

Enterprise-level security and compliance in the collaborative work environment

Cisco Systems, Inc.
3979 Freedom Circle,
Santa Clara, CA 95054 USA

Corp: +1.408.435.7000
Sales: +1.877.509.3239

Table of contents

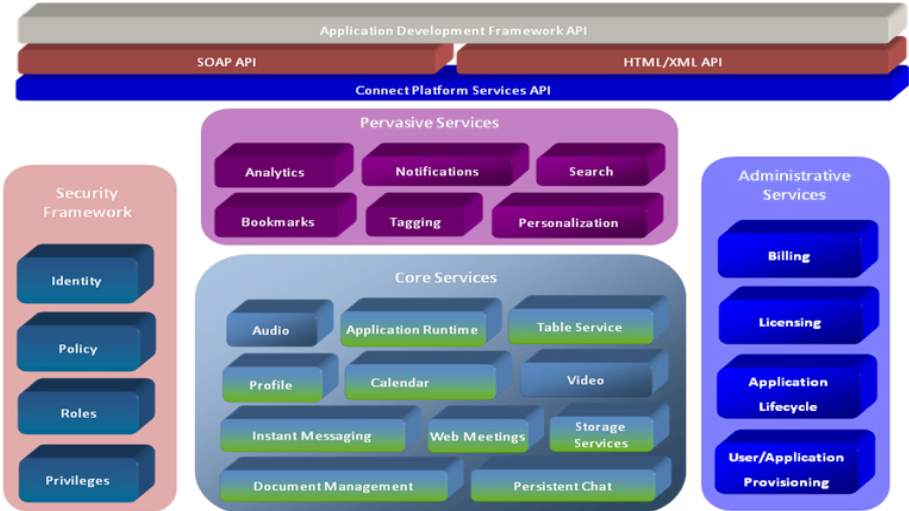
Introduction	3
About Cisco WebEx Connect	4
WebEx Connect architecture components	4
Collaboration platform security requirements	5
Cisco WebEx Connect physical site security	5
Cisco WebEx Connect application security	6
Cisco WebEx Connect network security	9
Cisco WebEx data integrity	10
Integrated partner application security	11
Third party security audits and accreditations	11
Conclusion	13

Introduction

The need for improved collaboration and information sharing inside and outside the enterprise is driving companies to adopt Web 2.0 applications. Businesses are investing billions of dollars in new technologies that are promising to better support today’s global, increasingly outsourced and distributed work environment. But with new, rich, interactive content of Web 2.0 applications come new concerns about application security, compliance, data integrity and protection of business-sensitive information. In the survey of IT professionals recently released by eWEEK, security was named as the number one reason why many enterprises are still hesitant to fully deploy social networks and other Web 2.0 technologies.

To help corporate IT overcome the security challenges of Web 2.0 applications, companies such as Cisco are engineering their collaboration platforms to the highest standards of Internet safety and integrity. Cisco takes a defense in depth approach to Unified Communications and collaboration encompassing four layers of security including infrastructure, communications management, endpoints, and the application level. This paper discusses different aspects and layers of security features in Cisco WebEx Connect, designed to protect corporate and personal data and preserve business-sensitive information. This paper will also demonstrate how Cisco achieves the highest level of security for its WebEx Connect customers through employing industry-standard best practices in physical site security, application and network security. Through a combination of technology and policies, working in partnership with industry leaders and complying with the strictest third-party security audit and certification requirements, Cisco is committed to provide the most secure and reliable collaboration applications possible

WebEx Connect Platform Service



About Cisco WebEx Connect

Cisco WebEx Connect is an enterprise class on-demand unified communication and collaboration client that combines instant messaging, team spaces, and integrated, customizable business applications to bring people, data and processes together — all on an extensible platform that helps companies keep up with the ever changing needs of their business users.

WebEx Connect instant messaging enables business users to instantly exchange information with their colleagues and partners using secure one-on-one or group IM that can also be extended through IM Federation. WebEx Connect provides presence notification to see which users are online and available. When IM chat is not enough, WebEx Connect can launch VoIP or video conferencing or desktop sharing to help virtual teams seamlessly work together. Distributed project teams can extend their productivity using WebEx Connect Spaces. Spaces enable all employees—inside and outside the firewall—to access shared project assets such as document libraries or discussion boards and share documents and files instantly from any computer. Finally, WebEx Connect is an extendable development ecosystem. Companies can take advantage of the many business applications and tools that easily plug into WebEx Connect to customize their business processes and enable collaboration across the enterprise.

