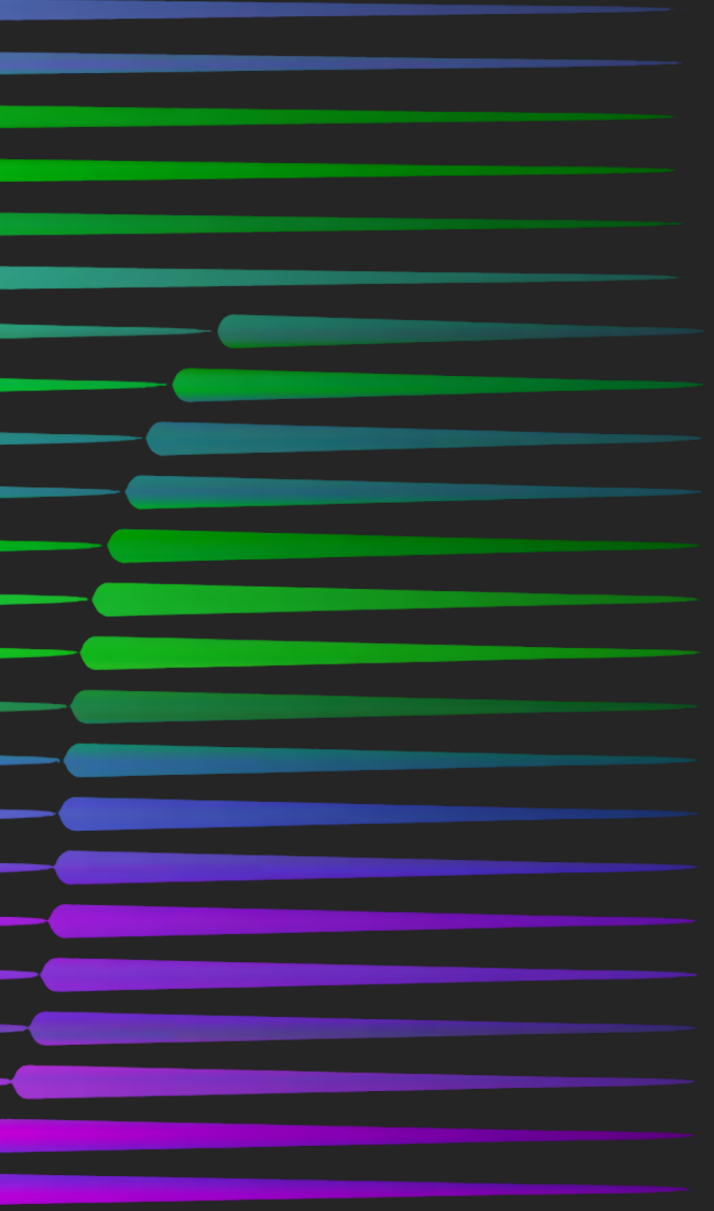


Securing your privileged identity & access in Azure AD

Thomas Naunheim

NORDIC — VIRTUAL SUMMIT —

Securing your privileged identity & access in Azure AD

Thomas Naunheim
Cloud Architect @glueckkanja-gab AG
Microsoft MVP

@Thomas_Live

www.cloud-architekt.net

NORDIC — VIRTUAL SUMMIT —

NORDIC
– VIRTUAL SUMMIT –

Securing your privileged identity & access in Azure AD

Privileged Identity

Privileged Access

Secure Admin Workstation

Level of Isolation and Seperation
= Your Balance of Security, Complexitity and Usability

