Websense®
Hosted Email Security

Today's email threat landscape is dominated by converged email and Web attacks with over 85 percent of unwanted email now containing an embedded URL. Organizations are also facing increasing risks associated with loss of data and violations of acceptable email use. And while email threats are becoming increasingly complex, managing email security doesn't have to be.

Websense® security-as-a-service (SaaS) email integrates best-in-class Web security and data security technology with email security to achieve unparalleled visibility into emerging threats and one of the highest levels of protection from inbound and outbound email security risks. This easy-to-manage service provides highly accurate protection against spam, viruses, spyware, phishing, and converged email and Web threats. Pre-defined content dictionaries help make it simple to prevent data loss, meet regulatory requirements, and enforce policies on acceptable email use.

> "Having our email controlled in the cloud [with Websense Hosted Email Security] takes the load off our in-house servers and eliminates the need for any day-to-day management."
>
> **Terry Kemp**
> Infrastructure Manager
> Nelson Marlborough
> District Health Board

How It Works:

Protecting email with Websense® Hosted Email Security is easy. Simply point MX records to the Websense datacenters and all email is filtered before it reaches the network, providing significant bandwidth and storage savings. Websense data centers are load balanced, redundant, highly available clusters located in 10 locations worldwide. The service provides a SLA-backed availablility of 99.999 percent and is certified to ISO27001 standards to provide the highest degree of global and localized security, privacy, and confidentiality.

Websense security as a service for email security enables customers to:

- **Reduce business costs and complexity** with no on-site equipment to install or maintain, savings in bandwidth and storage, predictable costs, and reduced administrative overhead.
- **Increase protection** with leading security from converged email and Web threats backed by industry-leading SLAs and the power of the Websense ThreatSeeker™ Network.
- **Retain control** with 24x7 access and flexible customization of policies, configuration settings, quarantine management, and reporting.
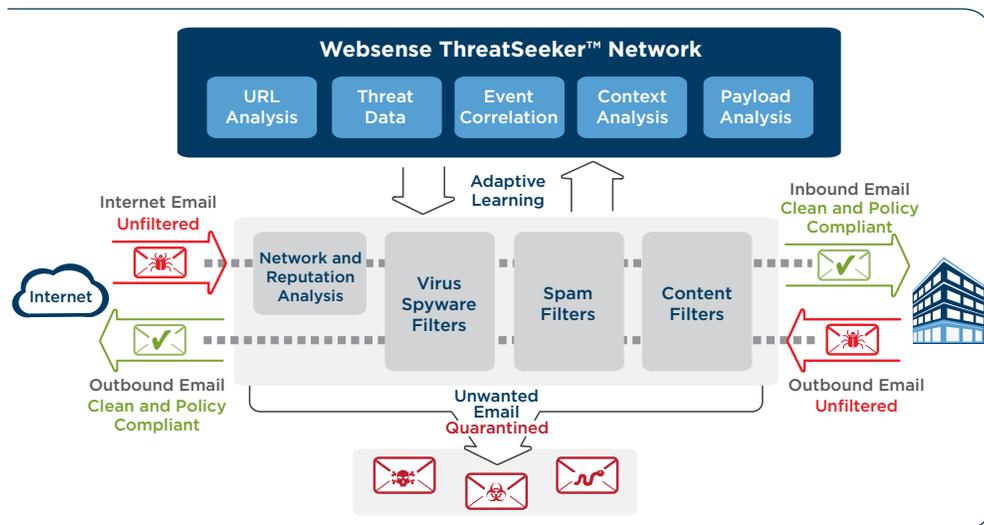
Hosted Email Security Service Overview

websense®
ESSENTIAL INFORMATION PROTECTION™

Hosted Email Security Capabilities

Hosted Email Security Packages	Antispam	Antivirus	Content FFilter	Encryption
Hosted Antispam	●			
Hosted Email Security	●	●		
Hosted Email Security and Content Control	●	●	●	●

Antispam

Websense provides highly accurate spam blocking with very low false positives that is backed by a 99 percent spam detection service level agreement. A combination of technologies is used to identify spam including sender reputation, adaptive learning, URL analysis, heuristics, digital fingerprinting, and optical recognition of image spam. Most importantly, it is the only solution that integrates Websense market-leading Web security technology to protect against phishing and converged email and Web threats. Each email is assigned an aggregate score, which is compared to a customer-defined threshold to determine what action should be taken.

Antivirus

Inbound and outbound email is scanned for viruses, spyware, and other forms of malware using a multilayered approach with multiple commercial antivirus engines and the Websense ThreatSeeker Network to protect against both known and unknown threats. ThreatSeeker provides zero-hour protection by continuously examining email and Web sites to detect trends and patterns that identify emerging threats—closing the window of exposure between a new malware outbreak and availability of a detection signature. The service is backed by as 100 percent known virus detection SLA.

Content Filter

Integrated technology from Websense market-leading data security solutions makes it easy to prevent data loss, meet regulatory requirements, and enforce policies on acceptable email use. Pre-defined dictionaries covering 20 topics in 12 languages plus built-in PCI-DSS and data privacy templates help organizations quickly identify and stop email policy violations. Unique inspection requirements can easily be met with advanced regular expressions and flexible policies. Violations are identified through in-depth inspection of both the email message and the content within the attachment. Messages can also be quarantined based on attachment true file type and deferred for later delivery based on size.

