Webex Calling Security

webex by CISCO

Contents

1. Introduction

Webex® Calling is a cloud-based phone system optimized for businesses of all sizes. It provides essential business calling capabilities for desktop, mobile, and remote workers and is delivered from the global Webex collaboration platform. Webex Calling leverages cloud delivery to provide flexibility, rapid innovation, predictable operating expenses, and instant global scale while protecting your on-premises investments by connecting them to the Webex collaboration platform.

A note on terminology, Webex and the Webex collaboration platform are referred to various locations throughout this document, they reference the entire Webex product line including Webex Calling, Webex Meetings, and Webex App services and the infrastructure they run on respectively. Webex Calling is a core service within the Webex product line and runs on the Webex collaboration platform.

The Webex Security and Privacy Difference

Webex has security and privacy built into its approach to product design and delivery. Webex has invested heavily to build a culture of security with the right checks and balances in place. All Webex services including—Webex Calling have secure default settings out of the box, thereby enabling users to start collaborating freely without having to worry about configurations. At the same time, Webex delivers a great user experience—one that doesn't compromise security.

Webex and Webex Calling are backed by Cisco's rich history and expertise in security—from the network, to endpoints, to the data centers and our cloud services. All the Webex products and services are built using Cisco's Secure Development Lifecycle (CSDL) which ensures that our products are built to a security baseline. The security of our products is independently verified by a team with hundreds of security advocates across multiple functions. Whether, inside your organization, or when collaborating across company lines, Webex provides an enterprise-grade hardened collaboration platform that keeps you secure by default and protects your data.

Privacy, security and transparency: Our three security principles

We are committed to respecting the **privacy** of your data:

- Webex does not rent or sell user data to third parties.
- Webex implements all features with security and privacy in mind.
- Webex is transparent about our privacy practices.

Webex is **secure** by default

- Webex security is built-in as a key foundational element and is secure by default. It's never your responsibility to opt-out of sharing your data, or change settings in order to be protected.
- Webex enables strong passwords by default for any service
- Webex has **security cyber governance** and is **transparent** when there are security issues
- Cisco's Security and Trust Organization oversees security and privacy for Webex, and publicly discloses security vulnerabilities.

Security is priority for Cisco. We have always invested—and will continue to invest—heavily in security and privacy. Webex Calling was built from the ground up to provide end-to-end security for you. We have the mature processes and governance in place to protect your privacy and deliver security you can trust. Our mission is to enable collaboration without compromise.

Webex Calling and the Webex collaboration platform provide multiple levels of security for tasks that range from administrative functions to end-user interactions. This paper outlines in detail the core security measures that underpin Webex Calling and the Webex collaboration platform infrastructure it runs on to help you with an important part of your investment decision.

1.1 What you will learn

You will learn about the Cisco® tools, processes, certifications, and engineering methods that secure Webex Calling and the Webex collaboration platform.

2. Cisco security model

Cisco remains firmly committed to maintaining leadership in cloud security. Cisco's Security and Trust organization works with teams throughout our company to build security, trust, and transparency into a framework that supports the design, development, and operation of core infrastructures to meet the highest levels of security in everything we do.

This organization is also dedicated to providing our customers with the information they need to mitigate and manage cybersecurity risks.

The Webex security model (Figure 1) is built on the same security foundation that is used across all Cisco products and solutions.

