



Microsoft Partner Event: Privileged Access Workstation

21st March 2022

Meet the Team



Julie McGourty
Cloud Solutions Architect
Security



James Noyce
Senior Cloud
Solutions Architect



Matthijs Hoestra
Senior Program
Manager - Identity



Luciana Blanchard
Cloud Solutions Architect
Identity



Gabriele Glodenyte
Partner Business Manager



Housekeeping



There will be speaker changes throughout the session



This is a one-way speaker to attendees audio, so please ask any questions in the Q&A



This will be recorded and links sent to you (*current delay on recordings being sent*)



Feedback – aka.ms/paw-feedback



These Resources will be shared with you (to share with others at your company)



All content is under your partnership NDA

Today's Agenda (GMT)

14:00 - Intro and Housekeeping – Julie McGourty

14:05 - Keynote – James Noyce

14:40 - Components for PAW-CSM Best Practice – Julie McGourty

14:50 – Verifiable Credentials - Matthijs Hoekstra

15:15 – Cross Tenant Access Highlights – Luciana Blanchard

15:40– Granular Delegated Admin Privileges - Gabriele Glodenyte

15:50 – Next Steps for Partner Success – Julie McGourty

16:00 – Event Ends

Keynote

James Noyce
Senior Cloud Solution Architect

Securing privileged access principles

Built-on Microsoft public security guidance

- Zero trust
- Enterprise Access Model from Securing Privileged Access

Run users with least privilege

- No local admin privileges

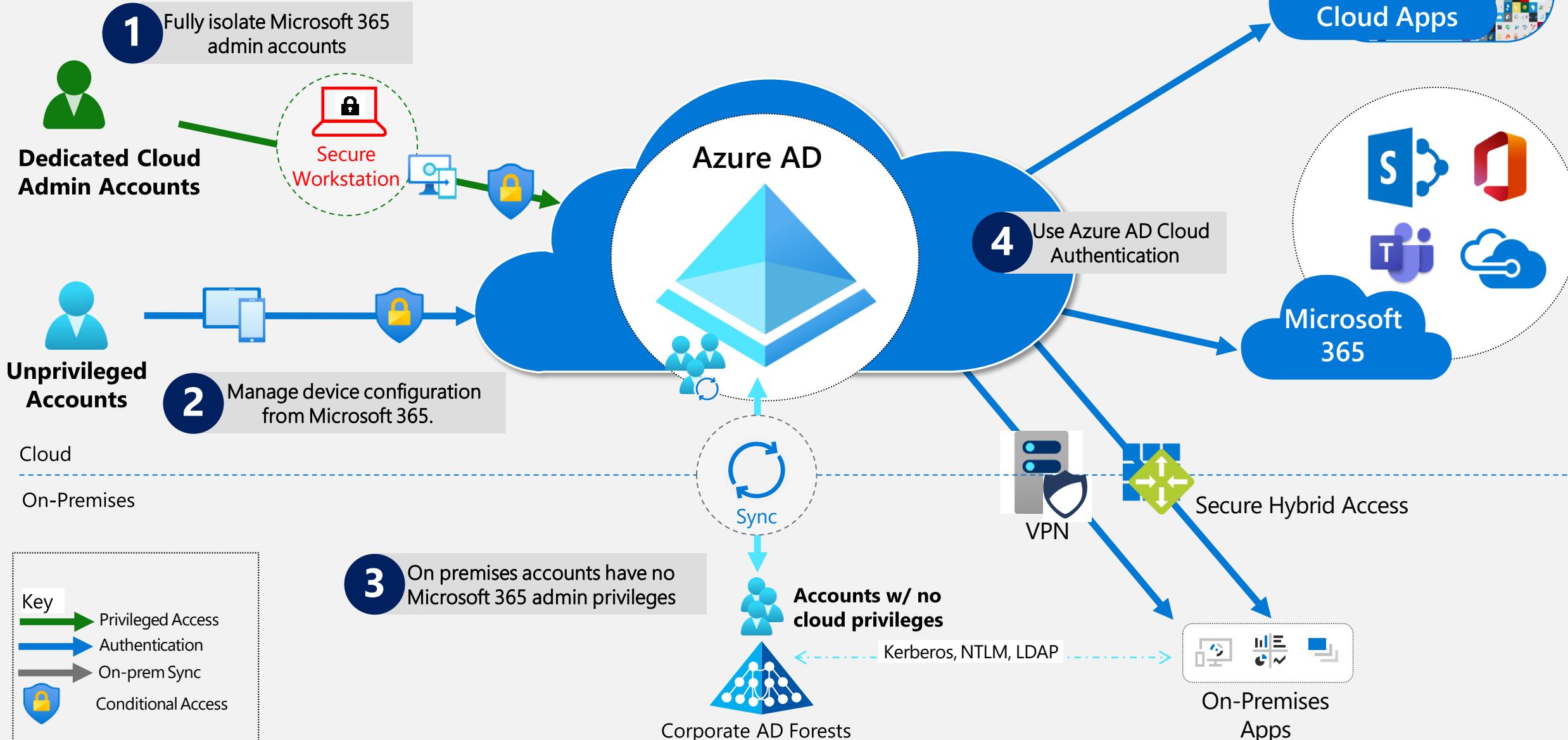
Reduce standing privilege

- Use just-in-time elevation of permissions

Clean keyboard (clean source)

- Assurance in device performing administration

Decouple from on-premises security controls



UK NCSC stance on secure privileged access

Maintain level of assurance in systems used to manage cloud services

UK National Cyber Security Centre (NCSC) Antipatterns -

Anti-pattern 1: 'Browse-up' for administration

When administration of a system is performed from a device which is less trusted than the system being administered.

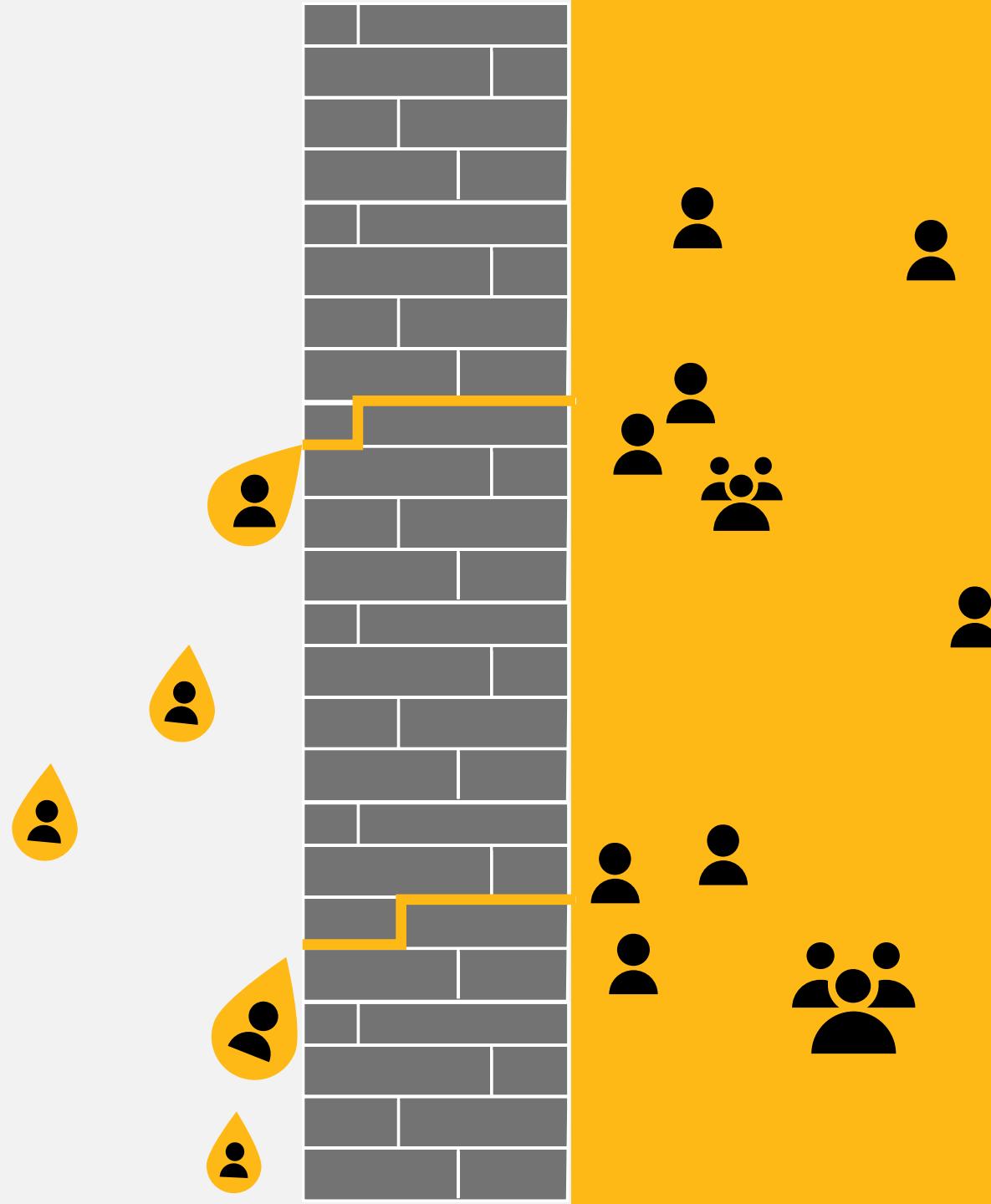
"if you don't have confidence in devices that have been used to administer or operate a system, you can't have confidence in the integrity of that system."

