



Websense® Web Security Suite™ provides an integrated web security solution that fills the time and technology gaps between antivirus and firewall applications. Websense Web Security Suite blocks spyware, malicious mobile code (MMC) and other web-based threats as well as spyware and keylogging transmissions back to their host sites. It also protects employees from phishing and controls the sending and receiving of instant messaging (IM) clients. Websense Web Security Suite provides real-time updates for immediate protection from new security threats and also includes robust reporting and analysis tools that provide organizations with complete information on user access to fraudulent sites or vulnerability to malicious code.

## Key Features and Benefits

### Prevent spyware, MMC, phishing, keylogging, and other web-based threats

Add an additional layer of security to your network by preventing employees from unknowingly accessing phishing sites, sites that contain or distribute spyware or keylogging software, and sites that are infected with MMC. Should spyware or keylogging software already reside on your corporate desktops, Websense Web Security Suite stops the transmission of sensitive information to host spyware and keylogging servers.

- Websense Web Security Suite stops spyware first by blocking access to sites that distribute spyware, then by preventing the transmission of employee and network information to host sites. Websense is able to identify spyware servers and block backchannel communications via port 80 connections.
- Websense Web Security Suite prevents organizations and their employees from being victimized by phishing and other frauds. Websense helps address phishing by identifying fraudulent websites and blocking employee access to those sites.
- Websense scans its database of millions of sites for malicious code, including ActiveX controls, Visual Basic script, JavaScript, and Java Applets. Websense Web Security Suite categorizes those sites infected with MMC and blocks employee access to them.
- Websense Web Security Suite stops keylogging by blocking access to sites that distribute keylogging software and then by preventing the transmission of keystroke data to a keylogger's host site.

### Control the sending and receiving of files via IM clients

IM has grown in popularity because it combines the convenience of email with the immediacy of the telephone. In the workplace, IM can contribute significantly to productivity by promoting collaboration and team-building among employees, partners, and customers. Because proprietary information can easily be sent to or accessed by unauthorized individuals via IM, companies may be reluctant to allow its use. With Websense Web Security Suite, organizations can

## Websense® Web Security Suite™

### Websense Web Security Suite

Websense Web Security Suite provides a robust web security solution for customers and fills the time and technology gaps inherent within existing security solutions such as antivirus software and firewalls.

- Blocks spyware, malicious mobile code (MMC), and other web-based threats including web-borne viruses, Trojan horses, worms, keylogging, script attacks, and rogue internet code
- Blocks spyware and keylogging transmissions back to host sites
- Protects employees and organizations from phishing and fraud-based attacks
- Controls the sending and receiving of files via instant messaging (IM) clients
- Provides real-time updates and immediate protection from new security threats
- Provides advanced reporting tools for detecting and analyzing security risks
- Includes subscription to Websense® Security Labs™ alerts, SiteWatcher™ and BrandWatcher™ services

### Websense Web Security Suite – Lockdown Edition

Websense Web Security Suite - Lockdown Edition provides a comprehensive security solution for customers at the internet gateway, network, and desktop.

Includes Websense Web Security Suite and:

- Stops the execution of unauthorized applications - such as spyware, peer-to-peer (P2P) file sharing, and hacking tools - on the desktop
- Offers enhanced end-point security for mobile computing
- Provides maximum control over desktop environments by allowing only approved applications to run on corporate PCs and servers through advanced lockdown features

control the use of unsafe IM applications and attachments. For example, organizations may allow IM use, but prohibit the use of file transfers using IM. Organizations can also choose to deny use of certain IM applications altogether.

### Real-time updates and immediate protection from new security threats

It often takes hours or days for vendors of other security solutions to develop an antidote to a new security threat, leaving the door open for network intrusion. Once the antidote or patch is provided, implementing these new threat signatures may require technical expertise or at least manual intervention to deploy. Websense Web Security Suite closes the window of exposure to security threats by automatically addressing those threats via database updates and with no manual administrative action required.

- Receive immediate database updates for web-based and application-based threats minutes after detection by Websense.
- Dramatically lower your organization's risk, save time, and increase productivity by identifying and managing security threats hours before other traditional security solutions are updated.

### Advanced reporting tools for detecting and analyzing security risks

Websense Web Security Suite includes Websense reporting tools that offer real-time and historical views of company risks related to employee web and application use. Using this information, IT administrators can refine internet access and application policies and effectively reduce the risks associated with employee computing in their organizations.

- Identify your organization's risk levels with respect to security.
- Detect the possible presence of MMC, spyware, or hacking tools in your network.
- Discover the use of instant messaging in your organization.
- Refine your internet and application use policies with insight from powerful reporting and forensic tools.

### Subscription to Websense Security Labs™ alerts and services

Websense Web Security Suite includes a subscription to the Websense Security Labs alerts, as well as SiteWatcher™ and BrandWatcher™ services. With extensive internet and malicious code categorization expertise, Websense Security Labs continuously monitors malicious events on the internet to deliver timely product and information updates to the security community and Websense customers to support their infrastructure security efforts. This includes, but is not limited to, the areas of malicious websites, phishing-based attacks, and other emerging threats associated with keylogging, spyware, IM attachments, and corporate use of peer-to-peer (P2P) applications.

- **Websense Security Labs Alerts** - Informs the security community and Websense customers of emerging threats and attacks such as malicious websites, phishing attacks, keyloggers, and other web-based threats.

- **Websense Security Labs SiteWatcher** - A service that alerts Websense customers if their organization's website has been infected with MMC. This allows the organization to take immediate measures to prevent the spread of MMC to customers, prospects, and partners visiting its website.
- **Websense Security Labs BrandWatcher** - A value-added service that alerts Websense customers if their organization's website or brand has been targeted in a phishing or malicious keylogging code attack. This service provides the organization with security intelligence including the attack details and other security-related information.

## Websense® Web Security Suite™ - Lockdown Edition

The Websense Web Security Suite - Lockdown Edition provides a comprehensive security solution for customers at the internet gateway, network, and desktop. The Websense Web Security Suite - Lockdown Edition includes the Websense Web Security Suite, and will also:

### Stop the execution of unauthorized applications - such as spyware, P2P file sharing, and hacking tools - on the desktop

Websense Web Security Suite - Lockdown Edition provides an important layer of desktop security to address the critical zero-day security loophole that is not effectively or practically addressed elsewhere in the industry. Websense Web Security Suite - Lockdown Edition helps stop the execution and propagation of known and unknown security threats by identifying and managing them at the desktop level.

### Provide enhanced end-point security for mobile computing

Today's corporate computing environments require a new type of management solution, a layered approach that focuses on the way employees use corporate computing resources. Websense Web Security Suite - Lockdown Edition provides multilayered protection at the gateway, on the network, and at the desktop. Furthermore, the "connected / disconnected policies" feature enables IT to enforce use policies for all users, including mobile employees' laptops.

### Ensure maximum control over desktop environments by allowing only approved applications to run on corporate PCs and servers through advanced lockdown features

Websense Web Security Suite - Lockdown Edition's Network Lockdown™ feature enables IT to close the window of exposure to unknown security threats by preventing these attacks from propagating over the network. Network Lockdown blocks network access to specific ports and protocols by application category. In addition, the Application Lockdown™ feature allows only an approved set of applications to run on corporate PCs and servers, thereby preventing unknown and potentially malicious applications from launching.