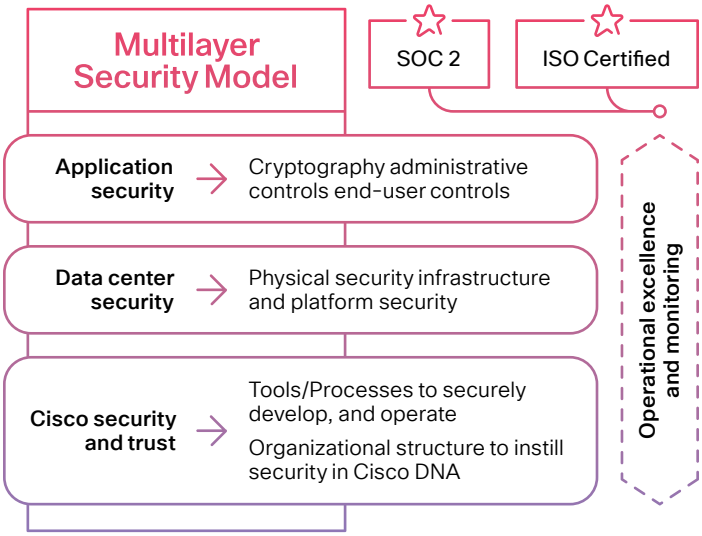


Figure 1. Webex security model

The Webex organization consistently follows the foundational elements to securely develop, operate, and monitor Webex services. We will discuss some of these elements in this document.

2.1 Cisco Security and Trust

All Cisco product development teams are required to follow the Cisco Secure Development Lifecycle (Figure 2). It is a repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products. The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle helps ensure defense in depth. It also provides a holistic approach to product resiliency. The Webex Product Development team follows this lifecycle in every aspect of Webex Calling product development.

Read more about the Secure Development Lifecycle.

2.2 Cisco foundational security tools

The Cisco Security and Trust organization provides the process and the necessary tools that give every developer the ability to take a consistent position when facing a security decision.

Having dedicated teams to build and provide such tools takes away uncertainty from the process of product development. Some examples of tools include:

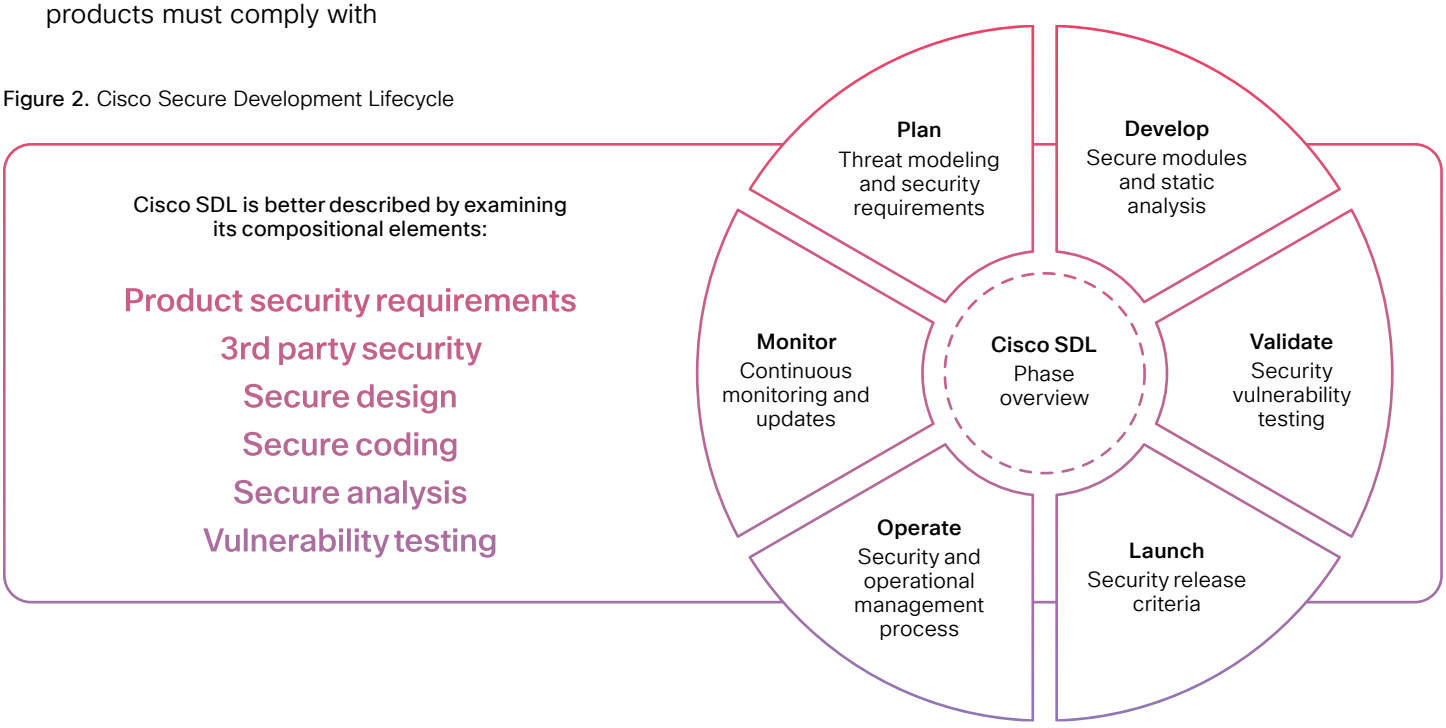
- Product Security Baseline (PSB) requirements that products must comply with
- Threat-builder tools used during threat modeling
- Coding guidelines
- Validated or certified libraries that developers can use instead of writing their own security code
- Security vulnerability testing tools (for static and dynamic analysis) used after development to test against security defects
- Software tracking that monitors Cisco and third-party libraries and notifies the product teams when a vulnerability is identified

