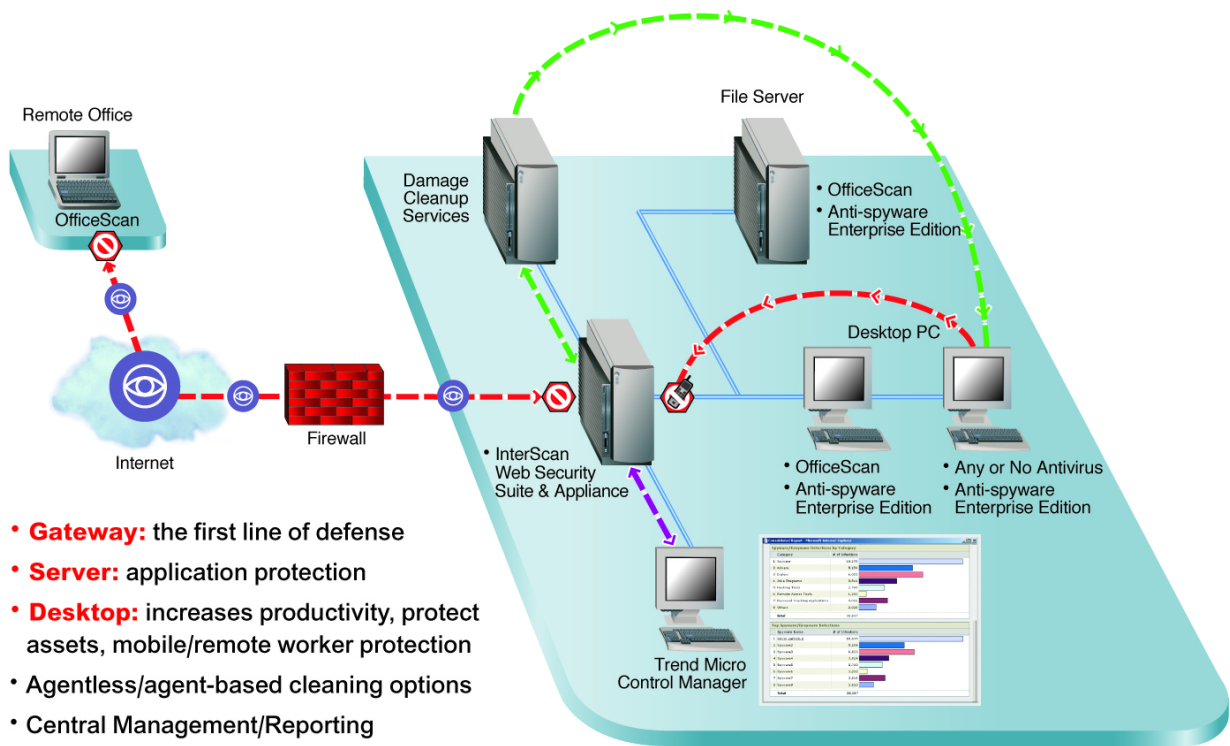
Multilayered Antispyware

Trend Micro provides spyware prevention, detection, and removal. To provide optimal protection, Trend Micro 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 Multilayered Antispyware Solution



Source: Trend Micro, 2006

Gateway Protection: InterScan Web Security Suite (IWSS) and InterScan Web Security Appliance (IWSA)

Trend Micro InterScan Web Security Suite/Appliance delivers high-performance security for HTTP and FTP traffic at the Internet gateway. The solution integrates antivirus, antiphishing, antispyware, malicious mobile code protection (optional), and URL filtering (optional) 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/IWSA includes flexible policy management with LDAP integration that allows for selective spyware blocking based on user or group roles. Furthermore, IWSS/IWSA can detect and block outgoing spyware traffic and inform Damage Cleanup Services (see below) for cleanup action.

For organizations that want a truly plug-and-play, high-performance Web gateway security hardware solution, Trend Micro IWSA offers all the capabilities and benefits of the software solution. Available in standard edition and enterprise edition, the later includes URL filtering and malicious mobile code protection as standard features. IWSA is optimally tuned to support groups of 5,000 users.

Desktop Protection: OfficeScan

Trend Micro OfficeScan is a comprehensive endpoint protection 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 prevents spyware from installing/loading on client machines. OfficeScan integrates a powerful, centrally managed cleaning functionality (DCS) to effectively remove all types of malware from infected systems. The product's reporting capabilities cover high-level overviews as well as drill-down detailed analyses.

Desktop Protection: Anti-Spyware Enterprise Edition

Trend Micro Anti-Spyware Enterprise Edition is a new standalone desktop option in the TM enterprise multilayered antispysware solution. The solution is designed for customers looking for best-of-breed capabilities in easy-to-deploy and easy-to-manage solutions. Trend Micro Anti-Spyware Enterprise Edition is positioned to offer organizations the following benefits:

- ☒ **Ease of use.** Intuitive Web interface, short learning curve.
- ☒ **Ease to deployment.** Simple to manage via Trend Micro Control Manager (TMCN) and Web console, scalable central server with MySQL, transparent push of agent to desktops; compatibility with leading desktop security solutions.
- ☒ **Minimal impact on IT administrators, end users, networks.** Trend Micro's Trickle Scan ensures that system performance is unaffected during a scan.
 - ☐ The solution requires no user interface on desktops thus reducing help desk calls and minimizing impact on users and IT departments.
 - ☐ The autodiscovery and autodeploy options help minimize impact on administration and lower bandwidth.
- ☒ **Best-of-breed detection and cleaning.** Anti-Spyware Enterprise Edition protects against all kinds of spyware, including grayware, keyloggers, adware, and rootkits. The Generic Monitoring technology proactively watches up to 150 items in the system commonly altered by spyware and prevents changes possibly resulting from an infection. (Both the Anti-Rootkit module as well as Generic Monitoring will be available in Service Pack 2, July 2006.) The integrated CWShredder is the most effective removal tool for the hard to eradicate CoolWebSearch family of browser-hijackers.

