Collaborate with confidence.

Gain a secure advantage with Cisco Webex Calling from Verizon.

White paper

To bring you a cloud-based phone system that's built for businesses of all sizes, Verizon, in partnership with Cisco, offers Cisco Webex® Calling. Delivered from the global Webex® collaboration platform, Webex Calling gives you essential business-calling capabilities for desktop, mobile and remote workers. It leverages cloud technology to provide greater flexibility, rapid innovation, predictable operating expenses and near-instant global scalability. And it does so while helping to protect your on-premises investments by connecting them to the secure Webex platform.

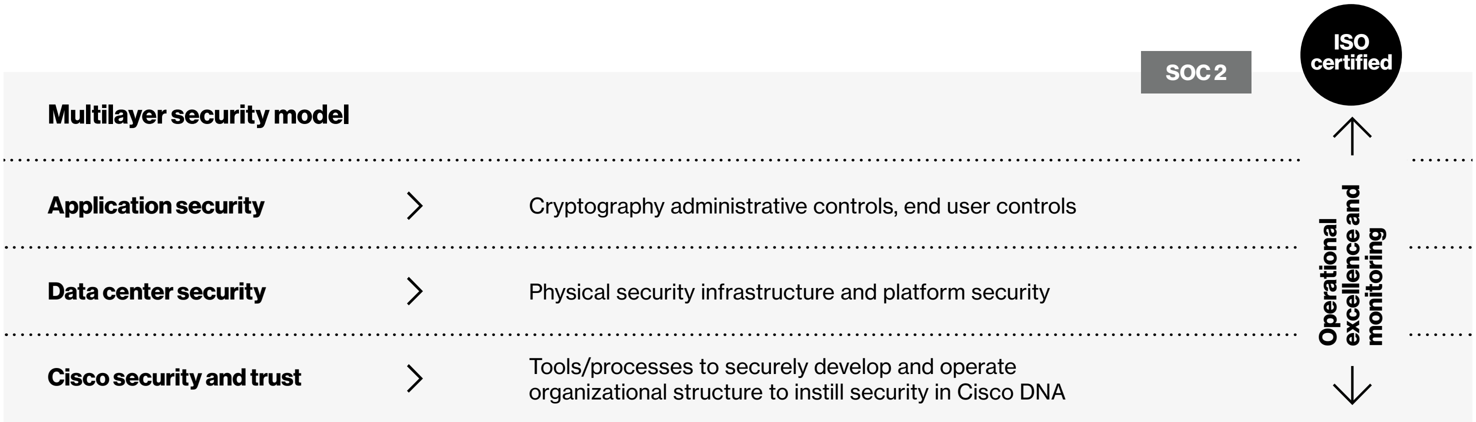
Cisco makes security the top priority in the design, development, deployment and maintenance of its networks, platforms and applications. And Webex Calling meets even the most rigorous security requirements. Both Webex Calling and the Webex platform provide multiple layers of security to protect tasks that range from administrative functions to end- user interactions. That means you can incorporate Webex Calling into your business processes with confidence.

To help you in your investment decision for Webex Calling, this paper outlines core security measures that support this solution and the Webex collaboration platform infrastructure. It also includes a discussion about the Cisco® tools, processes, certifications and engineering methods that secure Webex Calling and the Webex collaboration platform.

Built on a multilayer security model

Cisco firmly commits to maintaining leadership in cloud security. Its Security and Trust organization works with teams throughout the company to build a security, trust and transparency framework. This framework helps support the design, development and operation of core infrastructures to meet the highest levels of security in nearly everything Cisco does.

Both Verizon and Cisco are dedicated to providing you with the information you need to mitigate and manage cybersecurity risks. The Webex security model is built on the same security foundation that Cisco uses across all its products and solutions (see Figure 1). The Webex organization consistently follows this model's foundational elements to securely develop, operate and monitor Webex services.



