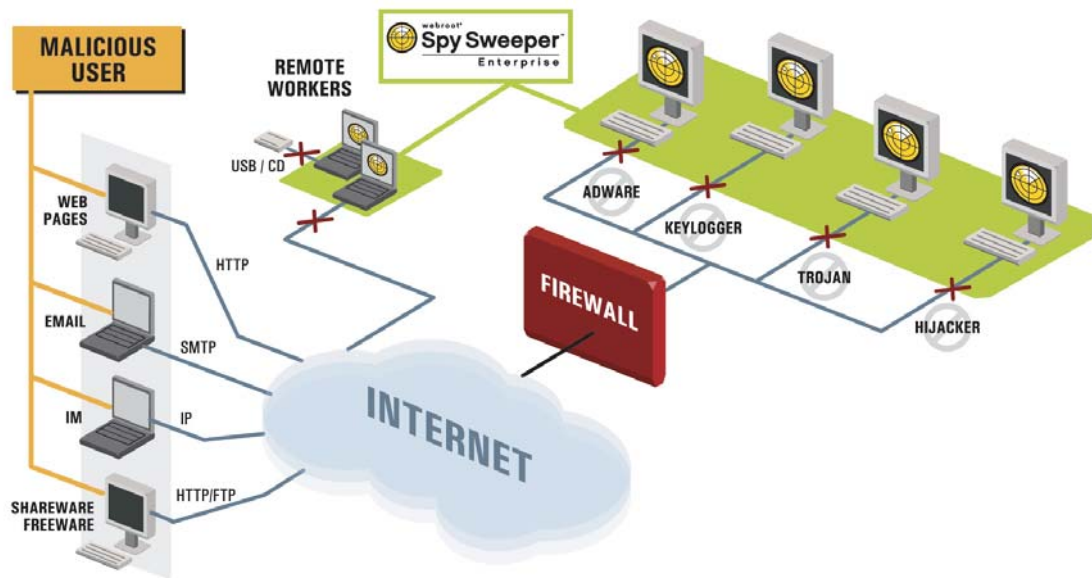




# ENTERPRISE and Medium Business

## 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 often 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 infesting a system and entrenching itself deep within an infected computer.



Spyware describes programs that monitor online activity and often secretly transmit information to a third party without end user's knowledge. The most nefarious forms of spyware continue to appear on enterprise networks at an alarming rate - and just a single undiscovered intruder can cause extensive damage to your business:

- Threatened security of intellectual property
- Legal exposure due to compromised consumer or 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

Adding a dedicated desktop anti-spyware solution to your security infrastructure is critical for maintaining optimal system performance and protecting intellectual property. Webroot Spy Sweeper Enterprise is an award-winning, centrally managed, scalable enterprise solution

that provides best of breed protection against all types of malicious spyware, adware, and other harmful intruders.

#### Webroot Spy Sweeper Enterprise provides:

- Most effective spyware detection, removal and blocking technology
- Centralized management from anywhere using the web-enabled admin console
- Unsurpassed performance and scalability for enterprise-wide spyware protection
- 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
- Dashboard view to quickly identify top threats, critical workstations, and more

# ENTERPRISE and Medium Business

## Webroot Spy Sweeper Enterprise: Key Features

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

### *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 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 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. The unique technology completely disables spyware programs detected on a system PC, rendering them ineffective. 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. Phileas rapidly 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 from any Internet-connected PC*

Using the Web-enabled admin console, IT administrators 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 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, or using Group Policy in Active Directory.

### *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). The lockdown feature allows administrators 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 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 email addresses and notification options to ensure the correct people in the organization are alerted when a threat is detected.

**“Estimates suggest that 70% of all companies go out of business after a major data loss and about 20% of all businesses experience a major disaster that affects IT every five years. Approximately 35% of disaster-recovery plans work when tested, leaving a significant opportunity for improvement. As stated earlier, only about 45% of businesses are using an intrusion detection system.”**

*Computer World, June 15, 2005*