Webex Calling Security White Paper

Proprietary
For Authorized Use Only

Copyright Notice

Introduction

Cisco Webex Calling is a cloud-based phone system optimized for midsize businesses. It has essential business calling capabilities you are likely to need. The system helps eliminate the expense and complexity of managing and securing an on-site phone system. We keep the Webex Cloud always on and always up to date so you can focus on your business.

For all these companies and agencies, security is a fundamental concern. The Webex Calling must provide multiple levels of security for tasks that range from Administrative functions to end-users securely interacting with the phone system. Cisco makes security the top priority in the design, development, , and maintenance of its networks, platforms, and applications. You can incorporate Cisco Webex Calling into your business processes with confidence, even with the most rigorous security requirements. This paper provides details about the security measures of Cisco Webex Calling and its underlying Webex infrastructure to help you with an important part of your investment decision.

What you will learn

You will learn about Cisco tools, processes, and engineering methods to secure Webex Calling, and Webex platform in general.

Cisco Webex 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 Cisco Webex security model (Figure 1) is built on the same security foundation deeply engraved in Cisco's processes.

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

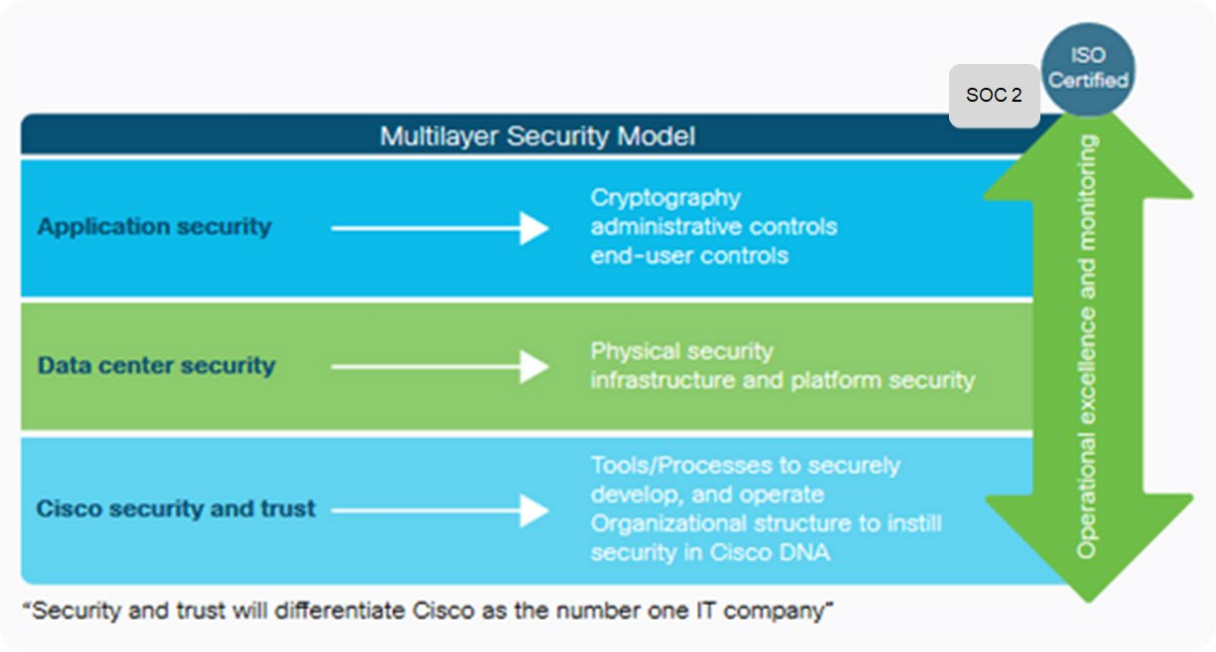

ISO Certified
SOC 2
Multilayer Security Model
Application security
Cryptography
administrative controls
end-user controls
Data center security
Physical security
infrastructure and platform security
Cisco security and trust
Tools/Processes to securely
develop, and operate
Organizational structure to instill
security in Cisco DNA
Operational excellence and monitoring
"Security and trust will differentiate Cisco as the number one IT company"

