Microsoft Security

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

Microsoft Security

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

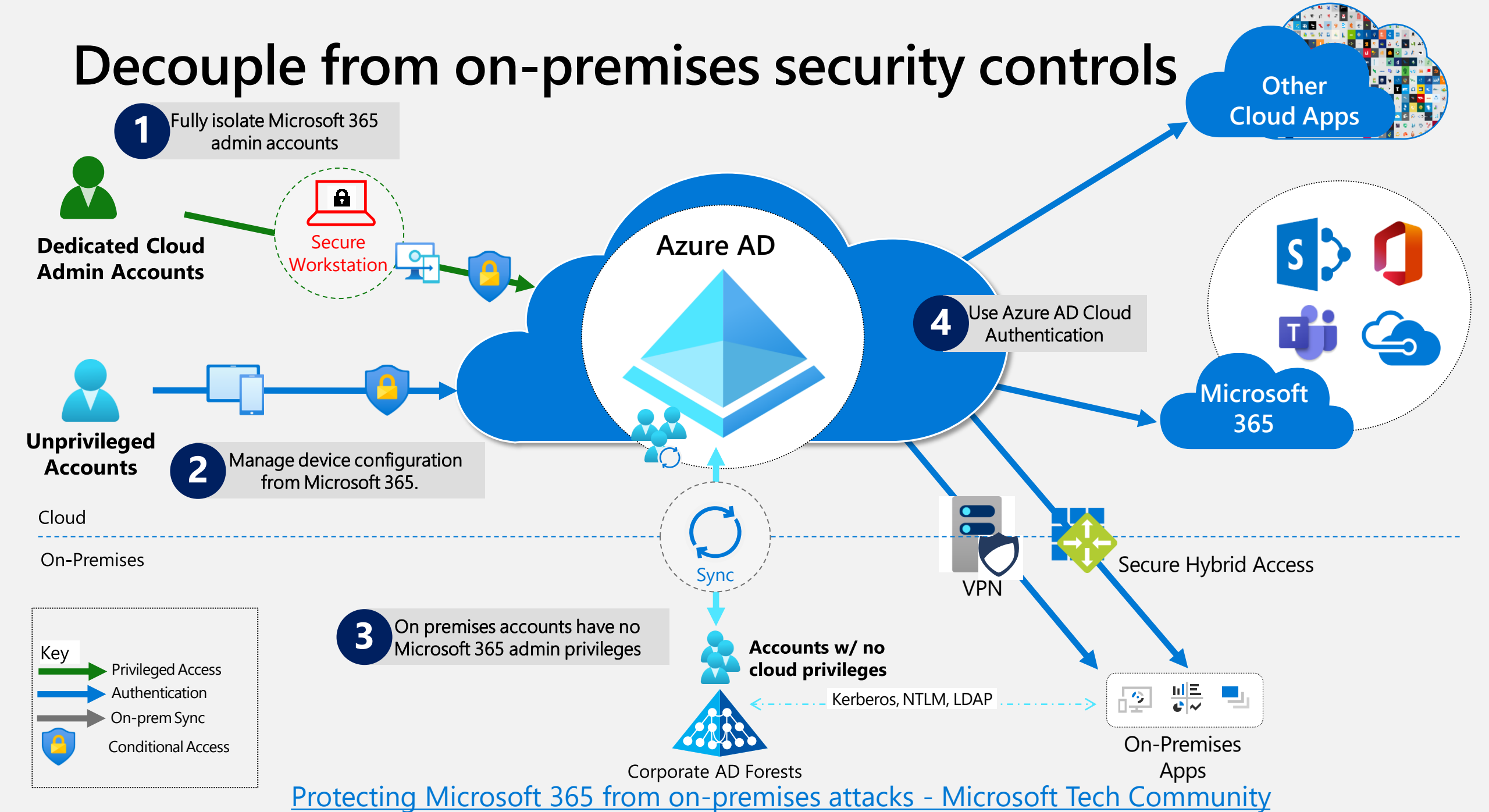
Reduce standing privilege

- Use just-in-time elevation of permissions

Clean keyboard (clean source)

- Assurance in device performing administration

Decouple from on-premises security controls



[Protecting Microsoft 365 from on-premises attacks - Microsoft Tech Community]

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."

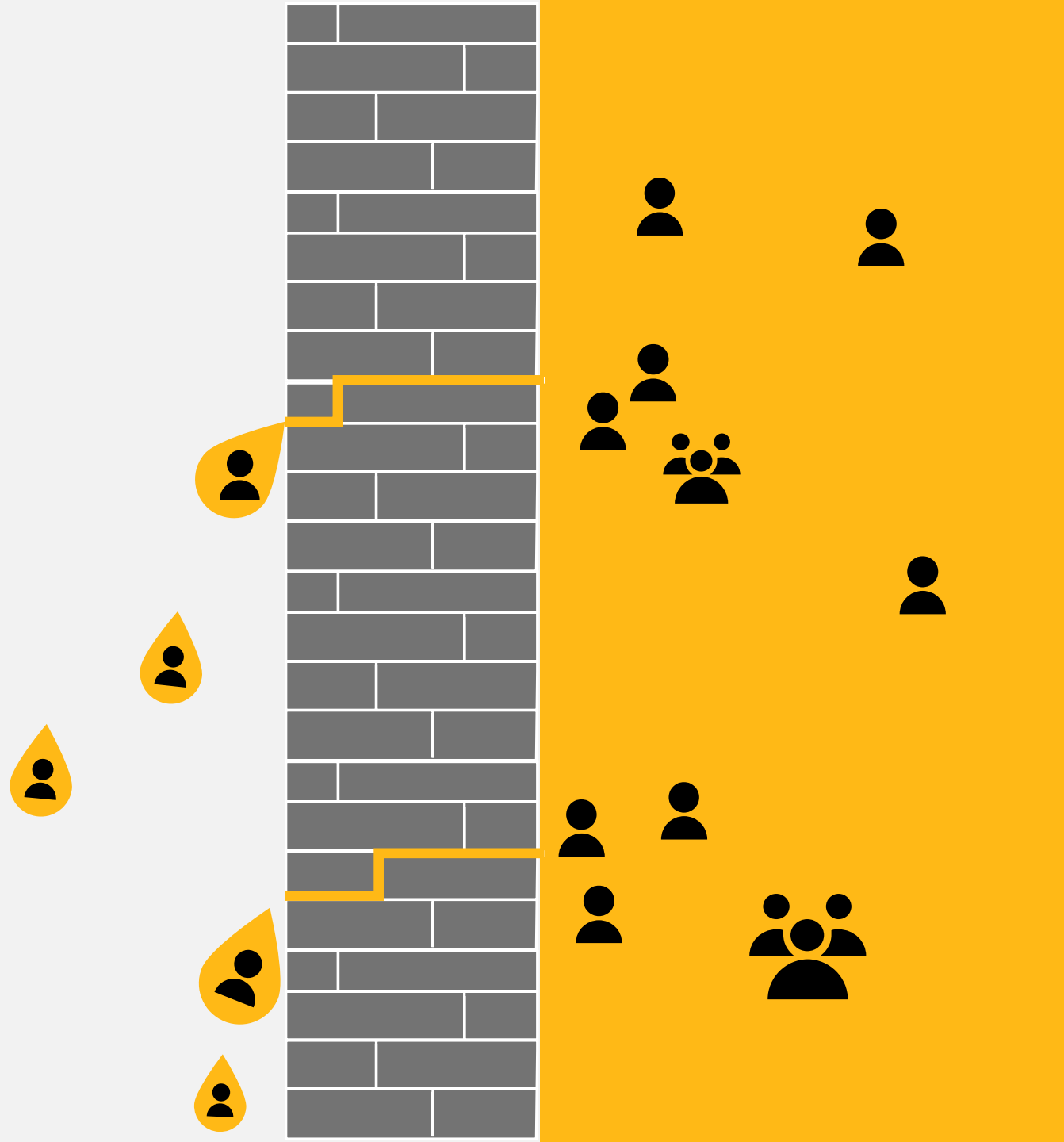
https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_3

Attackers are like water

Attackers take path of least resistance to achieve objectives

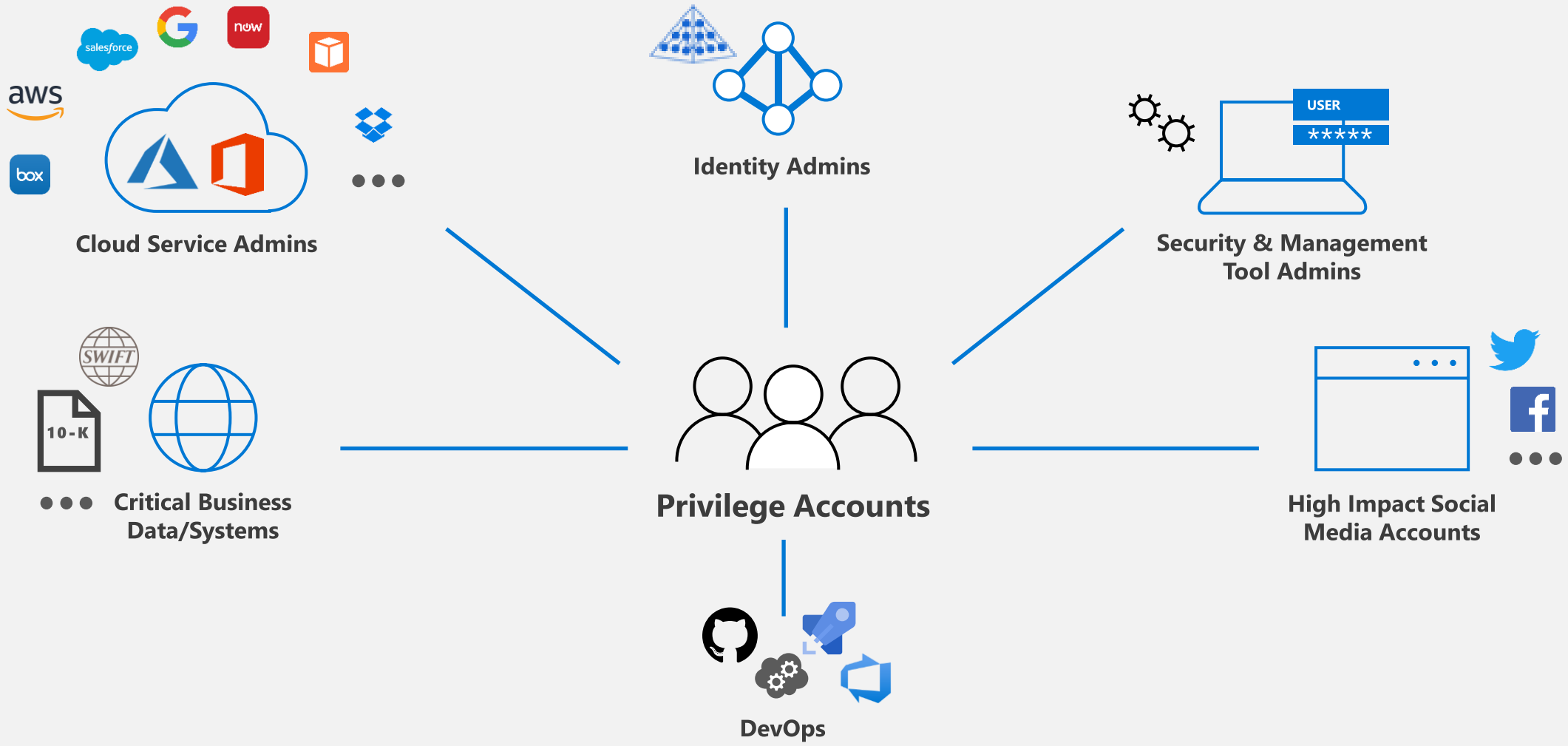
- Established paths/methods
- Easiest new openings

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



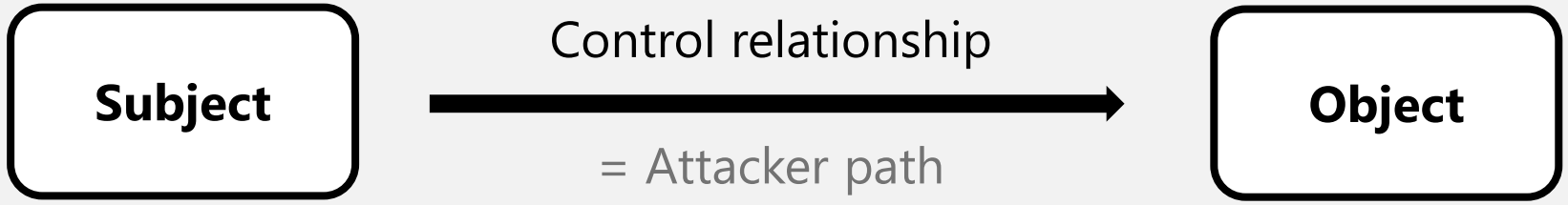
Privileged Access is more than Administrators

