



“Websense Hosted Email Security has enabled us to deliver a more resilient, professional, and cost-effective service to our users.”

**Martin Law**  
Head of IT  
NCP

Websense®

## Hosted Email Security Email Routing and Data Centre Security

Websense® provides clear and accountable benchmarks for maintaining the privacy and security of your email. On its way from sender to recipient, email travels through any number of locations including mail servers, mail relays, and multiple ISPs, all of which have a clear view into unencrypted email. As the location responsible for interrogating, cleaning, and quarantining your email, Websense maintains the very highest security standards.

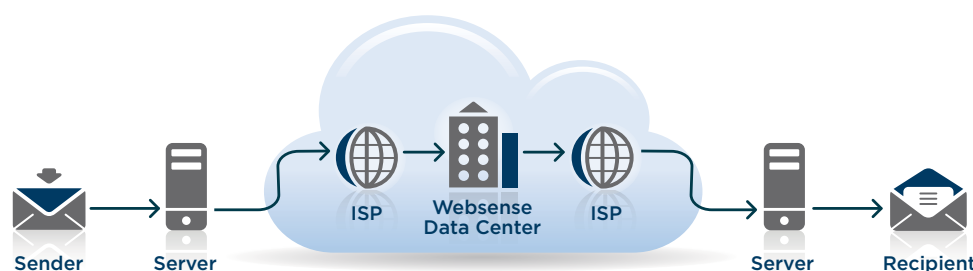


Diagram showing example routing of email on Internet

### Email Routing and Security

Email is routed to a Websense data centre in the same way that it would be routed to any email server or appliance. The difference is that Websense has published standards and measures around security that don't exist with other locations on the Internet. Of all the places your email visits, Websense data centres are among the safest locations it can be routed to. This is because of the stringent security and privacy safeguards Websense has built into the data centre 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 or anyone else to whom you have given access to your account.

### Stringent Security and Privacy Safeguards

Websense Hosted Email Security and Websense Hosted Web Security have gone through the stringent review process and have been certified as ISO 27001 compliant. This certification is awarded to solutions that comply with industry best practices and is a key component in helping to meet global legislative and regulatory requirements, providing global best practice guidance surrounding the protection of confidentiality as well as the integrity and availability of customer data. ISO 27001 is the highest security standard in the industry—exceeding SAS 70 requirements, which many competitors claim as their certification benchmark. Websense renews its ISO 27001 certification every six months.



**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

**Italy**  
websense.it

**Brazil**  
websense.com/brasil

**Japan**  
websense.jp

**Colombia**  
websense.com/latam

**Malaysia**  
websense.com

**France**  
websense.fr

**Mexico**  
websense.com/latam

**Germany**  
websense.de

**PRC**  
prc.websense.com

**Hong Kong**  
websense.cn

**Singapore**  
websense.com

**India**  
websense.com

**Spain**  
websense.com.es

**Ireland**  
websense.co.uk

**Taiwan**  
websense.cn

**Israel**  
websense.com

**UAE**  
websense.com

## Websense Internal Data Centre Security Requirements

In addition to the strict requirements provisioned in the ISO 27001 certification, Websense has internal requirements that mandate the very highest standards of privacy and security. The following internal security requirements are met for all data centre locations:

- The facility is staffed at all times (24 x 7 x 365).
- The facility provides physical intrusion detection systems and intruder alarms in all areas.
- All access doors are monitored and recorded by CCTV with a 30-day retention policy.
- Only authorised personnel have access to the facility; access is provided via a hand-scanner or proximity-card system.
- Access beyond the main security reception is via “mantraps,” meaning that only one person has access at a time.
- Twenty-four-hour notice is required for any visitors to visit the site. Visitors must be cleared with authorised personnel prior to admittance.
- All authorised personnel must provide photo ID for the release of their access card to the site. All ID cards are returned upon leaving site.
- Only authorised personnel have access to the data centre and client equipment. This is restricted to an authorised access list, as indicated by the card level.
- All racks are locked with a key unique to each installation. The key is released only to authorised personnel and must be signed in or out.
- Websense data centres perform weekly vulnerability testing as well as annual testing with a third-party organisation.

## Summary

Email is routed through any number of locations as it travels between the sender and the recipient. As the location responsible for interrogating, cleaning, and quarantining your email, Websense provides clear and accountable benchmarks, and maintains the very highest security standards to ensure the privacy and security of your email.

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).