All about Azure Hardening *by*

TEMS SECURITY SERVICES

PHILIP BERGER

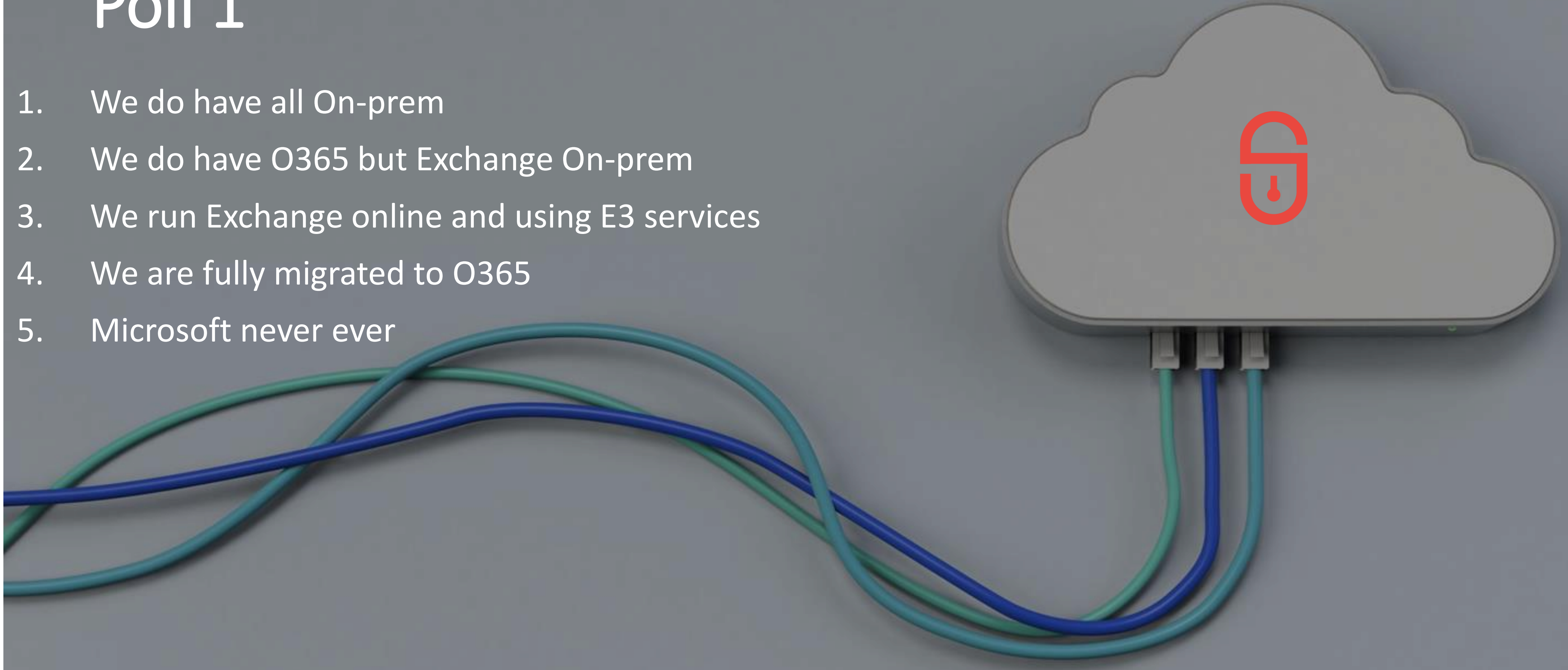
MICHAEL MEIXNER

Agenda

- Zero Trust Concept / Model
- Basic Azure Hardening
- Advanced Azure Hardening

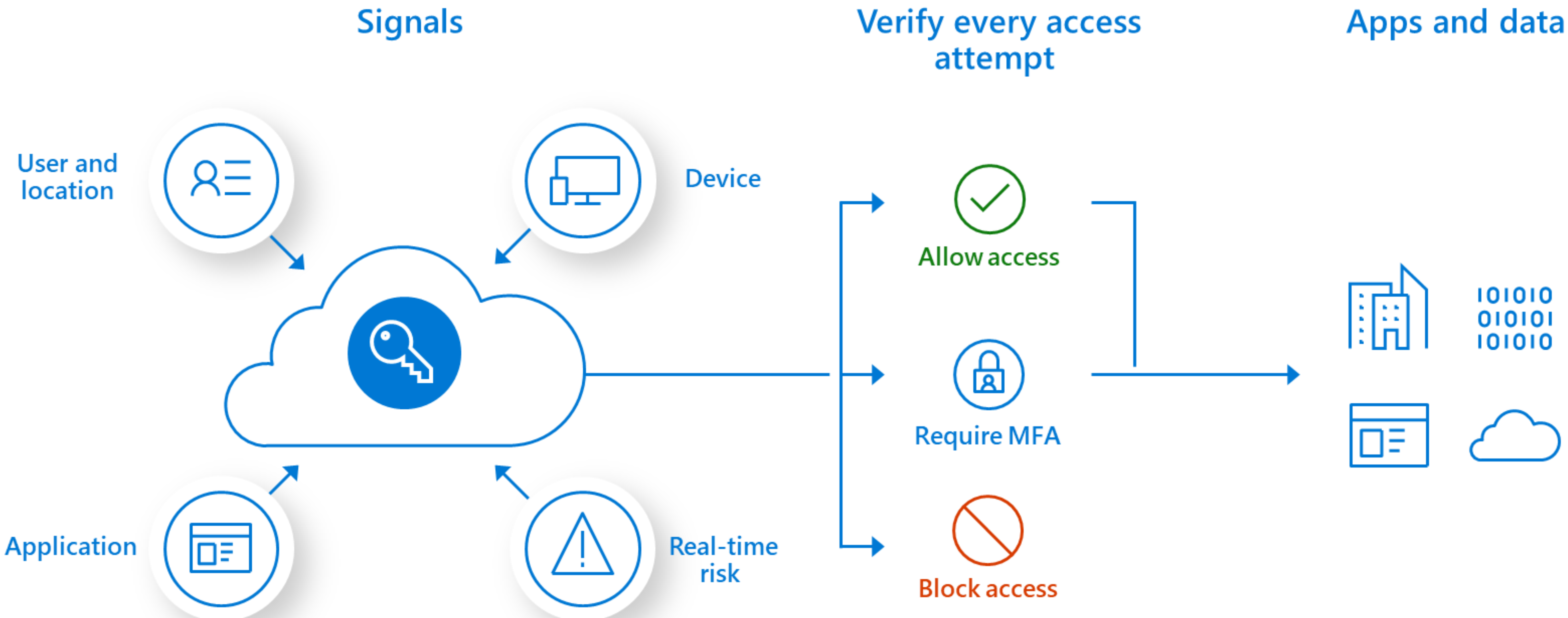
Poll 1

1. We do have all On-prem
2. We do have O365 but Exchange On-prem
3. We run Exchange online and using E3 services
4. We are fully migrated to O365
5. Microsoft never ever



