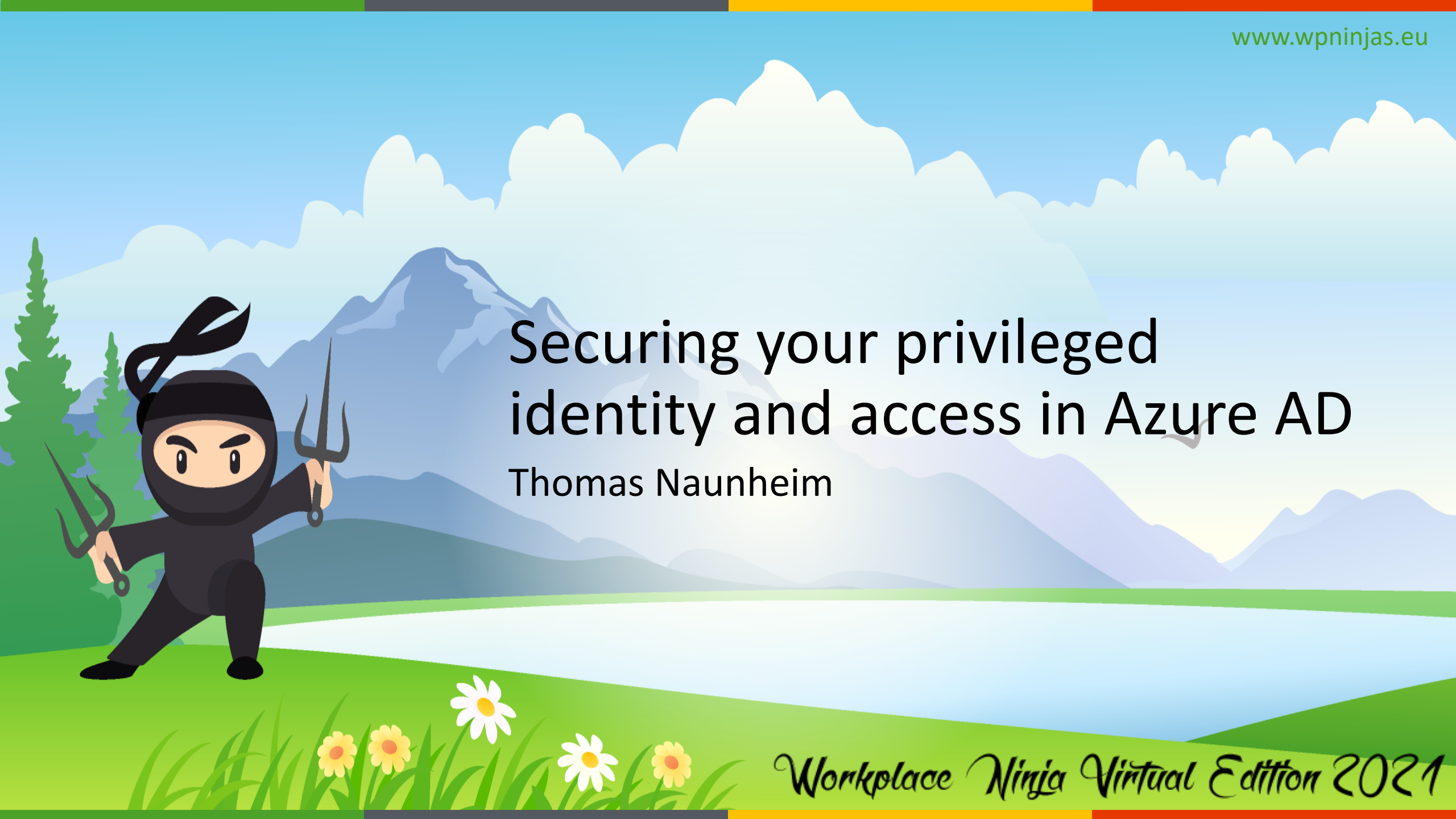
www.wpninjas.eu



Securing your privileged identity and access in Azure AD

Thomas Naunheim

Workplace Ninja Virtual Edition 2021

V-Platin Sponsor

nwc services
one step ahead

RECAST SOFTWARE

Patch My PC
PATCH MANAGEMENT MADE EASY

glueckkanja gab

Lenovo

Microsoft

V-Gold Sponsor

scopewyse
we are what's next

sepago®

baseVISION
SECURE & MODERN WORKPLACE

Patron Sponsors

SD:>_
SwissDev Jobs

About Me

Thomas Naunheim

Cloud Security Architect @glueckkanja-gab

Focus

Identity + Security
@Microsoft Azure

From

Koblenz, Germany

My Blog

www.cloud-architekt.net

Certifications

Azure Solutions Architect Expert
Azure DevOps Engineer Expert

Hobbies

Playing Bass Guitar, Hiking, Traveling

Contact

Thomas@Naunheim.net

@Thomas_Live

