Microsoft

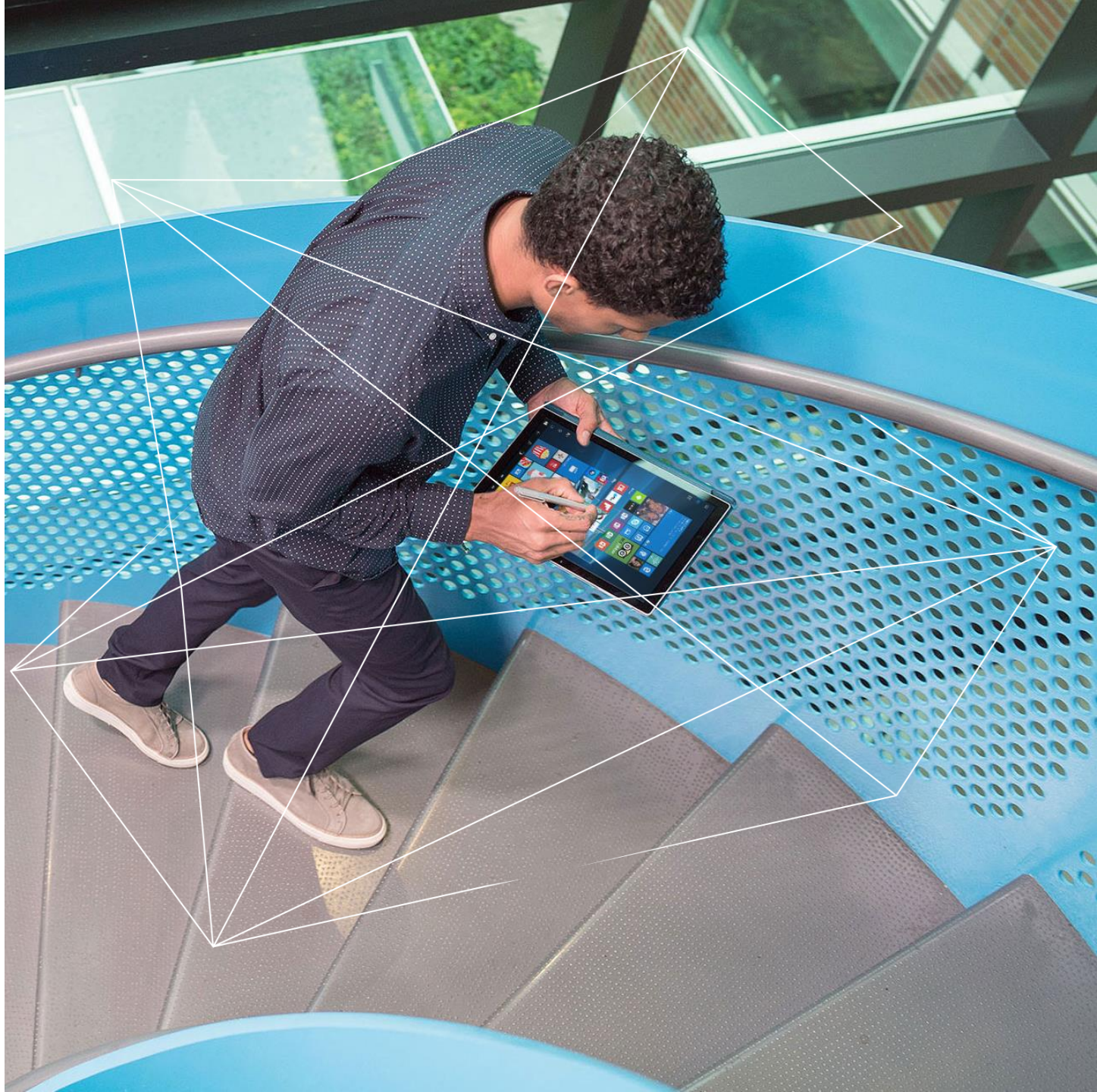
Security in Microsoft Cloud – what can we do today?

Damir Dizdarević
Logosoft d.o.o. Sarajevo
ddamir@logosoft.ba

MVP Microsoft® Most Valuable Professional

Microsoft® Regional Director

#ntk18



The mobile/cloud productivity challenge

User expectations

Collaborate and share with partners

Easy access to familiar apps

Work easily from anywhere on any device

IT challenges

Secure access to company resources

Protect company data and resources

Do more with limited resources

How to empower users to be productive, while protecting the massive amounts of data flowing through your mobile and cloud ecosystem?

Some common questions from cloud aware users

How do I gain visibility into cloud apps used in my organization and get a risk assessment?

How can I control and limit access to data in cloud apps?

How can I prevent data loss in cloud apps and stay compliant with regulations?

How do I protect cloud apps and the data in them from security attacks?

SaaS adoption challenge

73%

of enterprises indicated security as a top challenge holding back SaaS adoption*

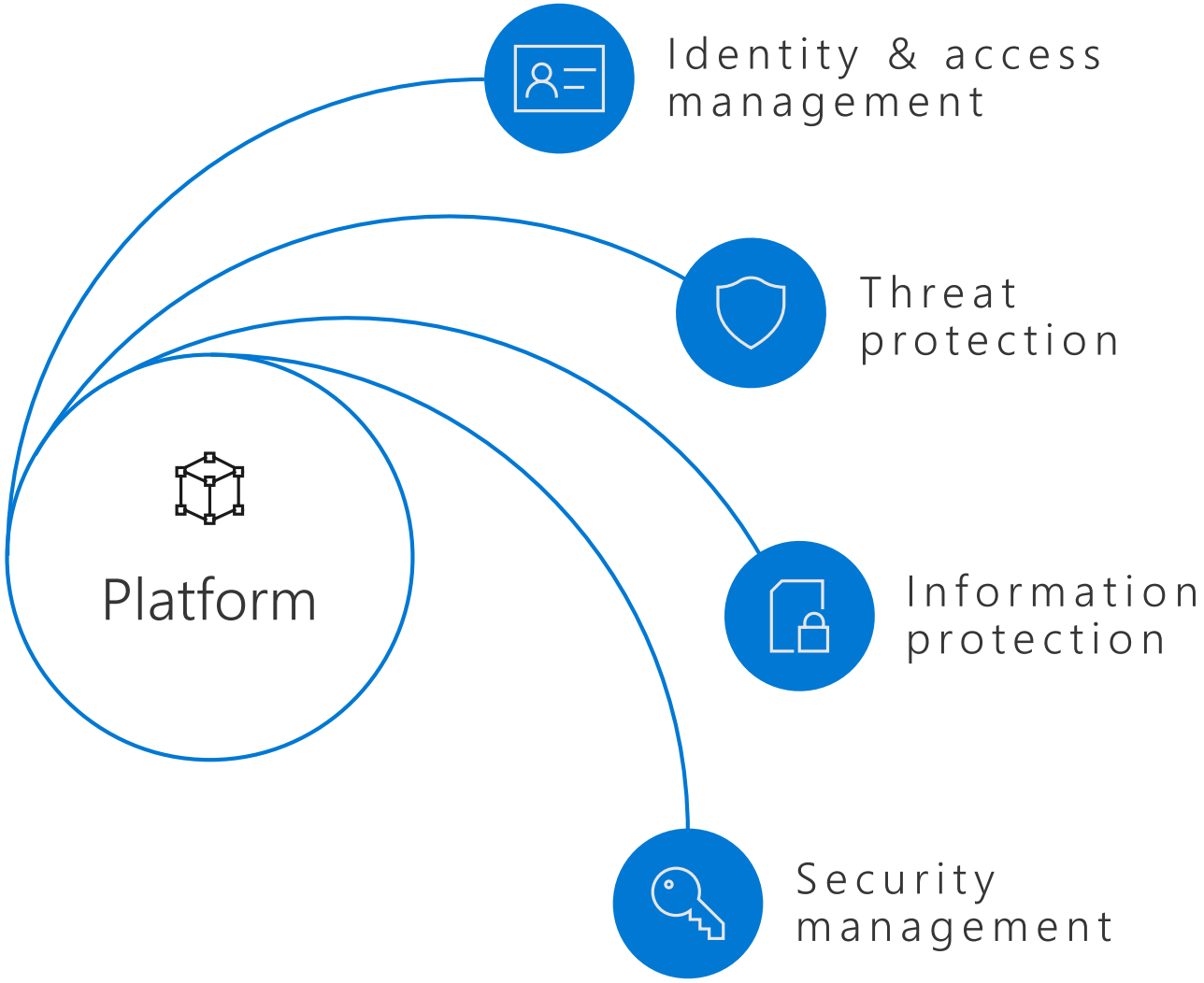
80%

>80% of employees admit to using non-approved SaaS apps in their jobs**

- Cloud Security Alliance (CSA) survey, Cloud Adoption, Practices and Priorities Survey Report 2015

** http://www.computing.co.uk/ctg/news/2321750/more-than-80-per-cent-of-employees-use-non-approved-saas-apps-report

BUILT IN
SECURITY



Microsoft Platform Security

Identity & access management

Protect users' identities & control access to valuable resources based on user risk level

- Azure Active Directory
- Conditional Access
- Windows Hello
- Windows Credential Guard

Threat protection

Protect against advanced threats and recover quickly when attacked

- Advanced Threat Analytics
- Windows Defender Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Office 365 Threat Intelligence

Information protection

Ensure documents and emails are seen only by authorized people

- Azure Information Protection
- Office 365 Data Loss Prevention
- Windows Information Protection
- Microsoft Cloud App Security
- Office 365 Advanced Security Mgmt.
- Microsoft Intune

Security management

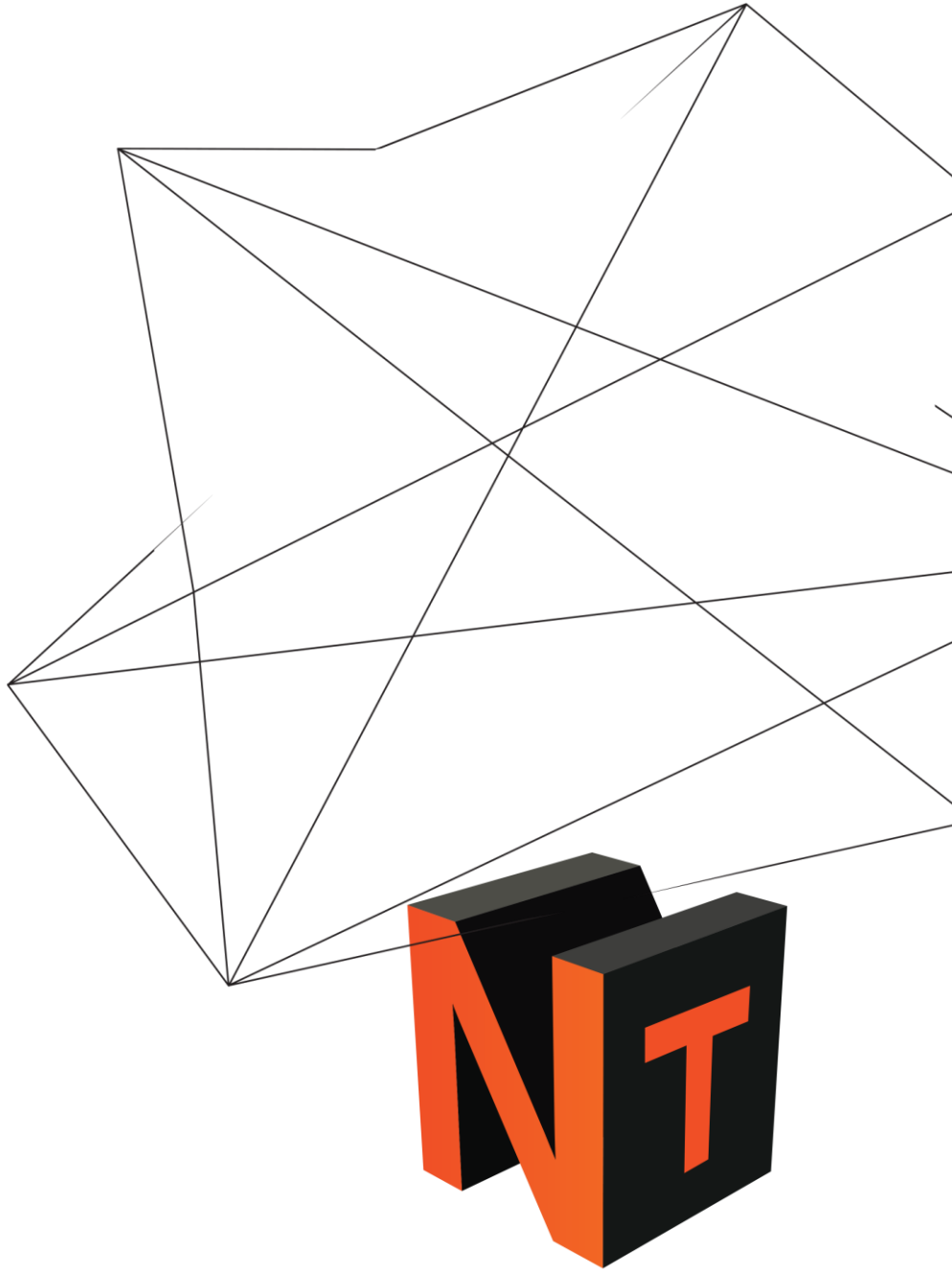
Gain visibility and control over security tools

- Azure Security Center
- Office 365 Security Center
- Windows Defender Security Center

