

Spyware: The first thing you need to know is that you probably have it.

Websense, Inc.
World Headquarters
10240 Sorrento Valley Road
San Diego, California 92121
USA
Tel: 800.723.1166 or 858.320.8000
Fax: 858.458.2950
www.websense.com

Abstract

Spyware—software installed on a computer usually without the user's knowledge or permission—along with adware and other similar software, gathers information and sends it back to the advertiser who initiated it or other interested parties. Spyware can collect and transmit information such as keystrokes, Web surfing habits, passwords, email addresses, and other sensitive information you may not want to share outside your organization. Spyware also misuses system resources and bandwidth as it tracks and transmits information. More seriously, spyware can also pose grave security, confidentiality, and compliance risks.

With its unique layered approach, Websense Enterprise® protects organizations by identifying spyware in an organization's network, blocking access to spyware Web sites, and preventing spyware applications from launching, whether the infected computer is connected to the network or not. Websense gives organizations complete confidence that spyware and adware will not gain a foothold in their IT environments and will not proliferate through their computer systems.

Contents

Executive Summary	1
Spyware: More Than Just An Invasion of Privacy	2
What is spyware?	2
What is adware?	2
How do spyware and adware spread?	3
Giving permission	3
Visits to certain Web sites	4
Clicking on deceptive or confusing pop-ups	4
During P2P transfers or other software downloads	4
What do spyware and adware do?	4
Compromise information security	5
Increase demands on IT Help Desk staff	5
Degrade worker productivity	7
Why Current Solutions Are Inadequate	7
Firewalls	7
Antivirus solutions	7
Spyware removal tools	7
How Websense Enterprise® Mitigates Spyware Risks	8
Detect the extent of spyware in the organization	8
Prevent and protect employees from accessing sites that distribute spyware	9
Prevent spyware from transmitting information to host spyware servers	10
Block the launching of spyware applications	10
Block the launching of spyware applications that carry spyware	11
The unique advantages of Websense Enterprise®	11
Conclusion	13
About Websense, Inc	13
Appendix: The Websense Enterprise® Solution	14

Executive Summary

Spyware programs collect data on users and their computing behaviors and then transmit that information back to the spyware host server. These programs can also monitor keystrokes, scan files on hard drives, secretly install other programs, and even make changes to default computer settings. Spyware is often acquired surreptitiously when users download a “real” application or file, visit certain Web sites, or click on a deceptive pop-up window.

Unlike spyware, which is acquired without user knowledge or approval, adware is installed with permission, usually after the user agrees to the terms of a long and confusing End User License Agreement. These more benign programs also collect information about users or user habits, but typically use it to tailor future pop-up advertisements to users’ preferences for marketing purposes.

These programs cause performance problems and use expensive computing resources (processing power, drive space, and bandwidth). They can also cause software conflicts with legitimate programs and affect employee productivity. Of most concern to organizations, however, is the fact that spyware compromises information security and consumes valuable IT Help Desk resources. Organizations whose investors and clients rely on them to safeguard personal, medical, and financial information need a way to prevent spyware from covertly accessing and transmitting critical corporate information. Similarly, organizations whose Help Desk resources are burdened to correct, often by “re-imaging” entire systems thereby preventing the corruption of the desktop computing environments.

The security measures currently in place in most organizations—a combination of a firewall, antivirus software, and spyware/adware removal programs—do not adequately address the threat of spyware. Since firewalls operate at the boundary of the network, they have no visibility into the spyware running inside the network. Antivirus solutions are not adequate either, since antivirus software typically doesn’t include spyware signatures and cannot prevent spyware from transmitting information. And spyware removal programs, which are targeted to individual consumers not organizations, do not provide a centrally managed solution and do not adequately address the burden of application conflicts.

Organizations need a way to keep spyware from gaining access to their systems in the first place. To do this, organizations must be able to prevent employees from visiting sites that distribute spyware and from downloading applications that are infected with spyware. For spyware that may be brought on to the desktops through other channels, such as home or mobile laptop use, or via CDs or eFlash drives, organizations also need a way to stop spyware from ever launching, thereby protecting the corruption of that desktop, as well as preventing the transmission of data back to host servers.

Organizations need Websense Enterprise® to stop spyware in its tracks. Websense Enterprise protects organizations by identifying spyware already on company computers, blocking access to spyware Web sites, and preventing spyware programs from launching—on employee desktops and even on laptops that are disconnected from the organization’s network.

Spyware: More Than Just An Invasion of Privacy

What is spyware?

U.S. Senate Bill 1436 defines spyware as “an executable program placed on your computer without your knowledge that monitors your actions or takes your personal information and reports it to a third party”.¹

Spyware programs usually collect information from a user’s computer – personal information, such as a name or an email address — and send it back to their host server.

