WEBSENSE WEB SECURITY SUITE

Websense® Web Security Suite™ is a leading internet security solution that protects organizations from emerging and existing web-based threats. Websense Web Security Suite protects against spyware, malicious mobile code (MMC), and phishing and pharming attacks. Unlike some other solutions, it also blocks spyware and keylogger backchannel communications from ever reaching their host servers. In addition, only Websense Web Security Suite includes the Websense Web Protection Services™—SiteWatcher™, BrandWatcher™, and ThreatWatcher™—to help protect organizations' websites, brands, and web servers.

WEBSENSE WEB PROTECTION SERVICES

SiteWatcher

SiteWatcher alerts Websense customers when their websites have been infected with MMC. SiteWatcher allows organizations to take immediate measures to prevent the spread of MMC to customers, prospects, and partners visiting the website.

BrandWatcher

BrandWatcher alerts Websense customers when their websites or brands have been targeted in phishing or malicious keylogging code attacks. BrandWatcher provides organizations with security intelligence, including attack details and other security-related information, allowing them to proactively notify their customers of the threat.

ThreatWatcher

ThreatWatcher provides Websense 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 through a web-based portal. ThreatWatcher helps customers prevent malicious attacks on their web servers before they happen.

Websense Web Security Suite blocks threats before they reach the endpoint, and also:

- Quickly identifies new threats.
- Decreases threat exposure time.
- Stops resident spyware from doing damage.
- Manages instant messaging (IM) and IM attachments.
- Prevents dangerous protocol-based applications from introducing security problems.

WEBSENSE WEB SECURITY SUITE – LOCKDOWN EDITION

What if you could be protected from high-risk threats as soon as they are discovered, reducing exposure time and cost?

Proactive Protection from Internet Threats

- **Blocks known threats before they reach the endpoint** – Websense Web Security Suite identifies security threats—including spyware, malcode, phishing, pharming, and keylogging—and blocks access at the internet gateway.
- **Quickly identifies new threats** – Websense mines and analyzes over 450 million websites per week for malicious activity and adds the results to the Websense Master Database in real time.
- **Decreases threat exposure time** – Real-Time Security Updates™ for the local database are available within minutes of the discovery of a new high-risk threat and require no administrative intervention—unlike other security solutions whose updates may take days to deploy.

WEBSENSE SECURITY LABS

Underlying all Websense security products is the technology and expertise of Websense Security Labs. Websense Security Labs identifies and investigates internet threats, researches and classifies them, and publishes timely research, product, and information updates to customers and the security community.

Websense Security Labs has a sophisticated process which includes:

- Global, 24x7 web analysis.
- Automated data mining and human analysis processes to crawl websites, P2P networks, and other systems looking for malicious content and applications.
- The Websense patent-pending WebCatcher™ and AppCatcher™ customer feedback loops
- Continuous monitoring of newsgroups, chat rooms, security websites, and online forums for the latest vulnerability releases and proof-of-concept exploits.

Through the work of Websense Security Labs, Websense proactively discovers and immediately protects customers from web security threats:

- First to discover websites using the Sony digital restrictions management (DRM) rootkit vulnerability to exploit users.
- First to discover large, zero-day exploits on Microsoft Internet Explorer and Microsoft Windows.
- First to identify the MSN Korea malicious code attack.
- First to discover cyber-extortion attempts.

- **Stops resident spyware and keyloggers from doing damage** – Websense Web Security Suite blocks spyware and keylogger backchannel communication to host servers.
- **Manages IM and IM attachments** – Websense Web Security Suite fills the security and compliance gap inherent in IM communications, which presents significant risks for intellectual property theft and malicious attacks.
- **Prevents dangerous protocol-based applications from introducing security problems** – Websense Dynamic Protocol Management™ offers the ability to extend policy control of protocols to the network level, including management of peer-to-peer (P2P), email, file transfer, and other protocols.

Websense Web Security Suite – Lockdown Edition™ extends security to the endpoint, adding endpoint "lockdown" capabilities and web security for remote and mobile users to Websense Web Security Suite.

Prevent Attacks

Websense Web Security Suite – Lockdown Edition provides an immediate "first line of defense" by:

- Addressing weaknesses in antivirus, anti-spyware, personal firewall, and patch management processes to prevent zero-day attacks.
- Protecting remote and mobile users that may operate outside perimeter defenses or that do not receive standard security updates or patches.
- Establishing levels of desktop "lockdown" to prevent the launch of unauthorized applications or mitigate the propagation of security attacks.

Control Application Use

Websense Web Security Suite – Lockdown Edition helps control application use by:

- Enforcing flexible and auto-updating application use policies that protect end users from malicious software.
- Preventing the installation and execution of unauthorized applications.
- Identifying and categorizing application data and delivering automatic daily updates.
- Reporting on application activity, with detailed forensics to help pinpoint potential problems.

