



The Experts Conference

Sponsored by Quest®

Jeff Bley
Adwoa Boateng-Kwakye

**Five steps to embark on your
Zero Trust journey with M365**

TEC

The Experts
Conference
Sponsored by Quest®



Jeff Bley

Senior Product Manager – Microsoft Identity CXE

He/Him

TEC

The Experts
Conference
Sponsored by Quest®



Adwoa Boateng-Kwakye

Founder, *BreachProtect Consulting LLC*

Former Senior Product Manager, *Microsoft Identity and Network Access*

Agenda

- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- 5 Zero Trust Steps
- Go-Dos

Disclaimer – Recent Brand Change

- Azure AD = Entra ID
- Hybrid Azure AD Join = Hybrid Entra ID Join
- Etc.

Forgive us if we use the wrong term ☺

Better than blurry pictures

You can find a PDF of this deck at aka.ms/5stepsZT (on GitHub)

Agenda

- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- 5 Zero Trust Steps
- Go-Dos

NotPetya Attack

- NotPetya attack: Maersk – June 2017
- Cost Maersk \$200- \$300 million and disrupted operations for two weeks

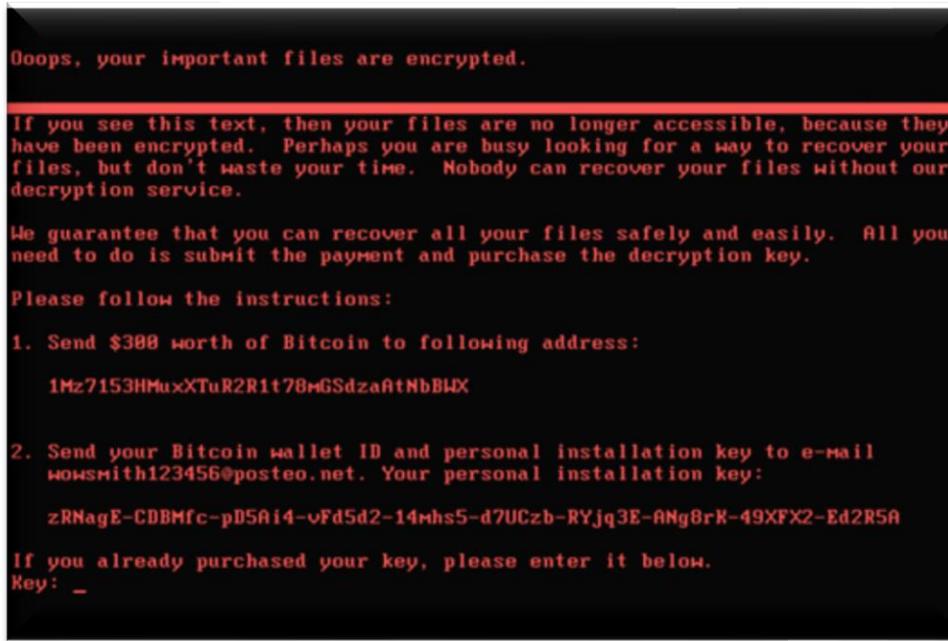


Photo credit: CrowdStrike



Maersk was hit by a worm dubbed NotPetya, which locked access to systems that the company uses to operate shipping terminals all over the world. Above, containers at a terminal in Germany in 2010. (Patrik Stollarz / AFP/Getty Images)

Maersk: Impact & Recovery



Trucks loaded with containers are lined up outside a terminal at the Jawaharlal Nehru Port Trust in Mumbai, India, Thursday, June 29, 2017. Operations at a terminal at India's busiest container port have been stalled by the malicious software that suddenly burst across the world's computer screens Tuesday, another example of the disruption that continues to be felt globally. (AP Photo/Rajanish Kakade)

twitter.com/tracyalloway/status/1034352176615882753

Tweet

@tracyalloway

A power outage in Ghana basically saved Maersk's shipping network:
[wired.com/story/notpetya...](https://www.wired.com/story/notpetya...)

After a frantic global search, the admins finally found one lone surviving domain controller in a remote office –in Ghana.

After a frantic search that entailed calling hundreds of IT admins in data centers around the world, Maersk's desperate administrators finally found one lone surviving domain controller in a remote office—in Ghana. At some point before NotPetya struck, a blackout had knocked the Ghanaian machine offline, and the computer remained disconnected from the network. It thus contained the singular known copy of the company's domain controller data left untouched by the malware—all thanks to a power outage. “There were a lot of joyous whoops in the office when we found it,” a Maersk administrator says.

- <https://www.hypr.com/security-encyclopedia/notpetya>
- <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

Zero Trust Isn't

- LITERAL - You can't build a practical strategy around absolutes
- AN ADJECTIVE – You aren't going to “be” zero trust
- FOR SALE – There's no such thing as “Zero Trust” tech
- INSTANT – You can't boil the ocean
- A REVOLUTION – Build on what you've got

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Zero Trust is a mindset

- Zero Trust requires 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

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Agenda

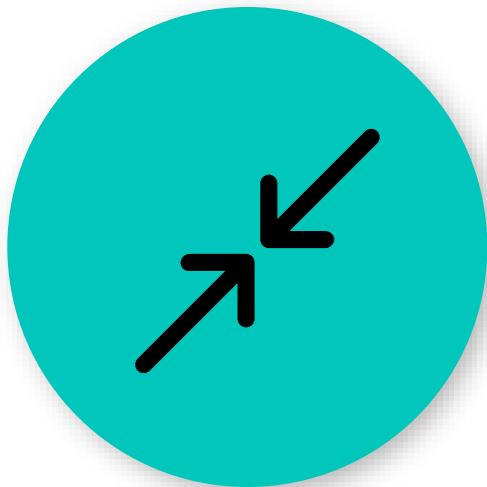
- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- 5 Zero Trust Steps
- Go-Dos

Core Principles of Zero Trust



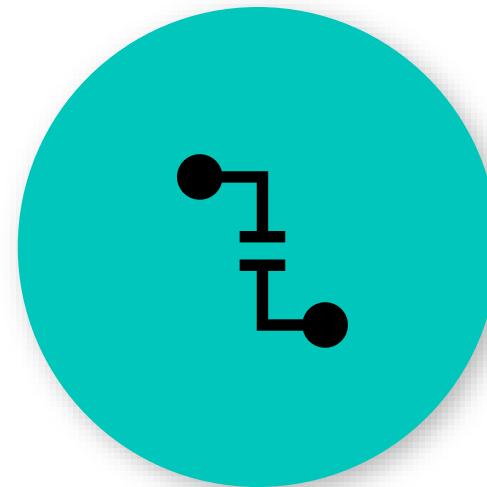
Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, and anomalies.



Least Privilege

Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive policies, and data protection which protects data and productivity.



Assume Breach

Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and application awareness. Verify all sessions are encrypted end to end.

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Pillars of Zero Trust



Identities



Devices/
Endpoints



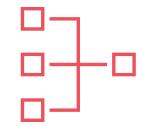
Applications



Data



Infrastructure



Network

aka.ms/ztmodel

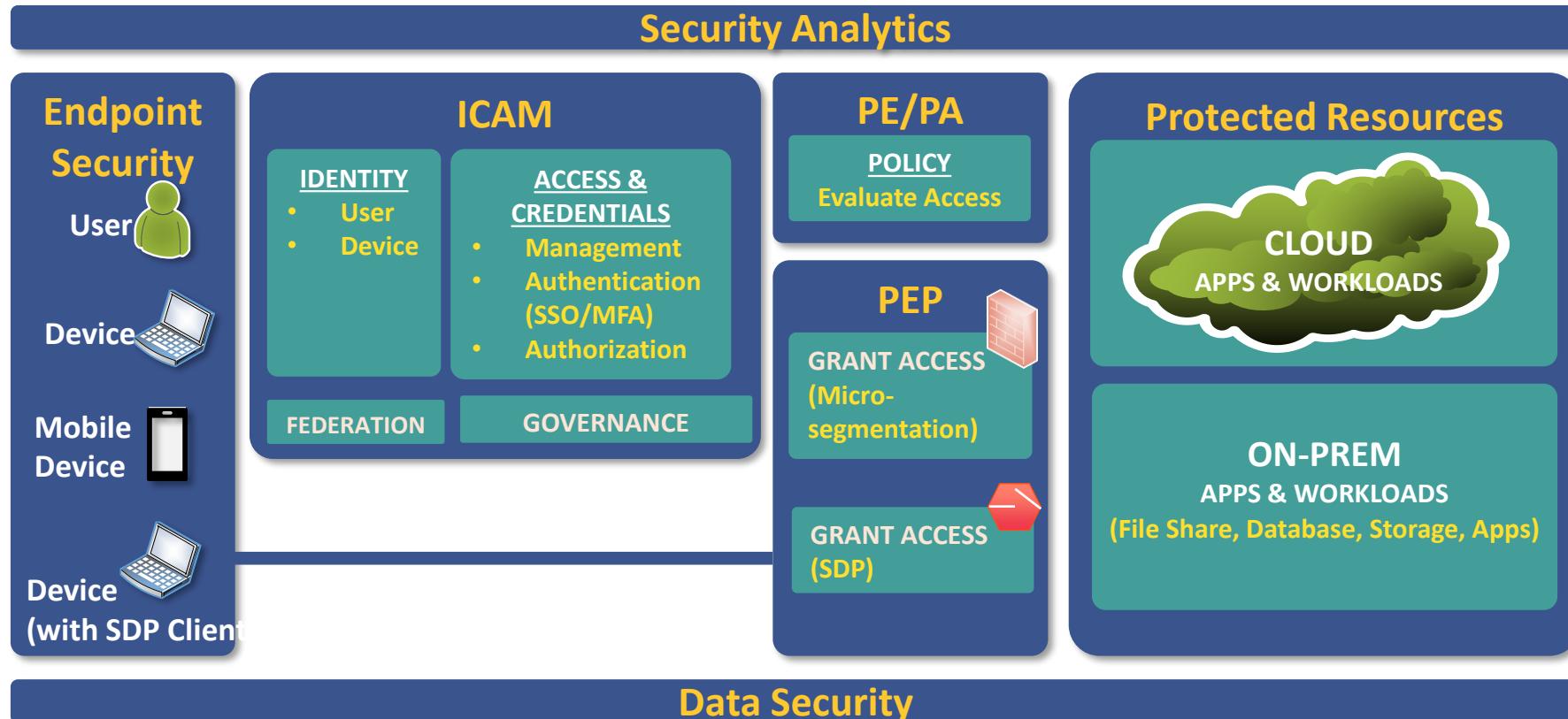
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

National Zero Trust Architecture - NIST



ICAM	<i>Identity, Credential and Access Management</i>
PA	<i>Policy Administrator</i>
PE	<i>Policy Engine</i>
PEP	<i>Policy Enforcement Point</i>
SDP	<i>Software Defined Perimeter</i>

