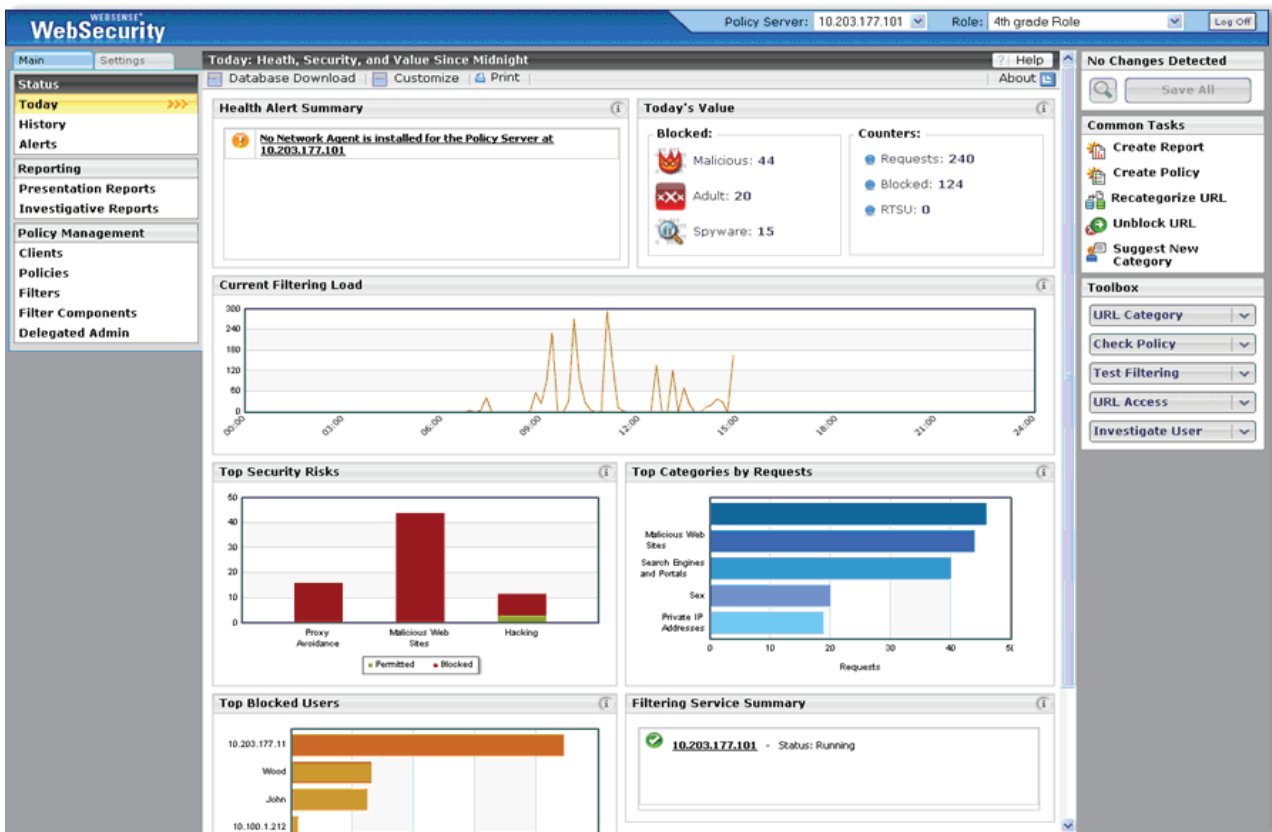


Web Security v7 and Web Security Gateway FREQUENTLY ASKED QUESTIONS



Web Security v7: New Web-Based Security Dashboard

CONTENTS

3 WHAT IS IT?

3 OVERVIEW

4 WHAT'S INCLUDED IN WEBSense WEB SECURITY V7?

5 WHAT'S INCLUDED IN THE WEBSense WEB SECURITY GATEWAY?

6 AVAILABILITY

6 RELEASE SCHEDULE

6 PRICING

6 DEMOS AND TECH PREVIEWS

6 PRODUCT FEATURES

6 WEBSense WEB SECURITY V7 FEATURES

7 WEBSense WEB SECURITY GATEWAY

9 POLICY CREATION AND REPORTING IN V7

9 LOCALISATION

9 PLATFORM & DEPLOYMENT

9 NETWORK ARCHITECTURE

9 CONTENT GATEWAY DEPLOYMENT

10 HARDWARE OPTIONS

10 PERFORMANCE

10 SCALABILITY

10 UPGRADES & INTEGRATION

10 UPGRADE PATHS

11 INTEGRATION WITH WEBSense DATA SECURITY SUITE

11 THIRD-PARTY PRODUCT INTEGRATIONS – FIREWALL/WEB PROXY

12 COMPETITIVE DIFFERENTIATORS

12 WEBSense VS. ALL SECURITY VENDORS

12 WEB SECURITY GATEWAY VS. ANTIVIRUS OR OTHER TECHNOLOGIES

WHAT IS IT?

OVERVIEW

