Microsoft

Securing Identity with Zero Trust

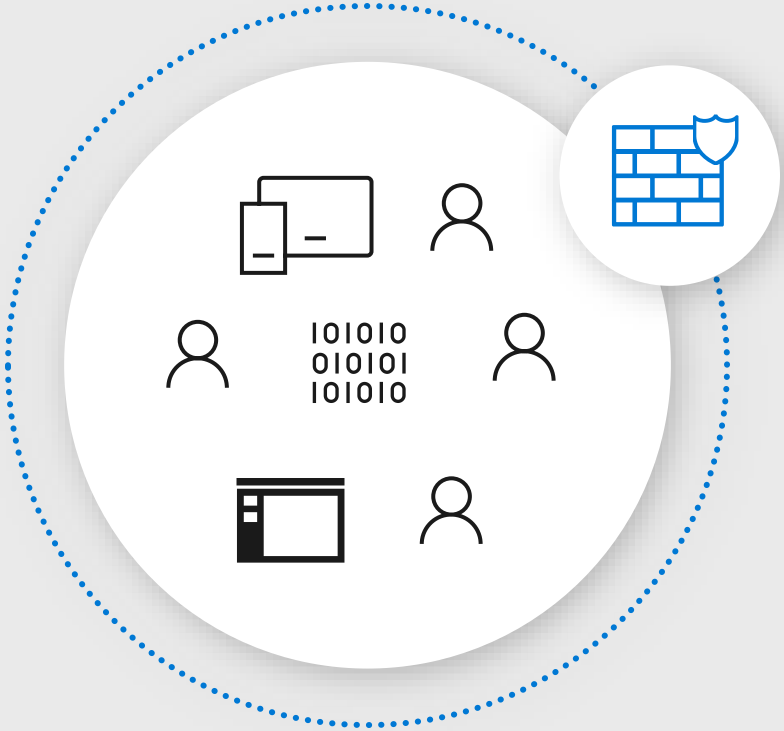
Ricardo Trigueiro
Sr. Partner Technical Consultant
Cloud Security, Compliance & Identity
ricardo.trigueiro@microsoft.com

Agenda

- What is Zero Trust?
- Microsoft approach to Zero Trust
- Zero Trust for Identity
- Resources available

1990s:
Employees work exclusively in a corporate office

Traditional Model



Users, devices, apps, and data
protected behind a network firewall

By 1995:

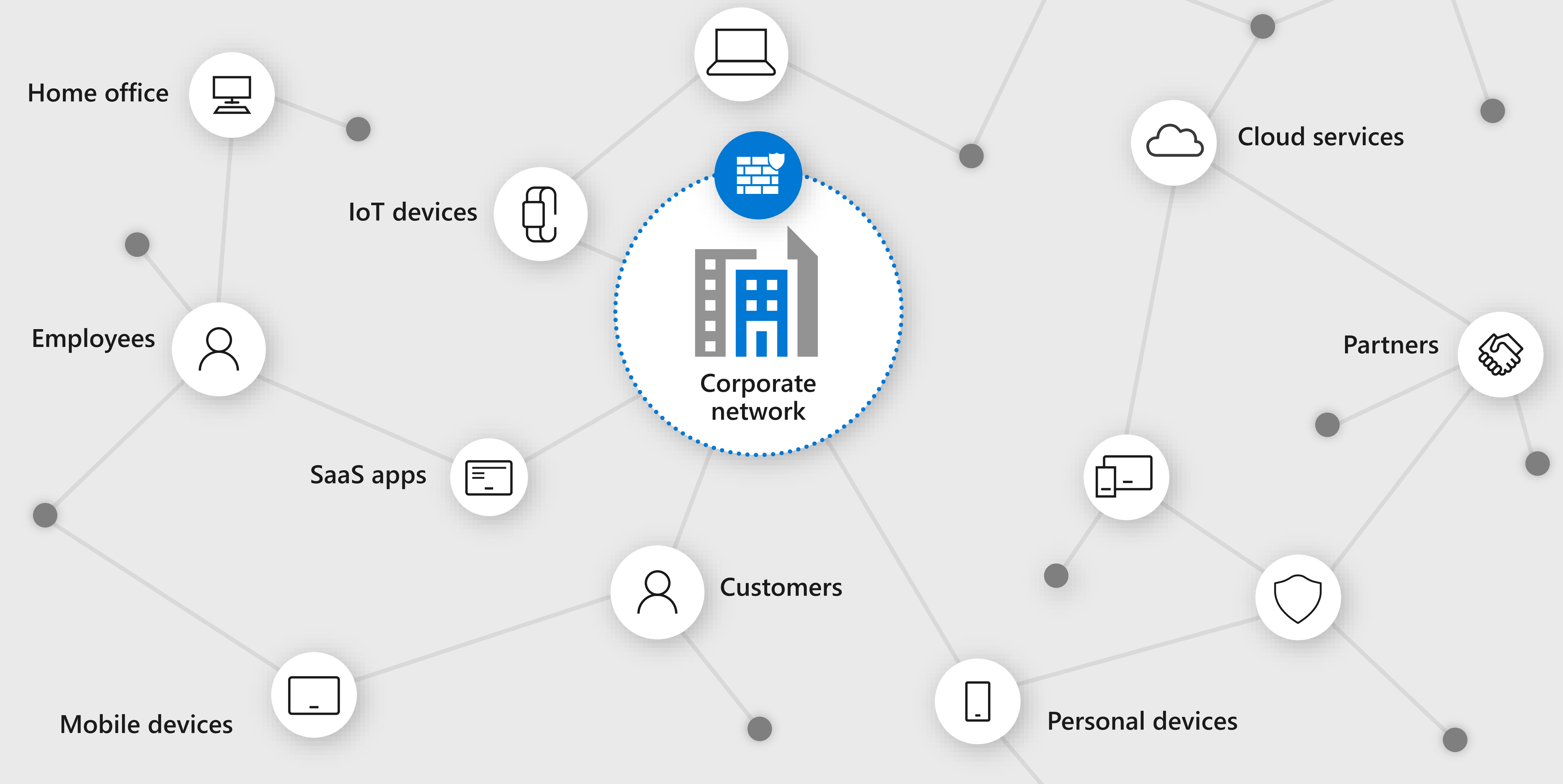
Most networks are connected by VPN and Internet replacing WANs – Firewalls and VPN dominate security conversation

Digital Evolution

2000	2005	2006	2009	2011
Salesforce SaaS launched	Concur transitions to Cloud	Iphone	FITBIT Tracker	Office 365 launches

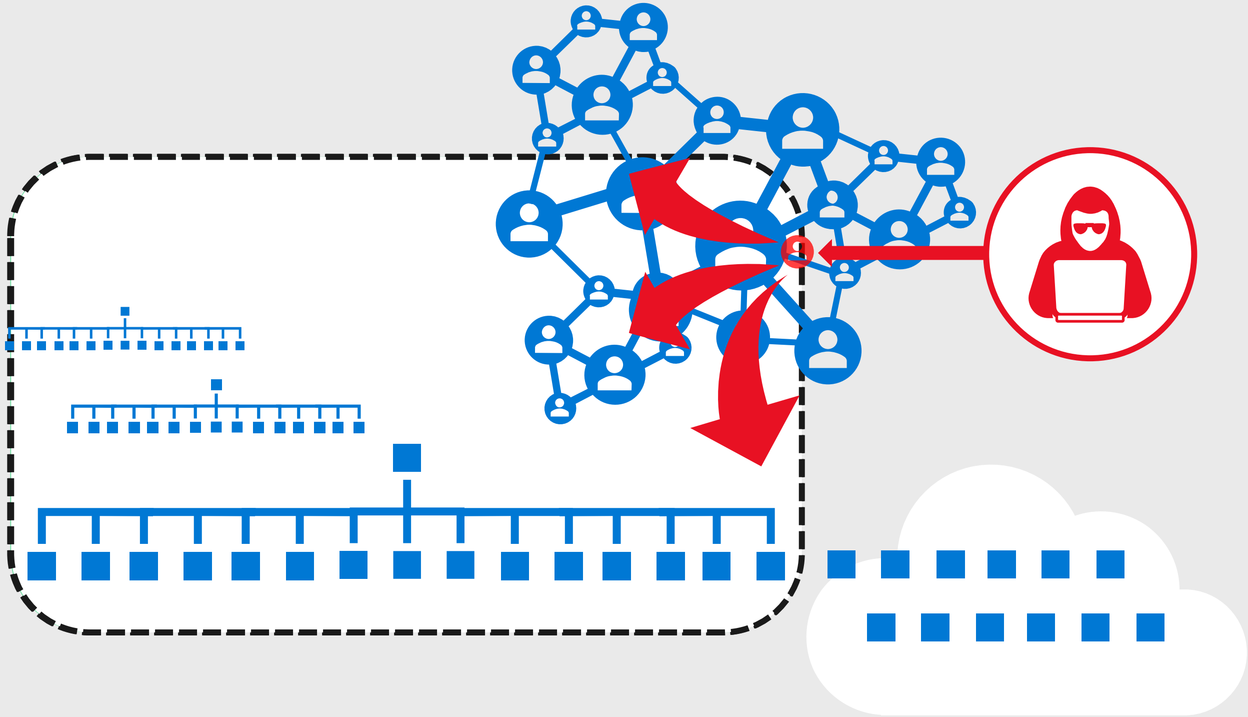
Today’s Model

Identity perimeter complements network perimeter



Why are we having a Zero Trust conversation?

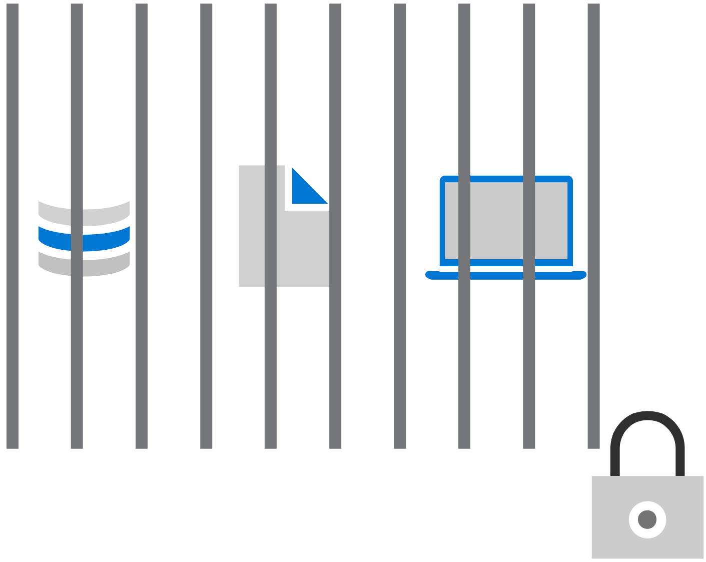
Keep **Assets** away from **Attackers**



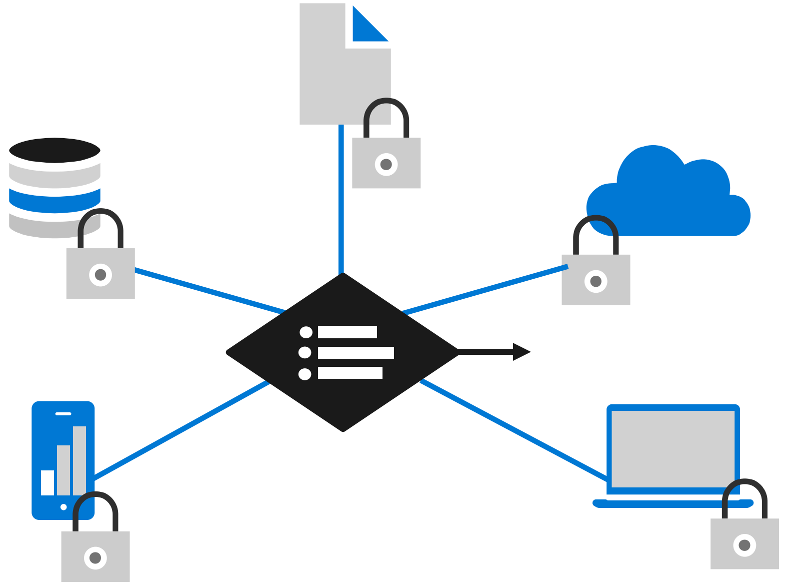
1. **IT Security is Complex**
   - Many Devices, Users, & Connections
2. **"Trusted network" security strategy**
   - Initial attacks were network based
   - *Seemingly* simple and economical
   - Accepted lower security within the network
3. **Assets increasingly leave the network**
   - BYOD, WFH, Mobile, and SaaS
4. **Attackers shift to identity attacks**
   - Phishing and credential theft
   - Security teams often overwhelmed

Secure assets where they are with Zero Trust

Simplify security and make it more effective



Classic Approach
Restrict everything to a 'secure' network



Zero Trust
Protect assets anywhere with central policy

Old World vs. New World

Users are employees	Employees, partners, & customers
Corporate managed devices	Bring your own devices
On-premises apps	Explosion of cloud apps
Corp network and firewall	Perimeter-less
Local packet tracking and logs	Explosion of signal

New World

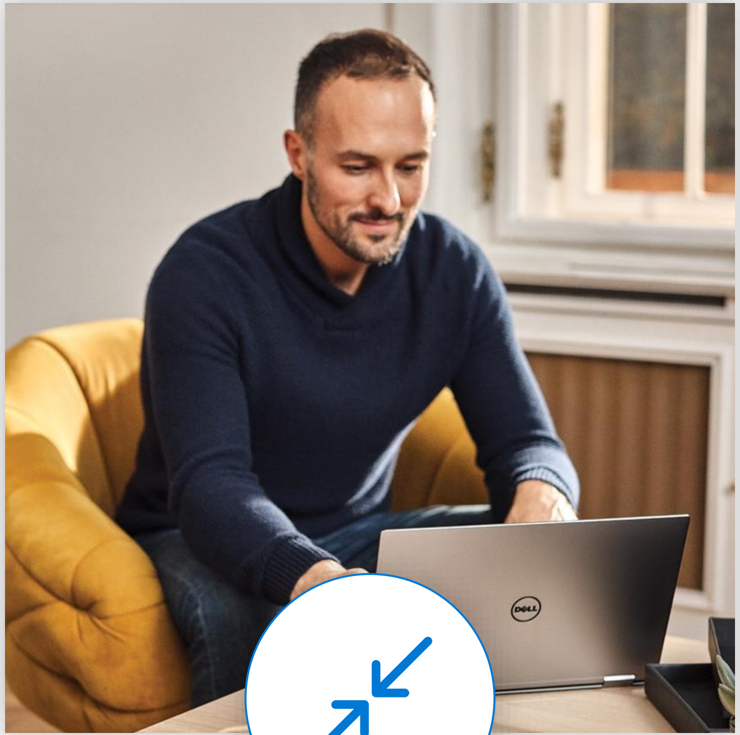
- Employees, partners, & customers
- Bring your own devices
- Explosion of cloud apps
- Perimeter-less
- Explosion of signal

