



# SECURING AZURE ACTIVE DIRECTORY

@OWASP Stammtisch Frankfurt

Thomas Naunheim




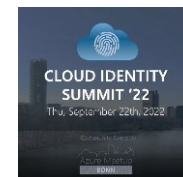
# THOMAS NAUNHEIM

Cloud Security Architect  
@glueckkanja-gab AG

Koblenz, Germany

 @Thomas\_Live

 cloud-architekt.net



# AGENDA



IDENTITY SECURITY  
POSTURE



CONDITIONAL ACCESS  
AND TOKEN SECURITY



PRIVILEGED IDENTITY  
AND ACCESS



WORKLOAD IDENTITIES  
AND APP INTEGRATION

# Underrated and critical aspect in #AzureAD security





# IDENTITY SECURITY POSTURE

# Insights of modern identity attacks

## The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks



# Security Default for Everyone

- Replacement of “Baseline”-Policies

Create your own policies and target specific conditions like Cloud apps, Sign-in risk, and Device platforms with Azure AD Premium →

POLICY NAME	ENABLED
Baseline policy: Require MFA for admins	✓ ...
Baseline policy: End user protection (Preview)	...
Baseline policy: Block legacy authentication (Preview)	...
Baseline policy: Require MFA for Service Management (Preview)	...

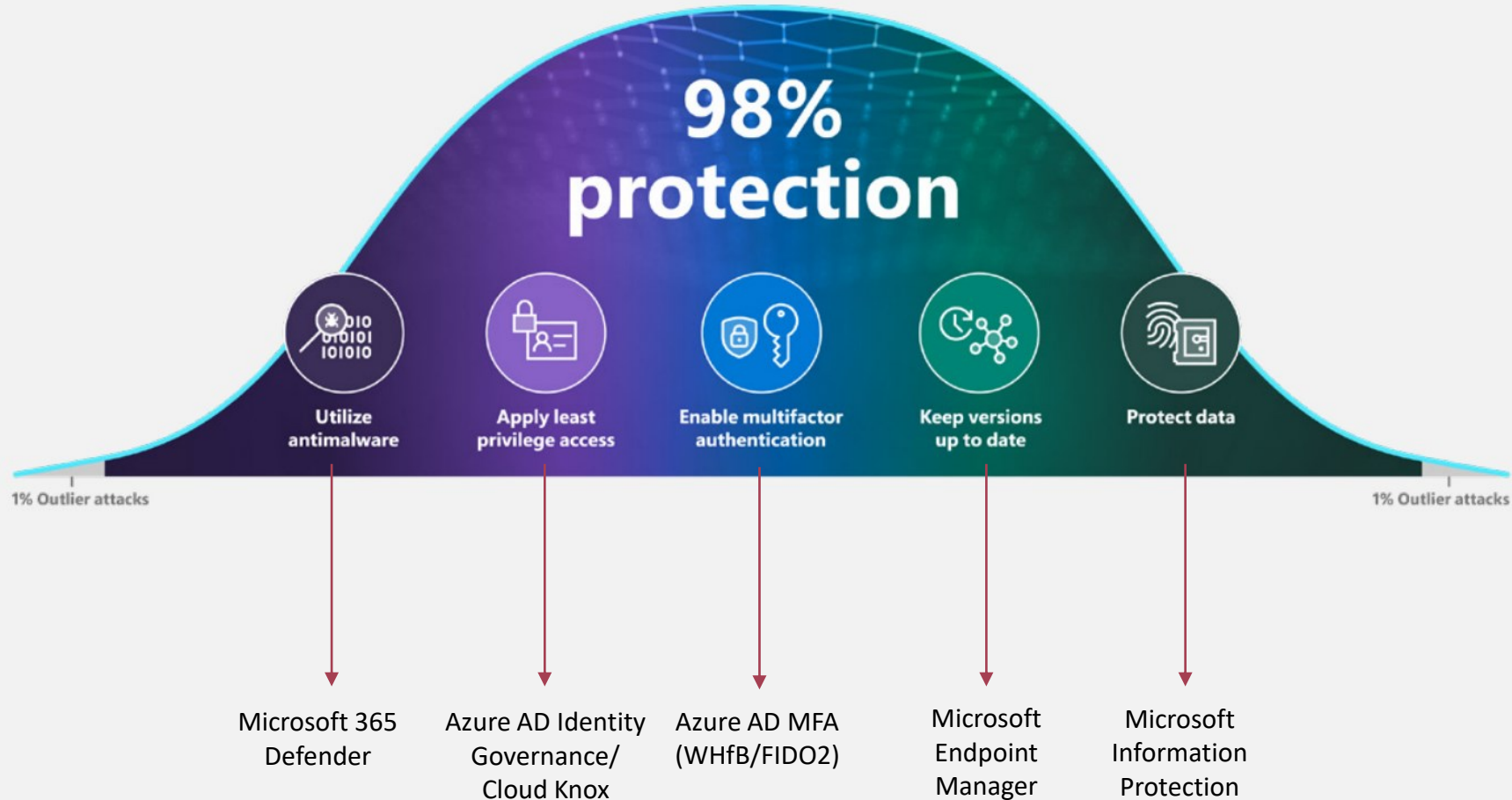
- No extra costs or AAD license required (available for all tenant, enabled by default)

- Minimal security baseline by enforced policies

- “Security defaults provide secure default settings that (Microsoft) manages on behalf of organizations to keep customers safe **until they are ready to manage their own identity security story.**”

