

WHITE PAPER

Securing Enterprise Environments Against Spyware: Benefits of Best-of-Breed Security

Sponsored by: Webroot

Brian E. Burke
November 2005

IDC OPINION

The threat of spyware in the corporate network has risen to a complicated and time-consuming epidemic for many IT professionals trying to ensure their users and network are protected from the hassle and harm spyware may bring. In response, many security vendors are creating anti-spyware software to seek out spyware and eradicate it from the enterprise network. Webroot's Spy Sweeper Enterprise is just such a product. A best of breed stand alone software solution, Spy Sweeper Enterprise is a leader in anti-spyware solutions.

It will be important for enterprises to seek out anti-spyware solutions offering proactive protection against the daily onslaught of blended threats. A few of the anti-spyware features enterprises should look for in addition to proactive protection are:

- Effectiveness in correctly identifying and cleaning spyware from the affected system
- Multilayered protection of desktops, servers, and gateways
- Cost effectiveness in relation to amount of IT time lost

IN THIS WHITE PAPER

This IDC paper focuses on the enterprise customers' challenges with spyware and what tactics they might take in addressing those challenges. This IDC White Paper:

- Illustrates some of the problems enterprises suffer from spyware
- Offers "best practice" features for responding to the spyware threat
- Provides a case study of an effective and successful deployment of Webroot's Spy Sweeper Enterprise solution in response to an entertainment company's spyware problems

This paper addresses the need for strong proactive anti-spyware technology to protect the enterprise and close the spyware gaps in the network's security. It discusses the challenges IT organizations face with spyware and offers best practices in addressing those challenges as well as one company's successful deployment of an anti-spyware solution.

SITUATION OVERVIEW

Faced with an increasing number of complex and blended threats, the enterprise struggles to defend its networks. The onslaught of complex viruses, worms, spyware, and other malware has enterprises scrambling to stay abreast of daily network menaces. While the sophistication of virus detection and intrusion prevention has grown, a security defense gap for spyware still exists in most enterprises. Traditionally, the approach to detecting viruses and malware is to either scan for known sources or to quarantine and observe the behavior of the potentially malignant program. While current antivirus and intrusion protection software works well for the targeted viruses, Trojans, and worms, it often overlooks spyware.

Spyware, if designed well, it is often transparent, silent, and running quietly under the radar screen of the completely unaware user. Additionally, spyware problems come less from the direct action of the spyware, but rather culminate as a result of the program's activities. Sometimes it takes infection by many different spyware applications before the system is residually affected enough for the user to take notice. This insidious ability to remain undetected for a potentially long period of time is what complicates spyware identification and removal.

This presents a problem for traditional virus detection methods as spyware behavior differs sometimes significantly from virus behavior. While there are many different options for software that can identify and clean spyware, most of them are limited to only a few different strains, requiring the user to manually maintain three or four different software packages to ensure that their machine is clean. When multiplied by an organization with thousands of users and machines, this problem is significantly magnified.

The industry should provide a spyware solution addressing threats at the source and uses effective specialized spyware techniques to clean infected machines. While many antivirus solutions purport to do this, in reality their ability to identify and then clean spyware is woefully inadequate, albeit a new revision improves on their capability. Unfortunately, like its virus predecessors, the spyware evolution is one step ahead of those writing software to stop it.

METHODOLOGY

IDC authored this paper in the fall of 2005. It is based on historical and current primary research. Augmenting this research, IDC talked to customers and vendors affected by the challenges of keeping spyware out of their networks. IDC conducted in-depth interviews with executives familiar with the challenges of spyware as well as interviewed many companies from different industries focused on implementing solutions specifically for dealing with malware and the problem it creates. Through these conversations, IDC developed an expansive and in-depth knowledge of spyware and the complications it causes for the enterprise.