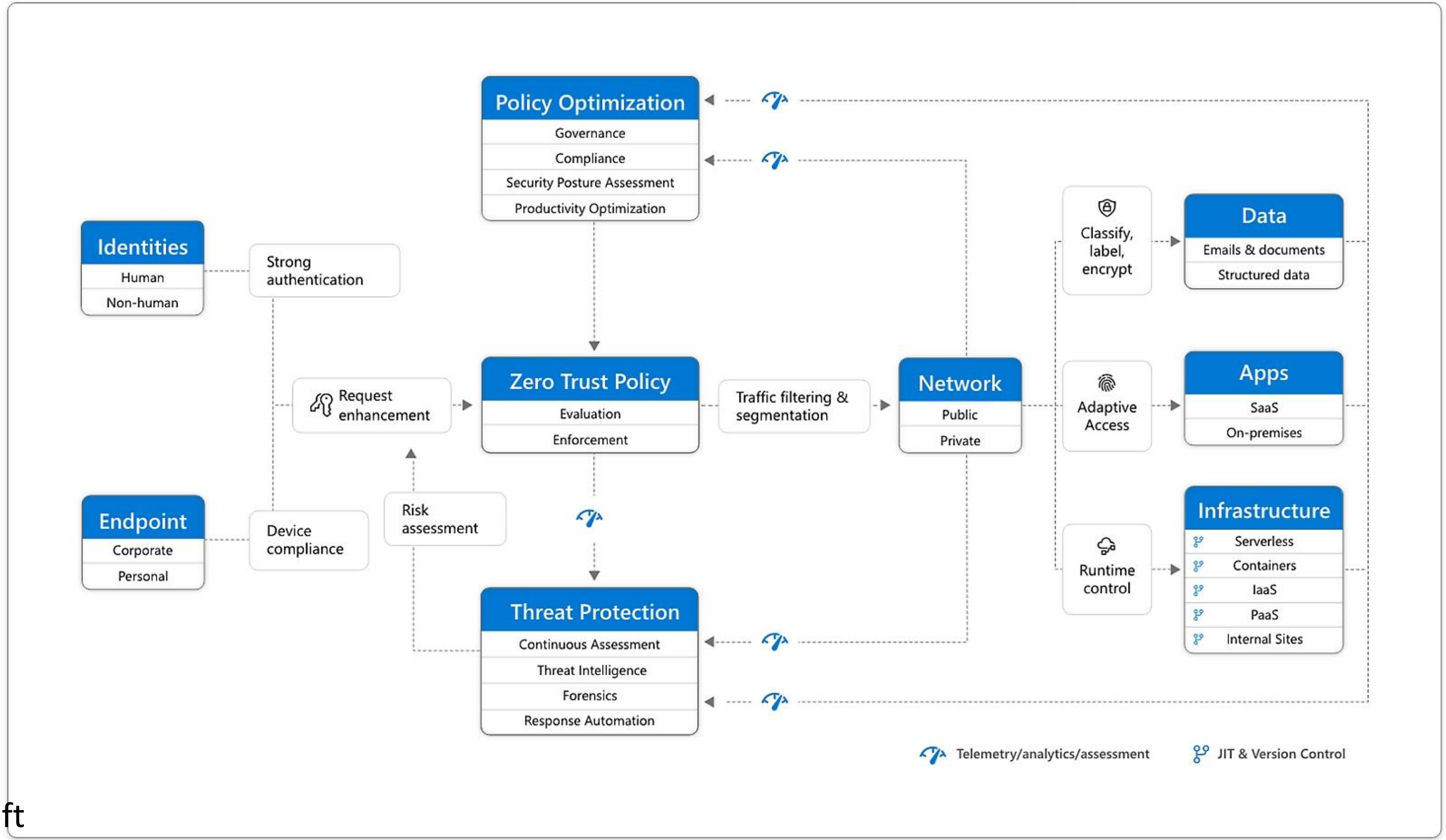
Zero Trust
Concept / Model

Zero Trust Model



Quelle: Microsoft

Zero Trust Model



Quelle: Microsoft

tems security

Zero Trust - Maturity Model

(1) First Stage:

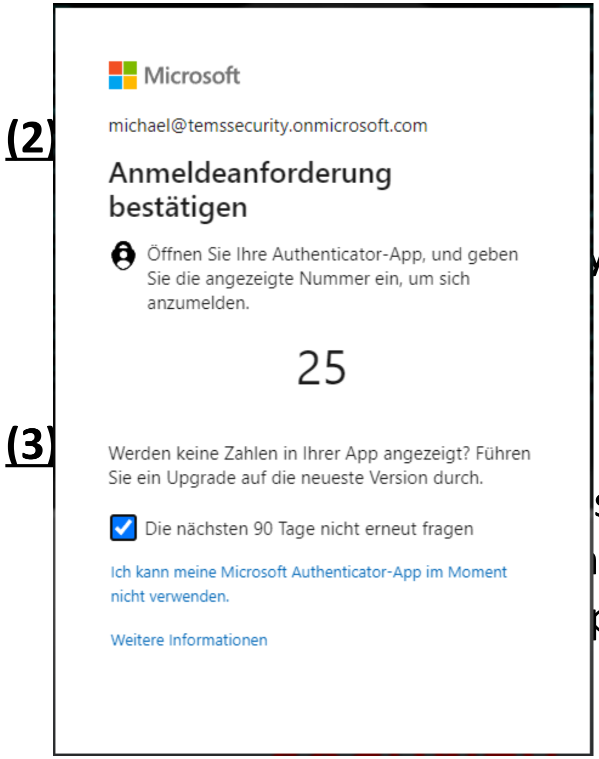
“good”MFA for all Users
Start with Compliance for Computers
Start with User RISK Levels
Privileged Identity Management (PIM) - LIV

(2)

y s
of

(3)

s
re
pe



Microsoft

michael@temssecurity.onmicrosoft.com

Anmeldeanforderung bestätigen

Öffnen Sie Ihre Authenticator-App, und geben Sie die angezeigte Nummer ein, um sich anzumelden.

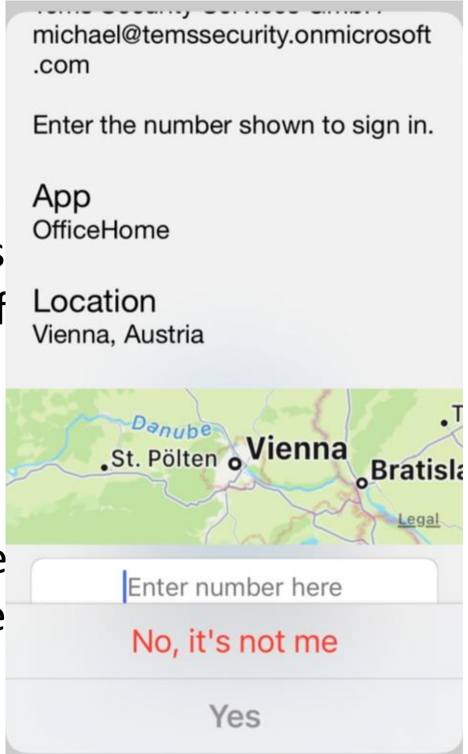
25

Werden keine Zahlen in Ihrer App angezeigt? Führen Sie ein Upgrade auf die neueste Version durch.

☑ Die nächsten 90 Tage nicht erneut fragen

Ich kann meine Microsoft Authenticator-App im Moment nicht verwenden.

Weitere Informationen



michael@temssecurity.onmicrosoft.com

Enter the number shown to sign in.

