



TechClub Collaboration

Jaroslav Martan
jmartan@cisco.com



Agenda

- Cisco – Microsoft Interoperability
 - Cisco video device in MS Teams conference
 - Cisco plugins for MS Teams
- Webex Teams Security
 - Compliance & DLP
 - Anti-malware
 - Hybrid Data Security



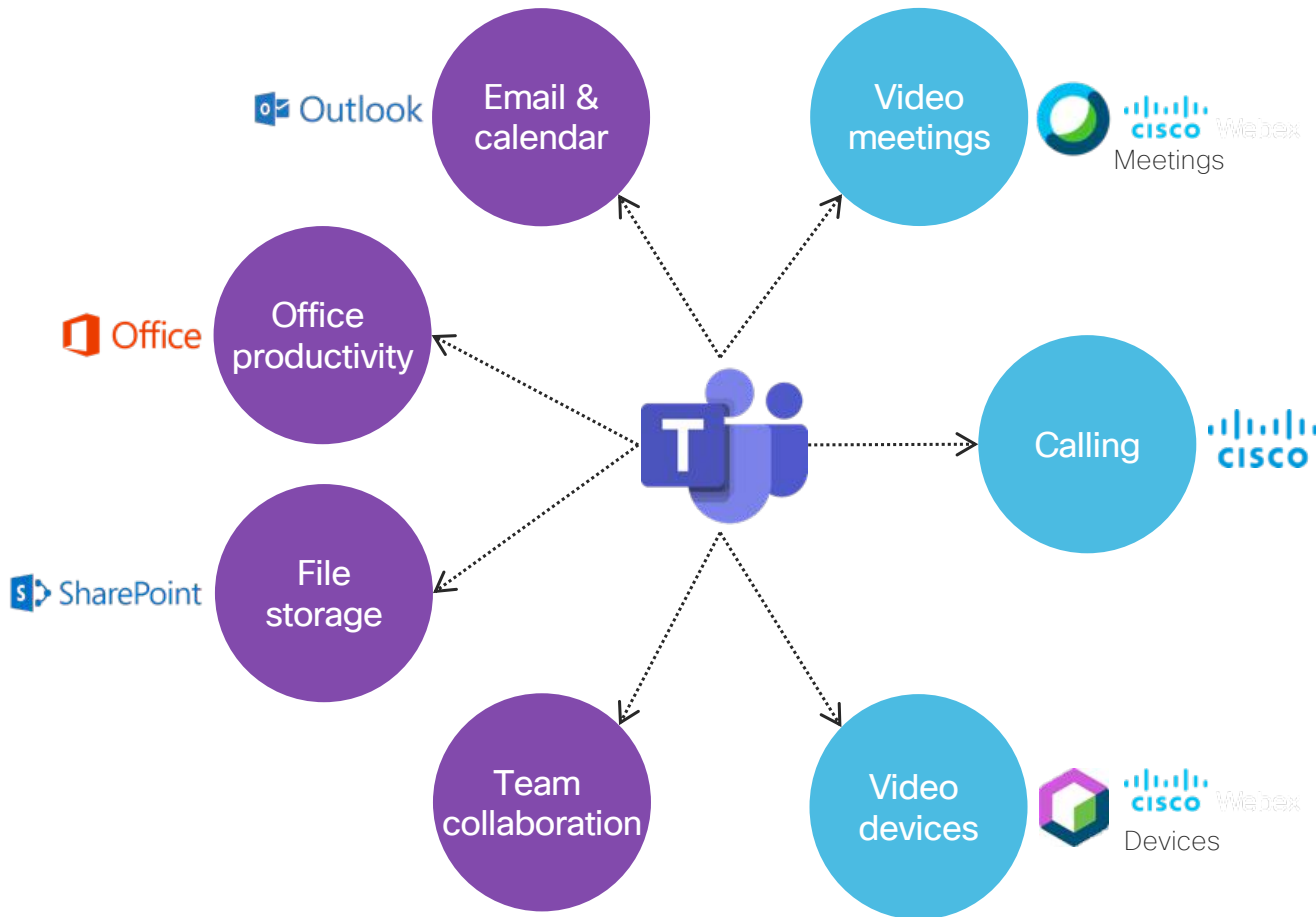


Cisco + Microsoft

Creating better experiences, together.



Client vs. Workload choice

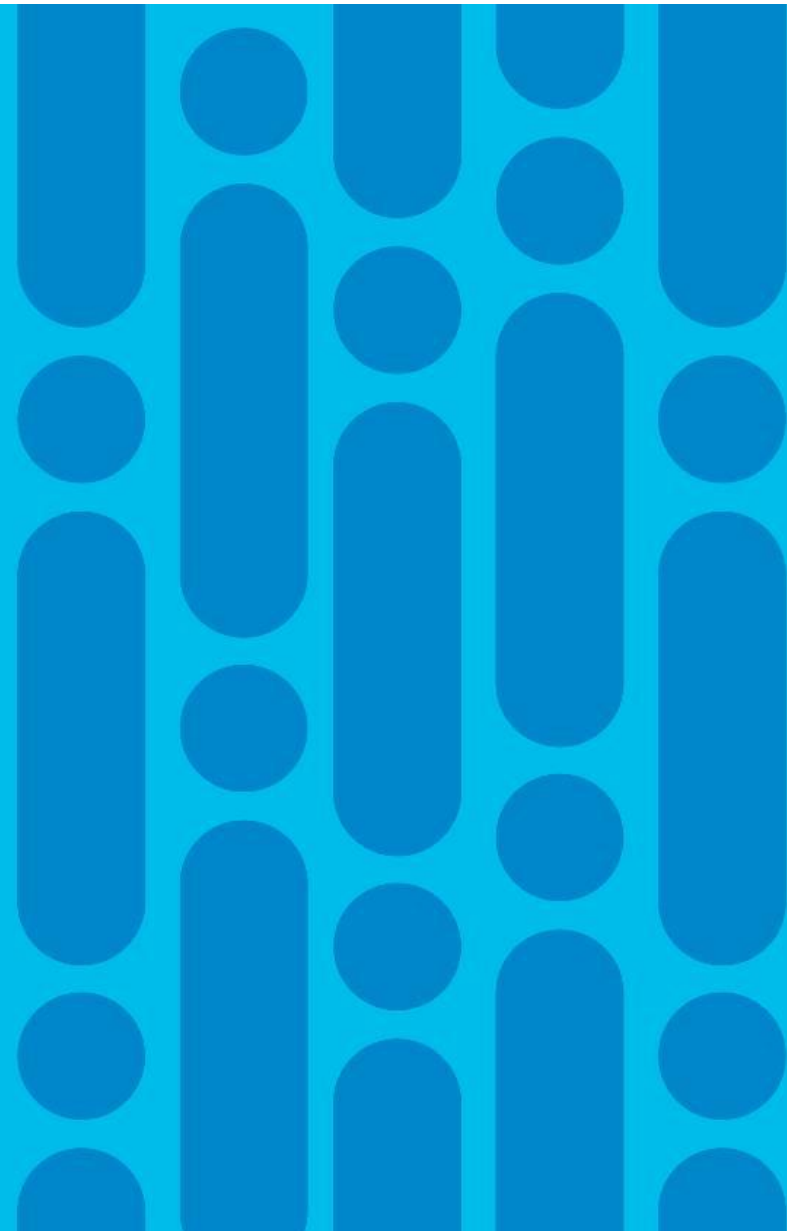


Using Microsoft Teams as a client does not prevent the use of Cisco for multiple workloads:

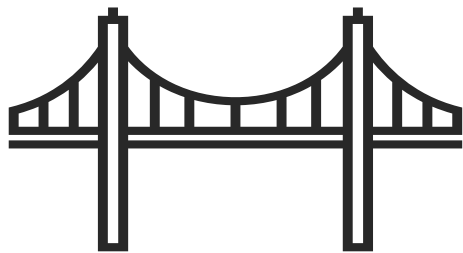
- Video endpoints (Webex Rooms)
- Meetings (Webex Meetings)
- Calling (on prem & cloud options)

Workload integrations based on Microsoft supported APIs

Video Integration for Microsoft Teams



Cisco + Microsoft Partnership for Meetings



Cisco and Microsoft
have come together
to deliver a better user
experience

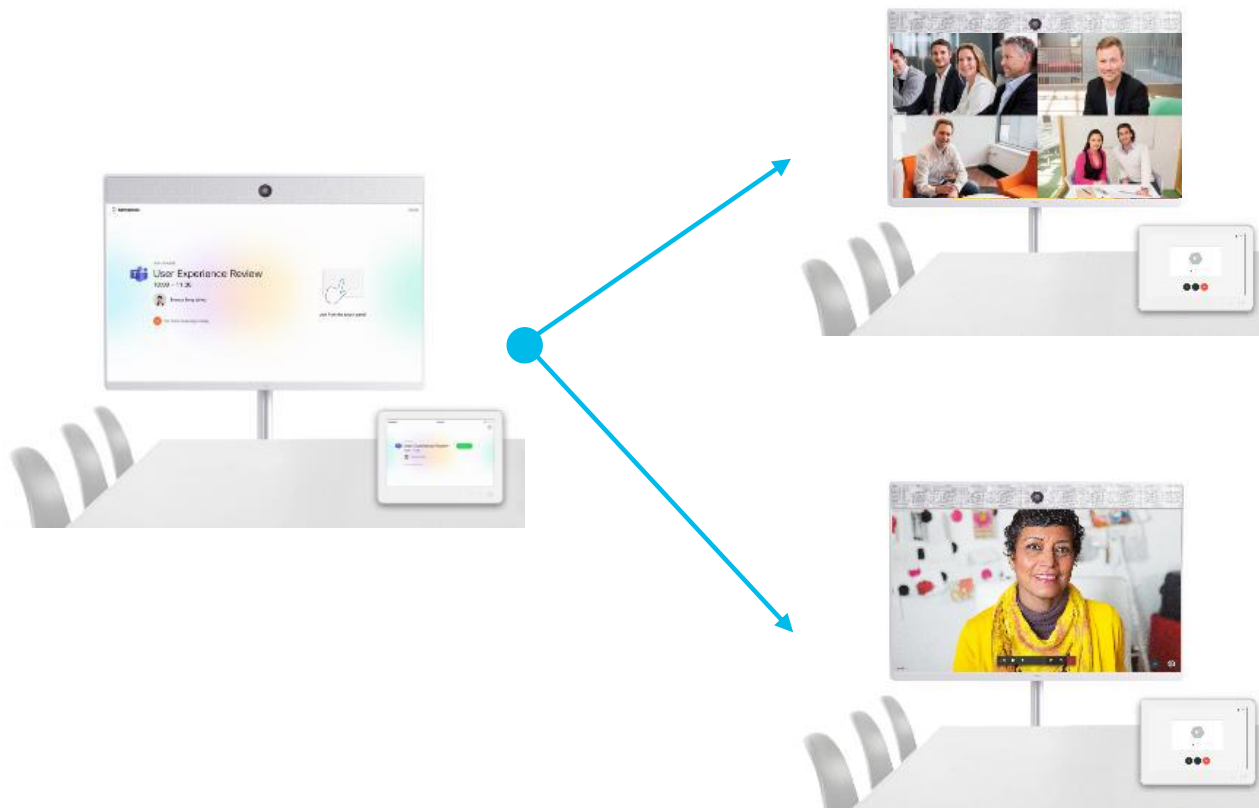
1

Cisco will be a certified Microsoft CVI partner

2

Microsoft Teams will work with Cisco Webex Rooms via modern web technologies

Video endpoints joining Microsoft Teams meetings



SIP-capable video endpoints can join Microsoft Teams meetings (hosted by my company) via CVI Cloud Gateway

Richer, seamless meeting experience, without requiring 3rd party interop

Cisco Webex web-engine capable devices* can join B2B Microsoft Teams meetings

Limited experience on Cisco devices using Microsoft Teams meeting web app

*Must be cloud registered or cloud aware



Video Integration for Microsoft Teams

Microsoft Cloud Video Interop

Joining Microsoft Teams meetings – CVI gateway

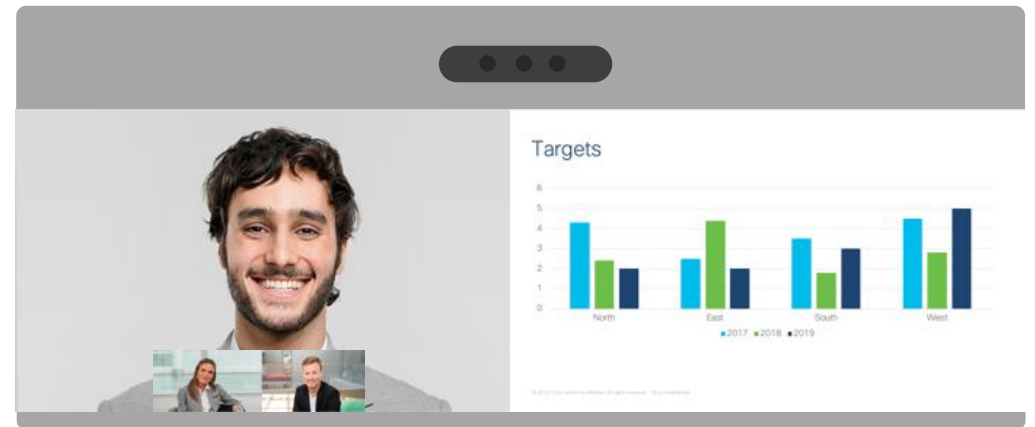
One Button to Push experience



Joining Microsoft Teams meetings– CVI gateway Layout example (dual screen)



Active Speaker



Active Speaker w/ Content Share

*Subject to changes in layouts of Webex Meetings/Webex Rooms

Single screen flexible layouts

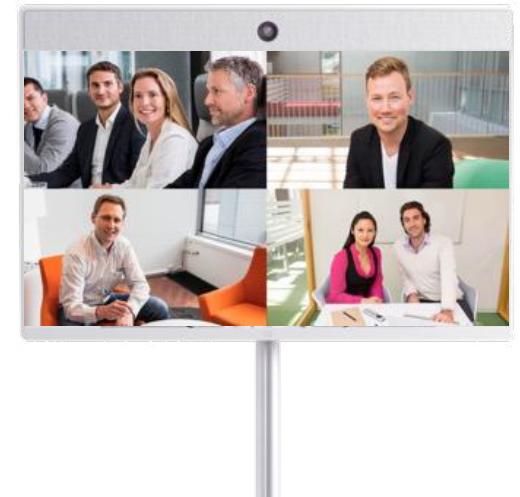
CVI Gateway will provide flexible layouts to video devices while Microsoft Teams users will see their respective layouts



Active Speaker

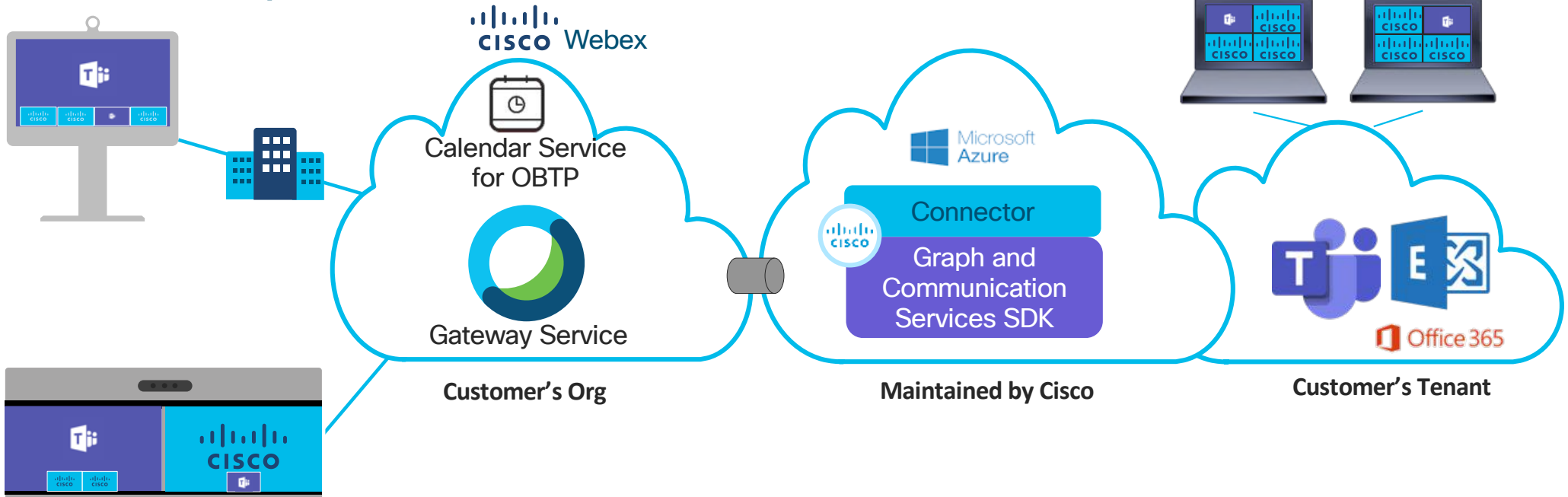


Overlay



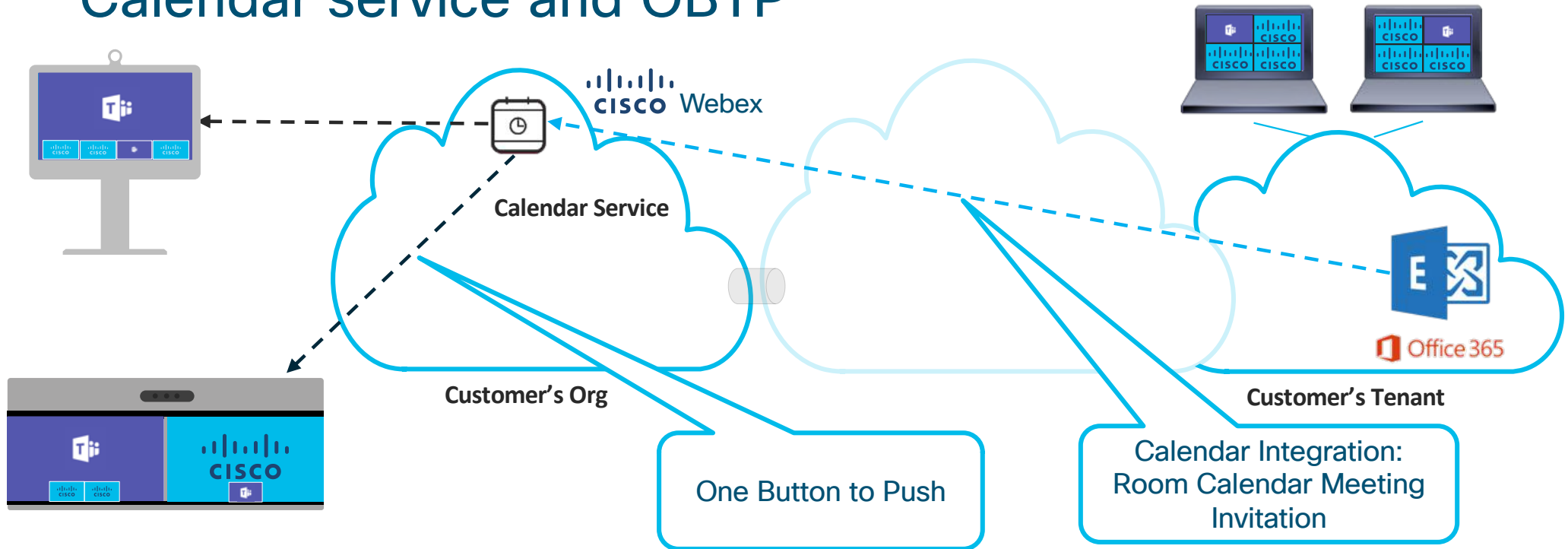
Equal

Cloud Video Interop gateway Cisco implementation



- **Cisco Cloud Video Interop gateway (CVI)** is a service provided by the Cisco Cloud and does not require on-premises components nor software upgrades on video devices
- **Webex video infrastructure and Microsoft SDK** are hosted in Azure and **maintained by Cisco** on behalf of customers
- Available to **On-prem Registered, Cloud Registered/Aware Webex Rooms**, and **3rd party SIP endpoints**

