Sunbelt Software

Spyware in the Enterprise:
The Problem and the Solution

CounterSpy Enterprise

Sunbelt Software White Paper

January 2007

Spyware in the Enterprise:
The Problem and the Solution

Executive Summary:

IDC, a top research and advisory company for the IT and telecommunications industries (www.idc.com), recently surveyed over 600 organizations to determine what companies perceived to be the greatest security threats to their organizations, and the results of that survey showed that spyware was listed fourth. According to estimates, well over half of consumer computers are currently infected with some sort of adware and/or spyware.

The spyware problem is already costing individuals and companies millions of dollars in lost time and productivity and money spent to address it, and it's expected to get worse. IDC's report indicated that $12 million USD was spent in 2003 on antispyware solutions, but that number is predicted to increase to more than twenty-five times that (that is, by 260 percent) within the next five years.

There are many antispyware products on the market, but the key component of any spyware removal tool is its ability to detect the spyware programs in the first place. Thus, antispyware software is only as good as its database (and that includes regular updates to that database, since new spyware programs are released on a daily basis). Enterprise level organizations, in particular, need more than a hit-or-miss solution. Large networks can't afford the problems that spyware causes. Because some antispyware solutions detect spyware that others miss, companies often end up using several different products.

What enterprises need is one comprehensive solution that is continually updated to detect and eradicate all known spyware threats as soon as they are discovered. Because one software company cannot possibly keep up with all the spyware programs that are emerging, this requires the formation of a "detection network" for the reporting of new spyware threats.

Table of Contents:

What is Spyware?

Computer users - from home users to those in the enterprise - are plagued today by three major threats to security and productivity: spam (unwanted commercial e-mail), malware (malicious software such as viruses, worms and Trojans), and spyware/adware (software, often installed along with or as part of a program that is knowingly installed, which collects information about the computer, user, or data on the system and surreptitiously sends it to another person or company across the Internet).

Spyware is a growing problem. According to statistics published by Earthlink in mid-2004 (http://www.earthlink.net/spyaudit/press/), computers they scanned averaged 26 instances of spyware per computer. The National Cyber Security Alliance reported in 2003 that up to 90 percent of all computers are infested with some sort of spyware.

Most definitions, such as the one provided by Whatis.com (http://whatis.techtarget.com), define *spyware* as any technology that is used to gather information without the target person's or organization's knowledge or permission. The term is actually used in two different, albeit related, contexts. The more common usage refers to software that contains an advertising component, in that the information it collects is returned to the software vendor to assist in future marketing strategies (adware). The term is also used to identify programs such as key loggers, screen capture utilities and other software that can record what a user does on the computer (what Web sites the user visits, all text the user types in, and so forth) and save it for or send it to someone else.

Spyware in the enterprise environment is a special problem. Performance slowdowns or system crashes caused by spyware on users' machines cost the company money. Even worse, sensitive business data may be at risk. In addition, many industries today operate under government regulations that require protection of certain types of information (for example, HIPAA requires that health care providers protect patient data and the Gramm-Leach-Bliley Act requires that financial institutions protect customers' personal information). Having programs running on your systems that collect unknown amounts of information and send it somewhere else may endanger your company's compliance with these laws and subject it to fines - or worse.

How Spyware Differs from Viruses and other Malicious Code

Although what it does may seem pretty unfriendly, spyware differs from traditional *malware* or malicious code in several ways:

- Traditional malware programs (viruses, worms and Trojans) are usually installed involuntarily. That is, when the user opens an e-mail attachment or visits a Web site, a script or control runs that downloads and installs the malicious program on the user's machine. The user generally has no idea software is being installed. Although "hit and run" installation of spyware is becoming more common, it is more often installed along with or as part of a program that the user intends to install. For example, many freeware toolbar add-ons and similar programs install spyware along with the legitimate program, or the program itself may have a spyware component. Peer-to-peer (P2P) file sharing applications are often bundled with spyware programs.
- Malicious software is usually created with the express intent to cause damage to the infected system or program - to crash the operating system, to slow down the system or cause a Denial of Service (DoS) on the network, to destroy data or program files, and so forth. The purpose of spyware programs is to collect data. If you become infected with a large number of such programs, they may cause your system to slow down, or conflicts with other software may cause odd computer behavior, but that is not the intent of the spyware writers/distributors.
- Viruses and worms often propagate themselves, spreading to other computers over the network by attaching themselves to e-mail messages, file transfer, and so forth. Spyware programs generally do not "spread" in this way, but instead are installed by a conscious act of the user, who installs the program for its other, beneficial features, however, recently hybrids of spyware and viruses/worms have been spotted.

