SECURING
AZURE ACTIVE DIRECTORY

@OWASP Stammtisch Frankfurt

Thomas Naunheim

THOMAS NAUNHEIM

Cloud Security Architect
@glueckkanja-gab AG

Koblenz, Germany

@Thomas_Live

cloud-architekt.net

Microsoft® MVP Most Valuable Professional

Azure Meetup BONN

CLOUD IDENTITY SUMMIT '22

AGENDA

IDENTITY SECURITY POSTURE

CONDITIONAL ACCESS AND TOKEN SECURITY

PRIVILEGED IDENTITY AND ACCESS

WORKLOAD IDENTITIES AND APP INTEGRATION

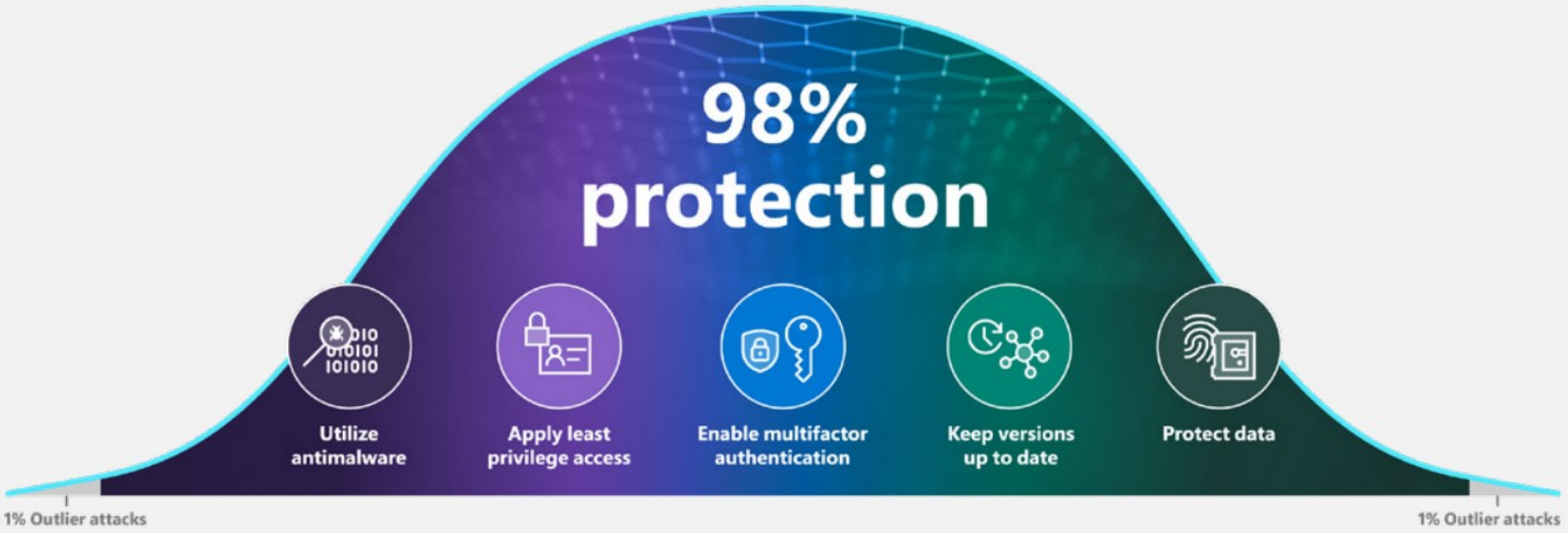
Underrated and critical aspect in #AzureAD security

https://twitter.com/Thomas_Live/status/1528011619179036672

IDENTITY SECURITY POSTURE

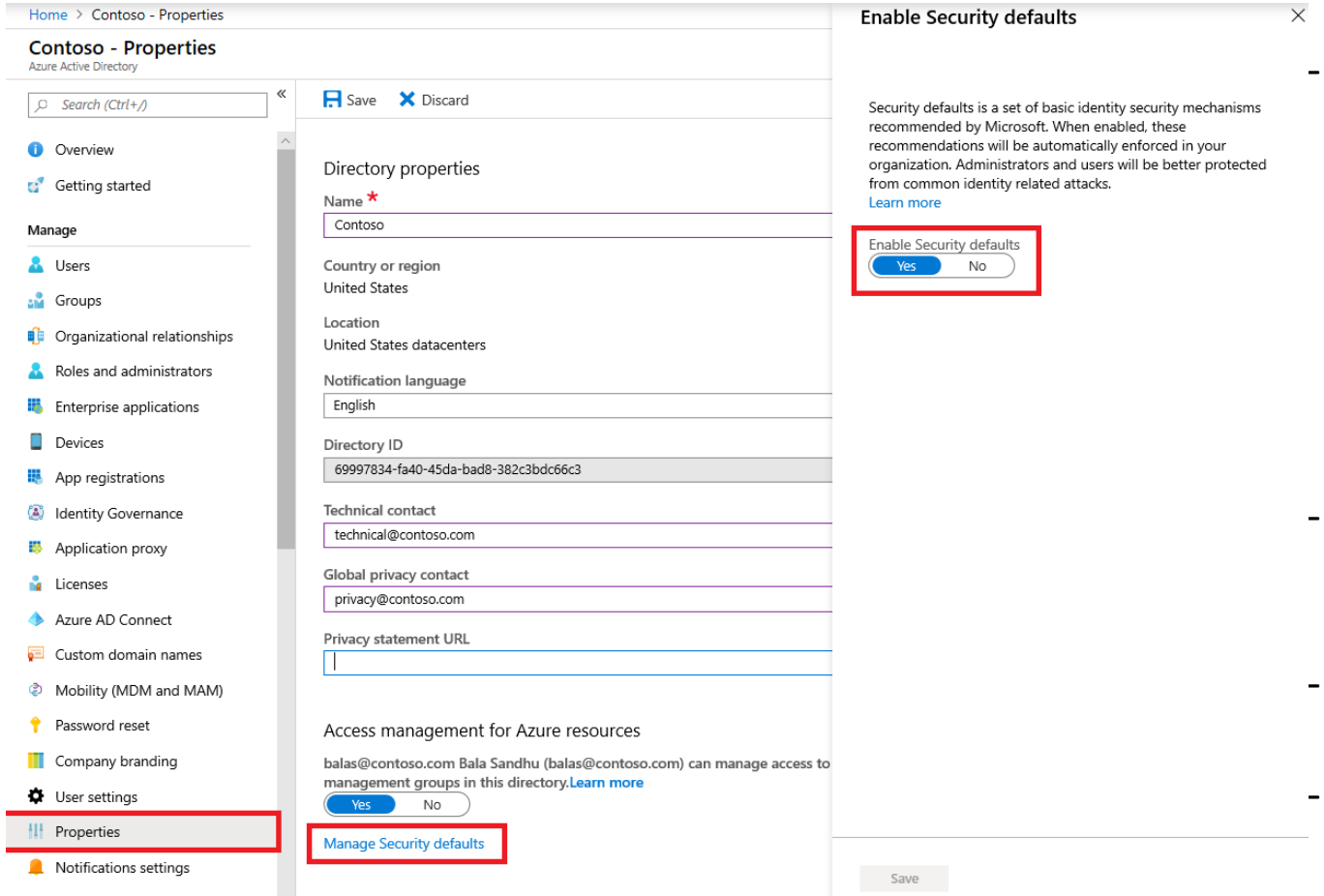
Insights of modern identity attacks

The cybersecurity bell curve:
Basic security hygiene still protects against 98% of attacks

