

WebSense Version Matrix

Web Security Suite



WebSense® Web Security Suite™ protects organisations from emerging and existing web-based threats such as spyware, malicious mobile code (MMC), and phishing and pharming attacks. WebSense Web Security Suite also blocks spyware and keylogger backchannel communications from ever reaching their host servers. New security protocol categories to manage bot traffic, email-borne worms and other malicious traffic are included.

Products and Features Introduced Since v5.5.2

WebSense Web Security Suite	Version				Value
	6.3	6.2	6.1	5.5.2	
Citrix® Integration	•				Citrix integration with Websense enables customers to set and enforce URL and protocol policies for all users. Visibility into user activity through usage and performance based reporting.
Linux support for Websense Manager and DC Agent	•				Websense (except Reporting Tools and CPM) can now run on a Linux platform.
Keylogging, Potentially Unwanted Software, and Bot Networks URL categories		•			Blocks access to drive-by spyware, adware/greyware, backchannel communication-related, and bot command-and-control center websites. Prevents malicious attacks and data leakage.
WebSense Web Protection Service™ ThreatWatcher™		•			Provides customers with a “hacker’s-eye” view of their web server, regularly scanning for known vulnerabilities and potential threats and reporting on risk levels and recommended actions; helps prevent malicious attacks on their web servers before they happen.
Bot Networks, Email-Borne Worms, and Other Malicious Traffic protocols		•			Provides enhanced protection against malicious traffic in the network.
Non-Port 80 malicious traffic management		•			Blocks malicious HTTP traffic on ports other than Port 80, blocking the ports used by sophisticated internet threats including spyware, phishing and keylogger backchannel communications.
Reporting Tools					
Database Administration	•				Replaces DB Manager. Create and delete partitions, rollover by size or time, view data across partitions and configure internet browse time jobs.
Multiple database partitions per log server	•				Reporting across multiple databases, schedule automatic database rollovers, and flexible management of the log server.
Supports Microsoft® SQL Server™ 2005 and MySQL® 5.0	•				MySQL 5.0 on Linux and Solaris platforms. MySQL 4.x not supported for Websense vers 6.3.
Port and Keywords added to flexible detail reports. Customisable column choices for default report views	•				Information provides improved metrics and improves decision making.
Additional standard reports		•			A total of 20 standard reports that allow management to quickly answer common questions.
Scheduling and emailing of Websense Explorer reports. Reporting roles, portal, standard reports, favourite reports, and export to PDF			•		Provides the ability to meet customers’ unique requirements through report customisation. Reporting improvements made for ease of use and accessibility.
Flexible detailed views and Favourites functionality			•		Detailed drill-down for better analysis.

Add-on Products

Client Policy Manager™	Version				Value
	6.3	6.2	6.1	5.5.2	
Registry protection	•				Machine level policies to control malware from writing, reading, modifying, or deleting registry entries provides improved protection against attacks.
Windows® Firewall enhancements	•				Policies for inside or outside network as well as connected via VPN. Periodic refresh of firewall settings acts as anti-tampering.
Addition of Bots and Potentially Unwanted Software application subcategories		•			Allows customers to prevent the launch of bot and potentially unwanted software applications (e.g. adware or drive-by spyware) on user desktops and laptops.
Integration with Windows® Firewall in Microsoft® Windows XP Service Pack 2		•			Simplifies firewall management and automates program exceptions through awareness of application and port content.
Support for Cisco® Network Admission Control (NAC)		•			Enforces policy on devices trying to enter the network, denying access to non-compliant endpoints.
Remote Filtering			•		Extends web filtering and web security to protect remote office and mobile laptop users outside as well as inside the organisation's network.
Express Lockdown™				•	Preempts attacks and vulnerabilities by immediately locking endpoint configurations to stop the execution of any new software that may be inappropriate, harmful, or seeking to exploit newly published operating system or application vulnerabilities.
Removable Media Lockdown™				•	Prevents portable media devices from being used on client workstations, minimising the risk of introducing malicious software to the organisation. Organisations can also block writable media, depending upon their policies.
Remote Filtering					
Policy options for Fail Close and Fail Close timeout	•				Allows time for connection through 3rd party ISP.
Remote Filtering			•		Extends web filtering and web security to protect remote office and mobile laptop users outside as well as inside the organisation's network. Included in the purchase of Client Policy Manager.
Corporate Edition					
Selective Category Logging	•				Streamlines the amount of data in the Websense log database. Addresses personal privacy concerns.
Corporate Edition			•		Adds features designed specifically for large, multi-site, and distributed organisations. Features include: delegated administration and reporting; remote administration; anonymous logging; auditing; and SNMP alerting.