New Principles

- Verify explicitly
- Use least privilege access
- Assume breach

Principles of Zero Trust

Verify explicitly



Use least privilege access

Assume breach

Zero Trust across the digital estate

Identity

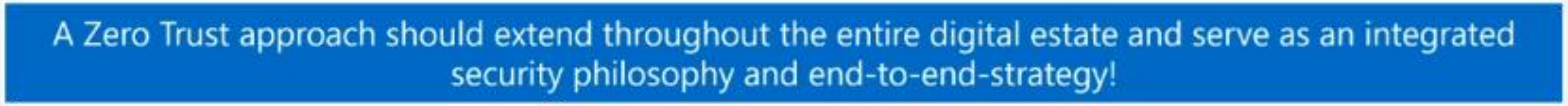
Devices

Apps

Infrastructure

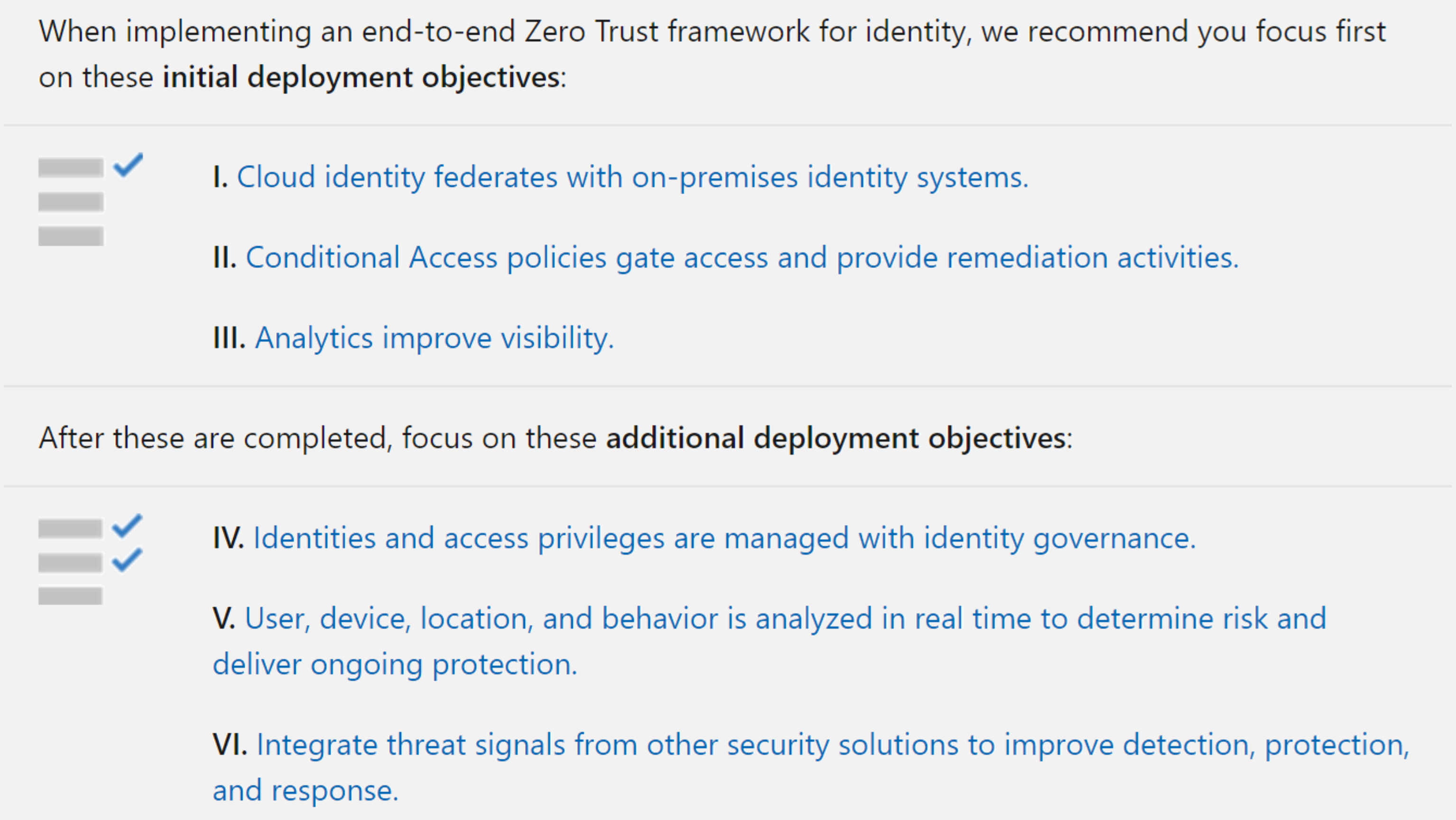
Networking

Data



A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end-strategy!

Securing Identity with Zero Trust



When implementing an end-to-end Zero Trust framework for identity, we recommend you focus first on these **initial deployment objectives**:

I. Cloud identity federates with on-premises identity systems.

II. Conditional Access policies gate access and provide remediation activities.

III. Analytics improve visibility.

After these are completed, focus on these **additional deployment objectives**:

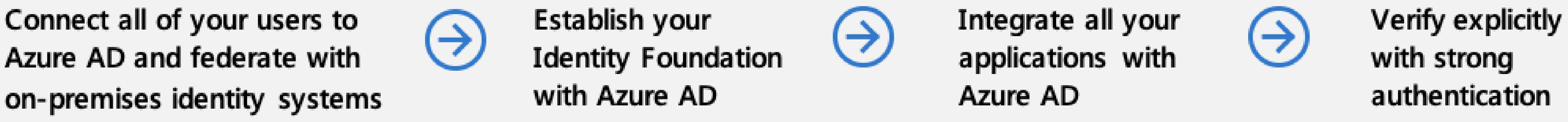
IV. Identities and access privileges are managed with identity governance.

V. User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection.

VI. Integrate threat signals from other security solutions to improve detection, protection, and response.

Securing identity with Zero Trust | Microsoft Docs

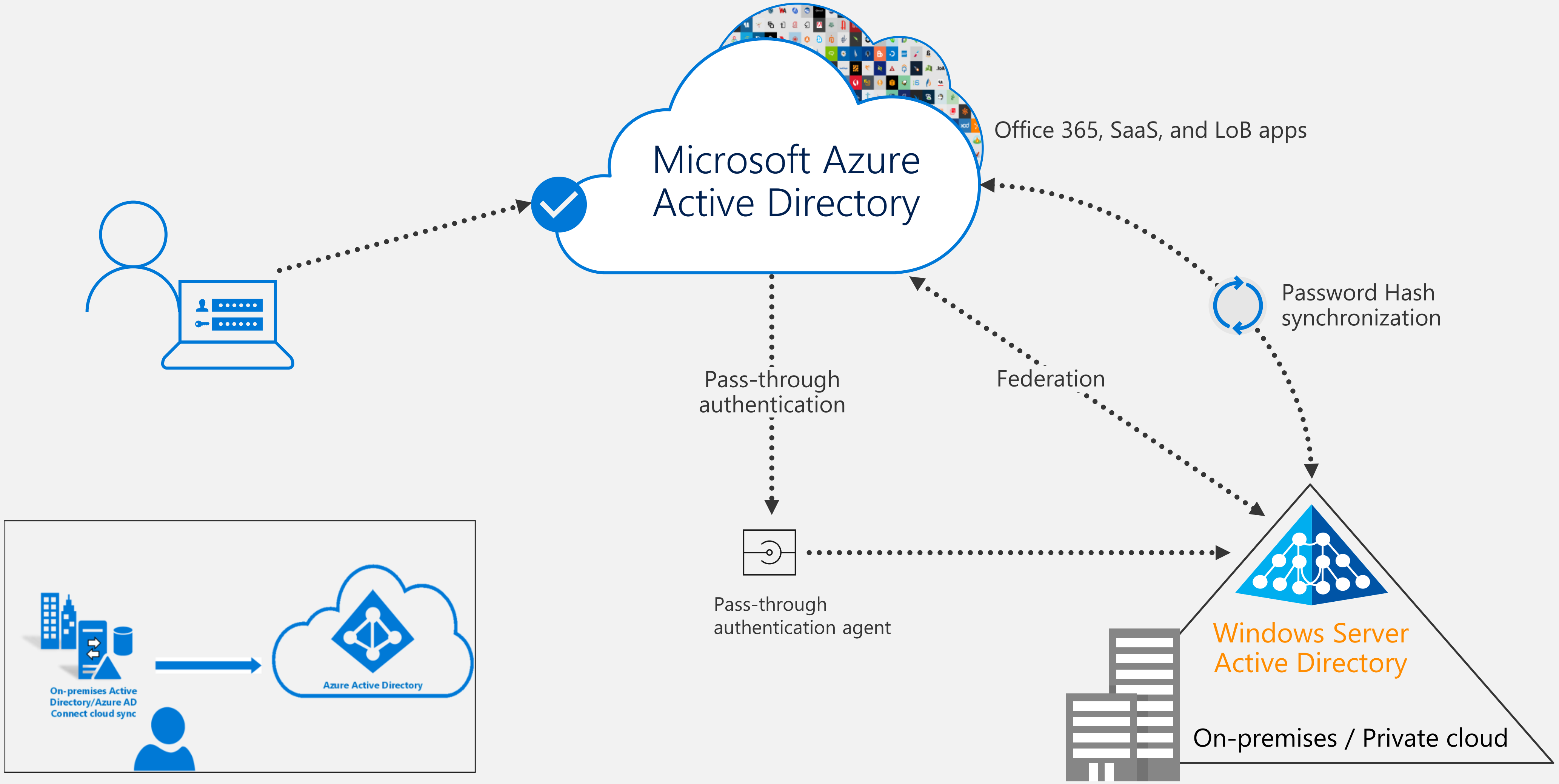
I. Cloud Identity integrates with on-premises identity



Connect all of your users to Azure AD and federate with on-premises identity systems → Establish your Identity Foundation with Azure AD → Integrate all your applications with Azure AD → Verify explicitly with strong authentication

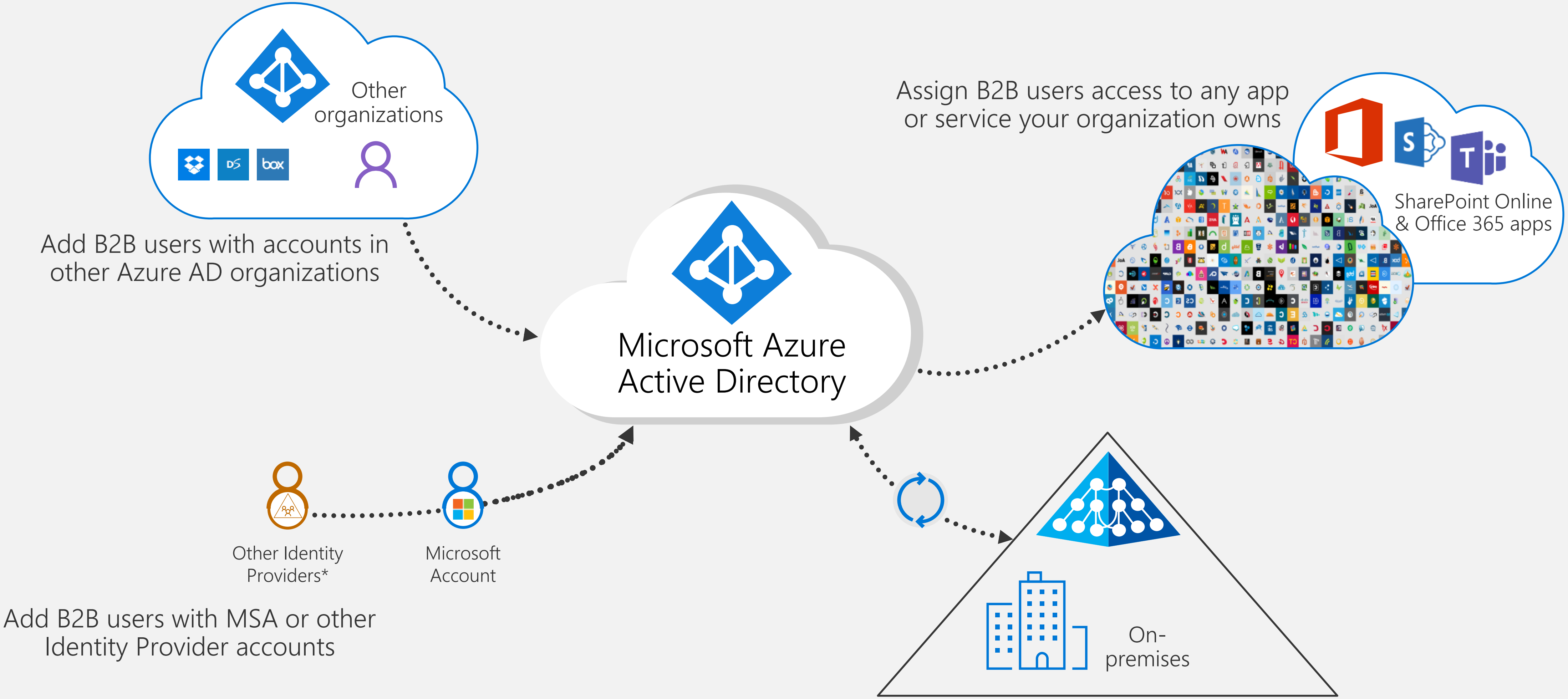
Securing identity with Zero Trust | Microsoft Docs

Connect your users to Entra ID (Azure AD)


Microsoft Azure Active Directory
Office 365, SaaS, and LoB apps
Password Hash synchronization
Pass-through authentication
Federation
Pass-through authentication agent
Windows Server Active Directory
On-premises / Private cloud
On-premises Active Directory/Azure AD Connect cloud sync
Azure Active Directory

