



Websense Enterprise®, the world's leading Employee Internet Management solution, defends organizations and employees using the Internet against new and emerging threats such as spyware and malicious mobile code. Websense Enterprise enhances security, improves employee productivity, reduces legal liability, and optimizes the use of IT resources. Websense Enterprise integrates seamlessly with leading network infrastructure products and offers unequalled flexibility and control.

GROWING RISKS AND PRODUCTIVITY CHALLENGES

Every organization with a connection to the Internet has faced the problem of users accessing inappropriate material on the web. To that problem have been added those of harmful applications downloaded from websites, spyware, the use of instant messaging (IM) and peer-to-peer (P2P) applications, and more. The result has been a dramatic increase in the costs and risks of maintaining an unmonitored network. Consider the following:

Spyware – As many as 9 out of every 10 computers are infected with spyware. Do you know how many of your desktops are infected? How do you prevent spyware from sending confidential information back over the Internet?

Malicious Mobile Code (MMC) – The number of malicious code attacks, which are often used to steal confidential data, rose nearly 50% in the last year.

Peer-to-Peer (P2P) File Sharing – 77% of organizations have at least one P2P file-sharing application on their network. With pornography being the target for more than 73% of P2P searches, P2P networks open a new back door to legal liability.

Instant Messaging (IM) – 1 in every 5 employees is using a public IM tool. IM can transmit proprietary company information in unencrypted format and transfer file attachments that bypass the existing security infrastructure.

Streaming Media – 44% of employees run streaming media applications during the workday. Streaming audio and video are so bandwidth intensive that it can leave critical business applications starved for adequate network resources.

Employee Hacking – In the last 12 months, 45% of businesses detected unauthorized access to computer files and resources by insiders. Hacking tools are more readily available on the Internet than ever before, increasing the security and legal liability risks from employee hacking.

The many and growing risks inherent in employee Internet activity and access to unauthorized applications are issues that IT must confront. How can a network administrator or an IT security manager leverage existing infrastructure investment to quickly and effectively manage these new threats? Websense® has the answer.

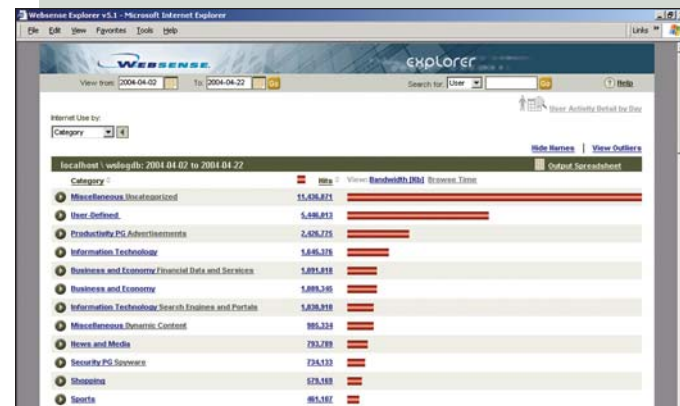
Websense Enterprise® Product Overview

Websense Enterprise Capabilities:

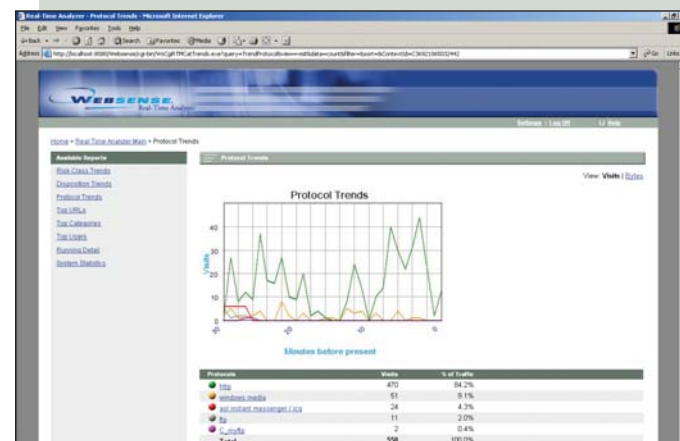
- Best-of-breed Internet filtering from the industry leader.
- Protection from spyware, phishing and other frauds, malicious websites, and employee hacking.
- Management of bandwidth resources.
- Management and analysis of peer-to-peer and instant messaging use.

