#GSCC

Azure AD Identity Security Posture Management

Sponsor

Wir bedanken uns bei unseren Sponsoren ohne diese die Konferenz nicht möglich gewesen ist.

KS KöllnService KöllnService GmbH

noovic

Noovic GmbH

Microsoft

BTC

Thomas Naunheim

Cyber Security Architect
@glueckkanja-gab AG

Koblenz, Germany

@Thomas_Live

cloud-architekt.net

Microsoft® MVP Most Valuable Professional

CLOUD IDENTITY SUMMIT '23
Koblenz, Germany
Thu, September 7th, 2023

Cloud Inspires Podcast
Stories and people behind "Cloud Transformation"

Azure Meetup BONN

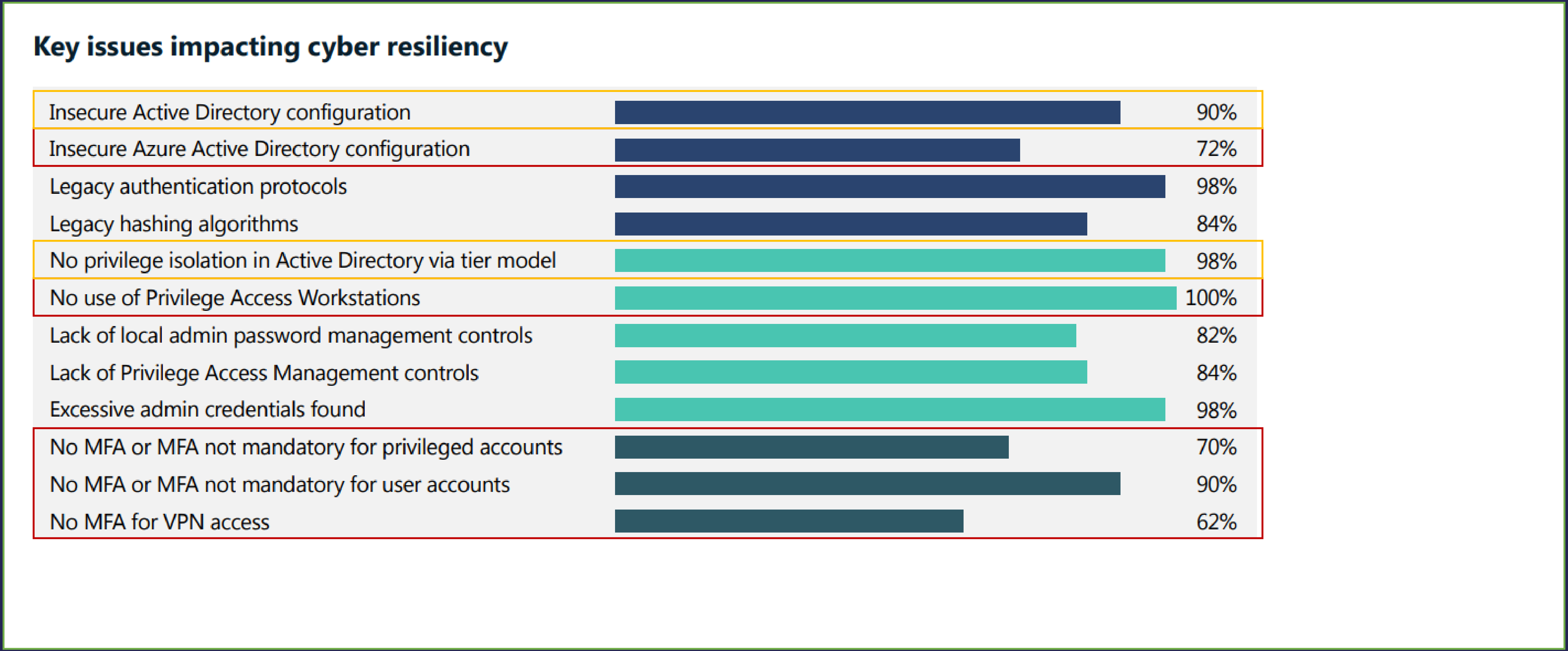
Agenda

- Key factors in Azure AD Cyber Resiliency
- Hybrid Identity Components
- Tenant (Default) Configuration
- Authentication Method and Token Security
- Conditional Access
- Privileged IAM

Key factors in Azure AD Cyber Resiliency

“Over 80% of security incidents can be traced to a few missing elements”

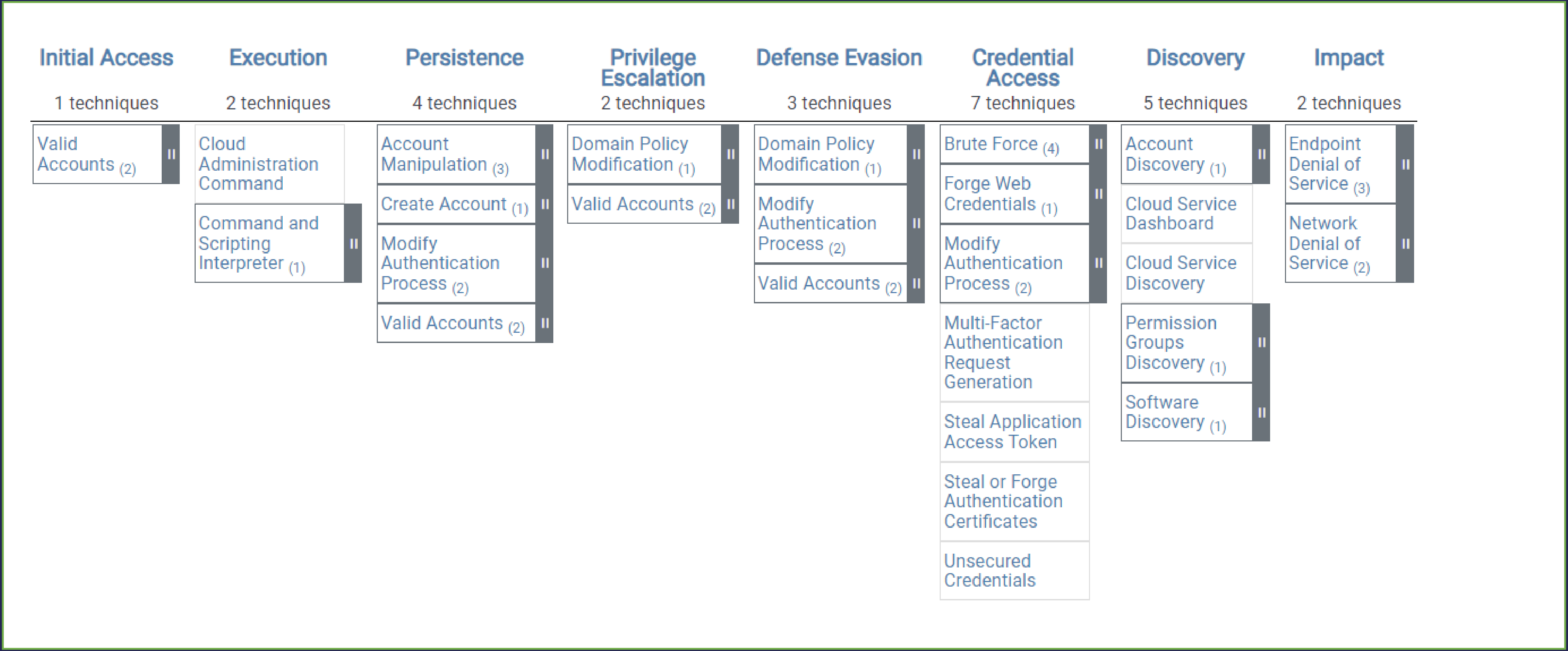
Image source: Microsoft Digital Defense Report 2022