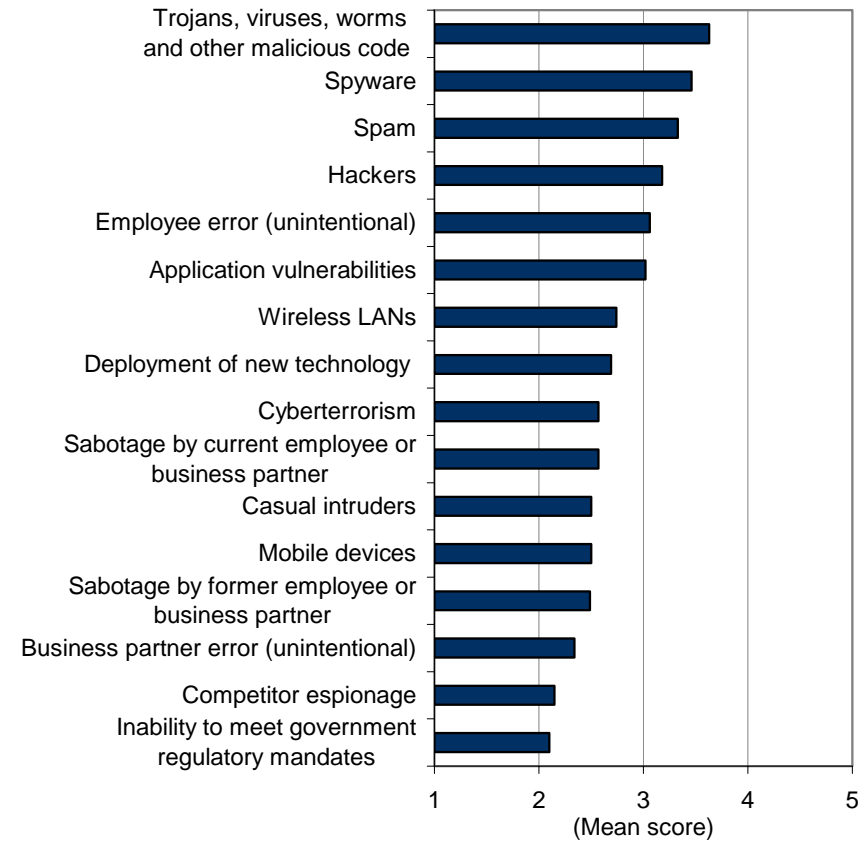
FUTURE OUTLOOK

The Evolving Threat Environment

IDC research shows spyware as the second greatest threat to enterprise security, behind only viruses, as shown in Figure 1. The volume and sophistication of attacks increase with each passing month, and enterprise IT organizations struggle incessantly to keep up with the constant barrage. While malicious software, or malware as it is deemed, is not a new problem, spyware brings additional complications. Spyware was not traditionally viewed as parasitic or all that problematic by the IT organization. While often pesky, it rarely caused enough significant problems to warrant the full attention of the IT organization. Most enterprises let their users deal with spyware on an as needed, manual basis.

FIGURE 1

Threats to Enterprise Security



n = 435

Note: Scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC's *Enterprise Security Survey*, 2005

Spyware is often suspected of causing other problems, such as machine slowness or constant crashing. Some of the more overt symptoms are hundreds of pop ups ads

dominating the screen or the hijacking of the user's Web page. While the problems and resulting complications attributed to spyware grew, there was little to no infrastructure available to the IT organization to diagnose and clean machines on an enterprisewide scale. This situation changed dramatically over the last few years.

The increase in spyware and its related problems is almost directly correlated to the change in motivations of people sending the spyware. The motives have changed from simple "ethical" delivery of ads or not so ethical mischief-making to stealing personal and private information for criminal intent. Spyware has moved from being mostly an annoyance to becoming an enterprise privacy and security threat. Invasive spyware lives unnoticed in the user's system reporting back Internet browsing habits, keystrokes, user names and passwords as well as a plethora of other sometimes personally identifiable information. These skulking bits of software collect information they have no right to collect and send it to someone who has no right to said information.

This situation leaves many enterprises in a precarious position. As regulations such as HIPAA, GLBA, and SOX increasingly demand enterprises to be accountable for information protection, a simple spyware breach may now lead to complicated and painful regulatory violations. Given regulatory violation penalties often include large fines and sometimes executive staff jail time; it behooves the enterprise to ensure their protection from such vulnerabilities.

Much like viruses, the root cause of spyware has moved from revenge and brownie point-seeking amateurs to the more insidious criminal professionals. Events such as the FTC's recent accusation of Walter Rines of Odysseus Marketing illustrate the escalation of spyware as an enterprise threat. The FTC has accused Rines of baiting users with free software containing hidden spyware. Once installed, the spyware cripples its host machine flooding the screen with pop-up ads and Web pages redirected to Rines's top clients. While Rines claims innocence and that users knew what they were downloading, the FTC clearly does not believe his excuse. It becomes all too clear that when it comes to making money, almost nothing is too low for some people. While the outcome of the FTC allegation of Rines has not been decided, the implications of the FTC's actions are obvious. The rise of criminal and fraud-driven acts perpetuated by spyware are on the rise. When there is monetary gain, there will be people taking advantage of any loophole and exploit they can find.

