Louisville Microsoft Users Group

A Forum for Computer Professionals

Special Thanks to our Platinum Sponsors

FORTINET
FAST. SECURE. GLOBAL.
www.fortinet.com

VIRTUAL TELECOMM
On your side of the connection
www.virtualtelecomm.com

FLEXENTIAL
www.flexential.com

DELL EMC
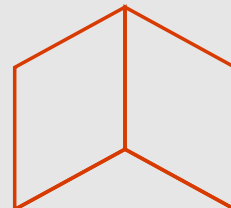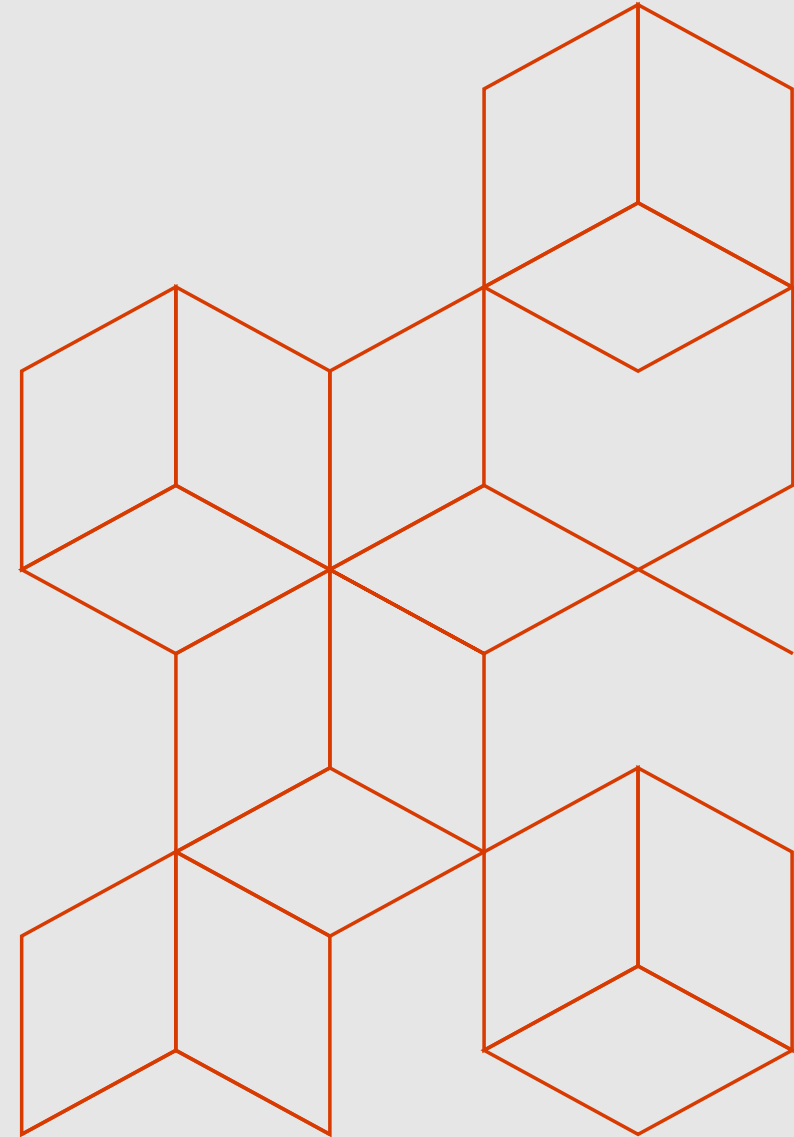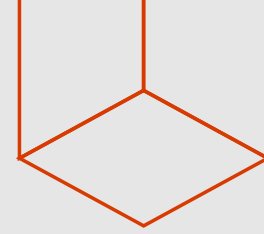www.dellemc.com

Microsoft

Microsoft Teams Administration – How to manage Microsoft Teams as an IT Pro!

Ben Powell
Teams Technical Specialist – Microsoft

Agenda

Microsoft Teams: the hub for Teamwork

- Teams Admin Role Assignments
- Teams Compliance
- Teams Policies
- Teams Operations & Reporting

Hello!

Ben Powell – Louisville's Microsoft Teams Technical Specialist

Pre-sales Technical specialist with a background in Unified Communications and Collaboration

Microsoft Teams Resource Cheat Sheet

Office 365 Roadmap

- All public feature delivery dates
- Filter by product

https://aka.ms/O365Roadmap

Microsoft Technical Community

- Product forums and blogs
- Driving Adoption forum
- O365 Champion's Corner
- Diversity & Inclusion forum

https://aka.ms/TeamsCommunity

Success with Teams Practical Guidance

- Learn how to plan, deliver, adopt and manage Microsoft Teams
- Skype for Business to Teams transition guidance

https://aka.ms/SuccessWithTeams

Coffee in the Cloud on YouTube

- Short how-to videos for IT Pro's and Champions
- Long form end user & administrator training