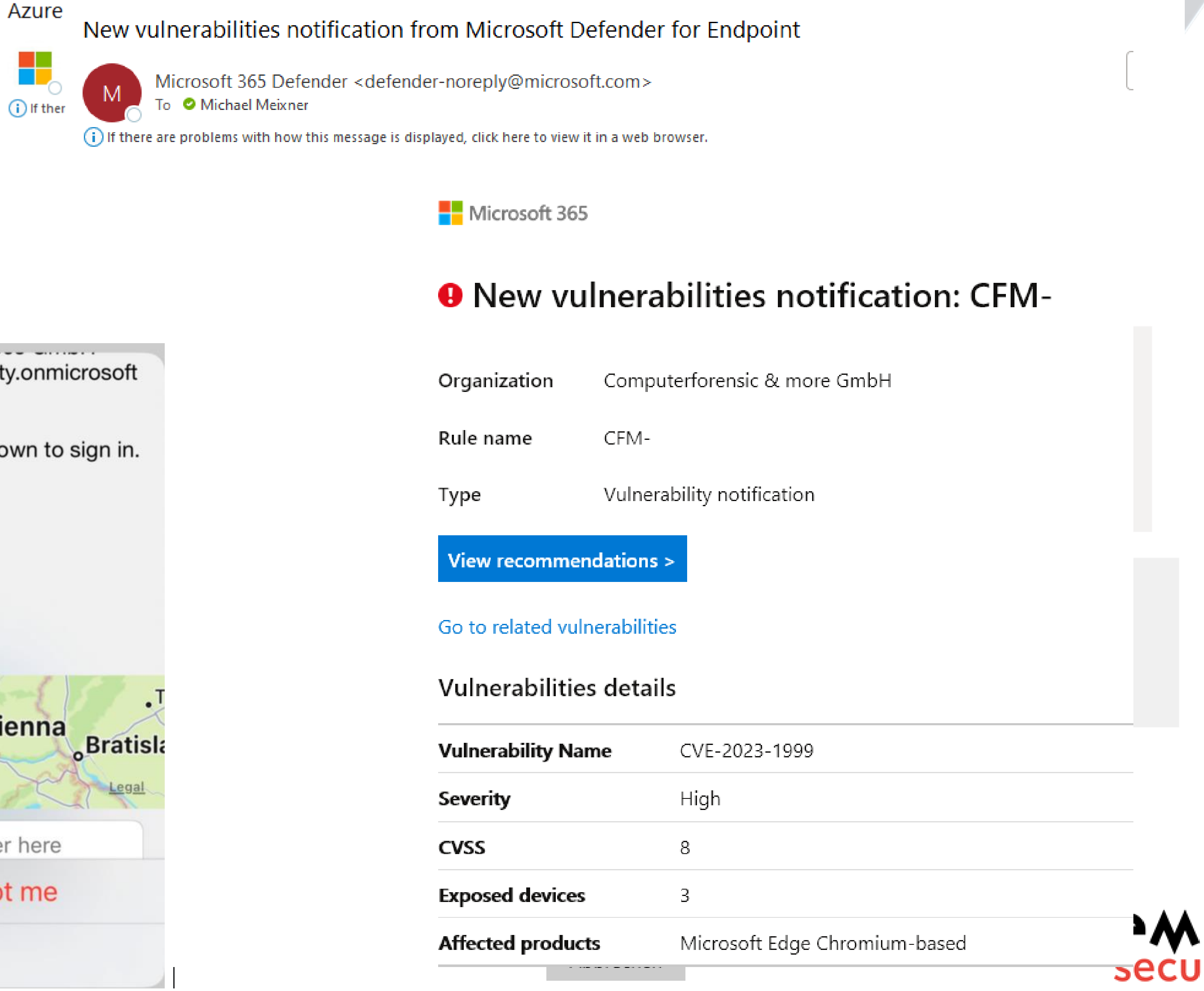
App
OfficeHome

Location
Vienna, Austria

Enter number here

No, it's not me

Yes



Azure

New vulnerabilities notification from Microsoft Defender for Endpoint

Microsoft 365 Defender <defender-noreply@microsoft.com>
To Michael Meixner

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft 365

New vulnerabilities notification: CFM-

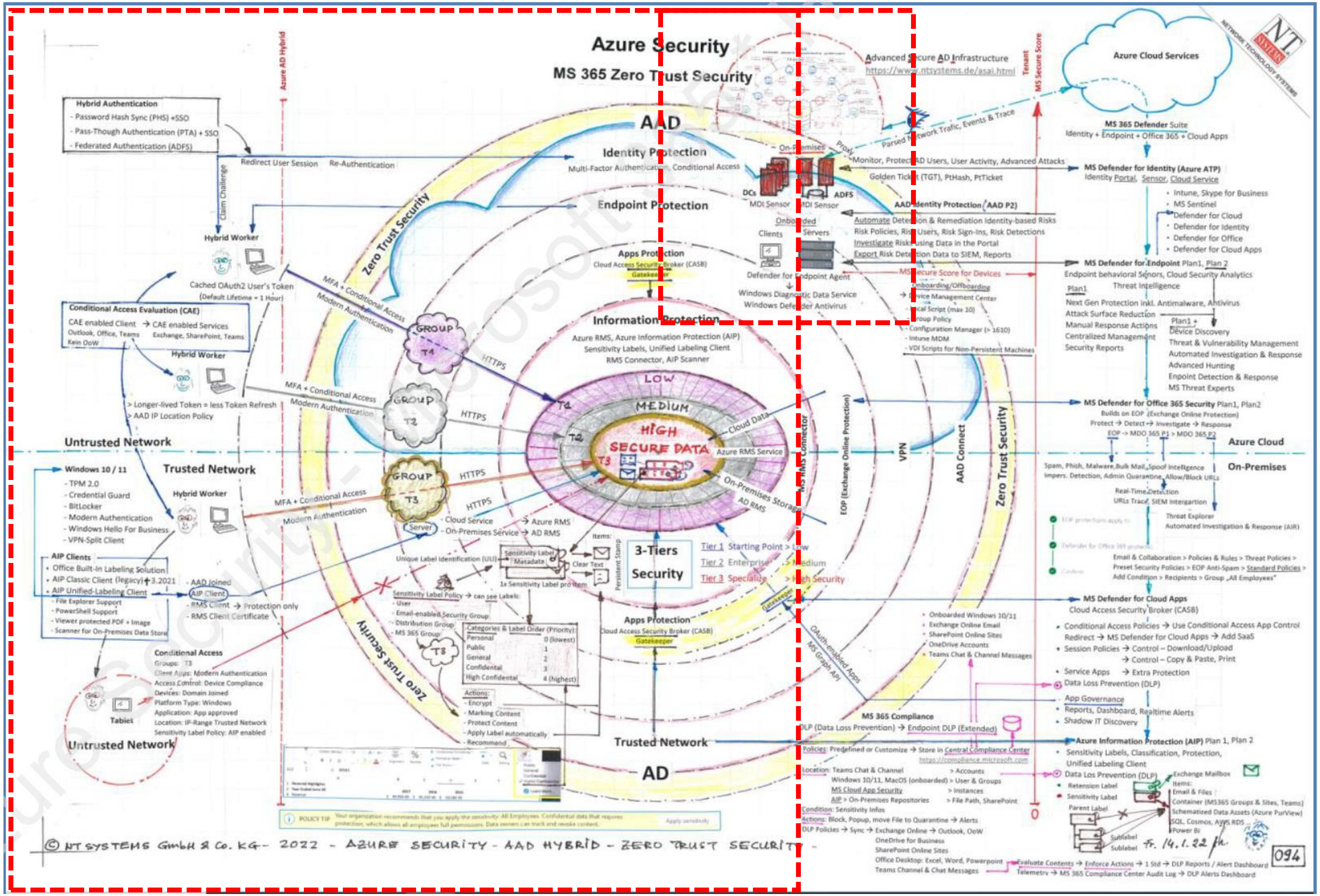
Organization	Computerforensic & more GmbH
Rule name	CFM-
Type	Vulnerability notification

View recommendations >

Go to related vulnerabilities

Vulnerabilities details

Vulnerability Name	CVE-2023-1999
Severity	High
CVSS	8
Exposed devices	3
Affected products	Microsoft Edge Chromium-based

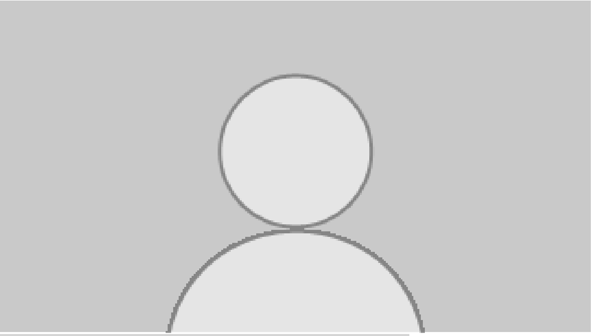


Azure Security
MS 365 Zero Trust Security
AAD
Identity Protection
Multi-Factor Authentication, Conditional Access
Endpoint Protection
Apps Protection
Cloud Access Security Broker (CASB)
Gatekeeper
Information Protection
Azure RMS, Azure Information Protection (AIP)
Sensitivity Labels, Unified Labeling Client
RMS Connector, AIP Scanner
LOW
MEDIUM
HIGH
SECURE DATA
Cloud Data
Azure RMS Service
On-Premises Storage
AD RMS
Hybrid Authentication
- Password Hash Sync (PHS) +SSO
- Pass-Though Authentication (PTA) + SSO
- Federated Authentication (ADFS)
Redirect User Session
Re-Authentication
Claim Challenge
Azure AD Hybrid
Hybrid Worker
Cached OAuth2 User's Token
(Default Lifetime = 1 Hour)
Conditional Access Evaluation (CAE)
CAE enabled Client → CAE enabled Services
Outlook, Office, Teams
Exchange, SharePoint, Teams
Kein OoW
> Longer-lived Token = less Token Refresh
> AAD IP Location Policy
MFA + Conditional Access
Modern Authentication
GROUP
T4
T2
T3
HTTPS
Zero Trust Security
Untrusted Network
Trusted Network
Windows 10 / 11
- TPM 2.0
- Credential Guard
- BitLocker
- Modern Authentication
- Windows Hello For Business
- VPN-Split Client
AIP Clients
• Office Built-In Labeling Solution
• AIP Classic Client (legacy) † 3.2021
• AIP Unified-Labeling Client
- File Explorer Support
- PowerShell Support
- Viewer protected PDF + Image
- Scanner for On-Premises Data Store
- AAD Joined
AIP Client
- RMS Client → Protection only
- RMS Client Certificate
Conditional Access
Groups: T3
Client Apps: Modern Authentication
Access Control: Device Compliance
Devices: Domain Joined
Platform Type: Windows
Application: App approved
Location: IP-Range Trusted Network
Sensitivity Label Policy: AIP enabled
Tablet
Untrusted Network
Server
- Cloud Service → Azure RMS
- On-Premises Service → AD RMS
Unique Label Identification (UUI)
Sensitivity Label
Metadata
Clear Text
1x Sensitivity Label pro Item
Items:
Persistent Stamp
Sensitivity Label Policy → can see Labels
- User
- Email-enabled Security Group
- Distribution Group
- MS 365 Group
Categories & Label Order (Priority)
Personal
Public 0 (lowest)
General 1
Confidential 2
Highly Confidential 3
4 (highest)
Actions:
- Encrypt
- Marking Content
- Protect Content
- Apply Label automatically
- Recommend
3-Tiers Security
Tier 1 Starting Point > Low
Tier 2 Enterprise > Medium
Tier 3 Specialized > High Security
Trusted Network
AD
POLICY TIP
Advanced Secure AD Infrastructure
https://www.ntsystems.de/asai.html
Tenant
MS Secure Score
On-Premises
Proxy
Parsed Network Trafic, Events & Trace
DCs
ADFS
MDI Sensor
MDI Sensor
Onboarded
Clients
Servers
Defender for Endpoint Agent
Windows Diagnostic Data Service
Windows Defender Antivirus
Azure Cloud Services
MS 365 Defender Suite
Identity + Endpoint + Office 365 + Cloud Apps
Monitor, Protect AD Users, User Activity, Advanced Attacks
Golden Ticket (TGT), PtHash, PtTicket
MS Defender for Identity (Azure ATP)
Identity Portal, Sensor, Cloud Service
• Intune, Skype for Business
• MS Sentinel
• Defender for Cloud
• Defender for Identity
• Defender for Office
• Defender for Cloud Apps
AAD Identity Protection (AAD P2)
Automate Detection & Remediation Identity-based Risks
Risk Policies, Risky Users, Risk Sign-ins, Risk Detections
Investigate Risks using Data in the Portal
Export Risk Detection Data to SIEM, Reports
MS Secure Score for Devices
Onboarding/Offboarding
Device Management Center
Local Script (max 10)
Group Policy
Configuration Manager (> 1610)
Intune MDM
VDI Scripts for Non-Persistent Machines
MS Defender for Endpoint Plan1, Plan 2
Endpoint behavioral Sensors, Cloud Security Analytics
Plan1
Threat Intelligence
Next Gen Protection inkl. Antimalware, Antivirus
Attack Surface Reduction
Manual Response Actions
Centralized Management
Security Reports
Plan1 +
Device Discovery
Threat & Vulnerability Management
Automated Investigation & Response
Advanced Hunting
Enpoint Detection & Response
MS Threat Experts
MS Defender for Office 365 Security Plan1, Plan2
Builds on EOP (Exchange Online Protection)
Protect → Detect → Investigate → Response
EOP → MDO 365 P1 → MDO 365 P2
Azure Cloud
On-Premises
Spam, Phish, Malware, Bulk Mail, Spoof Intelligence
Impers. Detection, Admin Quarantine, Allow/Block URLs
Real-Time Detection
URLs Trace, SIEM Intergartion
Threat Explorer
Automated Investigation & Response (AIR)
Email & Collaboration > Policies & Rules > Threat Policies >
Preset Security Policies > EOP Anti-Spam > Standard Policies >
Add Condition > Recipients > Group „All Employees"
MS RMS Connector
EOP (Exchange Online Protection)
VPN
AAD Connect
Zero Trust Security
MS Defender for Cloud Apps
Cloud Access Security Broker (CASB)
• Conditional Access Policies → Use Conditional Access App Control
Redirect → MS Defender for Cloud Apps → Add SaaS
• Session Policies → Control – Download/Upload
→ Control – Copy & Paste, Print
• Service Apps → Extra Protection
• Data Loss Prevention (DLP)
• App Governance
• Reports, Dashboard, Realtime Alerts
• Shadow IT Discovery
Gatekeeper
OAuth-enabled Apps
MS Graph API
• Onboarded Windows 10/11
• Exchange Online Email
• SharePoint Online Sites
• OneDrive Accounts
• Teams Chat & Channel Messages
MS 365 Compliance
DLP (Data Loss Prevention) → Endpoint DLP (Extended)
Policies: Predefined or Customize → Store in Central Compliance Center
https://compliance.microsoft.com
Location: Teams Chat & Channel > Accounts
Windows 10/11, MacOS (onboarded) > User & Groups
MS Cloud App Security > Instances
AIP > On-Premises Repositories > File Path, SharePoint
Condition: Sensitivity Infos
Actions: Block, Popup, move File to Quarantine → Alerts
DLP Policies → Sync → Exchange Online → Outlook, OoW
OneDrive for Business
SharePoint Online Sites
Office Desktop: Excel, Word, Powerpoint
Teams Channel & Chat Messages
Evaluate Contents → Enforce Actions → 1 Std → DLP Reports / Alert Dashboard
Telemetry → MS 365 Compliance Center Audit Log → DLP Alerts Dashboard
Azure Information Protection (AIP) Plan 1, Plan 2
• Sensitivity Labels, Classification, Protection,
Unified Labeling Client
• Data Los Prevention (DLP)
• Retension Label
• Sensitivity Label
Parent Label
Sublabel
Sublabel
Exchange Mailbox
Items:
Email & Files
Container (MS365 Groups & Sites, Teams)
Schematized Data Assets (Azure PurView)
SQL, Cosmos, AWS RDS
Power BI
Fr. 14.1.22
094
NETWORK TECHNOLOGY SYSTEMS
NT SYSTEMS
© NT SYSTEMS GmbH & Co. KG - 2022 - AZURE SECURITY - AAD HYBRID - ZERO TRUST SECURITY -

