



Websense®

Web Security Gateway Solutions

Dynamic, interactive Web 2.0 technologies have transformed the Web into a core business application platform. Traditional customer relationship and payroll applications are now delivered interactively over the Web, while applications like social networking are used on a daily basis for recruitment, lead generation, and other business processes. Along with Web 2.0, however, comes new risk as dynamic and user-generated content renders traditional security technologies, such as anti-virus and URL filtering, ineffective. These technologies also do not provide control over sensitive outbound data posted to Web 2.0 sites.

Websense® Web Security Gateway solutions lead the Secure Web Gateway market by providing the best protection against modern Web 2.0 threats with the lowest total cost of ownership (TCO). They are the only solutions to provide enterprise-class data loss prevention and unified management of hybrid cloud/on-premise deployments. Web Security Gateway solutions enable organizations to leverage the power of Web 2.0 without worrying about Web malware, inappropriate content, or disclosure of sensitive information.

How It Works

Web Security Gateway solutions inspect inbound and outbound content as it traverses organizational boundaries to protect businesses from dynamic Web malware, prevent sensitive outbound data loss, and enhance employee productivity. Websense TruHybrid™ deployment supports on-premise appliance as well as Security-as-a-Service (SaaS) platforms, while managing the entire environment from a single policy and reporting infrastructure. Unlike alternative approaches, Websense customers have the flexibility to choose the platform or mix of platforms that best meets their specific operational requirements without incurring the cost of managing multiple systems.

Websense Web Security Gateway solutions offer:

- **Outbound Data Loss Prevention and Compliance Controls** – Built-in enterprise-class data loss prevention establishes the controls needed to enable outbound communications to destinations like Web mail and social networks, while meeting compliance mandates to control disclosure of sensitive data.
- **Malware Protection** – The Websense TRITON™ Advanced Classification Engine (ACE) protects against legacy file-based attacks as well as dynamic, scripted attacks that circumvent traditional antivirus solutions.
- **Web 2.0 Employee Productivity** – The TRITON Advanced Classification Engine removes inappropriate content from complex, dynamic, and password-protected Web 2.0 sites that cannot be accurately classified by traditional URL filtering solutions.
- **Lowest Total Cost of Ownership (TCO)** – The Websense TRITON Console and TruHybrid deployment reduce the number of appliances, management systems, and vendors that must be supported across the enterprise.
- **Consistent, Enterprise-Wide Security Coverage** – TruHybrid deployment unifies policy across on-premise and SaaS deployments. As users move between locations or work at home, their unique policy is consistently enforced.

“90 percent of the top 100 Web sites are classified as social networking or search and more than 47 percent of these sites support user-generated content.”

Websense Security Labs™, 2009

“In the first half of 2009, more than 80 percent of the top 100 sites either hosted malicious content or contained a masked redirect to an illegitimate Web site.”

Websense Security Labs, 2009

Advanced Classification Engine

Websense Web Security Gateway solutions include the Websense TRITON Advanced Classification Engine (ACE), the most accurate* bidirectional security analysis engine that combines inbound analytics with deep, outbound data loss prevention. ACE combines both traditional security with cutting-edge content classification techniques such as antivirus, URL filtering, reputation services, and fingerprinting to accurately classify inbound and outbound risks. The Advanced Classification Engine, supported by the Websense ThreatSeeker® Network, analyzes content as it traverses the gateway with real-time security scanning, real-time content classification, and enterprise-class data loss prevention.

Real-Time Security Scanning

Antivirus technology alone cannot keep pace with the dynamic and scripted attacks that dominate the Web threat landscape. Websense proprietary real-time security scanning analytics address these “zero day” threats by identifying malicious content “on the fly,” without the need to reference previously known attack databases.

Real-Time Content Classification

Many of the most commonly used sites cannot be accurately classified by traditional URL filtering. For example, a single Google or Facebook page may contain a mix of content elements spanning multiple categories — making it impossible to apply any single category. As a result, many organizations are forced to either indiscriminately block valuable resources, or ignore acceptable use policy by allowing full access to dynamic Web 2.0 destinations.

