Whitepaper

Security advantage for Webex

webex
by CISCO

Contents

A majority of Fortune 100 companies use Cisco for their security needs

Based on Cisco's decades-long rich history of security, Webex gives you data security, compliance visibility, and control over your meetings. Inside your own organization, or even when collaborating across company lines, you get a hardened collaboration platform that helps keep your data secure.

Webex provides you with a single platform for calling, meeting, messaging, whiteboarding, video devices, and Unified Contact Center. We build all products in accordance with the Cisco Secure Development Lifecycle (SDL), which includes privacy impact assessments, proactive penetration testing, and threat modelling. Cisco's Security and Trust organization oversees security and privacy for Webex, and publicly discloses security vulnerabilities.

Privacy, security, and transparency

Our three security principles:

- Webex is committed to respecting the **privacy** of your data.
- Webex is **secure** by default.
- Webex has **security cyber governance** and is **transparent** when there are security issues.

Data privacy and security processes

Table 1 outlines the privacy and security features built into the Webex portfolio of products versus Zoom.

Table 1. Webex privacy and security policies, processes, capabilities, and commitments

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX	ZOOM
Security and privacy governance	· An independent security and trust organization exists and is separate from the product security organization to drive governance for corporate security controls and processes · A dedicated chief security officer for Webex · A companywide data protection and privacy program assures customers their data is private · Cisco Trust Center · Cisco Secure Development Lifecycle (SDL) · The Cisco privacy program has been validated by independent third parties, including the EU privacy regulators and TrustArc	· Zoom is only starting to build out its security team, after having many security issues come to light in the media · Zoom does not have users' individual privacy in mind, and users can't trust Zoom to keep their data safe. Reading through Zoom's privacy statement, it is clear to easily see (after working past the confusing language) that Zoom maintains the right to share users' data with third parties for business purposes. This is also exposed with the Apple iOS14 release, which shows that Zoom collects a lot of personal data about users and grants itself the right to use that information for advertising and marketing.
Transparent reporting of security issue or fixes	· A dedicated 24x7 global Product Security Incident Response Team (PSIRT) manages receipt and public disclosure of security vulnerabilities · Cisco Emergency Response, including CSIRT for comprehensive investigation and prevention of threats · Letters of attestation on outcomes of penetration testing available under NDA	· Zoom's reporting of security issues and fixes is not as comprehensive and thorough as Cisco's · Zoom has a history of not reporting and remedying security issues such as when Zoom had its Apple Camera flaw
Customer data residency choices	· Customers can select the region to store select user-generated content data and user identities · Encryption keys are generated and managed in your home region · Customers have the ability to pin media to a specific region for Webex Meetings	· Zoom does not offer admins a choice in their provisioned data center to store data and user identities · Zoom supports only media-pinning to a specific region, but customers must request a specific region for this

Table 1. Webex privacy and security policies, processes, capabilities, and commitments

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX	ZOOM
Support for China market	• Webex does not have any data centers in China that are connected to the Webex infrastructure backbone, so there is no chance that customer data is routed through China • Webex China is a separate entity that is operated through a local and independent third-party partner, TCL / Skytech • The Webex cluster in China is isolated, and no media, data, or operational overlap exists from this cluster to other clusters outside China. This cluster is not enabled for globally distributed meetings capabilities so there is never a risk of media traversing Chinese servers. • All encryption keys for the Chinese Webex service are generated in China	• Zoom has a data center in China but does not have built-in segmentation in its infrastructure and configuration changes can send traffic to China. Zoom admits calls got 'mistakenly' routed through China.
Cisco Trust Center and data privacy programs	• Cisco hosts a Trust Center to ensure privacy and transparency needs of our customers are addressed • Cisco's Trust Center is our platform for sharing our commitment to security, trust, data protection, and privacy • Cisco's Trust Center hosts has over 56 privacy data sheets and data maps, including for Cisco Webex Meetings, Messaging, and Messenger • Cisco's Trust Portal is an on-demand delivery platform for public and confidential security assurance documentation. Customers can download white papers, privacy data sheets, and more. • Privacy data sheets are reviewed and kept up to date by Cisco legal and security teams • Cisco has our own data privacy office and also has three regional data privacy officers, who keep up to date with regional privacy requirements to ensure Cisco products align with requirements in the Americas, EMEAR, and APAC	• Zoom's privacy and security webpage and practices are not as thorough as Cisco's