Agenda

Protection of Privileged Identity

Strong security baseline for high impact accounts

Security of Privileged Access

Lower exposure and least privileged RBAC design

Access from Secure Admin Workstation

Improve privileged security by using hardened endpoints

Protection of Privileged Identities

Strong security baseline for high impact accounts

Protection of Privileged Identities

Foundation of Privileged Accounts

Microsoft Account

Separation of work and privileged accounts

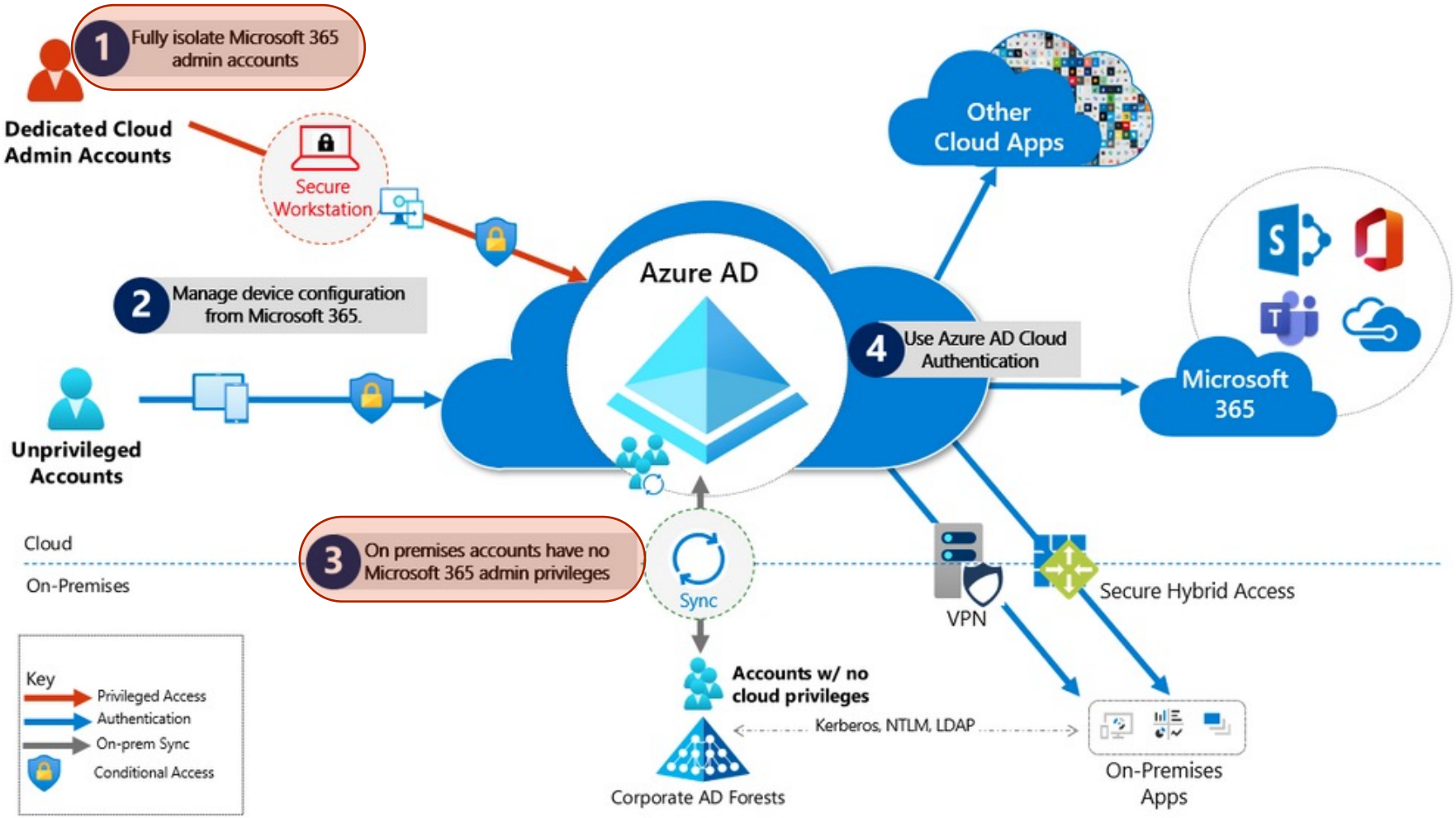
- ✓ Do not use unmanaged (personal) accounts
- ✓ Separate your work and privileged account(s)
- ✓ Do not sync from (AD) on-premises
- ✓ Implement identity lifecycle and access review
- ✓ Remove licenses of productivity workloads
- ✓ Forwarded mail address