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



Subject

Control relationship

= Attacker path

Object

User Account

Access data

= steal, modify or encrypt data

Business Critical Data / Systems

Workstation or Device

Logon and run apps with credentials

= steal credentials

User Account

Management and Security Tools

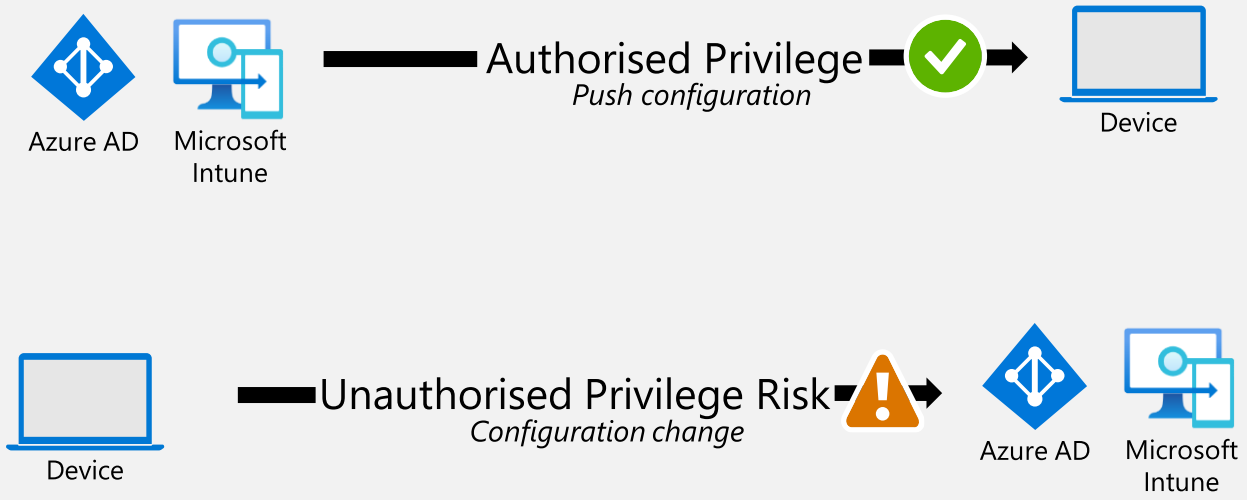
Manage with agent or service account

= install malware

Workstation or Server

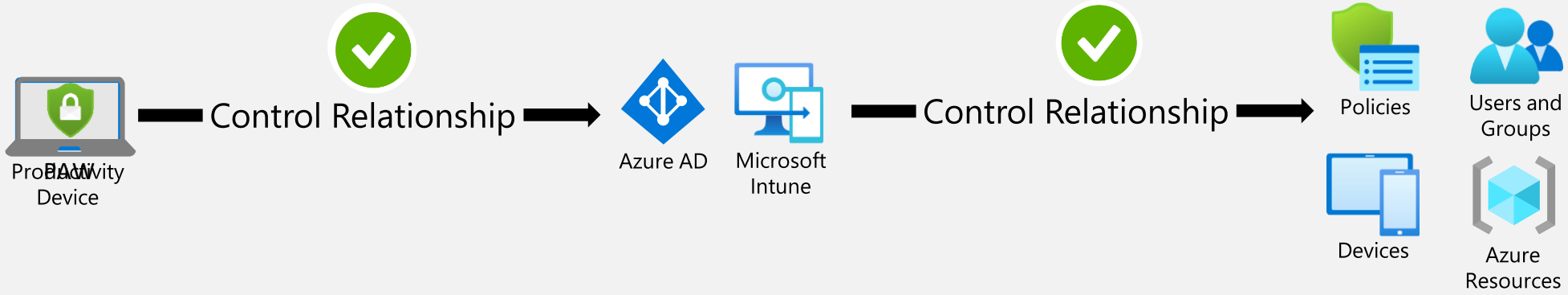
Clean Source and Clean Keyboard – Architecture and Design

- System is not dependent on lower trust systems



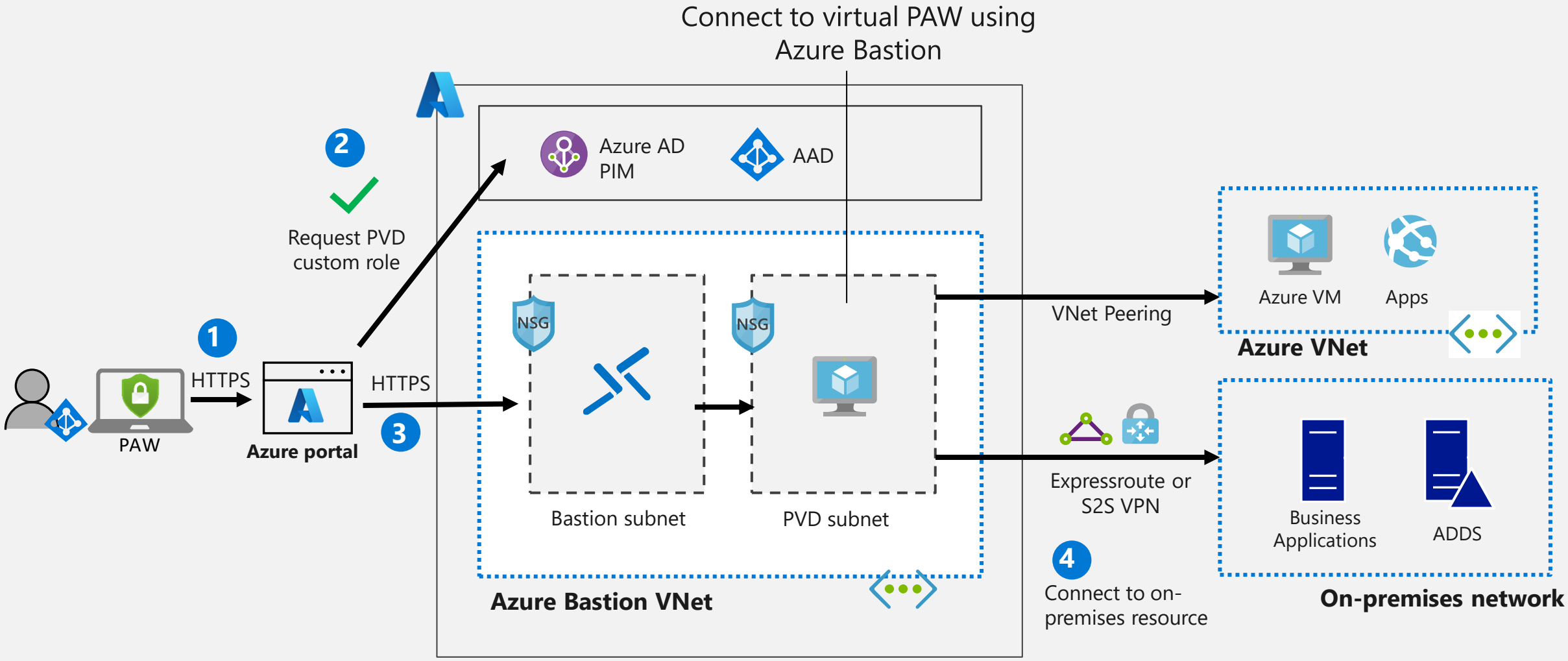
Clean Source and Clean Keyboard – Azure AD Control Relationship

