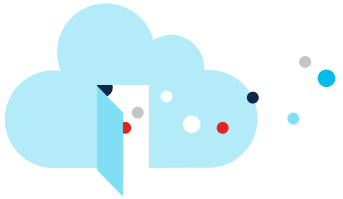

Cisco Webex
Securing collaboration in government
What you need to know about protecting people, data, and devices

Contents

Empower government to greater resiliency

At a time when the public sector workplace is constantly evolving, it's vital for government to create a flexible work environment that can respond quickly and securely to times of unexpected stress. One that enables teams to contribute from anywhere, at any time and to work across agencies securely.

By creating a flexible hybrid working environment, government has empowered workers to enhanced collaboration that can increase transparency, improve citizen engagement, and speed response - all while keeping data secure.



Innovative remote collaboration tools allow users to work together more closely, share ideas more quickly, and maximize productivity. Not only are they effective for government, but they are also cost-efficient for departments of all sizes.

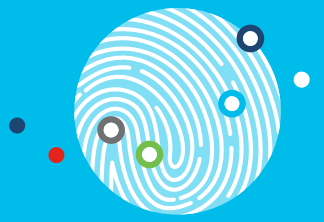
However, as government transitions to a hybrid work environment, the opportunity for risk increase. Remote working can make your data a target for hackers, extortionists, and even nation-states intent on harming us. They are relentless and the news is filled with stories about successful breaches against the public sector.

To enable a hybrid work environment for government, 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 for government offer "security," that security is often included as an afterthought and can still leave holes that expose your organization.

Cisco Webex empowers government with FedRAMP Authorized collaboration solutions for calling, messaging and meeting in an easy-to-use secure app that works with intelligent Cisco devices and native security tools to enhance collaboration and information sharing.



Cisco Webex features FedRAMP Authorized calling, messaging and meeting capabilities that meet the stringent security requirements of the federal government.

For the public sector, security must be more than a checkbox on a list of priorities—it must 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 solutions facing government.

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 end-to-end encryption.

Cisco Webex is uniquely positioned to help the public sector achieve this comprehensive security because its capabilities and features are 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. And with FedRAMP Authorized solutions for calling, messaging and meeting, Webex gives government agencies at all levels the same assurance of security enjoyed by federal users like the Department of Defense.

Section 1

Your identity should be just that—yours

Today's government IT 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 users, agencies, and vendors.

Securing your users and their user identity wherever they are working and however they are connecting is essential to supporting the next-generation workforce for government. Plus, it's critical embedding enhanced resiliency during emergencies that may take them outside their normal operating environments.

Cisco Webex helps government agencies like yours secure users through complete administrative control.

Remember, a collaboration service is only as strong as the security options given to those hosting it.

Secure collaboration for government 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. Cisco Webex gives administrators many options for fine-tuning password enforcement.