Table 1. Webex privacy and security policies, processes, capabilities, and commitments

CAPABILITIES	INCLUSIONS AND COMMITMENTS FOR WEBEX	ZOOM
Cisco Secure Development Lifecycle (SDL)	· Product security baseline: More than 200 specific security requirements · Threat modelling: Identify, assess, and mitigate risk for 1000+ features per quarter · Privacy and Data Impact Assessment of all new features · Mandatory security training for product and engineering; over 35,000 employees have been certified · Employee Code of Conduct · Annual employee training on data privacy, data categorization, and data handling	· No mention of secure development or training on Zoom's website
Cisco Cloud Access Provider Review (CASPR) of third parties	· Due diligence of third-party cloud vendor's security and assessment of its privacy practices · Master Data Protection Agreements (MDPAs) exist between Cisco and our affiliates to mitigate risk associated with the supply of products and/or services by Cisco to customers · Vendor risk assessment	· There is a gap in third-party vendor assessments, such as Zoom used Facebook SDK integrations that sent user data to Facebook unknowingly. Zoom fixed the gap only after it was discovered by outside parties.
Security and privacy certifications	· SOC 2 Type II and SOC 3 · FedRAMP Moderate · ISO 27001 / 27017 / 270188 / 27701 · Cloud Computing Compliance Controls Catalog (C5) · CSA STAR L2 · Cisco has started the process with the DISA Cloud Assessment and Authorization Division to achieve DoD Impact Level 5 (IL-5)	Zoom does not have: · ISO 27001 / 27017 / 27018 / 27701 · C5
Cross-border transfers	· Binding corporate rules · APEC cross-border privacy rules · APEC privacy recognition for processors · EU standard contractual clauses	· No mention of APEC on the Zoom website · No mention of binding corporate rules

Security and privacy governance

Zoom does not publicly document any independent security group. The lack of an independent security group leaves decision making on features and security capabilities to the same people. There is a possibility (if not a probability) Zoom will prioritize features over security. This can result in a product that has security vulnerabilities, is missing security features, or has inadequate security testing. In addition, security expertise may not exist, leaving the company and product open to rapidly increasing security risks.

Zoom doesn't have users' individual privacy in mind, and users can't trust Zoom to keep their data safe. Reading through Zoom's privacy statement, it is clear to see (after working past the confusing language) that Zoom maintains the right to share users' data with third parties for business purposes. This is also exposed with the Apple iOS14 release, which clearly shows that Zoom collects a lot more personal data about users, and grants itself the right to use that information for advertising and marketing.

Cisco Secure Development Lifecycle (CSDL)

Zoom does not publicly document use of a secure development lifecycle. The lack of a secure development lifecycle increases the likelihood of having a significant number and higher severity of vulnerabilities in software.

Zoom does not publicly document internal security awareness training. The lack of security awareness training increases the risk of exposing customer data and increases the likelihood of security-related defects in the product due to lack of knowledge by developers and operations staff.

Security and privacy certifications

Zoom does not have an ISO 27001 certificate or 27017 or 27018 or 27701 certificates. ISO 27001 is an international certification that is usually required by international and enterprise organizations. The ISO 27001 certification assures compliance with requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. The ISO 27017 certification assures a system is meeting information security controls in relation to cloud services. The ISO 27018 certification assures a system is meeting commonly accepted control objectives, controls, and guidelines for implementing measures to protect Personal Information (PI). ISO 27701 outlines a framework for personally identifiable information (PII) controllers and PII processors to manage privacy controls to reduce the risk to the privacy rights of individuals.