Business Impact

With the increasing criminal focus and intent, enterprises must face the impact that spyware has on their networks. As many IT organizations attest, that impact while significant is difficult to quantify. Because of the insidious nature of the software, it often causes symptoms seemingly unrelated to the actual cause. Help desks will witness an increase in help desk calls with problems such as computer slowness and crashing. Web pages will be hijacked and redirected. Pop up ads will flood the screen with irrelevant or illicit material. Computer memory will often be corrupted. Sometimes there is no description of problem to the help desk beyond the user complaining that the computer is "acting funny."

In some cases, spyware can have a physical impact on the PCs and their replacement cycles. A machine that must respond consistently to calls and processes which don't belong will not only suffer from major performance hits, but also will wear down over time. This will cause either a perceived, in the case of users thinking their machine is broken and they need a new one, or real, in the case of the PC's parts being worn out prematurely, shortening of the replacement cycle. Whether the need is perceived or real, the enterprise is still shouldering the real cost of a decreasing replacement cycle.

To add insult to injury, the spyware often uses significant bandwidth and network resources choking and slowing down the network. While spyware on one machine may be an annoyance, for a network of thousands of machines, each calling and reporting back to a remote unknown Internet host somewhere will quickly bog down a network and possibly swamp an unsuspecting network's resources.

All of these seemingly disconnected events waste enormous amounts of user and IT time and productivity. Users cannot work properly, and IT struggles to troubleshoot and identify phantom "ghosts in the shell" leading them everywhere and nowhere. However, simply installing blanket corporate security processes and software may kill spyware, but also take out needed applications and functions falsely identified as spyware. As complicated and confounding the situation is, the IT organization must ensure bad spyware is kept out while legitimate software is allowed in.

Finally, a rising trend in the area of criminal activity related to spyware is the theft of personally identifiable and private information, company intellectual property, customer records, and anything else the criminal thinks has value. Spyware can enter a system, find certain files or record certain keystrokes, and then send that information to an unknown third party. While corporate espionage is not new, and enterprises have been dealing with it for centuries, regulations and requirements for protecting customers, patients, users, employees, and any other people who have personally identifiable information located within the information are new. The IT organization needs to be able to protect the enterprise, its network, and its users from the assaults and complications that spyware brings. To do this, the organization should deploy software specifically designed to identify and clean machines infected with spyware.

Best Practices: Suites Versus Best of Breed

Through its extensive research, IDC identified several criteria needed for "effective" spyware detection and prevention. These are:

- ☒ **Security effectiveness** (performance, accuracy, effectiveness and false positives). Anti-spyware must first and foremost be effective. It should perform under a variety of workloads and in a variety of environments. The software should be accurate, picking out the spyware from the legitimate traffic and leaving the rest alone. Additionally, anti-spyware software should isolate and clean identified spyware from the machine while ensuring that it does not mistakenly identify legitimate traffic for spyware.

- ☒ **Cost of spyware in the network may outweigh the cost of prevention.** When adding up the time of users, the time of the IT organization, the cost of hardware, and in some cases software it becomes very easy to see how quickly the cost of not having anti-spyware will outweigh the actual deployment and management of the software itself.
- ☒ **Spyware prevention must be proactive, not reactive.** Unlike antivirus technologies, which are still mostly reactive, anti-spyware should be proactive from the start. Preventing initial infection is a significant requirement to reducing the amount of time wasted on the discovery and cleaning of infected machines. Additionally, enterprises will need to prove their machines are clean and not transmitting information to unauthorized parties in order to comply with many of the new regulations.
- ☒ **Required multilayered architecture for desktop and gateway.** By having an architecture stopping spyware both at the gateway and on the desktop, the enterprise increases its ability to control its environment and ensures that it stays as clean as possible in the face of a spyware onslaught.

It is obvious that any software designed to prevent spyware should do so effectively. To that end, both PC World and ZDNet have conducted studies rating the overall effectiveness of many different spyware products, both integrated suites and best of breed. In reading these studies, it is easy to draw a parallel to the antivirus industry and to reflect upon how the growth and development of that market shows the potential path the anti-spyware market will take.

The decision of integrated suite versus best-of-breed standalone products has many facets. Effectiveness is quickly becoming a key criterion for determining the right anti-spyware solution given the evolving nature of the threat and potential security and financial impact of malicious spyware to enterprises. If the enterprise is looking for the most effective solution to their spyware problems, they may well want to go with the best-of-breed solution. The advantage best-of-breed solutions has is that they are specifically designed to eradicate the problem at hand and keep pace with the evolving nature of spyware. In some cases the integrated suite provides just the coverage that the enterprise needs. The suite provides all of the integrated security pieces the enterprise needs, but its depth or effectiveness in one area is often sacrificed for breadth across many different areas.