https://aka.ms/CoffeeintheCloud

Microsoft Teams

The hub for teamwork in Office 365

Communicate
through chat, meetings & calls

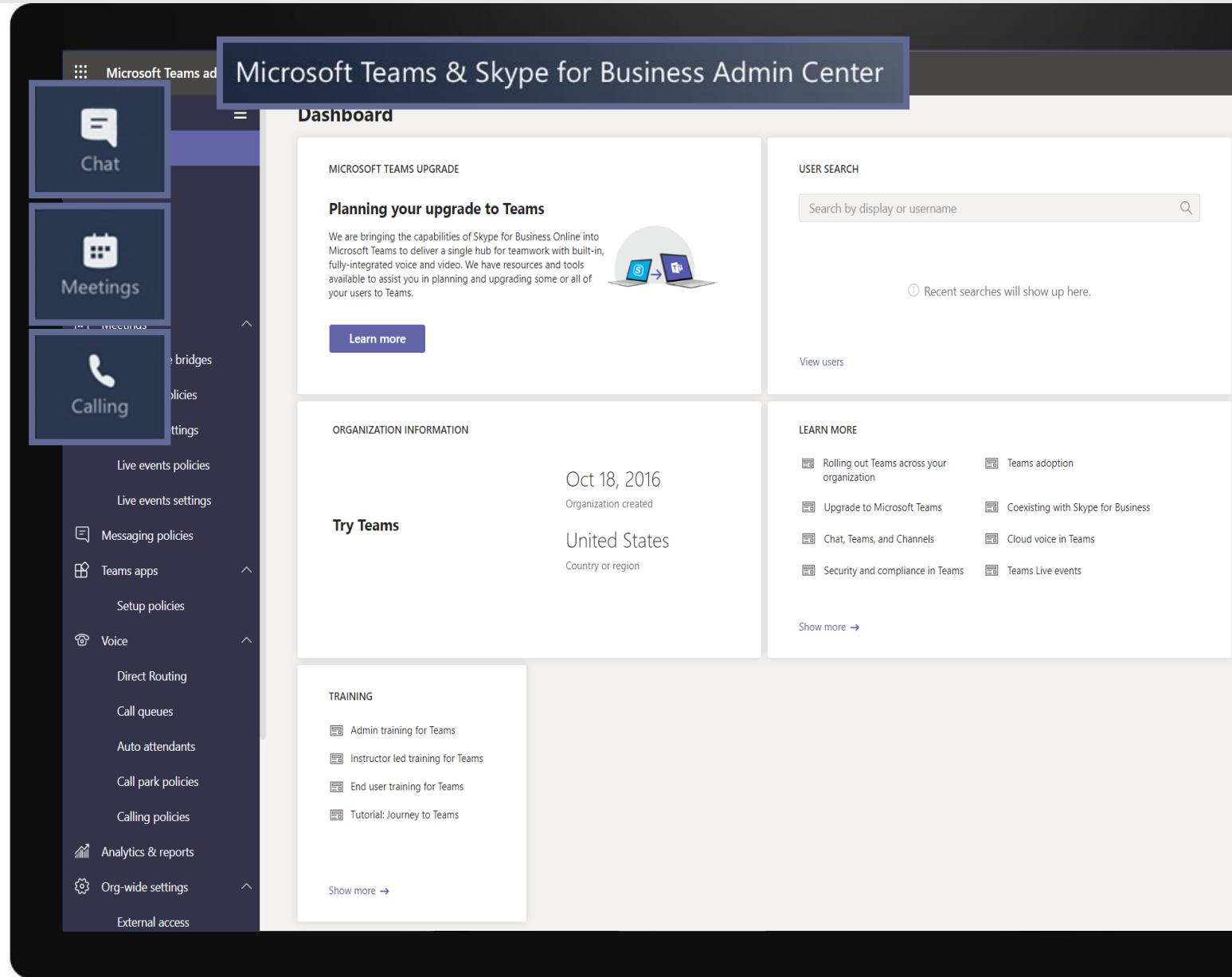**Collaborate**
with deeply integrated Office 365 apps

Customize & extend
with Office 365 apps, 3rd party apps, processes, and devices
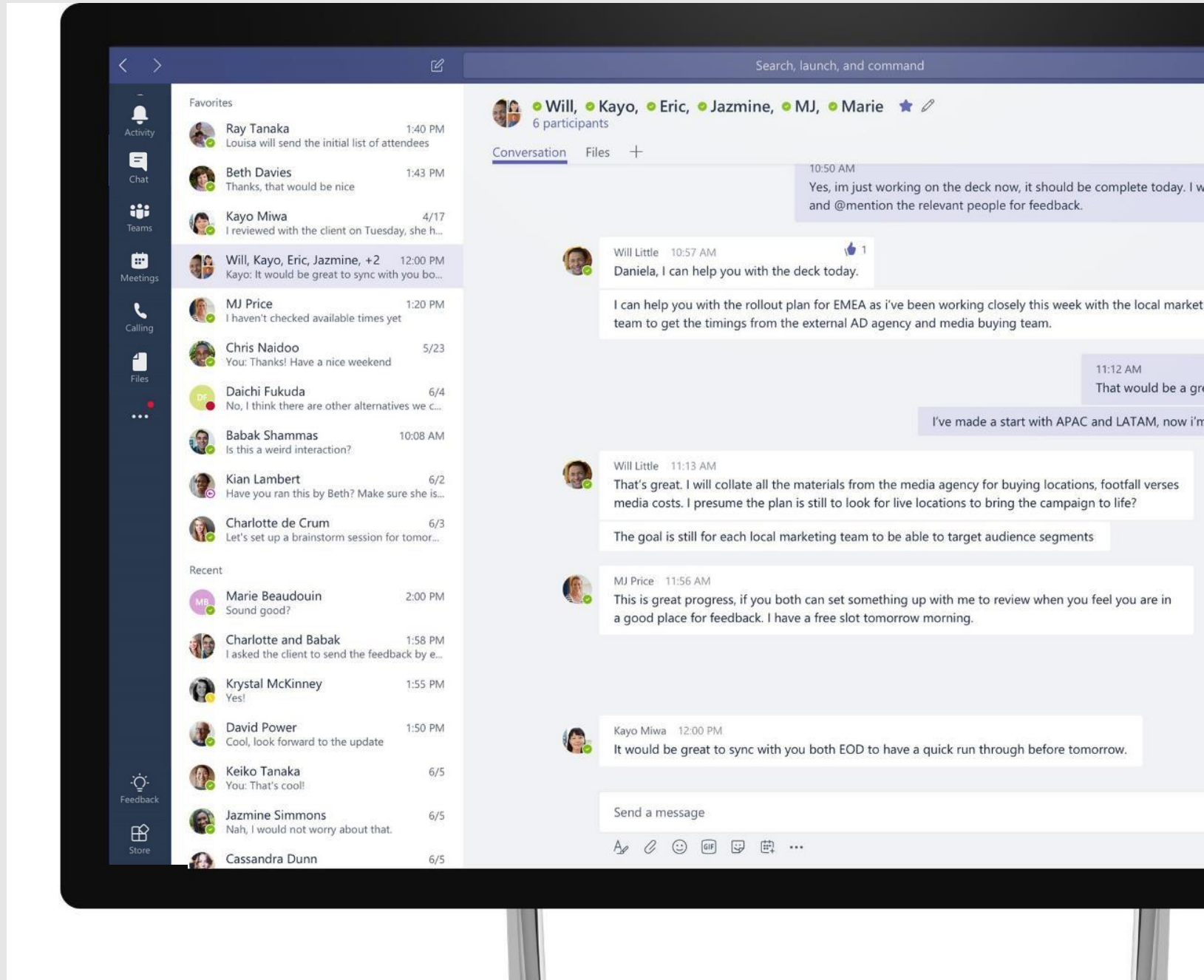
Work with confidence
enterprise level security, compliance, and manageability