We should note that in many cases, if the user reads the End User License Agreement (EULA) for the programs he or she has installed, notification that the spyware component was being installed will be there along with all of the other fine print. This means that in order to install the software you want, you have to agree to the installation of the spyware. The software vendors would argue that this gives you fair warning of what's being installed. Of course, most users never read the EULA - they simply click "I agree" and proceed with the installation of the software they want.

Despite the differences, there are some ways in which spyware is very similar to malware. One commonality is that both are continuously being modified and new versions are being released on a daily basis. That means that, just as with virus protection, antispyware software becomes outdated quickly unless it is regularly updated. Of course, the primary thing that spyware has in common with malware is that they are both *unwanted* by the user.

In fact, the line between spyware and malware has become more blurred, as some advertising companies have created their own Trojans that install themselves without the user installing another associated program. These can operate in "stealth mode," making them difficult to detect, and can even be written to appear to the operating system like a Windows system process so you can't terminate it.

Regardless of its level of malice, the type of spyware that is used for gathering marketing-focused data is actually a less obvious but more insidious outgrowth of a legitimate type of software called *adware.*

The Evolution of Adware

The term "adware" originally referred to software that is supported by advertising. Selling advertising to be included with the software makes it possible for software authors to distribute their products as "freeware," at no cost to the user. Of course, we all know the truth of the acronym made famous years ago by science fiction writer Robert A. Heinlein: TANSTAAFL, which means "there ain't no such thing as a free lunch" - or a free anything else. Freeware users paid for the software with their time, by viewing the ads that "pop up" or display as banners within the software interface.

Over time, the concept of selling advertising within the software grew into the idea of selling *information* to advertisers, which could be collected by the software. This seems to be less intrusive because the user doesn't have to see the ads and the software author still makes money from the advertising companies, who use the information to target their ads and better understand the audience to whom they want to sell their products. It was the perfect solution - until privacy advocates got wind of what was going on.

Many of the companies that distribute spyware promise that only general anonymous statistical data is collected and no personal information will be gathered or used. They may state this in their privacy policies, and it may even be true. What's the problem, then?

The Problem with Spyware

Users today store all sorts of information on their computers. This includes sensitive business information such as trade secrets, the company's financial data and confidential information about company personnel and customers. It can also include personal information such as bank account numbers, credit card numbers, social security numbers and other information that should not be made public.

When a spyware program is installed on a user's computer, the user has little or no control over what information is sent, nor does the user really have any way of knowing what is done with that information after it leaves his computer. He just has to trust the company not to use it improperly.

Many spyware programs are written so that, if you try to remove them, they can repair themselves. Some distribute their files throughout your hard disk in different locations, to make it harder to find and delete all of their components.

Some spyware turns your business or personal computer into a server that can serve up the data stored on your computer to other computers over the Internet. That idea doesn't set well with many computer users. In today's information-focused world, many people "live" on their computers and having an outsider snoop through their data feels like as much of a violation as having a stranger come in and snoop their homes.

Perhaps the most troubling aspect of spyware is not what it *does* do, but what it *can* do. While one spyware program might only "phone home" occasionally with fairly innocuous information about how many times the user clicked on a particular company's Web site, the same technology can (and perhaps has been) easily extended to send back information on every Web site the user visits, or to scan document files stored on the hard disk, or even to capture usernames and passwords entered into online banking forms.

Finally, intentional or not, spyware often affects system performance. Like any software, spyware uses system resources, and consequently those resources are not available for other, desirable programs.

Are Cookies a Form of Spyware?

Cookies are small bits of information that are downloaded to a user's computer by a Web site. They store such information as your settings or preferences for viewing the site, pages on the site you've visited previously, your name and other information that you might otherwise have to enter in each time you visited the site, and so forth. Cookies may be stored by the Web browser as individual files (Internet Explorer) or all in one file (Netscape, Opera).

They sound good (after all, from earliest childhood we're conditioned to associate the word "cookie" with a treat), but some computer users object to having information about them stored by a Web site, even when the information is stored on their own local computer.

Are cookies spyware? In a sense they are, because you may not know they're being placed on your machine and the information they store about you *is* sent back to the Web site when you visit it again. However, most Web browsers make it easy for you to refuse cookies (although this may cause some Web sites not to function properly, and some sites won't allow you to access them at all if you refuse their cookies).