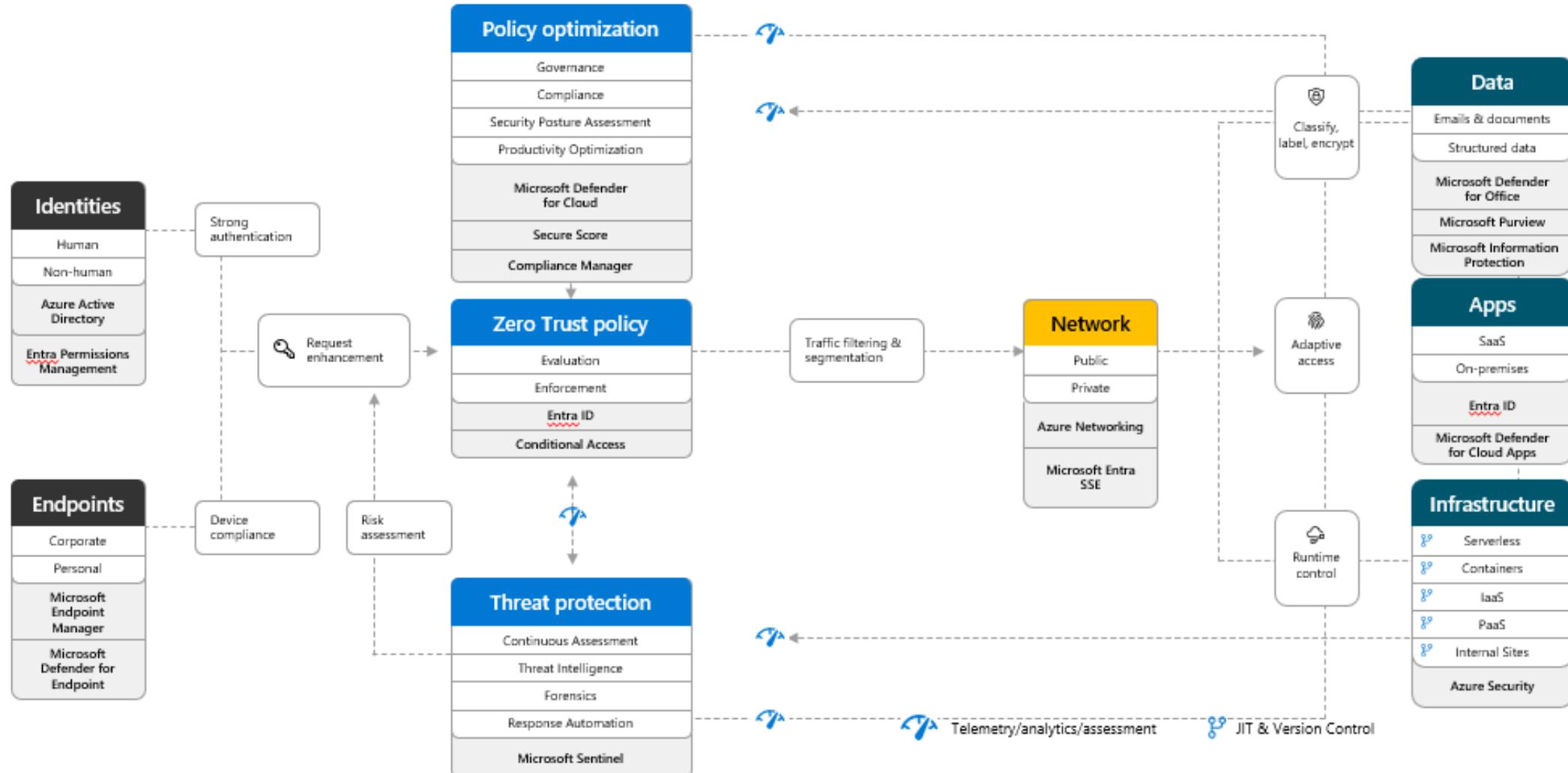
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Microsoft Zero Trust Architecture

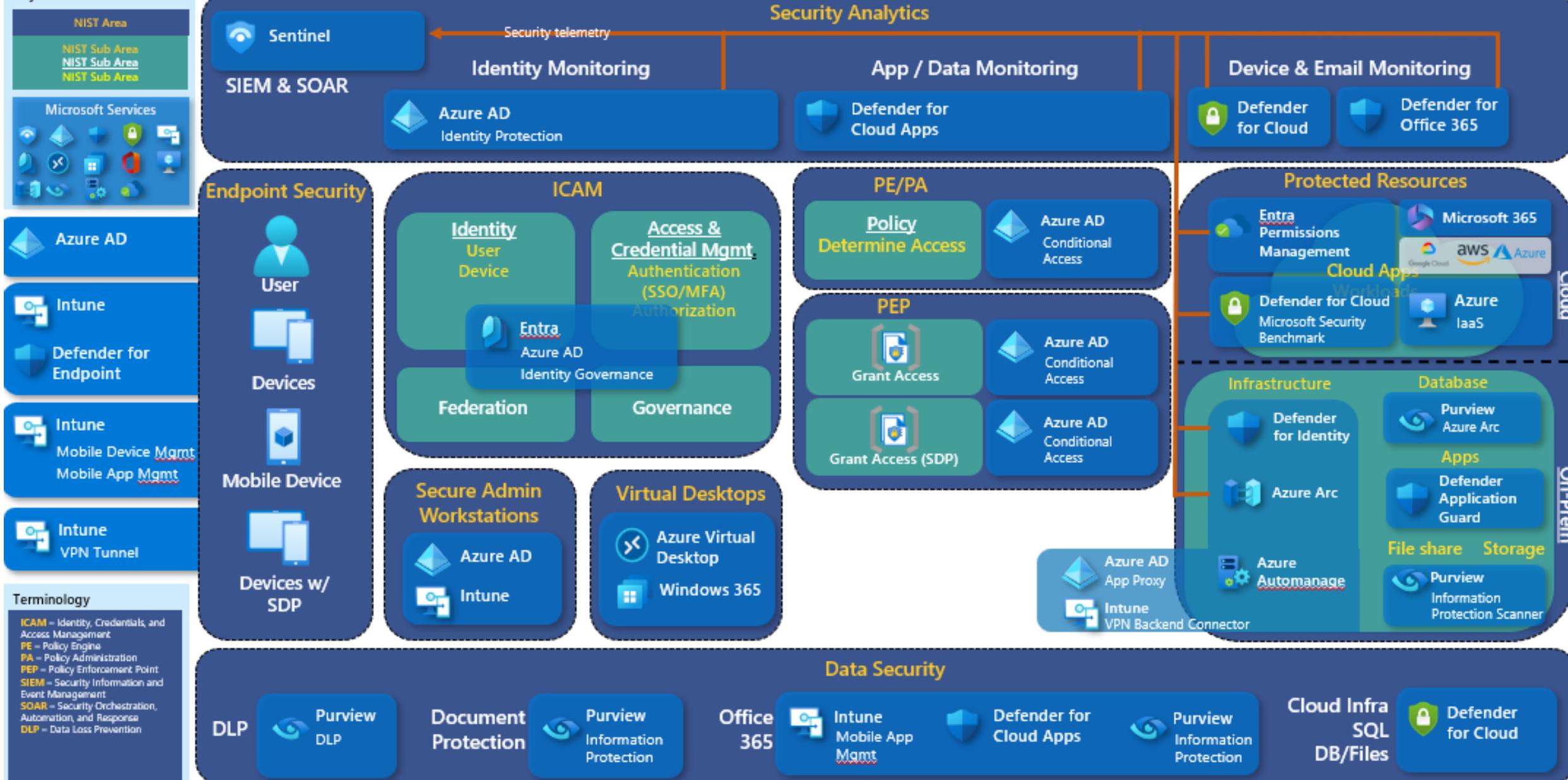


Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos



Agenda

- Introduction to Zero Trust
- Zero Trust Principles and Architecture
- **5 Zero Trust Steps**
- Go-Dos

1. Strengthen Identities



Deploy strong authentication
methods



Protect identities using Microsoft
Conditional Access and Identity
Protection



Modernize Conditional Access
policies

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Authentication Methods

Bad: Password

123456

qwerty

password

iloveyou

Password1

Good: Password
and...



SMS



Voice

Better: Password
and...



Authenticator
(Push Notifications)



Software
Tokens OTP



Hardware Tokens OTP
(Preview)



Authenticator
(Phone Sign-in)