- 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



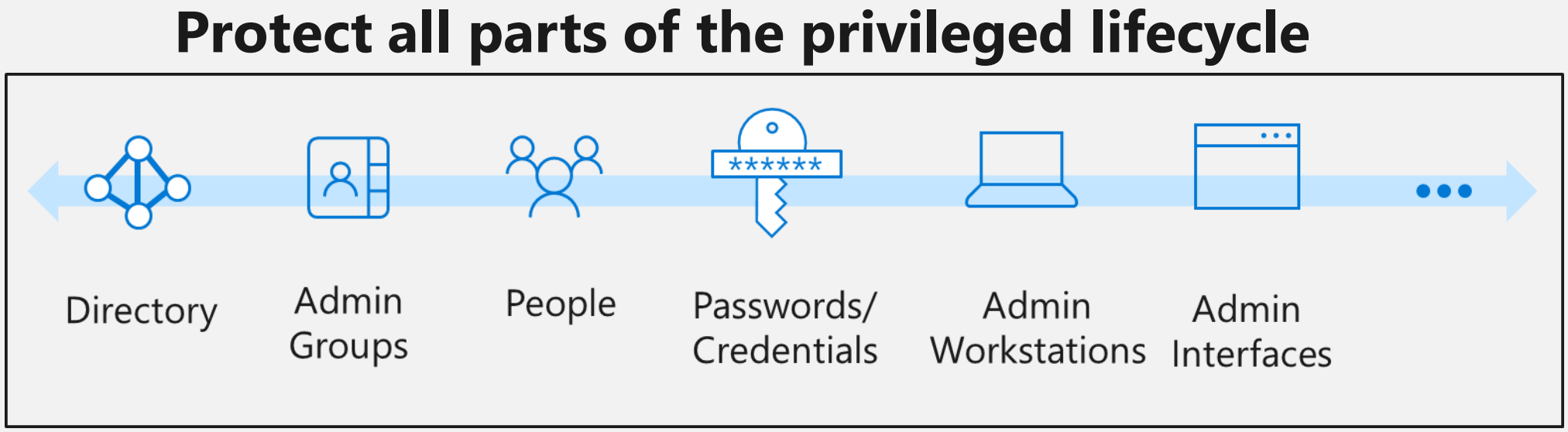
Microsoft Security

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



PAW : Key element of protecting assets anywhere with Zero Trust

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

User

- Groups/Role
- Location
- Privileges
- Session risk
- User Risk

Device

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

Microsoft Azure AD

Microsoft 365 Defender

Microsoft Defender for Endpoint

Microsoft Endpoint Manager

Security & Compliance Policy Engine

Microsoft Information Protection

Microsoft Cloud App Security

Microsoft Cloud

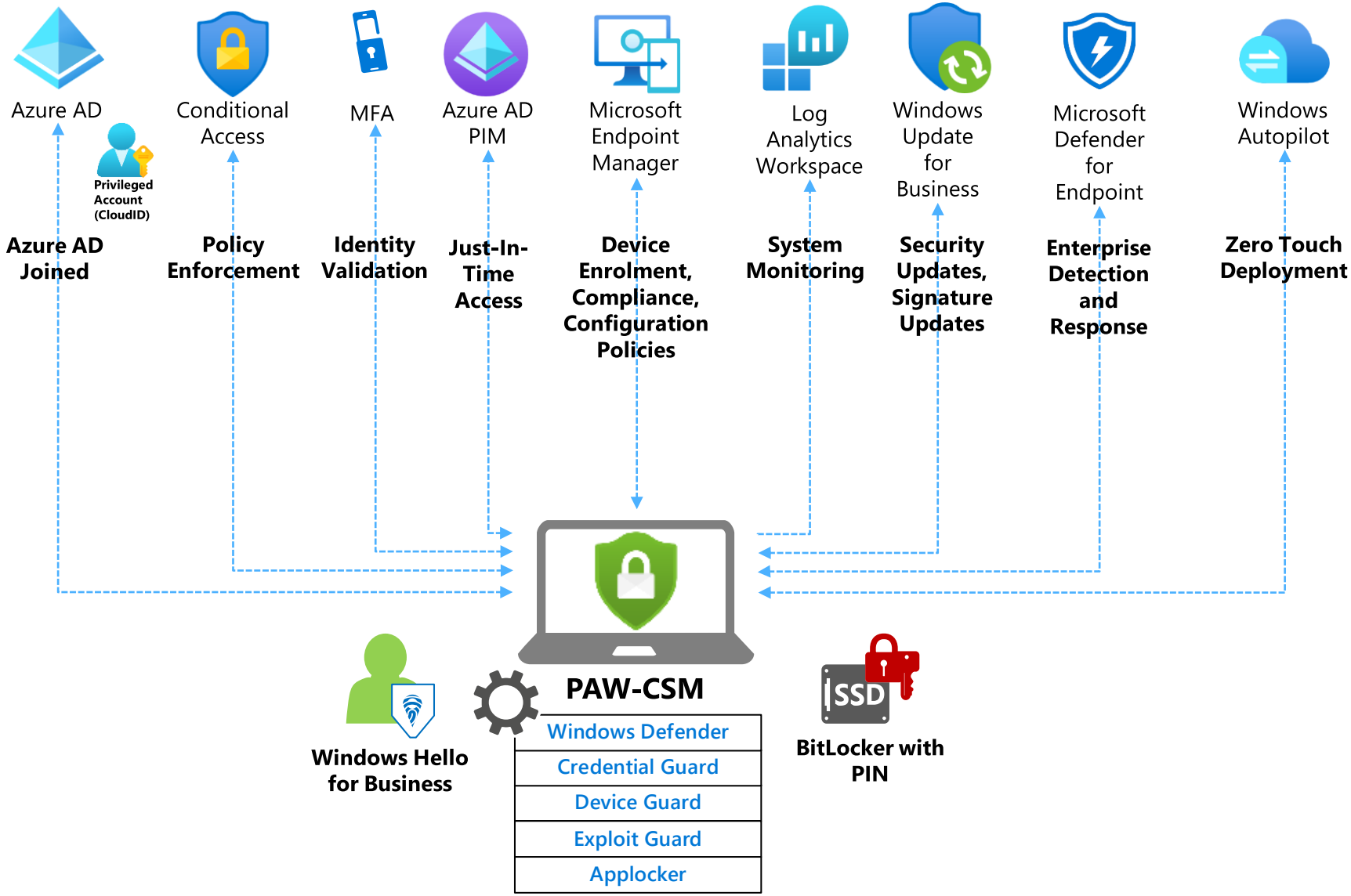
Cloud SaaS apps

On-premises & web apps

Azure Sentinel

aka.ms/zerotrust

PAW-CSM Components



Azure Lighthouse: Service Provider value proposition

Single pane of glass

Comprehensive management toolset

Flexible, granular and least-privileged access

Automated operations at scale across tenants on Azure

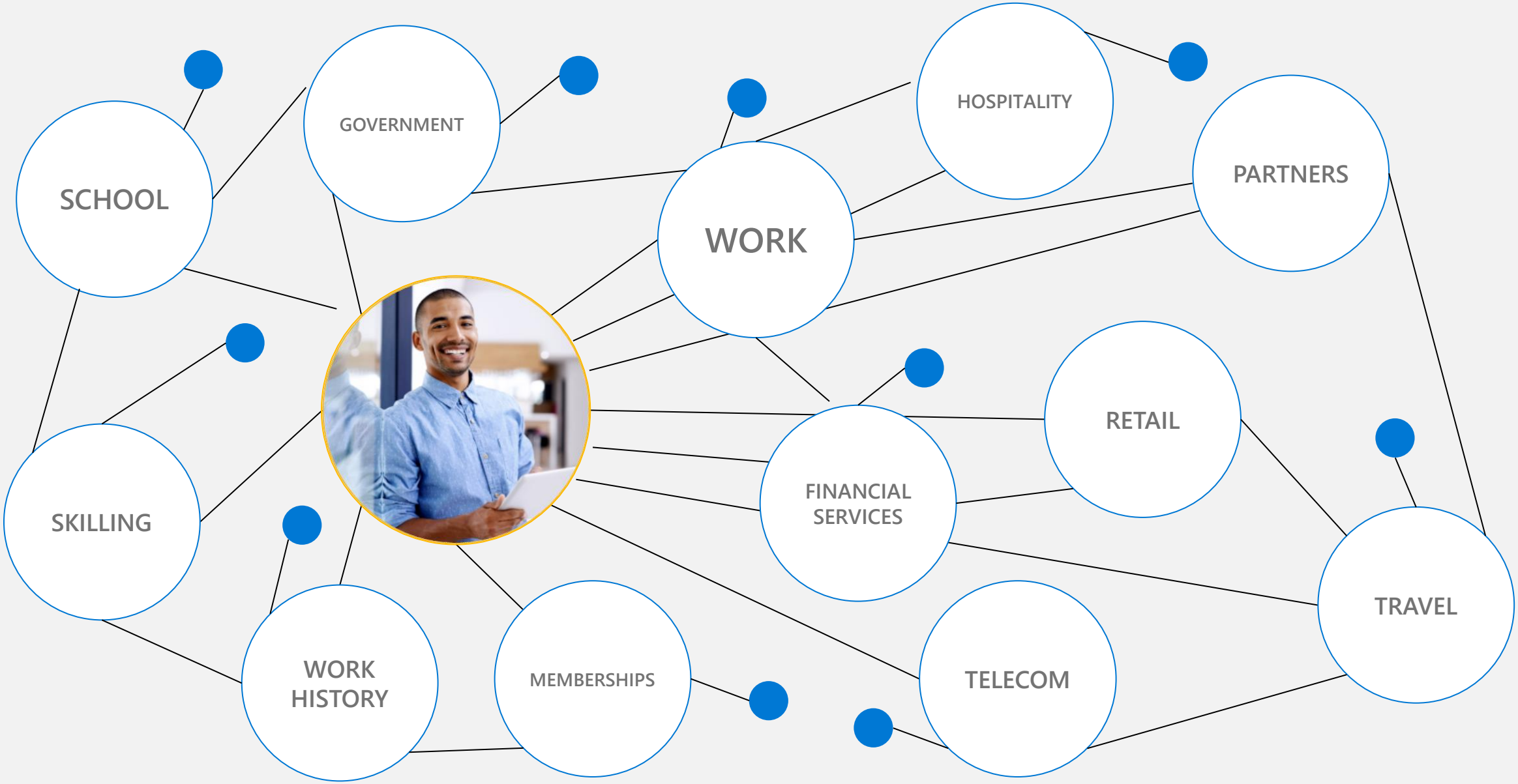
Governance at scale across tenants on Azure

Microsoft Security

Verifiable Credentials

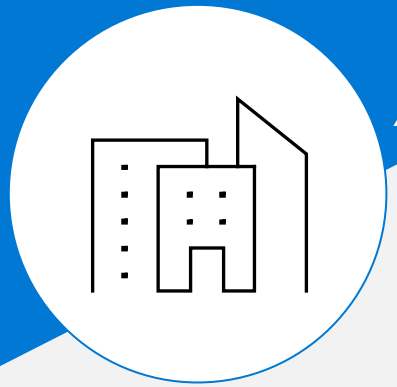
Matthijs Hoekstra
Matthijs.Hoekstra@Microsoft.com
Senior Product Manager
Microsoft Identity Engineering

Decentralized Identities: An ecosystem of trust

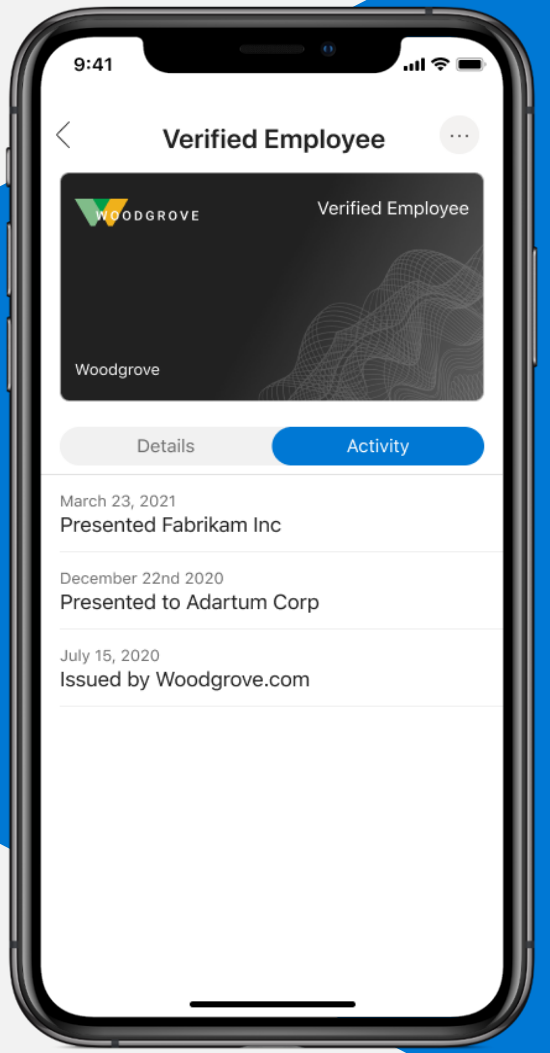


Verifiable Credentials

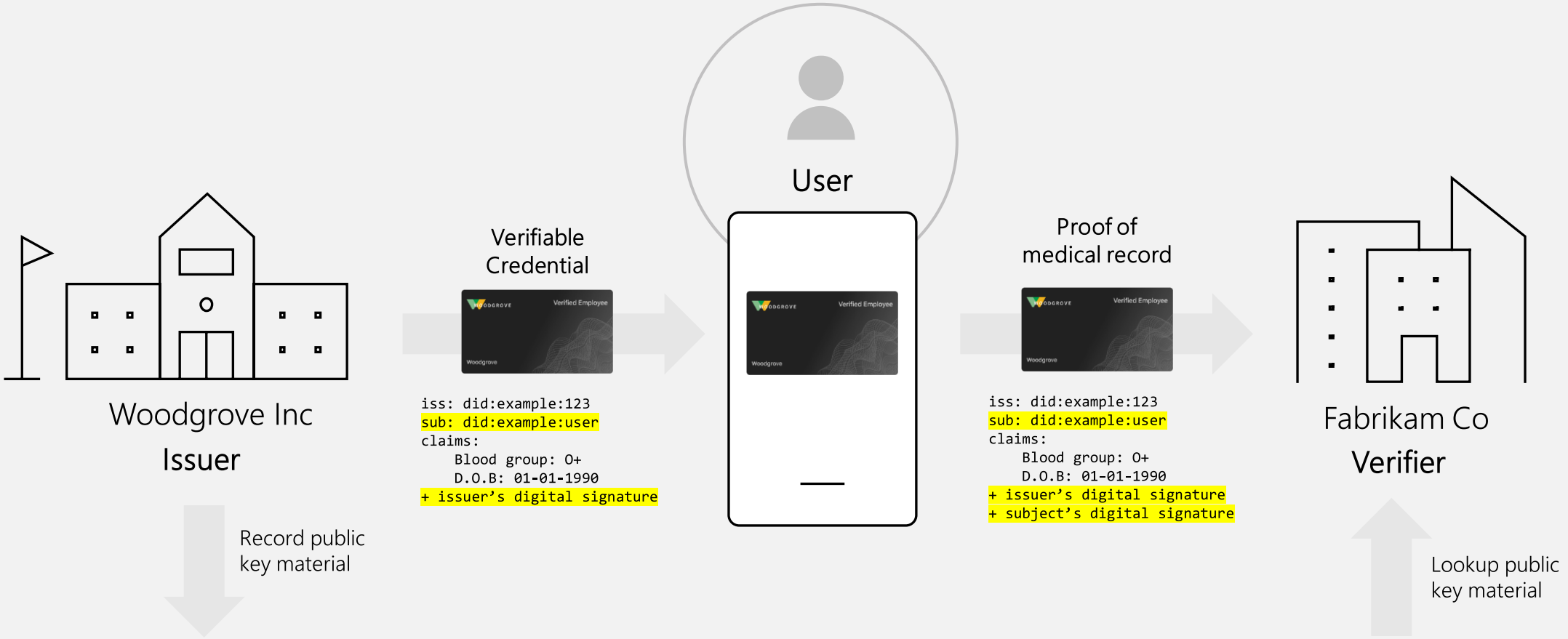
Issuer



Verifier



How does this work?



