Microsoft

Microsoft 365 Government Roadmap

February 2024

Richard Wakeman
Chief Architect - Aerospace & Defense
Microsoft Corp

Richard Wakeman
Chief Architect

Aerospace & Defense Microsoft

Microsoft Corp for 17 years

- Chief Architect - Aerospace & Defense
- Senior Director - Aerospace & Defense - Azure Global Engineering
- Global Black Belt - Aerospace & Defense
- Senior Architect - Microsoft Consulting Services

Sub-Contractor for Microsoft (5 years)

A Few Firsts

- Exchange 2000 SDK Developer
- Microsoft CRM 1.0 Developer
- Identity Integration Server 2003 (Now MIM)
- 1st Production ADFS 1.0
- 1st "*Cloud*" w/ Live@edu
- 1st PubSec Cloud Architect
- Microsoft 365 GCC & GCCH
- Dozen 1M+ Deployments
- CMMC Acceleration Program

Aerospace & Defense

- Architect & Specialist in security & compliance critical to the DIB
- Lead for Azure Secret onboarding DIB
- Public face for Microsoft for the CMMC

Notices

- Microsoft CMMC Acceleration provides customers and partners with resources to pursue CMMC compliance while leveraging Microsoft products and services— It does not address security practices occurring outside of Microsoft products and services.

- Please further note that the CMMC compliance standard has yet to be implemented to assess the suitability of in-scope entities' security practices and configurations. As a result, there may be additional nuance or complexity associated with CMMC compliance that will only materialize (if at all) through the practical application of the standard by the CMMC Accreditation Body (CMMC-AB). What's more, as of the date this article was written, the CMMC-AB has not issued formal guidance for Cloud Service Providers. As a result, the information herein, including all Microsoft CMMC related offerings, are provisional and may be enhanced to align with future guidance from the DoD and CMMC-AB.

- Microsoft does not guarantee nor imply any ultimate compliance outcome or determination based on one's consumption of this article or the resources linked from it — all CMMC certification requirements and decisions are governed by the CMMC-AB, and Microsoft has no direct or indirect insight into or bearing over CMMC-AB compliance determinations. The associations between compliance domains, practices, and Microsoft CMMC Acceleration may change at any time.

- Customers must individually determine the necessary steps required to ensure their organization fully satisfies each recommended CMMC compliance practice, in addition to or in place of what is described in resources. This responsibility spans all Microsoft (Azure, Microsoft 365, etc.) consumption decisions, including, among other things, which Microsoft offerings to procure, as well as all configuration decisions associated with such use and consumption.

Agenda

01 Cloud Service Offerings for the DIB

02 Microsoft CMMC Acceleration

03 Entra Updates & Roadmap

04 Microsoft Collaboration Framework

05 Microsoft 365 Copilot

06 New Teams

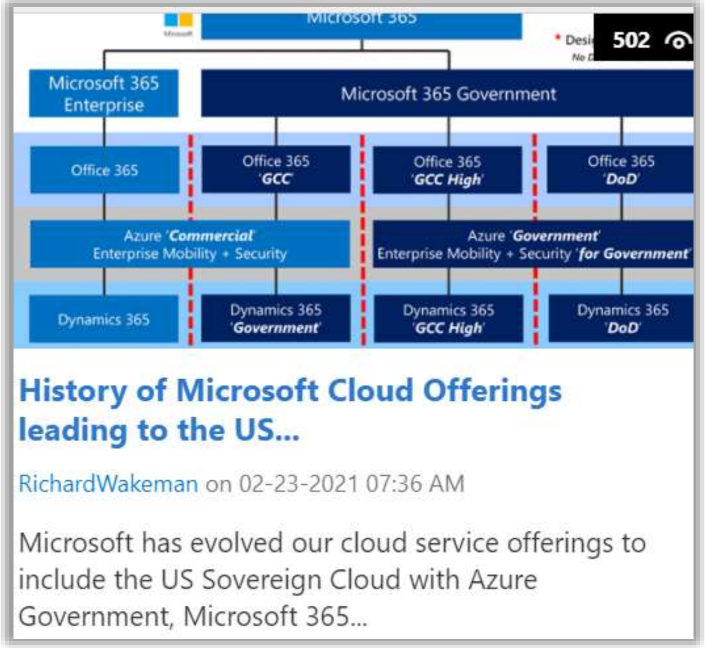
MICROSOFT

Cloud Service Offerings for the DIB

The mission-critical clouds

Public Sector Community

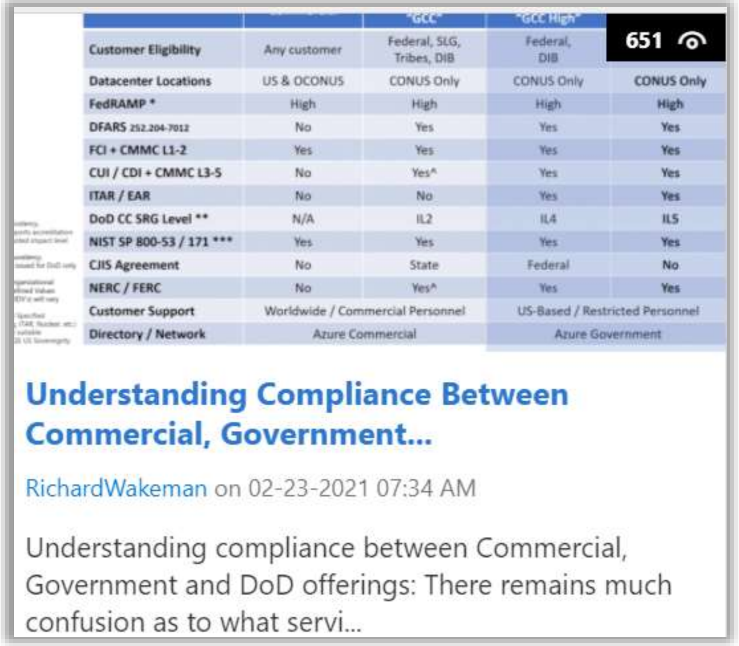
Public Sector Community Blog



History of Microsoft Cloud Offerings leading to the US...

RichardWakeman on 02-23-2021 07:36 AM

Microsoft has evolved our cloud service offerings to include the US Sovereign Cloud with Azure Government, Microsoft 365...


651

	[illegible]	"GCC"	"GCC High"	
Customer Eligibility	Any customer	Federal, SLG, Tribes, DIB	Federal, DIB	
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	CONUS Only
FedRAMP *	High	High	High	High
DFARS 252.204-7012	No	Yes	Yes	Yes
FCI + CMMC L1-2	Yes	Yes	Yes	Yes
CUI / CDI + CMMC L3-5	No	Yes^	Yes	Yes
ITAR / EAR	No	No	Yes	Yes
DoD CC SRG Level **	N/A	IL2	IL4	IL5
NIST SP 800-53 / 171 ***	Yes	Yes	Yes	Yes
CJIS Agreement	No	State	Federal	No
NERC / FERC	No	Yes^	Yes	Yes
Customer Support	Worldwide / Commercial Personnel		US-Based / Restricted Personnel	
Directory / Network	Azure Commercial		Azure Government	

Understanding Compliance Between Commercial, Government...

RichardWakeman on 02-23-2021 07:34 AM

Understanding compliance between Commercial, Government and DoD offerings: There remains much confusion as to what servi...

2,788

The Microsoft 365 US Government (GCC High) Conundrum - DIB...

RichardWakeman on 10-30-2019 10:00 AM

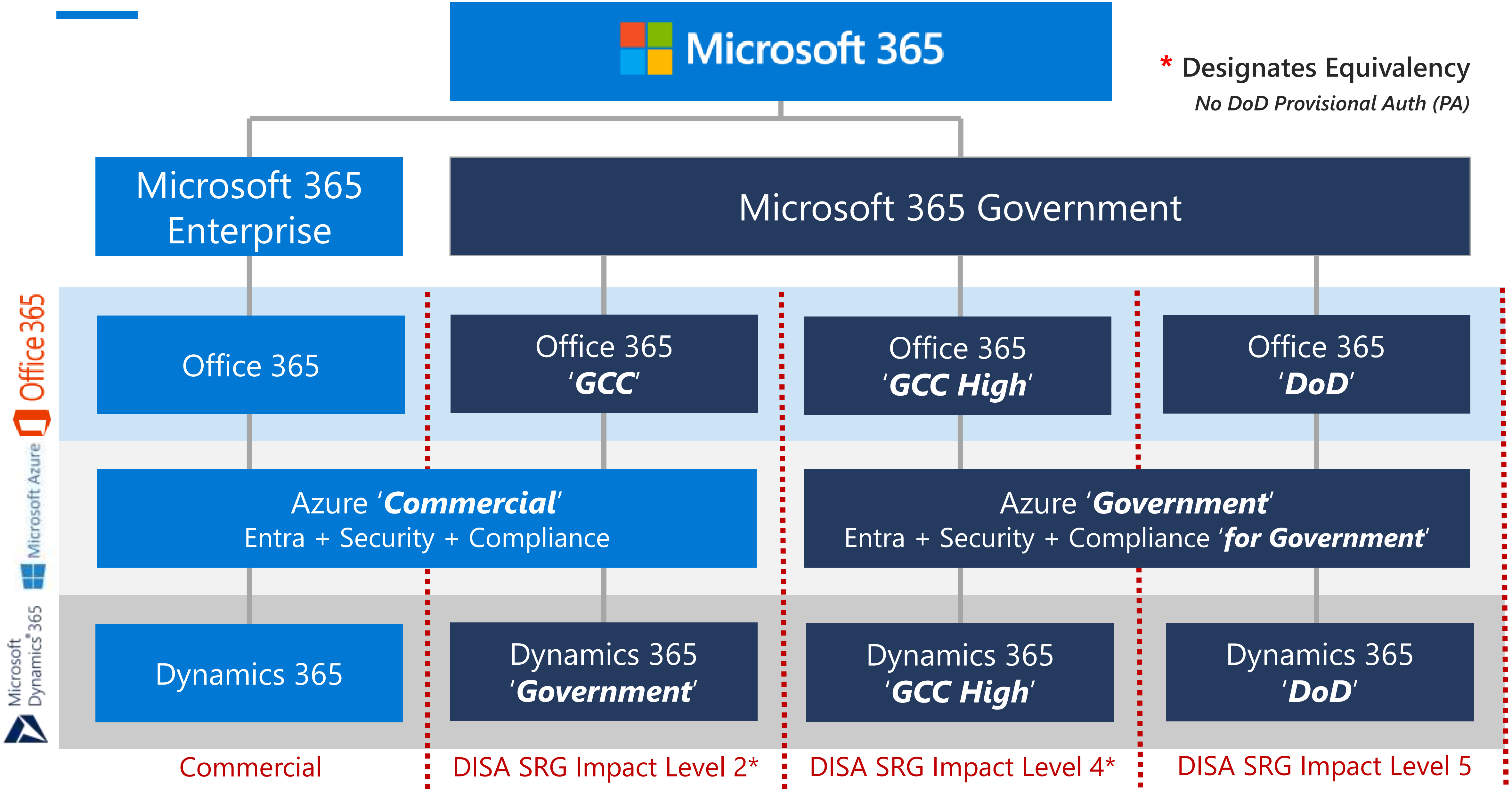
The DIB (Defense Industrial Base) are embracing M365 GCC High to achieve compliance with U.S. defense

History of Microsoft Cloud Service Offerings leading to the US

Understanding Compliance Between Microsoft 365 Commercial, Government and DoD Offerings

The Microsoft 365 US Government (GCC High) Conundrum - DIB Data Enclave vs Going All In

History of Microsoft Cloud Service Offerings leading to the US



Microsoft 365

* Designates Equivalency

No DoD Provisional Auth (PA)

Microsoft 365 Enterprise

Microsoft 365 Government

Office 365

Office 365

Office 365 '**GCC**'

Office 365 '**GCC High**'

Office 365 '**DoD**'

Microsoft Azure

Azure '**Commercial**'
Entra + Security + Compliance

Azure '**Government**'
Entra + Security + Compliance '**for Government**'

Microsoft Dynamics 365

Dynamics 365

Dynamics 365 '**Government**'

Dynamics 365 '**GCC High**'

Dynamics 365 '**DoD**'

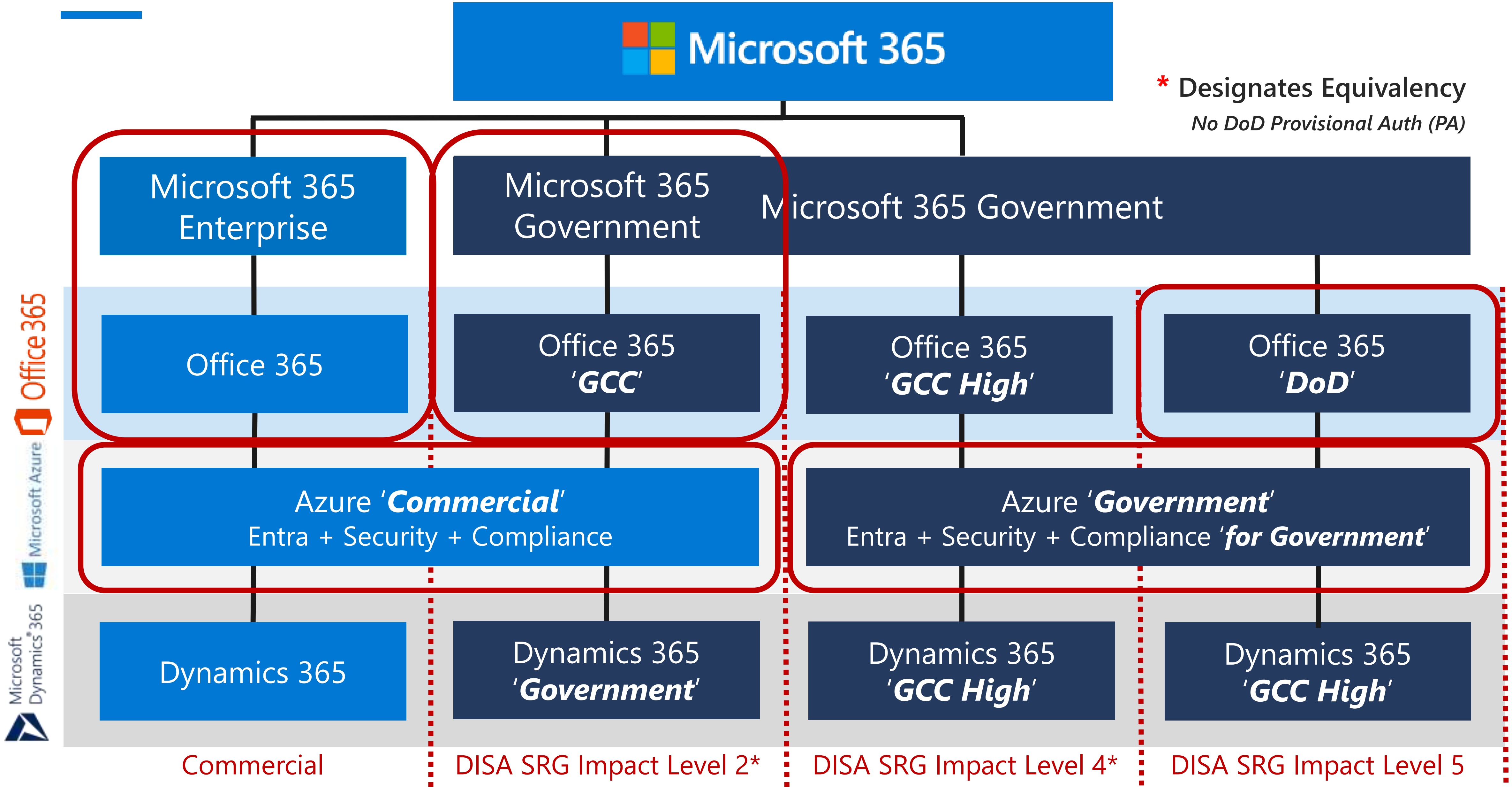
Commercial

DISA SRG Impact Level 2*

DISA SRG Impact Level 4*

DISA SRG Impact Level 5

History of Microsoft Cloud Service Offerings leading to the US



Microsoft 365

* Designates Equivalency

No DoD Provisional Auth (PA)

Microsoft 365 Enterprise

Microsoft 365 Government

Microsoft 365 Government

Office 365

Office 365 '***GCC***'

Office 365 '***GCC High***'

Office 365 '***DoD***'

Azure '***Commercial***'
Entra + Security + Compliance

Azure '***Government***'
Entra + Security + Compliance '***for Government***'

Dynamics 365

Dynamics 365 '***Government***'

Dynamics 365 '***GCC High***'

Dynamics 365 '***GCC High***'

Commercial

DISA SRG Impact Level 2*

DISA SRG Impact Level 4*

DISA SRG Impact Level 5

Azure US Government Clouds (DIB Focus)

	Commercial	Government	Secret	Top Secret
AUTHORIZATION	• FedRAMP High • DoD CC SRG IL2 • **CMMC 2.0 Level 1** • DFARS 252.204-7012 • FCI & CUI Basic (PII)	• FedRAMP High • DoD CC SRG IL2, IL4 & IL5 • **CMMC 2.0 Levels 1-3** • DFARS 252.204-7012 • FCI & CUI Specified (ITAR)	• DoD CC SRG IL6 + SaaS • **DCSA NISP** (Collateral S) *National Industrial Security Program* • **Joint Special Access** (S/SAR) *Implementation Guide (JSIG PL-3)* • ICD 503, ICD 705	• ICD 503, ICD 705 • Collateral TS • Joint Special Access
INFRASTRUCTURE	70+ Regions 35 countries	3 Regions >500 miles apart	2 Regions >500 miles apart	2 Regions >500 miles apart

Shared responsibility model

■

Customer management of risk

Data Classification and data accountability

◩

Shared management of risk

Identity & access management | End Point Devices

□

Provider management of risk

Physical | Networking

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	■	■	■	■
Client & end-point protection	■	■	■	◩
Identity & access management	■	■	◩	◩
Application level controls	■	■	◩	□
Network controls	■	◩	□	□
Host Infrastructure	■	◩	□	□
Physical Security	■	□	□	□

■ **Customer** □ **Cloud Provider**

Cloud Service offering differentiation – Microsoft 365

Public Sector Blog

	Microsoft 365 “Commercial”	Microsoft 365 Government (GCC)	Microsoft 365 Government (GCC High)	Microsoft 365 Government (DoD)
Customer Eligibility	Any customer	Federal, SLG, Tribes, Eligible Contractors (DIB, FFRDC, UARC)	Federal, Eligible Contractors (DIB, FFRDC, UARC)	DoD only
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	CONUS Only
FedRAMP	Moderate ATO, High[1] *equivalency*		High[1] *equivalency*	
DFARS 252.204-7012	No	Yes	Yes	Yes
FCI + CMMC L1	Yes	Yes	Yes	Yes
CUI / CDI + CMMC L2-3	No	Yes^	Yes	Yes
ITAR / EAR	No	No	Yes	Yes
DoD CC SRG Level	N/A	IL2 PA	IL4[2]	IL5 PA
NIST SP 800-53 / 171 [3]	Yes	Yes	Yes	Yes
CJIS Agreement	No	State	Federal	No
NERC / FERC	No	Yes^	Yes	Yes
Customer Support	Worldwide / Commercial Personnel		US-Based / Restricted Personnel	
Directory / Network	Azure Public “Commercial”		Azure Government	
			US Sovereign Cloud	

[1] *Equivalency*, 3PAO SAR for High Impact Level; Supports accreditation at noted impact level

[2] *Equivalency*, PA issued for DoD only

[3] Organizational Defined Values (ODV's) will vary

^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

Cloud Service offering differentiation - Azure

Public Sector Blog

	Azure Public "Commercial"	Azure Government "US Sovereign Cloud"
Customer Eligibility	Any customer	Federal, DoD, SLG, Eligible Contractors (DIB, FFRDC, UARC)
Datacenter Locations	US & OCONUS	CONUS Only
FedRAMP	High PA	High PA
DFARS 252.204-7012	Yes	Yes
FCI + CMMC L1	Yes	Yes
CUI / CDI + CMMC L2-3	Yes^	Yes
ITAR / EAR	No	Yes
DoD CC SRG Level	IL2 PA	IL2, IL4 & IL5 PAs
NIST SP 800-53 / 171 [1]	Yes	Yes
CJIS Agreement	No	Yes
NERC / FERC	No	Yes
Customer Support	Worldwide / Commercial Personnel	US-Based / Restricted Personnel
Directory / Network	Worldwide	CONUS Only