Window
Hello



FIDO2 security key



Certificates

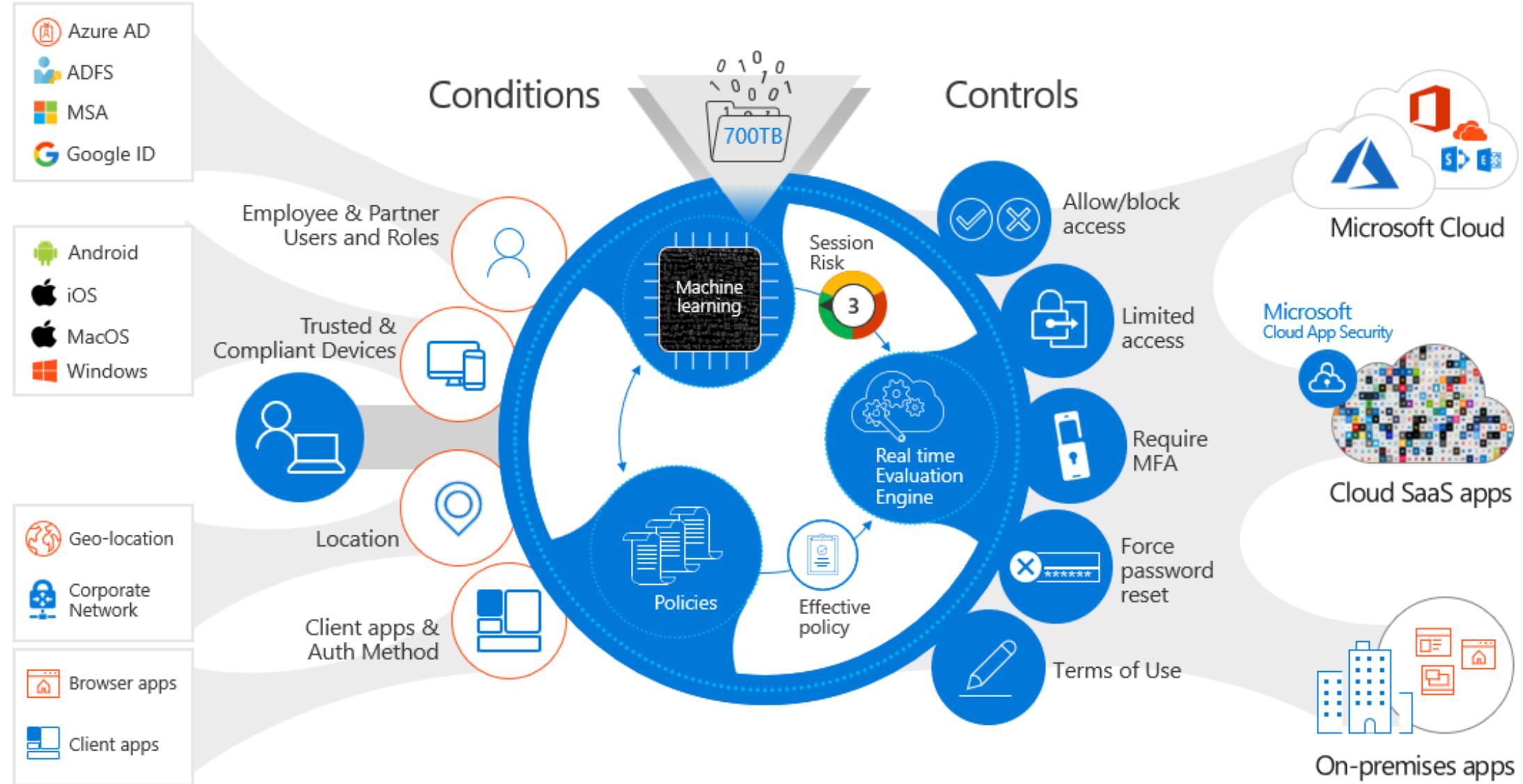
Introduction to ZT

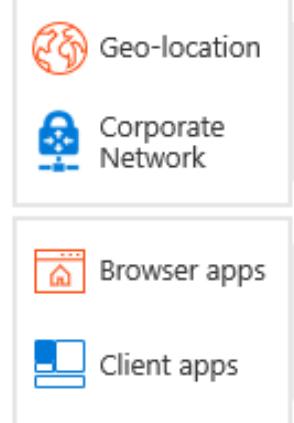
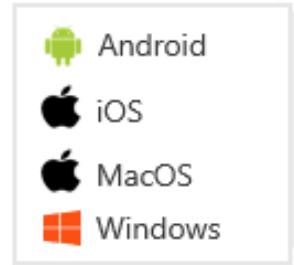
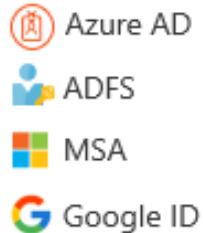
ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Microsoft Conditional Access





Conditions

Employee or Partner?
Users or Admins?



Managed or Personal?
Compliant or Risky?



Office or Internet?



Client or Browser?
Authentication Method?
Target Service?



Controls

Identity Protection



+ Dynamic Risk Evaluation

- User Leaked Credentials ?
- Unfamiliar Sign-In Properties (UEBA) ?
- Impossible / Atypical travel ?
- Unusual User Activity or Known Attack Pattern ?
- Malware linked / Malicious IP ?
- Anonymous IP ?

User risk
 High
Medium
Low

Sign-in risk
 High
Medium
Low



Allow/block access



Limited access



Require MFA



Force password reset



Block legacy authentication



Microsoft Cloud



Microsoft Cloud App Security



Cloud SaaS apps



On-premises apps

Modernize Conditional Access Policies

- Design an audience matrix with an established baseline
- Establish a naming convention

Policy Naming Prefix	Meaning
L	Lockdown
P	Privileged
A	All Accounts
G	Guests

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Modernize Conditional Access Policies

- **Avoid “Block All Applications” policy**
- Classify applications – ensure every application is subject to at least one Conditional Access policy

Example 1

High Business Impact (HBI)
Medium Business Impact (MBI)
Low Business Impact (LBI)

Example 2

Tier 1
Tier 2
Tier 3
Tier 4
Tier 5

Dynamic App targeting in Conditional Access

- Custom Security Attributes to dynamically target applications in Conditional Access

Home > Aperture Science | Custom security attributes > Applications | Active attributes >

New attribute ...

Add a custom security attribute (key-value pair) to your directory that you can later assign to Azure AD objects, such as users or applications. [Learn more](#)

Attribute name *	ApplicationTierLevel
Description	Classifies application sensitivity and subsequent controls based on tiered levels.
Data type *	String
Allow multiple values to be assigned	<input type="radio"/> Yes <input checked="" type="radio"/> No
Only allow predefined values to be assigned	<input checked="" type="radio"/> Yes <input type="radio"/> No
Predefined values	+ Add value
Value	↑↓ Is active?
Tier 1	✓ .
Tier 2	✓ .
Tier 3	✓ .
Tier 4	✓ .
Tier 5	✓ .

[Save](#)

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Dynamic App targeting in Conditional Access

Stardust | Custom security attributes

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Application proxy Self-service Custom security attributes

Attribute set Applications Attribute name ApplicationTierLevel Attribute description Classifies application sensi... Data type String Multi-valued No Assigned values

Tier 5

Tier 1

Tier 2

Tier 3

Tier 4

Tier 5

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Dynamic App targeting in Conditional Access

The screenshot shows the 'Edit filter (Preview)' screen for a new Conditional Access policy named 'Tier 5 - Highly Sensitive Access'. The left sidebar lists policy components like Assignments, Target resources, Conditions, Access controls, and Enable policy. The main area shows a single filter rule:

And/Or	Attribute	Operator	Value
	Applications_ApplicationTierLevel	Equals	Tier 5

Below the table, the rule syntax is displayed as: `CustomSecurityAttribute.Applications_ApplicationTierLevel -eq "Tier 5"`. A 'Done' button is at the bottom right.

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Use Authentication Strengths

Bad: Password **Grant** **Better: Password and...** **Best: Passwordless**

Control access enforcement to block or grant access. [Learn more](#)

123456 Block access Grant access

qwerty Require multifactor authentication

password 

iloveyou  "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Password1 Require authentication strength 
Phishing-resistant MFA 

Authenticator (Push Notifications)

Software Tokens OTP

Hardware Tokens OTP (Preview)

Authenticator (Phone Sign-in)

Window Hello

FIDO2 security key

Certificates

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Use Authentication Strengths

The screenshot shows the 'Grant' dialog box from the Microsoft Conditional Access policy configuration interface. On the left, there's a sidebar with sections like 'New Conditional Access policy', 'Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.', 'Name *' (set to 'Require Phishing-resistant MFA'), 'Assignments' (with 'All users' selected), 'Target resources' (with 'All cloud apps' selected), 'Conditions' (0 conditions selected), 'Access controls' (Grant tab selected, 0 controls selected), 'Session' (0 controls selected), 'Enable policy' (Report-only selected), and a 'Create' button.

The main area shows the 'Grant' configuration. It has two radio button options: 'Grant access' (selected) and 'Require multifactor authentication'. Below these are two checkboxes: 'Require authentication strength' (selected) and 'Require multifactor authentication'. A tooltip message states: "'Require authentication strength' cannot be used with 'Require multifactor authentication'." A dropdown menu for 'Phishing-resistant MFA' is open, showing the following options:

- Multifactor authentication: Combinations of methods that satisfy strong authentication, such as Password + SMS.
- Passwordless MFA: Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator.
- Phishing-resistant MFA: Phishing-resistant passwordless methods for the strongest authentication, such as FIDO2 Security Key.

A 'Select' button is at the bottom of the dropdown menu.

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✓	✓	✓
Windows Hello for Business	✓	✓	✓
Certificate-based authentication (Multi-Factor)	✓	✓	✓
Microsoft Authenticator (Phone Sign-in)	✓	✓	
Temporary Access Pass (One-time use AND Multi-use)	✓		
Password + something you have ¹	✓		
Federated single-factor + something you have ¹	✓		
Federated Multi-Factor	✓		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Example Policy Set – Core Tier Policies

Policy	App Tier	Targeted Scenario	Controls Enforced
A001 – Tier1 Require ToU	1	Any type of access to Tier 1 applications	Must accept Terms of Use
A002 – Tier2 Require MFA	2	Any type of access to Tier 2 applications	Require any type of MFA
A003 – Tier3 Zero Trust Passwordless	3 (Default)	Any type of access to Tier 3 applications	Require Stronger Auth Strength (no SMS or Voice MFA)
A004 – Tier3 Zero Trust Device State	3 (Default)	Any type of access to Tier 3 applications	Require compliant device or require Hybrid Azure AD Joined device
A005 – Tier4 Zero Trust Compliant + Phish Resistant	4	Any type of access to Tier 4 applications	Require compliant device and <i>phishing-resistant</i> Auth Strength
A006 – Tier5 Zero Trust Compliant + Phish Resistant	5	Any type of access to Tier 5 applications	Require compliant device and <i>phishing-resistant</i> Auth Strength
A007 – Tier5 PAW	5	Any type of access to Tier 5 applications	Block access unless the user is on a Privileged Access Workstation
A008 – Tier5 Trusted Network	5	Any type of access to Tier 5 applications	Block access unless the user is on a trusted network

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Example Policy Set – Specialty Policies

Policy	App Tier	Targeted Scenario	Controls Enforced
A009 – Interactive MFA for Intune Enrollment	n/a – Intune Enrollment app only	Require user-interactive MFA to enroll a device in Intune	MFA, Sign-In Frequency require interactive authentication
A010 – MFA to Register/Join Device	n/a	Require MFA to AAD Register or AAD Join a device to Azure AD	MFA
A011 – Tier2/3/4/5 App Access SIF on Unmanaged Devices	2, 3, 4, 5	Any type of access from an unmanaged device to Tier 2-5 apps	Sign-In Frequency maximum session lifetime of 12 hours
A013 – Tier4/5 Block Guests	4, 5	Any access to Tier 4 or 5 apps by a guest user	Block
G001 – Guests Require MFA	All	Any access to any app by a guest user	MFA
L001 – Block Untrusted Locations	All	Any access from countries you do not do ANY business in, such as sanctioned countries	Block
L002 – Block Legacy Authentication	All	Any access using legacy authentication	Block
W001 – Block Medium and High Risk Workload Identities	All	Any access by a workload identity identified as Medium or High Risk	Block

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Example Policy Set – Admin and Risk Policies

Policy	App Tier	Targeted Scenario	Controls Enforced
P001 – Admins Compliant + Phish Resistant	n/a	Any access by an Azure AD administrator role holder	Require compliant device and <i>phishing-resistant MFA</i>
P002 – Admins Compliant + Phish Resistant for Admin Actions	n/a	Any sensitive operation carried out by an administrator	Require compliant device and <i>phishing-resistant MFA</i>
R001 – MFA Sign In Risk	All	Any sign in categorized by Identity Protection as Low, Medium, or High Risk	MFA, Sign-In Frequency require interactive authentication
R002 – PWD Change High User Risk	All	Any access by a High Risk user	Require secure password change, Sign-In Frequency require interactive authentication

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Conditional Access Migration Strategy

