



Simply better network security.™

C O N T E N T

Executive Summary

The Spyware Threat

Business Requirements

Gateway Anti-Spyware

Desktop Anti-Spyware

Complete Protection

www.esoft.com

▣ **White Paper: Spyware Security and Privacy Protection**

Executive Summary

Corporate IT Managers are seeking refuge from the onslaught of Spyware causing network drains, slow desktop responsiveness and the critical security threats caused by this hard-to-prevent threat. Spyware has moved beyond the casual home user's computer and into the corporate network, but IT managers do not have adequate tools to stop it.

A multilayered approach is necessary to protect against the fastest growing threat on the Internet, Spyware. Spyware threats are growing at twice the rate and already more complex than advanced Virus threats. The first step is to deploy an Anti-Spyware gateway to prevent the entire network from the download of new Spyware and stop infected clients from sending information out of the network. Next, host protection must be installed to clean Spyware from computer programs, registries, and memory. Companies with more than a few employees will need centralized management tools to install and manage the host protection throughout the network without visiting every PC. Corporations must implement a layered approach much like they have with anti-Virus if they intend to protect against the privacy and security risks associated with Spyware.

eSoft's Anti-Spyware solution includes both gateway and client elements in a solution designed to provide complete protection from these threats. The gateway stops known Spyware from being downloaded to desktops and servers. It also stops pre-infected clients from sending private information outside the network without the user's consent. Client protection removes Spyware from infected servers, desktops and laptops. The client installation will also stop infections that come from inside the network such as USB storage, floppies, and other infected clients. Today's mobile workforce also requires protection for laptops and other computers that are taken outside the network. When implemented together, eSoft offers the most comprehensive Anti-Spyware solution available.

The Spyware Threat

Infection rates are estimated to be as high as 90% of computers with broadband Internet access (US National Cyber Security Alliance). IT help desks are flooded with calls about annoying pop-ups, slow responsiveness, computer crashes and bandwidth concerns. News accounts and magazines warn about potential losses associated with Spyware. Managers are frantically seeking ways to effectively clean infected machines and stop new infections on the entire network in order to prevent information loss that could prove catastrophic to the entire company.

The lack of agreement on what classifies as Spyware has translated into a similar uncertainty on what it means to protect against Spyware. Gateway protection against Spyware requires more than just anti-Virus with a handful of signatures to detect the most intrusive of Spyware. It also requires more than just blocking URLs of popular havens or sites known to distribute Spyware. It is more than blocking all active content in web pages, eliminating access to other applications where Spyware is common, or intrusion detection for clients that have already been infected. Complete gateway protection stops Spyware by combining all of these security technologies in a single, intelligent system to detect and stop Spyware before it enters the network.

There are several definitions as to what constitutes Spyware. Some forms of Spyware known as Adware are not malicious in their intent, but may still be defined as Spyware. Malicious versions of Spyware collect and send information about user behaviors to third-party collection servers often without their knowledge or consent. Some of the most common forms of collecting this information is done by:

Adware and Tracking Cookies

Targeted or indiscriminate pop-ups and banners, primarily just annoying but often installs cookies that monitor and track browser activity.



Browser Redirector/Hijacker

Resets browsers current page or launch page, often to a page where the third-party can target ads or win business.

Hostile Scripts and Dialers

Scripts and programs that access local computer files to gather information about the user or make toll calls without the user's knowledge.

Keystroke Loggers

Records keystrokes such as web pages that prompt for a username and password, generally sending results to an Internet-based collection server.

Trojans, Backdoors and Downloaders

Software installed on a host computer that can give access to someone on the outside.

Spyware is difficult to detect and remove. Methods including deceptive marketing, intrusive active content, Viruses, and Trojans are used to distribute Spyware and evade detection. Spyware development is often driven by marketing companies with deep pockets that result from gathering information about Internet users. The high dollars attract talent and questionable methods for gathering information.

The software that collects and sends this information to third parties is often installed in deceiving ways. Spyware installs on unsuspecting user's computers through embedded installs, drive-by installs, browser exploits, and email attachments.