[1] Organizational Defined Values (ODV's) will vary

^ CUI Specified (*e.g., ITAR, Nuclear, etc.*) not suitable REQS US Sovereignty

PA = Provisional Authorization / Provisional ATO

MICROSOFT CMMC

Acceleration

Microsoft CMMC Acceleration Update - March 2024

Reciprocity & Inheritance

Microsoft Product Placemat for CMMC

CMMC Technical Reference Guide

Microsoft Sentinel: CMMC 2.0 Solution

STIG Templates & STIG Automation & STIG with Intune

M365 Compliance Manager CMMC Assessment Templates

Defender for Cloud: Azure CMMC Policy

Azure Mission Landing Zone

Cloud Adoption Framework (CAF) Azure Landing Zone

Zero Trust Architecture

Microsoft Cybersecurity Reference Architecture

Entra Security Defaults

⬛ = No change   🟦 = Updated   🟩 = New

Microsoft Product Placemat for CMMC

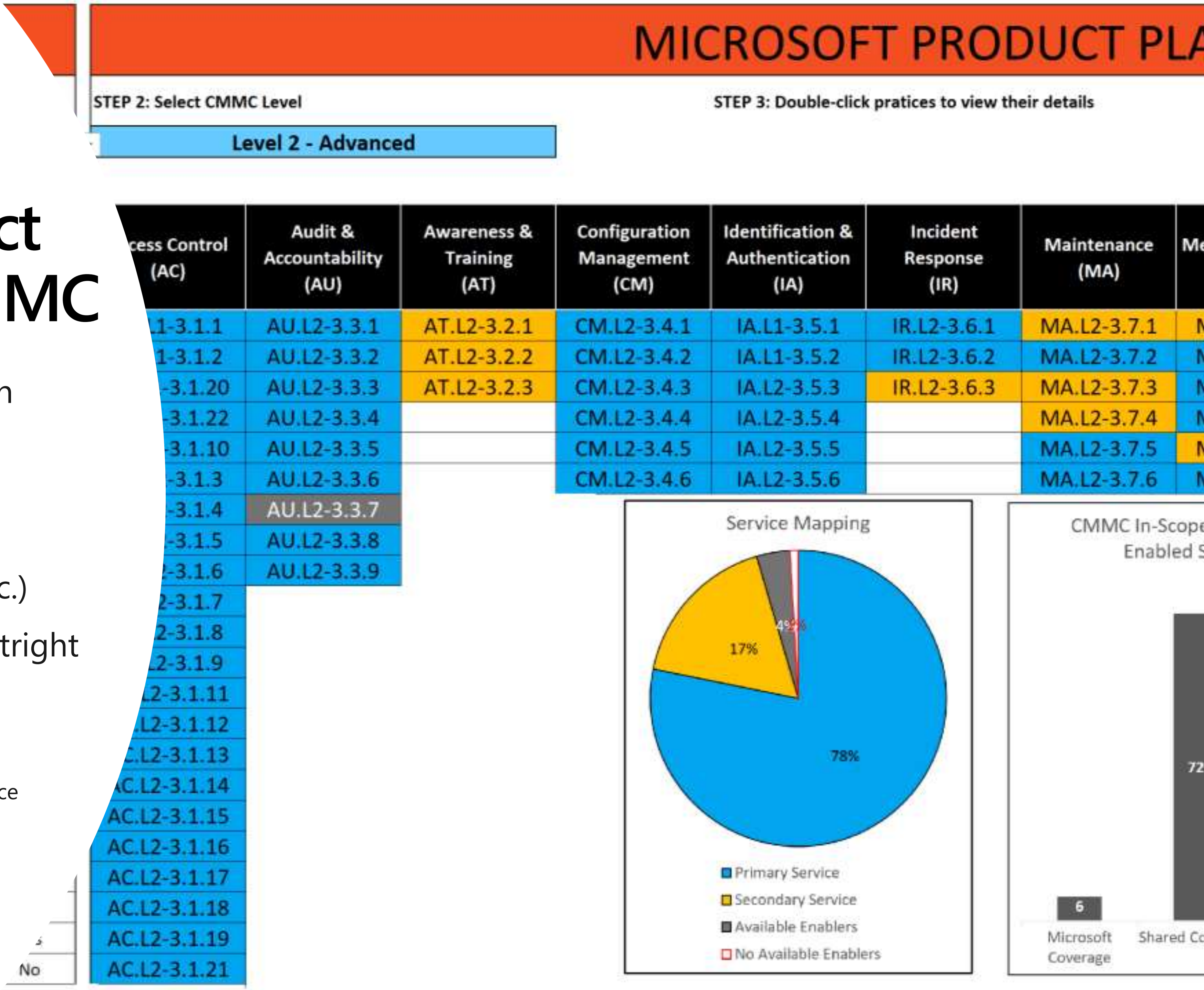
Illustrates CMMC Practices with Microsoft product coverage

Interactive with drill down of implementation statements

Select based on SKU (E5, E3, etc.)

M365 E5 covers 6 practices outright and 72 have Shared Coverage

Shared Coverage means that the customer is required to implement and configure the practice to the standard for your tenant.



MICROSOFT PRODUCT PLA

STEP 2: Select CMMC Level

Level 2 - Advanced

STEP 3: Double-click pratices to view their details

cess Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Me
1-3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	M
1-3.1.2	AU.L2-3.3.2	AT.L2-3.2.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	M
-3.1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	M
-3.1.22	AU.L2-3.3.4		CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4	M
-3.1.10	AU.L2-3.3.5		CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5	M
-3.1.3	AU.L2-3.3.6		CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	M
-3.1.4	AU.L2-3.3.7						
-3.1.5	AU.L2-3.3.8						
2-3.1.6	AU.L2-3.3.9						
2-3.1.7							
2-3.1.8							
2-3.1.9							
L2-3.1.11							
L2-3.1.12							
C.L2-3.1.13							
AC.L2-3.1.14							
AC.L2-3.1.15							
AC.L2-3.1.16							
AC.L2-3.1.17							
AC.L2-3.1.18							
AC.L2-3.1.19							
AC.L2-3.1.21							

No

Microsoft Product Placemat for CMMC

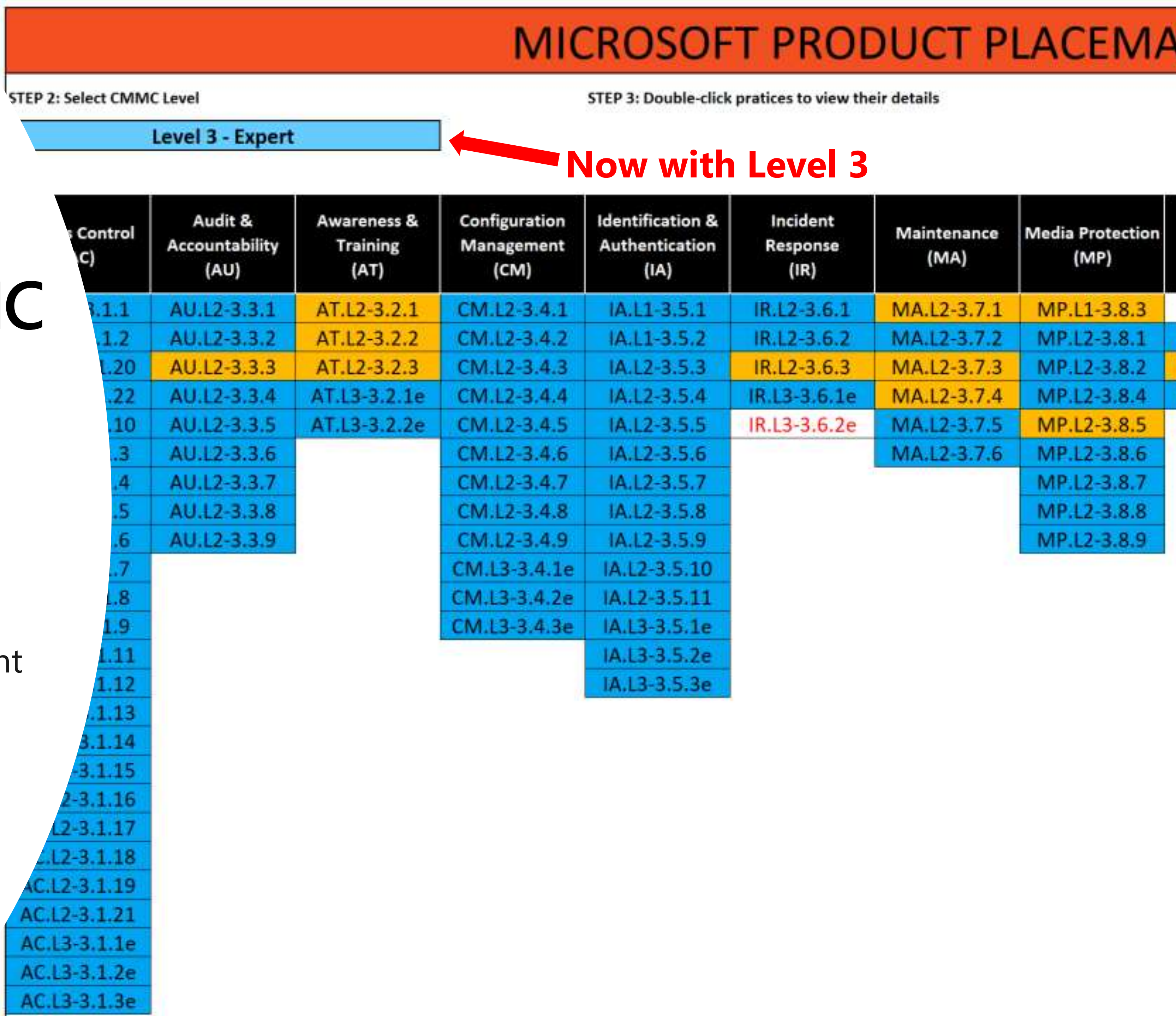
Illustrates CMMC Practices with Microsoft product coverage

Interactive with drill down of implementation statements

Select based on SKU (E5, E3, etc.)

M365 E5 covers 6 practices outright and 72 have Shared Coverage

Shared Coverage means that the customer is required to implement and configure the practice to the standard for your tenant.



MICROSOFT PRODUCT PLACEMA

STEP 2: Select CMMC Level

STEP 3: Double-click pratices to view their details

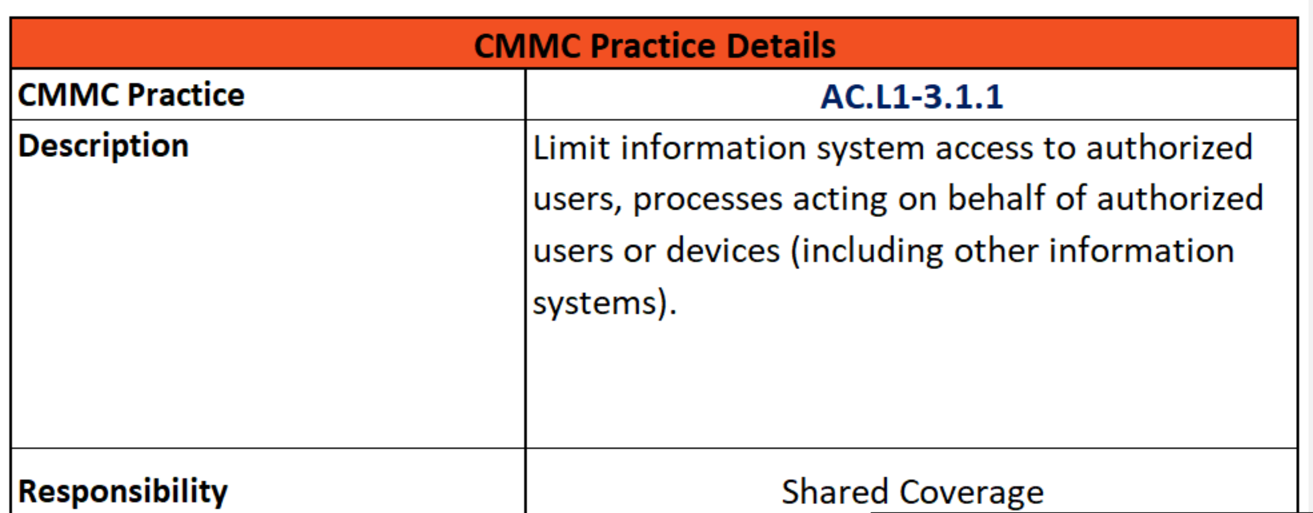
Level 3 - Expert

Now with Level 3

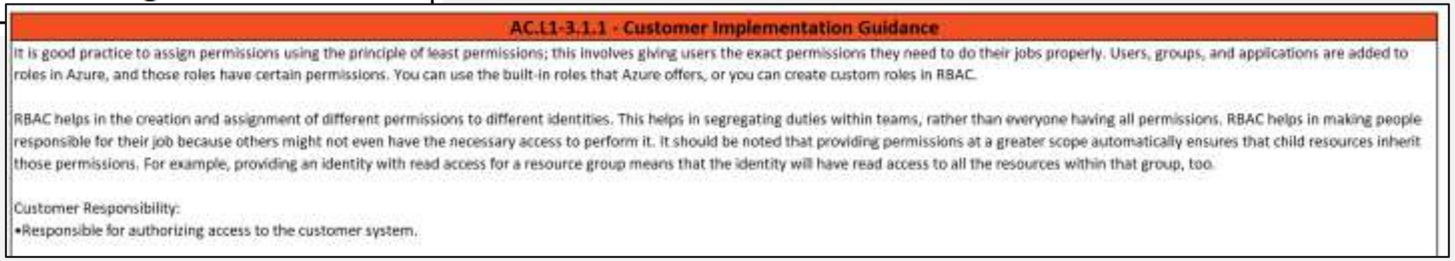
Control C)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)
3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L1-3.8.3
.1.2	AU.L2-3.3.2	AT.L2-3.2.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.1
1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2
.22	AU.L2-3.3.4	AT.L3-3.2.1e	CM.L2-3.4.4	IA.L2-3.5.4	IR.L3-3.6.1e	MA.L2-3.7.4	MP.L2-3.8.4
.10	AU.L2-3.3.5	AT.L3-3.2.2e	CM.L2-3.4.5	IA.L2-3.5.5	IR.L3-3.6.2e	MA.L2-3.7.5	MP.L2-3.8.5
.3	AU.L2-3.3.6		CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	MP.L2-3.8.6
.4	AU.L2-3.3.7		CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7
.5	AU.L2-3.3.8		CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8
.6	AU.L2-3.3.9		CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9
.7			CM.L3-3.4.1e	IA.L2-3.5.10			
1.8			CM.L3-3.4.2e	IA.L2-3.5.11			
1.9			CM.L3-3.4.3e	IA.L3-3.5.1e			
1.11				IA.L3-3.5.2e			
1.12				IA.L3-3.5.3e			
.1.13							
3.1.14							
-3.1.15							
2-3.1.16							
L2-3.1.17							
.L2-3.1.18							
AC.L2-3.1.19							
AC.L2-3.1.21							
AC.L3-3.1.1e							
AC.L3-3.1.2e							
AC.L3-3.1.3e							

Product Placemat Implementation Guidance

Drill down on specific practices for general implementation guidance



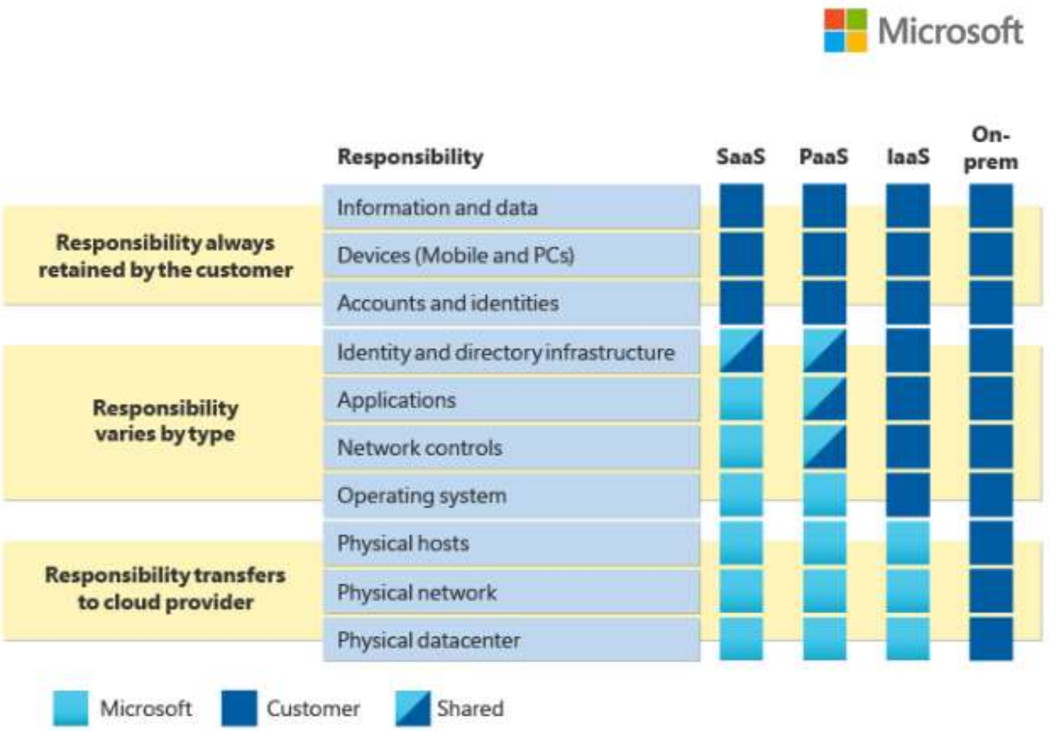
CMMC Practice Details	
CMMC Practice	AC.L1-3.1.1
Description	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).
Responsibility	Shared Coverage



AC.L1-3.1.1 - Customer Implementation Guidance
It is good practice to assign permissions using the principle of least permissions; this involves giving users the exact permissions they need to do their jobs properly. Users, groups, and applications are added to roles in Azure, and those roles have certain permissions. You can use the built-in roles that Azure offers, or you can create custom roles in RBAC. RBAC helps in the creation and assignment of different permissions to different identities. This helps in segregating duties within teams, rather than everyone having all permissions. RBAC helps in making people responsible for their job because others might not even have the necessary access to perform it. It should be noted that providing permissions at a greater scope automatically ensures that child resources inherit those permissions. For example, providing an identity with read access for a resource group means that the identity will have read access to all the resources within that group, too. Customer Responsibility: •Responsible for authorizing access to the customer system.

Download Today at https://aka.ms/cmmc/productplacemat!

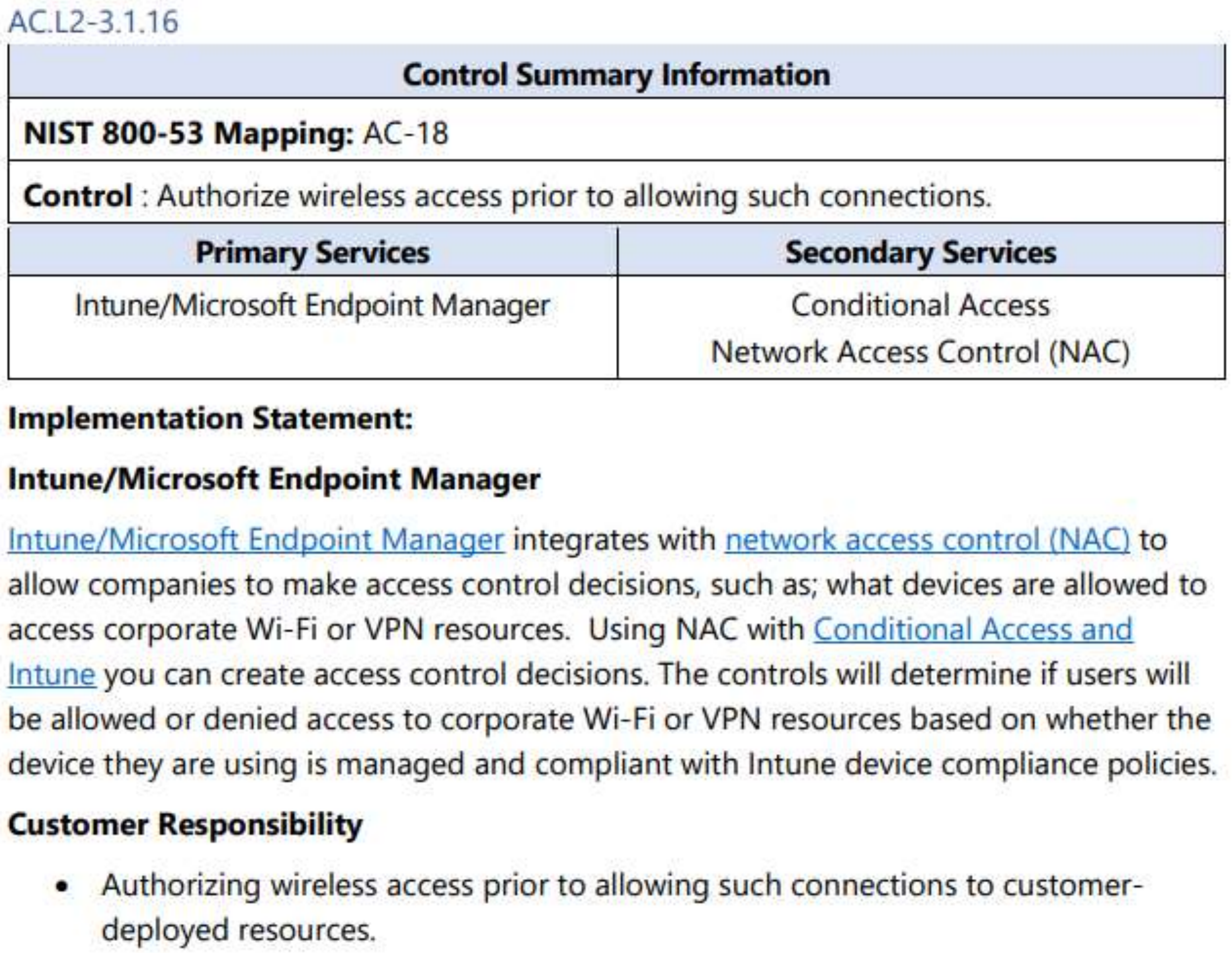
Microsoft Technical Reference Guide for CMMC 2.0



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

https://aka.ms/cmmc/techrefguide



AC.L2-3.1.16

Control Summary Information	
NIST 800-53 Mapping: AC-18	
Control : Authorize wireless access prior to allowing such connections.	
Primary Services	**Secondary Services**
Intune/Microsoft Endpoint Manager	Conditional Access Network Access Control (NAC)

Implementation Statement:

Intune/Microsoft Endpoint Manager

Intune/Microsoft Endpoint Manager integrates with network access control (NAC) to allow companies to make access control decisions, such as; what devices are allowed to access corporate Wi-Fi or VPN resources. Using NAC with Conditional Access and Intune you can create access control decisions. The controls will determine if users will be allowed or denied access to corporate Wi-Fi or VPN resources based on whether the device they are using is managed and compliant with Intune device compliance policies.