Key issues impacting cyber resiliency

Techniques and Tactics related to Azure AD

Image source: MITRE ATT&CK (Azure AD Matrix)



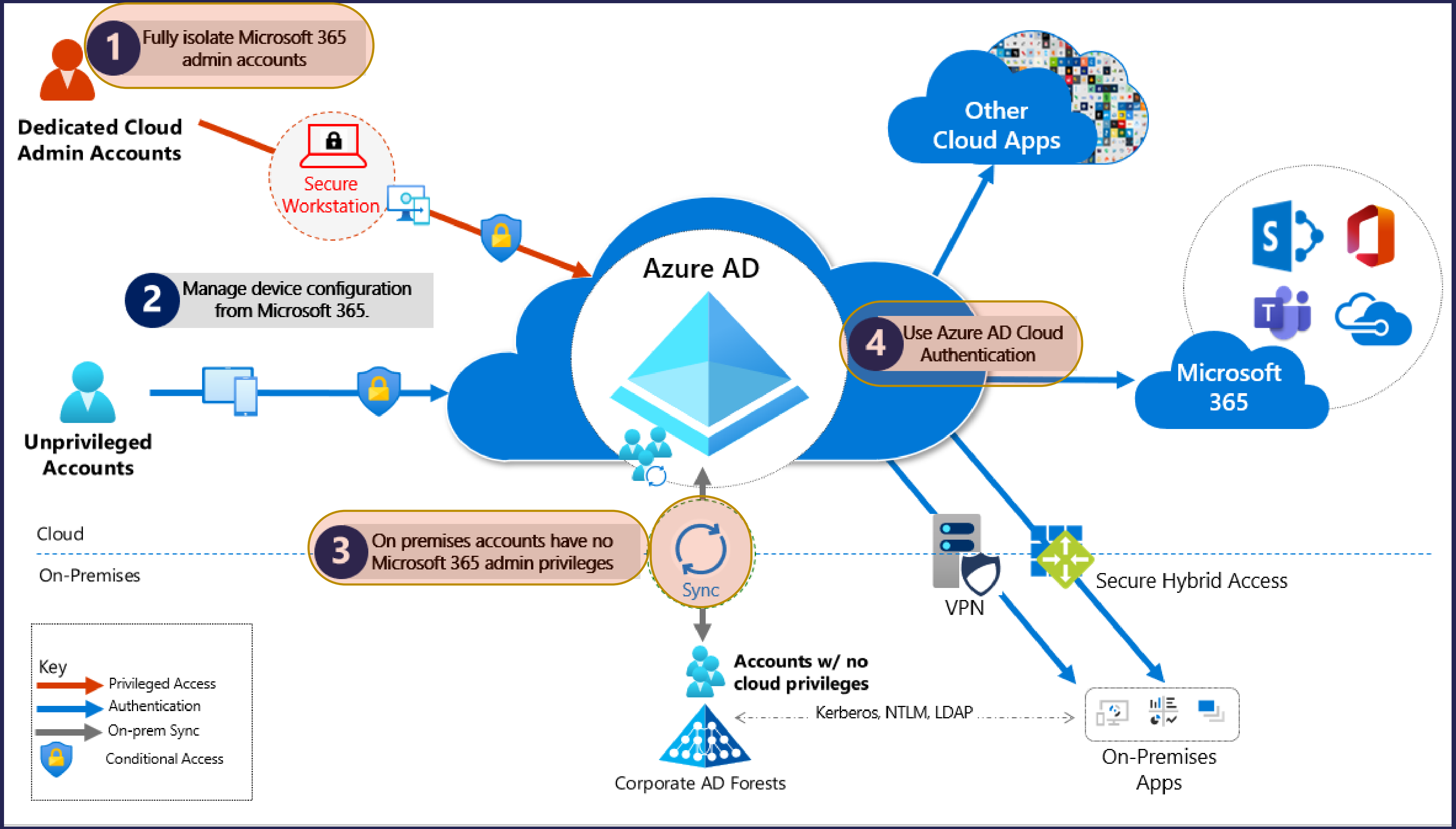
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
1 techniques	2 techniques	4 techniques	2 techniques	3 techniques	7 techniques	5 techniques	2 techniques
Valid Accounts (2)	Cloud Administration Command	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (1)	Endpoint Denial of Service (3)
	Command and Scripting Interpreter (1)	Create Account (1)	Valid Accounts (2)	Modify Authentication Process (2)	Forge Web Credentials (1)	Cloud Service Dashboard	Network Denial of Service (2)
		Modify Authentication Process (2)		Valid Accounts (2)	Modify Authentication Process (2)	Cloud Service Discovery	
		Valid Accounts (2)			Multi-Factor Authentication Request Generation	Permission Groups Discovery (1)	
					Steal Application Access Token	Software Discovery (1)	
					Steal or Forge Authentication Certificates		
					Unsecured Credentials		