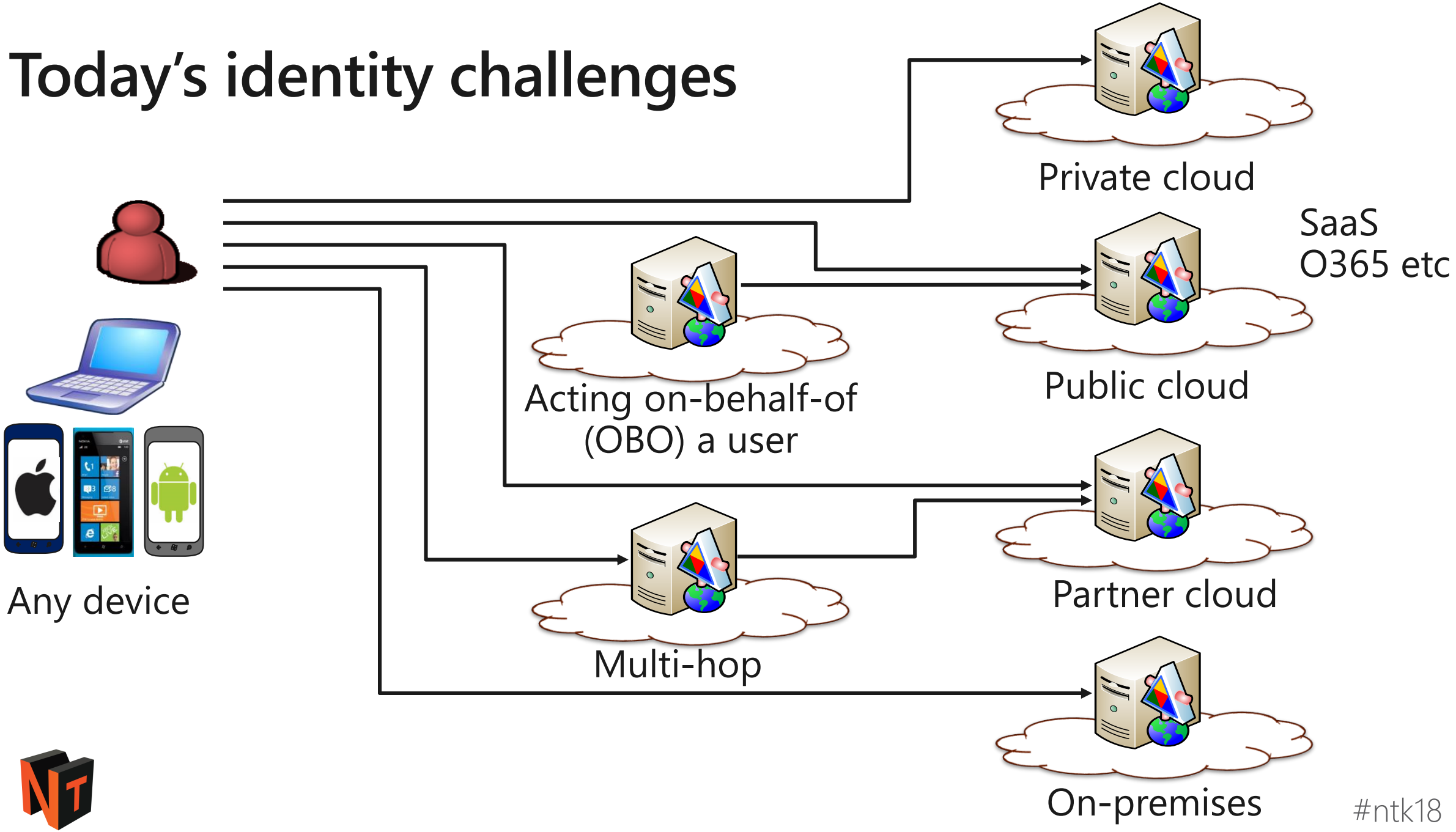
Key pillars of today's security

- Protecting identities
- Protecting data
- Protecting infrastructure and devices

Protecting identities

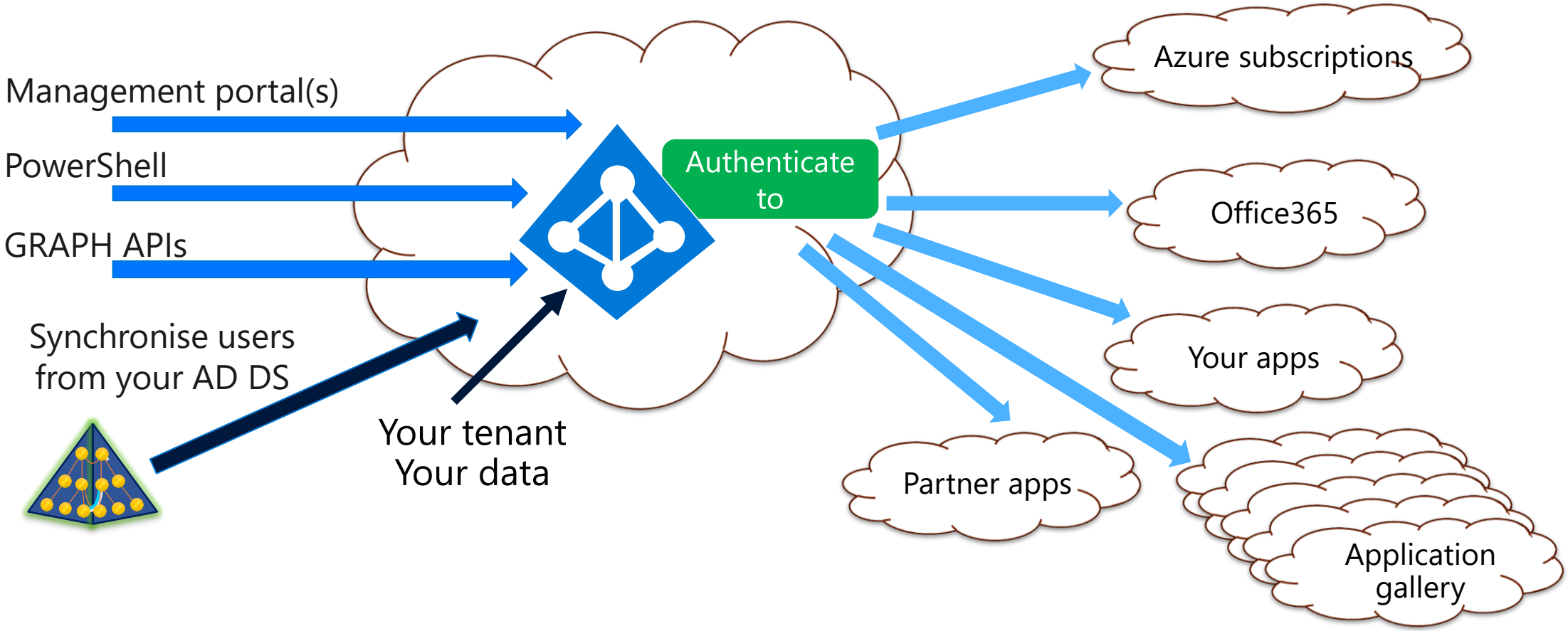


Today's identity challenges



Microsoft Azure AD

- Users signed-in to Azure AD have SSO to all applications



Azure Active Directory capabilities

- *Challenges arise when capabilities are not understood*

- Connect Health
- Cloud App Discovery
- Self-Service Password Reset
- Multifactor authentication (MFA)
- Identity Protection
- Privileged Identity & Access Management
- Security & activity reports

Azure Multi-Factor Authentication

- Strong and secure authentication for on-premises, hybrid & the cloud
  - Available as Azure MFA service and Azure MFA Server (on-premises)
  - App Passwords for users are needed for some non-browser apps that do not support MFA
  - Always enable MFA for admins, preferrably also for users with conditional access
    - Whitelist known and trusted IP address spaces to bypass MFA

Conditional Access

Azure AD Identity Protection Service

Windows Defender
Lookout
Skycure

Policy Conditions

User
- User identity
- Group membership
- Session Risk

Device
- OS Platform
- Is Compliant / Domain joined
- Is lost or stolen
- Device Risk

App
- Mobile or Cloud app
- Per app policy

Location
- IP range
- Country / Region

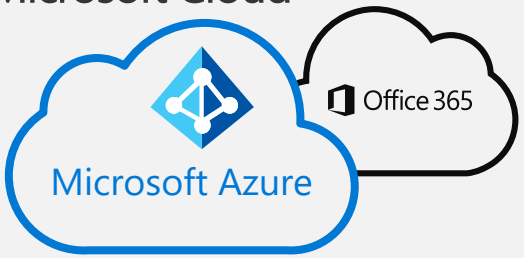
Policy Controls

Access Control
- Allow sign-in
- Block sign-in
- Enforce MFA
- Terms of Use
- Partners

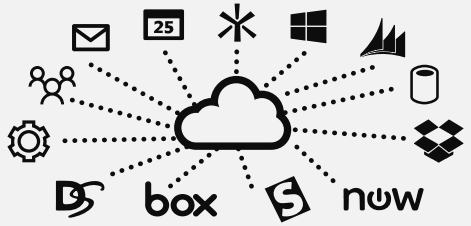
Session Restrictions
- Restrict download
- Disable print
- Prevent data leak

