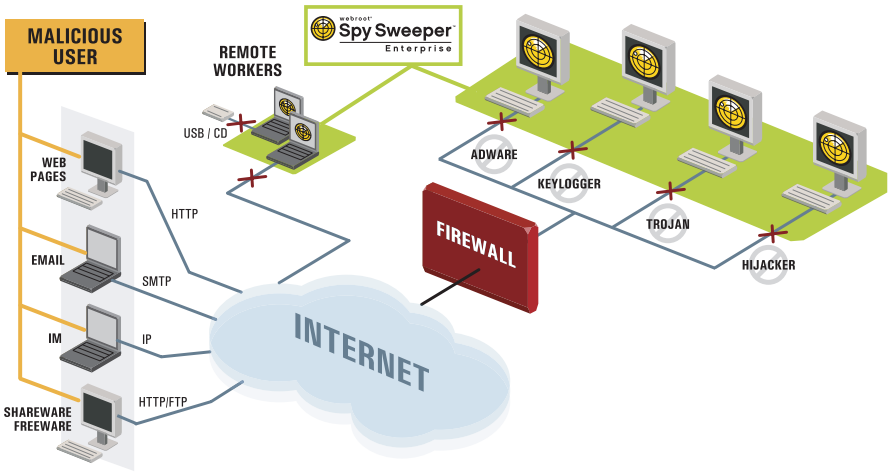
webroot®
# Spy Sweeper™ Enterprise

Data Sheet

## Defining the Spyware Threat

Enterprises today need to effectively block and remove new and rapidly evolving Internet security threats while minimizing system impact. Spyware and other malicious software is becoming more aggressive and insidious every day, with spyware developers using variations of old tricks to bypass new solutions. Given the significant financial incentives to stealing sensitive data or serving nuisance advertising, spyware has become adept at covertly infiltrating a system and installing itself deep within an infected computer.




### What is Spyware?

Spyware is any program that either monitors a user's online activities, or installs programs without a user's consent with the intention of profit or the capture of personal information. Spyware continues to become more sophisticated. It is designed to be difficult to detect and even more complicated to remove. Unfortunately for enterprises, spyware continues to appear on corporate networks at an alarming rate - and just a single undiscovered intruder can cause a variety of threats to your business:

- Compromised security of intellectual property
- Legal exposure due to exposed or stolen consumer and employee data
- Risk of violating compliance regulations
- Increased user downtime and costly drain on IT resources
- Paralyzed productivity at mission-critical workstations
- Diminished workstation performance and network stability

### Webroot Spy Sweeper Enterprise

Enhancing your security infrastructure with a centrally managed desktop anti-spyware solution is critical for maintaining optimal system performance and protecting intellectual property. Webroot Spy Sweeper Enterprise is an award-winning, scalable enterprise solution that provides the industry's most effective protection against today's most dangerous and nefarious Internet threats - including spyware, adware and other harmful intruders.

### Webroot Spy Sweeper Enterprise Provides:

- Protection from rootkits and other nefarious threats that have to ability to mask themselves from the Windows OS
- Kernel driver level protection to stop the most persistent threats
- Most effective spyware detection, removal and blocking technology
- Proactive blocking via Smart Shields defends against the most common exploits and protects known spyware entry points
- Centralized management from anywhere using a Web-enabled administration console
- Unsurpassed performance and scalability for enterprise-wide spyware protection
- Ability to download incremental definitions to reduce bandwidth consumption
- Automated or manual deployment of threat definitions and software updates
- Sweep setting enforcement and easy access to definition downloads for remote and mobile users
- Configurable sweep schedules with ability to scan select workstations on demand
- Ability to create and enforce flexible protection policies by group or workstation
- Customizable reports, summaries and alerting capabilities on detected threats
- Configurable SNMP alerts for detected spyware at conclusion of sweeps
- Dashboard view to quickly identify top threats critical workstations, and more

webroot® Spy Sweeper™ Enterprise

Data Sheet

## Webroot Spy Sweeper Enterprise: Key Features

Spy Sweeper Enterprise is the most trusted name in enterprise anti-spyware protection. This comprehensive solution provides:

### Advanced Real-time Blocking with Smart Shields

Only Spy Sweeper Enterprise offers Smart Shields to proactively defend against spyware infections. Smart Shields continuously protect the most common spyware behaviors to change a system, including changes to system memory, registry entries, host files, startup processes, browser hijackings, ActiveX installs, Browser Helper Objects and many other security settings.

### The Most Accurate Threat Detection

The detection of false positives in an enterprise environment can cause detrimental effects. Through its combination of thorough research and detection processes, Spy Sweeper Enterprise provides the most accurate threat detection — minimizing the potential risk from misidentifying a mission-critical application as spyware.

### Patent-Pending Comprehensive Removal Technology (CRT)

The Webroot Comprehensive Removal Technology (CRT) is the backbone behind the most advanced spyware removal engine in the industry. CRT ensures that all traces of spyware are completely disabled from a system PC by using adaptive recognition practices to remove processes, applications or files that may have changed during the remediation process or may not have been previously detected. Using CRT, Spy Sweeper Enterprise assures system stability during and after the spyware removal process.

### Industry Leading Threat Database — Backed by the Power of Phileas™

With the most technically advanced spyware detection process, the Webroot Threat Research Center delivers a standard of protection that is unmatched in the industry. Only Webroot offers the benefits of Phileas — the industry's first automated spyware surveillance system designed to proactively detect spyware on the Internet. This technology dramatically enhances Webroot's anti-spyware definition database and detection capabilities. Spy Sweeper Enterprise allows incremental definition downloads, reducing the overall definition file size significantly.

### Centralized Management from any Internet Connected PC

Using the Web-enabled administration console, IT administrators centrally configure and automate the deployment of definitions, policies, sweep schedules and program updates to the desktops from anywhere. The administration console allows multiple administrators to be simultaneously logged in with full audit logging of all user actions. Administrators 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 scalable to fit companies of any size. Spy Sweeper Enterprise is seamlessly deployed throughout the organization via login script, an internal software management solution, using Group Policy in Active Directory or through the WAC.

### Powerful Sweep Settings

IT administrators 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 (e.g. authorized system monitoring tools used by IT). Newly added client-side reboot notifications helps guarantee complete removal of any detected threats.

### 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 graphical executive summaries, spy reports, and status updates. Administrators can customize reports to provide detailed analysis of the spyware threat by workstation, group, type detected and time. In addition, alert settings allow administrators to configure multiple e-mail addresses and notification options to ensure the correct people in the organization are alerted when a threat is detected.

## System Requirements

### Server:

**OS:** Windows 2000 Pro / Server with SP4, Windows XP Pro with SP2, Windows 2003 Standard, Enterprise, or SMB with SP1
**CPU:** 1 GHz minimum
**Memory:** 1 GB Minimum

### Client:

**OS:** Windows 2000 Pro / Server with SP4, Windows 2003 Standard, Enterprise or SMB with SP1, or Windows XP Pro with SP2
**CPU:** 1 GHz Minimum
**Memory:** 128 Minimum, 256 MB or better recommended



**Webroot Software, Inc.** 2560 55th Street, Boulder, CO 80301 U.S.A. Tel 800.870.8102 www.webroot.com

webroot Software, Inc.