1. Create an empty security group

2. Include the group on all new policies

3. Exclude group on all old policies

4. Add users into the group created

5. Apply policies to "All Users"

6. Disable old policies, then delete later

2. Integrate Applications



Integrate SaaS + On-prem applications with Entra ID

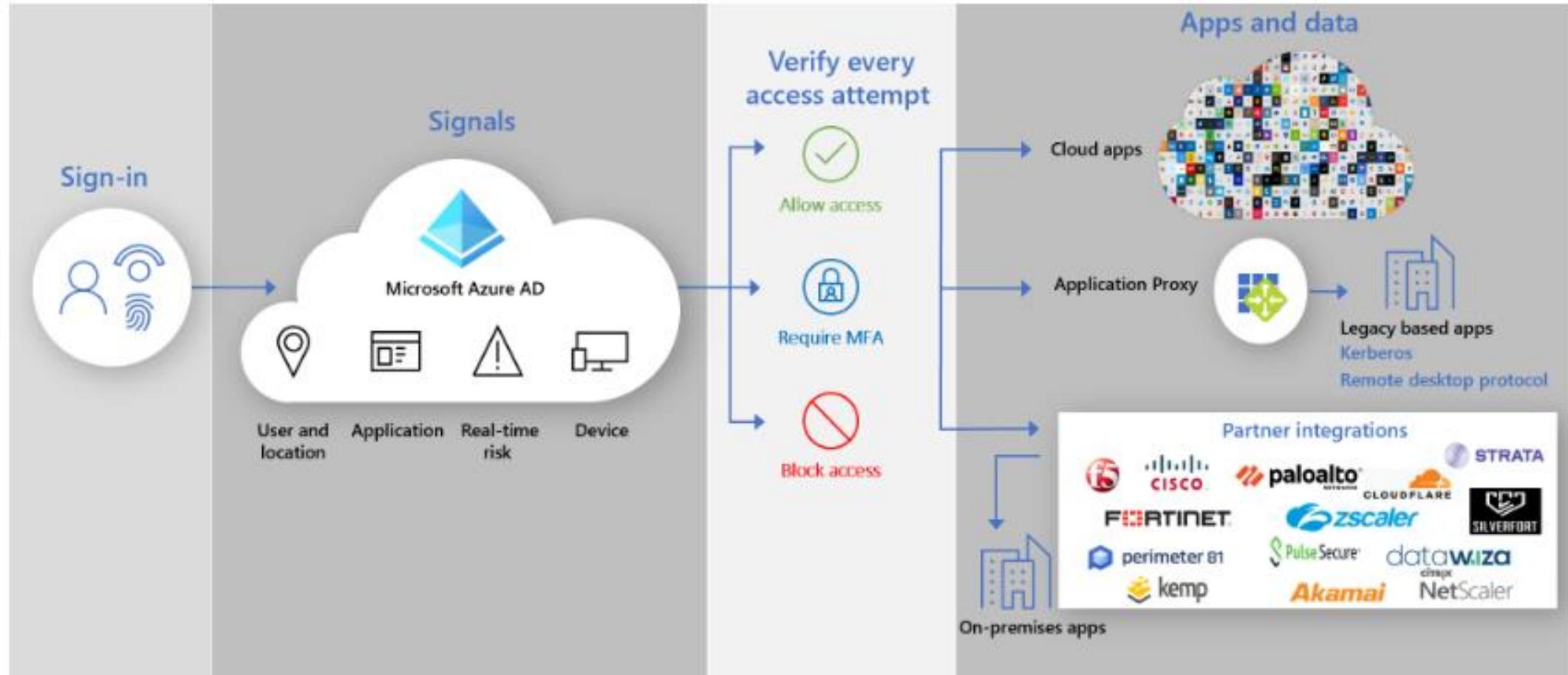


Protect applications with Microsoft Defender for Cloud Apps



Protect application data with Microsoft Purview

Integrate SaaS and On-prem Applications



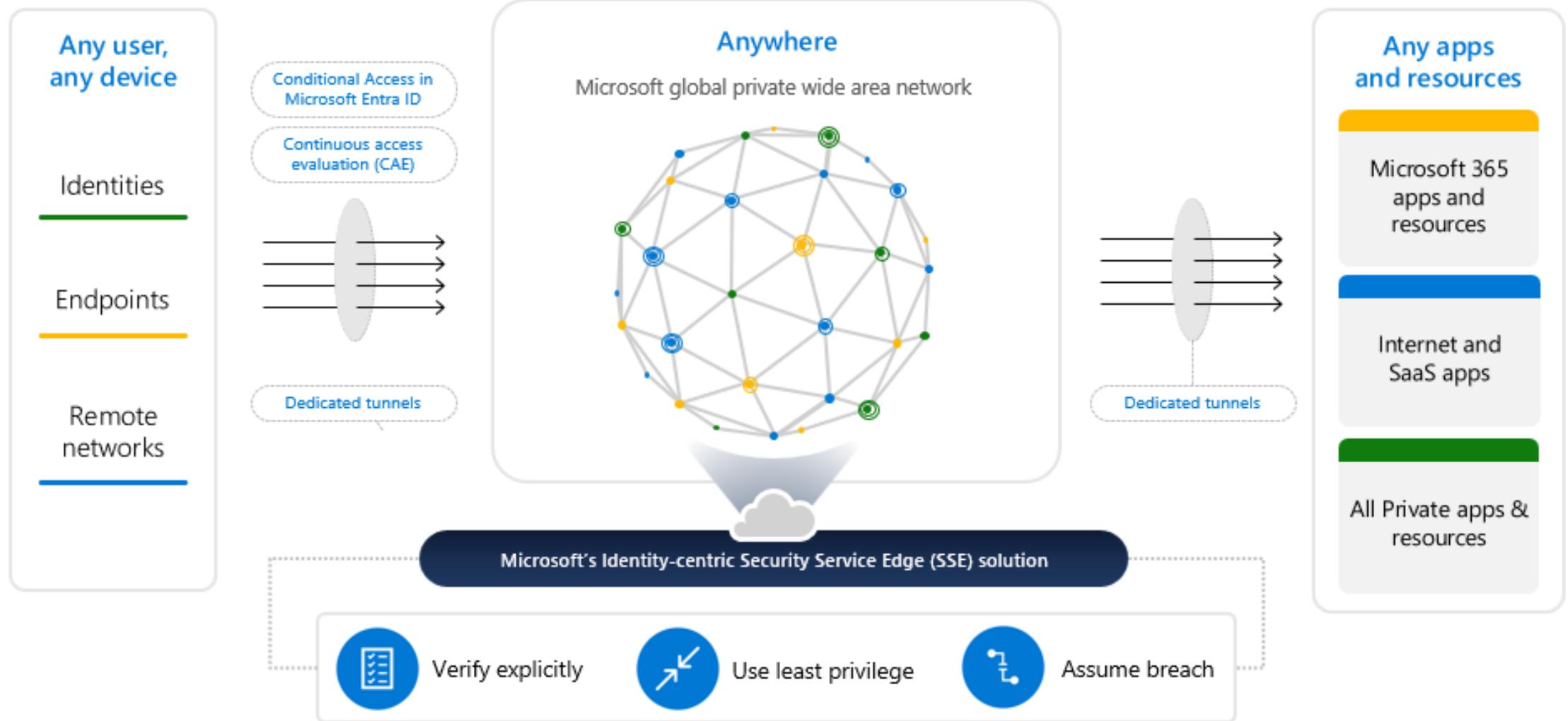
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Microsoft's Identity-centric SSE solution



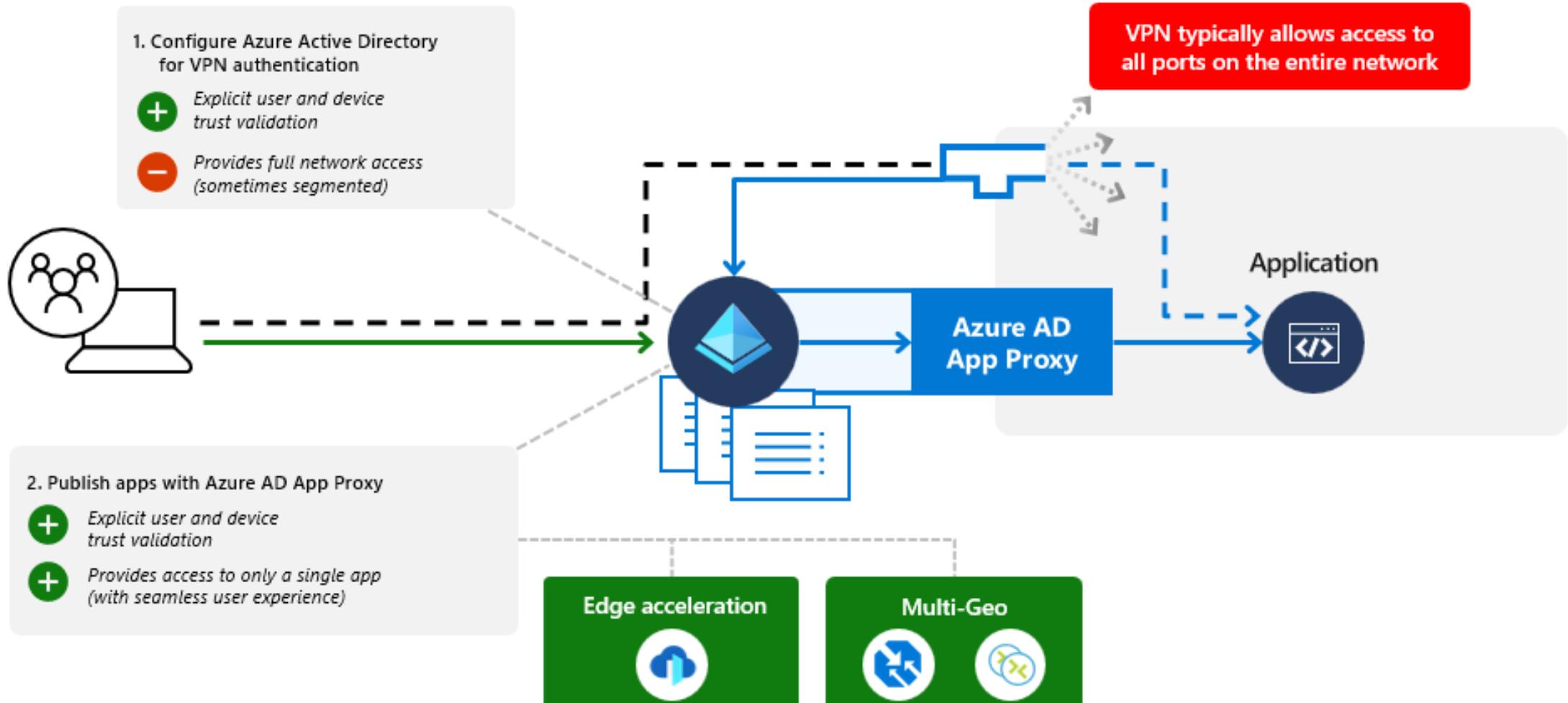
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Microsoft's Identity-centric SSE solution