Multilayer security model

Application security › Cryptography administrative controls, end user controls

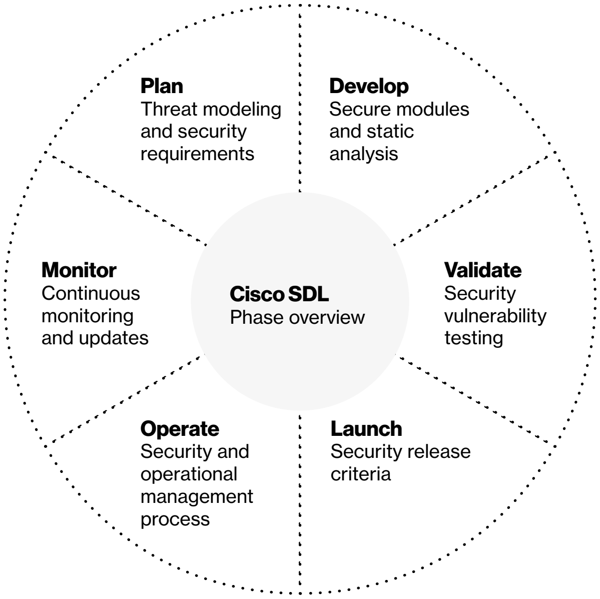
Data center security › Physical security infrastructure and platform security

Cisco security and trust › Tools/processes to securely develop and operate organizational structure to instill security in Cisco DNA

Figure 1. Cisco security model

Increasing product resilience and trust

Additionally, Cisco requires all of its product development teams to follow its Secure Development Lifecycle, or SDL (see Figure 2). Cisco designed this repeatable and measurable process to help increase the resiliency and trustworthiness of its products. The combination of tools, processes and awareness training introduced in all phases of the SDL help ensure defense in depth against potential cyberthreats. It also provides a holistic approach to product resiliency. The Webex product development team follows this life cycle in every aspect of Webex Calling product development.


Plan
Threat modeling and security requirements
Develop
Secure modules and static analysis
Monitor
Continuous monitoring and updates
Cisco SDL
Phase overview
Validate
Security vulnerability testing
Operate
Security and operational management process
Launch
Security release criteria

Cisco SDL is better described by examining its compositional elements:

- Product security requirements
- Third-party security
- Secure design
- Secure coding
- Secure analysis
- Vulnerability testing

Figure 2. Cisco Secure Development Lifecycle

To learn more about the Cisco Secure Development Lifecyle, visit
https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html#~trustworthysolutionsfeatures

Tools to help drive consistent security decisions

The Cisco Security and Trust organization also provides the processes and tools needed to help all of its developers make consistent security decisions. Having dedicated teams that build and provide these foundational security tools helps minimize uncertainty during the product development process.

The following are just a few examples of the tools that the Cisco Security and Trust organization provides Cisco developers:

- Product security baseline requirements for all Cisco products
- Threat-builder tools used for threat modeling
- Coding guidelines
- Validated or certified libraries for developers to use instead of writing their own security code
- Security vulnerability testing tools that provide static and dynamic analyses to test products for security defects after development
- Software tracking that monitors Cisco and third-party libraries for vulnerabilities with alerts to notify product teams of identified vulnerabilities

Instilling security processes company-wide

Cisco dedicates a number of departments and individual positions to instill and manage security processes across the entire organization. Specifically for Webex, every person on the team is responsible for security. Those within the greater Cisco organization who have dedicated security responsibilities include its Chief Security Officer for Cloud, Vice President and General Manager for Cisco Cloud Collaboration Applications, Vice President of Engineering for Cisco Cloud Collaboration Applications, and Vice President of Product Management for Cisco Cloud Collaboration Applications.

Additionally, Cisco relies on its Information Security (InfoSec) Cloud team, Product Security Incident Response Team (PSIRT) and Cisco Talos® threat intelligence team to help stay on top of security threats and challenges.

