A guide to secure collaboration

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

cisco Webex

ONX CANADA

Technology, covered.

Two things smart companies should know

Smart companies recognize the value in providing flexible work environments that enable their teams to contribute from anywhere, at any time. Positioning workers of all types to achieve their potential to dream up, share, and execute on innovations helps the entire organization disrupt the marketplace.

Smart companies leverage the power of collaboration tools to tap into the power of ideas. To allow users to work together more closely, share ideas more quickly, and maximize productivity.

But you probably knew that, right?

Unfortunately, the digitally connected workplace is also under constant attack. Its data is a target for cyberthieves, cyber mischief-makers, and cyber extortionists. These criminals are smart and relentless and the news is filled with stories about their successes in breaching the very systems designed to thwart them.

Smart companies prioritize cybersecurity to prevent the data loss, PR embarrassment, and remediation costs associated with breaches.

But you knew that, too.

And something they might not be aware of

At the intersection of collaboration solutions, the collaboration lifecycle, and cybersecurity solutions are gaps that hackers can exploit. Even smart companies can purchase collaboration solutions that offer "security," and in doing so, merely check a box off a list of priorities—not realizing that the level of protection they are settling for leaves them exposed to threats.

Even smart companies don't fully understand the gaps, the industry-specific vulnerabilities, and the fact that all security solutions are not created equal.

Maybe you didn't know that.

That's why it's important to better understand security challenges and security solutions.

Read on to explore how even smart companies can be smarter about collaboration solution security.

The multiplier effect created in layers

One of the most sinister thing about cybercriminals is how smart they are. They relentlessly search for and create new pathways around cybersecurity. That's why no single layer of security is adequate. Instead, security needs to be comprised of layers that work together. Layers like these.

True end-to-end encryption

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."

Integration with other solutions

Seamlessly combining security functionality with leading providers adds strength to strength.

Administrative control

A collaboration service is only as strong as the security options given to those hosting it.

Device management

Whether corporate-owned or BYOD, vulnerable access points need special attention.

Segmentation

Splitting your network access into different subnetworks strengthens your defenses.

All of these layers are important individually. But their real power to protect stems from the security multiplier effect they achieve when they act in concert. More on each layer in the following pages.

Collaboration isn't truly secure if it isn't encrypted end-to-end

Most collaboration service providers claim to be secure because they encrypt data "in transit" between users' devices and their servers or between their own data centers, and "at rest" while stored on their servers. However, even with encryption in transit and at rest, servers can still access unencrypted customer content.

That's right:

The collaboration provider's vulnerability to breaches becomes your vulnerability, making your attack surface significantly larger.

A vast improvement is end-to-end (E2E) security, a feature providing an extra layer of protection beyond standard security. With E2E security, data is encrypted "in use," meaning all customer data transmitted through a collaboration service provider is encrypted before being sent, so that components—on-premises or in the cloud—only handle customer data in a safe, encrypted form.

So even if one of these components is fully compromised—a situation where those systems that only encrypt data at rest or in transit would fail—the attacker still can't access customer data, because it's truly encrypted end-to-end.

With E2E security, data is encrypted "in use," meaning all customer data transmitted through a collaboration service provider is encrypted before being sent.

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, E2E encryption has been 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.

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.

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 more risk that customer information will be breached. But E2E encryption allows Webex to provide services while reducing the attack surface.

An added layer of security: Webex Teams components can't impersonate users.

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 Application Programming Interface (API) to integrate with your existing data 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 Team 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 Team supports integrations with Cloudlock, Cisco's cloud-native CASB that helps accelerate use of the cloud. Cloudlock secures cloud identities, data, and apps, combating 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
- Symantec
- SkyHigh
- Netskope
- Bitglass
- Verint Verba

Cisco makes application integrations easy

To provide developers with APIs that are easy to learn and use, Cisco does not require bots and integrations to explicitly integrate with the Webex E2E encryption system. Instead, developers can use a Webex Software Development Kit (SDK) or the Webex API.

Using the SDK is the more secure option

When developers use the Webex SDK, the SDK will handle all the work of integrating with the E2E encryption system. Customers that use SDK-based bots and integrations need to make sure that the code for the bots/integrations runs in a secure context, but they don't need to worry about Cisco Webex having access to any keys or content.

In contexts where it's not possible to use the SDK, Webex also provides an API server that can handle and decrypt content on behalf of the bot or integration. When a bot or integration requests access to encrypted content (such as a message or file), the API server requests the necessary encryption key, decrypts the content, and provides it to the bot or integration.