Websense Enterprise Benefits:

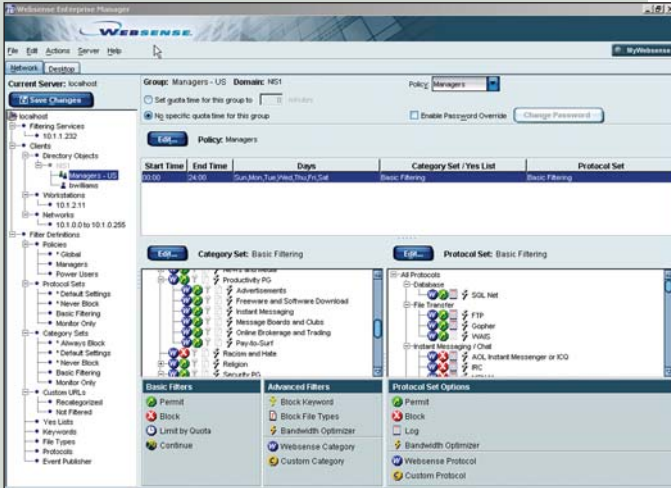
- Reduce the risk of security breaches.
- Improve employee productivity.
- Mitigate the risks of legal liability as a result of employee behavior.
- Optimize the use of IT resources, including bandwidth and desktop resources.
- Enforce Internet and application use policies.



Detect security risks or productivity problems arising from employee Internet activity quickly and easily using Websense Enterprise Explorer.



Quickly identify real-time problems in your network using Websense Enterprise Real-Time Analyzer™.



Customize policies for different users and groups easily with Websense Enterprise Manager.

WEBSENSE ENTERPRISE, MULTILAYERED PROTECTION FOR EMPLOYEE COMPUTING RESOURCES

Websense Enterprise is a comprehensive solution for combating the threats arising from employee use of the Internet and network.

Websense Enterprise allows you to:

- Manage employee Internet access
- Block spyware, phishing sites, and malicious mobile code
- Prevent P2P file sharing
- Manage instant messaging and IM attachments
- Manage the use of streaming media and other high bandwidth applications
- Prevent employee hacking

The Websense Master Database

The heart of Websense Enterprise is its Master Database.

The Master Database contains the most frequently accessed sites and protocols on the web. It is the largest, most accurate, and most up-to-date database in the Employee Internet Management industry.

The Master Database contains more than 6 million sites, classified into over 80 categories, allowing for greater customization of your organization's Internet use policy. The Master Database includes sites in over 50 languages, including English, French, German, Spanish and Japanese.

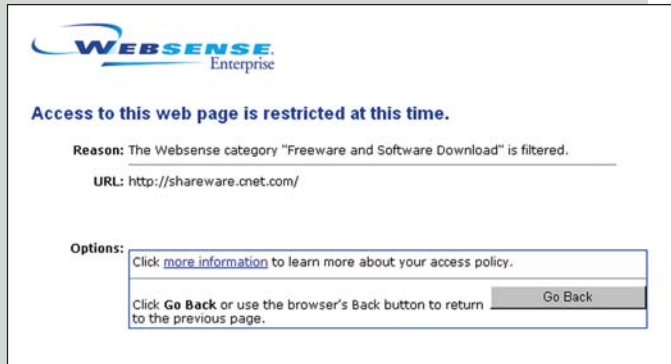
Best-of-breed Internet filtering

Websense Enterprise is the world's leading Employee Internet Management solution, combining powerful flexibility with rich functionality.

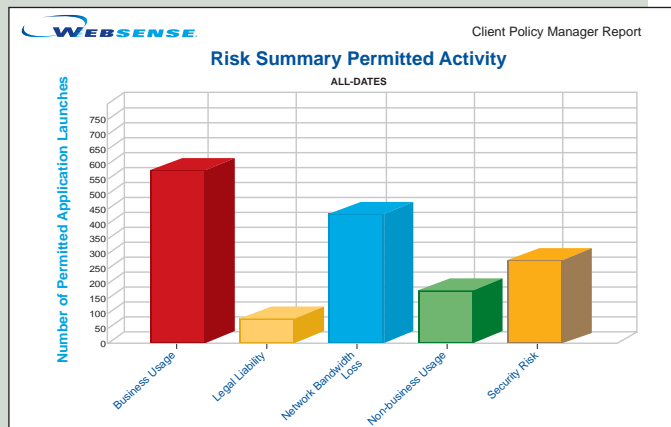
- Provides comprehensive and accurate Internet filtering supported by a database of URLs, built using a combination of automated and human classification and dynamically tuned to real-life surfing patterns with Websense WebCatcher™.
- Balances work-related and personal surfing by enabling IT administrators to set custom policies to manage employee Internet, network, and application use.
- Minimizes administrative overhead in setting and enforcing employee computing policies with the easy-to-use Websense Enterprise Manager.
- Provides report templates, block pages, and web page category names in ten languages: Chinese (simplified and traditional), English, French, German, Italian, Japanese, Korean, Portuguese, and Spanish.

Industry-leading analysis and reporting

Websense Enterprise provides the most advanced capabilities for detecting productivity losses and security risks arising from employee Internet and application use in your organization. No other solution provides such a broad range of tools to isolate and identify your risks:



Provide end-users with customized message pages.