*A recent study found that the average computer houses 28 items of monitoring software, unbeknownst to the user.*²

Some spyware programs collect information using “keystroke loggers,” which capture information about the user’s computer activities, including cookies and time spent on certain sites. Some capture all keystrokes users make; others are more focused, recording Web sites visited, passwords, emails, credit card numbers, and so on. Most keyloggers are invisible and save recorded keystrokes into a log file that is transmitted periodically back to the host server. Some can even record both sides of instant messaging chat conversations (for example, MSN[®] Messenger and Yahoo![®] Messenger).

Example—In one case, a college student was charged with enticing investors to help beta test a new stock-charting tool by downloading the tool on their computers. Unfortunately, the unsuspecting investors also installed a keylogger at the same time, which the student used to capture their usernames and passwords. The money taken from one TD Waterhouse account alone was about \$47,000.³

Spyware can also read a computer’s unique hardware ID number (MAC address) and IP address, and can combine that information with surfing habits and correlate it with any personal information provided during a “free” software download or when a file attachment was opened. This information can then be traded with affiliate advertisers, building a complex dossier on individual users and what they like to do on the Internet .4 Other programs are simple, “useful” applications like clocks, calendars, or mouse pointers, which are attractive bait for downloading spyware.

*Only six percent of employees who access the Internet at work said they have ever visited any Web sites that contain spyware; however, 92 percent of IT managers estimate that their organization has been infected by spyware at some point.*⁵

What is adware?

Although similar, adware is distinguished from spyware by the fact that, when downloading adware, the user is first given an opportunity to agree to its being placed on his or her computer. The explanation of an adware

1 Source: www.clickz.com/news/article.php/3349621

2 Source: Internet Service Provider Earthlink and Webroot Software

3 Source: <http://www.prweb.com/printer.php?prid=100583>

4 Source: <http://antivirus.about.com/library/weekly/aa020503a.htm>

5 Source: Websense “Web@Work Survey Results 2004”

program and what it will do is often buried in a long, complex End-User License Agreement (EULA) that many users simply scroll through and accept without reading completely. In practice, adware acts as spyware. Both may trigger the display of pop-up or banner advertisements, and both may gather and transmit information from the user's computer.

How do spyware and adware spread?

Spyware and adware can be acquired in several different ways:

- when users unknowingly give their permission while downloading/installing applications
- by simply visiting certain Web sites
- when users click on a deceptive or confusing pop-up
- during a peer-to-peer (P2P) file transfer or software download

Giving permission

Before installing most software programs, users are required to read and sign an End User License Agreement. But EULAs are long, confusing, and sometimes even deceptive. From a legal standpoint, everything may be duly disclosed in the EULA, but EULAs are often so long and complex that many users just click through them, never stopping to read them closely.

In a University of Washington study, researchers found that twelve different spyware and adware programs had been bundled with Kazaa, and every version of Kazaa released has included at least two different spyware programs.⁶

For example, a user who wants to install Kazaa must also install additional programs, including the following:⁷

Cydoor—Adware that exploits users' Internet connections to update its ads and store them on their hard drives.

Topsearch—A Browser Helper Object (BHO) that Internet Explorer loads on startup. BHOs are not stopped by firewalls, because firewalls see them as browsers. Some specimens of this technology search all pages viewed and replace banner advertisements with other ads. Some monitor and report on your actions. Some change the user's home page.

GAIN AdServer—The Gator Advertising Information Network software gathers information on computer use and uses that information to deliver targeted advertising.

PerfectNav—Software that sends users to PerfectNav's Web page when they type URLs incorrectly.

9.4.6 In exchange for downloading the Software at no cost, you expressly agree that you accept the Embedded Third Party Software and that you will not take any action, including downloading other software intended to, or modifying or permitting others to modify registry or other settings on your computer to, disable or remove the Embedded Third Party Software or to prevent its functioning.

Figure 1. The Kazaa EULA requires users to agree not to delete the embedded third party software.

⁶ Source: <http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf>

⁷ The language and content in this section is taken directly from the Kazaa End User License Agreement, May 11, 2004.

Visits to certain Web sites

Some spyware is secretly downloaded when a user launches a program acquired from a Web site. For example, a pop-up may notify the user that a special plug-in is required to run a video or movie file. In this case, what appears to be a legitimate plug-in could actually be spyware. Some spyware takes advantage of known vulnerabilities in the Microsoft® Windows operating system and Internet Explorer browser to secretly place spyware onto the user's computer. For example, one such method involves pushing malicious JavaScript and VBScript code to the user's Web browsers when they visit a seemingly ordinary Web page. If the user's Internet Explorer security preferences are set to the lowest levels, the code can install spyware programs on the user's hard drive and even set them so that they launch automatically the next time the user reboots. It can also insert toolbars and other objects into the browser itself, essentially changing the way the browser works in the future—all without the user's permission.

Another method bypasses the security settings altogether by exploiting a bug in Internet Explorer versions 4 and 5. These versions allow Web scripts to gain access to a hard drive by overflowing the browser with data. Malicious webmasters use this exploit to install spyware or modify the way the browser works.