Introduction to ZT

ZT Principles + Architecture

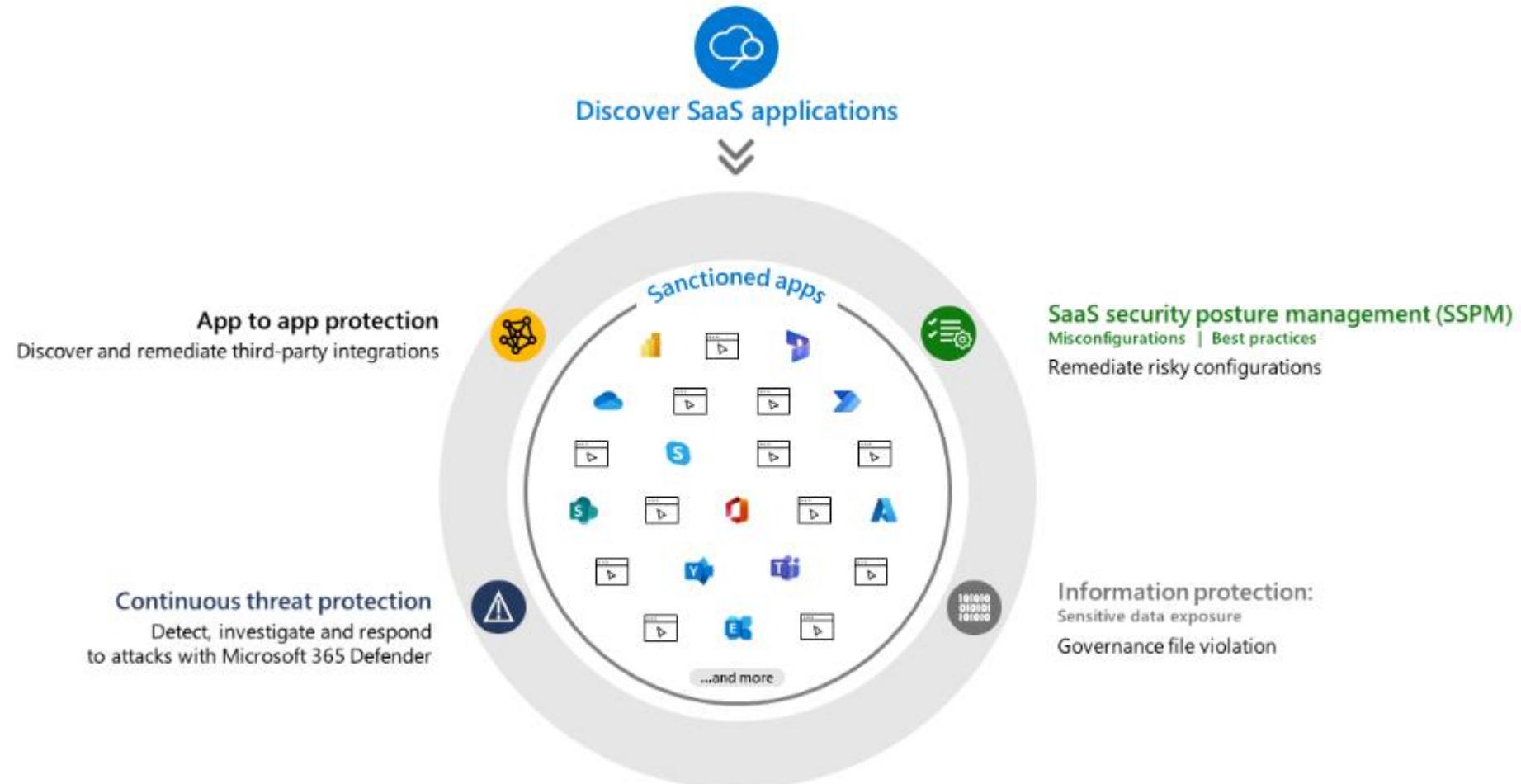
5 Zero Trust Steps

Go-Dos

Microsoft Entra Private Access Demo

The screenshot shows the Microsoft Entra admin center interface. The left sidebar navigation includes Home, Favorites, Identity, Protection, Identity governance, Verifiable credentials, Permissions Management, Global Secure Access (Preview), Get started, Dashboard, Devices, Applications, Learn & support, and a search bar. The main content area displays the "Woodgrove-Tunnel | Network access properties" page for a "Global secure access application". The page shows the application name "Woodgrove-Tunnel", its connector group "NOAM - App Proxy Group - North America", and a note about enabling access with a Global Secure Access client. A table lists a destination type "IP address" with a value of "172.16.66.70" and port "22", with a delete icon. At the bottom are "Save" and "Discard" buttons.

Microsoft Defender for Cloud Apps



Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Microsoft Purview



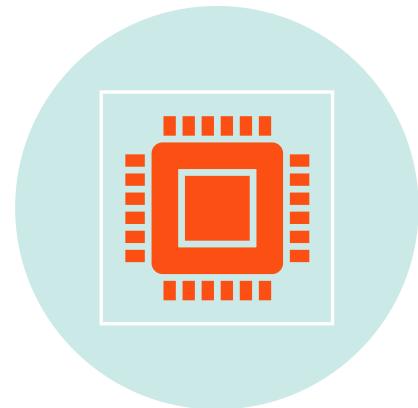
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

3. Adopt Least Privilege



Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA)



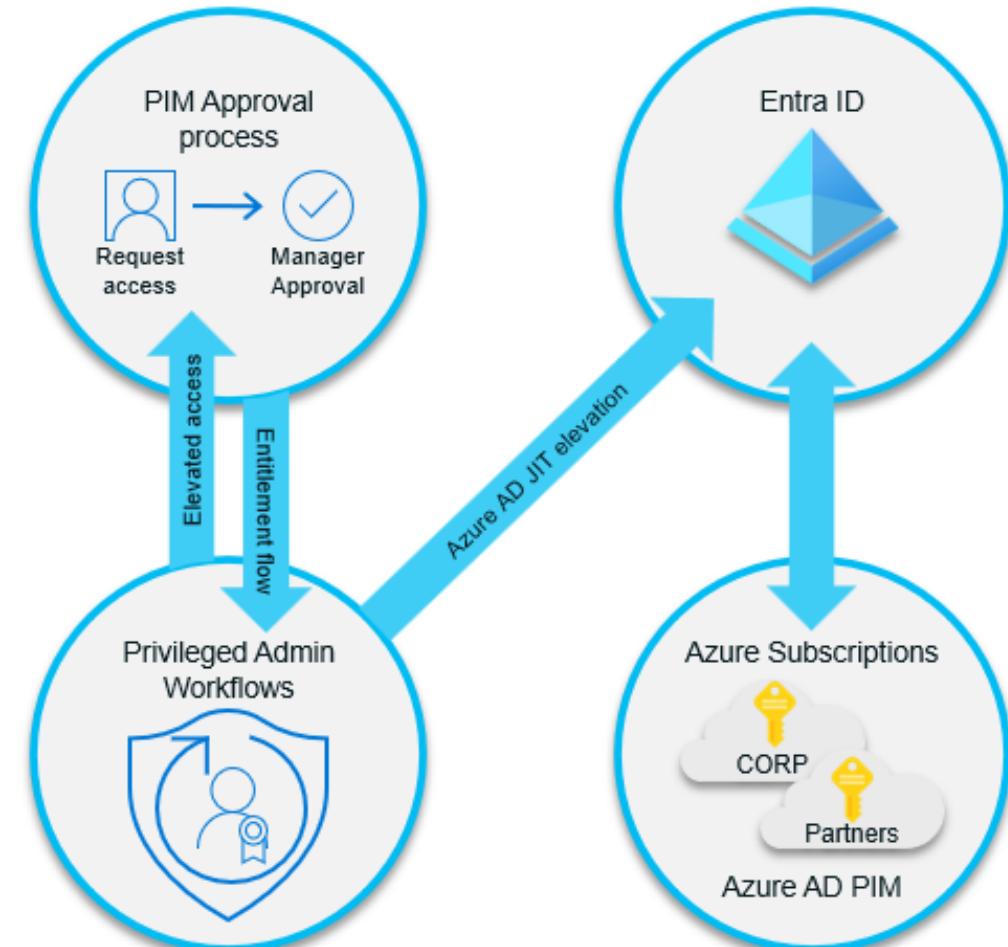
Leverage Privileged Identity Management



Leverage Entra Permissions Management

Privileged Identity Management (PIM)

- Privilege Management at Scale
 - Leverage JIT/JEA controls for Tier 0 roles, expand to other roles as well
- No Persistent Elevated Access
 - Do not allow persistent elevated access on-premises or in the cloud
- Reduce Surface Area
 - Significantly lower blast radius if identity is compromised



Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go Do's

PIM + Conditional Access Demo

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a tree view with 'Conditional Access' selected under 'Azure Active Directory'. The main content area is titled 'Conditional Access | Authentication context'. It shows two authentication contexts: 'Require Compliant Device' and 'XTAP Privileged Actions'. The 'Require Compliant Device' context is described as 'Require Compliant Device'. The 'XTAP Privileged Actions' context is described as 'Permissions considered sensitive when modifying Cross Tenant Access Policy'. The top navigation bar shows tabs for 'Edit role setting - Global Admin' and 'Conditional Access - Microsoft Edge'. The address bar shows the URL https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/AuthenticationContext/fromNav/Identity. The bottom taskbar shows various icons and the date/time 10:38 AM 9/1/2023.

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go Do's

Entra Permissions Management (EPM)

Managing permissions across multi-cloud environments requires *a new, dynamic approach*



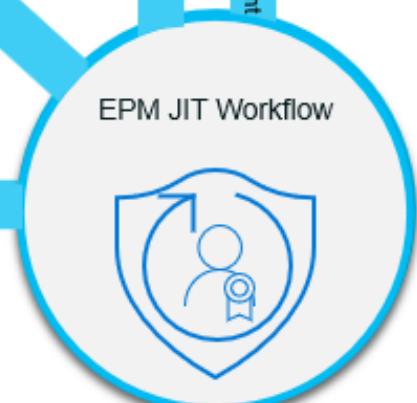
Grant permissions based on historical usage and activity