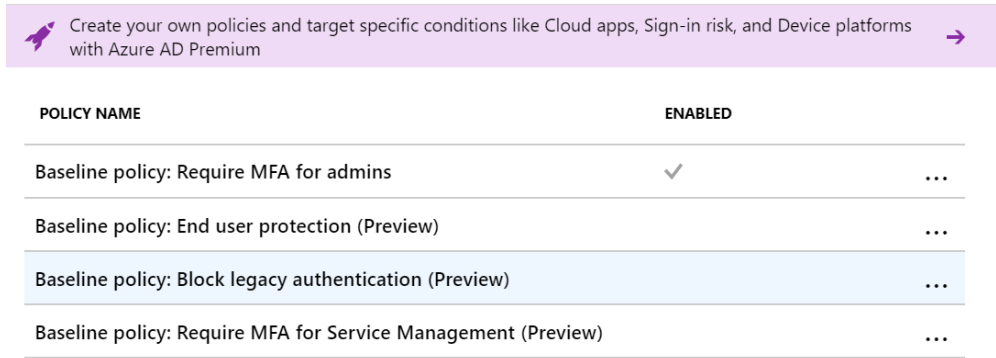


Source: Microsoft ("Identity is the new battle ground")

Security Default for Everyone



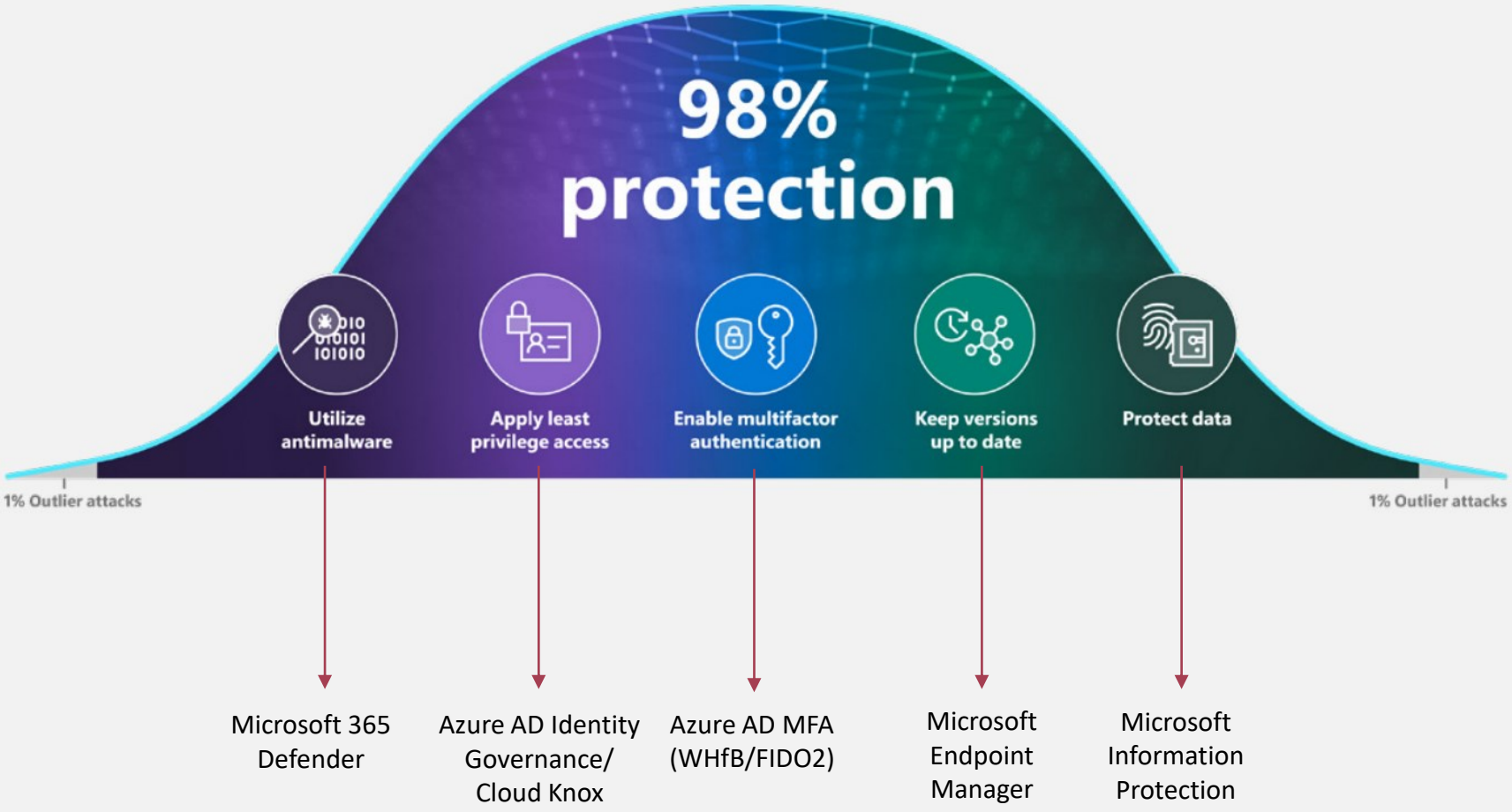
- Replacement of “Baseline”-Policies



- 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.**”*

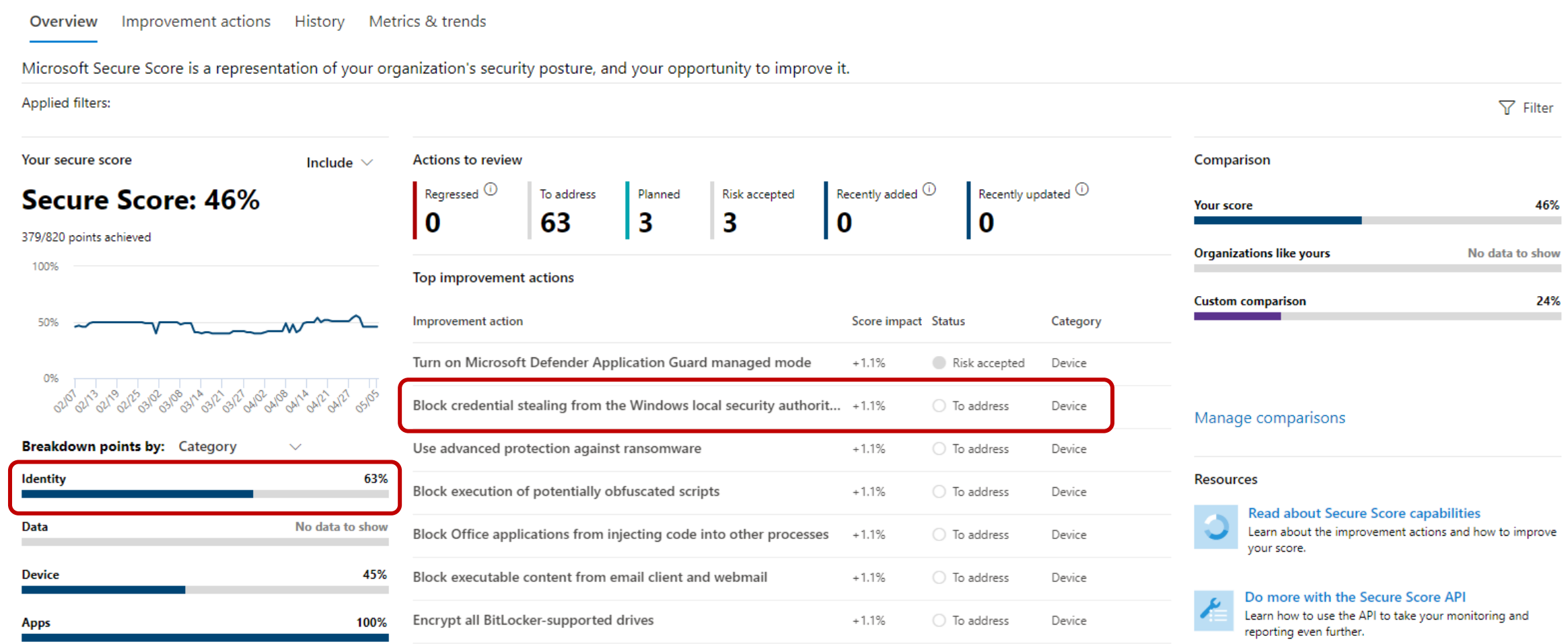
Quote from Alex Weinert’s Blog post