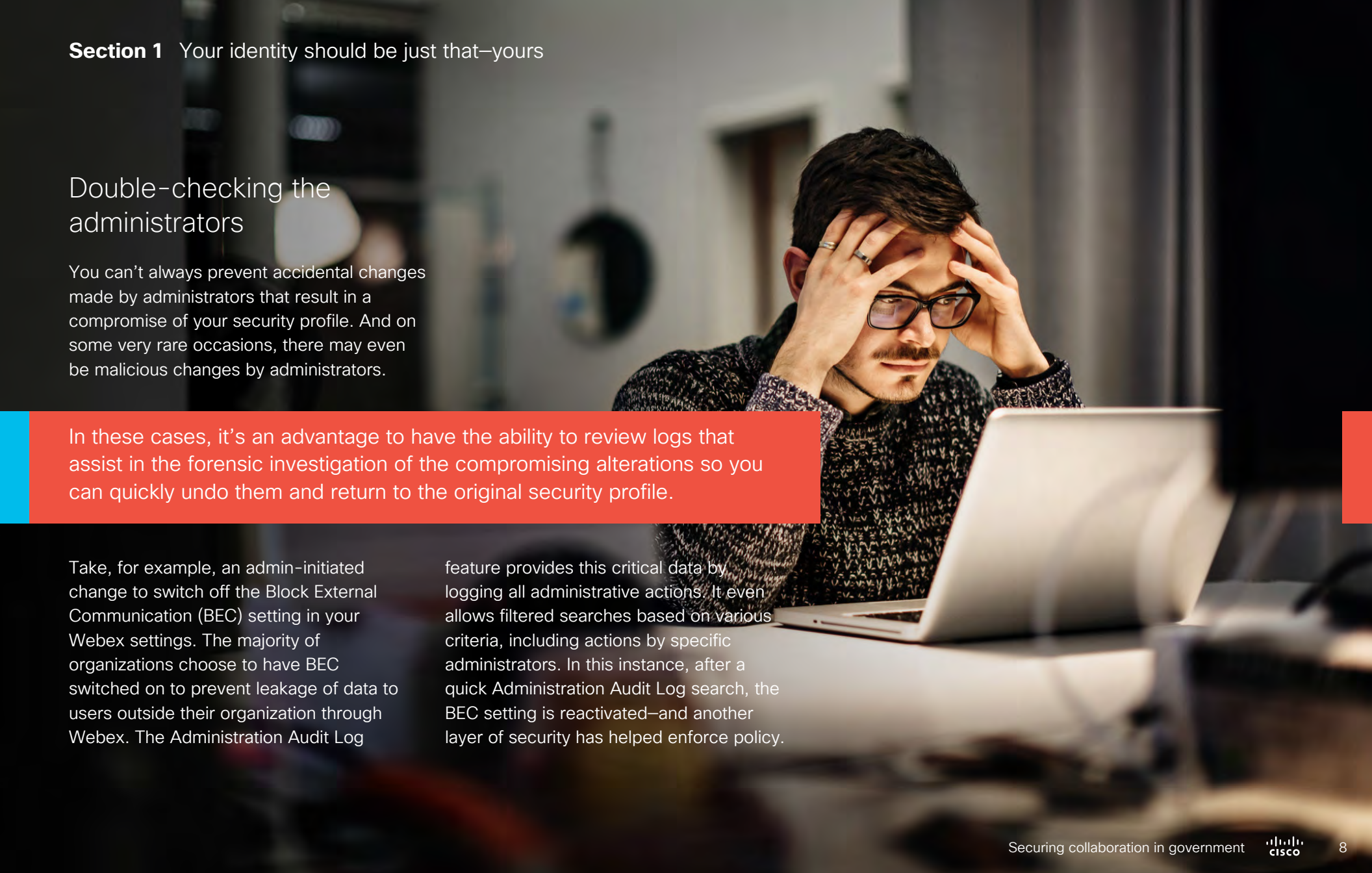
They can:

- 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 visually notify users when a team space contains participants that are not part of their enterprise organization.

Room moderator control in Webex 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 settings. The majority of organizations choose to have BEC switched on to prevent leakage of data to users outside their organization through Webex. 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 data.

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

Compare that to what happens with other team collaboration solutions: When a user needs to join another department or agency's team environment, a user's client must log out of their organization and log in to the other one with a guest account in that organization'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 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

