

# Protecting Endpoint Systems Against Spyware

---

## Table of Contents

<b>Executive Summary</b>		
SECTION 1: CHALLENGE	<b>2</b>	SECTION 4: CONCLUSIONS <b>13</b>
<b>Issues Surrounding Spyware Threats</b>		SECTION 5: REFERENCES <b>13</b>
What Is Spyware?		ABOUT CA <b>Back Cover</b>
SECTION 2: OPPORTUNITY	<b>3</b>	
<b>Requirements for Effective Spyware Protection</b>		
<b>What Is CA Anti-Spyware?</b>		
Client-Server Mode		
Client-Only Mode		
The Anti-Spyware Client		
Alerts		
Quarantine		
Signature Updates		
How Is CA Anti-Spyware Deployed?		
How Is CA Anti-Spyware Managed?		
Reporting		
SECTION 3: BENEFITS	<b>11</b>	
<b>Benefits of CA Anti-Spyware</b>		
Certification		
Platform Support		
<b>Business Benefits of CA Anti-Spyware in an Integrated Solution</b>		

# Executive Summary

## Challenge

---

Spyware is now one of the top computer threats, although it is not always easy to define what is and what is not spyware. There are many types of spyware, so good anti-spyware applications must be able to protect computers against all types of non-viral malware threats and also be able to rapidly respond to new and emerging types and varieties of spyware.

## Opportunity

---

Anti-spyware applications must be able to reliably and consistently identify and detect spyware. The characteristics that are used to identify spyware must be published, so that it is clear what criteria are being used.

An effective anti-spyware application must have a reliable scanning engine so that the application can remove spyware threats rapidly and effectively, and the application must be regularly updated when new spyware signatures are developed. Policies and deployment tools must be available, so that administrators can deploy, configure and manage anti-spyware clients from a central location.

## Benefits

---

CA Anti-Spyware uses signature-based techniques to protect computers against non-viral threats. These techniques complement the approach that is used by anti-viral applications and the behavioral techniques used by intrusion prevention applications, such as CA Host-Based Intrusion Prevention (CA HIPS). CA Anti-Spyware works with these other CA Threat Management Solutions providing a complete suite of threat management tools.

*For more information about types of malware, see “Technology Brief – The CA Threat Management Solutions”.*

---

## Issues Surrounding Spyware Threats

A recent IDC study<sup>1</sup> found that the top computer threats are viruses, spyware and unsolicited email, or spam. For this reason, anti-spyware is now fundamental to enterprise threat defense.

### What Is Spyware?

Spyware is a program that is installed, with or without the user's permission, and can monitor computer activity while broadcasting the information back to an outside party who controls the program. However, without clear definitions of what is and what is not “spyware” it is difficult to promote industry-wide standards and protection tools. Some spyware developers may claim their software is a legitimate marketing tool, and some software may only be considered “spyware” under particular circumstances. For example, some keylogger tools are used as part of health monitoring software to help reduce the risk of repetitive strain injuries (RSI) for office workers. For this reason, CA works with the Center for Democracy and Technology and other anti-spyware vendors, as part of the Anti-Spyware Coalition to help define spyware and establish best practices.

Common spyware behaviors include:

- **Adware** Spyware that displays unwanted advertising to your desktop / laptop can track your Web surfing habits and report them back to a central advertising server. This type of spyware can slow your PC to a crawl by bombarding it with unwanted ads.
- **Keyloggers** Spyware that can record every keystroke you make on your PC and steal your passwords and confidential data.
- **Browser Hijackers** Spyware that can reset your default homepage and search results. Some may prevent you from changing your browser homepage back to its original default or visiting a particular site.
- **Remote Access Trojans** Spyware that can give a hacker complete control over your PC, as if the hacker was at your keyboard.
- **Browser Helper Objects** Spyware that can search all of the pages you view in Internet Explorer and replace banner advertisements with targeted advertisements, monitor and report on your actions, and change your homepage.