Microsoft Teams

The fastest growing business app in Microsoft history

...so how do you manage it?

Teams Administrator Roles

Microsoft Teams runs on M365 Infrastructure

Teams clients

M365 and Azure AD Admin Tools

Controls for Groups, Identity, Licenses, Access

Teams and Skype for Business Admin Tools

Controls for managing communications and Teams specific features

Security & Compliance Admin Tools

Controls for managing Security & Compliance across M365

Azure
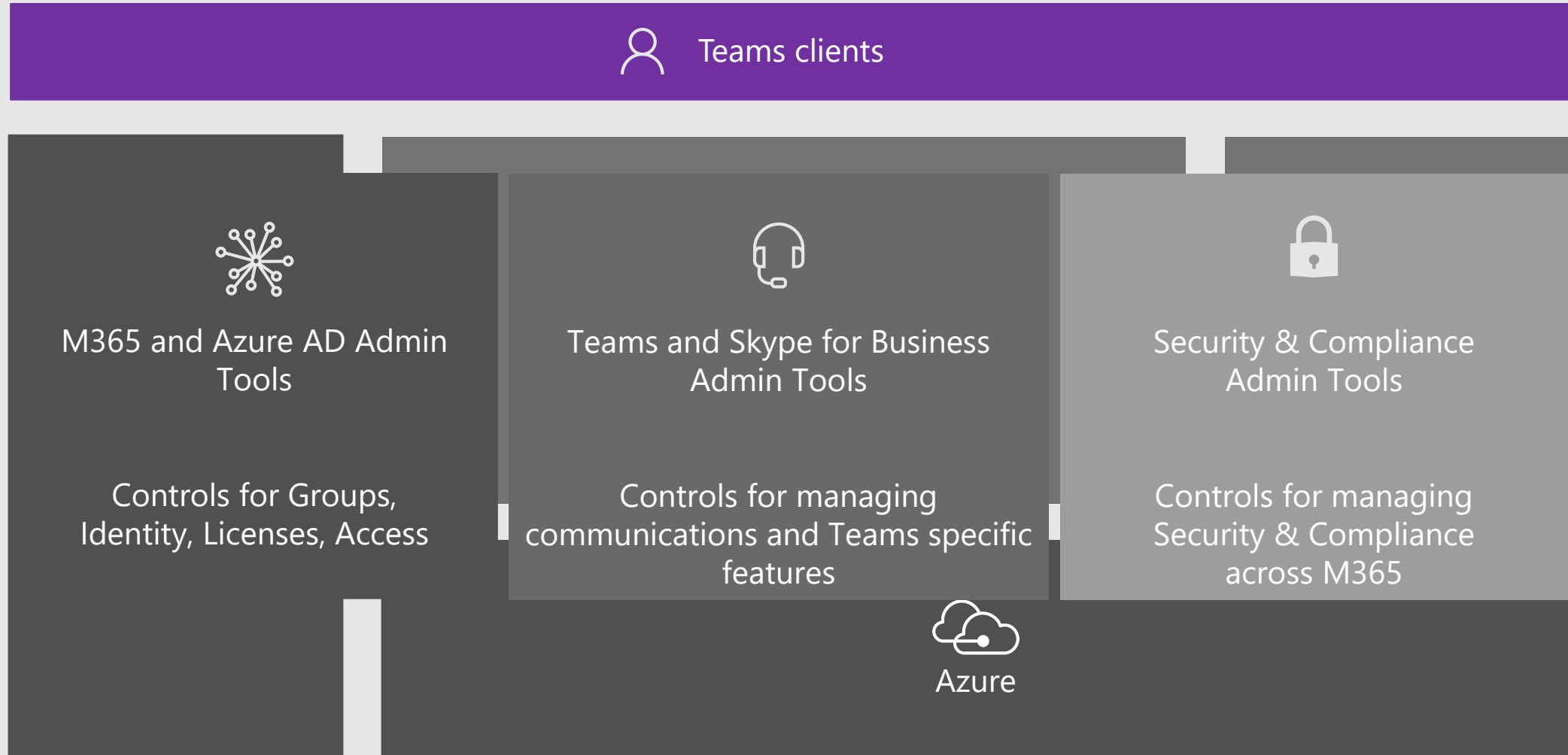
Role Assignments

Assign the right admin roles

- **Teams Service Administrator: The overall Teams workload admin, who can also manage O365 Groups**

- **Teams Communications Administrator**: Can manage meetings and calling functionality in Teams

- **Teams Communications Support Engineer**: Access to advanced call analytics tools

- **Teams Communications Support Specialist**: Access to basic call analytics tools

- Others, depending on your IT structure!