Zoom does not have a Cloud Computing Compliance Controls Catalog (C5) attestation. C5 is often required by companies in Germany. It is a German government-backed attestation scheme introduced in Germany by the Federal Office for Information Security (BSI) to help organizations demonstrate operational security against common cyber attacks within the context of the German government's Security Recommendations for Cloud Providers. Using the C5 certification, customers can evaluate how legal regulations (i.e., data privacy), their own policies, or the threat environment relate to their use of cloud computing services.

Cross-border transfers

Zoom has not committed to the Asia-Pacific Economic Cooperation (APEC) Privacy Recognition for Processors (PRP) and Cross Border Privacy Rules system (CBPRs). APEC CBPR and PRP are a commitment to protect customer data with compliance and accountability to globally recognized privacy standards within the Asia Pacific region.

The APEC CBPR and PRP systems are independently verified privacy certifications built upon the nine principles of the APEC privacy framework endorsed by the 21 APEC member economies. The CBPRs focus on controls and accountability for data controllers. The PRP certification demonstrates a data processor's ability to honor the obligations passed down from data controllers when handling data on another's behalf.

There is a clear trend toward people (data subjects) taking their privacy more seriously and companies (data controllers and processors) being called upon to honor privacy as a fundamental human right. PRP fits within the broader picture of emerging data privacy and security standards and is consistent with the current trend of stakeholders seeking external, independent program validation.

Securing your users and identity

Table 2 outlines capabilities available within the Webex portfolio of products to secure users and identities.

Table 2. Securing users and identity

CAPABILITIES	WEBEX	ZOOM
Automated enterprise-grade user provisioning and lifecycle management	• **Active Directory (AD) synchronization:** This one-way sync ensures users are not only provisioned when onboarded to the enterprise (reducing your total cost of ownership), but more importantly, it ensures users are deprovisioned and tokens are revoked when the enterprise decides they should be deprovisioned • **Identity proofing:** Admins verify their domains to ensure the users they provision are who they say they are so when you join a meeting you can trust who you are collaborating with • **System for Cross-domain Identity Management (SCIM) provisioning:** Onboard users through OKTA and Azure AD integrations using SCIM, the industry standard. Taking advantage of our relationships in the industry, Cisco is continuously adding leading identity providers to the list of products that we support. Because Cisco uses standards instead of proprietary protocols, we can add new identity providers (IdPs) faster. • The People API on developer.webex.com and CSV are also supported • Upon password change in AD, Webex will revoke tokens of the user and ask the user to reauthenticate	Unlike Webex, which provides a full functionality AD Connector that is managed through Control Hub and provides IT admins with visibility, monitoring, control, and seamless integration into IT systems, Zoom does not support enterprise-grade management, as is evident from a Zoom AD Sync support article. • Zoom offers limited attribute support. Cisco supports the synchronization of 22 different attributes, rooms, groups, and avatars. Zoom only syncs first name, last name, email, and department. • Multi-domain and multi-forest are not supported • Zoom does not support user reauthentication upon password reset in AD
Blocking use of a personal account login to Webex	• Reduce data loss concerns by restricting users to only use their company email for Webex on the corporate network	• Zoom provides no equivalent functionality

Table 2. Securing users and identity

CAPABILITIES	WEBEX	ZOOM
Multi-Factor Authentication (MFA)	· Reduce fraud via phishing and password stuffing attacks by using a second factor in the authenticating of users	· Both Cisco and Zoom include MFA capabilities, but in Zoom, MFA needs to be provisioned to users, groups, or the entire organization. Unlike Zoom, Cisco has enhanced capabilities to protect users by combining Cisco Duo with Webex. Cisco Duo includes MFA and also builds on the technology to provide zero trust by ensuring the devices joining the meetings, network, or services of the company meet the minimum security policies set up in an organization. This can include things like patch level and disallowing jailbroken phones, to name just two of the 32 policy attributes on a device.