What is CloudSync

Connect your partner identities



Other organizations

Add B2B users with accounts in other Azure AD organizations

Microsoft Azure Active Directory

Assign B2B users access to any app or service your organization owns

SharePoint Online & Office 365 apps

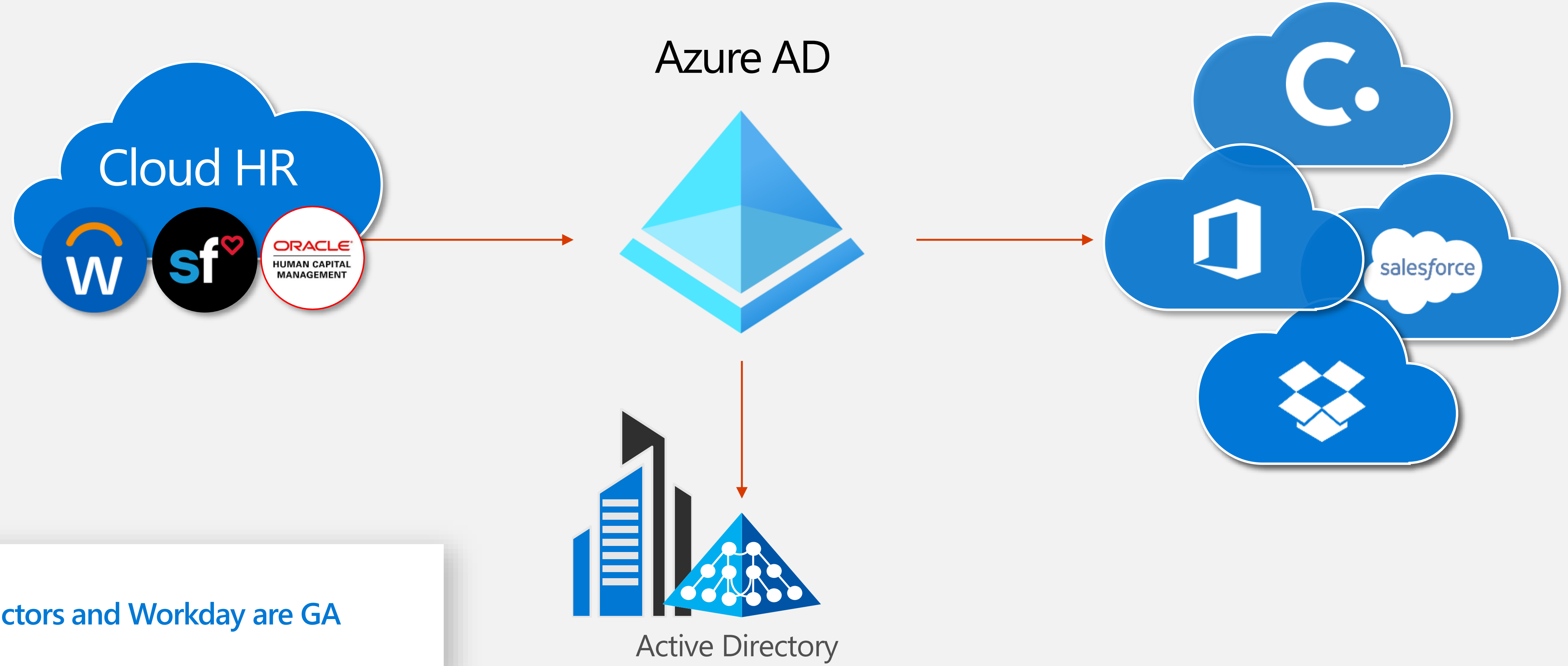
Other Identity Providers*

Microsoft Account

Add B2B users with MSA or other Identity Provider accounts

On-premises

Cloud HR user provisioning



Success Factors and Workday are GA

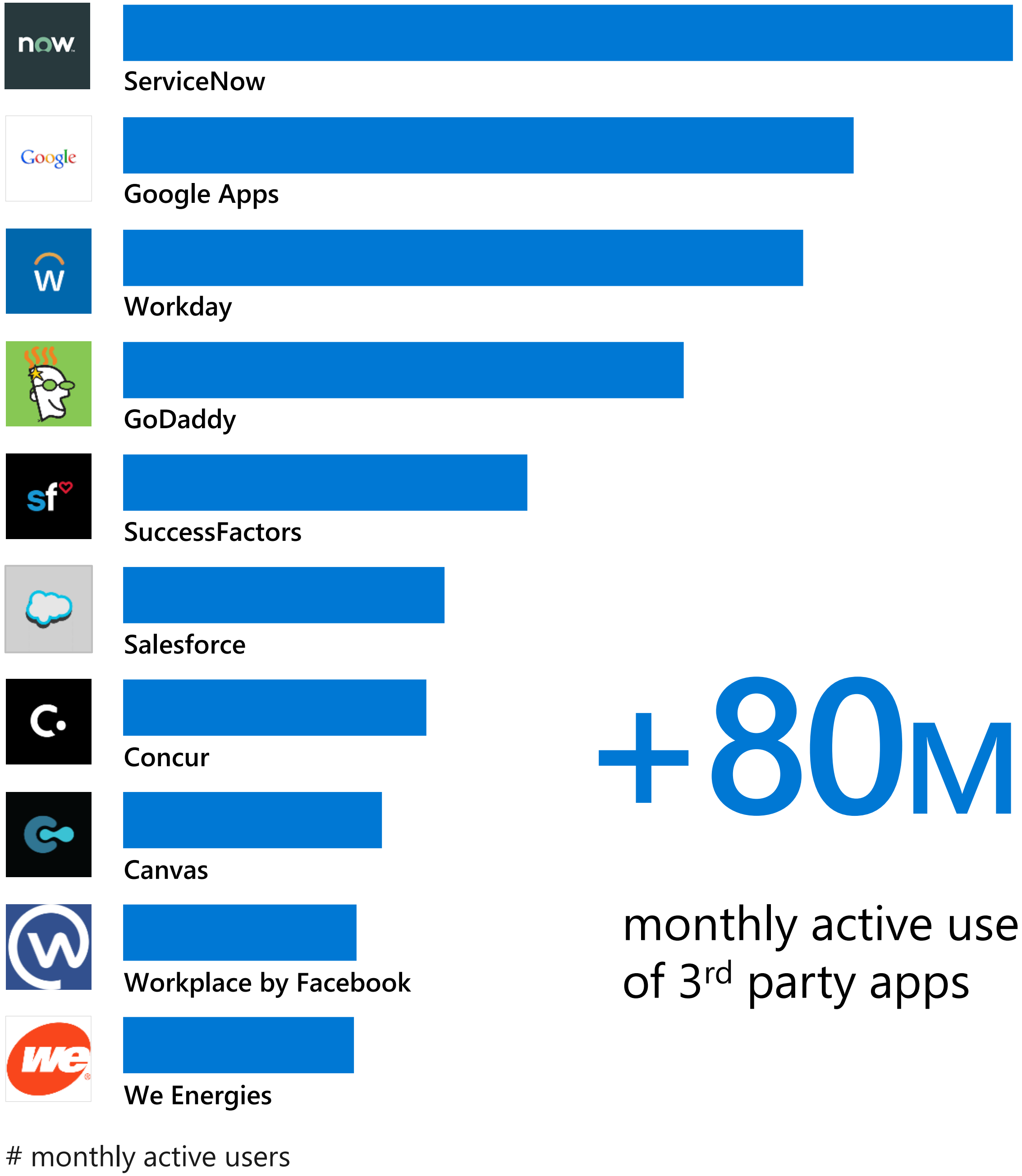
Azure Active Directory

3rd party applications

>2M

active apps

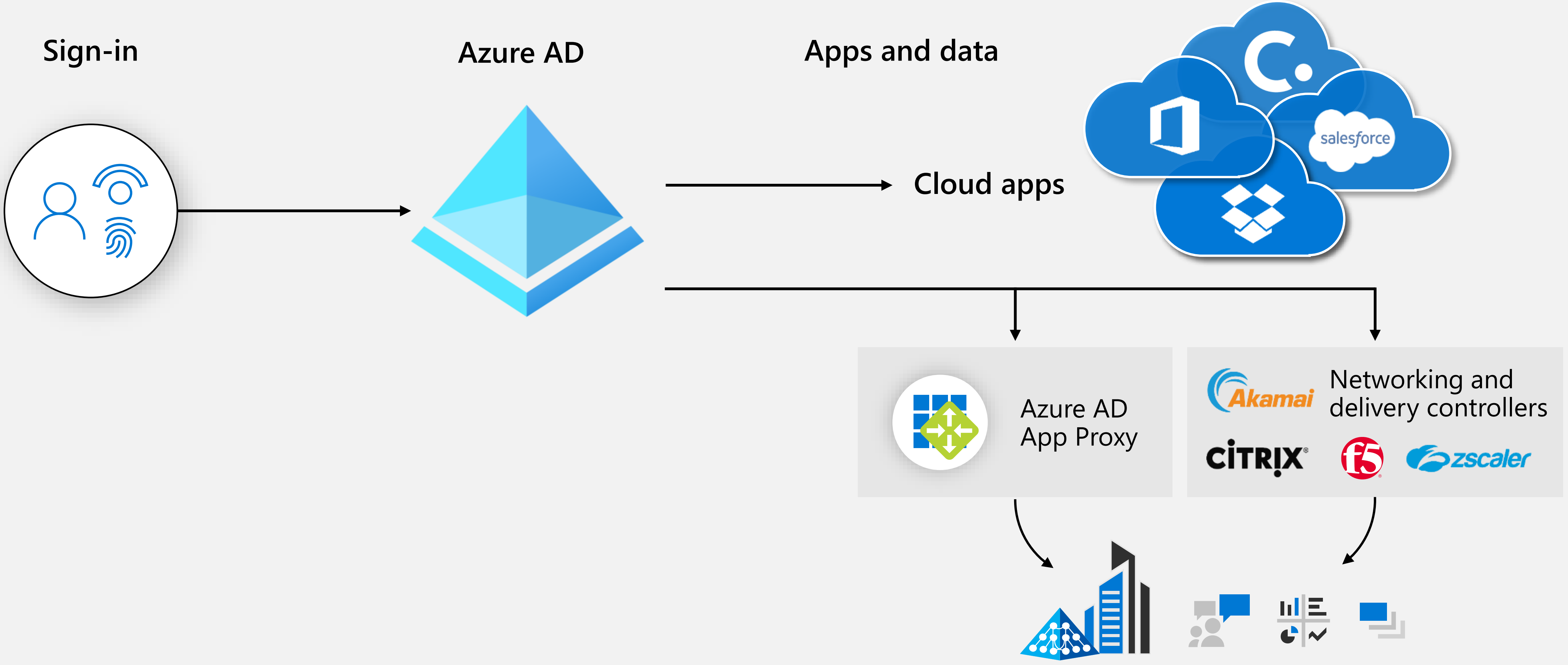
[Five steps to integrate your apps with Azure Active Directory - Microsoft Entra | Microsoft Learn]



+80M

monthly active users of 3rd party apps

Secure hybrid access



Sign-in

Azure AD

Apps and data

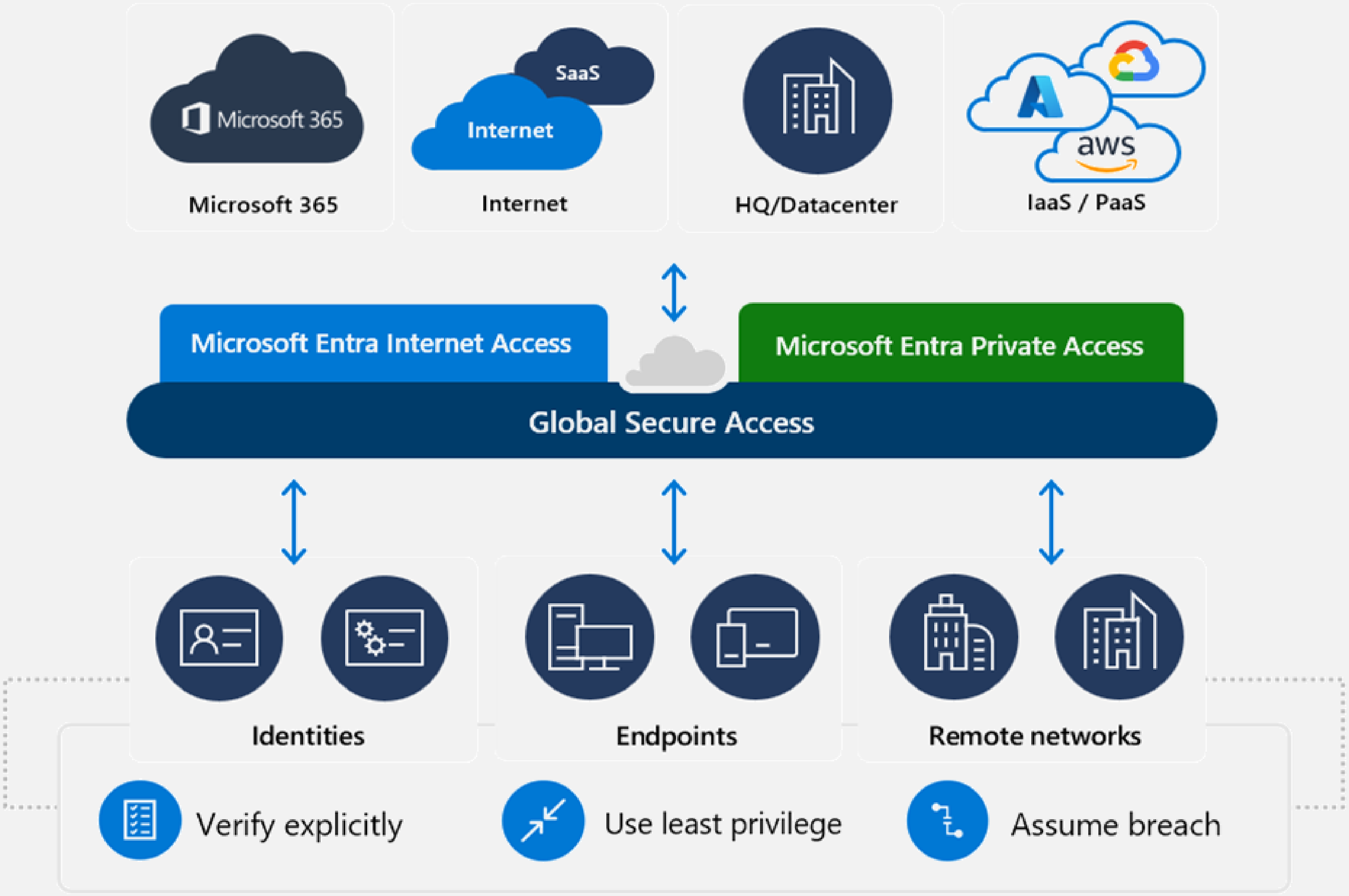
Cloud apps

Azure AD App Proxy

Networking and delivery controllers

On-premises perimeter-based networks

Global Secure Access (Preview)



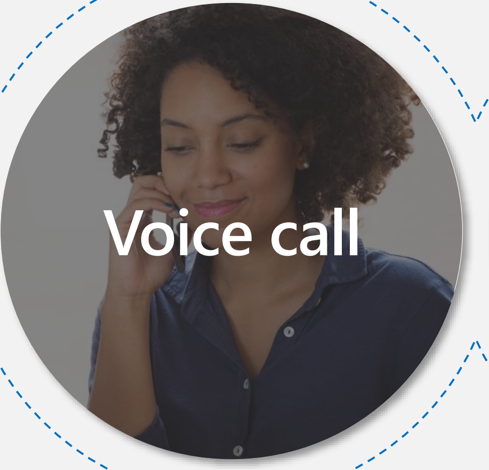
[What is Global Secure Access (preview)? | Microsoft Learn]

Verify with Strong Authentication

Multi-factor authentication prevents 99.9% of identity attacks

Push notificatio n

SMS



Voice call

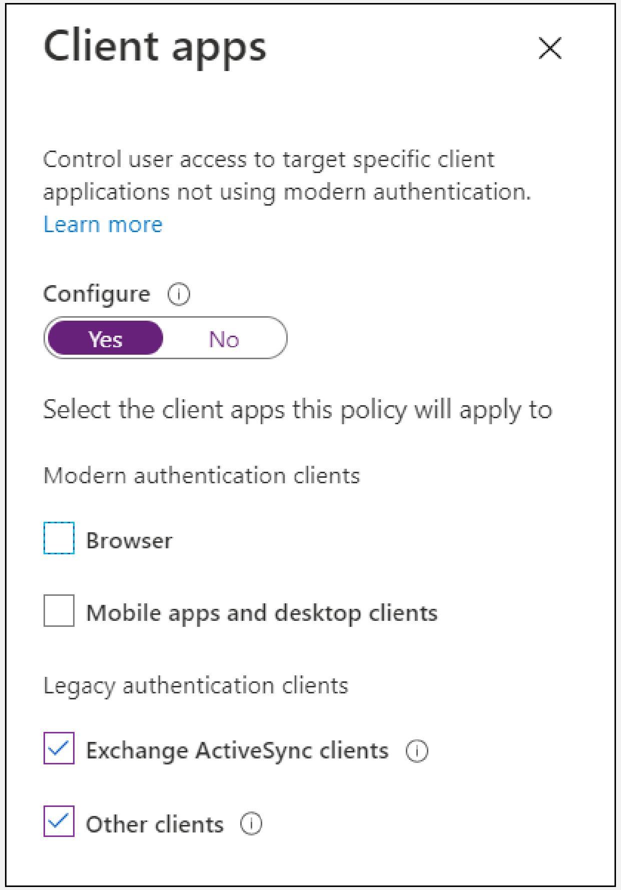
OATH Token

OATH codes

FIDO2
Passwordless

Block Legacy Authentication

- Legacy protocols are preferred by attackers:
  - More than 99 percent of password spray attacks use legacy authentication protocols
  - More than 97 percent of credential stuffing attacks use legacy authentication
  - Azure AD accounts in organizations that have disabled legacy authentication experience 67 percent fewer compromises than those where legacy authentication is enabled
- Block Legacy Authentication Directly or Indirectly
- Use Security Defaults



Client apps

Control user access to target specific client applications not using modern authentication. Learn more