The Webroot Solution

A company providing a best of breed solution to spyware is Webroot. Its flagship product, Spy Sweeper Enterprise is an enterprise-class, centrally managed, scalable solution for companywide protection against all types of spyware, adware and other malware. Spy Sweeper Enterprise is a dedicated desktop and server anti-spyware solution providing a critical addition for maintaining optimal system performance and protecting intellectual property. Webroot's anti-spyware solution provides the following key features:

- ☒ **Real-time blocking with Smart Shields.** Spy Sweeper Enterprise offers Smart Shields for proactive defense against spyware behaviors that change a system,

including changes to system memory, registry entries, host files, start-up processes, browser hijackings, and many other security settings.

- ☒ **Accurate threat detection.** Utilizing a combination of thorough research and detection processes, Spy Sweeper Enterprise provides very accurate threat detection reducing the potential risk from false positives.
- ☒ **Patent-pending Comprehensive Removal Technology (CRT).** Webroot Comprehensive Removal Technology is the backbone of their advanced spyware removal engine. CRT uses adaptive recognition practices to remove processes, applications, or files that may have changed during the remediation process or may not have been previously detected.
- ☒ **Threat database — backed by the power of Phileas™.** The Webroot Threat Research Center delivers a standard of protection that is unmatched in the industry. Phileas is an automated spyware surveillance system designed to proactively detect spyware on the Internet. Phileas identifies potential spyware and provides protection from new threats before users can unwittingly infect their PCs. This technology dramatically enhances Webroot's anti-spyware definition database and detection capabilities.
- ☒ **Centralized management.** Using the Web-enabled administration console, IT admins centrally configure and automate the deployment of definitions, policies, sweep schedules and program updates to the desktops from anywhere. The admin console allows multiple administrators to be simultaneously be logged in with full audit logging of all user actions. Admins are able to configure the client to be invisible to end users, allow user control over specific settings, or run in administrative mode with full control for advanced users.
- ☒ **Seamless, scalable deployment.** Spy Sweeper Enterprise is seamlessly deployed throughout the organization via login script, an internal software management solution, or using Group Policy in Active Directory.
- ☒ **Powerful sweep settings.** IT admins may specify sweep schedules, set policies for automated quarantine and removal of spyware, configure settings for coverage of files, memory, and registry in sweeps, and determine any software that should not be removed for selected groups (i.e., authorized system monitoring tools used by IT). The lockdown feature allows admins to dictate network and workstation settings for full compliance with the corporate security policy.
- ☒ **Laptop and remote user management.** Spy Sweeper Enterprise maintains the enforcement of administrator-set policies for laptop and remote users while they are away from the network. Laptop and remote users directly check the Webroot update server for definition updates while not connected to the corporate network to ensure continuous protection from spyware threats.
- ☒ **Reporting and alerting.** Extensive reporting features provide geographical executive summaries, spy reports, and status updates. Admins may customize reports to provide detailed analysis of the spyware threat by workstation, group, type deleted and time. In addition, alert settings allow admins to configure

multiple email addresses and notification options to ensure the correct people in the organization are alert when a threat is detected.

Spy Sweeper Enterprise provides a distributed anti-spyware solution using a client/server architecture with centralized management and reporting. The optional deployment of update distribution services allows large organizations to load balance client updates, while also enabling multi-site companies to conserve bandwidth by distributing updates from servers located on the same LAN. With Spy Sweeper Enterprise, IT administrators may configure security policies and sweep settings by individual workstation, specific groups of users, or companywide.

CASE STUDY

Spy Sweeper Enterprise in the Field

Putting Webroot to the test, IDC interviewed a large global media/entertainment company that chose Spy Sweeper Enterprise over many other anti-spyware products, including the product from their incumbent antivirus vendor. With over 30 decentralized locations worldwide this company was battling spyware infections and increasingly concerned with protecting its information and employee and customer privacy. However, simple concern for information and privacy_protection was not enough to drive management decision on something as costly as deploying an enterprisewide solution for spyware. The IT organization was required to show business justification and the solution's value in the spirit of "will the new solution either save or make us money?"

