

Spyware Protection & Application Control

SpyCatcher™ Enterprise provides continuous protection from evasive spyware and unwanted applications.



The Spyware Profiling Engine™ in SpyCatcher Enterprise goes beyond conventional antispyware and application control solutions by including several layers of technology, which provides maximum protection against unknown threats from spyware, key loggers, and other potentially harmful intruders.

Administrators may also prevent unwanted applications from being used by employees in an organization, which reduces IT troubleshooting, improves employee productivity, preserves bandwidth and resources that unsanctioned software may consume, and ensures compliance. Built from the ground up to address the needs of a dynamic business environment, SpyCatcher Enterprise easily scales across a global organization and provides intuitive web-based management tools.

THE IMPACT ON THE ENTERPRISE

Spyware has become ubiquitous. Nearly 85% of all computers have been infected at some point, according to a Poneman Institute survey. The FBI estimates that spyware and other computer-related crimes cost US businesses \$67 billion per year. Today's evasive spyware threats and unwanted applications present enterprises with a number of challenges:

Declining end-user productivity. When spyware renders computers useless, users can't work. Also, many organizations do not want their employees spending company time on non-related work applications such as gaming.

Declining IT administrator productivity. Spyware now accounts for 30% of all help desk calls, according to Gartner. IT administrators must spend time remediating spyware, re-imaging infected computers, and removing non-work related programs that have caused performance and other problems with users' systems.

Reduced network and desktop availability. Spyware and unwanted applications put a strain on network bandwidth and PC performance, wasting resources, time, and money.

Features

- Sophisticated Spyware Profiling Engine detects and removes evasive threats
- Manages all applications - not just spyware
- Preserves enterprise PC performance and maintains productivity for both end-users & IT
- Real-time detection identifies emerging spyware before it can infect
- Safe remediation automates and simplifies spyware removal without damaging computers
- Web-based management console provides anytime, anywhere administration
- Automated spyware sweeps are transparent to end users
- Scales across global enterprises and provides easy IT management
- Reports & alerts offer immediate visibility into possible infections

Compromised confidentiality. Spyware and other unwanted programs can put proprietary information into criminal hands, which can damage an enterprise's reputation, brand, customer loyalty, and bottom line.

The introduction of secondary vulnerabilities. Some spyware and other unwanted programs can establish a foothold for other malware to be installed, further infecting enterprise computers.

A threat to compliance. Evasive spyware threatens an enterprise's ability to protect its data at a time when corporations are struggling to implement new – and often costly – data center safeguards in order to be in compliance with Sarbanes-Oxley and other new government regulations.

LIMITATIONS OF CONVENTIONAL ANTISPYWARE SOLUTIONS

Security suite. With all of the issues that an IT department faces on a daily basis, they may find an antispyware add-on to a security suite is an attractive solution. It appears to have an initial lower cost of ownership because they already have experience with the management interface console and feel that little training will be needed. However, most vendors that offer security suites were originally developers of anti-virus software. These solutions tend to consume PC resources. Also, the reactive approach of the signature-based solutions used to eradicate viruses does not work on spyware. The potential financial impact of having spyware on your systems for any amount of time is too great. In addition, security suites offer limited or no application controls.

Client-side solution. Organizations with tight IT budgets and limited time to address the spyware problem may ask their employees to use a free client-side antispyware solution. While the up-front cost is attractive, the total cost of ownership is much higher than an enterprise solution. Administrators need to take into account the higher cost associated with installation, upgrades, management, and help desk incidents, compared to enterprise solutions. There are also other intangible costs associated with an organization not

being able to enforce its security policy because they lack the knowledge of what is running in their network.

Appliance-based solutions. A growing number of network security appliances installed at the gateway promise antispyware detection and blocking. Appliance based antispyware products rely on latent content filtering to block traffic to or from Web sites known to spread spyware. But these devices only provide protection at the network level, and not at the individual client level. Most importantly, appliance-based solutions offer no mechanism to remediate spyware or prevent reinstallation on individual PCs. These solutions can't protect mobile PCs or report which applications are running in an organization.