2.3 Organizational structure that instills security in Cisco processes

Cisco has dedicated departments in place to instill and manage security processes throughout the entire company. To constantly stay abreast of security threats and challenges, Cisco relies on:

- Cisco Information Security (InfoSec) Cloud team
- Cisco Product Security Incident Response Team (PSIRT)
- Shared security responsibility

Figure 2. Cisco Secure Development Lifecycle



2.4 Cisco InfoSec Cloud

Led by the chief security officer for cloud, this team is responsible for delivering a safe Webex environment to our customers. InfoSec achieves this by defining and enforcing security processes and tools for all functions involved in the delivery of Webex into our customers' hands.

Additionally, Cisco InfoSec Cloud works with other teams across Cisco to respond to any security threats to Webex.

Cisco InfoSec is also responsible for continuous improvement in the Webex security posture.

2.5 Cisco Security and Trust Organization – Incident Command

The Cisco Security and Trust Organization - Incident Command is a dedicated global team that manages the inflow, investigation, and reporting of security issues related to Cisco products and services. Incident Command uses different mediums to publish information, depending on the severity of the security issue. The type of reporting varies according to the following conditions:

- Software patches or workarounds to address a vulnerability, or a subsequent public disclosure of code fixes is planned to address high-severity vulnerabilities.
- Incident Command has observed active exploitation of a vulnerability that could lead to a greater risk for Cisco customers. Incident Command may accelerate the publication of a security announcement describing the vulnerability in this case without full availability of patches.
- Public awareness of a vulnerability affecting Cisco products may lead to a greater risk for Cisco customers. Again, Incident Command may alert customers, even without full availability of patches.

In all cases, Incident Command discloses the minimum amount of information that end users will need to assess the impact of a vulnerability and to take steps needed to protect their environment. Incident Command uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. Incident Command does not provide vulnerability details that could enable someone to craft an exploit.

Learn vulnerabilities published by Incident Command at tools.cisco.com/security/center/publicationListing.x.

Unmatched visibility and threat protection with Cisco Talos

Cisco Talos represents one of the largest commercial threat intelligence teams in the world with more than 300 researchers, Cisco Talos uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being used in attacks. Cisco Talos also feeds huge volumes of global internet activity into a combination of statistical and machine learning models to identify new attacks being staged on the internet. Using anti-virus engines, Cisco Advanced Malware Protection (AMP), and sandboxing from Cisco Threat Grid, Cisco Talos takes advantage of intelligence from millions of new malware samples analyzed daily for the most effective defense against malicious files.

2.6 Shared security responsibility

Although every person in the Webex group is responsible for security, the following are the main roles:

- Senior Vice President/General Manager, Security and Applications
- Senior Vice President/General Manager, Collaboration
- Vice President, Webex Platform and Infrastructure Engineering
- Chief Information Security Office, Collaboration

3. Webex Calling data center security

Webex Calling is a cloud solution delivered through the Webex cloud, a highly secure service-delivery platform with industry-leading performance, integration, flexibility, scalability, and availability. The Webex cloud is a communications infrastructure purpose-built for real-time audio, video, and content sharing.

Webex Calling uses computing equipment located in multiple data centers around the world. These data centers are strategically placed near major Internet access points and use dedicated high-bandwidth fiber to route traffic around the world.