Cisco InfoSec Cloud team

The Cisco InfoSec Cloud team has the responsibility to provide you a safe Webex environment. It does so by defining and enforcing security processes and tools for every aspect related to the delivery of Webex. The InfoSec team continuously works on helping to improve the security posture of Webex to fend off potential threats. The InfoSec Cloud team also works with other teams across Cisco to respond to any security threats to Webex.

Cisco PSIRT team

The global Cisco PSIRT team dedicates itself to managing the inflow, investigation and reporting of security issues related t o Cisco products and services. The PSIRT team publishes security information in a variety of ways, using the severity of specific security issues to decide how and when this information should be published. The following conditions may impact the type of reporting Cisco does:

- Vulnerabilities and high-severity vulnerabilities—The PSIRT team uses software patches or workarounds to address vulnerabilities, as well as provide public disclosures of code fixes to address high-severity vulnerabilities
- Active exploitations—When the PSIRT team observes an active exploitation of a vulnerability that could lead to a greater risk to its customers, it may speed up the publication of a security announcement to describe the vulnerability even if patches are not fully available
- Public awareness of a vulnerability—When the public becomes aware of a vulnerability that may impact Cisco products in a way that might lead to greater risks, the PSIRT team may alert customers even if patches are not fully available

To learn about vulnerabilities published by the Cisco PSIRT team, visit
https://tools.cisco.com/security/center/publicationListing.x

No matter the case, the PSIRT team works to disclose at least the minimum amount of information that its product users need to assess the effects of a vulnerability. It also takes steps needed to help protect users' environments. The team uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. It does not provide vulnerability details that could enable a potential hacker to create an exploit.

Cisco Talos threat intelligence team

To help provide unmatched visibility and threat protection for its products and customers, Cisco created and deployed one of the largest commercial threat intelligence teams in the world: Cisco Talos. Its 300-plus researchers work to uncover and block a broad spectrum of malicious domains, IPs, URLs and files that cybercriminals may use in their attacks. Cisco Talos also feeds huge volumes of global internet activity into a combination of statistical and machine learning models to identify emerging attacks currently being staged on the internet. The team uses anti-virus engines, Cisco Advanced Malware Protection (AMP) and sandboxing from Cisco Threat Grid® to take advantage of intelligence drawn from millions of new malware samples that it analyzes daily to help generate the most effective defense against malicious files.

Multifaceted data center protections

Cisco delivers Webex Calling as a cloud solution through its Webex cloud. This cloud provides a highly secure service delivery platform with industry-leading performance, integration, flexibility, scalability and availability. Cisco designed the Webex cloud communications infrastructure specifically to fuel near real-time web communications.

Cisco powers Webex Calling with computing equipment housed in multiple data centers located around the world. It has strategically placed these data centers near major internet access points to decrease latency. These data centers use dedicated high-bandwidth fiber to route traffic across the globe.

Cisco makes sure its data centers are SSAE 16 and SOC 2 compliant. This includes evaluating them annually for SOC 2 attestation of compliance in the following areas:

- Physical security perimeter
- Physical entry controls
- Securing of offices, rooms and facilities
- Protection against external and environmental threats
- Work in secure areas
- Supporting utilities
- Cabling security
- Delivery and loading zones

Cisco runs its Webex Calling applications and services on multiple servers within its data centers. It uses security and availability methods and procedures specifically designed to help assure that these applications and services meet specific criteria for the following:

- Physical access and protection
- Network connectivity
- Remote and local access
- Application and server management
- Availability
- Customer-sensitive data

Additionally, Cisco and Verizon partner with data center operators who have years of experience in design, implementation and operation of large-scale centers. These facilities provide physical, environmental and access security to help protect the Webex Calling physical and virtual application environments.

Examples of these environmental protections include:

- Security personnel onsite daily, 24/7
- 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 alarm (heat and smoke) and dual interlock with cross-linked event management
- N+1 redundant uninterruptible power source (UPS) system to support the entire data center capacity, as well as redundant backup generators
- Location-specific disaster recovery plans, such as for seismic or flood control
- Biometric scanning, two-factor authentication (2FA) for access
- All physical ingress and egress through vestibules, also known as mantraps
- 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 walled off from co-location areas
- For both physical ingress and egress, onsite security staff inspects all material upon arrival

Administrators use 2FA when accessing Webex Calling computing assets. Cisco logs all user and administrator activity. To detect and prevent attacks or misuse, the 24/7 Webex Calling Security Operations Center (SOC) monitors system logs as well as intrusion detection system (IDS) and firewall alerts.