Automated enterprise-grade user provisioning and lifecycle management

Active Directory (AD) synchronization

Zoom has a directory sync tool, but most enterprises concerned about security will not use the tool for several reasons.

1. Zoom stores the client secret and API key in the application on the local machine.
2. Zoom does not support container selection or an LDAP filter to select users.
3. Zoom does not have a policy filter, which limits deletion events to prevent large numbers of users from being deleted from Zoom.
4. Zoom does not support high-availability deployments for failover in case directory sync software is not available in the default location.
5. Zoom only supports five AD attributes. Cisco supports 22 AD attributes, room sync, and avatar sync from AD.
6. Zoom does not support monitoring of the synchronization process. Cisco Directory Connector has visibility into the synchronization service via the admin console in Control Hub (the admin console on the Windows OS) and natively plugs into Event Center tools within Windows so enterprise monitoring tools can alert if a log event meets specific thresholds.

7. Webex released a new capability that will listen for when users reset their password on-premises in the AD and notify Webex on the next incremental sync that the password has been reset. If the admin enables this feature, users' existing tokens in Webex will be revoked for Webex clients and the user will have to reauthenticate. This is part of Cisco's commitment to a strategy of continuous access evaluation. Zoom has no equivalent functionality.

Identity proofing

Zoom allows for users to be created without validating that those admins have the authority to manage the users from those domains. In Webex, admins verify their domains to ensure users they provision are who they say they are so when a person joins a meeting, they can TRUST the person with whom they are collaborating. This proofing mechanism ensures the administrator has the rights to the domain they verify so users can be created without having to receive an email or go through another proofing service to verify their identity.

SCIM user provisioning and deprovisioning

With Cisco, admins can onboard users through OKTA and Azure AD integrations using SCIM, the industry standard. Leveraging our relationships in the industry, Cisco is constantly adding leading identity providers (IdPs) to the list of products that we support. Because Cisco uses standards instead of proprietary protocols, we can add new IdPs faster.

Integrating with IdPs at this level allows for increased security by allowing IdPs to deactivate users when their status changes. This deprovisioning state immediately revokes the token, meaning users lose access within minutes of the event. Zoom and other systems rely solely upon time-based tokens to enforce security, which means users can still have access despite their status changing at the IdP.

Multi-Factor Authentication (MFA)

Most people today use less than five passwords across their different Internet sites, allowing attackers the ability to replay passwords from compromised sites in other accounts until they find a site where that password has been reused. Cisco Duo is the leading multifactor solution in the market, and when paired with Control Hub and a leading identity provider for lifecycle management, it offers a zero-trust collaboration environment. Cisco Duo provides more than just MFA; it can also identify risky devices, enforce contextual access policies, and report on device health using an agentless approach or by integrating with your device management tools.

Risk-based authentication

Webex has worked with leading IdP providers and zero trust solutions like Cisco Duo, OKTA, Microsoft Azure AD, ForgeRock, and Ping Identity to integrate with their risk-based authentication modules. Using these solutions in concert with Webex security, a customer can manage access. Use 30 different values, including IP address, location, device fingerprinting, login history, and geolocation with machine learning and artificial intelligence ML/AI to provide the best authentication challenge for right situation. Paired with SCIM-based provisioning, these risk-based engines can also inactivate users, so they lose access immediately.

Blocking use of personal account login to Webex

Zoom does not support restricting users to using only their company email; Zoom users can also use a personal email account. Enterprises may want to ensure that all users are using only their corporate accounts to access Webex. Cisco has worked with leading network proxies like Cisco Web Security Appliance (WSA) to add a rule that specifies which domains are allowed to authenticate to Webex. For example, if acme.com only wants users from acme.com to authenticate, they can specify acme.com in the rule and Webex will inspect the authentication header and deny authentication from all users that do not have acme.com domains. Read how to configure your network to achieve this functionality with Webex.

Securing your apps and devices

Table 3 outlines Webex capabilities to secure apps and devices.