Data centers are SSAE-16 and SOC-2 compliant, and are evaluated annually for SOC2 attestation of compliance in the areas of physical security perimeter, physical entry controls, securing offices, rooms, and facilities, protecting against external and environmental threats, working in secure areas, supporting utilities, cabling security, and delivery and loading zones. Webex Calling applications and services run on multiple servers within Cisco and third party data centers. Webex Calling is designed and built with security and availability methods and procedures that address physical access and protection, network connectivity, remote and local access, application and server management, availability, and protection of customer-sensitive data. Cisco partners with data center operators who have years of experience in design, implementation, and operation of large-scale data centers. These facilities provide physical, environmental, and access security, protecting Webex Calling physical and virtual application environments. Examples include:

- 24-hour daily onsite security personnel
- Non-descript and unmarked facilities with natural boundary protection
- Silent alarm system with automatic notification of local law enforcement
- Building code compliance to local governmental standards
- Environmental safeguards
- Fully redundant HVAC facilities
- Automatic fire suppression systems, dual alarm (heat/smoke), and dual interlock with cross-linked event management
- N+1 redundant Uninterruptible Power Source (UPS) system supporting the entire data center capacity, with redundant backup generators
- Location specific disaster recovery plan (seismic, flood control)
- Biometric scanning and/or 2-factor authentication for access
- All ingress and egress through vestibules (man-traps)
- Access requires a valid government-issued photo ID, and all access history is recorded for audit purposes
- Authorization required prior to access and provided only for legitimate business need
- Shipping and receiving are walled off from co-location areas
- For both ingress and egress, all material is inspected upon arrival by onsite security staff

Administrators use Two-Factor Authentication (2FA) when accessing Webex Calling computing assets. All user and administrator activity is logged. The 24x7 Webex Calling Security Operations Center (SOC) monitors system logs as well as Intrusion Detection System (IDS) and firewall alerts to detect and prevent attacks or misuse.

4. Infrastructure and platform security

Cisco's approach to security addresses the security of the network, systems, and the overall data centers that make up the Webex collaboration platform. Network services engineers harden and patch the operating systems and infrastructure to protect its systems from various security vulnerabilities. Servers must deliver data in a secure, reliable fashion.

Operating system, middleware, and application hardening involves:

- Security-sensitive ongoing hardening
- Security review and acceptance validation prior to production deployment
- Vulnerability scanning and assessment
- Security patching
- Protection against malware
- Implementations and configurations of robust logging
- Strong authentication
- Prudent configuration of access controls, “least privilege” and “need-to-know”
- Information backup

Hardened systems with appropriate access and controls further restrict system capabilities to only those that are explicitly required and tolerated for expected system functionality. Systems, software versions and upgrades are cross-checked and undergo suitable testing in a staging environment prior to acceptance for production deployment and use. Technical vulnerabilities of information systems are monitored and logged. The operations team evaluates any exposures to such vulnerabilities and takes appropriate patch management lifecycle measures to address any associated risk. Processes are in place to monitor the use of information processing facilities, and the team regularly reviews these activities.

5. Network communications security

Information and systems interconnected by the networks are important business assets. Maintaining and ensuring network security at all levels is essential. The operations team achieves this network security through both technical means and management procedures.

Network security includes the following:

- Demilitarized Zone (DMZ)
- Firewalls
- Intrusion detection
- System authentication
- Data encryption

The security management team determines the security features, service levels, and management requirements of all network services. The team manages and controls the networks—not only to protect them from threats—but also to maintain security for the systems and applications using the network, including information in transit. Detection, prevention, and recovery controls, along with appropriate user awareness procedures, protect against malicious code. Audit logs record all user activities, exceptions, and information security events. The operations and security team preserves these logs to assist in future investigations and access control monitoring. Independent reviews are conducted on a regular basis to ensure that information security processes are adequate, complete, fit for their purposes, and enforced.

6. Webex Calling application security

6.1 Cryptography

6.1.1 Protecting data in motion

Webex Calling implements data encryption for access-side network communications access. Webex Calling implements data encryption for access-side network communications access. Administrative access to the system is encrypted using the following Transport Layer Security (TLS) versions and strong cipher suites.