*Quote from Alex Weinert’s Blog post*

# Insights of modern identity attacks



Source: *Microsoft* ("Identity is the new battle ground")



# Azure AD Identity Secure Score

Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

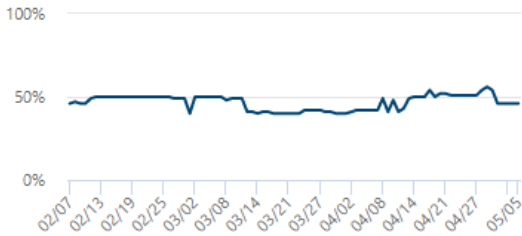
Filter

Your secure score

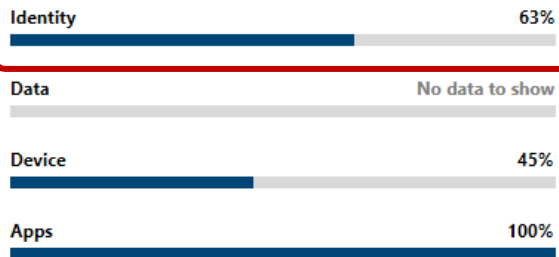
Include

**Secure Score: 46%**

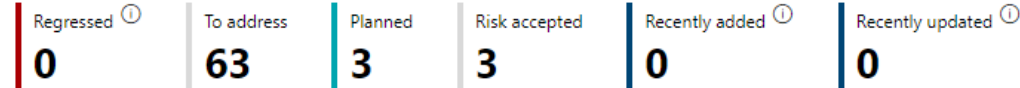
379/820 points achieved



Breakdown points by: Category



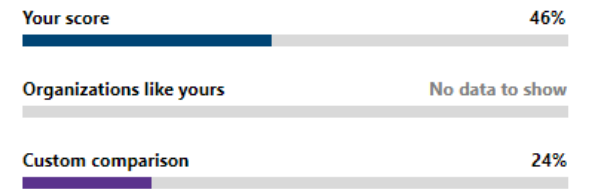
Actions to review



Top improvement actions

Improvement action	Score impact	Status	Category
Turn on Microsoft Defender Application Guard managed mode	+1.1%	<input checked="" type="radio"/> Risk accepted	Device
Block credential stealing from the Windows local security authorit...	+1.1%	<input type="radio"/> To address	Device
Use advanced protection against ransomware	+1.1%	<input type="radio"/> To address	Device
Block execution of potentially obfuscated scripts	+1.1%	<input type="radio"/> To address	Device
Block Office applications from injecting code into other processes	+1.1%	<input type="radio"/> To address	Device
Block executable content from email client and webmail	+1.1%	<input type="radio"/> To address	Device
Encrypt all BitLocker-supported drives	+1.1%	<input type="radio"/> To address	Device

Comparison



Manage comparisons

Resources

- [Read about Secure Score capabilities](#)  
Learn about the improvement actions and how to improve your score.
- [Do more with the Secure Score API](#)  
Learn how to use the API to take your monitoring and reporting even further.

# Operationalization of Identity Secure Score

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel

## Microsoft 365 Security Posture

lab-la-4d3e5b65-8a52-4b2f-b5cd-1670c700136b

Auto refresh: Off

Subscription: Platform (MSDN) TimeRange: Last 90 days

Azure Security Center **Microsoft 365** Defender for Endpoint Microsoft Cloud App Security

CurrentScore (Last) **495**

Category: All

### Microsoft 365 Secure Score Recommendations

RecommendationCategory ↑↓	ControlName	↑↓	Recommendation	↑↓	ImplementationStatus	↑↓
Apps	McasCloudAppNotification		App discovery policies can notify you when new apps or ...		Policy in place: false.	
Apps	TLSDeprecation		Review all your clients to check which ones use TLS 1.0/1....		Upgraded to TLS 1.2 or higher: True	
Identity	RoleOverlap		Limited administrators are users who have more privileg...		You have 4 users with limited administrative roles.	
Identity	AATP_PathRisk		Lateral movement paths are ways in which an attacker ca...			
Identity	AATP_UnsecureAccount		Every account in Active Directory has multiple attributes r...			
Identity	AATP_HoneyToken		Setting honeytoken accounts helps to trap malicious acto...		Honeytoken account configured: false	

# Azure Security Benchmark (V3)

🌟 Please take time to answer a quick survey, [click here](#).

## Control Areas

- Section ↑↓
- Assessment
- Network Security (NS)
- Identity Management (IM)
- Privileged Access (PA)

## Azure Security Benchmark

Welcome to the Azure Security Benchmark workbook. This workbook is designed to enable Cloud Architects, Security Engineers, and Governance Risk Compliance Professionals to gain situational awareness for cloud security posture and hardening. Benchmark recommendations provide a starting point for selecting specific security configuration settings and facilitate risk reduction. The Azure Security Benchmark includes a collection of high-impact security recommendations for improving posture. For more information, see the [Azure Security Benchmark](#).