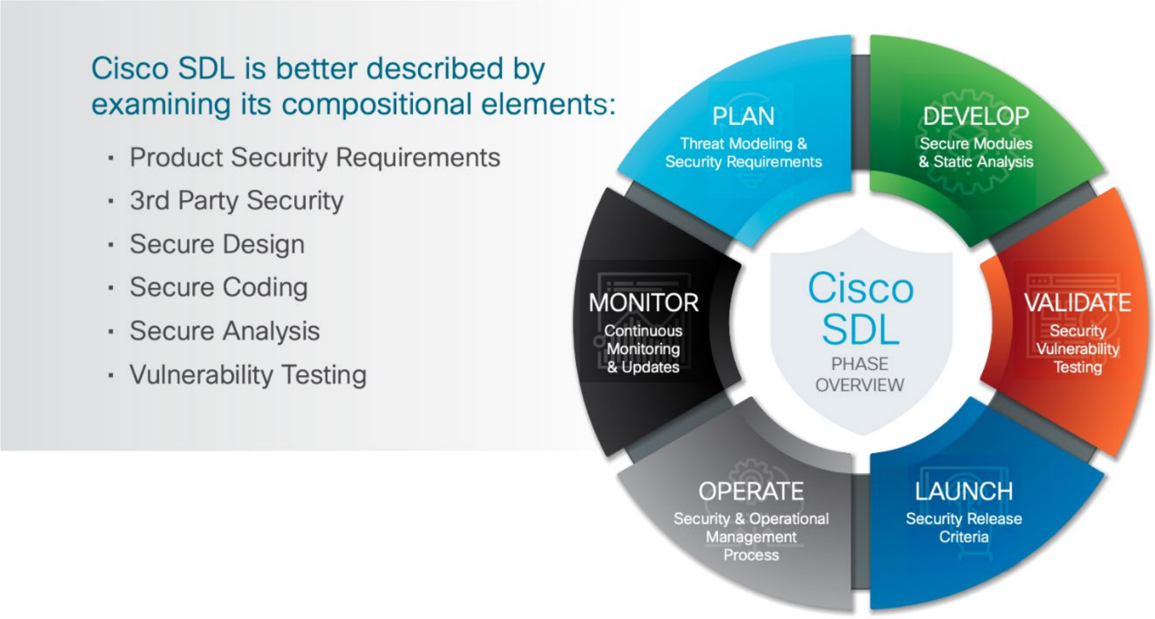
Figure 1. Cisco Security Model

Cisco Security and Trust

Cisco security tools and processes
Cisco secure development lifecycle

At Cisco, security is not an afterthought. It is a disciplined approach to building and delivering world-class products and services from the ground up. All Cisco product development teams are required to follow the Cisco Secure Development Lifecycle. 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 Cisco Webex Product Development team passionately follows this lifecycle in every aspect of product development.

Read more about the Secure Development Lifecyle.



Cisco SDL is better described by examining its compositional elements:

- Product Security Requirements
- 3rd Party Security
- Secure Design
- Secure Coding
- Secure Analysis
- Vulnerability Testing

PLAN
Threat Modeling & Security Requirements

DEVELOP
Secure Modules & Static Analysis

VALIDATE
Security Vulnerability Testing

LAUNCH
Security Release Criteria

OPERATE
Security & Operational Management Process

MONITOR
Continuous Monitoring & Updates

Cisco SDL
PHASE OVERVIEW

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf

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

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

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

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

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

Cisco Product Security Incident Response Team (PSIRT)
Cisco PSIRT is a dedicated global team that manages the inflow, investigation, and reporting of security issues related to Cisco products and services. PSIRT 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 exist to address the vulnerability, or a subsequent public disclosure of code fixes is planned to address high-severity vulnerabilities
- PSIRT has observed active exploitation of a vulnerability that could lead to a greater risk for Cisco customers. PSIRT 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, PSIRT may alert customers, even without full availability of patches

In all cases, PSIRT 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. PSIRT uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. PSIRT does not provide vulnerability details that could enable someone to craft an exploit.

Learn more about PSIRT online at cisco.com/go/psirt.

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

- Chief security officer, Cloud
- Vice president and general manager, Cisco Cloud Collaboration Applications
- Vice president, engineering, Cisco CloudCollaboration Applications
- Vice president, product management, Cisco Cloud Collaboration Applications

Cisco Webex Calling Data Center Security
Cisco Webex Calling is a cloud service solution delivered through the Cisco Webex Cloud, a highly secure service-delivery platform with industry-leading performance, integration, flexibility, scalability, and availability. The Cisco Webex Cloud is a communications infrastructure purpose-built for real-time web communications.

Cisco 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 center and cloud partners 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 zone.

Data centers are SSAE-16 and SOC-2 compliant.

Webex Calling applications and services are running on multiple servers within Cisco Datacenters. Webex Calling provides applications and services that are assured by the implementation of security and availability methods and procedures designed to cover physical access and protection, network connectivity, remote and local access, application and server management, availability and customer sensitive data. Cisco partners with datacenter operators with years of experience in design, implementation and operation of large-scale datacenters. These facilities provide physical, environmental and access security, protecting BroadSoft Government Cloud's physical and virtual application environments.