Applications

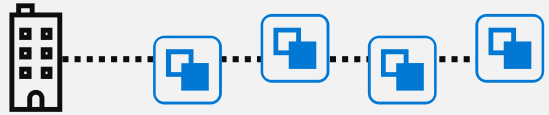
Microsoft Cloud



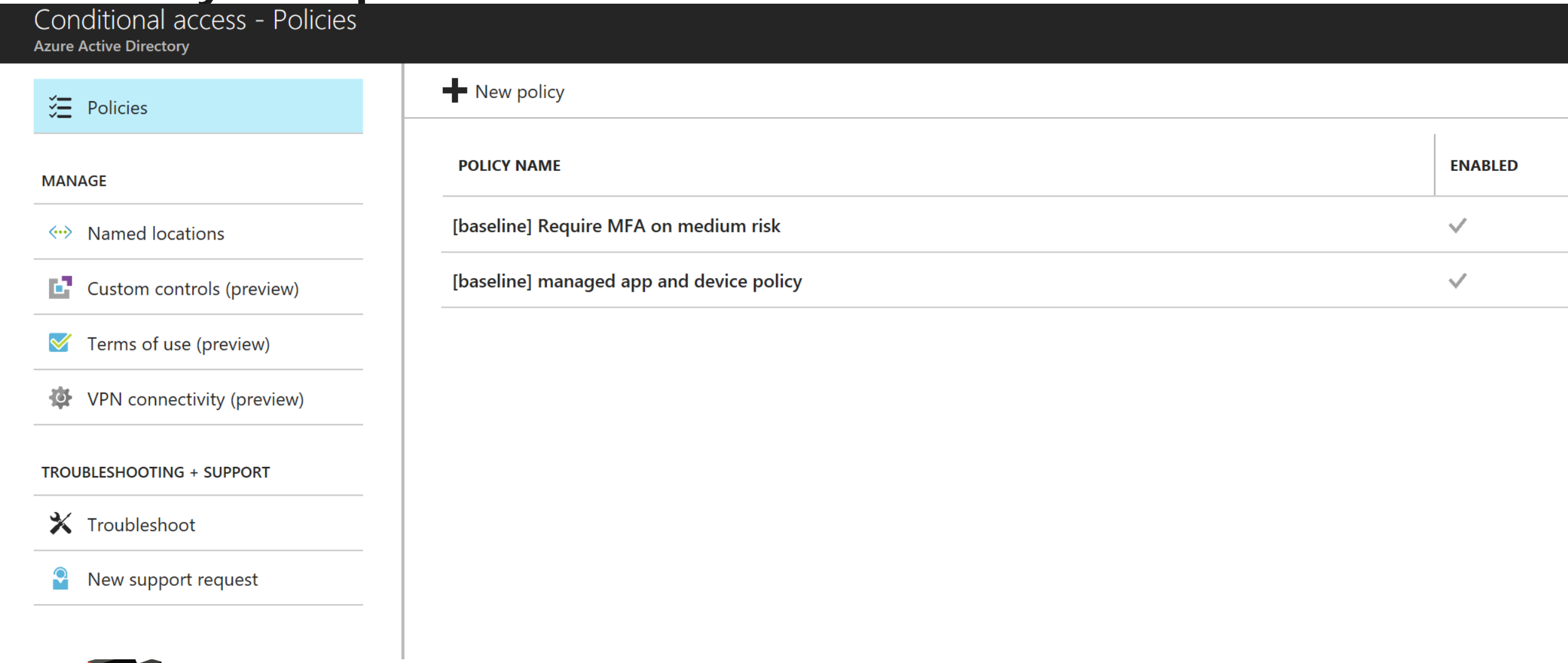
3rd Party SaaS Apps



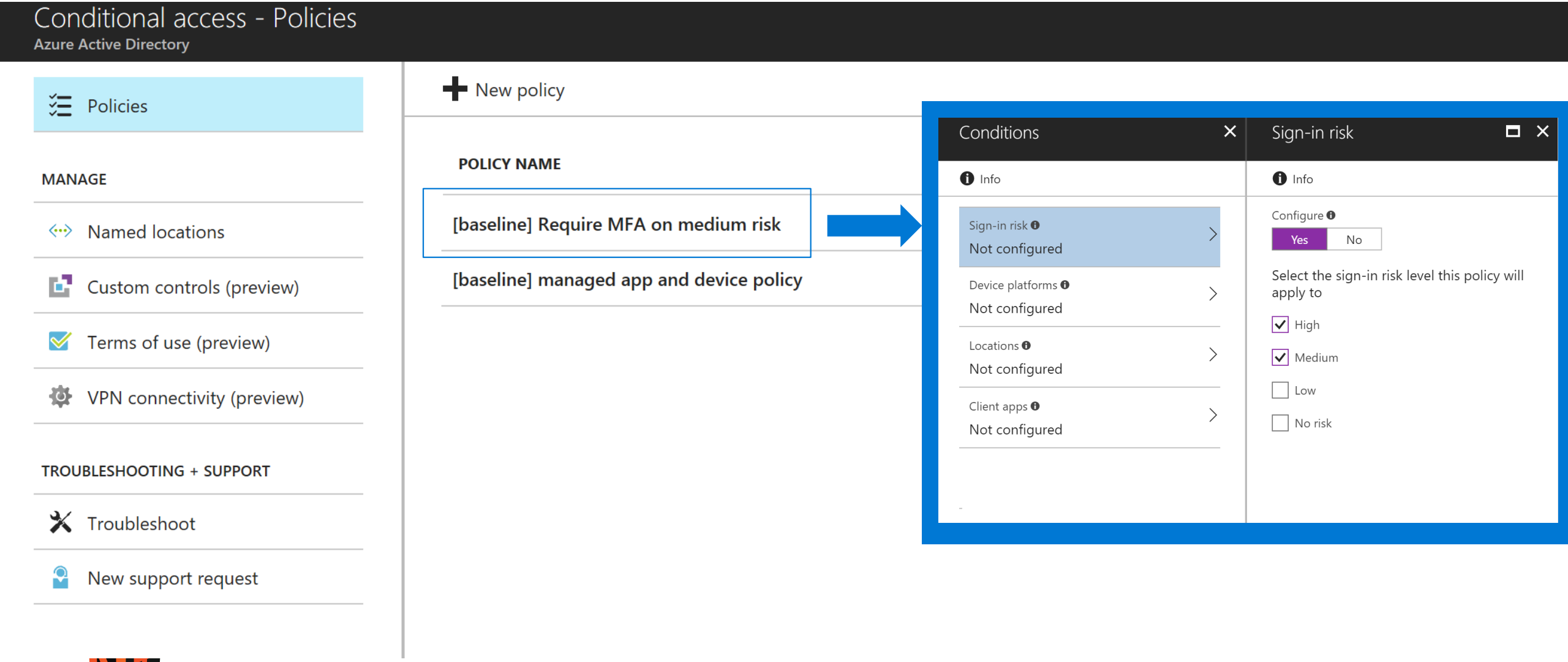
On Premises Apps



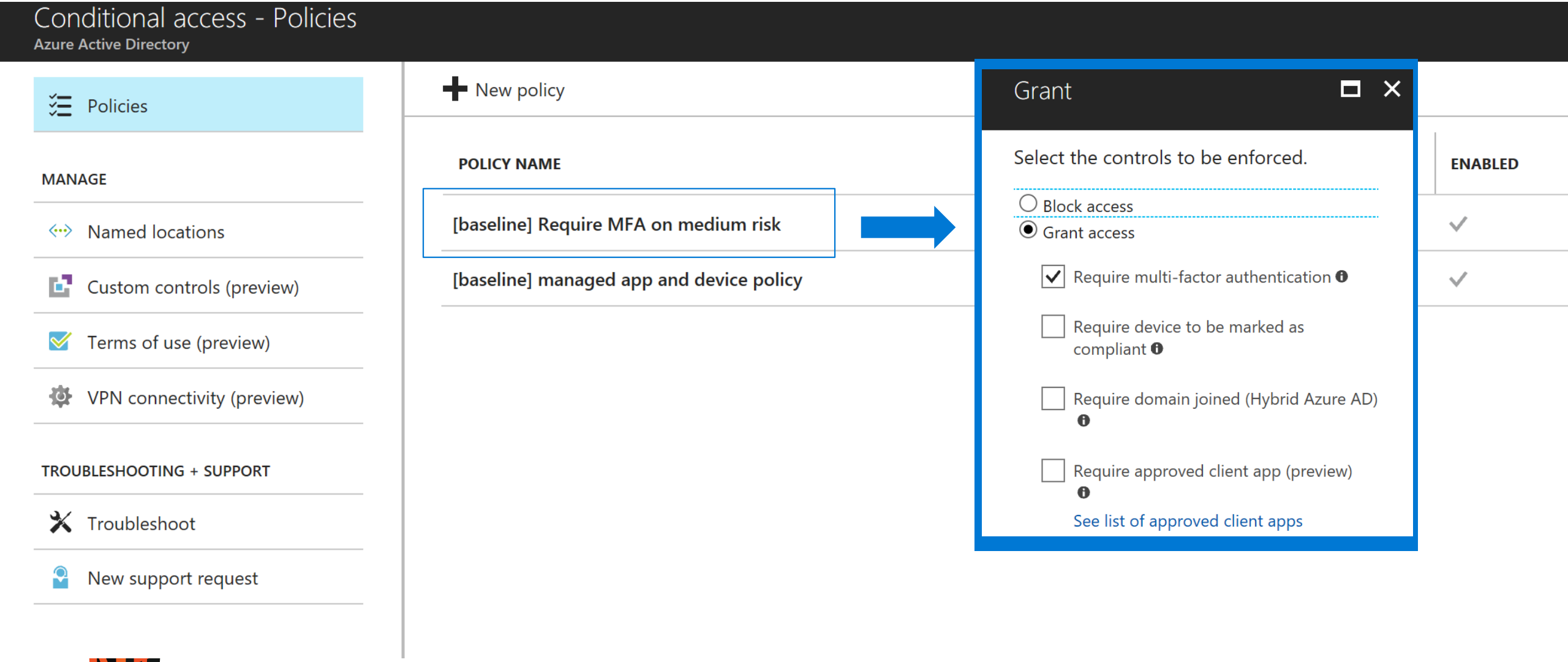
Policy composition



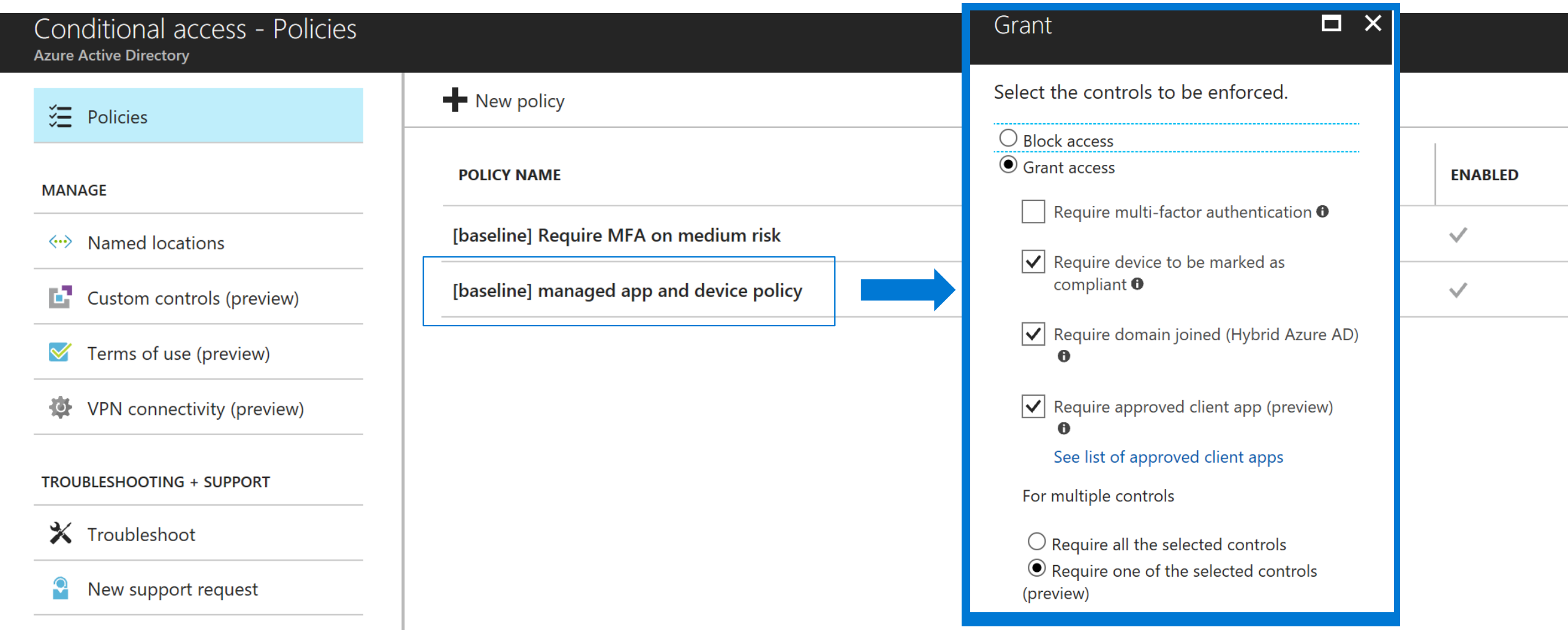
Policy composition



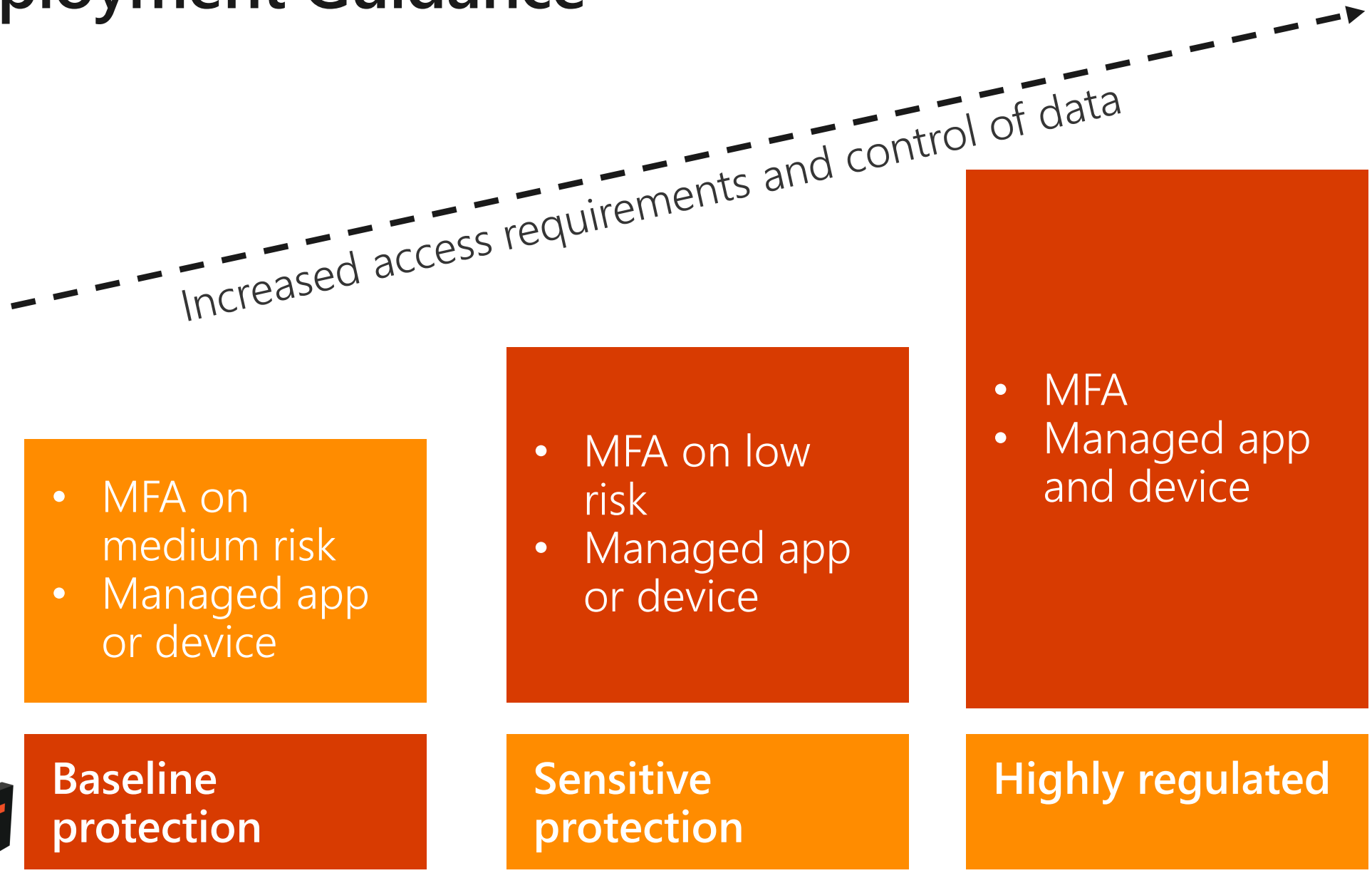
Policy composition



Policy composition

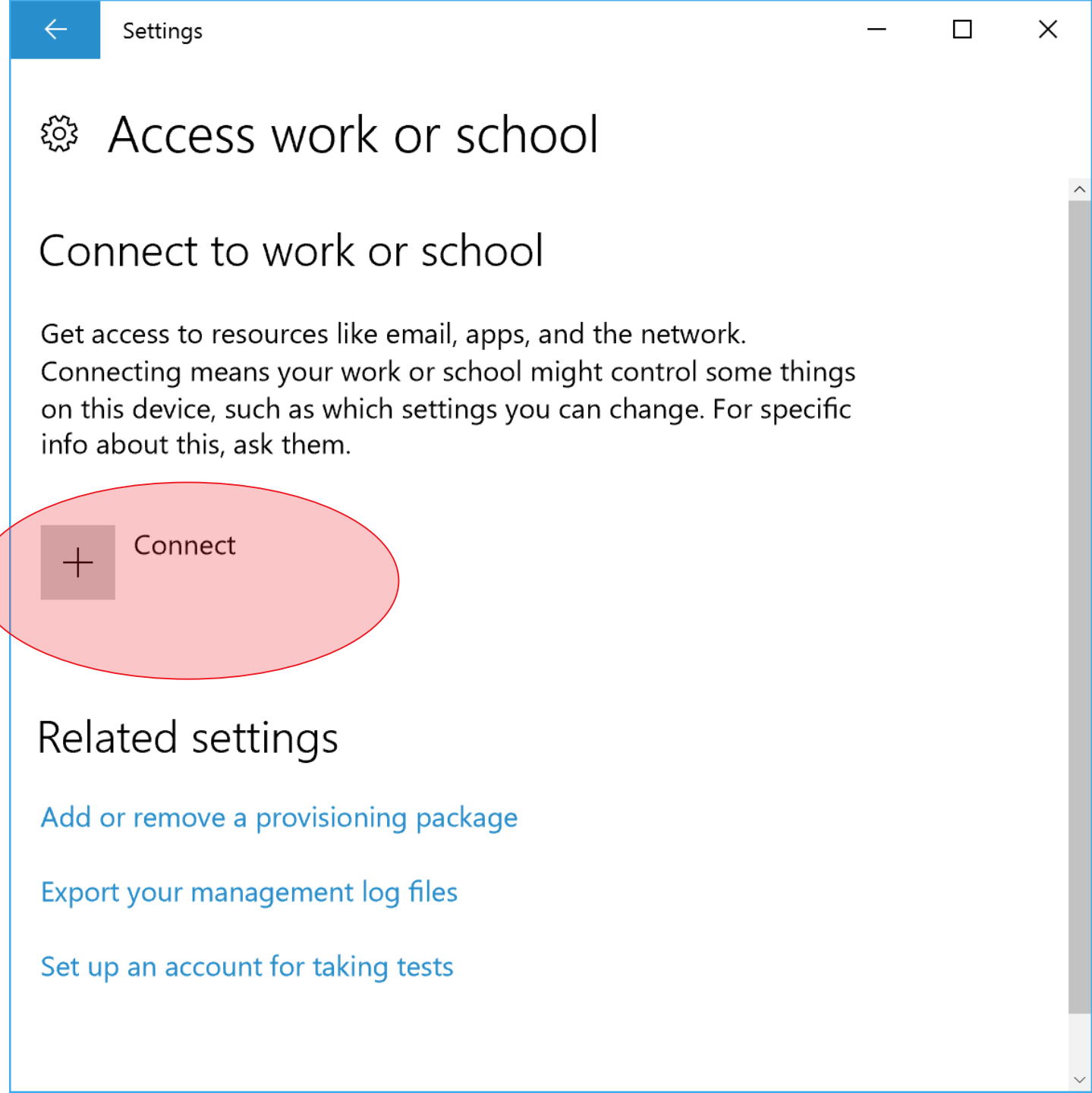


Deployment Guidance



Azure AD Join

- Integration with O365
- SSO with Edge or office apps
- OneDrive access

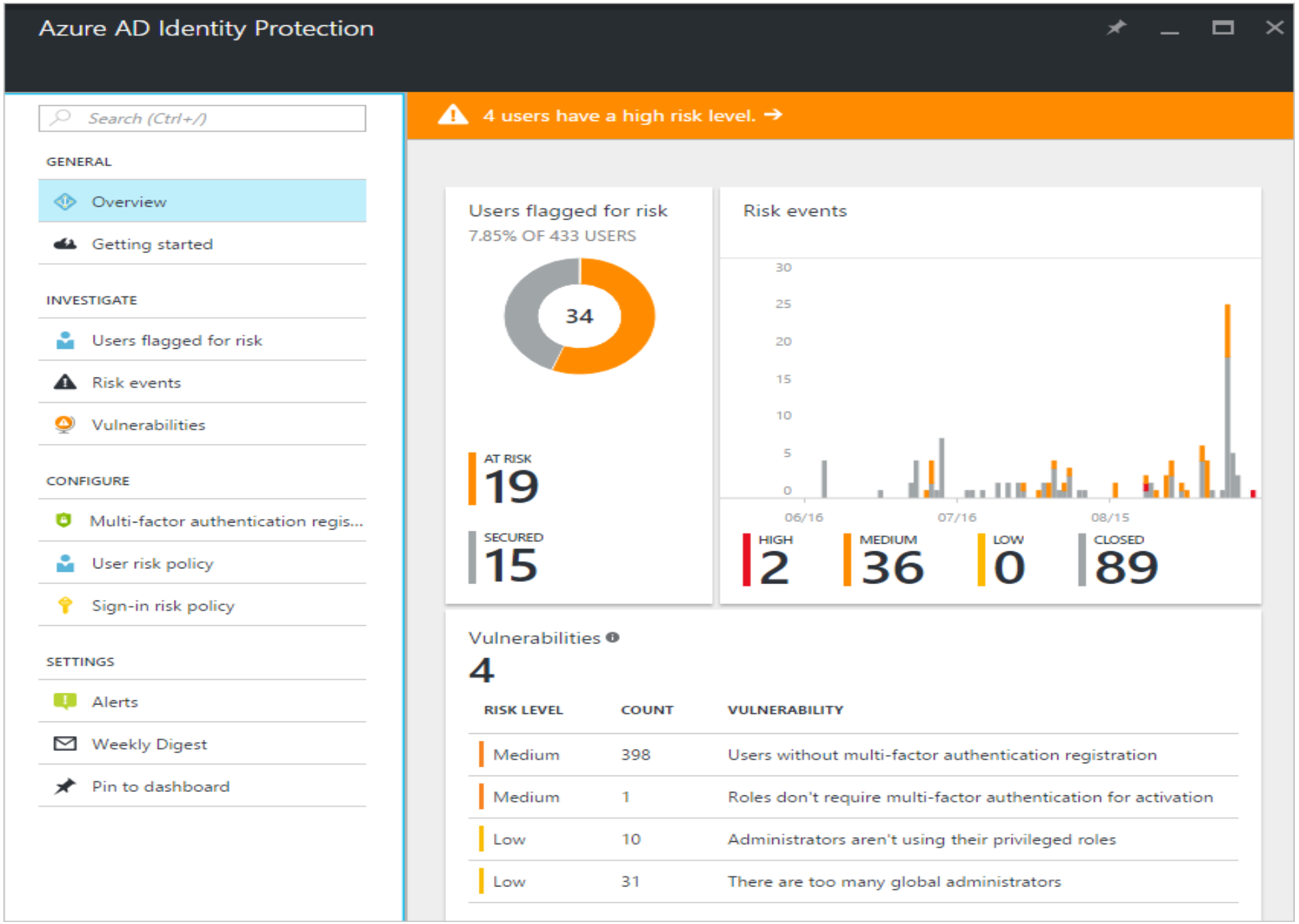


Windows Hello for Business

- User authentication to an AAD account
- PIN, biometric or gesture is verified locally with TPM
- The TPM holds the private key that never leaves the device.