Cloud Video Interop gateway Calendar service and OBTP

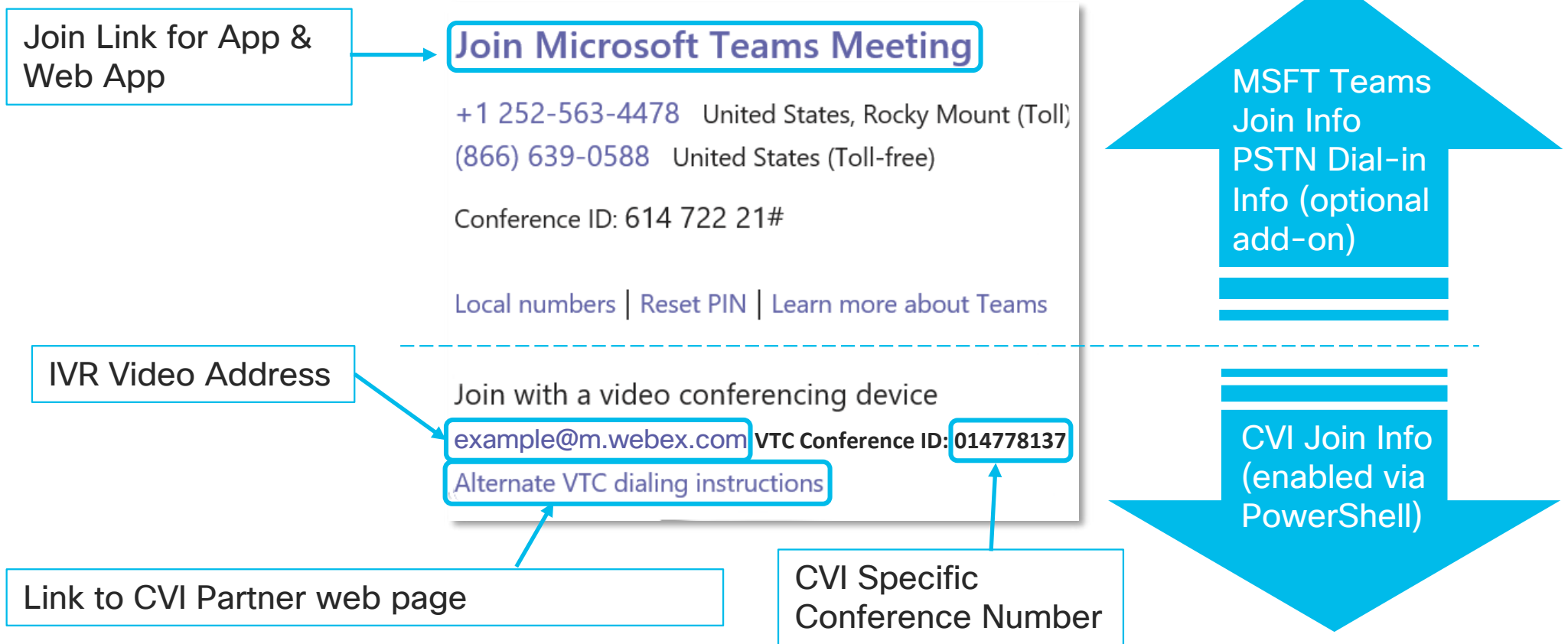


- OBTP traffic
- - - Graph API

- Calendar integration is required for OBTP
- OBTP is supported for Webex on-prem registered, Webex Cloud registered* and Webex Edge for Devices (cloud aware) video devices

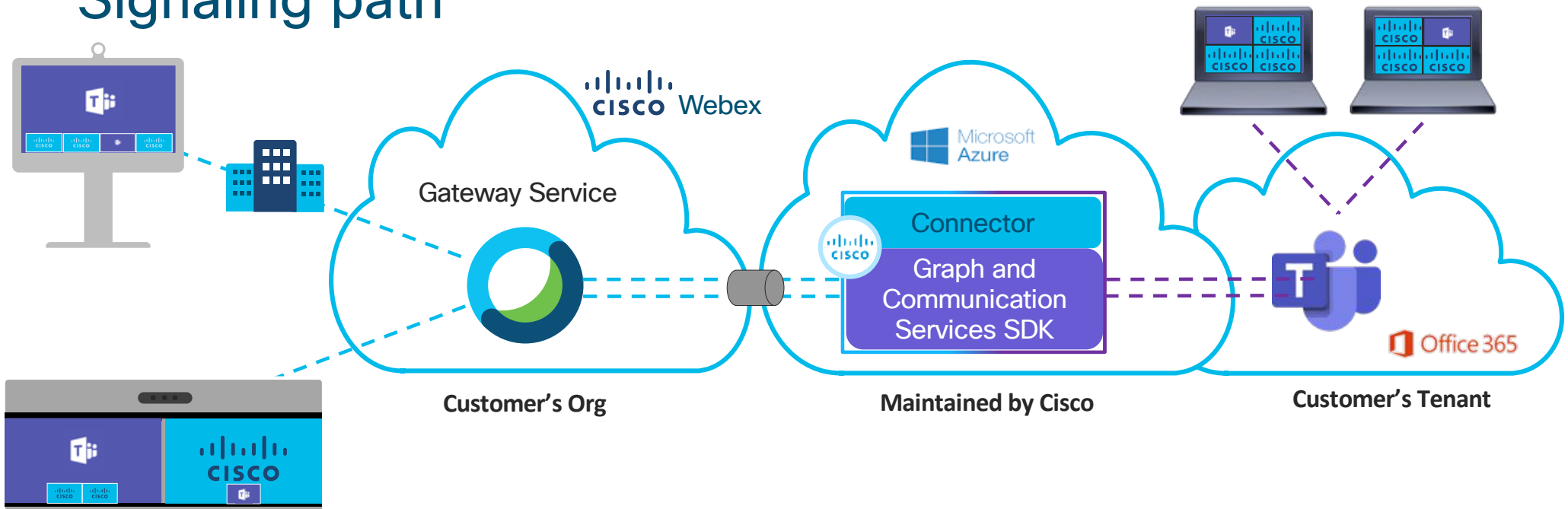
*Cloud registration is best practice as it also provides support for WebRTC

Example Teams invite (generated by Microsoft)



Cloud Video Interop gateway

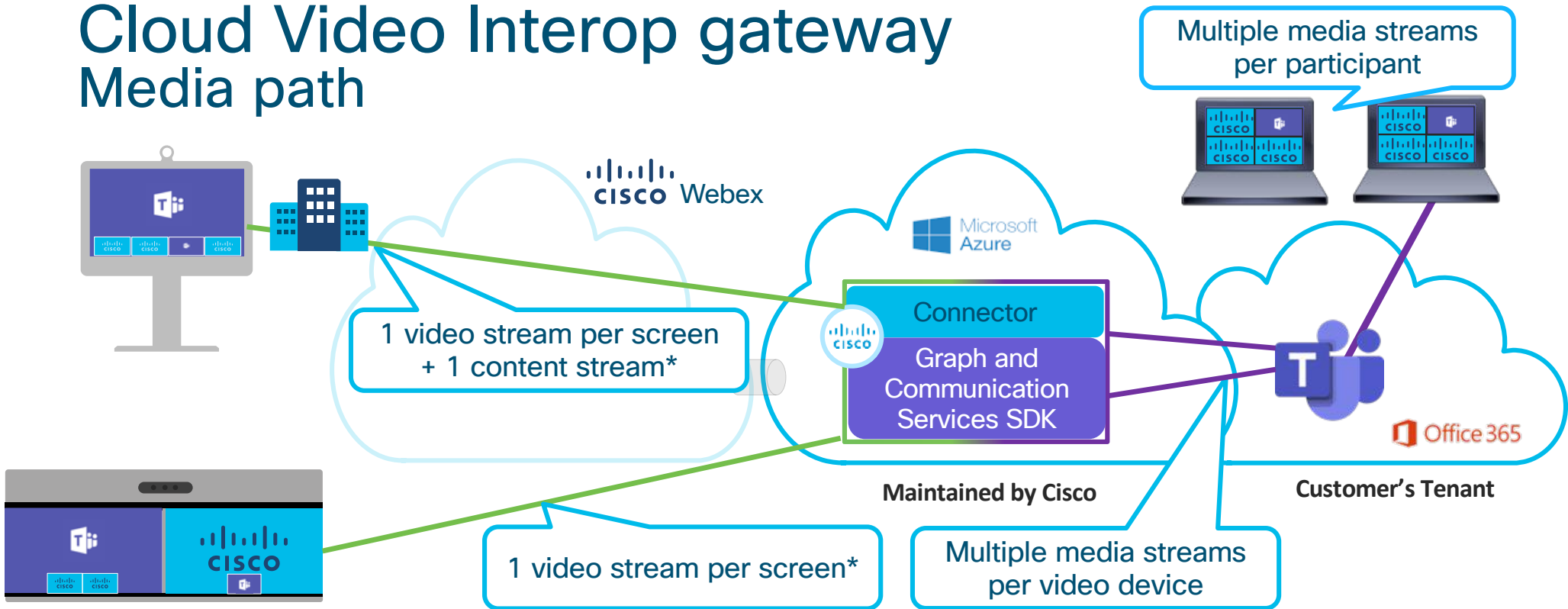
Signaling path



- Cisco signaling
- Microsoft signaling

- On-prem video devices must be able to call the Webex domain for CVI over SIP
 - Interworking to H.323 can be provided by **local on-prem infra** (i.e. VCS/Expressway)
- Example: Endpoint<->CUCM<->Expressway-C<->Expressway-E<-internet->WebexCloud

Cloud Video Interop gateway Media path



- Media of Webex cloud registered video devices flows directly to the Azure DC maintained by Cisco
- Media of on-premises-registered video devices flows to the Azure cloud maintained by Cisco via the local SIP infrastructure:
Example: Endpoint<->Expressway-C<->Expressway-E<-Internet->Cisco-maintained Azure Tenant
- No Video Mesh support

*Up to 2 video streams per endpoint and up to 10 participants from Teams

Cisco VIMT (CVI) Features Summary

Supported video devices

- Cisco Webex Cloud registered
- Cisco Webex on-prem registered
- Cisco Webex Edge for Devices
- SIP standard based
(H.323 via on-prem interworking)

Family of layouts for Video devices

2-way content sharing

Layout control via DTMF

Recording Indicator

Configurable lobby management policy (guest access)

Unique features for Cisco Webex Rooms

OBTP Join (One Button To Push)

Multi-screen support

Integrated Roster List with Indicators (i.e. Active Speaker, Content Share, Mute)

Full roster list

Unidirectional Whiteboarding from Webex Board and DeskPro (non-interactive)

Some of these features might be available at different times for different deployment models (cloud vs on-prem) ...*see next slide*

Caveats

- Content sharing will be possible via cable and wireless*
- No Video Mesh (Hybrid Media)
- Media traffic for Cisco Webex **Cloud-registered devices** will directly flow to the Cisco Azure Tenant
- Media traffic for **on-prem registered** video devices will be routed toward the Cisco Azure Tenant **via on-prem Expressway-C/E** or other CPE firewall traversal
- **One Microsoft Tenant** per Webex Org will be supported at GA

*wireless sharing does not work for cloud registered devices

Lobby Policy

- Meeting options (calendar invitation)

Meeting options

Who can bypass the lobby? People in my organization ▾

Always let callers bypass the lobby

Announce when callers join or leave

Who can present? Everyone ▾

Note: In the screenshot, the dropdown menu for "Who can bypass the lobby?" is open, showing options: Everyone, People in my organization and trusted organizations, People in my organization (highlighted), and Everyone.

- Meeting Policies (admin center)

Participants & guests

Participant and guest settings let you control access to Teams meetings for people that dial in using a phone. [Learn more](#)

Let anonymous people start a meeting ⓘ Off

Automatically admit people ⓘ Everyone in your organization ▾

Allow dial-in users to bypass the lobby ⓘ Everyone ▾

Allow Meet now in private meetings Everyone in your organization ▾

Enable live captions Everyone in your organization and federated organizations ▾

Allow chat in meetings Disabled but the user can override ▾

Allow chat in meetings Enabled ▾

Cisco Webex CVI provisioning - Setup page

The screenshot displays the Cisco Webex Control Hub interface. On the left is a dark sidebar with navigation options: Overview, Users, Places, Services (highlighted with a blue box), Devices, Analytics, Troubleshooting, and Settings. Below these are Media Fusion and Media Fusion 1 options. The main content area is divided into sections: 'On-Premises Resources' (Manage resources that are registered to the cloud and view related configuration. All Resources View), 'Video Mesh' (Resources View all, Service Edit settings, and an Impaired Service indicator), and 'Inactive Hybrid Services'. The 'Inactive Hybrid Services' section contains four cards: three for 'Hybrid Calendar' (Exchange, Office 365, Google) and one for 'Video Integration' (Microsoft Teams). Each card includes a description of the service and a 'Set Up' button. A blue arrow points from the 'Services' menu item to the 'Services page' label. Another blue arrow points from the 'Set Up' button in the 'Video Integration' card to the 'Click Set Up' label.

Services page

Click Set Up

Set up Flow

The screenshot displays the Cisco Webex Control Hub interface. On the left is a dark sidebar with navigation options: Overview, Users, Places, Services (highlighted in blue), Devices, Analytics, Troubleshooting, and Settings. At the bottom of the sidebar is Media Fusion. The main content area is a white modal window titled "Video Integration Setup" with a close button (X) in the top right corner. Below the title is the heading "Microsoft Teams". The text explains that the Microsoft Teams Meetings Video Integration Service needs permission to access Microsoft 365 on behalf of users. It instructs the user to click "Authorize" to sign into Microsoft and accept permissions, after which the browser should be redirected. If not redirected, the user should return to admin.webex.com and start the process again. A blue "Authorize" button is located in the bottom right corner of the modal.

Cisco Webex Control Hub

- Overview
- Users
- Places
- Services**
- Devices
- Analytics
- Troubleshooting
- Settings
- Media Fusion

Video Integration Setup

Microsoft Teams


The Microsoft Teams Meetings Video Integration Service needs permission to access Microsoft 365 on behalf of your users.


Click **Authorize** to sign into Microsoft and accept [permissions](#) for the service. After you accept, your browser should redirect you back here. If you're not redirected shortly, return to admin.webex.com and start this process again.

Authorize

Set up Flow (Microsoft Authorizations)

The image shows a two-step Microsoft authentication process. On the left is a sign-in screen, and on the right is a permissions request screen. A blue arrow points from the 'Next' button on the sign-in screen to the permissions screen.

Microsoft Sign in
cory.collaboration@example.onmicrosoft.com 
No account? [Create one!](#)
Can't access your account?
[Sign-in options](#)
Next

Microsoft
cory.collaboration@example.onmicrosoft.com
Permissions requested
Accept for your organization
 **Webex Video Integration for MS Teams**
[App info](#)
This application is not published by Microsoft.
This app would like to:
- Read domains
- Access media streams in a call as an app
- Initiate outgoing 1 to 1 calls from the app
- Initiate outgoing group calls from the app
- Join group calls and meetings as an app
- Join group calls and meetings as a guest
- Read online meeting details
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)
Cancel **Accept**

Azure App Permissions



- Microsoft 365 Global Admin must Accept the Azure consent flow
- Required by Microsoft for a Certified CVI Provider to use the Media SDK
 - Read domains: needed to look up verified domains
 - Access media streams in a call as an app: service accessing media streams
 - Initiate outgoing 1 to 1 calls from the app: future use for 1:1 calls
 - Initiate outgoing group calls from the app: needed to create call to access media
 - Join group calls and meetings as an app: future use to bypass lobby
 - Join group calls and meetings as a guest: join as a guest
 - Read online meetings details: retrieve join URL from VTC Conf ID

<https://docs.microsoft.com/en-us/microsoftteams/cloud-video-interop>



cory.collaboration@example.onmicrosoft.com

Permissions requested

Accept for your organization

 **Webex Video Integration for MS Teams**
[App info](#)

This application is not published by Microsoft.

This app would like to:

- ✓ Read domains
- ✓ Access media streams in a call as an app
- ✓ Initiate outgoing 1 to 1 calls from the app
- ✓ Initiate outgoing group calls from the app
- ✓ Join group calls and meetings as an app
- ✓ Join group calls and meetings as a guest
- ✓ Read online meeting details

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Automatic Setup Test Succeeds

Video Integration Setup

Microsoft Teams

— We verified the admin permissions required for the integration exist and are valid.

To complete the setup, copy & paste the following commands, which enable the integration for all users in your organization, to Microsoft PowerShell.

To enable or disable the integration for specific users, see the Microsoft documentation on Grant-CsTeamsVideoInteropServicePolicy.

```
New-CsVideoInteropServiceProvider -Name Cisco -TenantKey  
"example@m.webex.com" -InstructionUri  
"https://webex.com/msteams?confid={ConfId}&tenantkey=example&dom  
ain=m.webex.com" -AllowAppGuestJoinsAsAuthenticated $true -  
AadApplicationIds "7968d647-6a0f-4476-8931-206eff6c4d55"
```

```
Grant-CsTeamsVideoInteropServicePolicy-PolicyName Cisco  
ServiceProviderEnabled -Global
```

Once you've run the commands, click Ok.