Encryption

Websense encryption secures email communications without sacrificing the ability to inspect encrypted email for malware and content violations. Websense supports server-to-server encryption using industry standard transport layer security (TLS) and ad hoc park-and-pull encryption for communicating to individuals. Encryption policies can be set up to encrypt communications based on sender, recipient, outlook sensitivity settings, or a keyword in the subject. Encryption can be in used conjunction with content filtering to encrypt emails that contain specific content, such as sensitive or confidential information.

Websense security as a service (SaaS) for email also works hand in hand with Websense SaaS Web to provide integrated email and Web protection enabling organizations to consolidate management and reporting for both Web and email security.

Websense ThreatSeeker™ Network

The Websense ThreatSeeker Network adaptive security technology uses more than 50 million real-time data collecting systems that continuously monitor Internet content—including new and dynamic content—for zero–hour protection from emerging threats. This research and intelligence is fed, in real-time, to the Websense solutions portfolio. As a result, Websense is able to adapt to the rapidly changing Internet at speeds not possible by traditional security solutions.

Features	Benefits
Spam and virus protection	Highly accurate SLA-backed protection against spam, viruses, spyware, phishing, and converged email and Web threats.
Zero-hour threat detection	Protection from the ThreatSeeker Network identifies and stops emerging threats to close window of exposure.
Data loss prevention	Integrated technology from Websense market-leading data security solutions prevents data loss and helps meet regulatory requirements.
Content filtering	Pre-defined content dictionaries covering 20 topics in 12 languages makes it easy to quickly identify email policy violations.
Encryption	Protect sensitive and regulated data with secure email communications to business partners and individuals
Security-as-a-service delivery	Save time and money with no equipment to install or maintain, built-in resilience, predictable costs, and reduced administrative overhead.
Top-tier global data center infrastructure	Ten global datacenters with fully redundant power, cooling, and Internet connectivity provide high availability with a 99.999 percent uptime SLA.
Security certifications	Independent audit and certification of security practices to ISO27001 ensures the highest level of security, privacy and confidentiality
24x7 access and support	Access and manage the service through a Web-based portal available anytime from anywhere on the Internet, with 24 x 7 support for extra help when you need it.
Email spooling for disaster recovery	Built-in redundancy and email spooling ensures that email is never lost when a customer experiences a network or mail server outage.
Quarantine management	Powerful message search engine provides complete visibility and access to quarantined messages and logs.
End user self service	Scheduled and on-demand user access to view and release quarantined messages, and whitelist/blacklist senders reduces administrative overhead.
Directory service integration	Automatic synchronization of email addresses and groups with Active Directory and LDAP simplifies policy management.
Roles-based administration	Separate access controls for quarantine management, viewing reports, accessing audit trail, and other key functions allow for delegated administration.
Directory harvest prevention	Built-in protection stops spammers from capturing valid email addresses.
Reporting	Over 40 different reports types with summary and detailed drill-down forensics provide 360-degree visibility into threat types and volumes, messages processed, policy violations, and more.

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
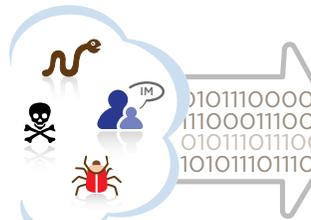websense.com/latam

PRC
prc.websense.com

Singapore
websense.com

Spain
websense.com.es

Taiwan
websense.cn

UAE
websense.com

Inbound Threats

Outbound Risks

Email Security

Web Security

Data Security

Built-in Web and Data Security Intelligence

- Spam
- Viruses
- Malicious URLs

- Data leaks
- Acceptable use
- Compliance

✓ ThreatSeeker
✓ Zero-Hour Intelligence
✓ URL Analysis

✓ Pre-Defined Dictionaries
✓ Deep Content Inspection
✓ Advanced Pattern Matching

Intelligent Email Security

Email Privacy

ISO 27001

Websense security as a service for email is independently audited and certified to the ISO 27001 standard to ensure the highest level of security, privacy, and confidentiality. ISO 27001 is an information security management system standard published in October 2005 by the International Organization for Standardization. This certification is widely accepted proof of the quality of an organization's security program and the most stringent security standard in the industry—exceeding the SAS 70 requirements, which many competitors claim as their certification benchmark.

Datacenter Security

Of all the places your email visits, Websense datacenters are among the safest locations that it can be routed to. Websense has built stringent security and privacy safeguards into the datacenter delivery network itself. Clean emails are not retained by the service, and other emails are only visible to those who have administrative rights into your system—specifically your network administrators and anyone else to whom you have given access to your account. Websense datacenters adhere to stringent physical security safeguards as well, including:

- 24 x 7 x 365 staffing
- Physical intrusion detection systems
- Video surveillance
- Restricted access lists
- Photo and biometric verification

Service Level Agreement Summary

Websense provides industry-leading SLAs to ensure the service performs to the highest levels.

- **Availability**—99.999 percent
- **Spam**—99 percent or higher detection rate
- **Viruses**—100 percent detection of known viruses
- **Processing Latency**—60 seconds or less for non-spam email less than two megabytes
- **Email logs and quarantine**—Available five minutes or less after email receipt

All SLAs are subject to the terms and conditions outlined in the customer service agreement.

websense®

ESSENTIAL INFORMATION PROTECTION™

For more information, to start a free trial of Websense email solutions, or to view an online demo, visit **www.websense.com/evaluations.**