The launch of Web Security v7 and the new Web Security Gateway includes:

- **Web Security v7:** a major update to the world's leading web security line of products including a redesigned Web-based UI and dashboard, delegated administration, selective authentication and a host of other new and enhanced features.
- **Web Security Gateway:** a new flagship product for Websense that incorporates Web Security v7 plus a new Content Gateway Module, providing real-time, inline analysis of dynamic content and Web 2.0 threats.

All existing Websense Enterprise and Websense Web Security Suite customers can benefit from this release. This document answers the major questions around this latest release.

This launch includes:

A. New product names

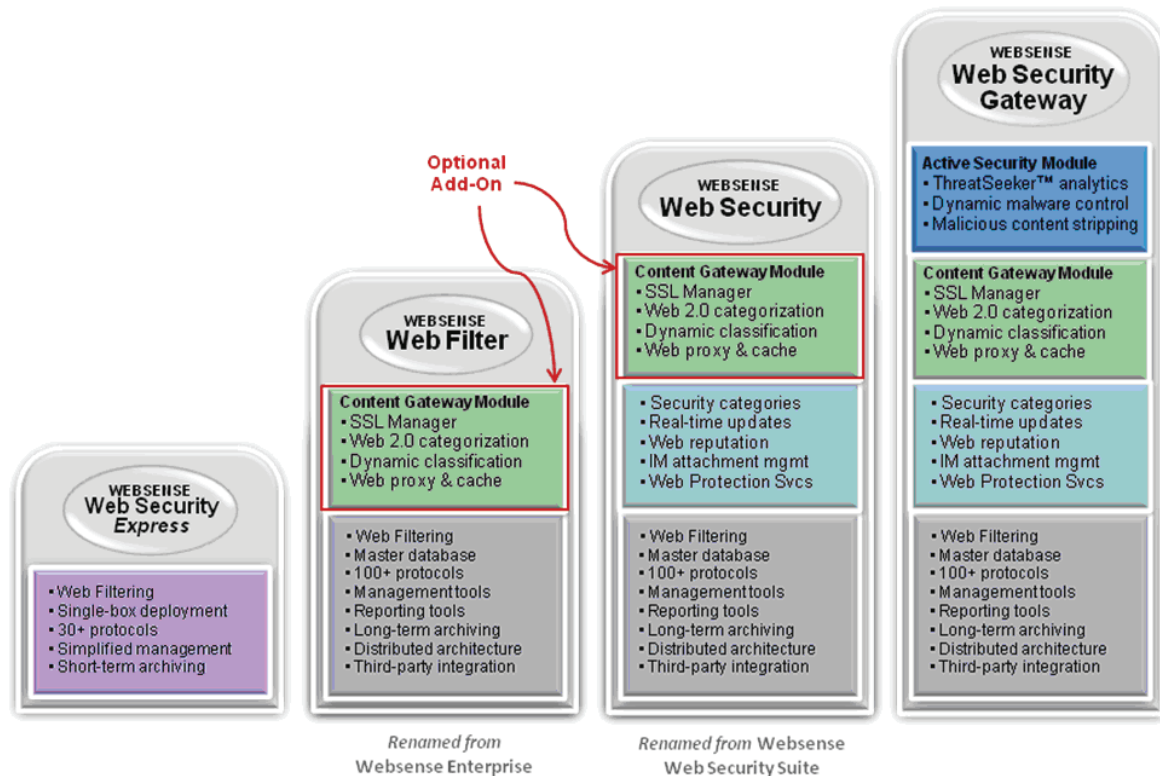
1. **Websense Express** changes to **Websense Web Security Express**
2. **Websense Enterprise** changes to **Websense Web Filter**
3. **Websense Web Security Suite** changes to **Websense Web Security**