Power BI administrator	Can manage all aspects of the Po...
Privileged role administrator	Can manage role assignments in...
Reports reader	Can read sign-in and audit report...
Security administrator	Can read security information an...
Security reader	Can read security information an...
Service administrator	Can read service health informati...
SharePoint administrator	Can manage all aspects of the Sha...
Skype for Business administrator	Can manage all aspects of the Sky...
Teams Communications Administrator	Can manage calling and meeting...
Teams Communications Support Engineer	Can troubleshoot communicatio...
Teams Communications Support Special...	Can troubleshoot communicatio...
Teams Service Administrator	Can manage the Microsoft Teams...
User administrator	Can manage all aspects of users a...

Select

Teams Compliance

How <u>compliant</u> is Microsoft Teams?

Controls

More than 950 Office 365 controls

- Access control
- Auditing and logging
- Identification and authorization
- Awareness and training
- Continuity planning
- Incident response
- Risk assessment
- Communication protection
- Information integrity
- Deployment Approvals and management

Ongoing compliance processes

- Recurring audits like SOC, FEDRAMP, ISO+ independent verification

Microsoft Teams Certification

Microsoft Cloud Services Verified with International, Regional and Industry specific standards and terms
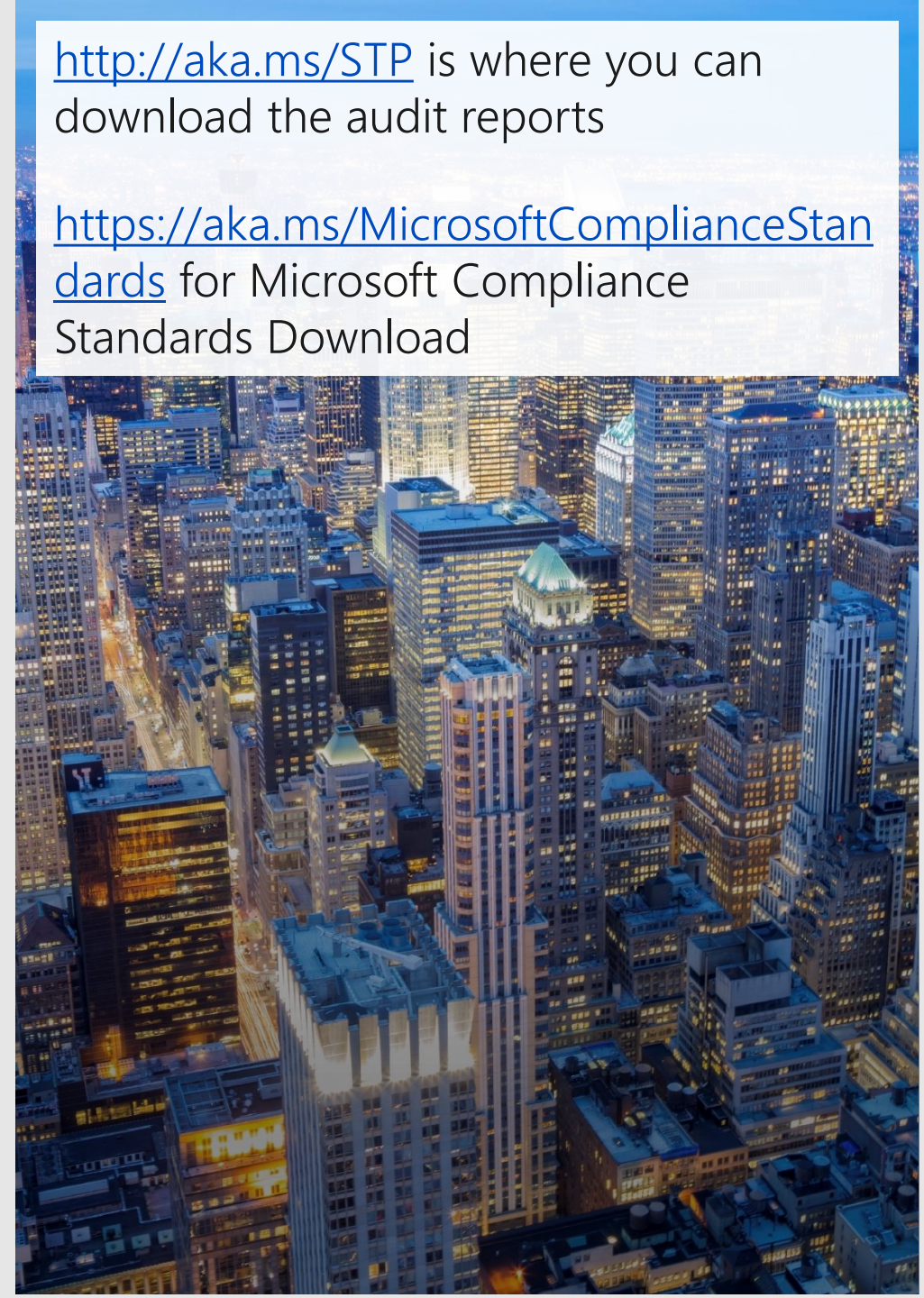
Strong Privacy and Security Commitments