Centralized Outbreak Management Console

Trend Micro Control Manager is a centralized outbreak management console designed to simplify enterprisewide coordination of outbreak security actions and management of Trend Micro products and services. Trend Micro Control Manager acts as a central command center for deployment of Trend Micro's threat-specific expertise across the network and selects third-party products to proactively manage outbreaks.

Designed to deliver the flexibility and scalability organizations need, Trend Micro Control Manager offers a multitier management structure with extensive customization options for expanded control. Robust graphical reporting provides vital security insights, such as sources of infections or vulnerabilities and consolidated, detailed information regarding virus events or unusual activities.

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 cost 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 Service, OfficeScan and InterScan Web Security Suite provide automated cleanup of spyware and viruses, including removal of the unwanted programs and cleaning of remnants such as dropped files and system registry changes.

TrendLabs

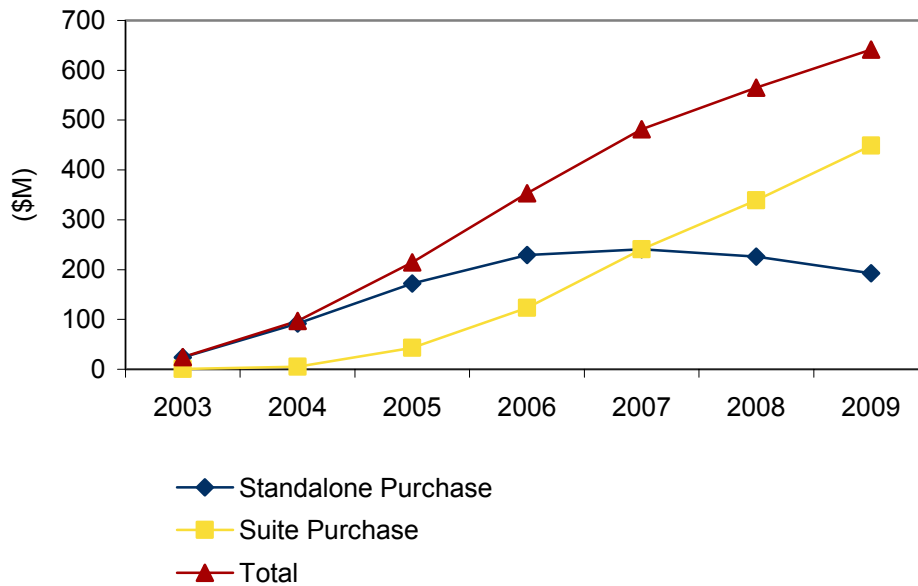
Increasingly, Spyware is becoming a very labor-intensive issue. Remediating Spyware requires a comprehensive research and support infrastructure from vendors offering effective antispymware solutions. TrendLabs is a global network of threat research and product support centers that serve as the backbone of Trend Micro's service infrastructure for providing continuous, round-the-clock coverage to Trend Micro customers around the world. With more than 800 engineers, researchers, and support personnel spread across its dedicated 15 service centers in locations such as Manila, Tokyo, Paris, Munich, Taipei, Boston, and Lake Forest, California, TrendLabs can monitor potential security threats and mount a rapid response to major virus incidents, new spam tactics, spyware, and other grayware.

MARKET OVERVIEW AND FUTURE OUTLOOK

The antispyware market grew explosively from 2003 to 2004. Worldwide revenue for antispyware solutions grew from \$24 million in 2003 to \$97 million in 2004, representing a 296% growth rate (as shown in Figure 2). With the growing concerns over the spyware threat, IDC believes that the antispyware market will continue to grow explosively over the next five years and reach \$641 million in 2009. We expect antispyware to be increasingly offered as part of an integrated solution. IDC believes Trend Micro is well positioned to offer customers a choice between integrated suites and best-of-breed point solutions to address the different needs of organizations.

FIGURE 2

Worldwide Spyware Revenue Forecast, 2003–2009



Source: IDC, 2006

CHALLENGES/OPPORTUNITIES

Trend Micro's dominance in the gateway and server antivirus market could present an obstacle for desktop deployments since some organizations prefer to use more than one vendor for antivirus protection. However, the Trend Micro standalone antispyware product doesn't require a customer to single source their antivirus so this allows them a presence on some competitor customer's desktop and gives them an opportunity to then move the customers to an integrated solution later. Trend Micro should position its solution set as a flexible multilayered solution that will not only improve security, but 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, as staff only need to be trained on one product. IDC believes corporations will increasingly look for security solutions that provide a high degree of integration and can 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. Trend Micro can overcome this challenge by positioning its antispyware solution as both an enterprise-class point solution and as a key feature of its enterprise protection strategy, which includes protection against hackers, viruses, worms, Trojans, and other types of malicious code. This will give customers the flexibility to choose which solution is best for their specific environment.

CONCLUSION

Enterprise security is increasingly moving away from a focus on a single type of protection, such as antispyware, and toward a focus on broad protection from a wide range of emerging threats. There are still many organizations that purchase standalone products, but IDC believes the increasing volume and sophistication of threats are forcing organizations to approach security with a more comprehensive solution. 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. Trend Micro's desktop solutions offer customers a choice of agent and agentless cleaning capabilities that gives the customer flexibility to choose a solution that best fits their needs. 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 2006 IDC. Reproduction without written permission is completely forbidden.