Customer Responsibility

- Authorizing wireless access prior to allowing such connections to customer-deployed resources.

Microsoft CMMC Acceleration Partners

Proven

CMMC AB Marketplace Registered Provider Organizations (RPOs)

Partner Network

Certified in the Microsoft Partner Network

Microsoft Gold Partner

- Abacode
- Agile IT
- Applied Information Sciences
- Applied Insight
- archTIS NC Protect
- Ardalyst
- BlueVoyant Conquest Cyber
- C3 Integrated Solutions
- Carahsoft Technology
- CloudFit Software
- CyberSheath
- Daymark Solutions
- Dox Electronics
- E-Share
- Exostar
- Hyperproof
- Insight
- KAMIND IT
- KTL Solutions
- Liftoff
- Microsoft Industry Solutions
- NeoSystems
- Oxford Computer Group
- Peerless
- Planet Technologies
- Pricewaterhouse Coopers
- Protiviti
- Quzara
- Red Level Group
- Sentinel Blue
- Summit 7 Systems

Microsoft AOS-G Partners (How to Buy)

Agile IT

Applied Information Sciences

C3 Integrated Solutions

Carahsoft Technology

CloudFit Software

Conquest Cyber

CyberSheath

Daymark Solutions

Dox Electronics

KAMIND IT

KTL Solutions

Liftoff

NeoSystems

Planet Technologies

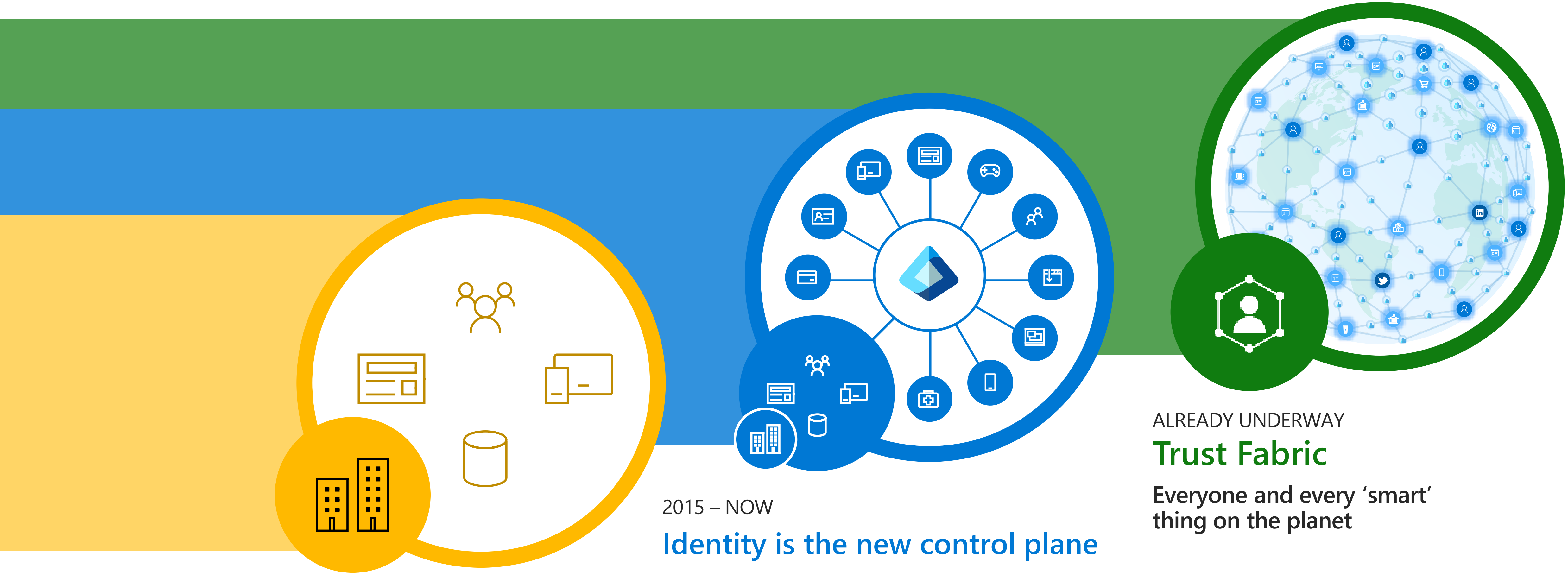
Sentinel Blue

Summit 7 Systems

Microsoft Branding Announcements

- Microsoft Entra - SaaS
- Microsoft Purview – SaaS & PaaS
- Microsoft Defender – SaaS & PaaS
- Microsoft Sentinel - PaaS
- Intune Suite – SaaS
- Viva – SaaS
- Copilot - SaaS

Entra - Updating our vision (*and branding*)



2000 – 2015

Directory services

Only for Microsoft

2015 – NOW

Identity is the new control plane

Enterprises that bet
on the cloud

ALREADY UNDERWAY

Trust Fabric

Everyone and every ‘smart’
thing on the planet

Microsoft Entra

Secure access for a connected world.

Entra ID
Azure Active Directory

+

Microsoft Entra
Permissions Management

+

Microsoft Entra
Verified ID

+

Microsoft Entra
Identity Governance

+

Microsoft Entra
Workload Identities

Protect access to any app or resource

Safeguard your organization by protecting access to every app and every resource for every user.

Secure and verify every identity

Effectively secure every identity including employees, customers, partners, apps, devices, and workloads across every environment.

Provide only necessary access

Discover and right-size permissions, manage access lifecycles, and ensure least privilege access for any identity.

Simplify the experience

Keep your users productive with simple sign-in experiences, intelligent security, and unified administration.

Microsoft Entra

Secure access for a connected world.

Drivers for Trust Fabric

→ **Zero Trust** driving category consolidation including a merge of **networking**, **identity**, and **device management**.

→ Enterprise customers are increasingly using **multi-cloud** + **hybrid** infrastructure strategies.

→ Static policies giving way to **adaptive access** + **identity governance** powered by **machine learning** + **artificial intelligence**.

→ ***Every*** identity (human, workload, device) requires **visibility**, **control**, and a **managed lifecycle**.

→ **Collaboration** regularly extends **beyond** traditional enterprise **boundaries**.

→ Global concern about **surveillance capitalism** and emerging **privacy legislation**.

Investment Areas

Manage and protect apps and resources on-premises and across clouds

Identity Lifecycle Management and Identity Governance

Multicloud permissions management and access governance

Unified Platform and Developer Experience

Enhanced Multitenant Support

Industry-leading Zero Trust security

Verifiable Credentials

Reliability

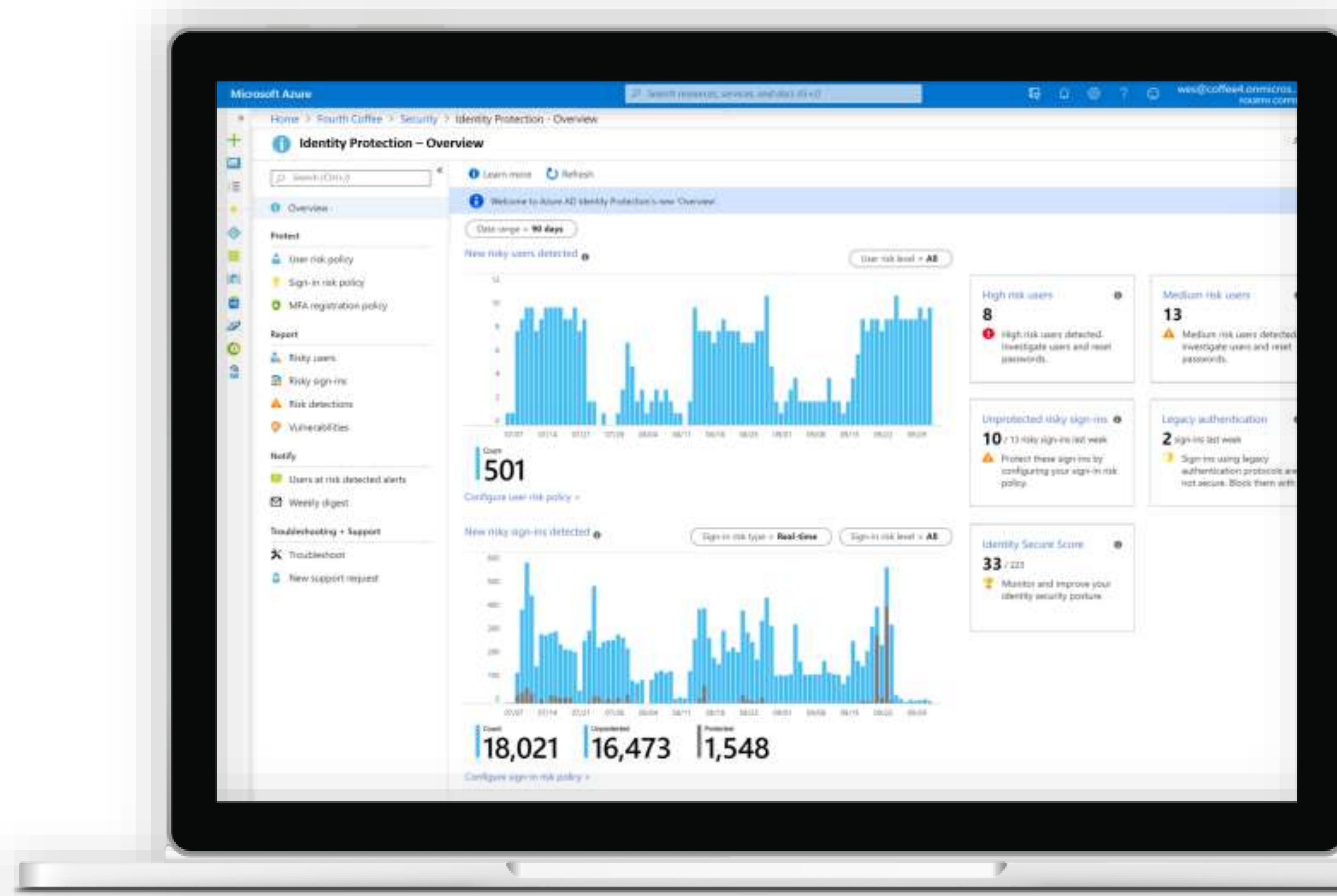
Entra Features Launched

Capability Area	General Availability: Oct – Dec'23	General Availability: Jan – Mar'24
Authentication	• FIDO2 support for native apps on macOS and iOS • SSO and Passwordless authentication for AVD & Windows 365 • Authenticator on Android is FIPS 140 compliant	• Microsoft Entra CBA as Most Recently Used (MRU) method • FIPS 140-3 enterprise compliance for Microsoft Authenticator app on Android
Authorization	• Support for Microsoft admin portals in Conditional Access • Chrome's CloudAPAuthEnabled available for device-based conditional access	• Conditional Access: Filter for applications • Microsoft Defender for Office alerts in Identity Protection • Real-time Entra ID threat intelligence detections • Suspicious API Traffic detection for Users
Administration	• Devices | All Devices blade is available • Windows Local Administrator Password Solution with Microsoft Entra • Windows MAM	• Define Azure custom roles with data actions at Management Group scope • Custom Security Attributes
Governance	• ServiceNow app for Microsoft Entra Permissions Management • Microsoft Entra Cloud Sync now supports ability to enable Exchange Hybrid configuration for Exchange customers • Permissions Analytics Report PDF	
Self – Service Management		
Customer IAM	• Guest Governance – Inactive guest insights	
Logging & Reporting		
Application Access		
Developer Support	• Managed identity soft delete • PIM for Groups API	

Identity protection

Intelligently detect and respond to compromised accounts

- Enhanced logging
- Threat alerts
- Risk scores
- Sign-in reports
- Privileged access insights



Identity Protection – Overview

Welcome to Azure AD Identity Protection's new 'Overview'

High risk users detected. Investigate users and reset passwords.

Medium risk users detected. Investigate users and reset passwords.

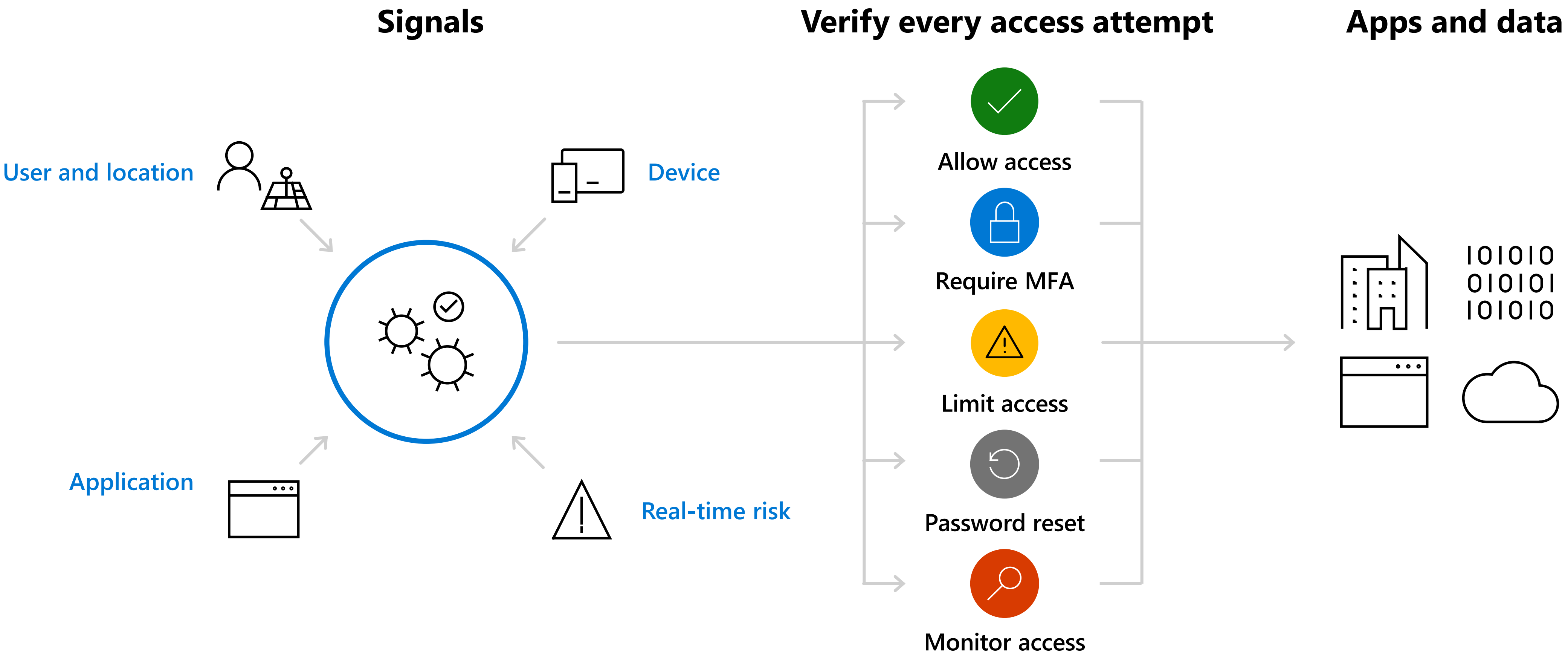
Protect these sign-ins by configuring your sign-in risk policy.

Sign-ins using legacy authentication protocols are not secure. Block them with

Monitor and improve your identity security posture

Protect resources with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



Seamless user experiences

Provides an easy, fast sign in experience to keep your users productive, reduce time managing passwords, and increase end user productivity

Single sign-on (SSO) for
any user type and any app

End user self-service portal to
discover and launch applications,
request access, and manage profile

Convenient, phishing resistant
passwordless credentials

Changing the game with passwordless

Make sign-in even more seamless and secure

Windows Hello

Microsoft Authenticator

FIDO2 Security Keys

Passwordless Momentum **200M+** | **Active passwordless users**

Verified ID

Enable more secure interactions while respecting privacy with an industry-leading global platform.

Fast remote onboarding

Validate identity information for trustworthy self-service enrollment and reduced time-to-hire.

More secure access

Quickly verify an individual's credentials and status to grant least-privilege access with confidence.

Easy account recovery

Replace support calls and security questions with a streamlined self-service process to verify identities.

Custom business solutions

Easily build solutions for a wide range of use cases with our developer kit, APIs, and documentation.

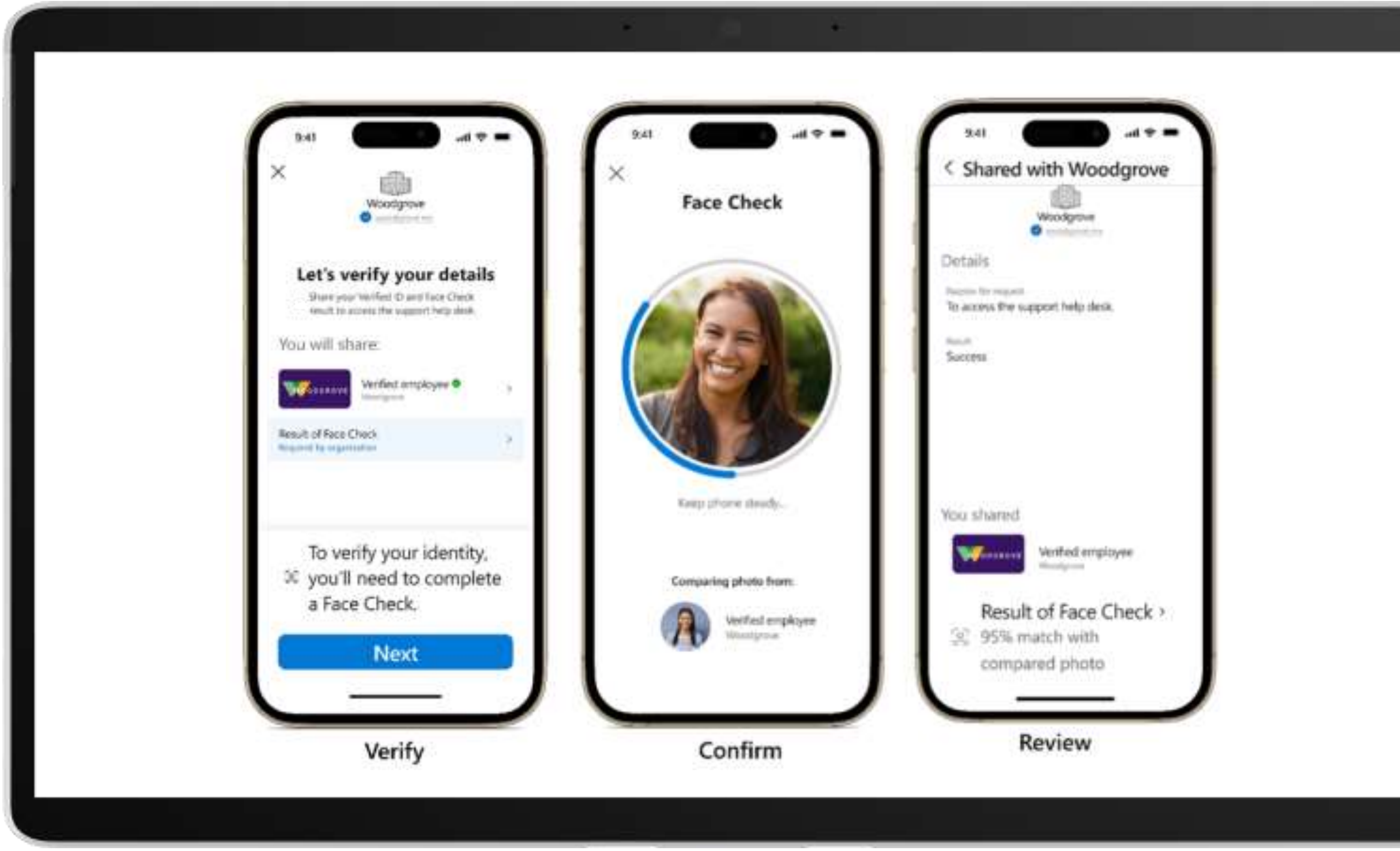
Face Check using Entra Verified ID

A privacy-respecting facial matching feature for high-assurance verifications

PUBLIC PREVIEW

Key Benefits

- Allows enterprises to perform high-assurance verifications securely, simply, and at scale.
- Face Check adds a critical layer of trust by performing facial matching between a user’s real-time selfie and a photo.