Table 3. Securing apps and devices

CAPABILITIES	WEBEX	ZOOM
Native Mobile App Management (MAM) control	Supported in Webex	Zoom does not have "native MAM" controls like Webex
Remote wipe: Native security controls	Supported in Webex	Zoom does not offer a native option for an administrator to remotely wipe out data stored in iOS and Android to handle scenarios for personally managed devices such as stolen devices and terminated users
Mobile pin-lock requirement: Native security control	Supported in Webex	Zoom does not offer a native option for an administrator to ensure users can only launch the Zoom app on mobile devices protected with lock screens
Disable the use of unmanaged apps: Native security control	Supported in Webex	Zoom does not offer a native option for an administrator to ensure users cannot log in to an unmanaged mobile app downloaded from the Apple Store or Google Play Store
File share controls by device type: Native security control	Supported in Webex	Zoom does not offer options for an administrator to apply policies to restrict users from downloading, previewing, or uploading files by device type such as mobile, desktop, or web
Full encryption of a local cache on clients	Supported for Webex desktop and mobile clients	Zoom does not support full encryption of data cached on a client device
Custom idle timeout for Web App and Control Hub	Supported for Webex browser-based clients and Control Hub	Zoom does not offer an option for an administrator to apply policies for how long a web user's session can stay idle before they're signed out for both in-network and off-network web users of the applications

Securing apps and devices

Zoom does not have native MAM controls like Webex does. The big drawback of this is that security-sensitive customers will be required to use either MDM or Intune MAM in order to secure the app from a data leak perspective. For instance, being able to revoke continued access to the app by a user who might have left the company or whose mobile device might be stolen.

The default Apple App Store or Google Play Store app has no additional administratively enforced controls such as pin lock or encryption at rest. Webex gives a baseline set of controls that allow IT administrators to deploy the tool without worrying or spending additional money on MDM or MAM licenses, if it is not already part of their deployment.

Securing your meetings and content by default

Table 4 outlines Webex capabilities to secure meetings and content by default.

Table 4. Securing content

CAPABILITIES	WEBEX	ZOOM
End-to-end encryption for Webex Meetings	· This optional control, available for more than 12 years, enables a meeting host to allow encryption when using the Webex Meetings app · Highly scalable · The meeting encryption key is generated by the meeting host and securely distributed to meeting participants. The Webex Cloud does not have access to meeting encryption keys. · Cisco will support standards-based end-to-end encryption and end-to-end identity with Zero Trust Security starting in Q2 CY2021	· Zoom only recently introduced end-to-end encryption for meetings, which is proprietary
End-to-end encryption in the messaging app	· User-generated content (messages and files) that are shared in Webex spaces are encrypted end to end by the Webex before being sent to the Webex cloud over TLS, with a few exceptions. This user-generated content is stored in its encrypted form in the Webex cloud. · End-to-end encryption keys are created for each Webex space using a Webex Key Management Service (KMS) · Customers can choose to use the Webex cloud-based KMS or deploy the KMS on their premises (as part of our Hybrid Data Security [HDS] service), which allows customers to hold keys	· Zoom does not support end-to-end encryption for IM or chat. Like Zoom meetings, Zoom claimed to offer end-to-end encryption as an option for its instant messaging service, but Zoom changed its messaging to "advanced chat encryption."

Table 4. Securing content

CAPABILITIES	WEBEX	ZOOM
In-house transcription of recordings	- All recordings and transcriptions are AES 256-encrypted and stored at rest in the Webex Cloud - Recordings are encrypted with a Webex KMS derived key - Webex KSM is hosted and operated by a separate Cisco security team. The Webex Meetings team does not have access to the keys. - Customer data is not used for transcription service training	- Zoom uses third-party Otter.ai with questionable security and privacy policies. Otter.ai uses customer data for training