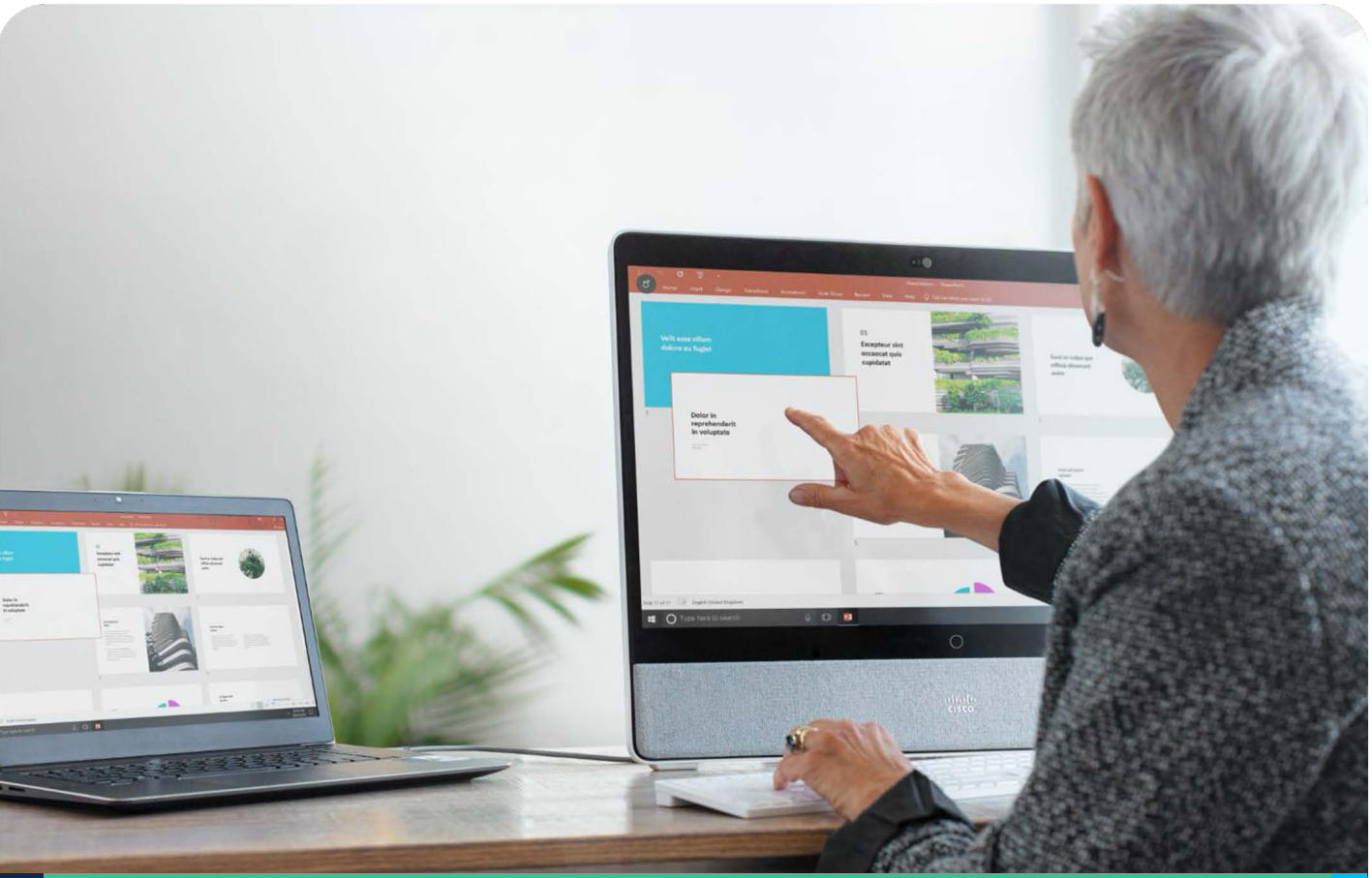
Securing your applications and devices

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

The number and variety of devices and applications that public sector 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.

Integration across 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 for government is its ability to give users convenient access using a wide range of devices, including organization-managed and personal devices. However, access using all those devices can present security risks.

To keep sensitive information shared through Cisco Webex 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 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 government data and devices safe shouldn't be complicated. With FedRAMP Authorized solutions for calling, messaging and meeting, Cisco Webex makes it easy to configure and set device security controls.

Section 3

“Secure” should be your default setting

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

With more public sector employees working remotely, more of your critical 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.

Cisco Webex delivers 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 organizations are still vulnerable to breaches of their collaboration service provider.