Notably, Cisco applies the same protections to content shared with third-party integrations. From a security perspective, the API server is a plaintext service, placing it on the end-to-end critical path. That means that it's up to each organization to decide whether to provide it access to the enterprise's content.

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, 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, device administrators, read-only administrators or compliance officers.

There are a multitude of 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 allow the Cisco Webex Teams app to make it clear to users, through visual indicators, when a room contains participants that are not part of their enterprise organization.

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

Double checking the administrator

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 on 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 re-activated—and another layer of security has helped enforce policy.

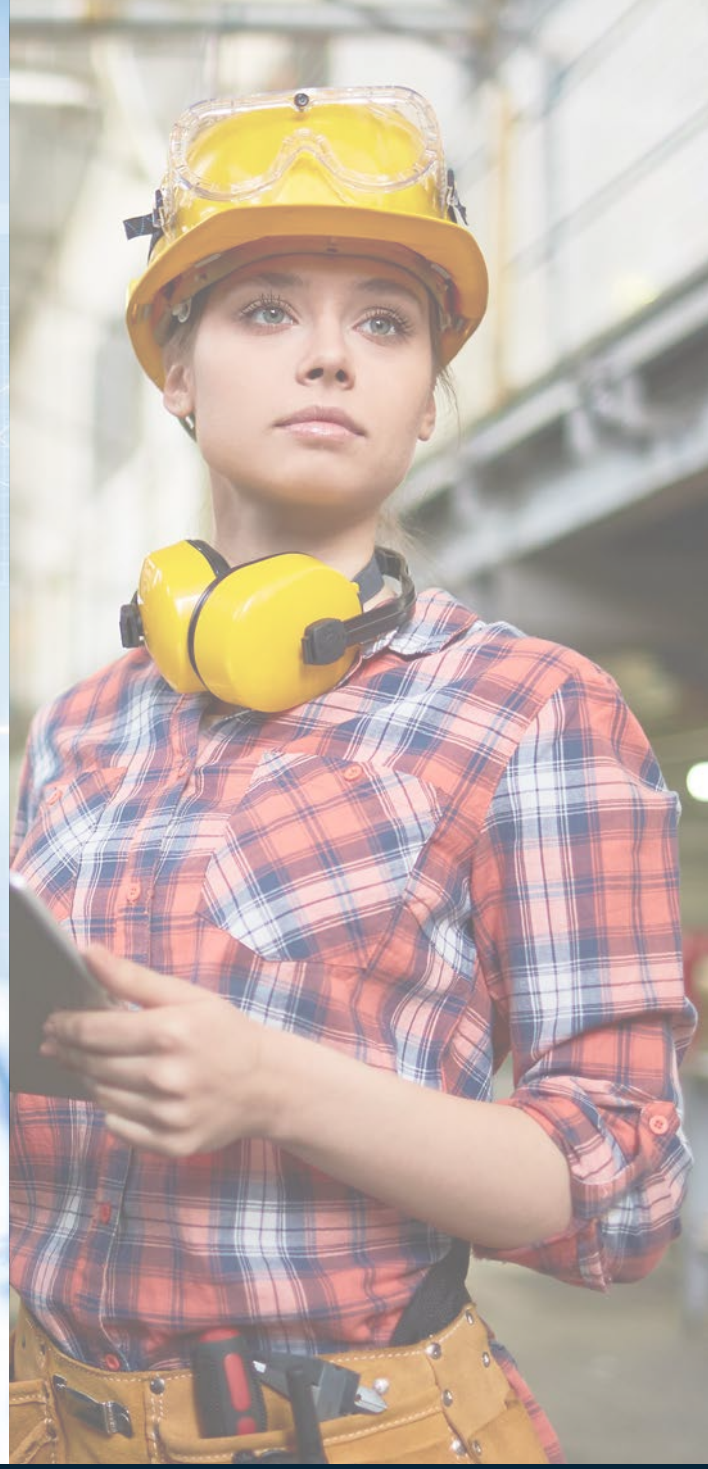
Many devices, many risks

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 assure the safety of their clients and themselves. Administrators can:

- Require that mobile devices are secured with a PIN.
- Remotely wipe Webex Teams content in the event 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.



Every industry is different

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 are protected.