Microsoft

192 countries

6000 identification documents

1000s organizational attributes

Millions individual ID attributes

Decades of experience to go from idea to implementation within hours

Trusted identity verification providers

acuant · AUTHENTIX IDENTITY INTELLIGENCE · CLEAR · Credivera · IDEMIA · jumio · LexisNexis RISK SOLUTIONS · onfido · Socure · VU

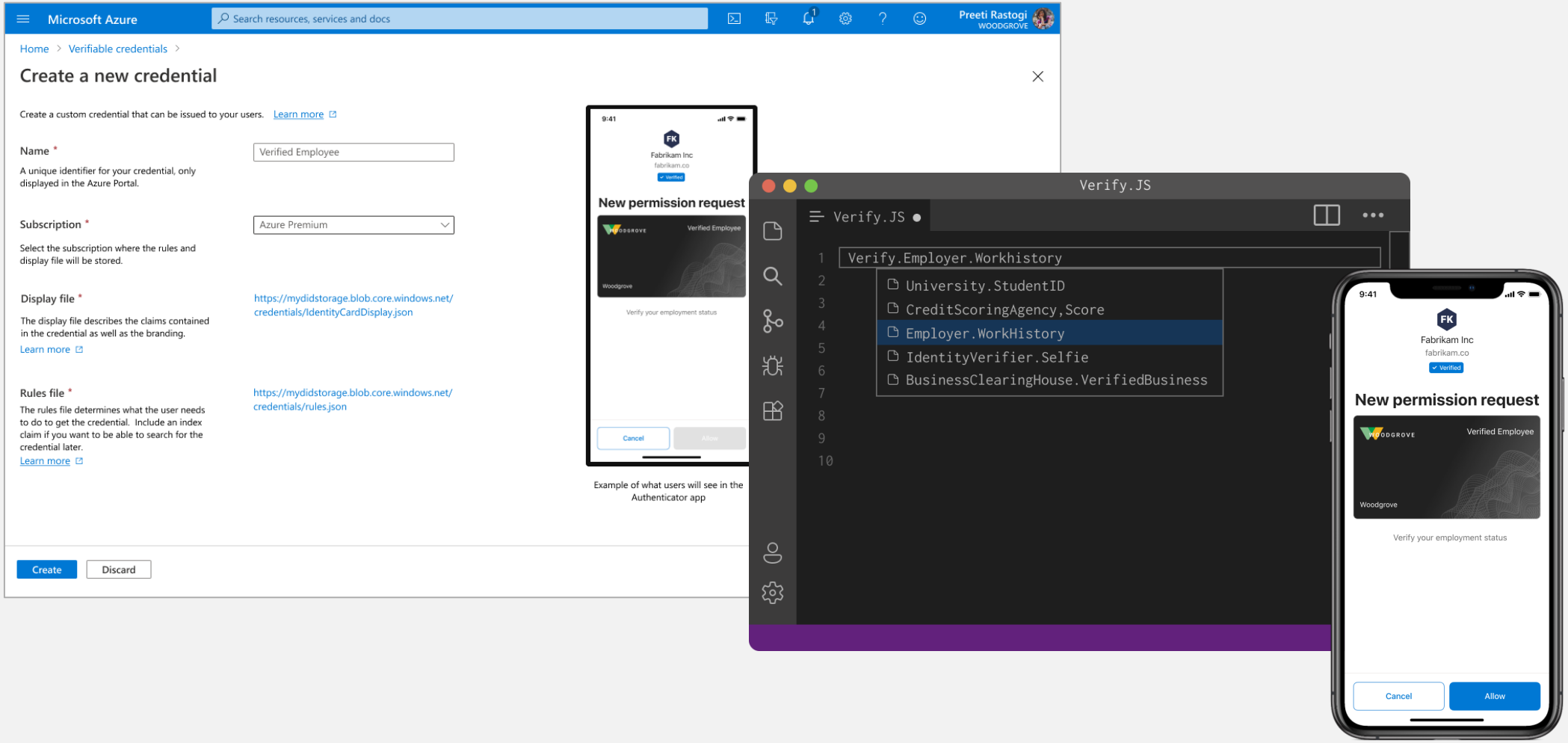
Adoption acceleration with technical solutions

AffinitiQuest.io · avanade · condatis a sitekit company · UNIFY SOLUTIONS · ITOCHU Techno-Solutions Corporation

Developed with global standards

DIF · ION · W3C CCG

Platform implementation



Issuer interface
(Azure AD)

Developer tools
(SDK + API)

End user wallet
(Microsoft Authenticator)

Trustworthy, fast, and easy identity verification

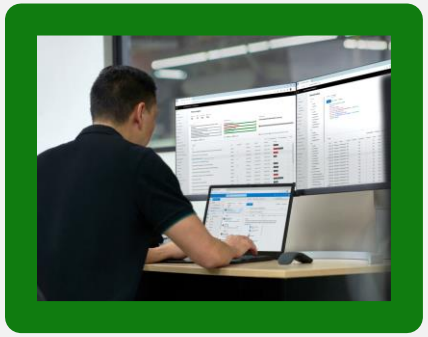
Example use cases for Enterprise

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

Accepts job offer

Visits employer portal to complete pre-onboarding

Identity validated by network partner

Receives **verifiable credential** with proven identify attributes

First day of work

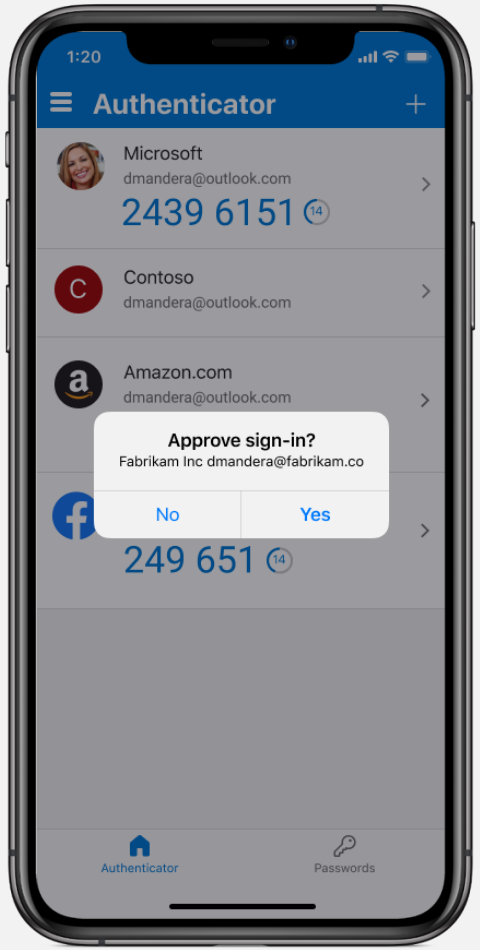
Uses verifiable credential to **remotely access** and set up new account

Receives **workplace credential,** enabling access & benefits

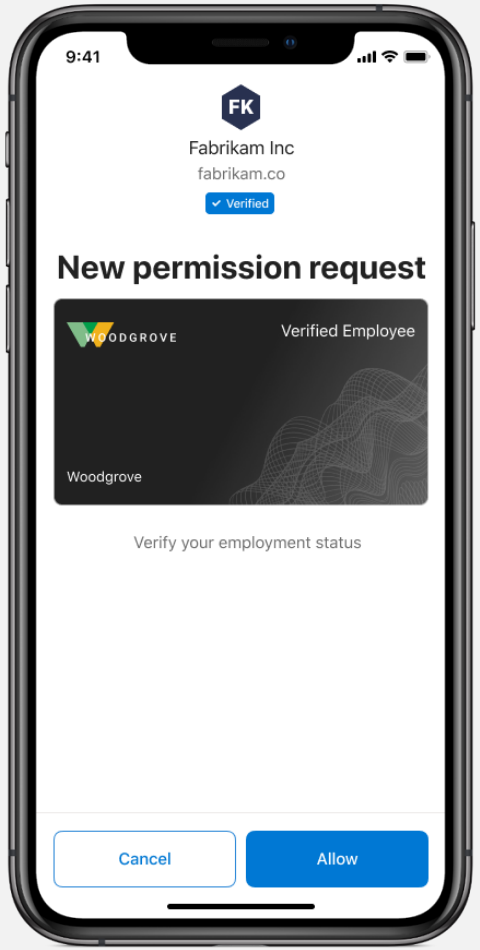
Completes **trainings**, attested to workplace credential for **compliance** and access

Efficient access to **employee perks** and ongoing life tasks

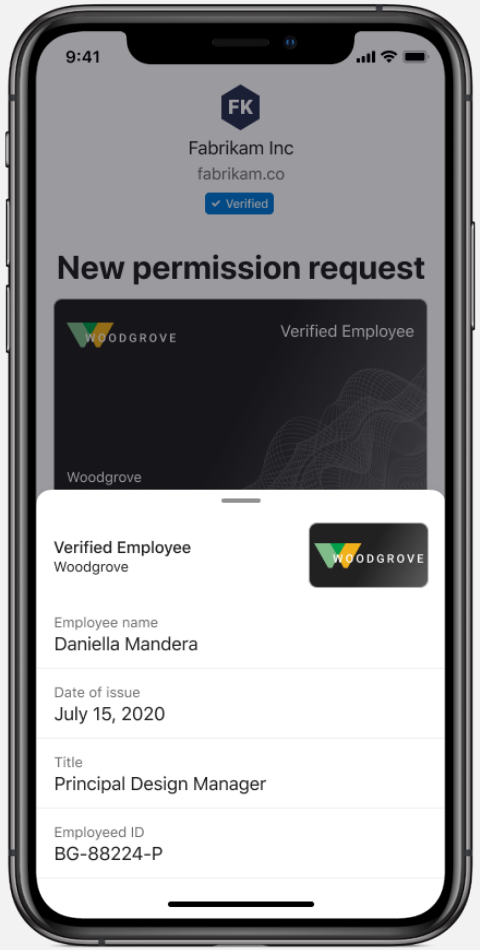
End user experience: Workplace Credentials