Insights of modern identity attacks



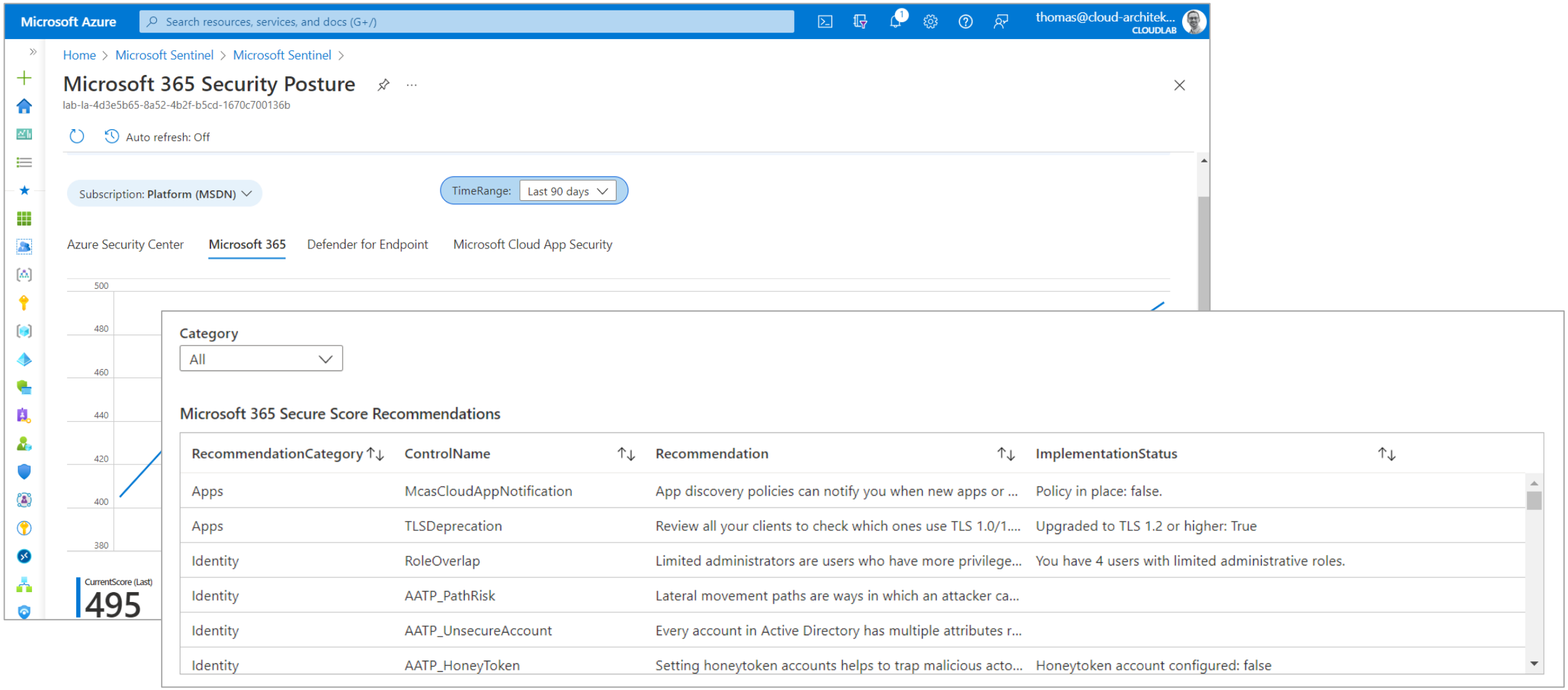
Source: Microsoft ("Identity is the new battle ground")

Azure AD Identity Secure Score



Source: Microsoft (Overview "Microsoft Secure Score")

Operationalization of Identity Secure Score



Azure Security Benchmark (V3)

Please take time to answer a quick survey, click here.