Secured and hardened Azure AD Tenant

- ✓ Strong baseline and tenant-level security
- ✓ Monitor and response for suspicious activities
- ✓ Isolation of work- and privileged resources

Protection of Privileged Identities

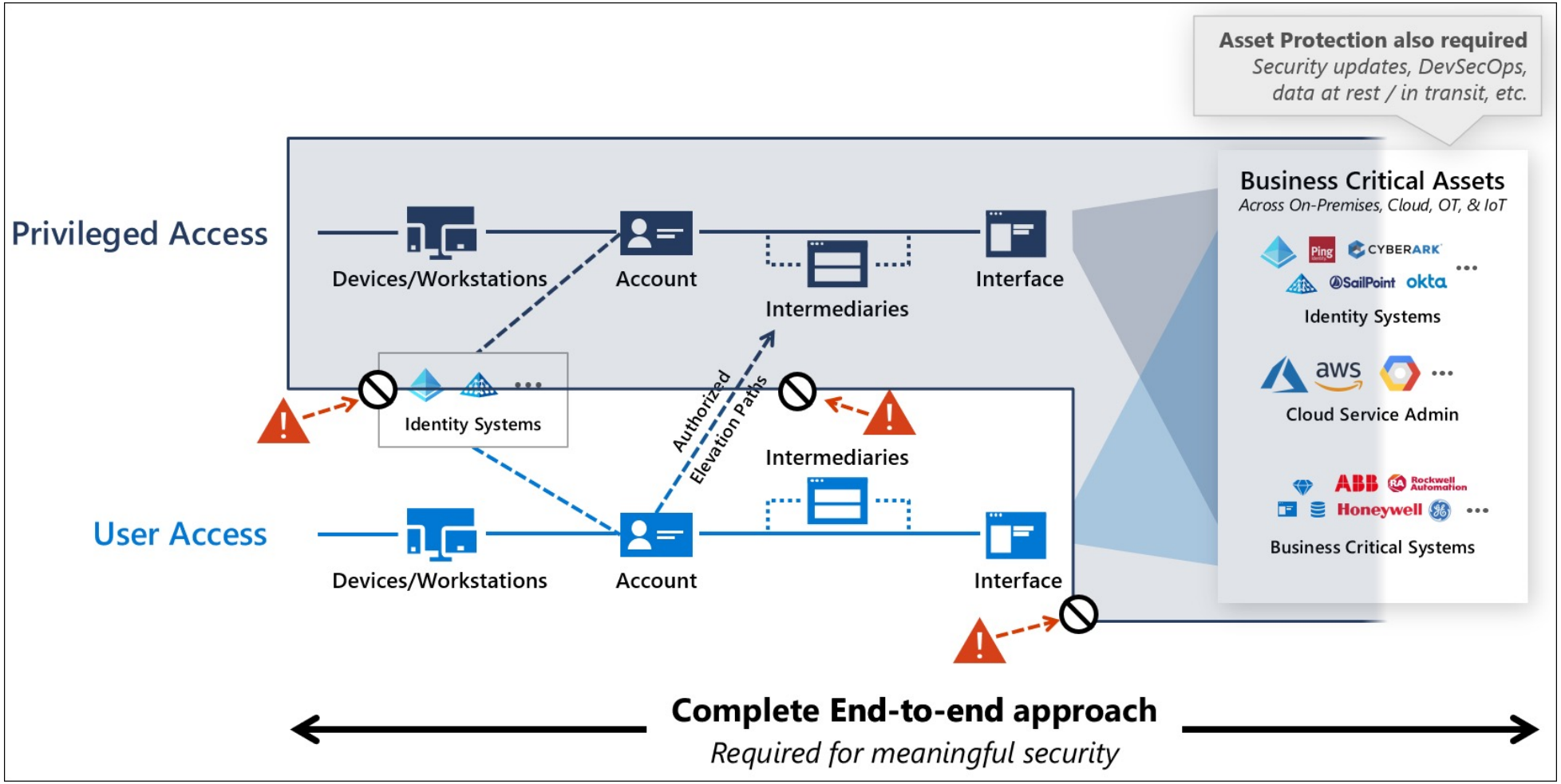
Protecting M365 from on-premises compromise