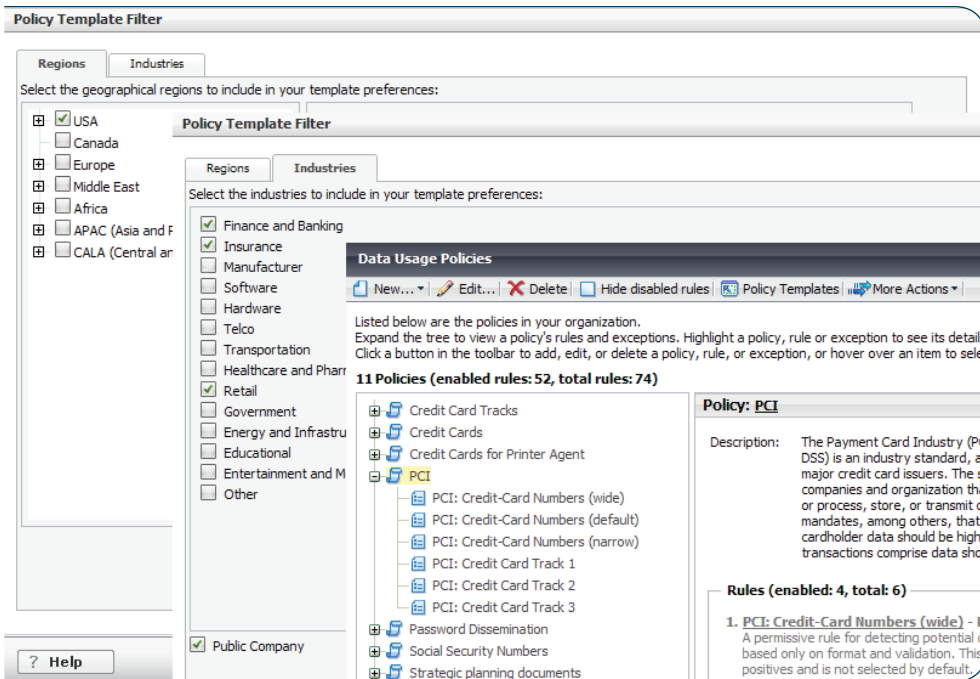
Web Security Gateway solutions offer real-time content classification to accurately extend acceptable use policies to dynamic Web 2.0 sites by classifying content elements within each Web page “on the fly.” If an individual content element violates policy, it can be stripped from the page while compliant information is allowed. This unique capability enables broad access to Web 2.0 business destinations while maintaining productivity and acceptable use policy compliance.

Enterprise-Class Data Loss Prevention

Built-in enterprise-class data loss prevention (DLP) establishes the controls needed to enable outbound business communications to destinations like Web mail and social networks, while meeting compliance mandates to control disclosure of sensitive data. Unlike alternative approaches whose DLP capabilities are limited to keyword inspection or require complex third-party integrations, Web Security Gateway solutions deliver all of the capabilities of the Websense market-leading DLP solution for http, https, and FTP network traffic. It includes over 800 out-of-the-box policies, fingerprinting for deep content inspection, and comprehensive compliance reporting.

Web DLP integration with Web Security Gateway solutions significantly reduces TCO by eliminating the need for dedicated, third-party DLP hardware at each corporate location. For organizations with longer-term plans for data loss prevention, Web DLP also provides solid investment protection — a simple software upgrade is all that is needed to extend control beyond the Web to include other traffic types (email, IM, P2P), endpoints, and data at rest (e.g., databases, file shares, Exchange, Share Point). Therefore, extending coverage from Web DLP to other channels does not require a rebuild. Existing policy and infrastructure investments are preserved.

* <http://www.websense.com/content/tolly-report-reg.aspx>



Simple DLP policy wizards help administrators rapidly define best practice policies that meet regional and industry-specific regulatory requirements.

