

WEBSense CAPABILITIES GUIDE

Lee Smith
Network Manager, Harvey Nichols

"We chose Websense® as we wanted to have confidence that employees would not be exposed to any risks."



Websense, Inc. is the global leader in web filtering and a leader in web and endpoint security. Websense software helps organizations meet the risks of internet use, offering maximum protection with minimal effort. Trusted by over 24,000 organizations worldwide and with over 24.1 million seats under subscription, Websense is the vendor of choice for leading Fortune 500 and FTSE 100 customers, as well as for government agencies and educational institutions. Websense proactively discovers and immediately protects against web-based threats such as spyware, phishing attacks, viruses, and others. Websense secures organizations from existing and emerging internet threats by providing proactive, policy-driven web filtering, web security, and endpoint security software. Websense 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.



IT CHALLENGES AND WEBSense CAPABILITIES

Challenge: Loss of Confidential Information

Organizations can lose their intellectual property, customer data, even system IDs and passwords to security attacks launched from outside or through the acts of internal employees. The harm done when secrets find their way into competitors' hands is not limited to the shattered trust of customers, vendors, or partners; there are also possible financial penalties from regulatory agencies, lawsuits from affected parties, and loss in employee productivity because of compromised network access.

Websense helps organizations prevent data loss. Organizations can set policies to prevent employees inside and outside the network from accessing websites known to host programs designed to steal confidential information. Even if a user has previously accessed, for example, a spyware- or keylogger-infected site and the malicious code is already on the user's computer, Websense will block the backchannel communications to the host servers, keeping any captured information from leaving the organization.

But malicious code and malicious websites are only part of the problem. Confidential information can leak out in instant messages (IM) and IM file attachments. Often, IM applications do not communicate using the same ports and protocols monitored or blocked by firewalls and other traditional security solutions. Websense allows organizations to set policies to manage the use of IM and IM file attachments to protect themselves from information loss and from the security threats that can enter through these channels.

Employees may also take confidential information with them by downloading it to removable media devices like CD/DVD drives, USB drives, and external hard drives. Websense allows organizations to block the use of removable media to prevent files from being transferred to these devices and leaving the organization. Organizations can also block writeable media, depending on their policies.



Challenge: Regulatory Compliance

In recent years, the inadequacy of policies and controls in certain high-profile organizations has led to the creation of new regulations. While each law has its own agenda, there are overriding issues that this new legislation collectively addresses: audit controls, information management, financial reporting, risk management, and security. These new regulations impose new requirements on organizations, establish standards for compliance, and institute penalties—some extremely harsh—for noncompliance.

Websense helps organizations meet regulatory requirements by preventing access to websites, protocols, and applications that may pose a security threat to the organization's confidential data. For regulations that require specific age groups to be prevented from viewing content classified as inappropriate, Websense allows organizations to filter that content for the groups.

Websense also helps organizations control the flow of information into and out of the organization, through the management of IM and IM attachments and removable media devices. Websense can also track and record attempted security breaches such as invalid login attempts, port scans, and requests for inappropriate access. Management can receive regular reports so corrective action can be taken and compliance maintained.

Challenge: The Rapidly Changing Nature of Attacks

Because traditional defenses, like firewalls and antivirus software, have adapted as exploits have been uncovered, cyber-criminals continue to improve their techniques. Where once viruses were a primary method of attack, now malicious mobile code and alternative attacks (e.g. attacks through peer-to-peer file sharing and IM programs) are used because of their ability to bypass traditional defenses. These new attacks can change system settings, get users to provide personal or corporate information, steal an organization's sensitive data, or even hold files hostage until a ransom is paid. The results of these attacks are many: increased calls to the Help Desk, decreased productivity, increased exposure to legal liability, and noncompliance with industry regulations, all serious and costly consequences for organizations.

Websense protects organizations from today's evolving web-based attacks at the internet gateway, on the network, and at the endpoint.