Hardened infrastructure and platform

Webex platform security measures cover the network, systems and data centers. Network services engineers harden and patch the operating systems and infrastructure to help protect its systems from various security vulnerabilities. They work to make sure servers deliver data in a secure, reliable fashion. Hardening efforts for the operating system, middleware and application include:

- Security-sensitive ongoing hardening
- Security review and acceptance validation before allowing production deployment
- Vulnerability scanning and assessment
- Security patching
- Protection against malware
- Robust logging of implementations and configurations
- Strong authentication
- Encryption of sensitive communications
- Prudent configuration of access controls, including least privilege and need-to-know
- Information backup

Additionally, hardened systems use access and controls to appropriately limit system capabilities to only what is explicitly required and tolerated for the system to function as expected. Cisco cross-checks and tests systems, software versions and upgrades in a secure staging environment before allowing them to be deployed for production and use. It also monitors and logs its information systems for potential technical vulnerabilities. The operations team evaluates any exposures to such vulnerabilities and takes appropriate patch management life-cycle measures to address any associated risks. The team then employs specific processes to monitor the use of its information processing facilities and regularly reviews these activities.

Secure network communications

The information and systems that networks connect to are vital business assets. That's why it's essential to help maintain and ensure network security at all levels. Cisco's operations team employs technology and managerial procedures in its efforts to provide this level of network security. This includes implementing the following:

- Demilitarized zones (DMZs)
- Firewalls
- Intrusion detection
- System authentication
- Data encryption

Cisco's security management team determines the security features, service levels and management requirements for all its 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 that use the network, including in-transit information. To protect against malicious code, the management team relies on detection, prevention and recovery controls, as well as appropriate user-awareness procedures.

Cisco also maintains audit logs to record all user activities, exceptions and information security events. Both the operations and security teams use these logs to help them with access control monitoring and assist them with potential investigations that could be needed in the future. Cisco has independent reviews conducted on a regular basis. These reviews help make sure that Cisco's information security processes continue to be sufficient, not have gaps, enforce policy and actually do what they were designed to do.

Security for the Cisco Webex Calling application

Cisco secures the Webex Calling application in a variety of ways, including using such methods as encryption, access controls and user authentication. For access-side network communications access, Cisco encrypts data using transport layer security (TLS) or Secure Real-time Transport Protocol (SRTP). For data at rest, Webex Calling uses the following safeguards to help protect the storage of your business-critical organizational and user data:

- Stores all user passwords with one-way hashing algorithms and salts
- Encrypts other passwords, such as Session Initiation Protocol (SIP) authentication
- Encrypts all backup files and archives

Webex Calling also governs the appropriate levels of access controls within the operating environment through policy definition and implementation. It applies access controls that match these policies to each system, application, database and network it uses. This process includes managing access controls for different types of data classifications and the users who can access those data types.

The access controls use standardized processes for requesting, approving, granting, revoking and modifying user access according to user role definitions. Additional aspects of access control include segregation of duties analysis, least-privileged access, user passwords, user identification policies and standards, user-access auditing expectations, network access control lists, and auditing of network and access activities.

Access control policy requires the use of user accounts and access controls for systems and applications that need access to configuration and information. The scope of the policies and controls only covers access to the infrastructure and applications owned and operated or managed by the Cisco Customer Experience organization (Cisco Services).