Attackers are like water

Attackers take path of least resistance
to achieve objectives

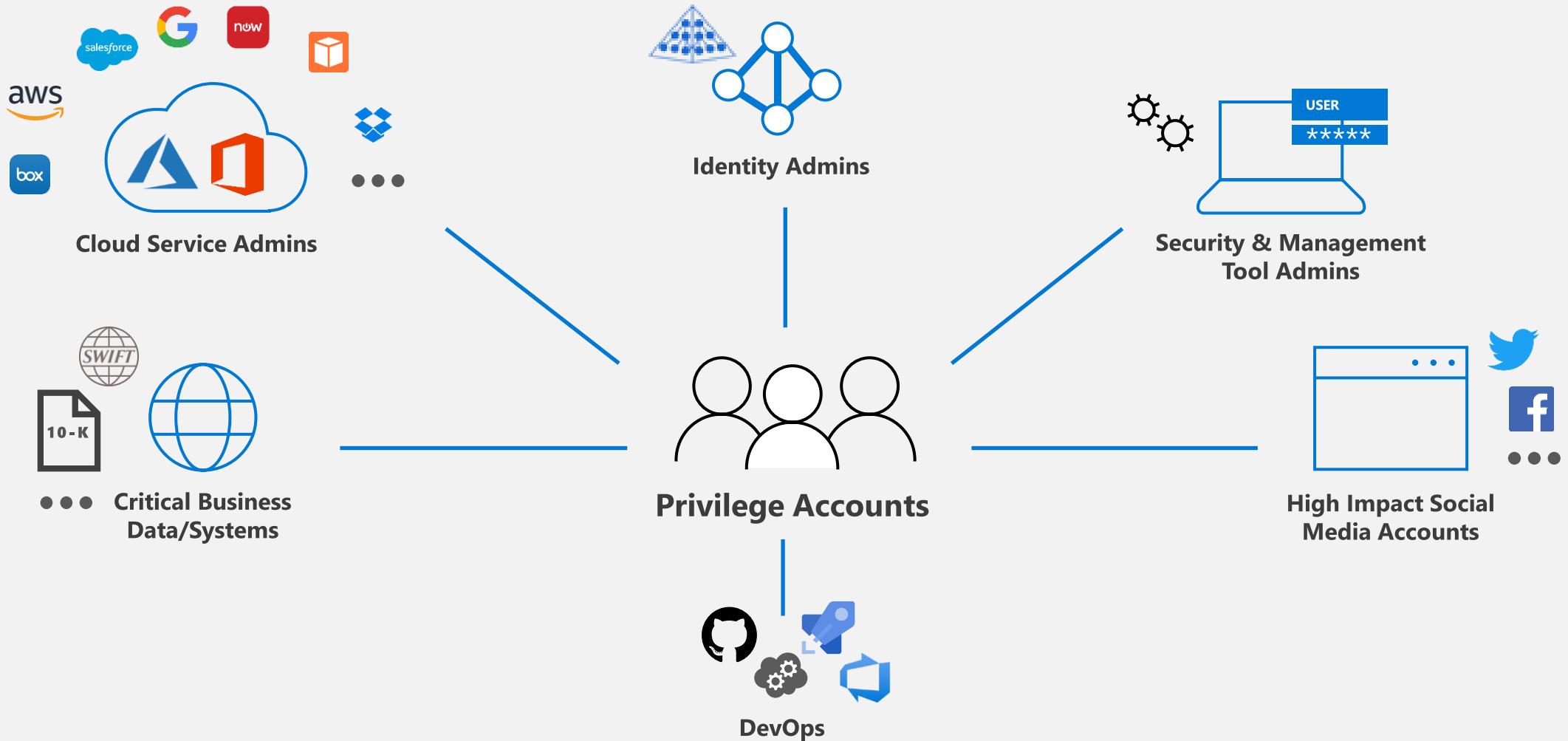
- Established paths/methods
- Easiest new openings

Attackers only bother when they get
good ***return on investment (ROI)***



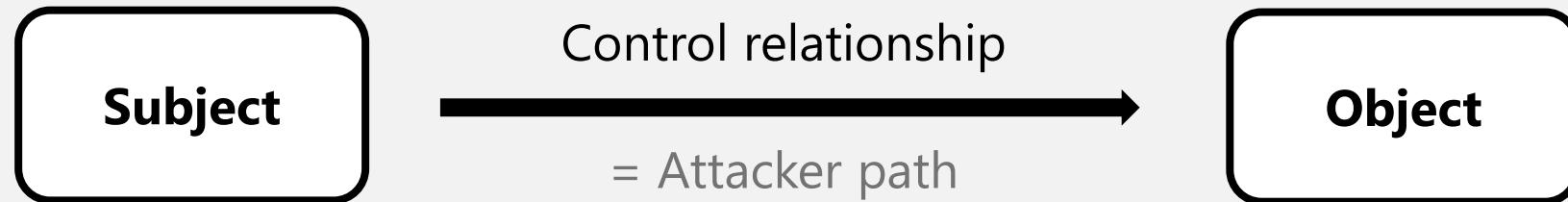
Privileged Access is more than Administrators

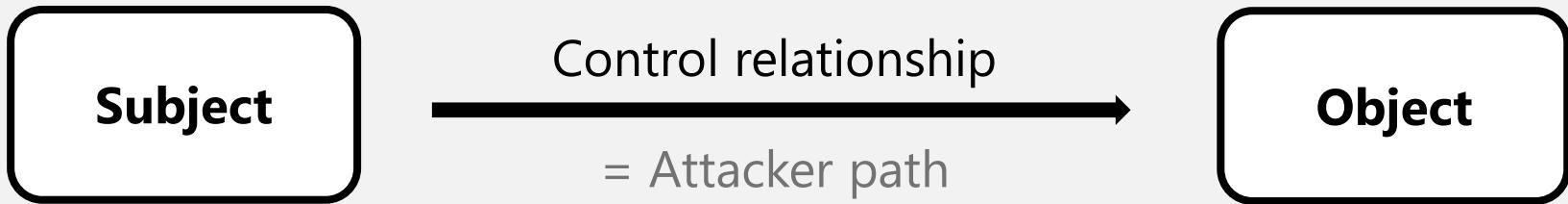
Protect high impact accounts/roles



Clean Source and Clean Keyboard Principle

- Clean Source principle requires all security dependencies to be as trustworthy as the object being secured





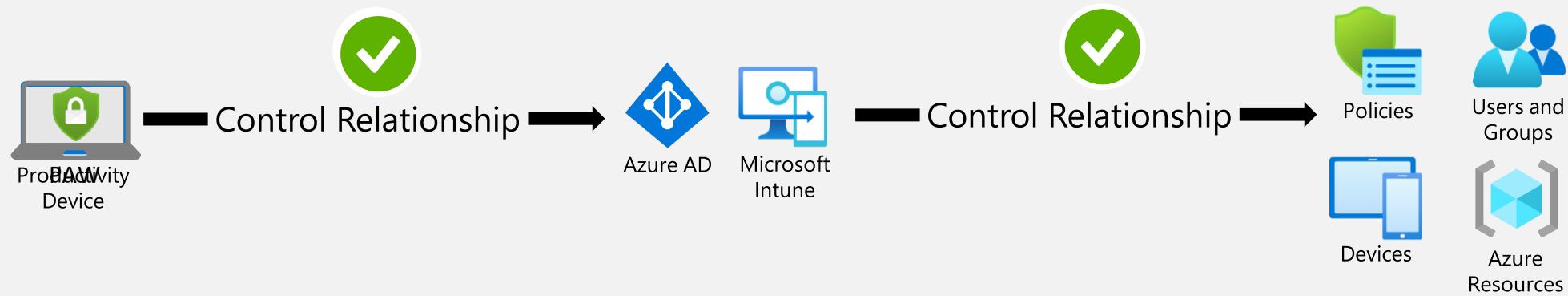
Clean Source and Clean Keyboard – Architecture and Design

- System is not dependent on lower trust systems



Clean Source and Clean Keyboard – Azure AD Control Relationship

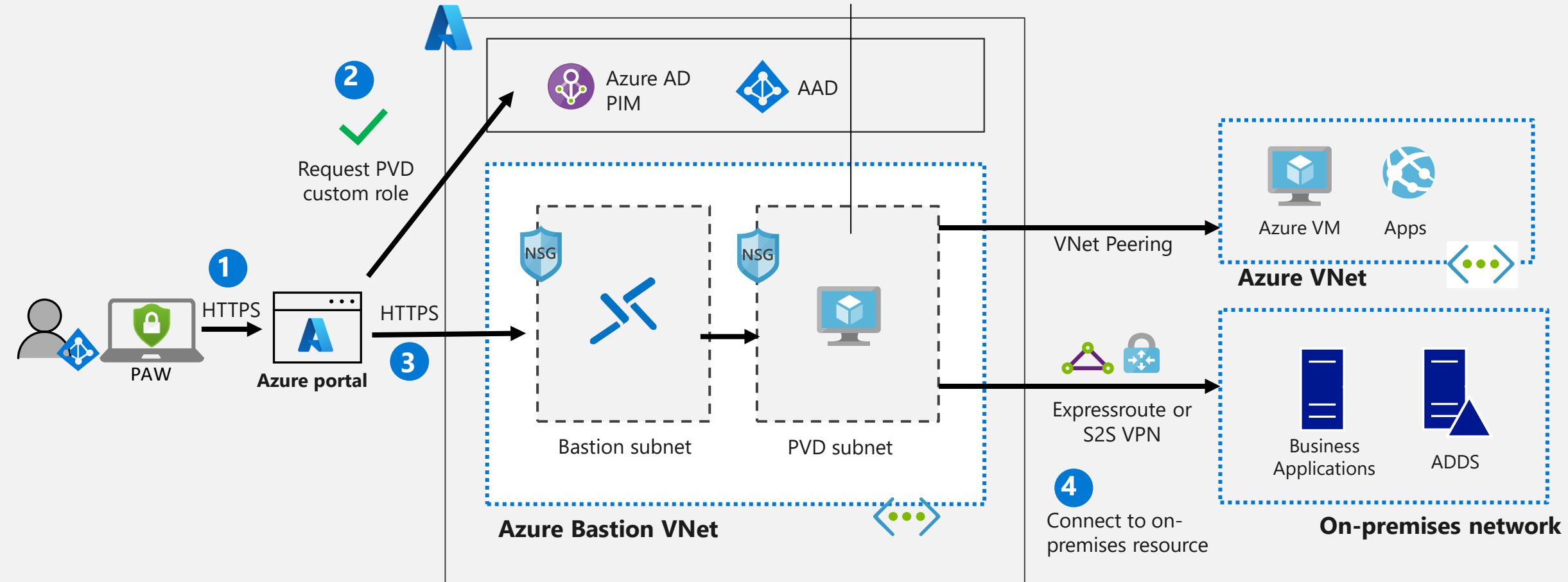
- Extending this to Azure AD and Azure resources
- But system is not dependent on lower trust systems
- System controlling Azure AD needs to be trusted



- PAW for Cloud Services Management device is required
- Anchored in Azure AD with no external trust dependencies

Hybrid Management Solution

Connect to virtual PAW using
Azure Bastion



PAW-CSM Solution Components

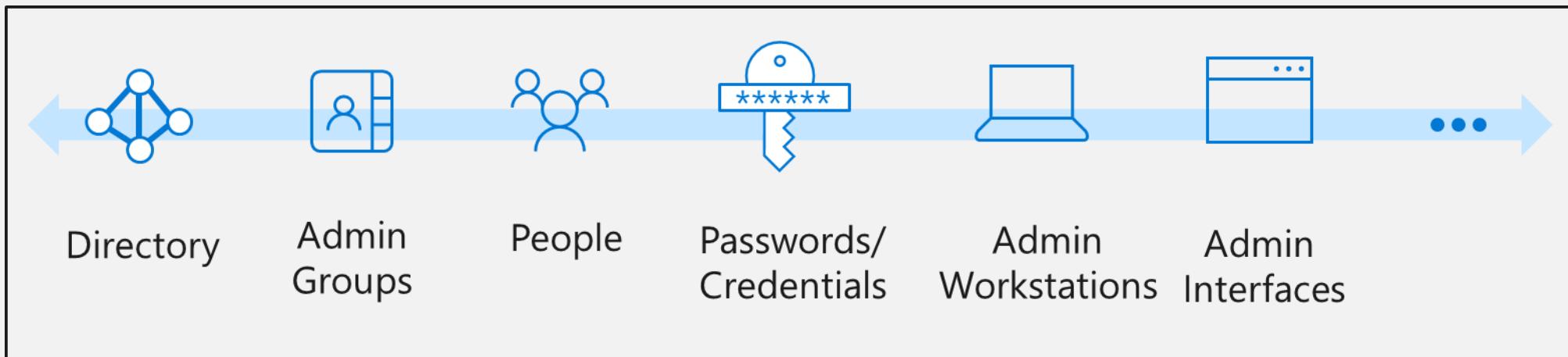
Julie McGourty
Cloud Solutions Architect - Security
Global Partner Solutions UK



Solution Overview

- Privileged Access Workstation for Cloud Services Management (PAW-CSM) enables secure Azure resource administration, whilst adopting a Zero Trust security model.
- PAW-CSM is built on fundamental security principles and industry-leading technologies to provide a hardened, limited-use workstation designed to administer the Azure environment while protecting against cyber attackers using multiple layers of threat protection.
- More than just vaulting admin passwords