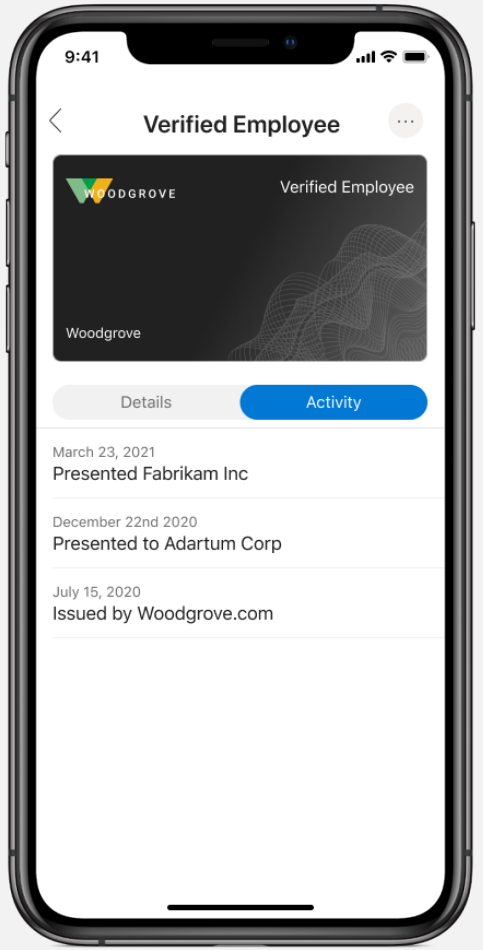
easy to use and secure



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**

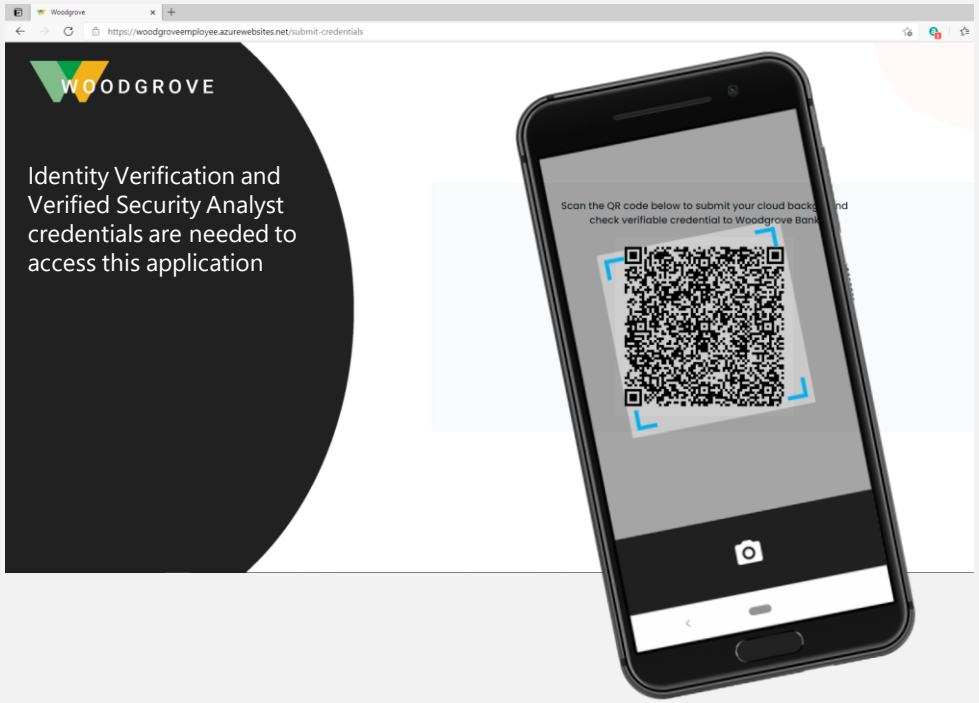
Secure access to applications

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

Start

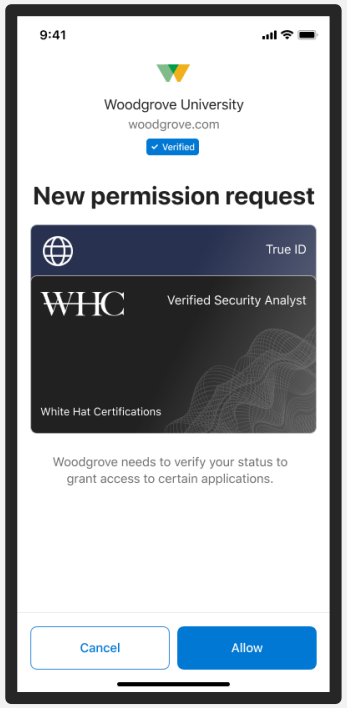
Sign in

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



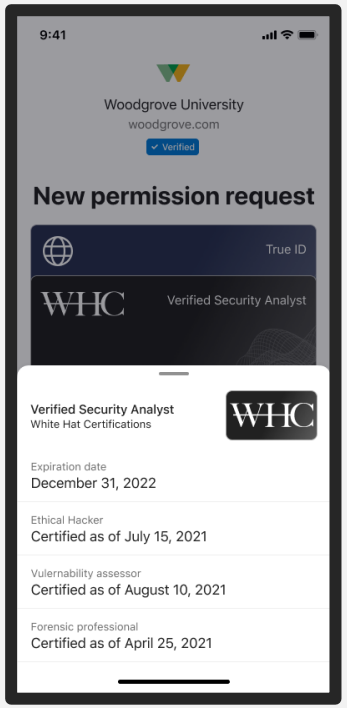
Presentation

User shares the requested verifiable credentials



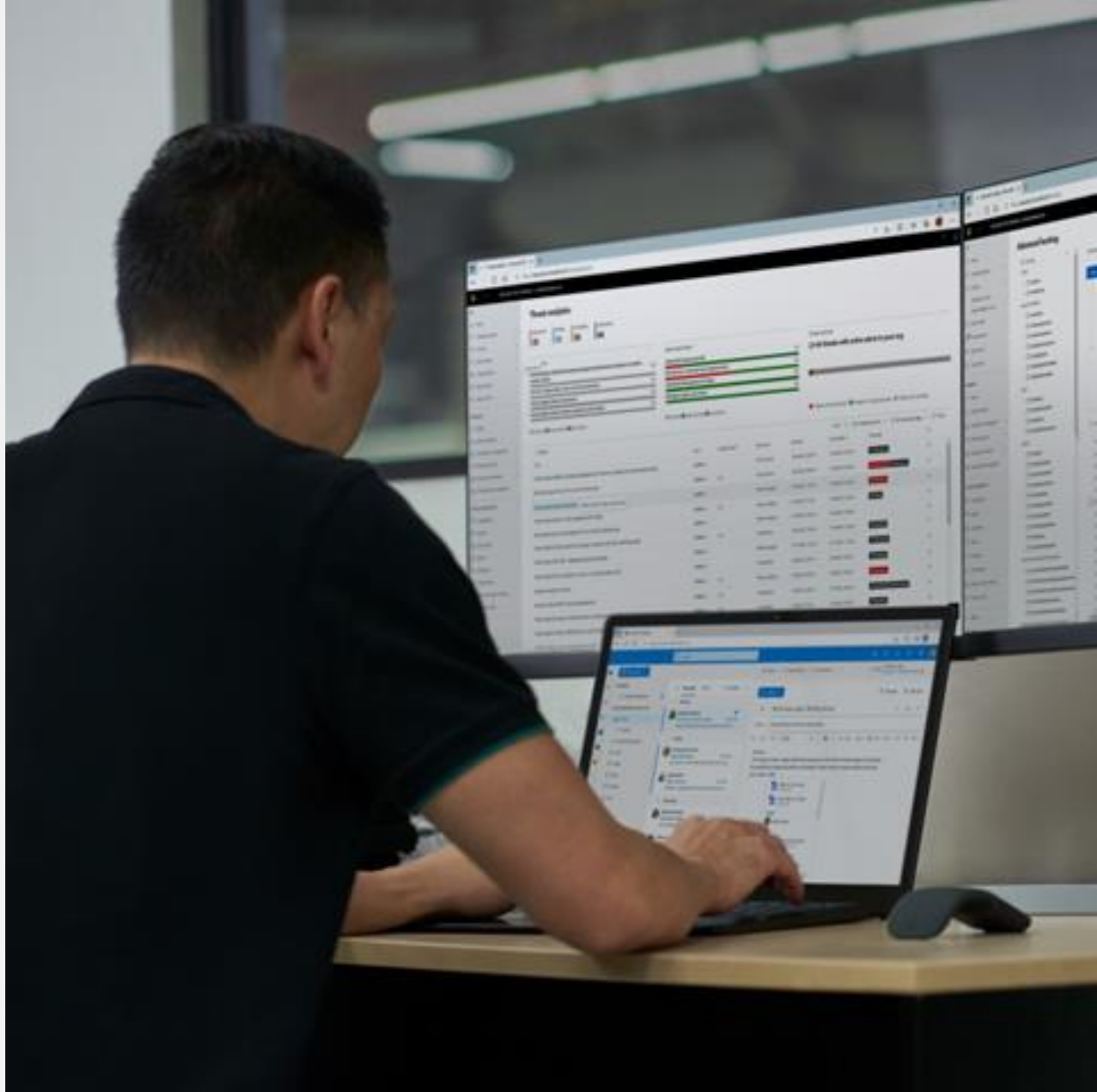
Detailed view

User confirms which claims are being shared



Account recovery & revocation

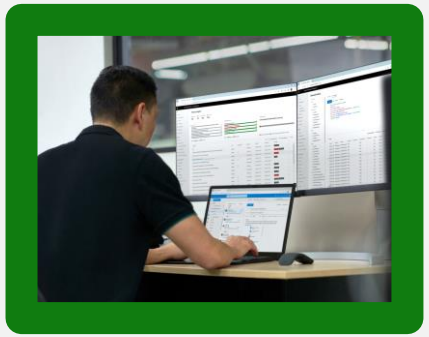
- Reduce help desk calls, “approval fatigue”
- Faster, self-service account recovery, password reset
- Revocation immediately visible to all partners/verifiers



Streamlined workflows

Ransomware attack; account is blocked

Self-service account recovery enabled by workplace credential

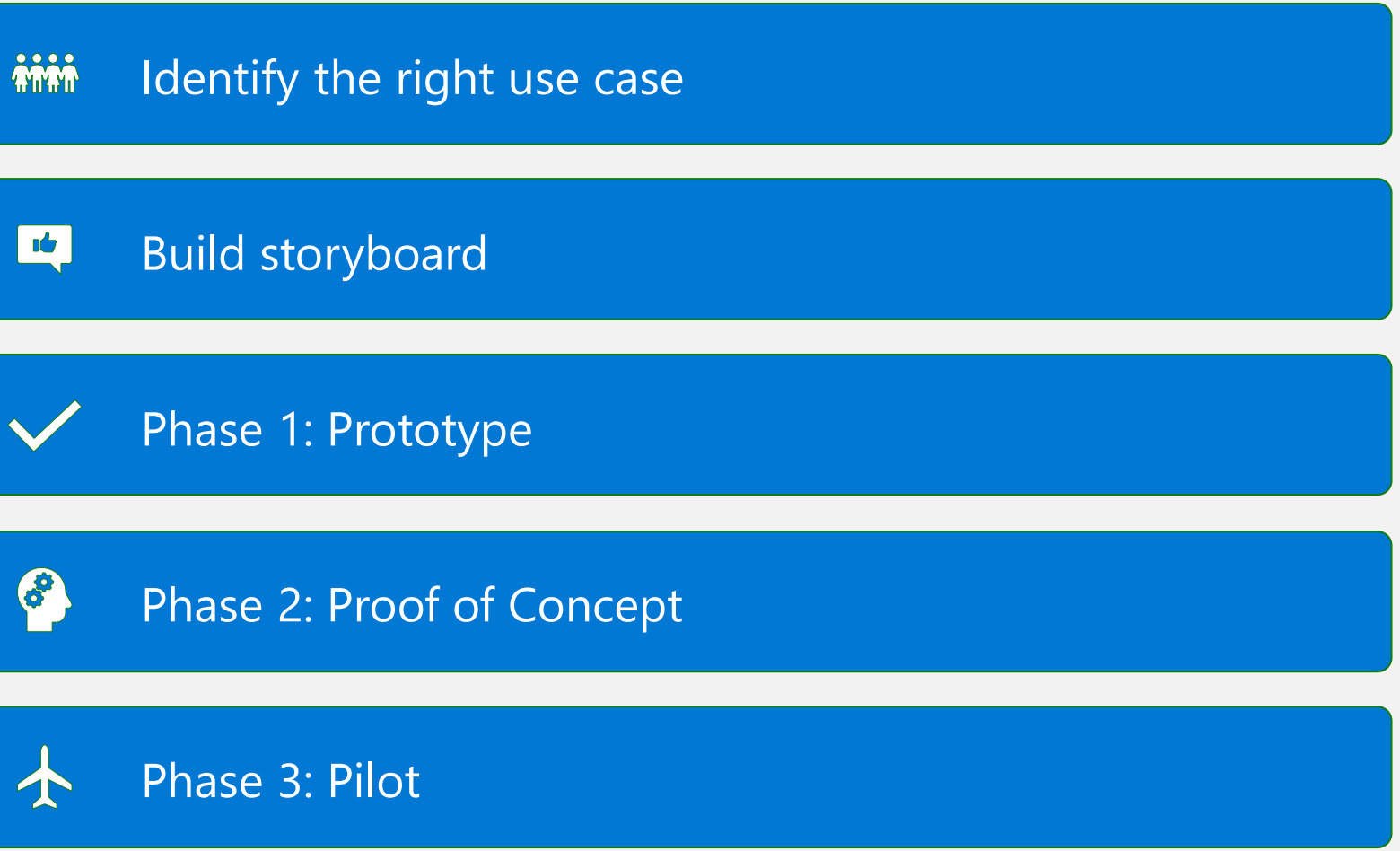


Employee leaves the company

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



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.

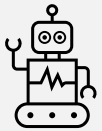
Asks

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

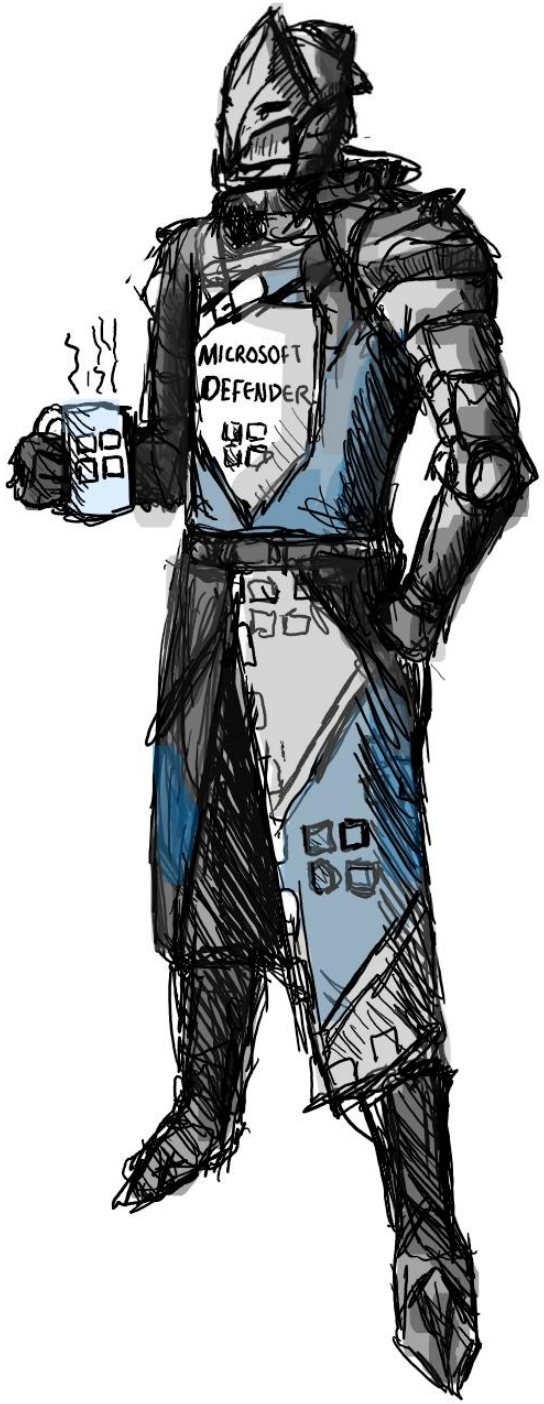
https://youtu.be/Whc9Im-U0Wg
Overview for developers: scenario walk-through and how-to