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

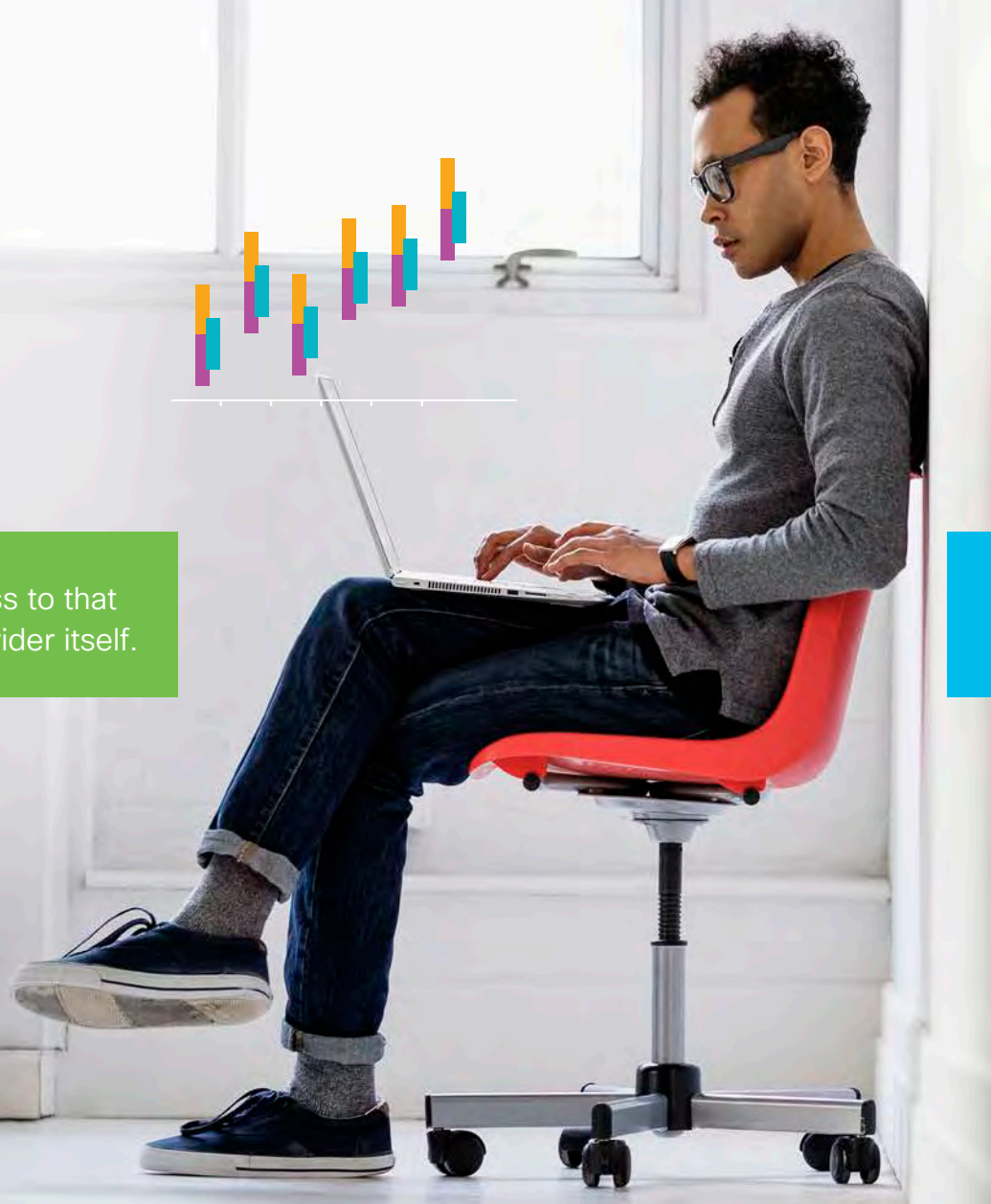
Secure collaboration in the cloud

The advantages of cloud collaboration for government 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 an agency's 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 government exposed to breaches in the cloud provider itself.

