Conditional Access Configured for Zero Trust

- Claus Jespersen
- Principal Security Consultant
- Microsoft ISD, AC & AI
- Twitter: @claus_jespersen
- LinkedIn

Official sponsors

PATCH MY PC

RECAST SOFTWARE

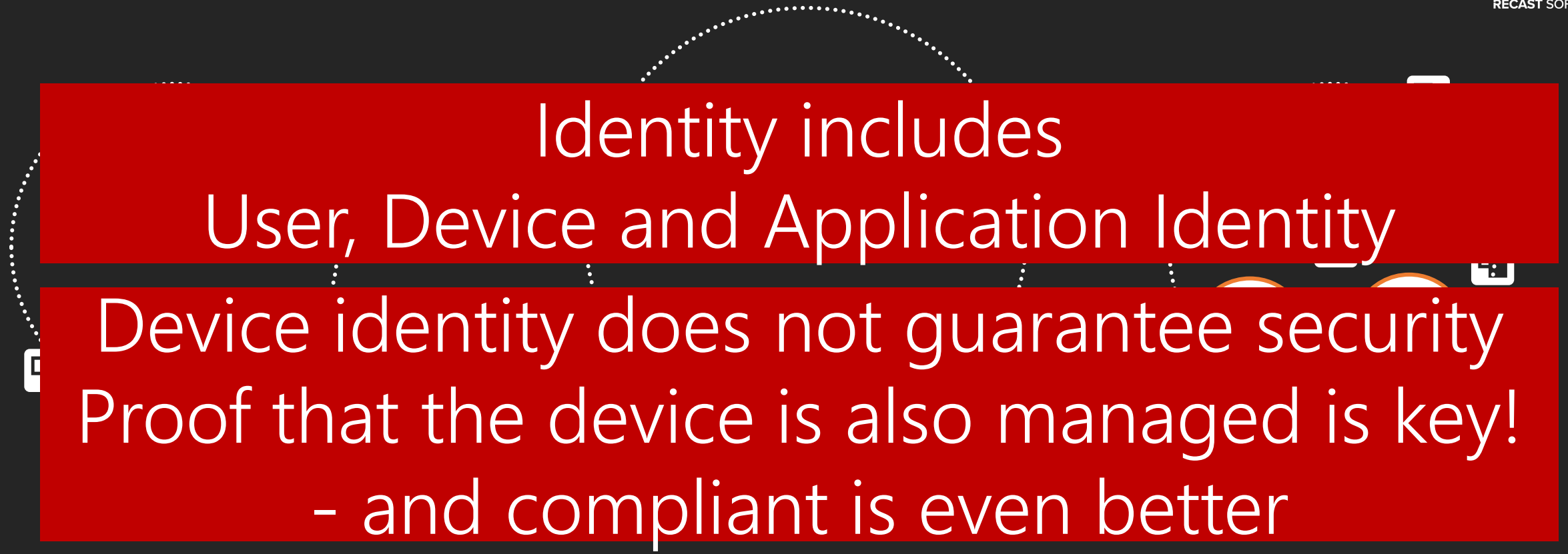
NORDIC — VIRTUAL SUMMIT —

Agenda

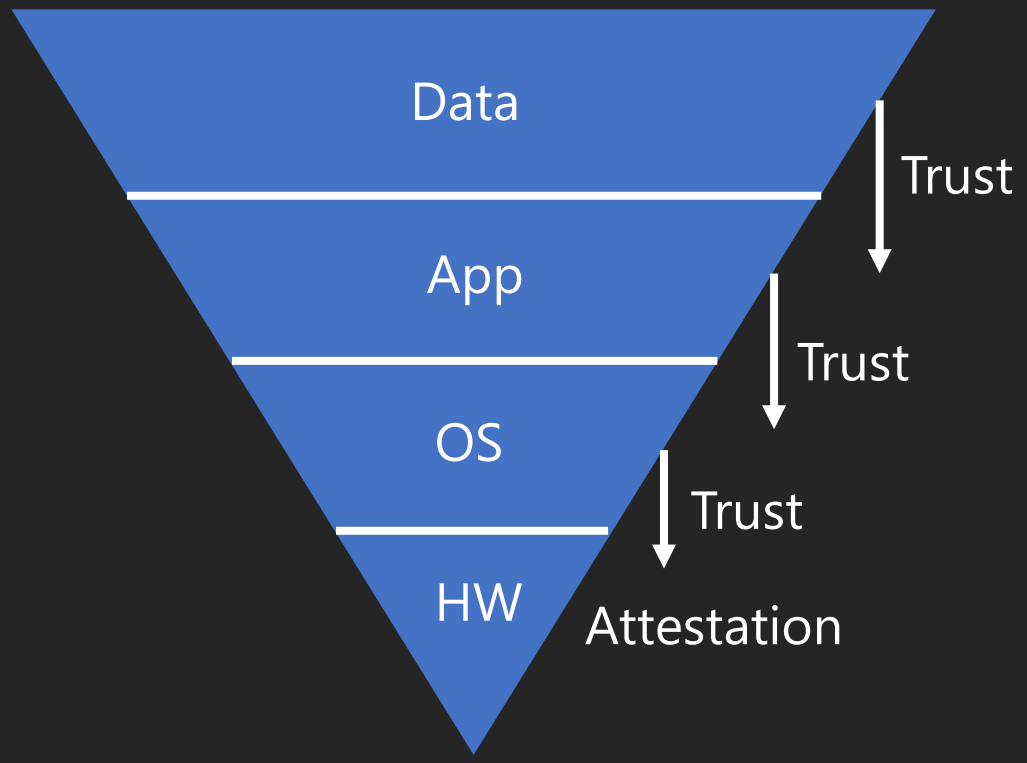
NORDIC
– VIRTUAL SUMMIT –

- Zero Trust principles related to Conditional Access
- Conditional Access Architecture
- Conditional Access Framework

Identity as the control plane



Importance of the physical device chain of trust



What I have learned so far..