---

1 Source: IDC, “Worldwide Secure Content Management 2006-2010 Forecast Update and 2005 Vendor Shares: “The Convergence of Secure Content and Threat Management,” #203550, September, 2006

## Requirements for Effective Spyware Protection

Applications that are detected by anti-spyware applications must be evaluated against a set of characteristics, such as those defined in the CA Anti-Spyware Scorecard. These criteria describe behavior that are typical of spyware and which may cause a loss of productivity, privacy and security. Although many of these behaviors are also common in legitimate software, the difference is that spyware either does not ask for user consent, or hides consent instructions deep within large readme files or installation agreements. Typical spyware behaviors include:

- **Installation** The software installs itself without obtaining user permission or even when the user selects "no", because the installation either does not provide an opt-out or does not provide a clear and explicit opt-out.
- **Uninstallation** The software cannot be uninstalled by Windows Add/Remove Programs and no uninstaller is provided with the application. In some cases the uninstaller is a covert re-installer. The uninstaller may leave potentially damaging running objects, executables or other components after reboot. The software defends itself against removal of, or changes to, its components.
- **Browsers** The software changes browser settings without clearly informing the user or obtaining permission.
- **System configuration** The software makes changes to the system configuration without informing the user or obtaining permission. For example, the spyware might create or modify the "hosts" file to divert domain name system lookups to use illegitimate IP addresses.
- **Dialing** The software dials phone numbers without user permission.
- **Popups** The software displays popup or popunder advertisements, even when the software is not being used, which are not connected with the software itself. Advertisements that do not have a clearly visible Close option.
- **Updates** The software updates itself without displaying any notice to the user, or without permission.
- **User information** The software transmits user data to a remote server without clearly informing the user of the information being passed, and without permission.
- **Covert behavior** The software covertly modifies another program or changes website content, such as changing search results.

Effective anti-spyware applications should include the following components:

- **Reliable and comprehensive scanning engine** It is essential that anti-spyware applications remove non-viral malware threats rapidly and effectively.
- **Regular signature and software updates** All anti-spyware applications must be able to be updated quickly when new spyware signatures are developed. Signature updates must be packaged so that updates can be rapidly deployed across all computers in an enterprise. The anti-spyware software itself must also be able to be updated, to meet new types of non-viral threats.

- **Policy-based Management** Policies enable administrators to configure and manage anti-spyware clients from a central location. Policies can be used to schedule updates and spyware scans, manage alerts and set the level of protection required. Policy-based management is important for most enterprises, because all users and computers do not need the same settings for anti-spyware protection.
- **Simple Deployment Tools** If multiple computers are installed across several physical locations, it is important to be able to rapidly deploy anti-spyware protection by using automated methods. It must also be simple to deploy software updates across the network and to identify any computers that have not been updated.

---

## What Is CA Anti-Spyware?

When deployed in standalone mode, CA Anti-Spyware provides anti-spyware security for business PCs, servers and Personal Digital Assistants. CA Anti-Spyware is a client (endpoint) protection tool that protects computers against all types of non-viral malware. CA Anti-Spyware can be installed as an Agent Only Install for isolated clients, such as home office computers, or can be configured and managed from a central management server.

You can use CA Anti-Spyware on its own, as a “standalone” threat protection, or as part of CA Threat Manager or a CA Protection Suite. In either case, CA Anti-Spyware can be installed in one of two modes: client-server mode, or client-only mode.

*For more information about the server components, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”*

### Client-Server Mode

For most enterprises, client-server mode is the best way to use CA Anti-Spyware, with a central server managing anti-spyware protection on client computers. In client-server mode, CA Anti-Spyware has the following components:

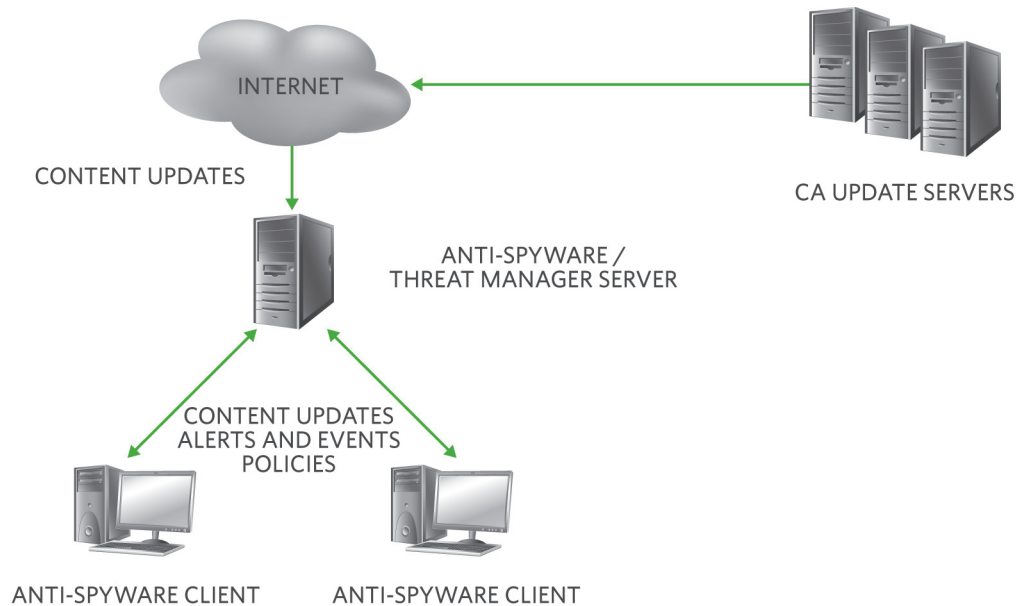
- **Server components** The main server component is the management server, which includes the web-based management console and Alert Manager. Policies are managed from the server and stored in a database, before they are deployed to client computers. There is also an option to install additional redistribution servers, to help distribute anti-spyware updates to client computers. Another optional server component is the Remote Install Utility, which deploys CA Anti-Spyware to Windows client computers.
- **Client components** The main client component is the anti-spyware agent, which includes a web interface and the shell scanner. The client components are described in more detail later in this brief.

Figure A shows CA Anti-Spyware used in client-server mode.

FIGURE A

CA Anti-Spyware is generally used in client-server mode.

#### CA ANTI-SPYWARE CLIENT-SERVER MODE



When the anti-spyware agent is running on the client computer, the agent initiates communications between itself and the web-based management console. To reduce bandwidth requirements, the frequency that the agent "phones home" to the management console to report its status and obtain new policy configurations is a separate configuration option to the frequency that clients poll for signature updates. The defaults for these two settings are every two days for "phone home" and every hour for signature updates.

A different process is used if a scheduled job, such as a hard disk scan, is defined as a policy on the server. In this case, at the time specified for the job, the server pushes the job details to all clients affected by the policy. The client does not store the details of this policy. This means that administrators can easily create new scheduled jobs, and have them run at any time, without having to wait for the clients to first contact the server to get updated information.

#### Client-Only Mode

If necessary, you can use CA Anti-Spyware in client-only mode. This mode can be useful in situations where it is not possible to use centralized management. Computers used by home office workers, or laptops used out of the office, may be suitable for this mode. In client-only mode, CA Anti-Spyware is installed directly to each client, and each client makes an independent connection to the CA Content Update servers to download updated spyware signatures and rules. In client-only mode there is no central management function, but you can easily migrate standalone clients to client-server operation by using discovery.

*For more information on the discovery process, see "Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions".*

FIGURE B

CA Anti-Spyware can be installed in client-only mode.