Embedded Installs

Embedded Installs package various Spyware packages in "free" programs that are downloaded from the Internet. The owner of the software installs Spyware in exchange for the free use of their program. One of the oldest and well known Spyware programs is

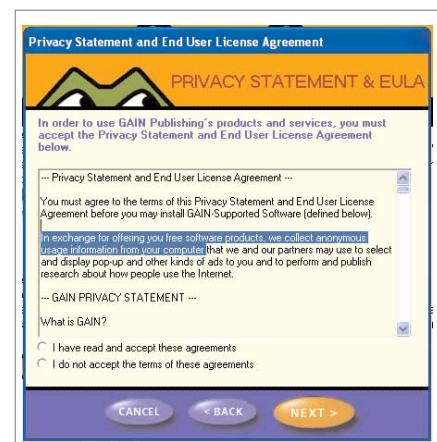


Figure 2: Embedded Install Example

Gator or GAIN. Gator is still installed with many free programs distributed on the Internet. Some of the most common include their own eWallet and Dashbar as well as most peer-to-peer applications. Every website address that is visited while the user is online is sent back to collection servers. The data is analyzed and Gator targets the user with pop-ups and advertisements based on past website visits and ads that are clicked on.

The figure to the right shows an example of an embedded install. During the install process the author commonly asks for user's authorization in an end user license agreement (EULA) to install additional programs or gather information about application or computer use.

Drive-by Installs

Drive-by Installs start downloading software as soon as a web page is visited. The web site displays and sometimes disguises the installation with a pop-up box that looks common to a computer user and may even install the software if the user clicks on the "No" or "Cancel" button. Depending on the browser settings for the computer, the software could be downloaded before the user is even prompted. The figure below represents an Active X component that is attempting to install software on to the computer.



Figure 3: Drive-by Install Example

Some recent Spyware variants are able to install software on the computer when a web site is visited without any user consent. Once such example is the Vloading Spyware; Vloading can infect a machine as soon as an infected website is visited. It then downloads and executes a program without any user consent.

Browser Exploits

Browser Exploits are the last method of infection. They infect computers that are vulnerable because they are not updated with the latest security patches. Similar to modern, unprompted drive-by installs, browser exploits push Trojan software on computers that will download and install more versions of Spyware and Malware without the user's consent. One such example is the Dumaru Trojan. When a version of Internet Explorer without recent security patches would connect to infected sites Dumaru would install itself on that computer. Once installed Dumaru would block access to common security sites preventing future updates that might detect it. The Trojan would then install a keylogger that could read information that was typed by the user including auto-complete text in the browser. There are documented cases where Dumaru was used to steal numerous credit card numbers from unsuspecting consumers.

Companies with Spyware infections have the risk of privacy invasion and theft resulting in loss of credentials or intellectual property, fraud, and even lawsuits. IT departments are faced with application errors, slow computer operations, bandwidth concerns, and increased help desk calls. Users with infected desktops have reduced productivity and frustrations.

Business Requirements

First generation Spyware removal tools were created to help the consumer detect and remove Spyware from their home computer. As Spyware becomes a problem in the business environment the first generation tools lack the sophistication and tools necessary to manage multiple computers. IT managers require centrally managed networks in order to meet the requirements of each demanding day.

Layered Protection

Anti-Spyware solutions must offer a layered approach to effectively protect today's corporate environments. It is essential that gateway solutions provide a multi-faceted approach to detecting and stopping Spyware from entering the network. Intrusion prevention, Anti-Virus/Spyware signature matching and URL filtering are all necessary at the gateway. Client software must be used to protect servers, desktops and laptops from internal threats. In a corporate environment, the client software should be centrally managed and prevent external threats for off-line clients that leave the network. Anything less will leave a corporate network at the risk of privacy invasion and security vulnerabilities.

Anti-Spyware vendors seldom offer a multilayered approach to protect against the fastest growing threat on the Internet. Anti-Virus protection has evolved into a client and gateway solution necessary for today's corporate environments. Spyware threats are growing at a tremendous rate and already more complex than advanced Virus threats. Corporations must implement a layered approach much like they have with anti-Virus to protect against the privacy and security risks associated with Spyware.

Gateway Anti-Spyware

Businesses first need to integrate a gateway solution to immediately stop new Spyware threats from entering their network and stop infected clients from sending private information outside the network. The most effective method for alleviating Spyware concerns is to stop the Spyware before it reaches the desktop. This must be performed at the Internet gateway. Gateway solutions need to have several levels of protection to combat the evolving threats common in Spyware. It must be effective at stopping Spyware, but at the same time the solution cannot affect business communications, timeliness, or productivity.

Intrusion Prevention

Deep Packet Inspection (DPI) is the new technology that is required to prevent against modern security threats. DPI allows the firewall or security appliance to look deep into the packet beyond the header information unlike traditional firewalls. DPI relies on regular updates to identify and thwart dangerous malware. These updates provide signatures or anomalies to compare against Internet traffic. Intrusion prevention is the core technology of DPI to inspect application-level threats.