Let's verify your details

Share your Verified ID and Face Check result to access the support help desk.

You will share:

Verified employee

Result of Face Check

To verify your identity, you'll need to complete a Face Check.

Next

Face Check

Keep phone steady...

Comparing photo from:

Verified employee

Shared with Woodgrove

Details

To access the support help desk

Success

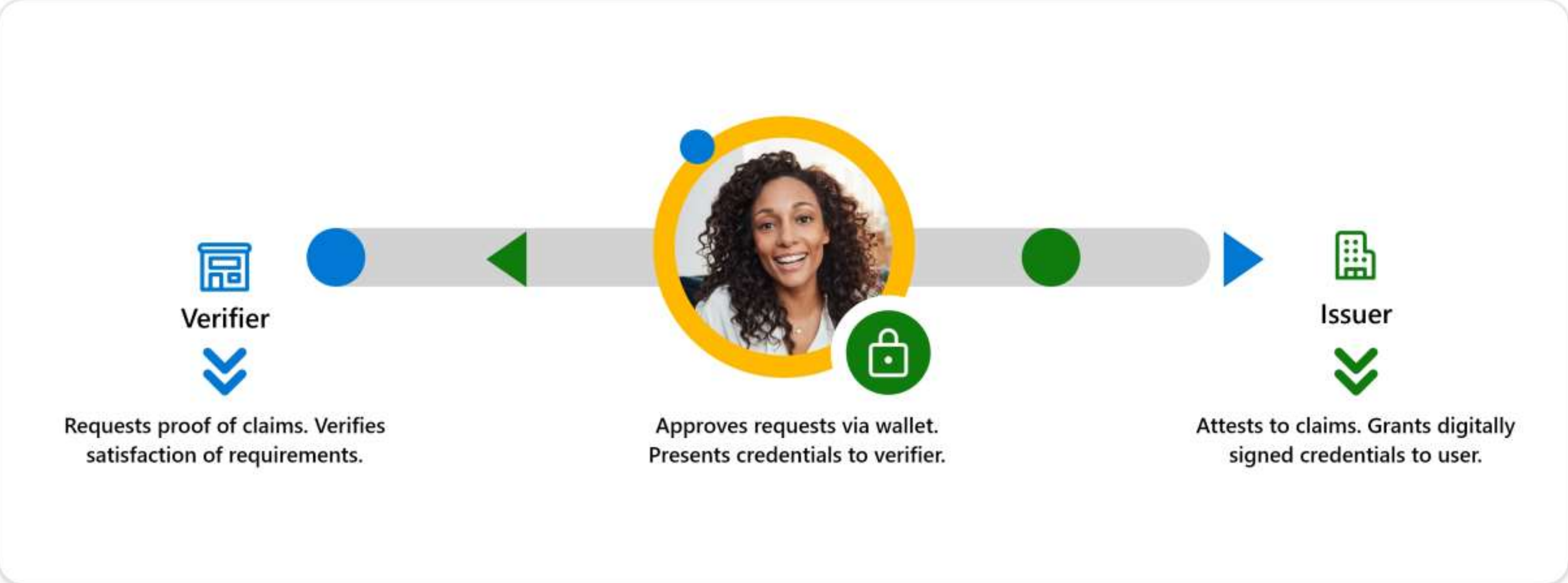
You shared

Verified employee

Result of Face Check

95% match with compared photo

How verifiable credentials works

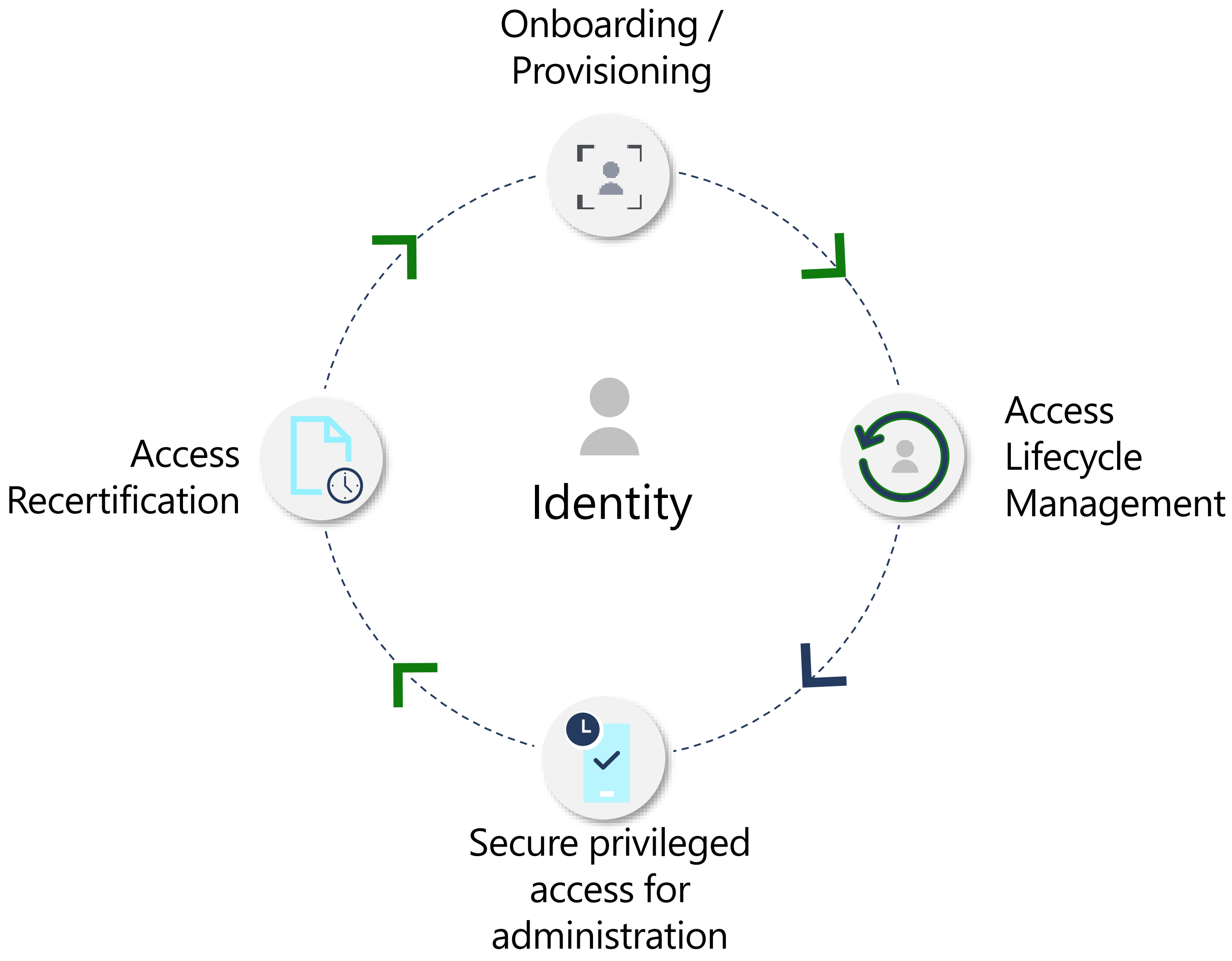


Requests proof of claims. Verifies satisfaction of requirements.

Approves requests via wallet. Presents credentials to verifier.

Attests to claims. Grants digitally signed credentials to user.

What is Microsoft Entra Identity Governance?


Onboarding / Provisioning
Access Lifecycle Management
Secure privileged access for administration
Access Recertification
Identity

01

Who has/should have access to which resources?

02

What are they doing with that access?

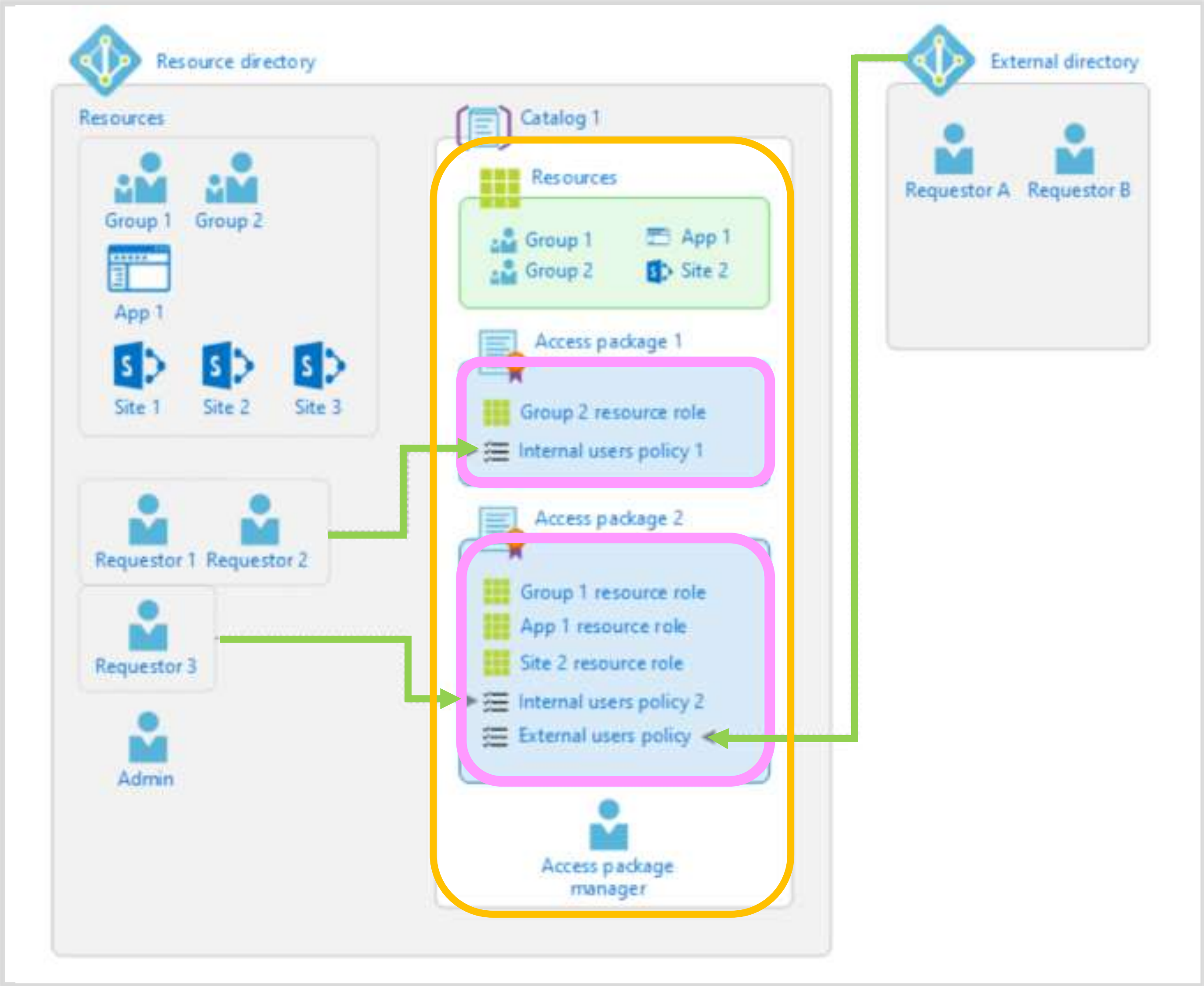
03

Are there effective organizational controls for managing access?

04

Can auditors verify that the controls are working?

What is Entitlement Management?



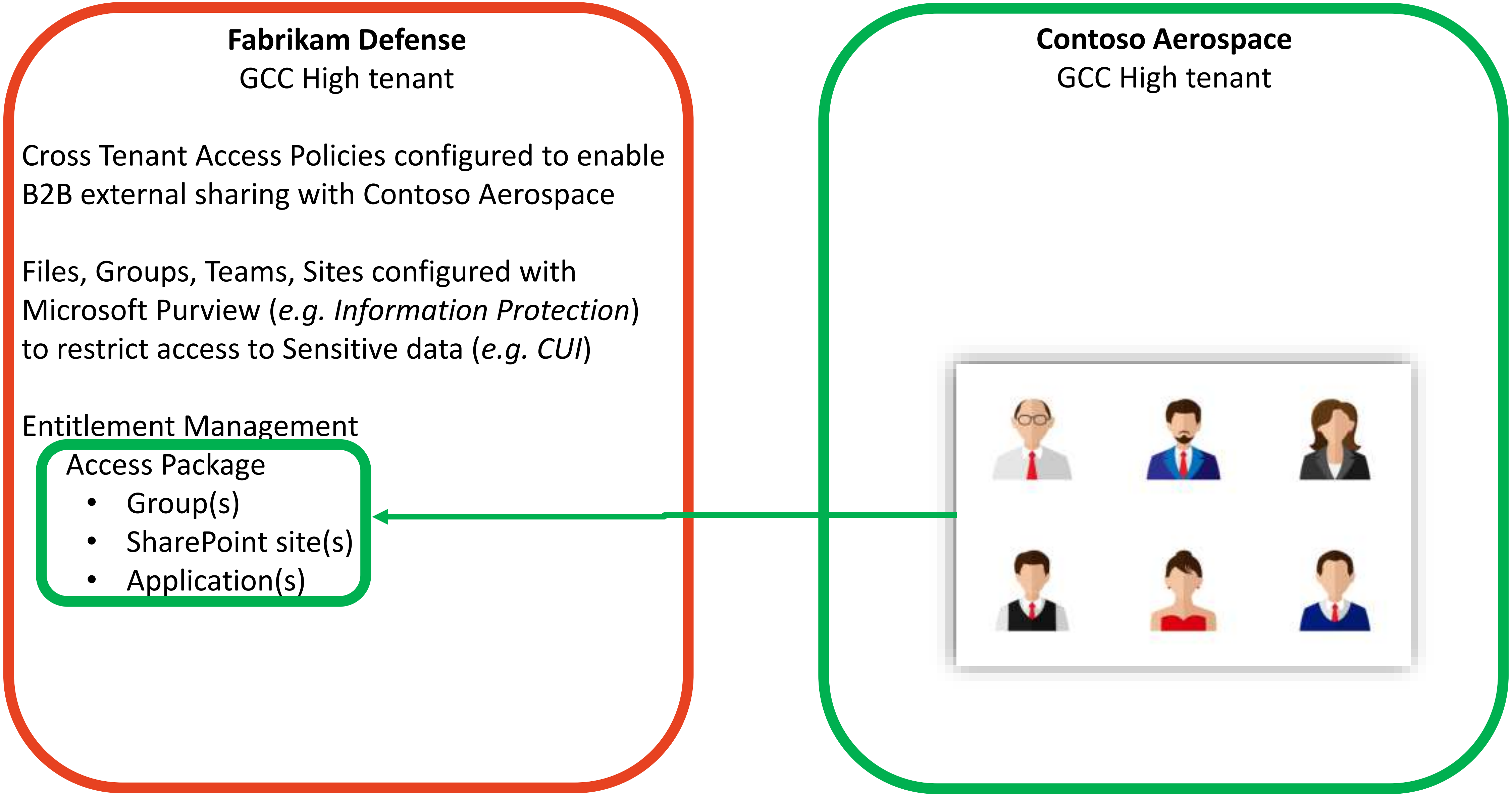
- **Packages**: Bundles of all the resources a user needs to work on a project or perform their work tasks

- **Policies**: define the rules/guardrails for assignment to a package
  - Request: How one *gets* an assignment
  - Lifecycle: What happens with their assignment once they have it

- An access package can have one or more policies linked to it. Each policy defines the access rules for a unique set of users *i.e. certain department, partner org, etc*

- **Catalogs**: Resource sandboxes for delegating entitlement management

GCC High & Commercial customer / partner



Fabrikam Defense
GCC High tenant

Cross Tenant Access Policies configured to enable B2B external sharing with Contoso Aerospace

Files, Groups, Teams, Sites configured with Microsoft Purview (*e.g. Information Protection*) to restrict access to Sensitive data (*e.g. CUI*)

Entitlement Management

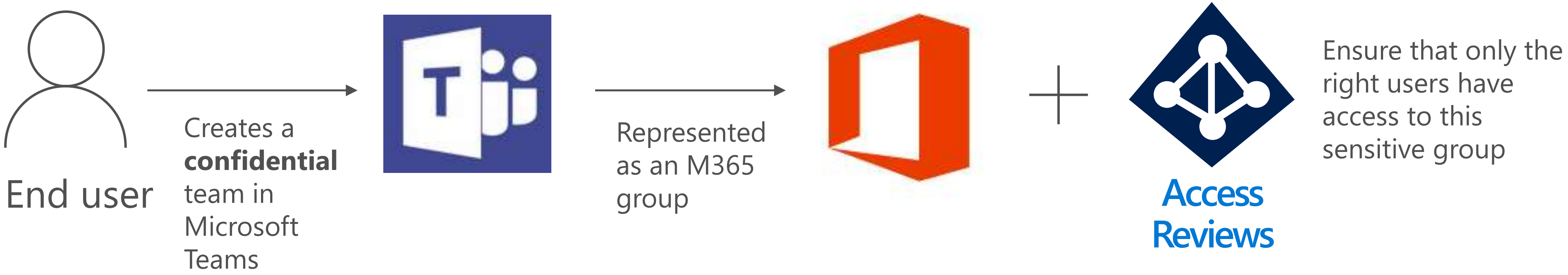
Access Package

- Group(s)
- SharePoint site(s)
- Application(s)

Contoso Aerospace
GCC High tenant

Entitlement Management - Access Reviews

1. Govern access to Microsoft Teams and M365 Groups



End user

Creates a **confidential** team in Microsoft Teams

Represented as an M365 group

Access Reviews

Ensure that only the right users have access to this sensitive group

Entitlement Management - Access Reviews

2. Govern access to critical applications

Who has access to your sensitive applications?

Is their access being periodically reviewed?