- ISO 27001
- ISO 27018
- EU Model Clauses (EUMC)
- <u>GDPR</u>
- <u>HIPAA Business Associated Agreement</u>
- SSAE 16 SOC 1 & SOC 2 Reports
- <u>FedRAMP Moderate and High</u>
- IRS 1075, UK Official (IL2)
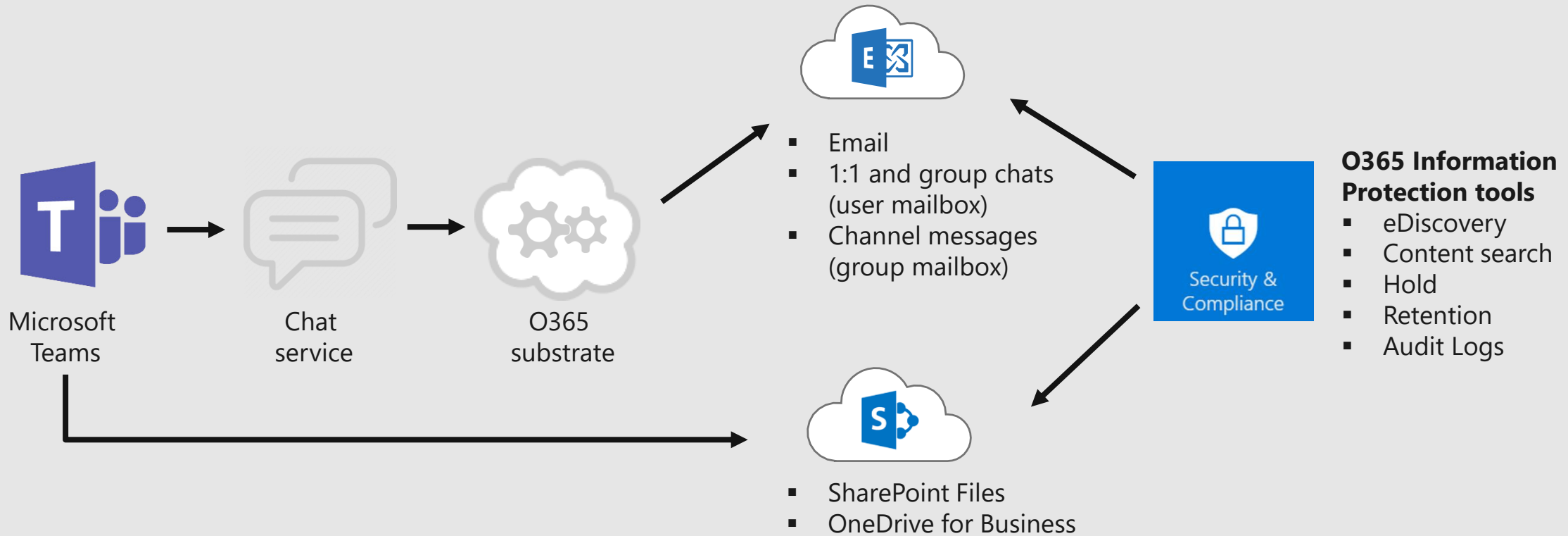- <u>Health Information Trust Alliance (HITRUST)</u>

Contractual commitment to meet US and EU data residency requirements

Compliance builds on Office 365: Messages and Files

Microsoft Teams → Chat service → O365 substrate

- Email
- 1:1 and group chats (user mailbox)
- Channel messages (group mailbox)

- SharePoint Files
- OneDrive for Business

Security & Compliance

O365 Information Protection tools
- eDiscovery
- Content search
- Hold
- Retention
- Audit Logs

Audit

Who created Team "Contoso"?

Who made Mallory a Teams owner?

Who changed the Channel settings?

I want to know whenever a Team is created!

- Audit allows to investigate specific activities across Office 365 services
- By default turned off
- Will record last 90 days starting when enabled
  - Private preview: 365 days for E5 or E3 with Advanced Compliance add-on
- Event displayed 30 minutes of event occurrence
- Reactive: review past events
- Proactive: get email notification for new events

Office 365 Security & Compliance

Alerts

Permissions

Classifications

Data loss prevention

Records management

Data governance

Supervision

Threat management

Mail flow

Data privacy

Search

    Content search

    Audit log search

    Productivity app discovery

eDiscovery

Reports

Home   > Audit log search

Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be ab related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search   ↺ Clear

Results

Activities

Date ▼	IP address	User	Activity	Item	Detail

Show results for all activities ▾

✕ Clear all to show results for all activities

Search ✕

Microsoft Teams activities

Created team	Deleted team	Added channel
Deleted channel	Changed organization setting	Changed team setting
Changed channel setting	User signed in to Teams	Added members to team
Changed role of members in team	Removed members from team	Added bot to team
Removed bot from team	Added tab	Removed tab
Updated tab	Added connector	Removed connector
Updated connector		

Dynamics 365 activities

Accessed out-of-box entity	Accessed custom entity	Accessed admin entity
Performed bulk actions (such as delete and import)	Accessed other entity type	Accessed Dynamics 365 admin center

➕ New alert policy

Content Search

Who posted about "Longhorn"?

What messages have been posted to channel "Secret"?

I need to find all message from Mallory!

What was the content of a certain deleted message?

