Cisco Webex

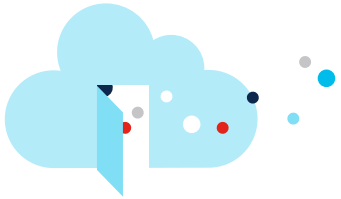
A guide to secure collaboration

What you need to know about protecting people, data, and devices

Contents

Working whenever, wherever, however

At a time when the workplace is constantly evolving, it's vital for companies to create a flexible work environment for their employees. One that enables teams to contribute from anywhere, at any time. By creating a flexible working environment, workers of all types will be empowered to collaborate at will and help the entire organization not only become more innovative and disruptive, but also more flexible and resilient in the marketplace.



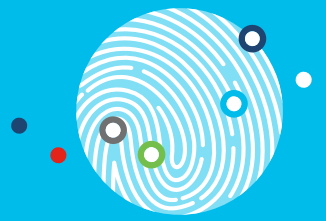
Overall, remote collaboration tools allow users to work together more closely, share ideas more quickly, and maximize productivity. Not only are they effective for your team, but they are also cost-efficient for your business.

However, remote work conditions open companies up to more risk. Remote working allows your data to be a target for cyberthieves, mischief makers, and extortionists. They are relentless, and the news is filled with stories about successful breaches that outsmarted even some of the brightest companies around.

To enable a flexible work environment, it's not just collaboration tools that are paramount, but security solutions, too.

Collaboration and security, together at last

At the intersection of collaboration, the collaboration lifecycle, and cybersecurity are gaps that hackers can exploit. And while many collaboration solutions offer “security,” that security often is included as an afterthought and can still leave holes that expose your organization.



Security needs to be more than a checkbox on a list of priorities—it should be one of the first considerations at all times.

To fully address the gaps and vulnerabilities that can be present in your collaboration ecosystem, it’s important to better understand security challenges and the solutions relevant to your specific industry.

Cisco security: A multipronged approach

One of the most sinister things about cybercriminals is their intelligence. They relentlessly search for and create new pathways around cybersecurity. That's why no single layer of security is adequate.

But with a multipronged approach that targets all security essentials, you can strengthen and widen your security net, regardless of how smart these intruders may be.

A comprehensive approach to security includes:

- Securing your users and identities through administrative control and segmentation
- Securing your applications and devices through device management and secure integration with other solutions
- Securing your content by default with true end-to-end encryption

Cisco Webex is uniquely positioned to help organizations achieve this comprehensive security with capabilities and features built into the solution, not bolted on. Unlike alternatives, Cisco Webex is built on three specific security pillars that enable the approach outlined above:

- Webex is committed to respecting the privacy of your data.
- Webex is secure by default.
- Webex has cybersecurity governance and is transparent when there are security issues (source: Cisco Webex Security Advantage).

All these layers of security capabilities are important individually, but their real power stems from the multiplier effect they achieve when acting in tandem with one another.

Section 1

Your identity should be just that—yours

Today, your users are connecting and collaborating in more ways than ever before, and in more places. Sometimes they may be interacting on external solutions that are native to other customers, partners, and businesses.

Securing your users and their user identity wherever they are working and however they are connecting is essential to supporting this new and more mobile workforce.

Webex helps secure your users through complete administrative control. A collaboration service is only as strong as the security options given to those hosting it.

Secure collaboration based on complete administrative control

Cisco Webex offers a central interface to manage your organization and users, assign services, view quality of service, monitor capacity and performance analytics, and more. With Cisco Webex Control Hub, you can set up a customer administrator with different privilege levels. They can be full administrators, support administrators, user and device administrators, read-only administrators, or compliance officers.

There are numerous ways that Webex puts control in the hands of administrators. Here are four:

Granting gatekeeper status to administrators guards against unauthorized access without disrupting the way participants can join. Webex gives administrators many options for fine-tuning password enforcement.