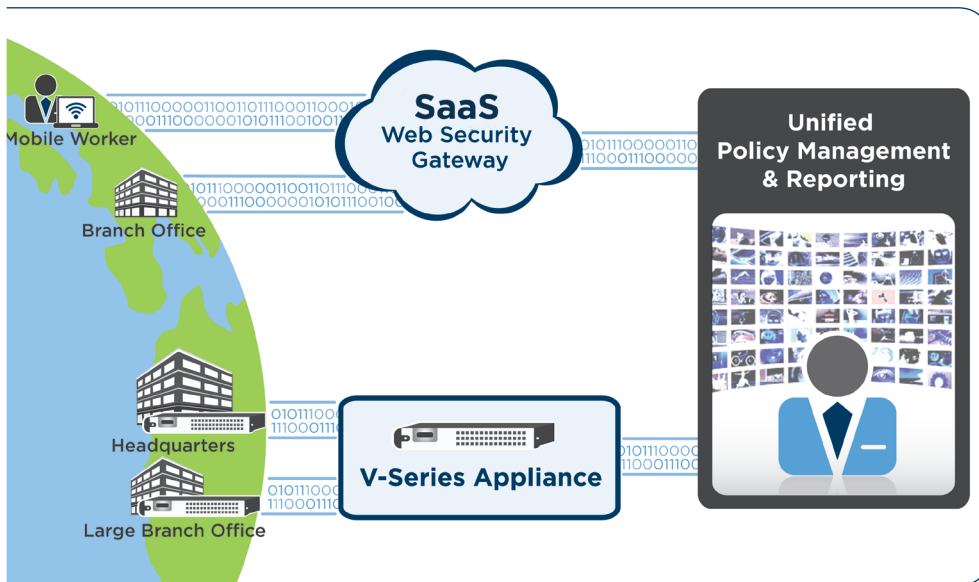
“We rely on the Websense V10000™ secure Web gateway appliance to enable our nurses to quickly get the information they need safely and securely. With the real-time scanning and the ability to create flexible policies around Internet use, I don’t worry about our field nurses encountering a Web site that has been compromised with data-stealing malicious code or accidentally sending confidential patient data to the wrong place.”

Larry Whiteside

Chief Security Officer
Visiting Nurse Service of New York

TruHybrid Deployment

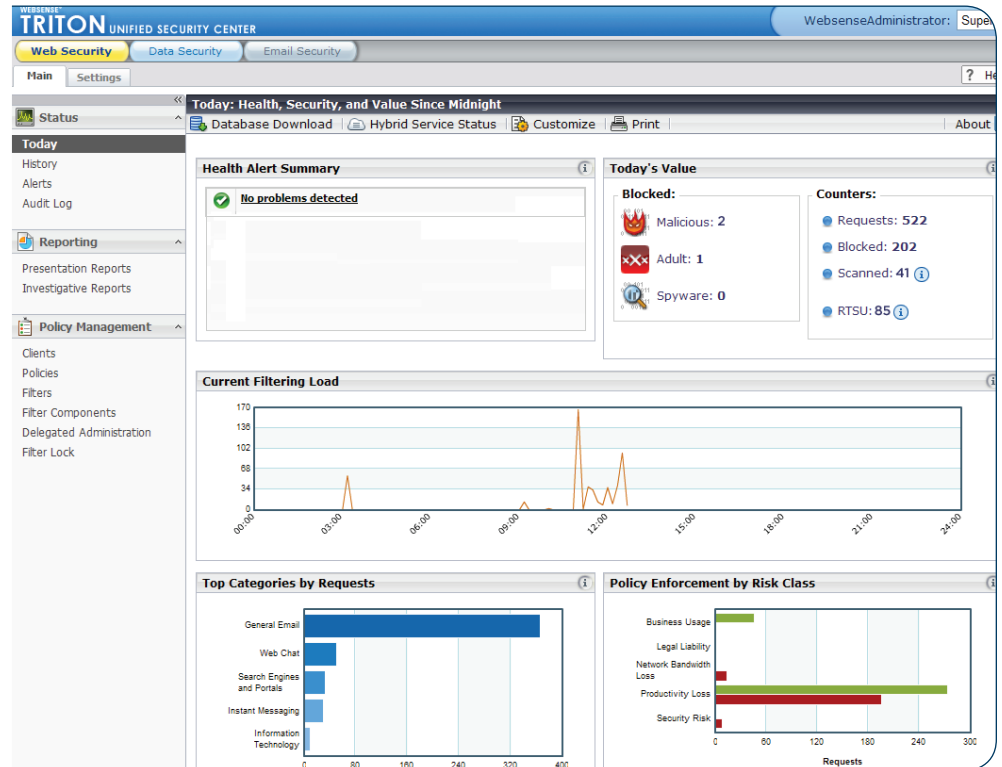
TruHybrid deployment provides the flexibility to select a mix of on-premise and SaaS deployment platforms, while managing the entire environment with a unique unified management system. You can extend security to branch offices or mobile users by leveraging the SaaS platform. At the same time, you can deploy high-performance appliances at corporate, large branch, or data center locations. Regardless of the mix of SaaS or appliance options chosen, you define a single enterprise-wide policy in one place. This unified approach not only cuts the cost of managing hybrid on-premise/SaaS deployments but also ensures consistent security coverage across all environments.