Control Areas

Search

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

Search

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

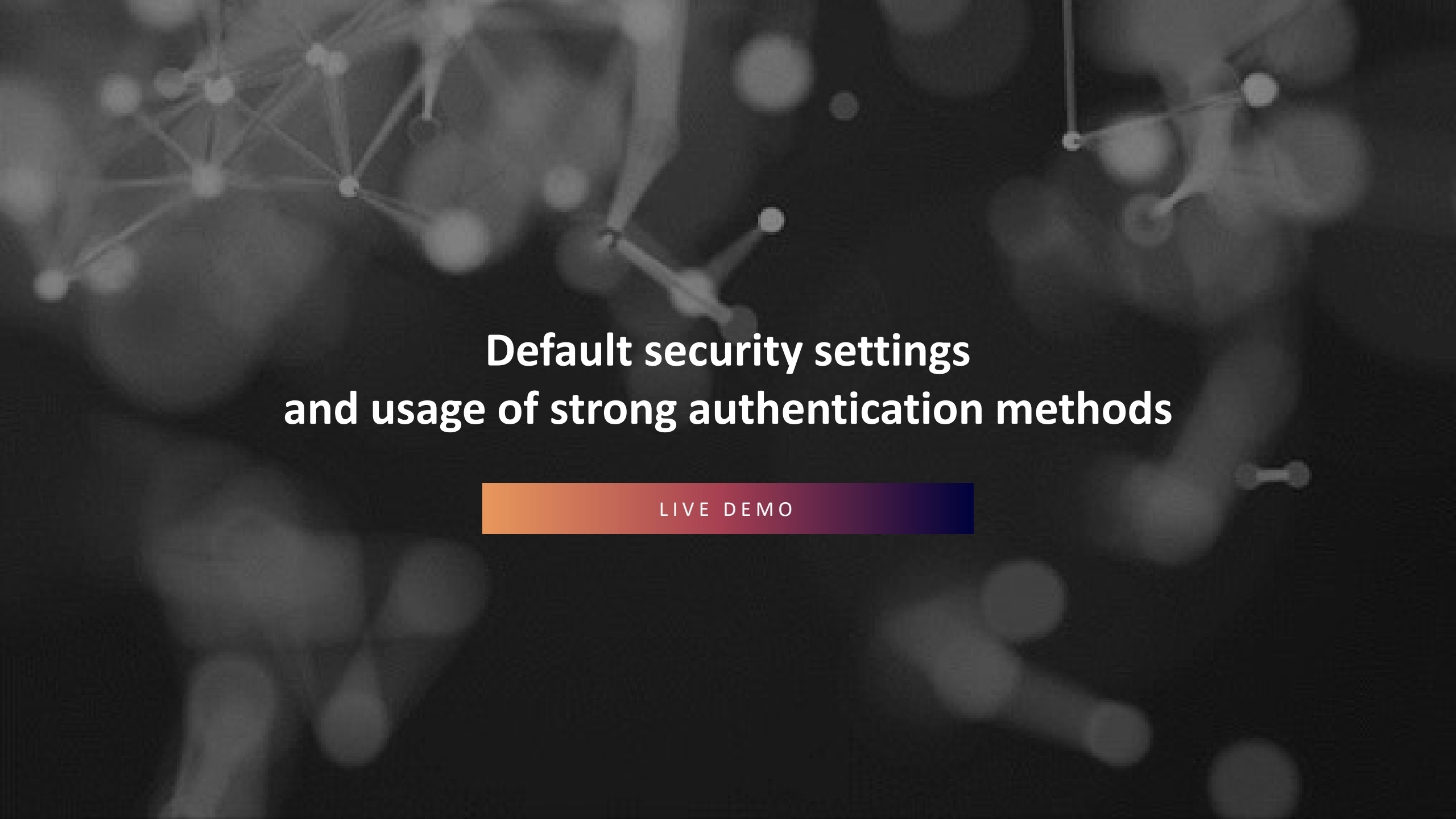
Recommended Logs

BehaviorAnalytics SecurityAlert Azure Sentinel

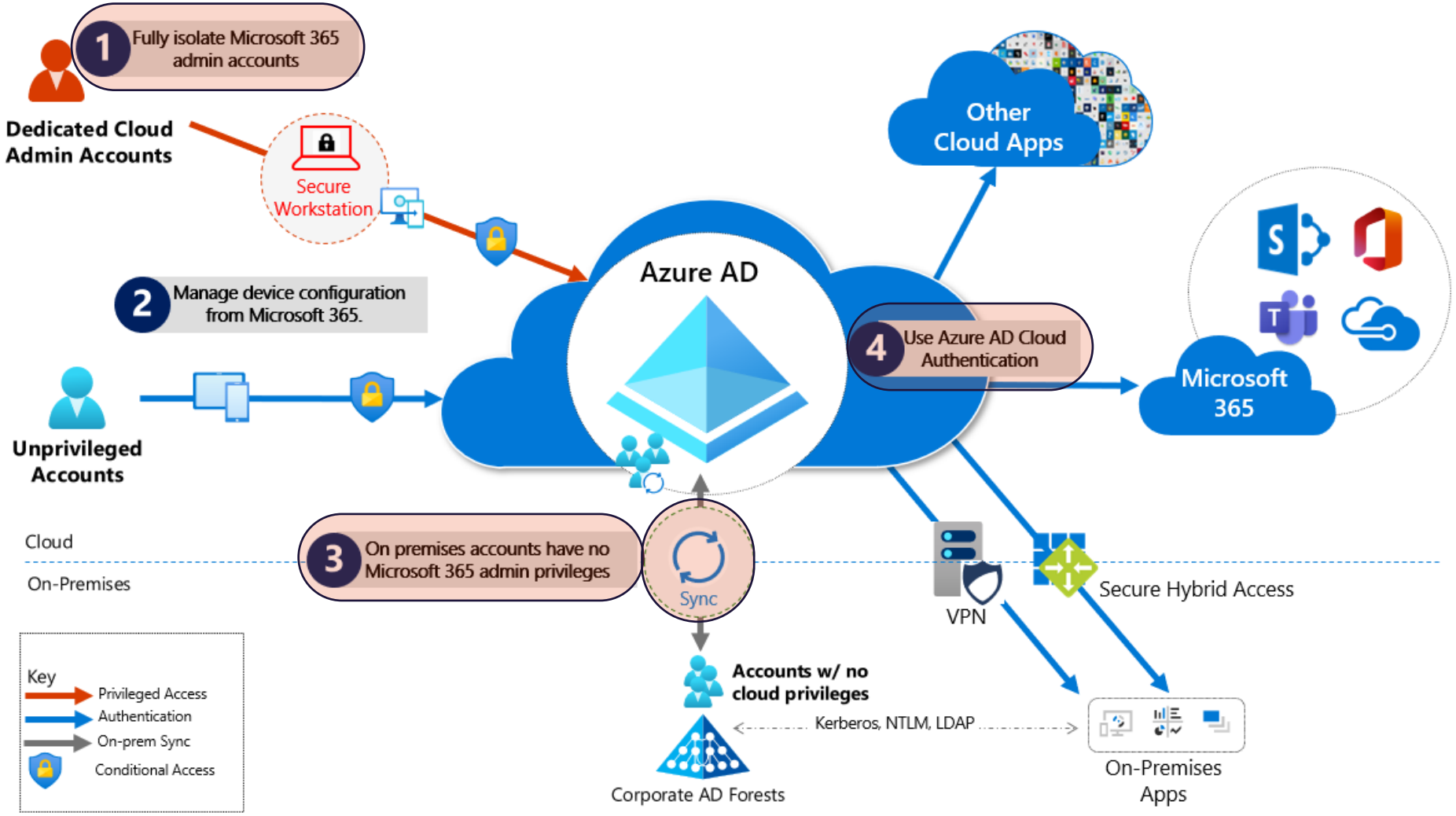
User Anomalies

Search

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

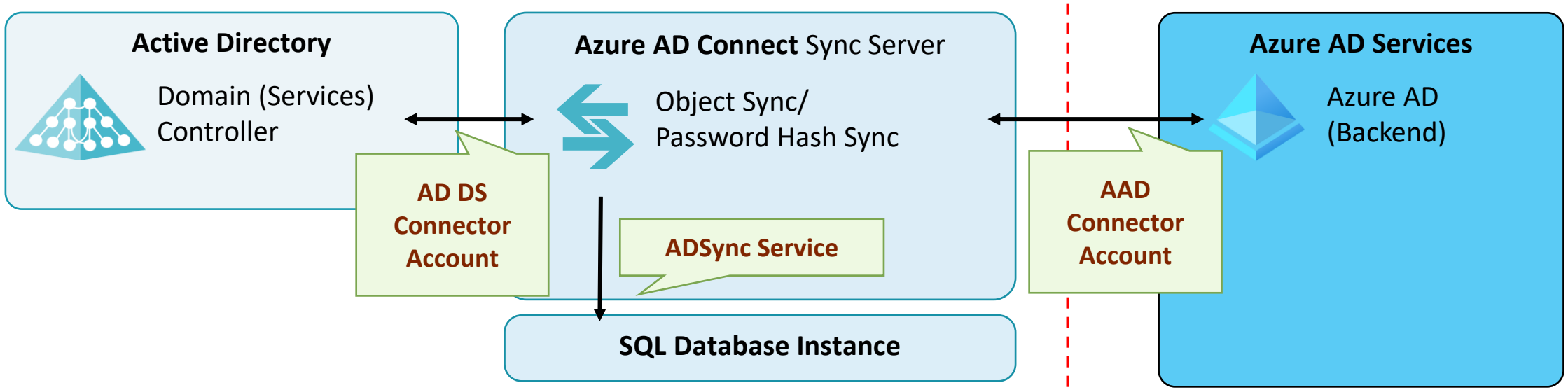

Default security settings
and usage of strong authentication methods
LIVE DEMO

Attack surface in hybrid identity environments



Source: Microsoft ("Protecting Microsoft 365 from on-premises attacks")