Hybrid Identity Components

Reduce dependencies to your on-premises infrastructure

Attack surface by hybrid identity sync

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

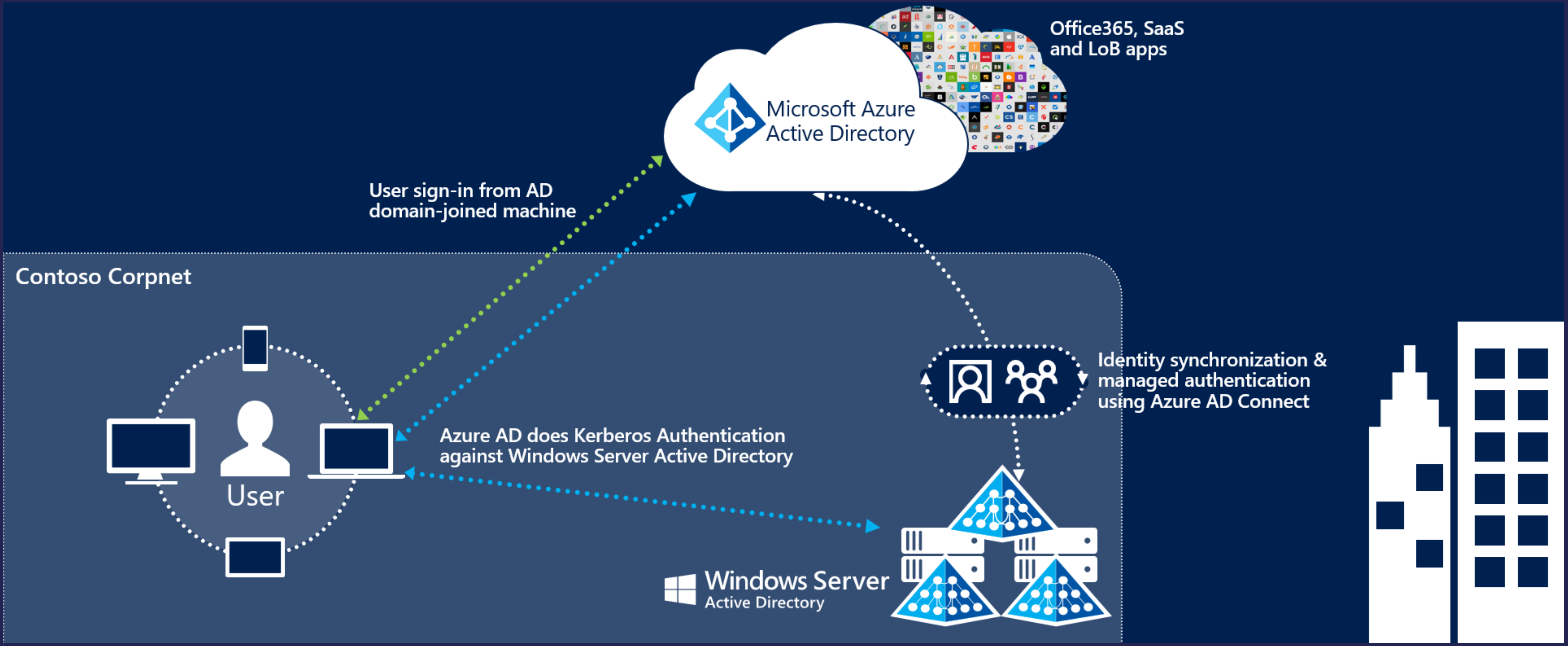


1 Fully isolate Microsoft 365 admin accounts
Dedicated Cloud Admin Accounts
Secure Workstation
Other Cloud Apps
Azure AD
2 Manage device configuration from Microsoft 365.
4 Use Azure AD Cloud Authentication
Microsoft 365
Unprivileged Accounts
Cloud
On-Premises
3 On premises accounts have no Microsoft 365 admin privileges
Sync
VPN
Secure Hybrid Access
Accounts w/ no cloud privileges
Kerberos, NTLM, LDAP
Corporate AD Forests
On-Premises Apps
Key
Privileged Access
Authentication
On-prem Sync
Conditional Access

Attack surface "Azure AD Seamless SSO"

Kerberos Attacks to gain access to cloud resources

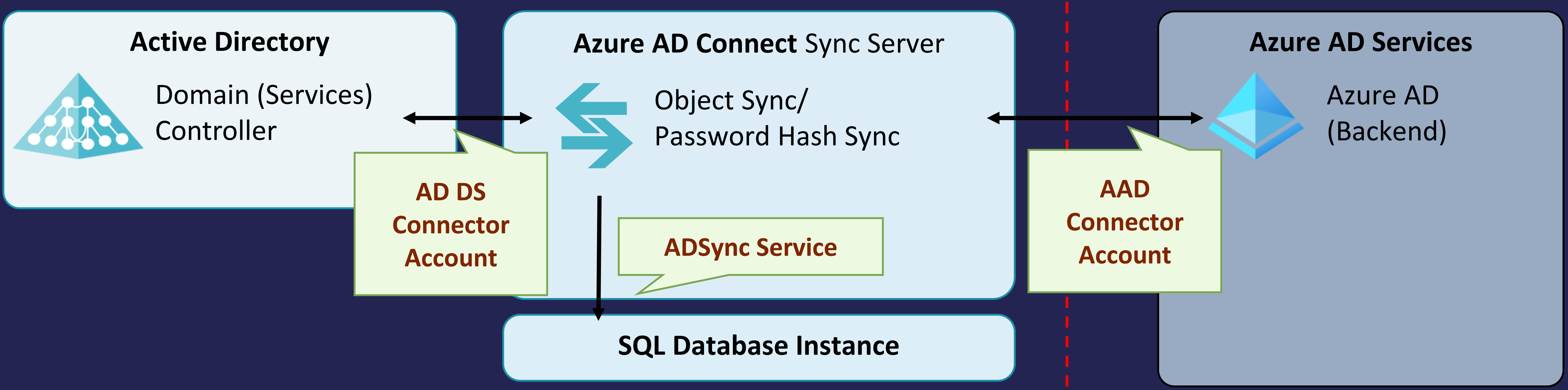
Image Source: Microsoft ("Azure Active Directory Seamless single sign-on")



Office365, SaaS and LoB apps
Microsoft Azure Active Directory
User sign-in from AD domain-joined machine
Contoso Corpnet
Identity synchronization & managed authentication using Azure AD Connect
User
Azure AD does Kerberos Authentication against Windows Server Active Directory
Windows Server Active Directory

Azure AD Connect Sync Server

Privileges and keys to both worlds



Active Directory

Domain (Services) Controller

Azure AD Connect Sync Server

Object Sync/ Password Hash Sync

Azure AD Services

Azure AD (Backend)

