

Spyware Doctor Enterprise

Key Features

Centralized management for client computers on a network

The centralized console allows system administrators to manage and operate **Spyware Doctor Enterprise** on networked computers in a multiple server and client environment.

Enhanced reliability through the use of Managed Domains

The Spyware Doctor Enterprise server installations are organized into **Managed Domains**, which may consist of one primary and multiple backup servers and behave as a single Enterprise Server. Managed Domains provide **uninterrupted functionality** when a backup server is automatically activated if the primary Enterprise Server becomes unavailable due to maintenance or unexpected hardware failure.

A highly scalable server and client architecture

Spyware Doctor Enterprise can manage an **unlimited** amount of client computers as required. The scanning engines are installed on each client computer to ensure **maximum server performance**.

The effective Spyware Doctor Scan Engine

Spyware Doctor Enterprise utilizes the powerful **Spyware Doctor** Scan Engine on all client computers, providing real time scanning and removal plus ongoing security features such as:

- Rapid Spider Scanning Technology
- A malicious Kernel Level Process Killer
- Rootkit scanning
- Malware detection and removal in Alternate Data Streams

A secure server and client architecture

The Spyware Doctor Enterprise system requires the domain administrator's permission to log into a Managed Domain, therefore remaining **continually secure**. Data passed between the Managed Domain and Clients is encrypted and unreadable to unauthorized parties.

An easy and intuitive console interface

The console interface allows system administrators to set up Spyware Doctor Enterprise on their networks **quickly and easily**.

Active Directory support

Client computers can be added to a Managed Domain using computers in a **Microsoft Windows Active Directory**, Domain or Workgroup.

Centralized Smart Updating of Spyware Doctor Enterprise Clients

Once a Managed Domain has been updated with the latest components from PC Tools, they can be dispatched to other Spyware Doctor Enterprise Clients or groups through a single **Smart Update** command.

An intelligent Smart Update Server component

The Smart Update Server component operates independently of the Enterprise Server component and is capable of retrieving updates from other Managed Domains. This can provide **faster update retrieval** and reduced Enterprise Server workload.

Automated retrieval of Smart Updates

The Managed Domain can be scheduled to retrieve Smart Updates from the PC Tools Web Site at regular intervals. Furthermore, any new Smart Updates can **automatically** be pushed to Spyware Doctor Enterprise Clients following a Server update.

Centralized management of Scan Scheduling

Spyware Doctor Enterprise allows the creation of multiple **Scan Schedules** for either **Scan and Report** or **Scan and Fix** commands. These Scan Schedules can be assigned to one or more Spyware Doctor Enterprise Clients groups through a Policy. If required, e-mail notifications can be configured to advise the administrator of the scan results.

Real-time reporting of infected computers on the network

After a **Scan and Report** command is completed, the scan results are sent back to the Spyware Doctor Enterprise Server. The System Administrator can then view scan results that indicate the **current state** of Spyware Doctor Enterprise Client computers as well as historical scan data, via the Console.

Immediate notification of infections or other warnings via e-mail

The Spyware Doctor Enterprise Server can be configured to send **e-mail notifications** to the administrator when client computers have been infected with malware, and for other issues requiring attention on the Server or Client.

Small footprint

The Spyware Doctor Enterprise Server, Console and Client components do not consume a substantial amount of hard drive space upon their initial installation, and only require about **10-20 MB of virtual memory** when active.

Comprehensive auditing of logins and commands

Spyware Doctor Enterprise provides comprehensive logging capabilities for logins, errors and warning events. All commands and results are logged in the Spyware Doctor Enterprise Server's information logs, each using **transaction IDs** which allow commands to be traced from their inception to their final result.

ODBC Support

Spyware Doctor Enterprise utilizes the common **Object Database Connectivity** (ODBC) interface, providing applications with the potential to access a wide range of databases on a network. Spyware Doctor Enterprise currently supports Microsoft SQL Server Desktop Engine (MSDE) and Microsoft SQL Server 2000 databases.

Easy Spyware Doctor Enterprise Database backups

The Spyware Doctor Enterprise Database component can be installed on a separate server in a Managed Domain. **Multiple Managed Domains** can connect to this database, which greatly simplifies the task of backing up the Spyware Doctor Enterprise Database on a multiple server and client network.

Policy implementation for predefined rules and settings to computer groups

Spyware Doctor Enterprise implements policies to define **scan schedules**, **OnGuard** settings, and **ignore list** selections for specific computer groups. This provides **easier management** of Spyware Doctor Enterprise Client settings at the computer group level. Computers assigned to a specific group are governed by the policy assigned to that group.

Customizable OnGuard settings

The settings of individual **OnGuard** tools can be specified through a Spyware Doctor Enterprise policy. Within a policy, each OnGuard tool can be selectively enabled or disabled. Some OnGuard tools provide **additional options**, which permit fine tuning of their behaviors on Spyware Doctor Enterprise Clients.

Enhanced infection and summary reports

The Spyware Doctor Enterprise **Reports** feature has been expanded to provide a greater range of reporting capabilities, including the ability to print report pages and list infected computers on your network by names of specific threats or threat risk levels. Summary and trend summary reports give additional information and new graphical results.

Enhanced Console interface and functionality

A number of features have been included in the Spyware Doctor Enterprise Console interface, making it more informative and **easier to use**. These features include a customizable computer list view showing a greater degree of computer status details, computer names included in infection alerts, and the ability to reboot Spyware Doctor Enterprise Client computers remotely.