Attack surface by hybrid identity sync

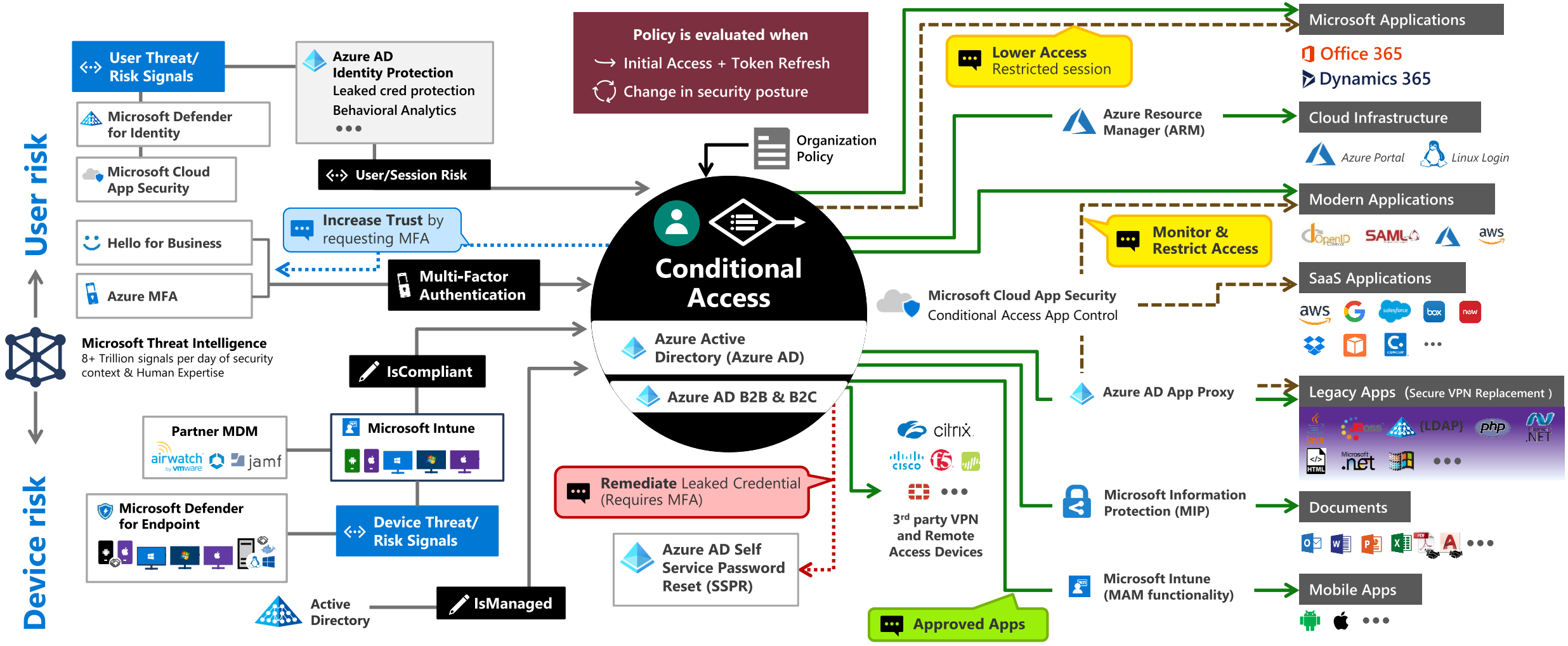



Privilege Escalation from
AAD Connect to Azure AD
LIVE DEMO

CONDITIONAL ACCESS AND TOKEN SECURITY

Conditional Access Overview

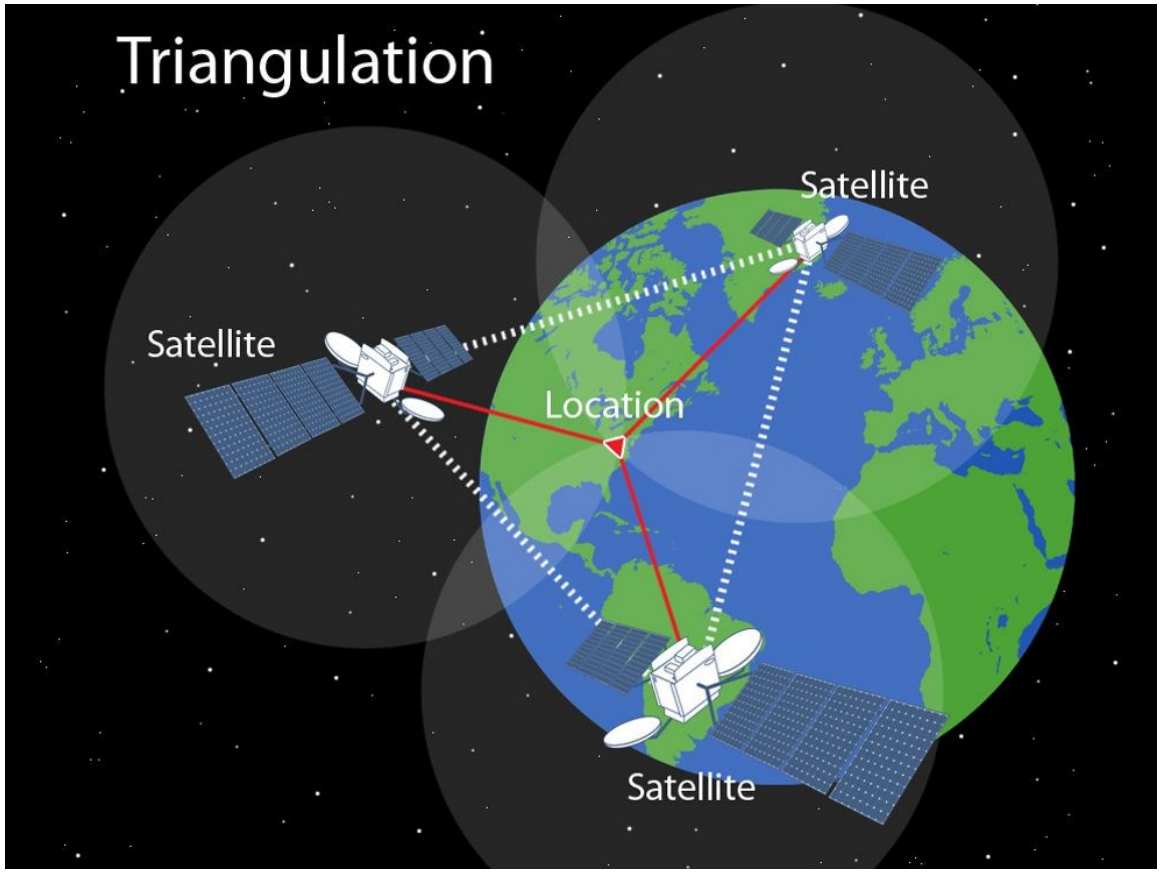
Image Source: Microsoft ("Zero Trust Definition and Models")



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



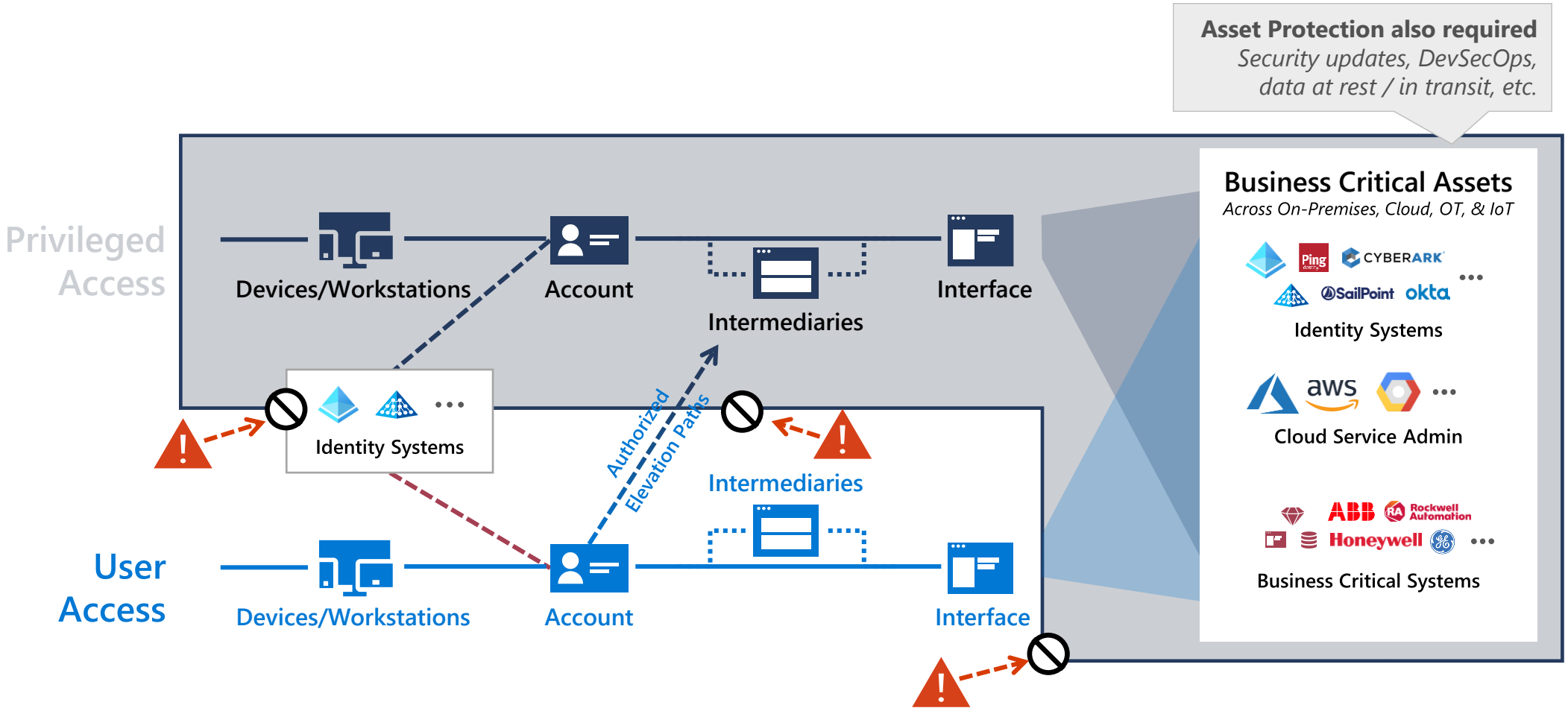
Conditional Access Baseline & CAE in action