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

Protection of Privileged Identities

Conditional Access for Privileged Identities



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

Source: "Privileged access Strategy (Microsoft Docs)"

Protection of Privileged Identities

Demos

- Conditional Access Design
- Monitoring and detection of suspicious activities with Azure Sentinel and MCAS
- Privileged Identity Compliance

Protection of Privileged Identities

Key takeaways

Privileged Identity

- Separated/isolated accounts from “productive” tasks
- Strong and passwordless authentication options
- Conditional Access Policies to protect authorization paths to interfaces/intermediaries
- MCAS and Azure Sentinel to detect suspicious events, monitor and audit privileged access

Securing Privileged Access

Lower exposure and least privileged RBAC design

Securing Privileged Access

Foundation of Privileged Access

Granular Task Scoped Access (Just Enough)

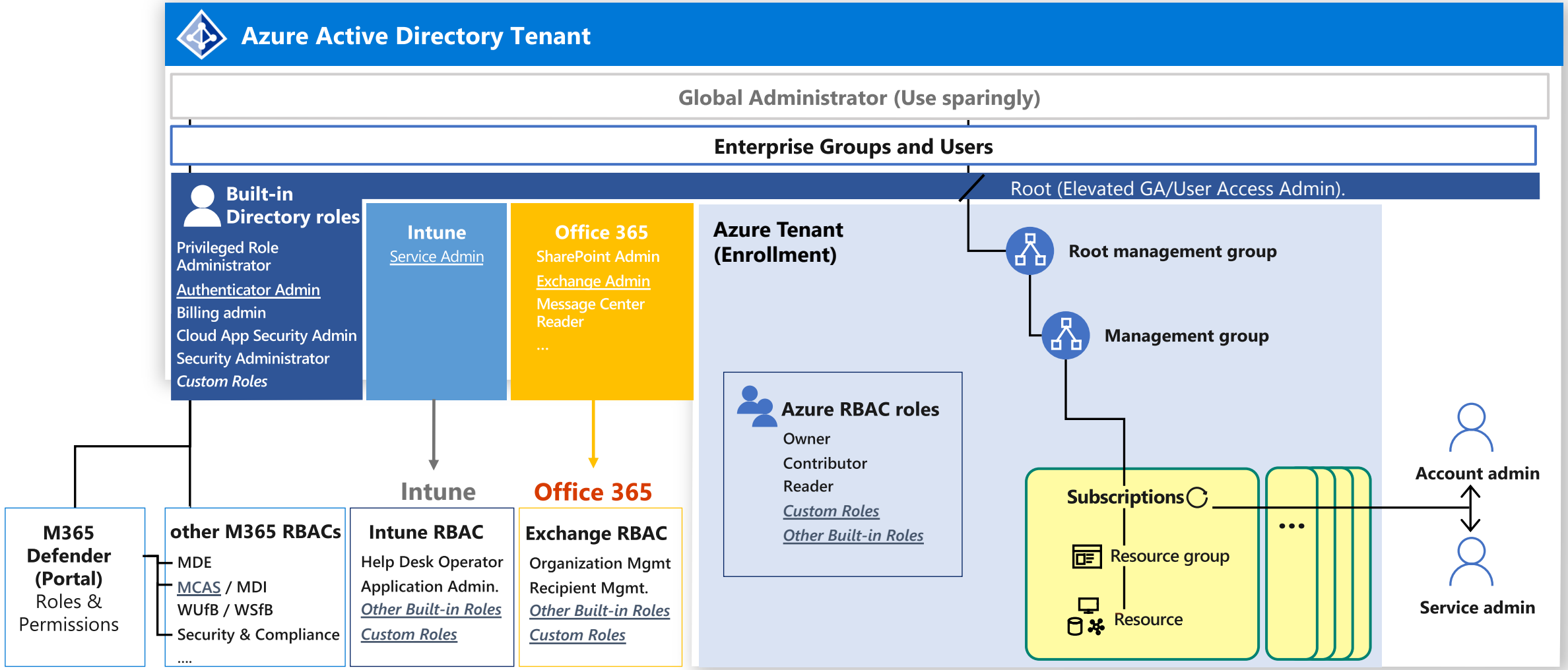
Just in Time Access

Privileged Admin Workflow

Audit Ready

Securing Privileged Access

Azure AD, M365 and Azure RBAC



Source: "Azure Security Compass (Microsoft)"

Protection of Privileged Identities

Demo: RBAC of Azure AD Roles

- Considerations of “Cross-Service” Directory Roles
- Built-in protection of privileged identities in Azure AD

Securing Privileged Access

Tiering of Privileged Access and Accounts

„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**.“

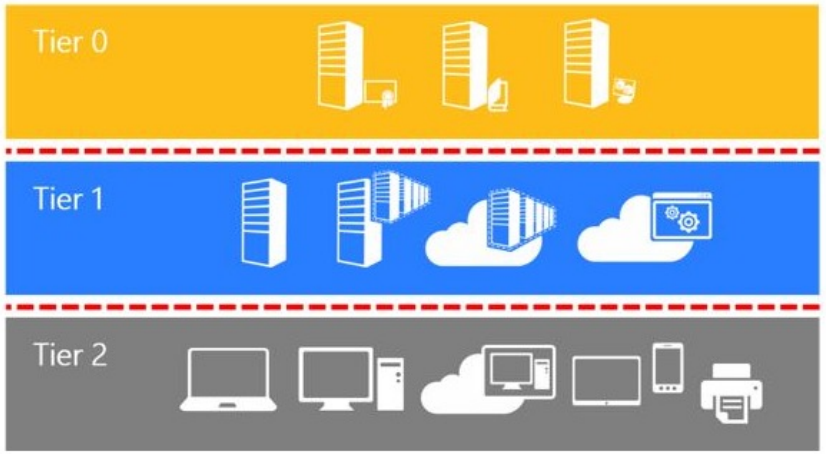
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“, Page 8

