# Conditional Access Configured for Zero Trust

- Claus Jespersen
- Principal Security Consultant
- Microsoft ISD, AC & Al
- Twitter: @claus\_jespersen
- <u>LinkedIn</u>

Official sponsors







NORDIC

- VIRTUAL SUMMIT -

### Agenda



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

### Identity as the control plane







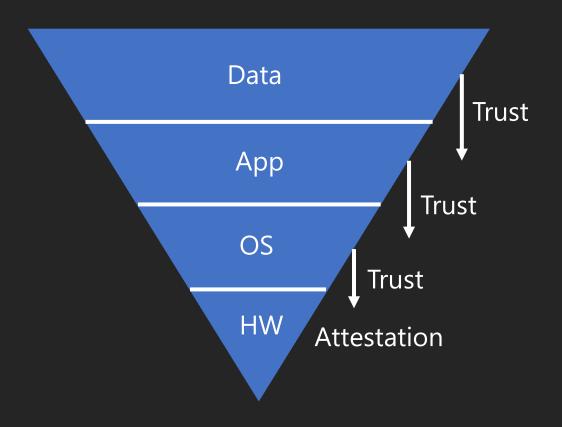
Identity includes
User, Device and Application Identity

Device identity does not guarantee security Proof that the device is also managed is key!

- and compliant is even better

## Importance of the physical device chain of trust





### What I have learned so far...

**C**onfidentiality





"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

<u>Integrity</u>

<u>A</u>vailability

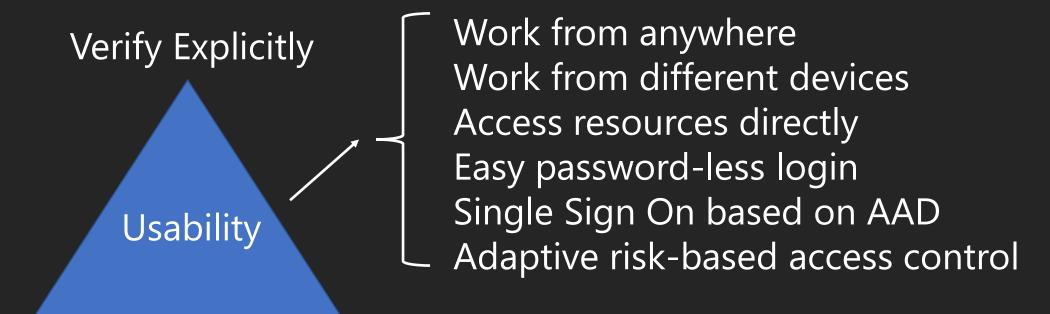


**Usability** 



### Zero Trust Principles - Usability





Assume Breach

Least Privileged Access

### Zero Trust principles related to CA



#### 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

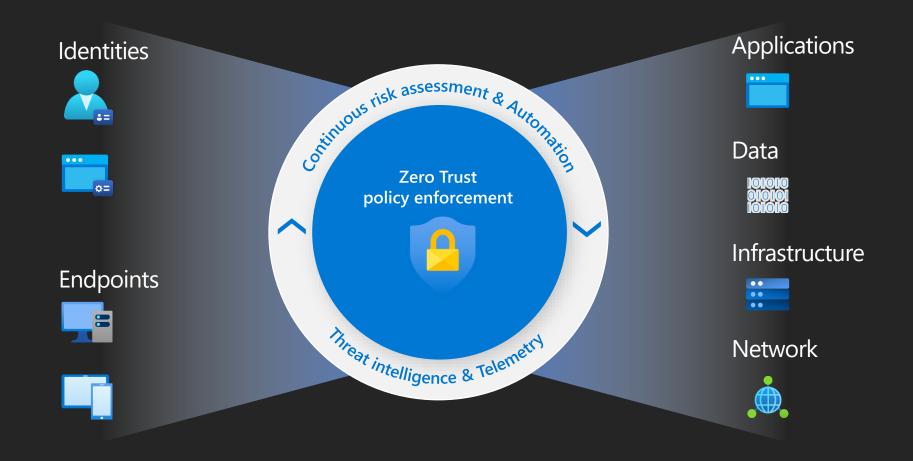
- Evaluate access based on compliance and risk (including user risk, sign-in risk and device risk)
- Use the following access priorities
  - Access the resource directly protected by Conditional Access
  - Publish access to resource using solutions like Citrix, ZScaler or Microsoft App Proxy, protected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