Clicking on deceptive or confusing pop-ups

Some pop-up screens don't actually deliver advertisements but attempt to install unwanted software on your system and change your system configurations. These pop-ups can be very clever. Instead of "To install this program, click Yes," the prompt unexpectedly reads, "To install this program, click No." After clicking on these pop-ups, the user may find that the computer now displays new bookmarks and a different home page as well as having unwanted software installed.

During P2P transfers or other software downloads

Some spyware hides out in group directories on peer-to-peer (P2P) networks, such as music sharing networks, and then spreads by infecting machines as users search for music selections. Other spyware is bundled with software that the user is intentionally downloading or purchasing. Some of these programs are bundled so tightly that, once installed, they are nearly impossible to get rid of.

In the U.S. House of Representatives, one computer was rendered inoperable by software conflicts caused by the programs bundled with P2P file-sharing programs. Even the computer technicians were unable to remove the offending programs completely. These experts suggested hard drive reformatting as the only way to resolve the resulting computer difficulties.⁸

What do spyware and adware do?

Employees may not even know that their computers have been infected until they find ads popping up all over their desktops. Or one day they may notice that their computers are working slower than usual, which happens when spyware programs are uploading information to a remote server or are downloading new ads. These are only symptoms of what can be a very serious problem for an organization.

⁸ Source: <http://reform.house.gov/UploadedFiles/P2P%20Security%20Report.pdf>

Compromise information security

Because spyware and adware exist as independent executable programs, these programs can monitor keystrokes, scan files on the hard drive, install other spyware programs, read cookies, and change the default home page on the Web browser. The programs continually relay this information back to the spyware author, who either uses it for advertising or marketing purposes or sells the information to another party.⁹ Organizations whose very existence depends on protecting their valuable intellectual property cannot risk losing this competitive edge to information thieves. And organizations whose investors and clients rely on them to safeguard and protect personal, medical, and financial information, to name just a few, cannot afford to question whether critical information is being accessed by spyware.

Organizations that need to demonstrate compliance with government regulations for information security are especially affected by spyware. These regulations include the Health Insurance Portability and Accountability Act, established to ensure the privacy of patient information; the Sarbanes-Oxley Act, established to ensure that financial statements are resistant to fraud; the Gramm-Leach-Bliley Act, established to safeguard customer information; and even the California Data Privacy Law (California SB 1386), established to protect the confidential information of state residents.

When spyware is part of the corporate computing environment, capturing confidential information or secretly perusing files and applications, regulatory compliance is virtually impossible¹⁰—without the assistance of Websense Enterprise. Even in computing environments that encrypt data, spyware remains a threat to the security of corporate data because its keystroke-logging components capture input before it can be encrypted.¹¹

Example—Queens resident JuJu Jiang admitted to installing a keylogger called Invisible KeyLogger Stealth (IKS) on public computers at 13 Kinko's stores in New York. Using the keylogger, Jiang acquired over 450 banking passwords and usernames from customers who used the public computers. Jiang used the stolen financial information to open new bank accounts and then siphon money from legitimate accounts into the new, fraudulent accounts. Although IKS markets its products to IT administrators and parents, Jiang's exploits illustrate how it and other similar programs can easily be used for illegal purposes.¹²

Increase demands on IT Help Desk staff

Spyware and adware significantly increases the burden of IT Help Desk staff by causing application conflicts, malfunction of legitimate applications, and system instability. Many times, the IT Help Desk staff may have to re-image the desktops/laptops to completely get rid of problems caused by spyware.

*[Spyware] is already responsible for more than 12 percent of all technical support calls in Dell's consumer hardware division, the biggest category of complaints this year. And they are not alone — Microsoft claims half of all computer crashes reported by its customers are caused by spyware and its equivalents. The support calls are costing the company "millions," said Jeffrey Friedberg, Microsoft's director of Windows privacy.*¹³

9 Source: <http://enterprisestorageforum.webopedia.com/TERM/S/spyware.html>

10 Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,92554,00.html>

11 Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,92554,00.html>

12 Source: <http://www.securityfocus.com/news/6447>

13 Source: <http://wired.com/news/print/0,1294,63345,00.html>

Create software conflicts with legitimate programs

When spyware and adware programs send information back to their home servers, they must connect to the Internet. In doing this, spyware can cause unexpected lockups and many other problems in Windows. When these events occur, calls to IT Help Desks increase as employees struggle to understand why their computers are crashing or business applications are running more slowly.

