

Completing the IT Security Solution

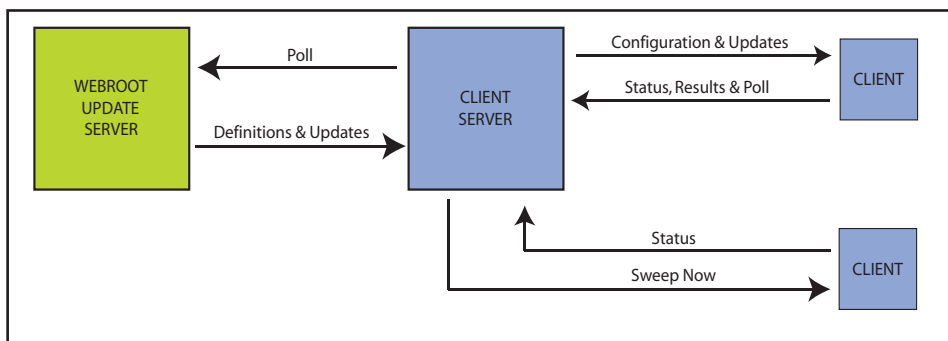
Corporations are immersed in a battle with a dangerous security threat that existing firewall and antivirus technologies do not sufficiently address - spyware. Spyware, which includes malware, trackware and adware, describes any program that monitors online activity and secretly transmits information to a third party without end user's knowledge. Due to its stealthy nature, most corporations are more familiar with the symptoms of spyware infection ranging from annoying pop-ups, sluggish network and PC performance to loss of intellectual property, rather than how to prevent spyware from installing in the first place.

Spyware programs are becoming more insidious and aggressive everyday. Corporate users can become infected through a variety of methods, often without their knowledge, including visiting websites or installing software applications without fully reading license agreements.

Adding an anti-spyware program to your security arsenal is crucial for maintaining optimal system performance and protecting corporate privacy. Spyware programs are generally more complex than viruses, with the ability to deposit hundreds of program traces throughout a PC, making manual removal nearly impossible. Firewalls are not an adequate defense because they lack the ability to discern illegitimate traffic from legitimate traffic and do not always block outbound communication. For complete network security protection, in addition to antivirus, firewall and perimeter technologies, companies need to incorporate a proactive anti-spyware solution.

Webroot Spy Sweeper Enterprise

Webroot Spy Sweeper Enterprise is an award-winning, corporate anti-spyware solution that provides centrally managed, desktop-level spyware protection. Offering the most thorough network-wide detection and elimination of spyware available, Spy Sweeper Enterprise proactively detects and removes all types of spyware including adware, Trojan horses, system monitors, keystroke loggers, dialers and other potentially unwanted software programs. The illustration below shows how Spy Sweeper Enterprise works in a network environment:



Spy Sweeper Enterprise provides distributed spyware management using a client/server architecture. The optional deployment of update distribution servers allow large organizations to balance the load of updating many clients quickly while also allowing multi-site companies to conserve bandwidth by distributing updates from servers located on the same LAN. IT administrators have complete manual control over the system or the ability to configure for full autonomous operation.

On the Record...

Two-thirds of IT managers named spyware as the number one threat to their networks' security in 2005. In addition, 65 percent said that between the three threats of viruses, phishing, and spyware, their network were least protected from spyware.

– Survey by Watchguard

An average corporate PC has 17.5 pieces spyware. Every 14.5 out of 100 scans reveals a system monitor, while 9 out of 100 detect a Trojan Horse.

– Results from Corporate Spy Audit by Webroot Software

Nearly 80% of IT managers claim their organizations have been infiltrated in the last 12 months by spyware.

– Information Week

In 2003, it was estimated that one or two out of every 100 support calls made by consumers concerned spyware. Now the estimated number of calls has ballooned to two out of every five.

– Brian Burke, IDC analyst

Webroot Spy Sweeper Enterprise

Spy Sweeper Enterprise Server runs within the network to manage the enterprise clients. The features in the enterprise server are delivered through the following major sub-components:

The *Admin Console* provides a user interface for configuring clients, managing updates, establishing alerts, viewing reports, performing real-time scans of remote systems, and all the other administrative features.