Safeguard Information

Websense Web Security Suite – Lockdown Edition helps block the potential theft of private information or intellectual property via removable media. Websense Web Security Suite – Lockdown Edition also provides another level of security by:

- Providing another layer of control over information at the desktop.
- Preventing the introduction of malicious software within the organization.
- Allowing system administrators to prevent devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being used on client workstations.
- Blocking writable media, depending upon the organization's policy.

Streamline Operations

Websense Web Security Suite – Lockdown Edition optimizes IT operations by ensuring only "approved" configurations are running, and allows IT to be proactive by eliminating calls and dispatches for desktop rebuilds due to performance or application compatibility problems. Websense Web Security Suite – Lockdown Edition requires minimal effort to deploy and manage, yet offers:

- Integration with leading directory services.
- A low-impact agent compatible with Microsoft Windows.

Websense Reporting Tools

Included at no additional charge with Websense Web Security Suite and Websense Web Security Suite – Lockdown Edition, Websense Reporting Tools provide organizations with the most advanced capabilities for identifying, analyzing, and reporting on internet and endpoint security risks.

Websense Reporting Tools help organizations to determine their risk profiles by

- Detecting the presence and location of MMC, spyware, hacking tools, and other security risks in the network.
- Performing critical software assessments that provide categorized and normalized views of programs and applications.

Real-time monitoring and powerful drill-down features give immediate, in-depth analysis, exception tracking, and trending capabilities throughout the organization. Pre-defined report templates and customizable reports can be run at pre-set intervals and emailed automatically to make sure information is available when, where, and how it is needed. Websense Reporting Tools enable early threat detection and identification of potential network and application vulnerabilities.

The Websense Web Security Ecosystem™

The Websense Web Security Ecosystem is a comprehensive framework of technology integrations that provides enhanced security and ease of deployment of Websense web security solutions in enterprise environments. The Websense Web Security Ecosystem incorporates world-class security and networking technologies including: internet gateways, network access control, security event management, identity management, and appliance platforms. With seamless integration across more than 40 different networking and security solutions, the Websense Web Security Ecosystem increases the effectiveness of identifying and mitigating web-based threats and vulnerabilities. Through these integrations, Websense is uniquely positioned to complement customers' current and future network environments.

Why Websense

Websense, Inc., is a global leader in web security. With over 24,000 customers, the company is the vendor of choice for leading Fortune 500 and FTSE 100 customers, as well as government agencies, and educational institutions. Websense proactively discovers and immediately protects against web-based threats such as spyware, phishing attacks, viruses, and crimeware. Websense secures organizations from existing and emerging internet threats by providing proactive, policy-driven web and endpoint security software. Websense security software fills the technology gaps left open by networks and defenses such as antivirus, anti-spyware, firewall, and other products. With diverse partnerships and integrations, Websense enhances its customers' network and security environments.

System Requirements

Websense Web Security Suite

- Microsoft Windows Server 2003 Standard or Enterprise Editions, or the same with SP1
- Microsoft Windows 2000 with SP3 or higher
- Red Hat Enterprise Linux 3 or 4: AS, ES, or WS, or Red Hat Linux 9
- Sun Solaris 9 or 10

Websense Web Security Suite – Lockdown Edition Server

- Microsoft Windows Server 2003 Standard or Enterprise Editions, or the same with SP1
- Microsoft Windows 2000 Server with SP3 or higher
- Red Hat Enterprise Linux 3 or 4: AS, ES, or WS, or Red Hat Linux 9
- Sun Solaris 9 or 10

Websense Web Security Suite – Lockdown Edition Client

- Microsoft Windows XP Professional with SP1 or SP2
- Microsoft Windows Server 2003 Standard or Enterprise Edition with SP1
- Microsoft Windows 2000 Professional, Server, or Advanced Server with SP3 or SP4

Summary

Today's computing environment demands a multi-layered, multi-dimensional security strategy. Websense Web Security Suite is a critical layer of that strategy, filling the gaps left by traditional defenses and blocking security threats before they reach the endpoint or extend throughout the network.

Websense, Inc.
San Diego, CA USA
tel 800 723 1166
tel 858 320 8000
www.websense.com

Websense UK Ltd.
Chertsey, Surrey UK
tel +44 (0) 1932 796300
fax +44 (0) 1932 796601
www.websense.co.uk

Australia
websense.com.au

Brazil
portugues.websense.com

Colombia
websense.com.es

France
websense.fr

Germany
websense.de

Hong Kong
websense.cn

India
websense.com

Ireland
websense.co.uk

Italy
websense.it

Japan
websense.jp

Mexico
websense.com.es

PRC
prc.websense.com

Spain
websense.com.es

Sweden
websense.co.uk

Taiwan
websense.cn

Download a free 30-day evaluation today www.websense.com/downloads

WEBSENSE
SECURING PRODUCTIVITY™