Allow temporary access to high-risk permissions on-demand



Continuously monitor and right-size identities to prevent privilege creep



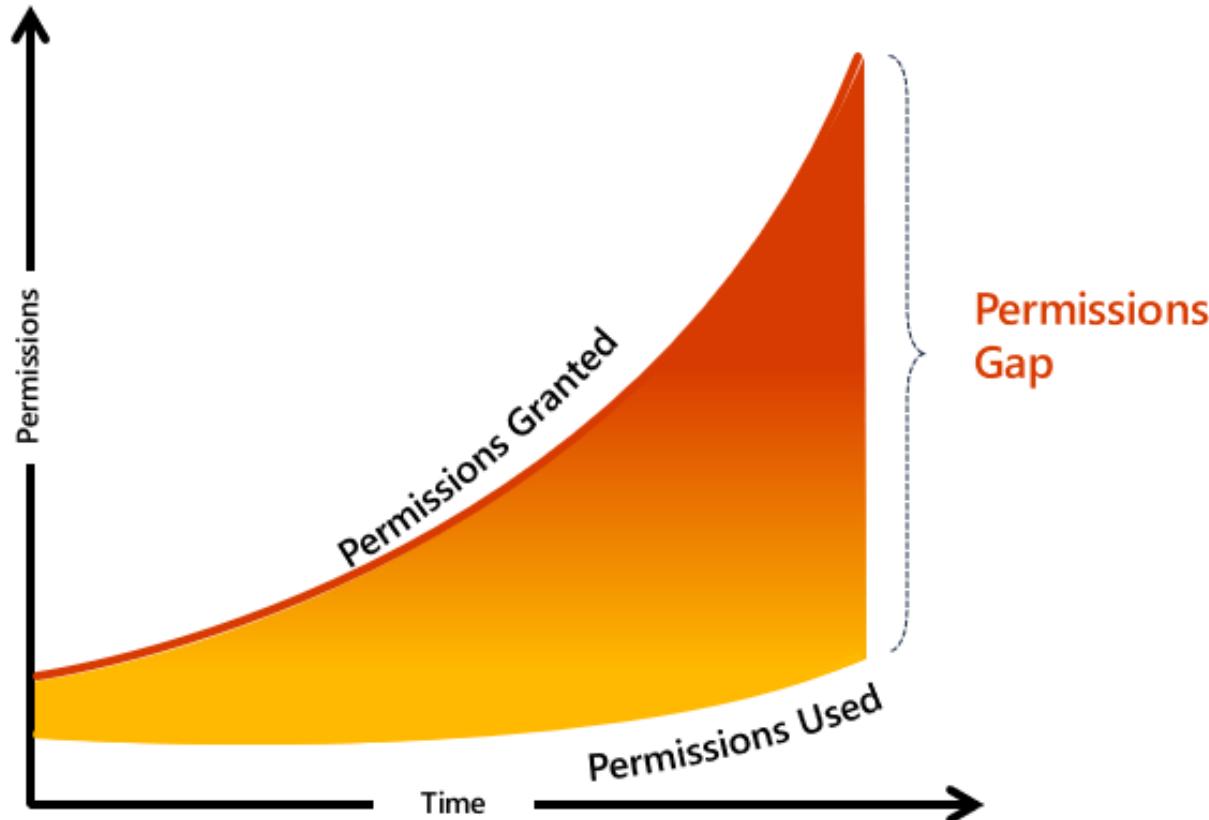
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Permissions creep



Lack of comprehensive visibility into identities, permissions and resources

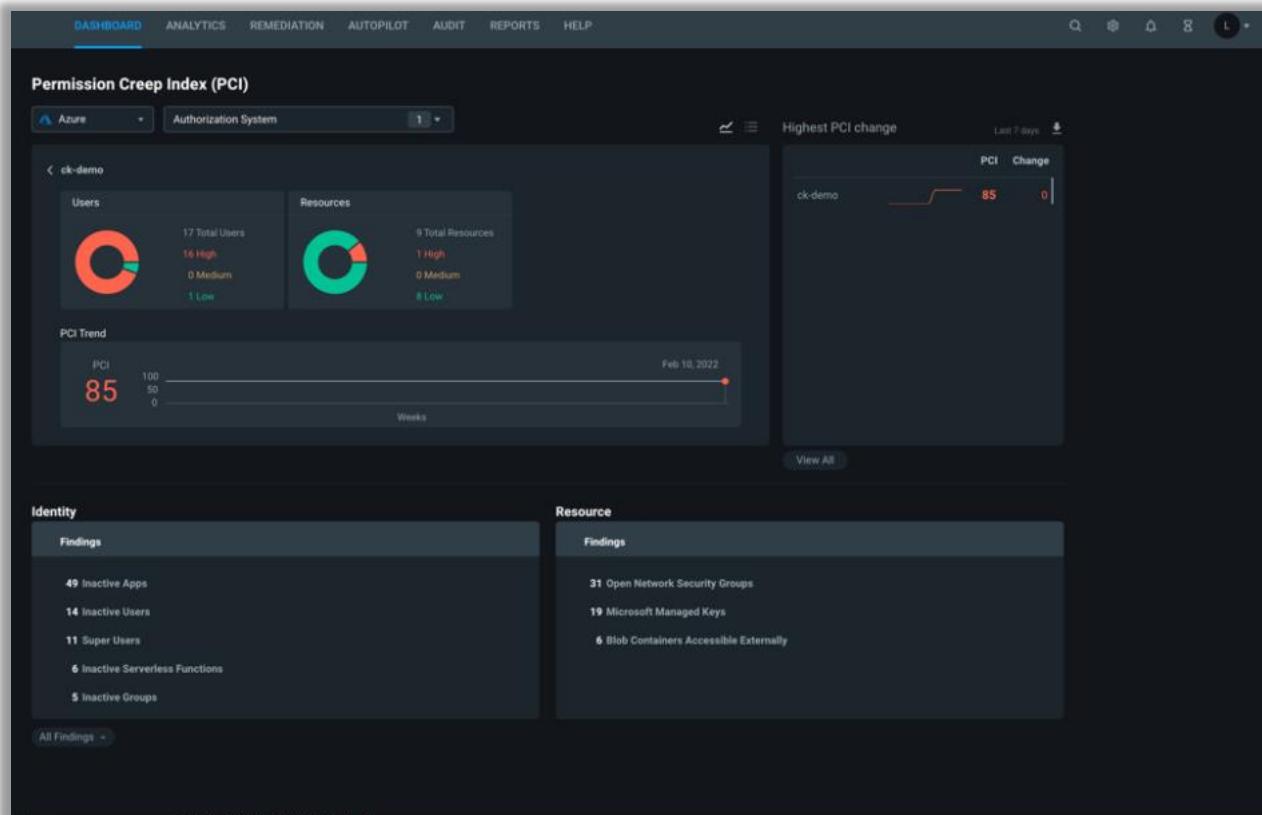


Increased complexity for IAM and security teams to manage permissions across multicloud environments



Increased risk of breach from accidental or malicious permission mis-use

Entra Permissions Management (EPM) Portal



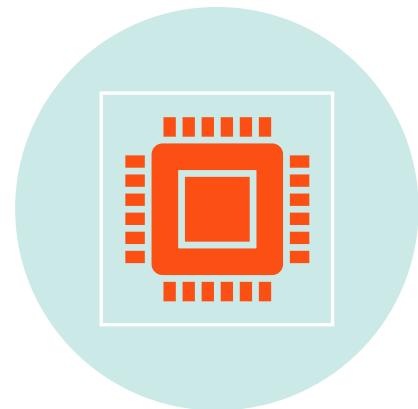
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go Do's

4. Strengthen Endpoints



Migrate to Entra ID joined devices



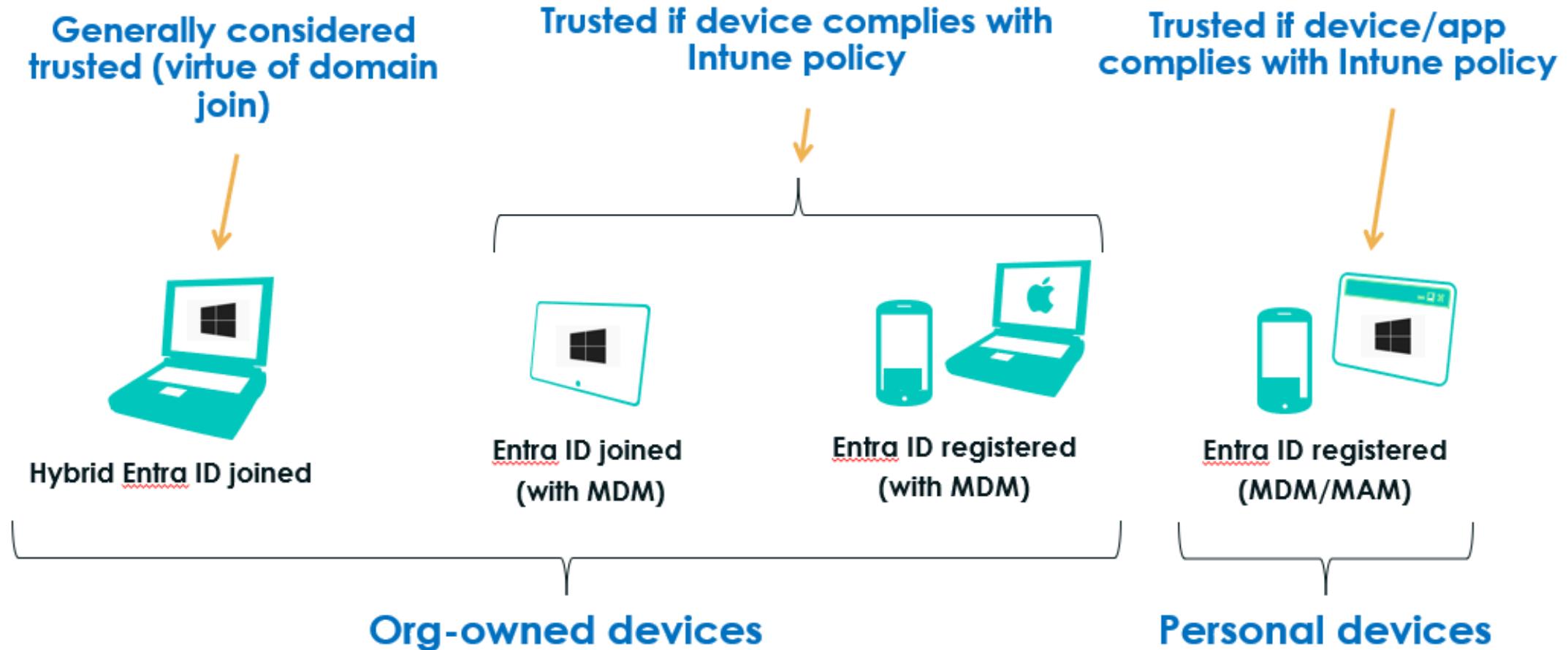
Manage devices with an MDM



Enhance device security with Microsoft Defender for Endpoint



Device States in Entra ID



Migrate from HEIDJ to EIDJ devices

- Decouple device management requirements from needing line-of-sight to Domain Controllers
 - E.g. Password changed in Entra ID, but I need the local cached password to update
- Simplify modern device deployment (aka Autopilot)
 - Out-of-the-box enroll in MDM and setup Windows Hello for Business
- Better security posture
 - EIDJ + MDM > HEIDJ