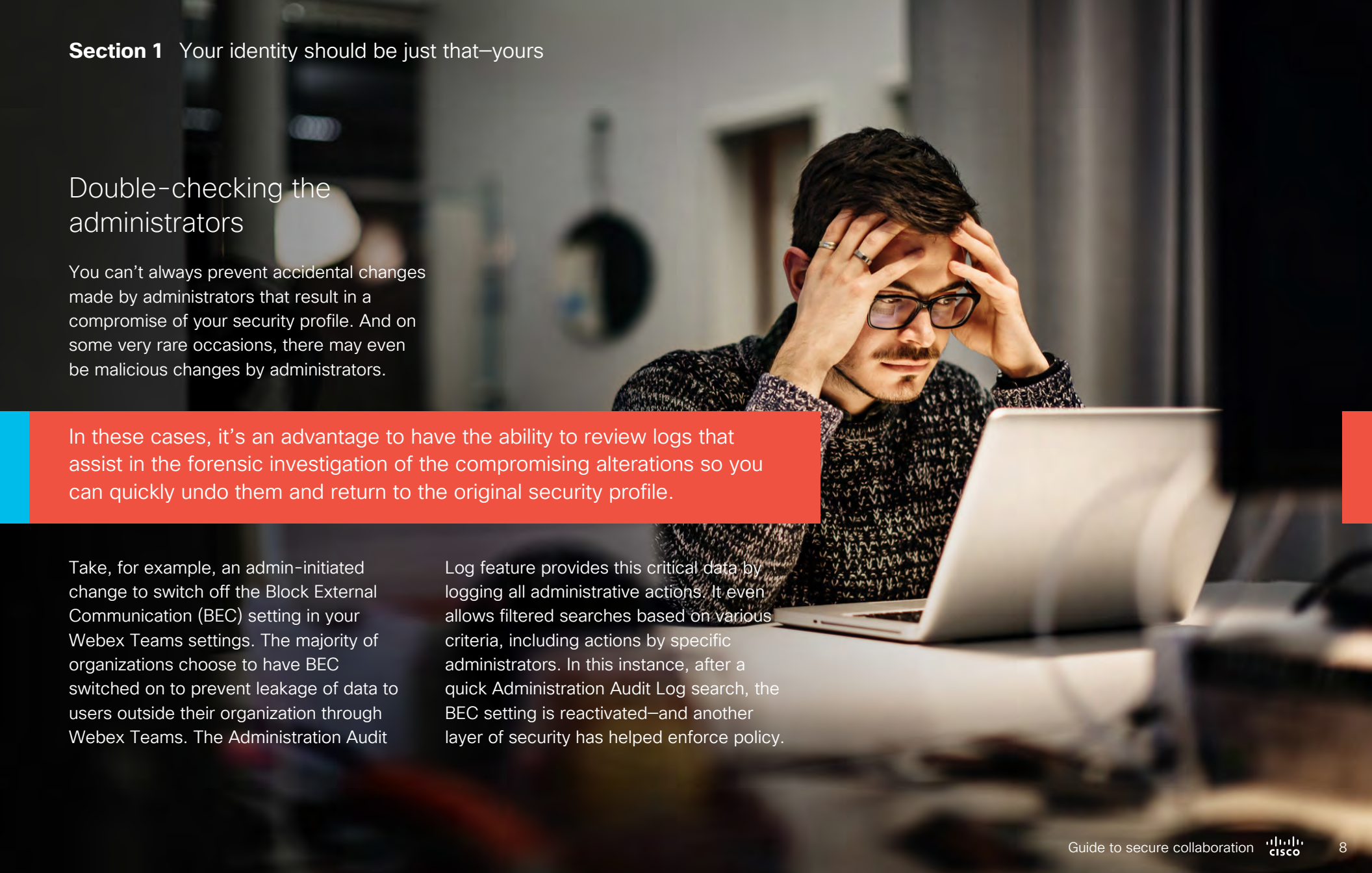
They can:

- Require a password change during someone's next login.
- Specify required password character composition and configure predefined lists of unacceptable passwords, like "password" or "123456."
- Enforce passwords for anyone joining over the phone or a video conferencing system.
- Set up administrator approval for any "Forgot password?" reset requests.

Role-based access reduces the dangers of threats by controlling what specific users can do. Administrators have extensive capabilities. For example, they can grant—and revoke—access to content such as integrations or even file sharing. Meeting hosts can lock meetings to prevent additional users from joining.

External participant indicators in Webex Teams visually notify users when a room contains participants that are not part of their enterprise organization.

Room moderator control in Webex Teams allows chosen room participants to become moderators with exclusive control of the room's title and participant list.



Double-checking the administrators

You can't always prevent accidental changes made by administrators that result in a compromise of your security profile. And on some very rare occasions, there may even be malicious changes by administrators.

In these cases, it's an advantage to have the ability to review logs that assist in the forensic investigation of the compromising alterations so you can quickly undo them and return to the original security profile.

Take, for example, an admin-initiated change to switch off the Block External Communication (BEC) setting in your Webex Teams settings. The majority of organizations choose to have BEC switched on to prevent leakage of data to users outside their organization through Webex Teams. The Administration Audit Log feature provides this critical data by logging all administrative actions. It even allows filtered searches based on various criteria, including actions by specific administrators. In this instance, after a quick Administration Audit Log search, the BEC setting is reactivated—and another layer of security has helped enforce policy.

Integration with data-loss-prevention solution providers

Integration with leading solutions has always been a hallmark of Cisco's approach.

Cisco has partnered with the industry's leading data-loss-prevention (DLP) and cloud-access-security-broker (CASB) solution providers for turnkey solutions, plus Cisco offers a leading CASB of its own. You can also use the Cisco Webex Events API to integrate with your existing DLP/CASB software to save and protect an unlimited amount of Cisco Webex Teams data.

Integration with leading DLP/CASBs gives Webex Teams administrators the ability to maintain oversight and control of employee security and compliance even when they join other companies' Webex Teams spaces.

Compare that to what happens with other team collaboration solutions: When a user needs to join another company's (B2B collaboration) Teams environment, a user's client must log out of their company and log in to the other company with a guest account in that company's cloud directory. There you have no view of your employee's activities, conversations, or shared files—and therefore no control over them.

Cisco Cloudlock

Webex Teams supports integrations with Cloudlock, Cisco's cloud-native CASB that helps accelerate use of the cloud. Cloudlock secures cloud identities, data, and apps, combatting account compromises, data breaches, and cloud app ecosystem risks, while facilitating compliance through a simple, open, and automated API-driven approach.