TLS 1.3 Cipher suites:

- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

TLS 1.2 Cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

6.1 Cryptography (Continued)

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SIP call control signaling between SIP endpoints and the service are encrypted using the following Transport Layer Security (TLS) versions and strong cipher suites.

TLS 1.2 Cipher suites:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Media streams between SIP endpoints and the service are secured using the Secure Real-Time Transport Protocol (SRTP), as described in RFC 3711.

6.1.2 Protecting data at rest

Webex Calling stores organization and user data that may be critical to your business. Webex Calling uses the following safeguards to protect data at rest:

- Encrypts data at rest using AES 256
- Stores all user passwords with one-way hashing algorithms and salts
- Encrypts other passwords (i.e., SIP authentication)
- Encrypts all backup files and archives

6.2 Access control

The service ensures that the appropriate levels of access controls are defined and implemented in the operating environment. Access controls consistent with this policy are applied to each system, application, database, or network utilized to manage various types of data classifications and the users who access that data. These controls consist of standardized processes for requesting, approving, granting or revoking, modifying user access, user role definition. Controls also consist of segregation of duties analysis, least privileged access, user passwords, user identification policies and standards, user access auditing expectations, and network access control lists, as well as auditing of network and access activities.

Access control policy requires the implementation of user accounts and access controls for systems and applications requiring access to configuration and information. The scope of the policies and controls are limited to access of the infrastructure and applications owned and operated or managed by the Cisco Customer Experience (Cisco Services) organization.

User account and access controls meet the following security requirements:

- All users are assigned unique IDs and must authenticate for access to assigned privileged components
- IDs and authentication credentials are not distributed beyond a single user and group/shared credentials are not shared or distributed
- Addition, deletion, and modification of user IDs, credentials, and other identifier objects are controlled by the system
- Restriction of access to privileged user IDs to the least privileges necessary to perform job responsibilities
- Privileged users must be identified for specific access
- Access for any terminated users is immediately revoked
- Inactive user accounts are removed or disabled
- Ability to manage IDs used by third parties to access, support, or maintain system components

6.2 Access control (Continued)

These controls are defined, approved, implemented, and overseen by management or designated security officers. These controls are reviewed for accuracy and effectiveness at least annually, both internally and by an independent auditing authority.

6.3 User authentication

Subscribers are registered in Webex Identity—a cloud-scale identity platform that provides either standalone identity management or customer premises hybrid identity integration. Integrations include Active Directory user account replication, Single Sign-On (SSO) with major providers (i.e., Okta, Ping Identity, etc.) and customer consumable APIs. Built on the latest technology and standards (e.g., SAML 2.0, OAuth2, REST), CI underpins Cisco's cloud collaboration portfolio and is built for growth, adaptation, and cloud-scale applications.