AD DS Connector Account

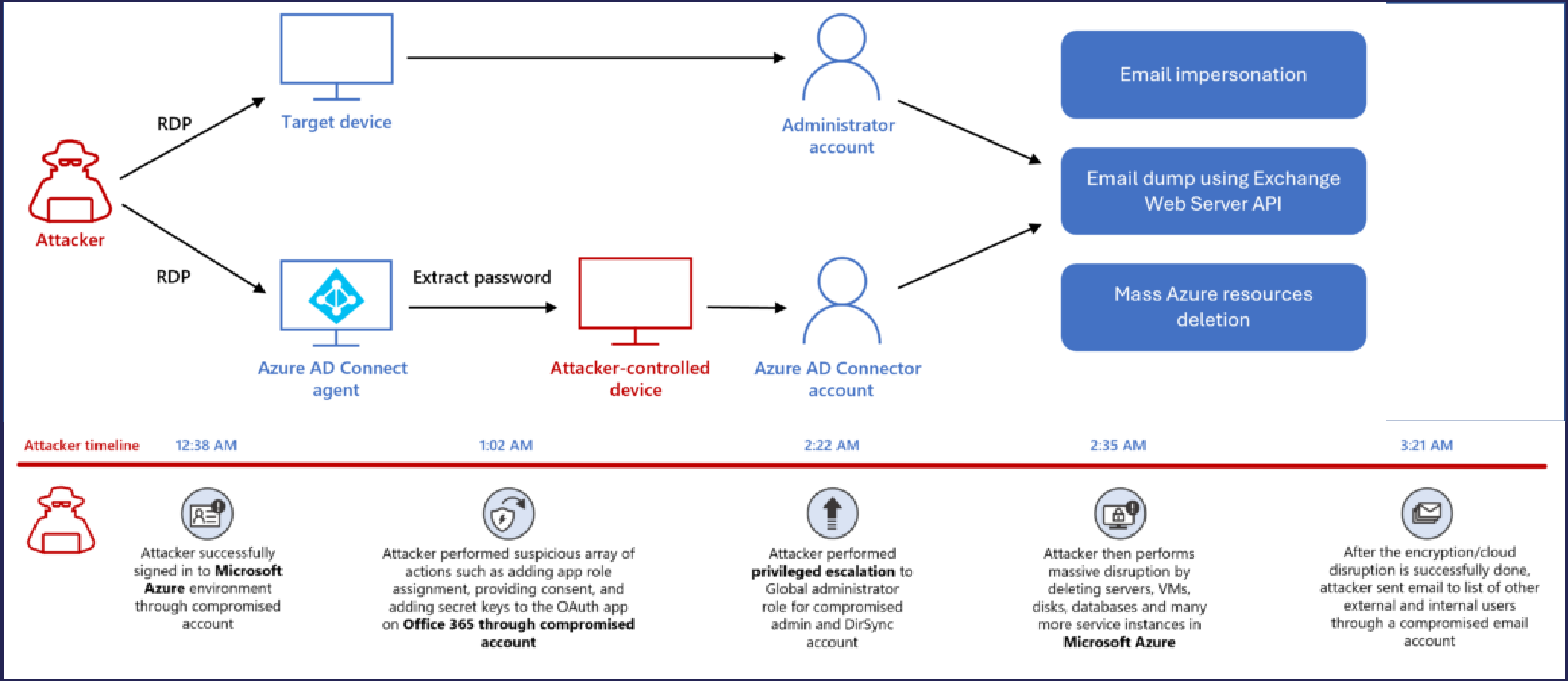
ADSync Service

AAD Connector Account

SQL Database Instance

Attack and abuse of Azure AD Connector Account

Source: Microsoft ("MERCURY and DEV-1084: Destructive attack on hybrid environment")



12:38 AM: Attacker successfully signed in to **Microsoft Azure** environment through compromised account

1:02 AM: Attacker performed suspicious array of actions such as adding app role assignment, providing consent, and adding secret keys to the OAuth app on **Office 365 through compromised account**

2:22 AM: Attacker performed **privileged escalation** to Global administrator role for compromised admin and DirSync account

2:35 AM: Attacker then performs massive disruption by deleting servers, VMs, disks, databases and many more service instances in **Microsoft Azure**

3:21 AM: After the encryption/cloud disruption is successfully done, attacker sent email to list of other external and internal users through a compromised email account

Demo: Sensitive Settings on Azure AD Connect

Azure AD Security Posture Management | Summary

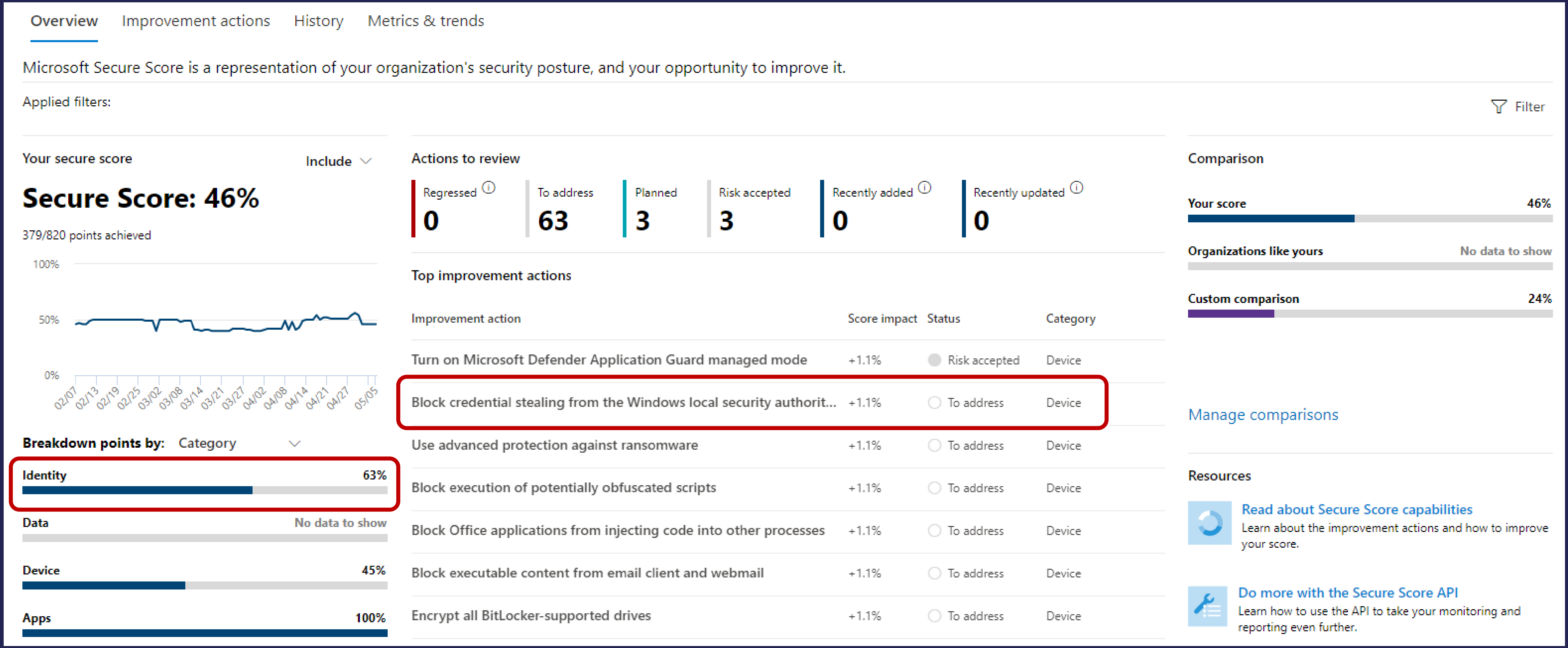
**Active Directory &
AAD Connect Sync Server**

- Microsoft Defender Vulnerability Management of installed components (incl. AADC, SQL, .NET, VC)
- **Get-MsolDirSyncFeatures (Soft/Hard Match settings)**
- Microsoft Defender for Identity (MDI) sensor health alerts and coverage on AD Domain Controllers
- MDI security posture assessments
- **Configuration of AADC sync rules and scopes**
- **ACEs and monitoring on AADC service accounts**

Tenant (Default) Configuration

Secure by default? (Regular) review and audit of tenant-level settings

Microsoft Secure Score



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

Applied filters:

Your secure score

Secure Score: 46%

379/820 points achieved

Breakdown points by: Category

Identity	63%
Data	No data to show
Device	45%
Apps	100%

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
0	63	3	3	0	0

Top improvement actions

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

Comparison

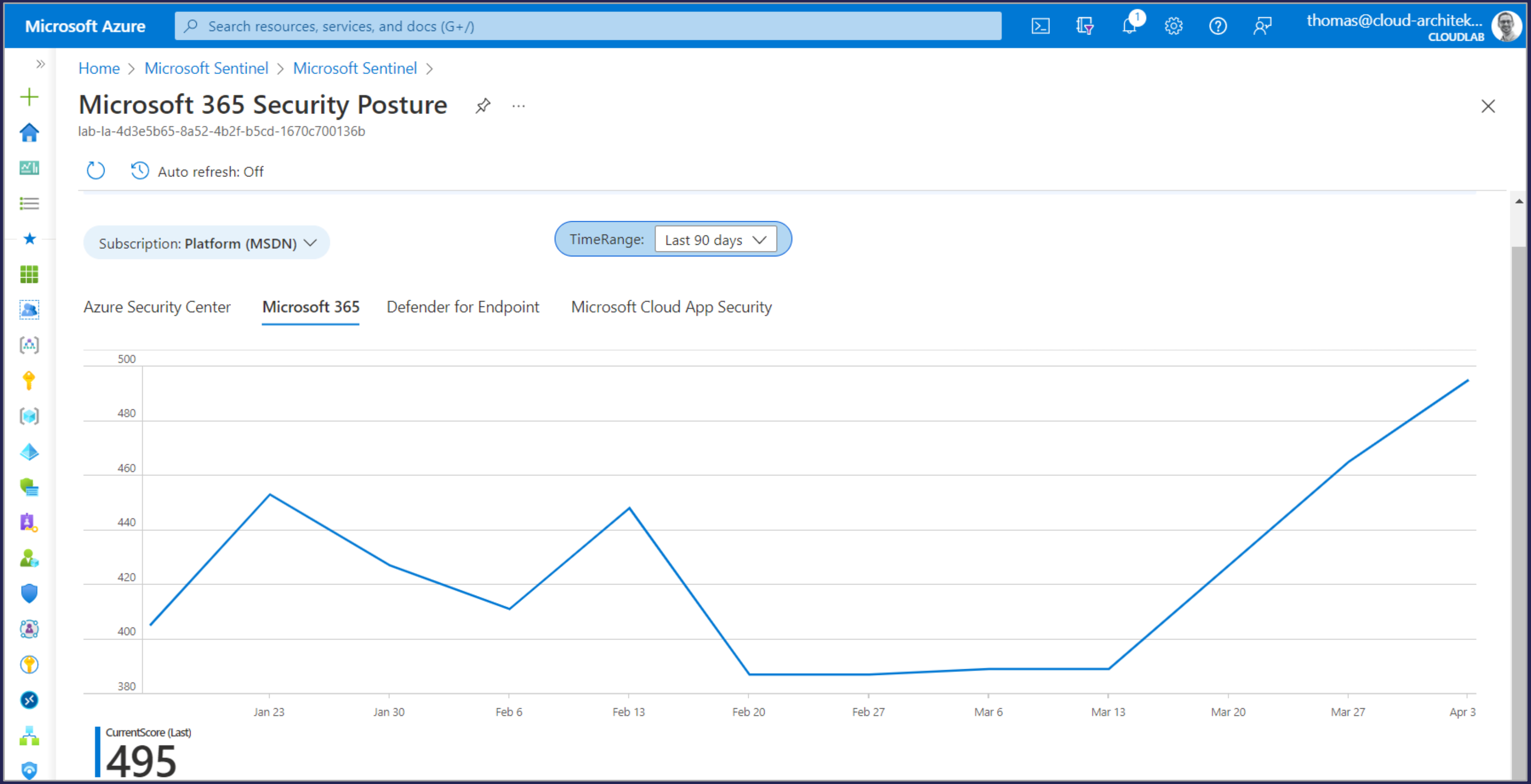
Your score	46%
Organizations like yours	No data to show
Custom comparison	24%

Resources

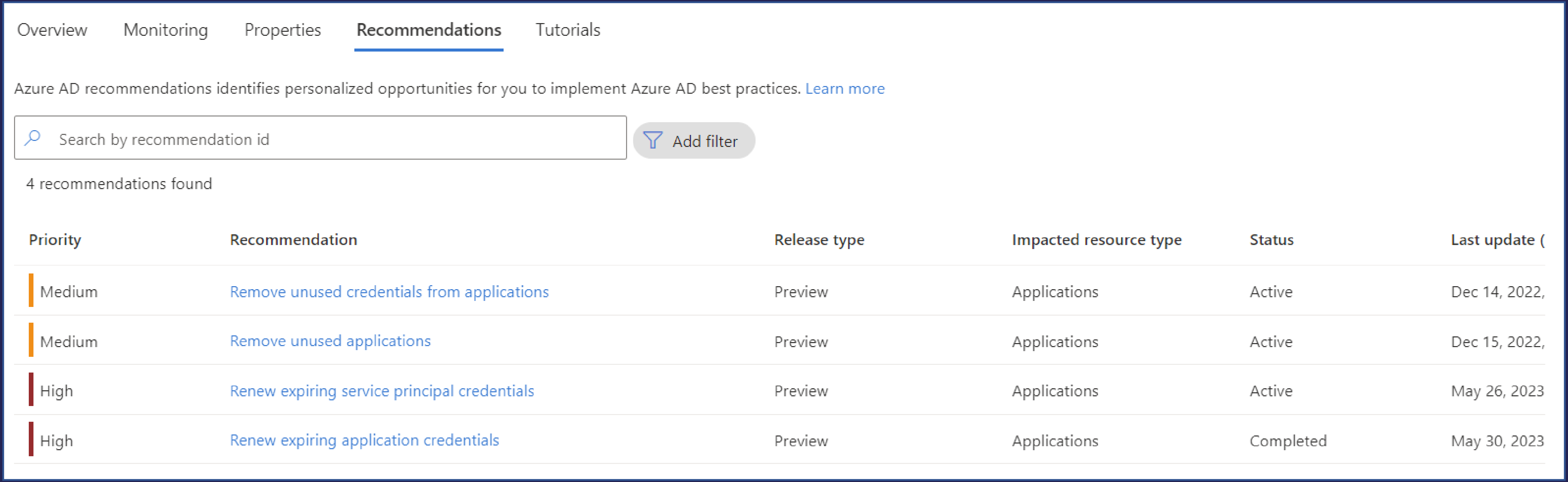
Read about Secure Score capabilities
Learn about the improvement actions and how to improve your score.

Do more with the Secure Score API
Learn how to use the API to take your monitoring and reporting even further.

Operationalization of Microsoft Secure Score



Azure AD Recommendations



Azure AD recommendations identifies personalized opportunities for you to implement Azure AD best practices. Learn more

4 recommendations found

Priority	Recommendation	Release type	Impacted resource type	Status	Last update (
Medium	Remove unused credentials from applications	Preview	Applications	Active	Dec 14, 2022,
Medium	Remove unused applications	Preview	Applications	Active	Dec 15, 2022,
High	Renew expiring service principal credentials	Preview	Applications	Active	May 26, 2023
High	Renew expiring application credentials	Preview	Applications	Completed	May 30, 2023

Demo: Default and Recommended Settings

Azure AD Security Posture Management | Summary

Active Directory & AAD Connect Sync Server

- Microsoft Defender Vulnerability Management of installed components (incl. AADC, SQL, .NET, VC)
- Get-MsolDirSyncFeatures (Soft/Hard Match settings)
- Microsoft Defender for Identity (MDI) sensor health alerts and coverage on AD Domain Controllers
- MDI security posture assessments
- Configuration of AADC sync rules and scopes
- ACEs and monitoring on AADC service accounts