Confidentiality

"When the right thing to do is the easiest thing to do,
you get the right level of security"

Companies not realizing this principle are more susceptible to Shadow-IT

Integrity

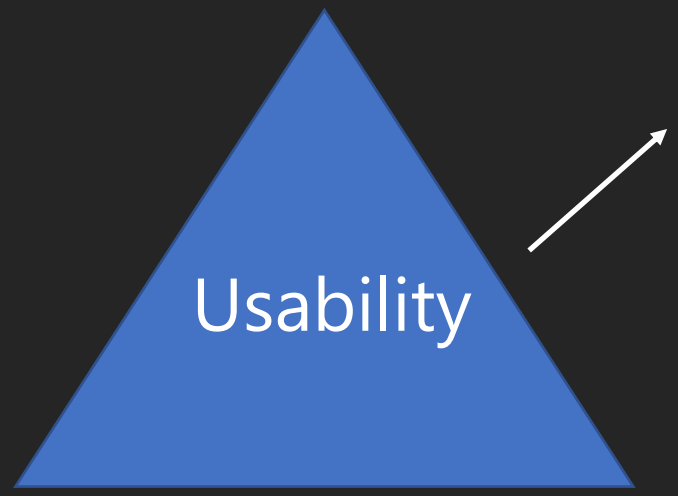
Availability

Usability

Functionality

Cost

Zero Trust Principles - Usability



Work from anywhere
Work from different devices
Access resources directly
Easy password-less login
Single Sign On based on AAD
Adaptive risk-based access control

Zero Trust principles related to CA

NORDIC
– VIRTUAL SUMMIT –

Verify explicitly

- Move control plane to the cloud (Integrate app with AAD and protect using Conditional Access)
- Consider all clients as external (even so you are connected to Corp net)

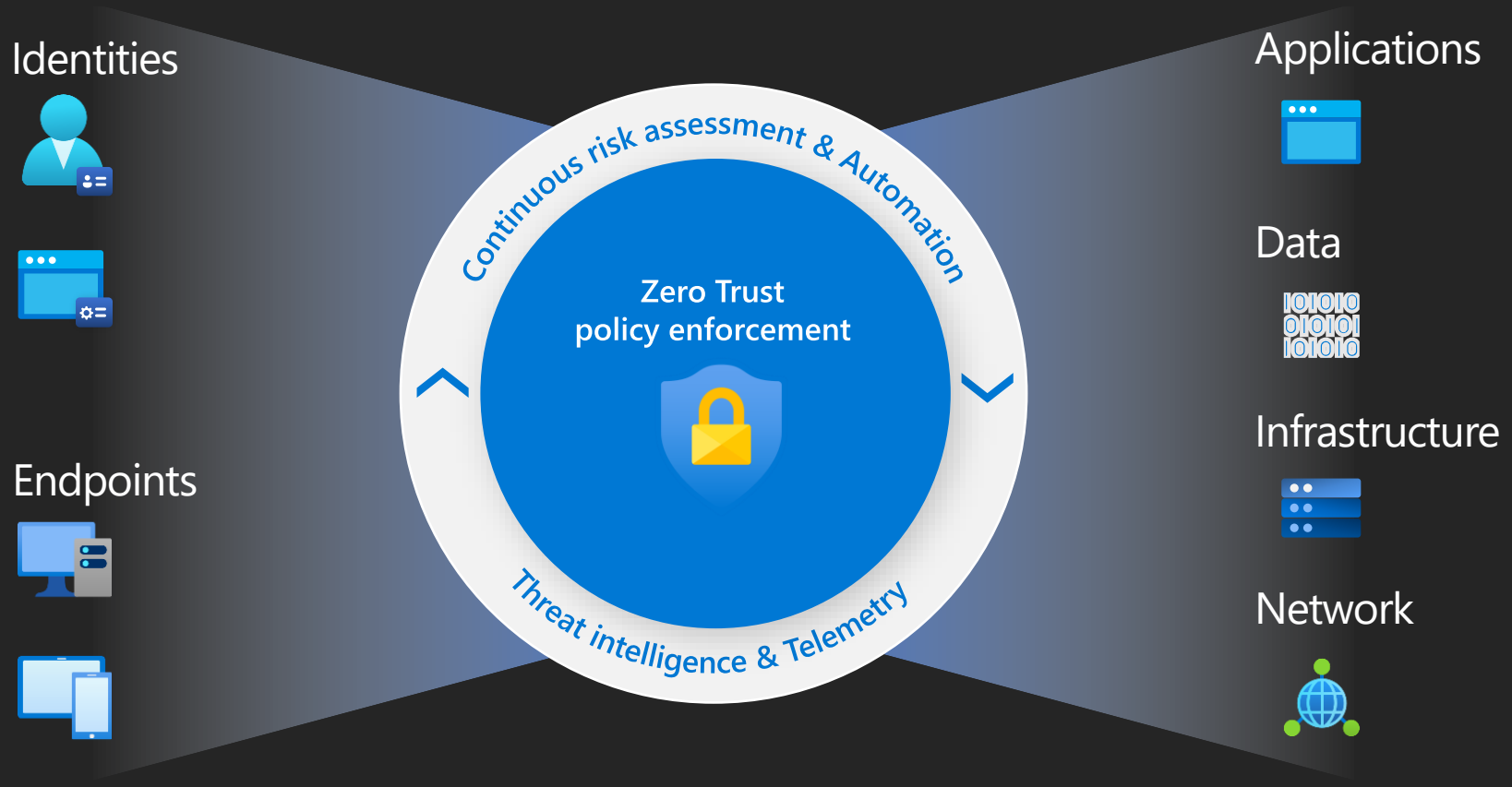
Least privileged access

- Evaluate access based on compliance and risk (including user risk, sign-in risk and device risk)
- Use the following access priorities
  - Access the resource directly protected by Conditional Access
  - Publish access to resource using solutions like Citrix, ZScaler or Microsoft App Proxy, protected by CA
  - Use CA based VPN to get access to the resource, constrained access protected by CA