Determine potential liability, bandwidth, productivity, and security risks within your organization with risk reports.



Websense Enterprise Real-Time Analyzer™ – Analyze current and recent network traffic with this real-time analysis tool, which captures a snapshot of network activity and answers important network-related questions quickly.

Websense Enterprise Explorer – Get quick and easy access to employee activity statistics with this forensic and reporting tool for IT, HR, legal, and business managers.

Websense Enterprise Reporter – Choose from over 80 predefined report templates with this robust engine, built on Crystal Reports® and offering the ability to customize and schedule reports for distribution via email.

Enhanced Internet filtering with Premium Groups™

The Websense Enterprise Premium Groups™ (PG) family of products enhances the standard filtering capabilities of Websense Enterprise with additional coverage of high-risk categories:

Websense Enterprise Security PG™

Minimize the risk of security breaches by blocking access to phishing and other frauds, spyware sites, and websites infected with malicious mobile code. Stop the transmission of sensitive information to host spyware servers.

Websense Enterprise Productivity PG™

Increase employee productivity by controlling access to many of the most popular cyber-slacking categories such as online advertisements, IM, freeware, and pay-to-surf.

Websense Enterprise Bandwidth PG™

Improve network performance by managing access to bandwidth-intensive downloads. Filter out sites that provide streaming media, Internet radio and TV, and P2P file sharing, among others.

Network Management and Bandwidth Optimization

Websense Enterprise offers the unique ability to extend policy control and enforcement to the network level. This allows organizations to:

- Manage IM, P2P, and streaming media applications by network protocol.
- Set policies based on application protocols and file types with Dynamic Protocol Management™. Automated updates to the protocol list ensure accuracy and minimize administration.

Websense Enterprise Bandwidth Optimizer™ (BWO) – Better utilize and conserve your available network bandwidth with BWO, an add-on module to Websense Enterprise. BWO seamlessly integrates with Websense Enterprise and allows organizations to prioritize critical business processing over non-work-related uses. BWO blocks personal Internet activity or application use when network bandwidth thresholds set by administrators are exceeded.

Websense Enterprise IM Attachment Manager™ (IMA) – Safeguard your enterprise from the largest security threat in instant messaging file transfers. IMA integrates seamlessly into your Websense Enterprise environment to allow maximum flexibility in your management of public instant messaging use on your network. Network administrators can set policies that block the sending and receiving of file attachments, minimizing the possibility of viruses or worms imported via IM applications.

Seamless integration for rapid and cost-effective installation.

Websense Enterprise can be deployed in any of three ways, depending on your network requirements: in an integrated, embedded, or stand-alone configuration. The wealth of deployment options ensures ease of installation and maintenance while maximizing scalability, performance, and feature support.

Websense Enterprise is currently integrated/embedded with:

- 3Com
- Lightspeed
- Blue Coat
- Microsoft
- Check Point
- Nokia
- Cisco
- Juniper Networks/NetScreen
- Crossbeam
- Network Appliance
- CyberGuard
- Novell Volera
- Dell
- ServGate
- F5
- SLMsoft
- Hewlett-Packard
- SonicWALL
- iMimic
- Squid
- Immunix
- Stratacache
- Infolibria
- Sun Microsystems
- Inktomi

WebSense® Client Policy Manager™ (CPM) delivers zero-day protection against unknown security threats

Only CPM provides zero-day protection from unknown security threats and enforces employee application use policies for corporate desktops, laptops, and servers with its unique and comprehensive database of categorized applications. CPM stops the execution of unauthorized applications, such as spyware, peer-to-peer (P2P) file sharing, and hacking tools. Complementing traditional firewall and anti-virus tools, CPM provides a proactive critical component that closes the window of exposure to today's fast-moving and blended security threats.

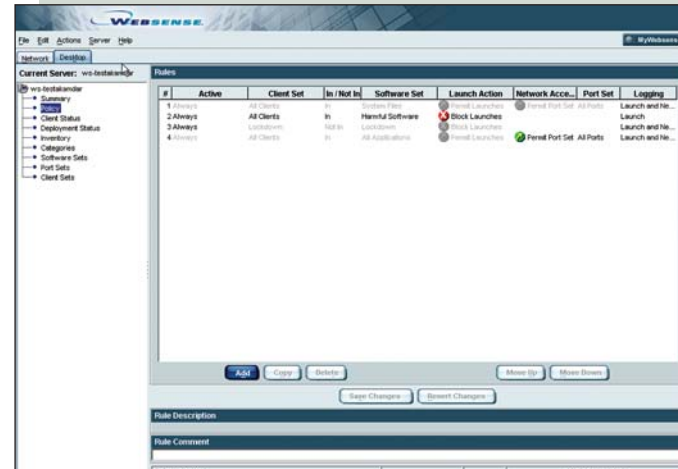
WebSense Enterprise system requirements

Hardware:

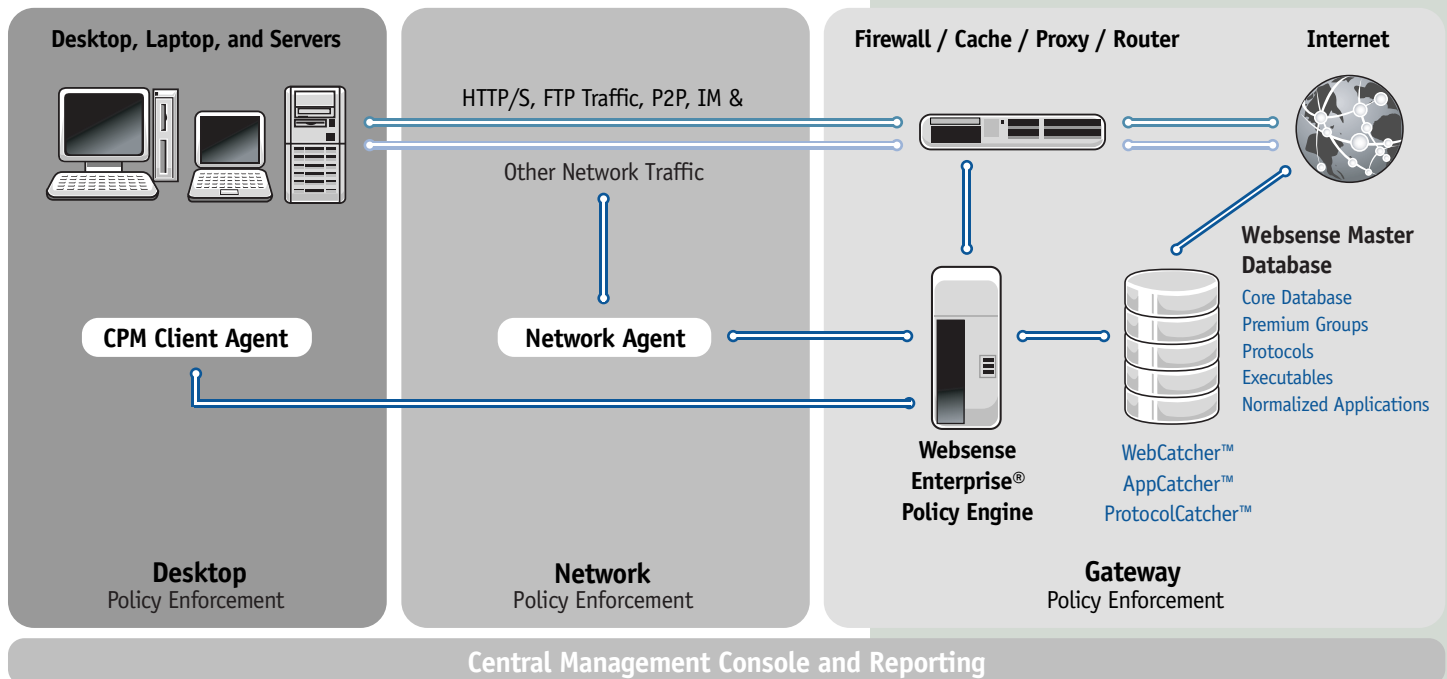
- Pentium III or Sun Ultra 10 processor or greater with at least 512 MB RAM. Hardware requirements will vary by configuration. Please see deployment guide for additional information.

Software:

- Microsoft® Windows® 2003 Server, Windows® 2000 Server (SP3 or greater)
- Red Hat Linux™ 9 or Red Hat Enterprise Linux™ 3
- Sun Solaris™ 8-9



Enforce flexible policies for malicious and unauthorized applications using central management console.



Download a free, fully-functional 30-day evaluation at www.websense.com/downloads today!

WebSense Inc.
San Diego, CA USA
tel 800.723.1166
tel 858.320.8000
www.websense.com

WebSense UK
Chertsey, England
tel +44 (0)1932. 796001
www.websense.co.uk

WebSense France
Paris, France
tel +33 (0)15660. 5814
www.websense.fr

WebSense Germany
Munich, Germany
tel +49 (0)89 24445. 4005
www.websense.de

WebSense Japan
Tokyo, Japan
tel +813.5322.1335
www.websense.co.jp

WebSense Australia
Sydney, Australia
tel +61 2 9006. 1621
www.websense.com.au

WebSense Greater China
Hong Kong
tel +852.2855.8811
www.chinese.websense.com
www.prc.websense.com

WebSense Latin America
Sao Paulo, Brazil
tel +55.11.4612.0798
www.espanol.websense.com
www.portugues.websense.com