THE SOLUTION:

SpyCatcher Enterprise's Profiling Engine offers the most comprehensive approach to identifying new and emerging spyware threats and controlling unwanted applications. SpyCatcher includes the following features:

Advanced behavioral analysis offers proactive protection, which is better at identifying spyware than the first generation behavioral analysis solutions. It analyzes and correlates a broad range of suspicious behaviors that are typical of spyware with applications and systems in a network. It ensures the correct file is blocked which is important because spyware often hides inside innocent applications.

Flexible application control provides administrators with a list of *all* applications (not just spyware) that are running in the enterprise, within a group or on a particular computer. Policies can be created to block unwanted applications or categories of applications such as *gaming*. This reduces the opportunity for security breaches and productivity declines.

Robust vendor management policies can be established for companies that digitally sign their software. Signed applications can help administrators distinguish legitimate software from spyware. It also streamlines the application management process since all software from a particular vendor can be allowed or blocked.

The Process Software Spyware Research Center

SpyCatcher Enterprise is backed by one of the largest knowledge-base of spyware and malicious software files. The knowledgebase is compiled by the Process Software Spyware Research Center, which collects millions of spyware submissions from various sources. The information collected is distilled into an extensive online repository of Spyware Profiles, which include meta data such as file size, location, and associated registry entries. The Spyware Profiles also includes a list of vendors that have digitally signed their software. The comprehensive Spyware Profiles go far beyond traditional signatures, providing the most accurate detection of newly emerging, evasive spyware threats.

Signature detection with DeepDefense™ blocks known spyware from executing by intercepting the operating system calls that launch these applications. Most antispymware solutions leave PCs vulnerable to problems by allowing malware to run in memory before being detected and cleaned. SpyCatcher Enterprise prevents spyware from installing and damaging systems.

KEY FEATURES AND BENEFITS

Continuous protection is always in force by constantly monitoring the state, health, and configuration of computers on the network.

- *Zero-Day Protection* continuously protects from new threats and other powerful, evasive forms of spyware and unwanted applications.

- *Mobile Computer Protection* ensures that laptop computers not connected to the corporate network can still receive signature updates.

Advanced remediation and fortification offers protection even from the most hostile attacks.

- *Fortification* protects SpyCatcher from being the target of a malicious program.

- *Safe Spyware Removal* automatically eradicates even the most persistent spyware without harming enterprise computers.

Easy deployment allows administrators a pull or push installation option, or administrators can use any MSI compliant third-party deployment tools such as SMS.

- *Small Memory Footprint* gives administrators the flexibility to deploy SpyCatcher on various types of systems without impacting their performance. The low CPU scanning option uses less than 10% of a system's overall CPU.

- *Robust Active Directory Integration* allows SpyCatcher to maintain a copy of the Active Directory on the server so database lookups are efficient. Administrators can configure a time interval for incremental updates from the Active Directory server.

Flexible configuration allows administrators to decide which applications or categories of applications can run in their organization by setting and enforcing policies.

- *Configurable Application-Based Policies* can be set for categories of applications (e.g. remote administration tools) and for individual applications.

- *No Risk Quarantine* allows administrators to easily recover files from quarantine.

Enterprise-class management provides easy installation, monitoring, and upgrading of SpyCatcher on thousands of computers via a central management console (see Figure 1). Antispymware protection and application control is transparent to end users, preserving their productivity.

- *Web-Based Management Console* makes it easy to centrally manage security policies, spyware scanning, administration and reporting. Anytime/anywhere access maximizes IT productivity.

- *Automated Spyware Sweeps* are transparent to end users and can be scheduled to run at any given time or at regular intervals.

- *Enterprise Environment Integration* ensures that SpyCatcher Enterprise seamlessly co-exists with, and augments, existing IT investments, such as antivirus solutions.

- *Scalability* makes it easy to manage and control thousands of enterprise computers.

- *Reports & Alerts* provide executive-level summaries, detailed reporting, and alerts regarding applications in use. Administrators have immediate visibility into which computers may have been infected in an outbreak and what programs they are running.