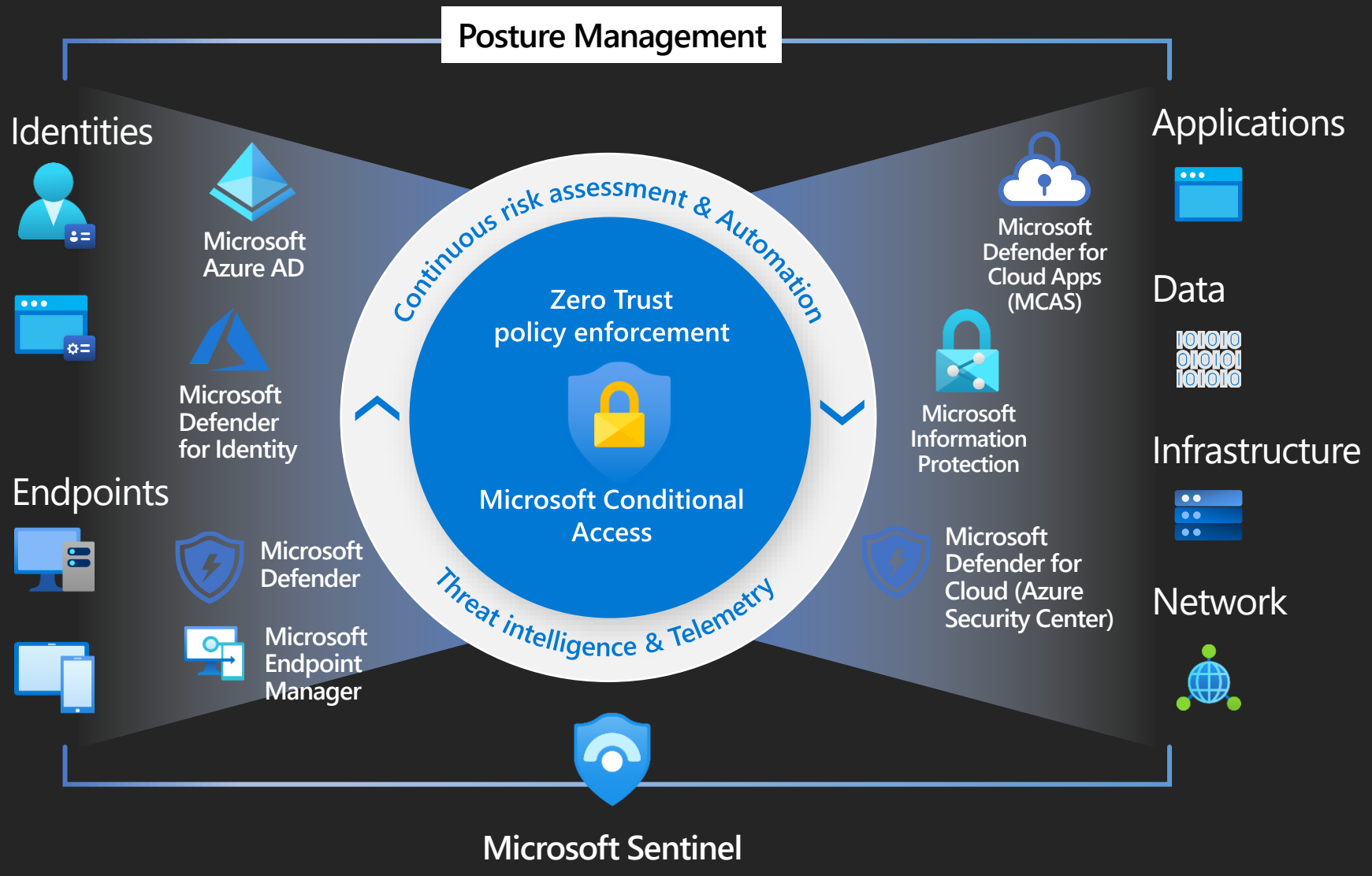
Assume Breach

- Segment network infrastructure, using named locations where device identity not known
- Minimize use of Enterprise PKI
- Migrate apps and SSO from AAD and ADFS to PHS
- Minimize dependencies on DCs using “Cloud KDC”
- Move management plane to the cloud (Manage devices with MEM which enables compliancy)