NORDIC
– VIRTUAL SUMMIT –

Protection of Privileged Identities

Strong security baseline for high impact accounts

Protection of Privileged Identities

Foundation of Privileged Accounts

NORDIC
– VIRTUAL SUMMIT –

Separation of work and privileged accounts

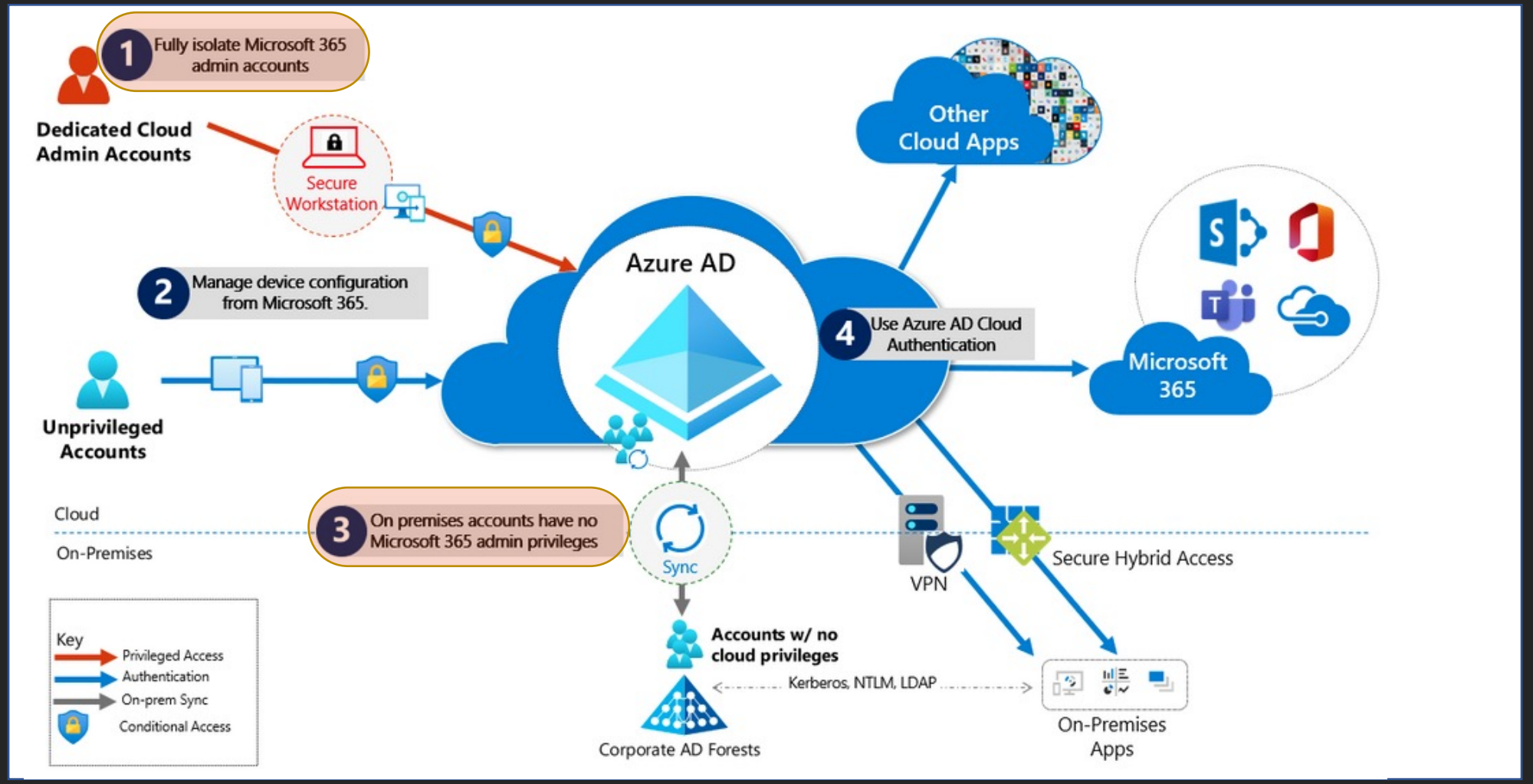
- ✓ Do not use unmanaged (personal) accounts
- ✓ Separate your work and privileged account(s)
- ✓ Do not sync from (AD) on-premises
- ✓ Implement identity lifecycle & access review
- ✓ Remove licenses of productivity workloads

