

Security considerations for SaaS email

Overview of Cisco WebEx Mail
multi-layer security model

Cisco WebEx LLC
3979 Freedom Circle,
Santa Clara, CA 95054 USA

Main: +1.408.435.7000
Sales: +1.877.509.3239

www.webex.com

Table of contents

Abstract	3
Background: hosted business email services	3
Built-in protection at multiple points	4
Security within the Cisco WebEx Collaboration Cloud	4
Securing data at rest	5
Securing data in motion	7
Message hygiene at the gateway	8
Third-party accreditation and transparency	9
Conclusion	11

Abstract

As enterprises increasingly turn to application outsourcing for the inherent cost and resource efficiencies, IT remains responsible for delivering the required uninterrupted capabilities to the business. When it comes to email, a foundational service for today's enterprises, an outsourced solution initially raises concerns about the loss of control over the content of messages flowing inside the organization and out to customers and partners. While it is true that some hosted email solutions fall short in the maturity of their security functionality, Cisco WebEx™ Mail offers businesses a higher level of reliability and security than can often be implemented by individual IT organizations.

This paper overviews the multi-faceted security enablers that allow the WebEx Mail service to often yield better protection compared to on-premise email solutions as well as other outsourced email alternatives. The security topics covered represent a checklist that should be considered by any IT organization that is evaluating hosted email alternatives, and span technology and practices employed within the Cisco WebEx Collaboration Cloud. The WebEx Mail service also provides customers with Cisco robust security policies and planning efforts; this paper describes those policies and efforts and gives an overview of the independent third-party organizations that routinely audit to provide both transparency and evidence of compliance with industry standards and best practices.

Background: hosted business email services

Many companies are currently considering software as a service (SaaS) as a way to save money while gaining a more scalable and reliable email solution. A SaaS model also offers companies competitive advantages through more efficient resource allocation. Rather than focusing on back-office IT tasks, such as mail server upgrades and maintenance, IT can focus on core projects while outsourcing non-core tasks to experts in the field. However, as with other outsourcing strategies, the issue of security raises concerns. These include the ability to protect trade secrets and intellectual property and avoiding misuse of employee and customer personal data.

It is important to understand that SaaS email providers vary widely in terms of their security approaches. Cisco, with more than 15 years of experience delivering highly reliable SaaS, considers security a top priority for email. Therefore, the WebEx Mail network and service architecture was designed for maximum data privacy and protection. Cisco adheres to best practices for secure handling and storage of sensitive customer data, which are validated through regular independent audits.

Built-in protection at multiple points

Cisco employs a mature, multi-layer security model for WebEx Mail that maximizes data security and protection and helps ensure service continuity. The contributing components of the security solution include:

- In-the-cloud security, to protect physical sites and introduce stringent controls over Cisco personnel that administer and manage the service.
- Data-at-rest security, to build in protection for information that is stored in the data centers and to avoid disruptions to the overall service.
- Data-in-motion security, to safeguard message transport between Microsoft® Outlook® mobile devices and the webmail client and the WebEx Collaboration Cloud.
- Message hygiene at the gateway, to filter out illegitimate content and threats that would otherwise diminish productivity or introduce vulnerabilities to the enterprise.

Combined with Cisco proven policies and regularly validated processes, these components of WebEx Mail security can often yield a higher level of protection compared to on-premise solutions. The Cisco data centers that host WebEx Mail operate under strict security policies and procedures that are nearly impossible to circumvent. While companies and government agencies often make headlines related to data loss, lost backup tapes, or internal security breaches, Cisco data centers offer customers a track record without such incidents.

WebEx Mail also eliminates the need for remote and mobile employees to access corporate email services using Virtual Private Networks (VPNs), which can expose a large part of the internal network. Users can have the convenience of anytime, anywhere access to email without introducing vulnerabilities to the corporate network.