Ok

<https://docs.microsoft.com/en-us/powershell/module/skype/grant-csteamsvideointeropservicepolicy?view=skype-ps>

What you need to use VIMT (CVI)

Required

- ❑ Webex Org w/ at least one user license

Recommended

- ❑ Sync users and enable for Calendar Service*
 - [Hybrid Directory Service Sync Tool](#) or [Azure AD SCIM API Setup](#)
- ❑ Configure [Hybrid Calendar Service](#) to provide OBTP
 - [How OBTP Works with Cloud-Registered Devices](#)
- ❑ For the best OBTP** experience, Webex Rooms should be registered directly or indirectly to the cloud
 - [Cisco Webex Cloud Registered \(direct\)](#)
 - [Cisco Webex Edge for Devices – Cloud Aware \(indirect\)](#)

*See notes

**On-prem registered Webex Rooms support OBTP for CVI only. Cloud reg/aware will support OBTP for WebRTC as well





Webex Rooms running Microsoft Teams
meeting web app (WebRTC)

Joining Microsoft Teams meetings - WebRTC

One Button to Push experience



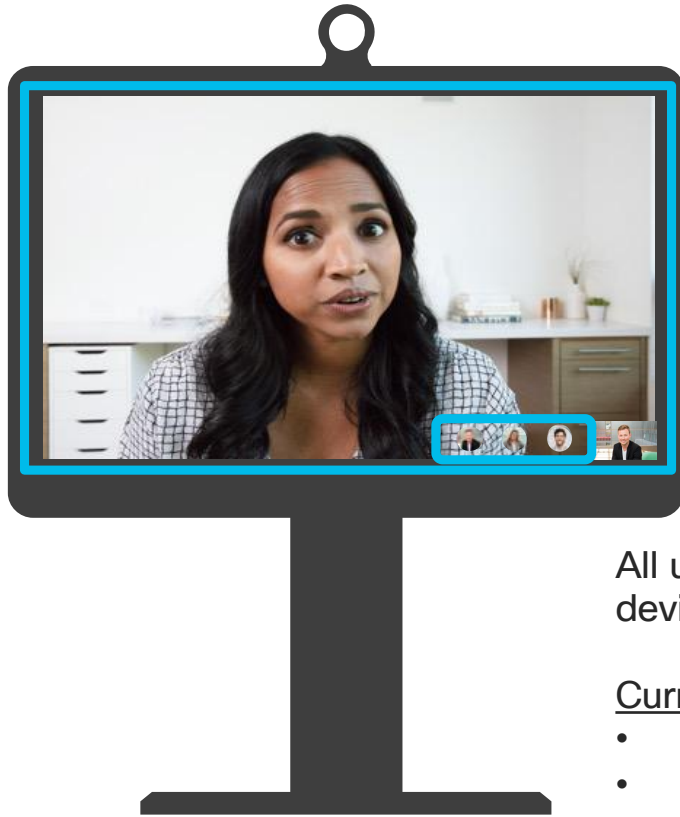
Joining Microsoft Teams meetings– WebRTC Layout example



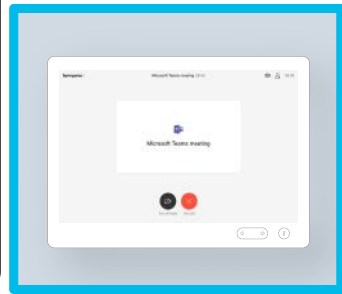
*See notes

Modern web technology – WebRTC

Layouts and UX summary



Video Endpoint Experience



Microsoft Teams Client
User Experience

All users get their native Teams experience from Microsoft, depending on the device/technology/use case

Current implementation of Microsoft Teams (Chromium) web app provides *one layout*:

- **Only the Active Speaker** is shown on video (self-view is always on)
- Other **participants** are displayed as **avatars** at the bottom of the screen
- In-meeting controls will be available via Touch10 (including Webex-style self-view)
- Microsoft Teams client's users get Continuous Presence 2x2

Modern web technology – WebRTC

Layouts and UX summary when content is shared



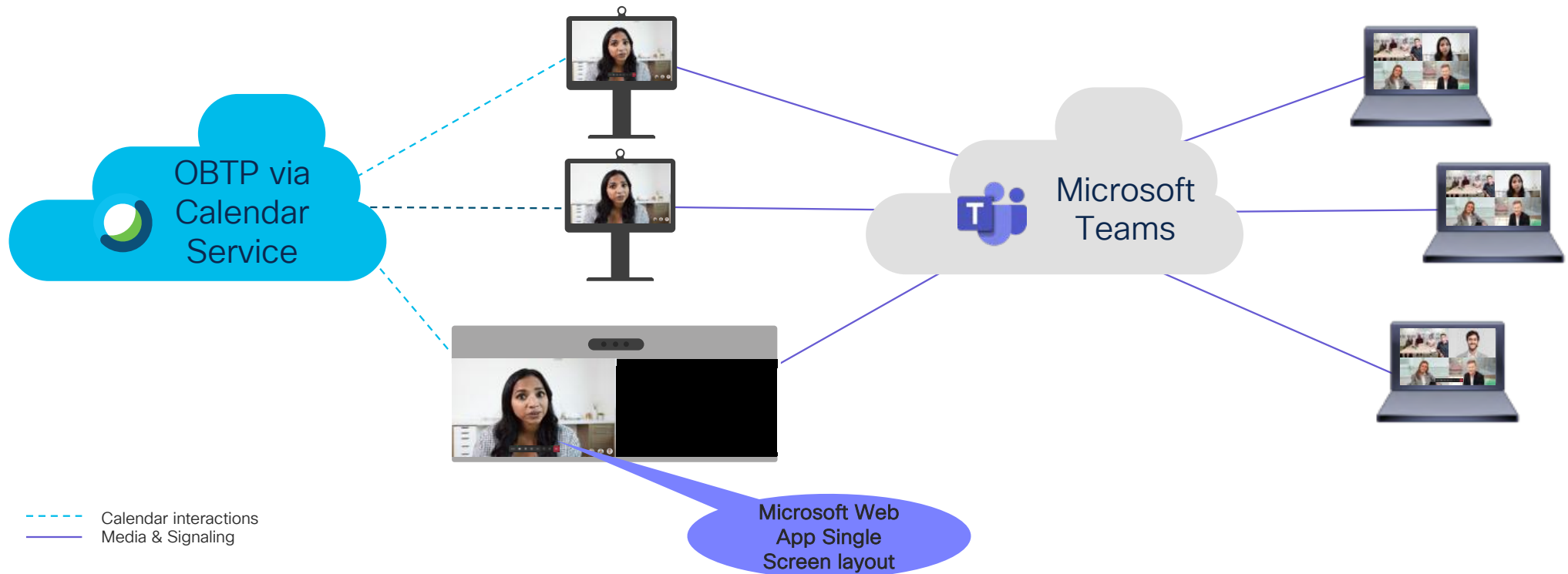
Video Endpoint Experience

- Content sharing replaces Active Speaker's video
- Current active speaker is highlighted in the avatars bar (self-view is always on)

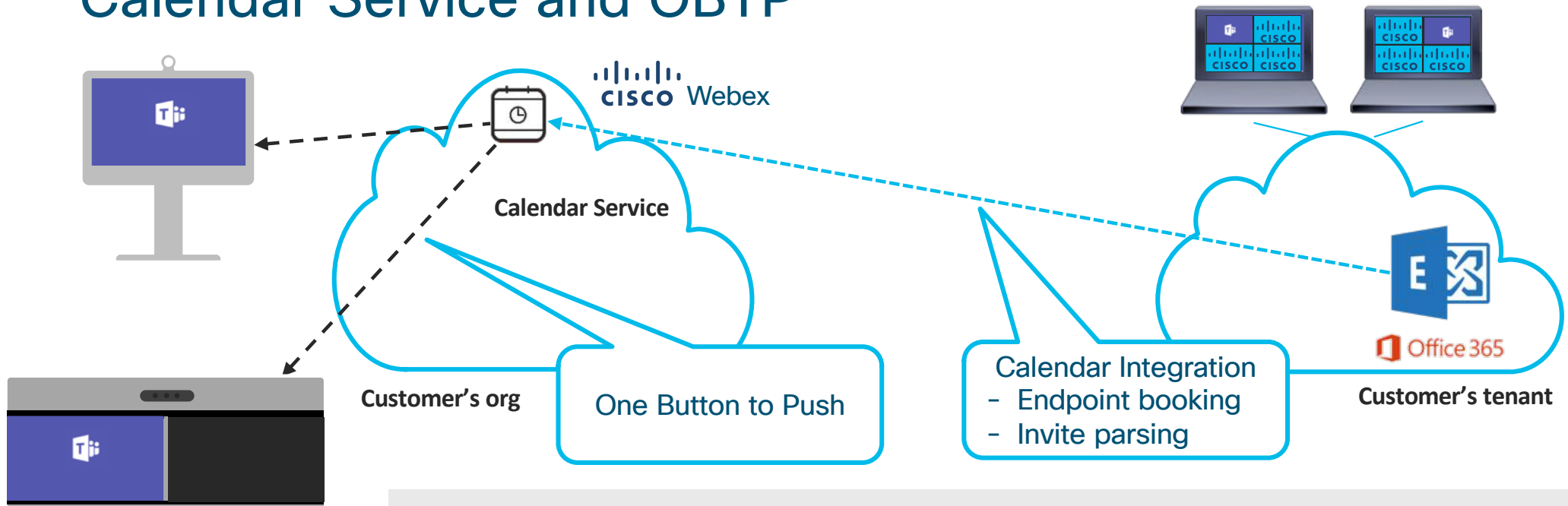
Cisco Webex Rooms for Microsoft Teams meeting

(Enabled via WebRTC)

Room Kits, Room Series, Boards, Desk Pro
(web-engine enabled devices) - devices
must be cloud registered or cloud aware
(Webex Edge for Devices)



Joining Microsoft Teams meetings– WebRTC Calendar Service and OBTP

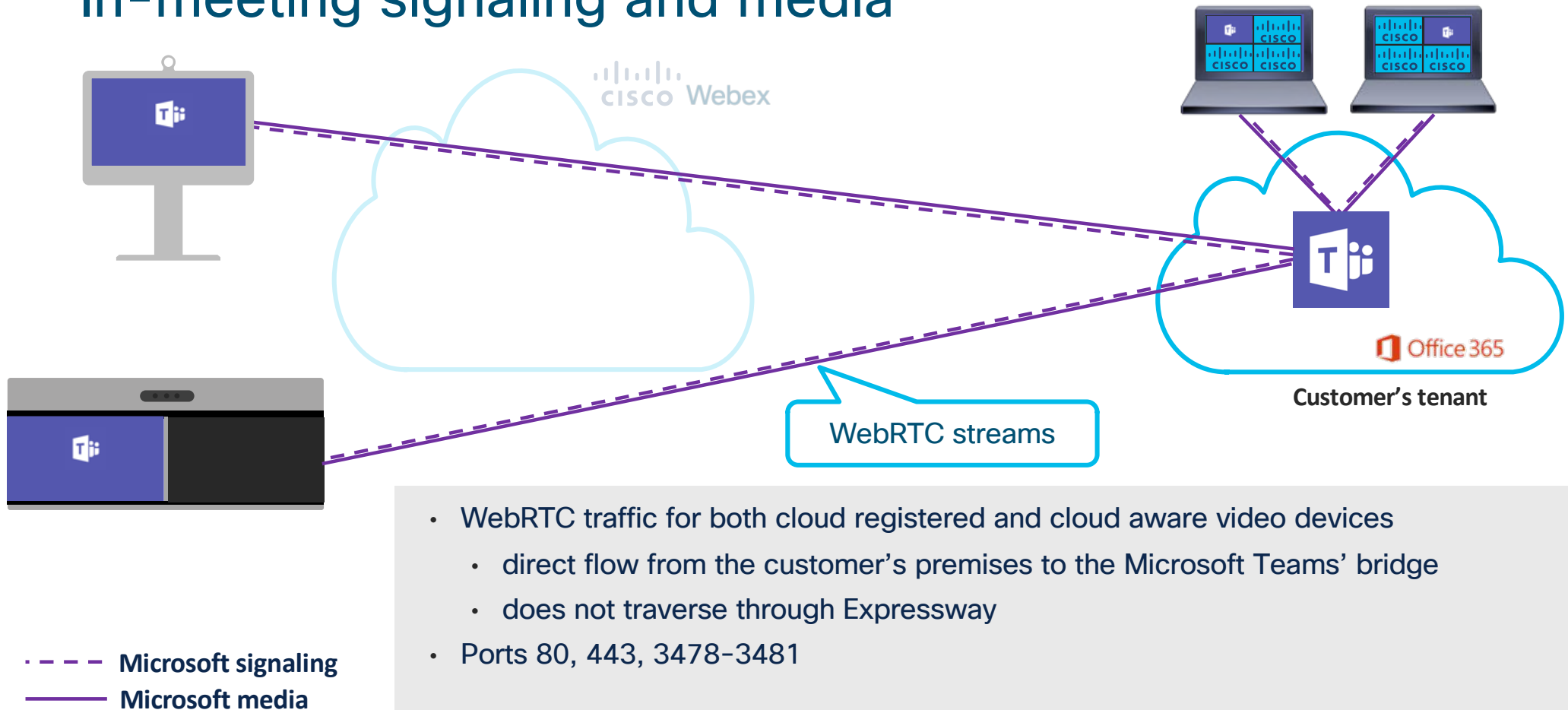


--- OBTP traffic
- - - Graph API

- Enabling **Webex Calendar Service** is required (WebRTC is available only via **OBTP**)
- **OBTP** is supported for both cloud registered and cloud aware (Webex Edge for Devices)
- **Cloud solution** requires no on-premises infrastructure – uses **embedded browser** in endpoint to directly join a Microsoft Teams meeting as a guest

Modern web technology – WebRTC

In-meeting signaling and media



- WebRTC traffic for both cloud registered and cloud aware video devices
 - direct flow from the customer's premises to the Microsoft Teams' bridge
 - does not traverse through Expressway
- Ports 80, 443, 3478-3481

What you need to use VIMT (WebRTC)

Required

- ❑ Webex Org w/ at least one user license or device license
- ❑ Configure [Hybrid Calendar Service](#) to provide OBTP
 - [How OBTP Works with Cloud-Registered Devices](#)
- ❑ Webex Rooms must be registered directly or indirectly to the cloud
 - [Cisco Webex Cloud Registered \(direct\)](#)
 - [Cisco Webex Edge for Devices – Cloud Aware \(indirect\)](#)

Recommended

- ❑ Sync users and enable for Calendar Service*
 - [Hybrid Directory Service Sync Tool](#) or [Azure AD SCIM API Setup](#)

*See notes



A decorative pattern consisting of vertical bars and circles of varying heights and widths, arranged in a grid-like fashion across the top half of the page.

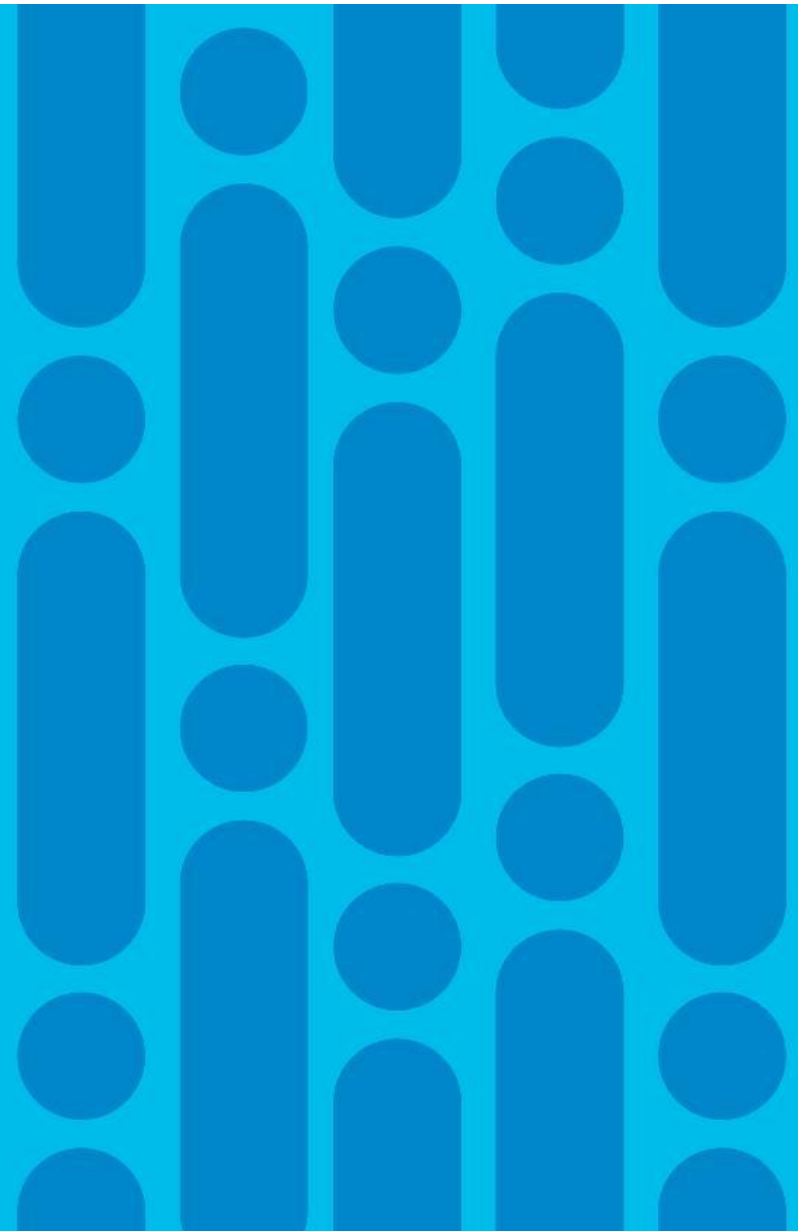
Summary of Meeting Interoperability

Two Methods to join Microsoft Teams meetings

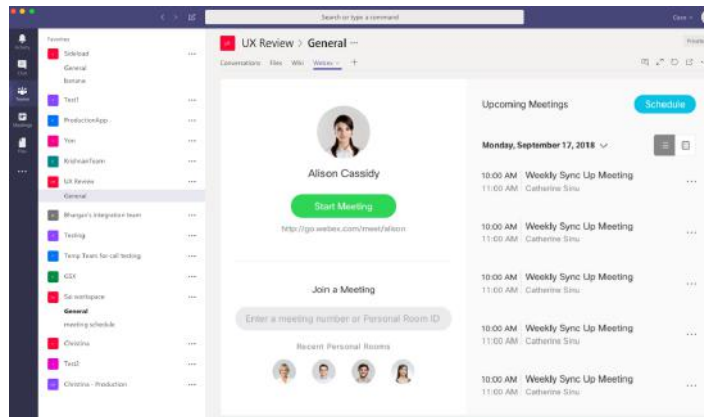
	Cloud Video Gateway (CVI enabled)	WebRTC web app
Intended for	Hosted by my company	Join any other Microsoft Teams meeting
Experience	Cisco Webex experience - multi Screen with flexible layouts Bi-directional content share (using a cable or wireless*)	Microsoft Teams experience - single screen with Microsoft Teams layout Ability to receive share only (Microsoft Teams layout)
Roster	Full roster list	Roster list with touch screen only (Webex Board & Desk Pro)
Devices supported	Cisco and any SIP-capable video devices Cloud and on-premises registered devices	Room Kits, Room Series, Boards, Desk Pro (web-engine enabled devices) - devices must be cloud registered or cloud aware
Join Experience	OBTP join with Calendar Service, direct dial in, or IVR join experience	OBTP join with Calendar Service for B2B meetings
Licensing	Add on license required	Webex Room registration (included in Flex)