TruHybrid deployment unifies management of hybrid on-premise/SaaS deployments.

“As much as 57 percent of malicious Web attacks include data-stealing code.”

WebSense Security Labs, 2009



TRITON Console interactive dashboards provide instant access to threat and policy violation activity as they happen.

SSL Visibility and Control

The increasing use of SSL traffic has created blind spots for legacy URL filters and opens backdoors for threats and data loss. Web Security Gateway solutions provide visibility and control over SSL traffic allowing organizations to apply policy to all Web communications.

Advanced Application Controls

The growth of network applications such as IM and P2P provides hackers with a means to disrupt business and steal confidential data. Web Security Gateway solutions control more than 125 network protocols and thousands of applications to mitigate risk and prevent data loss from unauthorized applications. Policy actions extend from simple application blocking to highly granular bandwidth controls.

Unified Content Security Management and Reporting

A significant feature also available with Web Security Gateway solutions, and only available through Websense, is the TRITON Console. It consolidates management of all Websense Web, data, and email security solutions into a single Web-based interface. An intuitive dashboard includes over 55 built-in reports and extensive customization capabilities to help illuminate user activity, facilitate troubleshooting, and further reduce risk. Administrative effort and cost is greatly reduced relative to competing solutions due to numerous easy-to-use features, including extensive drill-down capabilities, policy wizards, configuration templates, a scheduling sub-system, and automatic content updates. As content security needs expand beyond Web security over time, the unified management capabilities of the TRITON console can be easily extended to centrally manage email and full DLP.

Features	Benefits
TruHybrid Deployment	Reduces total cost of ownership (TCO) and ensures consistent policy across the enterprise through unified management of on-premise and SaaS deployments.
Enterprise-Class Data Loss Prevention	Prevents outbound data loss and establishes required compliance controls. Lowers TCO by avoiding a complex DLP deployment.
Real-Time Content Classification	Secures use of dynamic, password-protected, and mixed content Web properties through Web content filtering "on the fly."
Real-Time Security Scanning	Protects organizations from Web malware by identifying dynamic, scripted, and unknown threats "on the fly."
TRITON Console	Reduces TCO and vendor management costs through unified management of Web, data and email security solutions.
Integrated Antivirus	Protects against file-based virus attacks using both third-party and advanced Websense Web antivirus.
Leading Web Filtering with Advanced Reputation Analytics	Enables baseline acceptable use policy and blocks known malicious sites. Multipoint reputation analytics include property type, lexical reputation, Web 2.0 posts, URL category, nearest neighbor, search reputation, history, age, and geography.
ThreatSeeker Network Real-Time Updates	Reduces exposure to emerging threats by delivering security updates every five minutes.
SSL Visibility	Enables inspection of encrypted Web traffic with full SSL proxy and integrated certificate management.
Application Control	Minimizes risk, enhances productivity, and lowers bandwidth cost by managing use of network protocols and applications.
Enterprise-Class Web Proxy /Cache	Improves performance and reduces bandwidth cost by optimizing traffic. Supports both transparent and explicit proxy configurations.
Flexible User Authentication	Enables user and group-based policy with flexible authentication via Active Directory, LDAP, RADIUS, Novell,NTLM v2.
High Availability and Load Balancing	Enables system redundancy and large-enterprise scalability leveraging WCCP or external load balancers.