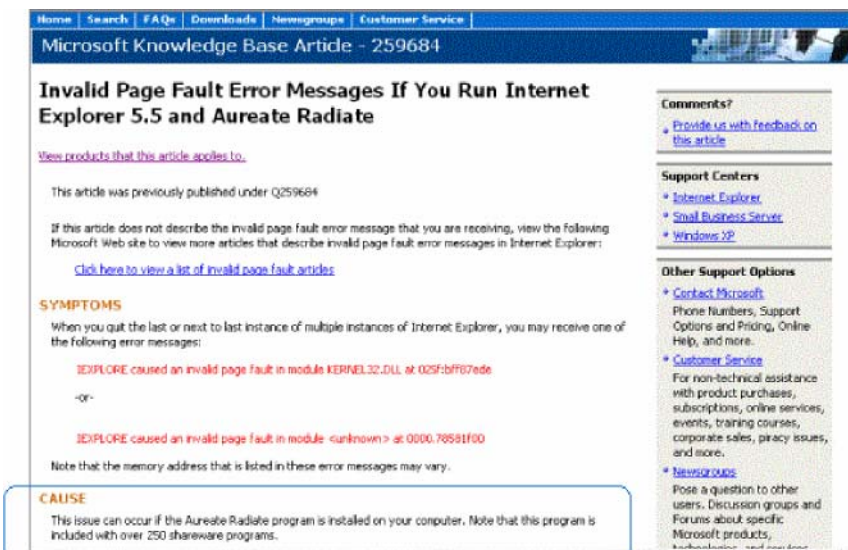


Figure 2. Microsoft Internet Explorer is only one application affected by spyware such as Aureate/Radiate.

Affect the functioning of legitimate programs

Some spyware binds itself to key operating system files and modifies critical registry entries. Attempts to delete these files can limit or even disable the system's Internet connection capabilities.

For example, WebHancer is a spyware program that automatically launches at Windows startup. It monitors Web sites being viewed and sends performance data back to WebHancer's servers. WebHancer has had conflicts with Microsoft IIS, causing problems with ASP scripts. It causes server script ASP pages to stop functioning when the Web application settings are in medium and high isolation modes. WebHancer has modified the computer's Windows Sockets configuration, binding itself to Winsock so that all packets are passed through WebHancer. Deleting WebHancer files may result in loss of ability to connect to the Internet.

Employees who consider themselves sophisticated computer users may try to locate and delete spyware programs themselves, inadvertently creating even greater problems, such as the WebHancer problem described above.

Affect system performance and stability

Since spyware and adware are piggyback programs that run separately from the program they accompany, they use additional processing power, hard drive space, and network bandwidth. Spyware uses computer memory resources and consumes bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware uses memory and system resources, the applications running in the background can lead to system crashes or general system instability. These files also consume a great deal of bandwidth and can create bottlenecks for critical business applications.

Degrade worker productivity

Having to close pop-up advertising windows and reset home pages that have been redirected by spyware is annoying and time consuming. Employee productivity is also affected by slow network performance and system instability. Many times, employees—unaware of the cause of their computer problems—contact the Help Desk frequently for support. This can seriously affect employee productivity and places an increased burden on Help Desk staff.

Why Current Solutions Are Inadequate

Most organizations rely on a combination of a firewall, antivirus solutions, and spyware/adware removal programs to protect their systems from spyware. However, the security weaknesses that expose system applications to spyware often involve vulnerabilities that these applications cannot address, or impose an administrative burden that renders these solutions impractical.

Firewalls

A firewall, which is designed to prevent unauthorized access to or from a private network, is one of the most fundamental security tools for any organization. Although a firewall can effectively enforce a network security policy, a firewall cannot protect against spyware, since the spyware problem originates within the network, in the use of the Internet. Firewalls operate at the *boundary* of the network and thus have no view of what goes on *inside* the network. In addition, many spyware applications use port 80 to transmit information back to their host sites. Firewalls cannot distinguish spyware-related traffic from other harmless HTTP traffic. Traditional firewalls also don't protect users who are outside the network, like telecommuters, business travelers, etc.

Antivirus solutions

Antivirus software is a vital component of an organization's total security strategy, but it cannot protect against spyware. Antivirus software does not typically include spyware signatures, since spyware is not in the same category as viruses. In addition, antivirus software does not prevent the transfer of information back to the spyware host sites.

Spyware removal tools

First generation spyware removal tools are targeted to individual consumers, not to organizations, and do not provide a centrally managed solution. This means that, to implement this solution, IT staff would have to update desktops individually—and continually—each time new species of spyware is identified. In addition, many of these spyware removal tools do not offer the centralized reporting, scalability, or reliability that would enable IT administrators to easily detect spyware, establish and enforce policies across all desktops and laptops. Second generation spyware removal tools may have centralized administration, but still these tools operate on the premise of removing the spyware application, often a risky and sometimes a debilitating proposition.

How Websense Enterprise® Mitigates Spyware Risks

Websense Enterprise provides a layered solution to help organizations address spyware concerns in the most effective manner, by blocking access to spyware Web sites at the gateway level and by preventing spyware applications from launching at the desktop, including the disconnected laptop. The Websense Enterprise platform includes an award-winning database of categorized Web sites, network protocols, and desktop applications that is updated daily. WebCatcher™ and AppCatcher™ allow customers to automatically submit unrecognized Web sites and applications to Websense for categorization and inclusion in the Websense Master Database. These newly categorized Web sites and applications are then quickly distributed to all Websense customers on a daily basis. The Premium Groups™ (PG) family of products—Security PG™, Bandwidth PG™, and Productivity PG™—includes additional categories and supplements the Websense Master Database. With spyware identified and categorized, policies can be set to restrict or deny access to certain categories of Web sites or applications and thus safeguard the organization.