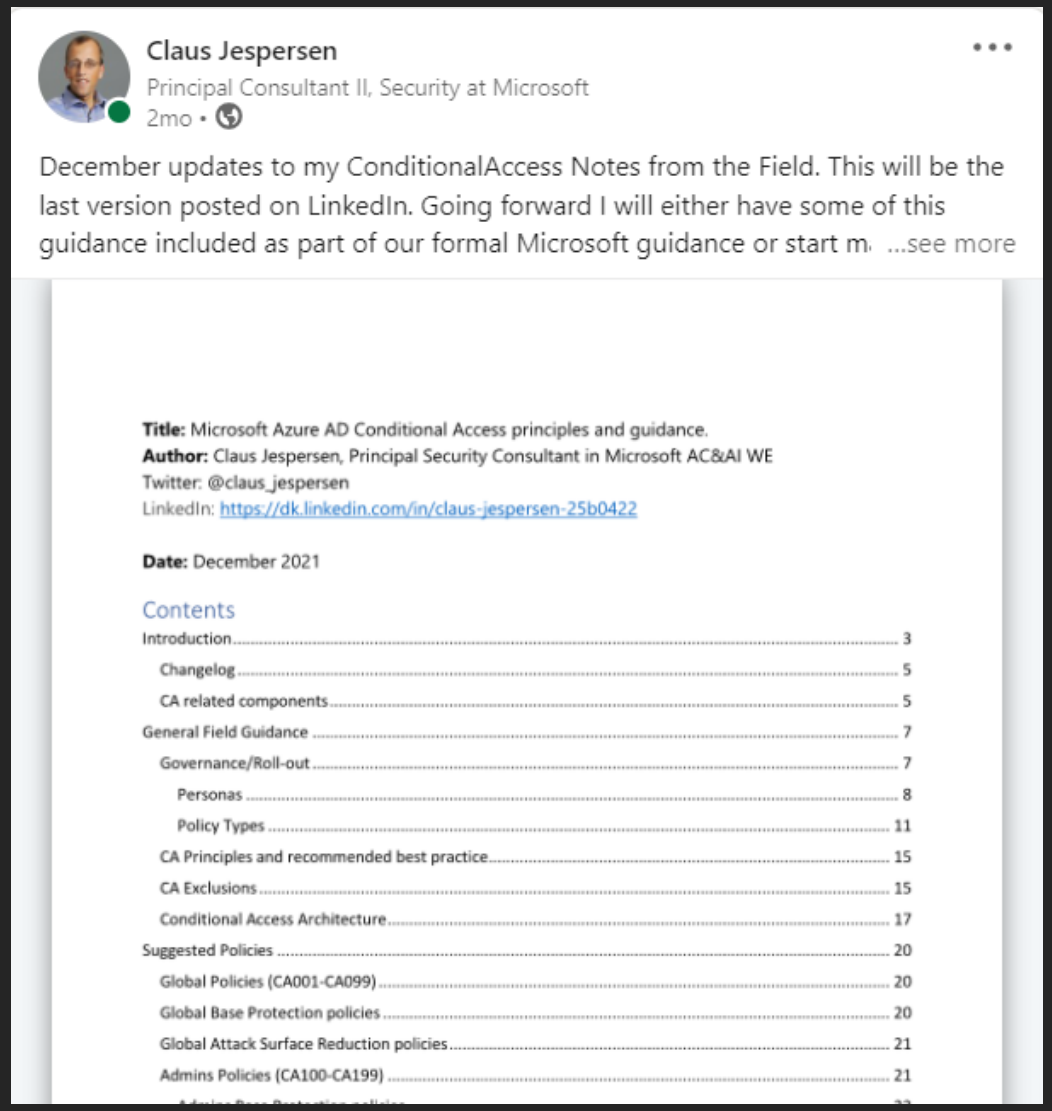
Zero Trust Approach from Microsoft

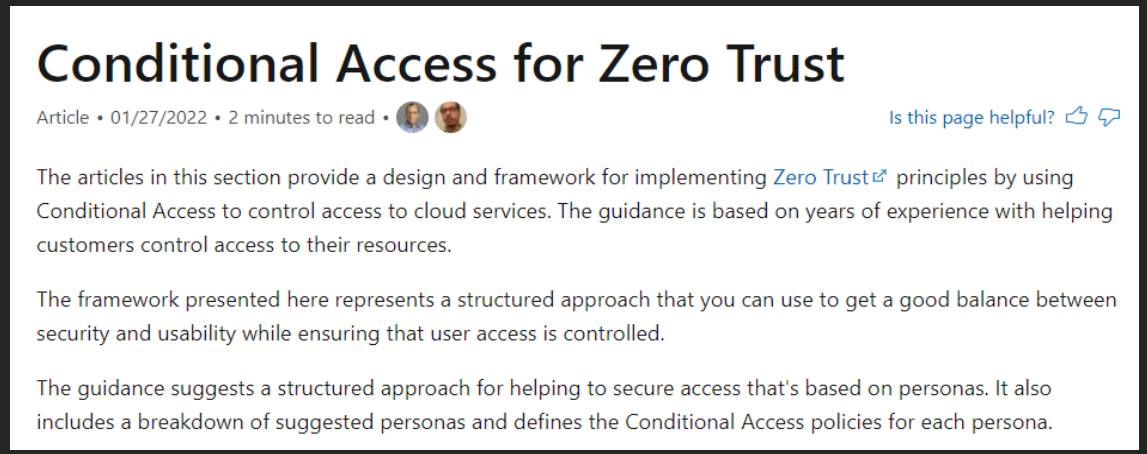


Microsoft Zero Trust Capabilities



CA Guidance for Zero Trust



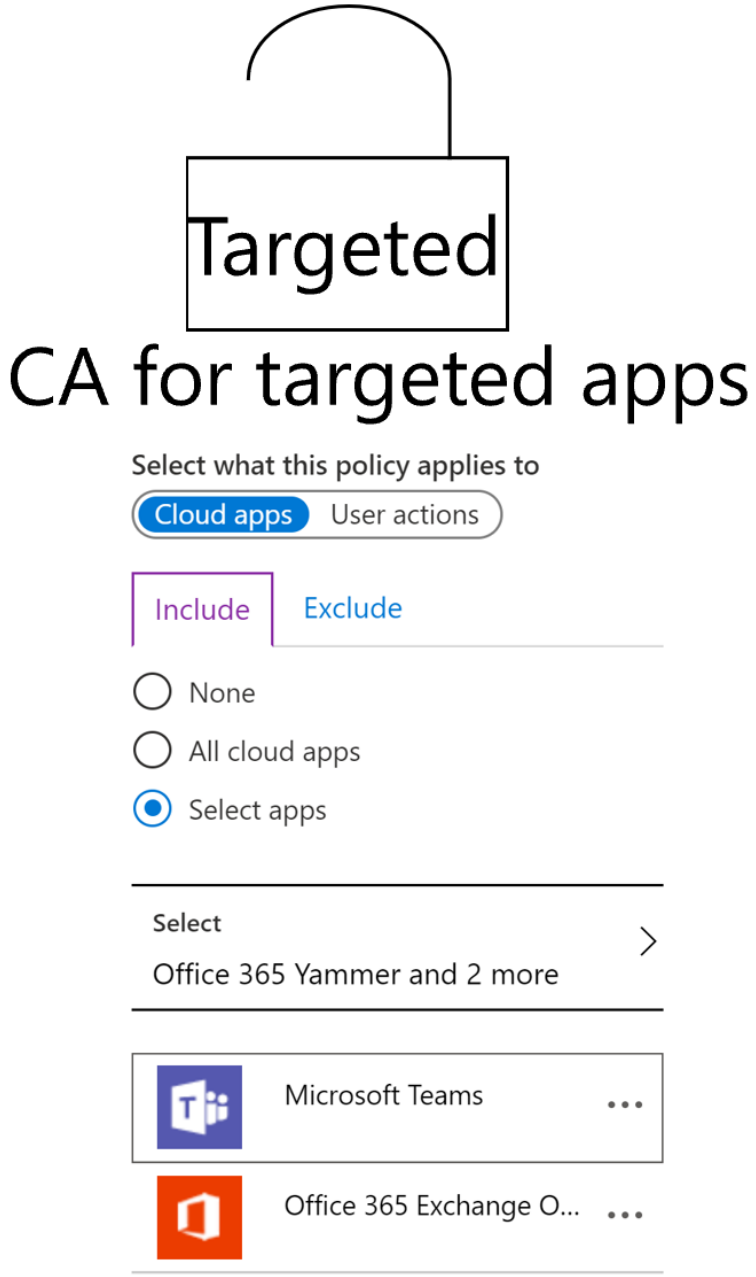


Notes from the field: LinkedIn post:
https://www.linkedin.com/posts/claus-jespersen-25b0422_conditional-access-guidance-december-2021-activity-6872879151271993344-u7Vd

Azure Architecture center design guidance:
Conditional Access for Zero Trust - Azure Architecture Center | Microsoft Docs

Spreadsheet with suggested policies
https://arch-center.azureedge.net/Conditional-Access-policies-for-personas.xlsx

Defining CA architecture type



Apps not protected using Targeted Architecture

- ea.azure.com
- security.microsoft.com
- portal.office.com
- aka.ms/devicelogin
- AAD Graph endpoints

CA Architectures - Pros/Cons

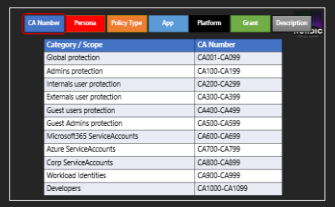
NORDIC
– VIRTUAL SUMMIT –

Area	Targeted Architecture	Zero Trust Architecture
Usability		
Functionality		
Security		
Maintainability		

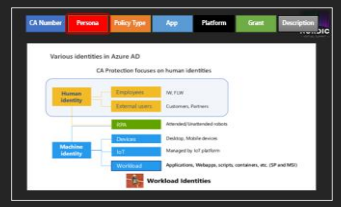
Conditional Access Framework

NORDIC
– VIRTUAL SUMMIT –

CA Number	Persona	Policy Type	App	Platform	Grant	Description



Category / Scope	CA Number
Global protection	CA001-CA099
Admins protection	CA100-CA199
Internals user protection	CA200-CA299
Externals user protection	CA300-CA399
Guest users protection	CA400-CA499
Guest Admins protection	CA500-CA599
Microsoft365 ServiceAccounts	CA600-CA699
Azure ServiceAccounts	CA700-CA799
Corp ServiceAccounts	CA800-CA899
Workload identities	CA900-CA999
Developers	CA1000-CA1099



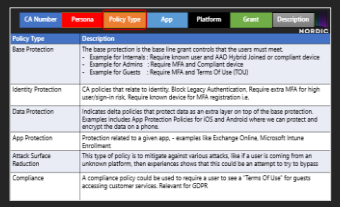
Various identities in Azure AD

CA Protection focuses on human identities

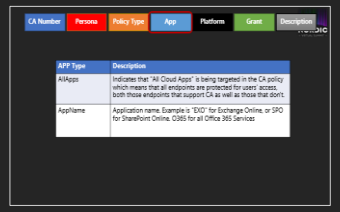
Human identity: Employees (NL FLW); External users: Customers, Partners