Secured and hardened Azure AD Tenant

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

Protection of Privileged Identities

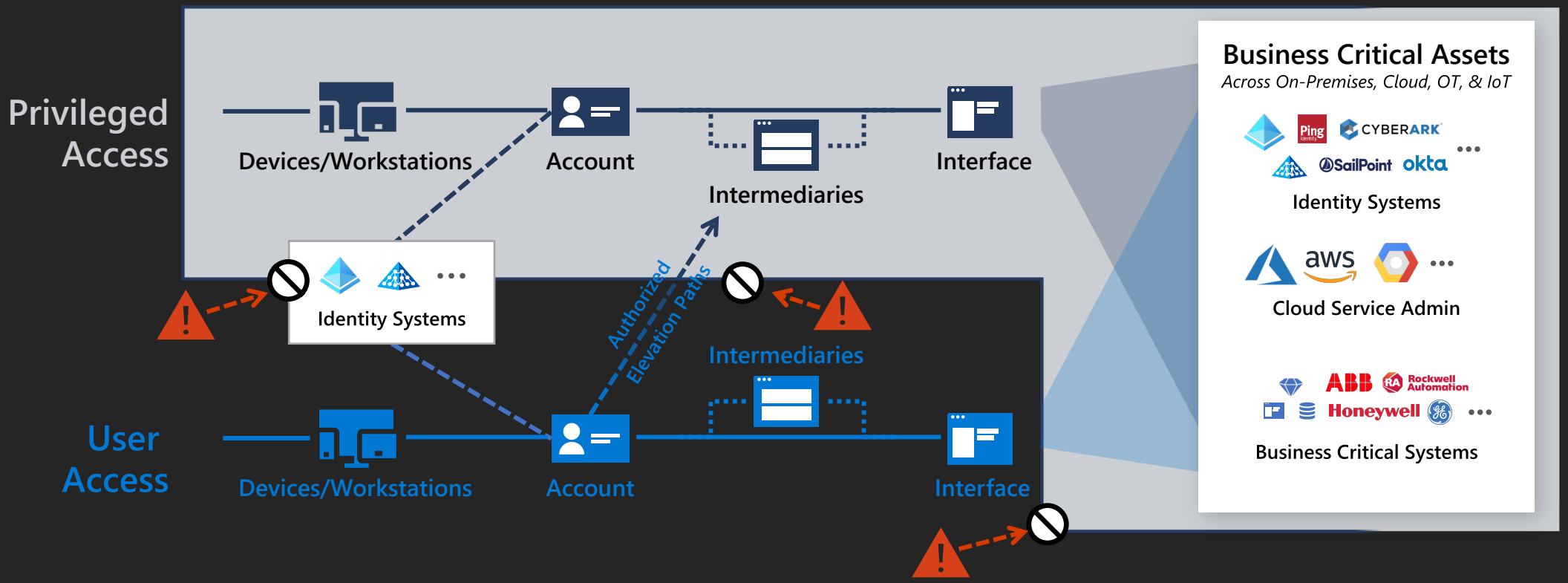
Protecting M365 from on-prem attacks



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

Protection of Privileged Identities

Authorized Elevated Paths



"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

Source: "Privileged access Strategy" (Microsoft)

Protection of Privileged Identities

Live Demo

NORDIC
– VIRTUAL SUMMIT –

- Conditional Access Design
- Detection of suspicious activities with Azure Sentinel and MCA