Quelle: NTSYSTEMS.DE

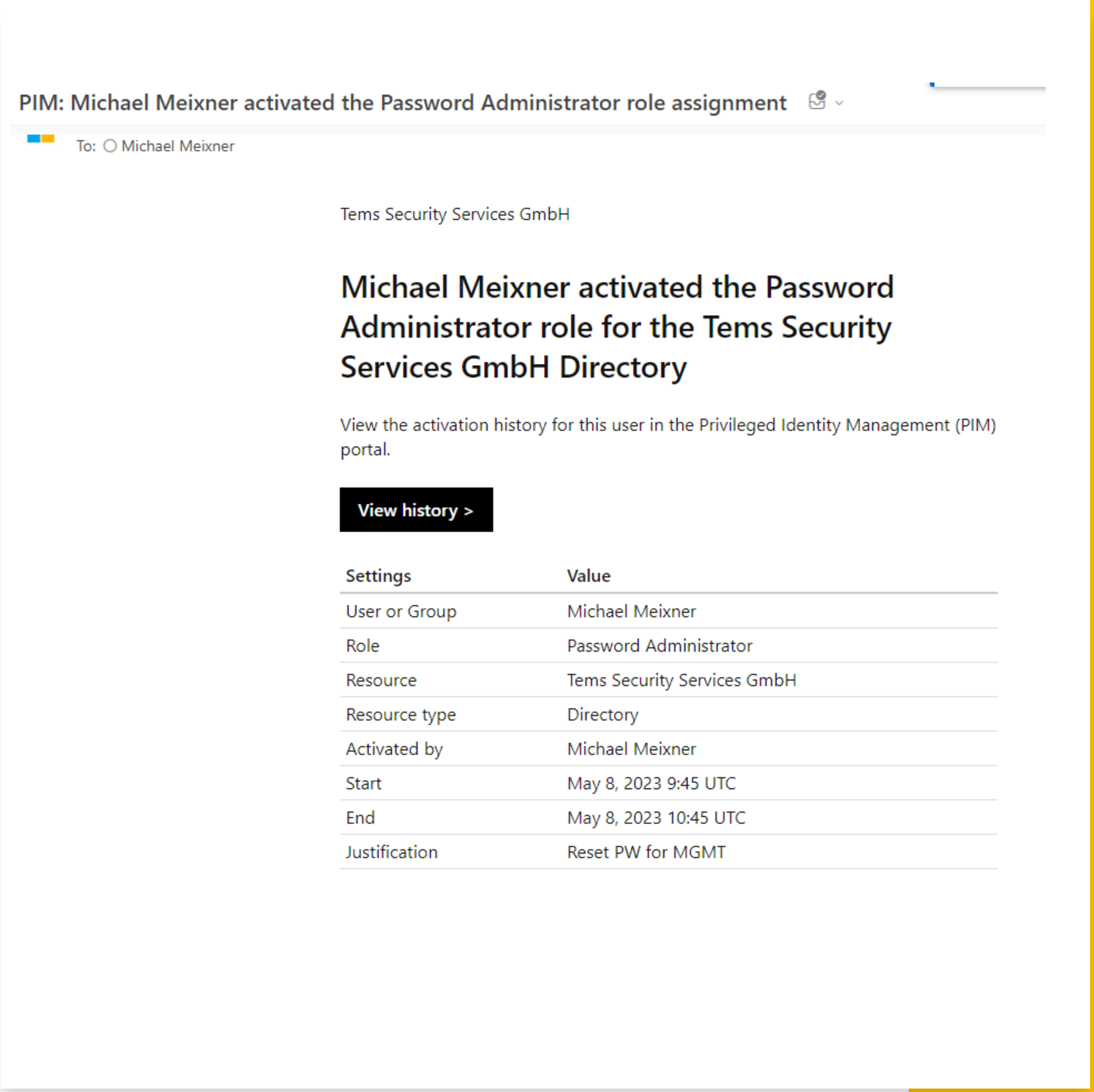
Basis Azure Hardening

Basic Azure Hardening



- ✓ Setup and configure BreakGlas Accounts
- ✓ Clean up Global Administrator Group
- ✓ Configure good MFA for all Users
- ✓ Implement Autopilot
- ✓ Move to Azure AD joined machines
- ✓ Configure Hello for Business
- ✓ Configure PIM for all high-privileged Tasks **- LIVE**
- ✓ E5 License for admins are required for Security
- ✓ Configure Threat Monitoring for MGMT and exposed users
- ✓ Rollout Company Portal to all machines and smartphones
- ✓ Configure and rollout MDM / Intune
- ✓ Limit Guest access to your Tenant
- ✓ Teams Hardening

PIM for all high-privileged Tasks



PIM: Michael Meixner activated the Password Administrator role assignment

To: ○ Michael Meixner

Tems Security Services GmbH

Michael Meixner activated the Password Administrator role for the Tems Security Services GmbH Directory

View the activation history for this user in the Privileged Identity Management (PIM) portal.