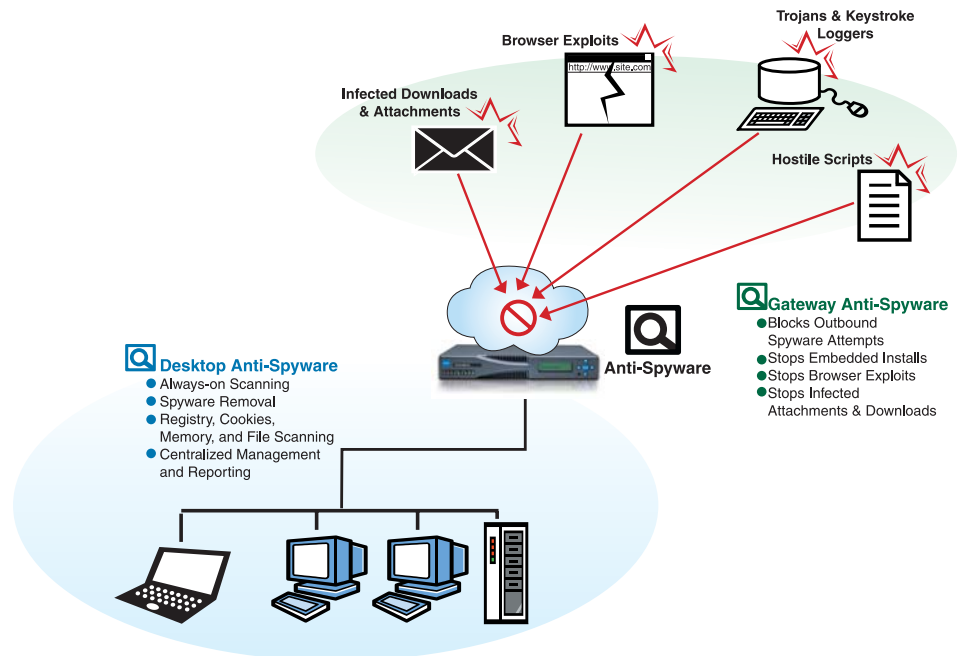
Signature Matching

Some Spyware can be detected using known signatures similar to viruses. Anti-Virus vendors are starting to match a small subset of signatures that include the most common and malicious Spyware. A comprehensive Anti-Spyware signature database will also contain a wide array of signatures to detect and block all types of Spyware including Adware.

URL Filtering

Vendors with Web Filtering techniques have introduced categories to block types of sites that commonly carry Spyware. URL filtering can be used to block categories of sites that are commonly infected or to block specific sites known to distribute Spyware. Filtering outbound web connections is also vital in preventing information being sent to third-party collection servers by infected clients.

This, like Intrusion Prevention and signature matching, is one piece of the total solution. Spyware can infect files on sites that are not categorized or sites that belong to a category that is not generally associated with Spyware distributions. Spyware distributors are often deceptive and can register many temporary domains and move their programs to different locations.



Desktop Anti-Spyware

An effective approach will use a variety of methods to keep up with the rapid evolution of the threats. The methodologies must also account for "off-line" connections that come from laptops and storage devices that leave the network and return infected.

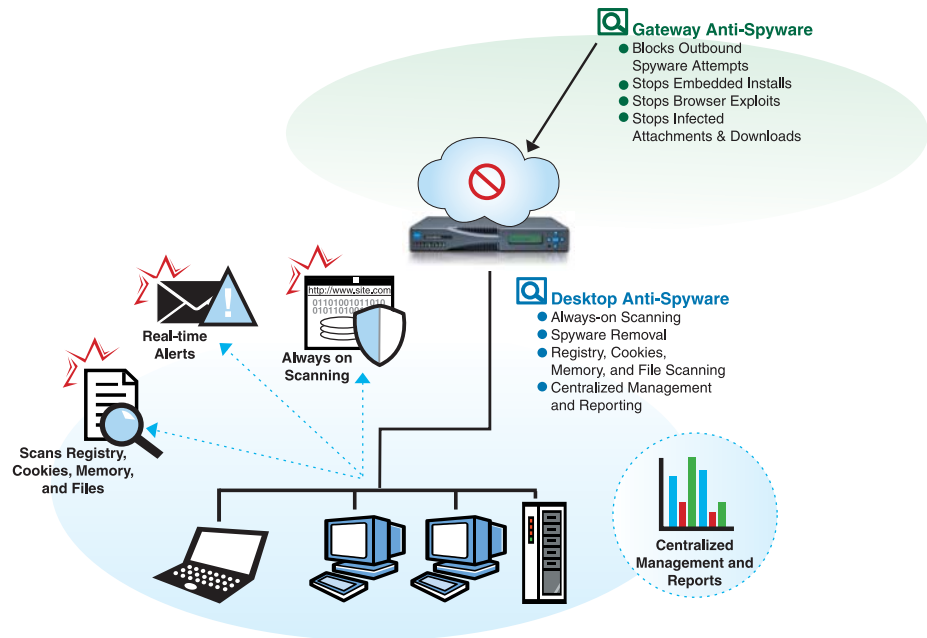
Client protection removes Spyware from infected servers, desktops and laptops by examining memory, system registries, cookies, and program files. The client installation will also stop infections that come from inside the network such as USB storage, floppies, and other infected clients. Today's mobile workforce also requires protection for laptops and other computers that are taken outside the network.