Configure: [✓ Yes] No

Select the client apps this policy will apply to

Modern authentication clients

□ Browser

□ Mobile apps and desktop clients

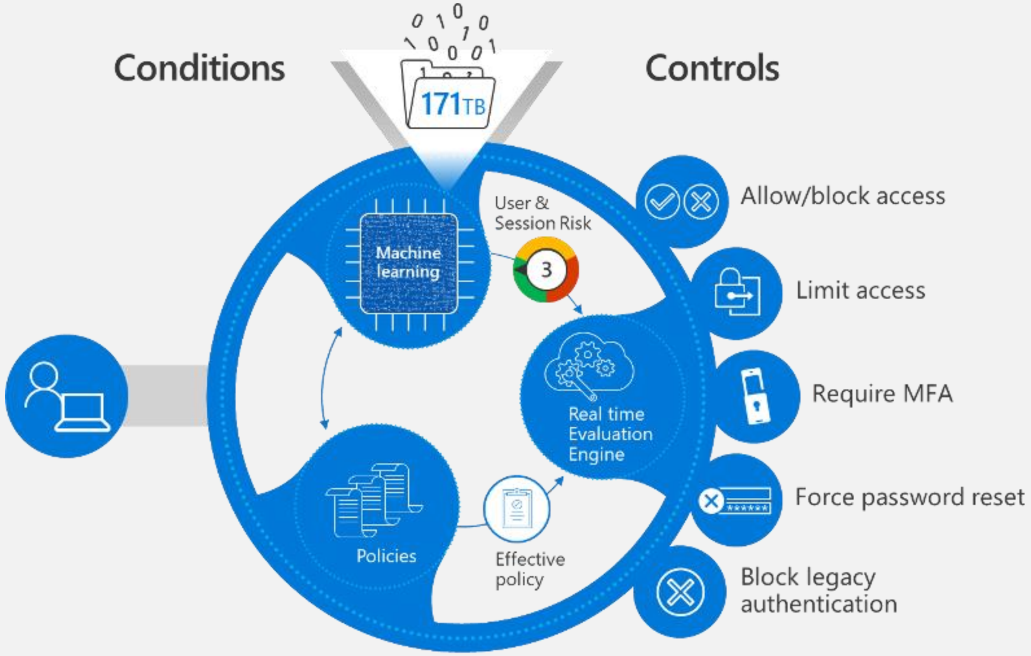
Legacy authentication clients

☑ Exchange ActiveSync clients

☑ Other clients

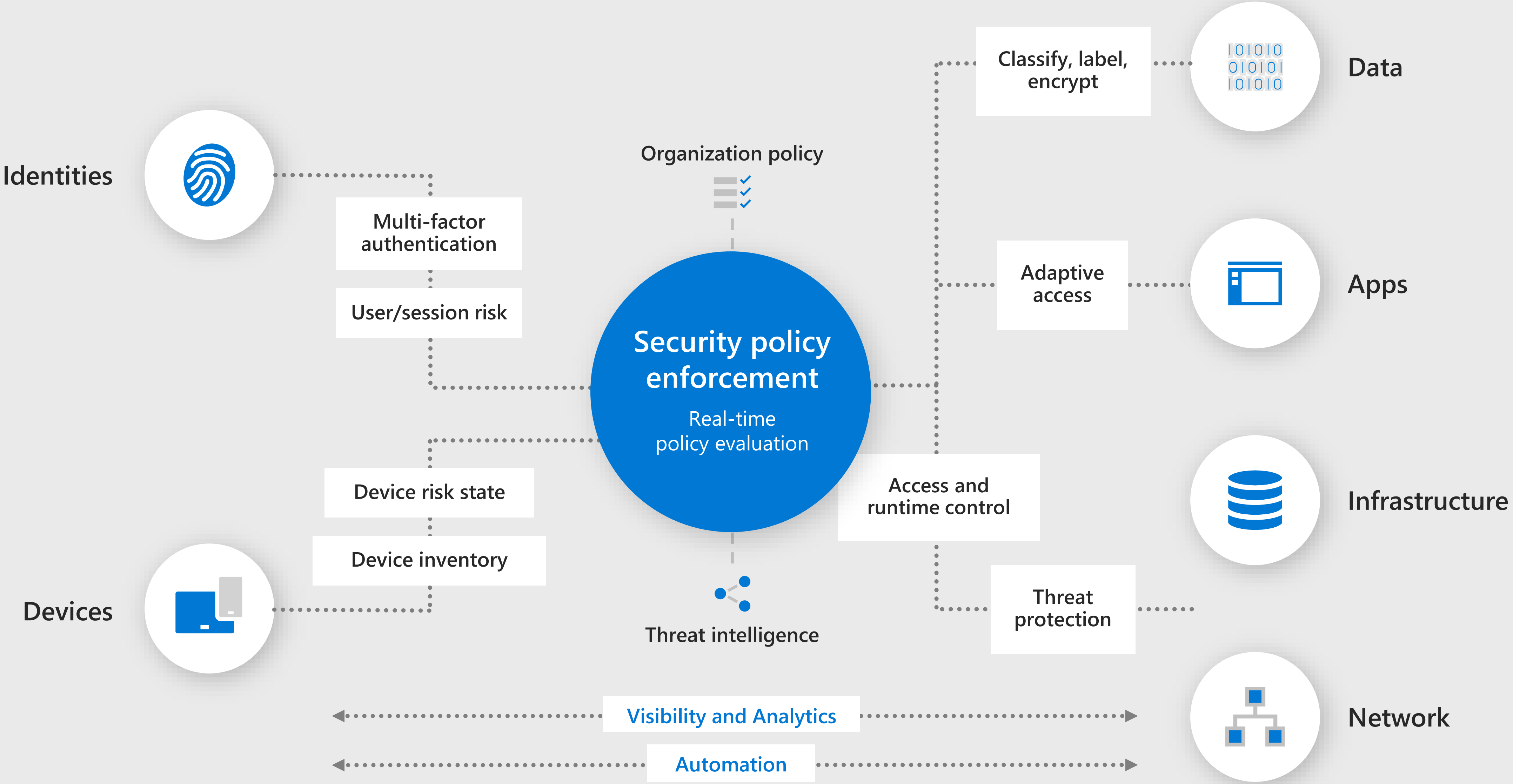
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

II. Conditional Access policies gate access and provide remediation activities

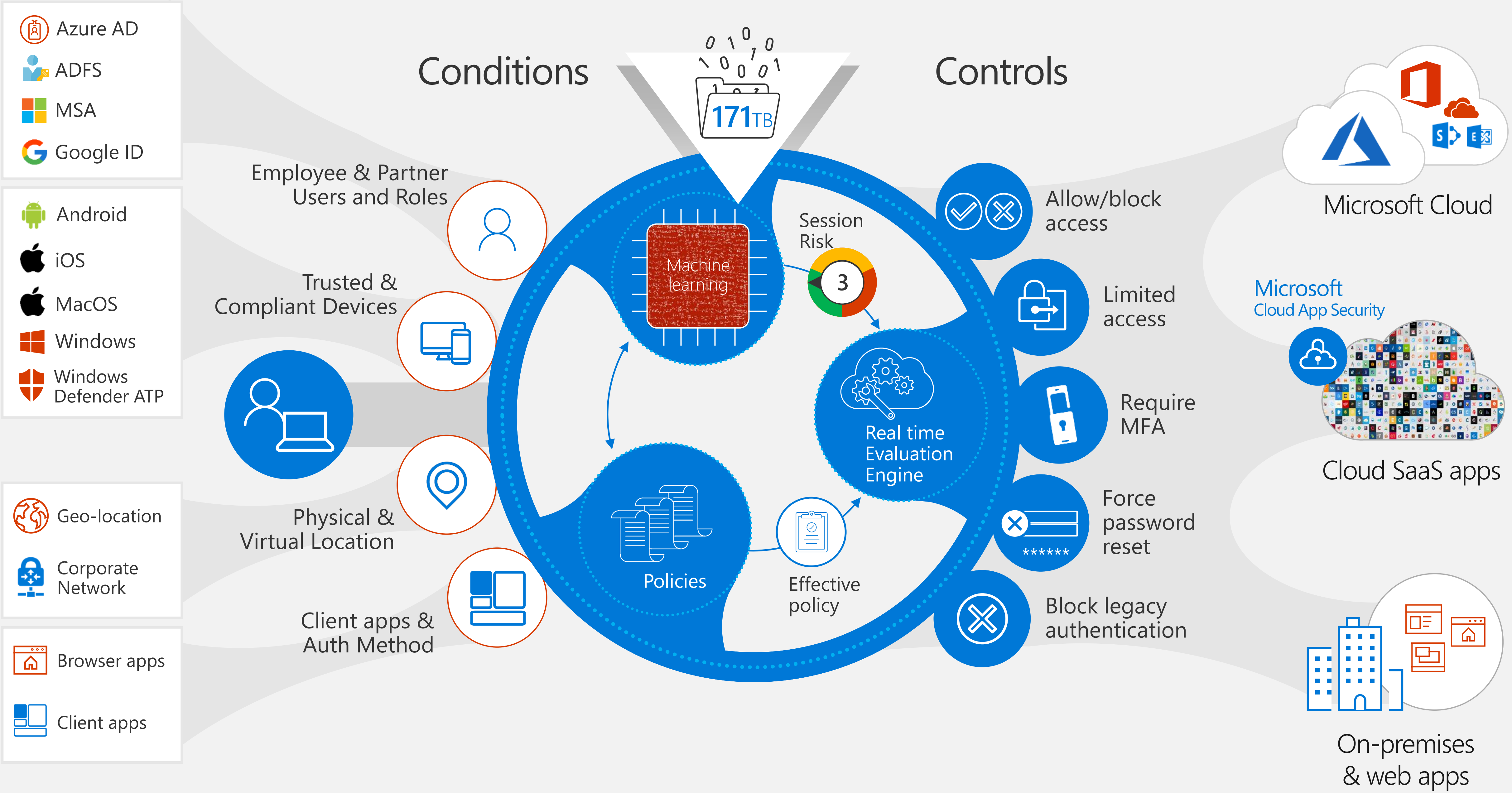


Securing identity with Zero Trust | Microsoft Docs

Microsoft Zero Trust architecture



Conditional Access Policies gate access and provide remediation activities



Azure AD
ADFS
MSA
Google ID

Android
iOS
MacOS
Windows
Windows Defender ATP

Geo-location
Corporate Network

Browser apps
Client apps

Conditions

Employee & Partner Users and Roles

Trusted & Compliant Devices

Physical & Virtual Location

Client apps & Auth Method

171TB

Machine learning

Session Risk

3

Real time Evaluation Engine

Policies

Effective policy

Controls

Allow/block access

Limited access

Require MFA

Force password reset

******

Block legacy authentication

Microsoft Cloud

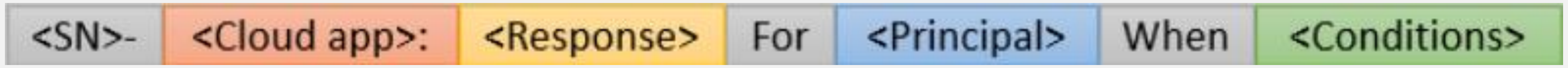
Microsoft Cloud App Security

Cloud SaaS apps

On-premises & web apps

Conditional Access Best Practices

- Naming Standard



<SN>-	<Cloud app>:	<Response>	For	<Principal>	When	<Conditions>

Example **CA01 – Exchange Online**: **Require MFA** For **IT Department** When **on external networks**

- Resilient access controls in outage/emergency scenarios
  - Avoid administrator lockout by using emergency access accounts
  - Implement MFA using Conditional Access (CA) rather than per-user MFA
  - Mitigate user lockout by using multiple Conditional Access (CA) controls
  - Mitigate user lockout by provisioning multiple authentication methods or equivalents for each user
- How are Conditional Access policies applied
  - All Policies that apply must be satisfied
  - All assignments are logically **ANDed**
  - Consider interconnected Office 365 apps

Plan an Azure Active Directory Conditional Access Deployment | Microsoft Docs

Conditional Access for Zero Trust - Azure Architecture Center | Microsoft Learn

III. Analytics improve visibility

Configure logging and reporting to improve visibility

- Plan Azure AD Reporting
- Route logs to:
  - Azure Storage account
  - Azure Monitor logs
  - Azure Event Hub
  - Connect AAD logs to Sentinel
- Azure AD Workbooks
  - Azure Monitor workbooks for Azure Active Directory - Microsoft Entra | Microsoft Learn

Securing identity with Zero Trust | Microsoft Docs

Azure Sentinel

Cloud-native SIEM for intelligent security analytics

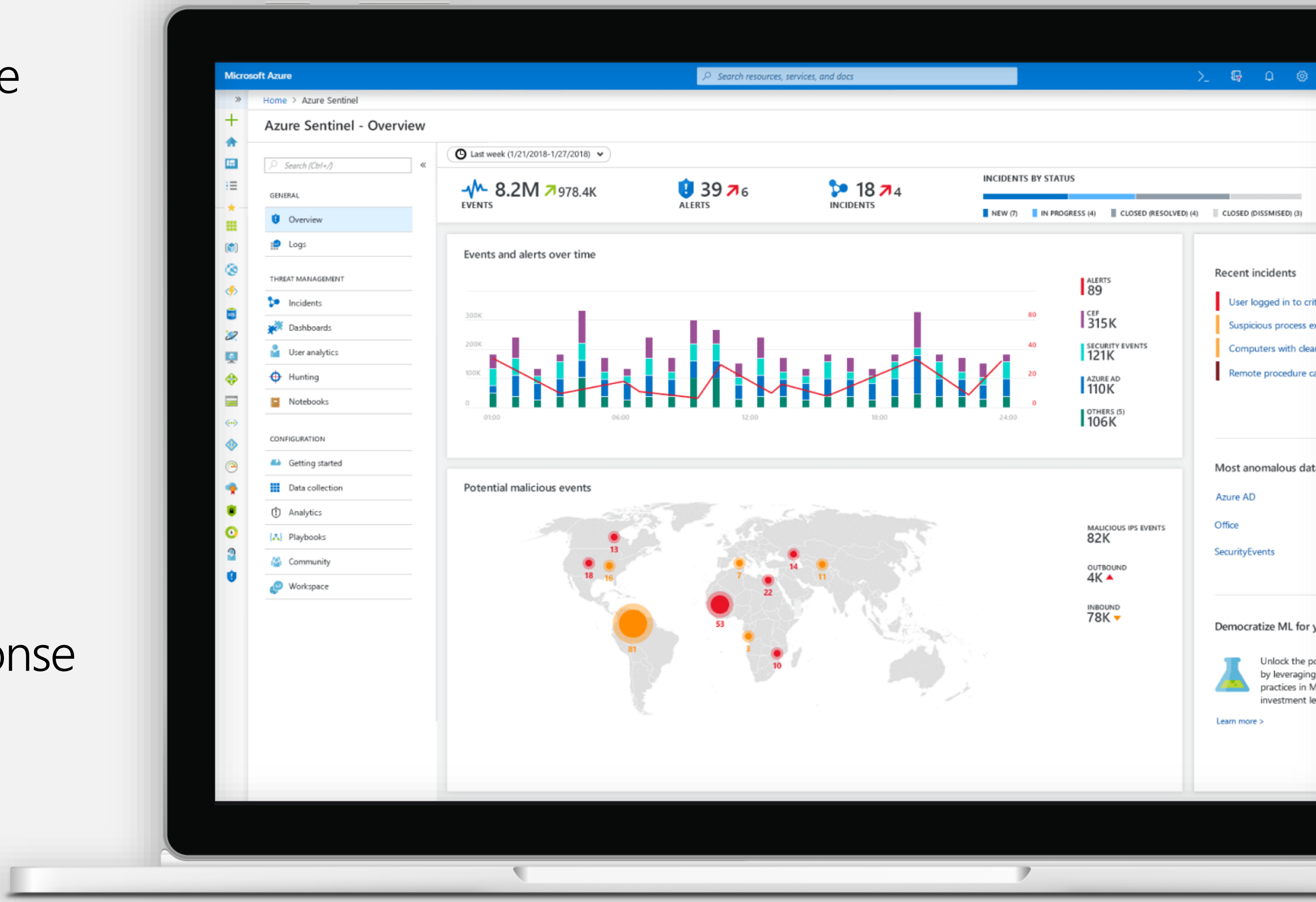
Limitless cloud speed and scale

Bring your Office 365 data for free

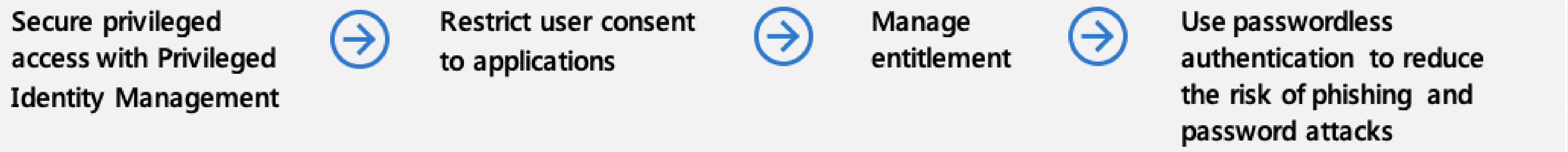
Faster threat protection with AI by your side