Azure AD Configuration and Reporting

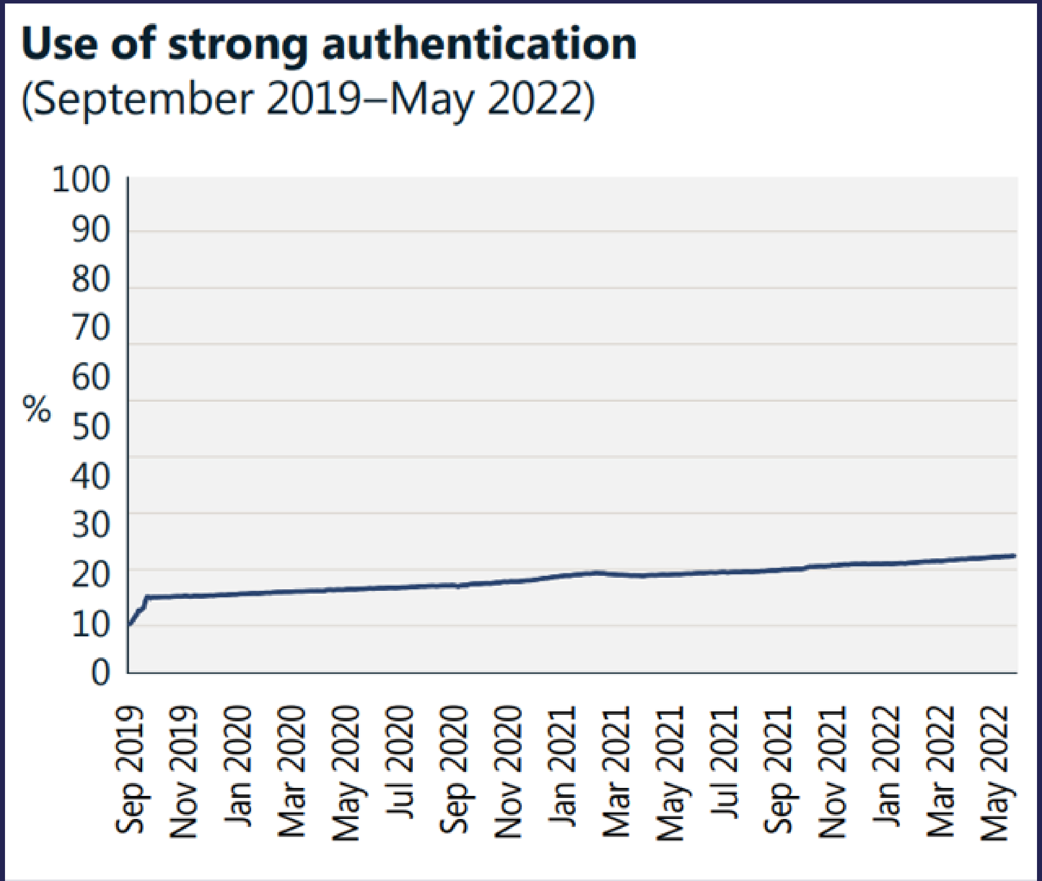
- Identity Secure Score
- AAD Recommendations
- Authentication Prompts Analysis Workbook
- Sign-in Analysis and other Operational Workbooks
- **Scenario Health and token issuance by Backup Authentication Service**
- **Tenant Restriction (V2)**
- Tracking changes of configuration endpoints (for example, Authorization Policy) via Microsoft Graph API (e.g., AADSCA)

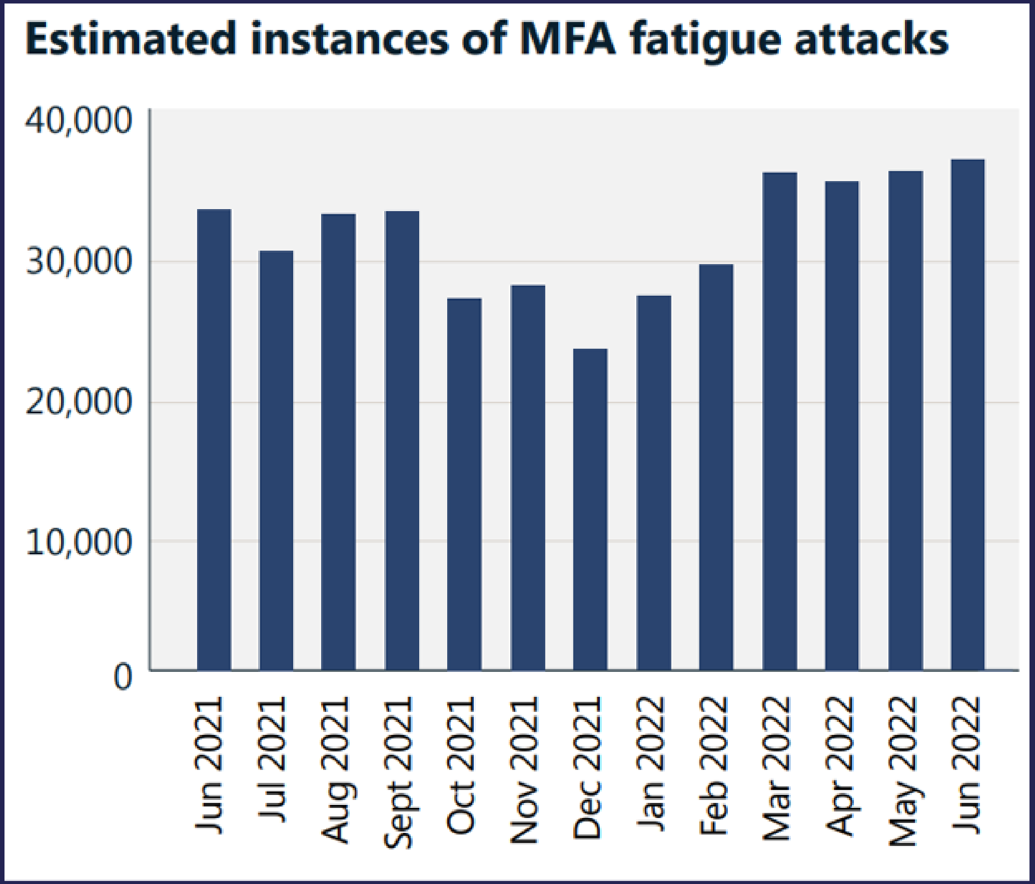
Authentication & Token

Strong phishing-resistant authentication and protected tokens

Multifactor authentication attacks

Image source: Microsoft Digital Defense Report 2022





Security and resiliency of Authentication methods

Image source: Microsoft Secure ("How identity security protects the bottom line")

Bad:
Password

- 123456
- qwerty
- password
- iloveyou
- Password1

Good:
Password and…

- SMS
- Voice

Better:
Password and…

- Microsoft Authenticator
- Software Tokens OTP
- Hardware Tokens OTP

Best:
Passwordless and Phishing resistant

- Windows Hello *
- Certificate-based authentication*
- FIDO2 security key *
- Microsoft Authenticator