- Chat and channel messages
  - Results will be displayed as individual messages, not as threaded conversation
- Meta data for calls and meetings
- Putting content on hold
  - Without hold, only latest version can be retrieved and no deleted items
  - With hold, all previous version and deleted items can be retrieved
- Results can be exported

Content Search

- Define conditions
  - Such as keywords, date, sender/author, recipient,...
- Define locations
  - Exchange store for all or some users, groups or teams
  - SharePoint and OneDrive for Business for some or all sites

Add conditions

Search

	Name	Group
☐	Date	Common
☐	Sender/Author	Common
☐	Size (in bytes)	Common
☐	Subject/Title	Common
☐	Compliance tag	Common
☐	Message kind	Emails
☐	Participants	Emails
☐	Type	Emails
☐	Received	Emails
☐	Recipients	Emails

Add   Cancel

Choose locations

Exchange email — None
Choose users, groups, or teams

Office 365 group email

Skype for Business

Teams messages

To-Do

MyAnalytics

SharePoint sites — None
Choose sites

OneDrive accounts

Office 365 group sites

Teams sites

Exchange public folders — None

eDiscovery

- *Electronic discovery is the electronic aspect of identifying, collecting and producing electronically stored information (ESI) in response to a request for production in a law suit or investigation.*

- Create "case" for eDiscovery process

- Combines a set of searches and hold configuration
  - Hold can be configured directly from eDiscovery
  - Search can be scoped to items on hold

- Results can be exported

eDiscovery dashboard

Hold

- Define locations and conditions
  - Same as for content search
- Once hold is enabled
  - All versions of modified items will be kept
  - Deleted items will be kept
- Can be configured via Exchange portal or eDiscovery case
- Data Locations

Scenario	What to place on hold
Microsoft Teams Private Chats	User mailbox
Microsoft Teams Channel Chats	Group mailbox used for the team
Microsoft Teams Content (e.g. Wiki, Files)	SharePoint site used by the team
Private Content	OneDrive for Business site of the user

Retention

- (Current) minimum for retention is 30 days
- Retention is retroactive
  - E.g. a policy set to delete content after 60 days, will delete all older content when enabled
- Possible delay in deletion
  - Exchange Life Cycle assistant (ELC) runs daily, but it has an SLA of 7 days
  - E.g. with retention policy to delete after 60 days, these items could persist for up to 67 days
  - In most cases, there is no delay

Retention

Create a policy to retain what you want and get rid of what you don't.

✅ Name your policy

⚪ Settings

⚪ Choose locations

⚪ Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

🔘 Yes, I want to retain it ⓘ

| For this long... ⌄ | 7 | years ⌄ |

Retain the content based on [when it was created ⌄] ⓘ

Do you want us to delete it after this time? ⓘ

⚪ Yes   🔘 No

⚪ No, just delete content that's older than ⓘ

| 1 | years ⌄ |

Need more options?

⚪ Use advanced retention settings ⓘ

[Back] [Next] [Cancel]

Create a policy to retain what you want and get rid of what you don't.

✅ Name your policy

✅ Settings

⚪ Choose locations

⚪ Review your settings

Choose locations

The policy will apply to content that's stored in the locations you choose.

⚪ Apply policy only to content in Exchange email, public folders, Office 365 groups, OneDrive and SharePoint documents.

🔘 Let me choose specific locations. ⓘ

Status	Location	Include	Exclude
⚫⚪	Exchange email		
⚫⚪	SharePoint sites		
⚫⚪	OneDrive accounts		
⚫⚪	Office 365 groups		
⚫⚪	Skype for Business		
⚫⚪	Exchange public folders		
🔵	Teams channel messages	All Choose teams	None Exclude teams
🔵	Teams chats	All Choose users	None Exclude users

[Back] [Next] [Cancel]

Feedback

Teams Configuration & Policies

About Teams configurations

- ## Teams is designed with smart defaults

  - Defaults are set to match most companies' requirements

- ## Throughout the deck we highlight

  - In which area of Office 365 a setting is configured

  - If a setting is applied per tenant, per user or per Group

    - All settings have a global default

Where a setting is configured?			Can it be user specific or is it global?		
Teams	Groups setting	Security & compliance	Global settings	User specific	Groups

Ability to create teams

- Why

  - Some companies want to have strict control over every team that is created

- Considerations

  - We recommend not to limit the ability to create teams, as this might negatively affect productivity

  - If only a subset of users can create teams, you need to create a process for users to request teams

  - Leveraging user education to ensure responsible Teams usage

  - You can audit who created which group

  - Requires Azure AD Premium P1 license

- How

  - Configured in the Office Admin Center and via Azure Active Directory PowerShell

  - Details: https://aka.ms/create-o365-groups

Naming of teams

- Why
  - Prefix-suffix naming conventions allow to add or append fixed strings or supported user attributes to the teams name
  - Blocked words can avoid (intentional or unintentional) misuse of teams

- Considerations
  - Naming policies require Azure AD Premium P1 or Azure AD Basic EDU license
  - Selected administrator roles are exempted from these policies

- How
  - Configured in the Office Admin Center and via Azure Active Directory PowerShell
  - Details: https://aka.ms/naming-o365-groups

Expiration policies

- ## Why
  - By default teams exist until they are deleted. Retention policies ask team owners to renew their teams. This helps to limit "stale" teams.