User account and access controls meet the following security requirements:

- Requires all users to be assigned unique IDs and authenticated to gain access to assigned privileged components
- Doesn't distribute IDs and authentication credentials beyond a single user and doesn't share or distribute group or shared credentials
- Controls addition, deletion and modification of user IDs, credentials and other identifier objects
- Restricts access to privileged user IDs to the least privileges necessary to perform job responsibilities
- Requires privileged users to be identified for specific access
- Immediately revokes access to terminated users
- Removes or disables inactive user accounts
- Manages IDs used by third parties to access, support or maintain system components

Cisco management or designated security officers define, approve, implement and oversee these controls. Both Cisco and an independent auditing authority review these controls for accuracy and effectiveness at least annually.

In terms of user authentication, Cisco requires all subscribers to register with the Cisco Collaboration Webex Common Identity Service, also known as CI. CI is a cloud-scale identity platform that provides the choice of stand-alone identity management or customer premises hybrid identity integration. The service supports the following hybrid identity integrations:

- Active Directory user account replication
- Single sign-on (SSO) from major providers, such as Okta, Ping Identity and others
- Customer consumable application programming interfaces (APIs)

CI is built on the latest technology and standards, including SAML 2.0, OAuth2 and REST. Designed for growth, adaptation and cloud-scale applications, CI plays an integral supporting role in Cisco's cloud collaboration portfolio.

Additionally, Cisco provides its Directory Connector as an on-premises application for identity synchronization to the cloud. It lets you maintain your user accounts and data in an Active Directory single source. To use the Directory Connector, you need to download the connector software from the Cisco Webex Control Hub and install it on one of your local machines.

Providing 99.99% availability

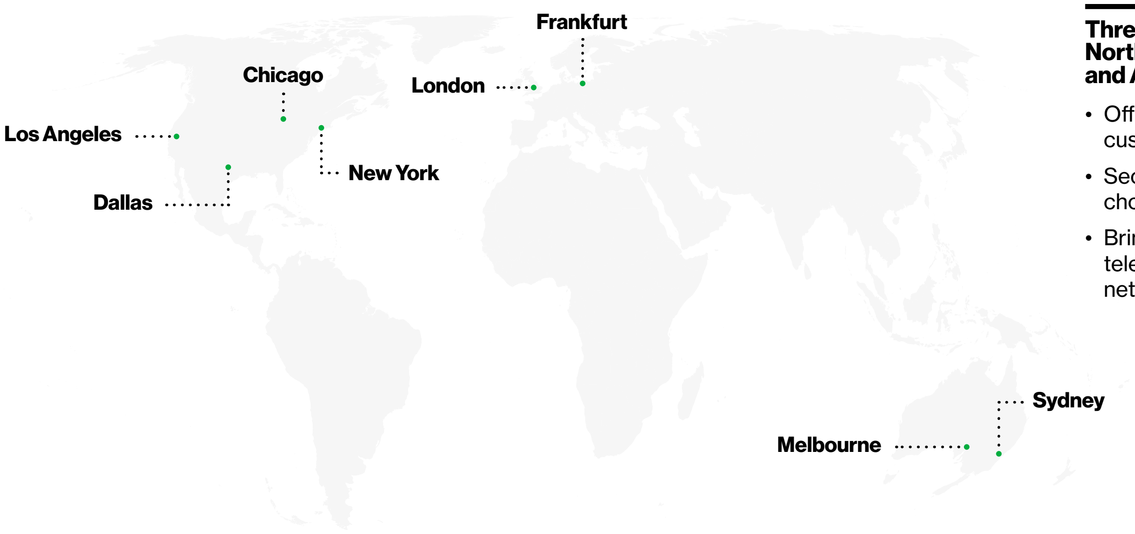
Cisco designed Webex Calling for enterprise-grade availability (99.99% availability). It strives to achieve this level of availability using the following methods:

- N+1 server clustering
- Geographic redundancy, including eight data centers on three continents (see Figure 3)
- Automatic data replication within and between data centers
- Distributed-denial-of-service (DDoS) attack detection and prevention

To help return network and service functionality to a working state as quickly as possible if a disaster strikes, Cisco has created its Cisco Cloud Calling Disaster Recovery Plan. The plan outlines the redundancy design of network and services elements that the Cisco Cloud Calling engineering and operations teams operate. As part of this plan, Cisco provides cloud-calling services through geographically redundant data centers. These data centers contain all data network and server equipment required to provide service to customers.

