

## Webroot Spy Sweeper Enterprise

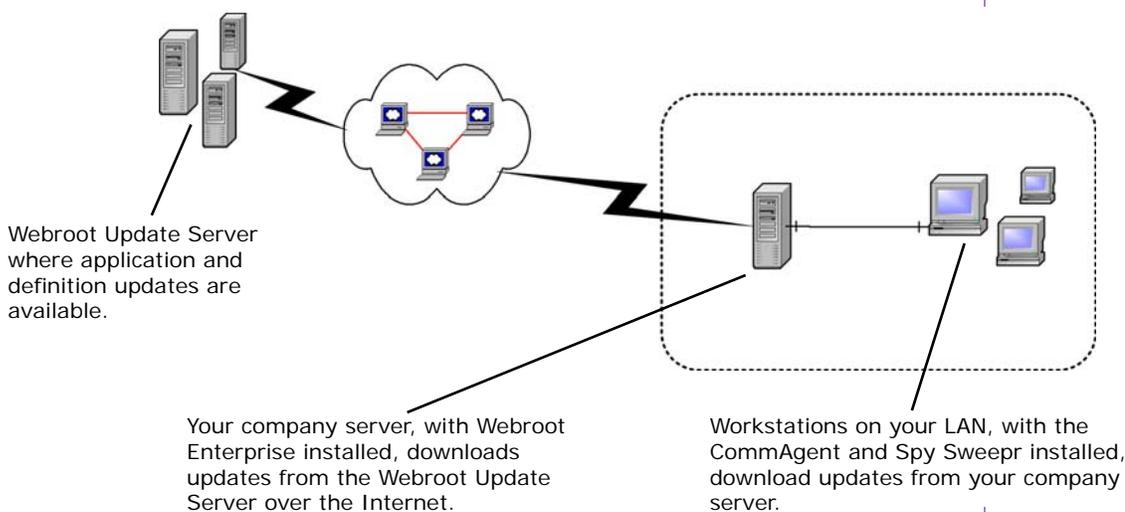
Today's corporations face a critical threat that current antivirus and firewall technologies simply don't address—spyware. Results from 900,000 computers scanned by Webroot's online Spy Audit tool revealed over 20 million pieces of embedded spyware—an average of 22 spyware programs per system. The pervasiveness of spyware in corporations illustrates that organizations are vulnerable to unknown outside parties such as competitors, hackers, or advertisers, who may access and retrieve confidential company information.

In addition, spyware programs eat up valuable bandwidth as they continually transmit information over the Internet and sap productivity from IT departments as network administrators struggle to locate and eliminate spyware programs from individual workstations.

Webroot Spy Sweeper Enterprise provides centralized, comprehensive spyware protection for companies concerned about online security and increasing IT support issues. Spy Sweeper proactively detects and removes adware, Trojan horses, system monitors, keyloggers, and more. Unlike consumer anti-spyware applications, which are not scalable for the corporate environment, Webroot Spy Sweeper is installed and managed through a centralized console without end user intervention.

## A Total Enterprise Solution

Webroot Spy Sweeper offers a total enterprise solution for distributed spyware management using a client/server architecture. This illustration shows how Spy Sweeper works:



### **Webroot Spy Sweeper provides:**

- *Centralized administration*
- *Ease of deployment for spy definition and software updates*
- *Consistent security network-wide*
- *Proactive detection and removal of spyware*

Three components work together on the network to manage updates, application configuration, and spyware detection and removal:

- The *Webroot Enterprise Server* is installed on the company server and periodically contacts the Webroot server for updates to both Webroot Spy Sweeper and spyware definitions. This automated update process ensures that the network always has the most current protection. The Webroot Enterprise Server also contains the Admin Console—the graphical user interface for the administration features—which provides centralized installation and management, enabling IT personnel to control and monitor the deployment of updates and Webroot Spy Sweeper settings across the enterprise.
- The *Communication Agent (CommAgent)* is installed on each workstation in the company and regularly contacts the company server to download and install Webroot Spy Sweeper updates, ensuring that all valuable computer resources have the most up-to-date protection available. The CommAgent also retrieves sweep scheduling and spyware detection and disposition options.
- The Spy Sweeper application is installed on each workstation in the company and scans the client system using a constantly evolving database of thousands of known spyware threats. If any files or traces of spyware match the threat definitions database, Spy Sweeper immediately quarantines them. Quarantining disables spyware functionality for immediate protection, while giving you the option to review and permanently delete suspect files or safely restore them if they are essential to the operation of desirable applications. Spy Sweeper proactively monitors and protects your system memory, home page, and new cookie additions for added peace of mind.

## Consistent Security Policy

To ensure that the company's computer resources are fully protected, it is important that IT personnel are able to define a security policy that is consistent throughout the organization. Using the Admin Console, IT security personnel can proactively set security policies and determine what settings, if any, end users can change.