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



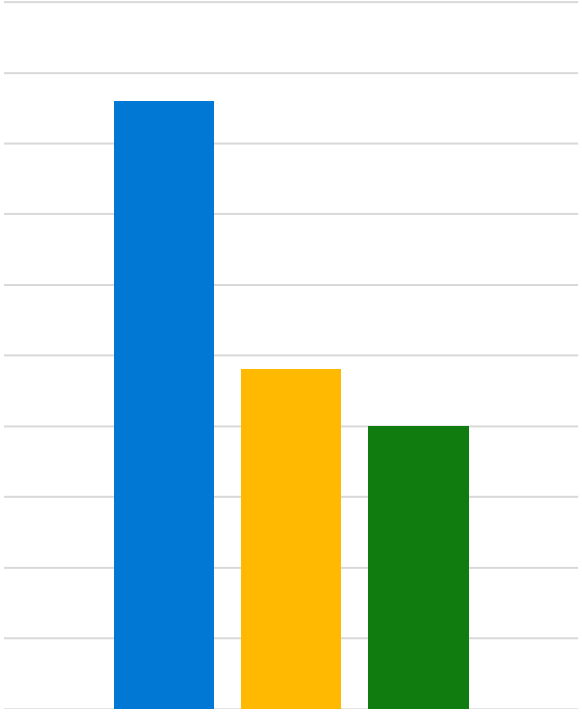
Microsoft Security

Cross-tenant access settings

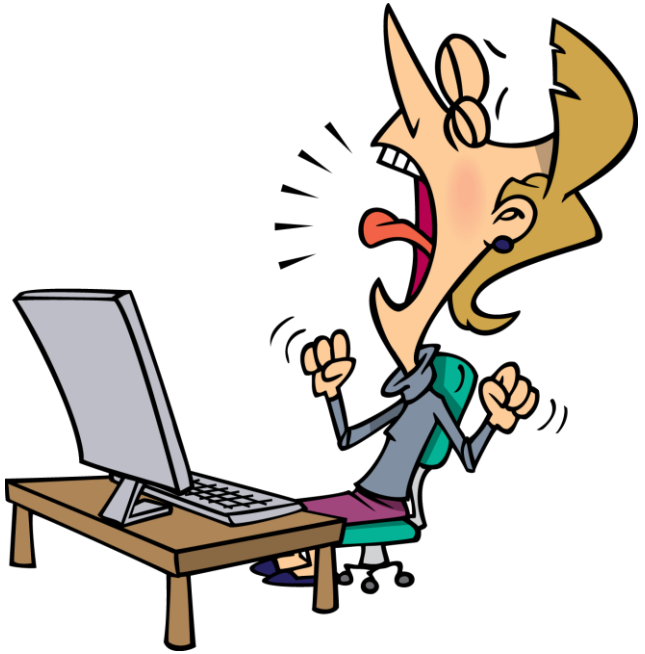
Luciana Blanchard
Luciana.Blanchard@microsoft.com
Global Partner Solutions UK

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?

- 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

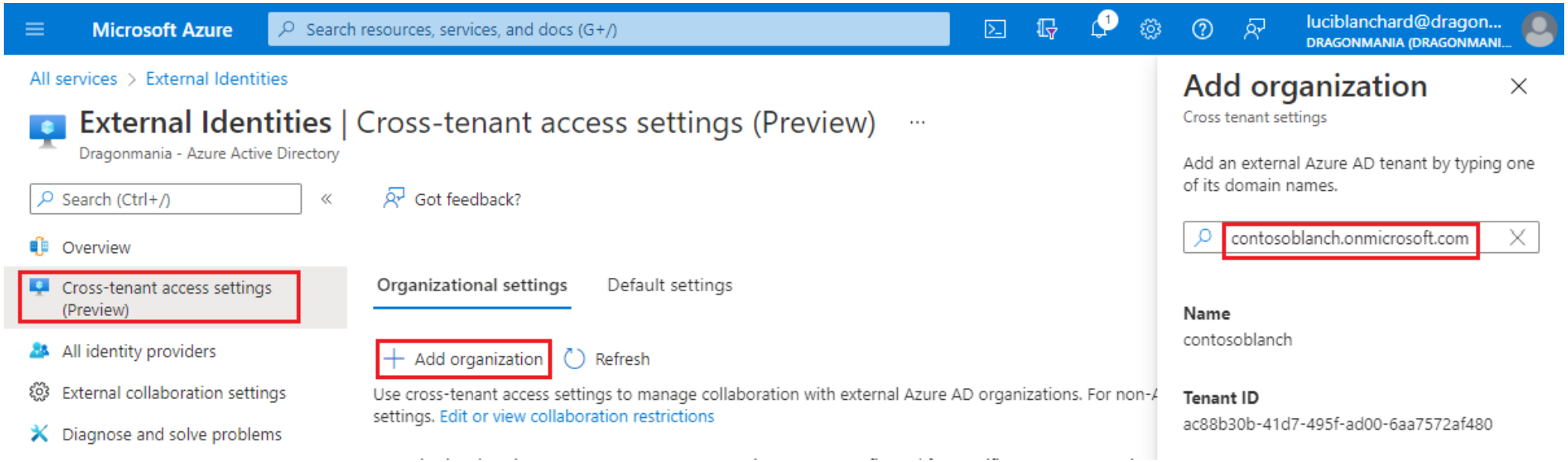
- ○ Allow invitations to be sent to any domain (most inclusive)
- ◉ Deny invitations to the specified domains
- ○ Allow invitations only to the specified domains (most restrictive)

Delete

Target domains
*.fabrikam.com

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

Cross Tenant Access Settings give you control at a Tenant level

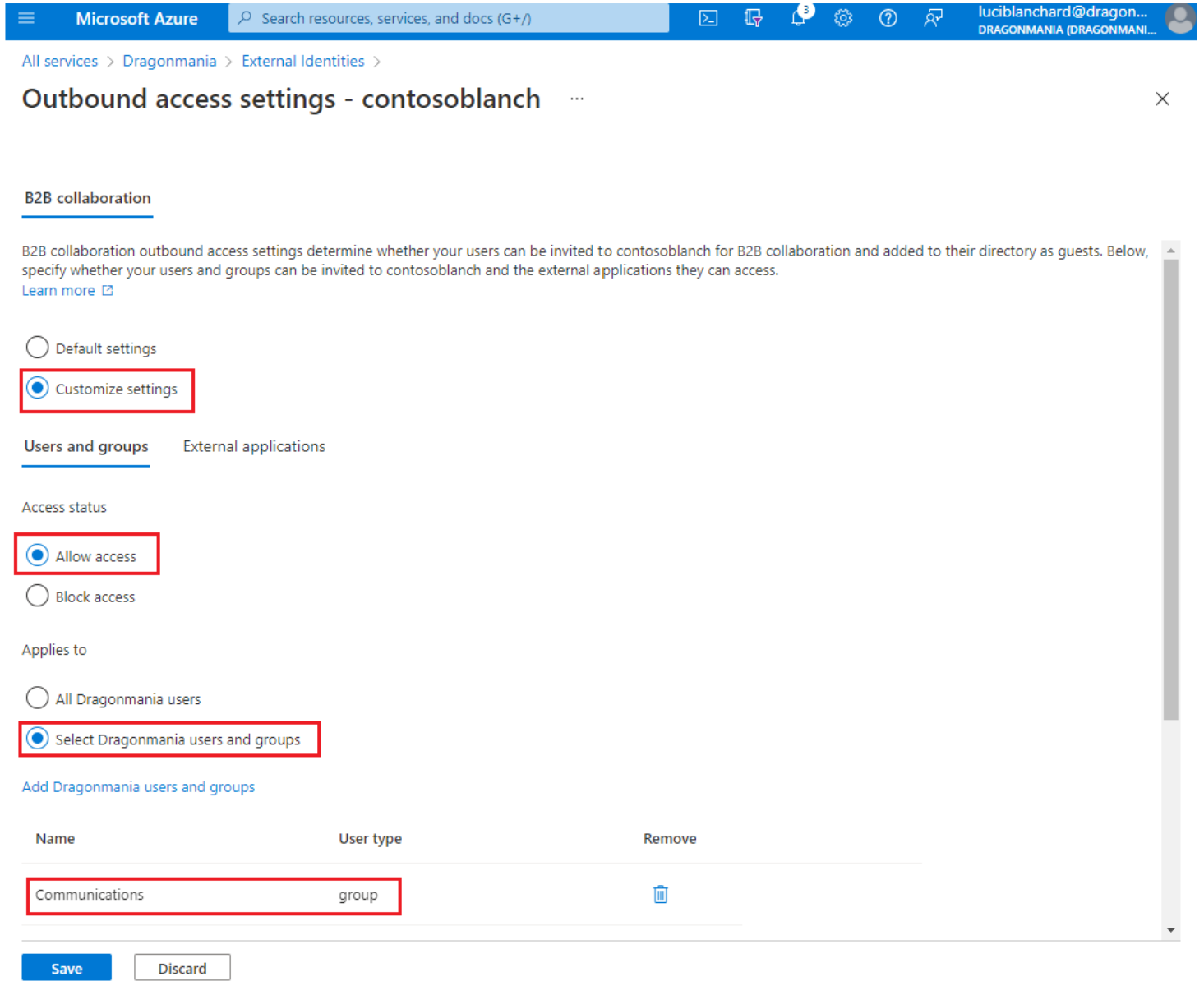


Cross Tenant Access Settings

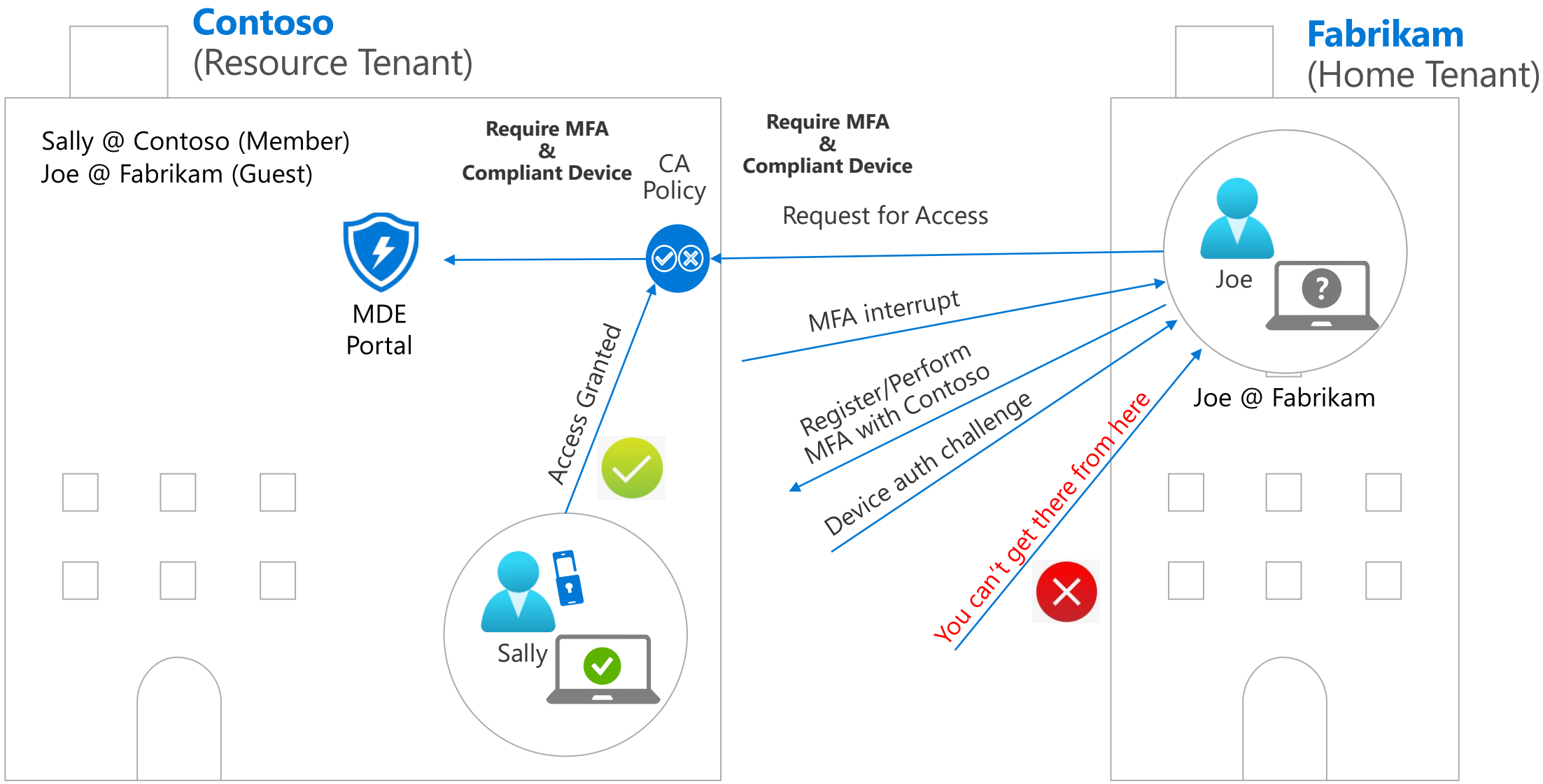
give you outbound & inbound **granular** control