Protection of Privileged Identities

Key takeaways

NORDIC
– VIRTUAL SUMMIT –

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

NORDIC
– VIRTUAL SUMMIT –

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

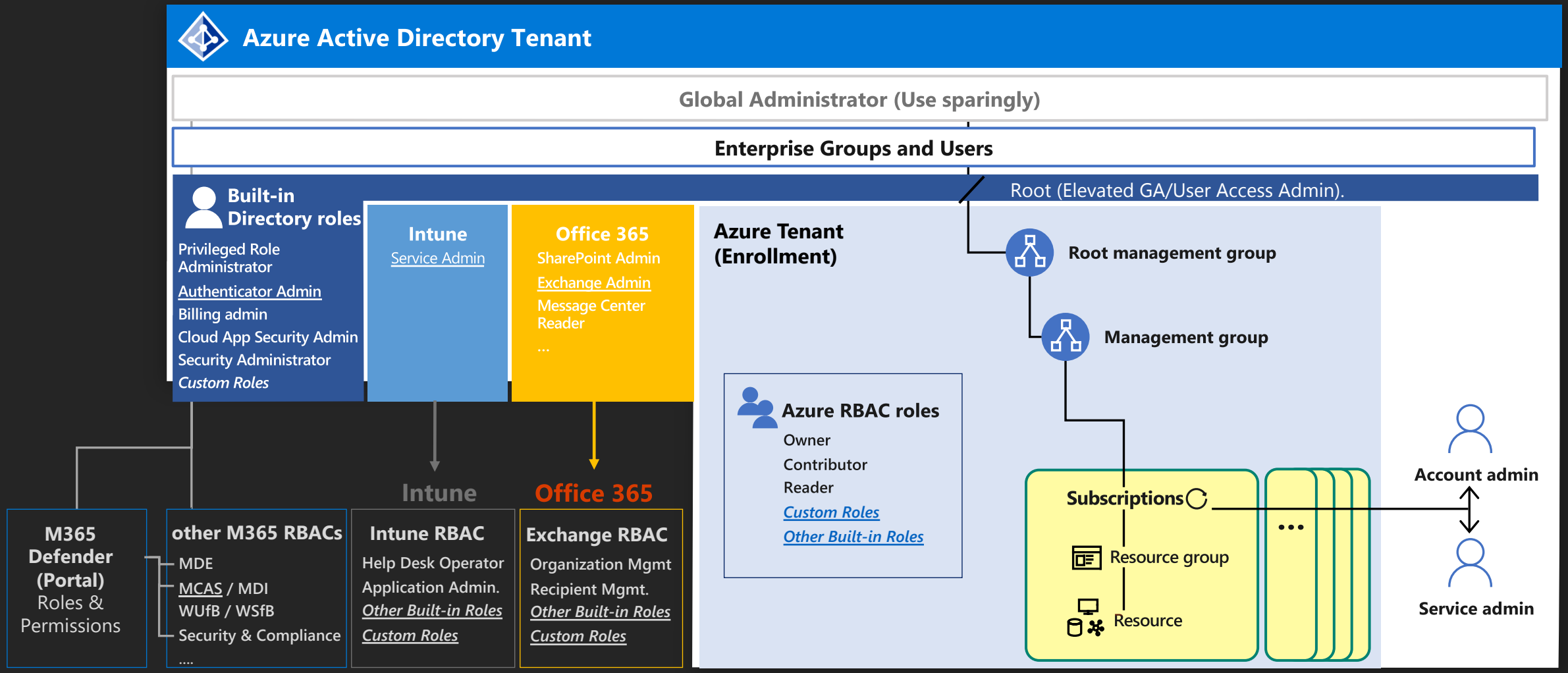
Privileged Admin Workflow

Audit Ready

Securing Privileged Access

RBAC(s) in Microsoft Cloud Services

NORDIC — VIRTUAL SUMMIT —



Source: "Azure Security Compass (Microsoft)"

Protection of Privileged Access

Live Demo

NORDIC
– VIRTUAL SUMMIT –

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

Protection of Privileged Access

Tiered Administration in Azure?

NORDIC
– VIRTUAL SUMMIT –

„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**."

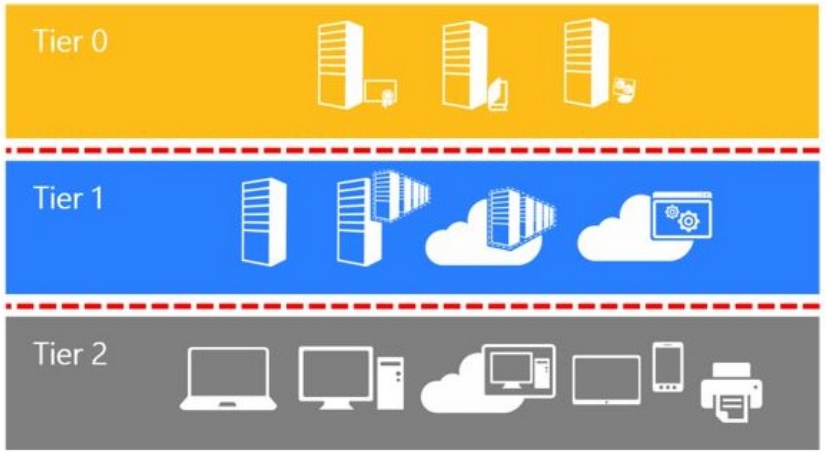
Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)", Page 8

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.