At the internet gateway, Websense:

- Prevents employees from accessing malicious websites.
- Blocks malicious HTTP traffic on all ports.

On the network, Websense:

- Allows organizations to manage the use of IM and IM attachments to lower the risk of intellectual property theft and malicious attacks through this channel.
- Prevents dangerous protocol-based applications from introducing security problems by extending policy control of protocols to the network level.
- Enables deep content inspection for web-based threats through proxy and cache capabilities.

At the endpoint, Websense:

- Prevents employees outside the network from accessing malicious websites.
- Blocks the launch of malicious applications.

Websense quickly identifies new security threats such as spyware, drive-by spyware, bots and bot network traffic, phishing, pharming, keylogging, and email-borne worms. Real-time updates automatically protect organizations and decrease their exposure time to new threats.

Challenge: Remote and Mobile Users

Remote and mobile users pose a unique set of challenges. They may regularly use outside networks. These networks may not be as secure as the organization's network and could expose these users to security threats. Spyware, keyloggers, malicious mobile code, and other malware can lodge on the endpoint, degrading performance, causing data loss, and requiring the IT department to spend time remediating or re-imaging the workstation. When the user re-enters the organization's network, the threat may spread throughout the network. Additionally, because of their locations, remote and mobile users may not receive software patches or updates as regularly as they would at the main office. This delay increases their exposure to emerging security threats. Infection can result in frequent and longer Help Desk calls and decreased productivity while machines travel between the user and the main office or until an IT representative can come on-site.

Websense provides remote and mobile users operating outside the network with the same level of protection as they have inside the network. By providing this proactive protection, the workload on IT is reduced. IT does not have to spend as much time troubleshooting and repairing damage caused by attacks on these remote and mobile users. The likelihood of an attack is the same for these users as it is for users within the organization's network. The benefit to organizations is that their labor, overhead, and in some cases, capital equipment costs related to remediating security-related attacks on remote and mobile users is reduced. Websense can also limit the remote and mobile environment to a known configuration to prevent users from introducing new applications that may cause conflicts with existing applications.

Challenge: Increased Complexity and Globalization of Organizations

IT departments in large, multi-site, and distributed organizations face scalability and administration challenges not typically experienced by smaller, single-site organizations. These challenges stem from the large number of users, devices, and offices requiring web security and web filtering protection. Third-party security and networking tools—network access control, security event management, identity management, internet gateway, and appliance solutions—are designed to help manage this complexity, but they may also inadvertently add to it. The volume of information generated, as well as the need for access to and control over this information by individuals at different levels and functional areas, can place a significant burden on the corporate IT resources.

Over 450 million sites per week are mined and analyzed through automated data mining and human analysis processes.

Websense addresses these particular needs of large, multi-site, and distributed organizations. Websense allows organizations to efficiently manage internet usage policies across multiple departments, business units and group without increasing the workload on the corporate IT resources. Policy decisions can be pushed closer to the end-users by delegating administrative capabilities. For organizations that operate in multiple states, countries, or regions, this is particularly important. Policies can be customized to suit the cultural and structural needs of a particular region. Even though organizations may choose to push policy decisions closer to the end-users, Websense allows organizations to track and analyze all administrative activities to ensure policy compliance with corporate guidelines and improve web security.

Challenge: Productivity

With the entire world available to them through their computers, employees can be distracted by non-work related or unproductive activities. These activities can impact the organization's overall productivity. Too many employees using bandwidth-intensive applications like streaming media can decrease the organization's network capacity or cause system downtime.

Websense allows organizations to define and enforce internet use policies to minimize inappropriate internet use and ensure available bandwidth for business-critical applications. Organizations can manage protocols and desktop applications used in non-productive activities to conserve the available bandwidth. Additionally, organizations can increase available bandwidth during peak times and automatically adjust to real-time network conditions through dynamic bandwidth policy enforcement. This dynamic policy enforcement helps organizations conserve and more effectively utilize their network bandwidth. Websense also offers an enterprise-class proxy and cache solution that accelerates the delivery of web-based content to users to increase network performance while decreasing bandwidth consumption.