*Requires on prem registration (or cloud aware)

Cisco plugins for MS Teams



Microsoft Teams customer joining Webex Meetings



Webex Meetings customers who also happen to have Microsoft Teams (e.g. for messaging or file sharing)



Webex Meetings is available today inside Microsoft Teams for seamless scheduling & join

Webex customers who might invite someone in another org that uses a Microsoft Teams Rooms system



They can also seamlessly join your Webex Meeting



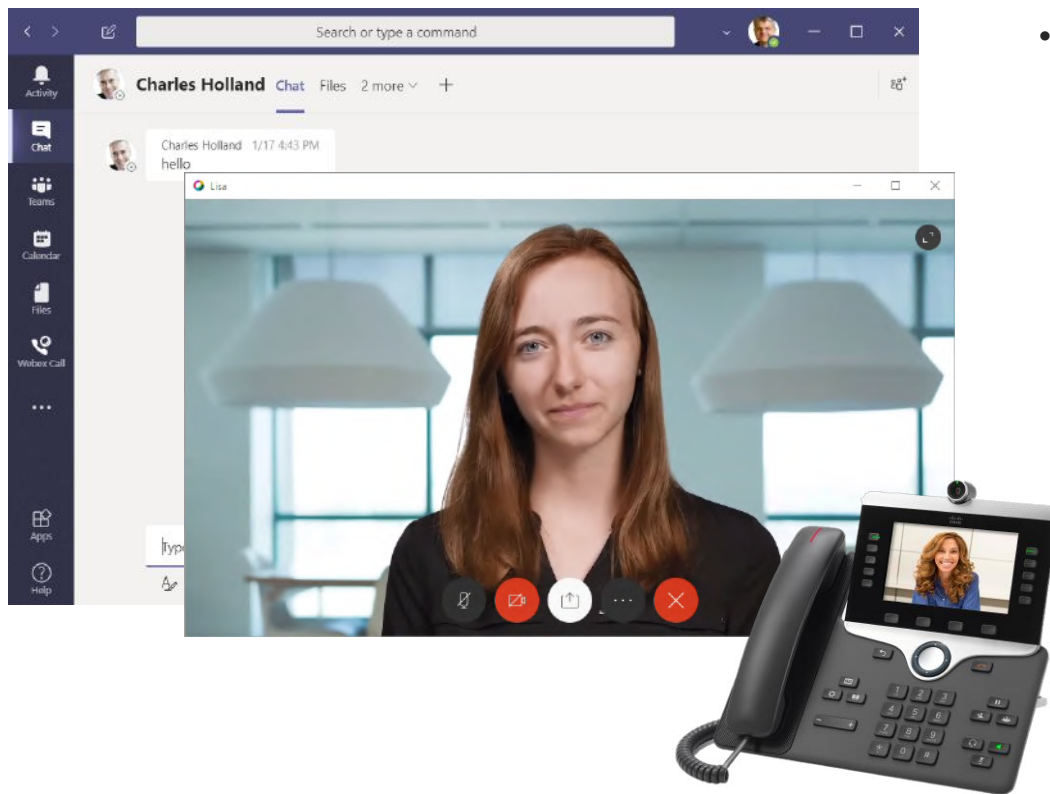
Webex Meetings advantages

Not available in Microsoft Teams meetings

- Market Leader in video conferencing
- **Wireless content sharing from any device**
- **Multi-stream with additional layout options**
- In-meeting Webex Assistant
- Companion Mode
- **Face recognition / name labels**
- People Insights
- Room panorama
- **Localized media via Video Mesh**



Introducing Cisco Calling Integrations for Microsoft Teams



- The simple way to integrate Microsoft Teams Messaging and Cisco Calling.
 - Uses your existing Cisco calling infrastructure
 - Click to call with your existing Cisco phones from Microsoft Teams
 - Use Cisco soft clients for video calls
 - No compromise on calling features
 - No dial plan or routing reconfiguration required
 - No additional license costs

Client based integration

- Simple to deploy Client side integration which works with your existing Cisco Calling Apps
- Client side means NO changes to Infrastructure or configuration
- Works with a choice of Cisco clients



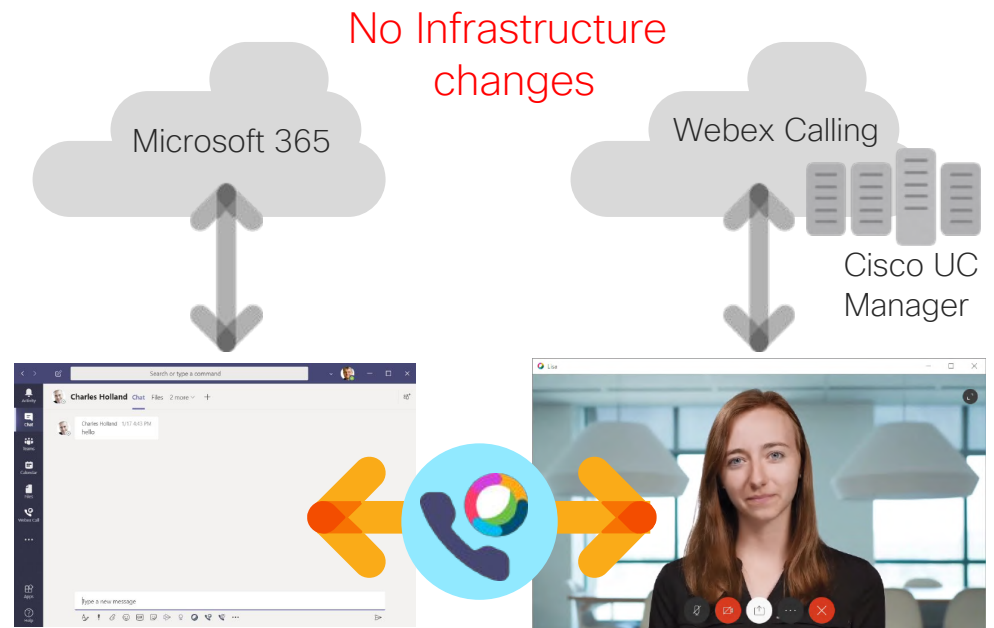
WebexTeams



Cisco Jabber



UC-One



Cisco Calling App added to MS Teams Client

Cisco calling with MS contact search

Call/Search Input
Enter a number, SIP address or type a name to search for a Azure AD/Outlook contact

Dial Tab
Access dialpad, contact search and speed dials

Contact Search
Search for personal and corporate contacts
Azure AD Contacts
Outlook 365 Contacts

Dialpad
Click digits to key in numeric dial destination

Call Button
Dial a number or SIP address

Add Speed dial
Click to add up to 25 speed dial cards

Speed dial
Pin frequent contacts as speed dials for easy access.

Call
Select number and call contact

Reorder
Drag and drop cards to organize them

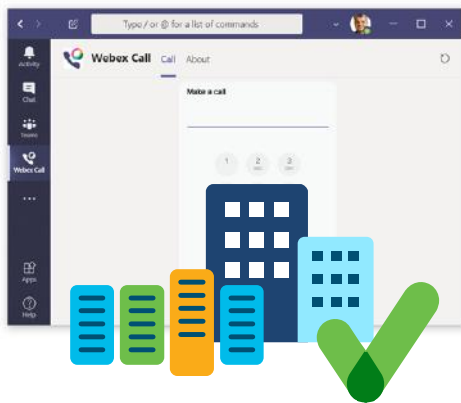
Delete
hover over the card and click delete icon to remove speed dial

Integration provides Flexible Work Styles

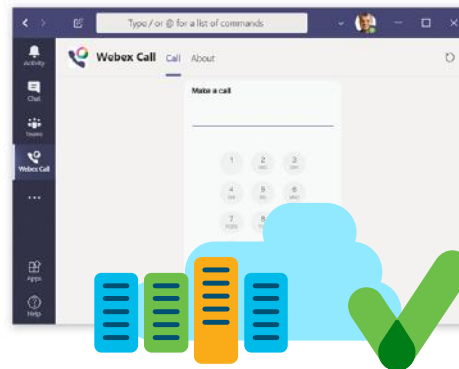


- Cisco Calling integrations support both Desk phone control and Soft phone calling
- No compromise on calling features and functionality including contact centre support
- Call your existing room video systems
- Work remotely using Cisco Expressway and Mobile Remote Access

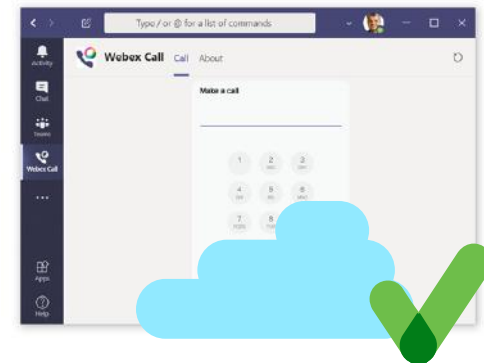
Choice of Calling Platforms



On Premise
UC Manager



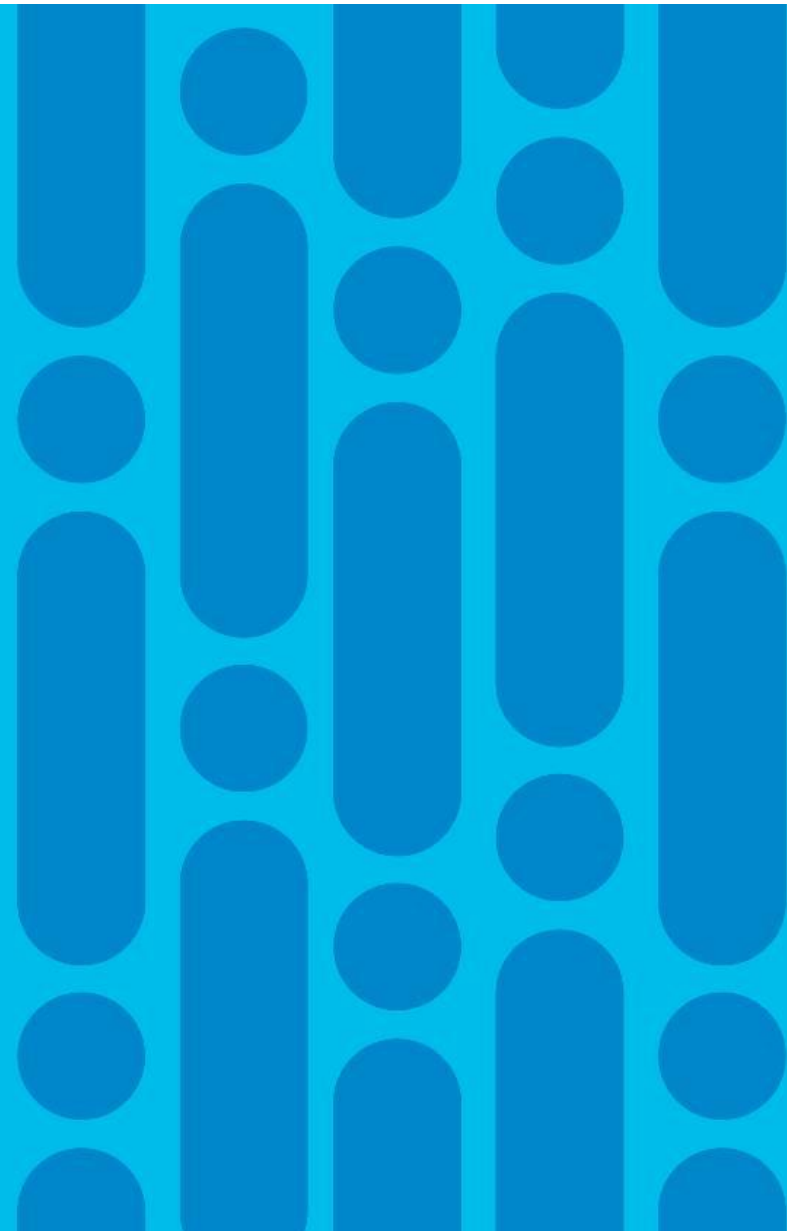
Hosted Platforms
HCS



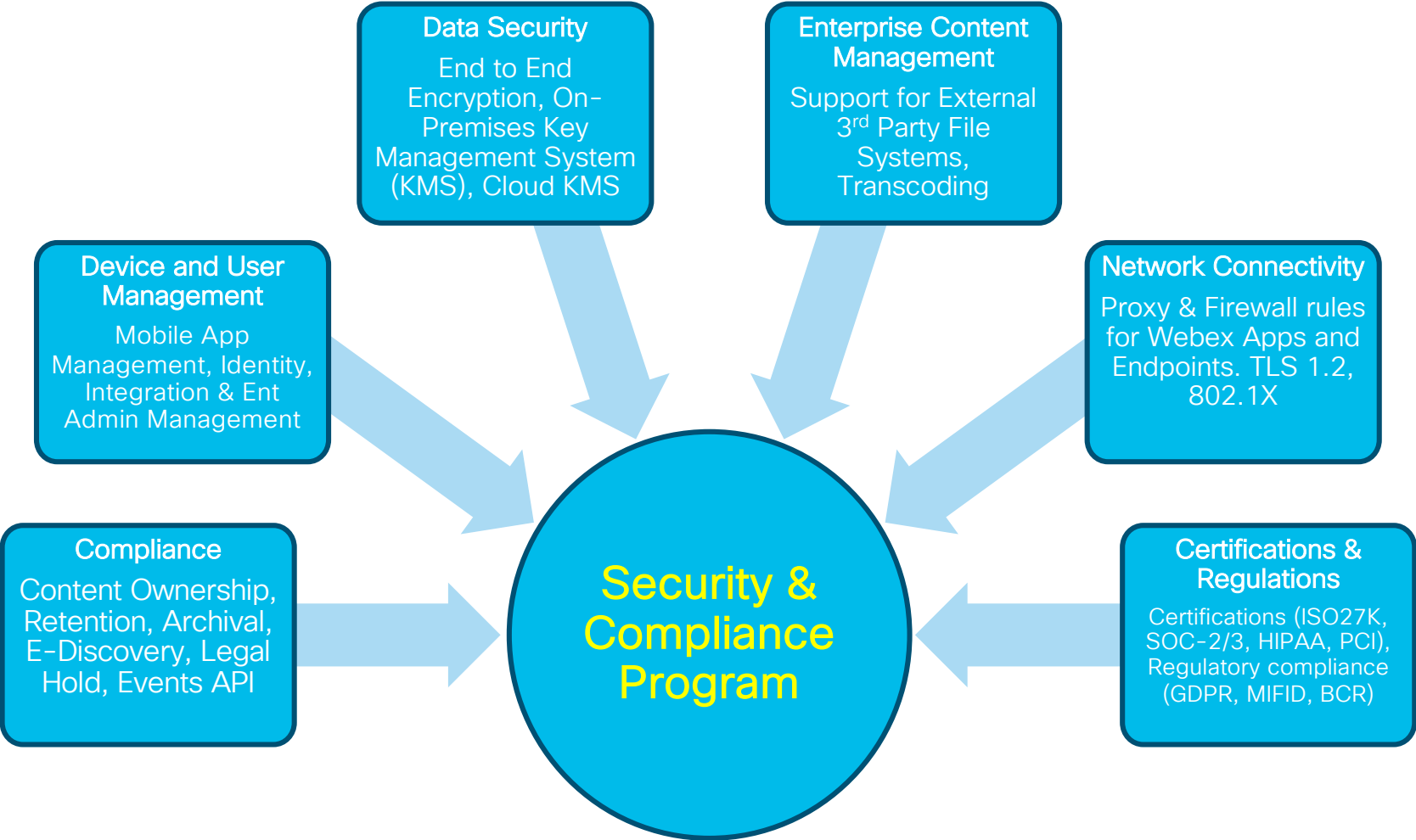
Cloud Platforms
Webex Calling, UCM
Cloud, BroadCloud

- Integration can be used with a choice of Cisco calling platforms
- Allows migration to cloud calling when ready

Webex Teams Security



Webex Teams Security and Compliance Initiative





Compliance & DLP

Webex Teams : Legal Hold

What:

- Compliance admins can add exceptions to retention policies during investigations.
- Features available:
 - Create a matter and put custodians (users) on legal hold
 - View and download matters
 - Release matters

Why:

- When employees are investigated, their content will be preserved and not purged by the org-wide retention policy

The screenshot shows the 'Create Matter' form in the eDiscovery Search and Extraction interface. The form is titled 'Create Matter' and has a close button (X) in the top right corner. It contains the following fields and options:

- Matter Name:** A text input field containing 'Classified Info NDA Leak'.
- Description (Optional):** A text area containing 'Employees have shared information publically without permission'.
- Add Custodians:** A text input field containing 'C:/ImportCustodiansList.csv' and a 'Browse...' button.
- Download CSV Template:** A link below the custodian field.
- Buttons:** 'Cancel' and 'Create' buttons at the bottom right.

The background shows a sidebar with 'All Matters 3' and 'My Matters' tabs, and a table with columns for 'Matter Name', 'Date Released', and 'Date Released'. The 'Date Released' column shows 'Feb 14, 2018 9:05 AM'.

The screenshot shows the 'All Matters' table in the eDiscovery Search and Extraction interface. The table has the following columns: Matter Name, Date Created, Created By, Description, Custodians, and Date Released. The table contains three rows of data:

Matter Name	Date Created	Created By	Description	Custodians	Date Released
Agents NDA Contract	Feb 14, 2018 9:05 AM	Nick Fury	Improper use of contract	5	Feb 14, 2018 9:05 AM
Headquarters Security Breach	Feb 13, 2018 10:15 AM	Nick Fury	Employees gained access to...	50	
Sokolov Accords Contract	Feb 12, 2018 5:03 PM	Phil Coulson	Break of contract agreement	14	

File Sharing Control

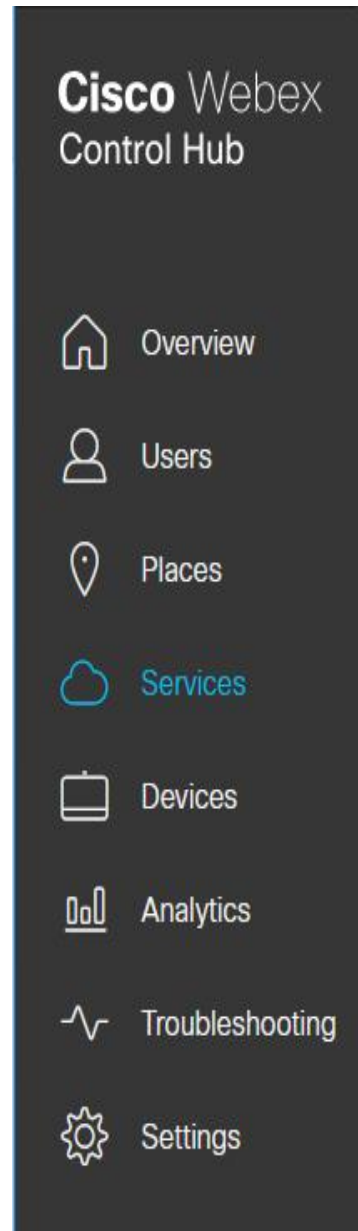
- Allows Webex Teams customers to control file downloads and uploads on specific client types : Desktop/ Web/ Mobile/ Bots
- Additional option to enable/disable restrictions on whiteboard and annotations.
- User warning if file share attempted

Addresses :

- Data Loss concerns
- Malware concerns

Provides :

- Mobile Application Management controls on Bring Your Own Devices



< Message

Collaboration Restrictions

Restrict what your users can share in the app.

