

Spyware Doctor Enterprise

Technical Data Sheet

The Best of Breed Anti-Spyware Solution for Businesses

Spyware Doctor Enterprise builds on the strength of the industry-leading and multi award-winning Spyware Doctor Consumer product to offer effective and powerful spyware removal and real-time protection for enterprise networks of all sizes.

Spyware Doctor Enterprise provides a complete, integrated protection solution for your business that guards your network, servers and client computers from threats of malware including: spyware, adware, Trojan viruses, keyloggers, network exploits, browser hi-jackers, Active-X based-threats, malicious web sites, spybots, dialers and tracking threats. Malware defense is an essential part of any corporate network's overall security protection.

What Spyware Doctor Enterprise offers

Centralized management - Spyware Doctor Enterprise enables centralized management, including installation and maintenance, threat management, monitoring, real-time reporting analysis and spyware detection/removal from an easy and intuitive console interface.

Lowered total cost of ownership - Spyware Doctor Enterprise lowers total cost of ownership by enabling real-time protection for client computers on your network and includes facilities for scheduled scans and updates to further automate protection and minimize administrator intervention.

High scalability - Spyware Doctor Enterprise offers high scalability, providing malware protection to an unlimited number of client computers on your Enterprise network.

Automatic Failover - Multiple Spyware Doctor Enterprise Servers can be assigned to a **Managed Domain**, which provides automatic switchover to backup Enterprise Servers should the primary Enterprise Server become unavailable due to maintenance or unexpected hardware failure.

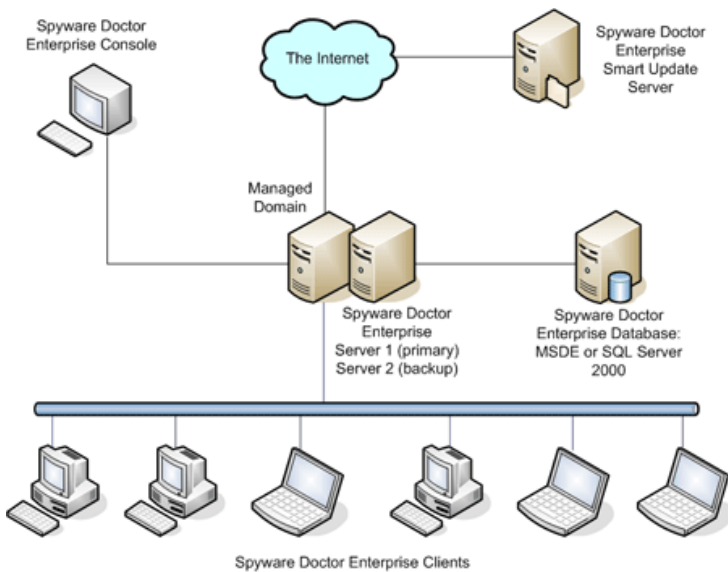
Enterprise Installation - Spyware Doctor Enterprise incorporates a flexible Wizard installer that caters to installations on common networks topologies through to more advanced network setups with built-in redundancy and facilitated database backups. In addition, the Spyware Doctor Enterprise database relies on an SQL server installation. If a business does not have an existing full version of Microsoft SQL server installation on their network, Spyware Doctor Enterprise will automatically detect this and install a scaled down version of SQL called Microsoft SQL Server Desktop Engine (MSDE).

Spyware Doctor Enterprise allows you to

- Manage the deployment, configuration, updating and reporting of malware protection within your enterprise from the convenience of an integrated management console.
- Respond quickly to malware infections through the rapid deployment of malware database updates and an enterprise-wide scan and clean.
- Provide a high-level, integrated response to malware infections for all users connected to your enterprise, including telecommuting users with remote connections.
- Obtain a consolidated view of scan and clean events, summaries and trends across all clients in your enterprise.

Spyware Doctor Enterprise Features

Smart Update Server



The smart Update Server executes independently of one or more Spyware Doctor Enterprise server installations. The Smart Update Server handles the tasks of downloading, client updates on the server and serving request for updates from other existing installations of a Spyware Doctor Enterprise server and/or client workstations.

The graphic below depicts a visual representation of how Spyware Doctor Enterprise interfaces within a typical business network environment.

Spyware Doctor Enterprise Console and Server Logs

Multiple managed Domains (and their associated workstations/servers) on a company's enterprise network can be centrally managed from within the same Spyware Doctor Enterprise Console (displayed on previous page). The console also provides comprehensive logging capabilities for logins, errors and warning events. All commands sent and their results are logged in the Spyware Doctor Enterprise Server's information logs. Each event uses transaction IDs, which allow commands to be traced from their inception to their final result.