Microsoft Collaboration Framework

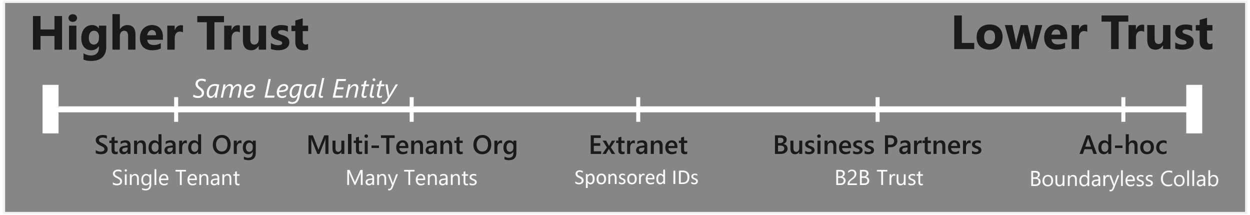
Cross Tenant Access Policies (XTAP) govern all Tenant-to-Tenant (T2T) interactions ***to*** *my tenant* and ***from*** *my tenant*

- Allow/Block **Access** to apps and data
- Allow Native **Federation** between tenants and globally
- Accept/Force **Multi-Factor Authentication**
- Accept **Compliant Device** across tenant boundaries
- Office: Allow **Global Address List** (GAL) visibility and access
- Office: Allow People/Data **Moves** between tenant

Preventative controls - prevent users from inadvertently being assigned access or requesting access to resources

Run-time checks requiring users to explicitly activate high-privileged roles needed for critical tasks like accessing CUI or stopping a production VM, combined with Conditional Access Policies and Defender to ensure those actions are monitored

After-the-fact detective controls with access reviews, Microsoft Sentinel and Defender with auditing/reporting



Higher Trust **Lower Trust**

Same Legal Entity

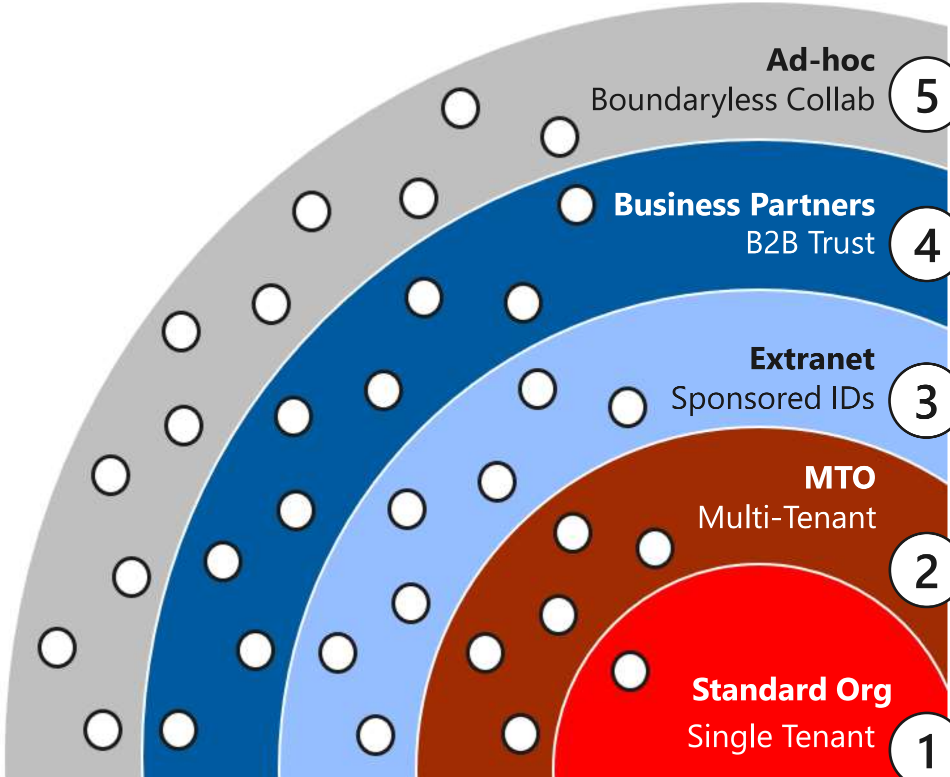
Standard Org
Single Tenant

Multi-Tenant Org
Many Tenants

Extranet
Sponsored IDs

Business Partners
B2B Trust

Ad-hoc
Boundaryless Collab



Ad-hoc
Boundaryless Collab
5

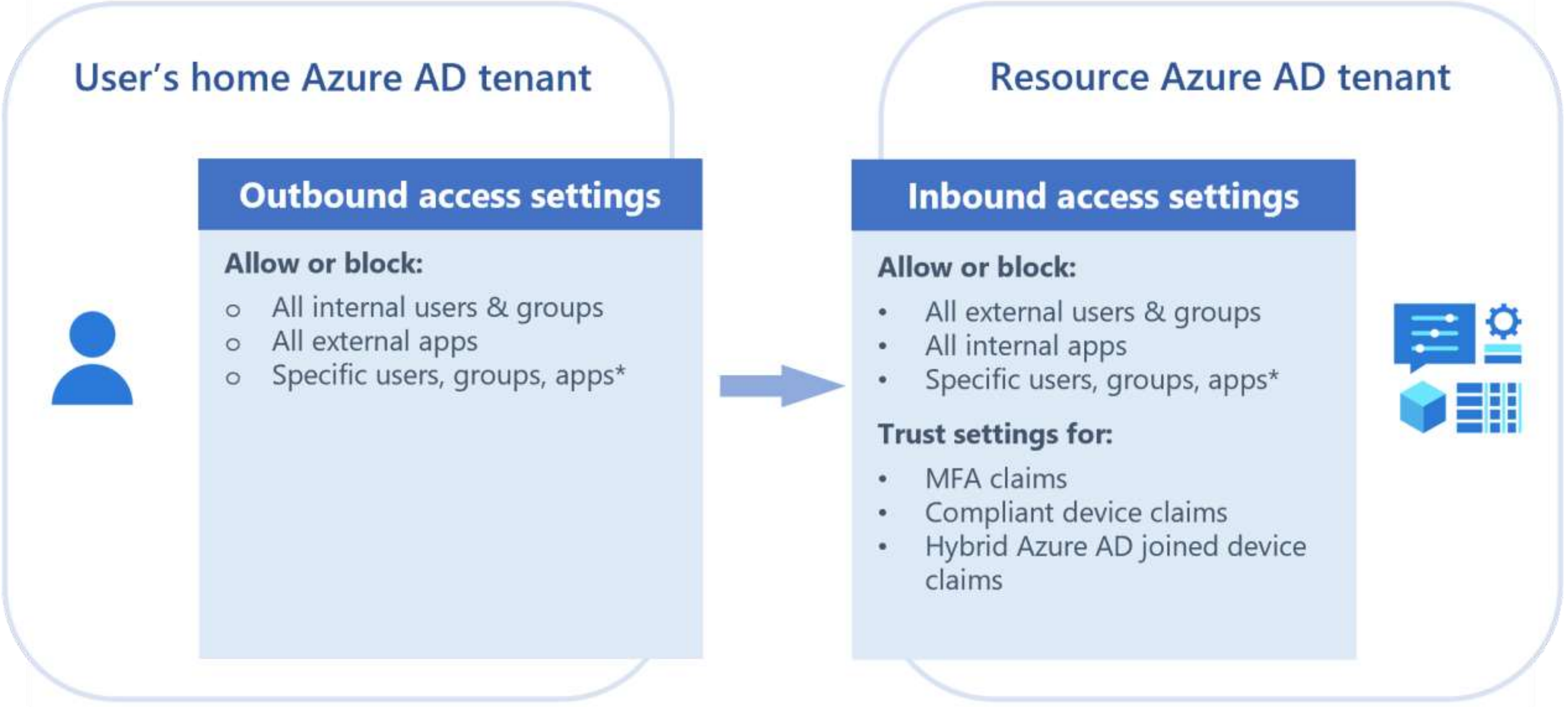
Business Partners
B2B Trust
4

Extranet
Sponsored IDs
3

MTO
Multi-Tenant
2

Standard Org
Single Tenant
1

Cross-tenant access settings for B2B collaboration



User's home Azure AD tenant

Outbound access settings

Allow or block:

- All internal users & groups
- All external apps
- Specific users, groups, apps*

Resource Azure AD tenant

Inbound access settings

Allow or block:

- All external users & groups
- All internal apps
- Specific users, groups, apps*

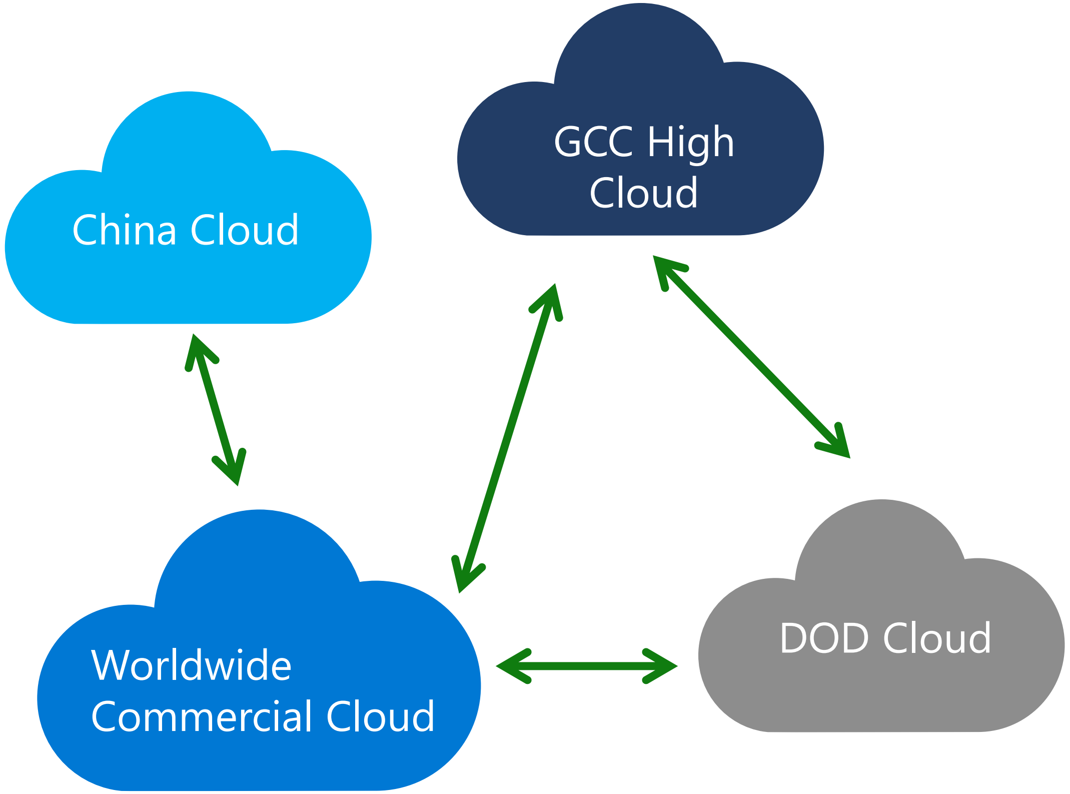
Trust settings for:

- MFA claims
- Compliant device claims
- Hybrid Azure AD joined device claims

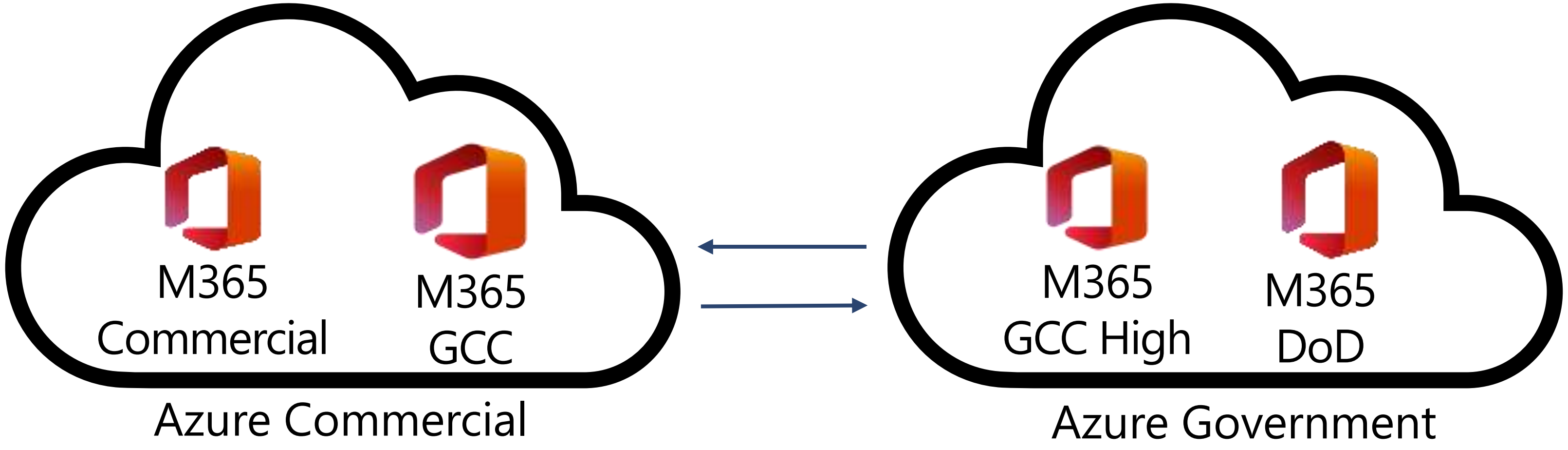
* To apply settings to specific users, groups, or apps, Azure AD Premium P1 is required

Cross Cloud Collaboration

- Cloud to cloud supported patterns
- Using B2B external access for cross cloud collaboration
- Controls for managing cross cloud with Cross Tenant Access Policies



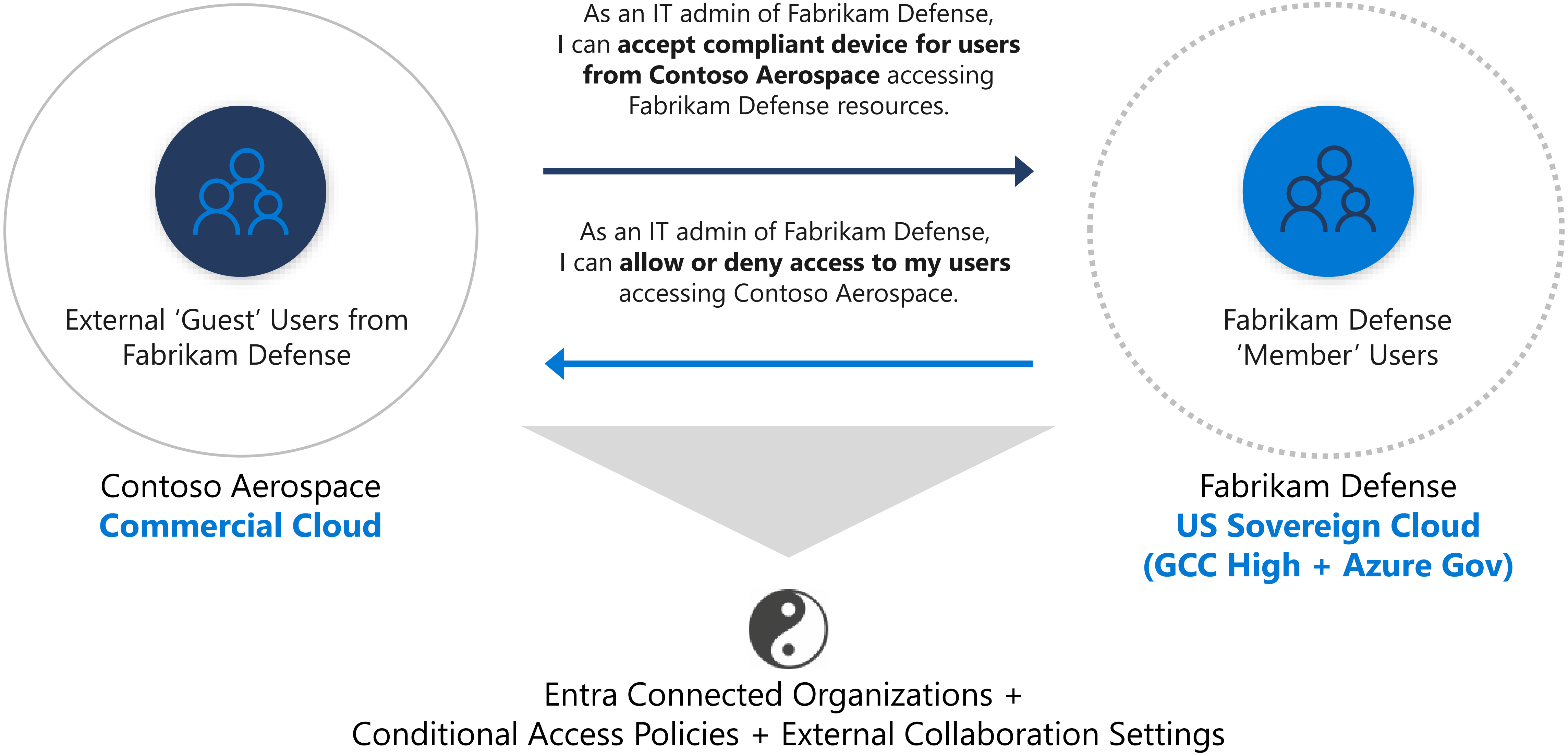
Collaborate across Microsoft clouds



Uses the current Microsoft Entra External ID solution that customers use today.

By default, collaboration with other clouds is not enabled, customers must enable this before invitations to a user from another cloud

B2B Core Scenarios for Cross Cloud Collaboration



As an IT admin of Fabrikam Defense,
I can **accept compliant device for users from Contoso Aerospace** accessing Fabrikam Defense resources.

As an IT admin of Fabrikam Defense,
I can **allow or deny access to my users** accessing Contoso Aerospace.

External ‘Guest’ Users from Fabrikam Defense

Contoso Aerospace
Commercial Cloud

Fabrikam Defense ‘Member’ Users

Fabrikam Defense
US Sovereign Cloud (GCC High + Azure Gov)

Entra Connected Organizations +
Conditional Access Policies + External Collaboration Settings

Office 365 collaboration modalities

Classic Collaboration

Same Cloud and Cross-Cloud Today

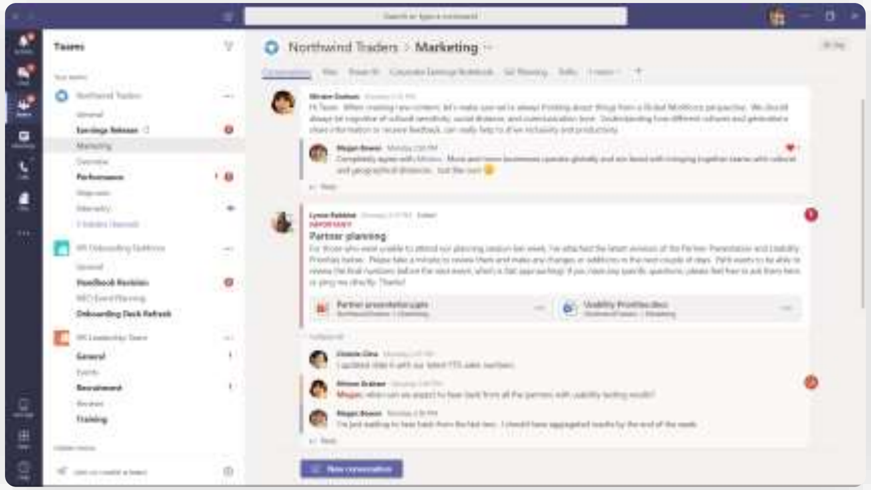
- Teams Meetings (audio and video) – *Anyone (web & client*)*
- Teams 1:1 Chat, VoIP & Video calls – *Federation*
- Teams Presence - *Federation*
- File sharing & coauthoring with any user from any cloud using only their email – *SharePoint & OneDrive One Time Passcode*
- See calendar availability – *Calendar Free/Busy*

*cross cloud anonymous meeting join via the Teams client available now.

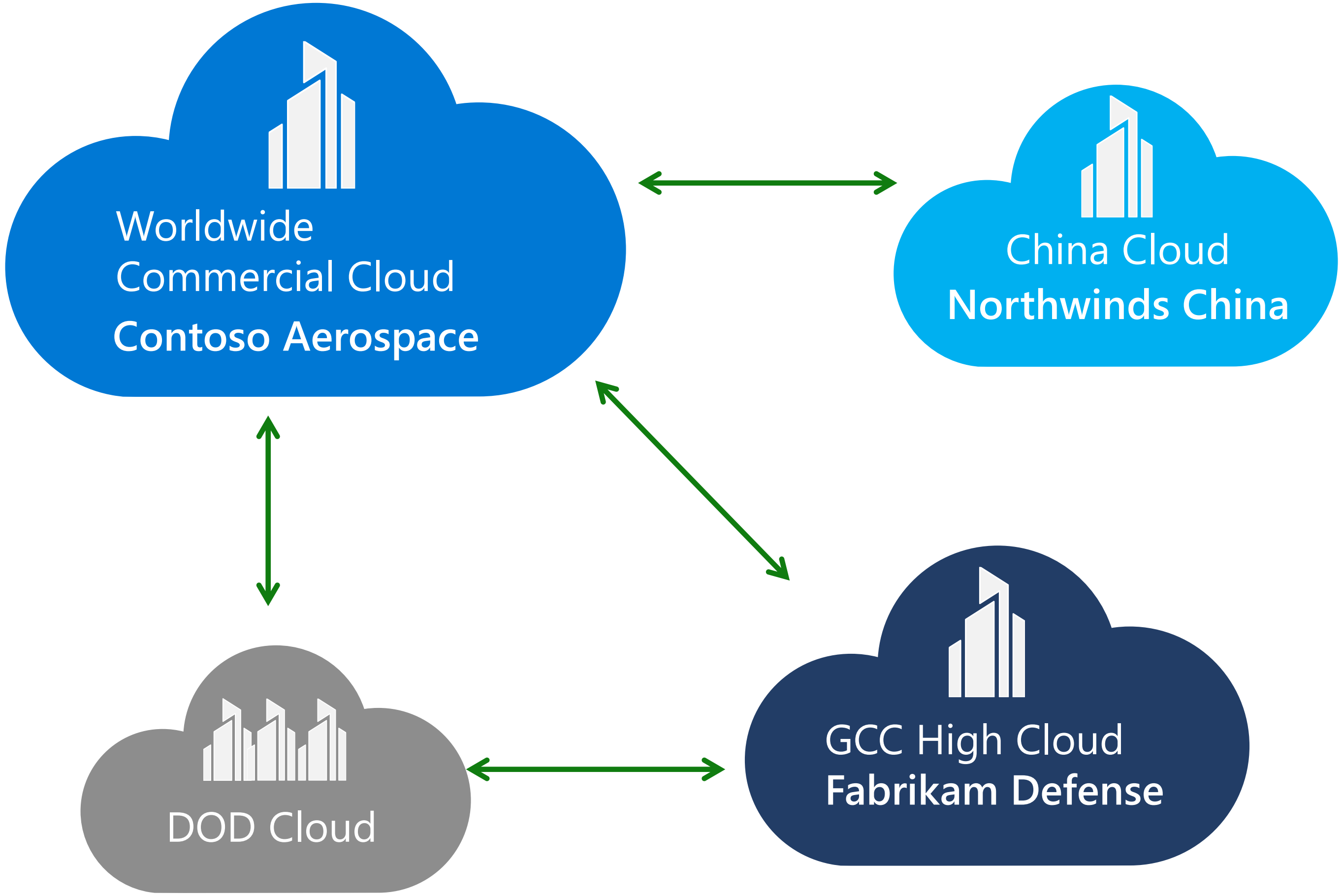
Rich Collaboration

Same Cloud & Cross-Cloud supported today!