A comprehensive solution to address spyware involves the following components:

- Detect the extent of spyware in the organization
- Prevent and protect employees from accessing sites that distribute spyware
- Prevent spyware from transmitting information back to host spyware servers
- Block the launching of spyware applications
- Block the launching applications carry spyware

Detect the extent of spyware in the organization

The first step in stopping the proliferation of spyware is to determine the extent of its presence in the organization. Websense Enterprise reporting tools help organizations manage spyware in two important ways: by identifying Web sites that distribute spyware and by identifying the specific spyware applications already in the network.

Identify Web sites that distribute spyware. Using Websense Enterprise Explorer, business managers and IT administrators can drill down into historical Internet access data and identify the extent of HTTP traffic that is prone to spyware.



Figure 3. Explorer illustrates the risk of spyware in the organization.

Administrators can also use Websense Enterprise Reporter, a full-featured Internet use reporting engine with predefined and customizable report templates, to view detailed historical Internet access data. And the Websense Enterprise Real-Time Analyzer™ gives IT administrators a real-time view of network activity within the last 24 hours.

Identify spyware in the organization. By referencing spyware application categories identified in the Websense Master Database, organizations can identify spyware that already exists in the organization and prioritize their anti-spyware efforts accordingly.

Websense Enterprise Client Policy Manager™ (CPM) provides several powerful tools to help organizations detect spyware. CPM Reporter is a browser-based reporting tool IT managers can use to produce out-of-the-box application-use and inventory reports that can be automatically scheduled and distributed. Application-use reports by department and category help managers identify and understand the extent of spyware and other security threats facing their organizations.

Websense Enterprise Inventory Manager performs critical desktop inventories that provide categorized views of applications and executables, enabling early threat detection and identification of spyware, employee hacking, P2P, and Instant Messaging (IM) applications. For example, Inventory Manager can identify the number of instances of a particular spyware application in an environment.

Explorer for CPM identifies spyware activity by application, showing explicit application launches, attempts on a given system, and the names of spyware executables.

The screenshot shows a web browser window displaying the Websense Explorer interface. The page title is 'explorer'. The interface includes a navigation menu with 'Home' and 'Help'. Below the menu, there are filters for 'Software Use by:' with 'Risk Class' set to 'Security Risk', 'Category' set to 'Spyware', and 'User' set to 'Cheong'. A 'Hide Names' link is visible. The main content area displays a table with the following data:

Date/Time	User Name	Category	Application	Launch Action	
1	2004-04-15 12:03:23	Cheong	Spyware	WhentUSearch	Block
2	2004-04-15 12:03:24	Cheong	Spyware	Updater Application	Block
3	2004-04-15 12:03:25	Cheong	Spyware	OME Client Application	Block
4	2004-04-15 12:03:30	Cheong	Spyware	Gator Client Application	Block
5	2004-04-15 12:07:03	Cheong	Spyware	Gator Client Application	Block
6	2004-04-15 12:07:25	Cheong	Spyware	OME Client Application	Block
7	2004-04-15 12:07:26	Cheong	Spyware	WhentUSearch	Block
8	2004-04-15 12:07:26	Cheong	Spyware	Updater Application	Block
9	2004-04-15 12:25:42	Cheong	Spyware	Updater Application	Block
10	2004-04-15 12:25:42	Cheong	Spyware	WhentUSearch	Block
11	2004-04-15 12:25:42	Cheong	Spyware	OME Client Application	Block
12	2004-04-15 12:26:43	Cheong	Spyware	Gator Client Application	Block
13	2004-04-16 07:12:54	Cheong	Spyware	Updater Application	Block
14	2004-04-16 07:12:54	Cheong	Spyware	WhentUSearch	Block
15	2004-04-16 07:12:55	Cheong	Spyware	OME Client Application	Block
16	2004-04-16 07:12:59	Cheong	Spyware	Gator Client Application	Block
17	2004-04-16 07:23:21	Cheong	Spyware	WhentUSearch	Block
18	2004-04-16 07:23:21	Cheong	Spyware	OME Client Application	Block

Figure 4. Explorer for CPM identifies spyware applications that are on the network.

Prevent and protect employees from accessing sites that distribute spyware

Organizations can prevent spyware from entering their network by blocking access to Web sites that distribute spyware. The Websense Security PG add-on module enables IT administrators to block employee access to Web sites that allow spyware downloads or downloads of applications that contain spyware. When employees attempt to visit these restricted sites, they receive the message shown in Figure 5.



Figure 5. Security PG prevents employees from accessing sites that have been categorized as spyware Web sites.

Websense actively updates and delivers the newest spyware Web site URLs with the daily download of the Websense Master Database. Thus, organizations can have complete confidence that their entire network is always protected from the threat of spyware. Once the policy of disallowing spyware within the organization is set, it is automatically enforced.