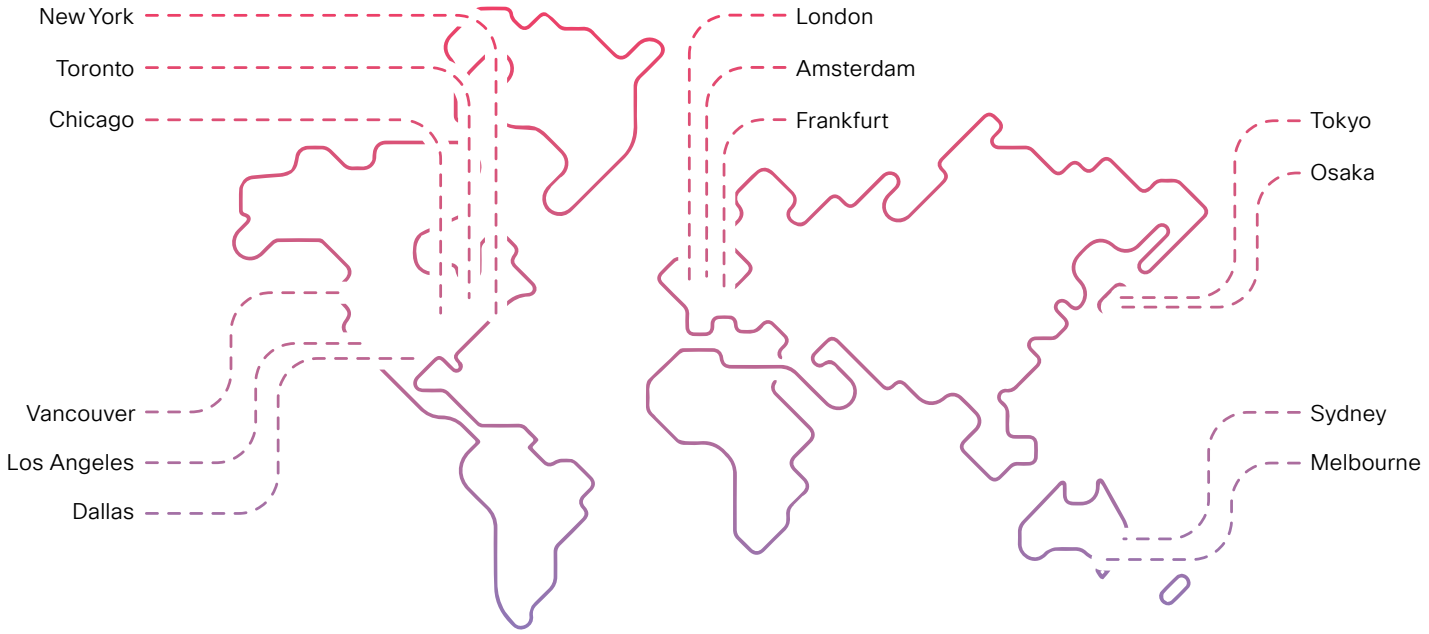
7. Availability

Webex Calling was designed for carrier-class availability (99.99% availability). Carrier-class availability is achieved via the following techniques:

- N+1 server clustering
- Geographic redundancy (ten data centers on three continents; see Figure 3)
- Automatic data replication within and between data centers
- Distributed Denial-of-Service (DDoS) detection and prevention

The Webex Calling Disaster Recovery Plan outlines the redundancy design of the network and services elements operated by Webex Calling engineering and operations teams and focuses on quickly returning network and service functionality to a working state in the event of a disaster. Cisco provides Webex Calling services through geographically redundant data centers.

Figure 3. Locations of data centers



These data centers contain all data network and server equipment required to provide service to customers. The offices where Cisco employees reside are physically independent from these data center locations. As a result, an event that would render one of the Cisco's employee offices unavailable would have no effect on the service being provided to customers through the data centers. If an event were to effect one of Cisco's offices, the Webex Calling Operations team would be able to operate the network and service elements remotely via secure VPN access from anywhere in the world.

In addition, the Webex Calling solution is designed and engineered such that if one of its data centers becomes unavailable; traffic can be redirected and processed by another data center. Cisco utilizes world-class data center vendors to provide the space and power required for the network and services to function. All vendors are SSAE 16 Type 2 compliant with greater than 99.99 percent uptime and 24-hour data center monitoring. All voice call control and voice service elements are designed to automatically migrate (failover) from one data center to another if one data center becomes unavailable. The entire failover process is automatic and will occur in near real time. All operating service elements, such as provisioning and configuration web interfaces, are designed in an active/standby architecture and can be manually migrated (failover) from one data center to another in the event that one data center becomes unavailable.

8. Webex Calling operational security

8.1 Security policy

Information, information systems, and all related assets are critical and vitally important to Webex Calling business processes. Webex Calling protects information assets in a manner commensurate with their sensitivity, value, and criticality. Security measures are employed regardless of the media on which information is stored, the systems that process information, or the methods used to transport information.

Cisco manages our information security policy using a Security Lifecycle Management process. This process includes the following components focusing on policy:

- Ratification, approval, and implementation
- Annual review, updates (as necessary), and recertification
- Annual communication and awareness training
- Exceptions management

8.2 Fraud detection

Cisco recognizes the importance of fraud detection. Therefore, we have developed a complex and extensive application that utilizes Calling Detail Records (CDR) to analyze calling patterns for fraudulent activity in order to assist Cisco operations and support teams in monitoring call traffic across the platform.