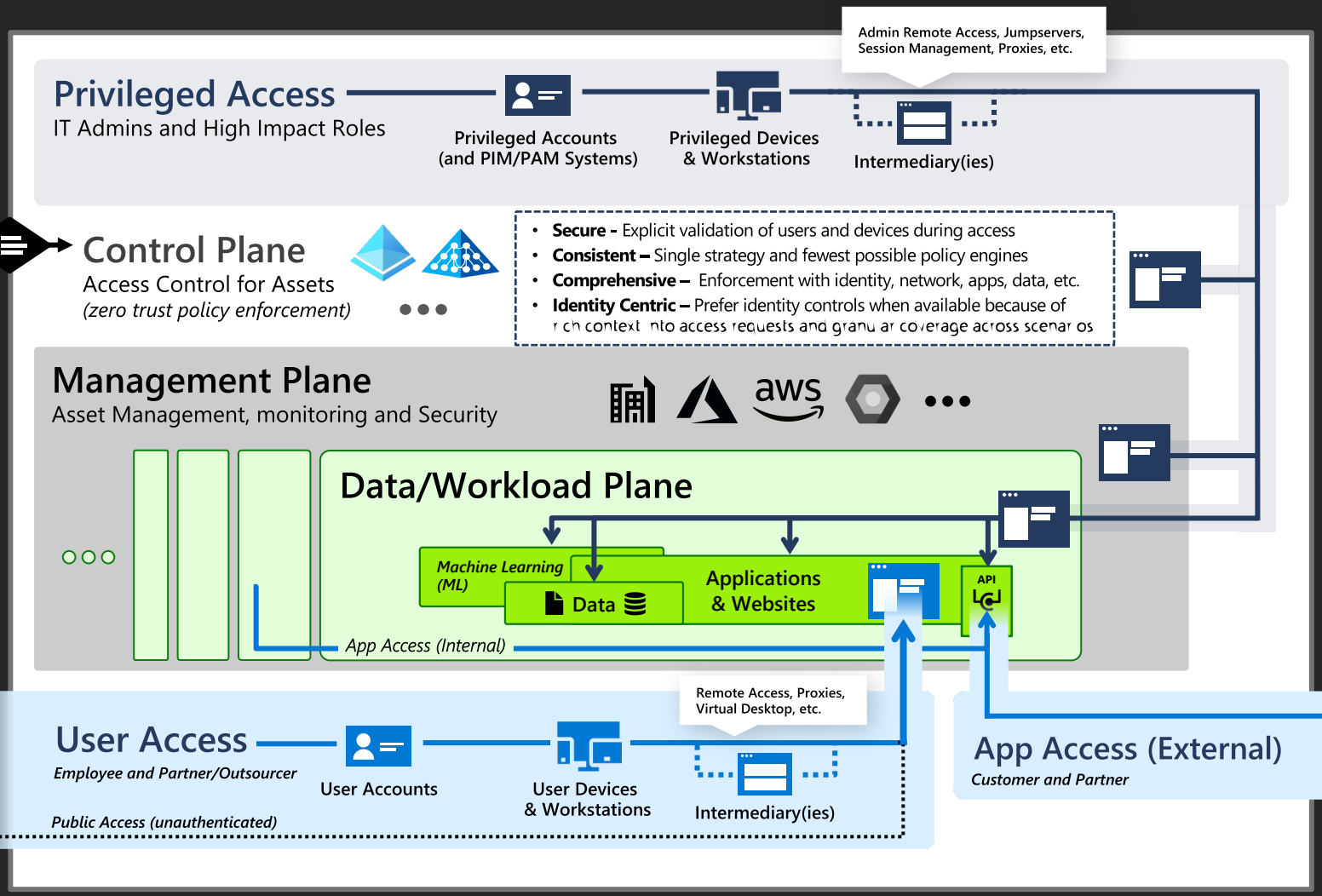


Source: "Securing Azure environments with Azure Active Directory"