Security within the Cisco WebEx Collaboration Cloud

WebEx Mail is delivered through the WebEx Collaboration Cloud, a private, high-performance network with carrier-class architecture. This communications infrastructure delivers real-time email and web communications services through data centers that are strategically placed near major Internet access points. Dedicated, high-bandwidth fiber routes traffic around the globe. The extremely scalable WebEx Collaboration Cloud serves as a highly available and secure infrastructure, unburdened by the physical limitations of on-premise solutions.

Physical security

Cisco operates all infrastructure used within the WebEx Collaboration Cloud. Currently this network consists of data centers throughout North America, Europe, Australia, and Asia. The physical security at the data centers includes perimeter devices for facilities and buildings, and employees must pass a two-factor identification for entry. Sites take advantage of a combination of state-of-the-art electronic access solutions (SmartCards), passwords, and biometric access controls. Video surveillance provides additional protection.

All Cisco data centers are audited annually. The criteria and metrics for the audits comply with the facilities-related guidelines within prevalent standards such as ISO 27001. (For more information about the controls covered by these standards, please refer to the Third-Party Accreditation and Transparency section later in this paper.)

Cisco security personnel

Cisco has a security department dedicated to WebEx services security. The team recommends and implements security procedures for WebEx products, services, and business operations. Team certifications include Global Information Assurance Certification (GIAC)-Certified Forensic Analyst, Certified Information Systems Security Professional (CISSP), GIAC-Certified Intrusion Analyst, Information Systems Security Management Professional (ISSMP), and Certified Information Security Manager (CISM).

Cisco security personnel receive ongoing training in all aspects of enterprise security from leading vendors and industry experts, in order to remain at the forefront of security innovation and to meet the criteria for security accreditations. Cisco data center personnel are available around the clock to enforce logistical security and operational management support. All security personnel have undergone extensive background investigations.

Organization membership

Cisco is a member of the Cloud Security Alliance, a consortium with the mission of promoting the use of best practices for providing security assurance within cloud computing environments and providing education on the uses of cloud computing. As an active member, Cisco is committed to adherence with consortium guidelines and recommendations. Find more information about the alliance and detailed guidelines for secure computing at: <http://www.CloudSecurityAlliance.org>.

Securing data at rest

Within the WebEx Collaboration Cloud, email and related data are protected with a combination of technology and policies encompassing data storage, access, and removal, host hardening, and high availability.

Data Storage, Access, and Removal

WebEx Mail enables IT organizations to offload the bulk of day-to-day maintenance of email servers and storage. The elimination of traditional backup to tape alone significantly decreases recovery time and the risk of data loss. Having large mailboxes eliminates the need to delete messages for the purpose of keeping mailboxes within quotas. Cisco employs granular access controls for administration, which permits separation of duties using least-privileged, role-based access levels. All administrative access to email systems and data are logged to facilitate compliance with policies and role definitions. As additional safeguards:

- Data is not stored in a human-readable form.
- Cisco tracks the evolving encryption standards, and incorporates commercial-grade advancements to continually increase data protection and maximize privacy for WebEx Mail users.
- Data from different companies are stored on identifiable logical unit numbers (LUNs) and disks.
- Since data is stored in a limited number of known systems, complete removal (with no associated remnant backup data) is possible. Accidental deletions can also be restored by the end user.
- Email data is never crawled or indexed.
- Administrators can perform remote data wipes to delete data from BlackBerry® mobile devices as well as Microsoft ActiveSync® mobile devices, such as the iPhone.

Unlike Microsoft Exchange®, WebEx Mail uses the Linux® file system instead of a database for storage. With more flexibility and superior performance to the Microsoft Jet Database Engine, the Linux file system easily scales to enable large mailboxes. It is worth noting that only an authenticated user with the appropriate permission can read the data and only authorized individuals can perform specific system administration functions.

Host hardening

Cisco host hardening practices provide additional security. Each server build includes a minimal installation of the Linux operating system, and system hardening based on guidance from Security Technical Implementation Guides (STIGs) published by the National Institute of Standards and Technology (NIST). Extraneous tools, libraries, and files have been removed to reduce the likelihood of system vulnerabilities and system misuse. As with all product resources, user access is strictly limited. All systems undergo a thorough security review and acceptance validation prior to production deployment, as well as regular ongoing hardening and vulnerability assessment.