Prevent spyware from transmitting information to host spyware servers

Since organizations must leave port 80 open to accommodate HTTP/Web traffic in and out of the network, spyware applications typically use port 80 to send information to its host server. With Security PG in place, HTTP transmissions aimed at spyware servers—along with the Web sites that deliver spyware, are identified and categorized as such in the Security PG section of the Websense Master Database. These transmissions are then blocked from sending data via back-channel port 80 connections. Once Security PG is implemented, back-channel communications are stopped immediately.

Block the launching of spyware applications

With CPM, organizations can define policies that block the launch of spyware applications right at the desktop. And CPM blocks spyware applications on all computers, even when they are disconnected from the organization's network. This means even remote, disconnected company laptops are protected from spyware infestation, thereby preventing those systems from creating problems when they re-connect to the network.



Figure 6. If a spyware application attempts to launch on an employee's computer, this message is displayed.

Websense regularly updates the Application Database, part of the Websense Master Database, by mining software and download sites for new applications. In addition, Websense AppCatcher™ automatically and anonymously forwards all uncategorized applications to Websense from customer sites for top-priority categorization.

Block the launching of spyware applications that carry spyware

Websense Enterprise allows IT administrators to manage employee access to network applications, such as peer-to-peer (P2P) applications, which can introduce spyware into their environments. Many P2P file-sharing programs contain spyware that tracks individual users' Internet-related activities. For example, when a user downloads and installs the free Kazaa software, additional software from third-party providers, such as Cydoor, Topsearch, and GAIN AdServer, is also installed. The capability to manage access to network applications is available as part of Websense Enterprise at no additional charge.

For more protection, organizations should use CPM to block the launch of spyware-enabling applications right at the desktop, even when computers are disconnected from the organization's network. Even if employees use their laptops remotely to download unauthorized applications, CPM will prevent spyware applications from launching. Instead, employees will receive a message similar to that shown in Figure 7.

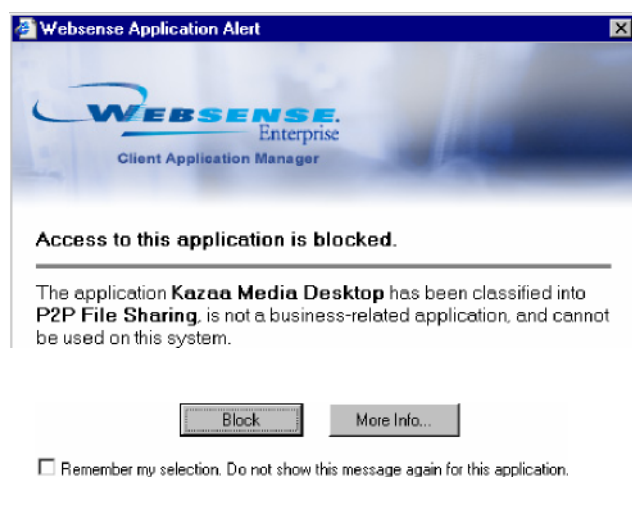


Figure 7. CPM blocks the launch of unauthorized applications on all employee computers, even when they are not connected to the network.

Since spyware can so easily be acquired at certain Web sites, organizations can also use Productivity PG to manage access to Web sites that fall into categories considered to be non-business related, such as advertisements, message boards, and freeware/software download Web sites.

The unique advantages of Websense Enterprise®

Websense Enterprise provides a comprehensive solution for blocking spyware and offers superior benefits and value over all other currently available solutions.

- **Comprehensive and accurate database**—The Websense Master Database, which includes categorized URLs, protocols, and applications, builds on the company's unique strengths in information retrieval and categorization and provides organizations with the most reliable filtering solution available. Developed using a combination of automated and human categorization, the database is

dynamically tuned to real-life surfing patterns with a feedback loop of sites visited and applications launched by employees at customer sites.

Spyware blocking fully integrated with Websense Enterprise—The enhanced Websense solution provides organizations with a multilayered, flexible, policy-based method for managing access to Web sites and applications. Customers use the same Websense Enterprise management console and policy model to block access to spyware Web sites and to spyware applications, with no new interfaces to learn or management consoles to deploy.

Comprehensive solution for threats from employee computing—The Websense product components that address spyware also effectively address other threats, including IM, P2P, and hacking tools, in addition to managing Web site access. Customers may use the same set of management and reporting tools to manage all the threats that result from the convergence of employee computing and the Internet, thereby getting the most from their investment.

Additional, critical point of policy enforcement for spyware protection on mobile laptops—Many organizations want to block spyware on their mobile computing devices, such as laptops when they are disconnected from the network, preventing them from introducing spyware into the network, once reconnected. CPM provides this additional layer of security and policy enforcement for spyware, P2P, IM, and other applications. Without this important additional protection layer, spyware threat mitigation cannot be complete.