- ## Considerations
  - Can be configured globally or for specific groups
  - Requires Azure AD Premium P1 for members of teams that have expiration policy
  - Team owners will get notifications about expiation 30, 15 and 1 day before expiration
  - Once expired, users can recovery team for 30 days
  - If enabled, default is 180 days

- ## How
  - Configured in the Office Admin Center and via Azure Active Directory PowerShell
  - Details: https://aka.ms/teams-expiration

Classification for teams

- Why

  - Classifications on teams allow a team to have specific settings assigned that control team behavior

- Considerations

  - Requires Azure AD Premium P1 to set a default classification

  - Requires custom PowerShell application to enforce settings per team

- How

  - Configured in the Office Admin Center and via Azure Active Directory PowerShell

  - Details: https://aka.ms/teams-classification

Retention policies

- ## Why
  - Retention policies can be used to define a range of days after all content will be deleted or a range of days that content cannot be deleted – or both

- ## Considerations
  - Retention can be set independently for chat messages and channel messages
  - Channel message policies can be applied globally or per team
  - Chat message policies can be applied globally or per user
  - Files use retention policies of SharePoint and OneDrive for Business

- ## How
  - Configured in Security & Compliance Center and Office 365 Security & Compliance Center PowerShell
  - Details: https://aka.ms/teams-retention

Messaging policies

Teams

User specific

- Why
  - Messaging policies are used to control what chat and channel messaging features are available to users in Teams

- Considerations
  - Are there any features (such as Giphy, stickers, edit, delete) that you need to restrict for some or all users?
  - You can use the default policy that is created or create one or more custom messaging policies for people in your organization

- How
  - Teams settings are configured via the Microsoft Teams & Skype for Business Admin Center and Skype for Business PowerShell
  - Details: https://aka.ms/teams-messaging

Meeting policies

- Why
  - Meeting policies are used to control what features are available to users when they join Teams meetings
- Considerations
  - You can use the default policy or create one or more custom meeting policies for people that host meetings in your organization
  - Meeting polices can be used to limit the ability for users to schedule meetings and to limit meeting features such as audio, video, content sharing or meeting recording
  - Limiting features might reduce users' ability to collaborate effectively
  - Does your organization have any requirements around guest or anonymous communication?
- How
  - Teams settings are configured via the Microsoft Teams & Skype for Business Admin Center and Skype for Business PowerShell
  - Details: https://aka.ms/teams-meeting-policies

Live events policies

- Why
  - Teams live events policies are used to manage event settings for groups of users
- Considerations
  - You can use the default policy or create additional policies that can be assigned to users that hold live events within your organization
  - Does your organization have a requirement to host webinar style conferences?
  - Is the ability to record or transcribe a live event important to your organization?
- How
  - Teams settings are configured via the Microsoft Teams & Skype for Business Admin Center and Skype for Business PowerShell
 - Details: https://aka.ms/teams-live-events

External access

- Why
  - External access lets your Teams and Skype for Business users communicate with users that are outside of your organization
  - Also known as "Federation"
- Considerations
  - Do you have business requirements to limit user communications with external participants?
  - Do you need to limit which external participants users can communicate with?
- How
  - Teams settings are configured via the Microsoft Teams & Skype for Business Admin Center and Skype for Business PowerShell
 - Details: https://aka.ms/teams-external-access

Guest access

- Why
  - Allows users without account in your Azure Active Directory to be invited as guests to Teams
- Considerations
  - Inviting external parties to teams can increase productivity
  - Comes with certain risk around which content is exposed to guest users
  - Allow and deny list can limit guest access to specific domains
  - Guest access can be limited to specific teams
  - Audit logs allow insights on who has invited whom
- How
  - Configured in the Office Admin Center and via Azure Active Directory PowerShell
  - Details: https://aka.ms/guests-o365-groups

Teams Operations and Reporting - day to day management in Modern Portal
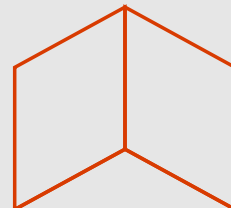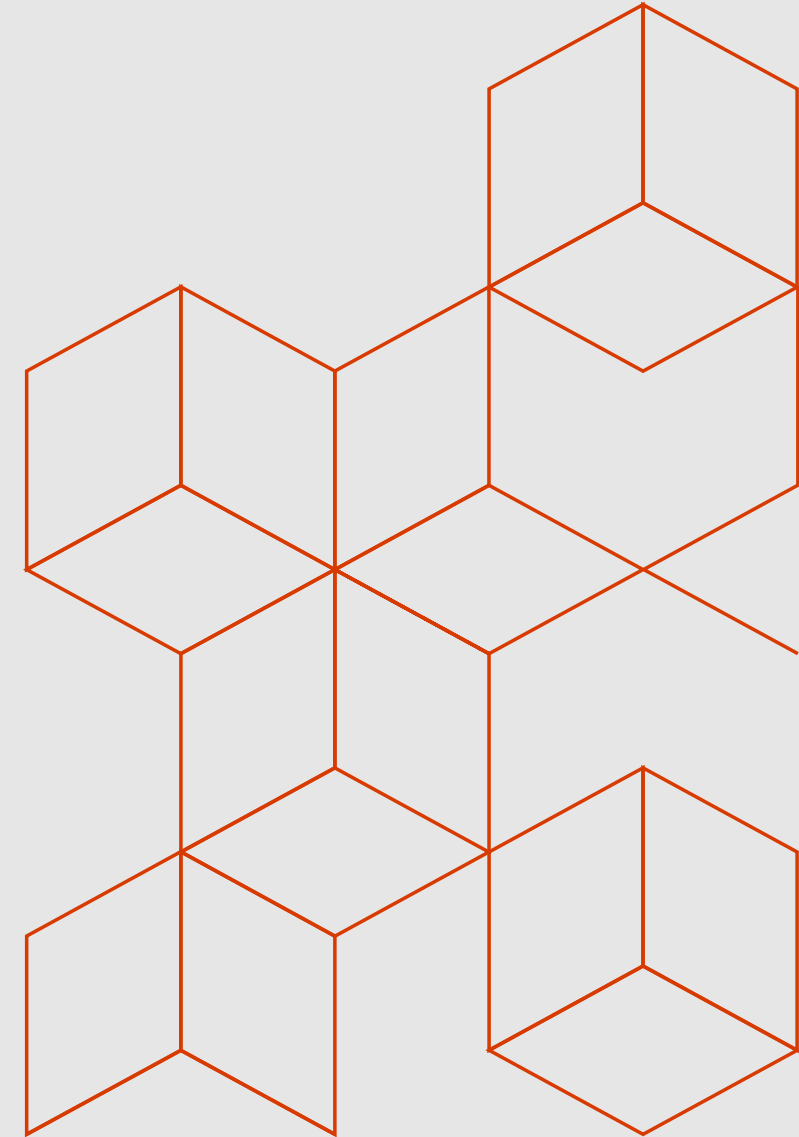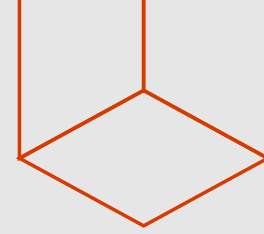
Teams Monitoring – Usage and Quality