WebEx Connect architecture components

The WebEx Connect architecture consists of the WebEx Connect Platform Service layer (back-end), the WebEx Connect client, and a developer tool kit to enable customers, channel partners or third-party developers to create business-specific applications within team spaces.

WebEx Connect Platform Services

The WebEx Connect back-end services are provided via a SOAP (Simple Object Access Protocol)/WSDL (Web Service Definition Language) and REST (Representational State Transfer) protocols that enable the Connect client and integrated application modules to interact with the Connect platform.

WebEx Connect client

The WebEx Connect client is available as a rich client or a web client (Internet Explorer, Firefox and Safari).

Spaces

The concept of Spaces provides the central means of collaboration for project teams—within and across the company boundaries. By incorporating the Connect Policy Model, Spaces allow organizations to create granular access rules to ensure that only authorized team members have the right to access, view, modify or delete project data.

Persistent chat

At the core of each Space is a tool that facilitates team discussion threads. Persistent chat rooms enable effective dialogue in the context of a project or team environment. They allow a team to build a comprehensive history of all team/project related discussions that can be searched and filtered. Persistent discussion topics can easily be escalated to other forms of communication—such as audio conferences or WebEx Meetings.

Application framework and application modules

The WebEx Connect Application Framework is a simple, modular and extensible model that provides access to the WebEx Connect Platform services API and enables WebEx Connect partners to build new custom applications on the WebEx Connect platform or expose their existing services as Connect applications. Application Modules—or widgets—are various types of software services that can be installed like a plug-in into a browser or application over the Internet. WebEx Connect brings the concept of Web 2.0-style widgets into the business application arena, including interfaces with traditional enterprise systems such as ERP, SFA or CRM.

Collaboration platform security requirements

A true enterprise-grade collaboration platform must be built on a foundation that is strong, flexible, multi-faceted and redundant. Companies deploying Web 2.0 applications need vendor assurance that their project data is protected within the collaboration spaces. Security for data that is being transmitted (data-in-motion) as well as the safety and integrity of stored data (data-at-rest), together with strict access control are critical factors for any enterprise choosing to implement a collaboration solution. In addition, an expandable collaboration platform that allows partner widget plug-ins needs to extend its security model to all “trusted” integrated services. Only vendors with the highest levels of security, application and network security, strong policies and up-to-date certifications can become providers of enterprise-ready Web 2.0 applications.

WebEx Connect physical site security

Cisco is dedicated to maintaining top grade physical site security for all its facilities. All data centers require a review by the Cisco security team to ensure that data center will have a favorable review for future audits.

Cisco data centers

WebEx Connect data is stored at Cisco owned and operated data centers worldwide. Each data facility—whether it is in California, Colorado, Virginia, London, Tokyo, Melbourne or Bangalore—is built to withstand worst case disaster scenarios and ensure continuous operations and data security.

Authorized access

Cisco maintains strict controls over both physical and remote access to its data center. Physical access to the Cisco Data Centers is limited to the Cisco Operations Team—a select group of authorized personnel for site operations and maintenance. Authorized personnel must pass through electronic and visual identity validation systems, including a biometric hand scan and proximity card readers. All Cisco equipment is kept in secured cabinets. The security system for the cabinets includes a rotational key cabinet system in which the non-descript numbered keys can be accessed only by security personnel. All Cisco Data Centers utilize the KeyTrak key security and management system that provides a total lockdown solution, enabling keys to be secured, controlled and monitored at all times.

All Cisco Operations Team members have signed special non-disclosure agreements with respect to the handling of customer data. Failure to uphold this agreement carries disciplinary actions up to and including legal penalties. Virtual access to the Cisco Data Centers is limited to the Cisco Operations Team via RSA two-factor authentication.

Security personnel

Cisco has a dedicated security team which includes a GIAC-Certified Forensic Analyst, two CISSPs, a GIAC Certified Intrusion Analyst and an ISSMP. All Cisco security personnel receive ongoing extensive training in various aspects of enterprise security from vendors and industry experts to remain at the forefront of security trends. The separation of duties that exists between the Cisco security personnel and other Cisco employees is a major factor that enabled Cisco to obtain both WebTrust and SAS-70 Type II reports, into which Cisco incorporates ISO-17799 control objectives.