Managing groups of computers

Spyware Doctor Enterprise provides network administrators the ability to manage multiple computers that reside in single or multiple computer groups. As an example, an Administrator can invoke a single action in the console for deployment of a predefined schedule to many computers simultaneously. Other features include deployment of the Threat Ignore list, scan fixes/reports and other various commands applicable to the client workstations.

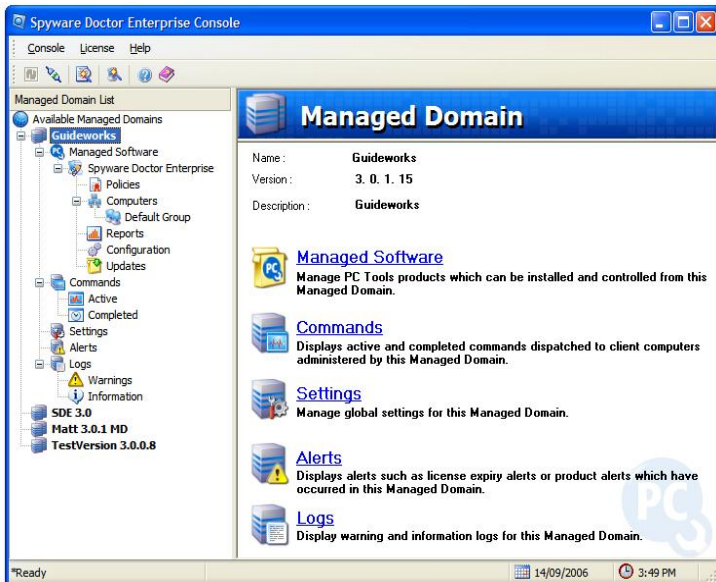
Remote client agent deployment

The Spyware Doctor Enterprise console provides the ability to conveniently install the client agent software onto all computers that are connected to your network.

Alerts

Spyware Doctor Enterprise includes visual Alert notifications of infections detected on your network as well as license expiry alerts, product alerts and infections which have occurred in the managed Domain(s). These Alerts can also be automatically emailed to the Network Administrators.

Managed Domains



Spyware Doctor Enterprise introduces the concept of a **Managed Domain**. A Managed Domain is a collection of one or more Spyware Doctor Enterprise servers grouped together to operate as a single server entity. This concept reduces server workload and also provides automatic failover in the case of a server going off-line due to maintenance or unexpected hardware failure.

There are no limits to the number of Spyware Doctor Enterprise servers that can belong to a Managed Domain. Additionally, Multiple Managed Domains can co-exist on the same network segment. By using a Managed Domain, Spyware Doctor Enterprise can support Automatic Failover and Scalability. Server workload is further reduced with the capabilities of our PC Tools Smart Update Server. Depending on the network topology, an administrator can configure Spyware Doctor Enterprise servers to obtain their smart updates from either the PC Tools website or from other existing Spyware Doctor Enterprise server installations in your network.

Policies

The Spyware Doctor Enterprise Policies section of the Console provides access to all policies available in the connected Managed Domain. A policy defines a set of rules which determine when scheduled scans are run, the behavior of OnGuard tools and threats which should be ignored in a scan. A Policy is applied to a computer group. Any workstations residing in a computer group will automatically inherit that policy.

Scheduler

Spyware Doctor Enterprise offers an easy to use interface for managing automatic scan/fixes and scan/reports of infections in your Enterprise network. The four default scheduled patterns are: Daily, Weekly, Monthly and Once Only. The Network Administrator can also create custom schedules.

Reporting

Spyware Doctor Enterprise offers Real-Time central reporting capabilities. They are: Summary Report, Infected Computers, Infected Computers by Threat level, Infected Computers by Threat Name and a Infection Trends Summary respectively. These reports offer a consolidated view of scan and clean events, summaries and trends across all clients in your enterprise.

Licensing

Spyware Doctor Enterprise provides a convenient and organized method for licensing workstations. The console includes a License Wizard. The wizard automatically assigns available licenses to workstations that are registered within Spyware Doctor Enterprise. Conversely, once a workstation is removed from the Enterprise, the license is available to be assigned to another workstation joining the company's network.

Integrated Authentication

Network Administrators can connect to a Spyware Doctor Enterprise server without providing user logon credentials. Once the Domain Administrator is logged into the operating system, the Spyware Doctor Enterprise console will reuse the logon credentials as needed.