Centralized Management

Network administrators should have complete control over deployment and management of Desktop Anti-Spyware client installations from a central location. A busy administrator does not have the time to individually visit each PC on the network to respond to threats. Policy controls should give the administrator flexibility to make the installation and administration of the Anti-Spyware client completely transparent to the user as well as prevent tampering or disabling of the client software. The centralized management console should offer secure centralized installation and administration, robust and versatile analysis and alert tools, and superior Spyware scan and prevention technology.

On-Access Protection

Corporate Anti-Spyware technology should stop Spyware BEFORE installation, with kernel-level protection. Reactive solutions, like spybot and Adware, that detect applications after they are installed are not adequate to protect against severe Spyware threats that could send corporate information to Internet collection servers or allow complete control of a user's computer within a few minutes of infection.



Complete Protection

eSoft Complete Anti-Spyware solution consists of both Desktop and Gateway elements, which are crucial for providing effective protection against complicated Spyware threats. eSoft is the industry's first comprehensive Spyware solution to include both multi-protocol Desktop and Gateway elements working in unison for thorough Spyware eradication.



eSoft Gateway Anti-Spyware

eSoft Gateway Anti-Spyware is an advanced multi-protocol Spyware detection system, providing protection from inbound as well as outbound threats, such as a keystroke loggers attempting to send data to a criminal collection server on the Internet. The SoftPak relies on deep packet inspection (DPI) technologies such as intrusion prevention, Anti-Virus signature matching and web content filtering, and is updated with real-time intelligence from eSoft's patented SoftPak Director™ threat prevention infrastructure. The result is an effective front-line deterrent for Spyware, regardless of where it originates.

eSoft Desktop Anti-Spyware

eSoft Desktop Anti-Spyware is a mandatory element of total Spyware eradication, providing not only always-on proactive scanning for threats at the kernel level, but also dynamically monitoring system registries, memory, storage and cookies for signs of Spyware presence. When Spyware is detected, eSoft Desktop Anti-Spyware removes and repairs the infected part of the system, an activity almost completely transparent to the user. eSoft Desktop Anti-Spyware is also centrally managed, so IT managers can more effectively enforce client updates and see real-time graphical statistics and detailed reports of the entire Anti-Spyware deployment, rather than just single devices.

Complete Anti-Spyware is deployed on an InstaGate Firewall/VPN device or on a ThreatWall appliance to complement an existing firewall. These award winning appliances offer unparalleled protection from today's dynamic, content based threats that elude traditional firewall technologies.

InstaGate Integrated Security Gateway

The InstaGate line of provides state-of-the art Firewall and IPSec VPN functionality. In addition to Anti-Spyware, the InstaGate offers other content security services such as Anti-Virus, Intrusion Prevention, and Anti-Spam. For the IT manager who wants full integration, many of the InstaGate products can be configured with optional office server elements such as an Internet web server, Email server, Webmail server and File/FTP and Print servers. InstaGate gateways currently integrate more Deep Packet security services than any other vendor on the market.

The ThreatWall is an award-winning platform that performs ultra-high-performance Deep Packet Inspection services. In addition to Anti-Spyware, the ThreatWall can also perform other Deep Packet Inspection services such as Anti-Virus, Anti-Spam and Web URL Filtering as well as Intrusion Prevention. ThreatWall is tailored for networks with an existing Firewall/VPN system, and can be deployed either in-line in Transparent mode, or in an off-line proxy mode, making it exceptionally versatile for diverse network environments. The ThreatWall scans in both inbound and outbound traffic, eliminating the necessity for different devices to be dedicated to inbound and outbound traffic (which many manufacturers require).