Protect all parts of the privileged lifecycle



PAW : Key element of protecting assets anywhere with Zero Trust

Verify **explicitly** | Use **least-privileged access** | Assume **breach**



Groups/Role
Location
Privileges
Session risk
User Risk



Microsoft
Azure AD



Microsoft
365 Defender



Managed or BYOD
Health & compliance
Device risk
Type and OS version
Encryption status
**Hardened, PAW
workstation**



Microsoft
Defender for
Endpoint



Microsoft
Endpoint
Manager

Security &
Compliance
Policy Engine



Azure Sentinel



Microsoft Cloud



Microsoft
Information
Protection



Cloud SaaS
apps

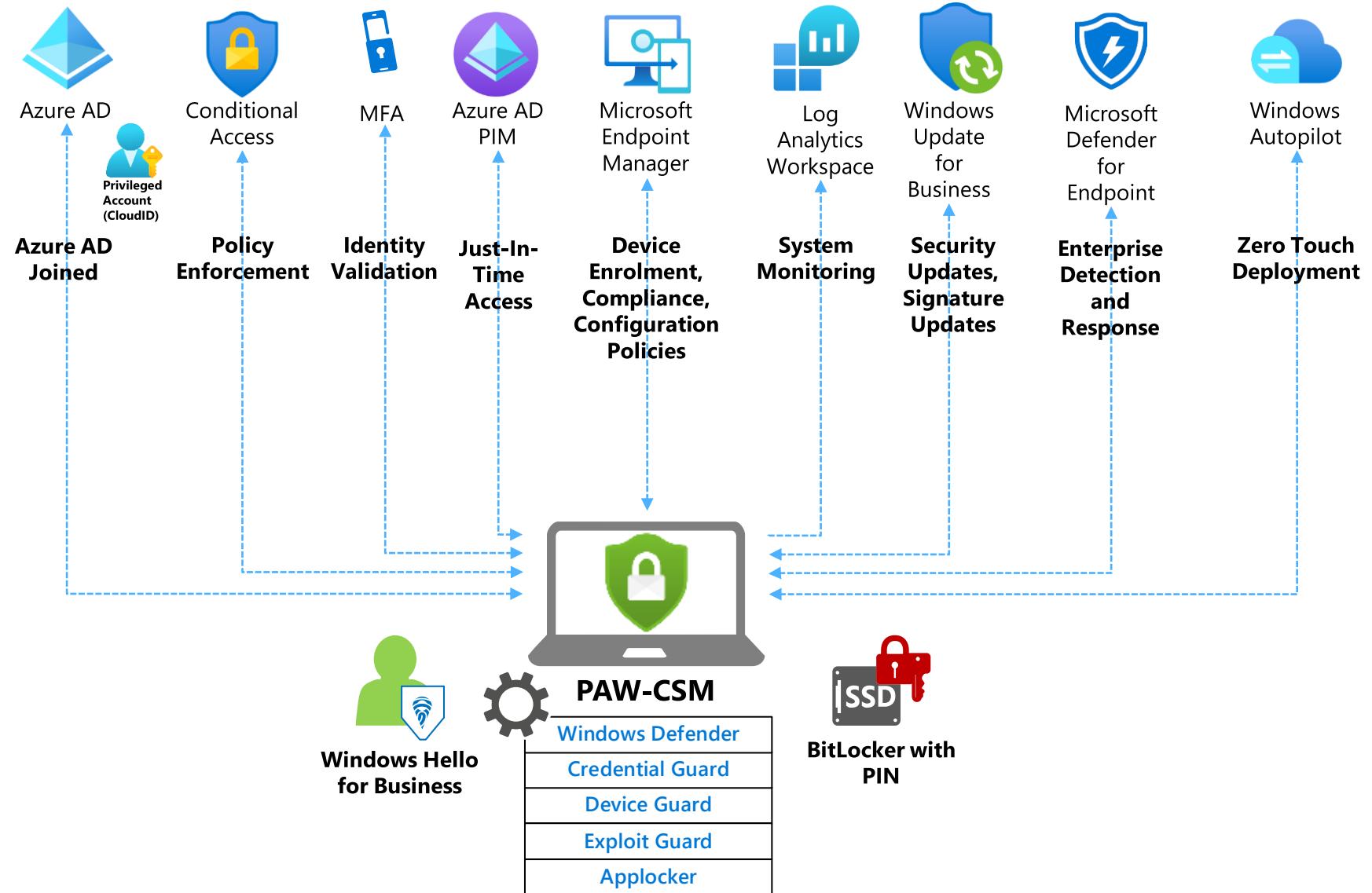


Microsoft
Cloud App
Security

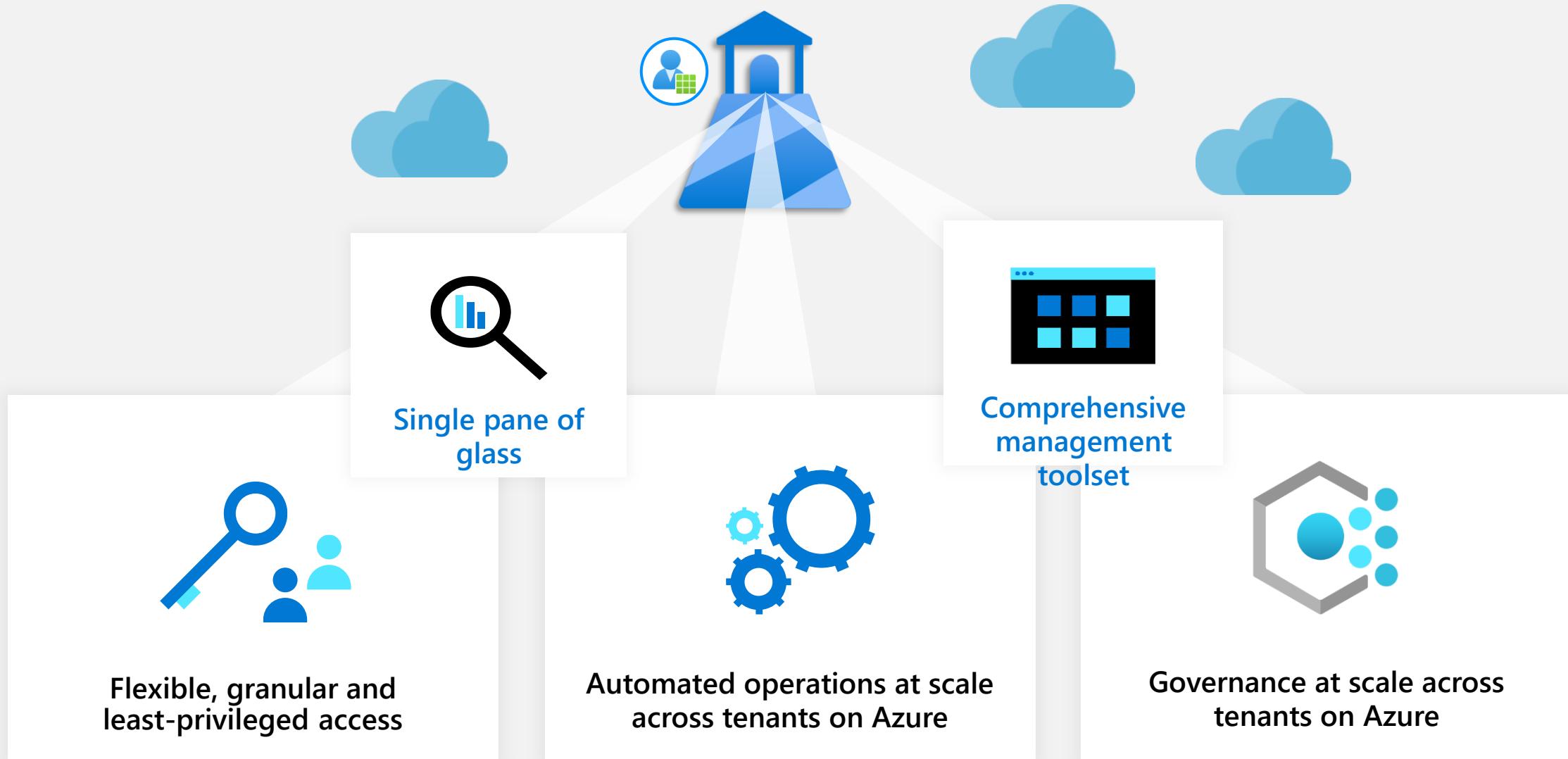


On-premises
& web apps

PAW-CSM Components



Azure Lighthouse: Service Provider value proposition



Verifiable Credentials

Matthijs Hoekstra

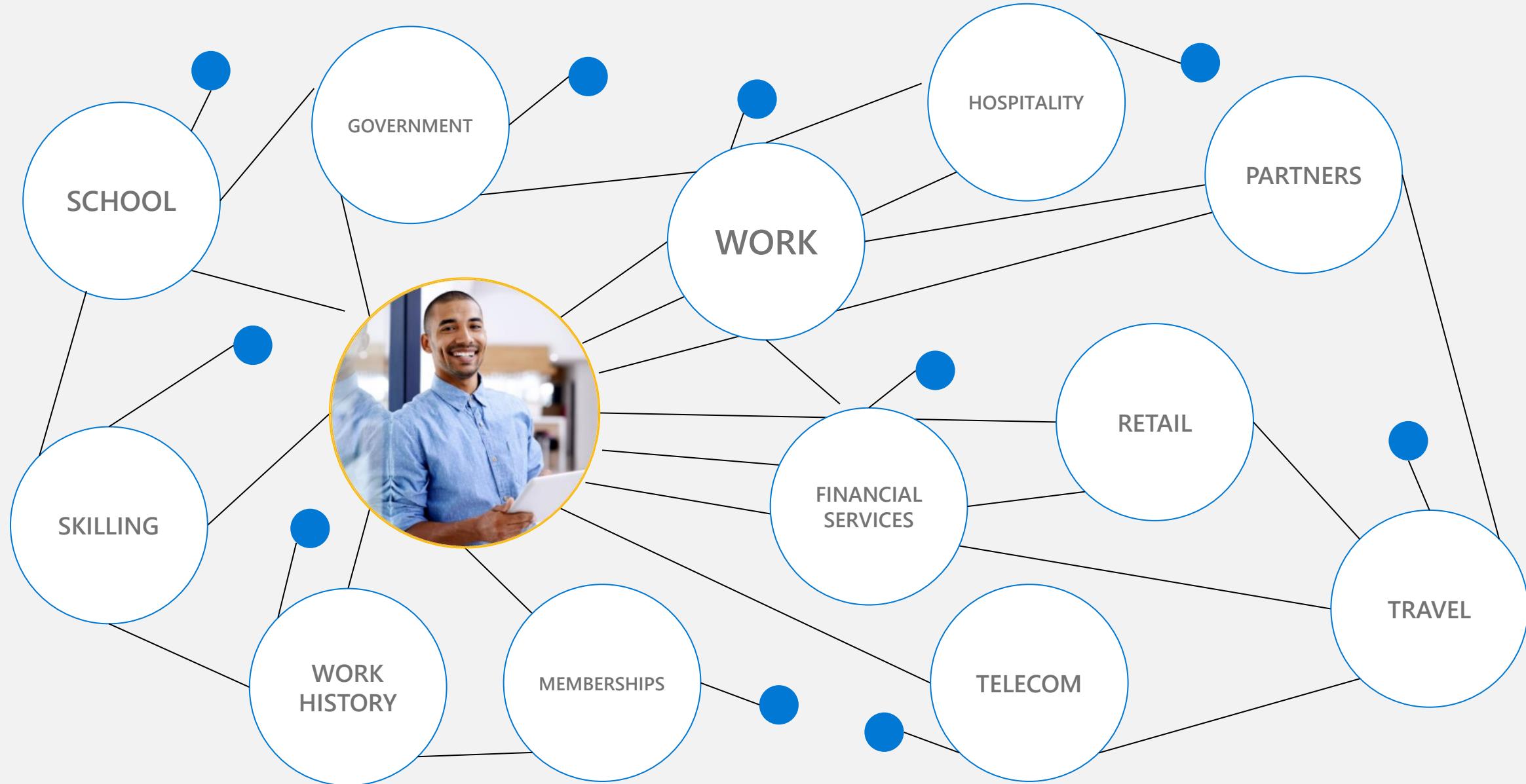
Matthijs.Hoekstra@Microsoft.com

Senior Product Manager

Microsoft Identity Engineering



Decentralized Identities: An ecosystem of trust

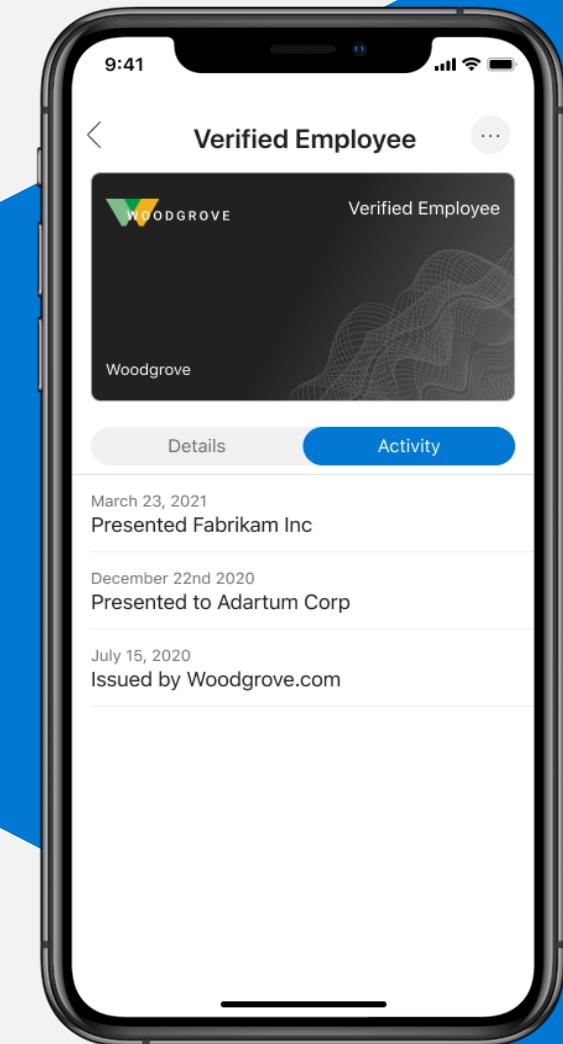


Verifiable Credentials

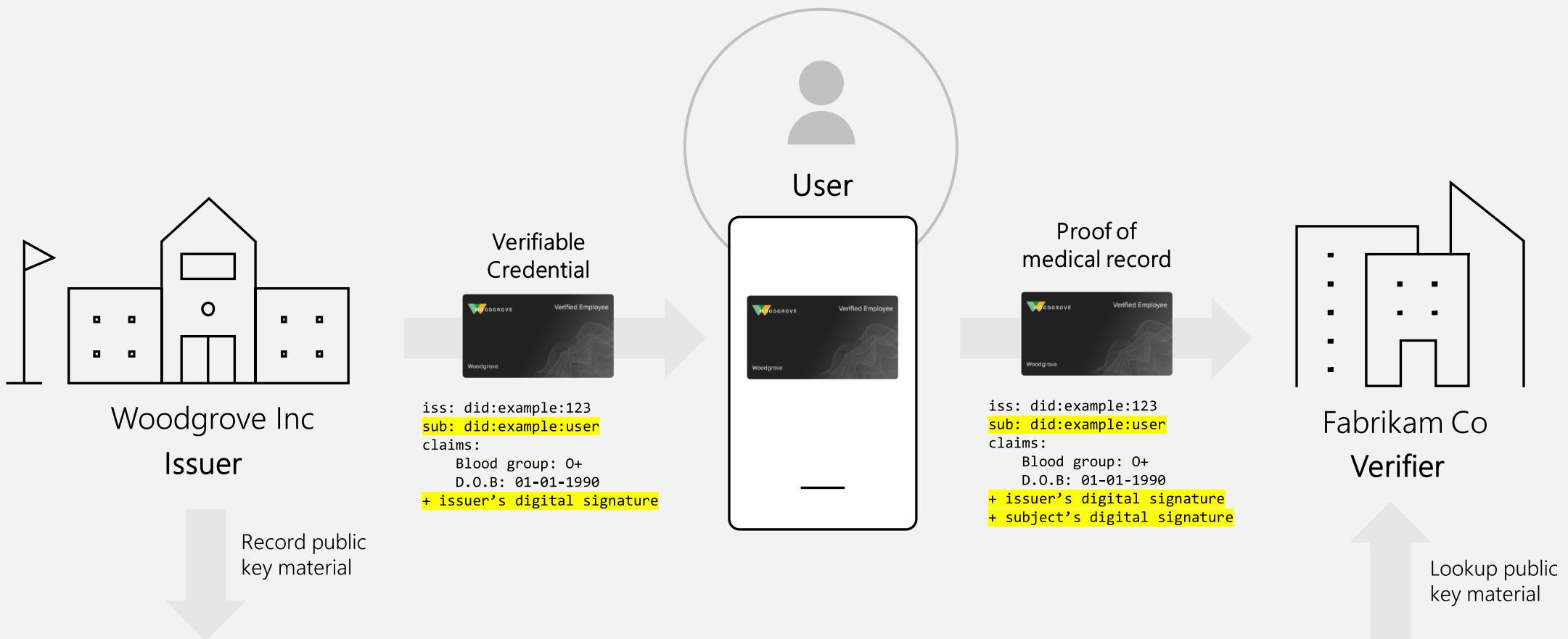
Issuer



Verifier



How does this work?



Distributed Public key infrastructure

Decades

Millions

1000s

192

countries

6000

identification
documents

organizational
attributes

individual ID
attributes

of experience to
go from idea to
implementation
within hours

Trusted identity verification providers



Adoption acceleration with technical solutions



Developed with global standards



Platform implementation