Preview and download files

No Restrictions

- Mac and Windows app
- iOS and Android app
- teams.webex.com
- Bots

Upload files

No Restrictions

- Mac and Windows app
- iOS and Android app
- teams.webex.com
- Bots

Whiteboard and Annotations



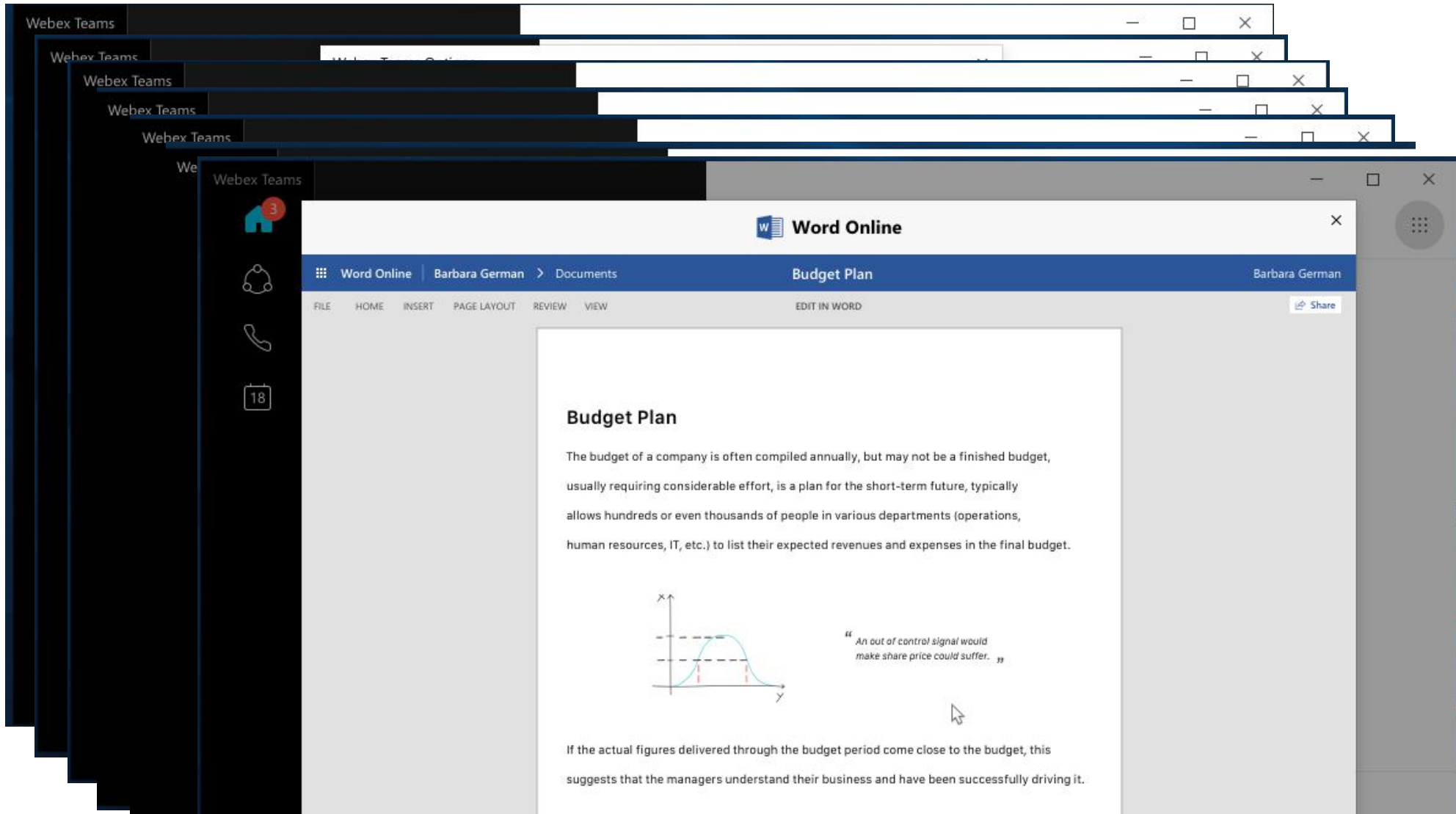
Webex Teams : Enterprise Content Management

Allows customers to replace Webex Teams File storage with their own content management system, through an optimised integration or a custom API



Microsoft OneDrive, SharePoint Online, Google Drive support today, others soon.....

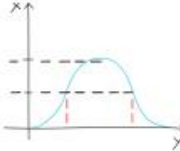
ECM: Share, Upload, View, Co-Edit File



The image shows a desktop environment with several overlapping Webex Teams windows. The foreground window displays a Microsoft Word Online document titled "Budget Plan" by Barbara German. The document content includes:

Budget Plan

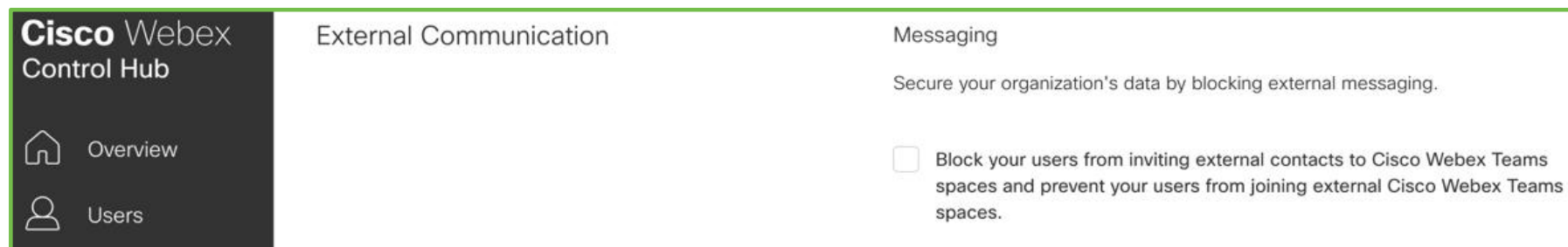
The budget of a company is often compiled annually, but may not be a finished budget, usually requiring considerable effort, is a plan for the short-term future, typically allows hundreds or even thousands of people in various departments (operations, human resources, IT, etc.) to list their expected revenues and expenses in the final budget.



“ An out of control signal would make share price could suffer. ”

If the actual figures delivered through the budget period come close to the budget, this suggests that the managers understand their business and have been successfully driving it.

Webex Teams : Blocking External Communication



What: Provide administrator with controls to prevent external communication

- Users within the org cannot add users outside the org in spaces owned by the org
- Users within the org will not be able to join external spaces
- Meetings are still allowed

Why: Need to control Webex Teams usage

- Mitigate data loss (accidental or intentional)
- Regulatory implications of external comms

Block External Communications (BEC) : Allowed domains

What:

- Admin can configure a list of allowed external domains in Control Hub
- Previously open communication channels (for messages and content) will be blocked.

Why:

- To prevent data loss, for enterprises that would like to control communication paths outside their organization

Block external messaging

Secure your organization's data by blocking external messaging.

This blocks your users from inviting external contacts to Cisco Webex Teams messaging spaces and prevents your users from joining external spaces.

Whitelist domains for external messaging

Type to search for specific domains. Add domain names by separating with commas or import from a CSV file.

Add domain

Enter Domain Name

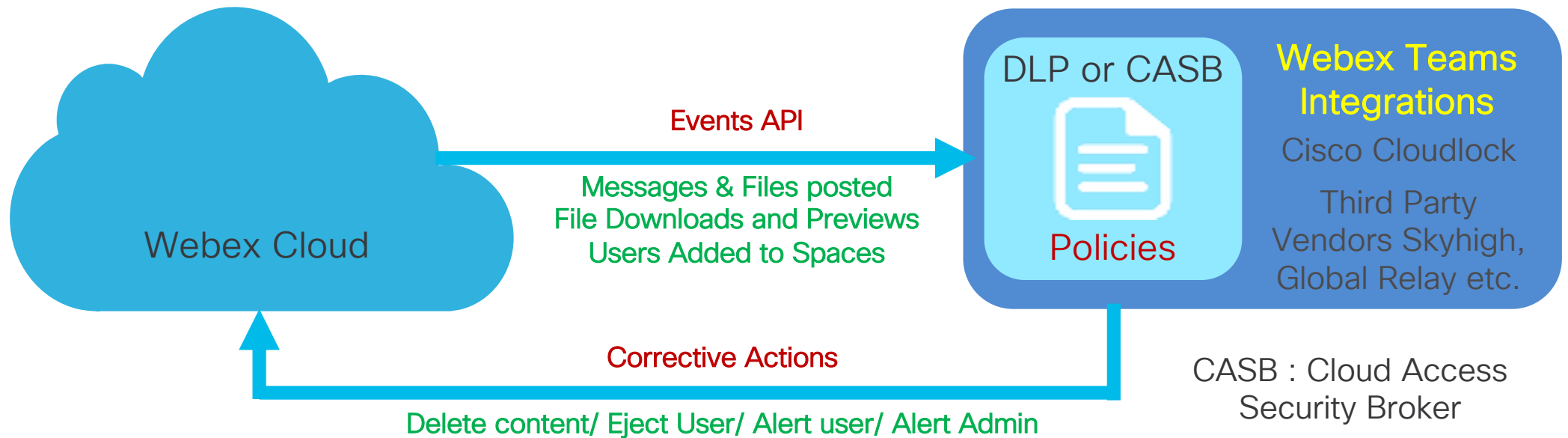
e.g. xyz.com, cisco.com

abscissa.com	● verified in Teams	⋮
boxborough.com	● claimed in Teams	⋮
cisco.com	● verified in Teams	⋮
delft.com	● claimed in Teams	⋮
enigma.com	● claimed in Teams	⋮

Data Loss Prevention (DLP) : Monitor and React

Webex Teams Events API enables polling for Events and Content generated by users

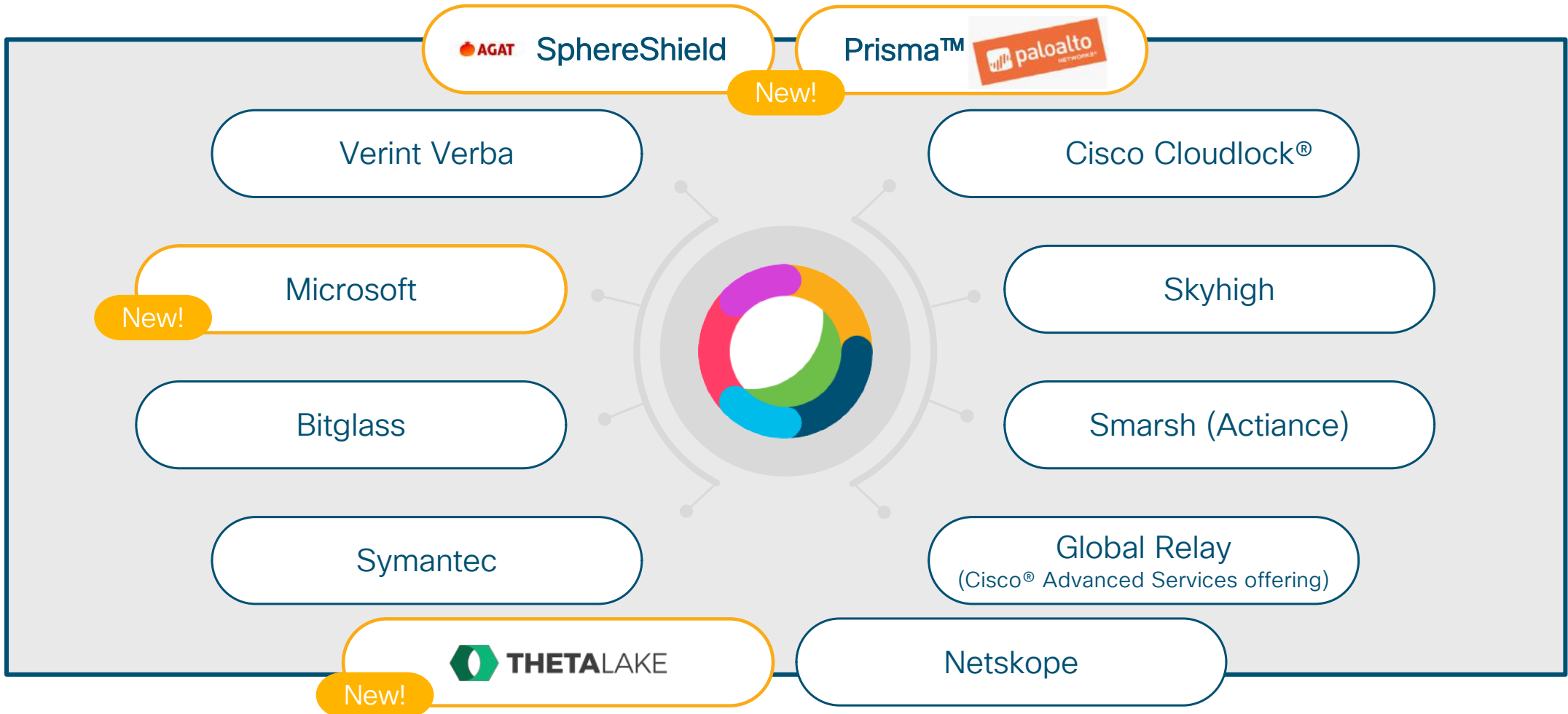
Allows organisations to monitor and correct user behaviour (e.g. Delete Content, Alert User, Alert Administrator), preventing the loss of sensitive data



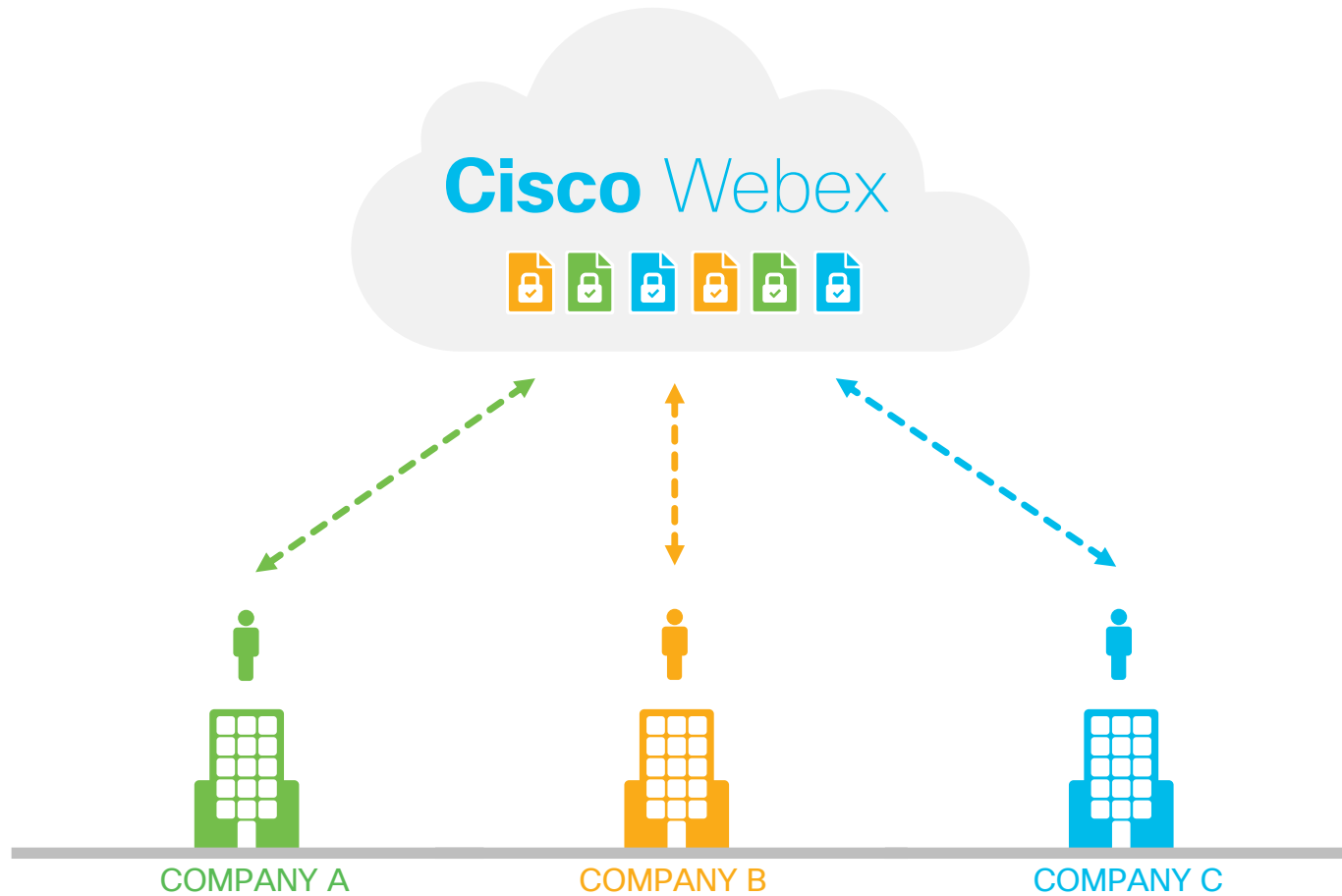
<https://learn-umbrella.cisco.com/datasheets/ds-cisco-cloudlock-for-webex-teams>

