

Spyware Matrix				
	WebSense	Microsoft	Apreo Spyware Solution (SurfControl Acquisition)	LavaSoft (Ad-Aware)
Target Market	Enterprise	Consumer: Home-user	Education	Consumer/ SMB
Global Distribution	Global	Global	Global	Global
Own vs. Acquired Technology	Own	Acquired-Giant Software	Acquired	Own
Product Launch/ Availability	Security PG was launched in 2002; CPM was launched in 2004; Web Security Suite was launched in 2005	Windows AntiSpyware BETA software is available now. Microsoft Enterprise AntiSpyware version will be available 2H05.	SurfControl announced the purchase of Apreo's anti-spyware technology on March 3, 2005. SurfControl has projected a fiscal Q4 2005 launch (April-June) of its SurfControl Enterprise Threat Shield (SETS) product.	LavaSoft launched Ad-Aware in 1999
Deployment	WebSense Security products have been deployed in approximately 13,000 organizations worldwide. There are several offerings which feature security from spyware including: Security PG, WebSense Web Security Suite, WebSense Web Security Suite-Lockdown Edition, and CPM.	The Microsoft AntiSpyware Enterprise product is projected to be launched calendar Q42005	SETS (SurfControl/Apreo product) is to be launched between April-June 2005 as a result there is no data on customer deployment. SETS will be sold as a separate product, not a part of SurfControl's base offering.	LavaSoft distributes its anti-spyware application Ad-Aware to over 80 million home and corporate users worldwide including 3000 partners in over 120 countries
How Spyware is addressed - Network	<ol style="list-style-type: none"> 1) Blocks sites that disseminate spyware 2) Blocks websites such as P2P and IM 3) Blocks network protocols other than IM and P2P 4) For the identification of spyware sites, WebSense uses WebCatcher, which anonymously uploads an XML-encoded list of uncategorized URLs to the WebSense Database Factory. These lists of URLs are merged, sorted and processed into an Oracle database. The web pages are then retrieved and analyzed by WebSense's automated, proprietary web classification system. Once classified, they are added to the WebSense Master Database. 5) After identifying the spyware site, WebSense then reverse engineers the spyware site to see where it posts to, allowing WebSense to block backchannel communications based on the port and URLs. 	Microsoft does not address the network, rather only provides a desktop solution. This is a consumer anti-spyware product not meant for the enterprise.	<ol style="list-style-type: none"> 1) The Apreo product does not provide protection from backchannel communication and does not have any network protection from spyware. 2) The Apreo product stops only a limited number of spyware applications from launching on customers' desktops. The Apreo Spyware category only blocked 2 out of 20 high profile spyware applications. 3)The product did not block MSN messenger. It also did not block any P2P file sharing applications, which allow spyware to come into the network and launch on the desktop. 	<ol style="list-style-type: none"> 1) Does not prevent access to sites containing spyware 2) Does not block backchannel communications