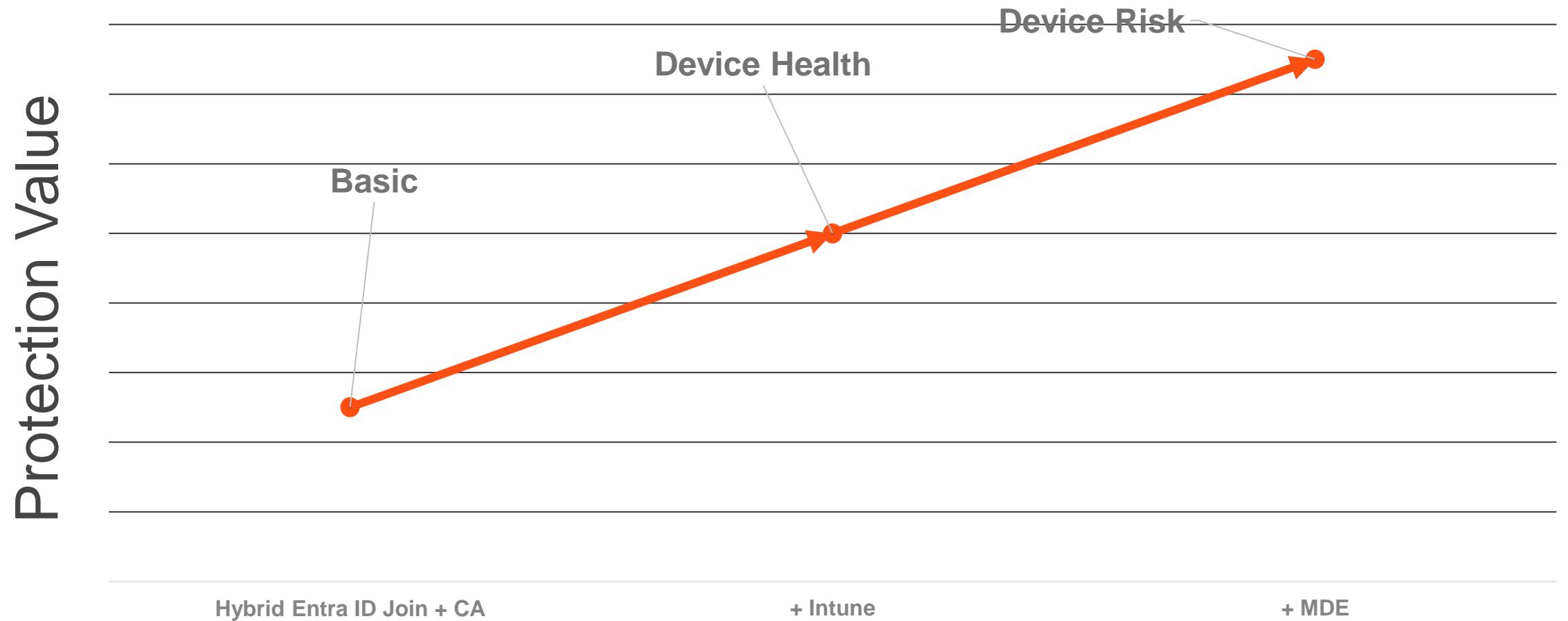
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Stages of Device-based Conditional Access



Device States in Entra ID

Ph0: Prep

Prep pilot,
HEIDJ existing
devices

Ph1: Pilot

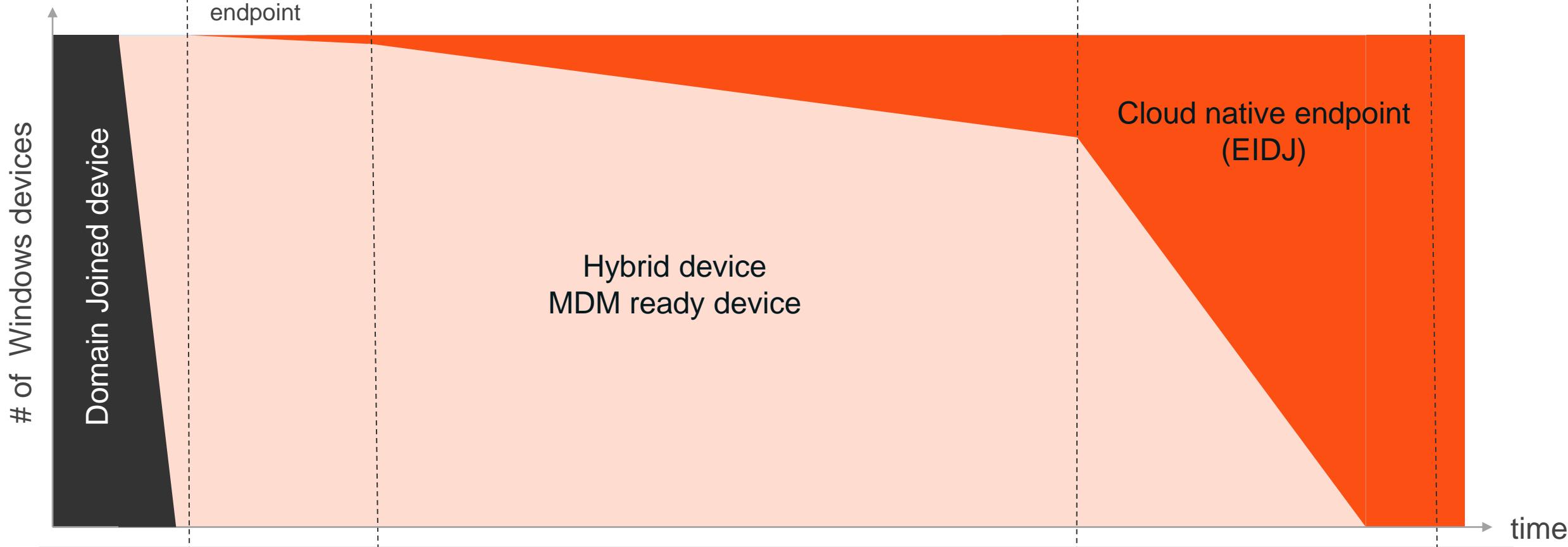
Small group
starts using
cloud native
endpoint

Ph2: Scale deployment

New device for all users gets EIDJ
(aka no more Domain Join)

Ph3: (optional) Velocity migration

Convert existing DJ/HEIDJ
devices to EIDJ via reset



Common Migration “Gotchas”

- GPO transition – one of the more challenging aspects of the migration
 - Need to move all policy and management to the MDM, leverage Intune Group Policy analytics
- “My users can’t SSO to on-premises resources, like printers and file shares”
 - Common perception, but its not true!
 - SSO to on-premises works for both password and Windows Hello for Business
 - Learn how it works at <https://aka.ms/EIDJonpremSSO>