Webex Teams Integrations

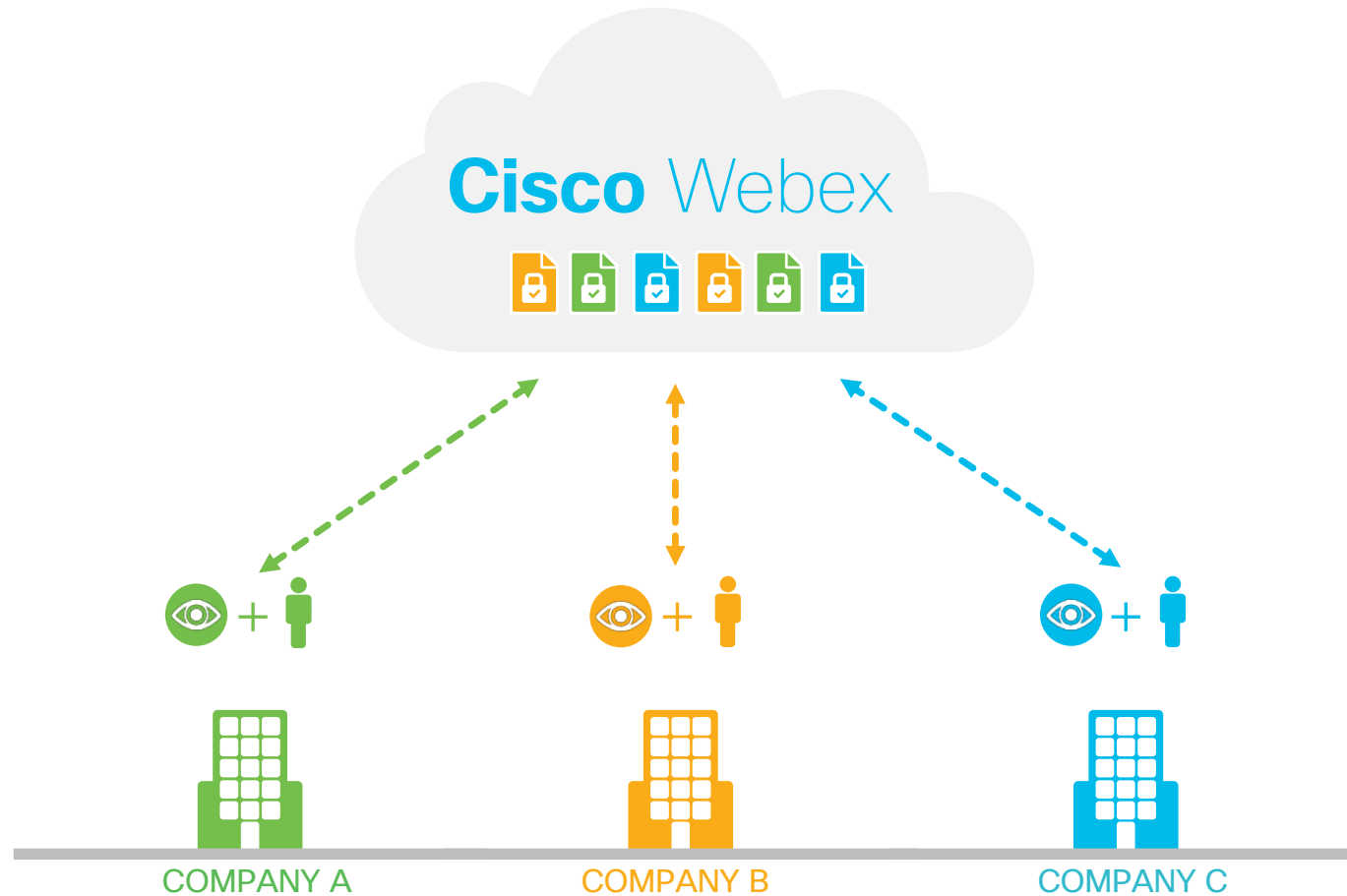
Compliance: Data Loss Prevention & Archival



Cisco Webex: 1 account



Cisco Webex promotes security and access



Cisco Webex DLP: Monitoring user activity



Hey, what's the latest on your upcoming
"Project Titan" launch we talked about at
lunch?

Message has been removed due to
policy violation

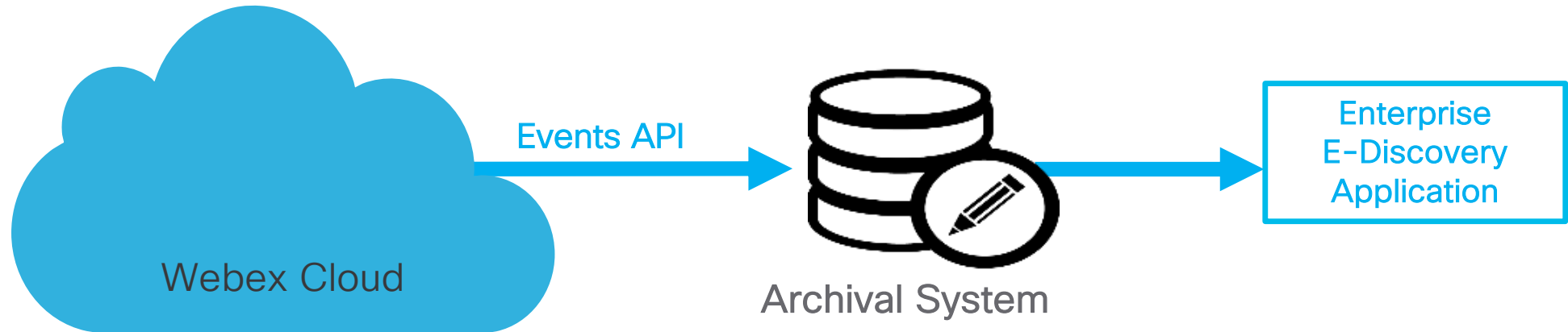


Compliance Rules:
"Project Titan" with
external users

Data Loss Prevention : Feature support

	Cisco Cloudlock	Symantec	SkyHigh	Netskope	Bitglass	Verint Verba	Palo Alto Aperture
Monitor Messages	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Monitor Files	Yes	Yes	Yes	Yes	Yes	No	Yes
Alerts on violations	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deletion of offending Messages	Yes	Future	Yes	Yes	Yes	Yes	Yes
Deletion of offending Files	Yes	Future	Yes	Yes	Yes	No	Yes
Malware detection/removal	No	Yes (Detection)	Future	Future	Yes	No	Yes
Configure policy per space or group	Yes (User, Space)	Yes (User, Space, Team)	Yes (AD groups)	Yes	Yes	Yes	No (future)

How can you archive Webex Teams data?



Use Cases

- Sophisticated eDiscovery
- Legal Hold
- Retention policies based on groups

Options

- **Out-of-the-box Solution** : Integrations with Archival partners e.g. Actiance
- **Custom Solution** : Cisco Advanced Services software & services e.g. Global Relay
- **DIY** : Use Systems Integrator or self integrate Events API with Archival software

Archival Vendors : Feature support

	Actiance	Global Relay	Verint Verba
Archive Messages	Yes	Yes	Yes
Archive Files	Yes	Yes	Yes
Integrate with eVaults	Veritas, HP, IBM	N/A	Yes
On-premise vs Cloud	On-Prem, Cloud, Hybrid	Yes	On-premise
Native-integration vs Services engagement	Native-integration	Cisco AS engagement	Native-integration

A decorative pattern consisting of vertical bars and circles of varying heights and widths, arranged in a grid-like fashion across the top half of the slide.

Anti-malware – Security pack

Built-in Anti-Malware Protection powered by Cisco Talos ClamAV

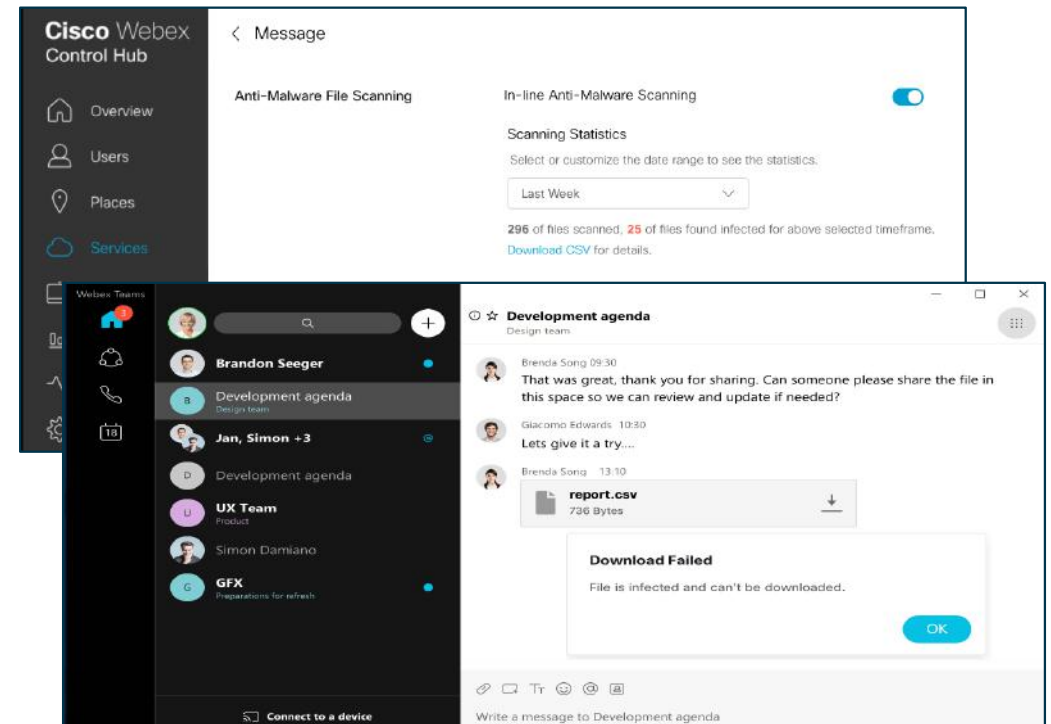
New!

What?

- In-line Anti-virus and malware scanning of files and blocking infected files
- Malware and phishing scanning of URLs and blocking unsafe URLs
- Administrator control to turn-off and turn-on scanning
- Administrator visibility into Scan history
- *Part of Extended Security Pack*

Why?

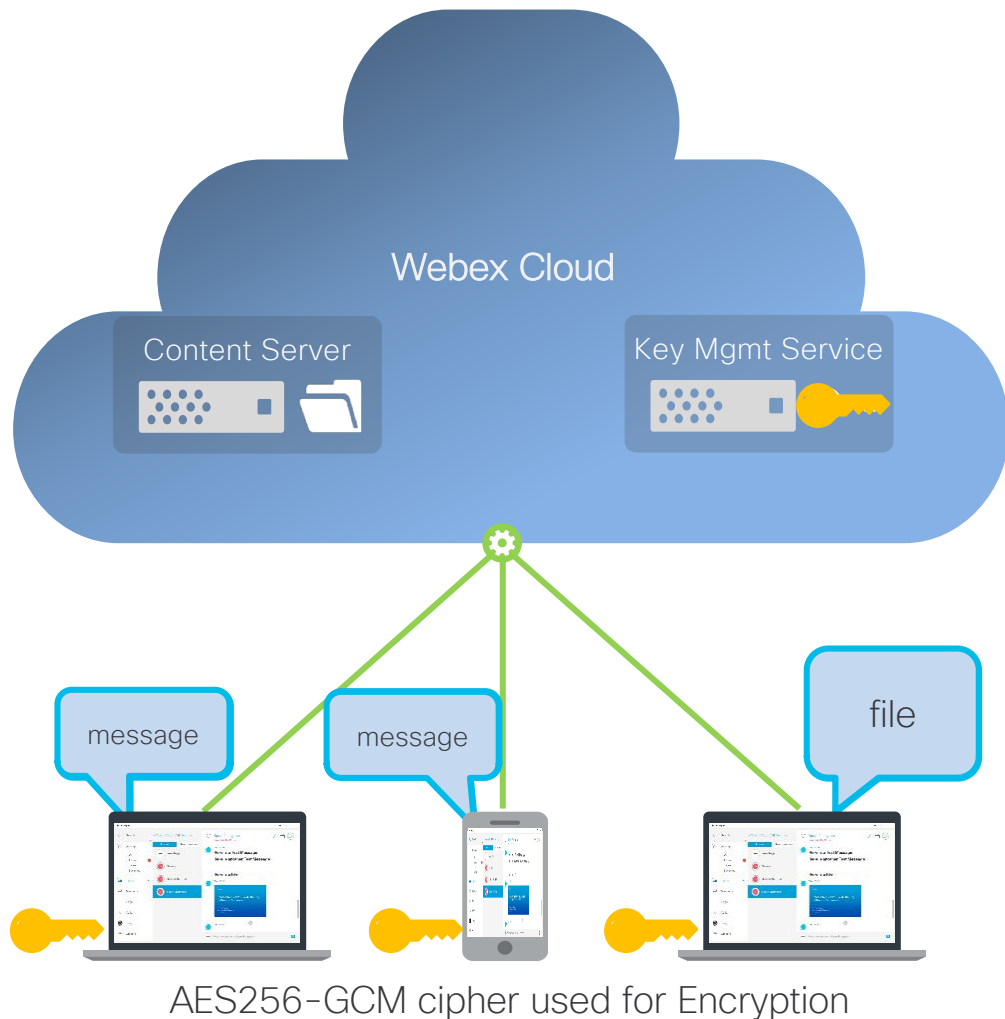
- Protect users by scanning files and URLs for virus, malware and phishing threats
- Reduce data loss risk



A decorative pattern consisting of vertical bars and circles of varying heights and widths, arranged in a grid-like fashion across the top half of the slide.

Hybrid Data Security

Webex Teams- Encrypting Messages and Content



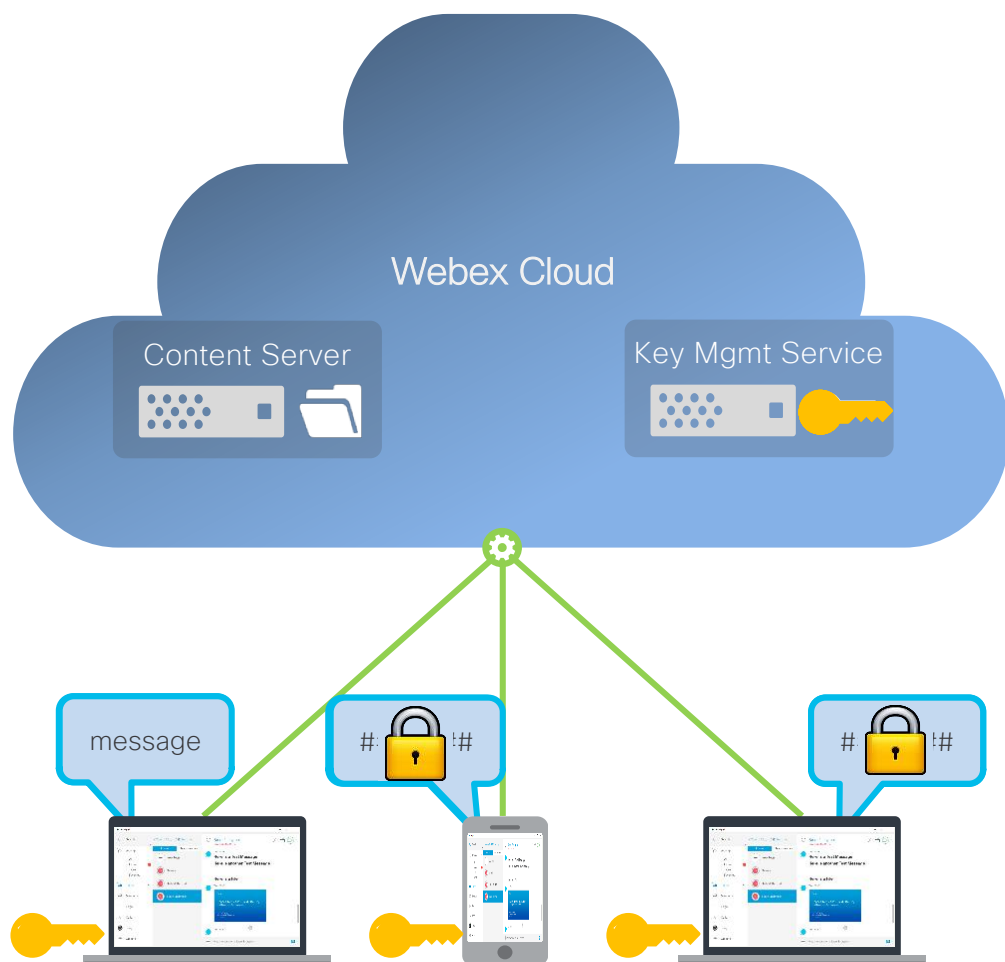
Key Management Service

Any messages or files sent by an App are encrypted before being sent to the Webex Cloud

Webex Teams App requests a conversation encryption key from the Key Management Service

Each Webex Teams Space uses a different Conversation Encryption key

Webex Teams - Decrypting Messages and Content



AES256-GCM cipher used for Encryption

Key Management Service

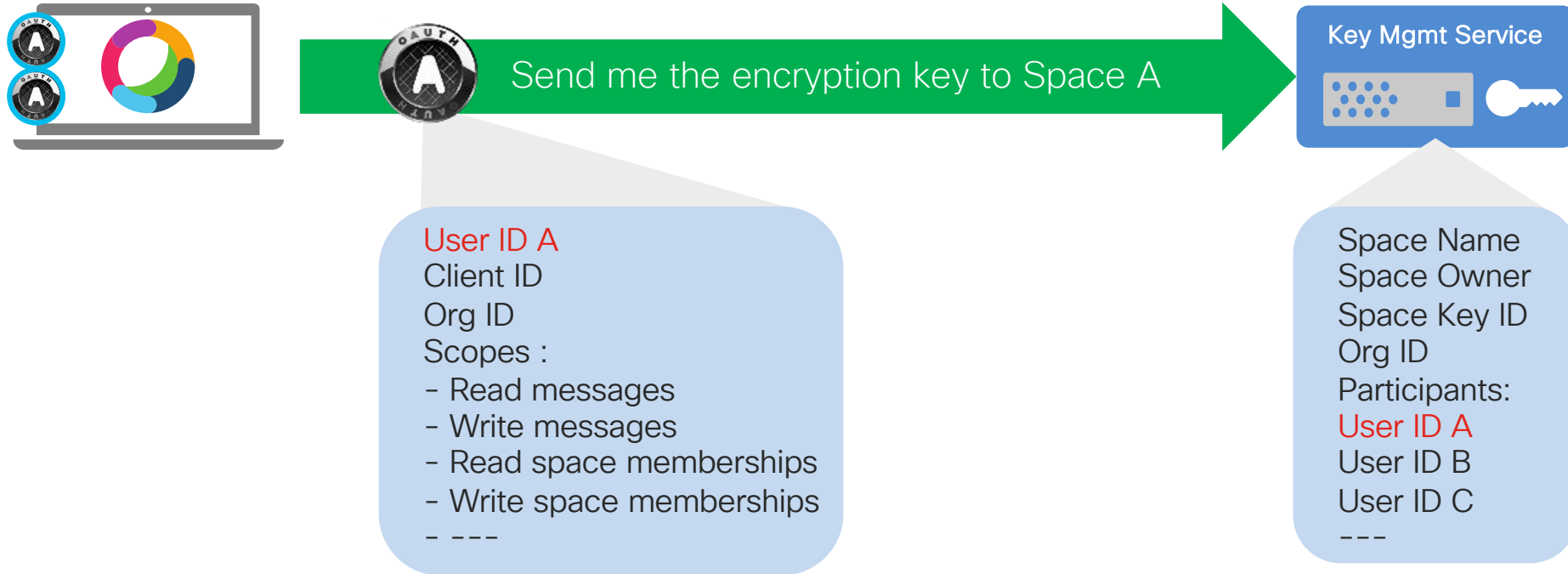


Encrypted messages sent by the App are stored in the Webex Cloud and also sent on to every other App in the Webex Teams Space