Active Directory administrative tier model

02/14/2019 • 33 minutes to read • +6

Applies To: Windows Server

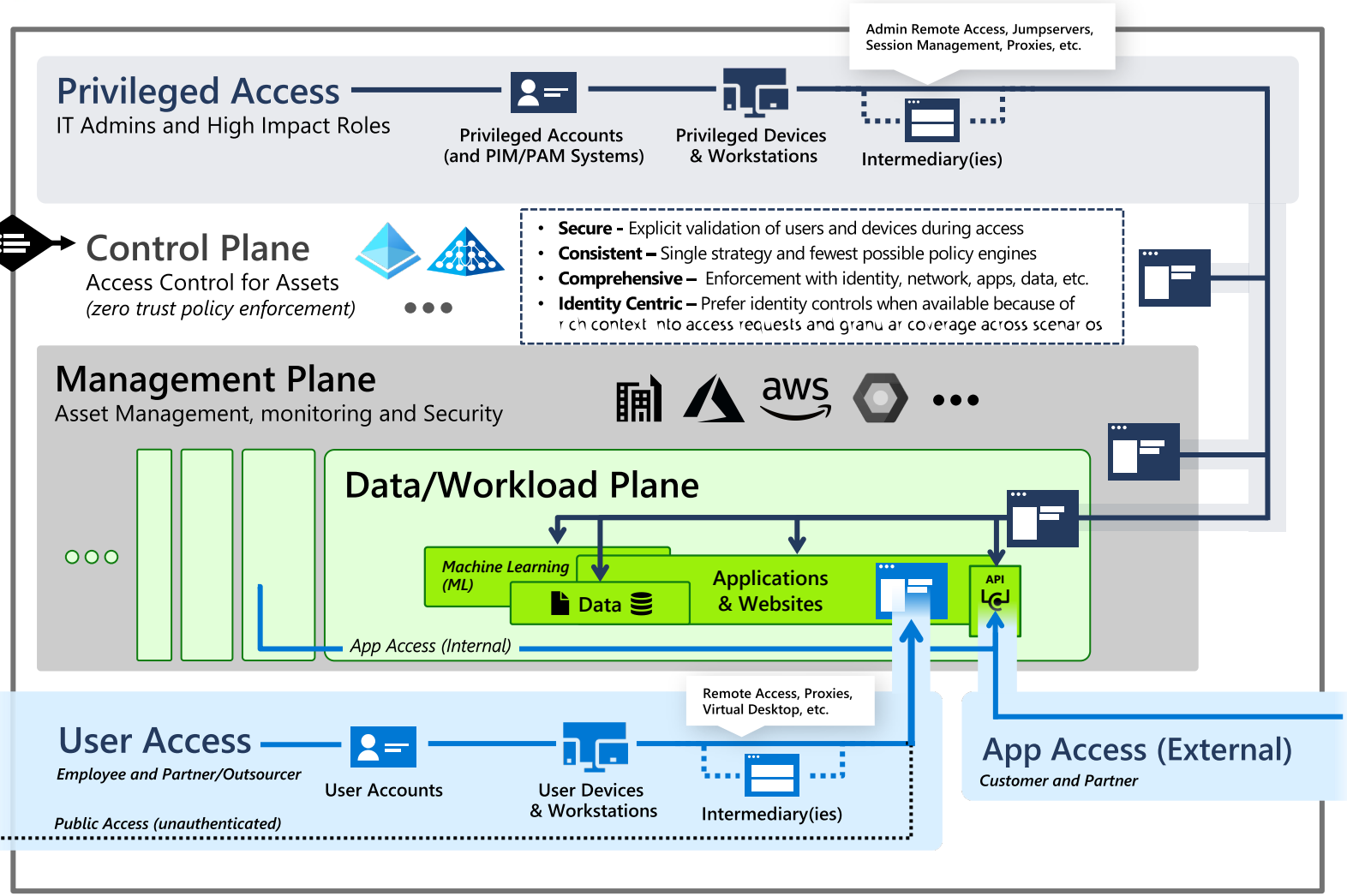
The purpose of this tier model is to protect identity systems using a set of buffer zones between full control of the Environment (Tier 0) and the high risk workstation assets that attackers frequently compromise.



Source: “Securing Azure environments with Azure Active Directory”

Securing Privileged Access

Evolution of ESAE: Enterprise Access Model (EAM)



Privileged Access

Enables IT administrators and other high impact roles to access to sensitive systems and data. *Stronger security for higher impact accounts*

Control and Management Planes

Provide unified access and management for workloads and assets *(and provide attackers shortcut for illicit objectives)*

Data/Workloads

Create and store business value in

- Business processes (in apps/workloads)
- Intellectual property (in data and apps)

User and App Access

How employees, partners, and customers access these resources

Source: "Enterprise Access Model (Microsoft Docs)"

My EAM implementation in Azure

www.wpninjas.eu

Control Plane: Identity Ops
Azure AD Tenant Management (Directory-Level)

Tier0

Access Controls
Cross/Service Directory Roles | Priv. Access & Entitlement | Cond. Access & Session Policies | (Admin) Consent & Pol.

DevOps Helpdesk/Administration
Scoped Delegation (Administrative Units-Level)

AU "Platform Management Accounts"

AU "Workload Management Accounts"

Root

Management Assets
Governance & Security | SP/MSI Identities

Management Plane: Platform
Management Group (Segment)

Data/Workload Plane
Resource Group (App Res.)