IM and chat end-to-end encryption

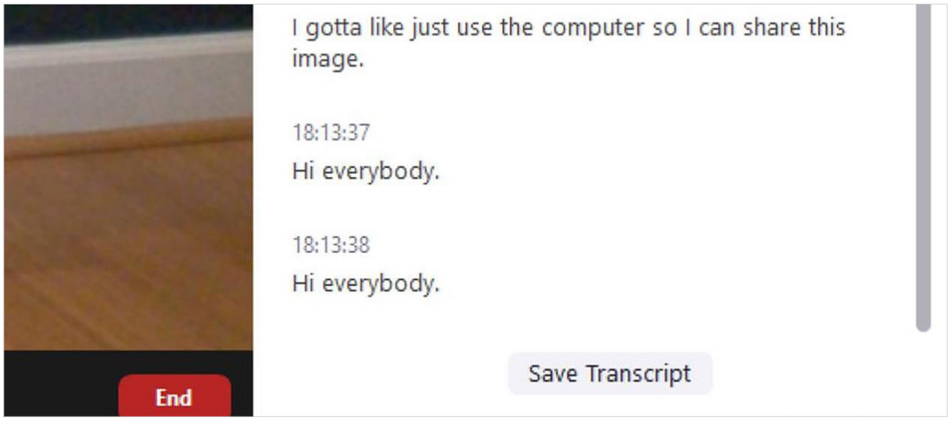
Zoom claimed to offer end-to-end encryption as an option for its instant messaging service, but the company recently changed this to advanced chat encryption, which uses the transport layer encryption protocol, Transport Layer Security (TLS), to encrypt chat messages. Zoom's documentation does not clearly state how this advanced chat encryption differs from the standard process of encrypting data in transit with TLS, which all cloud vendors use.

Webex uses an additional layer of encryption for messages and files that protects your data from interception in transit and at rest. Like all cloud collaboration vendors, Webex uses TLS to encrypt data in transit and encrypts data at rest in our apps and Webex Cloud content storage service.

By default, Webex also encrypts any messages or files that users send from Webex before it is sent over TLS to the Webex Cloud. This encrypted, user-generated content is securely stored in the Webex Cloud on content servers that use disk encryption. Webex uses a unique AES-256-GCM encryption key for each Webex space. These encryption keys can be generated and stored in the Webex Cloud, or optionally generated by the Webex Hybrid Data Security Service installed on a customer's premises and stored in the customer's on-premises database.

In-house transcription of recordings

Zoom does not offer its own transcription services for recordings and uses third-party Otter.ai with questionable security and privacy policies. Zoom is also not up front to customers that it uses third-party Otter.ai for transcription. Zoom fails to mention this information on its main and support webpages or in the Zoom app (see screenshot immediately following). This puts the burden of compliance on the customer and could result in increased compliance risk, sensitive data leakage, and privacy risks.


I gotta like just use the computer so I can share this image.

18:13:37
Hi everybody.

18:13:38
Hi everybody.

Built-in compliance tools eliminate need for third-party solutions

Tables 5 covers compliance tools customers can use to remove the need for third-party solutions.

Table 5. Available compliance tools

CAPABILITIES	WEBEX	ZOOM
Flexible retention control	Supports a flexible and customizable retention policy: • From 7 days up to 12 months of retention of recordings and transcripts • From 24 hours up to indefinite retention for messages and files	Zoom does not support a flexible retention policy for meeting recordings: • Recordings will be saved for a minimum of 30 days and a maximum of 120 days • If a customer wants to archive recordings for longer than 120 days, the customer will need to purchase a third-party archiving solution, which could result in increased cost, management, overhead, and compliance risk