Data-loss-prevention solutions

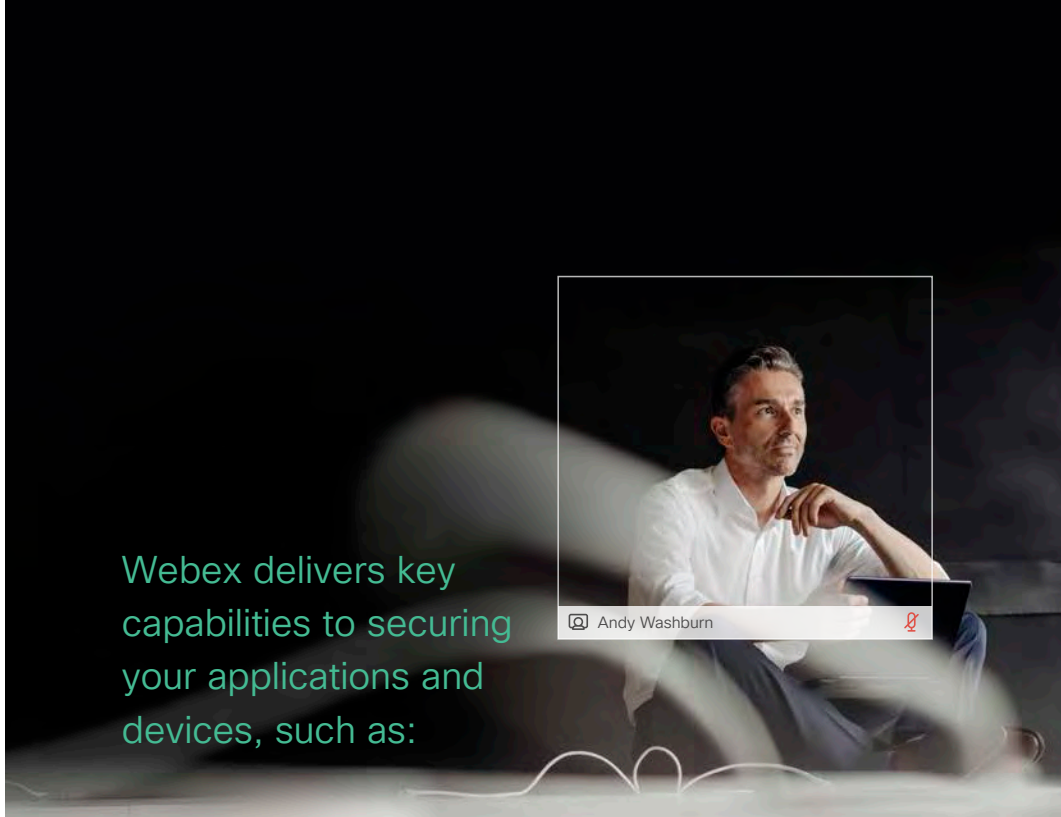
- Cisco Cloudlock
- Netskope
- Symantec
- Bitglass
- SkyHigh
- Verint Verba

Section 2

Securing your applications and devices

Webex creates the possibility of remote collaboration that's simple, reliable, and highly secure.

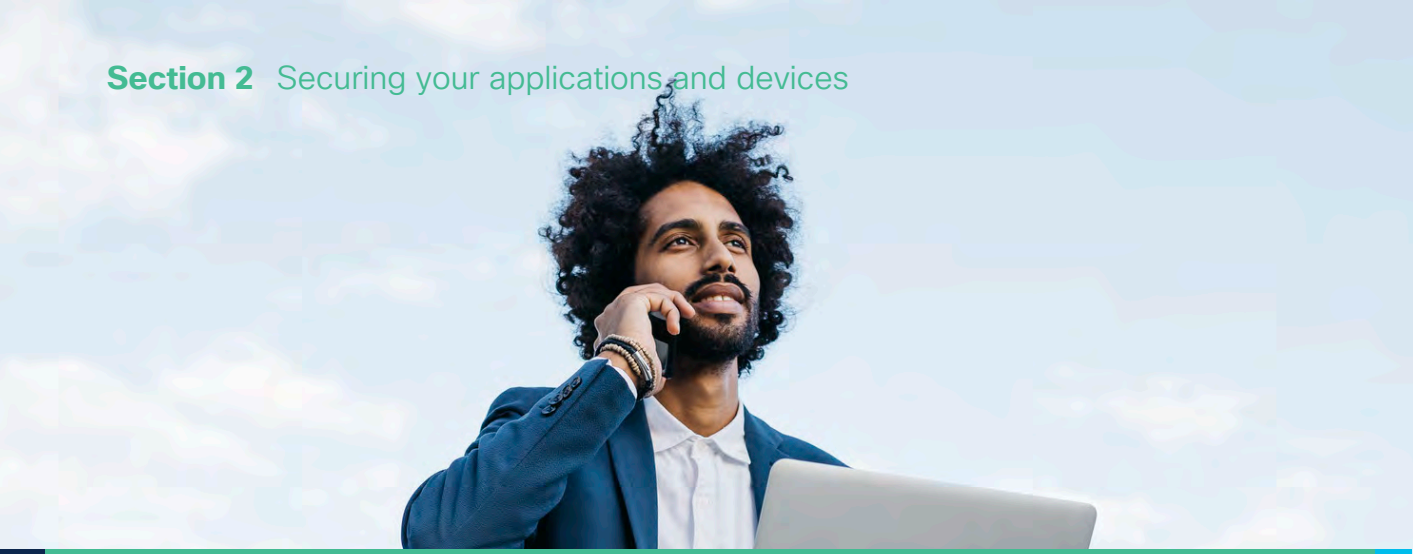
The number and variety of devices and applications that your employees use to connect has exploded. With new devices and applications come new ways to collaborate, but also new avenues for risk and attack—especially when you introduce your users' personal devices and home environments.



Webex delivers key capabilities to securing your applications and devices, such as:

Integration with other solutions:
Seamlessly combining security functionality with leading providers adds strength to strength.

Device management:
Whether corporate owned or bring your own device (BYOD), vulnerable access points need special attention.



Many devices, many risks

One of the most important capabilities of a collaboration solution is its ability to give users convenient access using a wide range of devices, including corporate-managed and personal devices. However, access using all those devices can present security risks.