Easy integration with your existing tools

Easily automate incident response



IV. Identities and access privileges are managed with identity governance



Secure privileged access with Privileged Identity Management

Restrict user consent to applications

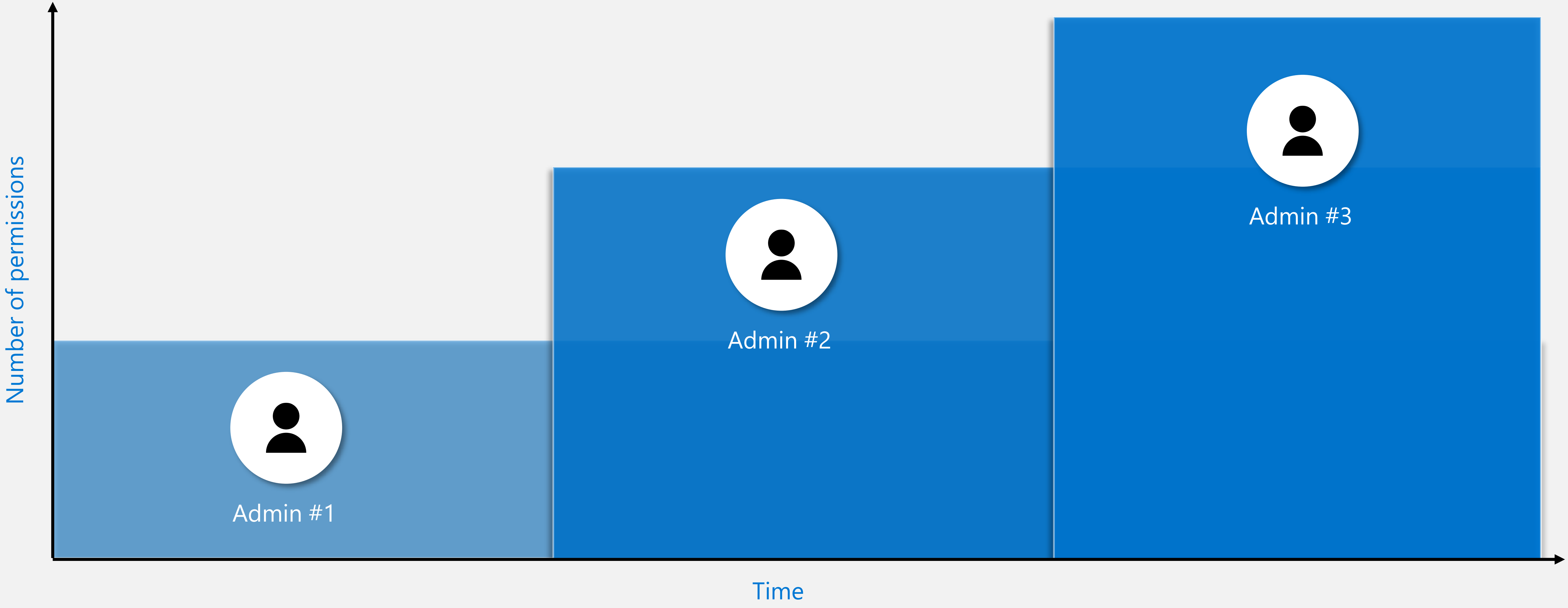
Manage entitlement

Use passwordless authentication to reduce the risk of phishing and password attacks

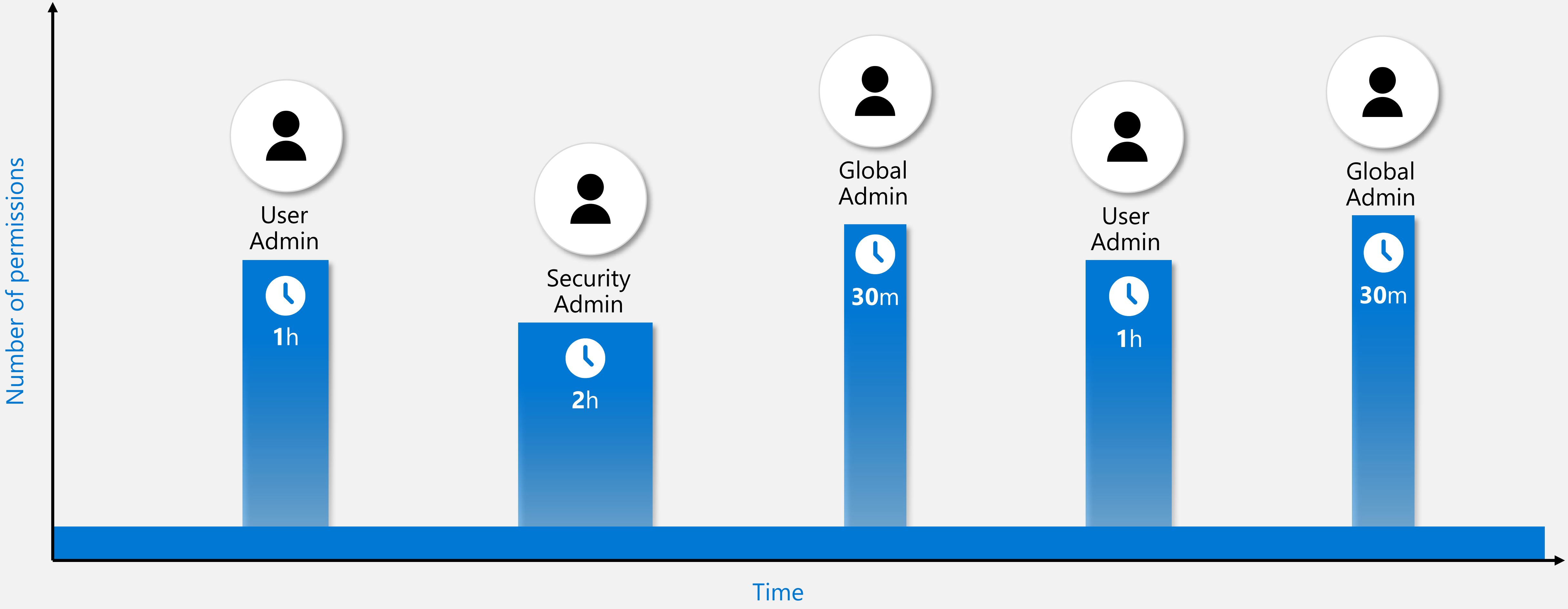
[Securing identity with Zero Trust | Microsoft Docs]

Accumulated risk

# admins with highest levels of privileges over time

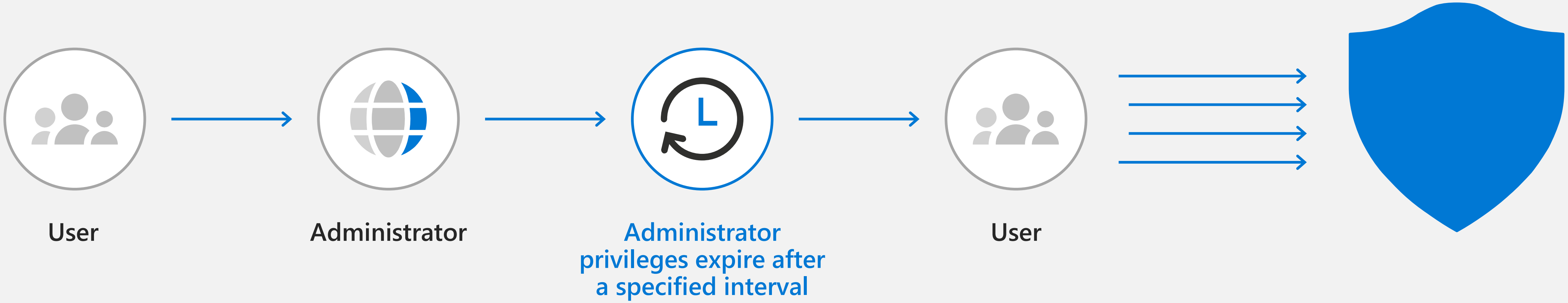


What you want: Least Privileged Access



Privileged Identity Management

Discover, restrict, and monitor privileged identity access



User

Administrator

Administrator privileges expire after a specified interval

User

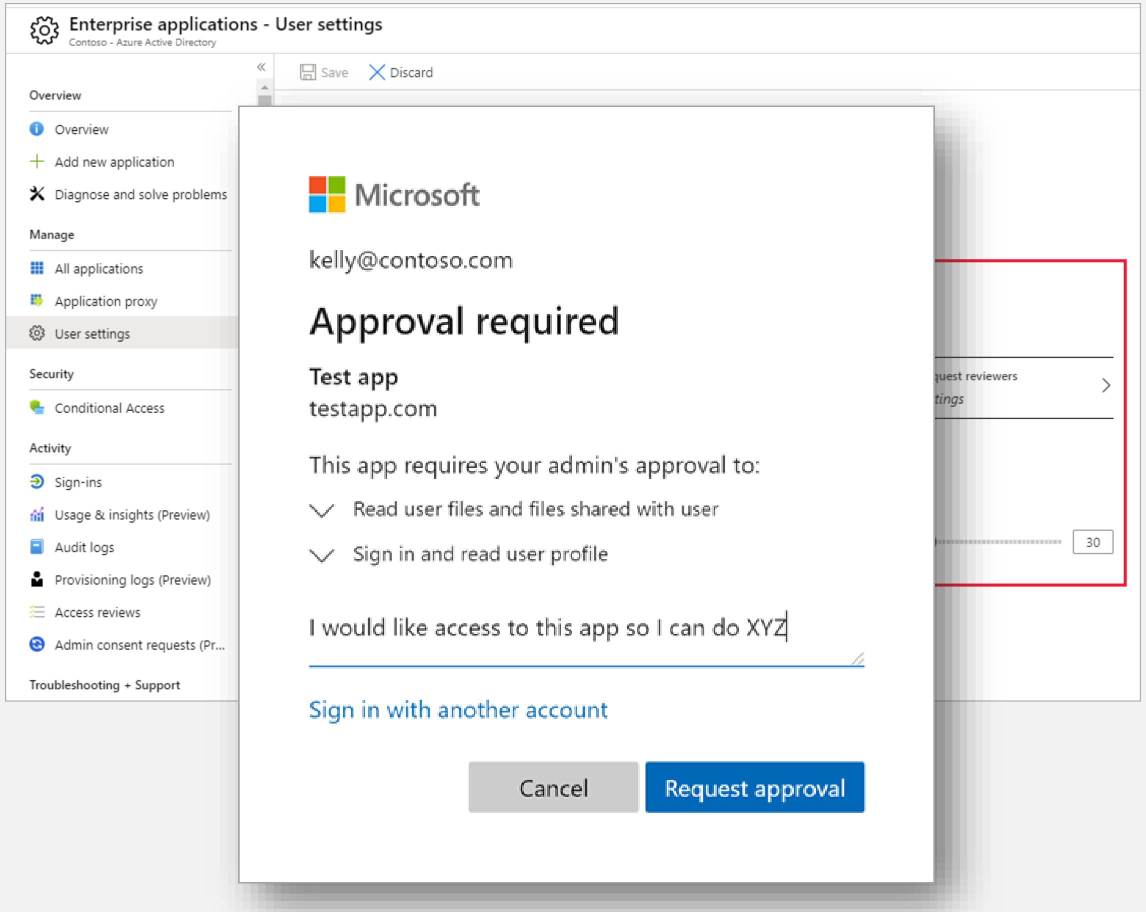
- → Enforce on-demand, just-in-time administrative access when needed
- → Ensure policies are met with alerts, audit reports and access reviews
- → Manage admins access in Azure AD and in Azure RBAC

Manage consent to applications

1. Enable the Admin Consent workflow

2. Ensure all admins understand the permissions and consent framework

3. Review existing processes



Enterprise applications - User settings
Contoso - Azure Active Directory
Save
Discard
Overview
Overview
Add new application
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Admin consent requests (Pr...
Troubleshooting + Support
quest reviewers
tings
30
Microsoft

kelly@contoso.com

Approval required

Test app
testapp.com

This app requires your admin's approval to:

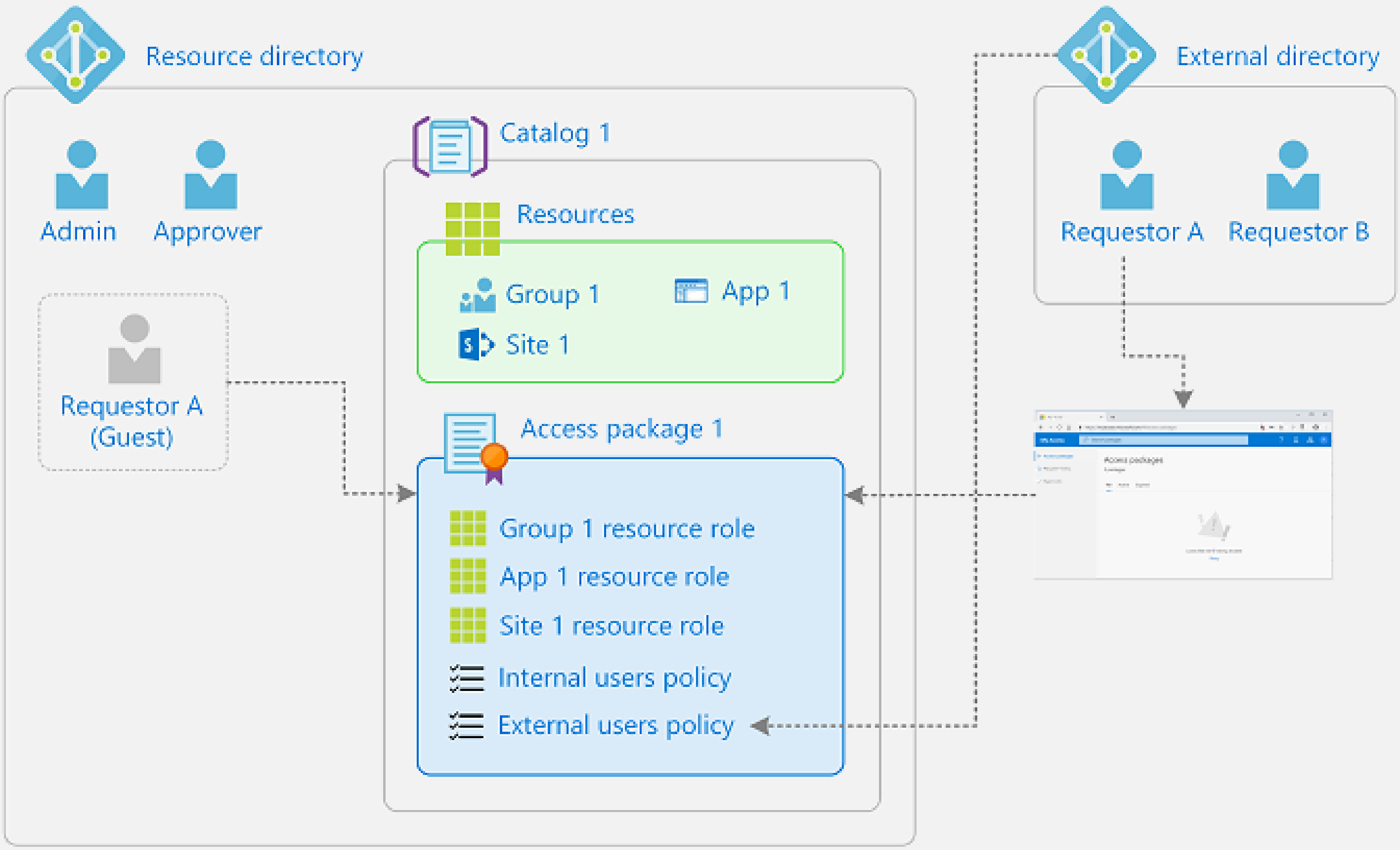
- Read user files and files shared with user
- Sign in and read user profile

I would like access to this app so I can do XYZ

Sign in with another account
Cancel
Request approval

[Manage consent to applications and evaluate consent requests - Azure AD]()

Entitlement Management



Only Hackers ♥ Passwords

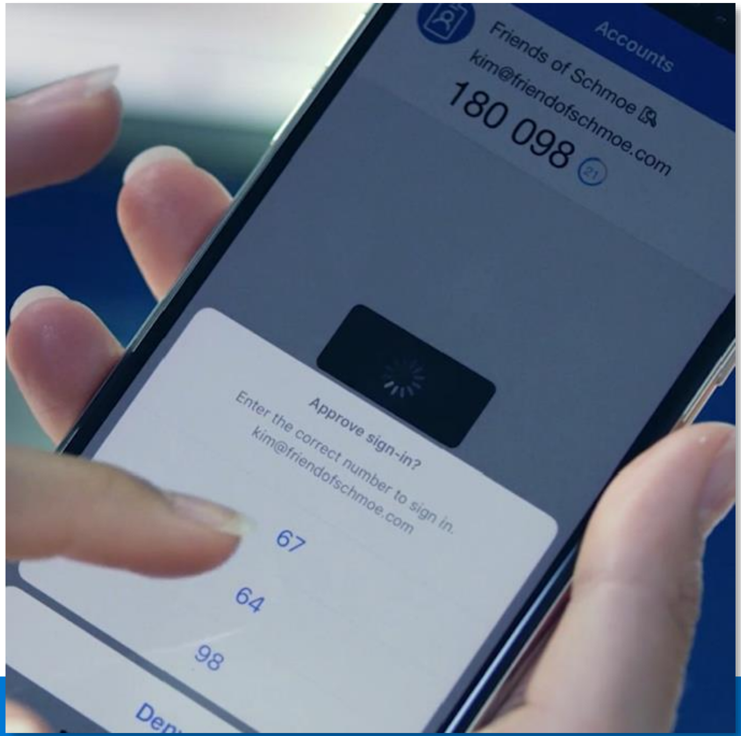
Phishing and hacking with **stolen credentials** are the top threat action varieties in breaches.