- AAD holds the public key and verifies identity against the device held private key.

No passwords = more secure

Azure AD Identity Protection

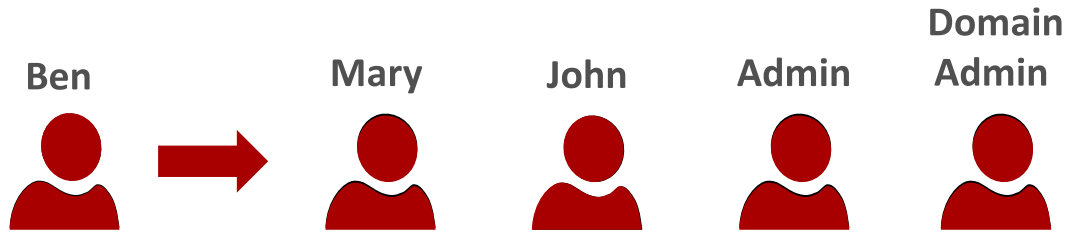


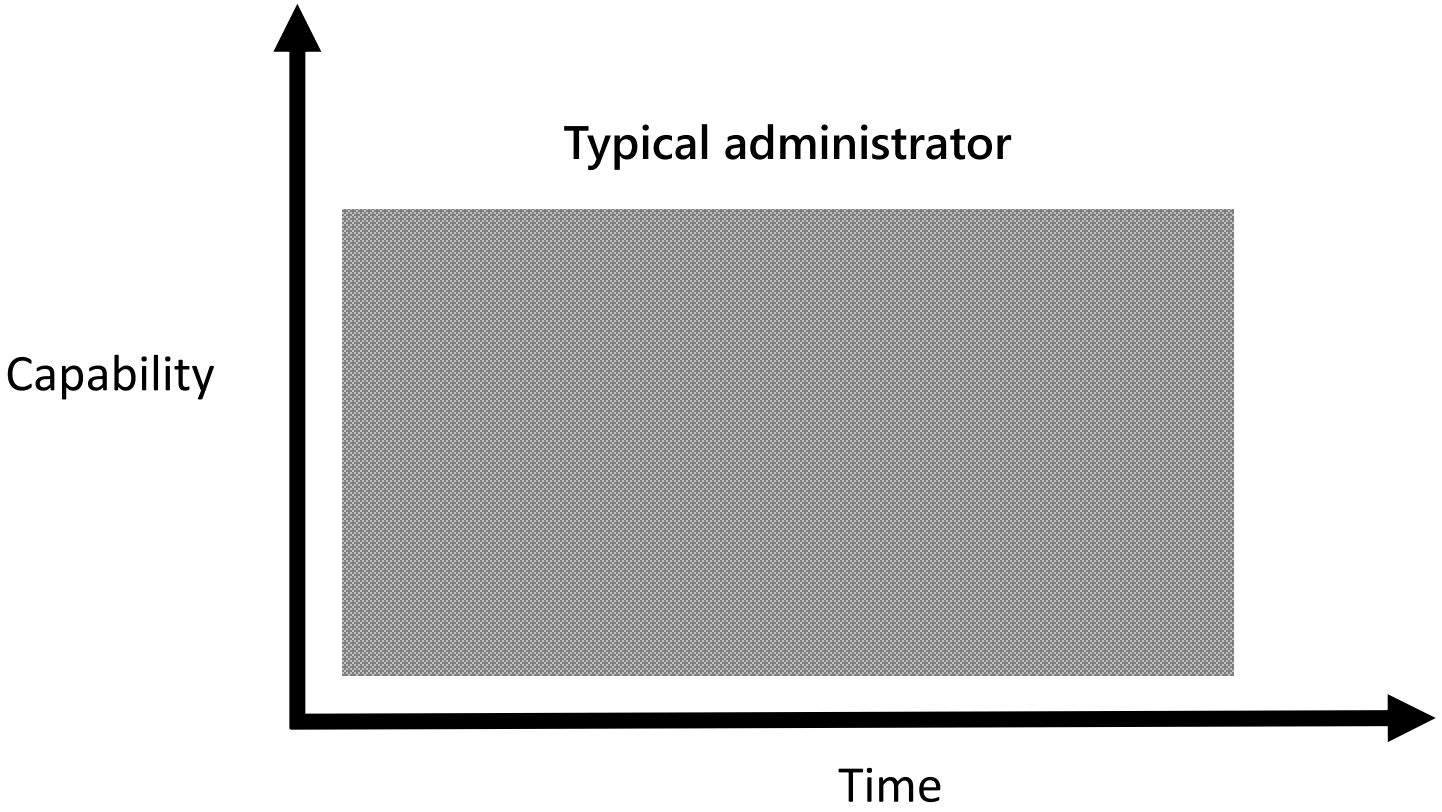
Challenges in protecting privileged identites

Social engineering leads to credential theft

Most attacks involve gathering credentials (PtH)

Administrative credentials typically provide unnecessary extra rights for unlimited time





Azure AD approach

Credential Guard

Prevents **Pass the Hash** and **Pass the Ticket** attacks by protecting stored credentials through Virtualization based Security

Just Enough Administration

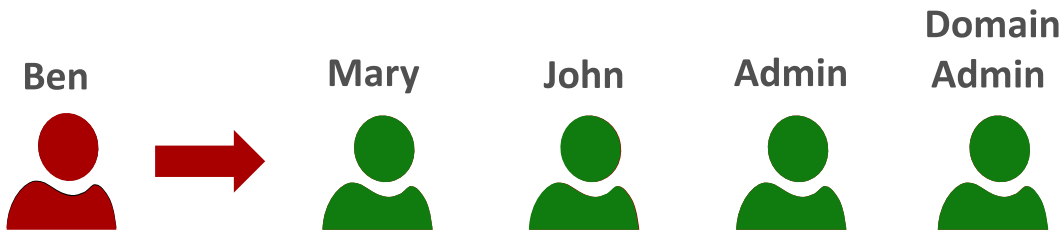
Limits administrative privileges to the bare-minimum required set of actions (limited in space)