To keep sensitive information shared through Cisco Webex Teams safe from attack, administrators have several ways to ensure the safety of their clients and themselves. Administrators can:

- Require that mobile devices be secured with a PIN.
- Remotely wipe Webex Teams content in the event that a device is lost or stolen, or if a user leaves the organization.
- Automatically log out devices after a period of inactivity.
- Prohibit file uploads or downloads from certain role-based types of client.

Keeping data and devices safe shouldn't be complicated. Cisco Webex Teams makes it easy to configure and set device security controls.

Section 3

“Secure” should be your default setting

Experience security that’s built in, not bolted on.

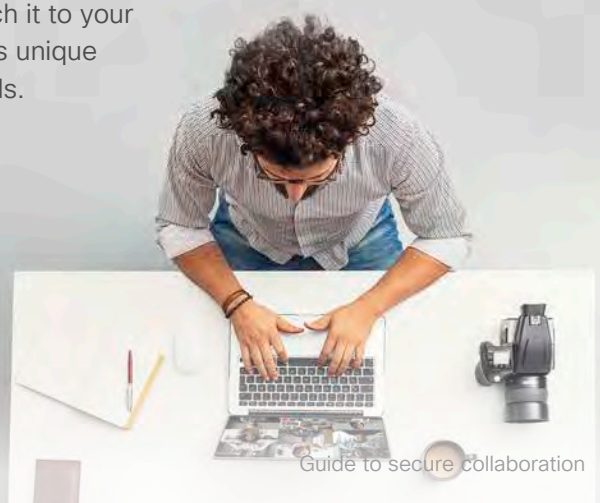
With more employees working remotely, more of your critical business discussions will inevitably move out of the office and into virtual spaces. But how those discussions move over your physical and virtual infrastructure is unpredictable. That means that securing the content of these virtual meetings and collaborations should happen by default.

Webex delivers true end-to-end encryption to secure your content by default.

Even with encryption in transit and at rest, servers can still access unencrypted content—meaning customers are still vulnerable to breaches of their collaboration service provider.

True end-to-end encryption keeps data safe when it is in use as well as when it is at rest and in transit.

With Webex Teams, end-to-end encryption is enabled by default for files, whiteboards, and messages, and is optional for Webex Meetings, so you can match it to your organization’s unique security needs.