Each encrypted message also contains a link to the conversation encryption key

If needed, Webex Teams Apps can retrieve encryption keys from the Key Management Service

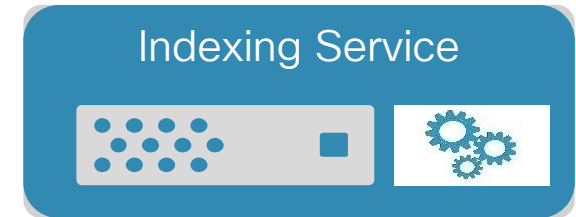
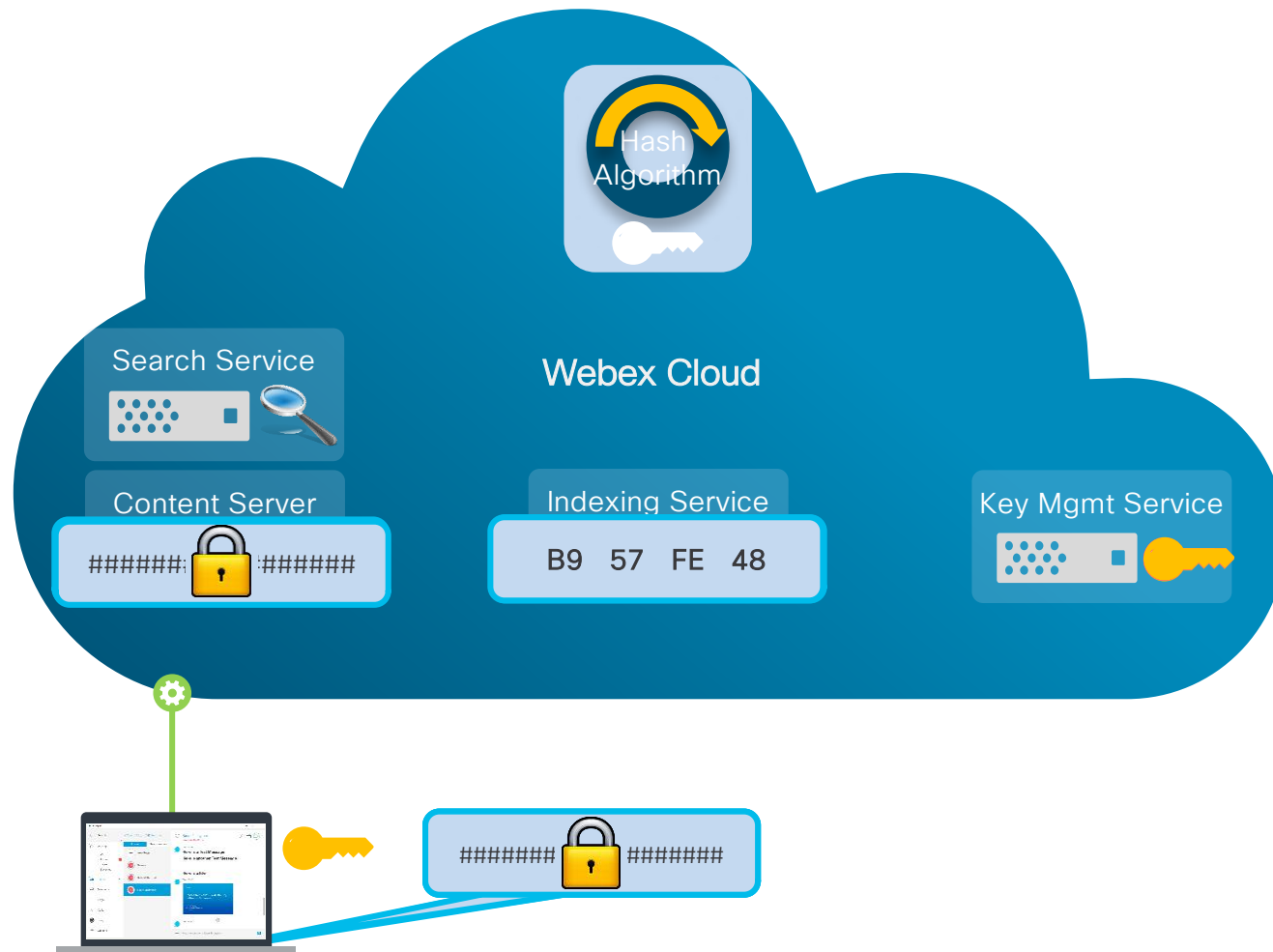
Webex Teams : Access Tokens and controlled access to User Generated Content



To gain access to any Webex Teams space and to read the content associated with that space, a user must first request the encryption key for that space using the KMS Access Token for their organization

KMS Resource Object (KRO)
A data structure that is used to track the encryption key for a space and the people that are authorized to receive the key

Searching Webex Teams Spaces: Building a Search Index



The Indexing Service :
Enables users to search for names and words in the encrypted messages stored in the Content Server without decrypting content

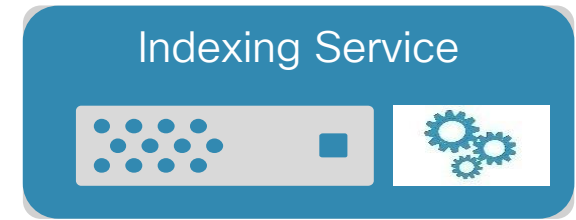
A Search Index is built by creating a fixed length hash* of each word in each message within a Space

The hashed indexes for each Webex Teams Space are stored by the Content Service

*A new (SHA-256 HMAC) hashing key (Search Key) is used for each space

Webex Teams spaces : Querying a Search Index

Search for the word "Webex"



App sends search request over a secure connection to the Indexing Service

The Indexing Service uses per space search keys to hash the search terms

The Search Service searches the for a match in the hash tables and returns matching content to the App

*

*A link to Conversation Encryption Key is sent with encrypted message

Webex Teams Platform Security

Hybrid Data Security

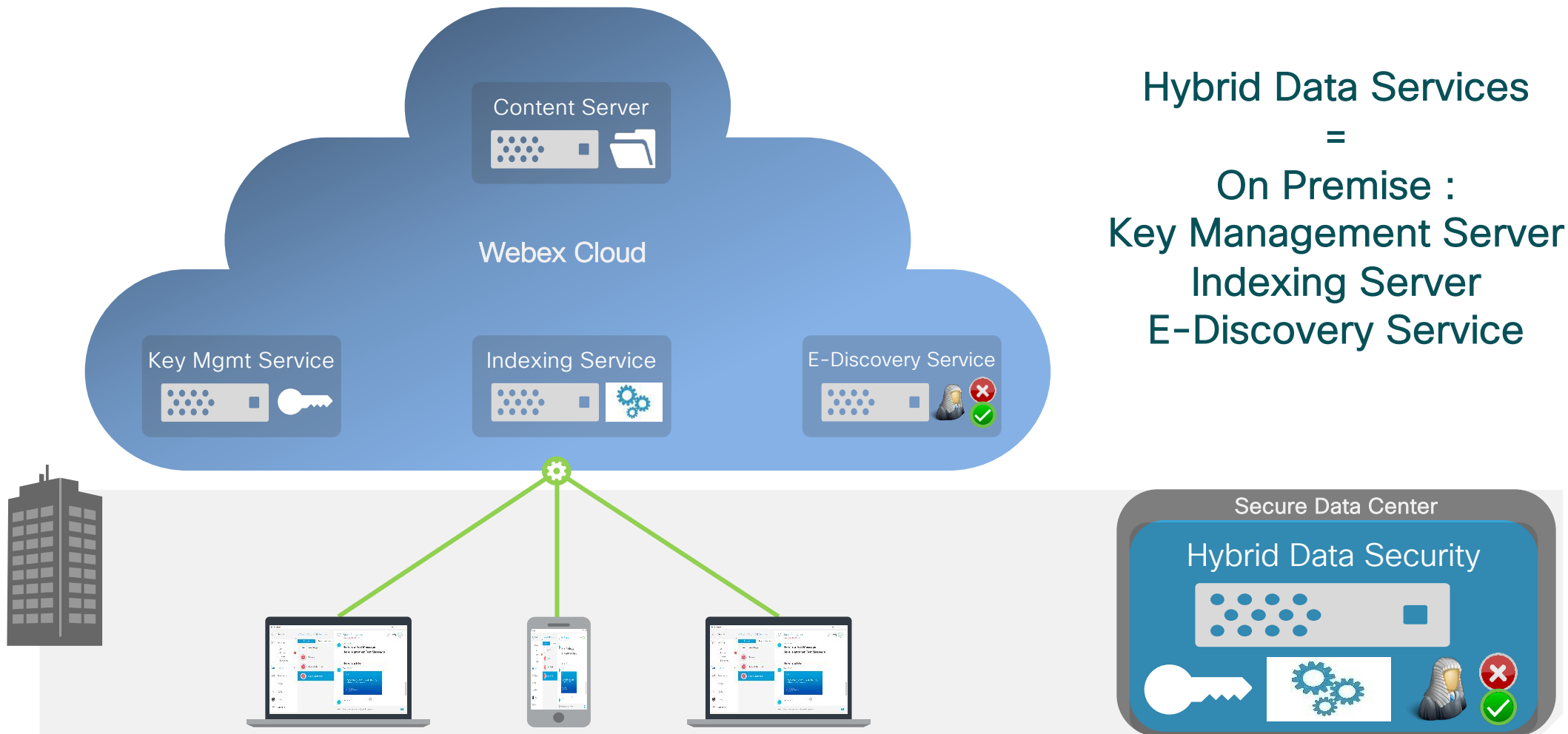
On Premises :

- Encryption Key Management
- Encryption Key Storage
- Content Indexing Service
- eDiscovery Service



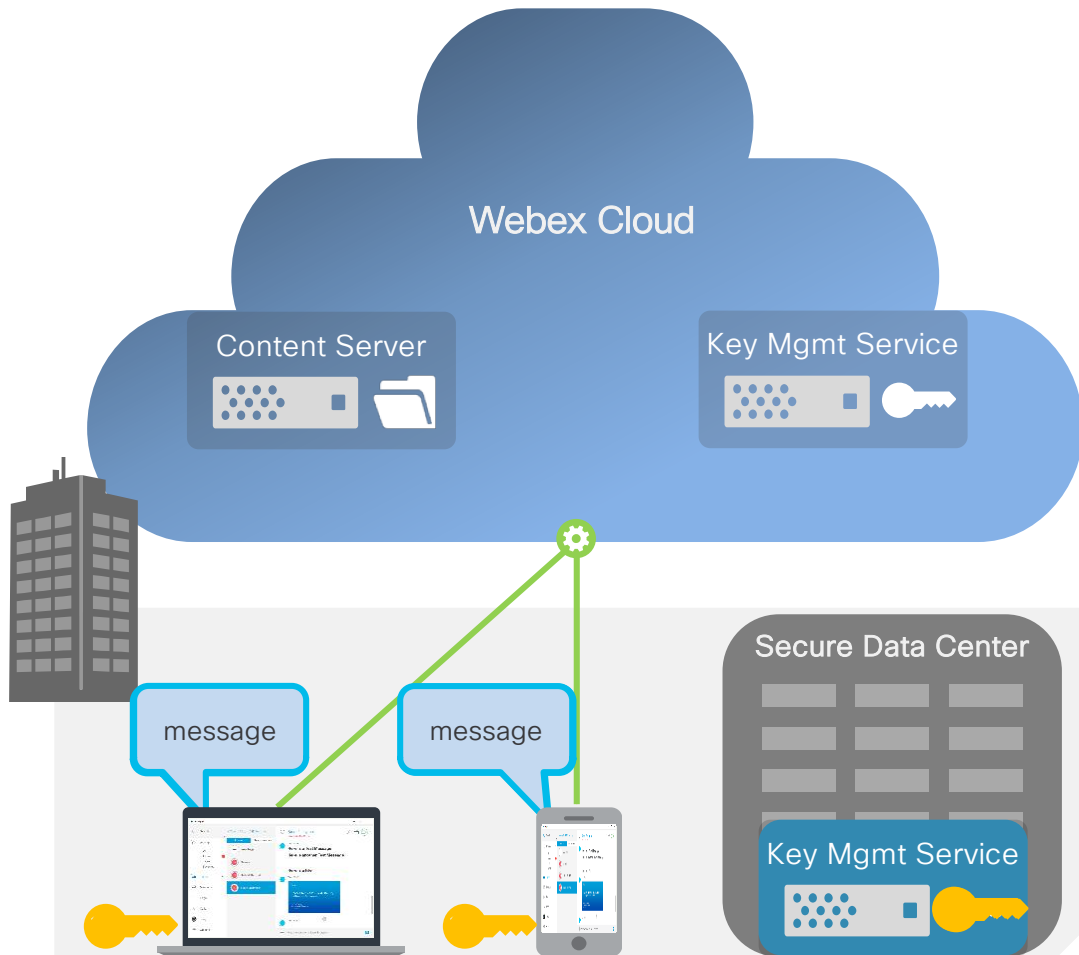
You make security **possible**

Webex Teams – Hybrid Data Security (HDS)



Hybrid Data Services
=
On Premise :
Key Management Server
Indexing Server
E-Discovery Service

HDS - Encrypting Messages & Content



Key Management Service



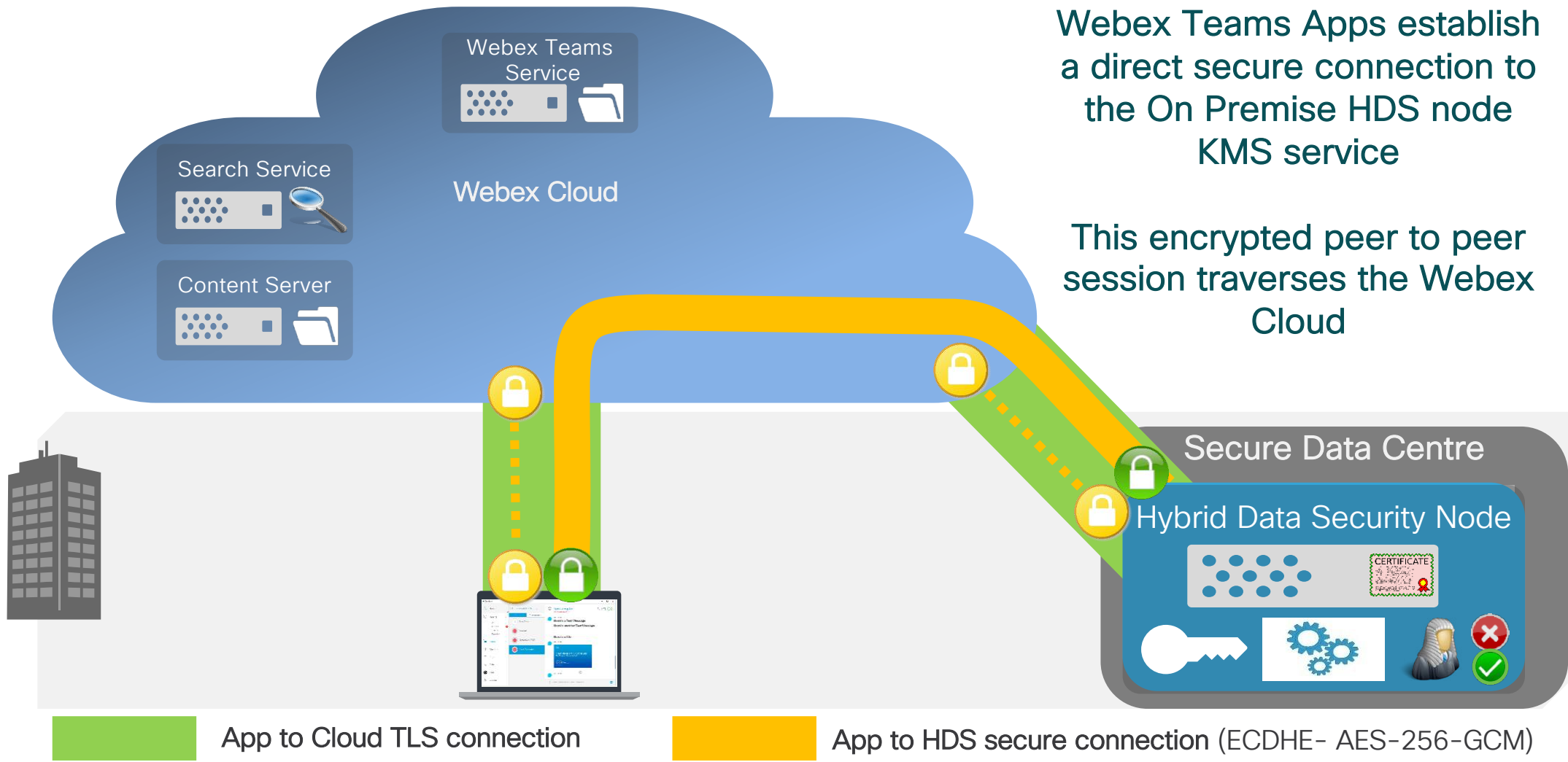
Webex Teams Apps request an encryption key from the **HDS** Key Management Server

Any messages or files sent by an App are encrypted before being sent to the Webex Cloud