Whereas most cookies are designed to store information for specific Web sites, some cookies are designed to be shared among many unrelated sites to track users' Web usage and browsing patterns. These "spyware cookies" are not of any use to the user.

While most users realize that some cookies can be useful, they would like to have a way to easily determine what cookies are on their systems, and a way to remove those cookies individually that they don't want stored on their machines. They would also like to have a way to know which cookies are known "spyware cookies."

Spyware as a "Monitoring" Tool

Some spyware products have nothing to do with advertising. They are designed to "spy" on you in the more traditional sense of the word. These programs are used by suspicious spouses, nosey employers, protective parents and others to secretly monitor what another person is doing on the computer.

Ranging from popular low-cost consumer programs to sophisticated proprietary software used in industrial espionage to special "law enforcement only" software used for criminal surveillance by government agencies, this type of spyware can be used to read the target's e-mail, capture screenshots, log instant messaging conversations, track Web surfing habits, view the contents of the hard disk and more.

Such programs can be installed and activated remotely or locally. Thus, unlike with hardware monitoring devices (such as hardware-based keystroke capture devices), the "spy" doesn't need to have physical access to initiate monitoring of a computer.

Spyware Turns Malicious

Some spyware goes beyond annoyance and poses a very real and serious threat to individuals and organizations. The same technology that is used to collect information about Web browsing habits can also be used to collect data such as e-mail addresses, phone numbers, physical addresses, passwords, credit card information and other personal information about individuals. This information can then be used to compile lists for spammers or even to steal the individual's identity and run up fraudulent credit card charges or open new accounts in the person's name.

Sensitive business information, such as financial information, customer lists, internal memos and documents detailing confidential research could also be "collected" by spyware tools and retrieved by competitors, disgruntled ex-employees or others who intend to use it against the company.

In this case, spyware is closely related to the phenomenon of "phishing," which is another method of collecting personal information to use for nefarious purposes. The difference is that phishing usually relies on tricking the victim into disclosing that information by entering it into a Web form that purports to be that of a legitimate business site such as PayPal, eBay or the victim's bank or credit card company. Spyware authors don't have to rely on getting the victim to visit their fraudulent sites; the software does the job for them, grabbing the same information from the victim's hard disk or when it's entered into a legitimate Web form, such as that of the victim's own bank.

This type of spyware is potentially the most dangerous of all, and can cost victim companies and individuals money, time and untold frustration. In some cases, the damage may be irreparable.

Categorizing Spyware

Based on the types of spyware discussed above, spyware can be categorized according to level of intrusiveness and/or use of the information collected. Low threat spyware includes cookies and most adware. "Monitoring" or "surveillance" spyware poses a medium to high threat. Spyware designed to collect information for criminal purposes should be considered a high threat level.

Some specific types of spyware programs include Browser Helper Objects (BHOs), which can scan the Web pages a user visits, report on his browsing habits, and insert "targeted" advertising based on information collected about him. Some BHOs change your browser homepage; these are known as browser hijackers. Another type of software often categorized as spyware is the Remote Access Trojan (RAT), that can allow a hacker to remotely control the user's computer as if sitting at it locally.

The Cost of Adware and Spyware

Adware and spyware may seem to be merely a privacy problem, but in reality, dealing with these threats costs individuals and businesses time and money. The larger the organization, the greater the potential loss when a spyware infestation occurs on the network.

The Cost of Countering Spyware

According to a recent report from IDC, consumers and businesses are expected to spend approximately $305 million on efforts to detect and eliminate spyware. That’s just the cost of implementing antispyware solutions; it does not include the significant costs in decreased network performance, employee time and lost productivity caused by the plethora of spyware programs that infest users’ systems.

The Hidden Costs of Spyware: Time and Productivity

The business truism that "time is money" brings to light the true cost of spyware. In addition to the money a company spends on antispyware solutions, the business also loses valuable "on the clock" employee time when spyware slows users' systems down to a crawl, often necessitating that the system be down for a period of time while IT personnel track down the problem. Then there is the cost of the time spent by the IT staff on finding and deleting the spyware.

How Spyware Threatens Security

By its nature, spyware sends data from infected computers to someone else. Whether that’s a marketing firm that plans to use the information to plan its sales strategies or a malicious hacker who plans to use it to steal identities or trade secrets, it’s a security threat; the question is just how *big* the threat is for a particular type of spyware.

The law generally defines theft as the intentional appropriation or taking of something without the consent of the owner. When a program intentionally takes data from your computer or network without your permission, it is in effect *stealing* your information. A system or network can never be considered secure when the user or network administrator has no control over the programs being installed on it or the information being sent out from it.