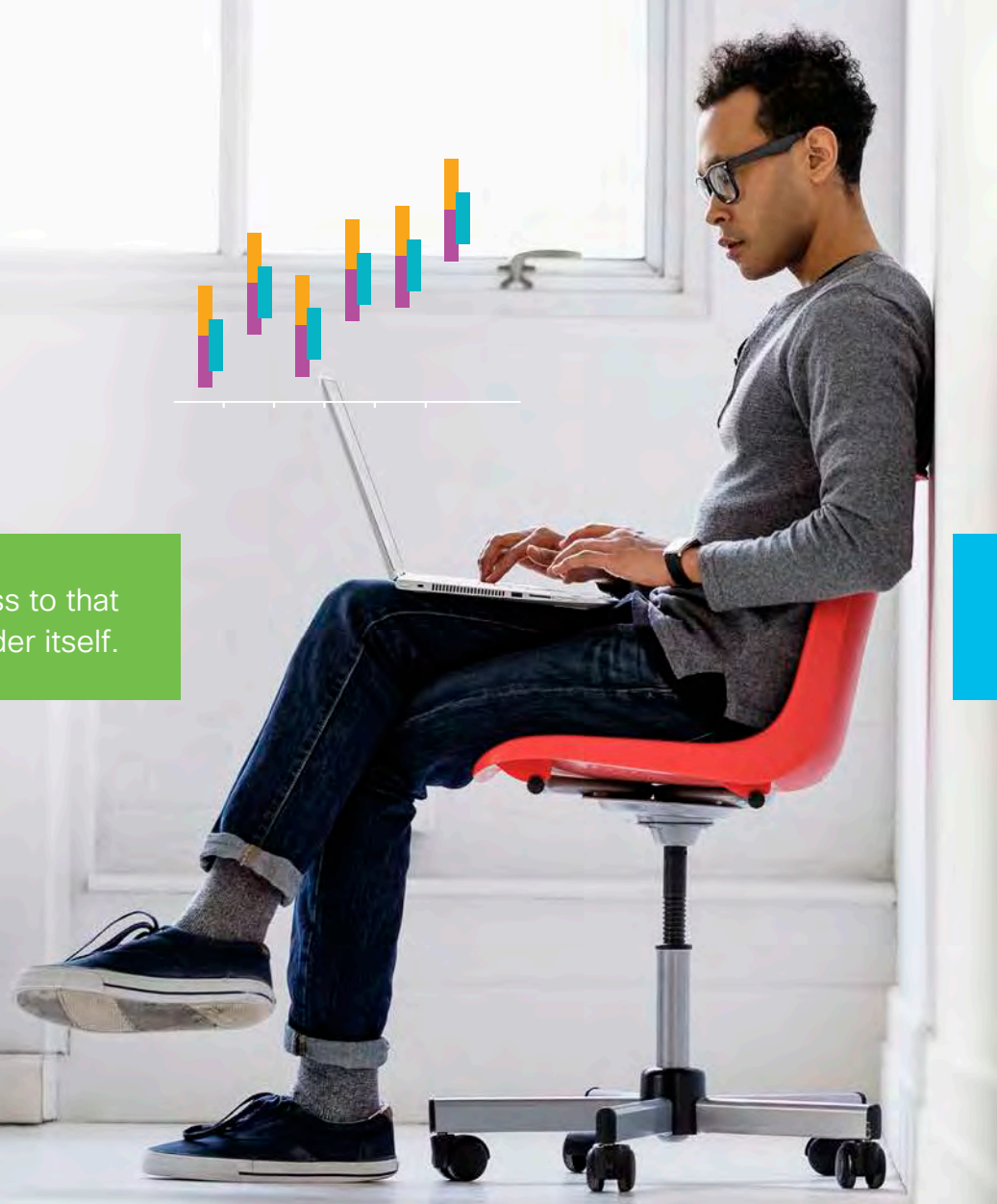
Secure collaboration in the cloud

The advantages of cloud collaboration are numerous. For instance, users have access to value-added features as soon they are released and ready integration with third-party applications. But for many cloud providers, adding value often means having full access to user data and content. In fact, for collaboration apps, most cloud providers directly access message, call, and meeting content in order to offer features like message search, content transcoding, or app integration.

Why is that a problem? As mentioned above, cloud provider access to that content leaves customers exposed to breaches in the cloud provider itself.

Compare that to an innovative team collaboration solution, Cisco Webex Teams. While additional features can be obtained by granting explicit access, end-to-end (E2E) encryption is the default built into the fabric of Webex Teams from the very beginning, which means many value-added features and functionality operate on encrypted data. For instance, Webex Teams supports features like global search of encrypted content without ever decrypting it in the Cisco Webex cloud.

Or consider Webex Meetings, which offers E2E encryption as an optional control. This gives organizations the flexibility to enforce encryption for their most sensitive meetings or users, or to deactivate it for others to enable a richer feature set as appropriate to their organization's needs.



The E2E encryption approach taken by Webex Teams is especially critical with value-added functionality like search features that rely on "plaintext" (which is unencrypted).

With typical services that handle customer information in plaintext, the more functionality the collaboration provider offers, the higher the risk that customer information will be breached. But E2E encryption allows Webex to provide services while reducing the attack surface.

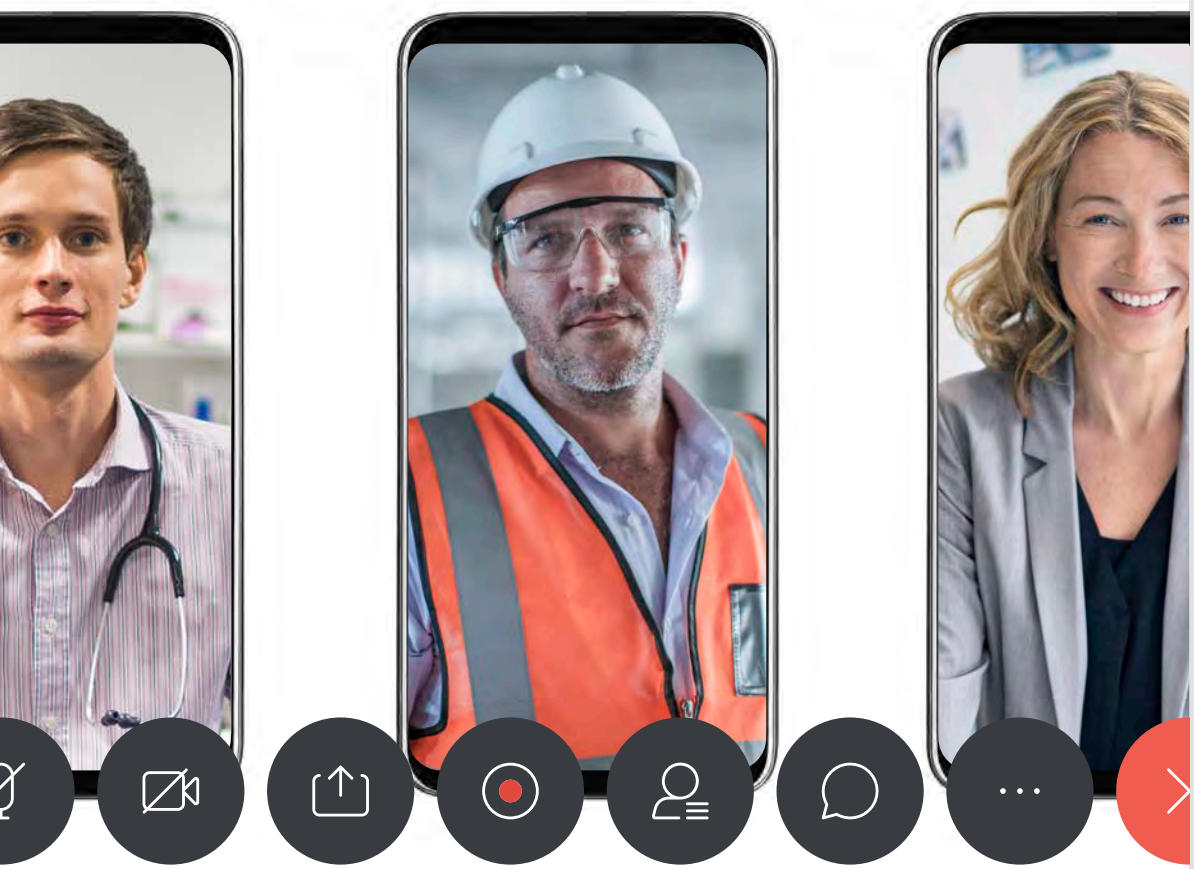
Two examples of E2E protection

Encrypted search

One of the most frequently used features in any messaging system is search. Search in Cisco Webex only requires access to the plaintext of a message once, to build an encrypted index—after that, clients can do searches directly on encrypted data, maintaining maximized E2E encryption.

eDiscovery

This same technology allows Cisco to provide services like eDiscovery with strong security guarantees. So when your compliance officer needs to make sure people are complying with both outside regulatory requirements and your internal policies, he or she can search encrypted content and get the search results in decrypted form.