The company has over 54,000 desktops globally. Their largest campus alone is almost 20,000 desktops covering a geographical area larger than Manhattan. About the same time it began looking for a spyware solution, the company was also migrating from a distributed, decentralized IT organization to a centralized one managed by a single CIO. Not a simple task, this migration will take a considerable amount of time and investment to accomplish fully. Spy Sweeper Enterprise is one of the few systems the entire company has centralized on so far. About 93% of worldwide desktops have deployed the Webroot solution. The company has about 2,000 IT people supporting its 54,000 desktops, and it has two people fully dedicated to addressing malware concerns. The company is mostly made up of Wintel machines, either of the desktop or server variety. So, while the malware folks are focused on solving the company's malware challenges regardless of platform, the reality of the situation is that most of their environment is Wintel.

To do their jobs well, the malware-focused IT team works with many other organizations within the company, such as telecom and networking. Team members rely on their partnerships with those other groups to ensure anti-malware solutions are an appropriate part of each organization's strategy. The malware team is primarily responsible for recommending and influencing the decisions made on security solutions. The centralization of IT overall will smooth out the process required for them to effectively protect their networks and implement companywide robust policy and solutions.

The Business of Spyware

Given this company's concern with security and privacy, the need to protect the company's intellectual property and their employees' and customers' personally identifiable information was obvious. However, what really rang true with management about the spyware problem was the amount of time and effort spent on troubleshooting, diagnosing, and cleaning specific spyware events from tens of thousands of PCs. As the IT team documented and tracked events related to spyware, the amount of time lost on reformatting hard drives, identifying elusive spyware, cleaning systems and responding to ambiguous help desk calls was unacceptably cost prohibitive. Additionally, the problem was complicated by the sheer physical size of some campuses. It is extremely inefficient to send IT people all over a campus that might be several miles across every time a user has unidentified and random computer misbehavior. Because of spyware's ambiguous symptoms identifying and cleaning the machines without sending a technician is difficult. Adding to the problem is the specific knowledge required for effectively eradicating spyware; it is difficult to ensure all technicians have the right knowledge to eliminate the problem effectively and completely.

Simply put, the time spent on spyware was simply not cost effective for the company. Once the senior management realized how much time, effort, and money was wasted on the presence of spyware, they approved the effort of testing and selecting a potential anti-spyware vendor. The company tested a wide variety of anti-spyware software in their search for a solution. Tests included integrated anti-virus suites, best of breed software and even freeware applications. However, it was Webroot that won out.

Certainly, there were a few integrated anti-spyware products that worked well within their suite, but at the time of testing many of those did not fulfill the company's requirements. In order to ensure they were able to get the needed functionality out of their malware software, the company created fairly extensive custom code so some small level of interoperability could be obtained. Once Webroot was chosen, the company found that the software not only performed as expected; it exceeded those expectations. The installation and deployment went very smoothly. Although there was one unexpected mishap regarding the throttling of a particular scanner, Webroot responded to address the problem immediately.

Using internal analysis and estimates, the company now believes that about 35% of their call volume was attributed to spyware prior to the installation of Webroot. Now, very few calls are spyware related, and the call volume has been dramatically reduced. Before the installation of Webroot, the company was about 90% infected with at least one instance of spyware on each computer at their main campus, which houses about 20,000 desktops. In addition, at least 64% of those infected machines were considered critically infected with at least five instances of spyware. After the introduction of Spy Sweeper Enterprise, only 48 machines, or about one-quarter of 1%, are identified as critically infected. This is a vast improvement on the previous situation. However despite these rather stellar results of effectiveness, the company didn't choose Webroot solely on that merit. What really sold them on Spy Sweeper Enterprise was the enterprise central management features.

While several vendors claim central management capabilities, the company felt that only Spy Sweeper Enterprise provided real centralized management. Considering the size and scope of this company, it makes complete economical sense to easily centrally manage software. Certainly features such as price were important, since management would never sign off something abhorrently expensive. But centralized management was important enough to the company that they would've been willing to sacrifice a certain amount of effectiveness to gain the easy management of tens of thousands of desktops from any location.

Since the deployment of Webroot the company has noticed a dramatic reduction in help desk calls, non help desk calls within IT and has fewer undefined problems overall. In the interest of full disclosure the company's IT organization was undergoing significant restructuring during this time to a more efficient structure so it is possible that some of the recognized benefits were influenced by all of the activities performed around that time.