WebEx Connect application security

WebEx Connect offers a range of customizable access controls for its collaboration spaces. These include customizable options for user authentication before accessing the space and permissions to access, view, modify or delete files and documents within the space, once a user has logged on. A 3rd party assisted source code review is performed to ensure that any defects are identified prior to the general availability of the product.

Organizational model

The foundation of the WebEx Connect platform is the Organizational Model. This model—embedded into WebEx Connect Platform Services—enables WebEx Connect to support organizational management policies and ensure data sharing and communication security. The Organizational model provides each company a “home” inside the WebEx Connect network. The Organizational Administrator (Org Admin) oversees roles and privileges, and can assign them to groups or people, as well as set certain global policies—including access control—for the entire Organization.

User authentication

WebEx Connect is designed so that each Org Admin can adjust the level of security for his/her company, choosing from a range of options. Every WebEx Connect user has a unique login/password combination.

Beginning with the login, user identity is authenticated by WebEx software on every user request. All subsequent requests are re-verified and if the user cannot be authenticated or the user’s status has changed (e.g., the user has been deleted by the Administrator), the user is forced back to the login screen.

Namespaces

A namespace is a virtual container used to hold unique identifiers—such as user names. Namespaces are essential for collaboration environments that support hundreds or even thousands of users, as they help to prevent user name confusion and collision.

For instance, two users with the same username who work for different companies can coexist in the WebEx Connect space without causing confusion, as they are associated with different namespaces. Users belonging to the same Organization have access to all objects in the Organization namespace. Namespaces also add an extra layer of protection for integrated third-party applications. Partner application-specific information can be contained within the designated namespace preventing unauthorized access.

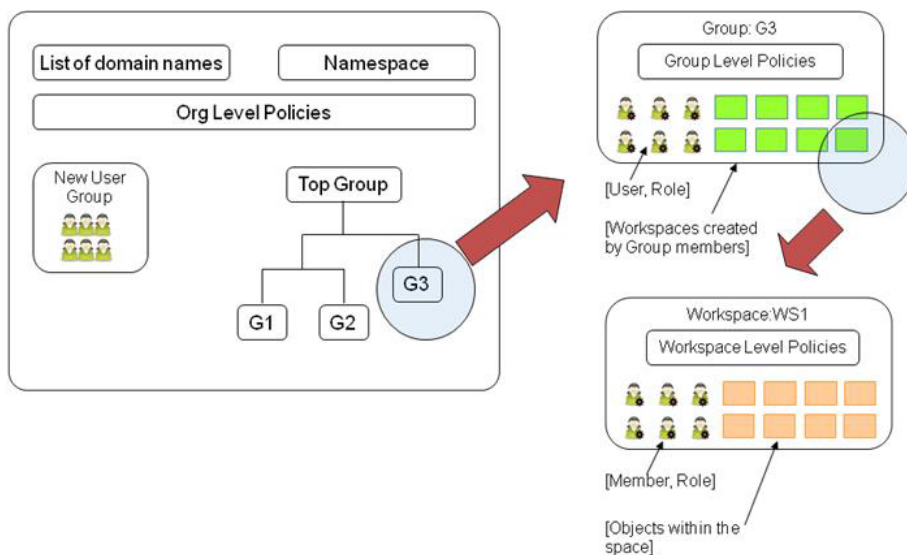
Permissions

WebEx Connect is set up with a customizable permissions system, so that once access to the Space has been established, the user will still need permission to perform certain actions such as viewing and editing documents. This granular access control and strict policy enforcement ensure that information stored in WebEx Connect Spaces is protected and can be viewed, modified or deleted only by users who are authorized to do so. The WebEx Connect permissions system is flexible enough to handle multiple permission levels, yet it is easy to use for all members. Permissions are based on concepts of Roles, Groups, and People.

Since many enterprise customers are deploying centralized policy or entitlement management systems for their on-premise applications, future versions of WebEx Connect will be designed to leverage rules and role/group assignments from these policy systems and apply them to resources that reside in Connect Spaces.

These policy servers, such as the one available from the Cisco acquisition Securent, enable organizations to externalize policy management from application silos, thereby improving security, compliance and governance. Other benefits include centralized auditing and logging and delegated administration.

The WebEx Connect Multi-Tier Permissions System



WebEx Connect features 6 built-in roles allowing for strict access control and tight security of all project data stored in WebEx Connect spaces.