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

Protecting collaboration in healthcare

Telehealth

Telehealth is the remote engagement and exchange of information between patients and care providers using some sort of technology, often including video. Why is telehealth (also called telemedicine, ehealth, or virtual health) predicted to explode? Because of looming physician shortages and higher patient service expectations. Also, the shift from volume-based to value-based reimbursement creates a greater sense of urgency to reduce costs and maximize operational efficiency. Telehealth programs solve for all of these concerns.

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 and costs associated with unneeded ambulance transport.
- Support patient engagement and self-management.
- Address a new competitive landscape.
- Avoid hospital readmissions and associated Medicare reimbursement penalties.
- Provide improved access to specialist consultations.
- Enable remote clinicians to work together from anywhere.
- Remotely monitor patients in the ICU.
- Educate patients and practitioners with video presentations.
- Expand the geographic footprint of healthcare organizations.

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.

September 2018

"Three Boston hospitals... paid the Office of Civil Rights $999,000 to settle potential HIPAA violations due to the unauthorized disclosure of patients' Protected Health Information."[1]

"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-Informatics.com. September 2018.

Reputation management and the power of consumer choice

On top of that, 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.[2]

[2] 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 log out in case someone forgets, remote wiping of data from devices, integrations with DLPs and CASBs—Webex solutions are HIPAA compliant.

With E2E encryption

The E2E encryption (in use, in transit, at rest, and within features like search) built into Webex Meetings and Webex Teams protects patients, providers, and facilities by shrinking the attack surface to a minimum, across endpoints and on-premises or virtual servers—that provides added peace of mind for everyone.

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

Protecting collaboration in manufacturing

From product development to fixing problems on the factory floor, collaboration solutions allow anytime, anywhere business and productivity in the manufacturing sector to flourish.

In product development, teamwork is essential

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 this sounds like a process driven by web conferencing and ongoing virtual teamwork, you would be 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/file sharing—and a high resolution industrial camera often becomes a participant in the conversation.

Benefits of virtual access to remote experts:

- Increased worker productivity.
- Reduced response and repair time.
- Improved equipment utilization.
- A next-gen workforce trained by veteran experts.

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.

Segmentation of networks

How can manufacturers add a layer of security to the product development process? By, for instance, segmenting critical, confidential 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 and authorized identity of mobile users and 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 or from 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.

Importantly, those expert viewpoints and the decisions they influence rely on confidentiality for value, 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

How can manufacturers add a layer of security to the product development process? 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 proprietary knowledge that doesn't belong to them.

One such agency at the federal level is the Federal Deposit Insurance Corporation (FDIC). Here is what they state in their 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 they do, 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. Cisco Webex Meetings FedRAMP-Authorized provides strong, risk-based security that meets those stringent standards—an extra level of trust.

Cisco Connected Mobile Experience (CMX) lets bankers detect, connect, and engage with customers through their mobile devices when they are in a branch.

The advent of virtual tellers

Online banking is an example of collaboration helping fulfill customer needs and demands. Online banking is open 24 hours 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 ever more complicated financial consultations at video-enabled, stand-alone kiosks and ATMs. And, as the IoT phenomenon continues to grow, bank-client interactions will increase further.

Cisco Connected Mobile Experience for retail banking

Cisco Connected Mobile Experience (CMX) lets bankers detect, connect, 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 both the financial analyst web conferencing and virtual teller cases, E2E encryption is vital. That 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 indicate 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 downloading 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 the trust of clients in branches, online, at kiosks, ATMs, and mobile phones on the go.

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 preventative 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 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, and security and data privacy best practices. Take a look:

Completed

- **ISO/IEC 27001**
- **SOC2 Type 1, SOC 2 Type 2**
- **EU-US Privacy Shield**
- **Swiss-US Privacy Shield**
- **ISO 9001**
- **APEC Cross Border Privacy Rules (Download list)**
- **EU Model Clauses**
- GDPR Compliance
- HIPAA compliance
- ISO 27017
- Cloud Computing Compliance Controls Catalog (C5) certification.

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
- FedRAMP

All data centers hosting our services are **ISO 27001** compliant.

About OnX Canada

OnX Canada is a leading technology solution provider that serves businesses, healthcare organizations, and government agencies across Canada. From unified communications to cloud services and beyond, OnX combines deep technical expertise with a full suite of flexible technology solutions that drive business outcomes, improve operational efficiency, mitigate risk, and reduce costs for its clients. OnX simplifies IT and Communications strategies with local knowledge and support for Canadian organizations. For more information, please visit www.onx.ca.

Learn more today at **onx.ca**

CISCO MASTER SERVICE PROVIDER