Token Replay

LIVE DEMO

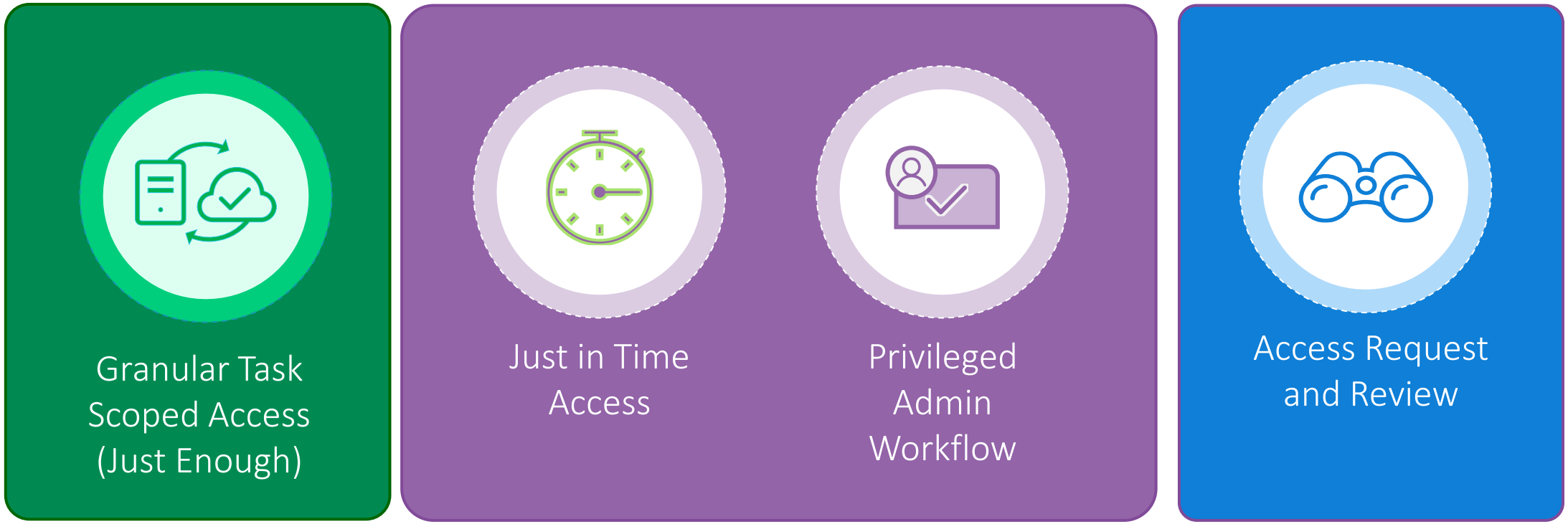
PRIVILEGED IDENTITY AND ACCESS

Authorized privileged and elevated paths



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

Foundation of Privileged Access



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**.“

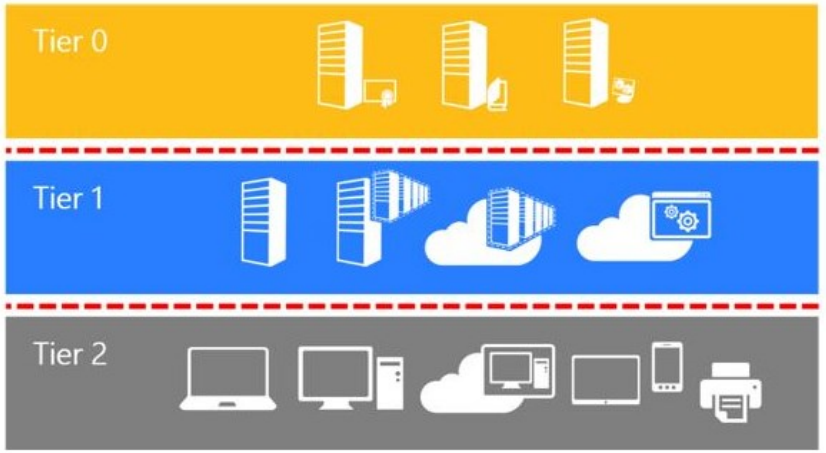
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8