High availability and disaster recovery

Prolonged downtime and data loss are damaging to any business. Companies should take into consideration service continuity and disaster recovery as part of their security planning. The WebEx Mail service is built upon a highly available architecture, and guards against downtime and data loss with capabilities including:

- Local and geographic redundancies
- Real-time data replication across data centers
- Granular, block-level data restores
- Complete daily snapshots

Securing data in motion

Email traffic, traveling between WebEx Mail clients and the cloud or between data centers, is protected with a combination of message transport security and network security measures.

Message transport security

To protect data in motion, all connections between Outlook, mobile, and web mail clients and the WebEx Mail servers within the WebEx Collaboration Cloud employ SSL/HTTPS. Compared to in-house email solutions, where remote users can access email using VPN tunnels, WebEx Mail makes use of RPC/HTTPS protocols. WebEx Mail further secures email using the latest encryption technologies.

Password policies and user authentication

Strict password policies and user authentication based on Active Directory limit access to only authorized individuals and administrators. In accordance with the adequate access controls required for compliance with the Sarbanes-Oxley Act (Section 404, access management), the Health Insurance Portability and Accountability Act (HIPAA), and other regulations, WebEx Mail requires strict adherence to password guidelines:

- Passwords must be at least eight characters in length.
- Passwords must contain both upper- and lower-case letters, mixed with numbers and symbols (! @ # \$).
- Passwords cannot be reused over the course of six password changes.
- Passwords must be changed every 90 days.

Network security

Block-level replication of data across geographically remote data centers speeds disaster recovery in the event of system failures, power outages, and other events that can affect entire sites or geographies. Data transmitted between the primary and backup data centers are carried out over private, secure networks. In addition, firewalls and best-in-class intrusion detection technologies at the network layer safeguard WebEx Mail infrastructure from external threats.

Message hygiene at the gateway

The most security-conscious enterprises take advantage of an additional layer of security at the gateway between the corporate network and the Internet. Introducing message hygiene at this point filters out unwanted or risky traffic before it impacts the network and servers, and thereby increases security while also improving system, network, and overall email service performance.

WebEx Mail customers get highly accurate anti-spam and anti-virus protection that is fully managed and kept up to date by the Cisco team. The hosting data centers include Cisco IronPort® Essentials email security appliances at the gateway, which filter traffic bi-directionally, block spam, viruses, phishing attempts, and other email-borne threats. By filtering outbound email, the appliances also protect the corporate and email reputation of the customer and prevent blacklisting.

Cisco IronPort is the leading enterprise mail security product on the market, protecting 40 percent of Fortune 1000 companies. It offers more than 99 percent accuracy in threat detection, and safeguards productivity by filtering out spam.

IronPort is backed by Cisco Security Intelligence Operations, which consists of three components that differentiate WebEx Mail security from its competitors:

- **SensorBase:** The world's largest threat monitoring system captures threat intelligence from the extensive global network of Cisco devices and services.
- **Threat Operations Center:** A global team of security analysts and automated systems extract intelligence from the collected data.
- **Dynamic Updates:** Real-time updates and recommendations are automatically distributed to IronPort appliances to improve filtering accuracy.

The WebEx Mail service does not preclude a customer from passing all email traffic through other anti-spam and anti-virus on-premise filters before it is sent to the WebEx Collaboration Cloud. Outbound traffic from the cloud can be configured to flow back to the customer site for additional outbound control including encryption, data loss prevention (DLP), or on-site Lightweight Directory Access Protocol (LDAP) integration using on-premise appliances.

Third-party accreditation and transparency

Cisco security teams actively combine forces to optimize the security built into all WebEx services. By participating in the Cloud Security Alliance, Cisco further enhances WebEx services by tracking and adopting the recommended best practices for cloud computing and is actively working towards the latest guidelines that will be published at the end of 2009. In addition, WebEx Mail application development benefits from adherence to industry-standard coding practices.