### 🔍 Single vs Multi-Factor Authentication by Account

UserPrincipalName	AuthenticationRequirement	AppDisplayName	count_
cloudadmin@c4a8ando.net	✅ multiFactorAuthentication	Azure Portal	3177
thomas@cloud-architekt.net	❌ singleFactorAuthentication	Microsoft App Access Panel	2600
thomas@cloud-architekt.net	✅ multiFactorAuthentication	Microsoft App Access Panel	2360
thomas@cloud-architekt.net	❌ singleFactorAuthentication	WindowsDefenderATP	747

## IM-5: Monitor and Alert on Account Anomalies

### Azure Security Center - Regulatory Compliance - Azure Security Benchmark

#### Recommended Logs

- ◆ BehaviorAnalytics
- ◆ SecurityAlert
- ✳️ Azure Sentinel

### 🔍 User Anomalies

UserPrincipalName	Uncomm...↑↓	Uncomm...↑↓	FirstTi
thomas.naunheim@outlook.com	26	26	
Sync_ANDS1_bbcab499138c@c4a8ando.onmicrosoft.com	23	44	

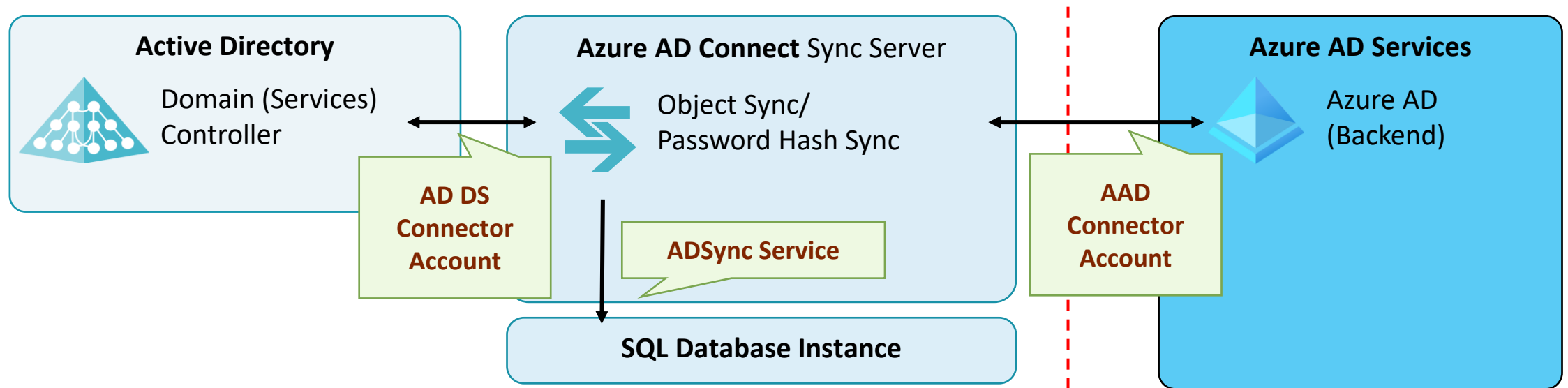
The background features a dark, abstract network diagram with interconnected nodes and lines, suggesting a digital or security theme.

# Default security settings and usage of strong authentication methods

LIVE DEMO



# Attack surface by hybrid identity sync



A dark background with a faint, light-colored network diagram consisting of interconnected nodes and lines, suggesting a complex system or data flow.