CA ANTI-SPYWARE CLIENT-ONLY MODE



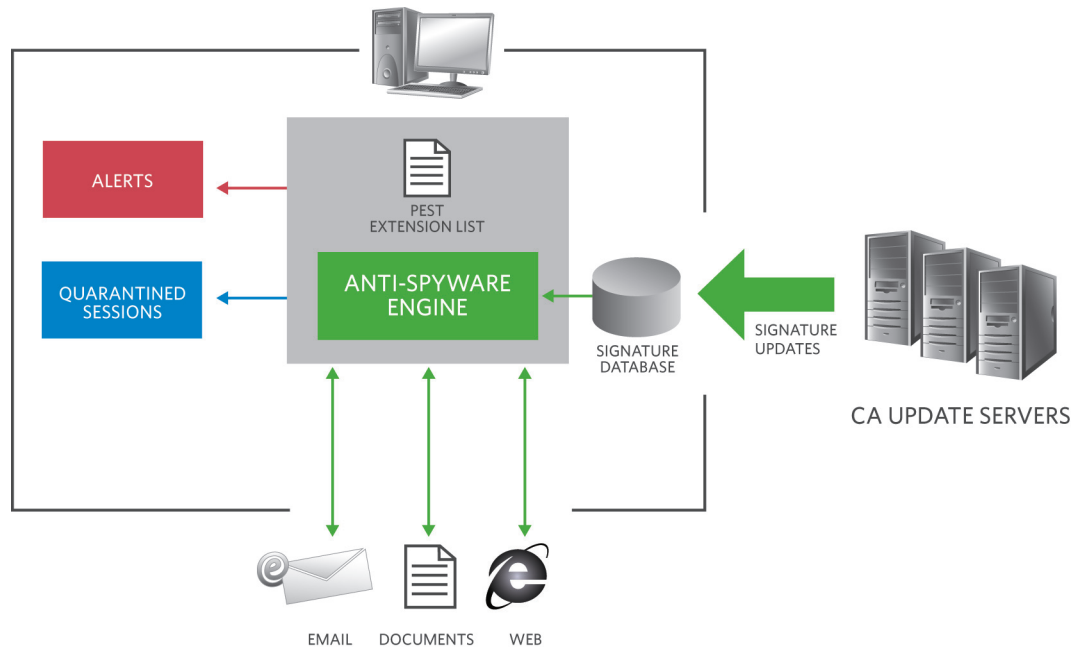
The CA Anti-Spyware Client

The anti-spyware client works the same way, whether used in client-server or client-only mode. CA Anti-Spyware provides comprehensive file scanning.

FIGURE C

CA Anti-Spyware uses several components as part of the spyware protection process.

CA ANTI-SPYWARE CLIENT COMPONENTS



### The main components of the anti-spyware client are:

- **Anti-Spyware Agent** This agent includes a real-time scanner that scans files as they pass through the computer, and a local scan engine for on-demand scanning. The agent is responsible for scanning files for spyware. The engine uses the signature database during the scanning process to compare the items it is scanning with spyware fingerprints and behaviors in the database. During real-time scanning the agent monitors system activity, so that if any potential spyware behaviors are detected the agent, subject to its configuration options, takes appropriate action, such as using quarantine or sending an alert, for example. This proactive monitoring of system calls is important, because it means that the anti-spyware agent can intercept spyware before it can run.
- **Pest Exclusion List** Some applications may be considered to be spyware in some circumstances, but not in others. Remote control software, for example, might be a legitimate tool for some network administrators, but not for all your users. You can, therefore, exclude some software from being scanned by using the pest name, pest category, or by a pathname. These “safe lists” of authorized applications, can be fine-tuned by department or individual, to prevent false alarms.

### Alerts

You can configure CA Anti-Spyware to generate an alert when spyware is detected. These alerts can be sent to:

- **The local Alert Manager (if available)** The Alert Manager utility is a Windows-only application and is normally run on the anti-spyware server. Alert Manager collects alerts and forwards them to system administrators by using email, SMS messages, and pager or enterprise management applications, such as CA Unicenter®.
- **Event logs** On Windows computers, alerts can be sent to the application Event Log; on UNIX/Linux computers, alerts can be sent to the System Log.
- **Another computer** Alerts can be forwarded to another computer, so that information from across the enterprise can be collected and processed centrally. In a typical configuration, client computers forward alerts to an anti-spyware or threat manager server. The server also forwards its own alerts to itself, so that all alerts (including its own) are collected. The server is also configured to send alerts to its own local Alert Manager, so that administrators receive immediate notification of priority alerts.

### Quarantine

CA Anti-Spyware uses sessions to quarantine infected files. A session is a time-stamped container that stores all pests that are detected and quarantined during a particular pest scan. Each session has a unique session name and the date and time of the scan. You can restore items from quarantine, by restoring the relevant session.

### Signature Updates

The spyware signature updates for CA Anti-Spyware use MicroDAT technology to ensure that content updates are less than 500 KB in size. This helps to ensure up-to-the-minute spyware protection, because the small size of the updates means distribution has minimal impact on network traffic. If a distribution server is unavailable, because the server is offline or a mobile user is using a laptop from a public network, anti-spyware clients automatically look for and acquire the latest signature from the next available designated distribution server.