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

Or consider Webex capabilities for 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 for its teams feature is especially critical with value-added functionality like search features that rely on “plaintext” (which is unencrypted).

With typical services that handle a government agency's information in plaintext, the more functionality the collaboration provider offers, the higher the risk that an agency's 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 state, local, or federally mandated regulatory requirements and internal policies, they can search encrypted content and get the search results in decrypted form.

Section 4

Driving better outcomes for all

Cisco Webex is where committees coordinate, courts dispense justice, departments engage citizens, first responders speed incident response, and leaders inspire their communities.

While the security features protecting Cisco collaboration solutions for the public sector are second to none, every user has different security requirements based on how they're serving others.

The next chapters explore the variety of ways that Cisco Webex helps government better serve citizens in a secure environment.

Enabling continuity of critical government services

Use Case: Connected Justice

Cisco Webex helps enable the continuity of justice by government via a flexible, scalable, and secure remote solution. As the foundation of the Cisco Connected Justice platform, Webex empowers community safety, courts, corrections, and community supervision agencies with real-time video conferencing and information sharing. By leveraging the proven and secure communications environment of Webex, justice agencies improve operational efficiencies and keep court activities moving. Cisco Webex also allows remote delivery of justice services during incarceration (telehealth, education, visitation) and after release (rehabilitation, reintegration, probationary, and community supervision).

Explore Cisco Connected Justice

By enabling real-time video conferencing and information sharing within the Webex FedRAMP Authorized solution environment, justice agencies benefit from industry-leading security that adds real value.

For workers

- Safer workplace environment
- Continuity of employment in emergencies
- Improved productivity
- More flexible work environment/schedule
- Reduced travel time/costs
- Improved collaboration/communication
- Enhanced security/data privacy.

For citizens

- Contact-free interaction with government
- Continuity of citizen services
- Improved citizen engagement/trust
- Reduced costs for government
- Enhanced privacy of personal data.

For government

- Continuity of operations/services
- Improved long-term resilience
- Reduced facilities/travel costs
- Increased efficiencies/productivity
- Improved collaboration/communication
- Enhanced network security/access control
- Deeper visibility in network/user behavior
- Improved citizen engagement/trust.

Security is critical to justice

Collaborative virtual justice experiences, while efficient and certain to grow in number, require protection. To successfully do their jobs and deliver quality services, justice workers often have to share sensitive government and citizen data. They need to do this quickly and easily without exposing that data to breaches.

Industry-leading security

Cisco Webex provides justice agencies with industry-leading security built with a Cisco IP Network mission fabric. It offers government the capability and tools to interconnect across justice, corrections, and community supervision agencies at every level, to seamlessly integrate wired and wireless technologies. It also lets you combine existing and next-generation mission critical apps while supporting multilevel security.

Unlike some real-time video solutions, Cisco Webex has built-in security and the ability to assure you meet U.S. FedRAMP Authorized requirements for calling, messaging and meeting to keep your agency and its data secure. Plus, it features advanced integration with the tools you use every day, like work calendars.

Community safety

Speed incident response and information sharing

Leverage Webex to perform daily operations remotely (roll calls, administrative, training, court appearances, evidence archiving), and enhance collaboration across local, county, state, or federal agencies.

Share real-time video from the field for improved situational awareness and collaboration between officers, specialists, and supervisors, including better control of crime scenes, immediate access to courts for E-warrants, and remote interpretation.

Corrections

Empower remote visitation with families, attorneys, and more

Deliver vital services including court proceedings, healthcare, attorney support, education programming, and even remote family visitation. Conduct arraignments via virtual court hearings, reducing movement of incarcerated persons.

Webex can also help you effectively isolate, quarantine, depopulate, and socially distance your corrections facility during unexpected events. You can also address overcrowding while improving the delivery of programs that can help reduce recidivism and lower relapse rates of addicted persons.