# Privilege Escalation from AAD Connect to Azure AD

LIVE DEMO

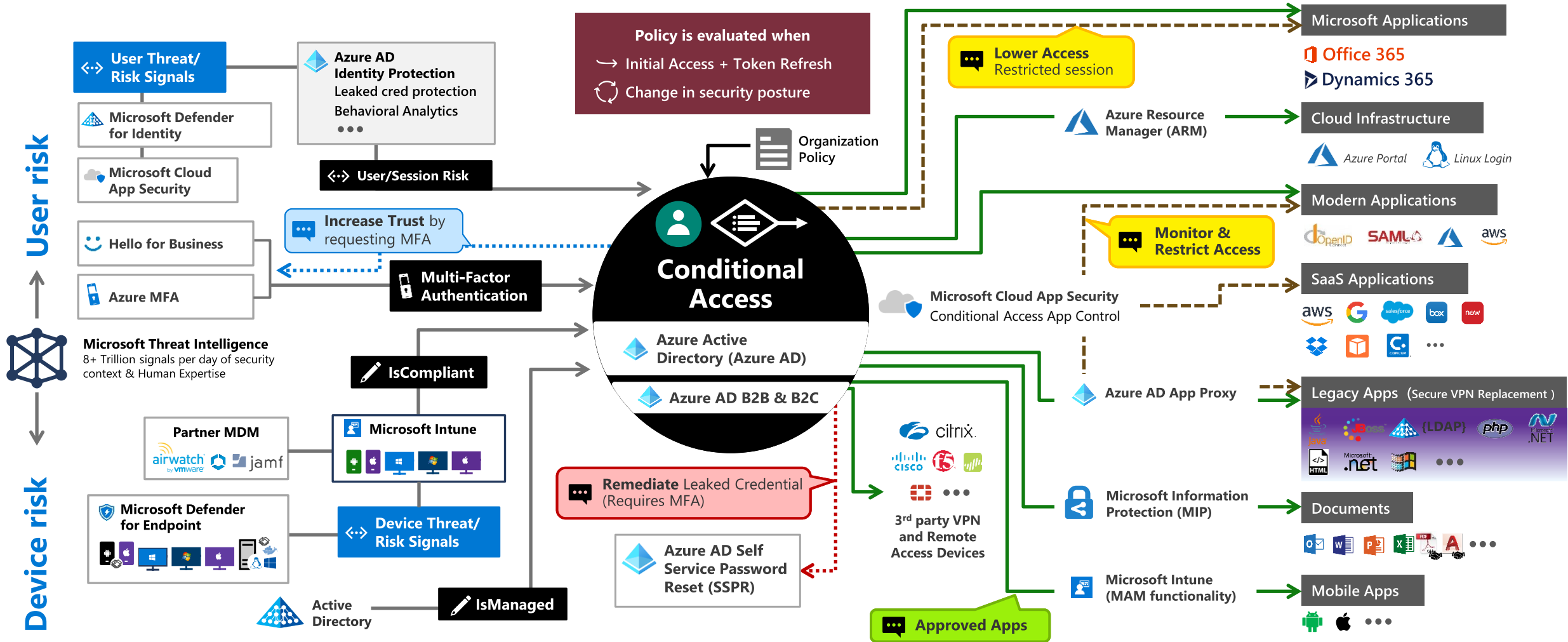


# CONDITIONAL ACCESS AND TOKEN SECURITY



# Conditional Access Overview

Image Source: [Microsoft](#) ("Zero Trust Definition and Models")



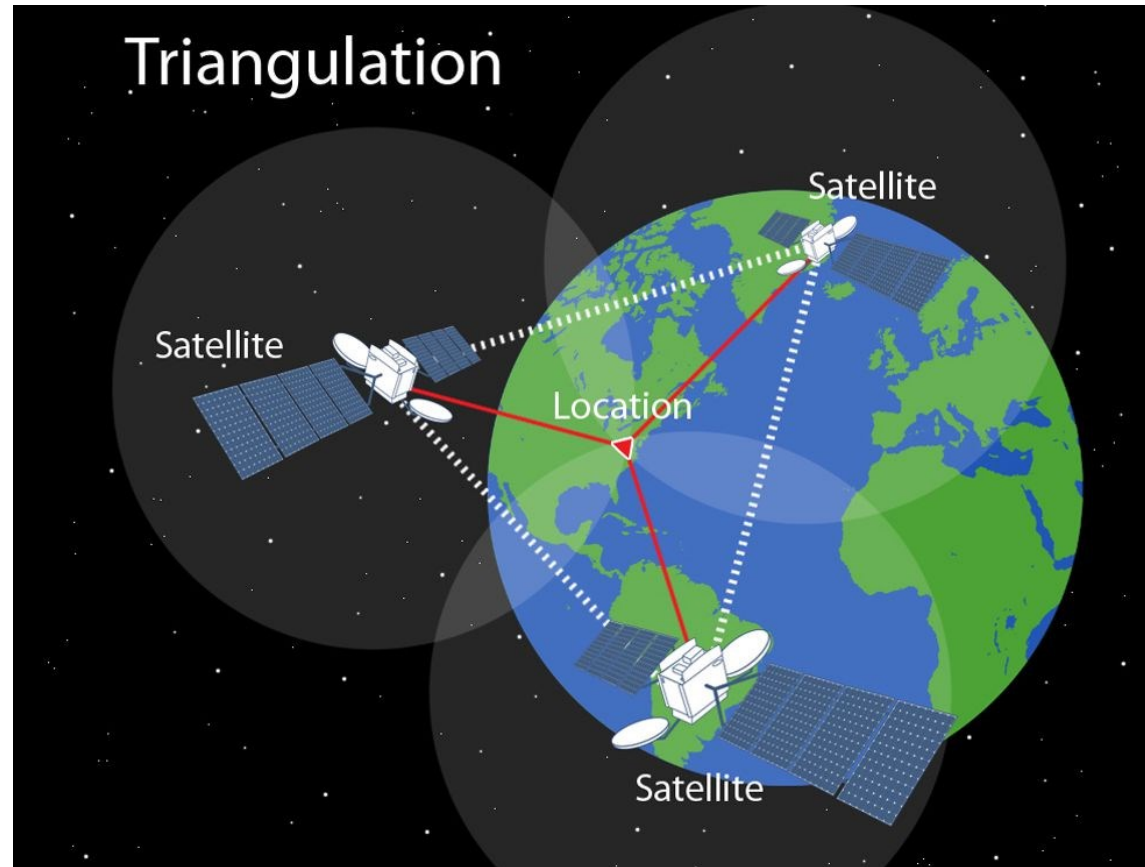
# Strong baseline for Conditional Access

---



Ensure to protect every user and every app by minimal but strong baseline!

# Strong claims & efficient controls in Conditional Access



A dark background with a faint, light-colored network diagram consisting of interconnected nodes and lines, suggesting a technical or digital theme.