Active Directory administrative tier model

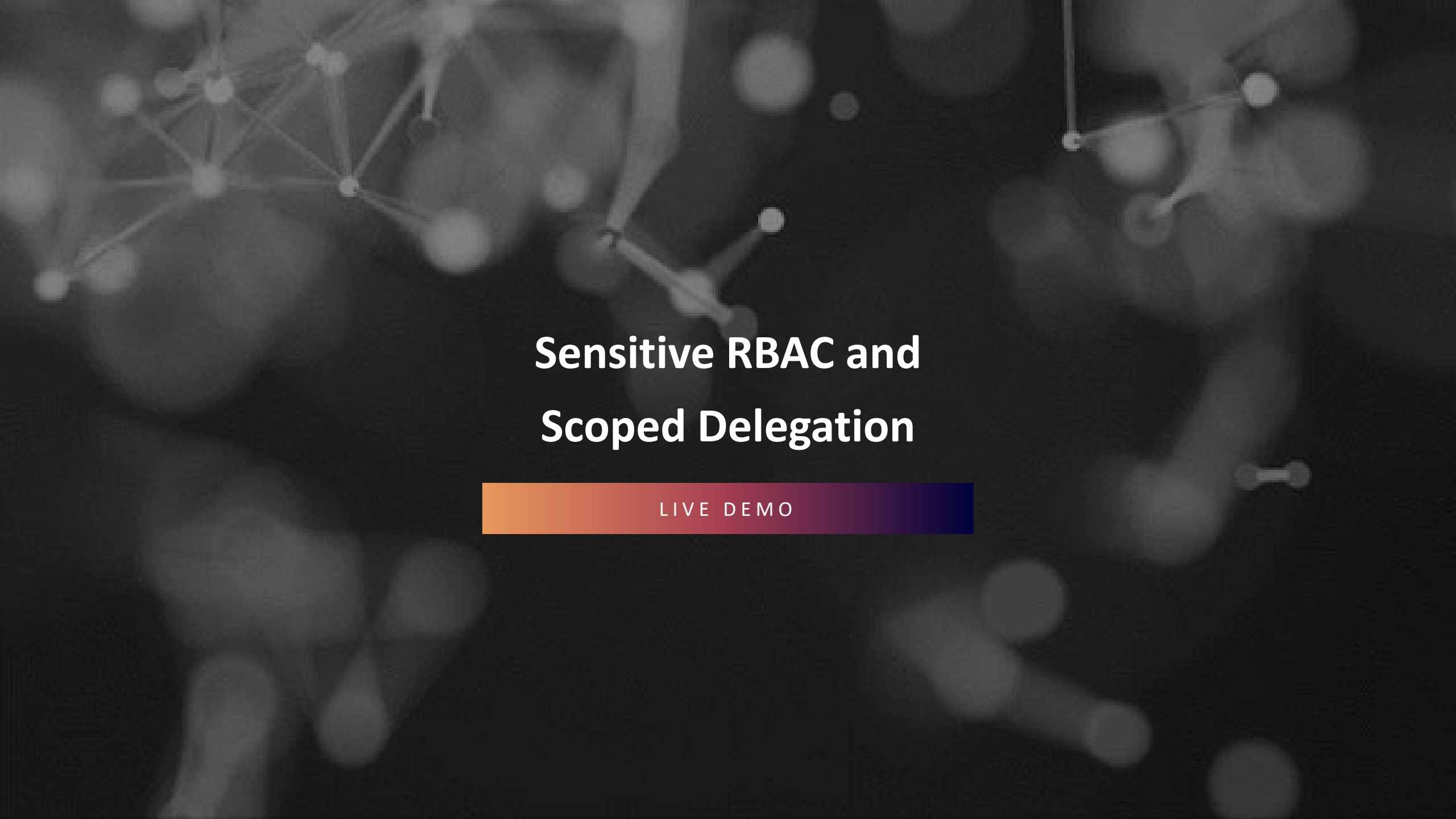
02/14/2019 • 33 minutes to read • +6

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.

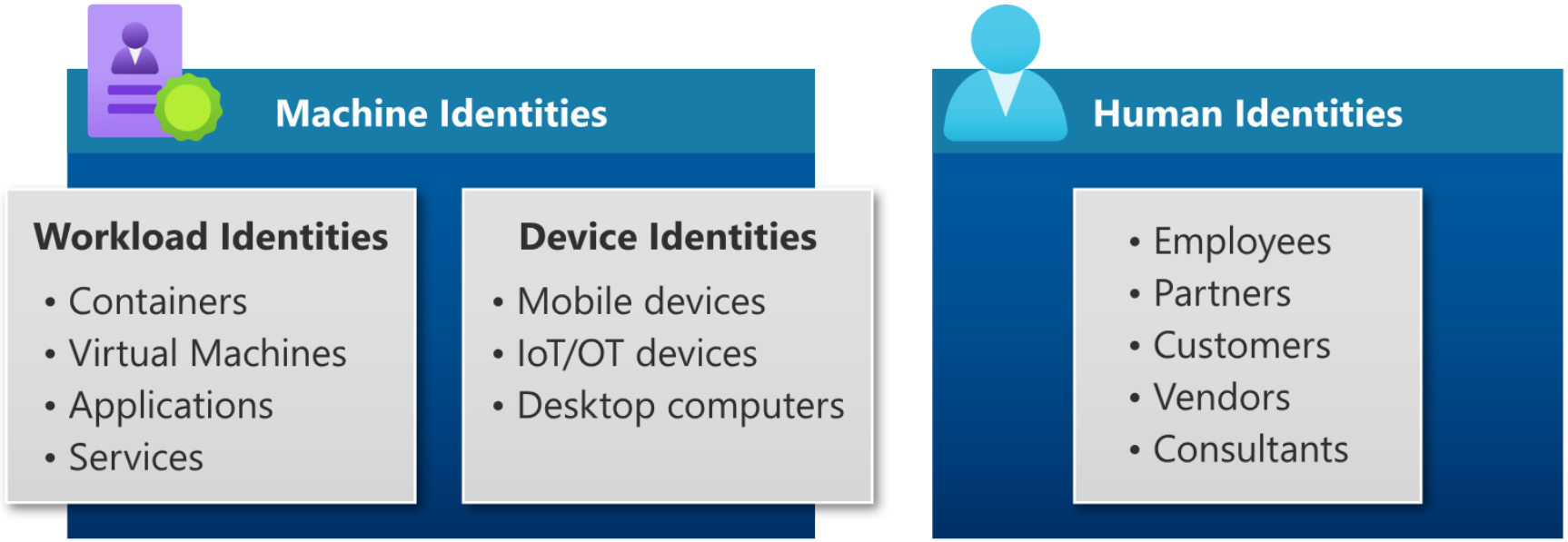


Source: “Securing Azure environments with Azure Active Directory”