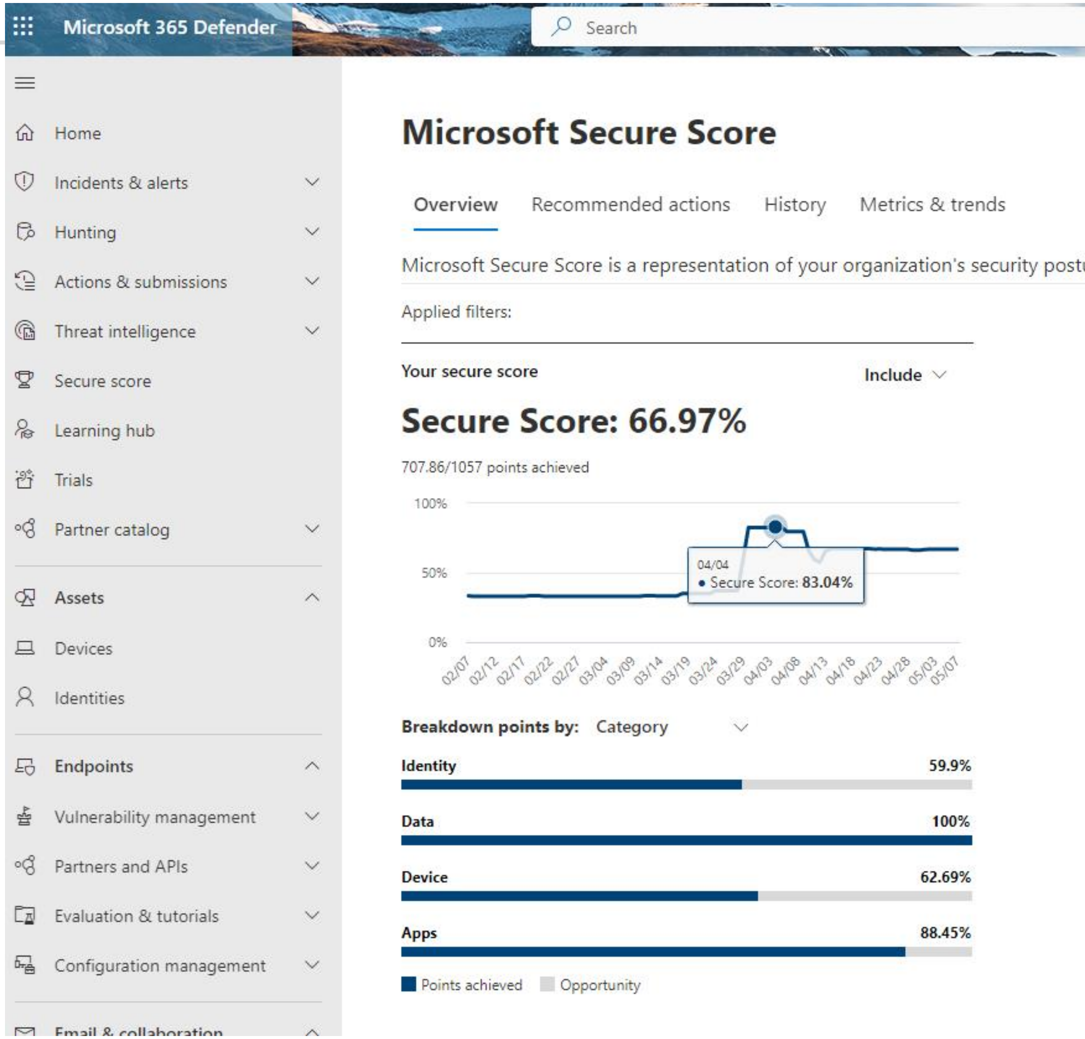
Settings	Value
User or Group	Michael Meixner
Role	Password Administrator
Resource	Tems Security Services GmbH
Resource type	Directory
Activated by	Michael Meixner
Start	May 8, 2023 9:45 UTC
End	May 8, 2023 10:45 UTC
Justification	Reset PW for MGMT

Advanced Azure Hardening

tems security

Azure Hardening Part 2 /1

- ✓ Secure Score
- ✓ Contitional access rules
- ✓ MIP (Microsoft Information Protection)
- ✓ DLP (Data Leagage Protection)
- ✓ Record Management
- ✓ Azure role-based access control (Azure RBAC)
- ✓ Endpoint Security with Defender (AKA APT)
- ✓ Data Lifecycle Management (DSGVO Compliance)
- ✓ Mulit Tenant Setup (Separate Admins from users)
- ✓ Configure Safe Links
- ✓ Configure Safe Attachments
- ✓ Strong Authentication for Admins (passwordless)
- ✓ CIS Benchmark - Compliance built-in checks
- ✓ Advanced Monitoring with Elastic



Microsoft Secure Score

Microsoft Secure Score is a representation of your organization's security post

Applied filters:

Your secure score

Include

Secure Score: 66.97%

707.86/1057 points achieved

04/04
● Secure Score: 83.04%

Breakdown points by: Category

Identity	59.9%
Data	100%
Device	62.69%
Apps	88.45%

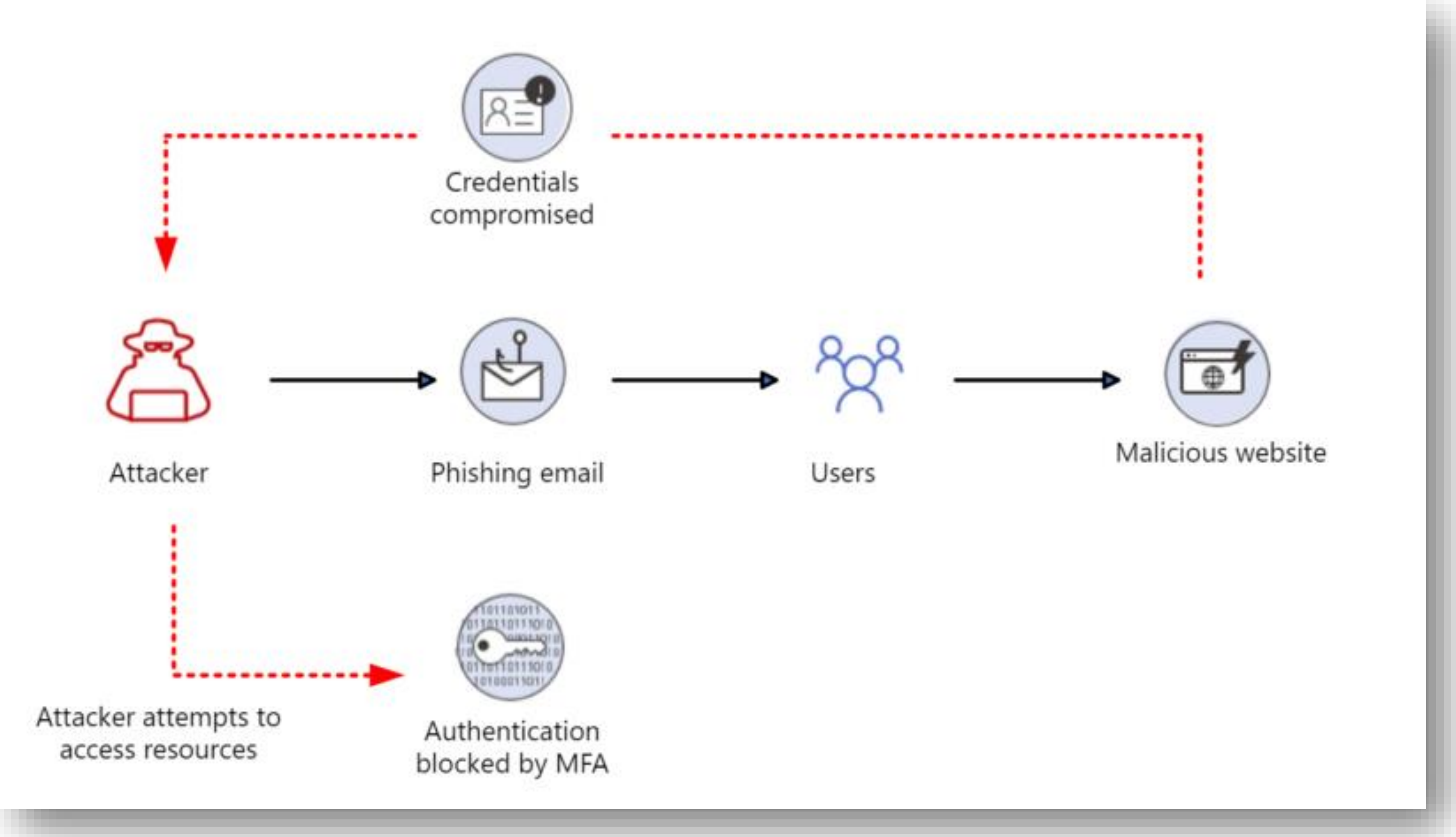
Azure Hardening – Admin MGMT

- max. 5x Global Administrators
    - 2x Break Glas Admins without MFA
    - 3x Function Users (with Yubikeys)

- All Users are only Rolladministrators with JEA (time-based 2 hours max)
    - Account Administrator
    - Exchange Administrator
    - Securitiy Administrator
    - Compliance Administrator
    - Global Reader
    - Billing Administrator
    - Intune Administrator