# Conditional Access Baseline & CAE in action

## Token Replay

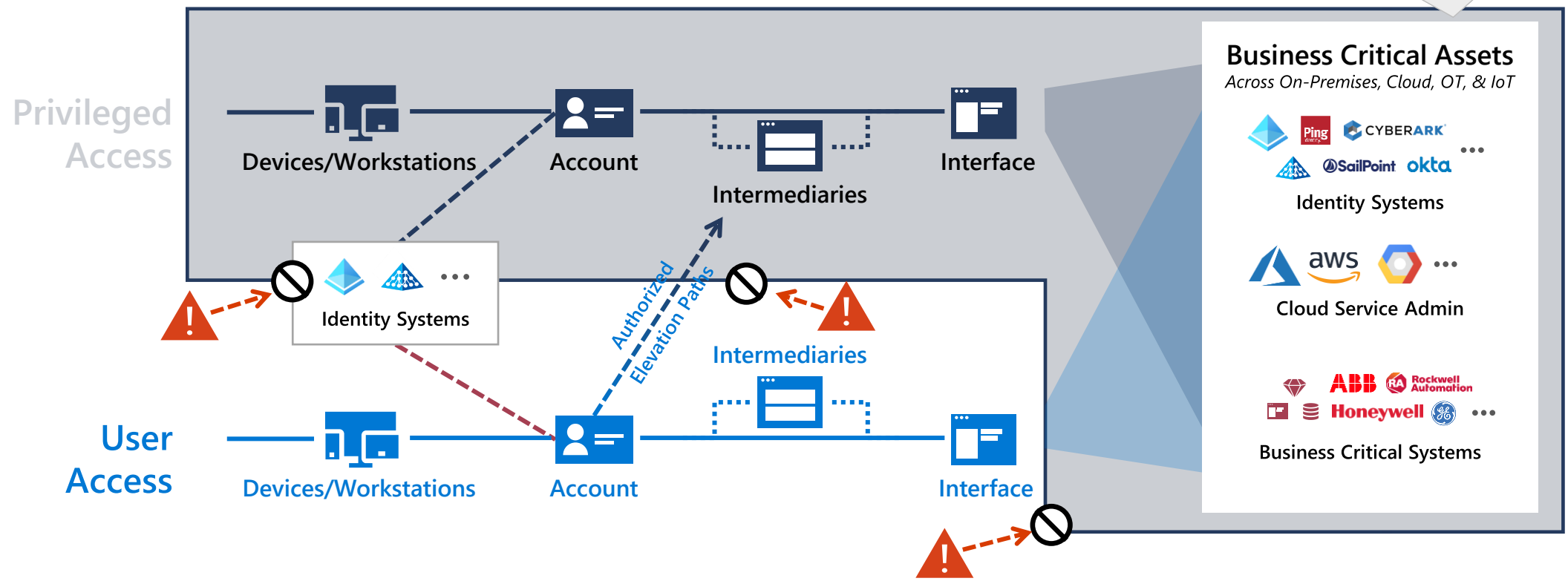
LIVE DEMO



# PRIVILEGED IDENTITY AND ACCESS

# Authorized privileged and elevated paths

**Asset Protection also required**  
*Security updates, DevSecOps,  
data at rest / in transit, etc.*



*“End-to-end  
Session Security -  
Establish explicit  
Zero Trust  
validation for  
privileged  
sessions, user  
sessions, and  
authorized  
elevation paths.”*

**Complete End-to-end approach**  
*Required for meaningful security*

# Foundation of Privileged Access



Granular Task  
Scoped Access  
(Just Enough)

CloudKnox

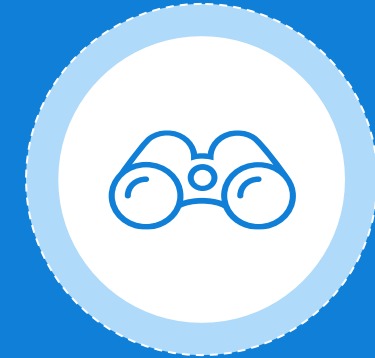


Just in Time  
Access



Privileged  
Admin  
Workflow

Privileged Identity Management (PIM)



Access Request  
and Review

Identity Governance

# Administrative Tier Model

„To mitigate risk of identity compromise, or bad actors, implement **tiered administration** and ensure that you **follow principles of least privilege for Azure AD Administrator Roles.**“

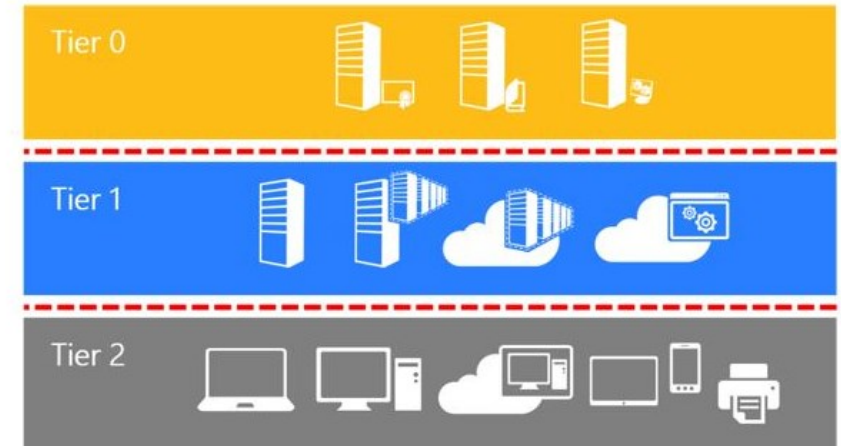
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8