B. An available upgrade at no additional charge to v7, for all Web Filter (Enterprise) and Web Security (Suite) customers;

C. A **new** add-on option – the Content Gateway Module, available for additional cost to Web Filter (Enterprise) and Web Security (Suite) customers;

D. A **new flagship product** – the **Websense Web Security Gateway**, that includes all functionality found in Web Filter, Web Security, and Content Gateway Module, as well as an additional Active Security Module. Upgrades to the full product will be available at additional cost for Web Filter (Enterprise) and Web Security (Suite) customers.

The following diagram shows the new and renamed products as they will be available at the GA date.



WHAT'S INCLUDED IN WEB SECURITY V7?

V7 of our Web Security products is a major update that will be offered at no charge to existing Websense Enterprise and Websense Web Security Suite customers with an active subscription.

V7 improves and expands the capabilities of the world's leading Web filtering and security products; enabling customers to save time and resources by quickly and easily identify security issues and access custom reporting all within a single screen. Coupled with the ability to discover potential issues with the deployment as well as suggested solutions, Web Security v7 increases the security level while reducing the management overhead.

Major enhancements in v7 include:

- New intuitive web-based interface replacing the existing Java-based interface
- Management Dashboard to view reporting and security incidents in a single view
- System Health Monitor
- User, Policy & lookup tools
- Improved usability with management and reporting tools now integrated into a single interface
- Selective Authentication
- Re-designed Delegated Administration

For more details, see the **Web Security v7 Features** section.

WHAT'S INCLUDED IN THE WEB SECURITY GATEWAY?

The Websense Web Security Gateway allows you to effectively secure Web traffic while still enabling the latest web-based tools and applications. Through a multi-vector traffic scanning engine, the Web Security Gateway analyses Web traffic in real-time – instantly categorising new sites and dynamic content, proactively discovering security risks and blocking dangerous malware.

Backed by Websense's powerful ThreatSeeker Network, the Web Security Gateway provides advanced analytics (rules, signatures, heuristics and application behaviors) to detect and block proxy avoidance, hacking sites, adult content, botnets, key-loggers, phishing attacks, spyware, and many other types of unsafe content. The Web Security Gateway also closes a common security gap – decrypting and scanning SSL traffic before it enters your network.

These real-time capabilities are tightly integrated with Websense's industry-leading Web Security platform providing Web filtering with over 90 categories, Web reputation, control over 120 network and application protocols, IM attachment management, and more.

Included in the Web Security Gateway is an all-new, easy-to-use management dashboard that provides system details, statistics, policy management, logging and reports needed by administrators in a single interface – saving time and effort while reducing errors that can lead to security breaches.

Websense Web Security Gateway contains all of the features of Web Filter, Web Security, as well as the following:

Content Gateway Module

- SSL decryption/encryption
- Automatic categorisation of dynamic Web 2.0 sites
- Automatic categorisation of new unclassified sites
- Proxy/cache

Active Security Module

- Inline analysis of new threats using ThreatSeeker™ analytics
- Dynamic malware control
- Malicious content stripping

Both of these modules require the installation of the Content Gateway Module as a proxy with visibility to HTTP and HTTPS traffic. See the "Platform and Deployment" for more information.