Additionally, the offices where Cisco employees work are physically independent from these data center locations. As a result, an event that might render one of Cisco's employee offices unavailable would likely have no effect on the service Cisco provides customers through its data centers. And if an event impacted one of Cisco's offices, the Cloud Calling Operations team would be able to operate the network and service elements remotely using VPN access from almost anywhere in the world. In addition, Cisco has designed and engineered each data center in such a way that if one data center becomes unavailable, it can redirect traffic to another data center for processing.

Cisco uses world-class data center vendors to make sure its data centers have the space and power required for its network and services to function properly. All vendors must be SSAE 16 Type 2 compliant with greater than 99.99% uptime and 24-hour data center monitoring. All voice-call control and voice-service elements have been designed to automatically migrate (failover) from one data center to another if a data center becomes unavailable. The entire failover process occurs automatically and in near real time. All operating service elements, such as provisioning and configuration web interfaces, have been designed with an active/standby architecture. If needed, they can be manually migrated from one data center to another if a data center becomes unavailable.



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 public switched telephone network and networks to the platform

Figure 3. Locations of data centers

Helping to maintain operational security

Cisco employs several methods in a variety of areas to help maintain the operational security of Webex Calling. These include the following:

- Security policy
- Fraud detection
- Information classification
- Asset management
- Segregation of duties
- Logging and monitoring
- Vendor management and supplier relationships
- Change management
- Human resources
- Training
- Customer support
- Information security incident management
- Business continuity and disaster recovery

Security policy

Information, information systems and all related assets play vital roles in Webex Calling business processes. Cisco makes sure Webex Calling protects information assets in a method that's on par with their sensitivity, value and critical nature. It employs security measures regardless of the media format used to store information, the systems that process information or the methods used to transport information. Additionally, Cisco manages the Webex Calling information security policy using its security life-cycle management process. This process involves the following policy-focused components:

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

Fraud detection

Cisco recognizes the importance of fraud detection. That's why it has developed a complex and extensive application that uses calling detail records (CDR) to analyze patterns for possible fraudulent activity. This helps Cisco operations and support teams monitor call traffic across the platform.

Information classification

Information classification helps Cisco apply the appropriate levels of security and protection to assets based on their content sensitivity, value to business service and impact on business continuity. Cisco management and resources maintain strict control over the internal or external distribution of any kind of media. This control includes:

- Classifying media to help determine data sensitivity
- 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 cardholder data cannot be reconstructed
- Securing storage containers for materials that will be destroyed

Asset management

Infrastructure asset management combines the application of management, financial, economic, engineering and other practices to physical assets. Its objective is to provide the necessary level of service in the most cost-effective manner. Webex Calling implements an infrastructure asset management inventory of systems and components to accurately and readily determine their owners, contact information and purpose. Asset management can include inventories of physical hosts as well as virtual machines.

Cisco operations management has responsibility for all assets deployed within the service platform environment. It doesn't allow unmanaged or unserviceable assets within the environment. If operations management discovers an unmanaged asset, it will either assimilate the asset under this team's responsibility or remove and block the asset from the environment.

In addition to our asset management efforts, Cisco recommends its customers to maintain their own inventory logs of all media and conduct media inventories at least annually, as well as when an asset moves, adds, changes or is disposed of.

Segregation of duties

To help reduce the risk of accidental or deliberate system misuse, Cisco enforces segregation of duties. Due diligence with policies, process and procedures helps prevent any single person from accessing, modifying or using assets without authorization or detection.

Event initiation is separate from its authorization. Cisco uses segregation-of-duties controls to provide the oversight and governance needed to help prevent possible collusion. It segregates the development, testing and production environments of its IT infrastructure and applications to help reduce the risk of unauthorized access or changes to operational systems. The company establishes, documents and reviews access control procedures based on business and security requirements for access. Additionally, it stores configuration and application code in an encrypted, secure database.