## Active Directory administrative tier model

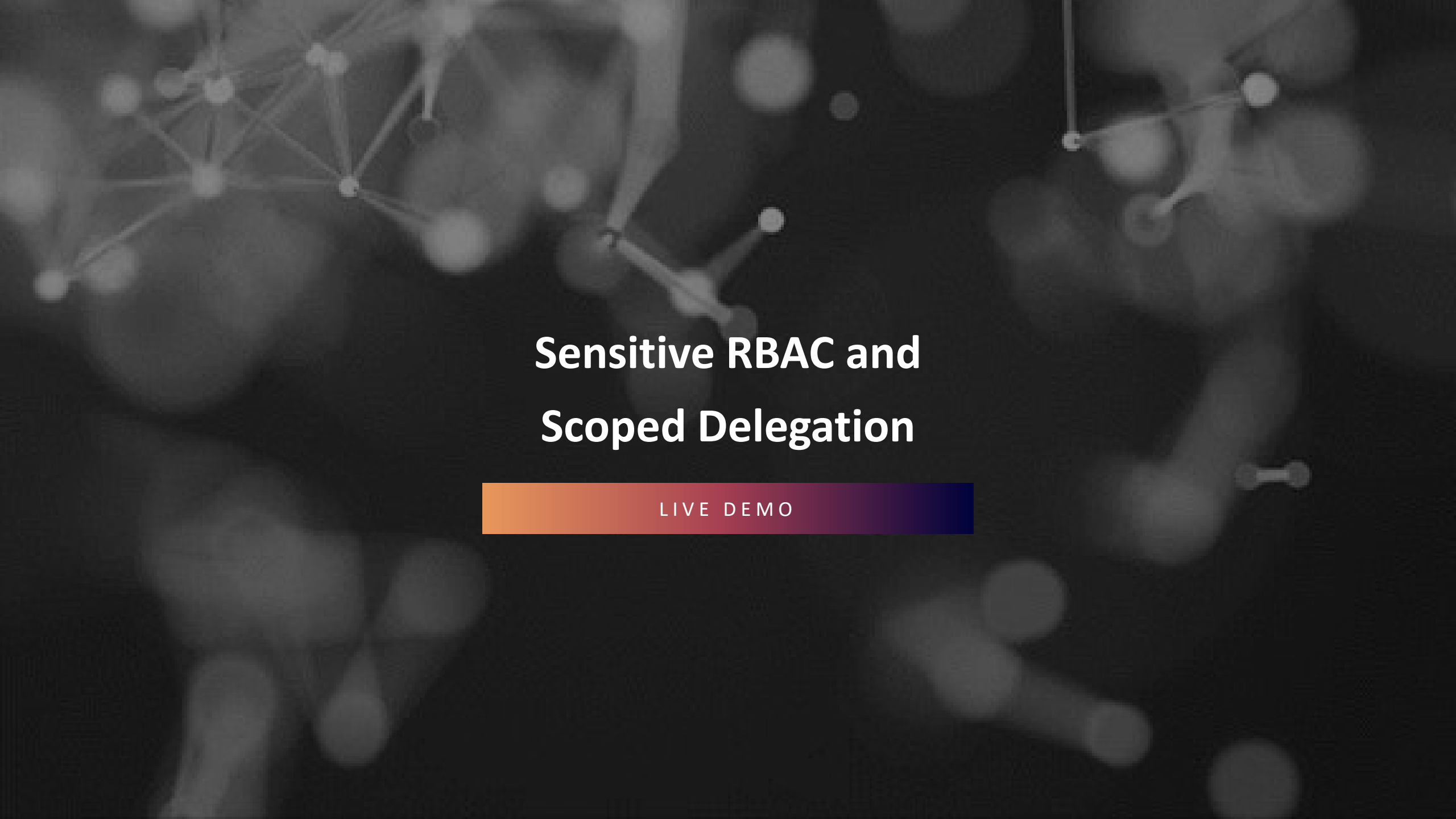
02/14/2019 • 33 minutes to read •  +6

Applies To: Windows Server

The purpose of this tier model is to protect identity systems using a set of buffer zones between full control of the Environment (Tier 0) and the high risk workstation assets that attackers frequently compromise.





The background features a dark, abstract network diagram with interconnected nodes and lines, suggesting a complex system or data structure. The nodes are represented by small circles, and the lines are thin, light-colored connections between them. The overall aesthetic is technical and modern.