- 24x7 facility on-site security personnel
- Nondescript 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 alarmed (heat/smoke), dual interlock with cross-linked event management
- N+1 redundant UPS power system supporting entire datacenter capacity, with redundant backup generators
- Where appropriate, localized disaster compliance (seismic, flood control) Access
- Biometric scanning and/or 2-factor authentication for access
- All ingress/egress through vestibules (man-traps)
- Access requires valid government issued photo ID, and all access history is recorded for audit purposes
- Authorization required prior to access and is only provided 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 on-site 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.

Infrastructure and platform security

Platform security encompasses the security of the network, systems, and the overall data center within the Cisco Webex Cloud. 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
- Encryption of sensitive communications
- Prudent configuration of access controls, “least privilege” and “need-to-know”
- Information Backup

Hardened platforms with appropriate access and controls further restrict system capabilities to only those that are explicitly required and tolerated for expected system functionality. Systems and 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 life-cycle measures to address any associated risk. Procedures monitor the use of information processing facilities, and the team regularly reviews these activities.

Network Communications Security

Information and systems interconnected by the networks are important business assets. Maintaining, and ensuring network security at all levels is essential. Operations achieves this network security through both technical means and management procedures. Network security includes the following:

- Demilitarized Zone
- 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-purpose and enforced.

Cisco Webex Calling Application Security

Cryptography

Protecting data in motion
Cisco Webex Calling implements data encryption for access-side network communications access. Data is encrypted by TLS or Secure Real-time Transport Protocols (sRTP).

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

- Stores all user passwords using one-way hashing algorithms and salts
- Encrypts other passwords such as for SIP authentication
- Encrypts all backup files and archives

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 is applied to each system, application, database, or network utilized to manage various types of data classifications and the users that access that data. These controls consist of standardized processes for requesting, approving, granting/revoking, modifying user access, user role definition, and segregation of duties analysis, least privileged access, user password, user identification policies and standards, user access auditing expectations; and network access control list and 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 to the Infrastructure and applications owned and operated/managed by Cisco Services.

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 shall not be distributed beyond the single user and or group/shared credentials are not shared/ distributed
- Addition, deletion and modification of user IDs, credentials, and other identifier objects is controlled by the system

- Restriction of access to privileged user ID to 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 / disabled
- Manage IDs used by third parties to access, support or maintain system components

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.

User Authentication

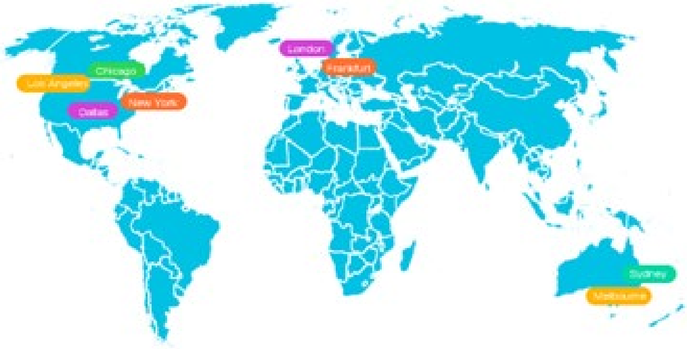
All subscribers will be registered in Cisco Collaboration Webex Common Identity Service (commonly known as "CI") -- a cloud-scale identity platform that provides either standalone identity management or customer premises hybrid identity integration. Integrations include Active Directory user account replication, Single Sign On with major providers (Okta, Ping Identity, etc.) and customer consumable APIs. Built on the latest technology and standards (ex. SAML 2.0, OAuth2, REST), CI underpins Cisco's cloud collaboration portfolio, and is built for growth, adaptation and cloud-scale applications.

Cisco Directory Connector is an on-premises application for identity synchronization to the cloud. It involves the downloading of the connector software from Cisco Webex Control Hub and installing it on a local machine. With Cisco Directory Connector, one can maintain your user accounts and data in the Active Directory single source.

Availability

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

- N+1 server clustering
- Geographic Redundancy (8 datacenters on 3 continents)
- Automatic data replication within and between Datacenters
- Distributed Denial of Service (DDoS) detection and Prevention



Three regional platforms
North America, EMEA and APAC

- Offer services to multinational customers from a single region
- Secure data and traffic within chosen region
- Bring your PSTN and networks to the platform

The Cisco Cloud Calling Disaster Recovery Plan outlines the redundancy design of the network and services elements operated by Cisco Cloud 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 services through geographically redundant 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 Cloud Calling Operations team would be able to operate the network and service elements remotely via VPN access from anywhere in the world.