Courts

Secure real-time court proceedings anywhere, anytime

Webex features high quality video/audio, document sharing, and all modes of interpretation (consecutive, simultaneous and teaming). It also includes judge and attorney siderooms that preserve attorney/client privileges when necessary. And reduces movement of inmates, increasing safety. Plus, our unique “plug and play” approach is built upon simple architecture that is easy to deploy and support.

Community supervision

Deliver critical rehabilitative support and supervision

Provide post-incarcerated individuals with the support and supervision they need to help reduce recidivism, despite distance or changing situations (family, living spaces, health).

Webex helps you provide compliance monitoring, automated mobile reporting, and bulk check-ins for clients via any smartphone. Connect personnel, service providers, agencies, and clients without physical contact. Plus, deliver therapy and rehab programs while reducing travel and keeping personnel safe from unknown situations.

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—Cisco Webex is designed to meet stringent federal requirements that can also serve to enhance security for state and local governments.

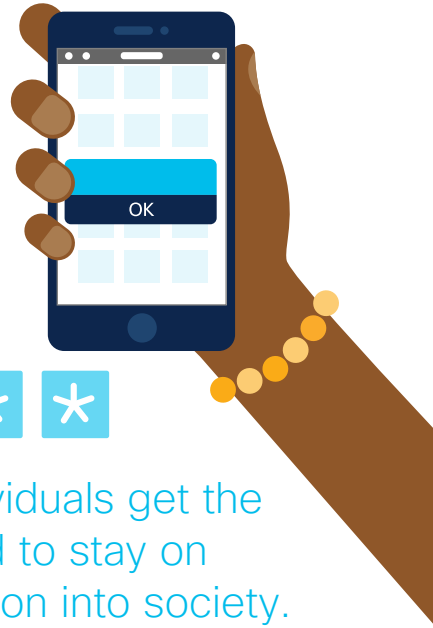
With E2E encryption

The E2E encryption built into Webex by default (and optional on the Webex teams feature) 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 Connected Justice are only as promising and effective as the security that protects them. That's why virtual justice programs supported by Cisco cloud collaboration solutions offer the most trusted security available.

With recidivism rates as high as 60% for some offense types, jail facilities are becoming overcrowded, incurring costs of up to $30,000 per offender, per year.

Webex helps justice agencies reduce recidivism by giving community supervisors and their clients direct access with each other anytime, anywhere.



This helps recently released individuals get the support and resources they need to stay on target for a successful reintegration into society.

Continuity of government in times of stress

Only Cisco can securely connect and enable the public sector to protect the continuity of operations and critical citizen services through remote access, collaboration, monitoring and assistance.

In government operations, continuous collaboration is critical to operations.

Enhancing resiliency in government during times of unexpected stress has become a requirement due to the recent pandemic. This includes the ability to rapidly transition to a hybrid work environment, allowing government workers to preserve critical services and promote transparency with citizens. Cisco Webex has become a key part of this process.

Enhancing resilience in government

Using Cisco Webex for government and wireless infrastructure delivered on handheld devices, facilities and maintenance teams can remotely manage and quickly diagnose issues for critical municipal systems. They can also resolve issues remotely, ensuring continuity of utilities, emergency communications, and other systems key to a community's resilience during times of stress.

Preservation of critical citizen services

The real-time video capabilities of Webex enable government to continue operations needed to maintain the health and welfare of citizens. Powered by industry-leading security, the Cisco Webex platform helps citizens securely gain access to much needed public services, including public safety, health and human services, and utilities. All while protecting their personal data and that of government.

A single and secure platform for communications

Cisco Webex provides a single communications platform for government. It works across agencies and levels of government, and combines calling, meeting, and messaging into a single easy-to-use solution. Public sector workers stay productive regardless of location, even in emergencies, and can securely collaborate and share information via real-time video with other agencies, institutions or contractors during an unfolding crisis. This can be done one-to-one or one-to-thousands, with the push of a button.