Machine identity: SPN: Attended/Unattended robots; Devices: Desktop, Mobile devices; IoT: Managed by IoT platform; Workload: Applications, Webapps, scripts, containers, etc. (SP and MSI)

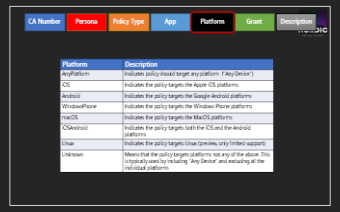
Workload identities



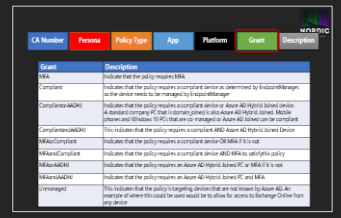
Policy Type	Description
Base Protection	The base protection is the base line grant controls that the users must meet. - Example for Internals : Require known user and AAD Hybrid Joined or compliant device - Example for Admins : Require MFA and Compliant device - Example for Guests : Require MFA and Terms Of Use (TOU)
Identity Protection	CA policies that relate to identity. Block Legacy Authentication. Require extra MFA for high user/sign-in risk. Require known device for MFA registration i.e.
Data Protection	Indicates data policies that protect data at an extra layer on top of the base protection. Examples includes App Protection Policies for iOS and Android where we can protect and encrypt the data on a phone.
App Protection	Protection related to a given app, - examples like Exchange Online, Microsoft Intune Enrollment
Attack Surface Reduction	This type of policy is to mitigate against various attacks, like if a user is coming from an unknown platform, then experiences shows that this could be an attempt to try to bypass
Compliance	A compliance policy could be used to require a user to see a "Terms Of Use" for guests accessing customer services. Relevant for GDPR



APP Type	Description
AllApps	Indicates that "All Cloud Apps" is being targeted in the CA policy which means that all endpoints are protected for users' access, both those endpoints that support CA as well as those that don't.
AppName	Application name. Example is "EXO" for Exchange Online, or SPO for SharePoint Online. O365 for all Office 365 Services