- 1 Organization Admin role is automatically created when the Organization is provisioned. The Org Admin has the most privileges, owns and controls all groups.
- 2 Group Admin is a global role that is assigned to an individual at the time the Group is created, and its privileges defined according to the group's requirements.
- 3 Group Member role has a default set of privileges and is assigned to any individual who becomes a member of a group.
- 4 Space Owner is a built-in role that is assigned to the creator of a Space when the Space is initiated. The Space Owner controls the content (Applications) in the Space, and is the only individual who can delete the Space.
- 5 Space Admin is a built-in role that has the privilege to manage space membership—invite or expel Space members, and assign their Space roles as members or guests.
- 6 Space Member is a built-in role that is assigned to all people who are invited to the Space as a member.

Groups

A Group represents an assembly of people within the Organization, or a collection of users working on a specific project across company boundaries. A group structure can reflect the reporting structure in the company, or it can represent a number of cross-functional roles who have joined forces to collaborate on an assignment. Organizational groups are designed to help a company map their corporate org chart to the WebEx Connect model. These types of groups can be imported into WebEx Connect from LDAP or Active Directory, ensuring strict login credentials and preventing unauthorized access. Cross-functional groups are more common in WebEx Connect spaces that are created to manage cross functional teams—both inside and outside the organization—for the duration of a project.

Policy Model

The WebEx Connect Policy Model is designed to be both flexible and comprehensive, allowing organizations to tightly control network and content access, both within and across corporate boundaries. The policy model is also intended to be easy to use for basic use cases, with a default out-of-the-box structure that will fit most companies' needs. It is the prerogative of the Organization Administrator to determine to what level of detail and granularity to define and enforce the access privileges based on the specific security considerations of the organization. Future versions of WebEx Connect will be able to leverage enterprise policy or entitlement management systems to provide more a single point of control over Connect Spaces as well as other enterprise applications.

The policy model is centered on two main concepts—Roles and Privileges. Individuals can belong to more than one Group, and can have more than one role assigned to them. Whatever access privileges are granted to the role, all users in this role receive them. Privileges are permissions for users to perform a certain action.

Privileges are divided into two categories—both designed to ensure the safety of the corporate infrastructure and protect sensitive information: Corporate Policies and Access Control. Corporate Policies represent a specific set of permissions aimed at controlling network communication capabilities, such as sharing information outside the company. Access Controls are the types of privileges that govern access to specific content, such as tabs, applications, user profiles, documents shared in Connect Spaces, tasks, or the Spaces themselves.

Roles

Roles grant specific privileges to individuals assigned to a given Role. Individuals can have more than one Role (for example, a Group Admin can also be a Space owner or a member of a different Group). Each role has an owner. Typically, the privilege of creating and modifying roles within a group is given to the group owner.

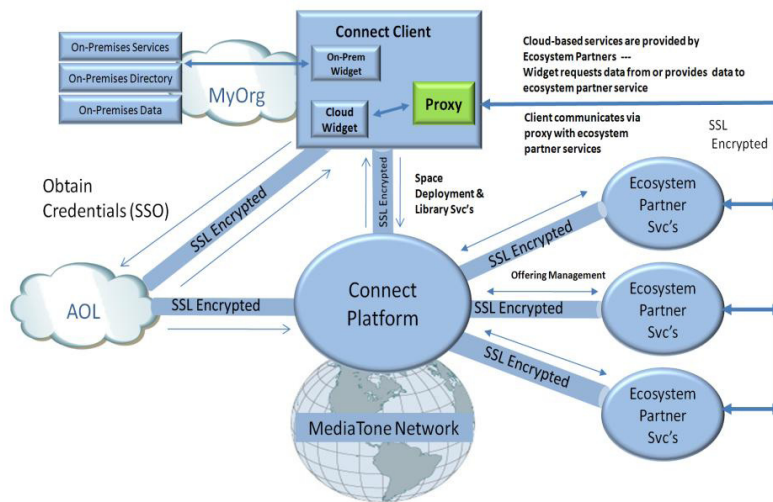
Implicit deny

To further enforce organizational security policies, WebEx Connect is equipped with the implicit deny mechanism. If a particular privilege is not explicitly granted to a role, that privilege is denied. When performing permission resolution, WebEx Connect inspects each role assigned to a person to determine if any of the roles grant the specific privilege. If the privilege is not found, the access is denied. This feature is particularly relevant for programmers who access the WebEx Connect services back-end and traverse the object model.