*For more information about content update servers, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”*

*The same deployment tools that are used to deploy CA Anti-Spyware are used to deploy CA Anti-Virus. For more information about the deployment options, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”*

### **How Is CA Anti-Spyware Deployed?**

There are several ways to deploy CA Anti-Spyware across an enterprise. If you have a small number of client computers you can use the CA Anti-Spyware CD-ROM and run setup on each computer. However, for most enterprises some form of automated deployment is required, so CA Anti-Spyware can be deployed by using several deployment tools:

- **Remote Installation Utility** This utility can be installed in the anti-spyware server, and is used to configure client installation options. These options are saved in an Installation Control File (ICF). The Remote Installation Utility can then push client installations to any computers on the network.
- **Command-line installation** You can use the ICF with a command-line installation tool to install CA Anti-Spyware from a network share point. If you wish, you can configure the installation to be silent, so that users are unaware that CA Anti-Spyware is being installed on their computers.
- **Software delivery** You can use an automated software delivery tool, such as CA Unicenter® Software Delivery or Microsoft SMS, to deliver CA Anti-Spyware application packages to client computers.
- **Login Scripts** You can use a login script together with any of the silent installation command-lines, to deliver silent installations across the network.

### **How Is CA Anti-Spyware Managed?**

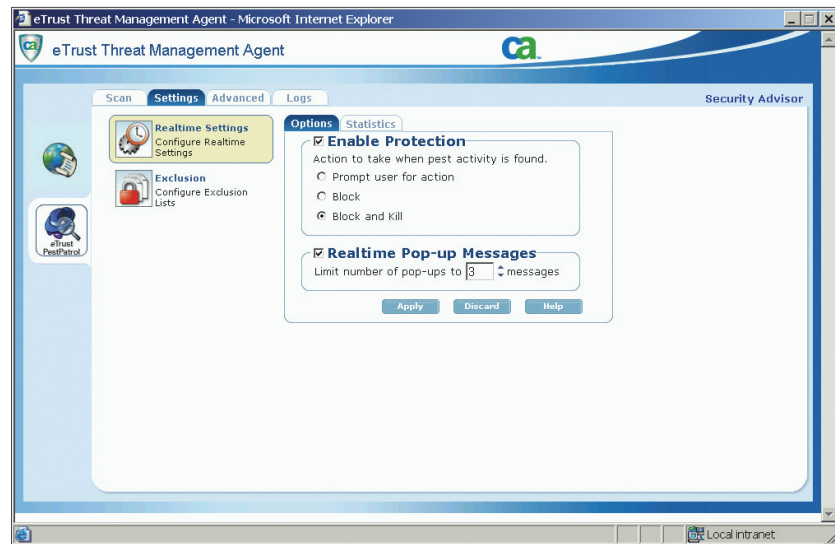
CA Anti-Spyware uses a multi-tiered architecture and a hierarchical organization structure, so that users and computers can be defined in relation to the business unit, location or other criteria. When you have defined your users and computers you can apply anti-spyware policies to the different parts of your enterprise by using your organization structure. Management tools are available on both the anti-spyware client and the management server.

**CLIENT USER INTERFACE** The anti-spyware client can be installed without a user interface by using an option in the ICF. If the user interface is enabled, the interface displays status information and includes several configuration options. However, even if the user interface is available, you can use policy options to prevent users from changing some of the settings.

FIGURE D

The anti-spyware client can be installed so that there is a user interface.

## CA ANTI-SPYWARE CLIENT USER INTERFACE



On Windows computers the client user interface is the same whether CA Anti-Spyware is installed on its own, with CA Anti-Virus, or as part of CA Threat Manager (CA Anti-Virus is also available for non-Windows platforms). If CA Anti-Virus is also installed, the interface includes an Anti-Virus tab. The user interface is divided into several tabs:

- The Dashboard tab provides the user with a summary of the current status of the anti-spyware client, including signature and engine versions and anti-spyware activity.
- The Scan tab enables the user to set up and configure scans of local disks.
- The Settings tab enables the user to configure options such as alerts and logging, if policies permit the user to do this.
- The Update tab enables the user to specify signature update frequency and which servers should be contacted for updates.
- The Advanced tab enables the user to manage quarantine activity and inspect the job queue, such as pending scanning or update jobs.
- The Logs tab enables the user to view activity logs.