The diagram illustrates the platform implementation of Verifiable credentials across three main components:

- Issuer interface (Azure AD):** A screenshot of the Microsoft Azure portal showing the "Create a new credential" page. It includes fields for Name (Verified Employee), Subscription (Azure Premium), Display file URL (<https://myidstorage.blob.core.windows.net/credentials/IdentityCardDisplay.json>), and Rules file URL (<https://myidstorage.blob.core.windows.net/credentials/rules.json>). Buttons for "Create" and "Discard" are at the bottom.
- Developer tools (SDK + API):** A screenshot of a developer environment showing a code editor with a file named "Verify.JS". The code defines a permission request for "Employer.WorkHistory".

```
1 Verify.Employer.Workhistory
2   University.StudentID
3   CreditScoringAgency.Score
4   Employer.WorkHistory
5   IdentityVerifier.Selfie
6   BusinessClearingHouse.VerifiedBusiness
```

A preview window shows a mobile application interface titled "New permission request" with the "Employer.WorkHistory" option selected.
- End user wallet (Microsoft Authenticator):** A screenshot of a mobile phone displaying the Microsoft Authenticator app. It shows a "New permission request" screen with the "Employer.WorkHistory" option highlighted. The "Allow" button is visible at the bottom.

Issuer interface
(Azure AD)

Developer tools
(SDK + API)

End user wallet
(Microsoft Authenticator)

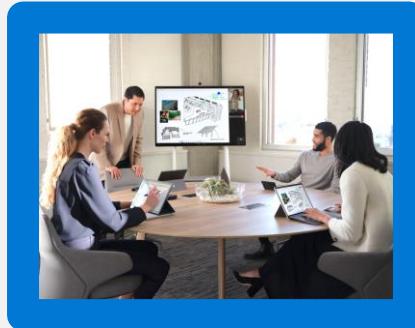
Trustworthy, fast, and easy identity verification

Example use cases for Enterprise



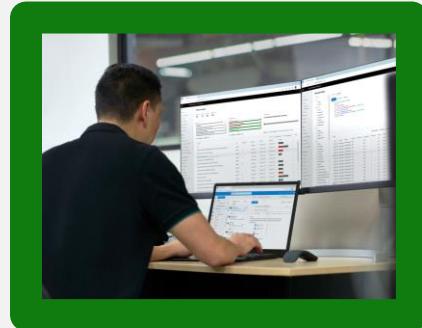
Employee onboarding & workplace credentials