WebEx Connect network security

To maintain organizational security and user privacy throughout the ecosystem, WebEx Connect employs multiple methods of web-based security using the latest standards and techniques for data encryption and user authentication.

The WebEx Connect Network Security Architecture



Cisco has built its network to be secure from the ground up. The WebEx Connect users' data is protected by numerous layers of state-of-the-art hardware and software security to prevent unauthorized individuals from gaining access to it. Cisco's dedicated global network is designed specifically for large scale, on-demand collaboration. It is fully compliant with ANSI and ISO standards, and receives annual validation and certification. The corporate network is protected from intrusive software or IP leakage at all times through the MediaTone resident, bidirectional compliance facility whether the connection is made inside our outside the network. In addition, Cisco has an experienced team of software engineers, IT professionals, and system architects who carefully monitor the latest developments in Web network security and implement new software and hardware security upgrades as appropriate.

Firewalls & Proxy servers

Most enterprises deploy firewalls between the local area network and the public Internet. This requires packets of data to conform to an approved protocol with valid source and destination addressing before entering the Intranet. The WebEx Connect traffic is encrypted and uses SSL (Secure Socket Layer) at Port 443 as the default setting.

However, firewalls alone are not able to control and perform deep inspection of IM traffic. To provide maximum security without impairing performance, WebEx Connect has an option to deploy a dedicated IM proxy. The IM Proxy is used for detecting and protecting against threats from SpIM, Day Zero worm blocking, and protection against other malware. With IM Proxy, customers can define their own blacklists and whitelists to allow or restrict IM exchanges. The IM Proxy solution extends security to the content level by enabling IM exchanges to be recorded.

Full system redundancy

Cisco is committed to eliminating all single points of failure. Therefore, the WebEx Connect infrastructure offers full redundancy of all its system components to provide reliable, continuous, and secure service.

The Cisco Data Centers are fully redundant with respect to hardware, power and Internet connectivity. There are two separate feeds into front-end routers. All network equipment, including the routers, switches, firewalls and load-balancers are fully redundant. There are multiple load-balanced web and application servers. The system is configured so that if one component fails, its twin will take over without interruption. This multi-server configuration facilitates efficient software upgrades, since individual servers can be taken out of rotation for upgrade without disrupting service. All back-end database and file servers are clustered and use RAID 5 (redundant array of independent disks) hardware to provide 100% availability even during maintenance.

Cisco WebEx Connect data integrity

Millions of data files reside within the WebEx Connect customers' collaboration Spaces, and millions more are transmitted via non-persistent IM chat and meetings. The WebEx Technology Group enlists a variety of methods to assure data integrity for data-in-motion as well as data-at-rest, including data protection based on network architecture, virus protection software and SSL data encryption.

Protected data storage

Data integrity is protected by numerous layers of state-of-the-art hardware and software security features to prevent hackers or other unauthorized individuals from gaining access to it. The WebEx Connect data is stored only on back-end DBMS and file servers that have no direct connection to the Internet. No customer data resides on the Web/Application servers. Only when data is requested by an authenticated user does it pass through the Application server to service the user request.

Encryption of data-in-motion

With WebEx Connect, all real-time communication stays private with 128-bit SSL encryption. All content exchanged between IM users is encrypted outbound, remain encrypted going through the IM cloud, and arrives encrypted at the receiving desktop. Only users authenticated by the WebEx Connect service receive a copy of the key to decrypt the communication.

At no time are messages sent over the public Internet in clear text format. Every message is encrypted with 128-bit SSL with the option to choose 256-bit AES (Advanced Encryption Standard). WebEx Connect examines headers to authenticate and establish the destination of the contacts and connect the chat session. When contacts communicate only with co-workers or those authorized to reside within a corporate network, all communications travel between the MediaTone infrastructure and the corporate network. IM Chat sessions are not being recorded (persistent) on IM servers, keeping the real-time chat content private and secure. User credentials are also encrypted for ultimate protection and never sent as clear text.

Integrated partner application security

WebEx Connect is an ecosystem of integrated value-add applications and services. To protect the Connect community from hacks, phishing and other malicious practices and ensure data safety and integrity, the WebEx Connect development team has put in place strict security measures, policies and guidelines.