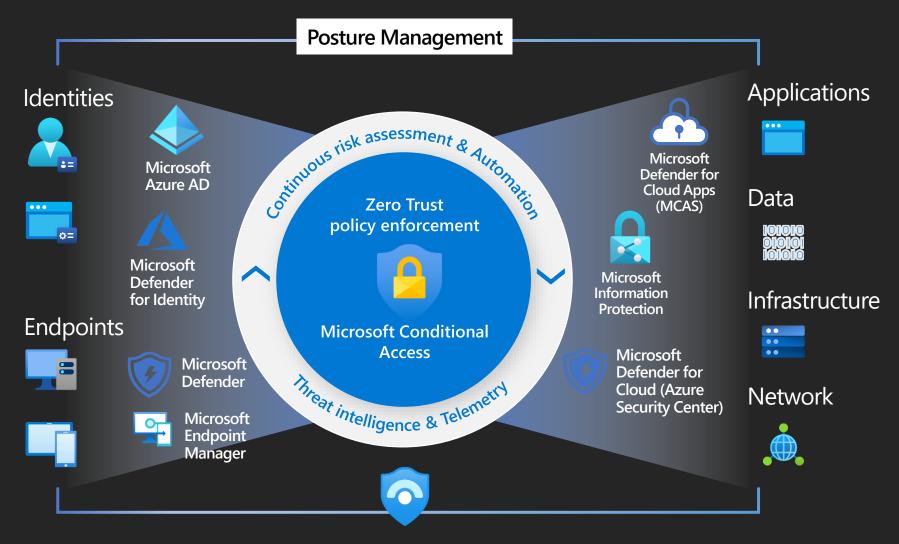
### Zero Trust Approach from Microsoft





### Microsoft Zero Trust Capabilities





**Microsoft Sentinel** 

### CA Guidance for Zero Trust





Claus Jespersen

Principal Consultant II, Security at Microsoft 2mo •



December updates to my Conditional Access Notes from the Field. This will be the last version posted on LinkedIn. Going forward I will either have some of this guidance included as part of our formal Microsoft guidance or start m. ...see more

Title: Microsoft Azure AD Conditional Access principles and guidance.

Author: Claus Jespersen, Principal Security Consultant in Microsoft AC&AI WE

Twitter: @claus\_jespersen

LinkedIn: https://dk.linkedin.com/in/claus-jespersen-25b0422

Date: December 2021

#### Contents

ntroduction
Changelog
CA related components
General Field Guidance
Governance/Roll-out
Personas
Policy Types
CA Principles and recommended best practice
CA Exclusions
Conditional Access Architecture
Suggested Policies
Global Policies (CA001-CA099)
Global Base Protection policies
Global Attack Surface Reduction policies
Admins Policies (CA100-CA199)

#### **Conditional Access for Zero Trust**

Article • 01/27/2022 • 2 minutes to read • 📵 📵

customers control access to their resources.



Is this page helpful? 🖒 🖓

The articles in this section provide a design and framework for implementing Zero Trust of principles by using Conditional Access to control access to cloud services. The guidance is based on years of experience with helping

The framework presented here represents a structured approach that you can use to get a good balance between security and usability while ensuring that user access is controlled.

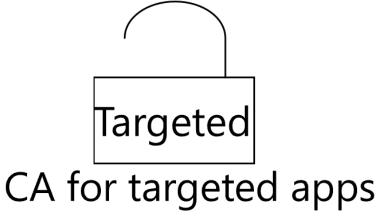
The guidance suggests a structured approach for helping to secure access that's based on personas. It also includes a breakdown of suggested personas and defines the Conditional Access policies for each persona.

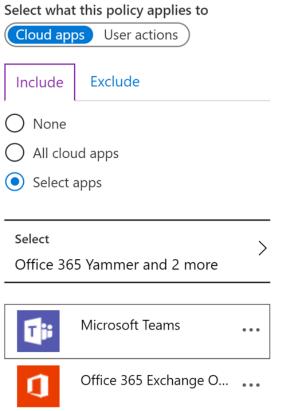
#### Notes from the field: LinkedIn post:

#### Azure Architecture center design guidance:

#### Spreadsheet with suggested policies

### 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





Area	<b>Targeted Architecture</b>	Zero Trust Architecture
Usability		
Functionality		
Security		
Maintainability		