Platform	Description
AnyPlatform	Indicates policy should target any platform ('Any Device')
iOS	Indicates the policy targets the Apple iOS platforms
Android	Indicates the policy targets the Google Android platforms
WindowsPhone	Indicates the policy targets the Windows Phone platforms
macOS	Indicates the policy targets the MacOS platforms
iOSAndroid	Indicates the policy targets both the iOS and the Android platforms
Linux	Indicates the policy targets Linux (preview, only limited support)
Unknown	Means that the policy targets platforms not any of the above. This is typically used by including 'Any Device' and excluding all the individual platforms



Grant	Description
MFA	Indicates that the policy requires MFA
Compliant	Indicates that the policy requires a compliant device as determined by IntuneMDM/Manager, so the device needs to be managed by IntuneMDM/Manager
CompliantorAADHJ	Indicates that the policy requires a compliant device or Azure AD Hybrid Joined device. A standard company PC that is domain joined is also Azure AD Hybrid Joined. Mobile phones and Windows 10 PCs that are co-managed or Azure AD Joined can be compliant
CompliantandAADHJ	This indicates that the policy requires a compliant AND Azure AD Hybrid Joined Device
MdmCompliant	Indicates that the policy requires a compliant device OR MFA if it is not
MfaandCompliant	Indicates that the policy requires a compliant device AND MFA to satisfy this policy
MfaorAADHJ	Indicates that the policy requires an Azure AD Hybrid Joined PC or MFA if it is not
MfaandAADHJ	Indicates that the policy requires an Azure AD Hybrid Joined PC and MFA
Unmanaged	This indicates that the policy is targeting devices that are not known by Azure AD. An example of where this could be used would be to allow for access to Exchange Online from any device

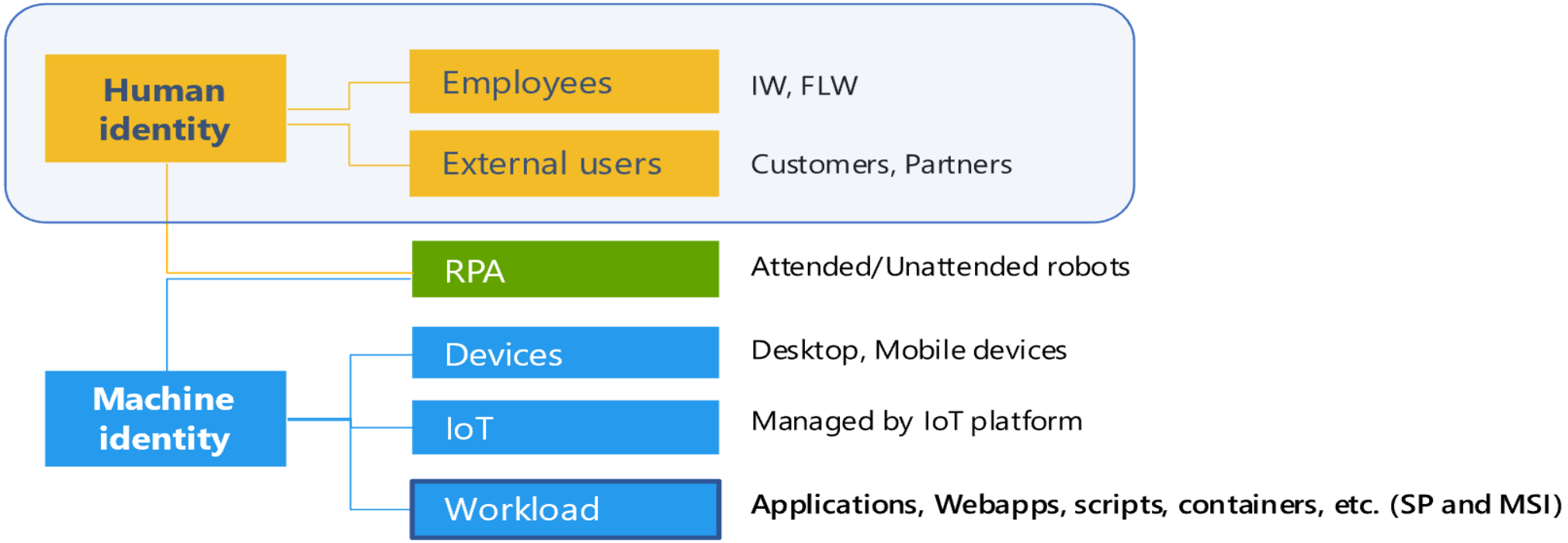
CA Number | Persona | Policy Type | App | Platform | Grant | Description

NORDIC
– VIRTUAL SUMMIT –

Category / Scope	CA Number
Global protection	CA001-CA099
Admins protection	CA100-CA199
Internals user protection	CA200-CA299
Externals user protection	CA300-CA399
Guest users protection	CA400-CA499
Guest Admins protection	CA500-CA599
Microsoft365 ServiceAccounts	CA600-CA699
Azure ServiceAccounts	CA700-CA799
Corp ServiceAccounts	CA800-CA899
Workload Identities	CA900-CA999
Developers	CA1000-CA1099

Various identities in Azure AD

CA Protection focuses on human identities



Workload Identities

Global “Persona” serves two purposes

1) “Catch All” – block access for non-persona requests
2) Policies that should apply to all personas

Policy Type	Description
Base Protection	The base protection is the base line grant controls that the users must meet. - Example for Internals : Require known user and AAD Hybrid Joined or compliant device - Example for Admins : Require MFA and Compliant device - Example for Guests : Require MFA and Terms Of Use (TOU)
Identity Protection	CA policies that relate to identity. Block Legacy Authentication, Require extra MFA for high user/sign-in risk, Require known device for MFA registration i.e.
Data Protection	Indicates delta policies that protect data as an extra layer on top of the base protection. Examples includes App Protection Policies for iOS and Android where we can protect and encrypt the data on a phone.
App Protection	Protection related to a given app, - examples like Exchange Online, Microsoft Intune Enrollment
Attack Surface Reduction	This type of policy is to mitigate against various attacks, like if a user is coming from an unknown platform, then experiences shows that this could be an attempt to try to bypass
Compliance	A compliance policy could be used to require a user to see a "Terms Of Use" for guests accessing customer services. Relevant for GDPR