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Strengthen Devices Strategy

1. Register your devices with Entra ID

2. Define MDM compliance policies for your devices

3. Enroll devices into MDM and apply policies

4. Configure Conditional Access policies to require compliant devices

5. Integrate Endpoint Threat Detection solution with compliance policies

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

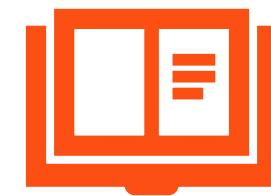
5. Use your Log Data



Establish a baseline of normal behavior in your environment

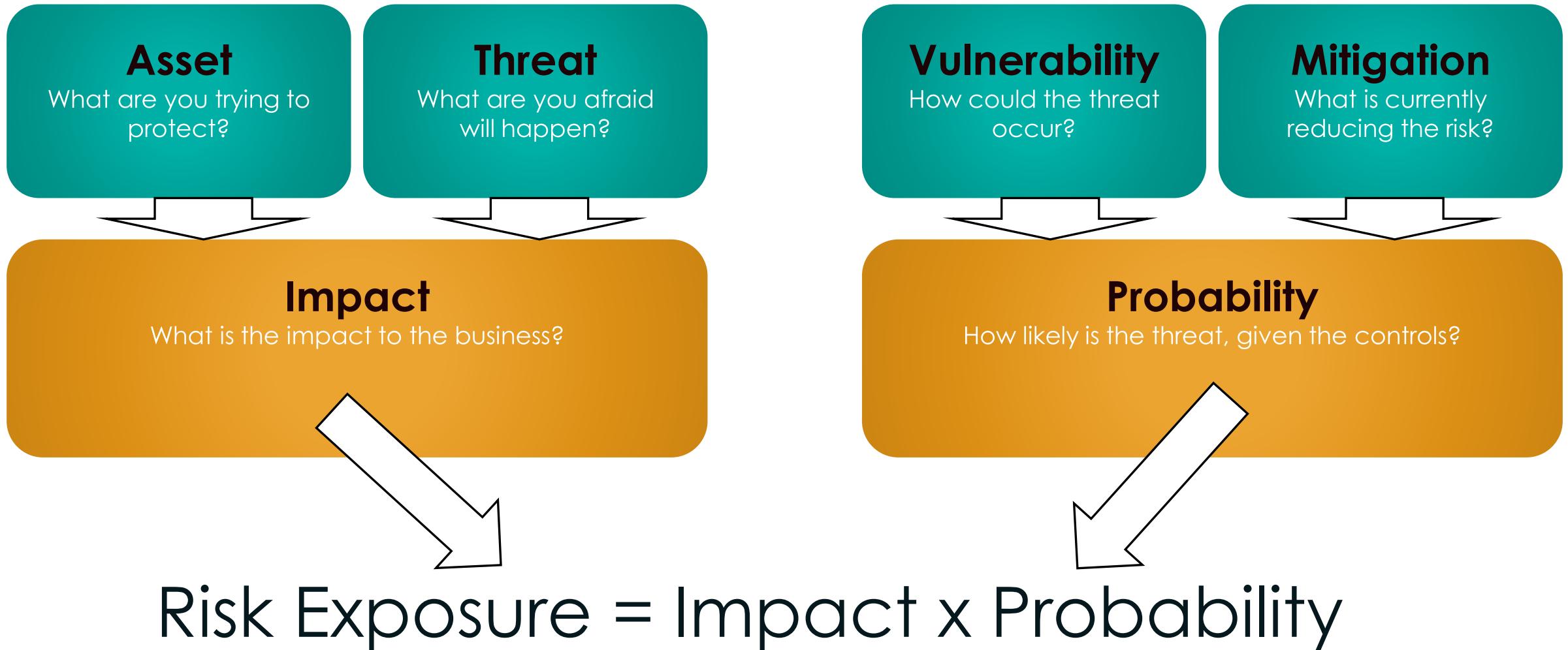


Leverage Microsoft Sentinel

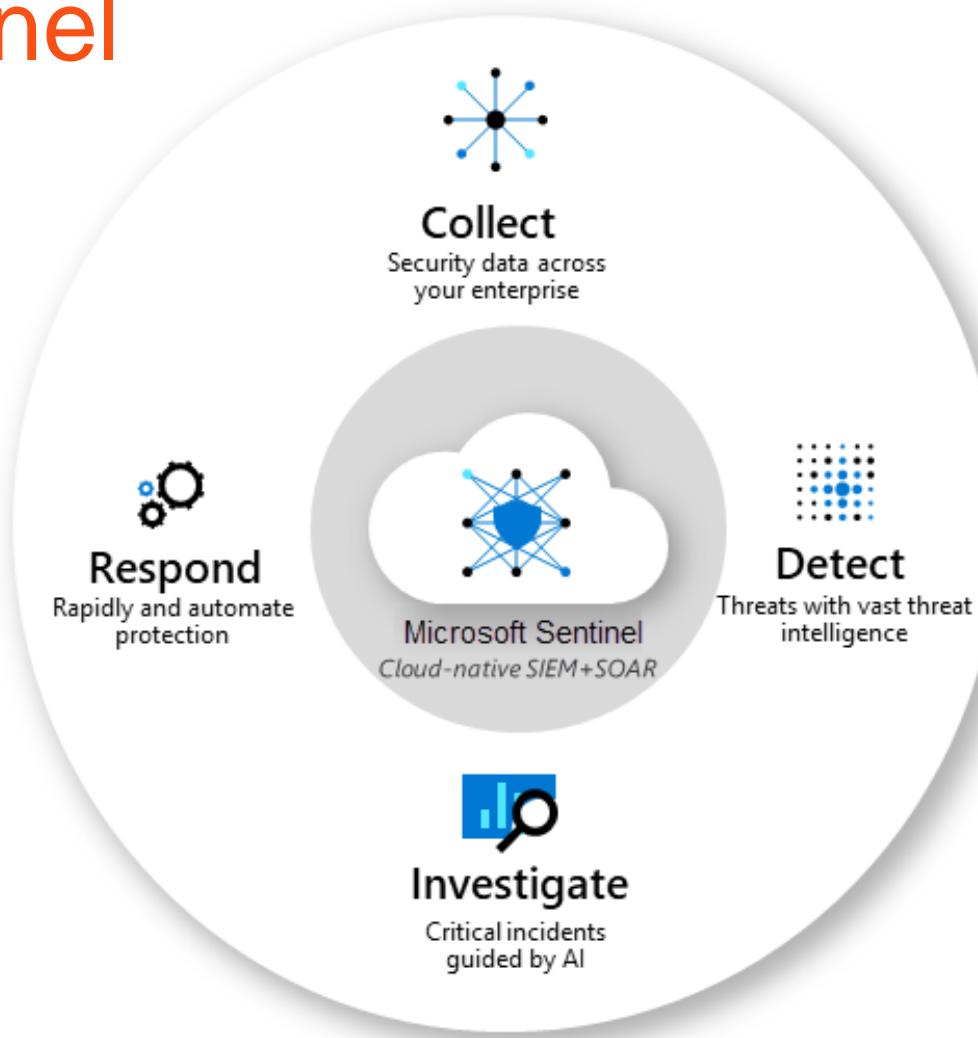


Read our SecOps Guide:
aka.ms/aadsecopsguide

Prioritize based on risk



Microsoft Sentinel



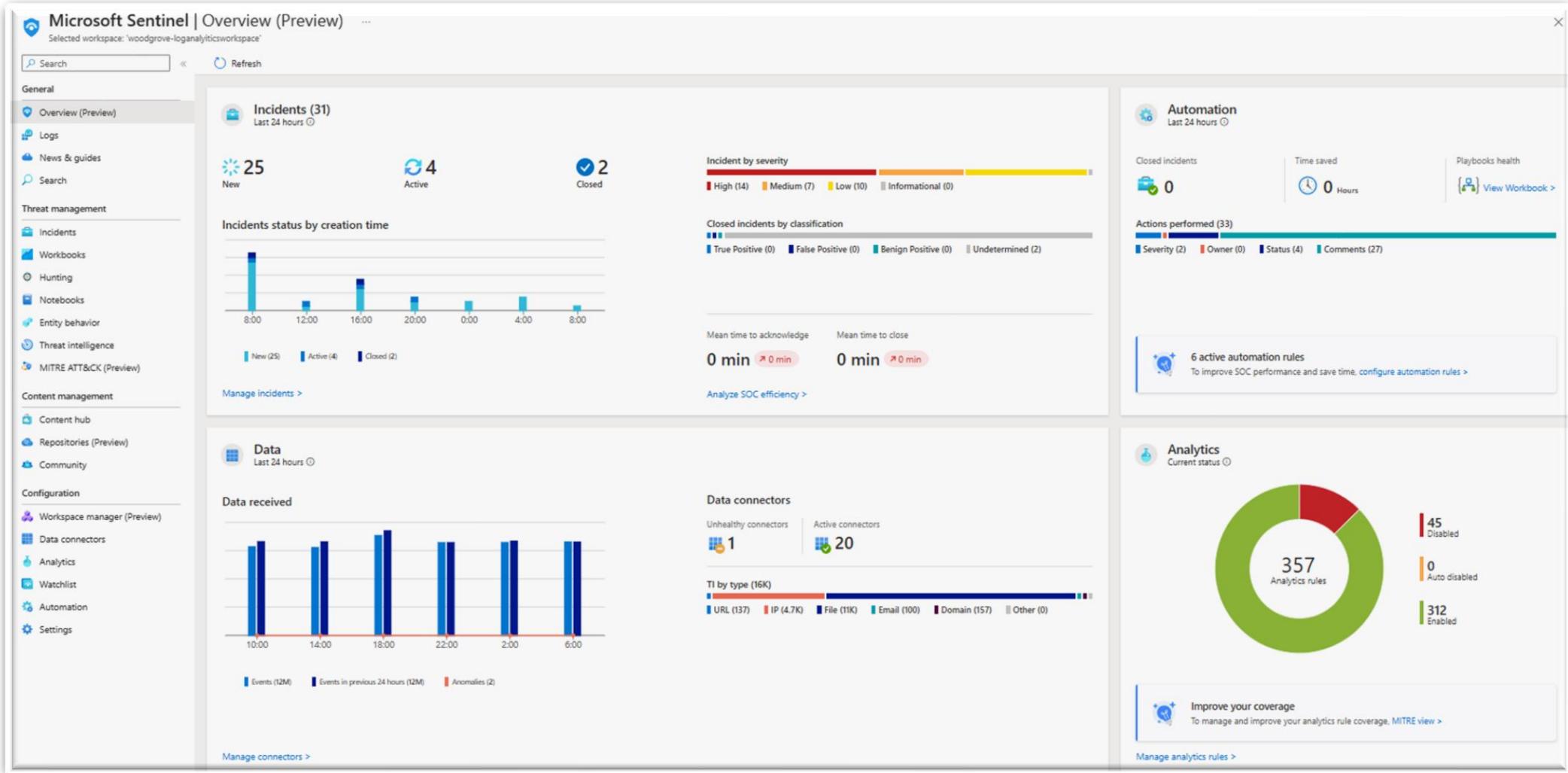
Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Microsoft Sentinel portal



Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

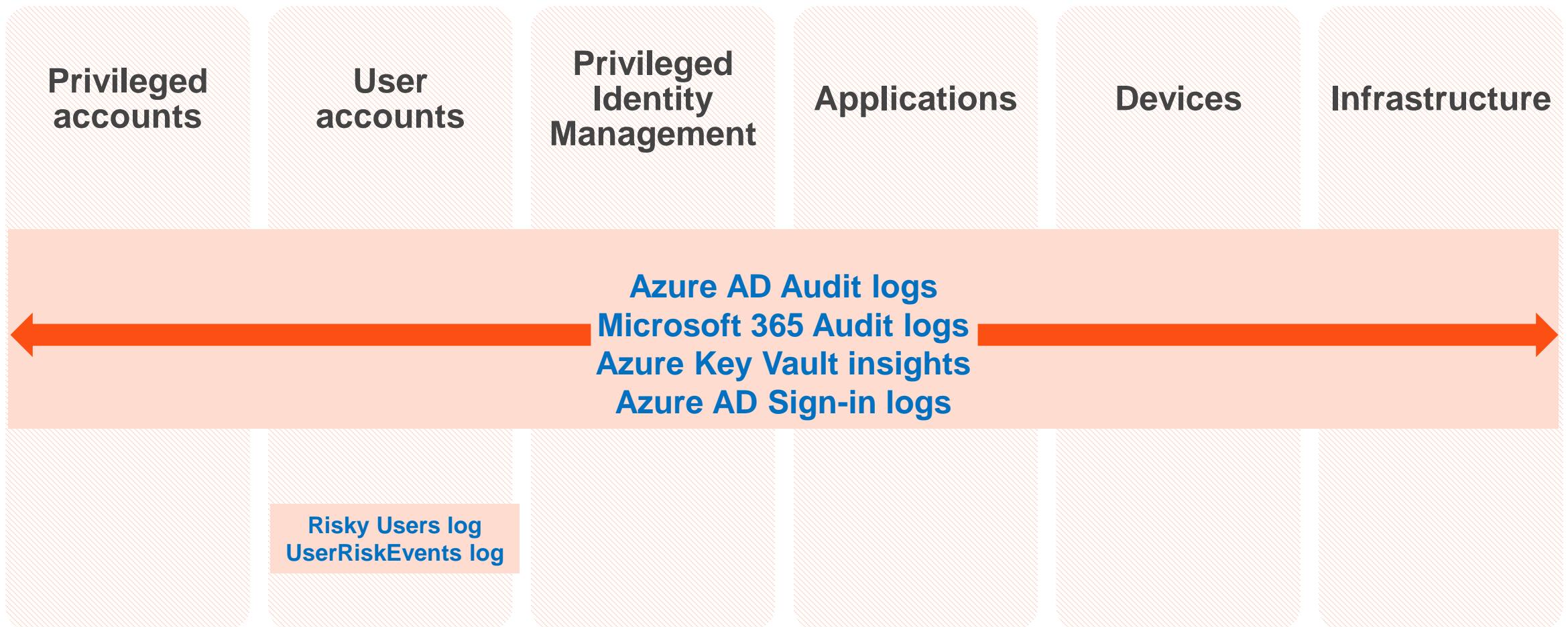
Go-Dos

SecOps guide scope

- Password audit and strategy recommendations
- Overview of the tools available for hybrid and cloud Azure environments
- SIEM configuration guidance
- Monitoring and alerting strategies for:-
 - User accounts
 - Privileged accounts
 - Privileged Identity Management
 - Applications
 - Devices
 - Infrastructure

aka.ms/aadsecopsguide

Log files to monitor



Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

Go-Dos

Strengthen Identities

Deploy strong authentication methods

Leverage **Conditional Access** and Identity Protection

Integrate Applications

Integrate applications with Entra ID, Entra SSE

Protect Applications with **Defender for Cloud Apps** and Purview

Adopt Least Privilege

Minimize user access with Just-In-time and Just-Enough Access (JIT/JEA)

Leverage **PIM** and Entra Permissions Management

Strengthen Endpoints

Migrate to EIDJ devices

Leverage **Microsoft Intune** and **Microsoft Defender for Endpoint**

Use your log data

Establish a baseline of normal behavior

Leverage **Microsoft Sentinel**

Read the SecOps guide:
aka.ms/aadsecopsguide

Introduction to ZT

ZT Principles + Architecture

5 Zero Trust Steps

Go-Dos

References

- aka.ms/NISTZeroTrust
- aka.ms/ztmodel
- aka.ms/EIDJonpremSSO
- aka.ms/aadSecOpsGuide
- <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths>
- <https://learn.microsoft.com/en-us/azure/global-secure-access/overview-what-is-global-secure-access>
- <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>
- <https://www.hypr.com/security-encyclopedia/notpetya>
- <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>



Questions?

Slides found at aka.ms/5stepsZT

Thank you!

Slides found at aka.ms/5stepsZT