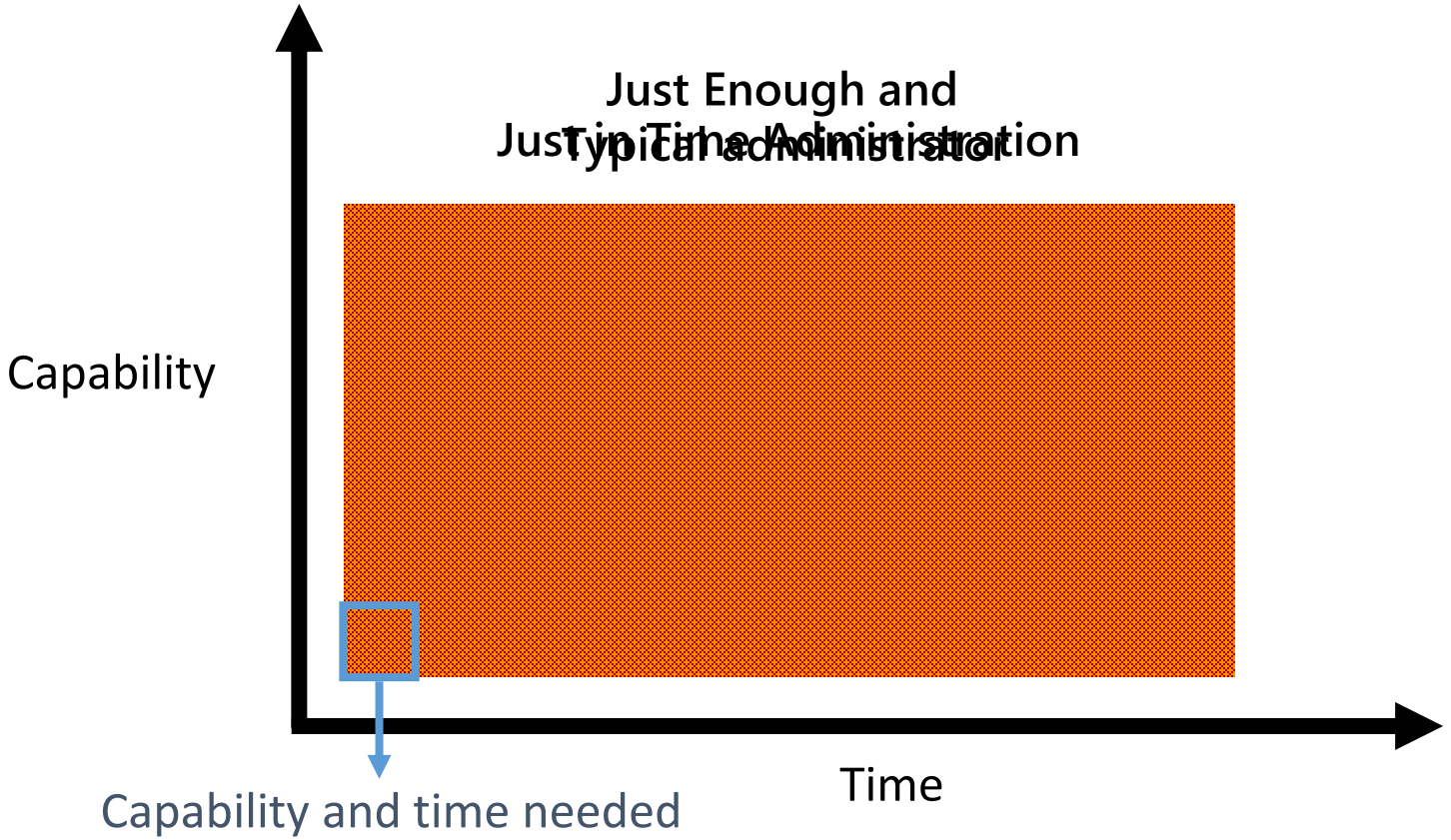
Just in Time Administration

Provide privileged access through a workflow that is audited and limited in time

---

JEA + JIT = limited in time & capability

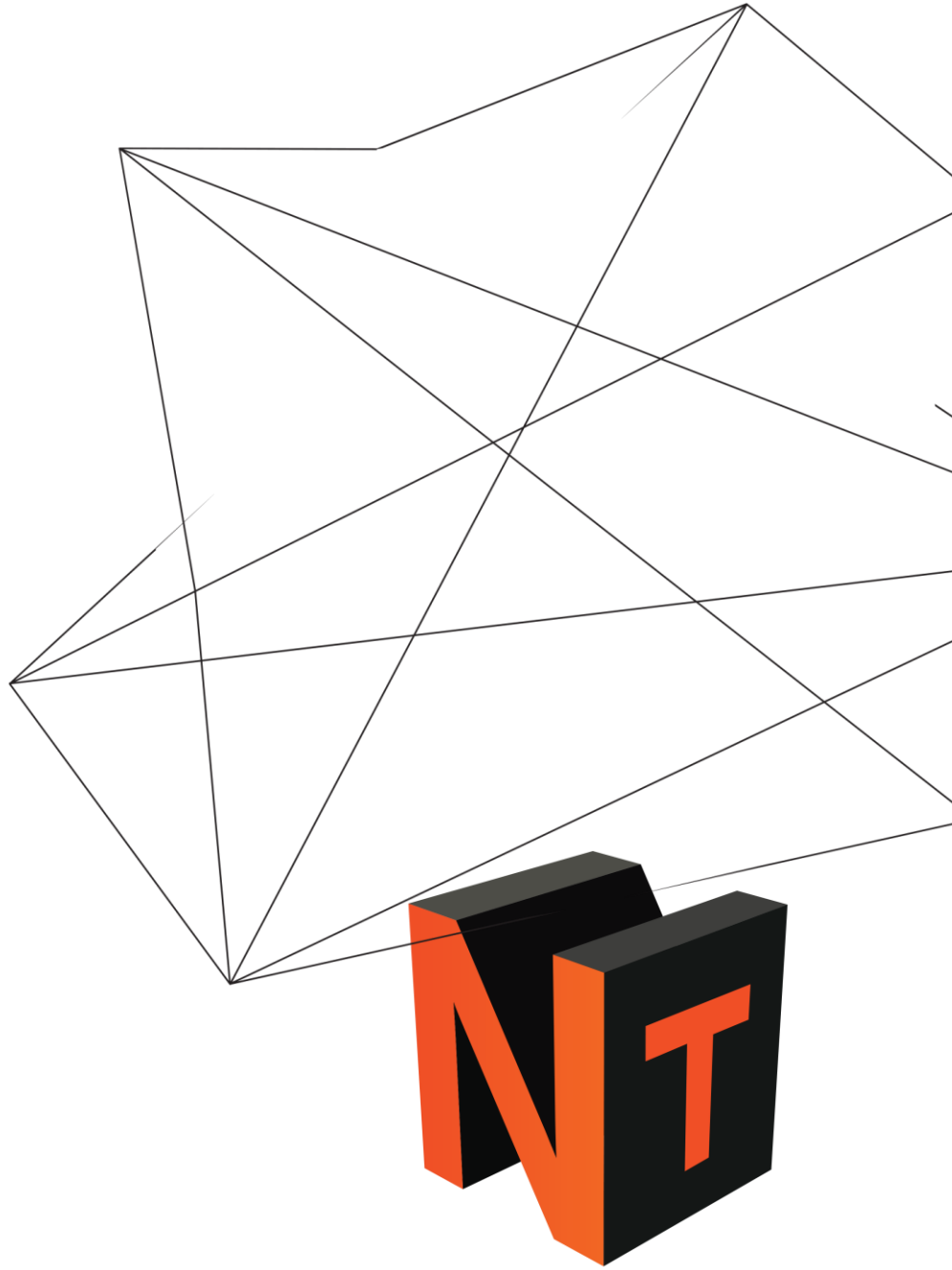




The proposition

Windows devices can be more secure by not being part of a traditional IT infrastructure

Protecting data



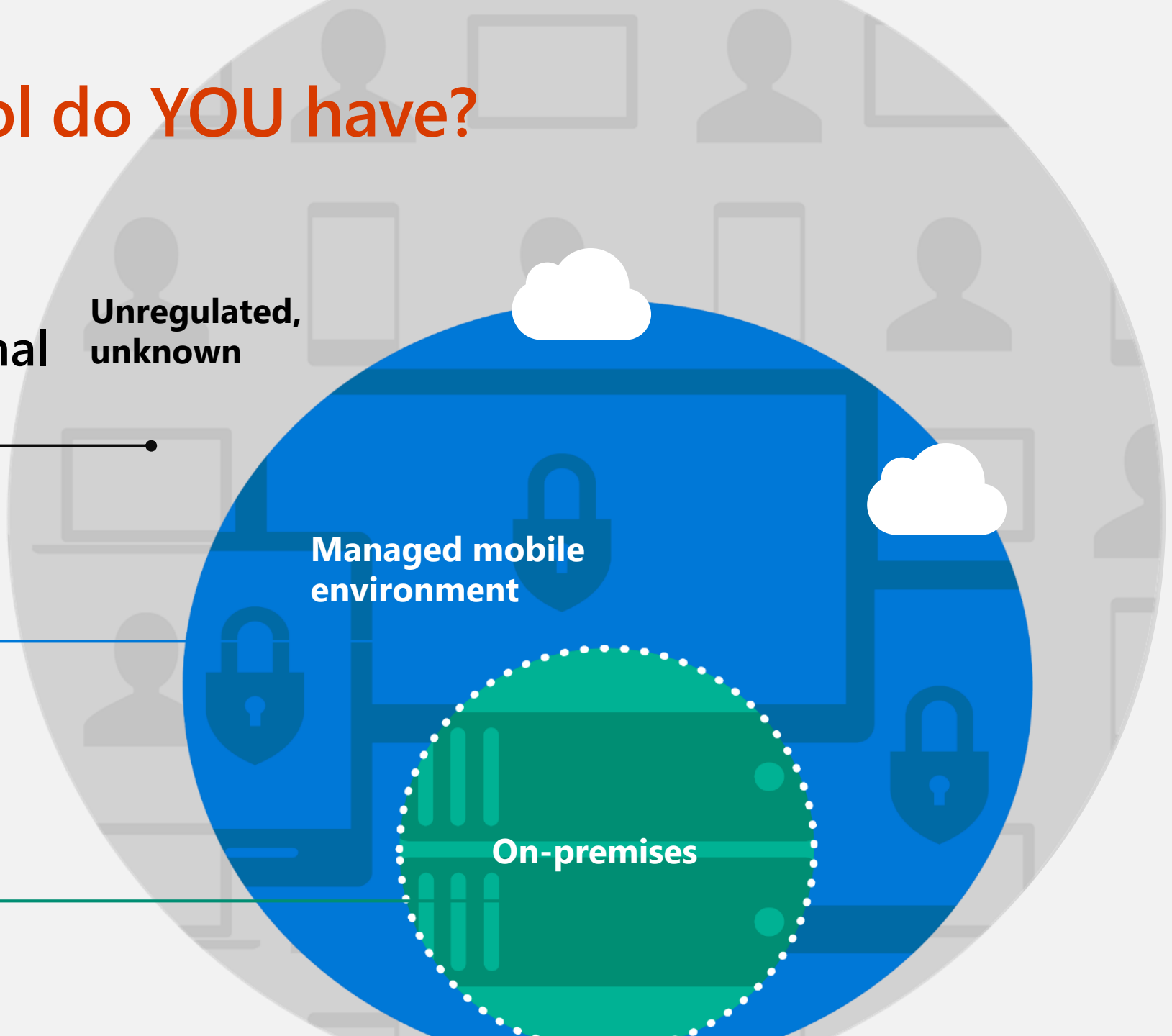
…focus on data leak prevention for personal devices, but ignore the issue on corporate owned devices where the risks are the same or worse – is wrong.

How much control do YOU have?

Hybrid data = new normal
It is harder to protect

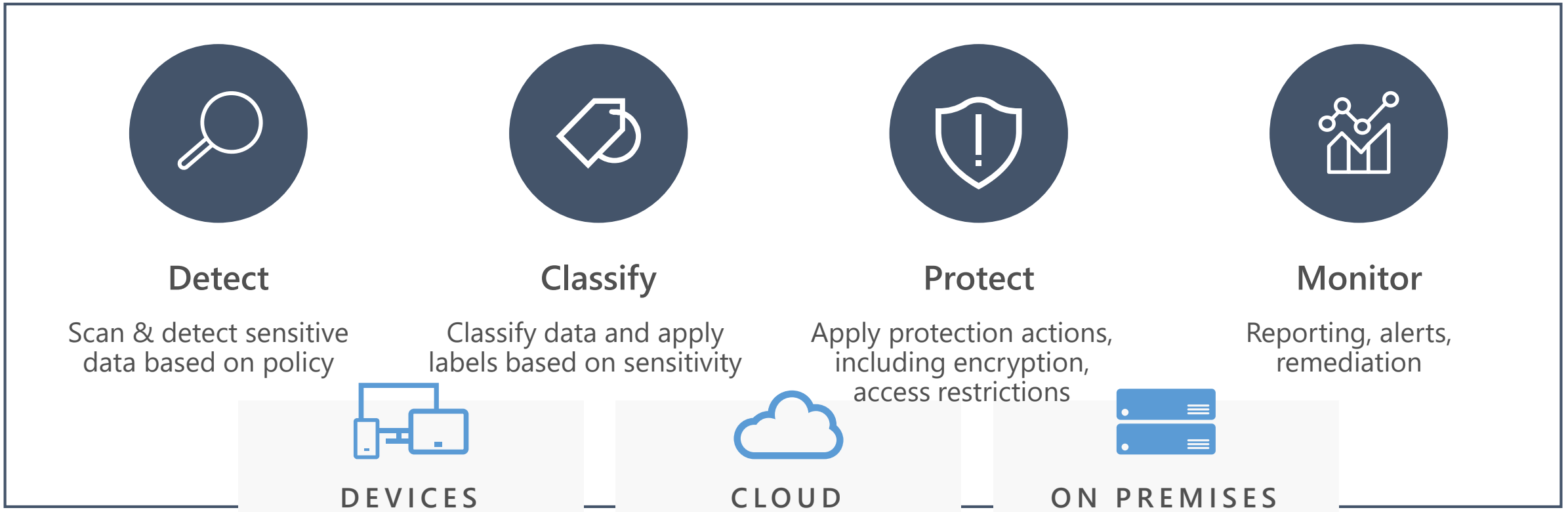
Identity, device management protection

Perimeter protection



MICROSOFT'S APPROACH TO **INFORMATION PROTECTION**

Comprehensive protection of sensitive data throughout the lifecycle – inside and outside the organization



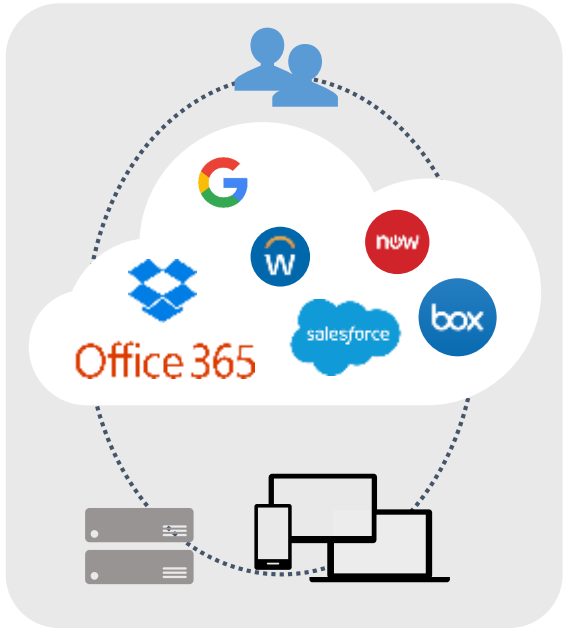
The lifecycle of a sensitive file

Data is created, imported, & modified across various locations

Data is detected
Across devices, cloud services, on-prem environments

Sensitive data is classified & labeled
Based on sensitivity; used for either protection policies or retention policies

Data is protected based on policy
Protection may in the form of encryption, permissions, visual markings, retention, deletion, or a DLP action such as blocking sharing



Data travels across various locations, shared
Protection is persistent, travels with the data

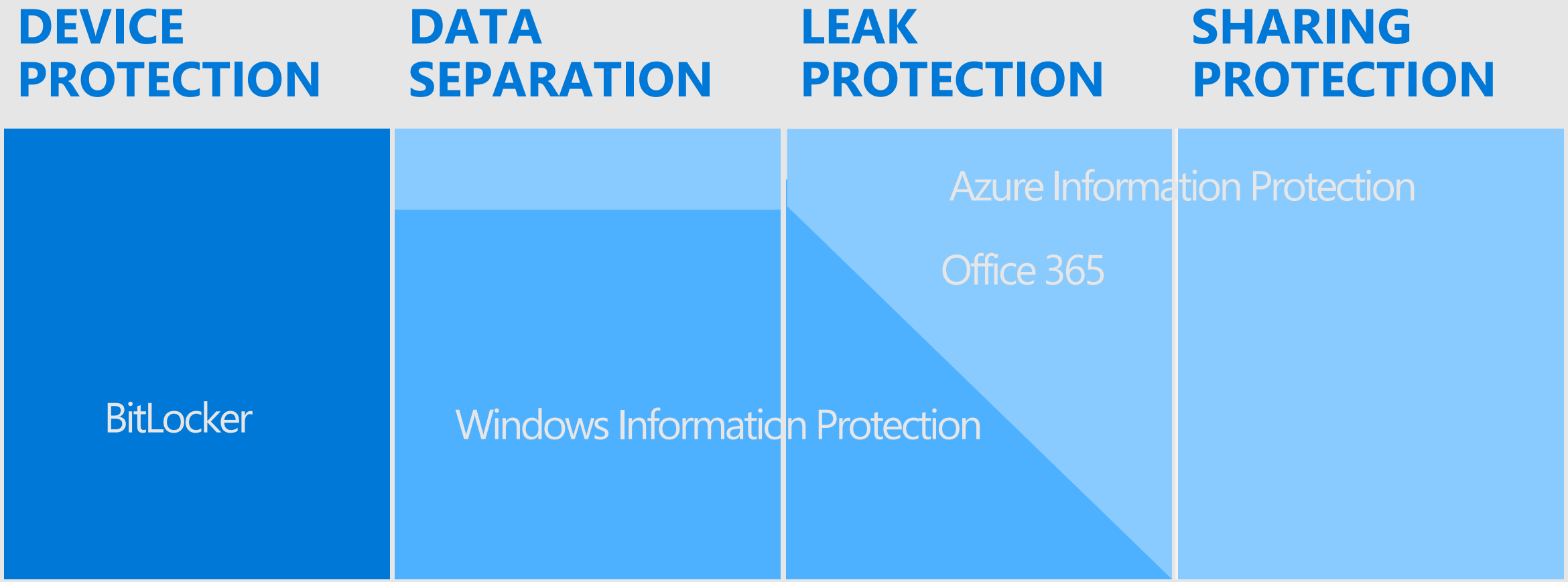
Data is monitored
Reporting on data sharing, usage, potential abuse; take action & remediate