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*

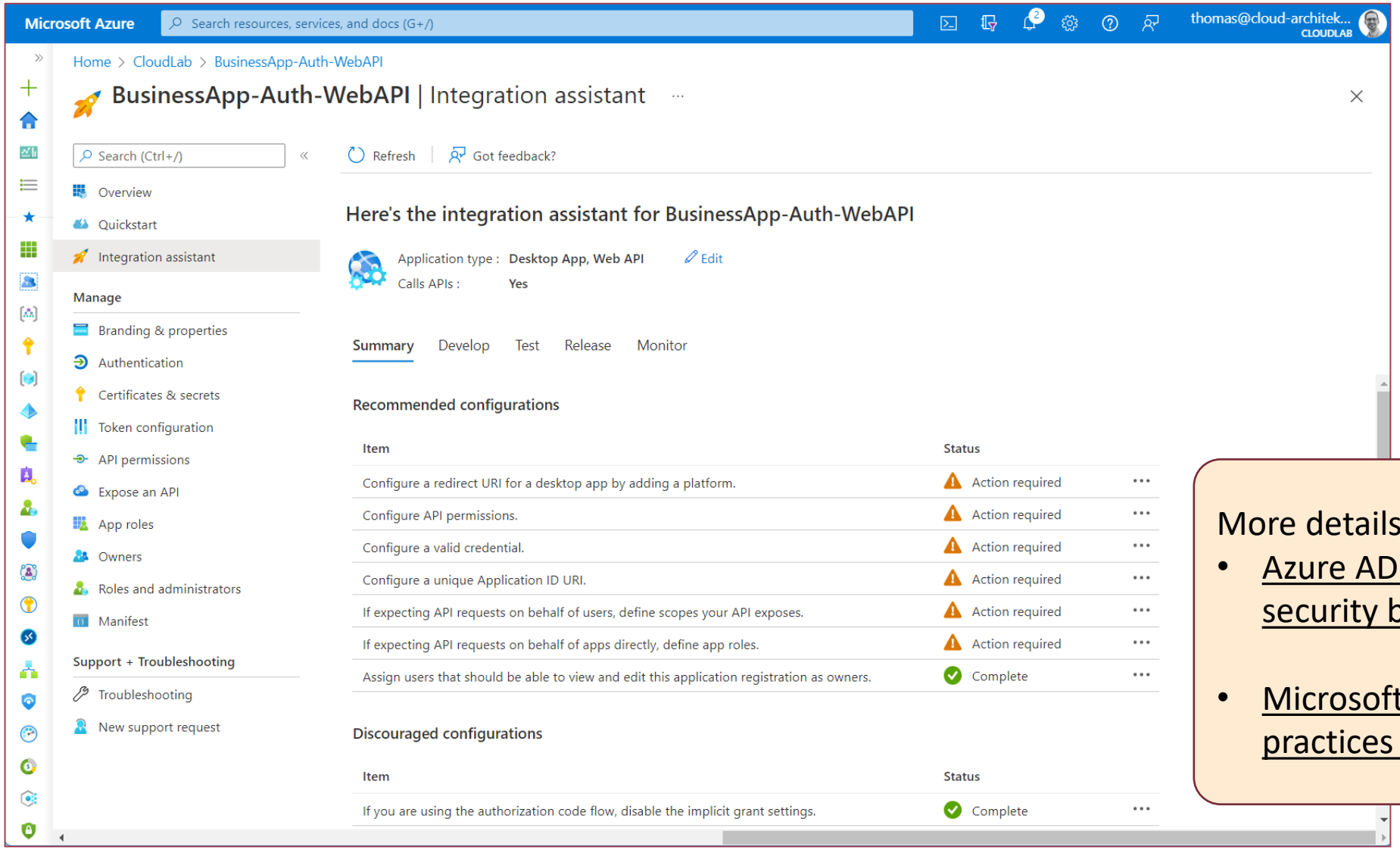
Types of workload identities

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

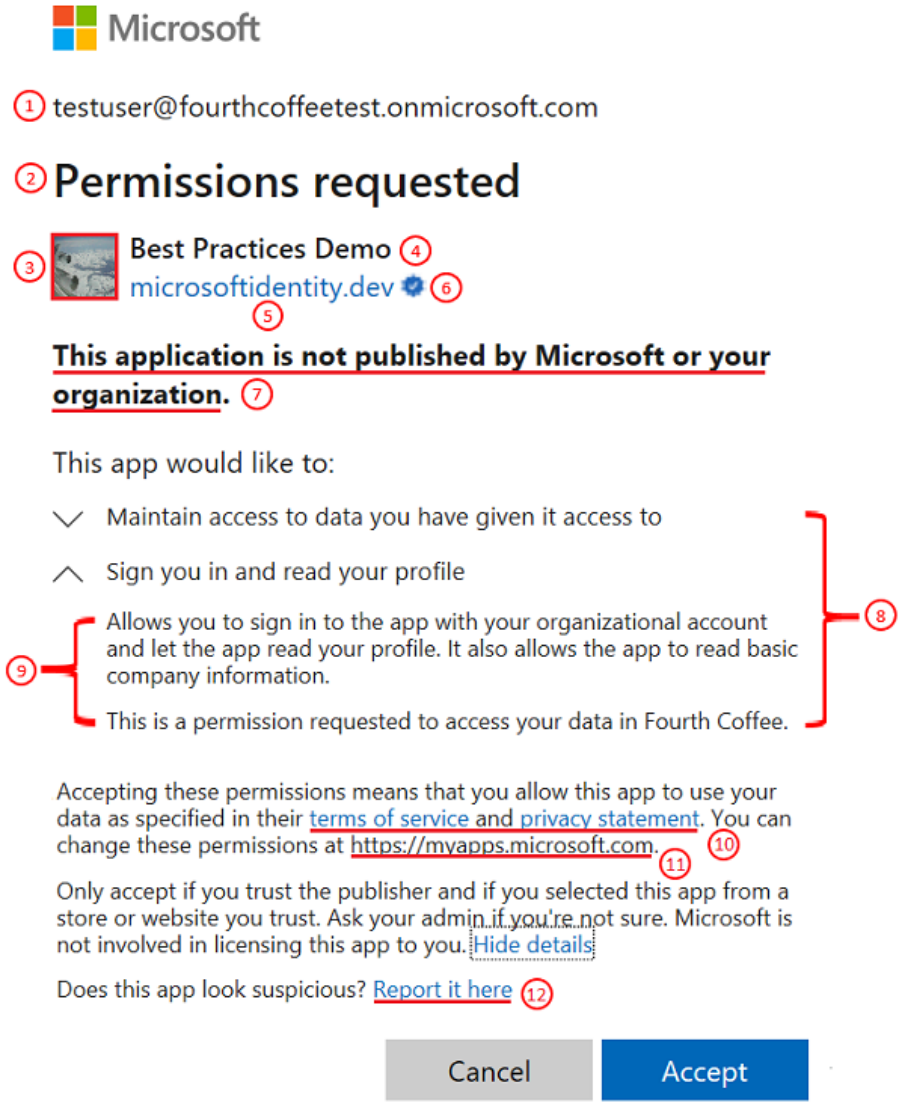
Security of App Integration



More details:

- Azure AD application registration security best practices
- Microsoft identity platform best practices and recommendations

App registration and consent grant



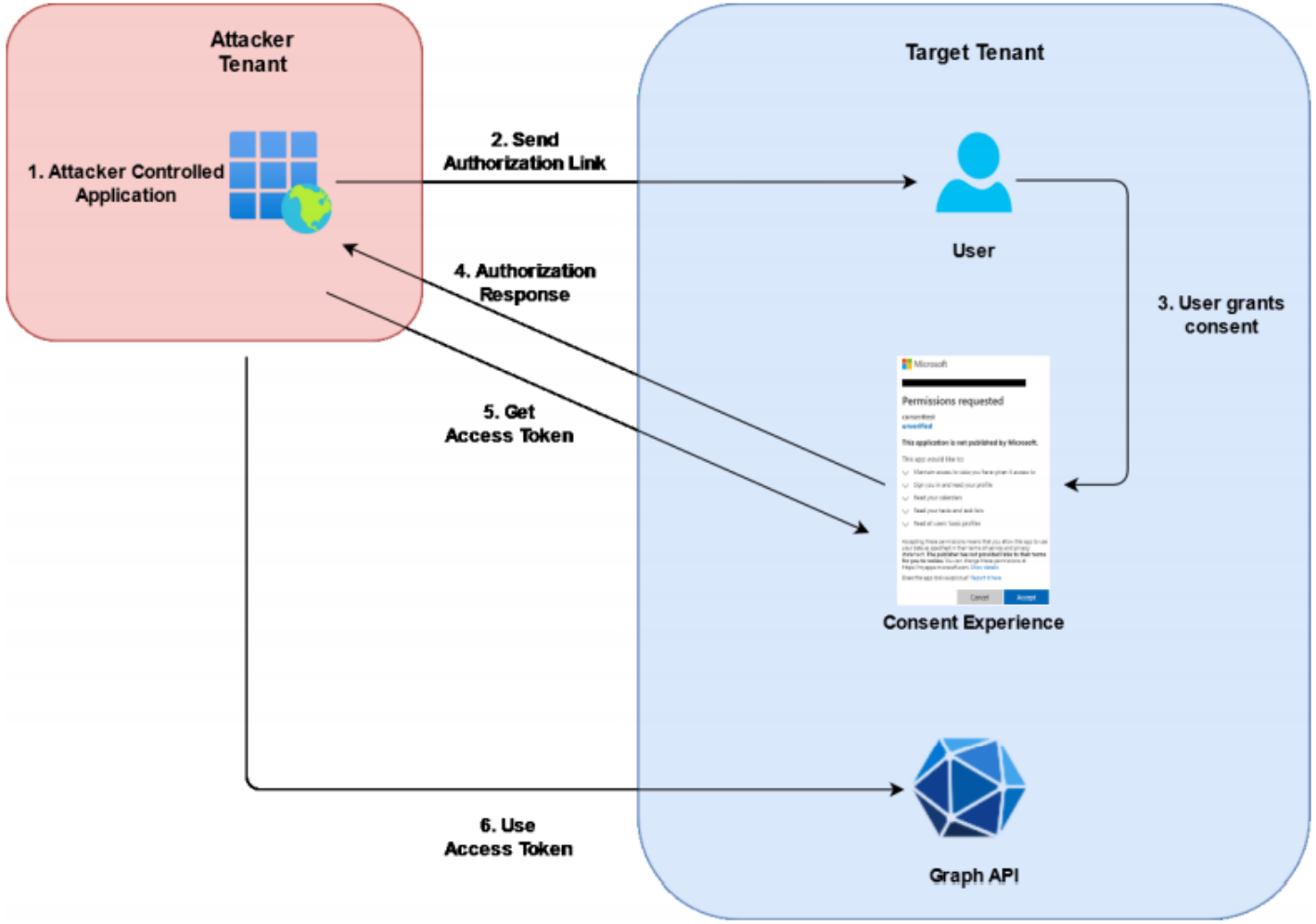


Image source: Introduction To 365-Stealer by Altered Security


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