For more details, see the **Web Security Gateway Features section**.

AVAILABILITY

RELEASE SCHEDULE

General Availability, including product evaluations, is scheduled for late September 2008.

PRICING

- Existing Websense Enterprise customers can migrate to Web Filter v7 at no additional cost
- Existing Web Security Suite customers can migrate to Web Security v7 at no additional cost

Web Filter and Web Security customers will also have an add-on or migration option available when the product is generally available (scheduled for late September, 2008):

1. Add the **Content Gateway Module** (includes SSL, dynamic classification, proxy cache)
2. Upgrade to the full **Web Security Gateway** (includes the CGM + the Active Security Module)

For pricing details, please contact your Websense Reseller who will be able to assist you.

DEMOS AND TECH PREVIEWS

- **Online Product Demo:** provides a detailed 15 minute walk-through of the product delivered by senior product managers and engineers. (There is also a 2-minute 'Preview' option). This demo is available on the Websense corporate site at: http://www.websense.com/welcome/MiscLandings/regPage/WWSG/web_security_gateway_register.php (registration is required).
- **Weekly Live Demos:** A weekly webcast, providing an interactive view of the product, with time for Q&A. Please register in advance for these demos at: http://www.intlwebsensemarketing.com/uk_webcasts/register.html

PRODUCT FEATURES

WEB SECURITY V7 FEATURES

Web-based interface

The existing Java-based interface has been replaced with a new web-based interface. Many of the new interface screens strongly resemble the existing interface, enabling existing customers to quickly adapt to the interface; however the look and feel, and usability of the interface overall has been greatly improved.

The new interface combines policy creation, management and reporting, making it a much simpler task to administer the product, saving IT administrators time and effort.

New Management Dashboard

Incorporated into the new interface is an easy-to-use dashboard that allows administrators to view all the critical information regarding their Websense solution in a single view. This includes Health Checks, security statistics, user and network reporting.

There are two main dashboard views, Today – which is the current day activity, and History – which is the past 30 days. These two views give administrators information at their fingertips to evaluate network and user behavior, policies, and make any changes as may be required.

Delegated Administration

Delegated Administration, a highly regarded feature by many of our customers, has been significantly improved in this release. Delegated Administration allows companies to divide control over their Internet security, network and users between different individuals or groups.

For example, in a school system, the school administrator might impose a general Web security policy, but allow each teacher the ability to edit policies and view reports as required for only the individuals in their specific grade or class. In this way, each grade has control over their policy and reporting without impacting other grades or having the ability to edit the global policy settings.

Selective Authentication

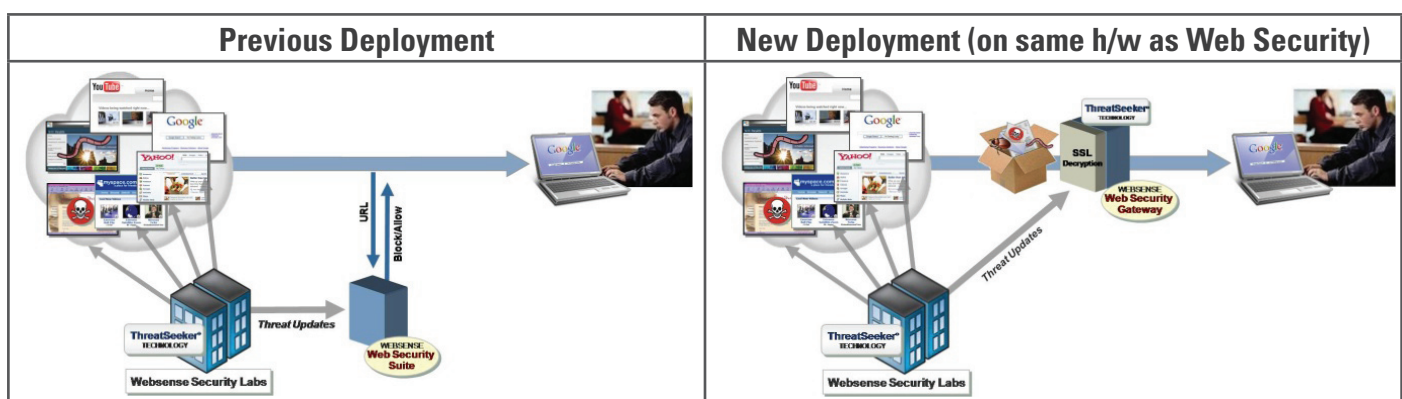
Another new feature that has been implemented in this v7 release is Selective Authentication. This feature allows end-user specific policies to be correctly applied to individual users based on their username and login, in cases where multiple individuals with different levels of access privileges share a single machine.