Section 4

Every industry is different

Webex is where employees work, doctors consult, governments serve, military and police protect, media reports, and teachers inspire.

While the security features protecting Cisco collaboration solutions are second to none, every collaboration customer has different security requirements based on their industry. The next chapters explore three of Cisco's sector-specific collaboration solutions and how they can help protect these industries.

Protecting collaboration in healthcare

Telehealth

Telehealth is the remote engagement and exchange of information between patients and care providers using technology, often including video. Why is telehealth (also called telemedicine, ehealth, or virtual health) so important to healthcare providers? It improves access to care, increases the availability of specialists, and improves staff efficiency with face-to-face healthcare via video conferencing and devices. Besides the convenience of doctor visits without a commute, sometimes it's essential to provide care remotely to keep everyone safe and healthy. We're here to help clinicians, care teams, patients, and families make the transition to virtual healthcare.

By empowering virtual healthcare provider-to-provider and provider-to-patient collaboration, Cisco collaboration solutions are already helping make good on exciting opportunities to:

- Improve patient services.
- Reduce travel costs.
- Support patient engagement and self-management.
- Address a new competitive landscape.
- Reduce hospital readmissions and associated Medicare reimbursement penalties.
- Provide improved access to specialist consultations.
- Enable remote clinicians to work together from anywhere.
- Educate patients and practitioners with video presentations.
- Expand the geographic footprint of healthcare organizations.

"Awesome app. Works perfectly. Last-minute lifesaver for a medical department to keep in touch daily during treacherous outbreaks."

–Webex Meetings user, App Store review

In healthcare, cybersecurity matters.

Collaborative telehealth experiences, while exciting and certain to grow in number, require protection. And beyond telehealth, to do their jobs and expedite patient care, healthcare workers have to share sensitive patient data. They need to do this quickly and easily without exposing that data to breaches.

HIPAA violations can be costly.

Healthcare providers are obligated by law to comply with an array of ever-shifting regulations surrounding patient privacy, such as HIPAA. The penalties for violations can be steep.

"Three Boston hospitals ... paid OCR [the Office of Civil Rights] $999,000 to settle potential HIPAA violations due to the unauthorized disclosure of patients' PHI [protected health information]. ... In April 2016, New York Presbyterian Hospital agreed to pay $2.2 million to settle potential HIPAA violations in association with the filming of 'NY Med.'"[1]

1. "HIPAA Settlements: Three Boston Hospitals pay $1M in Fines for 'Boston Trauma' Filming," Healthcare Innovation, September 21, 2018.

Reputation management

and the power of consumer choice

On top of HIPAA, data breaches, stolen medical records, insurance fraud, and ransomware negatively influence a healthcare facility's standing in the community. When patients perceive less-than-optimal protection of their privacy by care providers, some of them vote with their feet and opt to seek care elsewhere.

Ransomware attacks hit healthcare more

than any other industry.

With so many vulnerable endpoints at healthcare facilities–BYODs, apps, medical devices–attackers view them as easy targets. And because it takes practitioners twice the time to perform admin tasks manually when network-connected digital systems are shut down by ransomware attacks, unplanned downtime at healthcare facilities may cost an average of $7,900 per minute (source: "The Rise of Ransomware in Healthcare," csoonline.com, July 2018).

Cisco protects:

With multiple layers of security

Administrative control over role-based access, PIN-locked login authentication, forced logout in case someone forgets, remote wiping of data from devices, integrations with DLPs and CASBs—Webex solutions are designed to meet your HIPAA compliance needs.

With E2E encryption

The E2E encryption built into Webex Teams by default (and optional on Webex Meetings) protects patients, providers, and facilities by shrinking the attack surface to a minimum across endpoints and on-premises or virtual servers—which provides added peace of mind for everyone.

Innovations like telehealth are only as promising and effective as the security that protects them. That's why telehealth programs supported by Cisco cloud collaboration solutions offer the most trusted security available.

Cisco Webex Telehealth Connector for Epic

Cisco integrates with Epic electronic medical records (EMRs) to accelerate the growth of virtual healthcare. Webex Telehealth Connector allows healthcare staff and patients to connect via simple, easy-to-use video telehealth consultations scheduled directly from their Epic EMR portal.

Protecting collaboration in manufacturing

Only Cisco can securely connect and enable manufacturing customers to protect the continuity of operations with remote access monitoring and assistance.

In manufacturing operations, continuous collaboration is critical to plant operations.

First, engineers and technicians design something new and disruptive—and get the green light to bring it to market. Next, suppliers are brought into the conversation, then tooling vendors. Then processes are tested for proof of concept, efficiencies, and safety.

If you think this sounds like a process driven by web conferencing and ongoing virtual teamwork, you're right: From idea to blueprint to prototype to finished product to sales, inputs from teams all over the world are required, and access to expertise is crucial.

Collaboration maximizes equipment uptime.

Production is nearly always a time-sensitive undertaking—customers expect their goods based on precisely determined timelines. If a problem occurs on the factory floor, maintenance teams have to bring together a community of people to solve what can be a mission-critical issue. Formerly, this could mean flying people in to the plant, having meetings, and speculating about what's actually going wrong.

But today, using Cisco Webex and wireless infrastructure delivered on handheld devices, maintenance teams can quickly call remote experts located anywhere in the world, make them virtually available, and resolve issues where they occur on the factory floor.