The *Enterprise Database* stores the settings from the admin console. The database collects information from spyware sweeps as well as from the update and client services. Spy Sweeper Enterprise supports the use of a SQL Server database, or the pre-packaged database shipped with the product.

The *Update Service* checks the Webroot update server for updates to software or spy definitions. This runs automatically on a scheduled basis without requiring user login to ensure the latest updates are available. The update service can also be invoked from the admin console to manually check for updates. If distributed update servers are deployed, updates are automatically moved to local distribution servers. When a client polls for an update, it obtains a list of local distributors and will retrieve the update from one of the available local servers.

The *Client Service* responds to client polling requests to receive results as well as providing configuration settings and updates back to the clients. This component runs automatically to ensure that clients get the latest settings, software and definitions regardless of when clients are on the network.

The *Update Distribution Service* delivers software and spy definition updates to clients. This service runs automatically on the Enterprise Server and additional copies can be installed throughout the enterprise to balance load and minimize WAN bandwidth consumption.

Spy Sweeper Enterprise Client runs on the user workstations and laptops to provide desktop-level spyware protection. The client contains three major components deployed in a single installation:

The *Tray Icon Application* provides access to a graphic user interface for end users to interact with the Spy Sweeper Enterprise service. The client can be deployed invisibly to end user, visible with user control over specific settings or run in administrative mode with full control for advanced users.

The *Spy Sweeper Service* provides the engine for thorough sweeps of the system and uses proactive shields to protect against spies and their attacks. This component operates automatically so that scheduled sweeps or on demand sweeps will run even when users are not logged into the system.

The *CommAgent Service* handles communication with the client service running on the enterprise server. It checks for configuration changes or updates as well as delivers the results from the sweeps.

Spyware Detection and Control

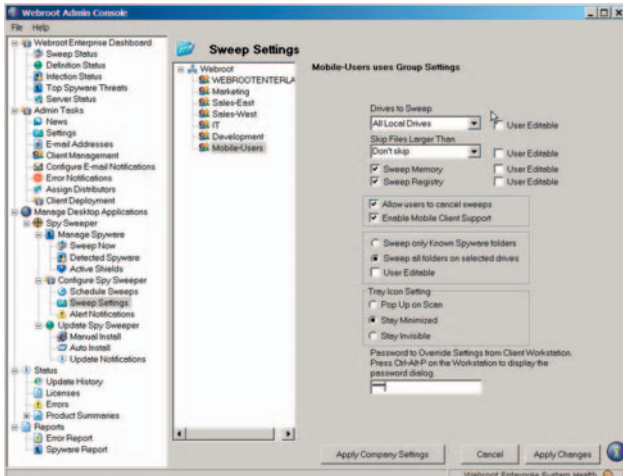
System administrators and IT staff need the ability to address spyware contamination on multiple workstations from a centralized location. The Admin Console simplifies control settings for Spy Sweeper Enterprise by enabling IT administrators to set up, manage and monitor settings from a single point.

Spy Sweeper Enterprise scans the client system using a constantly evolving database of thousands of known spyware threats. If any files or traces of spyware match the definitions database, Spy Sweeper Enterprise immediately quarantines the identified threat and notifies the administrator. Quarantining disables spyware functionality for immediate protection, while giving the administrator the option to review and permanently delete suspect files or

safely restore them if they are essential to the operation of desirable applications. Desirable files that are detected as suspect can be selected to “always keep” for specific users, groups or within the entire enterprise. Additionally, administrators can define accepted applications and block websites throughout the organization, using Spy Sweeper Enterprise to prevent employees from using unwanted software programs or to block access to specific Web sites.