Cisco provides Cloud Calling services through data network and server equipment located in geographically redundant data centers. Each data center contains a full complement of all network and service components. In addition, each data center is designed and engineered such that in the event that one data center 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 99.999% uptime and 24-hour data center monitoring. All voice call control and voice service elements are designed to automatically migrate (failover) from one datacenter to another if one data center becomes unavailable. The entire failover process is automatic and will occur in near real time. All service 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. Once initiated, the entire failover process will take less than 2 hours.

Cisco Webex Calling Operational Security

Security Policy

Information, information systems, and all related assets are critical and vitally important to Cisco, Cisco Webex Calling business processes. Cisco 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 its information security policy using a Security Life-Cycle Management process. This process includes the following components focusing on Policy:

- Security Life-Cycle Review
- Ratification, Approval and Implementation
- Annual Review, Updates (as necessary), and Recertification.
- Annual Communication and Awareness Training
- Exceptions Management

Fraud Detection

Cisco recognizes the importance of fraud detection and has developed a complex and extensive application which utilizes Calling Detail Records (CDR) to analyze calling patterns for fraudulent activity in order to assist Cisco Operations and Support teams to monitor call traffic across the platform.

Industry Standards and Compliance

Cisco Webex Calling service and systems are in queue for ISO 27001:2013 audit and certification and certification is expected in 2019. ISO is annually reviewed for recertification.

Cisco Webex Calling also SOC2 Type 1 attestation. SOC2 Type 2 attestation is under way and expected in 2019.

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.

Cisco Webex Calling has also conducted a HIPAA self-assessment based on the HHS Security Risk Assessment tool,

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:
http://www.cisco.com/web/about/doing_business/trust-center/transparency-report.html

Cisco Webex Calling maintains a Privacy Data Sheet describing the data collected, how it is protected, and what the retention periods for that data are.

Information Classification

Information classification assures that assets are applied an appropriate level of security and protection based on content sensitivity and value of asset to business service and business continuity.

Management and resources maintain strict control over the internal or external distribution of any kind of media, including the following:

- Classify media so the sensitively of the data can be determined
- Destroy media when it is no longer needed for business or legal reasons
  Shred, incinerate, or pulp hand-copy materials so that the cardholder data cannot be reconstructed. Secure storage containers used for materials that are used to be destroyed.

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.

Cisco 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 purpose of asset. Asset Management shall 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 not serviceable assets within the environment are not permitted. If an asset is discovered within the environment that is not managed, it must be either assimilated under the Operations management responsibility or removed and or blocked from the environment.

Maintain inventory logs of all media and conduct media inventories at least annually, and at time of asset moves, adds, changes and disposal.

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.

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 result in alarms and are address 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.

Vendor Management – Supplier Relationships

Cisco manages a vendor security assessment program to ensure that all 3rd party services provided to Cisco 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 that there are no changes to their security posture.

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 is crucial to successful implementation of the change. Change is initiated by a variety of groups: engineering, systems engineering, service management, support, professional services and even customer. It is important that the process of implementing any change is designed, reviewed, communicated across all organizations and 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 https://status.broadsoft.com/ that provides real time information on Cisco Webex Calling scheduled maintenance.

Human Resources

Administrator and Developer Background Check
Cisco has established a Background Check Policy to set forth the process and procedures related to the conduct of FCPA and other background checks for designated individuals and entities.

Terms and Condition of Employment - Acceptable Use Case
Employees and external party users 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.

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

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 operation and respond to network emergencies but also provide 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 on-going work necessary to quickly resolve them to the client's satisfaction. Cisco maintains a public web page https://status.Cisco.com/ that provides real time information on Cisco Webex Calling operational status.

This policy, together with the tiered support structure, ensures that a support incident that will protect against revealing private data to an unauthorized person.

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 identified in and applied to services who are providing a business-critical service, or maintaining any application, software, or hardware which 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 policy and procedures to handle security incident response and evaluation. Security Incidents shall be responded to in seven stages: identify, document, communicate, contain, assess, recover and eradicate.

Business Continuity and Disaster Recovery

Cisco 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. The various components of the organization's operations each have separately documented Recovery Point Objective (RPO) and Recovery Time Objective (RTO) targets.

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 that the organization designs and evaluates its business continuity/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 off-site for at least three weeks, full weekly backups are stored off-site 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 it is also in encrypted 3rd 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.

Conclusion

Businesses, institutions, and government agencies worldwide rely on Cisco® Webex Calling solutions. 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 Cisco Webex Teams and Meetings services.

Cisco 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.