The Problem with Adware and Spyware Solutions

When a problem as big as spyware rears its head, there are bound to be many "problem solvers" who rush in with potential solutions. Some of this are well-intended but incomplete, and others can make the problem even worse.

Awareness is Only the First Step

It's important to make users and administrators aware of the symptoms of a spyware infection, and the dangers of installing software (especially free software) that may come with "unexpected guests." CSI (the Consumer Spyware Initiative sponsored by Dell and the Internet Education Foundation) is one of several campaigns that have been launched recently to educate consumers and corporate users about telltale signs of spyware such as strange system behavior, popups, slowdowns, freezeups and shutdowns. But awareness is only the first step. Once the problem is identified, the next step is to do something about it.

User Education is the First Line of Defense

Educating users about spyware will reduce your network's exposure. Users should be taught basic spyware avoidance rules:

- Don't install software unless you know exactly what it is (in the enterprise environment, it is a good idea to make policies prohibiting most users from installing any software without IT approval).
- Don't click on pop-up ads - including clicking "No" or "click here to close." Instead, close the browser to get rid of the dialog box safely without installing anything.
- Don't open spam messages or click on links in spam displayed in the preview window.
- Don't use peer-to-peer (P2P) file sharing programs.
- Ensure that browser security settings do not allow anything to be installed without prompting the user for permission.

Unfortunately, even if all users follow these rules all the time, this will only reduce the chance of spyware getting into your network; it will not eliminate it. Spyware authors and distributors are always coming up with new tricks. User education is important, but enterprise networks require a multi-layered defense plan to protect against spyware.

Why Legislation Won’t Solve the Problem

There are laws in the works at the federal level that would make spyware illegal. The U.S. House of Representatives approved a bill (the Spy Act) in October 2004 that would create a complex set of rules for software that sends information across the Internet and would impose fines of up to $3 million on violators, to be enforced by the Federal Trade Commission. Along with a similar bill that was introduced in the Senate, these are just the latest of several attempts to regulate spyware.

Some states have already enacted antispyware legislation. But just as state and federal laws making it illegal to send unwanted commercial e-mail (spam) haven’t had much luck in stemming the flow of junk mail to users’ mailboxes, we can't expect antispyware laws to be a magical solution. The same problems that make the anti-spam laws hard to enforce -- jurisdictional issues, the difficulty of tracking down spyware perpetrators, lack of government resources to devote to enforcement -- are likely to prevail. Strong laws help, but legislation alone won't stop the flood of spyware.

Spyware is very much a technological problem, and as such, it begs for a technological solution.

Why Anti-virus Software isn't the Answer

One example of using technology to fight against unwanted software is the anti-virus industry. A good anti-virus program is absolutely essential for any computer that connects, directly or indirectly, to the Internet (and recommended even for computers that don't). But some users and network administrators make the mistake of thinking AV software will protect their machines from spyware. Unfortunately, most AV software is not effective against spyware. This shouldn't come as a surprise, since anti-virus programs are designed to protect against viruses, and spyware, which doesn't share the propagation characteristics of viruses, is less likely to be detected by traditional AV methods.

Why Your Firewall Won't Protect you from Spyware

Like AV protection, a firewall is a "must" to protect your internal network from external threats. However, spyware is one threat that a firewall may have trouble defending against. After all, it often "sneaks in" as part of desired software, and it is impossible for the firewall to separate the spyware component from the legitimate download.

Many firewalls are configured primarily to control inbound traffic, and so they don't address the spyware programs' outbound traffic. And all spyware doesn't conveniently use a common port that can be blocked to stop it.

Why You Should Beware of "Freeware" Spyware Removal Tools

There are many spyware detection and removal tools on the market. Some of these are offered as "freeware," but it's best to be cautious when trying out these supposedly no-cost solutions. Some may work as advertised. Some may be poorly written and/or poorly documented, and could result in inadvertent conflicts with other software or system crashes. They may not have been thoroughly tested for bugs. Most offer no support; you're on your own when it comes to getting the free tools to work.

Even worse, some malicious programmers take advantage of the spyware scare to distribute programs that are purportedly spyware removal tools, but which are actually themselves spyware or other malware. This is a common scam. Some of these tools actually *do* remove other spyware programs, only to install their own spyware.