8.3 Information classification

Information classification helps to ensure that assets are applied at an appropriate level of security

Management and resources maintain strict control over the internal or external distribution of any kind of media. Control includes:

- Classifying media so the sensitively of the data can be determined
- Destroying media when it is no longer needed for business or legal reasons
- Determining whether to shred, incinerate, or pulp hand-copy materials so that data cannot be reconstructed
- Secure storage containers for materials that are to be destroyed

8.4 Asset management

Infrastructure asset management is the combination of management, financial, economic, engineering, and other practices applied to physical assets with the objective of providing the required level of service in the most cost-effective manner.

Webex Calling implements an infrastructure asset management inventory of systems and components, which consist of a method to accurately and readily determine owner, contact information, and the purpose of an asset. Asset management can include inventory of physical hosts as well as virtual machines.

Operations management is responsible for all assets deployed within the service platform environment. Unmanaged or unserviceable assets within the environment are not permitted. If an asset is discovered within the environment that is not managed, it must either be assimilated under the operations management responsibility or removed and/or blocked from the environment.

We recommend customers maintain inventory logs of all media and conduct media inventories at least annually, and at the time of asset moves, adds, changes, and disposal.

8.5 Segregation of duties

Segregation of duties is enforced as a method for reducing the risk of accidental or deliberate system misuse. Due diligence with policies, process, and procedures prevents any single person from accessing, modifying, or using assets without authorization or detection.

The initiation of an event is separate from its authorization. The design of these controls provides for oversight and governance to the possibility of collusion.

Development, test, and production environments for IT infrastructure and applications are segregated to reduce the risk of unauthorized access or changes to operational systems. The team establishes, documents, and reviews an access control procedure based on business and security requirements for access. Configuration and application code is stored in an encrypted, secure database.

8.6 Logging and monitoring

The operations team has extensive operational processes to support high availability. These processes include the selection of key human resources, support and contact processes, system logging, monitoring, system testing processes, and network performance. Any anomaly resulting in alarms is addressed based on severity.

Operations continuously monitors all servers, Internet connectivity, latency, availability, bandwidth, and severity in maintaining these server network performances. All operational and security logs are retained for extended periods of time to ensure extended availability. The network operations team regularly reviews these logs as part of capacity planning.

8.7 Vendor management-supplier relationships

Cisco manages a vendor security assessment program to ensure that all third-party services provided to Webex Calling maintain a security posture commensurate with security risk and compliance requirements. As part of the program, key vendors are periodically reevaluated to ensure there are no changes to their security posture.

8.8 Change management

Change management is an important facet of service management, and a standard process by which change is introduced into the service delivery network. Change management is crucial to successful implementation of any change. Change is initiated by a variety of groups: engineering, systems engineering, service management, support, professional services, and even the customer.

It is important that the process of implementing any change is designed, reviewed, and communicated across all organizations, and that it is performed within a well-advertised time window. This allows all stakeholders to be informed about the change, anticipate issues from any perspective, be aware of it occurring, and be able to attribute anomalous behaviors, should they occur to the change being introduced. Cisco maintains a public web page that provides real-time information on Webex Calling scheduled maintenance.

8.9 Human resources

8.9.1 Administrator and developer background check

Cisco has established a background check policy to set for the process and procedures related to background checks on designated individuals and entities.

8.9.2 Terms and condition of employment: Acceptable use case

Employees and external parties using, or having access to Cisco assets, are made aware of the policies concerning their acceptable use as defined in the Cisco Policy and IT Handbook. All employees and contractors are required to sign off on having read and understood the Cisco Policy and IT Handbook. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.10 Training

All employees undergo extensive security training as part of the orientation process and receive ongoing security training annually. Depending on the job role, additional security relevant training may be required.

8.11 Customer support

Customer support engineers ensure that all systems and client applications are up and operational by utilizing tools that continuously monitor the health of every system component. These tools alert personnel at the first sign of any problem so that potential issues can be resolved even before they impact the operations of the network. These tools can also initiate automated problem resolution procedures (such as running diagnostics).

Support engineers also monitor network operations and respond to network emergencies as well as act as a critical communication link between customer support and its clients. Support engineers record customer-reported problems in an automated problem-tracking system and coordinate the ongoing work necessary to quickly resolve them to the client's satisfaction.