Access token protection

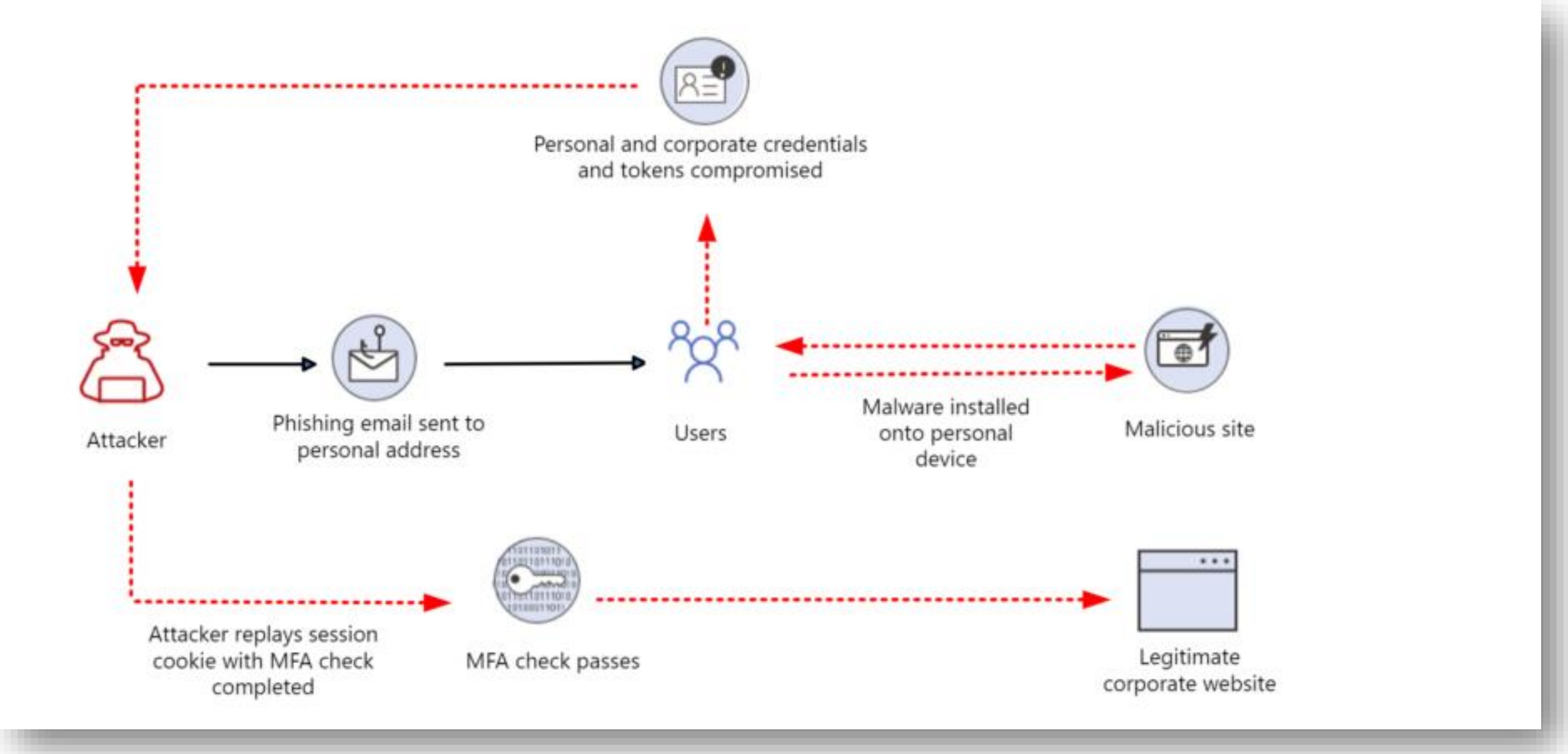
When Azure AD issues a token, it contains information (claims) such as the username, source IP address, MFA, and more. It also includes any privilege a user has in Azure AD. If you sign in as a Global Administrator to your Azure AD tenant, then the token will reflect that.



Source: Microsoft

Access token protection

When Azure AD issues a token, it contains information (claims) such as the username, source IP address, MFA, and more. It also includes any privilege a user has in Azure AD. If you sign in as a Global Administrator to your Azure AD tenant, then the token will reflect that.


Personal and corporate credentials and tokens compromised
Attacker
Phishing email sent to personal address
Users
Malware installed onto personal device
Malicious site
Attacker replays session cookie with MFA check completed
MFA check passes
Legitimate corporate website

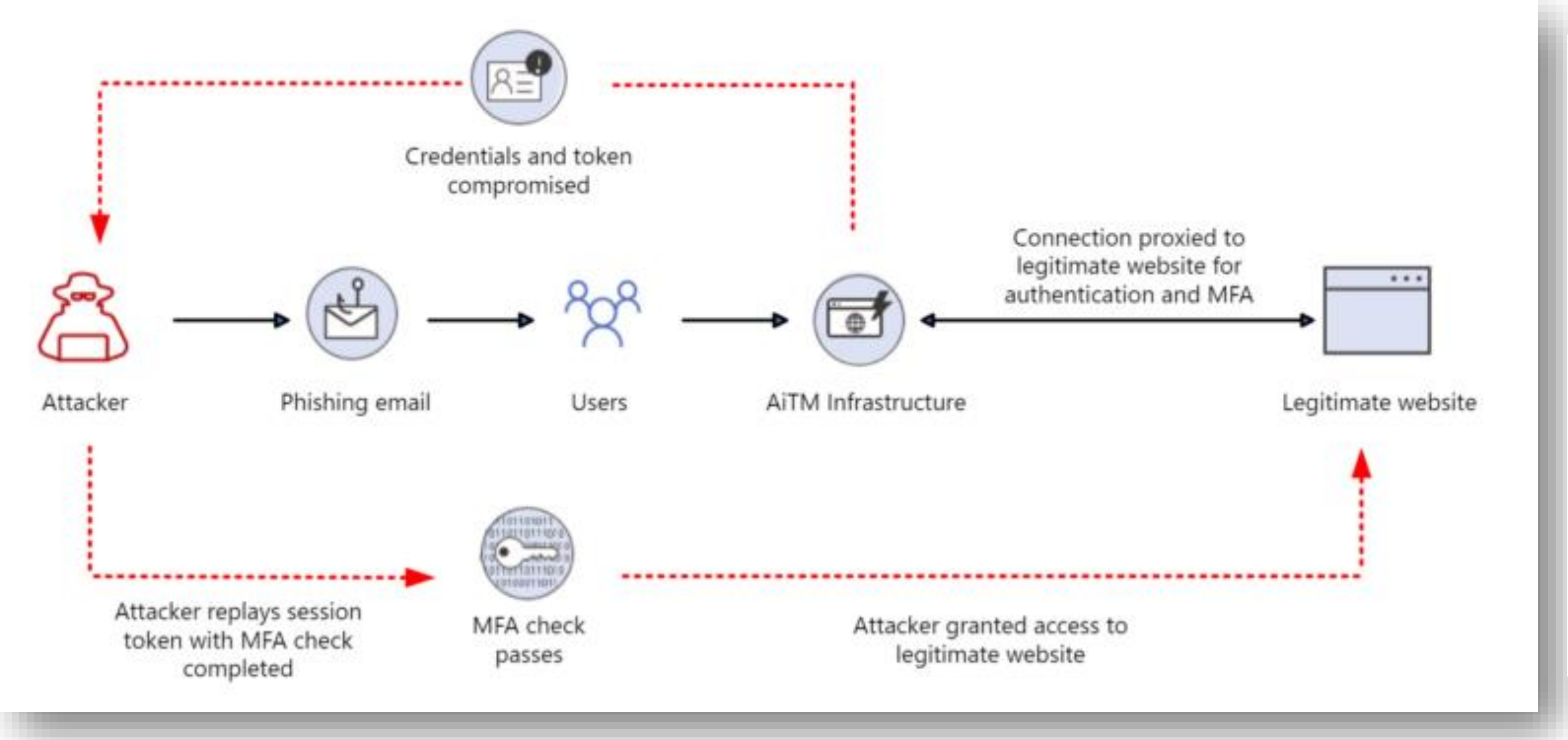
The *pass the hash* technique was originally published by Paul Ashton in 1997

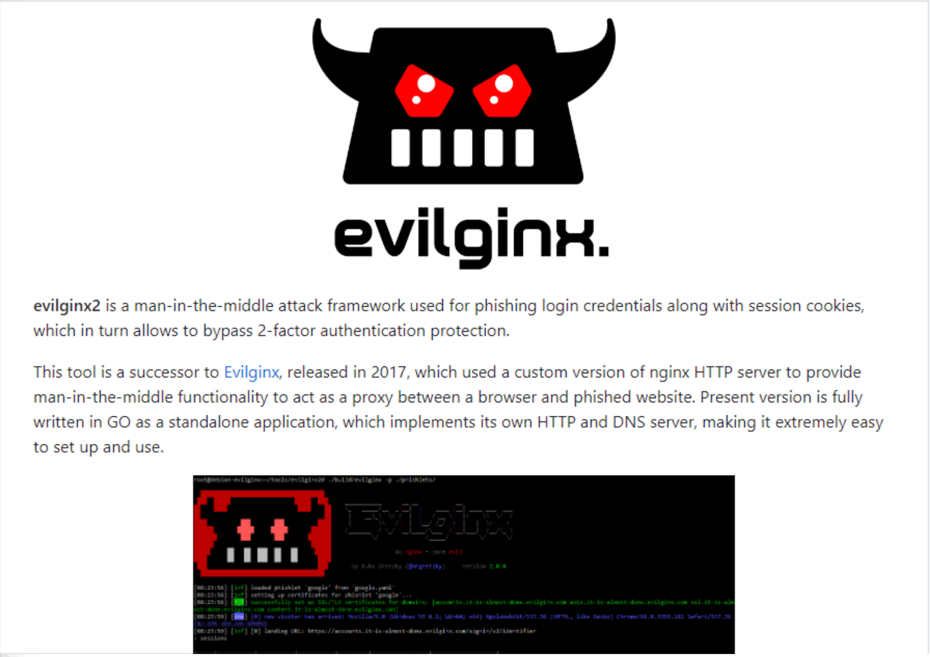
In 2008, Hernan Ochoa published a tool called the "Pass-the-Hash Toolkit"

Source: Microsoft

Access token protection

When Azure AD issues a token, it contains information (claims) such as the username, source IP address, MFA, and more. It also includes any privilege a user has in Azure AD. If you sign in as a Global Administrator to your Azure AD tenant, then the token will reflect that.