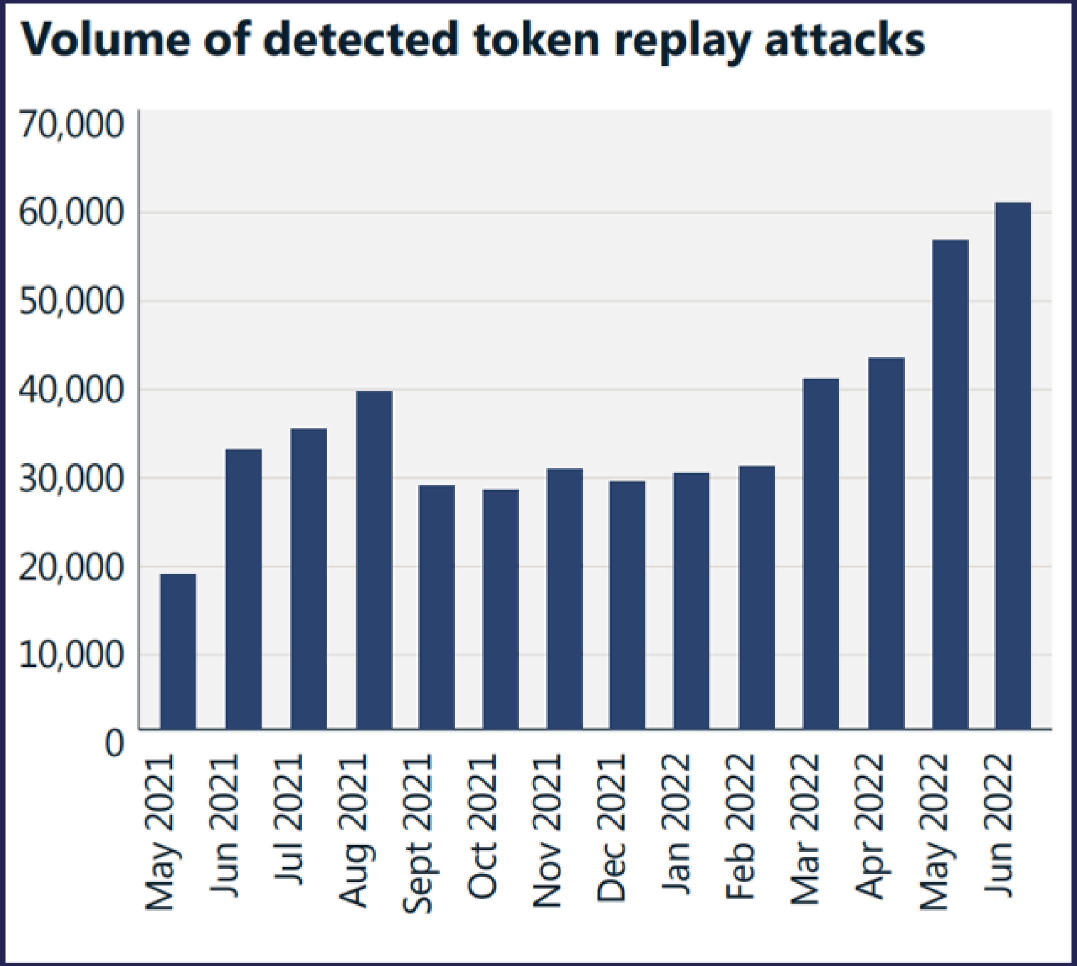
* Phishing-resistant MFA

Maturity Levels

Demo: Authentication Methods Analyses and Security

Post-Authentication Attacks

Image source: Microsoft Digital Defense Report 2022



Security Advantages of implementing Windows Hello for Business and ITDR in Azure AD

- Enforcement of TPM encryption	→ TPM protected private keys	⊖ PRT Replay
- No grace period of Intune compliance	→ Verify TPM Health immediately	⊖ TPM Bypass
- Require PIN or Biometrics	→ Device-bounded credentials	⊖ Password Replay, Phishing
- Authentication via WAM	→ Token Protection Capability	⊖ Token Replay

- Integrated XDR to Identity Protection	→ Anomaly & Endpoint Signals	⚠ Detection and Remediation
- Supported apps and signals to CAE	→ Revoke sessions and tokens	of Post-Authentication Attacks

Demo: Windows Hello Configuration and XDR Signals

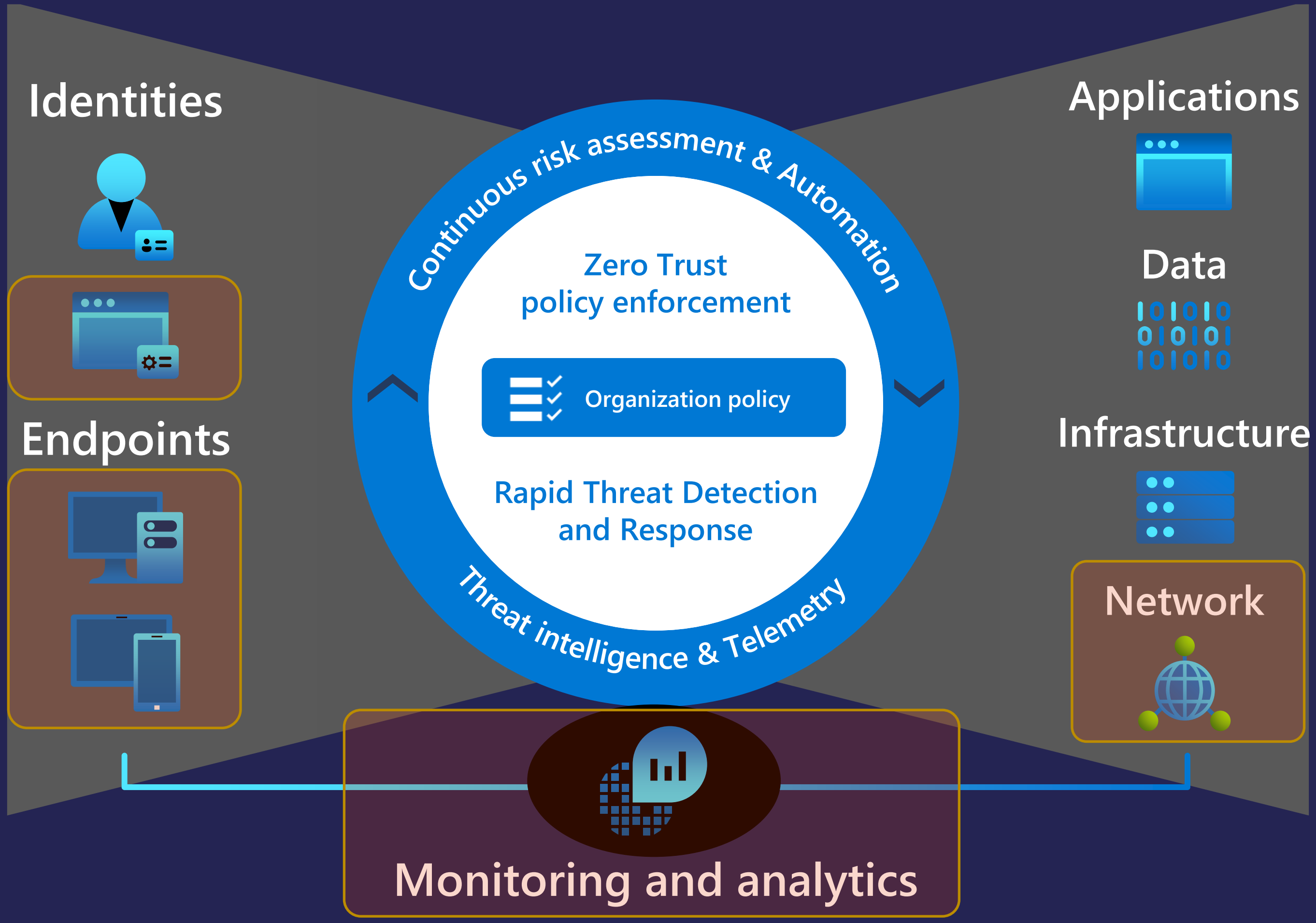
Conditional Access

Enforce a strong baseline and policy design to verify every access explicitly

Conditional Access Baseline Design

Ensure to protect every user and every app by minimal but strong baseline!
Avoid inconsistent or duplicated policies by smart policy design!