APP Type	Description
AllApps	Indicates that "All Cloud Apps" is being targeted in the CA policy which means that all endpoints are protected for users' access, both those endpoints that support CA as well as those that don't.
AppName	Application name. Example is "EXO" for Exchange Online, or SPO for SharePoint Online. O365 for all Office 365 Services

Platform	Description
AnyPlatform	Indicates policy should target any platform ("Any Device")
iOS	Indicates the policy targets the Apple iOS platforms
Android	Indicates the policy targets the Google Android platforms
WindowsPhone	Indicates the policy targets the Windows Phone platforms
macOS	Indicates the policy targets the MacOS platforms
iOSAndroid	Indicates the policy targets both the iOS and the Android platforms
Linux	Indicates the policy targets Linux (preview, only limited support)
Unknown	Means that the policy targets platforms not any of the above. This is typically used by including "Any Device" and excluding all the individual platforms

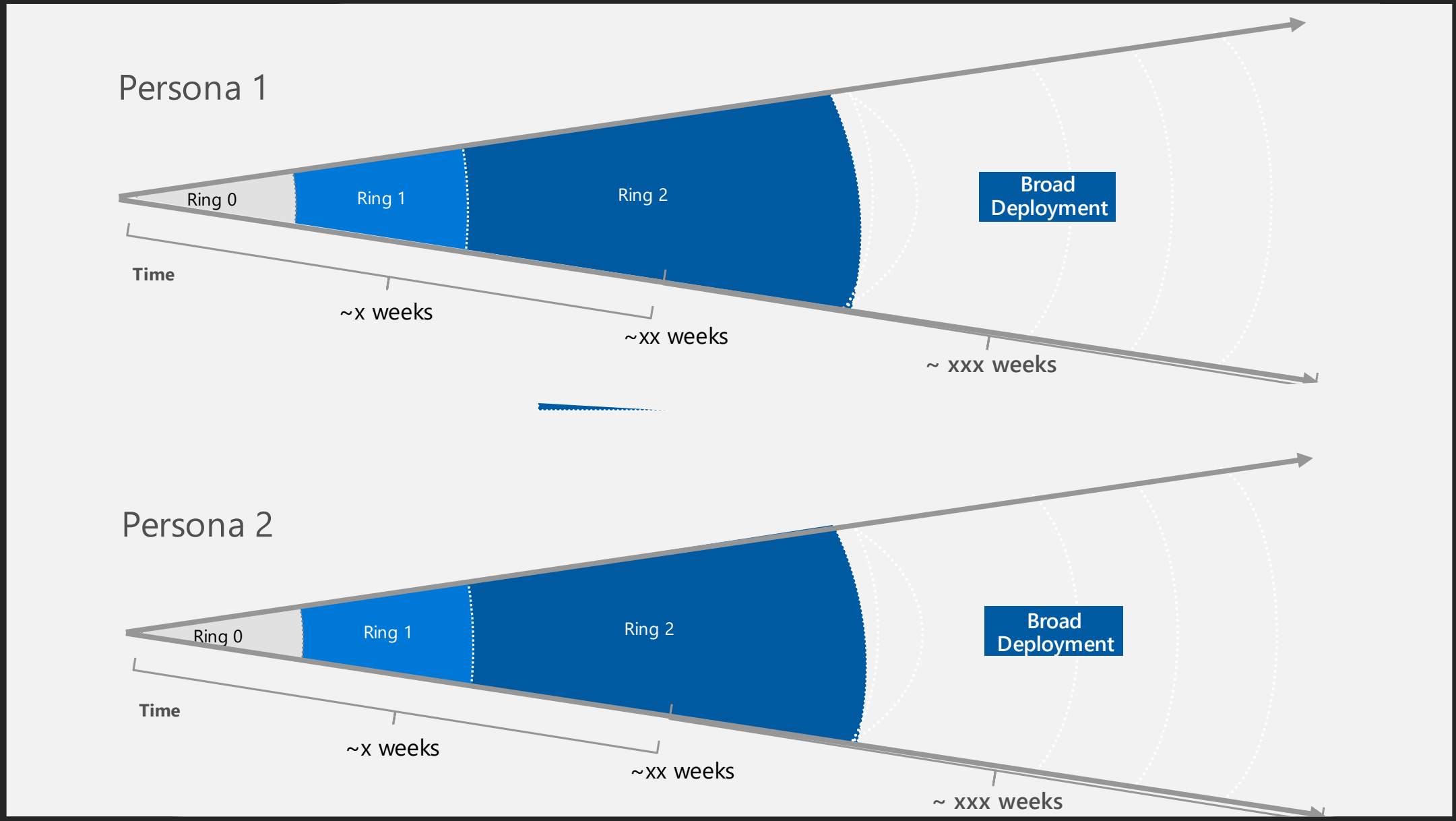
Grant	Description
MFA	Indicate that the policy requires MFA
Compliant	Indicates that the policy requires a compliant device as determined by EndpointManager, so the device needs to be managed by EndpointManager
CompliantorAADHJ	Indicates that the policy requires a compliant device or Azure AD Hybrid Joined device. A standard company PC that is domain joined is also Azure AD Hybrid Joined. Mobile phones and Windows 10 PCs that are co-managed or Azure AD Joined can be compliant
CompliantandAADHJ	This indicates that the policy requires a compliant AND Azure AD Hybrid Joined Device
MFAorCompliant	Indicates that the policy requires a compliant device OR MFA if it is not
MFAandCompliant	Indicates that the policy requires a compliant device AND MFA to satisfythis policy
MFAorAADHJ	Indicates that the policy requires an Azure AD Hybrid Joined PC or MFA if it is not
MFAandAADHJ	Indicates that the policy requires an Azure AD Hybrid Joined PC and MFA
Unmanaged	This indicates that the policy is targeting devices that are not known by Azure AD. An example of where this could be used would be to allow for access to Exchange Online from any device