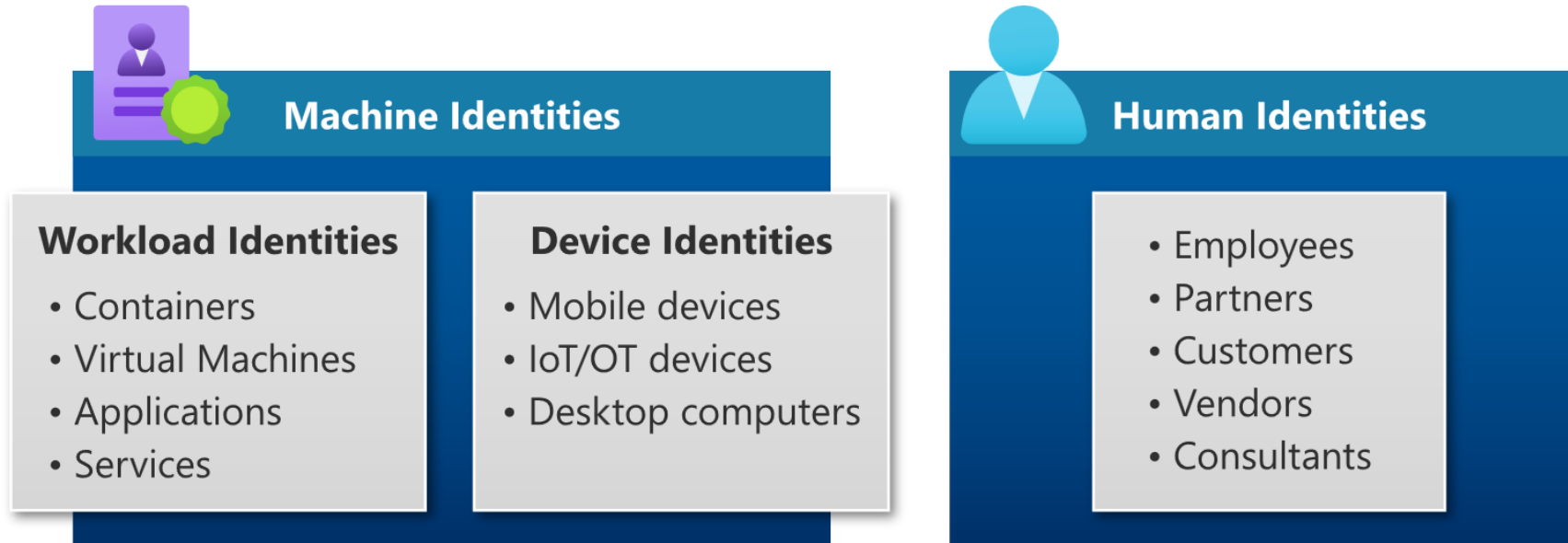
# Sensitive RBAC and Scoped Delegation

LIVE DEMO



# APP INTEGRATION AND WORKLOAD IDENTITIES

# Types of identities



# Types of workload identities

Criteria	Service Principal (Key- or Certificate)	Managed Identity (System- or User Assigned)	Service Principal (Federated Credentials)
Supported use cases	No limitation	Limited to supported Azure Resources	Limited to supported Workload Identity Federation Provider
Security boundary	Single- or multi-tenant	Single-Tenant*	Single- or multi-tenant*

# Types of workload identities

Criteria	Service Principal (Key- or Certificate)	Managed Identity (System- or User Assigned)	Service Principal (Federated Credentials)
Supported use cases	No limitation	Limited to supported Azure Resources	Limited to supported Workload Identity Federation Provider
Security boundary	Single- or multi-tenant	Single-Tenant*	Single- or multi-tenant*
Lifecycle management	Managed by Admin	Managed by Azure (System-) or Admin (User-Assigned)	Managed by Admin
Prevention of privilege escalation	Service Principal and assigned permissions (Roles, Owner)  Secure storing of credentials  Detection of unusual creation of credentials (MDA, Sentinel)	Azure resource with assignment to identity  Azure RBAC to resource object	Service Principal and assigned permissions (Roles, Owner)  Security of the Federated IdP and workload

# Types of workload identities

Criteria	Service Principal (Key- or Certificate)	Managed Identity (System- or User Assigned)	Service Principal (Federated Credentials)
Supported use cases	No limitation	Limited to supported Azure Resources	Limited to supported Workload Identity Federation Provider
Security boundary	Single- or multi-tenant	Single-Tenant*	Single- or multi-tenant*
Lifecycle management	Managed by Admin	Managed by Azure (System-) or Admin (User-Assigned)	Managed by Admin
Prevention of privilege escalation	Service Principal and assigned permissions (Roles, Owner)  Secure storing of credentials  Detection of unusual creation of credentials (MDA, Sentinel)	Azure resource and delegation to manage them	Service Principal and assigned permissions (Roles, Owner)  Security of the Federated IdP
Restrict token acquisition	Conditional Access (risk-based conditions on leaked cred. or suspicious sign-ins)	Not available	Conditional Access (risk-based conditions on suspicious sign-ins), Entity (subject identifier)
Exfiltration/Token replay	Active monitoring required (incl. inventory and usage history) IPC risk detections available		IPC risk detections available

# Security of App Integration

Microsoft Azure Search resources, services, and docs (G+)

Home > CloudLab > BusinessApp-Auth-WebAPI

## BusinessApp-Auth-WebAPI | Integration assistant

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

### Here's the integration assistant for BusinessApp-Auth-WebAPI

Application type : Desktop App, Web API [Edit](#)

Calls APIs : Yes

Summary Develop Test Release Monitor

#### Recommended configurations

Item	Status
Configure a redirect URI for a desktop app by adding a platform.	⚠️ Action required ...
Configure API permissions.	⚠️ Action required ...
Configure a valid credential.	⚠️ Action required ...
Configure a unique Application ID URI.	⚠️ Action required ...
If expecting API requests on behalf of users, define scopes your API exposes.	⚠️ Action required ...
If expecting API requests on behalf of apps directly, define app roles.	⚠️ Action required ...
Assign users that should be able to view and edit this application registration as owners.	✅ Complete ...

#### Discouraged configurations

Item	Status
If you are using the authorization code flow, disable the implicit grant settings.	✅ Complete ...

## More details:


- [Azure AD application registration security best practices](#)
- [Microsoft identity platform best practices and recommendations](#)

# App registration and consent grant



① testuser@fourthcoffeetest.onmicrosoft.com

## ② Permissions requested

③  Best Practices Demo ④  
[microsoftidentity.dev](https://microsoftidentity.dev) ⑤ ⑥

This application is not published by Microsoft or your organization. ⑦

This app would like to:

- ✓ Maintain access to data you have given it access to
- ^ Sign you in and read your profile

⑨ } Allows you to sign in to the app with your organizational account and let the app read your profile. It also allows the app to read basic company information. ⑧  
 This is a permission requested to access your data in Fourth Coffee.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. ⑩

Only accept if you trust the publisher and if you selected this app from a store or website you trust. Ask your admin if you're not sure. Microsoft is not involved in licensing this app to you. [Hide details](#)