Their collaboration experiences include voice, web conferencing, video, augmented reality, chat, and application and file sharing—and a high-resolution industrial camera often becomes a participant in the conversation.

Benefits of collaboration between operations, maintenance, and remote experts:

- Increased worker productivity
- Reduced response and repair time with visual execution
- Improved equipment utilization
- Support for remote sites, working from home, and data entry
- A next-gen workforce trained by veteran experts
- Ability to involve your critical partners in onsite operations, even when they are remote

Product development and protecting intellectual property

The value of a new product can't be realized if plans for the project fall into the wrong hands before it can reach the market.

Connecting the frontline with virtual experts

Webex Expert on Demand empowers frontline workers by helping to enable hands-free collaboration with global experts using Webex Teams and the RealWare HMT-1 augmented reality device.

Segmentation of networks

How can manufacturers add a layer of security to the product development process? An example is by segmenting assets within networks, wireless access points, and hybrid-cloud-based services to isolate and protect them. Segmentation allows teams to play their roles with defined security policies while preventing them from accessing assets they don't need. Cisco builds segmentation into collaboration.

Authenticating users and devices

In the case of equipment repair on the factory floor, Cisco Security Connector deployed through mobile device management protects supervised devices. Through greater visibility, it helps to ensure the policy and procedure compliance, as well as the authorized identity, of mobile users, as well as the their enterprise-owned devices. And with added controls, it protects device users from connecting to malicious sites on corporate and cellular networks, or on public Wi-Fi.

This is the reality of cyberattacks and theft by insiders: If your collaboration solutions can't authenticate users and verify device compliance, your confidential information and intellectual property could be exposed.

Protecting collaboration in financial services

Human capital in one virtual room

Investment decisions are inherently risky. As such, they are taken very seriously. When financial services companies bring human capital together from far-flung locations to expertly analyze potential investments during Cisco Webex-hosted meetings, the outlooks expressed constitute intellectual property.

The value of those expert viewpoints and the decisions they influence rely on confidentiality—for instance, in the case of timing a stock market play, or outmaneuvering rivals in a merger or acquisition. In terms of time frames, collaboration is also critical in bringing parties together to close and sell in lending markets as deadlines loom.

An ethical wall

Government agencies and other financial industry watchdogs erect an "ethical wall" to keep confidential information out of the hands of those who would illegally profit by jumping ahead of trades based on improper access to propriety knowledge that doesn't belong to them.

One such agency at the federal level is the Federal Deposit Insurance Corporation (FDIC). Here is what it states in its *FDIC Information Technology Strategic Plan: 2017–2020*:

"The FDIC carries out its supervision programs through a geographically dispersed workforce and in close collaboration with other agencies and institutions. The FDIC's ability to carry out its supervision programs depends upon the availability of various IT platforms. Better collaboration through systems, processes, and tools; systems enhancements; better connectivity; and increased amounts of secure data storage capacity are needed to ensure the continued availability and integrity of these IT platforms."

Will the FDIC shift to more cloud-based services for collaboration? If it does, Cisco is ready.

Cisco Webex Meetings—FedRAMP authorized

The Federal Risk and Authorization Management Program (FedRAMP) processes are designed to assist federal government agencies in meeting Federal Information Security Management (FISMA) requirements for cloud systems. With Cisco Webex Meetings, a FedRAMP-authorized solution, your agency gets a robust, industry-leading, cloud-based, web meeting solution that adheres to stringent federal security requirements.

The advent of virtual tellers

Online banking is an example of collaboration helping fulfill customer needs and demands. Online banking is open 24 hours a day, and it eliminates the need to transfer funds, make deposits, pay bills, research financial products, and maintain records in person or on actual paper.

Beyond convenient online banking, meetings with bankers and advisors are encompassing increasingly complicated financial consultations at video-enabled, standalone kiosks and ATMs. And as the Internet of Things (IoT) phenomenon continues to grow, bank-client interactions will evolve further.

Cisco Connected Mobile Experiences for retail banking

Cisco Connected Mobile Experiences (CMX) lets bankers detect, connect to, and engage with customers through their mobile devices when they are in a branch. That means bankers can greet VIP customers by name and offer immediate assistance, tell customers which lines have the shortest wait times, and promote new services. CMX adds another layer of security as well by being able to identify the presence of mobile devices within a branch when the branch is closed. CMX sends alerts to bank security teams for further action.