Boost worker productivity



Access to high-value apps and resources

Secure B2B collaboration



Self-service account recovery & revocation

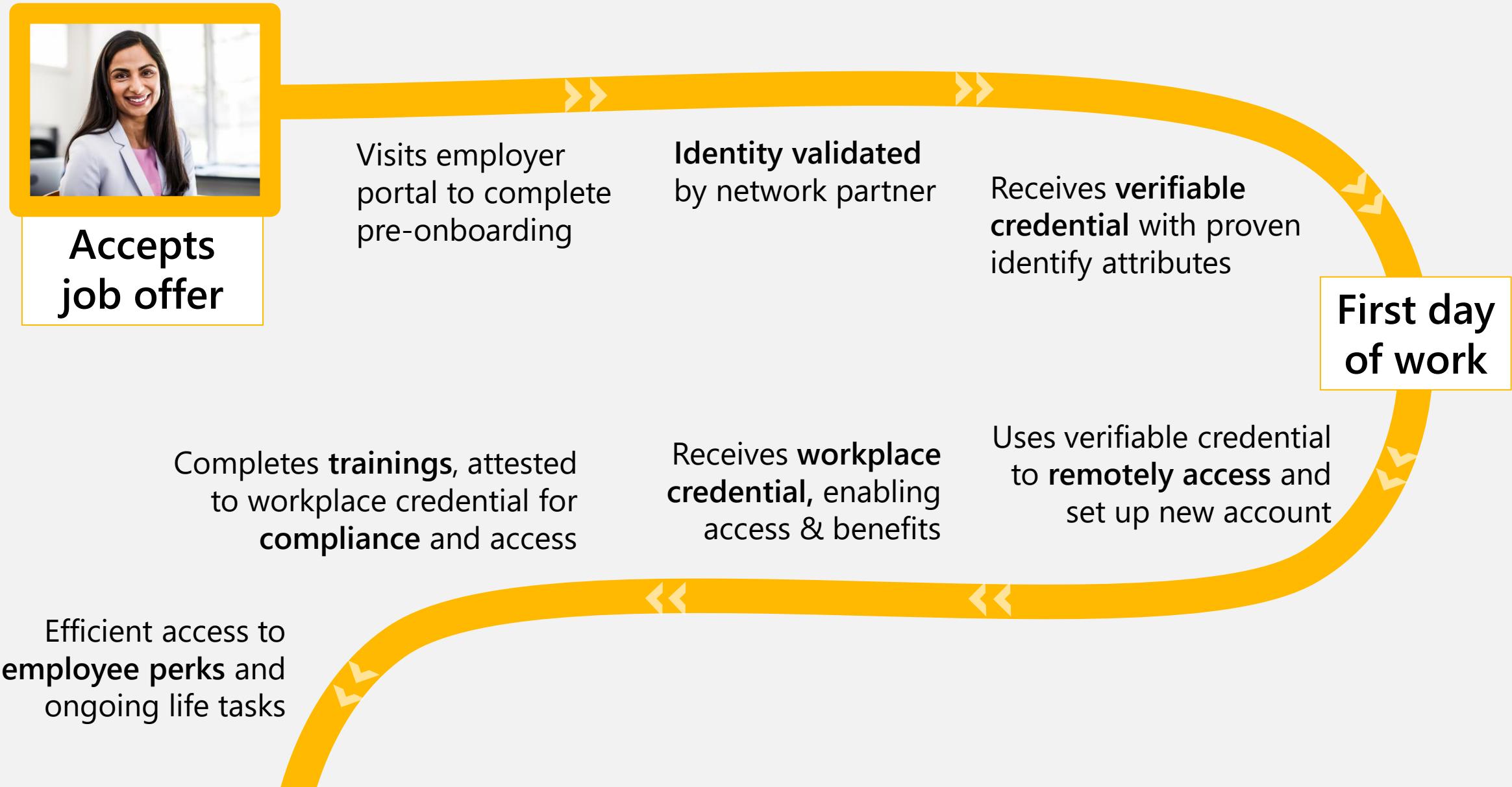
Streamline workflows

Employee Onboarding & Workplace Credentials

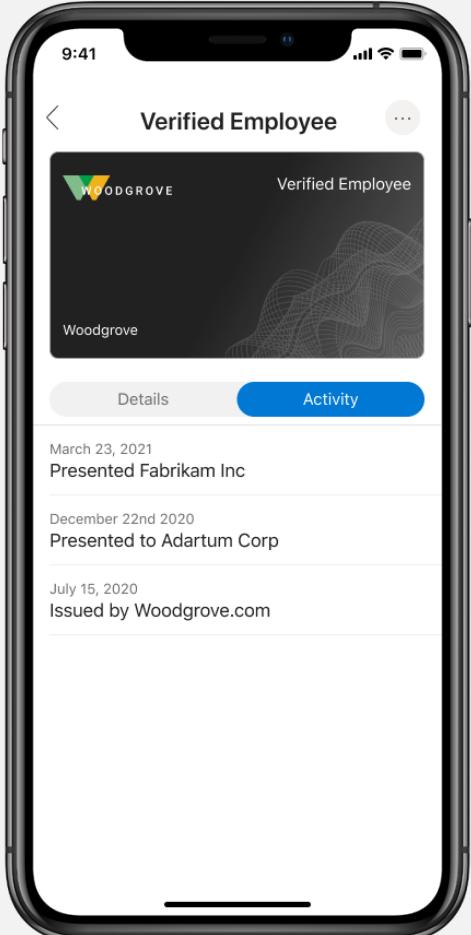
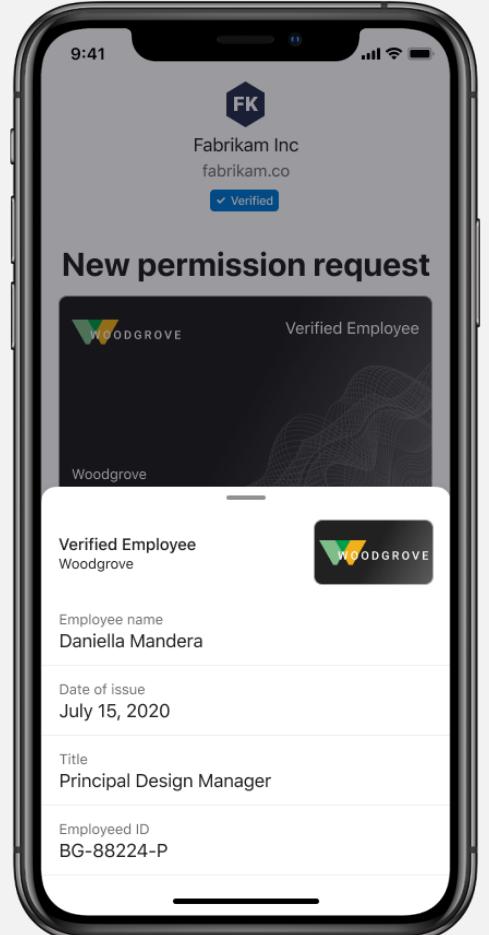
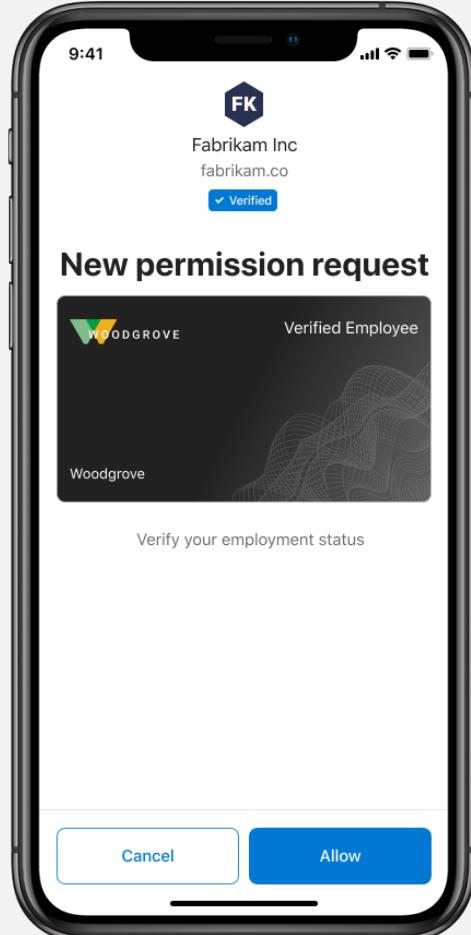
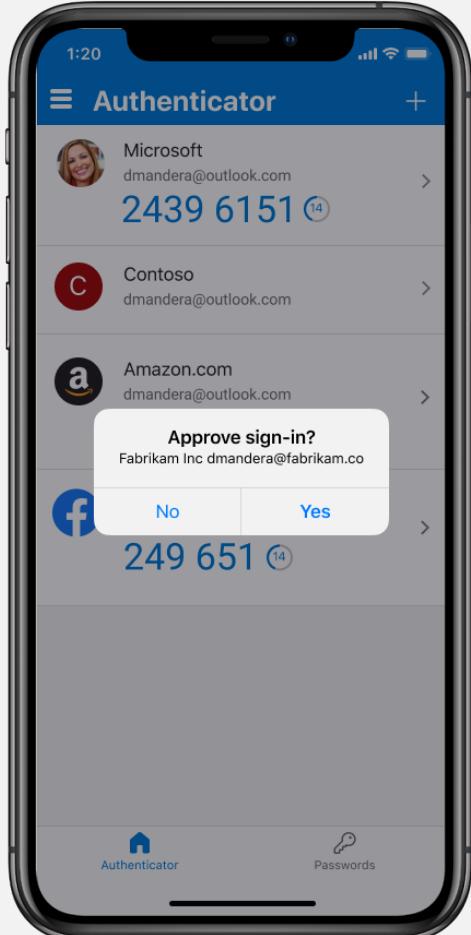
- Faster time-to-hire
- Faster time-to-productivity
- Reduces tedious proofing processes in work & life
- Credential portability for gig workers, transfers, new hires



Ongoing value journey: Worker productivity



End user experience: Workplace Credentials



easy to use and secure

verifiable

transparent

convenient

Employee Onboarding & Workplace Credentials

Demo

Access to high-value apps & resources

- Partners, contractors, gig workers, and employees
- Works with existing Enterprise Management in Azure AD
- More secure workflows for external access to resources
- Faster verification of individual's employer, credentials, project ID



Faster B2B collaboration

Starts project with external partners

Remotely receives partner access package via self-serve with workplace credential

Granted least-privilege access to collaboration tools and files to get the job done



At partner office, gets wifi access based on her workplace and **project credentials**

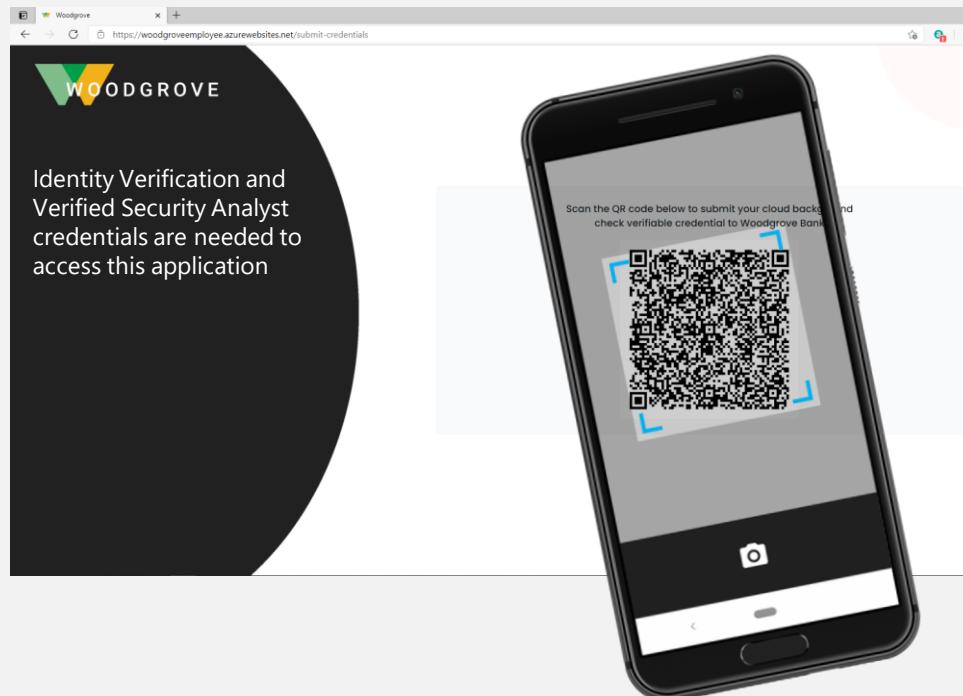
Secure access to applications

Quickly verify credentials and get access to sensitive resources that have advanced security requirements