Websense is positioned in the leaders quadrant by Gartner in their most recent Magic Quadrant for Secure Web Gateway.

Gartner, Inc.

"Magic Quadrant for Secure Web Gateway"* by Peter Firstbrook and Lawrence Orans
January 8, 2010

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

Websense UK, Ltd.
Reading, Berkshire UK
tel 0118.938.8600
fax 0118.938.8697
www.websense.co.uk

Australia
websense.com.au

Brazil
websense.com/brasil

Colombia
websense.com/latam

France
websense.fr

Germany
websense.de

Hong Kong
websense.cn

India
websense.com

Ireland
websense.co.uk

Israel
websense.com

Italy
websense.it

Japan
websense.jp

Malaysia
websense.com

Mexico
websense.com/latam

PRC
prc.websense.com

Singapore
websense.com

Spain
websense.com.es

Taiwan
websense.cn

UAE
websense.com

Deployment Platform Availability

On-premise deployments can be implemented with Websense V-Series™ appliances or with software running on general purpose servers. SaaS deployments are supported with the Websense Hosted Web Security Gateway solution.

- **V-Series Appliances** V-Series appliances deliver enterprise-class performance, reliability, and simple deployment for on-premise deployments. Proven in Fortune 100 environments, V-Series appliances integrate component-level redundancy while supporting an array of enterprise deployment features, including load balancing and high availability. V-Series appliances are also designed to support future Websense solutions without upgrading hardware — extending the life and value of the platform.
- **Hosted Web Security Gateway** Websense Hosted Web Security Gateway solutions shift security inspection processes to 10 globally available and redundant data centers located “in the cloud.” This SaaS delivery model not only accelerates deployment, but it can significantly reduce operational costs by eliminating the need to support on-premise hardware at each corporate location. Websense data centers are ISO 27001 certified to meet the strict security and availability standards that would be extremely costly for individual organizations to match on premise, especially at remote office locations. When deployed as a standalone SaaS-only solution, Websense Hosted Web Security Gateway offers the optional added benefit of SaaS email security integration.



The Websense V10000™ Appliance

Websense Web Security Gateway Solution Options

Websense Web Security Gateway Anywhere — For deployments requiring TruHybrid on-premise*/SaaS management, enterprise-class Web data loss prevention, or the Websense Remote Filtering client.

Websense Web Security Gateway — For on-premise* deployments.

Websense Hosted Web Security Gateway — For SaaS deployments.

Minimum Server Requirements for Software Deployments:

Operating System

Red Hat Linux v4,
update 5* or Windows Server 2003/
Server 2008†

CPU: 2 x Dual-core 2.8GHz processors

Memory
4GB RAM

Hard Disk Drive

Two physical disks:†

* 100GB for OS and application and

temporary data, 100GB for cache*

* 100GB (recommended RAID 1)†

Network interfaces

Two x 10/100/1000 Ethernet interfaces

* On-premise deployments may be implemented on Websense V-Series appliances or as software running on general purpose servers.

†The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

websense®
ESSENTIAL INFORMATION PROTECTION™

For an online product demonstration or a free evaluation of Websense Web Security, visit www.websense.com/evaluations.

© 2010 Websense, Inc. All rights reserved. Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other registered and unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners. 02.01.10