Logging and monitoring

The Cisco operations team uses 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. It addresses anomaly-resulting alarms based on their severity. Operations continuously monitors all servers, internet connectivity, latency, availability, bandwidth and severity in maintaining server network performance. It retains all operational and security logs for extended periods of time to help ensure extended availability. Cisco's network operations team regularly reviews these logs as part of its capacity planning.

Vendor management and supplier relationships

Cisco manages a vendor security assessment program to ensure that all third-party services provided to Webex Calling maintain a security posture equal to security risk and compliance requirements. As part of this program, Cisco periodically reevaluates key vendors to ensure that no changes to vendors' security posture have occurred.

Change management

Change management plays an important role in Cisco's service management. Whenever a change is introduced into its service delivery network, Cisco uses a standard process to help ensure the successful implementation of the change. A variety of groups have the potential to initiate change, including engineering, systems engineering, service management, support, professional services, and in some cases, even customers.

Cisco recognizes the importance of designing, reviewing and communicating across all organizations the process of implementing any change. It also strives to perform all changes within their well-advertised window of time. This allows all stakeholders to be informed about the change so they can better anticipate any associated issues and appropriately attribute anomalous behaviors to the change. To help with the effort, Cisco maintains a public web page that provides real-time information on the scheduled maintenance for Cisco Webex Calling.

Human resources

Cisco has established a policy that requires its human resources team to follow specific processes and procedures in performing background checks on certain individuals and entities. This includes administrators and developers.

Additionally, all Cisco employees and external parties that use or have access to Cisco assets are made aware of and are subject to acceptable use policies for company assets. These policies are defined in the Cisco Policy and IT Handbook. All employees and contractors are required to sign off that they have read and that they understand the handbook. If Cisco discovers that an employee has violated this policy, that employee may be subject to disciplinary action, up to and including termination of employment.

Training

All Cisco employees participate in extensive security training as part of their initial orientation process. They also receive ongoing security training on an annual basis. Depending on their job roles, they may be required to take additional training on specific aspects of security.

Customer support

To help keep all Cisco systems and client applications up and operational, Cisco customer support engineers use tools that continuously monitor the health of every system component. These tools alert company personnel at the first sign of any problem. This allows Cisco to resolve potential issues before they can impact network operations. These tools can also initiate automated problem resolution procedures, such as performing diagnostics.

Cisco support engineers also monitor network operations and respond to network emergencies. They act as a critical communication link between customer support and its customers. Support engineers record customer-reported problems in an automated problem-tracking system and coordinate the ongoing work required to quickly resolve problems to your satisfaction. Cisco also maintains a public web page that provides real-time information on the operational status of Cisco Webex Calling and other Cisco Cloud solutions.

Additionally, Cisco employs policies within its tiered support structure to help prevent any private data that might exist in a support incident from being revealed to any unauthorized person.

Information security incident management

All Cisco services personnel who provide business-critical services or maintain applications, software or hardware that support such services are required to follow the company's incident management policies. Cisco details these policies in its Incident Response Plan Management Manual. This manual follows the National Institute of Standards and Technology (NIST) 800-61 Computer Security Handling Guide.

Incident management seeks to restore normal service operations as quickly as possible and minimize the impact on business operations. Cisco defines normal service operation as operating within the agreed SLA limits. Cisco documents policies and procedures to handle security incident response and evaluation. Cisco responds to security incidents in seven stages:

- Identify
- Document
- Communicate
- Contain
- Assess
- Recover
- Eradicate

Business continuity and disaster recovery

The Webex Calling organization provides business continuity plan scripts to its operational units. The organization manages its operations – as well as the spare capacity in its multiple data centers – in a way to help ensure continuous availability. The organization adheres to ISO 22301 guidelines, which specify the 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 objectives (RPOs) and recovery time objective (RTO) targets.