Cisco Webex features:

- A simple to use interface that can exist on a variety of platforms.
- Real-time video conferencing capabilities to support thousands of attendees.
- Advanced and secure information sharing in real-time.
- Enterprise-grade security backed by U.S. FedRAMP Authorization and In-Process designations.
- Integration with popular productivity apps like Microsoft Office and ServiceNow.
- An advanced management control hub for security, visibility, and control.

Greater transparency in and trust of government

With the Cisco Webex unified communications platform, agencies empower a daily outlet for streaming live briefings, including via social media platforms, that are easily accessible on citizen’s tablets and smartphones. Such transparency can help increase compliance by citizens to urgent requests during emergencies, resulting in better outcomes. By leveraging Webex, the public sector can increase their engagement with, and trust in, government by their workers, the media, and the citizens they all serve.

Protecting the layers of transportation

In today's environment, the safe and reliable use of mass transit, aviation, maritime, roadways, and rail requires a unique approach to collaboration and security.

> Discover how

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 and the RealWare HMT-1 augmented reality device.

Segmentation of networks

How can government add a layer of security across departments? 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 asset management within facilities and across campuses, 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 non-governmental 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 department's data - and the private personal data of the citizens you serve - could be exposed.

Enabling the next-generation workforce for government

Empowering human capital through secure collaboration

Is your organization ready for the next-generation of government workers? Now is the time to prepare and Cisco Webex helps agencies lay the foundation of innovation the next-generation desires (and expects) as it enters the public sector workforce.

Creating better outcomes for citizens and enhancing resilience in government are key goals for the next-generation of government employees. So it's critically important for government leaders to understand how to attract and retain those workers.

Technology helps attract and retain workers

As governments face aging workforces approaching retirement, many of their leaders are trying to better understand the changing career preferences of the next-generation of workers and young professionals.

Adults under the age of 38 now comprise the largest proportion of the U.S. workforce, representing 65 million working Americans, according to the Pew Research Center. And while much has been written about the impact of Millennials in the workplace, the oldest members of that demographic group are rapidly approaching the age of 40. However, less is understood about the next-generation of workers who are under the age of 30 – many of whom are just now entering the workforce – and how governments can ensure they attract the best and brightest of them to serve the public in the decades to come.

Next-generation workers value collaboration in their workplace – and the technology that enables it. They want to be connected anywhere, learn online, and have access to up-to-date technology.

In a recent survey of early-career working professionals by the Center for Digital Government (CDG), more than one-third (34 percent) said slow adoption of new technology in the public sector is a negative aspect of working in state and local government. Governments must recognize that technology adoption – and playing a direct role in exploring new technologies – is expected by their next-generation of workers. In addition, nearly nine in 10 respondents (86 percent) say they always or sometimes expect an employer to provide the most advanced technologies available. And nearly as many (83 percent), expect to at least sometimes be invited to explore using newer technologies in the workplace.