Server tools. When you install the server components you get these tools:

- **Server console** This provides information about the server, software versions and the clients that are managed from the server. The console is also the tool you use to manage clients and client policies, and receive reports about threat activity. The console provides a complete view of the anti-spyware situation within your enterprise.
- **Alert manager** The Alert Manager enables you to configure how alerts are sent to people or devices in your organization so you can quickly respond to alerts. For example, alerts can be sent to an email Inbox, a pager, an NT event log, an SNMP trap, CA Audit®, or CA Unicenter. The Alert Manager runs on Windows only.

*For more information about the server components, see “Technology Brief — Protecting Endpoint Systems Using Threat Management Solutions.”*

- **Redistribution server** This can also be installed on its own, for a computer that only acts as a redistribution server. When this is installed, in addition to the standard agent components and UI, an extra item on the Update tab enables you to configure the redistribution.

### **Reporting**

When installed in client-server mode, you can configure the anti-spyware client to send status and event information to the central server. You can configure severity levels for the different types of information sent, so that critical messages are forwarded to the server Alert Manager for immediate attention. The server stores all the event information it collects from anti-spyware clients and periodically processes this information into reports, by default every 24 hours. All CA Anti-Spyware reports are generated on the server by using the web console.

The reporting engine in CA Anti-Spyware provides 75 different types of graphical and detailed reports, including:

- **Top ten pests** This report gives a summary of the most prevalent spyware across your network.
- **Top ten computers** This report gives a summary of the computers that have reported the most spyware-related events across your network.
- **Top ten users** This report gives a summary of the user accounts that have reported the most spyware-related events across your network.

All the top ten reports can be formatted for hourly, daily, weekly, monthly and quarterly reports.

- **Signature exception lists** This report shows the clients that have not received the latest signature updates, which can be a useful indicator of network problems or mis-configured clients.

Reports can be created based on the workstation name, the date and time, security risk priority and pest category. You can also create reports about specific pests to assist with risk evaluation.

By default, every two days, the reporting engine also runs a discovery process across the network, and collects information about all the Windows computers by domain or workgroup, and whether they are running CA Anti-Spyware or other CA Threat Management Solutions. These sets of reports also show which computers do not have anti-spyware installed, so they provide an up-to-date list of systems that represent potential risks because they are not protected.

## Benefits of CA Anti-Spyware

CA Anti-Spyware includes a range of features that are designed to protect client computers from spyware threats and include:

- **Comprehensive Real-Time Scanning** CA Anti-Spyware proactively monitors system calls. This is important because it intercepts spyware before it can run. Additional scans can be scheduled from the management console.
- **Central Web-Based Management** A single web-based management console for managing any size of diverse environment is important, because:
  - It provides a complete view of the anti-spyware situation in your enterprise.
  - You can use any suitable Windows platform as the core platform for managing all CA Anti-Spyware clients.
- **Bandwidth Savings for Pest Updates** MicroDAT signature updates (less than 500KB) help to ensure up-to-the-minute spyware protection, because their small size speeds up the distribution with minimal impact on network traffic.
- **Real-time Alerts** If CA Anti-Spyware detects spyware, CA Anti-Spyware generates an alert and logs the event, and enables you to remove pests from computers in real-time. You can define “safe lists” or exclusion files of authorized applications, fine-tuned by department or individual, to prevent false alarms.

### Certification

CA Anti-Spyware is certified by industry experts and has received the Anti-Spyware Desktop Checkmark certification from West Coast Labs. West Coast Labs is an independent organization that tests the effectiveness of information security products for detecting Trojans, keyloggers and other assorted malware. Certifications provide enterprises with independent verification that CA Anti-Spyware is effective in protecting their computers against current spyware threats.

### Platform Support

CA Anti-Spyware has multi-language support, and supports English, French, Italian, German, Spanish, Japanese, Brazilian Portuguese, Traditional Chinese and Simplified Chinese. If your enterprise is multi-lingual or global, you can select the best language for your users.