The Admin Console enables security personnel to set security options for the whole company or specific groups of users and to control settings for:

- Proactive and continuous monitoring to detect tracking cookies, spyware that invades computer memory, and attempts to change the Internet Explorer home page
- Where to sweep for spyware, including the registry, memory, and drives
- Specific spyware to always keep or always remove
- Disposition of specific types of spyware such as adware, system monitors, and Trojan horses
- Enforcement of policies for mobile users when they are not on the network and facing external threats

## **Spyware steals resources by:**

- *Reducing system performance and stability*
- *Reducing worker productivity*
- *Creating software conflicts with legitimate programs*
- *Increasing support needs*
- *Stealing network resources*
- *Increasing network overhead*
- *Decreasing network performance*

## **On the record...**

*"Spyware removal tools are as important as firewall and anti-virus packages these days."*

~ Konstantinos Karagiannis  
PC Magazine

*"If you have spyware on your machine, you're almost certainly getting more advertising than someone who doesn't."*

~ ZD Net

*"Without a marvelous program from Webroot, called Spy Sweeper, this privacy invasion could have gone on indefinitely."*

~ Dan Dubno  
CBSNEWS.com

*"I recommend three programs: Spy Sweeper from Webroot Software, the established leader..."*

~ Stephen H. Wildstrom  
BusinessWeek

## Enterprisewide Deployment and Management

Increasing productivity is critical to the success of any business. Webroot Spy Sweeper offers system administrators and other IT support members complete deployment, management, and monitoring capabilities; using the Admin Console, the IT team can easily handle all administrative functions from one server.

### Configure Update Handling

Configure the handling of all update functions with just a few clicks of the mouse:

- Automatic updates to the Webroot Enterprise Server and CommAgent
- Manual deployment of updates for all workstations or for one or more user groups
- Notification when each update type becomes available
- Determination of Webroot Spy Sweeper version installed on each workstation
- Setup of automated deployment of Webroot Spy Sweeper and definition updates by user group and update type (such as definitions, minor update, or major update) as shown here:

**Spyware comes in many flavors:**

- Trojan horses
- System monitors
- Key loggers
- Dialers
- Adware
- Adware cookies

Select the Auto Install function.

Select the group you want to set up.

Drag an update type to the group.

Click **Apply Changes**.

Type	Description
New Product	New Webroot application
Major Update	Major update of an existing Webroot application
Minor Update	Minor update of an existing Webroot application
Bugfixes	No functionality was changed, only bugs were fixed
SpyDefs	New spy definition file

To specify updates to be installed automatically, you can drag an item from the grid and drop it on the desired group (or Company) node in the tree. You can also delete updates from the tree with the Del key.

## Manage Workstations and Licenses

Manage workstations and licenses remotely by:

- Setting up workstation groups for administration purposes
- Applying updates and application settings to the whole company or by group
- Checking the date of a workstation's CommAgent last contact with the company server for updates

- Configuring workstation alerts by alert type for error, warning, and informational events
- Displaying the number of licenses purchased and in use

## Spyware Detection and Control

System administrators and IT personnel must be able to address spyware contamination on multiple workstations from a centralized location. The Admin Console makes controlling settings for Webroot Spy Sweeper simple by enabling system administrators to set up, manage, and monitor settings from a single point.

### Set Up Spyware Sweeps

Control what to sweep for spyware and when to run sweeps by:

- Configuring which workstation drives to sweep for spyware
- Setting sweeps to include or exclude memory and the registry
- Excluding files of a specific size from sweeps
- Creating a password so administrators can change the settings on a workstation
- Determining spyware disposition by spyware category or by exact spyware name
- Enabling "shields" to proactively remove tracking cookies and protect memory
- Scheduling when to run sweeps by group; or if a critical situation arises, run a sweep instantly

The built-in flexibility of Webroot Spy Sweeper lets system administrators apply the same settings to all company workstations or specify different settings for different groups.

### Monitor Sweep Results

Maintain central control of sweep results, enabling IT personnel to:

- Configure who receives alerts when specific types of spyware are detected
- View summaries of detected spyware 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

Spyware management capabilities ensure that spyware detection settings are uniform, that sweeps are run regularly to find and eliminate unwanted intruders from company computers, and that IT personnel have visibility into the spyware contamination status of their network.

© 2004 Webroot Software, Inc.—All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior consent of Webroot Software, Inc. Webroot and Webroot Spy Sweeper Enterprise and their logos are registered trademarks of Webroot Software, Inc.

## System Requirements

### Server

- *Operating System: Windows NT 4.0 SP5 or higher, Windows 2000, Windows XP, Windows Server 2003*
- *CPU: 200 MHz minimum; 350 MHz or better recommended*
- *Memory: 256 MB recommended*
- *Disk: 30 MB free disk space for operation. Additional free disk space will be needed for database growth. We recommend 1 GB of free disk.*

### Client with Webroot Spy Sweeper Software

- *Operating System: Windows 98, 2000, Me, XP, or NT 4.0*
- *CPU: 150 MHz or better recommended*
- *Memory: 32 MB RAM minimum; 128 MB RAM or better recommended*
- *Disk: 15 MB free disk space*



Webroot Software, Inc.  
 2990 Center Green Court  
 Boulder, CO 80301  
 tel: (303) 442.3813  
 fax: (303) 442.3846  
 www.webroot.com