Encrypted messages and content stored in the cloud

Encryption Keys stored locally

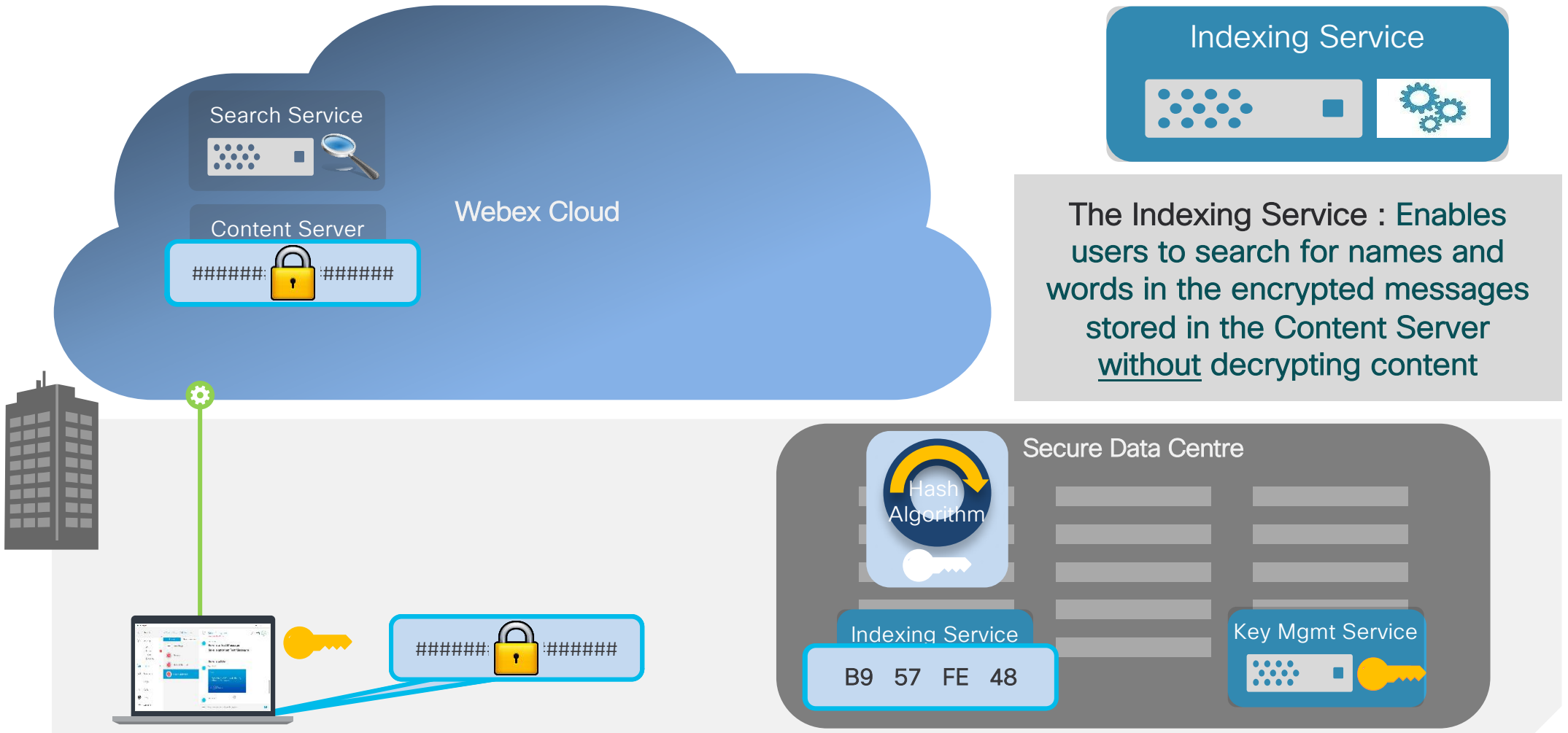
Hybrid Data Security – Secure App Connections



Webex Teams Apps establish a direct secure connection to the On Premise HDS node KMS service

This encrypted peer to peer session traverses the Webex Cloud

Hybrid Data Security: Search Indexing Service

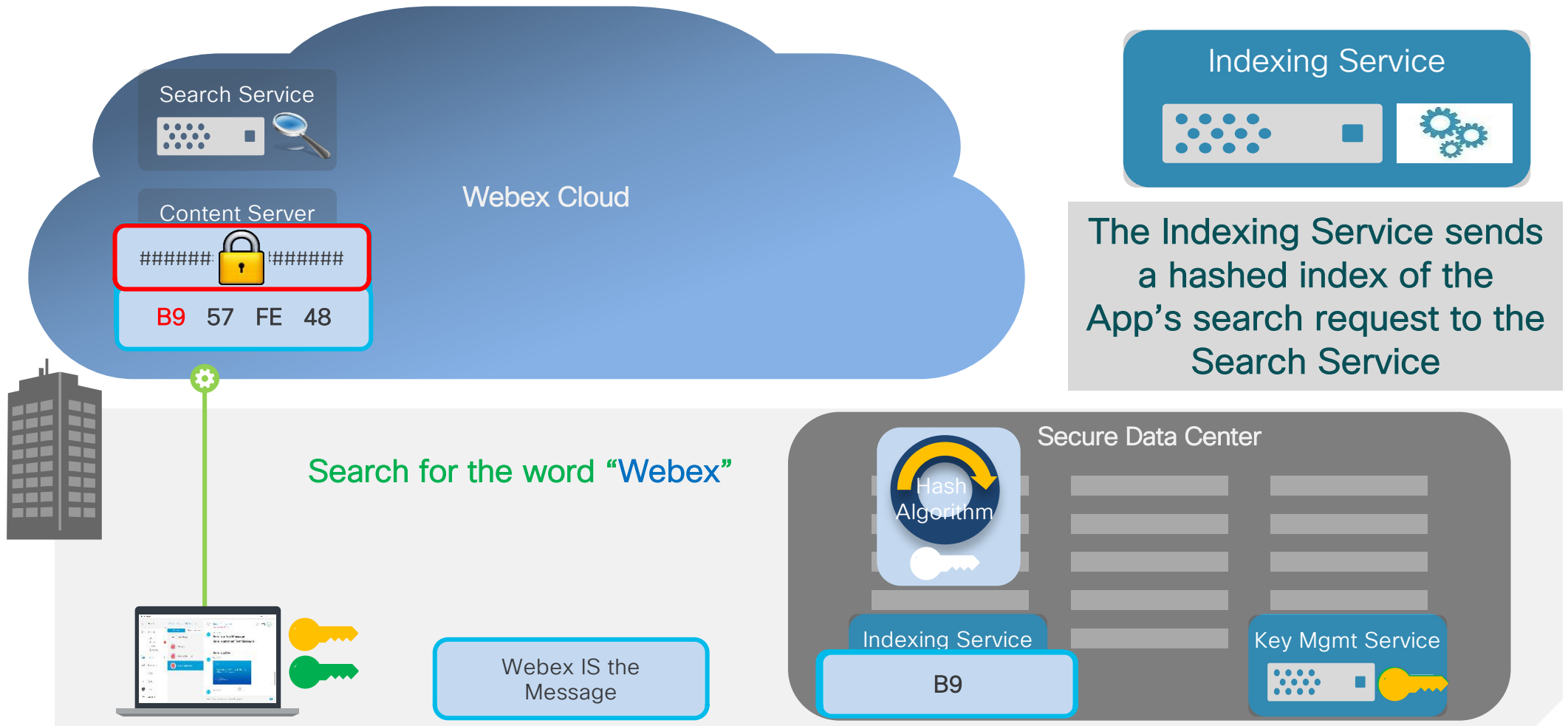


The Indexing Service : Enables users to search for names and words in the encrypted messages stored in the Content Server without decrypting content

* A new hashing key (Search Key) is used for each space

Hybrid Data Security: Querying a Search Index

Search for the word "Webex"



*A link to Conversation Encryption Key is sent with the message

Customer Controlled Security :

Key Management Server Federation with other Webex Teams Orgs.

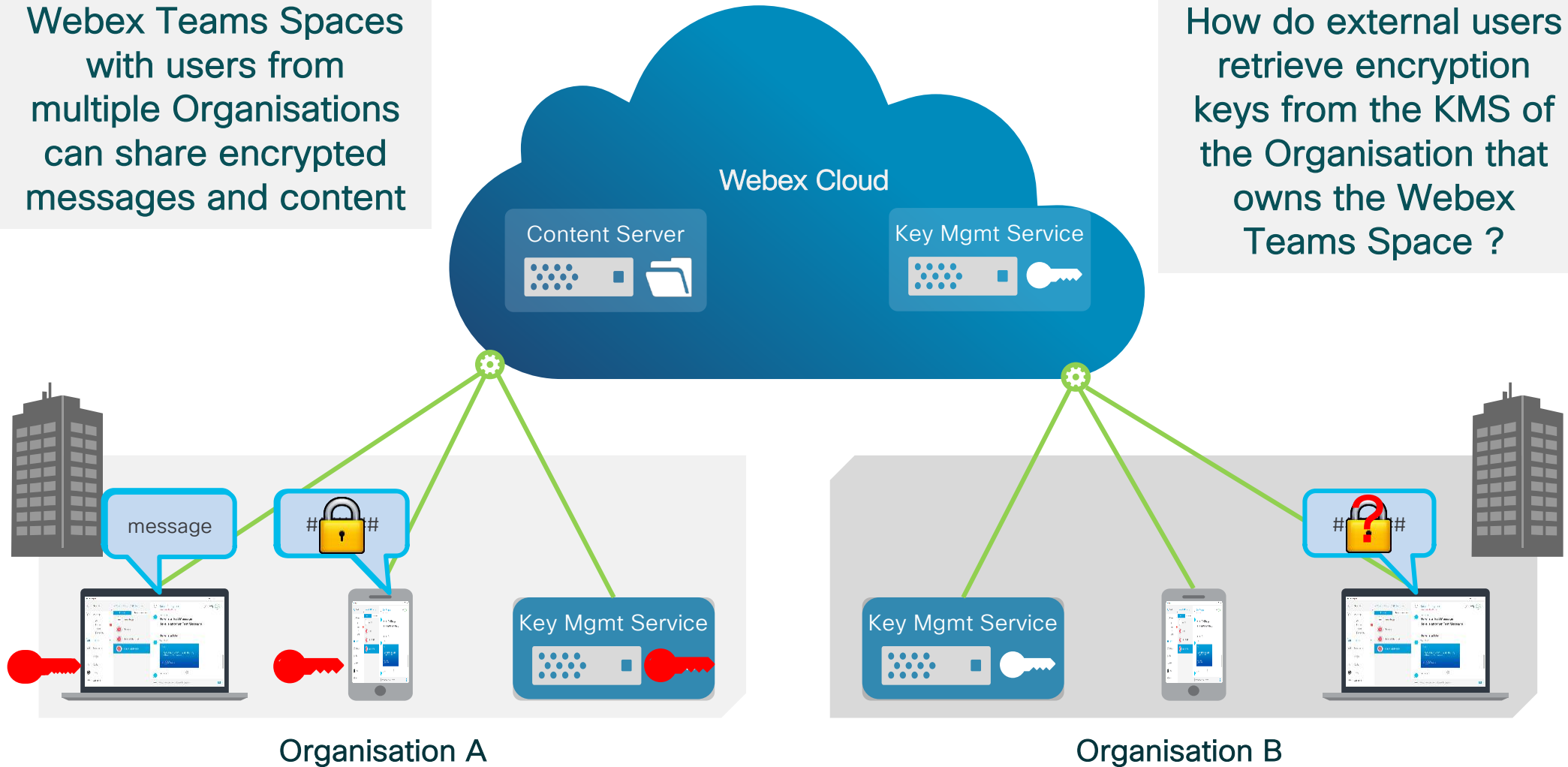


You make security **possible**

HDS: Encryption Keys & Users in other Organizations

Webex Teams Spaces with users from multiple Organisations can share encrypted messages and content

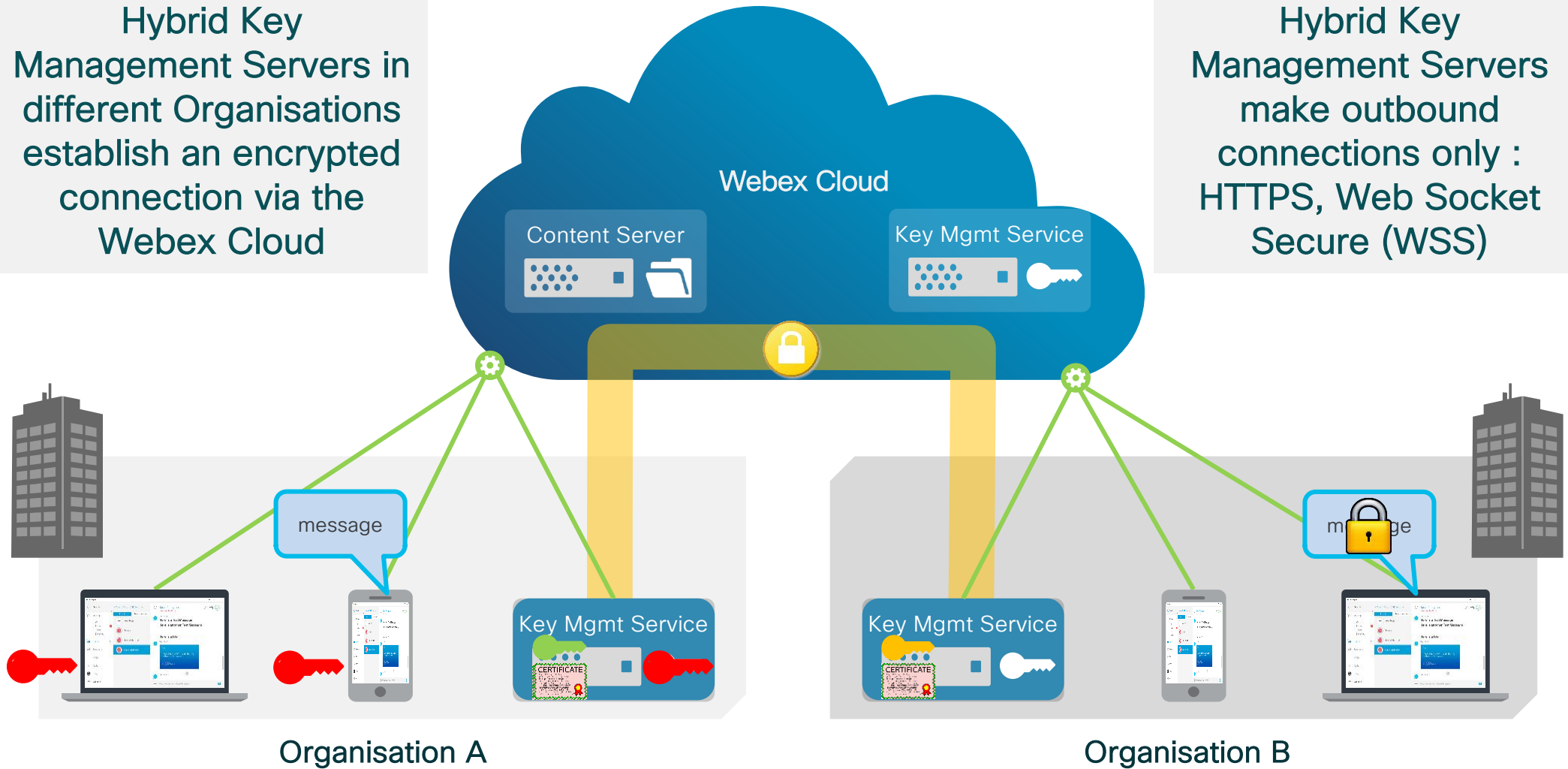
How do external users retrieve encryption keys from the KMS of the Organisation that owns the Webex Teams Space ?



HDS: Key Management Server Federation

Hybrid Key Management Servers in different Organisations establish an encrypted connection via the Webex Cloud

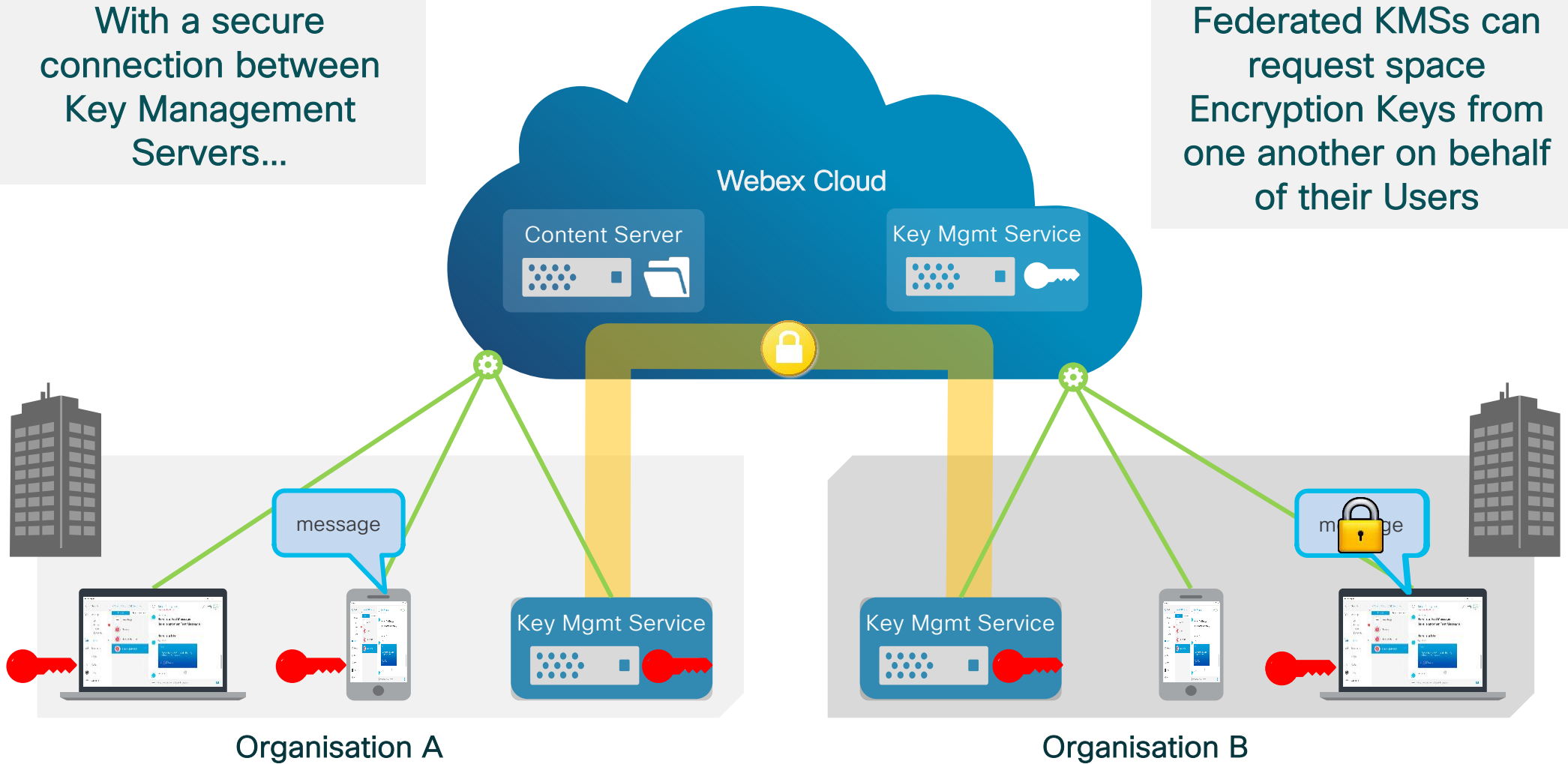
Hybrid Key Management Servers make outbound connections only : HTTPS, Web Socket Secure (WSS)



HDS: Key Management Server Federation

With a secure connection between Key Management Servers...

Federated KMSs can request space Encryption Keys from one another on behalf of their Users



Webex Teams Security – Documentation

Webex Teams Privacy and Security White Paper

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf Foundational document covering the Webex Cloud platform

Webex Teams Applications – Security White Paper

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Webex-Apps-Security-White-Paper.pdf (Teams Apps – Windows/Mac/iOS/Android)

Data Handling and Privacy for Cognitive Collaboration White Paper

<https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-742369.html>

Webex Teams Privacy Data sheet

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf Details on the processing, storage and encryption of Personal Data

Webex Teams Tech Ops and Security – Frequently Asked Questions (FAQs)

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Spark-Security-Frequently-Asked-Questions.pdf

Network Requirements for Webex Teams Services

<https://collaborationhelp.cisco.com/article/WBX000028782>



You make **possible**