CA Anti-Spyware is available for Windows computers only. CA Anti-Spyware r8.1 supports the following Windows versions for the client:

- Windows NT 4.0 SP6a
- Windows 2000 Workstation and Windows 2000 Server
- Windows XP (32-bit)
- Windows Server 2003 (32-bit)
- Windows Vista (32-bit)

CA Anti-Spyware r8.1 supports the following Windows versions for the management server:

- Windows NT 4.0 Server (SP6a or later)
- Windows 2000 Server
- Windows Server 2003

The anti-spyware server is managed using a web console, and can be accessed using the following browsers:

- Internet Explorer 6 SP1 and above
- Mozilla Firefox 1.5 and above

---

## Business Benefits of CA Anti-Spyware in an Integrated Solution

### How CA Anti-Spyware Works with Other CA Threat Management Solutions

One product or technique cannot protect against every possible threat. Multiple layers of defense are required, which are provided by different products for different threats. A combination of products that work together is needed to protect network-enabled workstations and mobile devices from network-based attacks. CA Anti-Spyware has been designed to integrate with CA Anti-Virus to provide protection against both spyware, and other non-viral malware, and viral threats.

When used together, CA Anti-Spyware and CA Anti-Virus are managed from the same web-based administration console that runs on an integrated threat management server, and both client applications are deployed as a single agent. This integration works in the same way whether you buy CA Anti-Spyware and CA Anti-Virus as separate products, or buy them bundled as CA Threat Manager.

**CA ANTI-SPYWARE** is a core product within the CA Threat Management Solutions which includes solutions for both endpoint systems (desktop, server, laptop, and other network access points) and gateways:

- **CA Anti-Virus** Standalone anti-virus protection for endpoint systems.
- **CA Threat Manager** Integrated anti-spyware and anti-virus protection for endpoint systems.
- **CA HIPS** Personal firewall, intrusion detection system (IDS) and intrusion prevention system (IPS) for endpoint systems.
- **CA Protection Suites** Integrated anti-spyware and anti-virus protection for endpoint systems, together with data backup and optional endpoint anti-spam.
- **CA Secure Content Manager** Anti-virus protection for the gateway, SMTP and HTTP filtering for incoming Web and messaging threats/spam and content filtering of outgoing email traffic.

CA Anti-Spyware is designed to work with other products in the CA Threat Management Solutions to provide comprehensive endpoint threat protection:

- CA Anti-Spyware is designed to detect and remove non-viral threats. When used with CA Anti-Virus, either standalone or as part of CA Threat Manager or the CA Product Suites, CA Anti-Spyware detects and removes malware threats that evade detection or that previously infected the endpoint.
- CA HIPS helps to prevent known and unknown threats, such as malware, spyware, adware and rogue software, from penetrating the network. CA HIPS provides proactive, host-based security against zero-day attacks. System administrators can use the key functionality within CA HIPS to learn system behavior and then create or edit existing policies to detect anomalies.
- CA Secure Content Manager monitors, filters and blocks potential threats from messaging, such as malware in spam, and infected Web traffic.

---

#### SECTION 4: CONCLUSIONS

Anti-spyware tools are fundamental to enterprise threat defense. CA Anti-Spyware works with other CA Threat Management Solutions to help provide a complete suite of threat management tools. CA Anti-Spyware signature-based techniques identify non-viral threats, and these techniques complement the approach used by anti-virus applications and the behavioral techniques used by intrusion prevention applications, such as CA HIPS.

---

#### SECTION 5: REFERENCES

“Anti-Spyware Coalition”:

<http://www.antispywarecoalition.org>

---

“CA Anti-Spyware scorecard”:

<http://www3.ca.com/securityadvisor/pest/content.aspx?q=95590>

---

“CA Security Advisor”:

<http://www3.ca.com/securityadvisor>

---

“Center for Democracy and Technology”:

<http://www.cdt.org>

---

“West Coast Labs”:

<http://www.westcoastlabs.org>

---

To learn more about the CA Anti-Spyware architecture and technical approach, visit [CA Anti-Spyware Product Page](#) .

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies complex IT management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

TB05ASPED01E MP317600607

---

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