Tenant Root Group

Corp

Platform

Landing Zone(s)

Subscription(s)

	Platform Ops	SecOps	NetOps	Service Admin	AppOps/ DevOps
	Eligible Built-in Owner (PIM Approval by Tier0) and Contributor role on MG Levels	*with a horizontal view across the entire access controls and management assets*	*Platform-wide global connectivity operations*	**Service Admin** *(Break Glass Access)* *Primarily used for initial configuration and emergency access* *(Shared Responsibility between Tier0 and Tier1)*	
Management					
Connectivity					
Identity (AD DS, PKI, AAD Automation,...)	*Restrict Access*	*Monitors suspicious privileged activities in Azure and Azure AD incl. Potential Escalation Paths*	*Restrict Access*		
Secure Admin Access (Cloud Shell, Bastion, SAW, VPN,)	*Restrict Access*		*Restrict Access*		
Security Operations (Sentinel, Playbooks,...)	*Restrict Access*		*Restrict Access*		
SAP/Corp/Online (Workload)	*Management group and subscription lifecycle management*		*Management of VNets, UDRs, NSGs, NVAs, VPN, and others*		*(Resource) Contributor*
...					

Tier1

Protection of Privileged Identities

Demo: Tiered Administration Model

- Administrative Units (AUs)
- Custom Roles in Azure AD
- Role-Assignable Groups and Privileged Access Groups (PAG)
- Entitlement Management and Access Package

Protection of Privileged Access

Key takeaways

Privileged Identity

- Separated/isolated accounts from “productive” tasks
- Strong and passwordless authentication options
- Conditional Access Policies to protect authorization paths to interfaces/intermediaries
- MCAS and Azure Sentinel to detect suspicious events, monitor and audit privileged access

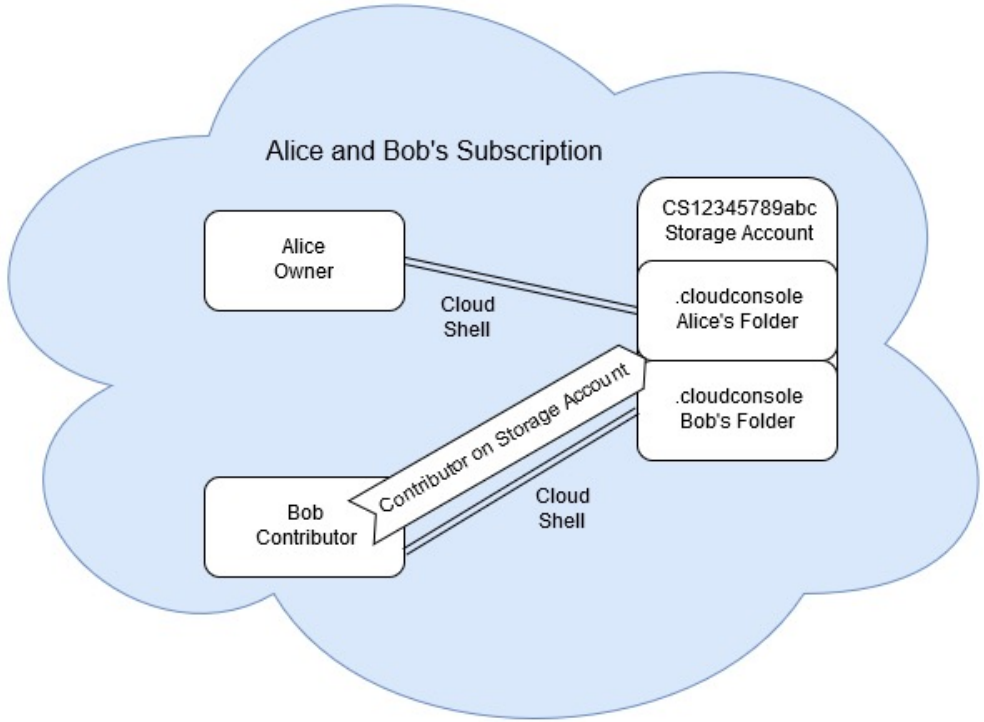
Privileged Access

- Just-in-Time Access by Azure PIM
- Protection of critical privileged users & groups by role-assignable / privileged access groups
- Approval, assignment and review of (scoped) privileged roles by Identity Governance
- Design of least privileged by defined and tiered RBAC model (Scoped vs. Directory-Level)

Securing Privileged Access

Privilege Escalation from Storage Contributor

Azure Privilege Escalation via Azure Cloud Shell (Blog post by Karl Fosaaen)




```
$token = (curl http://localhost:50342/oauth2/token --data
"resource=https://management.azure.com/" -H Metadata:true -s)
```

