White Paper | September 2005

McAfee®
Proven Security™

Anti-Spyware
Choosing the Right Solution for Your Business

Table of Contents

Choosing the Right Solution for Your Business

Spyware and other potentially unwanted programs are rapidly becoming the number one threat to business systems with over 90 percent of personal computers already compromised. Spyware is any software whose function includes the transmission of company or personal information to a third party without their knowledge. The consequences of undetected spyware and other potentially unwanted programs (PUPs) can include identity theft, system and network corruption, slower Internet access, reduced system productivity, and an increased number of pop-up ads. The key to eliminating these risks is to proactively block, or quickly detect and safely eliminate potentially unwanted programs—before they can execute their damaging activities.

Anti-Spyware: Finding the Right Solution for Your Business

There is a lot of confusion in the anti-spyware market about signature databases, detection rates, and cleaning ability. Much of this confusion stems from the lack of anti-spyware standards for naming conventions, PUP characterizations/labeling, and proper methods for counting/reporting PUPs and including them in a signature database. Choosing an anti-spyware product can be a daunting task, and will remain so until the industry solidifies around globally accepted methodology and unbiased testing procedures from credible, independent third-party testing organizations.

Anti-Spyware: Business-Grade versus Consumer

A critical factor in choosing an anti-spyware product is to make sure that it was designed for your business environment and not the consumer, since both environments have unique needs and requirements.

Corporate customers require robust, centralized management of their anti-spyware solution. The central management system must allow the installation and update of the anti-spyware agent on desktops throughout the organization. It must provide IT with reports detailing which desktops are protected and at what level, as well as provide the ability to define and push anti-spyware policies to those desktops. In addition, the central management system must report detections and cleaning information in meaningful reports. IT managers want to be alerted of what PUPs have been detected and cleaned from their users' computers. They are less interested in lengthy logs that identify every last item touched during that cleaning process. The sheer volume of such logs reduces value and obscures the actionable information.

Corporate customers also face much stricter legislative requirements for information security and loss prevention. Because of this, they look for PUPs solutions that provide the strongest ability to stop PUPs *before* they are installed on a computer. In this way those PUPs have no chance to collect and transmit sensitive information across the Internet. A corollary to this is that the signatures and drivers that allow an anti-spyware product to recognize and block PUPs must be updated on a regular and consistent basis to ensure ongoing protection of corporate information. Last, corporate customers demand integration of anti-spyware into their other security tools (anti-virus, firewall, etc.) to help streamline security policies and deployment.

Consumers, on the other hand, don't need central reporting, generally feel happier when their system utilities report lots of activity—even if much of it is redundant—and are usually comfortable with receiving intermittent signature updates.

Anti-Spyware Checklist

The following table provides an overview of the business requirements that you should consider when selecting an anti-spyware product.

Business Need	Function	Anti-Spyware Best Practices
Prevention and protection capabilities	• Detection and blocking of PUPs from getting onto your systems • Scanning and cleaning—scans running processes in memory. Detects, alerts, and blocks the installation of PUPs in real time	• Use multiple techniques to detect/identify/block PUPs • Use true On-Access scanning and blocking to prevent any known spyware from installing on your systems • Prevention is better than the cure
Centralized management	• Centralized management for the anti-spyware software agent—that is sized appropriately and scales with your business	• Ability to manage more than just your anti-spyware solution • Automatic updates of the signature files—no manual action required • The ability to remotely deploy and update anti-spyware software to clients without end-user action • Understandable, relevant reports
Integration with other security products	Solid end-point security strategy means protecting against a wide variety of threats by integrating multiple products such as: • Anti-virus—protection against traditional malware • Anti-spyware—protection against PUPs • System/personal firewall—network port control (blocking) and application access control • Host Intrusion Prevention Security (HIPS)—protection from zero-day attacks like buffer overflow exploits and other threats • Management agent(s)—multiple agents to control and configure your security products	• A security solution provider with the ability to integrate multiple security functions • Fully integrated management console for all security solutions • Consistent security policies applied in layers protect all systems in your IT environment
Strong security solution provider	• Extensive knowledge of business security solutions • Innovative • Certified security experts	• Critical tasks—identifying, categorizing, and providing cures for known and zero-day threats • Proven history of successful security solutions • A dedicated support organization—24/7/365 • Global, credible, and experienced research organization
Return on investment (ROI)	• Increased productivity with less down time due to PUPs and other threats • Reduction of manual tasks	• Single source for security products means single source for troubleshooting and support, as well as leveraging existing education, best practices, and knowledge base

Conclusion

Select an anti-spyware security product as if your business depends on it. Look for a vendor that is stable and can provide you with the necessary products and services that your specific business requires for now and into the long-term future.

If you are looking to solve a security problem, take care to ensure that you not only are you choosing the best product from a technological perspective, but also that you are choosing a security partner that understands your business concerns and will be there for you in the long term.

Find Out More

For more information on spyware detection read the McAfee® white paper: *Counting Spyware Detection* or the *McAfee AntiSpyware Enterprise Evaluation Guide*. To learn more about McAfee AntiSpyware Enterprise at *www.mcafee.com*.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

6-sps-asw-crs-001-1005