Does this app look suspicious? [Report it here](#) ⑫

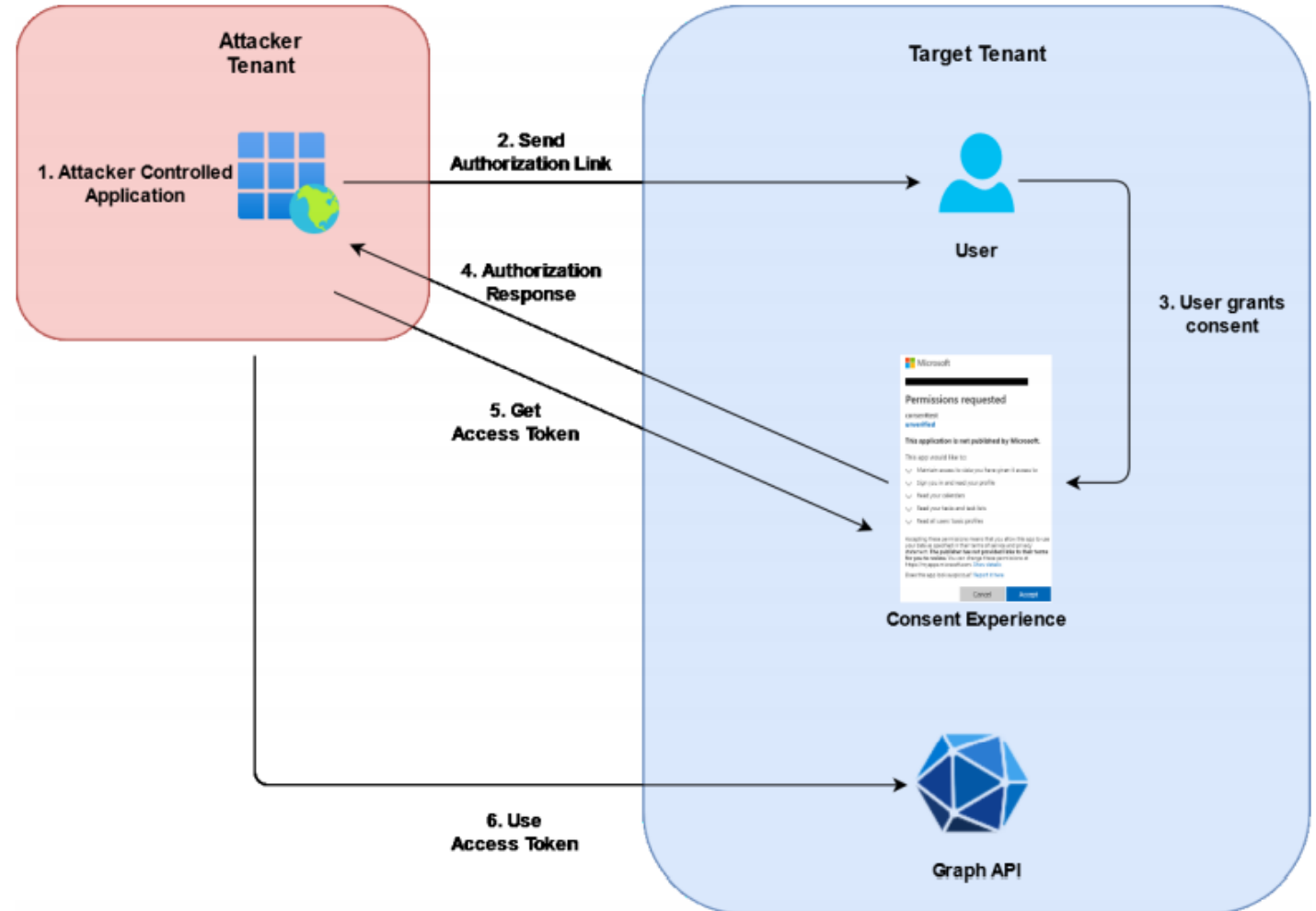


Image source: *Introduction To 365-Stealer by Altered Security*



A dark background with a faint, light-colored network diagram consisting of interconnected nodes and lines, suggesting a digital or data network.

# **Illicit Consent Grant Attack**

## **Auditing and Monitoring of Service Principals**

LIVE DEMO

# AZURE AD ATTACK & DEFENSE PLAYBOOK

written by Sami Lamppu, Joosua Santasalo and Thomas Naunheim



# SECURING AZURE AD CALL FOR ACTIONS



Implement an active identity security posture management and review of (default) settings  
Use cloud and phishing resistant authentication methods (PHS + FIDO2/WHfB)  
Protect your Azure AD connect as Tier0 asset (of both worlds) incl. MDE and monitoring



Use clear and enriched signals as conditions in your Conditional Access Policies  
Monitor and review your efficiency and coverage of policy configuration  
Enforce strong controls for user access (device compliance, always MFA)



Enforce authorization paths for privileged access (incl. device filters for access from SAW/PAW only)  
Consider access paths by directory-level roles, partner access delegation or other RBAC systems  
Implement least-privileged RBAC design (Tiered Admin Model) with Identity Governance processes



Disable user consent for (risky) permissions and implement admin approval flow  
Replace owner permissions by scoped Azure AD roles, restrict access to sensitive delegated permissions  
Implement a lifecycle model, inventory and active monitoring with IR for workload identities

# THANK YOU



@Thomas\_Live



Thomas@Naunheim.net

[www.cloud-architekt.net](http://www.cloud-architekt.net)