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

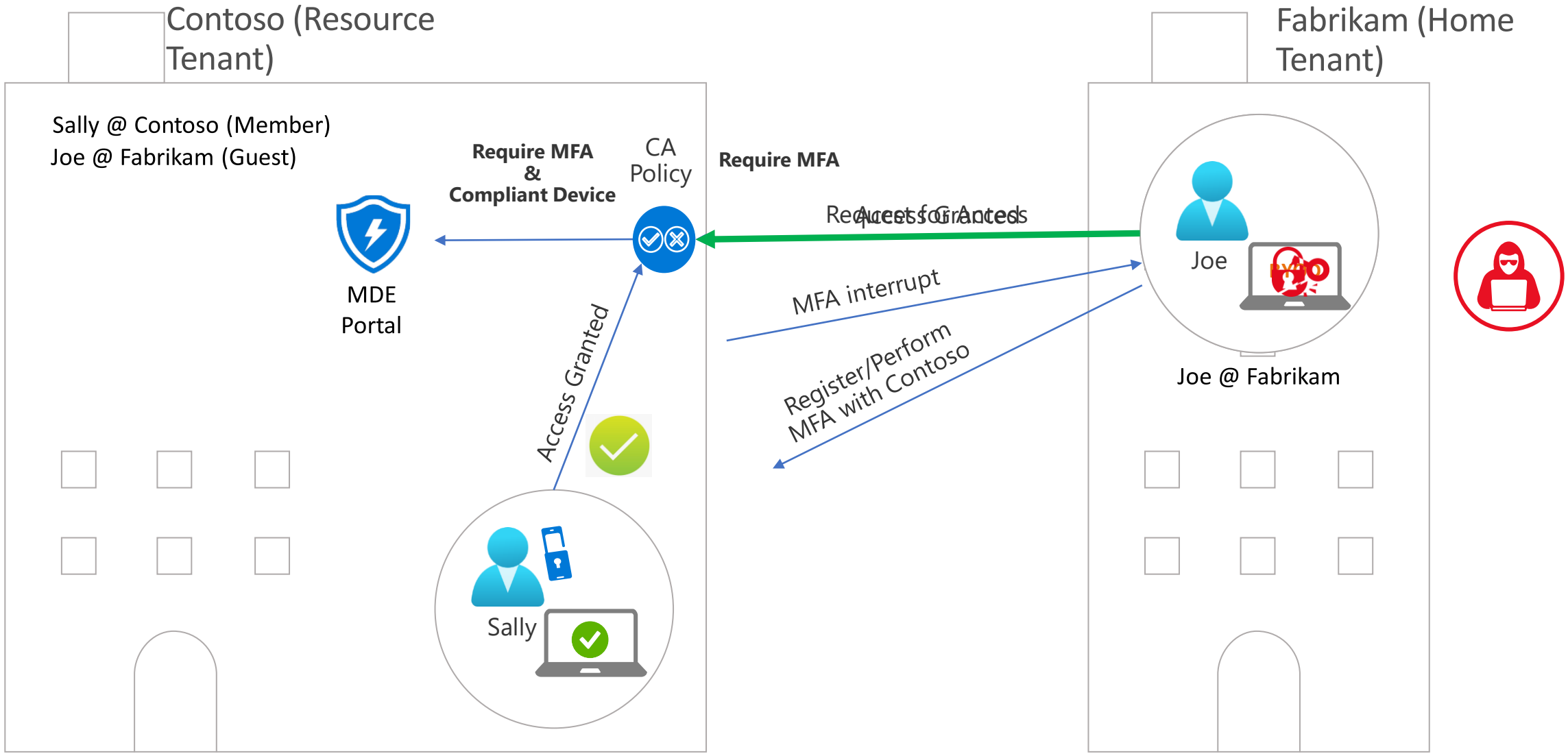
Allow only **specific users or groups** from an external tenant to access your organisation



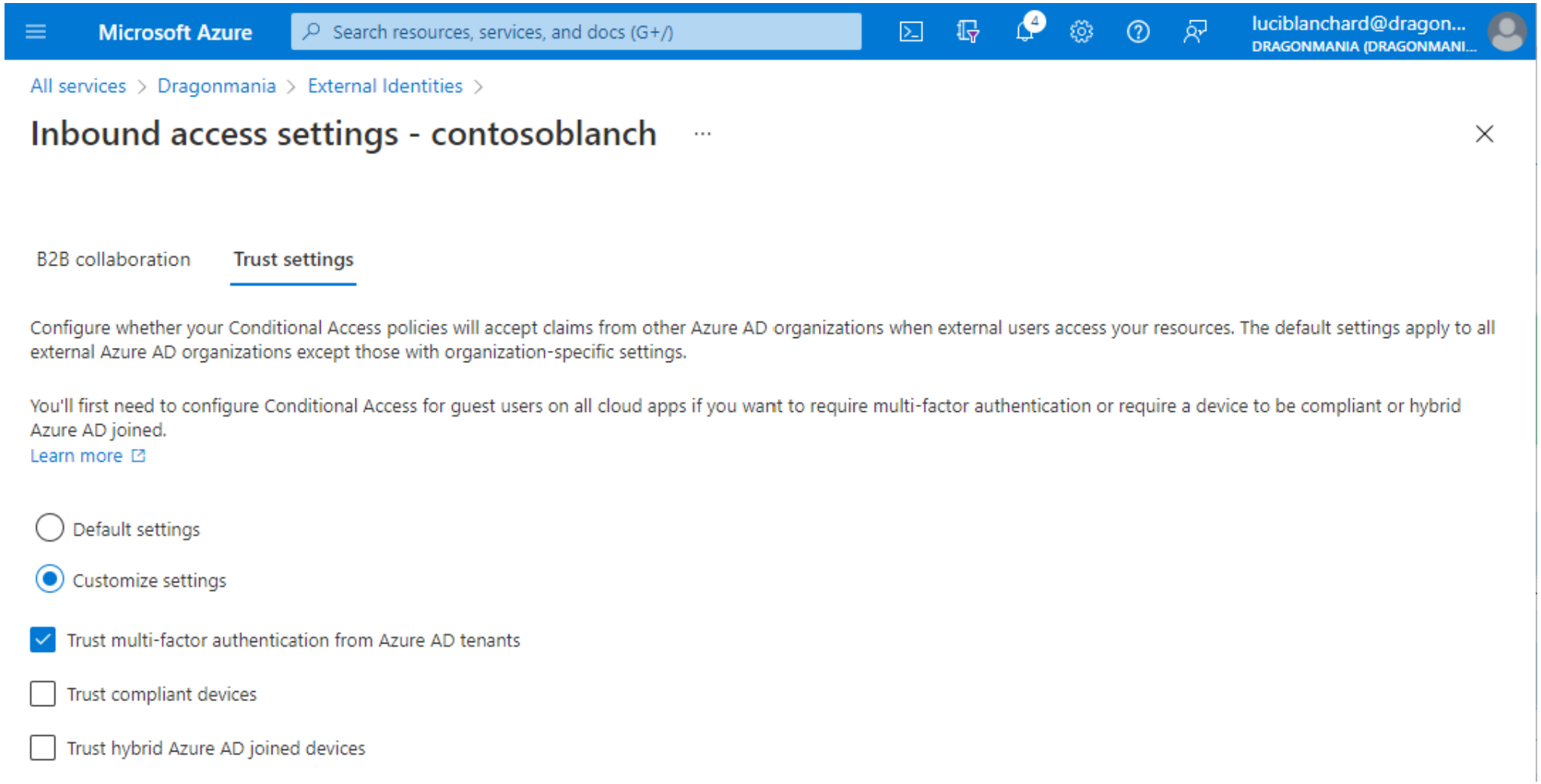
Inbound Access w/o Cross Tenant Access setting



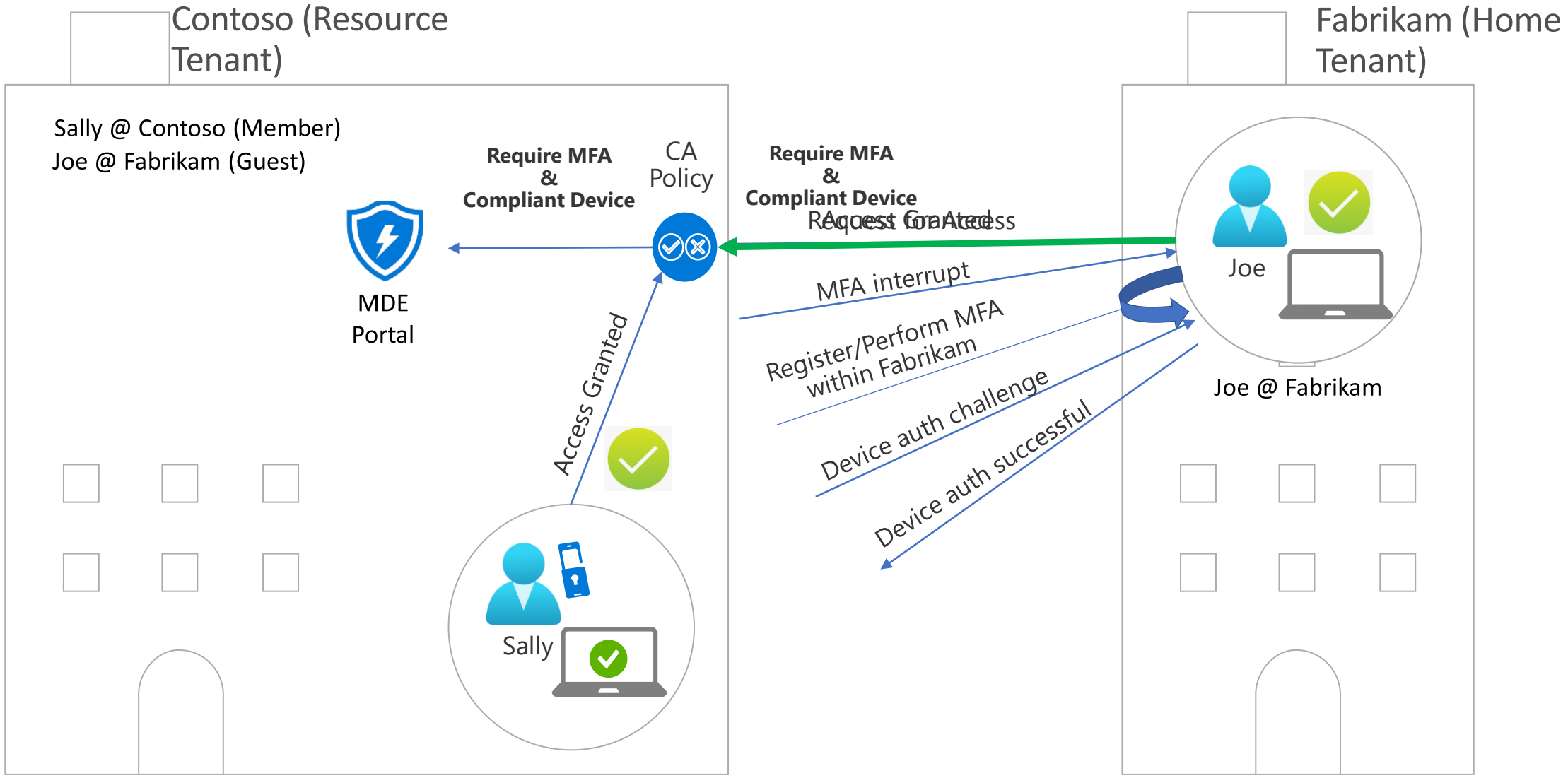
Inbound Access w/o Cross Tenant Access setting