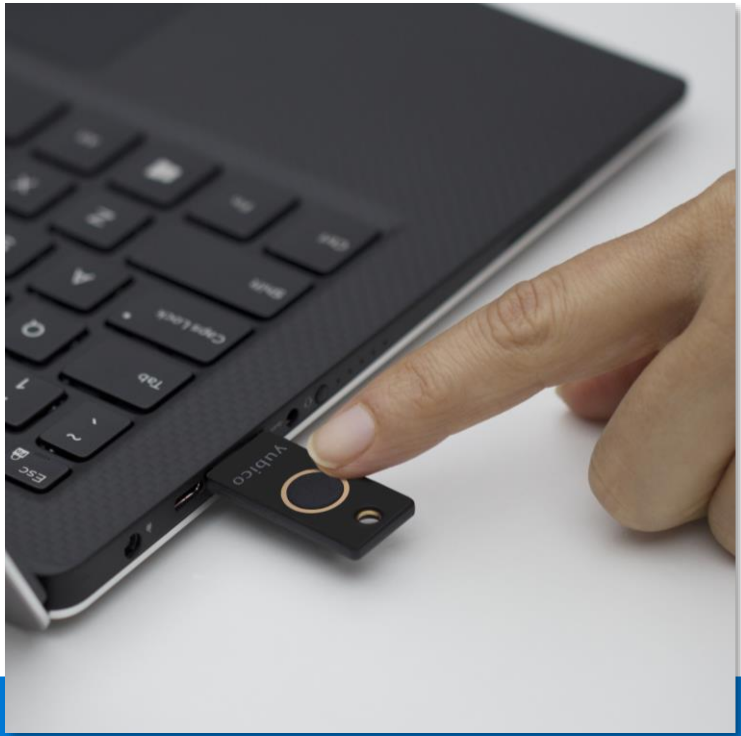
verizon✓ Data Breach Investigations Report 2019

Bad: Password	**Good:** Password and…	**Better:** Password and…	**Best:** Passwordless
123456	SMS	Microsoft Authenticator	Windows Hello
qwerty	Voice	Software Tokens OTP	Microsoft Authenticator (Preview)
password		Hardware Tokens OTP (Preview)	FIDO2 security key (Preview)
iloveyou			
Password1			

Getting to a world without passwords

High security, convenient methods of strong authentication

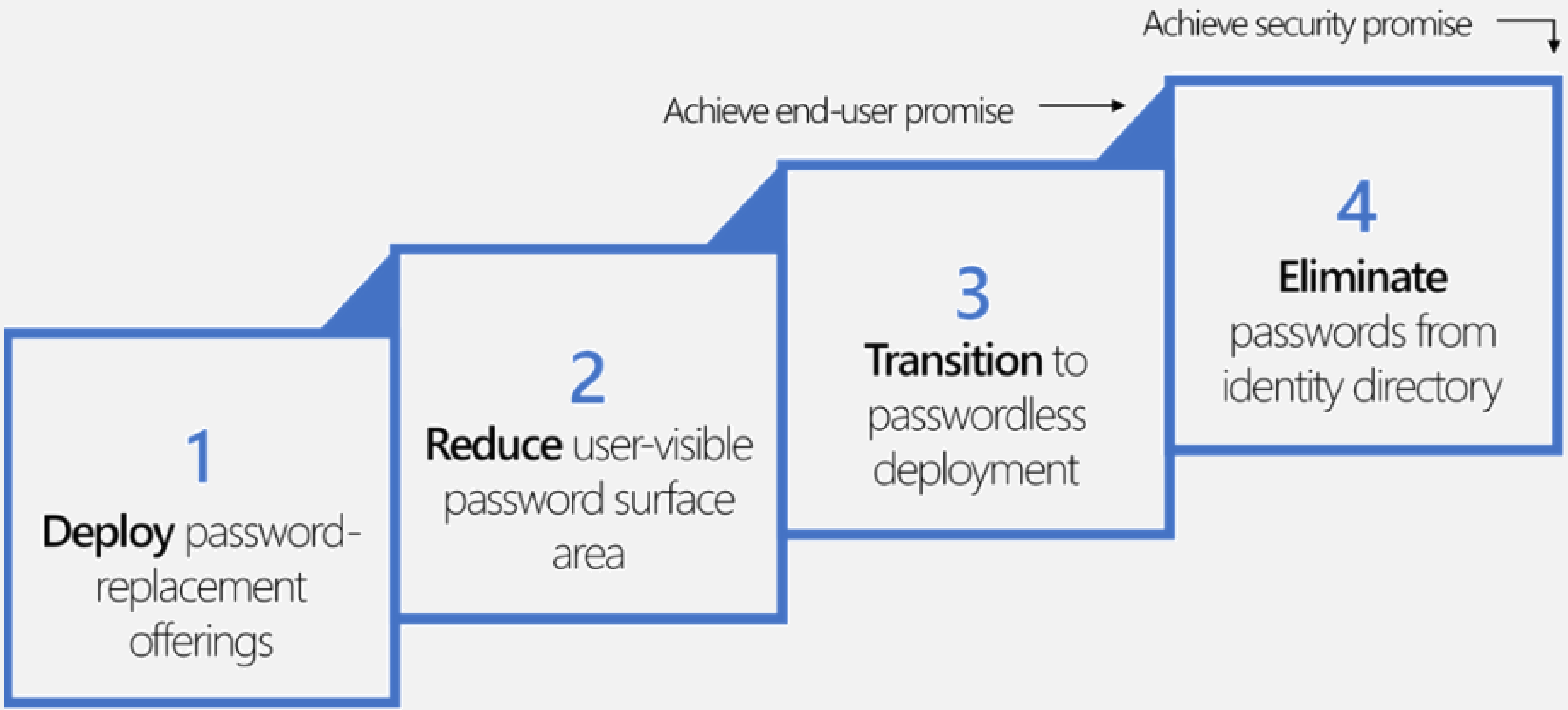




200M+ Monthly active passwordless users

#nomorepasswords

Microsoft passwordless strategy



Achieve security promise

Achieve end-user promise

1
Deploy password-replacement offerings

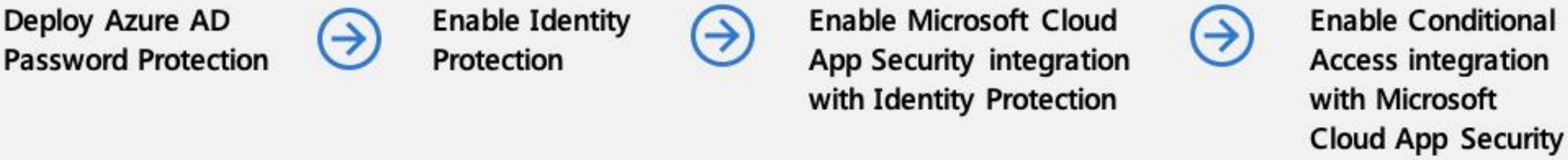
2
Reduce user-visible password surface area

3
Transition to passwordless deployment

4
Eliminate passwords from identity directory

Plan a passwordless authentication deployment with Azure AD | Microsoft Docs

V. User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection



Deploy Azure AD Password Protection

Enable Identity Protection

Enable Microsoft Cloud App Security integration with Identity Protection

Enable Conditional Access integration with Microsoft Cloud App Security

Securing identity with Zero Trust | Microsoft Docs

Azure AD Password Protection

Dynamically bans passwords based on known bad patterns and those you define.

Global banned password list

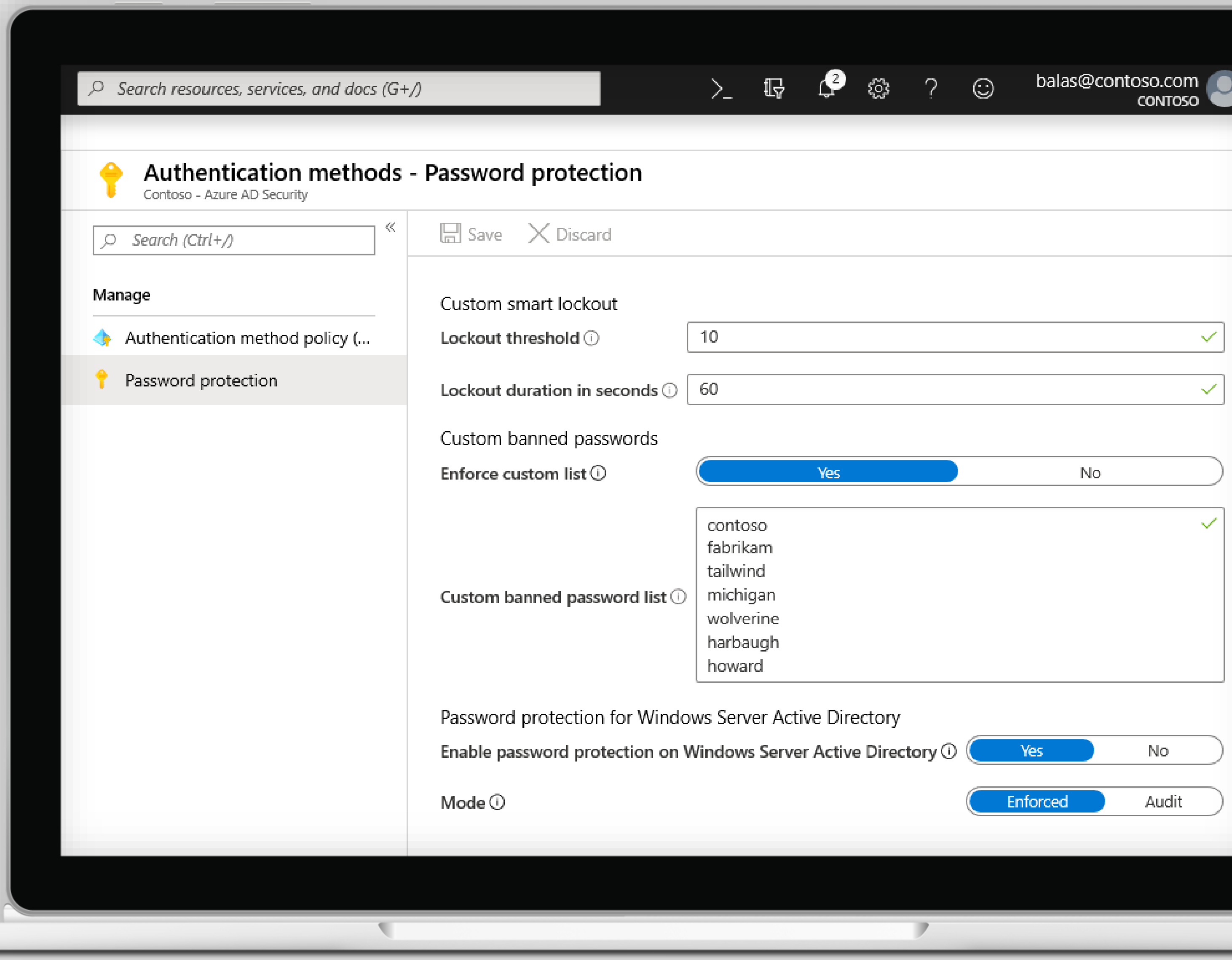
Microsoft defines a global list with almost 2,000 words, phrases, patterns.

Custom banned password list

1,000 words and phrases unique to your organization.

Banned password algorithm

Finds all weak password variations.



Authentication methods - Password protection

Contoso - Azure AD Security

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:

contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: [✓ Enforced] Audit

Identity protection

- Intelligently detect and respond to compromised accounts

300%

increase in identity attacks over the past year

Real-time detection

Automated remediation

Connected intelligence

Azure AD Identity Protection

Gigantic datasets

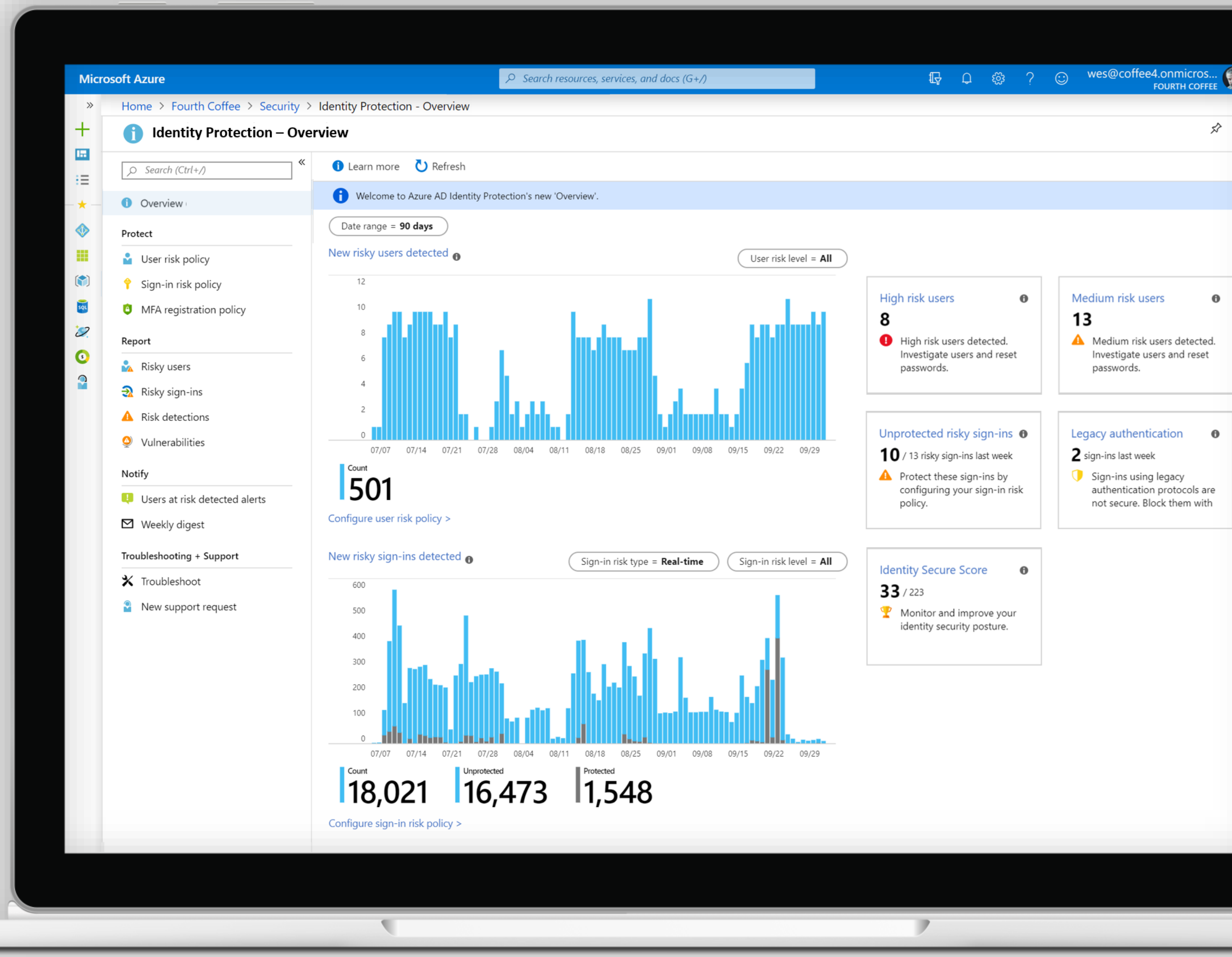
World-class machine learning

Security experts

Continuously evolving algorithms

Global threat intelligence

Realtime, automated mitigations



Microsoft Azure

Search resources, services, and docs (G+/)

wes@coffee4.onmicros...
FOURTH COFFEE

Home > Fourth Coffee > Security > Identity Protection - Overview

Identity Protection – Overview

Search (Ctrl+/)