CHALLENGES/OPPORTUNITIES

In Spy Sweeper Enterprise, Webroot has a leading best-of-breed product. Yet, still, even with a strong product, there is room for improvement. Webroot needs to pay attention to the demands of its clients and find easier ways for its products to integrate with other existing antivirus and security software. While providing a fully integrated suite of anti-spyware, antivirus, firewall, and more may be an attractive proposition, it is generally difficult to get an enterprise to completely rip and replace currently installed and customized technology that already suits some of their needs. However, even with multiple best-of-breed endpoint security solutions installed, customers will still demand centralization of all client security management from a single console with endpoint management capabilities.

By taking Spy Sweeper Enterprise to the next level, Webroot will be able to better provide even more interoperability and integration that their customers are clamoring for. This will increase their ability to please their customers and outpace their competitors.

CONCLUSION

As spyware enters and further complicates the enterprise threat environment, businesses need security software defending and protecting their networks from the onslaught of malware. Much like the rise of antivirus software, anti-spyware solutions will evolve to better adapt and respond quickly to attacks on the networks they protect. However, unlike antivirus software when it began, anti-spyware must contend with significant amounts of security software already in place. This is the significant advantage of having a best-of-breed product; the enterprise selects the solution most suited for its needs.

However, the need for solid integration and combined reporting and centralized management are increasing with the complexity of blended threats. In addition, drivers such as increasing regulatory rules require enterprises to provide a significant amount of documentation proving that all the proper compliance protections and

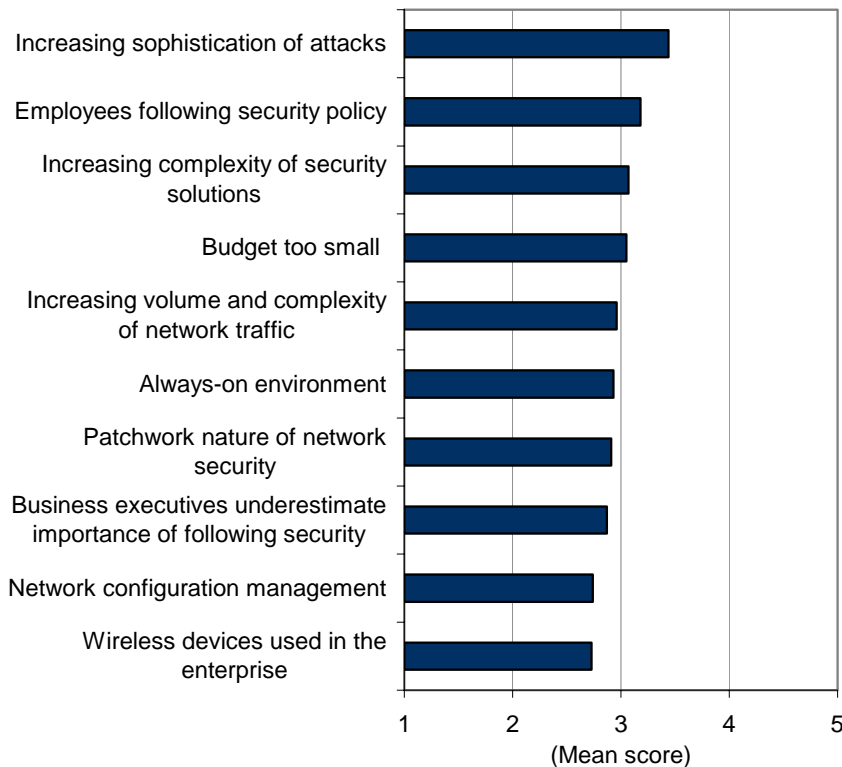
audits are in place. Drivers like these will require the tight integration of all security products, whether they are a suite or a solution. Best-of-breed products are all moving their road maps in the direction of providing this level of interoperability and integration with established products for logging, reporting and alerts.

Webroot's Spy Sweeper Enterprise is a leader in enterprise anti-spyware solutions providing many of the most crucial features needed to protect the enterprise network. Criteria such as effectiveness, justifiable cost, proactive protection and multilayered architecture are necessary pieces of anti-spyware that IDC has identified as important. As the anti-spyware market grows and evolves, Webroot is well positioned to maintain a leadership position, providing it continues to offer the features that customers clamor for.

Our survey results clearly show that the increasing sophistication of attacks is regarded as the top security challenge organizations face over the next 12 months (see Figure 2). We believe this will continue to drive the demand for best-of-breed security products and services.

FIGURE 2

Security Challenges Organizations Face over the Next 12 Months



n = 435

Note: Scores are based on a scale from 1 to 5, with 1 being no challenge and 5 being a significant challenge.

Source: IDC, 2005

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.