This policy, together with the tiered support structure, helps to ensure that a support incident protects against revealing private data to an unauthorized person.

8.12 Information security incident management

Cisco's Incident Response Plan Management Manual follows the National Institute of Standards and Technology (NIST) 800-61 Computer Security Handling Guide. Incident management policies are applied to services personnel who provide a business-critical service, or maintain any application, software, or hardware that supports a business-critical service.

The goal of incident management is to restore normal service operations as quickly as possible and minimize the impact on business operations. Normal service operation is defined as operating within the agreed Service-Level Agreement (SLA) limits.

Cisco documents policies and procedures to handle security incident response and evaluation. Security incidents are responded to in seven stages: identify, document, communicate, contain, assess, recover, and eradicate.

8.13 Business continuity and disaster recovery

Webex Calling has business continuity plan scripts for its operational units. The organization maintains its operations, including spare capacity in multiple data centers, to ensure continuous availability. The organization adheres to guidance in ISO 22301, which specifies requirements for establishing and maintaining an effective business continuity management system.

Testing for the business continuity plan is scheduled annually. Following a real-world incident, follow-up actions and post-mortem analysis is conducted for the purpose of evaluating and improving future operations. The business impact analysis reflects on the organization's designs and evaluates its business continuity and disaster recovery systems according to levels of risk assessed against a variety of operational failure scenarios to ensure that operational commitments are consistently met.

The organization implements backup procedures. Incremental backups are conducted daily and are stored offsite for at least three weeks, full weekly backups are stored offsite for at least three weeks, and some backups are retained for years. Backups are stored on storage nodes in two redundant data center locations, and also in encrypted third-party cloud storage. Backup integrity is tested at least monthly in practice, and backup testing is required in conjunction with annual testing of the contingency plan.

9. Industry standards and compliance

Webex Calling has ISO 27001:2013 certification and has been assessed against the additional controls of ISO 27017:2015 and ISO 27018:2019. ISO is annually reviewed for recertification. Webex Calling also has SOC 2 Type 2 attestation to the applicable trust services criteria and related controls of security, availability, confidentiality and privacy. SOC 2 attestation is also done annually.

Webex Calling is certified to these standards:

- ISO 27001: 2013
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- SOC 2 Type II for applicable trust services criteria for security, availability, confidentiality
- SOC 2 Type II Privacy
- SOC 3

Compliance with these standards entails maintaining a high level of operational security, performing vulnerability assessments and penetration tests, undergoing annual audits by a third-party auditor, and adhering to an SLA for incident response times.

Webex Calling has also conducted a HIPAA self-assessment based on the U.S. Department of Health and Human Services (HHS) Security Risk Assessment tool, as well as a Payment Card Industry Data Security Standard PCI DSS v3.2.1 self-attestation of compliance.

10. Transparency

Cisco is committed to publishing data regarding requests or demands for customer data that we receive from law enforcement and national security agencies around the world. We will publish this data twice yearly (covering a reporting period of either January to June or July to December). Like other technology companies, we will publish this data six months after the end of a given reporting period in compliance with restrictions on the timing of such reports.

More information can be found at:
cisco.com/web/about/doing_business/trust-center/transparency-report.html

Cisco maintains a privacy data sheet that describes the data collected by the Webex Calling service, how such data is protected, and the retention periods for that data.

Conclusion

Businesses, institutions, and government agencies worldwide rely on Webex Calling for critical business communications. For all these companies and agencies, security is a fundamental concern. Cloud-based telephony must provide multiple levels of security for tasks that range from placing calls to authenticating mobile participants to collaborating using the Webex App and Webex Meetings services.

Webex Calling offers a scalable architecture, carrier-class availability, and multilayer security that is validated and continuously monitored to comply with stringent internal and third-party industry standards. We connect everything more securely to make anything possible.

Contact Cisco Sales to get started with a free 90 day trial of Webex Calling.

Learn more about security on the Webex collaboration platform.

Learn more about Webex Meetings security.

Learn more about the Webex Single Platform Advantage.

For more information
Please visit webex.com

July 2021