Application categories

The first major aspect of the WebEx Connect security model is the notion of “approved” or “trusted” applications. Applications can be classified by WebEx or by an Organization as approved or not approved for internal use.

Applications in the “unapproved” category are usually those developed by independent providers, not affiliated with the WebEx Connect partner program tiers and not part of the Organization. When these types of applications are used in a WebEx Connect Space, the system will warn the user of their “unapproved” status. The warning is similar to those users typically receive when attempting to install an unsigned plug-in. The user can then choose to accept or deny the application. Approved applications are flagged as such in the WebEx Connect Platform service back-end, and no warning messages are needed.

Sensitive parameter management

The application definition includes declaration of any parameters that it needs to operate. Some parameters may be deemed as “sensitive” by the application.

The classic example of such a parameter is user credentials (name and password) used to access a 3rd party service. The WebEx Connect Framework treats these parameters with the highest level of security. All sensitive parameters are encrypted and stored locally on the client machine. Only the designated application can access them, and use them to interact (such as authenticate) with its own service. Passwords are never sent in clear text over the Internet.

Event security

The WebEx Connect event model is designed to be open and allow all application modules to publish and subscribe to events. However, for any partner who wishes to keep their events private within their internal modules, WebEx Connect offers an option to securely encrypt/decrypt the event contents.

Auditing and analytics collection and reporting

In order to ensure compliance with assigned Roles, Privileges and rights, WebEx Connect continuously gathers full activity statistics. This data is used to create reports of all user activity within the WebEx Connect ecosystem and can be used for auditing and compliance purposes.

Third party security audits and accreditations

As a service provider, Cisco recognizes the value of conducting audits on a regular basis, to ensure that all security policies, practices, and systems are effective in ensuring the security of its customers' data. Independent security audits are conducted annually by one of the Big 4 Accounting Firms. These audits include penetration tests—attempts to attack the system through known hacker tactics. In addition, the Cisco security model has been independently tested—and met the requirements—of many customers, including the military, aerospace and government sector. Cisco routinely passes all security audits and any issues that are flagged are fixed in a timely manner.

SAS-70 Type II

PriceWaterhouseCoopers performs an annual SAS 70 Type II audit and provides Cisco with a corresponding report. The Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).

The SAS-70 Type II audit is widely recognized, and it represents that Cisco has been through a stringent and in-depth audit of its control activities. The report allows Cisco to demonstrate that it has rigid controls and safeguards when it handles and processes data belonging to its customers.

SAS-70 is the authoritative guidance that allows Cisco to disclose its control activities and processes in a uniform reporting format. The SAS-70 Type II audit and corresponding report certify that an independent auditor (Ernst & Young) audits, on an ongoing basis, the controls and safeguards Cisco has put in place around the data confidentiality and security of its customers data. This SAS-70 Type II report is available for review by customer security and audit teams under NDA.

Compliance

In response to an increasing amount of sensitive information being transmitted over computer networks and stored electronically, governments are creating laws requiring organizations to comply with strict information protection guidelines. Under the Sarbanes-Oxley Act, the California Senate Bill 1386, HIPPA (Health Insurance Portability and Accountability Act) and other regulations such as the EU Directive for Privacy, organizations are being mandated to accurately report all electronic assets, disclose any breach security and ensure the privacy and security of medical and other sensitive data.

As discussed earlier in this paper, WebEx Connect provides multiple levels of security—from its physical site protection, to application and network security and data integrity—to help its customers and partners comply with regulatory guidelines relating to the use, disclosure, and storage of sensitive information. Its numerous awards, security certifications and audit results demonstrate that Cisco can meet even the toughest information security standards and help companies put in place compliance mechanisms and policies.

Conclusion

WebEx Connect is a global collaboration platform and a growing ecosystem of integrated Web 2.0 applications. In order to meet strict enterprise security guidelines, Cisco has developed multi-layered security practices. The WebEx Connect customer data is protected by the highest level of physical security at WebEx data centers, the latest hardware and software in network security, comprehensive user authentication policies and granular access rules.

Cisco has a proven track record of being a trusted service provider for Web collaboration applications, and numerous 3rd party independent certifications that demonstrate the solid nature of its security models and policies. Enterprise customers can fully enjoy the benefits of WebEx Connect, knowing that their real-time and offline communications and data are safe and secure with Cisco.