Retain, expire, delete data
Via data governance policies

INFORMATION **PROTECTION NEEDS**

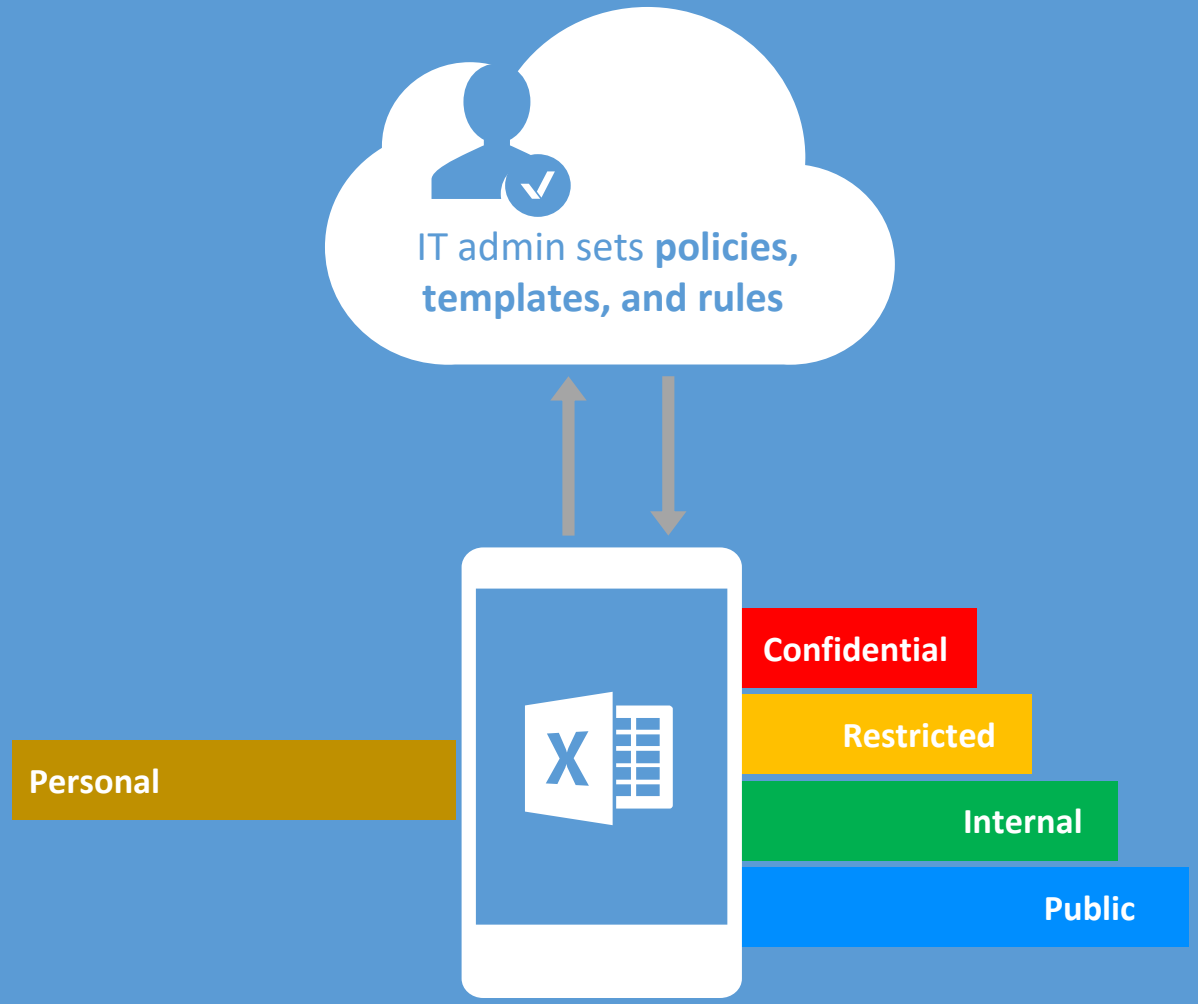
DEVICE PROTECTION	DATA SEPARATION	LEAK PROTECTION	SHARING PROTECTION
Protect system and data when device is lost or stolen	Containment Data separation	Prevent unauthorized users and apps from accessing and leaking data	Protect data when shared with others, or shared outside of organizational devices and control

INFORMATION **PROTECTION NEEDS**



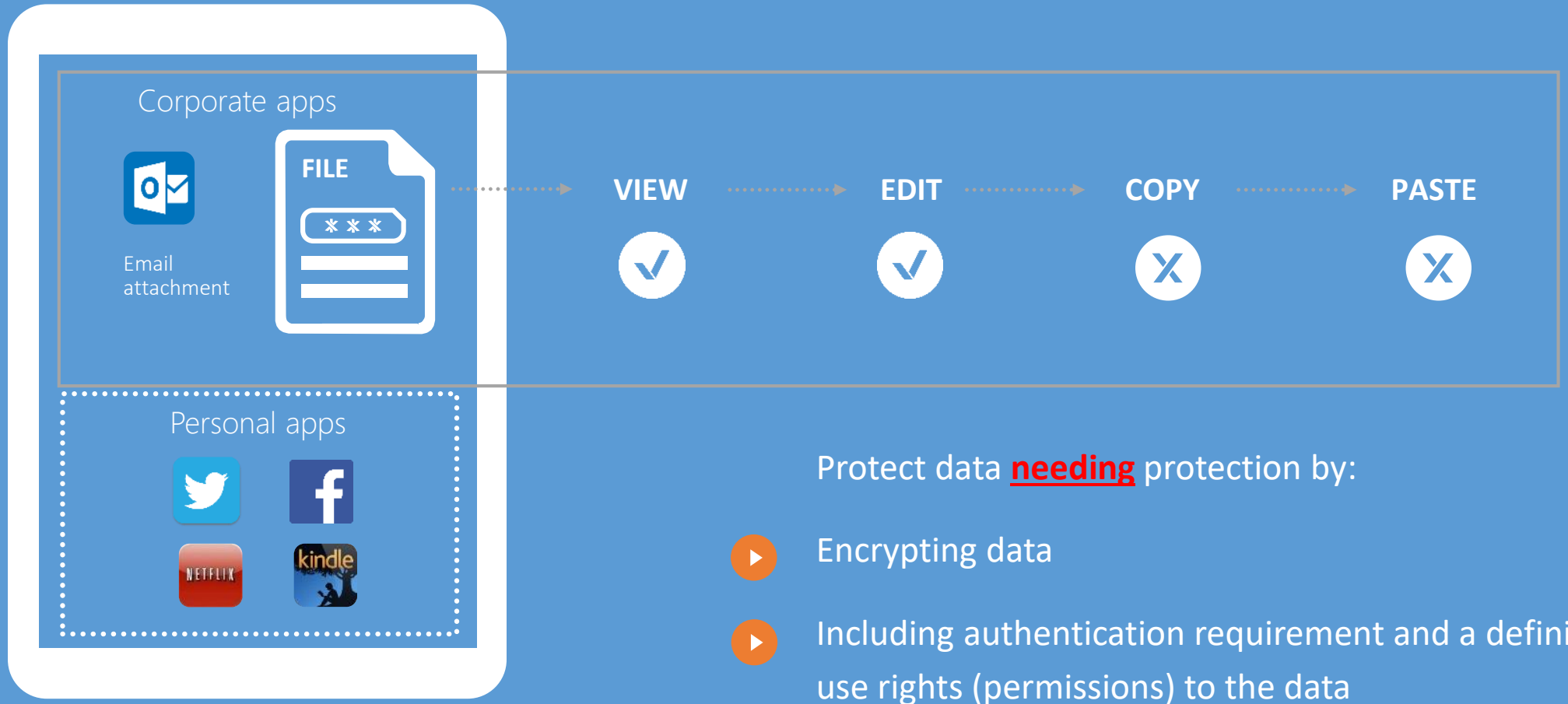
Classify Data – Begin the Journey

Classify data based on sensitivity



- Start with the data that is most sensitive
- IT can set automatic rules; users can complement it
- Associate actions such as visual markings and protection

Protect data against unauthorized use

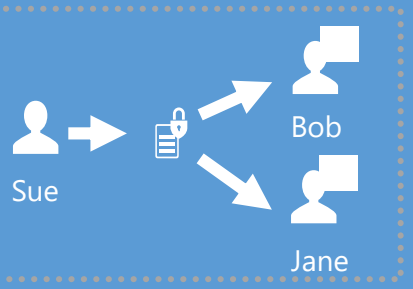


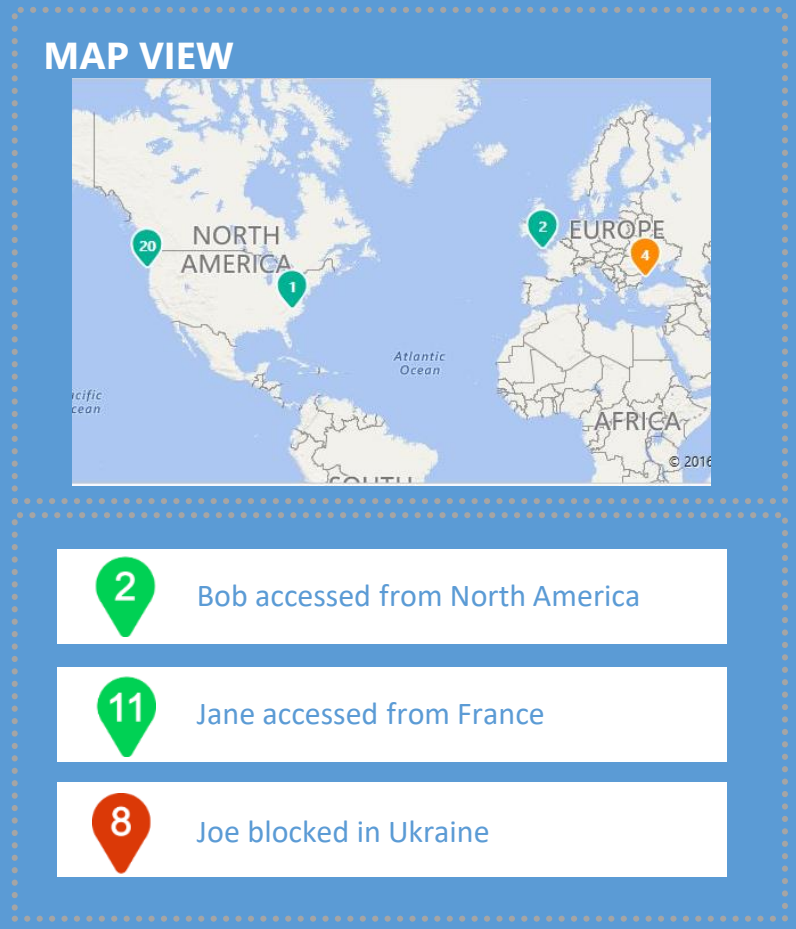
Protect data **needing** protection by:

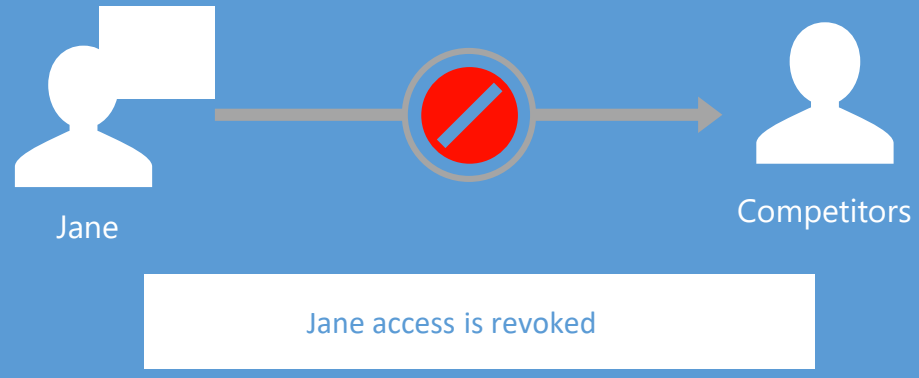
- Encrypting data
- Including authentication requirement and a definition of use rights (permissions) to the data
- Providing protection that is persistent and travels with the data

Monitor and Respond

Monitor use, control and block abuse







Better user experience and integration into Office native clients

Now:

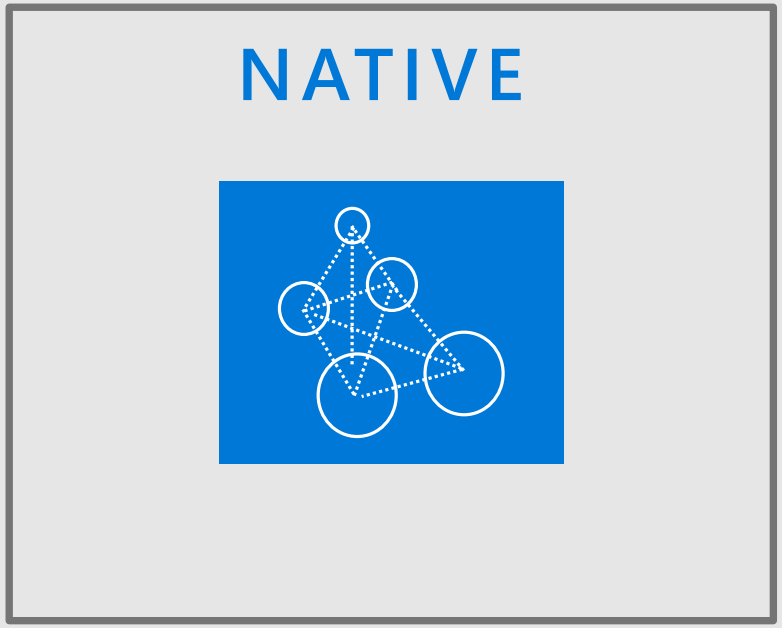
Delightful labeling experience – for everyone!