Protecting both high-finance and personal accounts

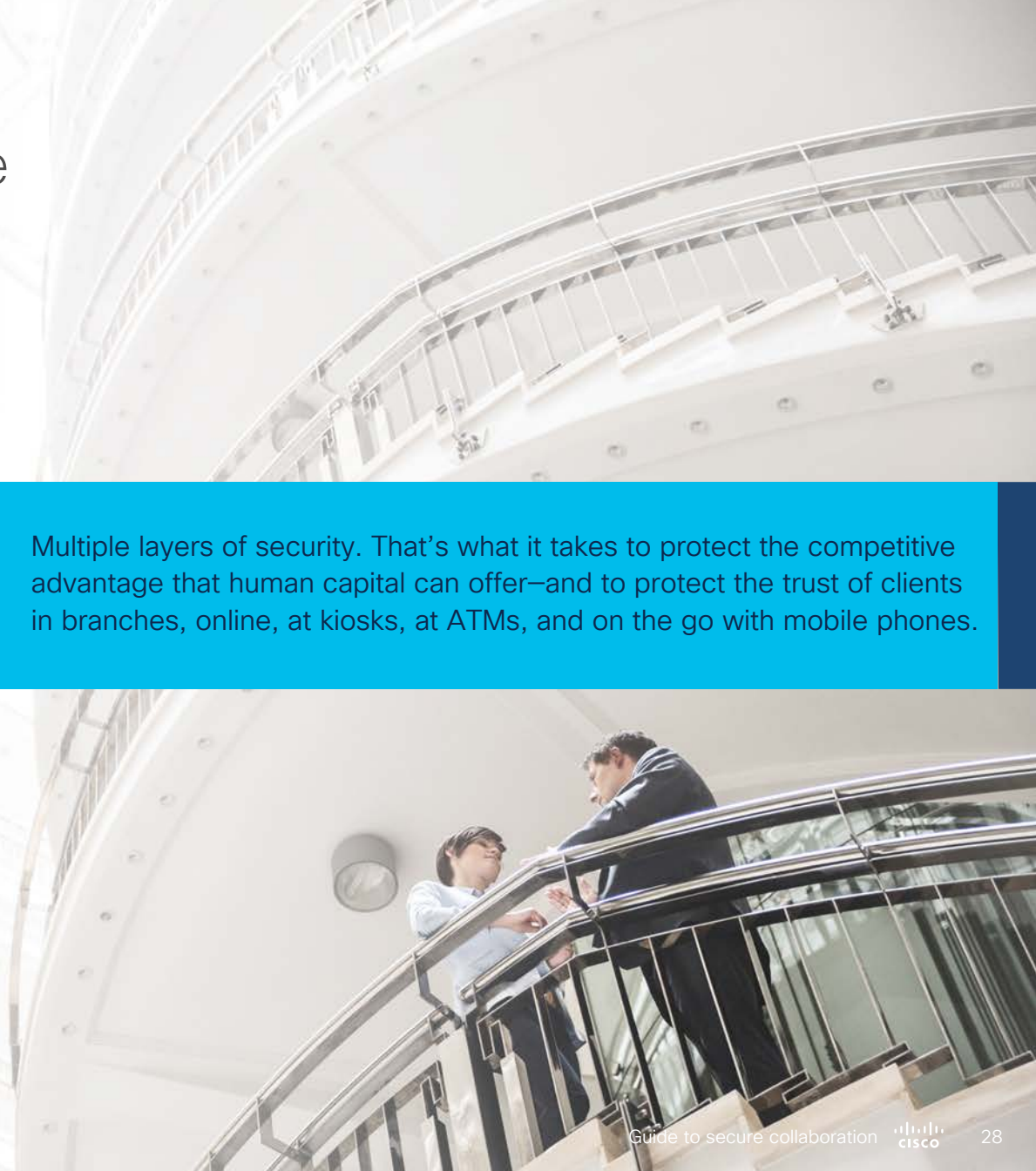
In the case of both financial analyst web conferencing and virtual tellers, E2E encryption is vital. This includes encryption that reduces the attack surface:

- Between the wide range of devices used to access meetings and share files
- Between endpoints connecting bank customers to online accounts and tellers at video ATMs and kiosks
- Within content like financial documents passing through or stored in the Webex cloud
- Within eDiscovery searches that auditors might conduct

Also, recall that:

- The Webex Teams app uses visual indicators to reveal when a room contains participants that are not part of their enterprise organization.
- Role-based access reduces the dangers of threats by controlling what specific users can do, such as download files.
- Segmentation of clouds, partner networks, and guest wireless isolates and protects critical, confidential assets.

Multiple layers of security. That's what it takes to protect the competitive advantage that human capital can offer—and to protect the trust of clients in branches, online, at kiosks, at ATMs, and on the go with mobile phones.



Across every industry and sector served, across every solution Cisco provides: Cisco does security pervasively.

Cisco collaboration solutions have something in common with every solution in the Cisco portfolio: Security is foundational and pervasive. Cisco provides the most comprehensive and advanced security solutions in the industry. Here are just a few:

Cisco Talos

The Talos team protects your people, data, and infrastructure. Talos researchers, data scientists, and engineers collect information about existing and developing threats. Then they deliver protection against attacks and malware. Talos underpins the entire Cisco security ecosystem.

Cisco Umbrella

Through domain name system (DNS) server and IP layer enforcement, Umbrella stops ransomware over all ports and protocols, whether you are on or off the network. And instead of proxying all web traffic, Umbrella routes requests to risky domains for deeper URL and file inspection, effectively protecting without delay or performance impact.

Cisco Advanced Malware Protection (AMP) for Endpoints

Using multiple preventive engines and cloud-based threat intelligence, AMP automatically identifies and stops advanced threats before they reach your endpoints. AMP drastically reduces investigation and remediation time by providing a complete scope and history of threats, and it has the power to remediate across your environment with just a few clicks.

Cisco Webex Teams certifications

Cisco Webex Teams leads the segment in international regulatory compliance, as well as security and data privacy best practices. Take a look:

Completed

- ISO 9001, ISO 27001, and ISO 27018 certified
- Service Organization Controls (SOC) 2 Type II, SOC 3 audited
- FedRAMP certified for Webex Meetings
- Cloud Computing Compliance Controls Catalogue (C5) attestation
- Privacy Shield Framework certified

Best practices

- All data centers hosting our services are ISO 27001 compliant.
- Cisco Security and Trust Organization performs regular and automated penetration and vulnerability tests.
- Development follows the Cisco Secure Development Lifecycle (CSDL).
- Cisco P-SIRT process is followed related to security incidents.
- SLA-backed addressing of security incidents.

In process

- HITRUST compliance

The bridge to possible

Cisco collaboration

Learn more today