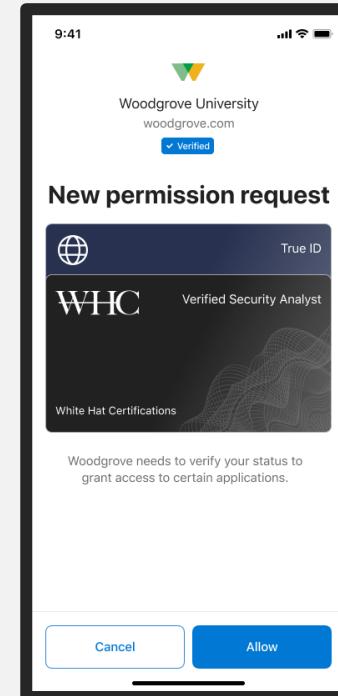
Sign in

User attempts to sign in to a high-privilege app at Woodgrove



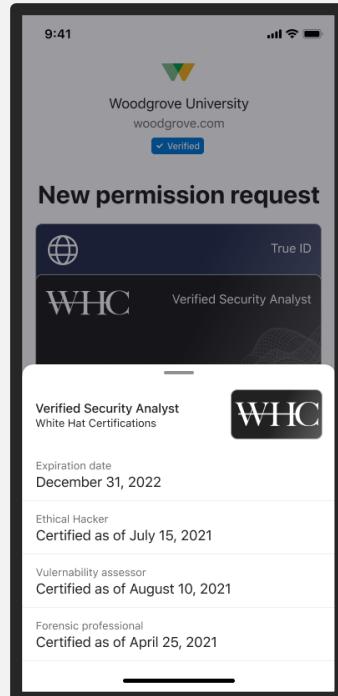
Presentation

User shares the requested verifiable credentials



Detailed view

User confirms which claims are being shared



Account recovery & revocation

- Reduce help desk calls, “approval fatigue”
- Faster, self-service account recovery, password reset
- Revocation immediately visible to all partners/verifiers



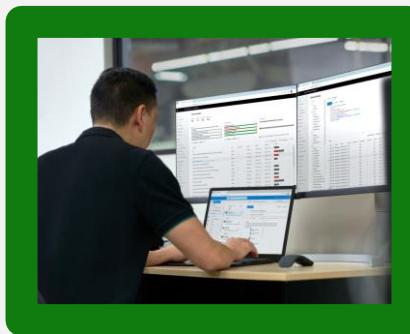
Streamlined workflows

Ransomware attack;
account is blocked

Self-service account
recovery enabled by
workplace credential

Employee leaves
the company

Termination date recorded
on workplace credential;
granted alumni status



Individual retains proof of
employment dates, job titles,
etc for verification by others



From idea to pilot with Azure AD Verifiable Credentials



Identify the right use case



Build storyboard



Phase 1: Prototype



Phase 2: Proof of Concept



Phase 3: Pilot

Customer Stories



Keio University

Leading research institution implementing digital student IDs so that students can certify enrollment, transcripts, and graduation information from a smartphone.



National Health Service

Using verified credentials to support staff movement between organizations, allowing staff to privately store their own verified records for employment, clearance, and other attributes.



Government of Flanders

Citizens will be able to request a verifiable credential with citizenship status for use across civic and private sectors, including the citizen portal, to streamline processes.

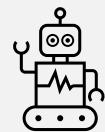
Asks

-  Commit to 0.5 day with 1 developer/technical architect to build a prototype

-  Provide candid feedback to help us identify gaps in the Product

-  Be a customer case study

Gives

-  Get a working Prototype > PoC > Pilot which is aligned to a business use case/scenario, free of charge

-  Access to expertise in Product Engineering to shape the solution to fit your specific needs

Resources

<http://identity.foundation>

Industry working group for all things Decentralized ID (DID)

<http://aka.ms/didwhitepaper>

White paper by Microsoft: approach for DID + Verifiable Credentials

<http://aka.ms/didexplained>

Quick overview

<https://youtu.be/Whc9Im-U0Wg>

Overview for developers: scenario walk-through and how-to

<http://aka.ms/didfordevs>

Developer documentation

<http://aka.ms/azuread/did>

Blogs (including scale and performance and self-owned key recovery)

Break
Please return at 15:15pm GMT





Cross-tenant access settings

Luciana Blanchard

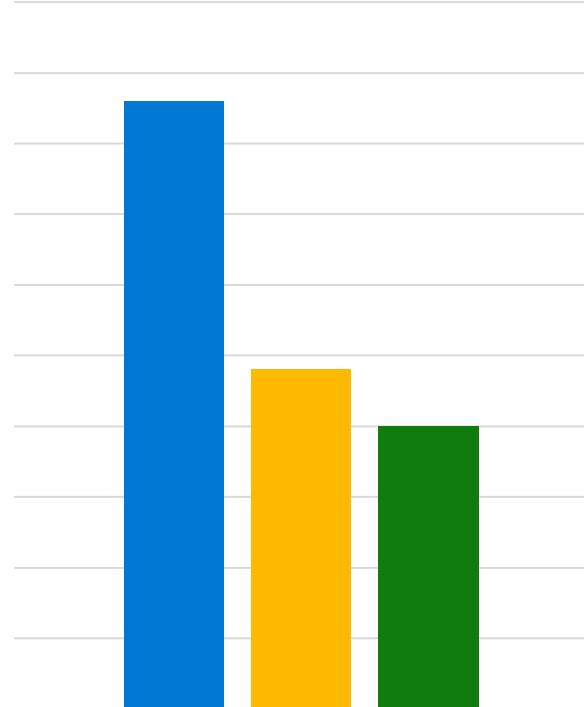
Luciana.Blanchard@microsoft.com

Global Partner Solutions UK

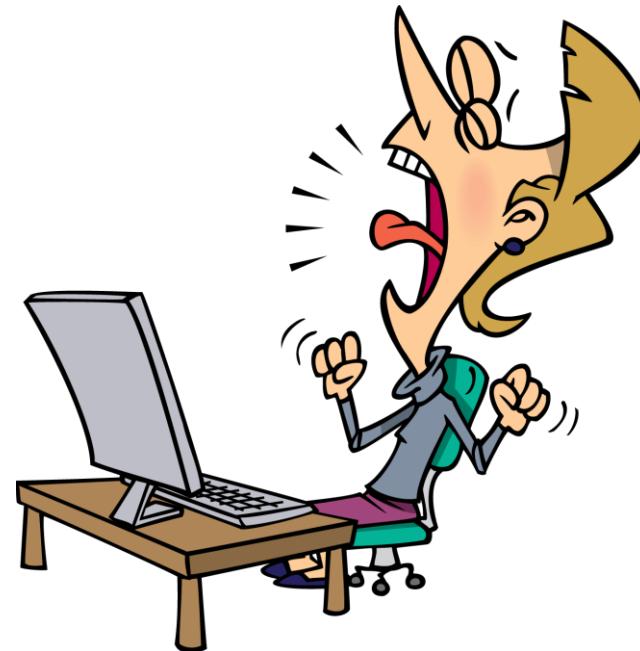


How is it going?

Azure AD launched B2B collaboration several years ago and has seen explosive growth and growing more than 100% in active usage YoY



However, consistent feedback was lack of controls for better security and productivity



What do customers want?



OUTBOUND



INBOUND

- Controls that apply to users in your Azure AD organization when signing into external Azure AD organizations.
- Prevent identities in your Azure AD organization from being used in un-sanctioned ways.

- Controls that apply to users from external Azure AD organizations signing into your Azure AD organization.
- Prevent un-sanctioned access to your resources.
- Controls that allow you to trust claims from external Azure AD organizations, for example trust MFA, trust managed devices claims.

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

 Delete

Target domains

*.fabrikam.com

example.com or *.example.com or example.*



Cross Tenant Access Settings

give you control at a Tenant level

Microsoft Azure Search resources, services, and docs (G+) Luciblanchard@dragon... DRAGONMANIA (DRAGONMANI... User icon

All services > External Identities

External Identities | Cross-tenant access settings (Preview) ...

Dragonmania - Azure Active Directory

Search (Ctrl+ /) Got feedback?

Overview Cross-tenant access settings (Preview) Add organization Refresh

Organizational settings Default settings

+ Add organization Refresh

Use cross-tenant access settings to manage collaboration with external Azure AD organizations. For non-Azure AD settings. [Edit or view collaboration restrictions](#)

Add organization X

Cross tenant settings

Add an external Azure AD tenant by typing one of its domain names.

contosoblanch.onmicrosoft.com X

Name
contosoblanch

Tenant ID
ac88b30b-41d7-495f-ad00-6aa7572af480

Cross Tenant Access Settings

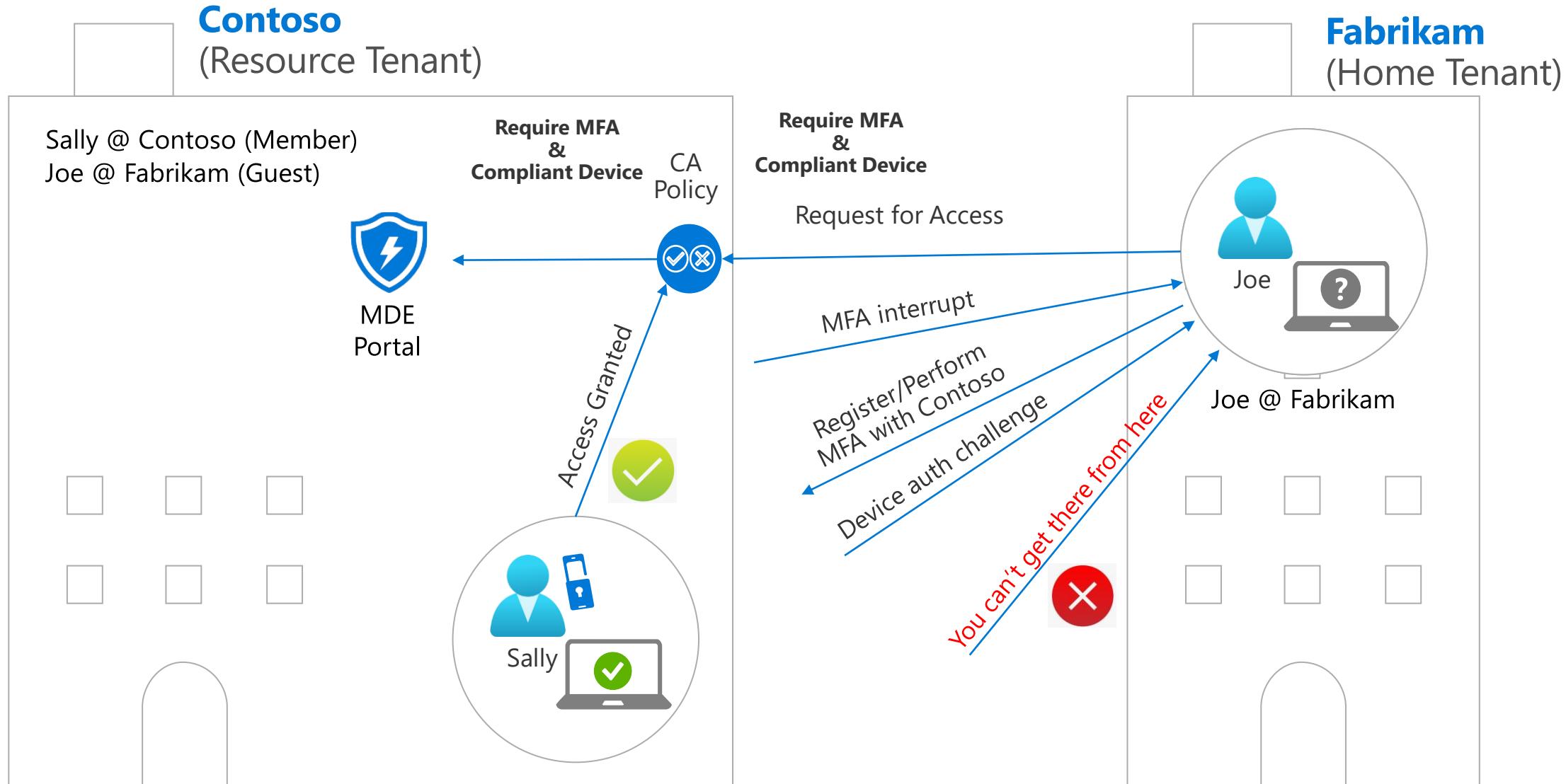
give you outbound & inbound **granular** control

Allow only **specific users or groups** from your organisation to access an external tenant.