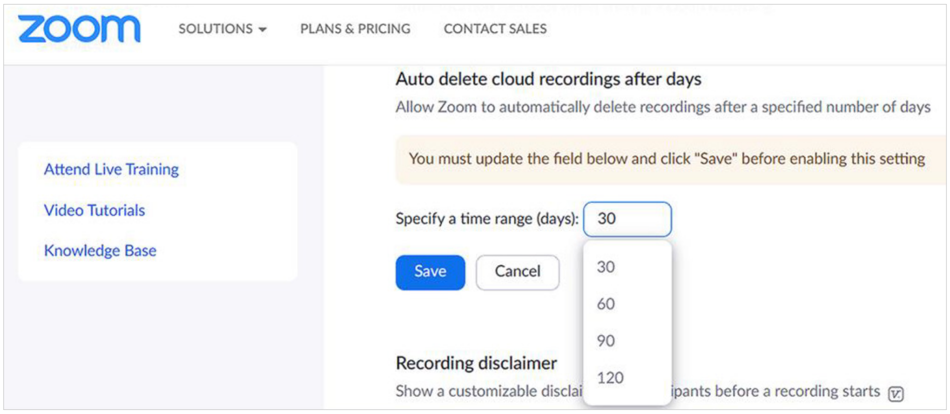
Table 5. Available compliance tools

CAPABILITIES	WEBEX	ZOOM
Legal hold	Native support for messaging (messages and files) and meeting[1] (recordings and transcripts) content generated by users	Zoom does not have native support for placing custodian data on a legal hold. This requires leveraging a limited set of third-party integrations.
eDiscovery	Native eDiscovery support for space messaging (messages and files) and meeting[1] (recordings and transcripts) content generated by users, with reports in the standard eml output format that is compatible with downstream eDiscovery tools	No native support is included. Limited support is available via some third-party integrations

[1] Legal hold, eDiscovery, and DLP support for meetings recordings and transcripts for FedRamp is on the roadmap for release.

Retention

The Zoom retention policy support for meeting recordings is not flexible since a customer can retain recordings for only up to 120 days. For example, if a customer has a requirement to retain recordings for a year for corporate compliance, then Zoom does not offer the flexibility out of the box.



Auto delete cloud recordings after days

Allow Zoom to automatically delete recordings after a specified number of days

You must update the field below and click "Save" before enabling this setting

Specify a time range (days): 30

Recording disclaimer

Show a customizable disclai ipants before a recording starts

Legal hold and eDiscovery

Legal hold and eDiscovery are essential tools for enterprise compliance. The failure to identify, preserve, and discover all the Electronically Stored Information (ESI) that is relevant to a legal action or litigation may lead to a claim of spoliation of evidence. This can result in massive fines from a court or even more serious sanctions such as a dismissal of claims or defenses. An example of such ESI includes user messages, files, meeting recordings, and transcripts.

Zoom does not support legal hold capabilities for messaging or for meetings recordings and transcripts. Zoom does not natively support eDiscovery and has limited eDiscovery support via a few third-party vendor integrations. This means the compliance burden is on the customer and could result in increased compliance risk, costly mistakes, increased cost, and the need to work with new third-party vendors.

Data loss protection

details data loss protection (DLP) capabilities built into Webex products.

Table 6. Available data loss protection capabilities

CAPABILITIES	WEBEX	ZOOM
Protect sensitive data leakage	· Integrated data loss protection with Cisco Cloudlock® and third parties for both Webex meetings and messaging · Detection and remediation policies are purpose-built and tuned for Webex (space memberships, message, and file-based violations) · Out-of-the-box policies are available for several regulated industries (finance, healthcare, etc.) to accelerate deployment time	· No native or integrated data loss prevention offer is available for Zoom chat