Credentials and token compromised
Attacker
Phishing email
Users
AiTM Infrastructure
Connection proxied to legitimate website for authentication and MFA
Legitimate website
Attacker replays session token with MFA check completed
MFA check passes
Attacker granted access to legitimate website



evilginx.

evilginx2 is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to Evilginx, released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.

```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                         Evilginx

                    no nginx - pure evil

          by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [+++] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-almost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36 ([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions
```

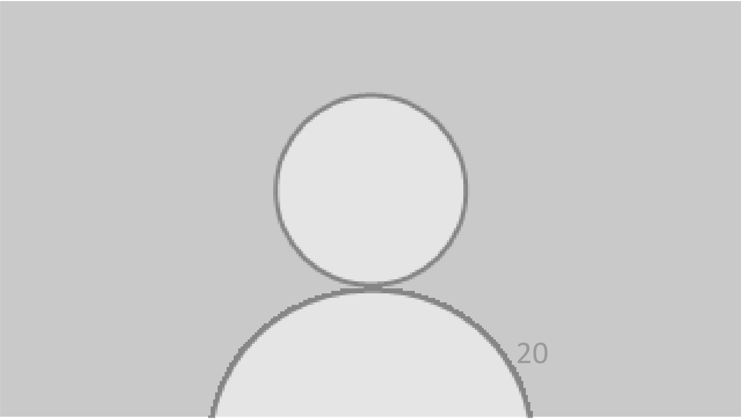
Source: Microsoft

Poll 3

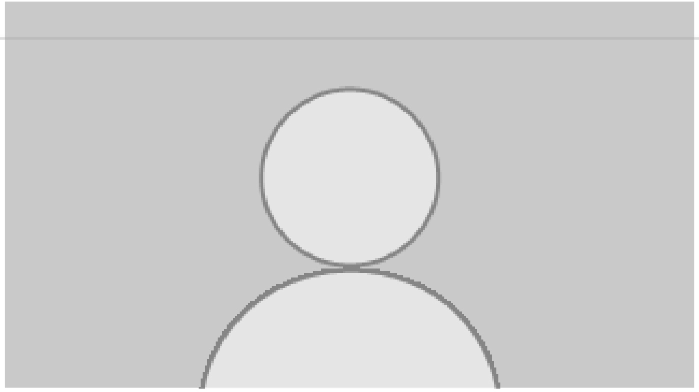
1. Do you think that can work without local admin rights?

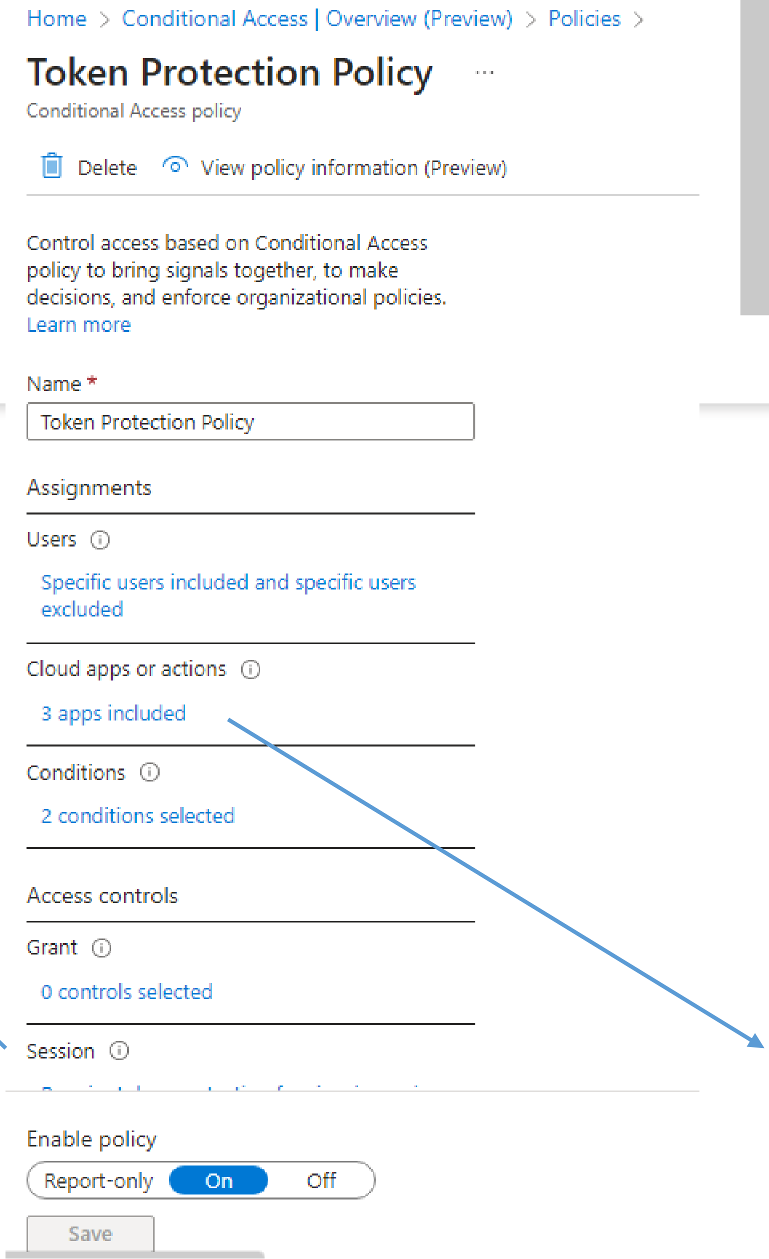
Access token protection – Part 2 – Live

```
strings64.exe WINWORD.DMP | findstr /i eyJ0eX
```



Access token protection **mitigation**





Home > Conditional Access | Overview (Preview) > Policies >

Token Protection Policy ...

Conditional Access policy

Delete   View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Token Protection Policy

Assignments

Users ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

3 apps included

Conditions ⓘ

2 conditions selected

Access controls

Grant ⓘ

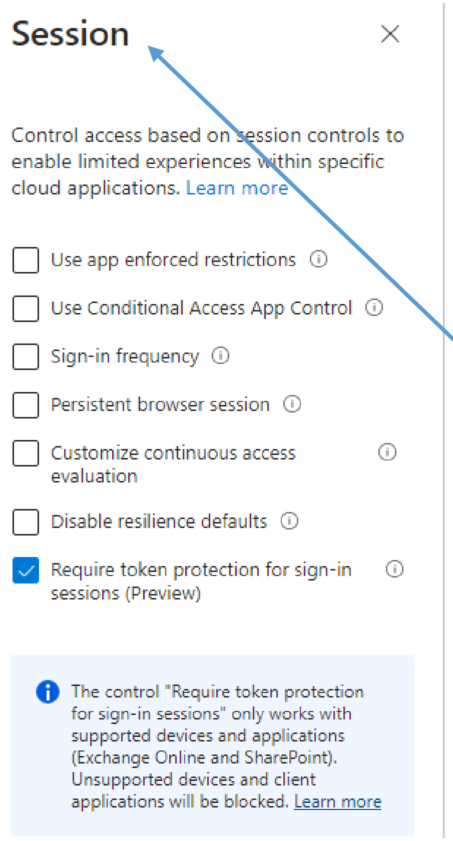
0 controls selected

Session ⓘ

Enable policy

Report-only | **On** | Off

Save

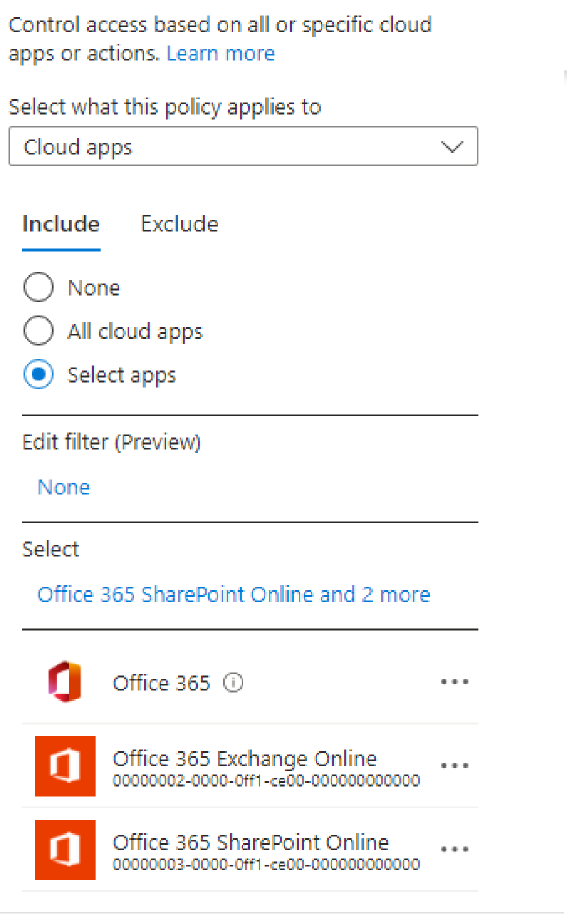


Session

Control access based on session controls to enable limited experiences within specific cloud applications. Learn more