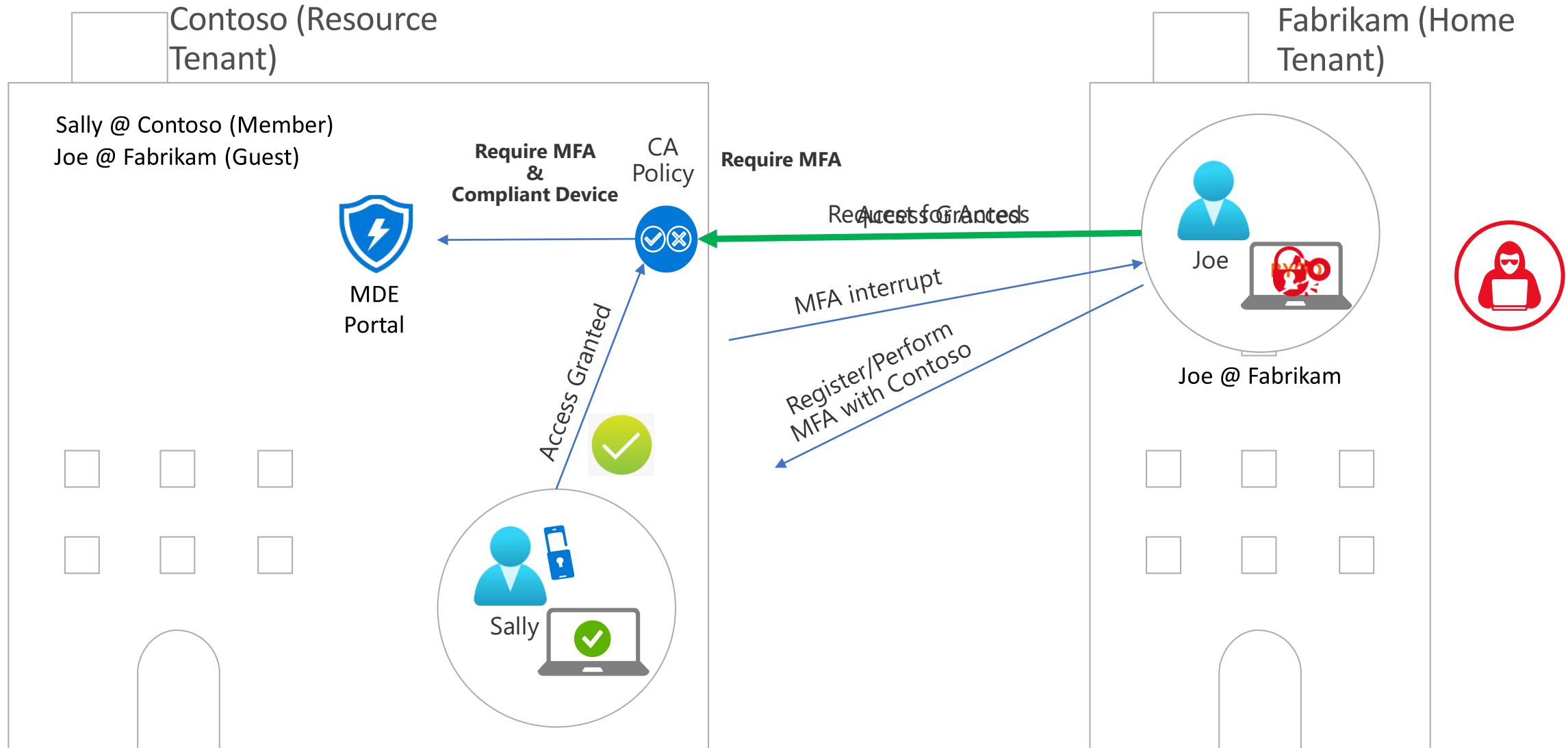
Allow only **specific users or groups** from an external tenant to access your organisation

The screenshot shows the 'Outbound access settings - contosoblanch' page in the Microsoft Azure portal. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and various icons. Below the navigation, the path 'All services > Dragonmania > External Identities >' is shown. The main title is 'Outbound access settings - contosoblanch'. A sub-section titled 'B2B collaboration' is selected, indicated by an underline. Below it, a description states: 'B2B collaboration outbound access settings determine whether your users can be invited to contosoblanch for B2B collaboration and added to their directory as guests. Below, specify whether your users and groups can be invited to contosoblanch and the external applications they can access.' A 'Learn more' link is provided. The 'Customize settings' radio button is selected and highlighted with a red box. Below this, there are two tabs: 'Users and groups' (selected) and 'External applications'. Under 'Access status', the 'Allow access' radio button is selected and highlighted with a red box. Under 'Applies to', the 'Select Dragonmania users and groups' radio button is selected and highlighted with a red box. A 'Add Dragonmania users and groups' button is available. A table lists a single entry: 'Communications' (User type: group). At the bottom, there are 'Save' and 'Discard' buttons.

Inbound Access w/o Cross Tenant Access setting



Inbound Access w/o Cross Tenant Access setting



Trust MFA from Guest User's Home Tenant

The screenshot shows the Microsoft Azure portal interface. At the top, there is a blue header bar with the Microsoft Azure logo, a search bar containing "Search resources, services, and docs (G+)", and several icons for notifications, settings, and help. On the right side of the header, the email address "luciblanchard@dragon..." and the name "DRAGONMANIA (DRAGONMANI..." are displayed, along with a user profile icon.

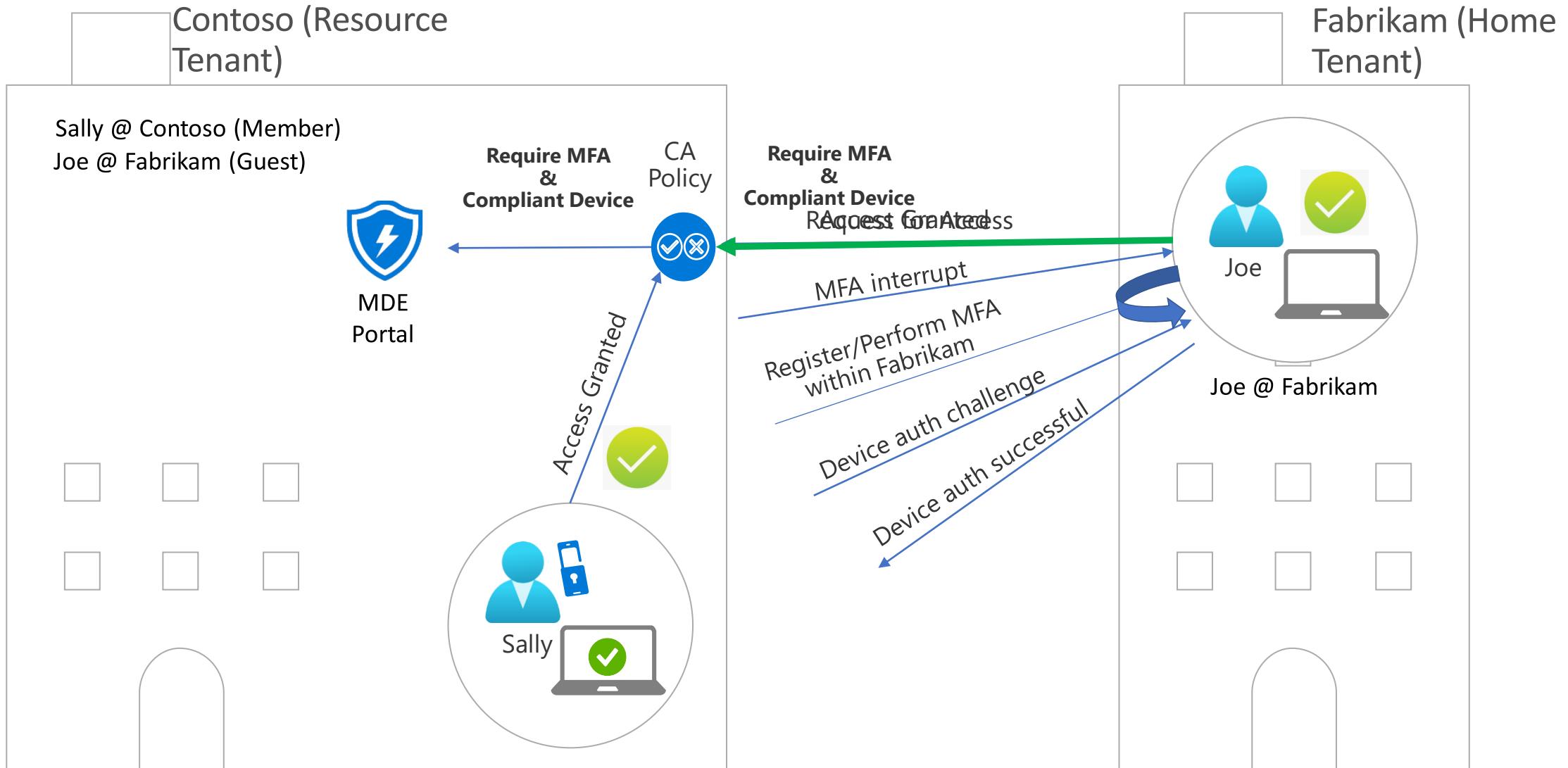
Below the header, the navigation path is shown as "All services > Dragonmania > External Identities >". The main title of the page is "Inbound access settings - contosoblanch".

Under the title, there are two tabs: "B2B collaboration" and "Trust settings", with "Trust settings" being the active tab. A descriptive text block states: "Configure whether your Conditional Access policies will accept claims from other Azure AD organizations when external users access your resources. The default settings apply to all external Azure AD organizations except those with organization-specific settings." Below this text, a note says: "You'll first need to configure Conditional Access for guest users on all cloud apps if you want to require multi-factor authentication or require a device to be compliant or hybrid Azure AD joined." followed by a "Learn more" link.

There are two radio button options: "Default settings" and "Customize settings", with "Customize settings" being selected. Under "Customize settings", there are three checkboxes:

- Trust multi-factor authentication from Azure AD tenants
- Trust compliant devices
- Trust hybrid Azure AD joined devices

Inbound Access w/ Cross Tenant Access setting



How can I minimize the risk?

[Aka.ms/CrossTenantWorkbook](https://aka.ms/CrossTenantWorkbook)

Microsoft Azure Search resources, services, and docs (G+/-)

All services > Dragonmania

Dragonmania | Workbooks | Gallery

Azure Active Directory

Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security

Monitoring

Sign-in logs
Audit logs
Provisioning logs
Log Analytics
Diagnostic settings
Workbooks

+ New Refresh Feedback Help Community Git repo Browse across galleries

Private and favorite Workbooks are deprecated and not accessible in Workbook gallery. If you want to retrieve them, follow these instructions. →

All Workbooks Public Templates My Templates

Filter by name or category Subscription : All Resource Group : All Reset filters

Quick start

Empty A completely empty workbook.

Recently modified workbooks (0)

Usage (10)

Sign-ins using Legacy Aut... Sign-ins Access Package Activity App Consent Audit
SSPR Reset Funnel Sign-In Analysis (Preview: ...) Identity Protection Risk An... Authentication Prompts A...
Tenant restriction insights Cross-tenant access activity

Before making changes, check Cross Tenant Activity Workbook!!