How is spyware addressed? - Desktop	Websense scans the files, through a 2200+ spyware application database. This database provides automatic updates, a white list, custom block lists, employee pop-up notification, and scheduled scans/inventory. It can also run automatically on reboot and has the capability to automatically scan (central administration). In addition, Websense prevents access to sites containing spyware applications, both known and unknown threats, and it blocks the execution of applications and back channel communications to their host sites.	Windows AntiSpyware (Beta) displays detailed information about every spyware program detected, including a description of the threat, where it is located on the computer, a risk rating, and a recommended action to take. Detected spyware can be either temporarily disabled using Spyware Quarantine or permanently removed from the computer.	Apreo provides a customizable database of 21,000 signatures, delivered with a separate spyware category. This product does not provide custom block lists or scheduled scan/inventory capabilities. The Apreo database is only updated on a monthly basis. This is done through human process only and then disseminated through the use of a central management console. This leaves customers vulnerable for as long as a 30-day period, if a new spyware application were to surface.	LavaSoft Ad-Aware scans files, registry, startup areas, memory, local drives, and remote drives for spyware through a 21,200+ spyware application database. This database provides automatic updates, a white list, and scheduled scans/inventory. It can also run automatically on reboot and has the capability to automatically scan (central administration) and manually scan by the administrator. In addition, LavaSoft prevents launching of spyware applications, provides real-time blocking of keyloggers and removal of cookies.
Pricing	Refer to price list	Free	SETS (SurfControl/Apreo product) pricing is unknown at this time.	\$39.95
Prevents access to sites containing spyware	Websense stops access to spyware websites. Websense provides an extremely accurate database, supports 50+ languages, 8.5+ million URL sites, and 700,000+ applications covering 90+ categories. Websense uses a variety of automated site-mining processes to find new websites and applications including WebCatcher, a proprietary tool that captures the uncategorized URLs visited by users at customer sites and returns them for priority handling, and the similar AppCatcher. AppCatcher automatically and anonymously forwards to Websense Master Database any known and unknown applications and its network behavior at customer sites so that policies stay current. Automated classification software helps sort other new websites before they are examined by the Web Analyst staff for categorization.	Microsoft stops access to known spyware on a consumer computer using SpyNet. SpyNet is a voluntary worldwide community of Windows AntiSpyware users that determine which suspicious programs are classified as spyware. Any user can choose to join SpyNet and report potential spyware to Microsoft. Signatures are created for programs that are identified as spyware and made available to all users. Then Microsoft researchers develop methods to block the spyware application, and updates are automatically downloaded to the users computer so they stay up to date. This spyware solution is based on an open database, which is slow to manually combat and categorize spyware signatures.	The Apreo product stops access to spyware websites, when it identifies them. According to a recent test conducted by Websense only 2 out of 20 spyware sites were blocked, and the product did not block MSN messenger. In addition, the list of sites is only updated on a monthly basis which leaves users vulnerable for 30 days.	LavaSoft does not stop access to sites containing spyware. LavaSoft scans and inventories already deployed spyware applications and quarantines them based on its database of 21,250+ spyware applications.
Blocks back channel communications	Websense blocks backchannel communications. After infected sites have been identified, Websense then reverse engineers the sites to see where it posts to, allowing Websense to block backchannel communications based on the port and URLs. The blocking of backchannel communications proactively stops any information from being illegally accessed from outside the company.	No information available at this time.	The Apreo product does not provide protection from backchannel communication and does not have any network protection from spyware.	LavaSoft does not block backchannel communications.

<p>Prevents launching of spyware apps</p>	<p>Websense prevents spyware application from ever entering the network, through a combination of technologies including , WebCatcher, AppCatcher, proprietary software and human categorization. (For a more detailed description of these technologies refer to above).</p>	<p>If the program finds spyware, it presents the user with a list of the spyware found, detailed information about each spyware application found, as well as recommendations for dealing with each threat. However, the user can override the recommended action by selecting a new action from the list of actions displayed for each spyware application</p> <ul style="list-style-type: none"> • Ignore.This action temporarily ignores the threat until the next time the user runs a spyware scan.(If ignore is chosen in error, the user may infect their computer). • Always Ignore. This action does not quarantine or remove the threat. The threat is added to the users "Ignored Threats" list and is not marked as a threat the next time the user runs a spyware scan. • Quarantine. This action removes the spyware application from the users computer and stores it in their spyware quarantine. Any threats in the spyware quarantine do not run on the users computer and the user can restore these items back to their original state at any time.(A weakness of this option is that it is easily bypassed by the user.) 	<p>Apreo stops spyware applications from launching. The Apreo product can protect files from manipulation by spyware, which is relevant as spyware has a tendency to write to files. It also blocks spyware application using its database. Weaknesses include: -The Apreo product only updates its list of spyware applications every 30 days, which leaves the network and PC extremely vulnerable to new spyware threats.</p>	<p>LavaSoft Ad-Aware does prevent the launching of spyware applications on the desktop, but not on the network.</p>
<p>Removes Spyware</p>	<p>Websense does not remove spyware, rather identifies existing spyware on the network or desktop, and prevents the execution or backchannel communication to those host servers. Moving forward, Websense minimizes the activity that employees have to access sites that contain spyware.</p>	<p>Windows AntiSpyware (Beta) displays detailed information about every spyware program on the users machine and gives the user the option to remove it from the computer. If the user inadvertently removes any programs, they will have to reinstall the programs mistakenly deleted. Removal can be very dangerous for a computer.</p>	<p>SETS (SurfControl/Apreo product) scans for spyware signatures and provides spyware removal.</p>	<p>Ad-Aware identifies spyware, quarantines it then gives the option to delete the applications from the desktop. This can be dangerous, because application deletion in error can cause loss of fields such as autoexec files and directory files.</p>
<p>Spyware Categories</p>	<p>Spyware Keylogging Phishing and Other Frauds IM and P2P Web chat Web mail Advertisements Freeware and Software Downloads Mobile Malicious Code</p>	<p>Spyware Pop-Up Advertising (This information is provided by SpyNet, it is not local on the desktop).</p>	<p>Spyware Instant Messenger Client File Swapping(P2P)</p>	<p>No information available</p>