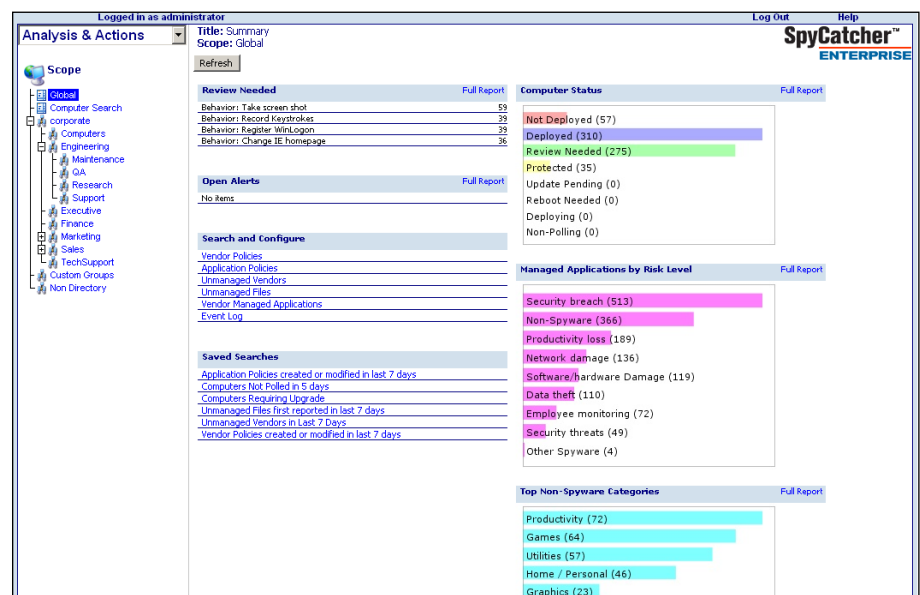


Figure 1 SpyCatcher's Global Summary allows you to evaluate the state of your enterprise at a glance.

PROACTIVELY PROTECTING THE BOTTOM LINE

Other antispyware, antivirus and appliance-based solutions aren't able to detect and remove today's evasive spyware or control application usage, which means enterprises constantly face potential financial, productivity, and other losses. With SpyCatcher Enterprise, end-user and IT productivity is preserved. PC performance and network bandwidth aren't vulnerable to resource-draining spyware or unsanctioned applications. The enterprise is protected against spyware designed to steal data or introduce secondary vulnerabilities. And when enterprises are continuously protected against evasive spyware and restricted to running sanctioned applications, they are better positioned to be in compliance with strict regulatory requirements, such as Sarbanes-Oxley. In other words, SpyCatcher Enterprise is the only antispyware solution that proactively protects an enterprise's bottom line.

PROCESS SOFTWARE'S TECHNICAL SERVICES PROGRAM

Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include consulting, training, software maintenance, online resources, and various support programs.

ABOUT PROCESS SOFTWARE

Process Software is a premier supplier of communications software solutions to mission critical environments. Since the company was founded in 1984, Process Software has grown its customer base to over 3,000 organizations, including Global 2000 and Fortune 1000 companies. Process Software has earned a strong reputation for meeting the stringent reliability and performance requirements of enterprise networks. The Tenebril division of Process Software delivers award-winning security solutions for home and enterprise customers. The products include SpyCatcher, a leading antispyware solution for enterprise and consumer markets and GhostSurf, an Internet privacy and anonymous surfing software for consumers.

SYSTEM REQUIREMENTS

SPYCATCHER ENTERPRISE SERVER:*

- Microsoft Windows Server™ 2003 (SP1, SP2), Windows XP Pro (SP2)
- 2.8 GHz processor
- 60 GB available hard disk space (Raid 0 or Raid 5)
- Internet Explorer 6 or higher

SPYCATCHER ENTERPRISE CLIENT:

- Microsoft Windows 2000 (SP4), Windows XP Pro (SP1, SP2), Windows 2003 Server (SP1, SP2), Vista
- Processor 700 MHz or better
- 256 MB RAM or better
- 100 MB disk space or better

*These are minimum system requirements. Recommended configurations vary depending on the number of clients to be managed.

FREE EVALUATION SOFTWARE!

To learn more about shielding your enterprise from evasive spyware and controlling applications with SpyCatcher™ Enterprise, please visit us at www.process.com.

For pricing information or to start your SpyCatcher Enterprise Evaluation, please call us at 800.722.7770 or 508.879.6994.

Process Software
959 Concord Street
Framingham, MA 01701

Telephone:
U.S./Canada (800)722-7770
International (508)879-6994

Fax: (508)879-0042

Web: www.process.com

Email: info@process.com