Beyond its own stringent internal procedures, the WebEx Office of Security engages multiple independent third parties to conduct rigorous audits against internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications.

WebEx Mail security auditors currently include the firm of Information Security Partners, LLC (iSEC Partners), which carries out exhaustive application testing and PricewaterhouseCoopers (PwC), for SAS-70 Type II evaluation including auditing of progress against ISO 17799 controls.

Independent testing provides transparency to Cisco customers, and gives access to audit results that demonstrate Cisco leadership in the field of email security. You may request copies of audit reports from the WebEx Office of Security.

iSEC Audits

iSEC issues an Independent Security Report (iSR) at the completion of each security assessment. The iSR summarizes the high-level security goals of the assessment and validates specific security assertions made by Cisco. While the testing methodology is flexible, each assessment includes the following processes:

- Documentation review
- Developer interviews
- Threat profiling
- Design review of new features and functions
- Active testing of features and functions
- Review of changes made to fix previously identified issues of concern
- Manual and automated penetration testing
- Code review (for validation and discovery)
- Validation testing of "security assertions"

The *iSEC Source Code Review* has been completed for WebEx Mail.

In the source code review, iSEC Partners performed ongoing, in-depth code-assisted penetration tests and service assessments. During these engagements, iSEC Partners received access to the WebEx Mail servers, source code, and engineering staff. Unlike black-box testing, this high degree of access enables iSEC Partners to:

- Identify critical application and/or service vulnerabilities and propose solutions.
- Recommend general areas for architectural improvement.
- Identify coding errors and provide guidance on coding practice improvements.
- Work directly with Cisco engineering staff to explain findings and provide guidance for remediation work.

SAS-70 Type II

Cisco processes and the data centers that host WebEx Mail have been audited and found to be SAS-70 compliant. PwC performs the annual SAS-70 Type II audit in accordance with standards established by the American Institute of Certified Public Accountants (AICPA) and based on ISO-17799 standards. The highly respected and recognized third-party audit validates that WebEx services have been compared to accepted control objectives and activities relating to the handling and processing of customer data. For additional information on the SAS-70 standard, please visit www.sas70.com/index2.htm

ISO-17799

ISO-17799 is an internationally recognized information security standard published by the International Organization of Standardization (ISO) that recommends best practices for information security management. It defines requirements for corporate security policies, data management, and access control, among other things. PwC compared WebEx security policies and practices to the control objectives described in ISO-17799, second edition for Information Technology—Security Techniques. The result of the audit was positive. In the opinion of PwC auditors, WebEx services provide adequate controls as defined in this standard. For additional information on the ISO-17799 standard please see: www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

ISO-27001

The ISO board recently released a new security certification: ISO-27001. Cisco is actively pursuing this certification and has engaged Ernst & Young to assist with implementing an information security management system (ISMS) based on ISO-27001. The information security management covers all Information Assets and Information processing facilities procured and maintained by Cisco to provide Software as a Service to their customers. Cisco plans to complete the ISO 27001 certification process by the end of the Cisco fiscal year 2010.

Conclusion

WebEx Mail takes the work out of securing mission-critical email communications with built-in end-to-end protection. By eliminating the need for an extensive in-house security skill set, IT teams can better focus on the unique requirements of the business. The cost efficiencies of the hosted email solution include the elimination of many up-front deployment costs (compared to an on-premise solution), and cover ongoing maintenance and continual upgrades to allow companies to keep up with the latest security threats effortlessly.

For more information

A white paper on Cisco WebEx Collaboration products, "Unleashing the power of real-time collaboration: Security overview of Cisco WebEx solutions" can be found at: http://www.cisco.com/en/US/prod/collateral/ps10352/cisco_webex_security_overview.pdf

© 2009. Cisco Systems, Inc. and/or its affiliated entities. All rights reserved. Cisco WebEx and the Cisco WebEx logo are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliated entities in the United States and other countries. Other product or brand names are trademarks or registered trademarks of their respective owners.

Learn more about Cisco WebEx Mail.

Visit us online at www.ciscowebexmail.com.