Examining Antispyware Technologies

There are two elements to any antispyware product:

- The ability to detect which programs are spyware
- The ability to remove all of the components of detected spyware programs

Detection of spyware can be difficult because spyware comes in many different varieties and new spyware programs (or old ones with modifications) are constantly appearing. In order to identify spyware programs, antispyware software must have access to a constantly updated database that contains the definition or signature files for known spyware programs. The effectiveness of any antispyware solution in detecting spyware is only as good as its database.

Once spyware has been identified, all of its components must be removed. This can be more difficult than removing viruses and other types of malware because of the way spyware often distributes its files across the disk, disguises them, incorporates its code into files that are also used by legitimate, associated software, and even reinstalls itself when it is deleted.

Enterprise Network Requirements

Spyware removal solutions for an enterprise network require that administrators have a high level of control over the antispyware software. Protecting the enterprise is more complex than protecting a home computer, because it requires centralized control over multiple machines that may be running many different operating systems. An enterprise environment also includes many different users who have different levels of access, expertise and exposure.

The best solutions for the enterprise allow *policy-based* protection. This allows you to create different policies that are appropriate for particular machines or users. Policies can be quickly applied, enabled or disabled as desired. Policies allow scheduling of scans and make it possible for you to allow or disallow specific threats.

Enterprise administrators also need *information* about the activities of antispyware software on their networks. They need a mechanism for notification when threats are detected or actions are taken. They also need a comprehensive reporting system that will make it easy to provide documentation for their own use and for keeping management informed and justifying budget expenditures.

The CounterSpy Solution

CounterSpy Enterprise is a business-class spyware detection and removal solution offered by Sunbelt Software. It is built on the same excellent spyware database as their CounterSpy consumer edition, but provides the centralized management, control, notification and reporting features that enterprise networks need.

CounterSpy combines a unique philosophy with the power of "grassroots" collaboration to maintain the most up-to-date spyware definitions possible.

The CounterSpy Philosophy and ThreatNet™

The concept of a "counterspy" is that of using the tactics of the enemy against that enemy. By "spying on the spyware," that is, putting into place a vast network of "counterspies" that report back about newly discovered spyware *before* it can become widespread, Sunbelt has created a way to fight fire with fire and stay a step ahead of the spyware threat.

ThreatNet extends across the globe, incorporating users of CounterSpy as its agents. Information on new threats is anonymously transmitted to the research center, where updates for the software can quickly be created and distributed to all CounterSpy users. This information is secure because it only includes the threat signatures; it does not include any identifying information about the user or the source computer. The client software uses the standard HTTP port 80 to communicate with the SFN servers. Updates are distributed via a subscription service, and updates are not aggregated and saved for a particular update time or date; they are distributed as soon as they are available, so there's no waiting for the protection against the latest threats.

How CounterSpy Enterprise Works

CounterSpy Enterprise consists of three components:

- The server component, which provides centralized deployment and management.
- The administrative console, which can be installed on the administrator's workstation for remote management of the server component.
- The agent software, which is installed on the network computers that will be scanned.

The CounterSpy server component is installed on a machine running Windows Server 2003, XP Pro, Windows 2000 Server with SP3, or Windows 2000 Pro with SP2. You can also install the administrative console on a machine running any of these operating systems. You also need to have the .NET framework v.1.1 and Internet Explorer v.5 or above installed.

The agent software can also be installed on XP Pro or Home, Windows 2000 Pro with SP2, NT 4 Workstation with SP6, Windows Me, Or Windows 98/98SE. Hardware requirements are minimal: a Pentium 200 or above with at least 96 MB of RAM. The .NET framework is not required on the client.

To open the CounterSpy administrative console on the server machine or on another machine, you must log on with the server name and port number (18083 if you accepted the defaults), domain/username and password. The agents can be managed from the administrative console, and their databases and software can be automatically updated when updates become available. You can view and manage the installed agents by name or IP address, and see their status, time of last scan, software and threat database versions, what policies are assigned, quarantined items and a scan history.

Policy Based Deployment

CounterSpy Enterprise has sophisticated policy creation and management functionality that gives you the flexibility to control scheduling of both quick scans and deep scans, set scan options (including scanning of known locations, whether to scan cookies, whether to scan running processes), and allow specific threats from the database. Through policies, you can configure e-mail notification based on the severity of the threat (so that you don't have to be bothered with notifications of less critical threats).

Your policies can specify updating of the agent threat databases and agent software, and you can customize a message advising when the agent machines need to be rebooted after removal of threats. You can also choose an action to take when a particular threat is found. The default is to quarantine all threats. You can then view the quarantined threats and choose whether to remove them or unquarantine them.