- Usage Reporting in M365 admin portal and Office 365 Adoption Content Pack

- Call Quality Dashboard
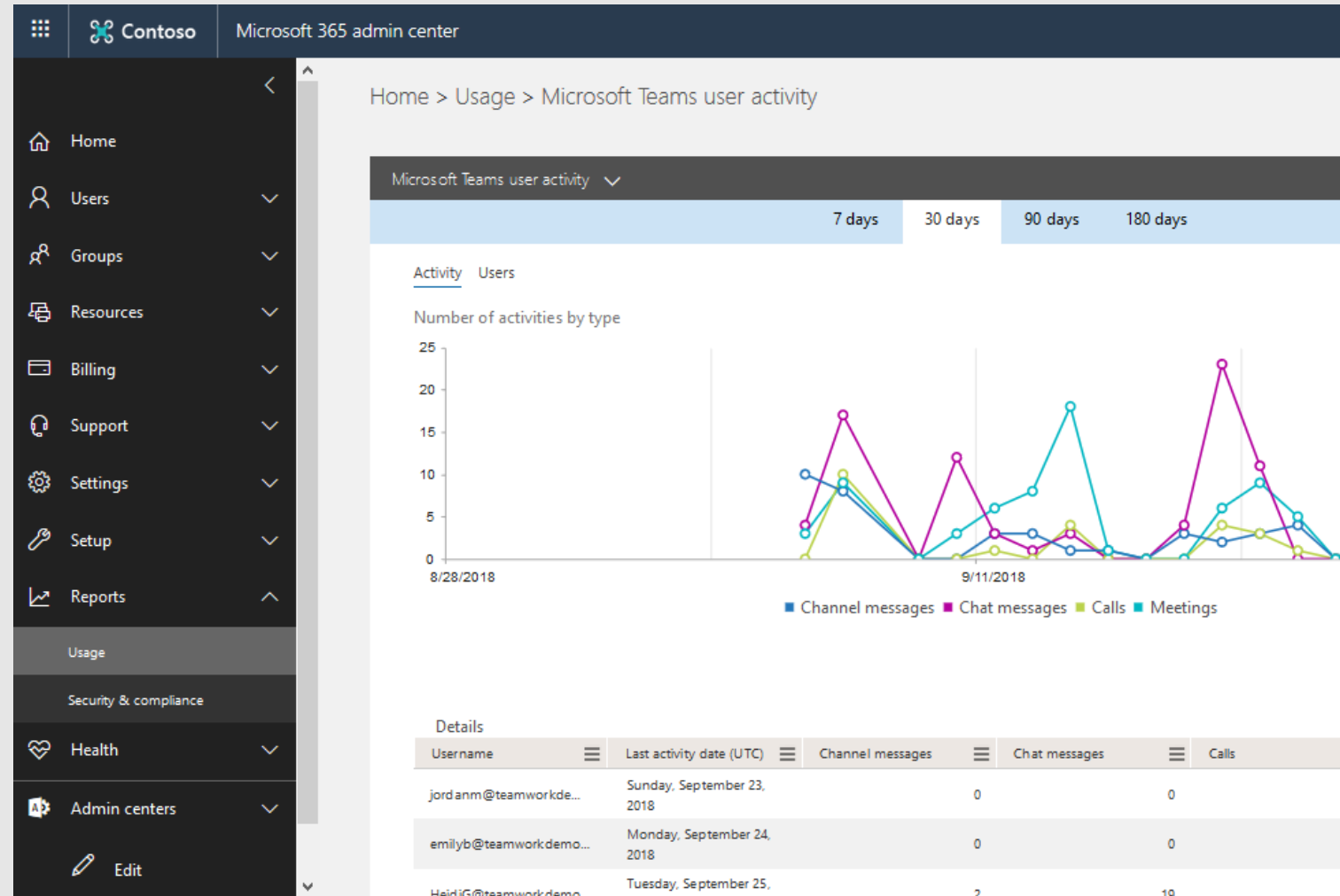
Demo: admin portal reporting

Microsoft Teams Resource Cheat Sheet

Office 365 Roadmap

- All public feature delivery dates
- Filter by product

https://aka.ms/O365Roadmap

Microsoft Technical Community

- Product forums and blogs
- Driving Adoption forum
- O365 Champion's Corner
- Diversity & Inclusion forum

https://aka.ms/TeamsCommunity

Success with Teams Practical Guidance

- Learn how to plan, deliver, adopt and manage Microsoft Teams
- Skype for Business to Teams transition guidance

https://aka.ms/SuccessWithTeams

Coffee in the Cloud on YouTube

- Short how-to videos for IT Pro's and Champions
- Long form end user & administrator training

https://aka.ms/CoffeeintheCloud

For Customers

Thank you! Questions?