### **Conditional Access Framework**



**CA Number** 

Persona

**Policy Type** 

App

**Platform** 

**Grant** 

Description











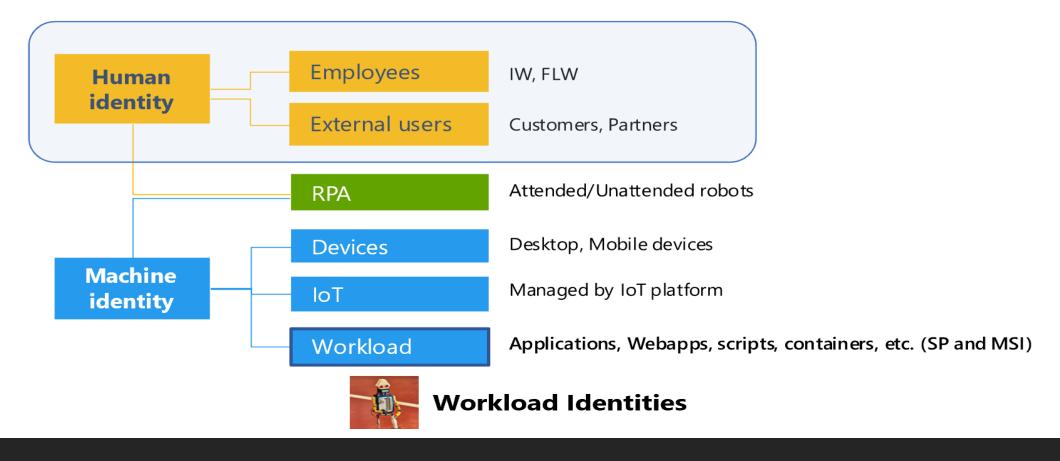


Category / Scope	CA Number
Global protection	CA001-CA099
Admins protection	CA100-CA199
Internals user protection	CA200-CA299
Externals user protection	CA300-CA399
Guest users protection	CA400-CA499
Guest Admins protection	CA500-CA599
Microsoft365 ServiceAccounts	CA600-CA699
Azure ServiceAccounts	CA700-CA799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

- VIRTUAL SUMMIT

#### Various identities in Azure AD

#### CA Protection focuses on human identities



Persona

**Policy Type** 

App

**Platform** 

Grant





### Global "Persona" serves two purposes

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

CA Number Pe	ersona	Policy Type	Арр	Platform	Grant	Description NORDIC
Policy Type	Descrip	tion				
Base Protection	- Exam	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	Example	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		liance policy cou g customer serv		equire a user to s or GDPR	see a "Terms Of	Use" for guests

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

CA Number	Persona

Policy Type

App

**Platform** 

Grant



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



**CA Number** 

Persona

Policy Type

App

**Platform** 

Grant

Description

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** 

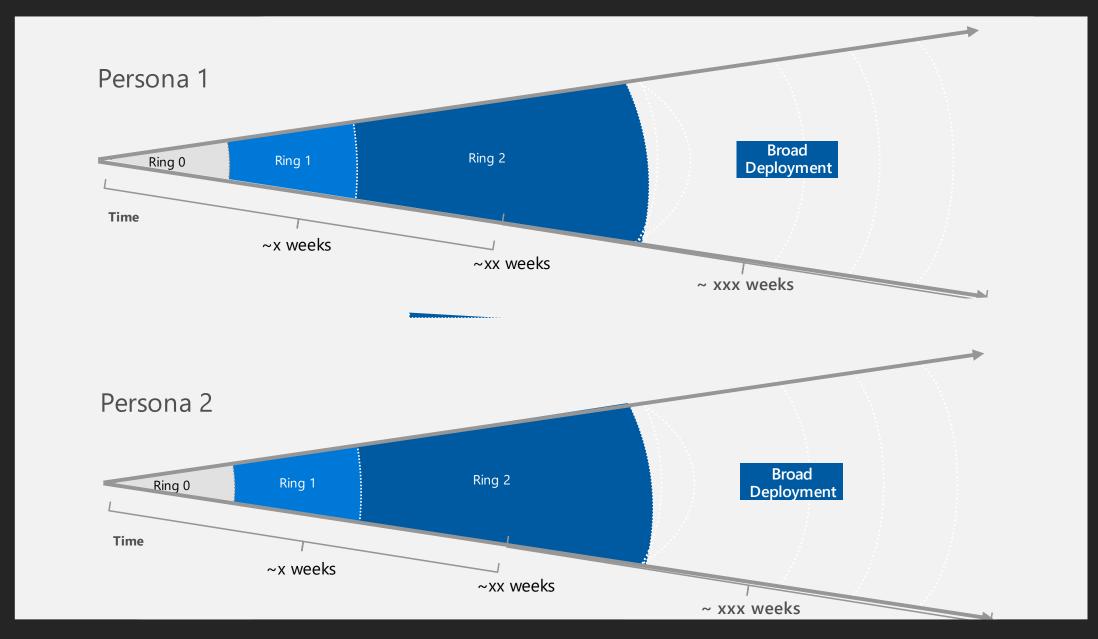
Grant

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 Gro			dd				
		Include	[x] All users				
			Select users and groups >	[_] All guest and external user	rs		
				Directory roles	>	Multi-select roles [_][_][_]	
				Users and groups	>	Multi-select users/groups [_][_][_]	
		Exclude		Users and groups	>	CA-BreakglassAccounts, CA-Persona-A	
	Cloud apps, Actions			[_] None			
	or Authentication		Include	[x] All cloud apps			
	Context	Cloud apps		Select apps	>	Multi-select cloud apps [_][_]	
			Exclude	Select excluded cloud apps	>	Multi-select cloud apps [_][_][_]	
				7			
		User actions	[_] Register security information				
			[_] Register or join devices				
				٦			
		Authentication Context (preview)					
		,		J			
	T. David						
	Conditions	User risk *	[_] High	_			
		User risk .	[_] Medium				
			[_] Low				
			[ ] Lligh	7			
			[_] High				
		Siøn-in risk *	[_] iviedium				

### FAQ & Evals





Evals: <a href="https://stream.nordicvirtualsummit.com/feedback">https://stream.nordicvirtualsummit.com/feedback</a>



### A big thanks to our sponsors









Please remember to fill out the evals!