- ☐ Use app enforced restrictions ⓘ
- ☐ Use Conditional Access App Control ⓘ
- ☐ Sign-in frequency ⓘ
- ☐ Persistent browser session ⓘ
- ☐ Customize continuous access evaluation ⓘ
- ☐ Disable resilience defaults ⓘ
- ☑ Require token protection for sign-in sessions (Preview) ⓘ

ⓘ The control "Require token protection for sign-in sessions" only works with supported devices and applications (Exchange Online and SharePoint). Unsupported devices and client applications will be blocked. Learn more



Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include | Exclude

- ○ None
- ○ All cloud apps
- ● Select apps

Edit filter (Preview)

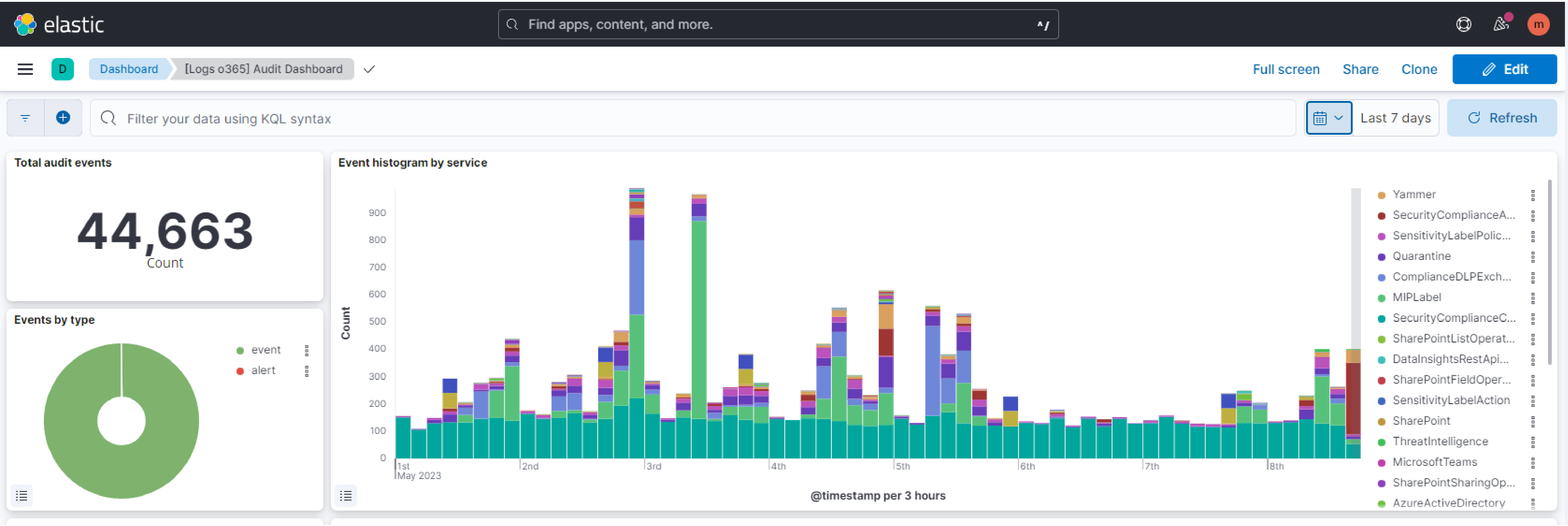
None

Select

Office 365 SharePoint Online and 2 more

Office 365 ⓘ	...
Office 365 Exchange Online 00000002-0000-0ff1-ce00-000000000000	...
Office 365 SharePoint Online 00000003-0000-0ff1-ce00-000000000000	...

Advanced Monitoring



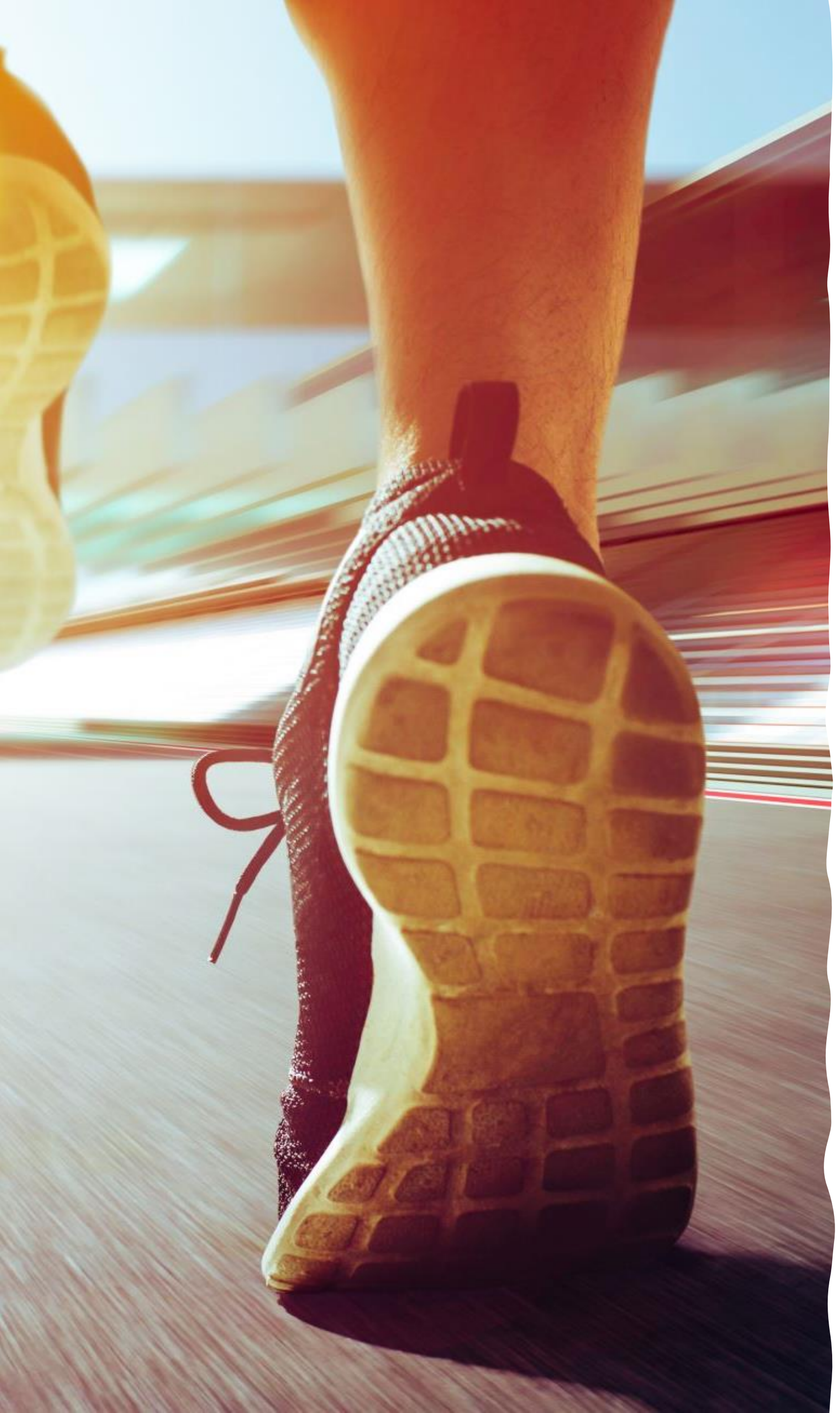
ChatGPT

Here are 10 security settings that an admin should perform to secure an Azure tenant:

- Multi-Factor Authentication (MFA): Require MFA for all users and admins accessing your tenant to prevent unauthorised access in case of password theft.
- Conditional Access: Use conditional access policies to enforce access controls and restrict access to sensitive data based on location, device, or user group.
- Role-Based Access Control (RBAC): Use RBAC to grant permissions only to the necessary users or groups, minimising the risk of unauthorised access to critical resources.
- Azure AD Identity Protection: Enable Azure AD Identity Protection to detect and remediate identity-based risks and vulnerabilities in your tenant.
- Azure AD Privileged Identity Management (PIM): Use PIM to manage and monitor admin access to critical resources, providing just-in-time access for specific tasks and revoking admin rights when they are no longer required.
- Azure Security Center: Enable Security Center to monitor the security posture of your tenant and get actionable security recommendations for improving security across your tenant.
- Azure Network Security Groups (NSGs): Use NSGs to restrict inbound and outbound traffic and control network traffic flow within your tenant.
- Azure Firewall: Use Azure Firewall to protect your tenant from network-level threats, including DDoS attacks, malware, and unauthorised access.
- Azure Key Vault: Use Azure Key Vault to securely store and manage cryptographic keys, secrets, and certificates to encrypt and authenticate data and applications in your tenant.
- Azure Storage Service Encryption (SSE): Use SSE to encrypt data at rest in your Azure storage accounts, protecting your data from unauthorised access in case of a data breach or theft.

Poll 3

1. Yes the webinar was helpful for me
2. We have implemented already some topics
3. We already implemented everything
4. Azure Security we don’t need



Next Webinar

✓ June 7th 2023 09:00am

Secure Azure AD Connect

Would fileless Malware work ?

temS security

Q&A

tems security

Get in contact with us

Philip Berger
Managing Director

☎ +43(664) 343 8644

✉ Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director

☎ +43(664) 1453328

✉ Michael.meixner@tems-security.at