For example, in a hospital, there might be publicly available computers that patients or doctors use for general Internet access – maybe to check webmail or browse the Internet. When doctors log in to the system, they will get the doctor’s policy – allowing them to gain access to specific, restricted content; however when patients use the machine, they will get more restrictive policy and privileges designated for them.

WEBSense WEB SECURITY GATEWAY

Content Gateway Module

The Content Gateway Module offers new functionality to our web security customers and should be deployed on a different hardware platform to the Web Filter/Web Security software. This module must be deployed in line with traffic – this is a change in deployment scenario for our current customers.



The Content Gateway Module offers the following functionality:

Content analysis of encrypted SSL traffic: Encrypted traffic can be a back door to any security policy if the content cannot be analysed to verify that it fits to the defined security policy. The Content Gateway Module enables the decryption of SSL traffic, to allow content analysis, followed by the re-encryption of the traffic to complete the communication – the module sits in the middle of the SSL transmission.

Categorisation of Web 2.0 websites and applications: Classification for traditional filtering categories (e.g. “Travel”, “Sports”, “Adult Content”, etc.) by extracting Web page elements (e.g. natural language, images, colors, fonts, titles, backgrounds, etc.) and classifying the content in real-time using Websense proprietary machine learning algorithms based on 15 years’ of Web research.

Dynamic classification: Using automated algorithms, developed by Websense Security Labs, unclassified websites can be analysed. The algorithms are looking for hints and pointers that would indicate the category of an unclassified website. By identifying these sites, the increased level of security of Websense customers can be maintained.

Proxy/cache functionality: The enabling functionality behind the features above is a Web proxy. This has been developed from software purchased from Inktomi and is based on a mature proxy product. Our proxy can be deployed in either explicit or transparent mode.

Active Security Module

The Active Security Module, which is built on top of the Content Gateway Module, offers the ability for our customers to securely leverage Web 2.0 technology. Built using some of the ThreatSeeker analytics, the Active Security Module can scan Web content to identify and block malicious code in real-time.

This functionality is especially important when you consider the rise in adoption of Web 2.0 and the fact that over 45% of the Top 100 sites are 100% user-contributed, and therefore, there are lower levels of security compared to fully-regulated sites such as www.espn.com.

The Active Security Module provides real-time, security-focused analysis of threats like “Spyware”, “Phishing”, etc. The Active Security Module extracts the “active” elements (e.g. scripts, exploits, binary code, images, etc.) of Web content that can trigger unwanted activity. It can also dynamically categorise emerging and unknown malicious websites.

The real-time analytics engine can logically join together any number of elements into an attack profile. For a simple example, if a Web page:

- is located on a social networking site AND
- has forms for “login” and “password” AND
- has a logo or keywords that are trying to associate these forms with a financial institution

THEN given that no bank hosts authentication credentials on social networking sites, the page is almost certainly trying to steal banking information and can be categorised as a Phishing site. It is important to note that this is not a specific detection for a specific attack but rather generalises to an entire class of phishing attempts (financial credentials on social networking sites). Our real-time security scanning currently supports hundreds of profiles for other attack classes, including attacks on instant messaging, program files, Web 2.0 applications and a number of others.