Conditional Access Baseline Design



Demo: Analyses of CA Coverage and Policy Change Tracking

Azure AD Security Posture Management | Summary

Active Directory & AAD Connect Sync Server

- Microsoft Defender Vulnerability Management of installed components (incl. AADC, SQL, .NET, VC)
- Get-MsolDirSyncFeatures (Soft/Hard Match settings)
- Microsoft Defender for Identity (MDI) sensor health alerts and coverage on AD Domain Controllers
- MDI security posture assessments
- Configuration of AADC sync rules and scopes
- ACEs and monitoring on AADC service accounts

Azure AD Configuration and Reporting

- Identity Secure Score
- AAD Recommendations
- Authentication Prompts Analysis Workbook
- Sign-in Analysis and other Operational Workbooks
- Scenario Health and token issuance by Backup Authentication Service
- Tenant Restriction (V2)
- Tracking changes of configuration endpoints (for example, Authorization Policy) via Microsoft Graph API (e.g., AADSCA)

Security Policies & Threat Detection

- Authentication Methods Activity (Register, Usage) and SSPR Reports
- Windows Hello for Business Policy (incl. Require TPM)
- Token Protection capability
- Conditional Access Security Alerts, Gaps and Insights
- Policy Effectiveness (WhatIf, Sign-in Logs) and Change Tracking (e.g., AADOps)
- **Identity Protection risk statistics (Dashboard/API)**
- **Health status of analytics rules, playbooks and data connector in Sentinel**

Privileged IAM

Foundation of Privileged Identity & Access Management

Granular Task Scoped Access (Just Enough)

Just in Time Access

Privileged Admin Workflow

Access Request and Review

Entra Permissions Management & App Governance

Privileged Identity Management (PIM)

Identity Governance (Entra ID Governance)

Demo: Analyses of Privileged Identites & Access

Azure AD Security Posture Management | Summary

Active Directory & AAD Connect Sync Server

- Microsoft Defender Vulnerability Management of installed components (incl. AADC, SQL, .NET, VC)
- Get-MsolDirSyncFeatures (Soft/Hard Match settings)
- Microsoft Defender for Identity (MDI) sensor health alerts and coverage on AD Domain Controllers
- MDI security posture assessments
- Configuration of AADC sync rules and scopes
- ACEs and monitoring on AADC service accounts

Azure AD Configuration and Reporting

- Identity Secure Score
- AAD Recommendations
- Authentication Prompts Analysis Workbook
- Sign-in Analysis and other Operational Workbooks
- Scenario Health and token issuance by Backup Authentication Service
- Tenant Restriction (V2)
- Tracking changes of configuration endpoints (for example, Authorization Policy) via Microsoft Graph API (e.g., AADSCA)

Security Policies & Threat Detection

- Authentication Methods Activity (Register, Usage) and SSPR Reports
- Windows Hello for Business Policy (incl. Require TPM)
- Token Protection capability
- Conditional Access Security Alerts, Gaps and Insights
- Policy Effectiveness (WhatIf, Sign-in Logs) and Change Tracking (e.g., AADOps)
- Identity Protection risk statistics (Dashboard/API)
- Health status of analytics rules, playbooks and data connector in Sentinel

Identity Governance and Entitlement Management

- Azure AD Privileged Identity Management (PIM) Discovery and insights
- PIM Alerts for Azure AD roles and Azure roles
- **Insights and Reporting in Identity Governance**
- **Health of Lifecycle Workflows schedules**
- PCI Score and Analytics in Entra Permissions Management
- Tracking changes of connected organizations, assignments and delegations on catalogs and access packages

Application and Workload Identities

- Usage & Insights Reports about application, service principal sign-in and credential activity
- Attack Paths and Cloud Security Explorer query in Microsoft Defender for Cloud
- MDA App Governance Policy Alerts (for example unused API permissions)
- Microsoft Cloud Security Benchmark (MCSB) Controls related to Identity Management or Privileged Access

Azure AD Security Posture Management | Summary

Active Directory & AAD Connect Sync Server

- Microsoft Defender Vulnerability Management of installed components (incl. AADC, SQL, .NET, VC)
- Get-MsolDirSyncFeatures (Soft/Hard Match settings)
- Microsoft Defender for Identity (MDI) sensor health alerts and coverage on AD Domain Controllers
- MDI security posture assessments
- Configuration of AADC sync rules and scopes
- ACEs and monitoring on AADC service accounts

Azure AD Configuration and Reporting

- Identity Secure Score
- AAD Recommendations
- Authentication Prompts Analysis Workbook
- Token Protection capability and Tenant Restriction (V2)
- Sign-in Analysis and other Operational Workbooks
- Scenario Health and token issuance by Backup Authentication Service
- Tracking changes of configuration endpoints (for example, Authorization Policy) via Microsoft Graph API (e.g., AADSCA)

Security Policies & Threat Detection

- Authentication Methods Activity (Register, Usage) and SSPR Reports
- Windows Hello for Business Policy (incl. Require TPM)
- Conditional Access Security Alerts, Gaps and Insights
- Policy Effectiveness (WhatIf, Sign-in Logs) and Change Tracking (e.g., AADOps)
- Identity Protection risk statistics (Dashboard/API)
- Health status of analytics rules, playbooks and data connector in Sentinel

Identity Governance and Entitlement Management

- Azure AD Privileged Identity Management (PIM) Discovery and insights
- PIM Alerts for Azure AD roles and Azure roles
- Insights and Reporting in Identity Governance
- Health of Lifecycle Workflows schedules
- PCI Score and Analytics in Entra Permissions Management
- Tracking changes of connected organizations, assignments and delegations on catalogs and access packages

Application and Workload Identities

- Usage & Insights Reports about application, service principal sign-in and credential activity
- Attack Paths and Cloud Security Explorer in Defender for Cloud
- MDA App Governance Policy Alerts (for example unused API permissions)
- Microsoft Cloud Security Benchmark (MCSB) Controls related to Identity Management or Privileged Access
- Tracking changes on assigned (API) permissions and delegations.

Internal/External Attack Analyses

- Security Awareness Training for Users (Attack Simulation, for example phishing)
- Verify attack surface, mitigations & ITDR detections (AADInternals, ROADtools,…)
- Attack Path Management (BloodHound, Forest Druid, Stormspotter,…)

Azure AD Attack & Defense Playbook

Contributors: Sami Lamppu, Markus Pitkäranta, Joosua Santasalo and Thomas Naunheim

Feedback

Feedback Global Security und Compliance Konferenz 2023

https://forms.office.com/e/J5TB8AN3Ve