Real-Time Spyware Monitoring/Removal Technology

The Spyware Doctor Enterprise client agent software consists of our award winning **On Guard** real time monitoring technology. The On Guard feature is comprised of real-time monitoring guards. These guards are specifically designed to cover all spyware entry points to a computer. This approach ensures that many different types of spyware are stopped and defeated before they can infect your company's computers. **On Guard** Tools includes:

- 🔒 **Startup Guard** - Monitors and removes malicious files which try to run automatically on your system.
- 🔒 **Exploit Guard** - Protects programs from security flaws or vulnerabilities that may be utilized to perform malicious activities.
- 🔒 **Browser Guard** - Checks for browser hijackers and removes them automatically.
- 🔒 **Immunizer Guard** - Ensures that your computer is immunized against the latest ActiveX based threats that may sneak into your system.
- 🔒 **Keylogger Guard** - Prevents malicious programs from recording your keystrokes.
- 🔒 **Network Guard** - Prevents malicious changes to your network settings.
- 🔒 **Cookie Guard** - Monitors for new potentially malicious cookies and removes them promptly.
- 🔒 **Process Guard** - Stops malicious programs from running before they have a chance to damage or compromise your computer. Process guard can also detect hidden processes using our new Malicious KL (Kernel Level) Process killer technology. Spyware Doctors Enterprise's "KL Process killer" technology detects, kills & removes malicious processes which operate at the Windows Kernel level. This enables Spyware Doctor the ability to stop troublesome processes from running that either hide themselves or attempt to restart upon termination.
- 🔒 **Site Guard** (anti phishing) - Prevents access to suspected malicious web sites which may be masquerading as legitimate businesses or e-commerce sites that are designed to distribute spyware or steal confidential corporate information.
- 🔒 **IM Guard** - A new **OnGuard** real-time protection tool, IM Guard, protects users of Instant Messaging applications such as MSN Messenger from access to any potentially malicious URLs received. Such URLs can lead to phishing sites or sites which attempt to exploit your web browser.

Scanning Engines

In addition to Spyware Doctors Enterprise's **On Guard** features are State-of-the-art scanning engines including: file scan, memory scan, registry scan, browser helper objects scan, cookie scan & disk scanner respectively. These scanners are designed to detect and remove spyware on the computer's hard drive and Windows registry. Spyware Doctors' scanners are programmed to perform a full system scan of:

- 🔒 Running processes
 - 🔒 Layered Service Provider (LSP) threats
 - 🔒 All startup locations
 - 🔒 Entire system registry
 - 🔒 Contents of the Hosts file
 - 🔒 Browser defaults, Favorites folder and registry Zone Map section
 - 🔒 Internet Explorer's cookies and temp files
 - 🔒 All fixed hard drives
 - 🔒 Browser hijackers and malicious browser helper objects
-

Spyware Doctors' scanner also includes:

- **New Spider Scanning Technology (patent pending)**

Spyware Doctor Enterprise is pleased to introduce its new innovative *Spider Scanning Technology* (patent pending). The technology promises to significantly reduce scanning time (in some cases up to 25%) and produce more threat detections. The spider scan works by using a combination of signature and behavioral scanning techniques to quickly and effectively identify spyware threats.

- **New Rootkit scanning**

Along with the "Hidden process detection" feature (which blocks rootkits at the kernel driver level), Spyware Doctor Enterprise now adds an additional layer of Rootkit protection by incorporating a new Rootkit scanner. Spyware Doctor Enterprise is now fully capable of detecting and removing hidden processes associated with complex threats and rootkits. Such threats are otherwise difficult to remove by conventional means.

- **New ADS detection & removal capability**

Some nasty types of spyware have the ability to attach themselves to ordinary, harmless files through "Alternate Data Streams" (ADS). When this occurs, the item of spyware is hidden, and the harmless file appears unchanged to the user. Spyware Doctor Enterprise now has the ability to detect these types of nasty threats which hide themselves in ADS.

Spyware Doctor Enterprise **Server** and Console Requirements

Supported platforms:

- Windows Server 2003 Family (excluding x64 Edition)
- Windows 2000 Server and Advanced Server
- Intel Pentium 4 (or equivalent)
- 512 MB of RAM
- 115 MB* of free hard disk space (or 40 MB on a system already running an existing installation of Microsoft SQL Server Desktop Engine (MSDE))

Spyware Doctor Enterprise **Client** Requirements

Supported platforms:

- Windows XP Professional (with Service Pack 2)
 - Windows 2000 Professional (with Service Pack 4), Server and Advanced Server
 - Windows 98 Second Edition and Windows ME
 - Windows Server 2000 and 2003 Family (excluding x64 Edition)
 - Intel Pentium (or equivalent)
 - 64 MB of RAM
 - 15 MB of free hard disk space
-