In this way, malicious code can be blocked while legitimate content is allowed to enter the network.

POLICY CREATION AND REPORTING IN V7

All policy creation and reporting is integrated into the single web-based user management interface.

LOCALISATION

The Websense Content Gateway will be available only in English. For Websense Web Filter and Web Security we will “support” (install on) ten languages: English, Spanish, French, German, Italian, Korean, Simplified Chinese, Traditional Chinese, Brazilian Portuguese, and Japanese. Note, however, that not all components are localised, notably the management UI and reports. We localise elements such as block pages, categories, protocols, etc.

PLATFORM & DEPLOYMENT

NETWORK ARCHITECTURE

To picture the architecture of this solution, consider two separate elements:

- a. Websense Web Filter/Websense Web Security
- b. Content Gateway Module/Active Security Module

For existing customers upgrading to v7, but not adding either module, the network architecture and deployment remains exactly as it is today – no changes are needed.

For existing customers upgrading to v7 or the Web Security Gateway, any existing hardware that is deployed for the Websense solution remains in place. A new hardware platform is required for the Content Gateway/Active Security Module. This platform has to be placed in line with traffic.

CONTENT GATEWAY DEPLOYMENT

It is recommended that the Content Gateway is deployed at the WAN access points of the network, behind any existing network firewall.

HARDWARE OPTIONS

The Content Gateway/Active Security Modules require either general purpose server hardware or an appliance. The minimum specification for a general purpose server is calculated to be:

| Content Gateway/Active Security Module | Web Filter/Web Security & Reporting |
|---|---|
| <p>Operating System: Red Hat AS Enterprise Linux v4, update 5 (kernel module 2.6.9-55.ELsmp)</p> <p>CPU: 2 x Dual-core 2.8GHz processors</p> <p>Memory: 4GB RAM</p> <p>Disk space: Two physical disks – 100GB for OS and Application and temporary data 100GB for cache</p> <p>Network interfaces: Two – 10/100/1000 Ethernet interfaces</p> | <p>Operating System: Windows 2003 Server</p> <p>CPU: 2 x Dual-core 2.6GHz processors</p> <p>Memory: 4GB RAM</p> <p>Hard Disk Drive: 100GB, (recommended RAID 1)</p> |

Although it is likely that some appliance hardware will be certified to run this software, there is currently no platform that has been certified.

PERFORMANCE

We do not yet have final performance numbers, and performance will vary depending on the hardware platform chosen. We currently offer guidance for an expected minimum system specification for the Content Gateway Module (in line with traffic), which is as shown in **Hardware & Appliance Options section**.

SCALABILITY

All Websense products are enterprise focused and designed to be scalable to support some of the largest organisations – Websense Web Security Gateway is no exception. Depending on the choice of hardware platform, there are several options for scalability and redundancy including support of third party solutions such as load balancers and L4 switches.

UPGRADES & INTEGRATION

UPGRADE PATHS

Web Security Suite or Websense Enterprise to v7

To upgrade to v7, customers need to be using a minimum of v6.2. Customers using product older than this will need to upgrade to at least v6.2 before being able to upgrade to v7. No new hardware is required.

Web Security Suite or Websense Enterprise + Content Gateway

To upgrade to v7, customers need to be using a minimum of v6.2. Customers using product older than this will need to upgrade to at least v6.2 before being able to upgrade to v7. New hardware will need to be deployed for the Content Gateway Module.

Web Security Suite to Web Security Gateway

To upgrade to the Web Security Gateway, it is recommended that customers should be using a minimum of v6.2. Customers using product older than this will need to upgrade to at least v6.2 before being able to upgrade to v7. It is also possible to carry out a fresh install of the Web Security Gateway.

New hardware will need to be deployed for the Content Gateway Module & Active Security Module. See **Hardware & Appliance Options section** for more details.