Installing and Configuring CounterSpy

Installation of CounterSpy Enterprise is straightforward and fast. One installs the product on a supported machine by downloading the executable and double clicking to begin the installation. After you accept the license agreement, the Setup Wizard, asks you to select either a setup type:

- Complete setup, which installs all features and requires about 233 MB of disk space
- Admin Console only, which allows you to install the administrative console interface on a workstation that you can use to administer CounterSpy Enterprise remotely

You can install the program to be used by all users, or only by the account with which you're logged on for the installation. You'll be asked to provide a serial number along with a name and organization name.

The next page of the Setup Wizard may be a little confusing. You're asked to provide port numbers for the following:

- Policy
- Reporting
- Update Service
- Agent

There are default ports provided (18083 through 18086) and generally you can accept these. You can accept or change the default installation location in the c:\Program Files folder. Then the installation begins.

The software installs three services: the policy service, reporting service and update service. These all start automatically and run under the local system account. The interface is comprehensive. Instead of hiding everything in menus, you'll see four category lists in the left pane:

- System: includes registration, updates and configuration tasks.
- Policies: contains the default policy and any policies you have created.
- Manage: lets you view and manage agents, quarantine and threats.
- Report: you can quickly generate and view reports.

For even faster access to common tasks, you'll see icons across the top of the interface. The Connect icon brings up the CounterSpy logon screen to allow you to connect to a server. You can save your current settings with one click of the Save Settings icon. The Add Policy icon lets you create a new policy. There are also icons to view quarantine, agents, threats and reports. The Research Center icon takes you to http://research.sunbelt-software.com.

Administrators can easily configure how often the software should check for updates to the agent components and the threat database. You can set an update schedule ranging from hourly to every twelve hours, or never. You can also run a manual check for updates at any time.

It is also easy to view the threat database, with entries categorized as adware, "low risk" adware, adware bundler, AOL exploit, backdoor, browser hijacker, browser plug-in, commercial key logger, commercial remote control, cookie, dialer, e-mail flooder, enabler, hostile ActiveX control, ICQ exploit, joke program, consumer key logger, loader, nuker, password hijacker, potential privacy risk, remote access Trojan (RAT), search hijacker, security disabler, spyware, stealth notifier, surveillance tool, toolbar, regular Trojan, Trojan downloader, Trojan FTP, Trojan telnet, updater, worm or a miscellaneous threat. The database also includes information on the author and the URL where the threat is downloaded (if applicable).

The easy-to-use report generator is especially helpful. You can specify the time period the report is to cover and you can easily print the report or export it to a file (saved as a Crystal Reports .rpt file, an Adobe Acrobat .pdf, a Microsoft Excel .xls file, a Microsoft Word .doc file, or a rich text .rft file). Reports include an executive summary, summary of infected machines, details on infected machines, machine history, details of threats found, summary of threats found, and the top 10 infected machines. There is also a handy search feature for finding keywords within the text of a report.

Summary

Spyware is a serious threat to the enterprise network, and the threat is growing. Awareness campaigns and user education are useful, but they're not enough. Legislation may deter some spyware distributors, but many more (overseas-based) will continue to create and release programs that threaten your network's security and your users' and organization's privacy. Anti-virus software is not designed to deal with the unique characteristics of spyware, and firewalls cannot discern what is and is not spyware.

There are many "free" spyware removal tools on the market, but some of these are ineffective (or only partially effective), some are poorly written and untested and may cause conflicts and system crashes, and others are actually spyware or other malware disguised as antispyware programs.

The needs of an enterprise network are different and more complex than those of the home or small business computer user. Enterprise administrators require a way to manage spyware detection and removal for a large number of computers from a centralized location, and they need a solution that relies on the most updated threat database possible, because spyware can cost a large company hundreds, thousands or even millions of dollars in downtime, administrative overhead and lost productivity.

CounterSpy Enterprise provides a cost-effective technological solution to the spyware problem that is easy to use but sophisticated enough to address the needs of the largest enterprise. ThreatNet is a unique mechanism for the reporting of new threats and updating of the database before those threats can become widespread. The fact that Microsoft will update Sunbelt with their threat definitions assures the CounterSpy database us up-to-date. Policy-based deployment and administration and a server-agent software module make it easy to protect all of your machines, regardless of operating system or location.

For more information about CounterSpy Enterprise, visit:
http://www.sunbelt-software.com/CounterSpyEnterprise.cfm