Trust MFA from Guest User's Home Tenant

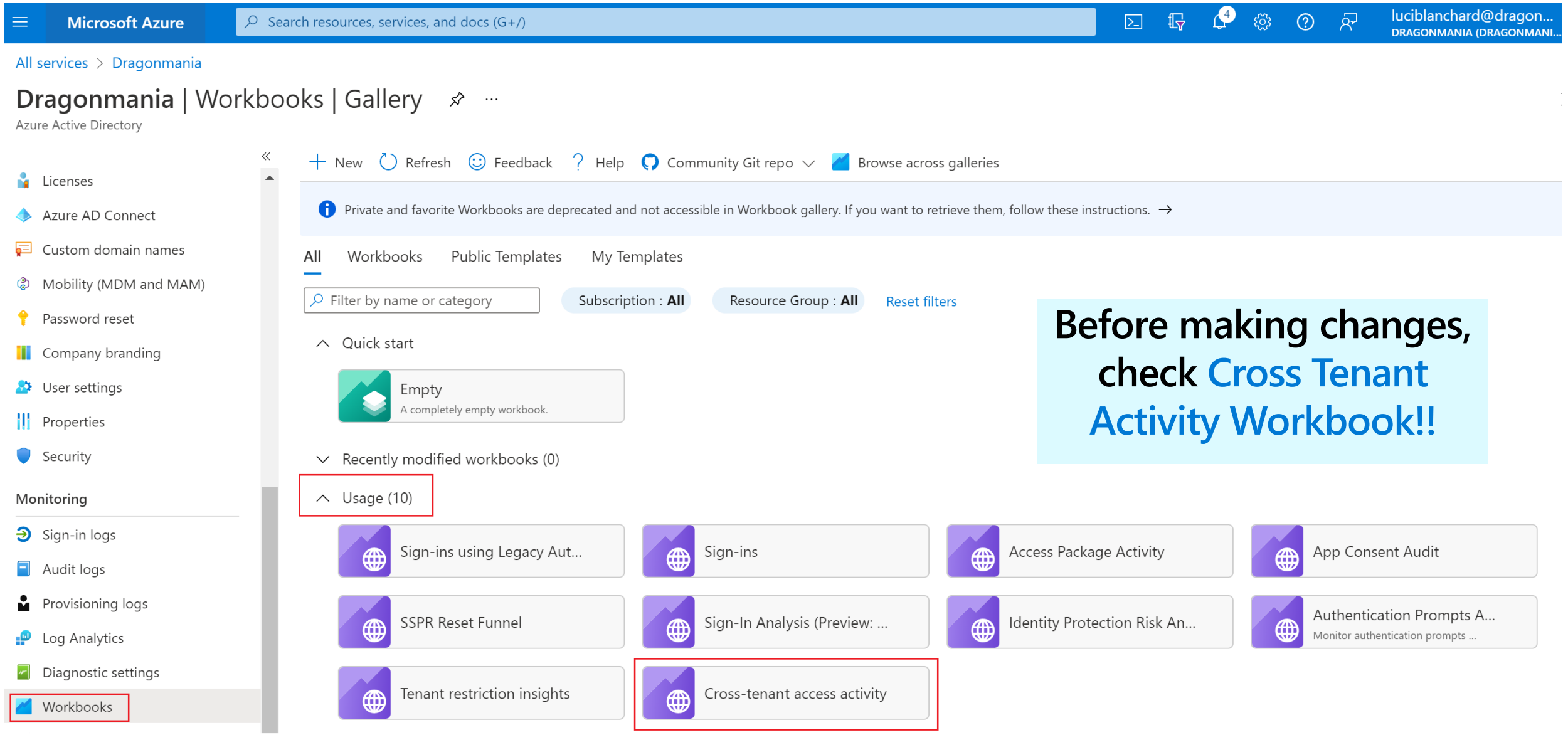


Inbound Access w/ Cross Tenant Access setting



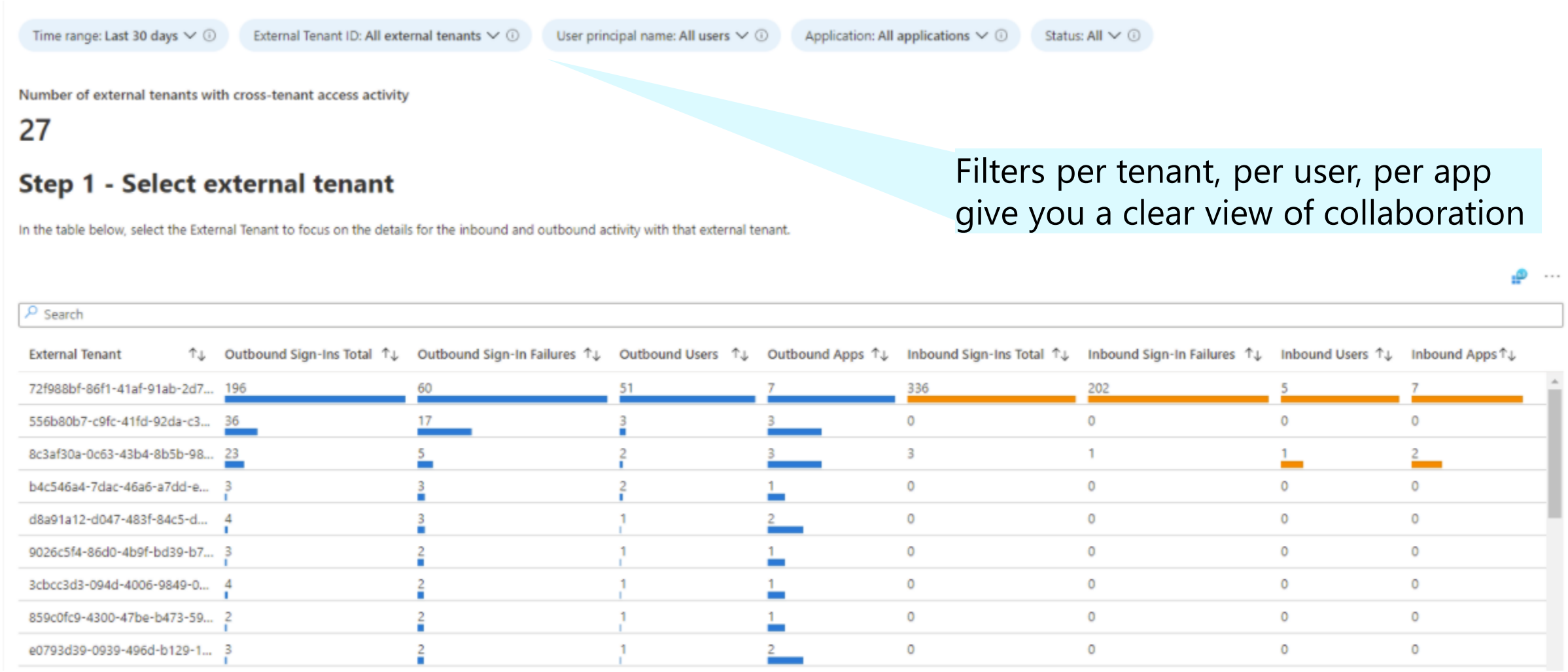
How can I minimize the risk?

Aka.ms/CrossTenantWorkbook



Before making changes, check Cross Tenant Activity Workbook!!

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



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

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

Search

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-c000-000000000000	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-dfdbc9a8f650	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

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

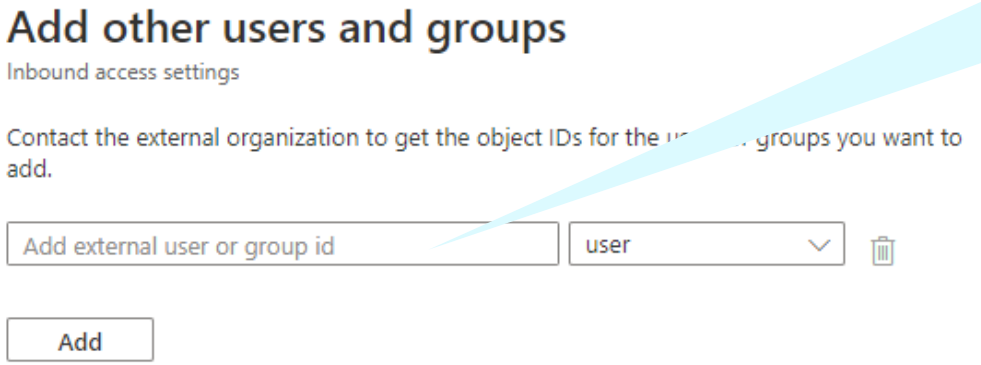
- Default settings
- Customize settings

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

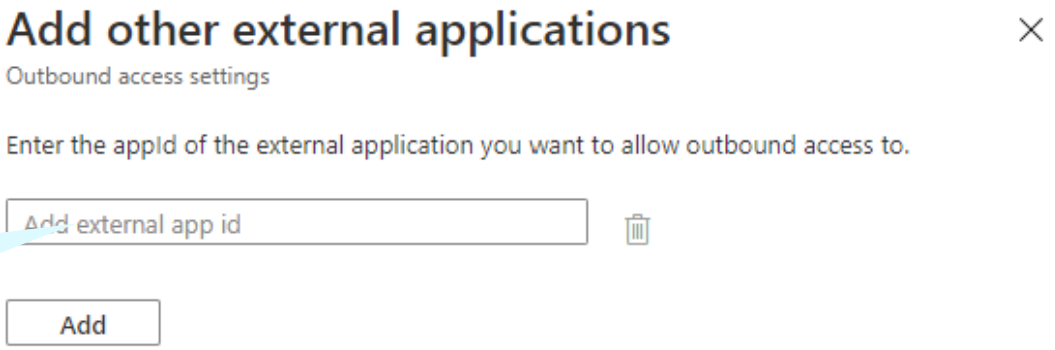
AAD Premium P1 Licensing is required

User Experience

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



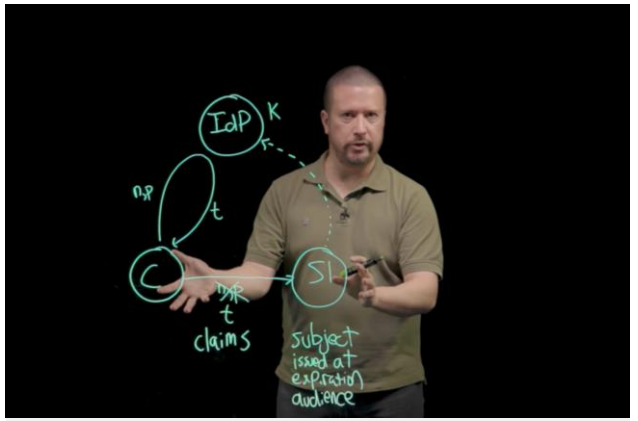
Limits and considerations

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
Aka.ms/CrossTenantOverview
Aka.ms/CrossTenantGraphAPI



Stay current with the latest Identity news
Aka.ms/identityyoutube
Aka.ms/azureadblog
Aka.ms/azureaddocs

Thank you!

Microsoft Security

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.

Microsoft Security

Next Steps for Partner Success

Microsoft Security

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)

Azure Security Engineer (AZ-500)

Training includes
- 32 hours of Microsoft Learn content
- 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 365 Security Administrator Associate (MS-500)

Training includes
- 14 hours of Microsoft Learn content
- 10 hours of exam prep instructor training
- 4-day instructor-led training (English)

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)

*Azure Network Engineer Associate (AZ-700)

Training includes
- 10 hours of Microsoft Learn content
- *Exam prep instructor training not available*

Expert Certifications

Coming Soon Microsoft Cyber Security Architect

Online modules coming soon

- Go here for the latest certification roadmap **Microsoft training and certifications**.

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.

Microsoft

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?

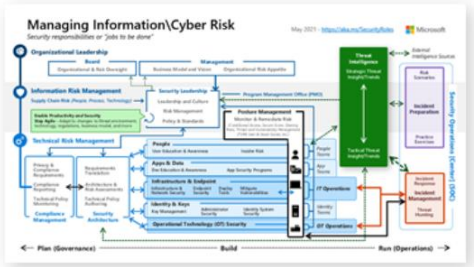
Attack Chain Coverage

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?

- 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

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

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