Industry-leading integration and flexible deployment—Websense Enterprise integrates with a wide range of leading security and network products, including firewalls, proxy servers, caches, switches, routers, and appliances, providing organizations with flexible options for deployment in their network. The Websense Enterprise solution can be implemented in any of three ways, depending on specific network requirements: in an integrated, embedded, or stand-alone configuration.

Centralized policy management—IT can effectively manage spyware using the central management console, freeing IT staff from the additional administrative burdens of trying to combat spyware on a computer-by-computer basis.

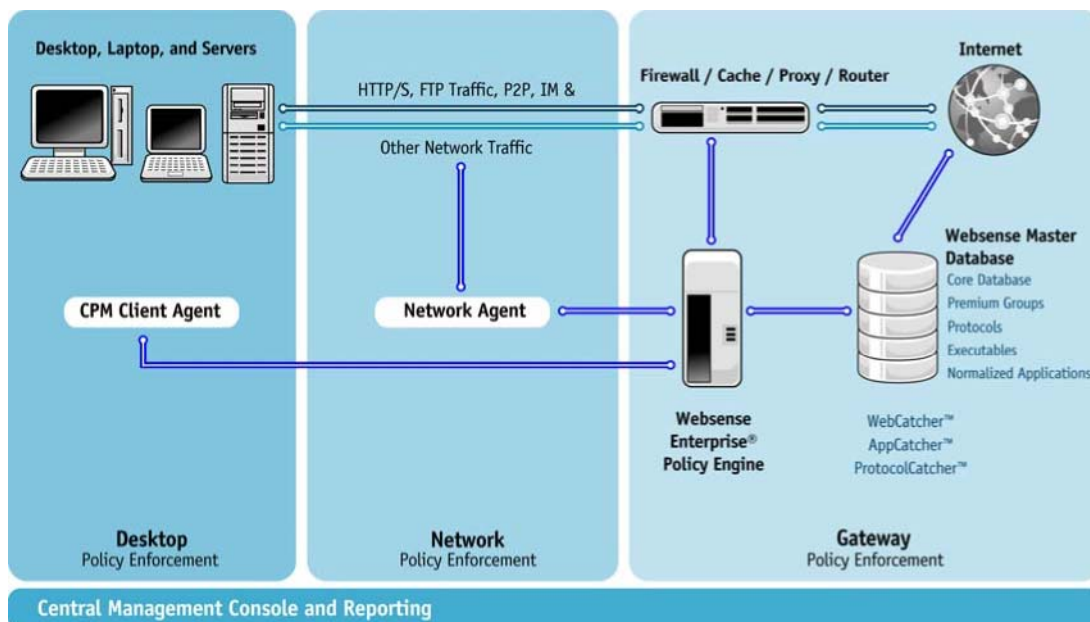


Figure 8. Websense Enterprise provides protection at the gateway, on the network, and at the desktop.

Conclusion

Spyware is a growing concern to organizations interested in safeguarding their own proprietary intellectual property and protecting the personal, medical, and financial information of their clients. In addition to compromising information security, spyware places an increased burden on Help Desk staff, who must respond to employee complaints of unstable and slow system performance. Spyware uses valuable company computing resources (memory and bandwidth) when it transmits information back to the spyware host server and can cause software conflicts with legitimate software programs. It also affects worker productivity. In short, spyware is a serious threat to the organization and must be stopped.

Websense Enterprise presents a comprehensive, multi-layered solution that blocks access to spyware Web sites at the gateway and prevents spyware applications from launching at the desktop. With spyware identified and categorized on an on-going basis, policies can be set and automatically enforced to stop spyware in its tracks.

For more information and to download a free, fully functional 30-day trial, [click here](#)

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), the world's leading provider of employee Internet management solutions, enables organizations to optimize employee use of computing resources and mitigate new threats related to Internet use including IM, P2P, and spyware. By providing policy enforcement at the Internet gateway, on the network, and at the desktop, Websense Enterprise software enhances productivity and security, optimizes the use of IT resources, and mitigates legal liability for our customers. Websense serves more than 21,200 customers worldwide, representing 16.8 million seats. For more information, visit www.websense.com.

© 2004, Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Appendix: The Websense Enterprise® Solution

Websense Enterprise software enables organizations to manage the way employees use corporate computing resources. Organizations of all sizes can optimize the use of the Internet, network protocols, and desktop applications by employees by means of administrative options that define what may be accessed, by whom, at what time of day, and for what length of time. Other administrative management options include warning pages to notify employees that a requested Web site, protocol, or application may fall outside their organization's defined use policy.

The Websense Enterprise platform includes a highly accurate, award-winning database of categorized Web sites, network protocols, and desktop applications that is updated daily. Relying on this database, IT administrators can use the Websense Enterprise central management console to create employee-based policies to effectively:

- Manage employee Internet access.
- Manage IM and IM attachments.
- Control P2P file sharing.
- Manage the use of streaming media and other high-bandwidth applications.
- Block spyware and malicious mobile code.
- Mitigate exposure during zero-day malware attacks.
- Prevent hacking.

Websense Enterprise also provides the most advanced capabilities for detecting productivity issues and security risks arising from employee use of the Internet and computer applications.