<p>Updates</p>	<p>Websense provides daily database updates. Websense is the only known provider of Real Time Security Updates (RTSU). Websense Real-Time Security Updates allow organizations to obtain immediate protection from new security threats. The Websense Security Labs group, researches, monitors and analyzes known and emerging web security threats. Then they notify the Websense Database Operations team to create, test, and publish updates in the quickest manner possible once received. Specifically, Real-Time Security Updates polls the download servers every five minutes requesting a database update. If available it is delivered, if not, the product is given an "up-to-date" code and the connection is terminated. The typical response time is around 45 minutes from notification to publication.</p>	<p>Microsoft does provide scheduled updates, the user must manually set them up or the user has the option to run updates as needed. Real-Time Protection is a Microsoft Windows AntiSpyware monitoring system that monitors more than 50 checkpoints in Windows. These checkpoints are triggered when programs make changes to your Windows configuration. These changes can occur when the user installs software on their computer, or they can occur when spyware or other potentially unwanted software attempts to install on the computer.</p> <p>If Real-Time Protection detects a change in any checkpoint, Windows AntiSpyware alerts the user and provides the option to allow or block the change. In some cases—for example, when installing software—users can choose to allow the change in order to continue the installation process.</p>	<p>The Apreo database is only updated on a monthly basis. This is done through human process only and then disseminated through the use of a central management console. This leaves customers vulnerable for as long as a 30-day period, if a new spyware application were to surface.</p>	<p>Updates once a week. It is a manual scan.</p>
<p>Reporting and Monitoring</p>	<p>Websense provides reporting and monitoring tools: Reporter, Explorer, and Real Time Analyzer. These tools are included in the Websense Enterprise subscription. Reporter offers more than 80 pre-defined report templates and custom reports that can be generated at scheduled times and emailed to specific recipients. Websense Reporter supports Microsoft MSDE, MySQL, and SQL Server databases. Websense Explorer, a web-based reporting tool. It does not require selection or modification of pre-defined reports. Instead, users simply drill-down into protocols, website categories, group or individual users. Websense provides Real-Time Analyzer (RTA), which is an out-of-the-box monitor that network administrators can use to examine real-time trends for website access and application usage. RTA contains only a limited number of real-time monitoring reports covering protocols, websites, categories, and individual users. RTA also displays Websense system statistics for IT administrators. RTA can store and display a maximum of 24 hours of information.</p>	<p>No information available at this time.</p>	<p>The Apreo product provides both e-mail based alerts when rules are matched and web-based reporting. The product only provides eight reports, including real-time client activity reports, client status reports, time of day reports, and category accessed reports. The product has a built-in timer for time of day reports.</p>	<p>No reporting, just logs.</p>

Support	Regular or priority 24/7 technical support available	No technical support available	Since SurfControl acquired only the code from Apreo and not the people, there will be limited support staff knowledgeable on this product, which means they will be slow to add new features.	Web-based customer service, e-mail tech support, no on-site customer support.
OS Support	Microsoft, Linux, Solaris, etc. (See Report Sheets for CPM OS Support)	MS Win 2000, Win XP, or Win Server 2003	Windows Domain NT4, Active Directory, MSDE (Microsoft SQL Server Desktop Engine), MS Access, and NDS.	Microsoft Windows 98/Me/NT/2000/XP/2003