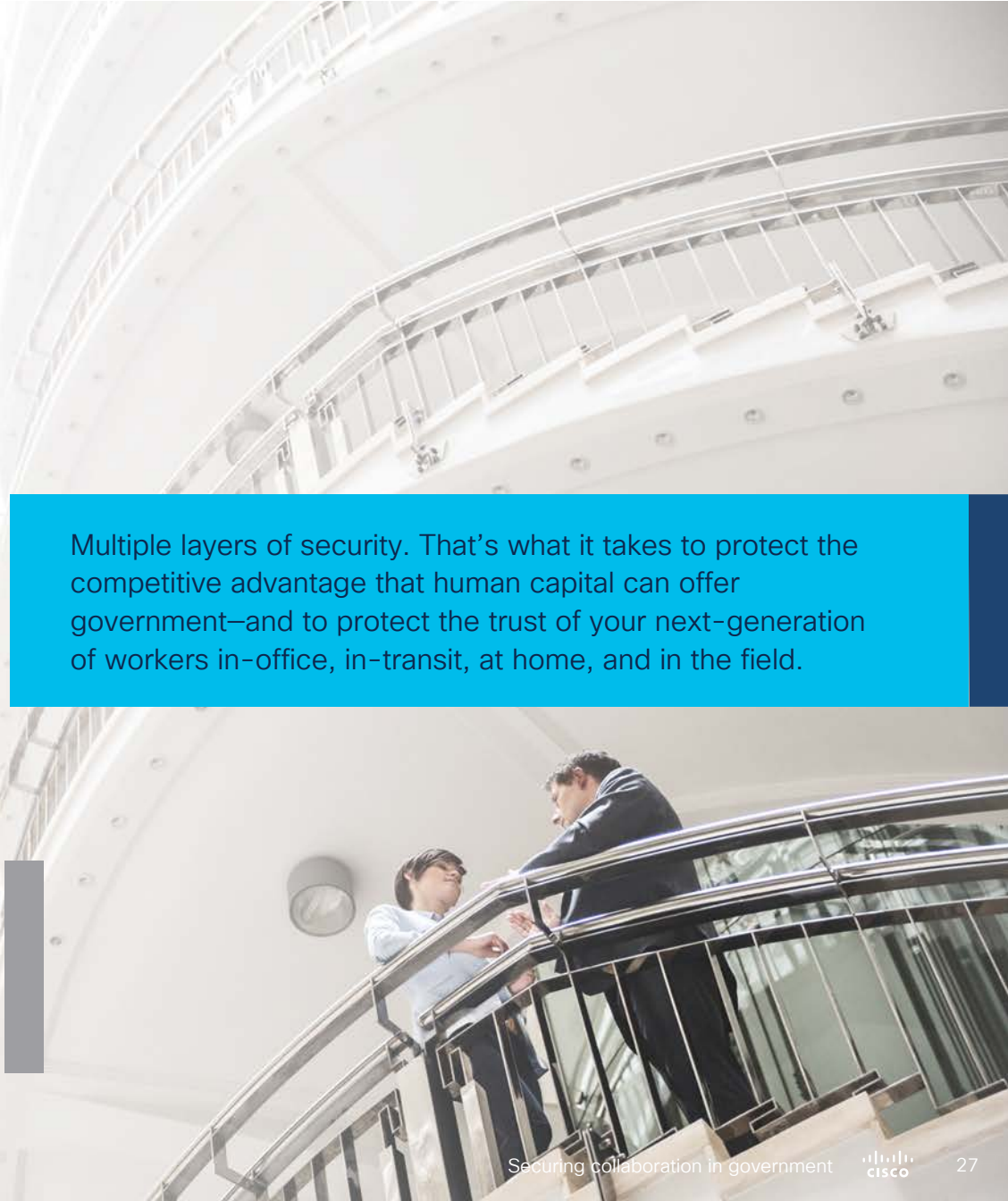
Pervasive security is their new normal

Younger generations recognize the importance of security in the workplace. They expect advanced security as the norm. And it must work behind the scenes without interrupting their workflow. This means the public sector must provide secure and reliable collaboration via a variety of devices (laptops, tablets, smartphones) that is powered by reliable and secure remote access, plus robust Wi-Fi. In addition, governments must use E2E 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.

The Webex teams feature 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. And 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 government—and to protect the trust of your next-generation of workers in-office, in-transit, at home, and in the field.



Across every aspect of government, across every solution we provide: 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 public sector. 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 and helps keep government networks, data, and users more secure.

Learn more

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.

Learn more

Cisco Secure Endpoint

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

Learn more

Cisco Webex certifications

Cisco Webex offers FedRAMP Authorized features for calling, meetings, and messaging that also lead the segment in international regulatory compliance, as well as security and data privacy best practices.

Completed for teams feature

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

Best practices for teams feature

- 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 for teams feature.

The bridge to possible

Cisco collaboration for government

Learn more today