Microsoft Security Response Center (MSRC) response:

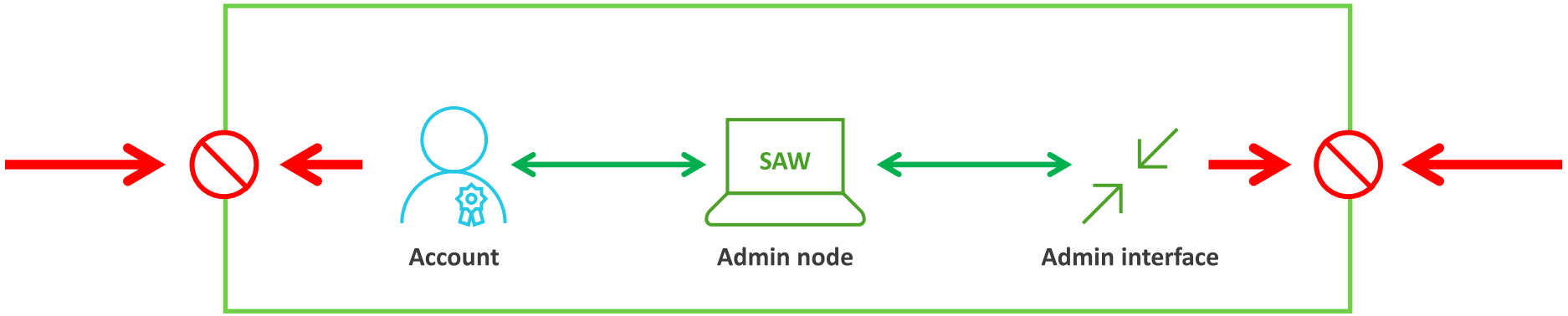
*"…**confirming** that this is the **currently designed behavior**. We have expanded **our guidance** on this issue here (…) and the team will look into **possible design changes** related to storage accounts."*

Access from Secure Admin Workstations

Improve privileged security by using hardened endpoints

Access from Secure Admin Workstation

Overview of Secure Admin Workstation



- DISA STIG requires Privilege Access Workstations (PAW) for Cloud Tenant Management
- **CIS (C4)**: Administrators shall use a dedicated, isolated machine for all administrative tasks

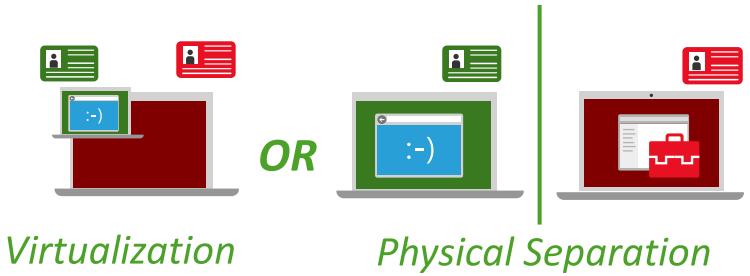


Image source: "Microsoft CISO Workshop 4a - Threat Protection Strategy"

Access from Secure Admin Workstation

Demos

- SAW template from Microsoft
- Windows Logon with FIDO2
- MyAccess and MyRoles
- MCAS: Restricting and monitoring to unprivileged access

Securing your privileged IAM

www.wpninjas.eu

Privileged Identity

- Separated/isolated accounts from “productive tasks”
- Strong and passwordless authentication options
- Protected authorization paths to priv. interfaces/intermediaries by Conditional Access & MCAS
- Using MCAS & Azure Sentinel to detect suspicious events, monitor and audit privileged access

Privileged Access

- Just-in-Time Access by Azure PIM
- Protection of critical privileged users & groups by role-assignable and privileged access groups
- Approval, assignment and review of (scoped) privileged roles by Identity Governance
- Design of least privileged by defined and tiered RBAC model (Scoped vs. Directory-Level)

Secure Admin Worktation

- Privileged access from hardened (cloud managed) device only (using device filters in CA Policies)
- Balance between usability and security of administrators
- Protection of privileged intermediaries (VPN, Cloud Shell)
- Separation of User and Privileged Endpoint Management and Helpdesk Support

Privileged Service Principals

Auditing and protecting of secrets and priviliged access in Automation tasks or DevOps Pipelines (CI/CD)

Thank You