The organization schedules annual testing of its business continuity plan. To evaluate and improve future operations, it performs a real-world incident, follow-up actions and post-mortem analysis. The business impact analysis gives insights on the effectiveness of the organization's designs. The analysis also evaluates its business continuity and disaster recovery systems according to the levels of risk assessed against a variety of operational failure scenarios. These all help the organization in its efforts to consistently meet its operational commitments.

As part of its business continuity efforts, the organization also implements backup procedures. It conducts incremental backups daily, which it stores offsite for at least three weeks. It performs full backups every week and stores these for at least three weeks. It stores certain backups for years. It stores backups on storage nodes in two redundant data center locations. It also stores them in encrypted third-party cloud storage. The organization tests backup integrity at least monthly and requires backup testing to be performed as part of its annual contingency plan testing.

Adhering to industry standards and compliance

Webex Calling has ISO 27001:2013 certification and is annually reviewed for recertification. Additionally, Webex Calling has SOC2 Type 2 attestation. To comply with these standards, Webex Calling has to maintain a high level of operational security, perform vulnerability assessments and penetration tests, undergo annual audits by a third-party auditor, and adhere to an incident response time SLA. Webex Calling has also conducted a HIPAA self-assessment based on the HHS Security Risk Assessment tool.

Data privacy transparency

Cisco has committed to publish data regarding requests or demands it receives from global law enforcement and national security agencies for customer data. The company publishes this data twice a year. These reports typically cover periods from January to June and July to December. Similar to other technology companies, Cisco publishes this data six months after the end of each reporting period. This is in compliance with timing restrictions for these types of reports. You can find more information on these reports and requests at https://www.cisco.com/c/en/us/about/trust-center/transparency.html. Additionally, Webex Calling maintains a privacy data sheet that describes the data collected, how it is protected and the retention periods for the data.

Staying safe with Verizon

Advanced communications solutions from Verizon give you access to a host of tools to protect your communications. Our solutions can help you manage and secure desktops, laptops and mobile devices all in one place through simple access and authentication rules. We can help you secure voice calls to protect them against being intercepted by outsiders. We have solutions to help you set up your own wireless private network. We also provide backup connections to the cloud and alternate data centers to help you enjoy business continuity and data preservation against the threat of downtime.

Our security experts can help you build and test a security plan focused on your unique needs, as well as risks specific to your industry. That includes helping you create a tailored and efficient incident response plan using near real-time monitoring and big data analytics. With the sophistication and stealthy nature of today's cyberattacks, it can take months to detect a data breach on your own. We have the experience, expertise and solutions to help you detect and respond to breaches faster. And we can help you strengthen your defenses to help you protect against future breaches.

Relying on enterprise-grade calling and team collaboration services

Businesses, institutions and government agencies worldwide rely on Webex Calling for critical business communications. We know that security is a fundamental concern for you, as well as for all these companies and agencies. You need cloud-based telephony that provides multiple levels of security. That includes securing tasks from phone calls to authentication of mobile participants to collaboration with Webex Teams™ and Webex Meetings services. That's why Verizon partners with Cisco to offer Webex Calling. The solution provides you a scalable architecture with enterprise-grade availability and multilayer security. Cisco validates and continuously monitors Webex Calling to comply with stringent internal and third-party industry standards.

Taking advantage of Cisco Webex Calling through Verizon's partnership with Cisco can help you have confidence in the safety of your sensitive business information. No matter how many stakeholders or employees need to access that information and no matter the device they need in order to access it, we can help you keep it secure. This helps your workforce be better coordinated and more responsive. And it leads to happier customers.

To find out how you can take advantage of this enterprise-grade, cloud-calling and team-collaboration solution, contact your Verizon Account Manager.

To learn more about how Cisco secures Webex Calling and related services and platforms, take a look at the following Verizon and Cisco resources:

Verizon Business Communications ›

Verizon Security Services ›

Verizon Network Services ›

Webex Collaboration platform ›

Webex Meetings security ›

Cisco Webex Single Platform Advantage ›

verizon✓