- Entra ID authenticated application access - Guest User Access
- SharePoint & OneDrive – Guest User Access
- Teams groups & channels - Guest User Access
- Teams meetings identity attestation - Guest User Access
- Teams meeting recording access - Guest User Access



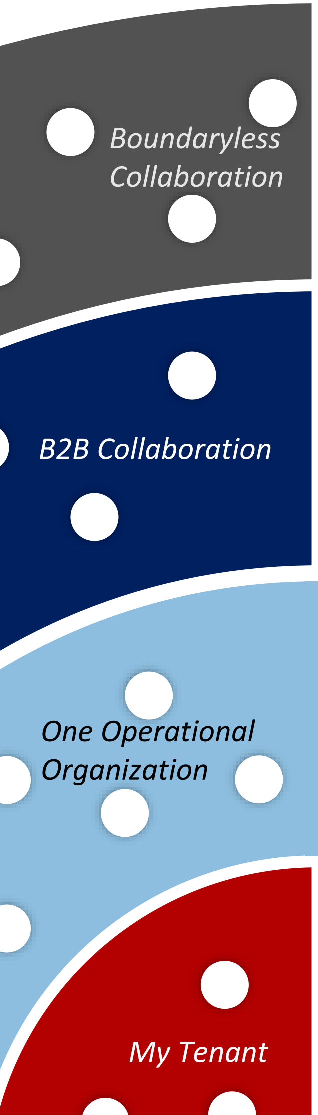
Organization to Organization



Collaboration:

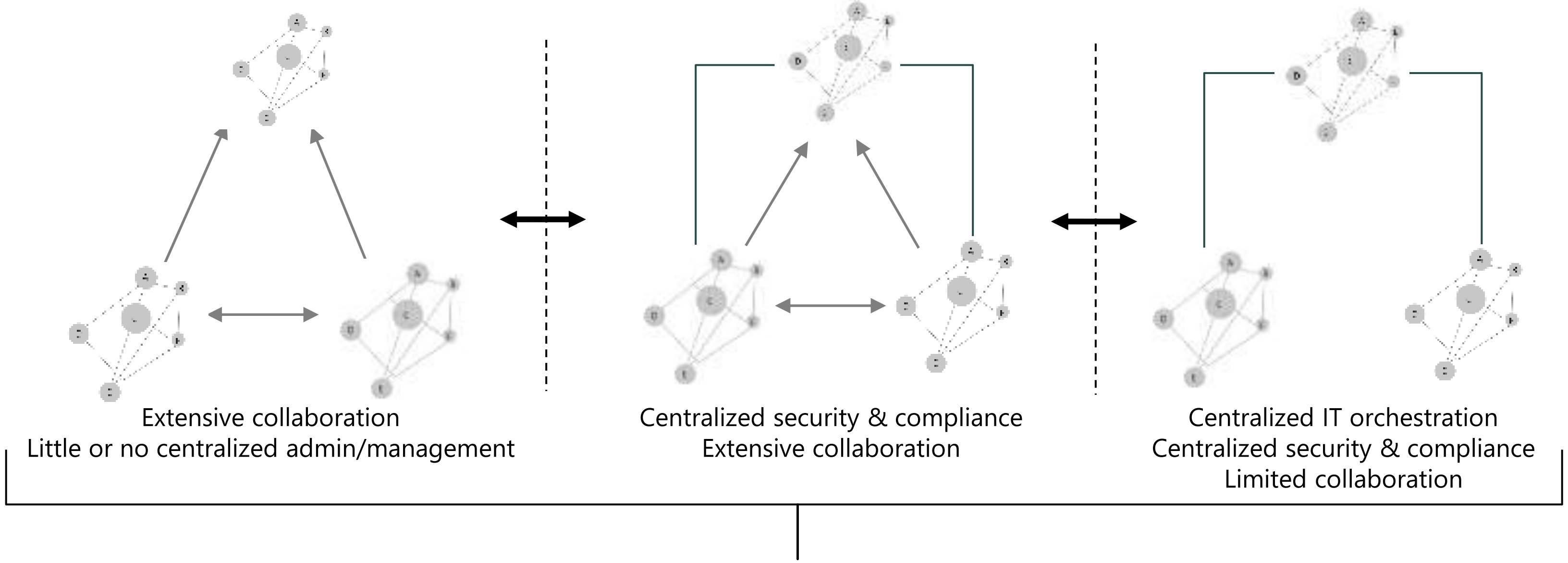
- **Teams**
    - Files/Chat…
    - 1:1 Chat
    - Meetings
    - Groups
- **Exchange**
    - Calendaring (FB)
    - Secure Email
- **SharePoint/OneDrive**
    - Sharing
    - Co-editing
- **SSO** for Applications that use Entra ID as Identity Provider

Enterprise Collaboration Rings of Trust



M365 Ecosystem

Business Partners



Extensive collaboration
Little or no centralized admin/management

Centralized security & compliance
Extensive collaboration

Centralized IT orchestration
Centralized security & compliance
Limited collaboration

Multitenant Organization

- A single organization with multiple tenants where administration is distributed but there are centralized policies and settings requirements
- Many self-managed tenants with common resources and a need to collaborate among tenants
- Single administrative group managing multiple tenants

Tenant

Experiences Optimized for MTO

	Feature	Multi-tenant experience
Workforce Collaboration	People search & people card	Search for people across tenants using Outlook, Teams, ODSP, and Viva/Yammer, and see a single contact View rich profile, contact and presence information on people cards across tenants Open people cards across tenants and view org charts
	Calling, chatting, meetings	Same chat experience for single and multi tenant organizations (single chat thread) Place calls to contacts in other tenants without tenant switching. Receive calls and meeting notifications from other tenants without tenant switching
	File, folder & site sharing	Share any file/folder or site with a user or group across the multi-tenant organization Share any file/folder or site with the entire multi-tenant organization without naming specific users or groups.
	Communication	Leaders in MTO organizations can reach employees across multiple tenants
Administration	Infrastructure	IT admins can define and create an MTO tenant group IT admins can provision users and groups across the MTO at scale with full lifecycle management
	Security	Security personas can get aggregated visibility & control over their connected tenants in the Security Operations Center
	T2T Migration	Tenant Admins can move user data (Exchange, ODB and private chats) as well as shared content (Teams and SharePoint sites) at scale between tenants to support M&A activities and/or Tenant consolidation

MTO Collaboration Public Preview

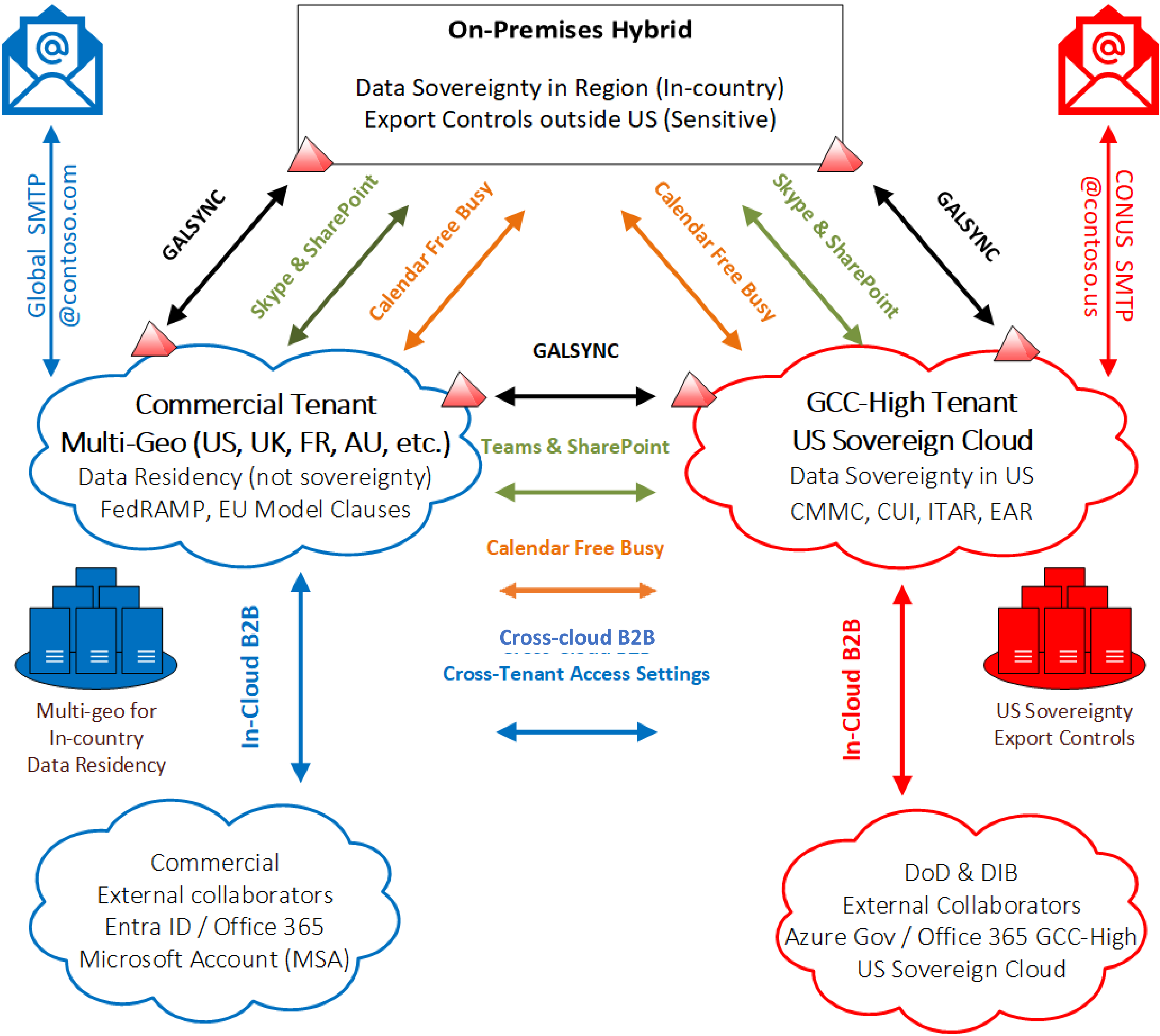
Announced August 28, 2023

1. Seamless people search across tenants (Universal GAL)
   - Users can search by name for colleagues across MTO orgs.
   - Users will not see duplicate results (B2B and native) for their colleagues across MTO orgs.
2. Single native chats (no duplicated B2B chats)
   - Users can establish native chats with colleagues across MTO orgs without the need to do tenant switch.
   - Users can easily navigate from existing in tenant B2B chats to native chats for collaboration.
3. Cross tenant calling and call notifications.
4. Cross tenant meeting join, and meeting start notifications.
   - Users can join meetings/calls bypassing the lobby (authenticated).
   - Users can access meeting artifacts like white board and meeting recordings.
5. Document collaboration in ODSP
   - Co-authoring and sharing documents with individual users and with MTO group.
6. Tenant admin capabilities
   - Simple UI in MAC to setup and view MTO policy and group.

Collaborative Experience in a multi-tenant model

H2 CY 2023 (Future State)

- ✓ In-Cloud B2B and Cross Tenant Access Policies for bi-directional sharing scenarios across GCC High & DoD
- ✓ Cross-Cloud B2B Generally Available for bi-directional sharing scenarios across Commercial, GCC High & DoD
  - ✓ Cross Tenant Access Policies
  - ✓ Document Sharing with SharePoint Online, OneDrive for Business & Teams with external sharing features to Guest accounts
  - ✓ Web application sharing Cross-Sovereign Cloud scenarios
  - ✓ Teams anonymous meeting join
  - ✓ Microsoft Information Protection Encryption
  - ✓ Teams authenticated meeting join (Preview)
  - ✓ Teams Channel Guest Access (Preview)
- ✓ Exchange Free/Busy Calendar Sharing is bi-directional
- ✓ Teams meeting cross-cloud (web)
- ✓ Document Sharing via SharePoint Online & OneDrive for Business with Email + Passcode Verification
- ✓ Microsoft Information Protection & Office Message Encryption (OME) encryption works Cross-Cloud



On-Premises Hybrid

Data Sovereignty in Region (In-country)
Export Controls outside US (Sensitive)

Commercial Tenant
Multi-Geo (US, UK, FR, AU, etc.)
Data Residency (not sovereignty)
FedRAMP, EU Model Clauses

GCC-High Tenant
US Sovereign Cloud
Data Sovereignty in US
CMMC, CUI, ITAR, EAR

Multi-geo for
In-country
Data Residency

US Sovereignty
Export Controls

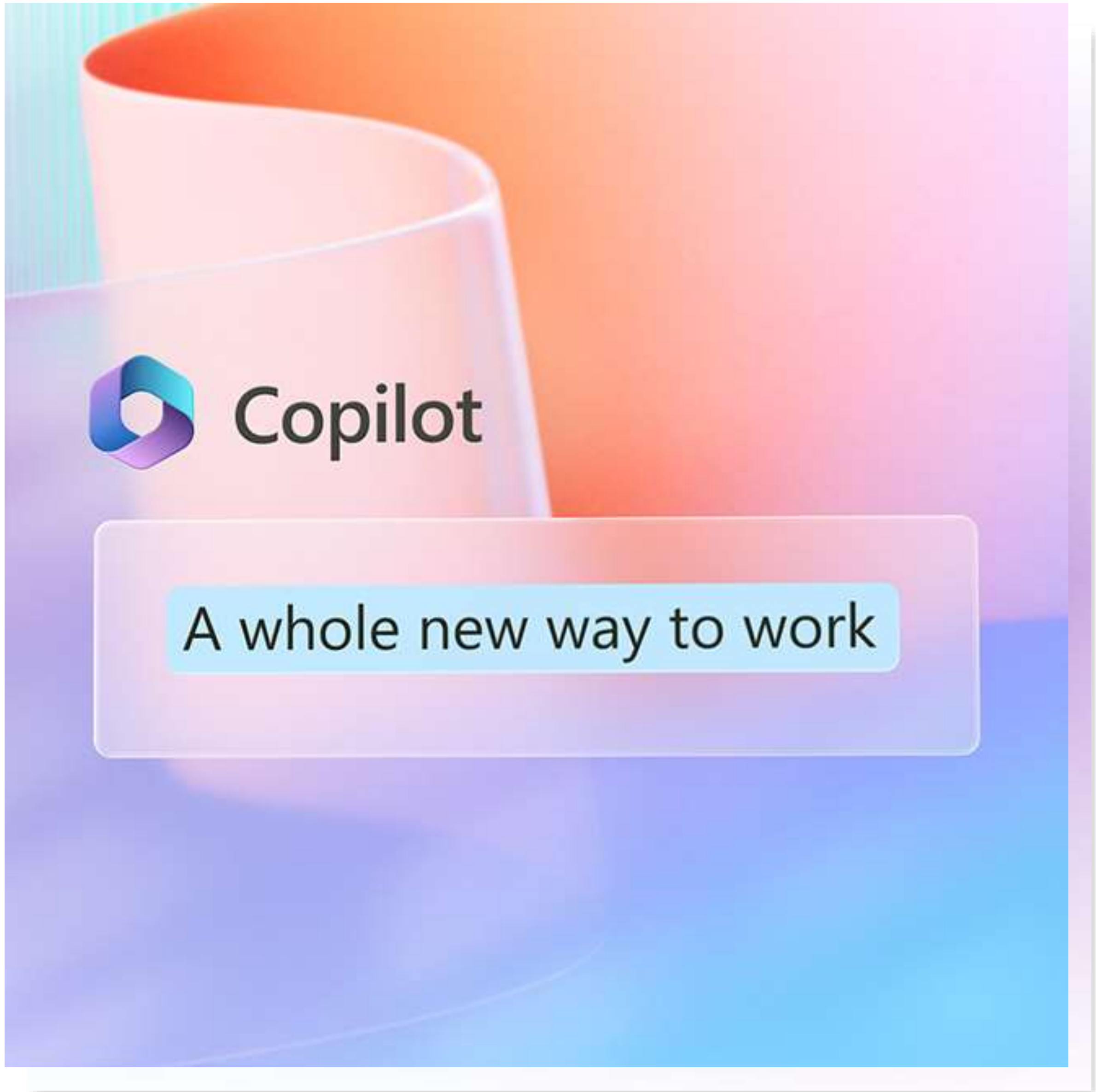
Commercial
External collaborators
Entra ID / Office 365
Microsoft Account (MSA)

DoD & DIB
External Collaborators
Azure Gov / Office 365 GCC-High
US Sovereign Cloud

Microsoft

Introducing

Microsoft 365 Copilot
your AI assistant at work



Microsoft and OpenAI Partnership

OpenAI

Ensure that artificial general intelligence (AGI) benefits humanity

Microsoft

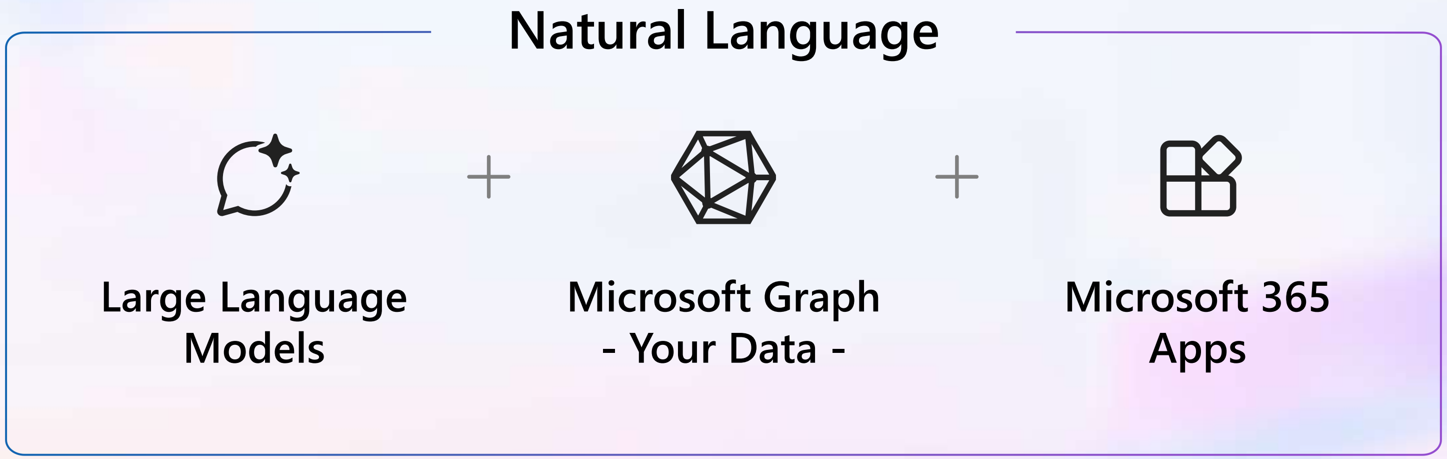
Empower every person and organization on the planet to achieve more

Azure OpenAI Service – as of November 15, 2023

GPT-4, GPT-4-Turbo, GPT-3.5-Turbo	GPT-4-Turbo with Vision	Babbage, Davinci, GPT-3.5-Turbo	DALL·E 3	Whisper
Language	Multi-Modal	Fine Tuning	Images	Transcription & Translation

Azure AI Studio

Microsoft 365 Copilot



Natural Language

Large Language Models + Microsoft Graph - Your Data - + Microsoft 365 Apps

Microsoft 365 Copilot

Grounded in
your business data

Connecting cutting-edge AI to your business data in a secure, compliant, privacy-preserving way.

Comprehensive
security, compliance, & privacy

Copilot inherits your security, compliance, and privacy policies set up in Microsoft 365.

Protected with
secure data partitions

Your data never leaves its secure partition, and it is never used for training purposes.

Integrated into the
apps you use every day

Word, Excel, PowerPoint, Outlook, Teams, and more.

Individual user & admin
always in control

User decide what to use, modify, or discard.

Designed to
learn new skills

As Copilot learns about processes, it can perform more sophisticated tasks and queries.