Overview

Protect

- User risk policy
- Sign-in risk policy
- MFA registration policy

Report

- Risky users
- Risky sign-ins
- Risk detections
- Vulnerabilities

Notify

- Users at risk detected alerts
- Weekly digest

Troubleshooting + Support

- Troubleshoot
- New support request

Learn more   Refresh

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

Date range = **90 days**

New risky users detected

User risk level = **All**

Count
501

Configure user risk policy >

New risky sign-ins detected

Sign-in risk type = **Real-time**   Sign-in risk level = **All**

Count 18,021   Unprotected 16,473   Protected 1,548

Configure sign-in risk policy >

High risk users
8
High risk users detected. Investigate users and reset passwords.

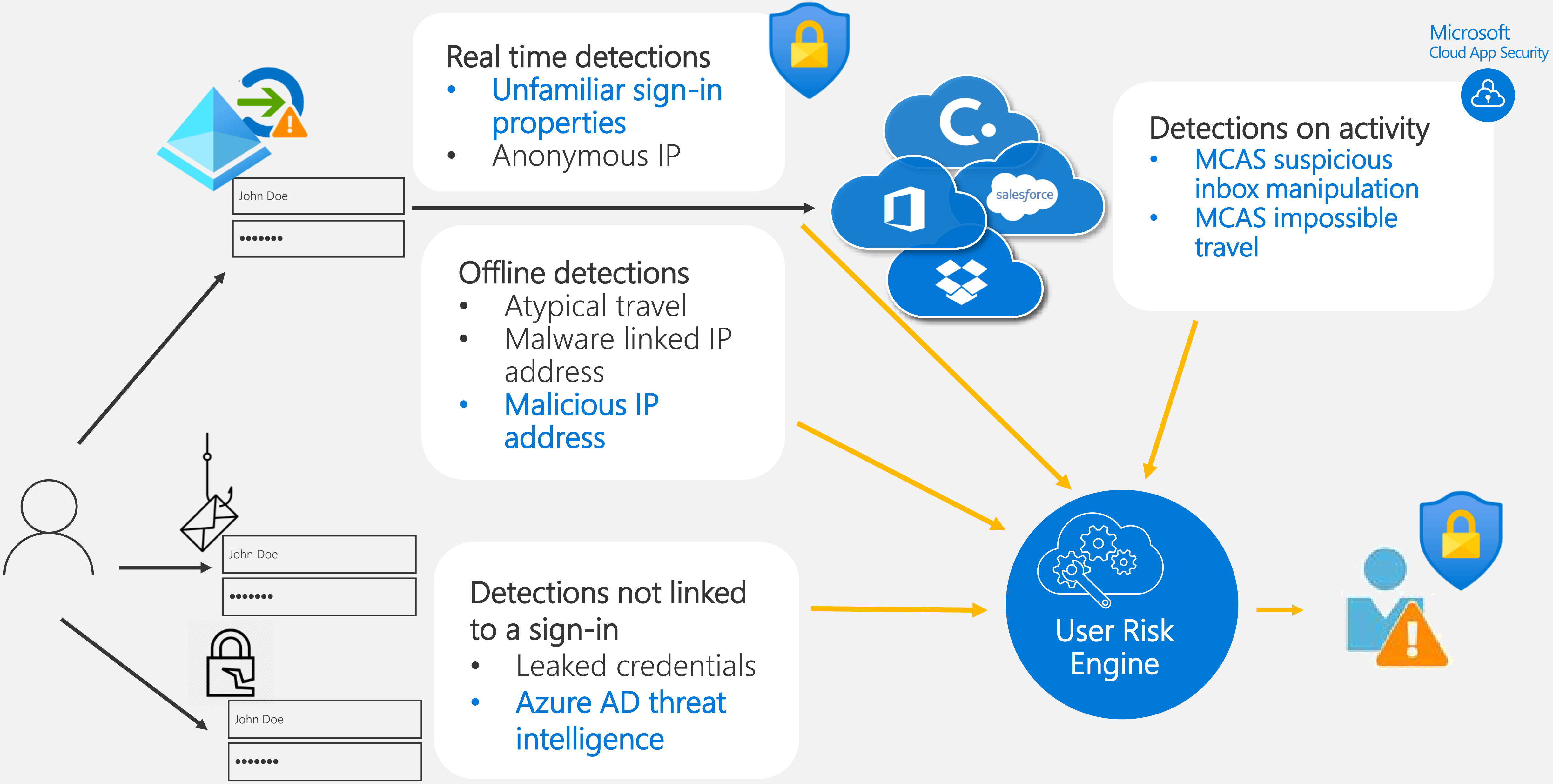
Medium risk users
13
Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins
10 / 13 risky sign-ins last week
Protect these sign-ins by configuring your sign-in risk policy.

Legacy authentication
2 sign-ins last week
Sign-ins using legacy authentication protocols are not secure. Block them with

Identity Secure Score
33 / 223
Monitor and improve your identity security posture.

Risk detections and risk engine



Real time detections

- Unfamiliar sign-in properties
- Anonymous IP

Offline detections

- Atypical travel
- Malware linked IP address
- Malicious IP address

Detections not linked to a sign-in

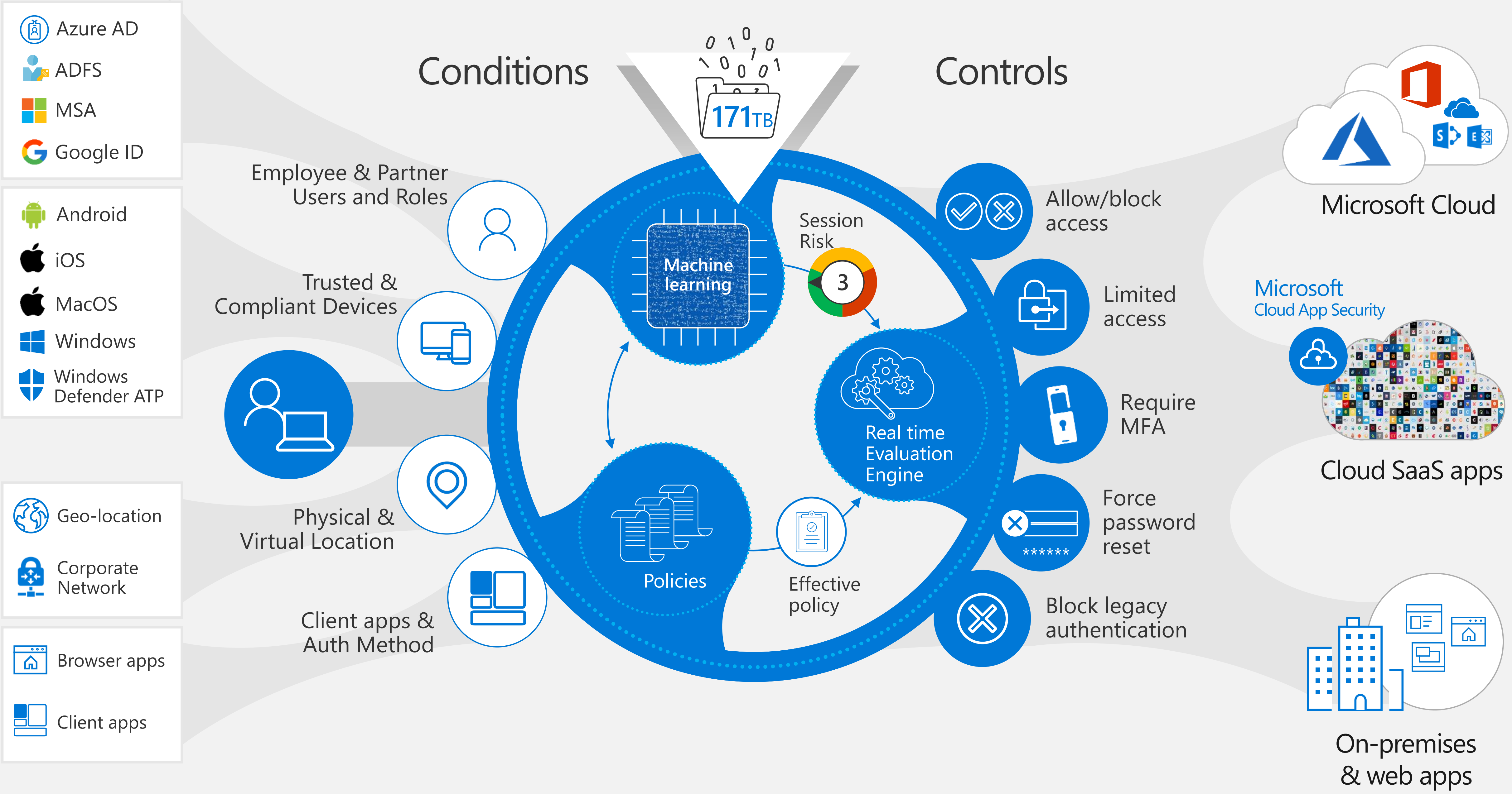
- Leaked credentials
- Azure AD threat intelligence

Detections on activity

- MCAS suspicious inbox manipulation
- MCAS impossible travel

User Risk Engine

Conditional Access Policies gate access and provide remediation activities



Azure AD
ADFS
MSA
Google ID

Android
iOS
MacOS
Windows
Windows Defender ATP

Geo-location
Corporate Network

Browser apps
Client apps

Conditions

Employee & Partner Users and Roles

Trusted & Compliant Devices

Physical & Virtual Location

Client apps & Auth Method

171TB

Machine learning

Session Risk

3

Real time Evaluation Engine

Policies

Effective policy

Controls

Allow/block access

Limited access

Require MFA

Force password reset

******

Block legacy authentication

Microsoft Cloud

Microsoft Cloud App Security

Cloud SaaS apps

On-premises & web apps

VI. Integrate threat signals from other security solutions to improve detection, protection, and response

- Integrate Microsoft Defender for Identity with Microsoft Defender for Cloud Apps
- Enable Microsoft Defender Endpoint

Securing identity with Zero Trust | Microsoft Docs

Zero Trust User Access

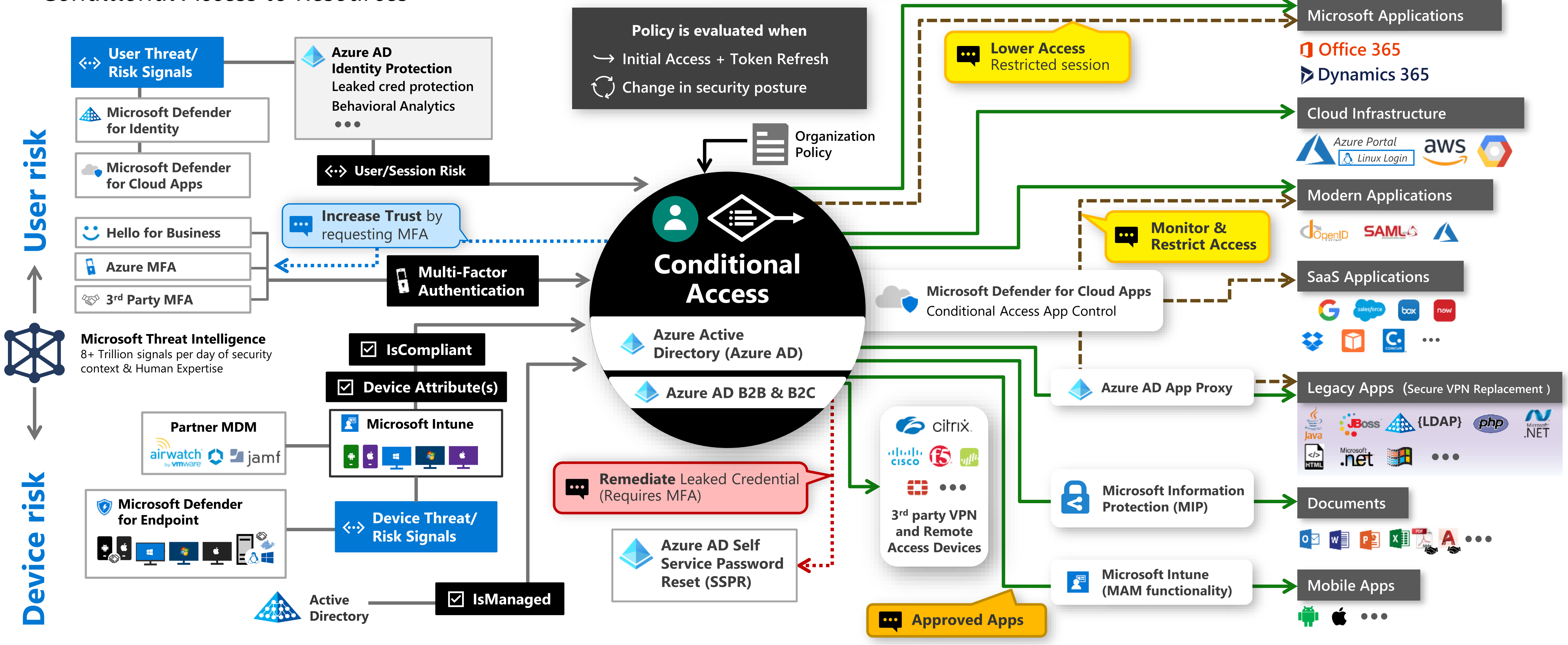
Conditional Access to Resources

Legend

🟩	Full access	▨	Limited access
■ ■ ■	Risk Mitigation	💬	Remediation Path

Microsoft

December 2021 – https://aka.ms/MCRA



User risk

Device risk

User Threat/ Risk Signals

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••

User/Session Risk

Hello for Business

Azure MFA

3rd Party MFA

Increase Trust by requesting MFA

Multi-Factor Authentication

Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise

IsCompliant

Device Attribute(s)

Partner MDM
airwatch by vmware
jamf

Microsoft Intune

Microsoft Defender for Endpoint

Device Threat/ Risk Signals

Active Directory

IsManaged

Policy is evaluated when
Initial Access + Token Refresh
Change in security posture

Organization Policy

Conditional Access

Azure Active Directory (Azure AD)

Azure AD B2B & B2C

Remediate Leaked Credential (Requires MFA)

Azure AD Self Service Password Reset (SSPR)

Lower Access
Restricted session

Monitor & Restrict Access

Microsoft Defender for Cloud Apps
Conditional Access App Control

citrix
cisco
•••
3rd party VPN and Remote Access Devices

Azure AD App Proxy

Microsoft Information Protection (MIP)

Microsoft Intune (MAM functionality)

Approved Apps

Microsoft Applications
Office 365
Dynamics 365

Cloud Infrastructure
Azure Portal
Linux Login
aws

Modern Applications
OpenID
SAML

SaaS Applications
salesforce
box
now
•••

Legacy Apps (Secure VPN Replacement)
Java
JBoss
{LDAP}
php
.NET
HTML
Microsoft .net
•••

Documents
•••

Mobile Apps
•••

Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Microsoft Zero Trust Principles

Guidance for technical architecture

Verify explicitly

Always validate all available data points including

- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

Assume breach

Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

Zero Trust Deployment

Securing **identity** with Zero Trust

Identities, representing people, services, or IoT devices, are the common dominator across today's many networks, endpoints, and applications. In the Zero Trust security model, they function as a powerful, flexible, and granular way to control access to data.