Websense Enterprise to Websense Web Security Gateway

To upgrade to the Web Security Gateway, it is recommended that customers should be using a minimum of v6.2. Customers using product older than this will need to upgrade to at least v6.2 before being able to upgrade to v7. It is also possible to carry out a fresh install of the Web Security Gateway.

New hardware will need to be deployed for the Content Gateway Module & Active Security Module. See **Hardware & Appliance Options section** for more details.

INTEGRATION WITH WEBSense DATA SECURITY SUITE

Websense inbound Web filtering and Web security products work tightly with Websense outbound data controls for DLP. This functionality is packaged as an additional module and set of modules that can be combined with any Web security deployment. The functionality includes more than just DLP for the Web channel. It includes visibility and control of data by user and by category. This allows an organisation selective blocking and more granular reporting. For example, users may be allowed to visit blogs or social networking sites, but they can simultaneously be blocked from posting sensitive data from those types of destinations. Or, a particular user group may be allowed to post sensitive financial data to a partner, but no other group is allowed to post that data anywhere on the Web.

THIRD-PARTY PRODUCT INTEGRATIONS – FIREWALL/WEB PROXY

Websense Web security solutions integrate with a large number of partner solutions including firewalls and Web proxies. Some customers use Websense “on-box” with one of our integration partners (such as Juniper or Blue Coat) – these customers will need to migrate to an “off-box” solution in order to take advantage of the increased functionality in v7.

For existing customers who are upgrading to v7, nothing changes with their existing integration.

For existing customers upgrading to either the Content Gateway Module or the Web Security Gateway, it is recommended that the Content Gateway element of the solution be located behind the existing firewall/ Web proxy. Although the Content Gateway could replace an existing Web proxy, proxy chaining the Content Gateway behind the existing Web proxy will show how many threats are getting through the existing proxy, and therefore, the value of our solution.

It is also important to point the existing off-box solution to the Content Gateway rather than the existing firewall/Web proxy. In essence, the integration is being moved to the Content Gateway – this integration can provide a higher level of functionality and security.

THIRD PARTY INTEGRATIONS – AUTHENTICATION

There are no changes to any existing integrations with authentication services such as LDAP or Active Directory.

COMPETITIVE DIFFERENTIATORS

WEBSense VS. ALL SECURITY VENDORS

- **Adaptive protection** using our ThreatSeeker Network™ on-box via real-time scanning or proactively in-the-cloud via our Internet HoneyGrid™; backed by a dedicated 24x7 global security research team that developed the patent-pending technologies
- **Simple control** requiring only one deployment and one integrated Web-based management and reporting user interface to monitor dashboards, delegate role-based control to managers, configure user policies, set alerts and investigate incidents
- **Complete visibility** of legal, bandwidth, productivity and security risks by analyzing the dynamic Web content, executable code, site category and reputation of all Web-based communications via any port, 120+ protocols, SSL-encrypted, and Web 2.0 technology

WEB SECURITY GATEWAY VS. ANTIVIRUS OR OTHER TECHNOLOGIES

- **Antivirus engines** rely on signature and heuristic techniques that detect threat payloads impacting the endpoint, no matter if the technology is deployed at the endpoint or Web gateway. Signatures are reactive and create a window of exposure to emerging attacks, while heuristics are too passive reducing false positives, but increasing false negatives.
- **Web-based security** requires proactive discovery of threats on the Web – active or staged, known or unknown – analyzing not only the payload, but the vector that exploits vulnerable Web 2.0 technologies (i.e. social network widgets, iFrames) or blended communications (i.e. IM or email links). Content classifiers are continuously developed and adapted by security researchers in-the-cloud and then pushed to the Web gateway.

For a demonstration or evaluation go to websense.com/downloads

Websense UK Ltd, Reading, Berkshire UK. Tel: +44 (0) 1260 296200 Fax: +44 (0) 118 938 8697 www.websense.co.uk