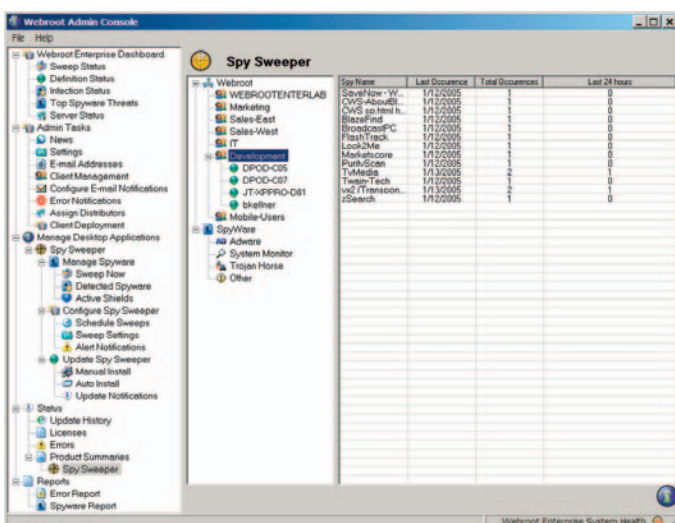
Client Management

Schedule Spyware Sweeps



- Configure specific workstation drives to sweep for spyware
- Set sweeps to include or exclude memory and the registry
- Exclude files of a specific size from sweeps
- Determine spyware disposition by spyware category or by exact spyware name
- Enable Active Shields to protect the common spyware entry points, including changes to system memory, registry entries, host files, start up processes, browser hijackings and other security settings
- “Poll Now” command allows administrator to update workstation configuration, client software or spy definitions on command
- Schedule when to run sweeps by group; or if a critical situation arises, run a sweep instantly by individual workstation or group

Monitoring, Reporting and Alerts



- Configure who receives alerts when specific types of spyware are detected
- View enterprise-wide summaries of spyware detected by group or spyware category
- Display errors that occur during sweeps to aid technical support in resolving the problem
- Generate reports of alerts and spyware found
- Create custom reports if using SQL Server database and crystal reports

Remote and Laptop Users

Spy Sweeper Enterprise maintains the enforcement of administrator-set policies for laptop or remote users while they are away from the network. Laptop and remote user machines, when logged into the network, automatically check with the Spy Sweeper Enterprise Server to download new definition or product updates and send reports of spyware detected since last logging into the network. Additionally, the remote client sends report information, such as spyware detected and previous sweep date and time, allowing IT administrators to maintain accurate reporting capabilities. While disconnected from the network, laptop and remote users may check the Webroot update server directly so that they continue to receive the most up-to-date protection from spyware threats.

Corporate-wide Security Policies

To guarantee the company's network resources are fully protected, it is important that IT administrators define a security policy that is consistent throughout the organization. IT administrators configure security options by individual workstation, specific groups of users or company-wide. The control settings include:

- Continuous monitoring to prevent spyware invasions; proactive protection includes system shields to prevent spyware from installing on desktops and browser shields protect against redirected web searches, unauthorized favorites list additions and homepage hijackers and more.
- The ability to set up workstation groups for administrative purposes, for example, laptop users or geographical regions
- Configuration locations to sweep for spyware, including the registry, memory and drives
- Sweep on demand by entire company or specific groups of users and view progress of scans as they occur
- Quarantine feature disables spyware functionality for immediate protection, while giving the administrator the option to delete or restore the suspect file
- Disposition options based on specific type of spyware such as adware, system monitors and Trojan horses. The administrator can specify whether to always keep or always remove spyware – for example, IT system monitors can be ignored
- Manual or automatic deployment of spy definition and program updates by user group and update type (such as spy definitions, minor update or major update)

About Webroot Software, Inc.

Webroot Software, a privately held company based in Boulder, Colorado, creates innovative privacy, protection, and performance products and services for millions of users around the world ranging from enterprises, Internet service providers, government agencies, higher education institutions, small businesses and individuals. The company provides a suite of high-quality, easy-to-use software that guides and empowers consumers as they surf the Web, protecting personal information and returning control over computing environments. Webroot software consistently receives top ratings and recommendations by respected third-party media and product reviewers.

System Requirements

Server:

OS: Windows NT 4.0 SP5 or higher, Windows 2000, Windows XP, Windows Server 2003

CPU: 200 mHz minimum; 350 mHz or better recommended

Memory: 512 MB recommended

Disk: 30 MB free disk space for operation. Additional free disk space necessary for database growth. 1 GB free disk space recommended.

Client:

OS: Windows 98, 98 SE, Me (all require Internet Explorer 6.0 with Service Pack 1), 2000, XP, NT 4.0, or 2003

CPU: 150 MHz or better recommended

Memory: 32 MB RAM minimum; 128 MB RAM or better recommended

Disk: 15 MB free disk space



2560 55th Street, Boulder, CO 80301

Toll Free: 800.870.8102
Telephone: 303.442.3813
Facsimile: 303.442.3846

www.webroot.com