Microsoft Security

Microsoft Security Copilot

Defending at machine speed and scale

Microsoft Security Copilot

Defending at machine speed

> ***"It takes us three minutes to do a task that used to take at least a few hours"***

- Private preview customer

Enable response in minutes, not hours

Simplify the complex with natural language prompts and easy reporting

Catch what others miss with deeper understanding of your enterprise

Upskill your security talent with cyber-trained generative AI

Classified as Microsoft Confidential

Security Copilot working with Microsoft Security

Microsoft Defender for Endpoint

Monitor devices in real-time
Detect and prevent threats
Control policy and access
Respond to incidents and hunt

Microsoft Sentinel

Manage logs
Detect advanced threats
Monitor and alert in real-time
Get compliance and reporting

Microsoft Intune

Manage device inventory
Enforce configurations and policies
Deploy and update software
Deliver conditional access

Security Copilot

- Run queries using natural language
- Prepare reports, summaries, and graphs
- Upskill teams via prompts and guidance
- Reverse engineer malware
- Enrich alerts

+

- Run queries using natural language
- Prepare reports, summaries, and graphs
- Upskill teams via prompts and guidance
- Reverse engineer malware
- Enrich alerts
- Enrich incidents

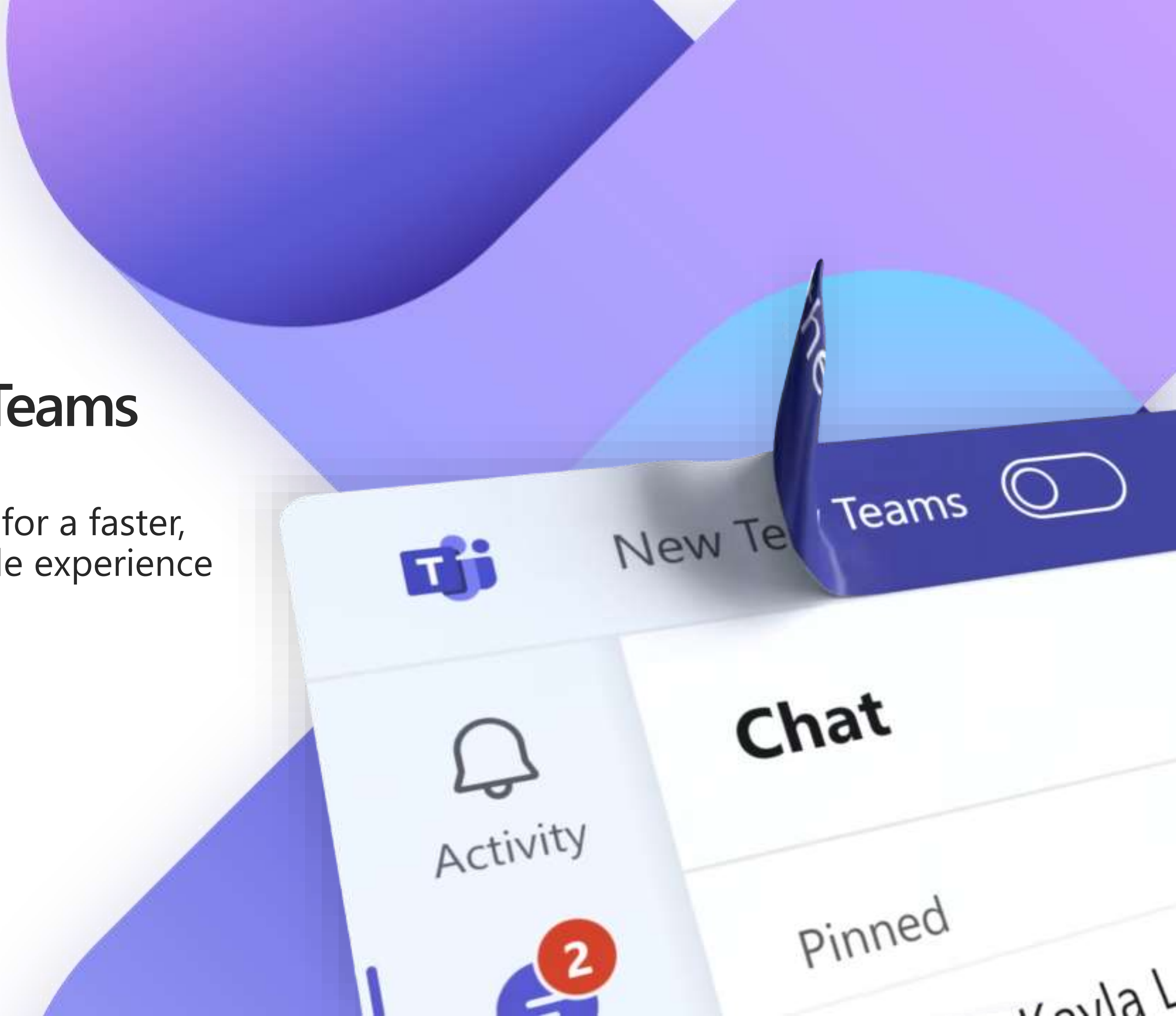
+

- Run queries using natural language
- Prepare reports, summaries, and graphs
- Upskill teams via prompts and guidance
- Reverse engineer malware
- Enrich alerts
- Enrich incidents
- Assess security posture of devices

Microsoft Teams

Welcome to the new era of Microsoft Teams

Reimagined from the ground up for a faster, simpler, smarter, and more flexible experience



GCCH June 2024

Continuously improving Microsoft Teams

Over the past several years, we've collected your feedback regarding Microsoft Teams' performance. Customers want continued performance innovations, and we've heard you loud and clear.

Top customer feedback

App responsiveness

Memory consumption

Meeting experience

We've reimagined Teams from the ground up.

- Faster performance
- Simpler UX
- Smarter AI experiences
- More flexible collaboration

The result is: the new Microsoft Teams.

Microsoft Teams

Microsoft Teams Premium
The better way to meet

Bring advanced capabilities into your meetings with Microsoft Teams Premium

Too much time spent in meetings:
Resulting in lost productivity and missed opportunities

Intelligent productivity

Focus on what matters most with meetings powered by AI, including GPT from OpenAI

Risk of leaked information from meetings:
Meetings involving confidential information create security concerns

Advanced protection

Lock down sensitive meeting information and customize Teams management to collaborate more securely and meet your organization's unique needs

Meetings aren't one-size fits all:
Experiences feels generic and don't tailor to the audience

Richer engagement

Bring brand into every interaction to establish trust and grow your business

The cost of multiple tools adds up:
Managing licensing and security for multiple meeting tools is expensive and time-consuming

Do more with less

Reduce costs using one collaboration solution for chat, calling, 1:1 and 1:many meetings, virtual appointments, and webinars

Microsoft Teams Premium

The better way to meet

Intelligent productivity

Focus on what matters most with meetings powered by AI, including GPT from OpenAI

Advanced protection

Collaborate more securely with advanced protection and customized Teams management

Richer engagement

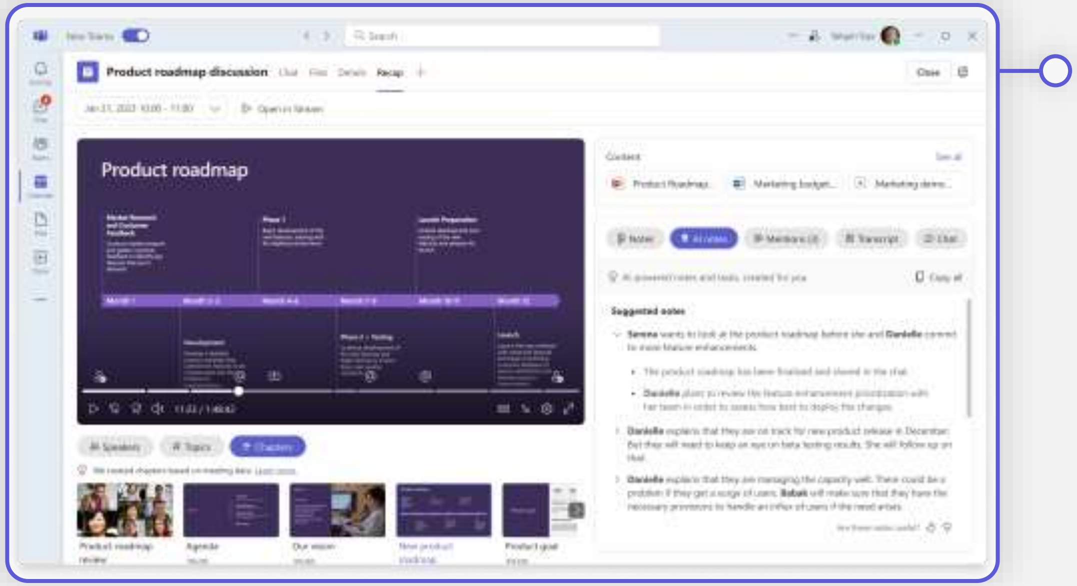
Create deeper engagements with personalized experiences that help grow your business and brand

Intelligent productivity

Focus on what matters most with meetings powered by AI, including GPT from OpenAI

80%

of people are comfortable with AI summarizing their meetings and action items[1]



Suggested notes

- Serena wants to look at the product roadmap before she and Danielle commit to more feature enhancements.
  - The product roadmap has been finalized and shared in the chat.
  - Danielle plans to review the feature enhancement prioritization with her team in order to assess how best to deploy the changes.
- Danielle explains that they are on track for new product release in December. But they will need to keep an eye on beta testing results. She will follow up on that.
- Danielle explains that they are managing the capacity well. There could be a problem if they get a surge of users. Babak will make sure that they have the necessary provisions to handle an influx of users if the need arises.

Are these notes useful?

Save time and effort with intelligent meeting recap*

Use AI-generated meeting notes and tasks for key points and action items

Quickly discover important moments in the meeting, such as when your name was mentioned, a screen was shared, and when you've joined or left—only visible to you

Speaker timeline markers allow you to jump to different speakers—organized by those you work most closely with

Chapters and topics divide the meeting into sections so it's easy to jump right to where you would like to review

Break down language barriers

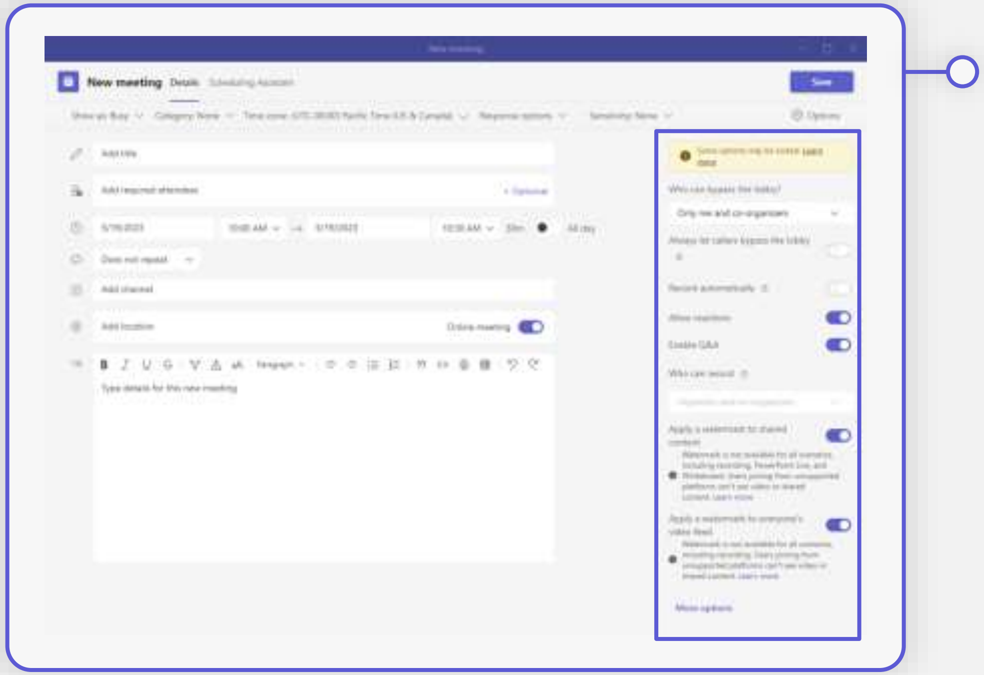
Turn on live translated meeting captions in your chosen language

[1] Microsoft 2023 Work Trend Index: Annual Report by Edelman Data x Intelligence, May 2023

*** Denotes feature not yet available for GCC-H and DoD**

Advanced protection

Collaborate more securely with advanced protection and customized Teams management



New meeting Details Scheduling Assistant

Save

Options

Add title

Add required attendees

Does not repeat

Add channel

Add location

Online meeting

Type details for this new meeting

Who can bypass the lobby?

Only me and co-organizers

Always let callers bypass the lobby

Record automatically

Allow reactions

Enable Q&A

Who can record

Apply a watermark to shared content

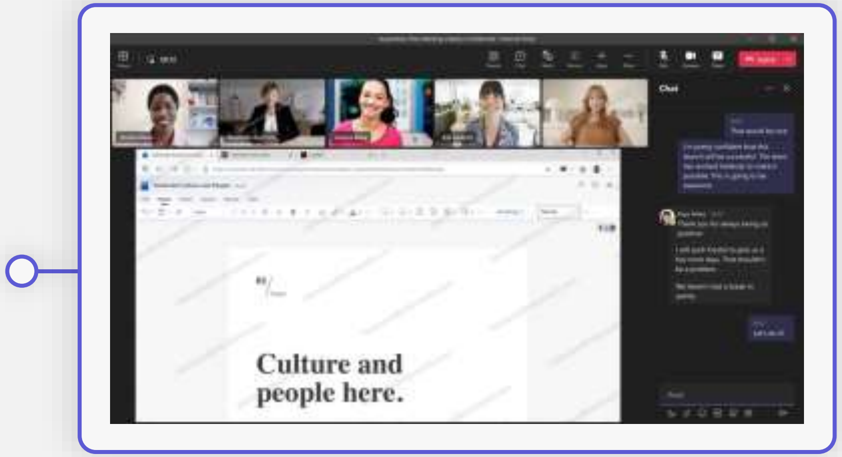
Apply a watermark to everyone's video feed

More options

Increase meeting security

Schedule meetings from customized templates created by IT, taking the work out of setting the right meeting options or controls

Leverage an end-to-end encryption option for meetings that need additional privacy protections*



Culture and people here.

Protect sensitive information

Help deter data leaks with in-meeting watermarking over screen shares and video feeds

Safeguard the meeting by limiting which attendees can record

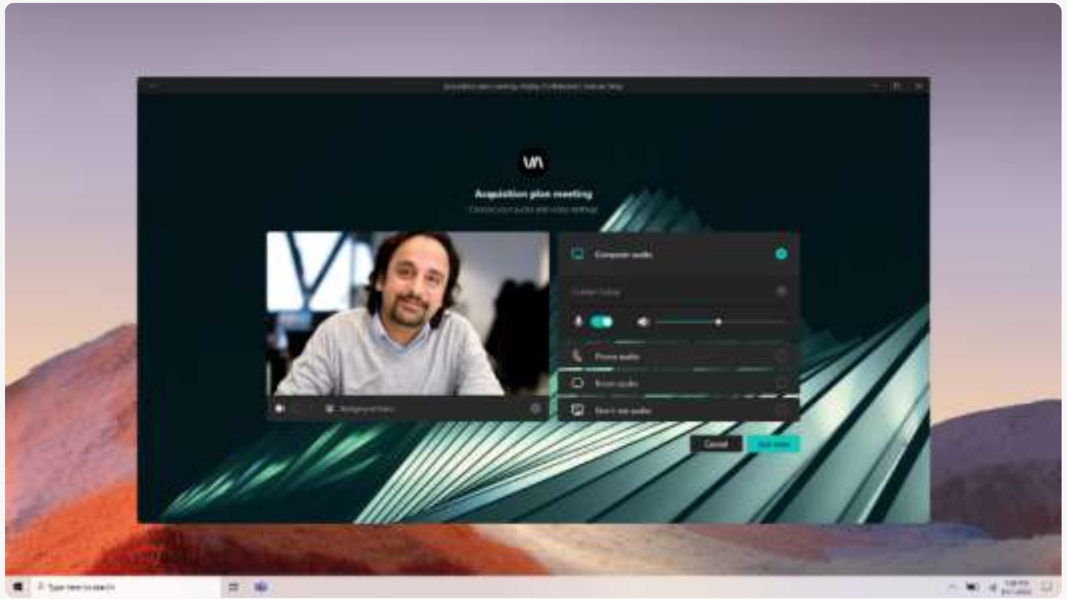
Apply sensitivity labels to help uplevel protections in sensitive meetings**

*Teams protects your data with encryption in transit and at rest for all meetings

**Customers with an E5 license or E5 compliance

Richer engagements

Create deeper engagements with personalized experiences that help grow your business and brand



Build your brand into every interaction

Let your brand shine with custom branding when your attendees join the meeting

Create custom backgrounds to bring people together and highlight your brand

INFORMATION ON THIS SLIDE IS SUBJECT TO CHANGE

Microsoft Teams Premium

Feature availability

	Teams Premium feature	GCC High
Intelligent productivity	Intelligent recap: Auto-generated chapters in meeting recording w/ PPT Live chapters	*TBD* *Pending Azure Open AI in Azure Government*
	Intelligent recap: Personalized timeline markers in meeting recordings (leave/join)	
	Intelligent recap: Personalized timeline markers in meeting recordings (@mention, screenshare)	
	Intelligent recap: Intelligent search w/ speaker suggestions in transcript	
	Intelligent recap: Auto-generated chapters in meeting recording w/ AI created chapters	
	Intelligent recap: AI-generated notes	
	Intelligent recap: AI-generated tasks	
	Live translation for captions from 40 languages	**Available now**
Advanced protection	End-to-end encryption for online meetings (up to 50 participants)	**Available now**
	Watermarking	**Available now**
	Limit who can record	**Available now**
	For Microsoft E5 customers: Sensitivity labels for Teams meetings (including prevent copy/paste)	**Available now**
Richer engagements	Meeting templates, pre-configured by IT	**Available now**
	Custom branded meetings	**Available now**
	Custom organization backgrounds	**Available now**
	Custom organization together mode scenes	*TBD*
	Custom user policy packages	
Advanced webinars	Green room	
	Manage attendee view	
	Waitlist & manual approval	
	Limit registration date & time	
	RTMP-In	
Advanced Virtual Appointments	Custom lobby room with branding, logos	
	On-demand and scheduled appointment, queue views	
	SMS notifications	
	Consumption and usage analytics for admins in TAC	
	Analytics at departmental and organizational levels	
eCDN	1P eCDN for Teams Live Events (bundled as a part of Teams Premium)	

INFORMATION IS SUBJECT TO CHANGE

Microsoft

Introducing

The Microsoft Intune Suite

Today: Organizations still seek to fill scenario gaps…

Application management lifecycle

Assist employees wherever they are

Access to corporate resources for BYO

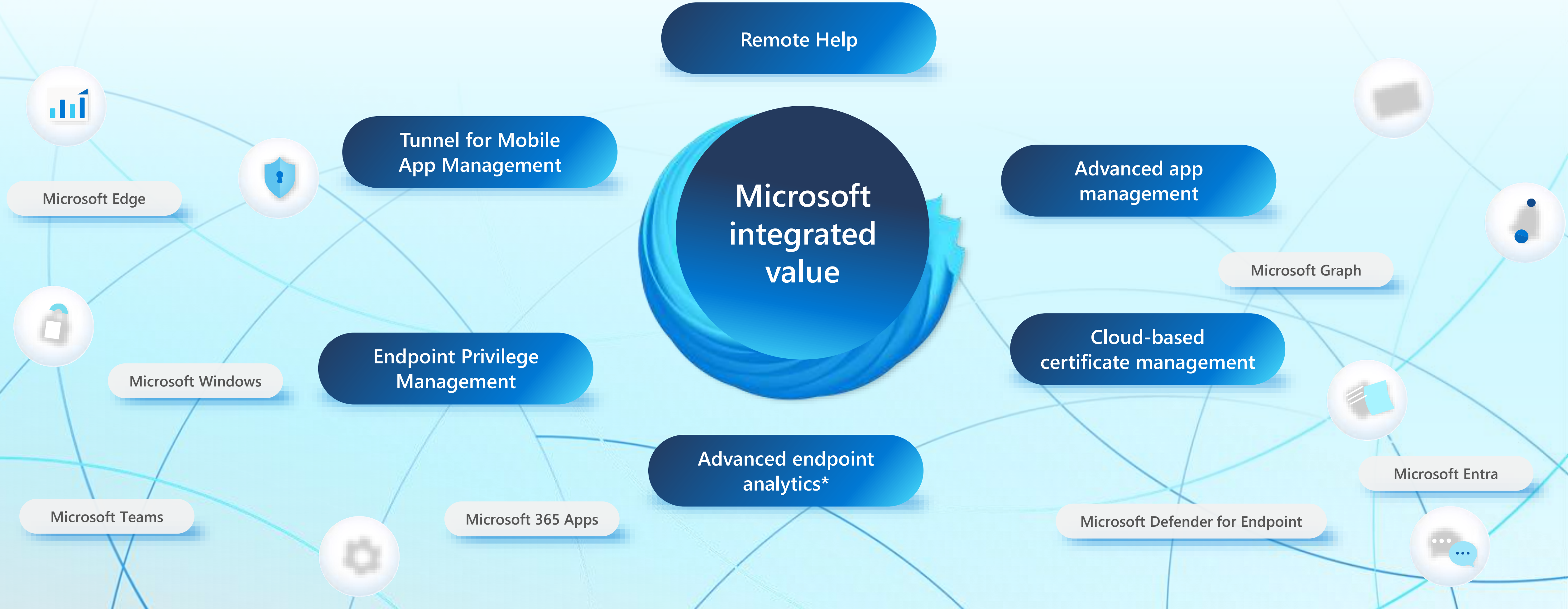
Improve end user outcomes: reducing IT efforts

Enable least privilege access enabling standard users

Certificate management

…and they’re augmenting endpoint management with 3rd-party solutions.