Before an identity attempts to access a resource, organizations must:

- Verify the identity with strong authentication.
- Ensure access is compliant and typical for that identity.
- Follows least privilege access principles.

Once the identity has been verified, we can control that identity's access to resources based on organization policies, on-going risk analysis, and other tools.

When implementing an end-to-end Zero Trust framework for identity, we recommend you focus first on these **initial deployment objectives**:

I. Cloud identity federates with on-premises identity systems.

II. Conditional Access policies gate access and provide remediation activities.

III. Analytics improve visibility.

After these are completed, focus on these **additional deployment objectives:**

IV. Identities and access privileges are managed with identity governance.

V. User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection.

VI. Integrate threat signals from other security solutions to improve detection, protection, and response.

Securing identity with Zero Trust

Zero Trust… is a mindset

→ One of the biggest benefits of Zero Trust is a change in mindset

→ An approach to security which treats every access attempt as if it's originating from an untrusted network

→ An approach to security which assumes pervasive risk

→ How do we behave in an environment of pervasive risk?

Simple to start

1. Integrate with on-premises identity systems.
2. Verify explicitly with Strong Authentication: Enable MFA (no Exceptions) and Block Legacy Authentication
3. Strengthen Credentials: Enable AD Password Protection
4. Enable Self-Service Password Reset

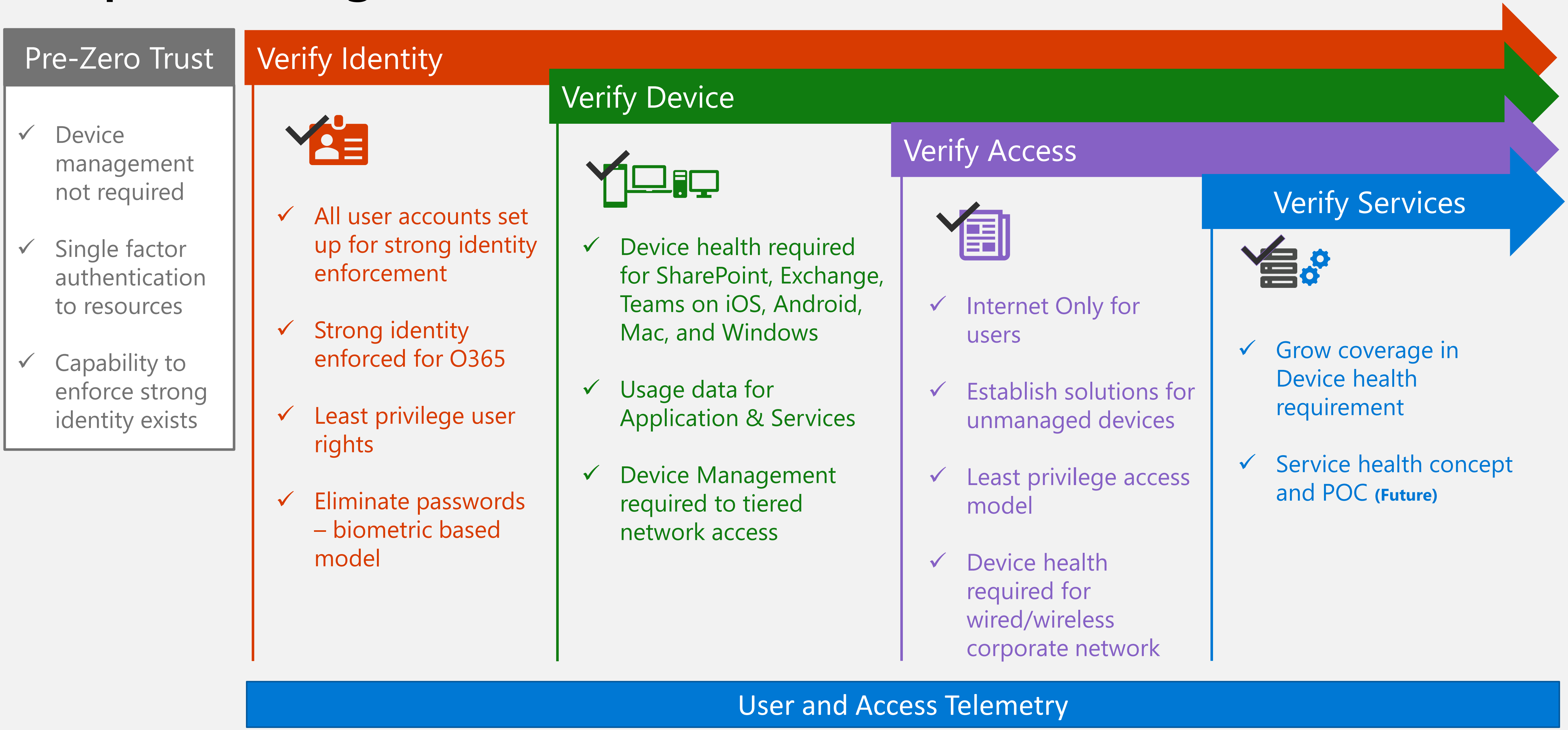
Next:

1. Implement Conditional Access
   - Check Conditional Access for Zero Trust - Azure Architecture Center | Microsoft Learn
2. Register devices with Azure AD and Intune
3. Develop a plan to move your apps to Azure AD
4. Configure your logging and reporting to improve visibility

Zero Trust maturity assessment tool

Check Securing identity with Zero Trust | Microsoft Docs and 10 tips for enabling zero trust security

Implementing Zero Trust at Microsoft



Pre-Zero Trust

- ✓ Device management not required
- ✓ Single factor authentication to resources
- ✓ Capability to enforce strong identity exists

Verify Identity

- ✓ All user accounts set up for strong identity enforcement
- ✓ Strong identity enforced for O365
- ✓ Least privilege user rights
- ✓ Eliminate passwords – biometric based model

Verify Device

- ✓ Device health required for SharePoint, Exchange, Teams on iOS, Android, Mac, and Windows
- ✓ Usage data for Application & Services
- ✓ Device Management required to tiered network access

Verify Access

- ✓ Internet Only for users
- ✓ Establish solutions for unmanaged devices
- ✓ Least privilege access model
- ✓ Device health required for wired/wireless corporate network

Verify Services

- ✓ Grow coverage in Device health requirement
- ✓ Service health concept and POC **(Future)**

User and Access Telemetry

[Implementing a Zero Trust security model at Microsoft]

Resources

Zero Trust web page: aka.ms/Zerotrust

Zero Trust assessment tool: https://aka.ms/ZTTool

Zero Trust App Deployment: aka.ms/ZTforAppsBlog

Zero Trust with on prem apps: aka.ms/ZTforApps

Zero Trust Maturity model paper: aka.ms/Ztmodel

Zero Trust live session: aka.ms/ZTLiveTalk

Zero Trust Guide: aka.ms/ZTGuide

Zero Trust Deployment Plan: aka.ms/ZTDeploymentPlan

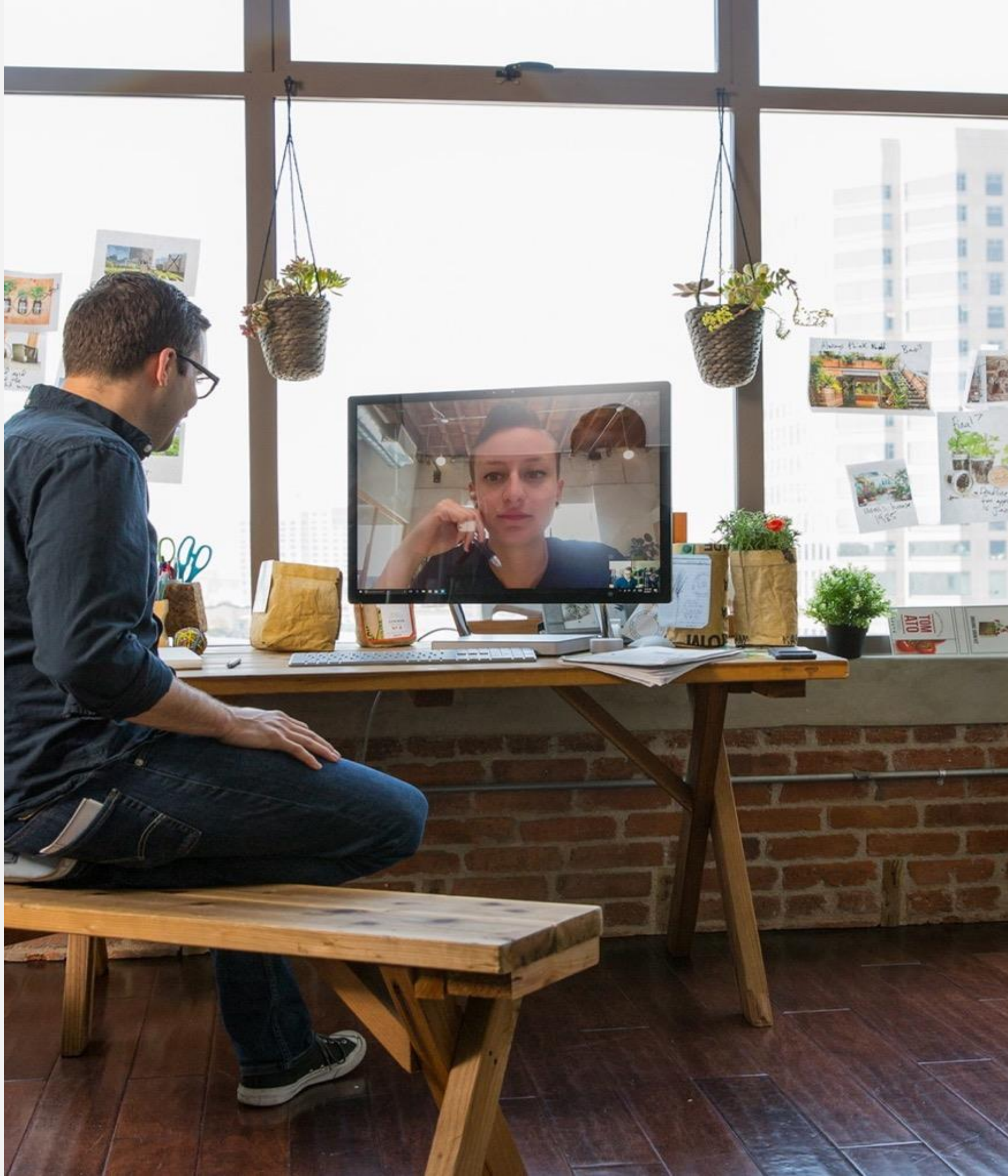
Zero Trust eBook: aka.ms/ZeroTrustEbook

Zero Trust BusinessPlan: aka.ms/ZeroTrustBusinessPlan

Implementing Zero Trust approach with Azure AD Paper: Link

Zero Trust with AAD Learning: Link

Lessons Microsoft learned from applying Zero Trust during COVID-19: Link

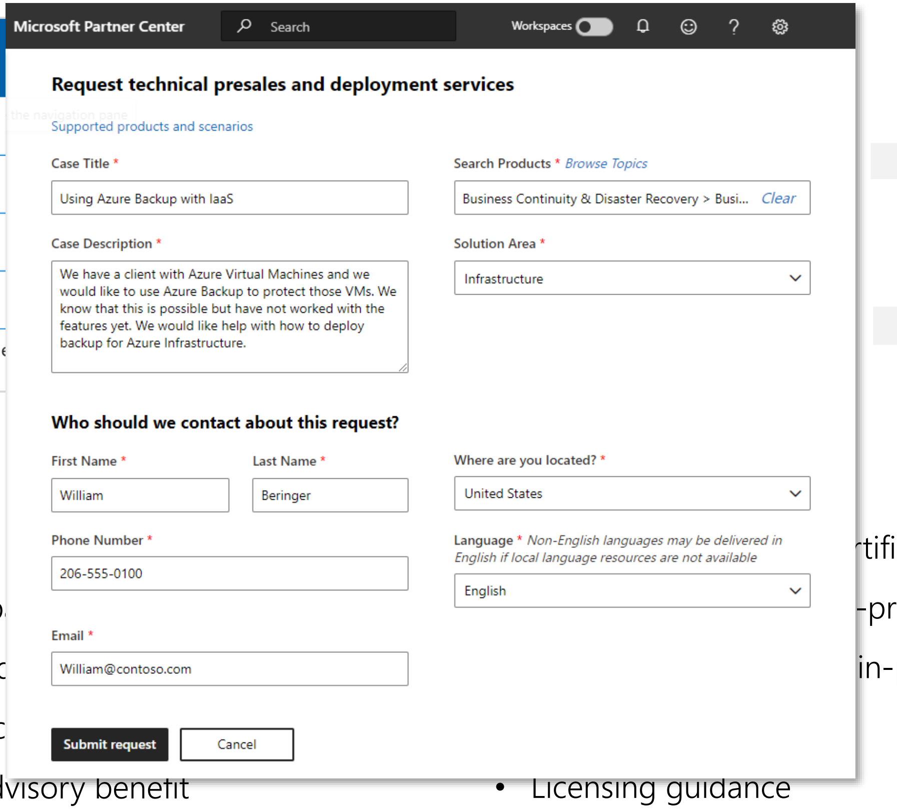


Leverage your Microsoft AI Cloud Partner Program benefits and engage TP&D Services

Technical presales and deployment services to help you deliver services and applications faster.

	Advisory hours
Network Member	Not available
Microsoft Action Pack	5
Solutions Partner	50
Specialization / Expert*	50

*Specialization and Expert MSP designation and TPD benefits shown are the same
Partner designation benefits.



Microsoft Partner Center

Request technical presales and deployment services

Supported products and scenarios

Case Title * : Using Azure Backup with IaaS

Search Products * *Browse Topics* : Business Continuity & Disaster Recovery > Busi... *Clear*

Case Description * : We have a client with Azure Virtual Machines and we would like to use Azure Backup to protect those VMs. We know that this is possible but have not worked with the features yet. We would like help with how to deploy backup for Azure Infrastructure.

Solution Area * : Infrastructure

Who should we contact about this request?

First Name * : William

Last Name * : Beringer

Where are you located? * : United States

Phone Number * : 206-555-0100

Language * *Non-English languages may be delivered in English if local language resources are not available* : English

Email * : William@contoso.com

Data & AI (Azure)

Digital & App Innovation (Azure)

Security

Business Applications

Technical consultations scope:

- Delivered remotely
- Consultation service to help plan, build and grow p
- Provides technical resources, recommendations and
- Focuses on common partner questions and technic
- Packaged as a Microsoft Cloud Partner Program advisory benefit

tification / approval of a proposed partner solution

-production deployment assistance

in-production or technical issues

- Licensing guidance

Visit http://aka.ms/tpd and select ‘Create a new TPD request’ towards the top of the page, or log into your Partner Center dashboard and select the Benefits tile > Technical benefits.

Microsoft

Thank You!