



Websense encryption eliminates complex key management and the need for additional hardware and software.

Websense®

## Hosted Email Security Encryption Service

Websense® encryption is a policy-driven service that enables the secure delivery of email communications to business partners and individuals. Easy administration, no complex key management, and no additional hardware or software requirements eliminate the traditional cost and complexity barriers to implementing email encryption. Plus, full integration with Websense Hosted Email Security means you don't sacrifice the ability to inspect encrypted email for malware and content violations. Websense encryption provides a simple and cost-effective solution to help organisations comply with regulations and protect the confidentiality of sensitive information.

### How It Works:

Websense supports server-to-server encryption using industry standard transport layer security (TLS) and ad hoc push-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 used in conjunction with content filtering to automatically encrypt emails that contain specific content, such as sensitive or confidential information.

Websense encryption offers:

- **Automatic encryption of sensitive email** to meet regulatory requirements and ensure your confidential information stays secure.
- **Simple setup and management** with no complex key management, and no additional hardware or software required.
- **Web-browser-based access** for universal compatibility with mobile devices, operating systems, and email systems without the need for plug-ins.
- **Interoperability** with standard email gateways and industry-standard TLS encryption.
- **Malware and content inspection** of encrypted email to stop threats and prevent data loss.

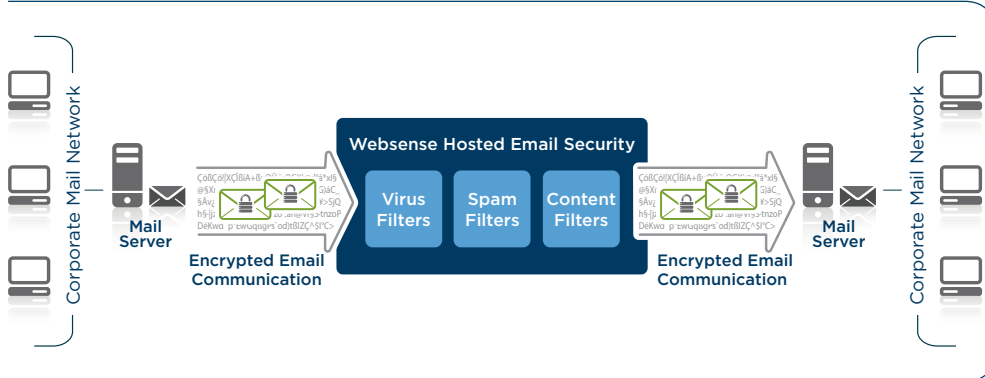
Encryption is included at no additional charge with Websense Hosted Email Security and Content Control.

**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

<b>Australia</b> websense.com.au	<b>Italy</b> websense.it
<b>Brazil</b> websense.com/brasil	<b>Japan</b> websense.jp
<b>Colombia</b> websense.com/latam	<b>Malaysia</b> websense.com
<b>France</b> websense.fr	<b>Mexico</b> websense.com/latam
<b>Germany</b> websense.de	<b>PRC</b> prc.websense.com
<b>Hong Kong</b> websense.cn	<b>Singapore</b> websense.com
<b>India</b> websense.com	<b>Spain</b> websense.com.es
<b>Ireland</b> websense.co.uk	<b>Taiwan</b> websense.cn
<b>Israel</b> websense.com	<b>UAE</b> websense.com

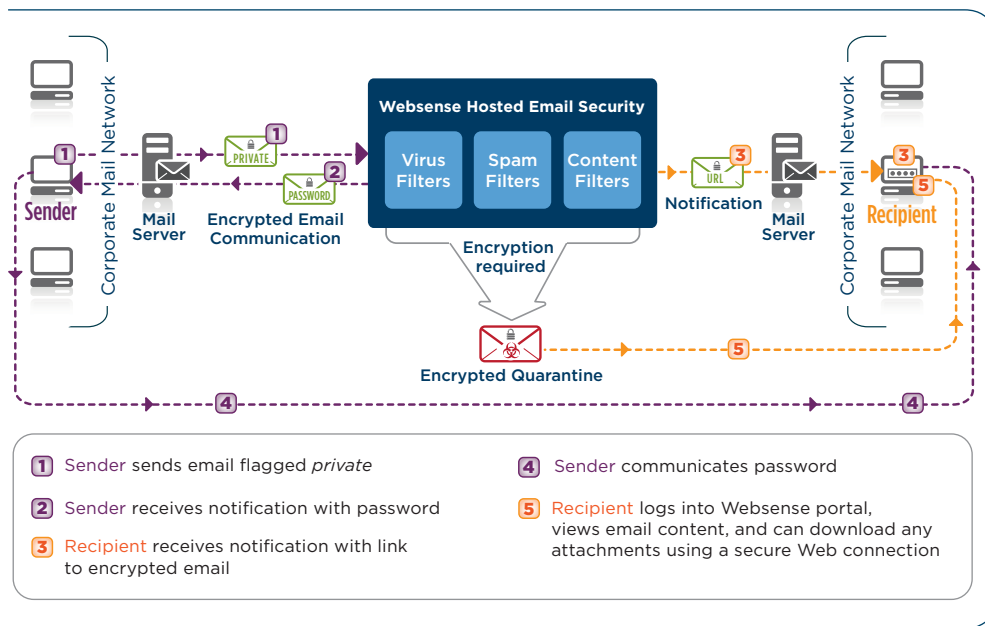
## TLS Encryption



Server-to-server TLS encryption process

Server-to-server encryption using TLS allows organisations to automatically encrypt email to specified domains by establishing a secure, encrypted tunnel between the organisation's mail server, the Websense datacentre, and the recipient's mail server. TLS is used when available for all communications, and can be mandated for specific destinations. Required encryption strength and certificate parameters can be configured on a connection by connection basis. With TLS encryption, organisations can secure email communication with their partners and restrict the transmission of sensitive data to protected channels.

## Park-and-Pull Encryption



- |   |   |
|---|---|
| <b>1</b> Sender sends email flagged <i>private</i>                    | <b>4</b> Sender communicates password   |
| <b>2</b> Sender receives notification with password                   | <b>5</b> Recipient logs into Websense portal, views email content, and can download any attachments using a secure Web connection |
| <b>3</b> Recipient receives notification with link to encrypted email |   |

Individual-to-individual park-and-pull encryption process

Park-and-pull encryption secures email based on policy, sender, group, or other criteria, including the ability to use integrated content controls to encrypt and prevent the loss of sensitive data. End users can trigger encryption for the email they send, or the rules for encryption can be established at a global level. When encryption is triggered, Websense securely stores the email and notifies the recipient. Recipients access the email using a secure, Web-based connection and a password supplied by the sender, removing the need for complex key management and exchanges.

For more information, to start a free trial of Websense email solutions, or to view an online demo, visit [www.websense.com/evaluations](http://www.websense.com/evaluations).