WEBSense ADVANTAGES

Automatic Protection

Websense offers automatic, real-time updates for critical website and application security threats. Unlike other solutions, these updates do not require a full product upgrade or IT intervention to deploy.

Easy-to-Use Reporting

Websense solutions offer unparalleled reporting that includes web-based, drill-down capabilities usable by IT as well as non-technical groups such as Human Resources, Legal, and Management—at no extra cost. Websense Reporting Tools offer “Risk Classes” that provide management-level summary information on the network security, legal liability, employee productivity, and bandwidth risks of an organization. Whether presenting a real-time or historical view of categorized network activity, Websense Reporting Tools provide easily-understood information quickly across terabytes of data.

Flexibility

Websense solutions integrate with all leading enterprise directories, such as Microsoft® Windows NT®, Windows® Active Directory®, LDAP, Novell® eDirectory, and RADIUS, making deployment and administration easy. Websense solutions allow the creation of policies based on the users/groups defined in these enterprise directories.

Scalability

Websense solutions scale from 50-user organizations through 250,000 users and beyond with full reliability and accuracy. Offering either standalone or integrated deployments for maximum flexibility and scalability, the Websense architecture allows a single-box deployment or a distributed component approach.



WEBSense TECHNOLOGY AND EXPERTISE

Research and Development Philosophy

Websense is a web filtering, web security, and endpoint security company. All of the company's research and development spending is devoted to these areas and not divided among other, unrelated areas as is often the case with other companies in these markets. Over the last five years, Websense has invested more than \$62 million in research and development, increasing its expenditures in that area each year.

Security Expertise

Security is a key focus for Websense. A dedicated global team of security researchers proactively discovers and investigates internet threats, researches and classifies them, and publishes timely product and information updates to the security community and Websense customers to support them in securing their infrastructures.

A worldwide network of computers provides global, 24 x 7 analysis of the web. Over 450 million sites per week are mined and analyzed through automated data mining and human analysis processes. Programs crawl websites, peer-to-peer networks, and other systems looking for malicious content and applications. Honeypots and honeynets—computers and networks deliberately configured with vulnerabilities—wait to be attacked by the latest security threats.

Additional websites and applications come through the Websense patent-pending WebCatcher™ website and AppCatcher™ application customer feedback loops while security researchers continually monitor newsgroups, chat rooms, security websites, and online forums for the latest vulnerability releases and proof-of-concept exploits. Expert staff from all over the world, skilled in multiple languages and international cultures, reviews websites, applications, and protocols on a regular basis to ensure the accuracy of categorization. The work of these researchers is available to the community through free email alerts and a blog, and to customers in the form of free daily database downloads and premium real-time database updates.

Websense plays an active role in key web security research organizations, such as the Anti-Phishing Working Group (APWG) and the Anti-Spyware Coalition (ASC). A member of both organizations, Websense has taken the lead role in the APWG's Phishing Data Repository project. Because of its research and industry participation, Websense staffers are asked to participate in influential web security consortia as well as speak at conferences and events worldwide.

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. Through seamless integration with more than 40 different technology solutions, the Websense Web Security Ecosystem helps organizations identify and mitigate web-based threats and vulnerabilities.

WEBSense CAPABILITIES GUIDE

WEBSense FIRSTS

- First to discover that the Google™ website hosting service, “Google Pages,” was hosting malicious code.
- First to discover a major exploit in Microsoft Internet Explorer® that allowed the installation of an SDbot variant.
- First to discover websites exploiting the Microsoft Windows vulnerability in .WMF image files to distribute spyware.
- First to discover cyber-extortion (ransomware).

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.ie

Italy
websense.it

Japan
websense.jp

Mexico
websense.com.es

PRC
prc.websense.com

Spain
websense.com.es

Sweden
websense.com

Taiwan
websense.cn

For more information, visit www.websense.com or contact your authorized Websense reseller

