

Hit Malware Hard. Your Weapon: CounterSpy Enterprise.

Is your network protected against blended malware threats? Cybercriminals are using combinations of spambots, worms, Trojans, rootkits, and social engineering to infect your users' machines. Spyware has morphed into malware. Protecting your organization against today's increasingly complex and blended threats continues to be a never-ending headache for IT. These threats often cause machine slowdowns, crashes, and data privacy concerns. Moreover, malware can cripple an organization's critical web-based applications, causing lost productivity and ultimately lost business.

Designed to make it painless for IT managers to rid their company of malware, CounterSpy Enterprise combines next-generation system management architecture with the industry's first hybrid antimalware scanning engine that provides unparalleled malware detection, remediation, and real-time protection for today's evolving blended threat landscape.

Industry's first "hybrid" antispyware scanning engine with VIPRE™ technology

CounterSpy Enterprise is powered by a hybrid engine that merges spyware detection and remediation with Sunbelt's VIPRE technology. VIPRE incorporates both traditional antivirus and cutting-edge antimalware techniques. This marriage of technologies enables CounterSpy Enterprise to respond more effectively than other products to today's increasingly complex and blended threats.

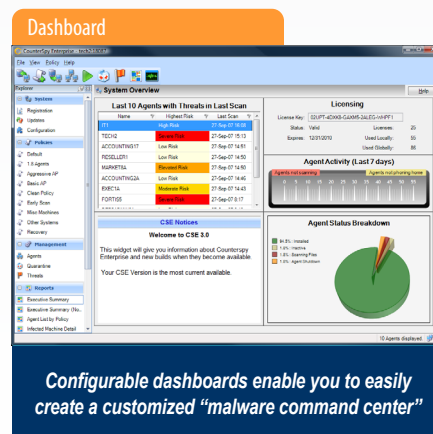
True enterprise antispyware management

Designed "by admins for admins", CounterSpy Enterprise has been built from the ground up for real-world enterprise spyware remediation. CounterSpy Enterprise provides a centrally managed means to fight malware with real-time protection that detects and removes a broad range of adware, spyware, keyloggers and other malware from your corporate network.

Centralized management

CounterSpy Enterprise's central management console allows you to access and control agent deployment, threat database updates, quarantined spyware, configuration, agent policies, scan scheduling, and recommended actions to identified malware threats. The management console provides four customizable dashboards for at-a-glance views of scanning and remediation activities that show overall network

health and performance. These configurable dashboards enable you to easily create a customized "malware command center" that gives instant access to your most used reports and policy controls. Deployment throughout your organization is seamless, featuring an intuitive policy-based user interface with multiple methods to deploy transparently.



Kernel level real-time protection

CounterSpy Enterprise's Active Protection™ works inside the Windows kernel, watching for malware and stopping it before it has a chance to execute on a workstation. The Active Protection Monitors deliver real-time protection to reduce the chance of malware infection— proactively stopping

system changes such as home page hijacks, Active X installations, and browser helper objects (BHOs).

Best threat definition database in the industry

CounterSpy Enterprise benefits from multiple sources for its threat definition updates, making it the premier antimalware solution to protect your end-users and networks from malware. Updated daily, the threat definition database includes a rapidly growing library of hundreds of thousands of threat signatures. These multiple sources for the new definitions include:

Sunbelt Threat Research Team

Sunbelt's Threat Research Team actively researches new spyware and malware outbreaks, creating and testing new threat definitions on a constant basis.

ThreatNet™

ThreatNet is Sunbelt's user community of hundreds of thousands of CounterSpy users that opt-in to anonymously send new information about possible spyware and malware to our Threat Research Center.

Sunbelt CWSandbox

Sunbelt CWSandbox leverages unique technology for the automatic behavior analysis of malware. CWSandbox collects information automatically from different inputs and provides fast and autonomous analysis of large volumes of malware samples to populate the database with new malware threats.





Powerful, comprehensive scanning agent technology

CounterSpy Enterprise utilizes a high speed threat scanning engine that can scan large volumes of information for spyware threats in a short period of time with limited performance impact on the end user's PC. The agent scanning engine automatically scans your users' systems for spyware threats and leverages the Checkmark certified antispysware technology found in CounterSpy for consumers. With its agent user interface, users can stop and start scans and manage their own quarantine.

FirstScan™

FirstScan is CounterSpy Enterprise's scan and remove on-boot technology designed specifically to detect and remove the most deeply embedded malware. Triggered through a system scan, FirstScan will run at boot time on the user's system, bypassing the Windows operating system, to directly scan certain locations of the hard drive for malware, removing infections where found as well as rootkits not seen by the Windows operating system.

Multiple methods of deployment

CounterSpy Enterprise supports multiple methods of agent deployment to allow you flexibility in how agents are pushed to your users' systems. Within the Admin Console, an agent deployment wizard helps you select a deployment option and assists you with your deployment configuration. Agents can be deployed using silent push install (using either WMI or RPC and admin shares), as an MSI file or a self-extracting executable.

Additionally, you can create policies based on organizational units (OU) and CounterSpy Enterprise will automatically deploy agents to any users or machines added to that OU. This means you no longer have to add each machine to a policy. CounterSpy Enterprise will use the policy settings you defined in the console when deploying the agents based on your OUs. Auto-deployment can also be done using IP ranges and machine lists. Truly set it and forget it.

Policy-based management

CounterSpy Enterprise has sophisticated policy creation and management functionality that gives you the flexibility to control scheduling of both quick scans and deep scans, set scan options (including scanning of known locations, whether to scan cookies, and whether to scan running processes), and allow specific threats from the database. Additionally you can set up policies for remote workers and where they download updates from as well as configure different settings for each user based on skill level (i.e. access to end user UI, abort scan, etc.)

Reporting

CounterSpy Enterprise's reporting features make it easy for administrators to schedule its library of reports. A report scheduler allows you to easily schedule any report to run at a designated time with the ability to email reports to specified users; simplifying report distribution to management.



Technical Specifications

CounterSpy Enterprise Version 3.1

Admin Console and CounterSpy Server Component:

Windows 2000 Server with SP4
Windows 2003 Server
Windows XP Professional (32 and 64 bit)
Windows Vista (32 and 64 bit)
Terminal Services and Citrix are supported
Pentium® class server with at least 250MB free disk space.

Workstation Agent:

Windows 2000 SP4
Windows XP (32 bit) All versions
Windows Vista (32 bit)
Minimum: Pentium 200 with 200 MB RAM

Supports Microsoft Access, SQL Server 6.5 or newer, SQL Express

Software Prerequisites

The following programs are prerequisites for installing and using CounterSpy Enterprise:

- The Management Console requires the Microsoft .NET Framework v2.0.
- The CounterSpy Enterprise server requires at least MDAC 2.6.
- All systems require Internet Explorer version 5 or higher.

**COUNTER
SPY™**
ENTERPRISE

Features are subject to change without notice.
All products mentioned are trademarks or registered trademarks of their respective companies.
Copyright © 2007-2008 Sunbelt Software, Inc.

csdatasheet December 2008