Conditional Access Policies - Examples

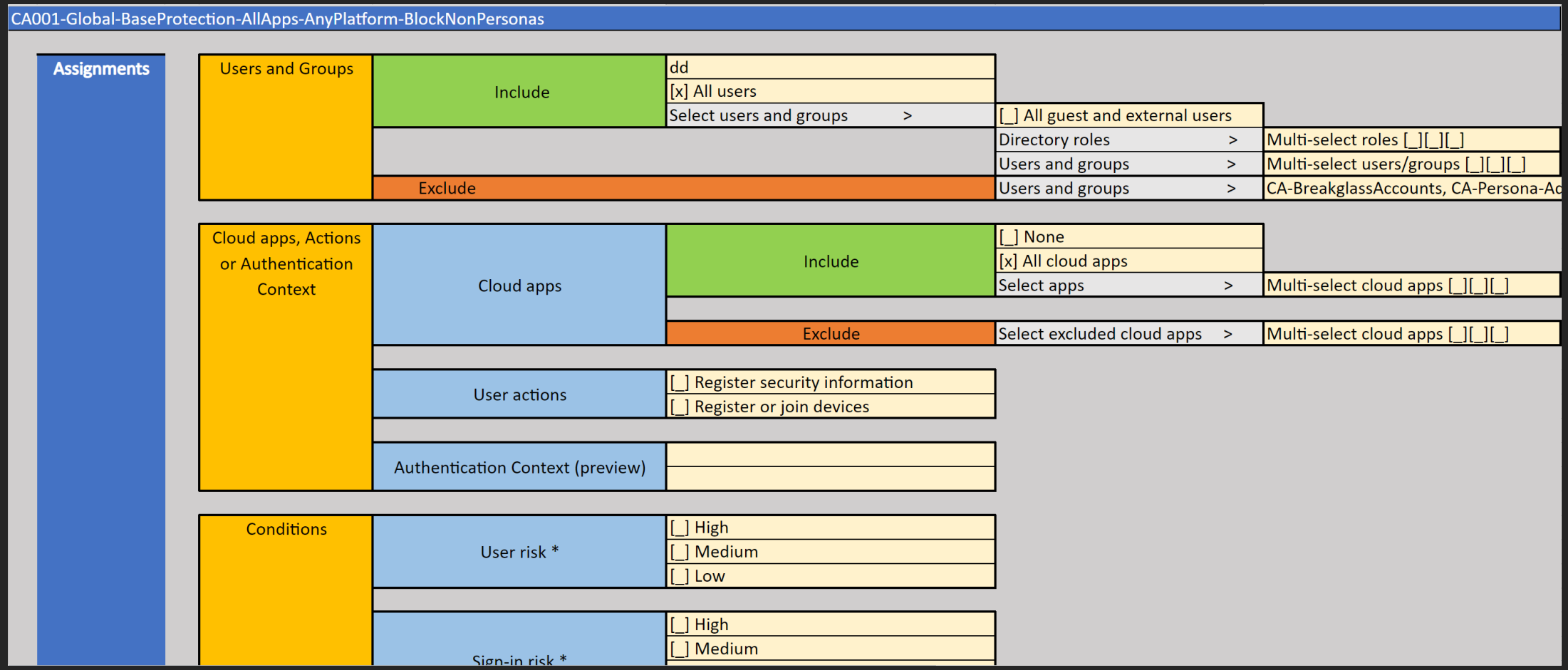
CA Number	Persona	Policy Type	App	Platform	Grant	Description

- CA001-Global-BaseProtection-AllApps-AnyPlatform-MFA
- CA002-Global-AttachSurfaceReduction-AllApps-AnyPlatform-BlockLegacyAuth
- CA100-Admins-BaseProtection-AllApps-AnyPlatforms-MFAandCompliant
- CA101-Admins-IdentityProtection-CombinedRegistration-Compliant
- CA200-Internals-BaseProtection-AllApps-AnyPlatform-AADHJorCompliant
- CA201-Internals-AppProtection-Windows365-AnyPlatform-MFA
- CA202-Internals-DataProtection-O365-Windows10-Unmanaged-DLPSessioncontrol
- CA203-Internals-AppProtection-O365-iOSAndroid-EMAppProtection
- CA204-Internals-AppProtection-SPO-iOSAndroid
- CA300-Externals-BaseProtection-AllApps-AnyPlatform-AADHJorCompliant
- CA303-Guests-Compliance-AllApps-AnyPlatform-RequireTOU
- CA404-GuestAdmins-Compliance-AllApps-AnyPlatform-RequireTOU

Conditional Access Deployment Model



Conditional Access Sample Policies



CA001-Global-BaseProtection-AllApps-AnyPlatform-BlockNonPersonas

Assignments					
Users and Groups	Include	dd			
		[x] All users			
		Select users and groups >	[_] All guest and external users		
			Directory roles >	Multi-select roles [_][_][_]	
			Users and groups >	Multi-select users/groups [_][_][_]	
	Exclude		Users and groups >	CA-BreakglassAccounts, CA-Persona-Ac	
Cloud apps, Actions or Authentication Context	Cloud apps	Include	[_] None		
			[x] All cloud apps		
			Select apps >	Multi-select cloud apps [_][_][_]	
		Exclude	Select excluded cloud apps >	Multi-select cloud apps [_][_][_]	
	User actions	[_] Register security information			
		[_] Register or join devices			
	Authentication Context (preview)				
Conditions	User risk *	[_] High			
		[_] Medium			
		[_] Low			
	Sign-in risk *	[_] High			
		[_] Medium			

https://arch-center.azureedge.net/Conditional-Access-policies-for-personas.xlsx

FAQ & Evals

Evals: https://stream.nordicvirtualsummit.com/feedback

A big thanks to our sponsors

NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

RECAST SOFTWARE

Thank you!

NORDIC
– VIRTUAL SUMMIT –

Please remember to fill out the evals!