- Simplified interface for information labeling
- More robust content matching engine

Medium and long term:

Integration into native Office clients:

- Starting with Word, Excel and PowerPoint for Mac
- Full Office for Mac
- Office web apps
- Office for iOS & Android
- Office for Windows



Unified with Office Information Protection and Azure AD policies

Now:

Unified information types for Office DLP & AIP (80+ types)

Enforcing Conditional Access for protected data

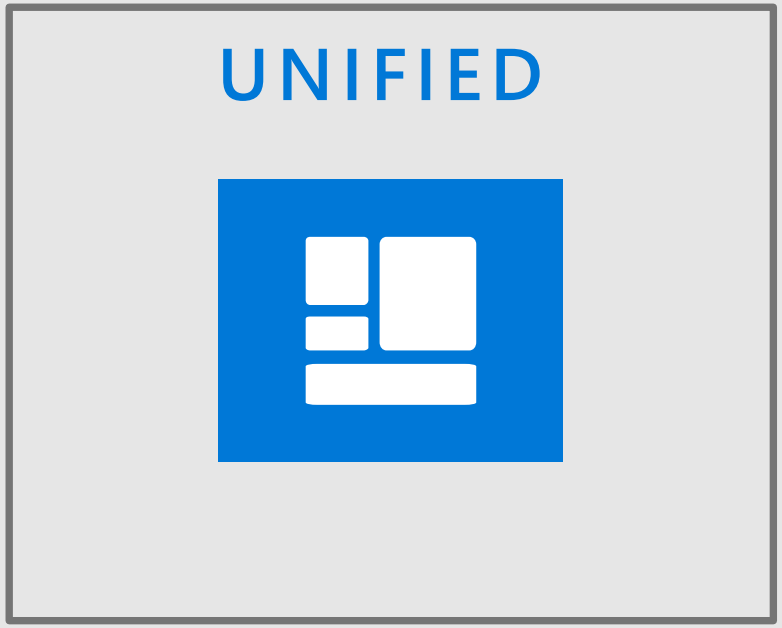
Short term:

SharePoint sync client support for encrypted files (in preview now)

Medium and long term:

Unified Information Protection policy for Office DLP & AIP

- Unify label management
- Unified labeling experience in Office clients & SPO/OD4B
- Unified classification policy

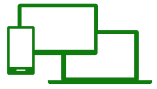


Protecting infrastructure and devices

Managed mobile productivity

Productivity

Enable a mobile experience that works the way employees want it to.



Device choice

Easy access to resources

Self-service options

Familiar Office apps

Data Protection

Ensure that the right data protection is applied to the right scenarios.

User, device, app, file control

Conditional access

Protection after access

Management

Tools and services that empower IT pros to do strategically more with less.

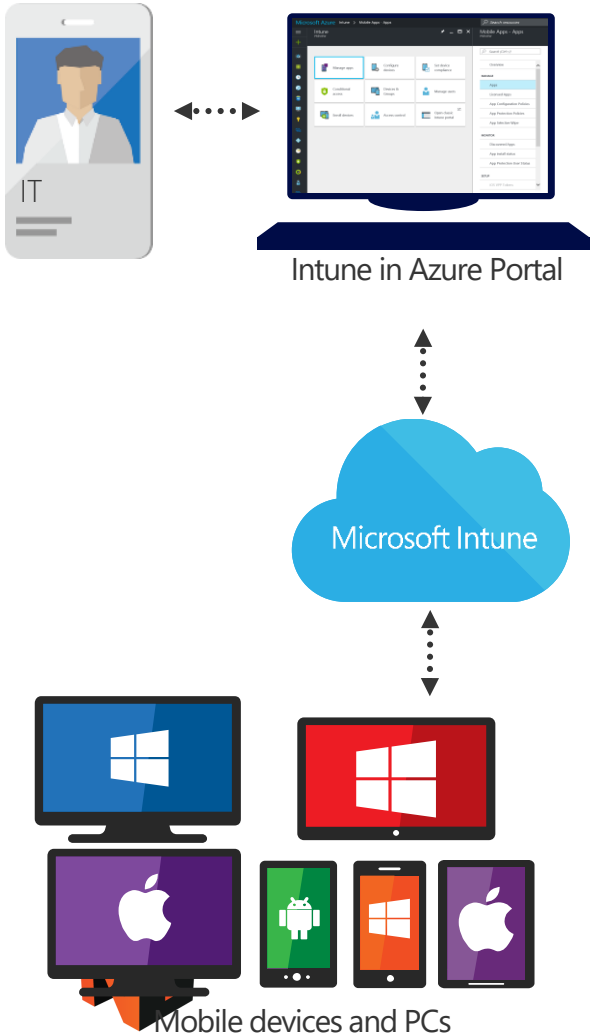
Unified management

Cloud-based scalability and reliability

Deployment support

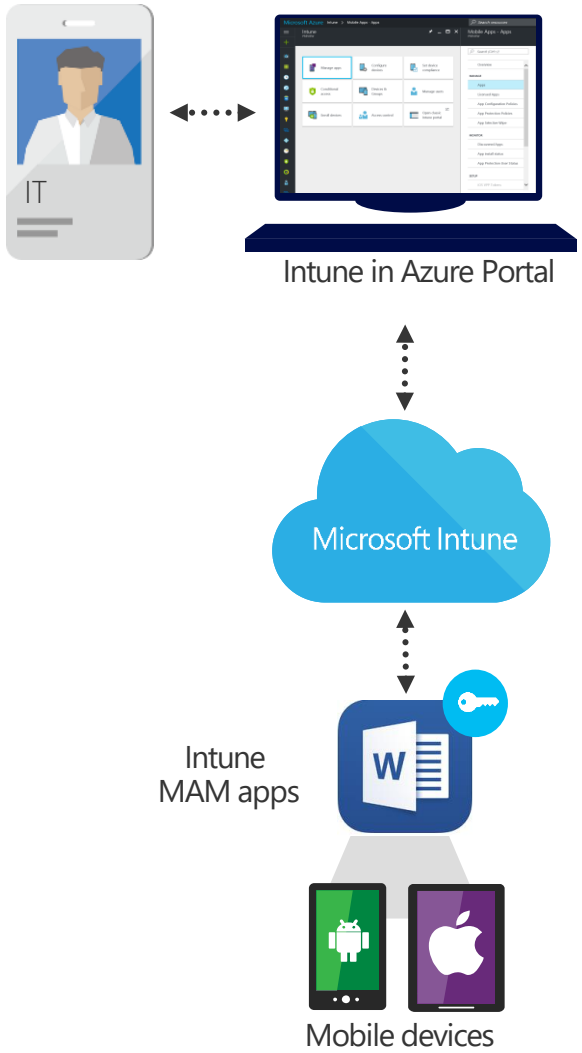
Trusted mobile devices and mobile apps

Intune Mobile Device Management



- Device policies
- Device inventory
- Device wipe
- App push
- Device configuration (certs; VPN)

Intune Mobile App Management

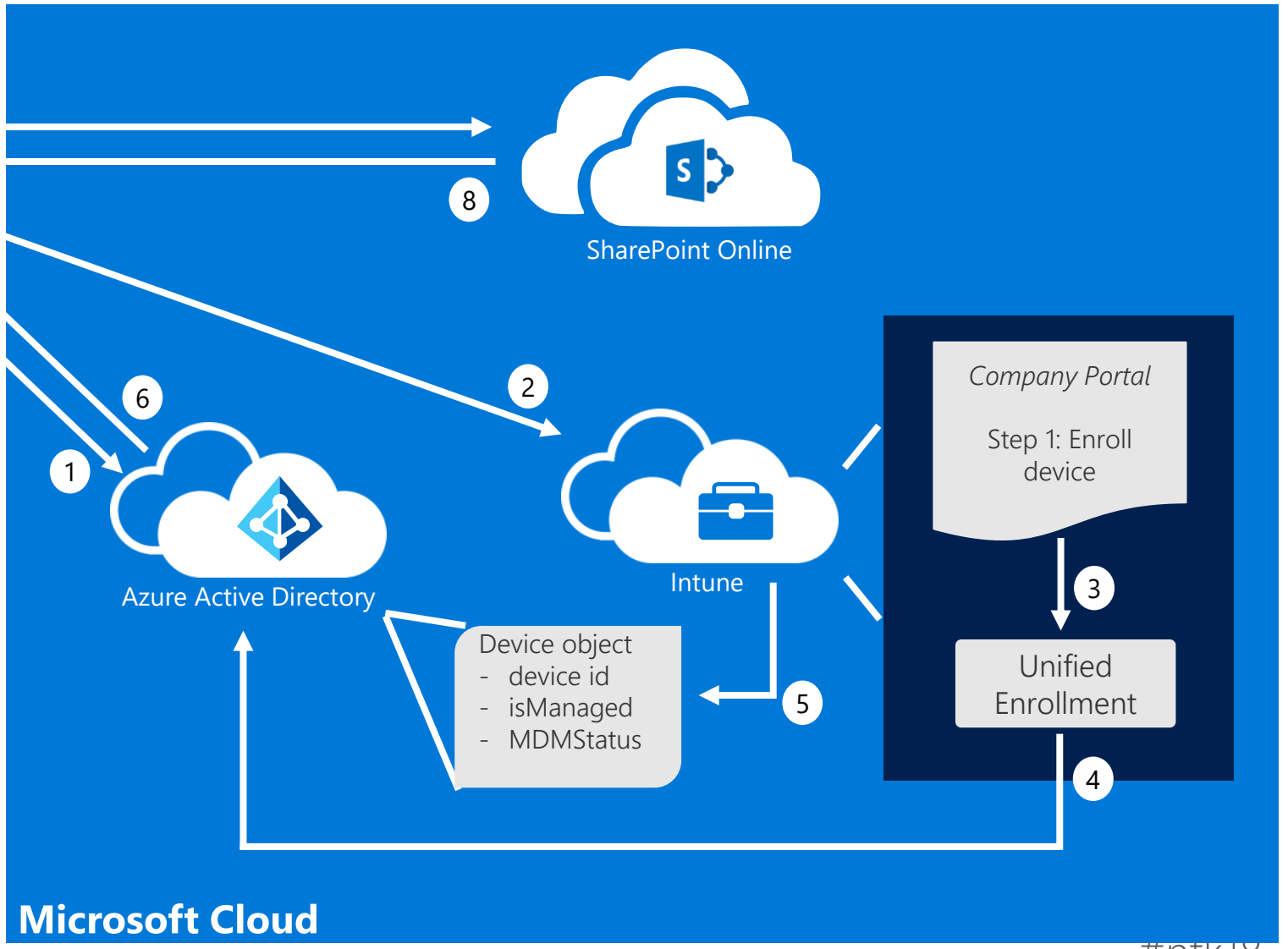


- App protection policies (APP)
- App wipe
- App configuration
- App deployment self-service

Conditional access from Intune managed devices

1. Client signs in; Azure AD performs a redirect to Intune
2. Client is directed to install the Intune company portal
3. Device begins enrollment via company portal
4. Device enrolls in Intune and is registered in AAD
5. Device management and compliance status is set in AAD
6. AAD issues direct access token
7. Client accesses service with direct access token
8. Data is delivered to client

7



So how is this more secure?

- Intune managed devices are controlled via CSPs.
- CSPs control device behaviour.
- Updates can be deployed without the IT infrastructure – great for road warriors.
- Defender and Windows updates can be deployed this way.

Up to date device = more secure

Microsoft Cloud App Security

Discover and assess risks

Identify cloud apps on your network, gain visibility into shadow IT, and get risk assessments and ongoing analytics.

Control access in real time

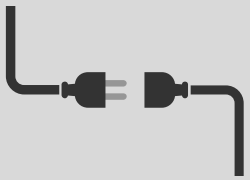
Manage and limit cloud app access based on conditions and session context, including user identity, device, and location.

Protect your information

Get granular control over data and use built-in or custom policies for data sharing and data loss prevention.

Detect threats

Identify high-risk usage and detect unusual behavior using Microsoft threat intelligence and research.



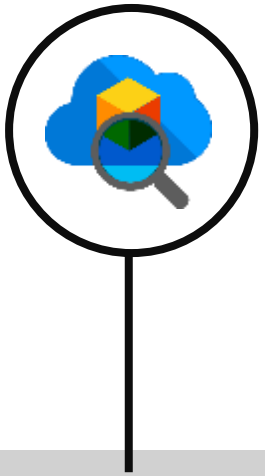
Extend Microsoft security

Threat detection: Microsoft Intelligent Security Graph, Office ATP
Information Protection: Office 365 & Azure Information Protection
Identity: Azure AD and Conditional Access

To your cloud apps

box now salesforce + more

Cloud discovery



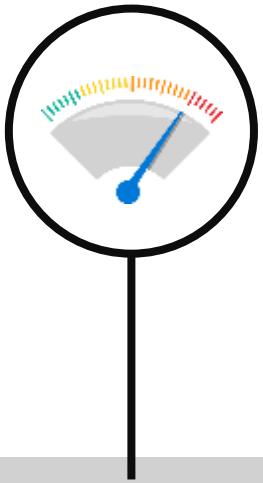
Shadow IT discovery

Discover cloud apps in use across your networks

Investigate users and source IP cloud usage

NEW Create custom views and reports for business units, networks and groups

NEW Optional PII anonymized reports

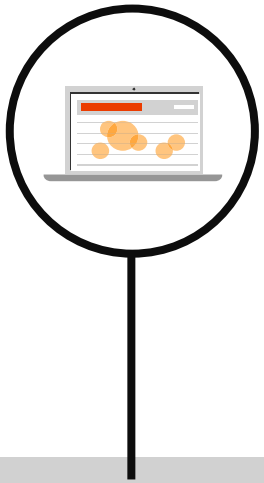


Risk assessment and migration to business-ready apps

Risk assessment for 15,000+ cloud apps based on 60 security and compliance risk factors

Un-sanction, sanction and protect apps

NEW Customize labels, notes, weight in risk scoring and override per app risk assessment to support internal workflows