Microsoft Intune Suite



Microsoft integrated value

Remote Help

Tunnel for Mobile App Management

Advanced app management

Endpoint Privilege Management

Cloud-based certificate management

Advanced endpoint analytics*

Microsoft Edge

Microsoft Windows

Microsoft Teams

Microsoft 365 Apps

Microsoft Graph

Microsoft Entra

Microsoft Defender for Endpoint

Simplicity | Security | Savings

Endpoint Privilege Management

Supports: Windows

Enforce least privilege access

Enable productivity

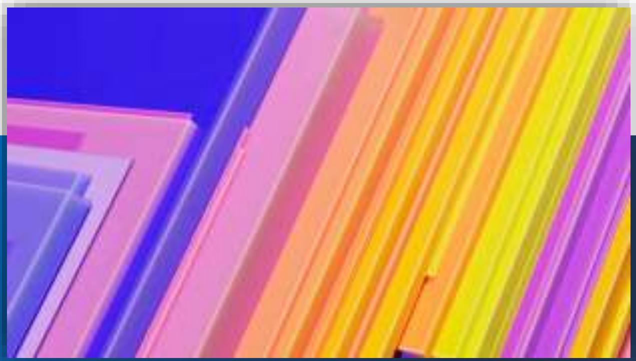
Deliver key insights

Mitigate systemic risks and vulnerabilities of local admins

- Automatic or user-confirmed elevation
- Insights based on elevation audits
- Rules based on organizational requirements
- Easy addition or removal of rules
- Tenant level enablement, per device rollout

Coming soon

- Support approved elevation
- Require MFA for elevation
- Pre-defined elevation templates



77%

of organizations say they've experienced attacks as a result of unmanaged or poorly managed endpoints.

Source: "Endpoint Management Vulnerability Gap," prepared by Enterprise Strategy Group for Microsoft.

Remote Help

Supports: Windows | Android, macOS coming soon

✓ Support workers anywhere

✓ Improve efficiency

✓ Mitigate security risks

Secure and easy-to-use, cloud-based remote assistance

- Trusted help desk support for users
- Role-based access controls
- Device compliance warnings
- Session reporting
- ServiceNow incident details
- Annotations, chat, and more

Coming soon

- Conditional access
- Copy/paste of files and text
- Launch from Intune

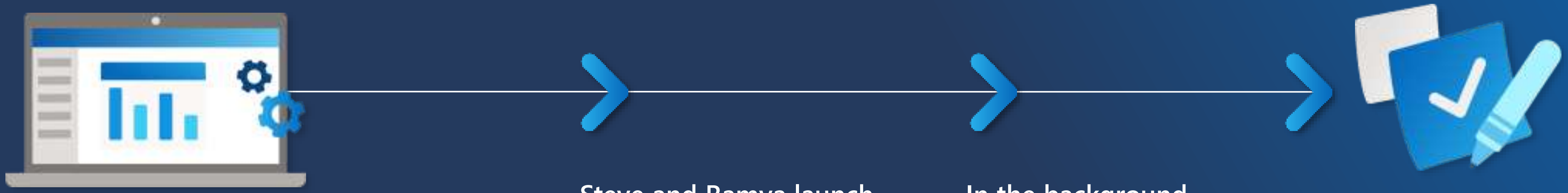
44% of organizations say providing IT support for remote workers is one of their biggest challenges.

Source: IDC, Future of Work Survey, March 2021.

Fix device compliance and performance issues from the cloud

Intune Remote Help

Provide trusted, easy-to-use remote assistance



While working from a coffee shop, Steve runs into issues with Teams on his laptop. He calls Ramya at the help desk.

Steve and Ramya launch Remote Help, sign in, and exchange a code. Azure AD authenticates and requires MFA for Steve.

In the background, Microsoft Defender alerts Ramya to a compliance issue with Steve’s device before the session starts.

Ramya can then help Steve address this security issue—enabling BitLocker—while also addressing the Teams problem.

Microsoft Intune

Microsoft Windows

Microsoft Entra

Microsoft Defender for Endpoint

Microsoft Tunnel for Mobile App Management

Supports: Android | iOS

✓ Secure access to corporate data

✓ Flexibility for end users

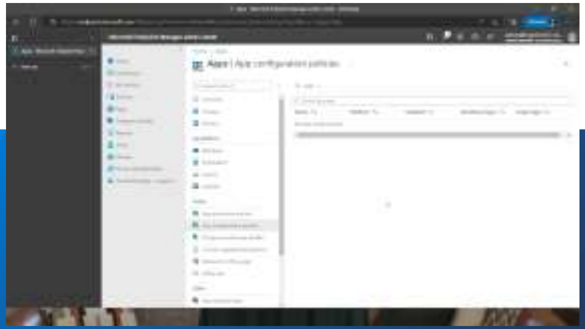
✓ Enable BYOD

Secure access for mobile users on unenrolled devices

- App or device-wide VPN
- Auto launch
- Personal account privacy and secure browsing to on-prem resources with Microsoft Edge
- Company portal (Android) or no sign-in required (iOS)
- Defender (Android) or Tunnel for MAM SDK VPN

Coming soon

- Trusted root certificate support



UP TO $\frac{1}{3}$ of mobile devices connecting to organizations are unmanaged.

Source: "Endpoint Management Vulnerability Gap," prepared by Enterprise Strategy Group for Microsoft.

Advanced app management

Will support: Windows | macOS

Increased IT efficiency

Reduced security risks and vulnerabilities

Stay current with updates and alerts

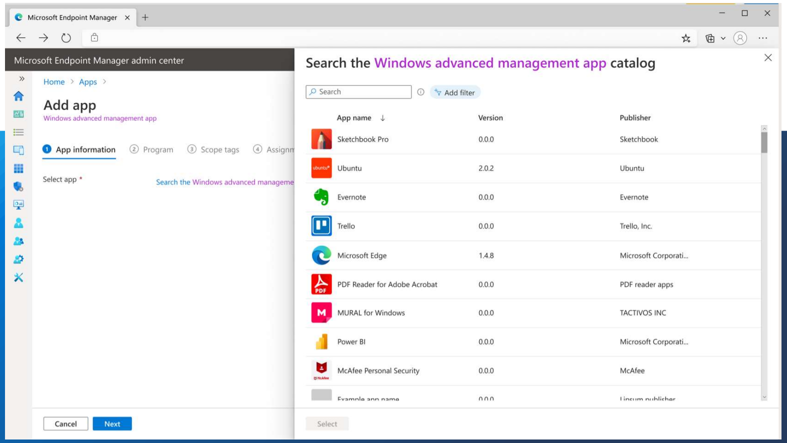
Simplify app discovery, delivery, and updates

Preview

- Securely hosted app catalog
- Prepackage and preconfigure apps
- Graph API scripting for automated supersedence
- No wrapping, no install commands

Coming soon

- Advanced update notifications
- Guided remediation



Microsoft Endpoint Manager admin center

Home > Apps >

Add app

Windows advanced management app

1 App information   2 Program   3 Scope tags   4 Assignm

Select app *   Search the Windows advanced manageme

Search the Windows advanced management app catalog

App name ↓	Version	Publisher
Sketchbook Pro	0.0.0	Sketchbook
Ubuntu	2.0.2	Ubuntu
Evernote	0.0.0	Evernote
Trello	0.0.0	Trello, Inc.
Microsoft Edge	1.4.8	Microsoft Corporati...
PDF Reader for Adobe Acrobat	0.0.0	PDF reader apps
MURAL for Windows	0.0.0	TACTIVOS INC
Power BI	0.0.0	Microsoft Corporati...
McAfee Personal Security	0.0.0	McAfee
Example app name	0.0.0	Lipsum publisher

78%

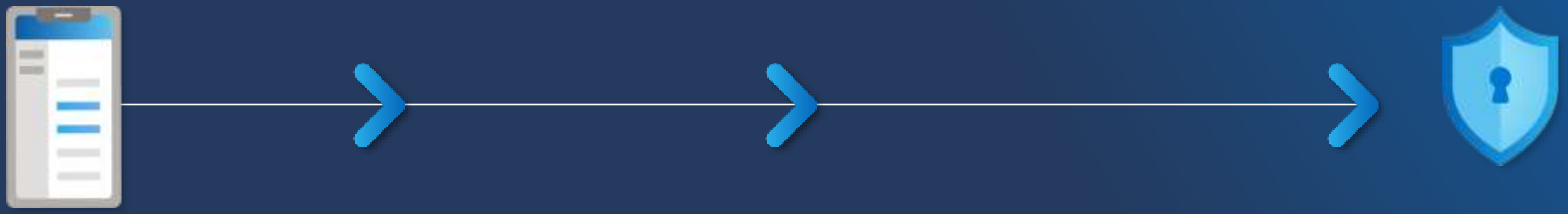
of devices remain unpatched nine months after a patch fixing a critical vulnerability is released.

Source: Microsoft Digital Defense Report 2022.

Power identity-based privacy and data protection

Microsoft Tunnel for
Mobile App Management

Enable workers to securely work with BYOD



Daniela likes to use her personal iPhone for work.

During lunch, her manager asks her to review and approve quarterly financial results.

From Outlook, she clicks a link to open the report in Edge. In the background, Azure AD authenticates her access while Tunnel connects her.

After reviewing the report, Daniela toggles to a personal app. She's prevented from accidentally copying corporate data there.

Microsoft Defender for Endpoints

Microsoft Entra

Microsoft Tunnel

Microsoft Edge

Microsoft Outlook

Intune app protection policies

Supercharge app updates safely

Advanced app management: preview

Tailor app updates to mitigate vulnerabilities

As an administrator, Alex has access to a Microsoft hosted app catalog

Alex can prepackage and preconfigure apps for his organization

Alex can automate app supersedence with familiar scripts

Alex can reduce the risk of old app version across his organization

Microsoft Windows Store for Business

Microsoft Azure

Microsoft Graph

Advanced Endpoint analytics

Supports: Windows | mobile, macOS coming soon

✓ Gain visibility of end-user experience

✓ Proactively detect issues

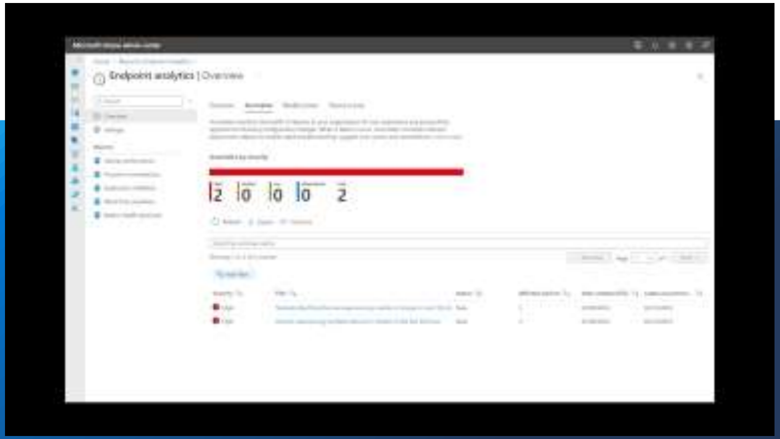
✓ Efficiently troubleshoot and remediate

Proactively address endpoint performance issues

- Detect anomalies based on device level events and signals that correlate to anomalous behavior
- Use an enhanced device timeline view that includes anomalies to ease and speed troubleshooting
- Get detailed report of the analytics for a subset of devices using IT-defined scope tag

Coming soon

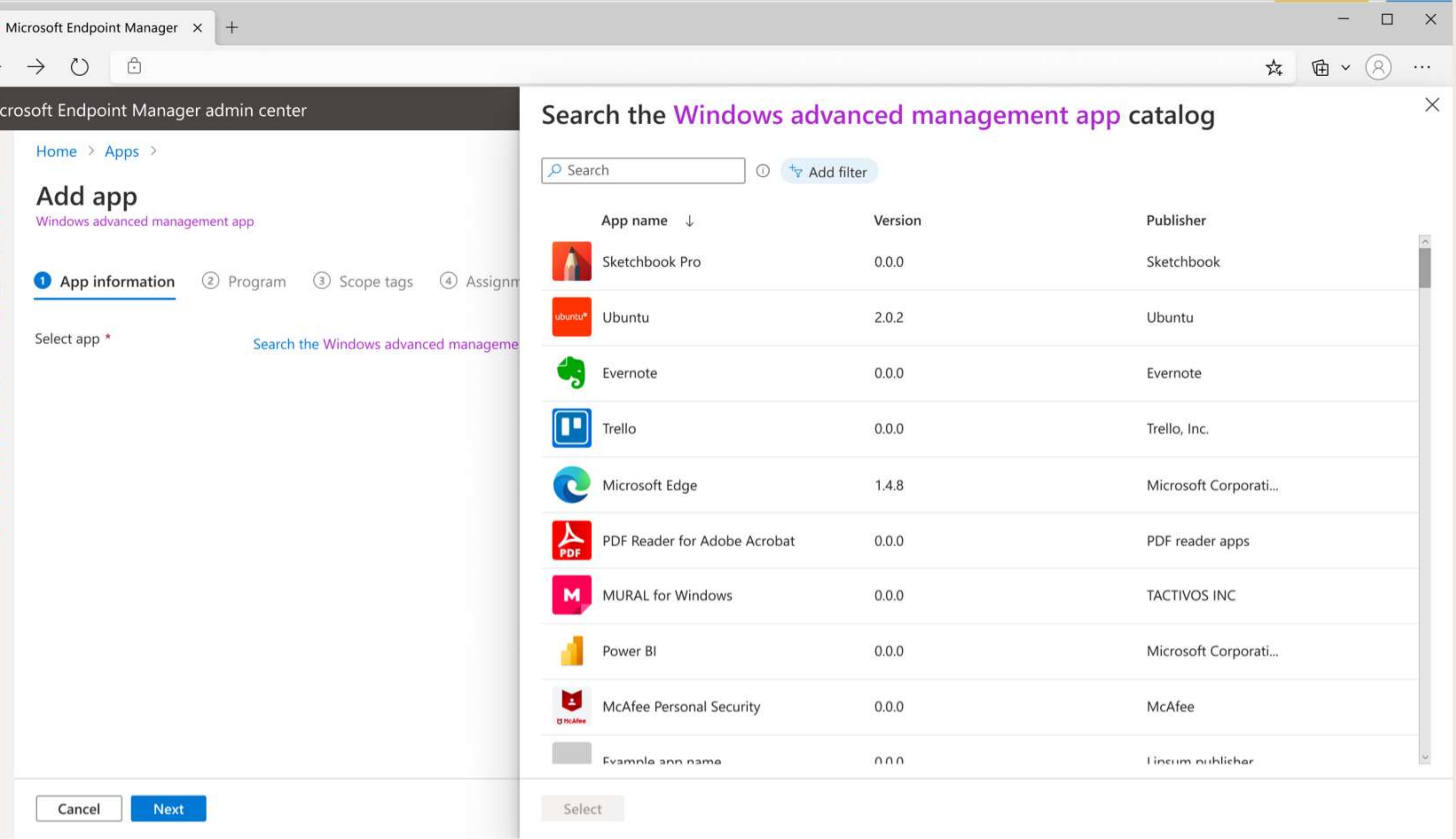
- AI powered device correlation for troubleshooting anomalies.
- Software and hardware insights to reduce IT expenditure and enable smart IT asset management
- App insights for mobile



53%

Of employee and customer experience decision makers consider improving employee experience a top priority.

Source: Forbes December 5, 2022: Three Ways to Improve Employee Experiences for Better Business Outcomes.

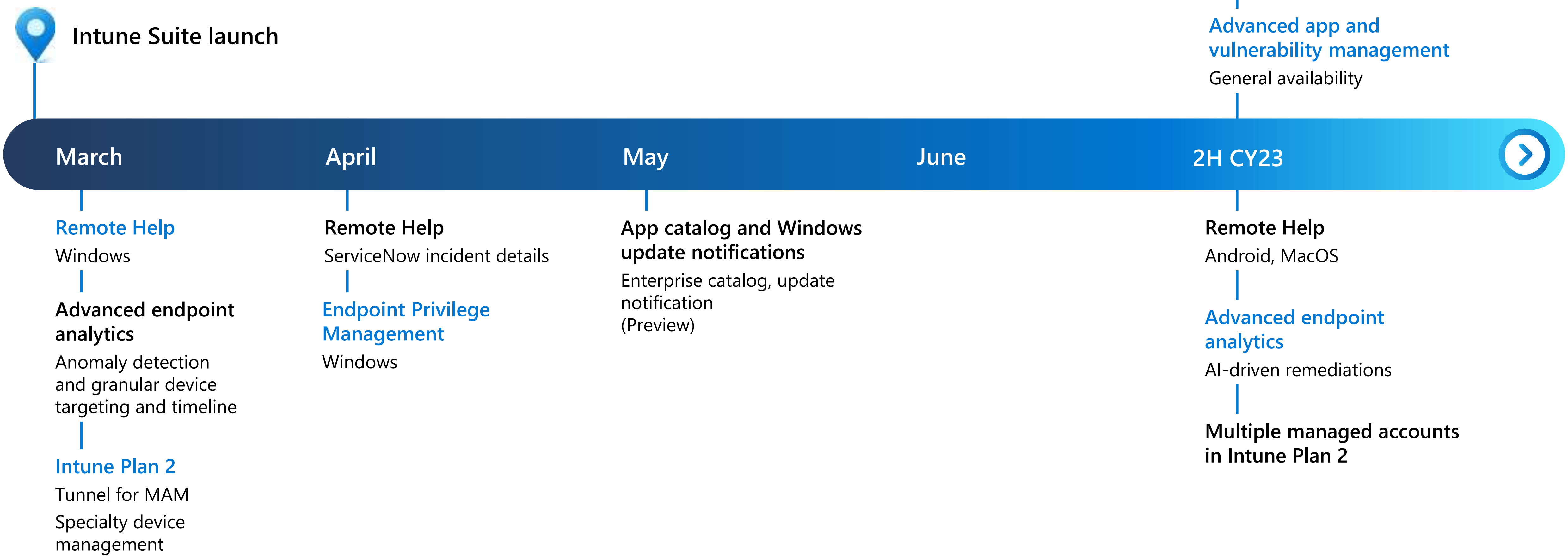

Microsoft Endpoint Manager
crosoft Endpoint Manager admin center
Home > Apps >
Add app
Windows advanced management app
1 App information
2 Program
3 Scope tags
4 Assignm
Select app *
Search the Windows advanced manageme
Cancel
Next
Search
Add filter
Select

Search the Windows advanced management app catalog

	App name ↓	Version	Publisher
	Sketchbook Pro	0.0.0	Sketchbook
	Ubuntu	2.0.2	Ubuntu
	Evernote	0.0.0	Evernote
	Trello	0.0.0	Trello, Inc.
	Microsoft Edge	1.4.8	Microsoft Corporati...
	PDF Reader for Adobe Acrobat	0.0.0	PDF reader apps
	MURAL for Windows	0.0.0	TACTIVOS INC
	Power BI	0.0.0	Microsoft Corporati...
	McAfee Personal Security	0.0.0	McAfee
	Example app name	0.0.0	Lipsum publisher

The approach

Adopt the cost-effective bundled suite or any combination of individual add-ons



Intune Suite launch

March

Remote Help
Windows

Advanced endpoint analytics
Anomaly detection and granular device targeting and timeline

Intune Plan 2
Tunnel for MAM
Specialty device management

April

Remote Help
ServiceNow incident details

Endpoint Privilege Management
Windows

May

App catalog and Windows update notifications
Enterprise catalog, update notification
(Preview)

June

2H CY23

Cloud certificate management
(Preview)

Advanced app and vulnerability management
General availability

Remote Help
Android, MacOS

Advanced endpoint analytics
AI-driven remediations

Multiple managed accounts in Intune Plan 2

Separate add-on licensing option

🔵 Preview
● General Availability

		TODAY	MARCH	APRIL	MAY	JUNE	2H CY23
Remote Help	Windows	●					
	ServiceNow incident details		🔵	●			
	Android					🔵	●
	Mac						●
Endpoint Privilege Management	Windows		🔵	●			
Advanced app and vulnerability management	Enterprise catalog				🔵		●
	Advanced update notification and guided update controls						🔵
Advanced endpoint analytics	Anomaly detection and enhanced device timeline (RANSOMWARE!!!)		●				
	AI-driven analytics						●
Tunnel for Mobile App Management			●				
Specialty device management			●				
Multiple managed accounts							●
Cloud certificate management							🔵

Microsoft Intune plans

Intune Plan 1

Included in EMS E3 or Microsoft 365 E3, ME5, F1, F3, and Business Premium plans

Intune Suite

Add to Plan 1 to utilize these solutions

Included solutions*

- Remote help
- Endpoint Privilege Management
- Advanced Endpoint analytics
- Advanced app management
- Cloud certificate management
- *Future advanced solutions***
- All Intune Plan 2 features

Prerequisite

- Intune Plan 1

Intune Plan 2

Add to Plan 1 to utilize these features:

Included features

- Tunnel for Mobile App Management
- Specialty device management
- *Future advanced capabilities***

Prerequisite

- Intune Plan 1

Also available as individual add-ons

***Additional advanced features to be added in future releases*

aka.ms/IntuneSuitePricing

Classified as Microsoft Confidential