Websense Enterprise® Real-Time Analyzer™

A Web-based real-time investigation and analysis tool for IT administrators that enables the analysis of Internet and network activity, including those problematic activities that may be contributing to security risks or slow network performance.

Websense Enterprise® Explorer

A powerful Web-based forensics and analytics tool that provides a highly dynamic interface for analyzing employee use of computing resources. It removes bottlenecks caused by reporting processes that require IT to generate and deliver reports to various departments, supports role-based reporting, and is easy enough for corporate managers to generate reports independent of IT staff.

Websense Enterprise® Reporter

A full-featured reporting engine for IT administrators, with predefined and customizable report templates for viewing detailed, historical Internet-access and application-access data.

Websense Enterprise features the following value-enhancing modules to control P2P applications:

Websense Enterprise® Premium Groups™ (PG)

Extends the URL filtering capabilities of Websense Enterprise by providing enhanced, high-value categories for productivity (Productivity PG™), bandwidth conservation (Bandwidth PG™), and security (Security PG™).

WebSense Enterprise® Client Policy Manager™

Delivers zero-day protection against unknown security threats, including today's sophisticated malware at desktops, laptops, and servers. CPM stops the execution of unauthorized applications such as spyware, P2P file sharing, and hacking tools, while enabling flexible policy management of applications such as instant messaging or remote access tools, which only designated users or groups are allowed to use. Only CPM enforces employee application use policies for corporate desktops, laptops, and servers with its unique and comprehensive database of categorized applications, which is updated daily. Complementing traditional firewall and antivirus tools, CPM closes the window of exposure to today's fast-moving blended security threats.

WebSense Enterprise® IM Attachment Manager™

Extends the IM management capabilities of WebSense Enterprise by enabling organizations to effectively implement policies that oversee IM file attachments. IM Attachment Manager enables network administrators to define custom file attachment policies for any combination of IM client, users, groups, or workstations, using options such as time-based quotas, password authorization, and warn/continue.

WebSense Enterprise® Bandwidth Optimizer™

Adds adaptive policy enforcement to WebSense Enterprise in response to changing real-time network conditions. Bandwidth Optimizer gives organizations the flexibility to permit non-business-critical employee Internet activities until a predefined network bandwidth threshold is reached. When this threshold is reached, activities such as viewing streaming media are temporarily restricted, helping to ensure that ample bandwidth is available for critical business applications. When adequate bandwidth becomes available, employees are automatically allowed to access high-bandwidth applications.

Figure 9 summarizes WebSense Enterprise and its associated modules.

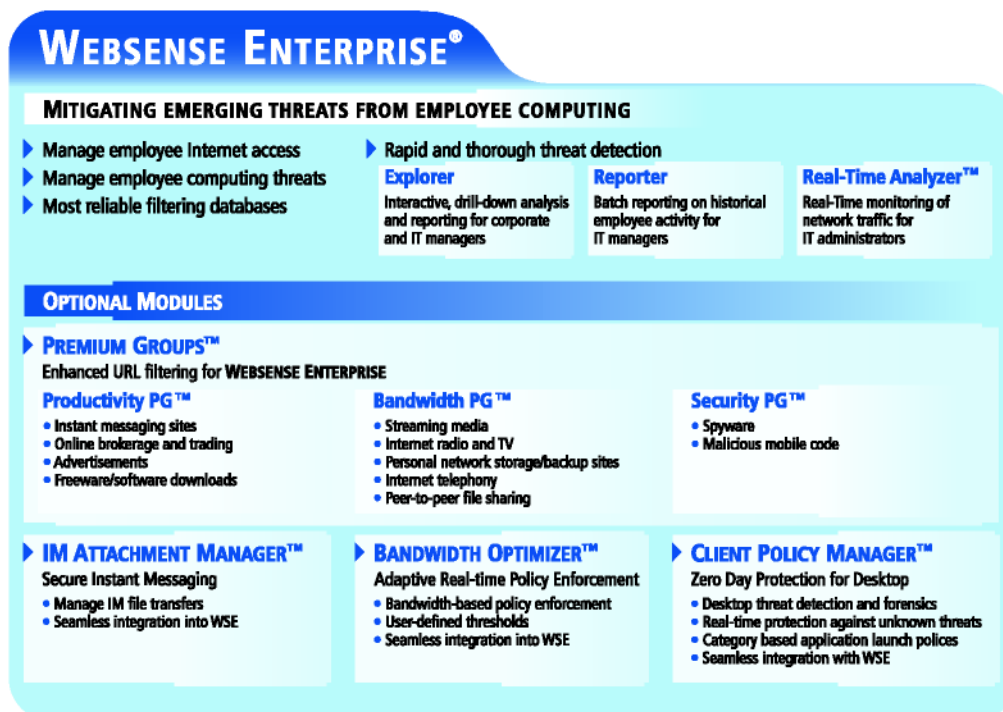


Figure 9. WebSense Enterprise and optional modules