Cross Tenant Access Activity workbook gives you a summary of all inbound and outbound collaborations

Time range: Last 30 days ⓘ External Tenant ID: All external tenants ⓘ User principal name: All users ⓘ Application: All applications ⓘ Status: All ⓘ

Number of external tenants with cross-tenant access activity

27

Step 1 - Select external tenant

In the table below, select the External Tenant to focus on the details for the inbound and outbound activity with that external tenant.

Filters per tenant, per user, per app give you a clear view of collaboration

External Tenant	↑↓	Outbound Sign-Ins Total	↑↓	Outbound Sign-In Failures	↑↓	Outbound Users	↑↓	Outbound Apps	↑↓	Inbound Sign-Ins Total	↑↓	Inbound Sign-In Failures	↑↓	Inbound Users	↑↓	Inbound Apps	↑↓
72f988bf-86f1-41af-91ab-2d7...	196			60		51		7		336		202		5		7	
556b80b7-c9fc-41fd-92da-c3...	36			17		3		3		0		0		0		0	
8c3af30a-0c63-43b4-8b5b-98...	23			5		2		3		3		1		1		2	
b4c546a4-7dac-46a6-a7dd-e...	3			3		2		1		0		0		0		0	
d8a91a12-d047-483f-84c5-d...	4			3		1		2		0		0		0		0	
9026c5f4-86d0-4b9f-bd39-b7...	3			2		1		1		0		0		0		0	
3cbcc3d3-094d-4006-9849-0...	4			2		1		1		0		0		0		0	
859c0fc9-4300-47be-b473-59...	2			2		1		1		0		0		0		0	
e0793d39-0939-496d-b129-1...	3			2		1		2		0		0		0		0	

Cross Tenant Access Activity workbook lets you drill down to get detailed information

Step 2 - Select outbound or inbound access activity

Inbound sign-in status summary for selected external tenant

Inbound sign-in status summary for selected external tenant				...		
Sign-In Status C...↑↓	Status	↑↓	Sign-In Status Code	↑↓	Sign-In Status Reason	↑↓
3	Success	0			Success	

Was the sign-in successful?

Was it a failure?

What were the failures?

What applications are being accessed in the external tenant?

Which users are accessing this external organization?

Step 3 - Review local applications accessed from the external tenant

After selecting the external tenant above, select an application below to filter by external users accessing that application in Step 4.

Inbound application activity by selected tenant

Local Resource App Id	↑↓	Local Resource App Display Name	↑↓	Local Client App Id	↑↓	Local Client App Display Name	↑↓	Inbound ...↑↓	↑↓	Inbound ...↑↓	↑↓	Inbound ...↑↓
00000002-0000-0000-000000000000		Windows Azure Active Directory		0000000c-0000-0000-c000-000000000000		Microsoft App Access Panel		1		1		0
00000003-0000-0000-c000-000000000000		Microsoft Graph		2793995e-0a7d-40d7-bd35-6968ba142197		My Apps		1		1		0
00000002-0000-0000-c000-000000000000		Windows Azure Active Directory		b2ebdf15-9fb0-4d2b-9287-dfdc9a8f650		AWS Single-Account Access-Account-AzureADIntegration		1		1		0

Roles that can manage cross tenant access



The following roles are able to **fully manage** cross tenant access settings

Global Administrator
Security Administrator



The following roles can **read** cross tenant access settings

Global Administrator
Security Administrator
Global Reader

These apply to managing the settings via API or through the Azure Portal

Licensing Requirements

External users and groups

Applications

i Blocking all users by default blocks all external applications

Access status

- Allow access
- Block access

Applies to

- All external users and groups
- Select external users and groups
- Default settings
- Customize settings
- Trust multi-factor authentication from Azure AD tenants
- Trust compliant devices
- Trust hybrid Azure AD joined devices

**AAD Premium P1
Licensing is required**



User Experience

Add other users and groups

Inbound access settings

Contact the external organization to get the object IDs for the users or groups you want to add.

Add external user or group id user

Customers will need to use a **GUID** provided by the partner they are collaborating with

Customers will need to use a **GUID** provided by the partner they are collaborating with

Add other external applications

Outbound access settings

Enter the appid of the external application you want to allow outbound access to.

Add external app id

Limits and considerations

If a customer adds a **lot of partners**, they will hit our **policy size limit – 25kb**; we are working on a scalable solution, but this limit will be in place for the next **~6 months**

If customers **block all inbound/outbound** access by default, **this will block Office Message Encryption from working** if they send encrypted emails; recommendation is to add the OME app id in to the policy as an allowed app by default if customers choose to block all inbound/outbound access.

Identity Resources

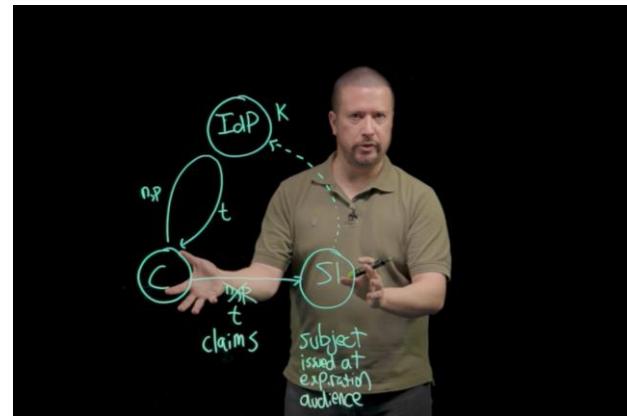


Learn more about Cross Tenant Access Settings

[Aka.ms/CrossTenantWorkbook](https://aka.ms/CrossTenantWorkbook)

[Aka.ms/CrossTenantOverview](https://aka.ms/CrossTenantOverview)

[Aka.ms/CrossTenantGraphAPI](https://aka.ms/CrossTenantGraphAPI)



Stay current with the latest Identity news

[Aka.ms/identityyoutube](https://aka.ms/identityyoutube)

[Aka.ms/azureadblog](https://aka.ms/azureadblog)

[Aka.ms/azureaddocs](https://aka.ms/azureaddocs)

Thank you!

Granular Delegated Admin Privileges (GDAP) in CSP

Gabriele Glodenyte
Partner Business Manager

Granular Delegated Admin Privileges

Summary

Microsoft has released a technical preview for GDAP in CSP which is now available via Partner Center and API.

Details

With the new capability, partners can control more granular and timebound access to their customers' workloads than the current Delegated Admin Privileges (DAP). This means that partners can better address security concerns from their customers. Partners can also provide more services to customers who are uncomfortable with the current levels of partner access and who have regulatory requirements to **provide only least privileged access to partners**.

We recommend that partners start their transition from DAP to GDAP as soon as possible to minimize security risk. In FY22 Q4, Microsoft will begin **disabling DAP relationships that have been inactive** for 90 days. Shortly after, we will start **transitioning active DAP** relationships to limited GDAP roles.

Next Steps

- Inform the relevant stakeholders in your organization about the upcoming changes.
- Start planning your transition from DAP to GDAP using the resources available within the [Operations Readiness gallery collection](#) and [Partner Center documentation](#).

Next Steps for Partner Success



Security, Compliance, Identity Enablement Guide for Partners

Access the latest partner-facing version here:
<https://aka.ms/scipartnerenablement>

Simplified Guide to SCI Partner training resources for the role-based exams, learning journeys across Security, and other key resources to support you and your organization on your skilling journey.

Security, Compliance, Identity Certifications and Exams

Fundamental Certifications

Microsoft Security, Compliance, and Identity Fundamentals (SC-900)

Training includes

- 7 hours of Microsoft Learn content
- 8 hours of exam prep instructor training
- 1-day virtual training day

Associate Certifications

Microsoft Security Operations Analyst (SC-200)

Training includes

- 30 hours of Microsoft Learn content
- 10 hours of exam prep instructor training
- 4-day instructor-led training (English, Japanese, Chinese (Simplified), Korean)

Microsoft Identity and Access Administrator (SC-300)

Training includes

- 12 hours of Microsoft Learn content
- 8 hours of exam prep instructor training
- 4-day instructor-led training (English, Japanese, Chinese (Simplified), Korean)

Microsoft Information Protection Administrator (SC-400)

Training includes

- 10 hours of Microsoft Learn content
- 8 hours of exam prep instructor training
- 2-days of instructor-led training (English, Japanese, Chinese (Simplified), Korean)

Expert Certifications

Coming Soon Microsoft Cyber Security Architect

Online modules coming soon

This page lists the certifications and exams that are recommended for partners looking to build and extend their Microsoft security, compliance, and identity practices.

The [Microsoft Security, Compliance, and Identity certification portfolio](#) includes the following certifications:

- Microsoft Security, Compliance, and Identity Fundamentals
- Microsoft Security Operations Analyst
- Microsoft Identity and Access Administrator
- Microsoft Information Protection Administrator
- Azure Security Engineer
- Microsoft 365 Security Administrator
- Microsoft Cybersecurity Architect

*Azure Network Engineer Associate is categorized in the Azure certification portfolio and is also relevant to our partners.

Go here for the latest certification roadmap [Microsoft training and certifications](#).

- Go here for the latest certification roadmap [Microsoft training and certifications](#).

Microsoft Cybersecurity Reference Architectures

We are excited to announce an **update to the Microsoft Cybersecurity Reference Architectures (MCRA)**. The MCRA describes Microsoft cybersecurity capabilities. The diagrams describe how Microsoft security capabilities integrate with Microsoft platforms and third-party platforms such as Microsoft 365, Microsoft Azure, third-party apps such as ServiceNow and Salesforce, and third-party platforms such as Amazon Web Services (AWS) and Google Cloud Platform (GCP).

[View the update and download the file here.](#)

Capabilities

What cybersecurity capabilities does Microsoft have?



Build Slide

Azure Native Controls

What native security is available?



Attack Chain Coverage

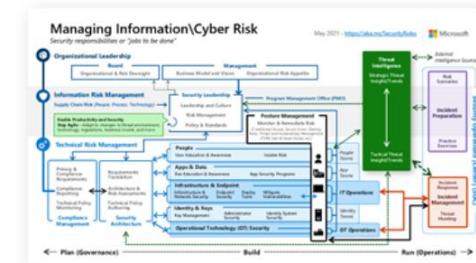
How does this map to insider and external attacks?



Build Slide

People

How are roles & responsibilities evolving with cloud and zero trust?



Multi-Cloud & Cross-Platform

What clouds and platforms does Microsoft protect?



aka.ms/MCRA | May 2021 |  Microsoft

Zero Trust User Access

How to validate trust of user/devices for all resources?



Security Operations

How to enable rapid incident response?



Operational Technology

How to enable Zero Trust Security for OT?





Share your thoughts, **feedback** via our survey!
<https://aka.ms/paw-feedback>

- Complete the **Privileged Access Management** reading:
[Developing a privileged access strategy | Microsoft Docs](#)
- Pass the **SC-300 Microsoft Identity & Access Administrator exam**
- [**Cloud Accelerator**](#) for Securing Identities Workshops
- **Consider incorporating PAW-CSM into your practice**
- **Share the training** and materials with others at your organization
- **Help your customers** with their security needs across the Microsoft security stack

Contact your local GPS Team to get started!
UK – protectanddefend@microsoft.com



Thank you! Feedback:
<https://aka.ms/paw-feedback>