On-going protection and analytics

Anomalous usage alerts

New apps and trending apps alerts

Identify and close policy enforcement gaps

NEW Programmatically generate blocking scripts to supported network appliances

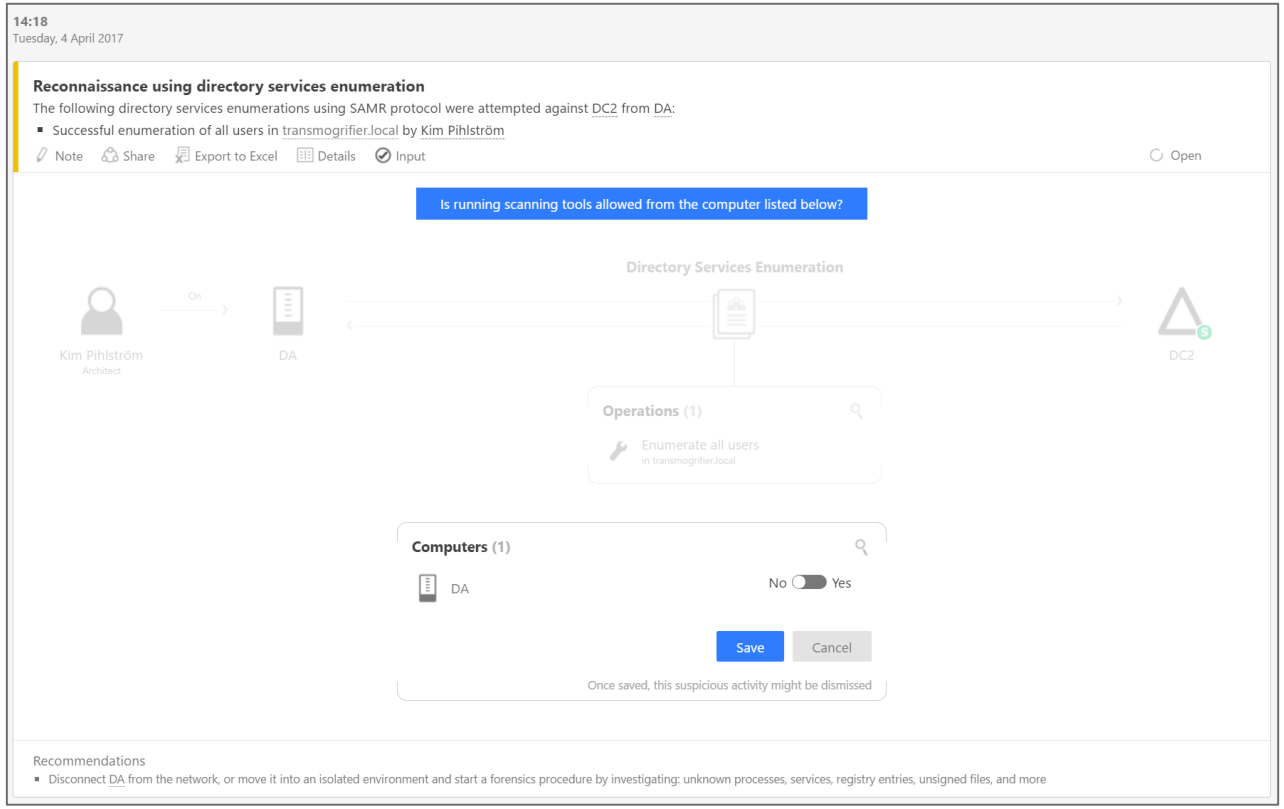
Integrates with

Your network appliances, SIEM

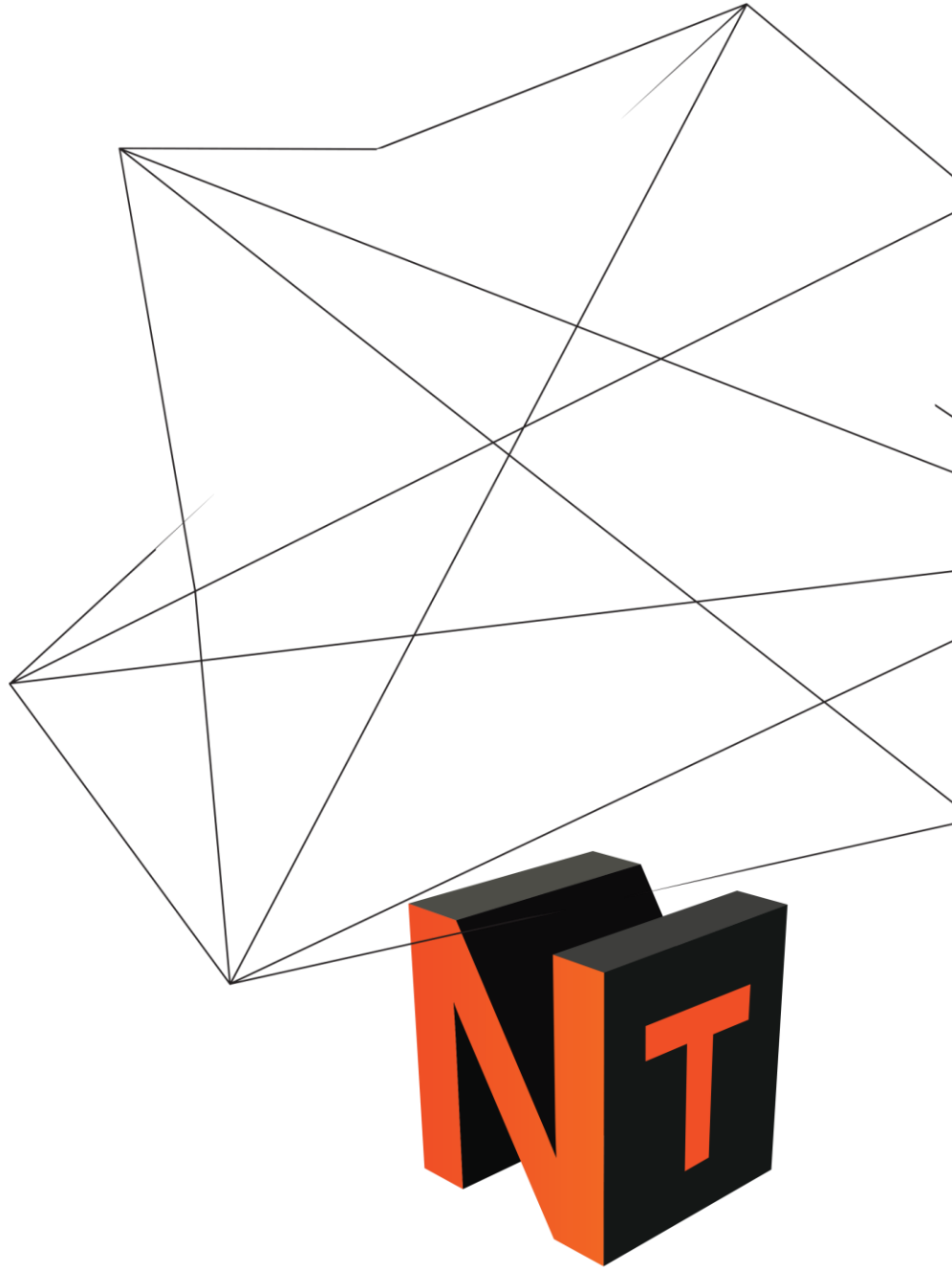
Advanced Threat Analytics

- ATA works by combining analysis of network traffic, events and contextual data from Active Directory

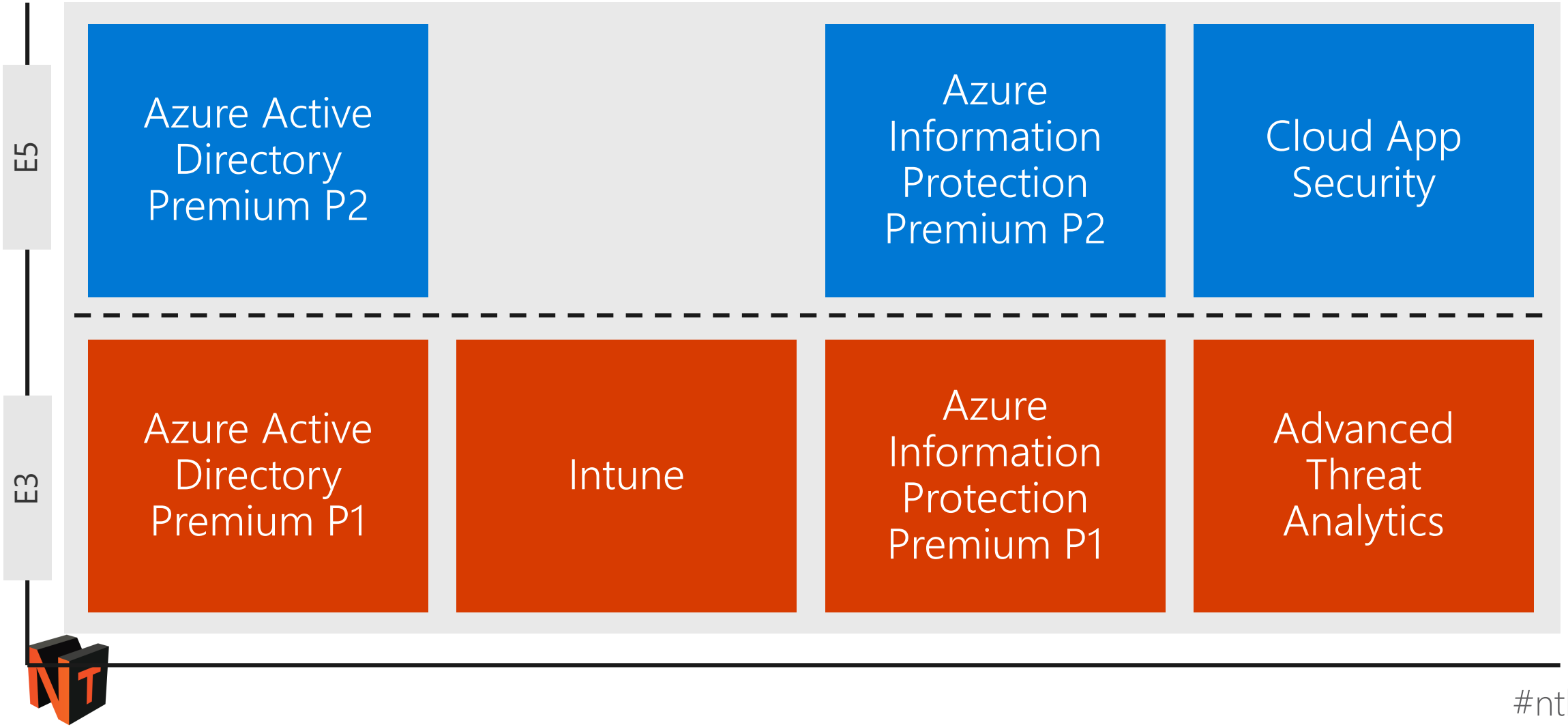
- Deploy, configure and let ATA start monitoring your network



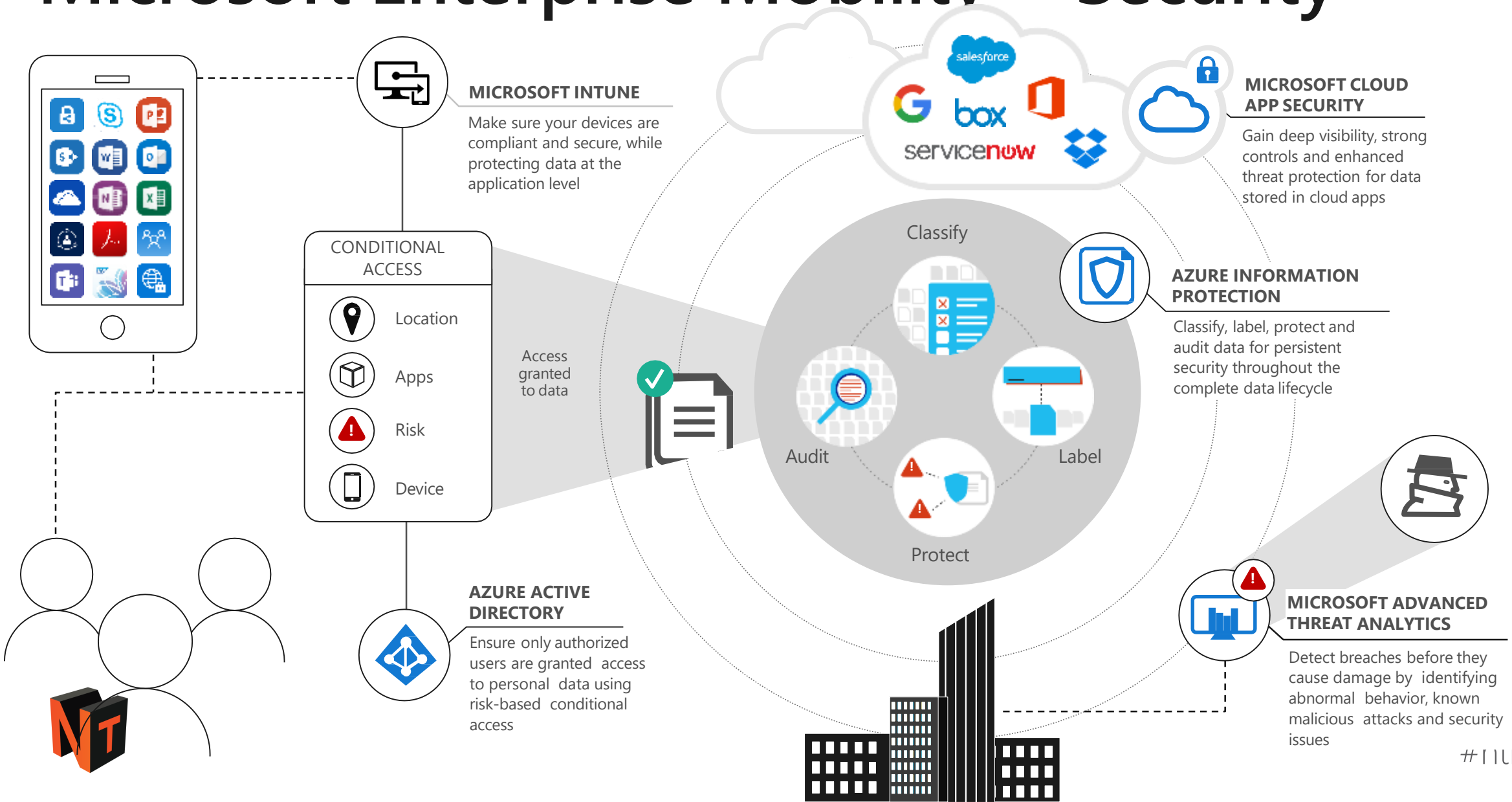
Enterprise Mobility + Security



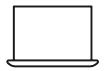
Identity-driven security solution



Microsoft Enterprise Mobility + Security



Microsoft Enterprise Mobility + Security

	Technology	Benefit	E3	E5
 Identity and access management	**Azure Active Directory Premium P1**	Secure single sign-on to cloud and on-premises app MFA, conditional access, and advanced security reporting	●	●
	Azure Active Directory Premium P2	Identity and access management with advanced protection for users and privileged identities		●
 Managed mobile productivity	**Microsoft Intune**	Mobile device and app management to protect corporate apps and data on any device	●	●
 Information protection	**Azure Information Protection P1**	Encryption for all files and storage locations Cloud-based file tracking	●	●
	Azure Information Protection P2	Intelligent classification and encryption for files shared inside and outside your organization		●
	Microsoft Cloud App Security	Enterprise-grade visibility, control, and protection for your cloud applications		●
 Threat protection	**Microsoft Advanced Threat Analytics**	Protection from advanced targeted attacks leveraging user and entity behavioral analytics	●	●

Thanks for your attention!

Feel free to ask : ddamir@logosoft.ba