Table 6. Available data loss protection capabilities

CAPABILITIES	WEBEX	ZOOM
Data loss protection (DLP) and archival partner ecosystem	· An extensive partner ecosystem includes more than 10 industry-leading archival and data loss protection/Cloud Access Security Broker (CASB) vendors for messaging and meetings · Prebuilt and tested integrations result in faster time to market and reduce custom development work · A large partner ecosystem gives customers the option to use existing data loss protection products from their partner vendors	· Limited support is available for a general-purpose, leading enterprise DLP and archival system
Cross-organizational policies	· Block all external communication in Webex spaces · Allow external communication with specific domains in Webex spaces	· Zoom may not have adequate protection and controls when a user communicates with external organizations
Ethical Wall: Block internal communication	· The Ethical Walls capability allows IT admins to prevent interaction between groups within an organization and ensures that you and your teams always adhere to regulatory policy requirements when sharing information	· No support for an Ethical Wall for Zoom IM/Chat
Space classification based on data governance policies	· An admin can define labels based on data governance policies and enforce all users to classify spaces they create (for instance, as public, confidential, highly confidential, or secret)	· No support for data classification for Zoom IM/Chat
Manage external integrations	· Granular access control is supported for individual integrations	· Granular access control is not supported for individual integration. External integration can only be globally turned off or on for all external integrations or for none.
Manage bots	· Supported in Webex	· Not supported

Zoom does not natively support sensitive data leakage prevention for messaging and meetings recordings and transcripts. This could result in a potential compliance risk, loss of data, and increased risk when scaling out the solution enterprise-wide.

Zoom has minimal archival and a minimal DLP partner ecosystem for IM/chat messaging, meeting recordings, and transcripts. This might necessitate a custom and costly effort to use third-party DLP and archival products that are not pre-integrated. Without an extensive partner ecosystem and pre-built solutions, customers may have to work through onboarding new partners, resulting in increased expenses and time to complete a rollout.

Webex supports archival and DLP functionality, either natively or via pre-integrated solutions with leading, enterprise-grade archival and DLP solutions for messaging and meetings. For customers in regulated verticals that have strict compliance and data loss requirements (including high-risk users), Webex offers near-native, easy-to-set-up policies out of the box. Webex also provides a diverse choice of partners to meet different customer needs.

Managing external integration

Zoom supports all external integration to be globally turned on or off but it does not support granular admin control for managing external integrations, such as control to allow or deny Zoom users to integrate Google, Microsoft Office 365, Facebook accounts, and other third-party applications with a Zoom account. Zoom also does not empower administrators to allow only those third-party apps that meet its security and data handling standards.

Zoom does not provide admin controls to manage cross-organization collaboration for IM and chat, such as the ability to restrict all users in the organization from communicating with anyone in external organizations or allowing users the ability to communicate with external users from only admin-approved domains.

Data loss prevention policies are critical when collaborating with external users (such as users who belong to a different organization, like partners and vendors). This rapidly expanding external surface area of communication poses a risk of inadvertent or intentional loss of data and intellectual property. Unlike Zoom, Webex can prevent unauthorized instant messaging with users from external organizations and enforce (near native or via partners) data loss prevention policies when users generate content in external spaces.

Webex protects different surface areas of information leaks effectively while giving admins and security personnel the latitude to define policies that best meet their risk and security posture.

Cisco on the Cisco advantage and extended security options

Table 7. Available extended security options

CAPABILITIES	WEBEX	ZOOM
Security Bundle: Cisco Cloudlock	Integrated CASB and DLP for Webex messaging and meetings in the Webex app	Not supported in Zoom and lacks bundling of advanced security capabilities for easy purchase and deployment
Security Bundle: Cisco Talos® ClamAV	Integrated anti-malware scan of all files uploaded and downloaded to protect users from malicious threats in Webex	Not supported for Zoom IM/chat

While Zoom partners with external third parties for DLP, it does not currently offer an integrated security bundle. Zoom does not offer any native protection to prevent sensitive data leakage, specifically when its users are collaborating externally with their customers and partners. Examples of such sensitive data could include intellectual property, personally identifiable information (PII), personal health information (PHI), and payment cards. If your user is sharing such sensitive data in a file or message, either accidentally or intentionally, Zoom cannot detect and prevent such data leakages.

Zoom also does not offer anti-malware protection from Trojans, viruses, and ransomware attacks from malicious actors. Viruses and malware may get distributed in your organization, either accidentally or intentionally, while sharing files externally, or when using devices that aren't managed by your corporate IT teams.

For more information
Please visit webex.com

January 2022

webex by cisco