Protection of Privileged Access

Enterprise Access Model (EAM)

NORDIC
— VIRTUAL SUMMIT —



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

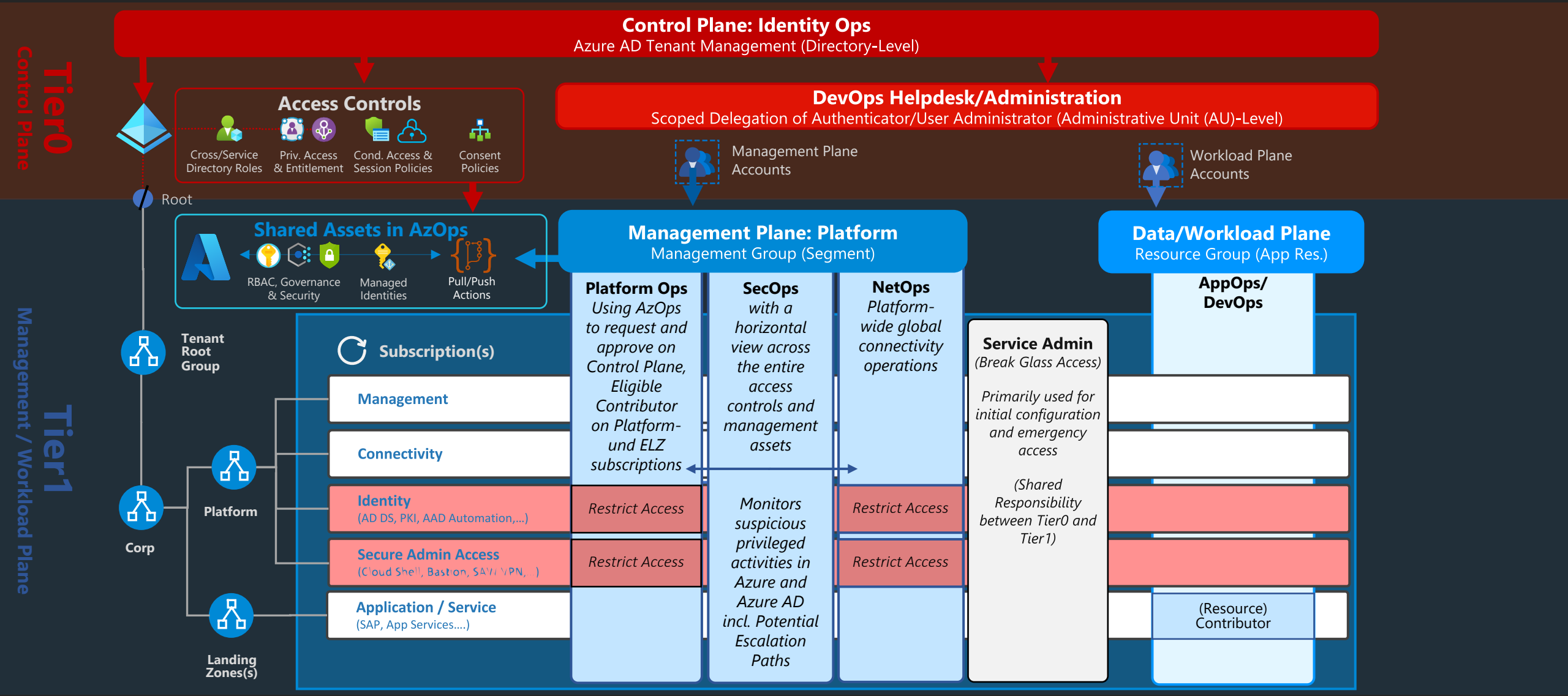
How employees, partners, and customers access these resources

Source: "Enterprise access model" (Microsoft)

Protection of Privileged Access

My EAM implementation in Azure

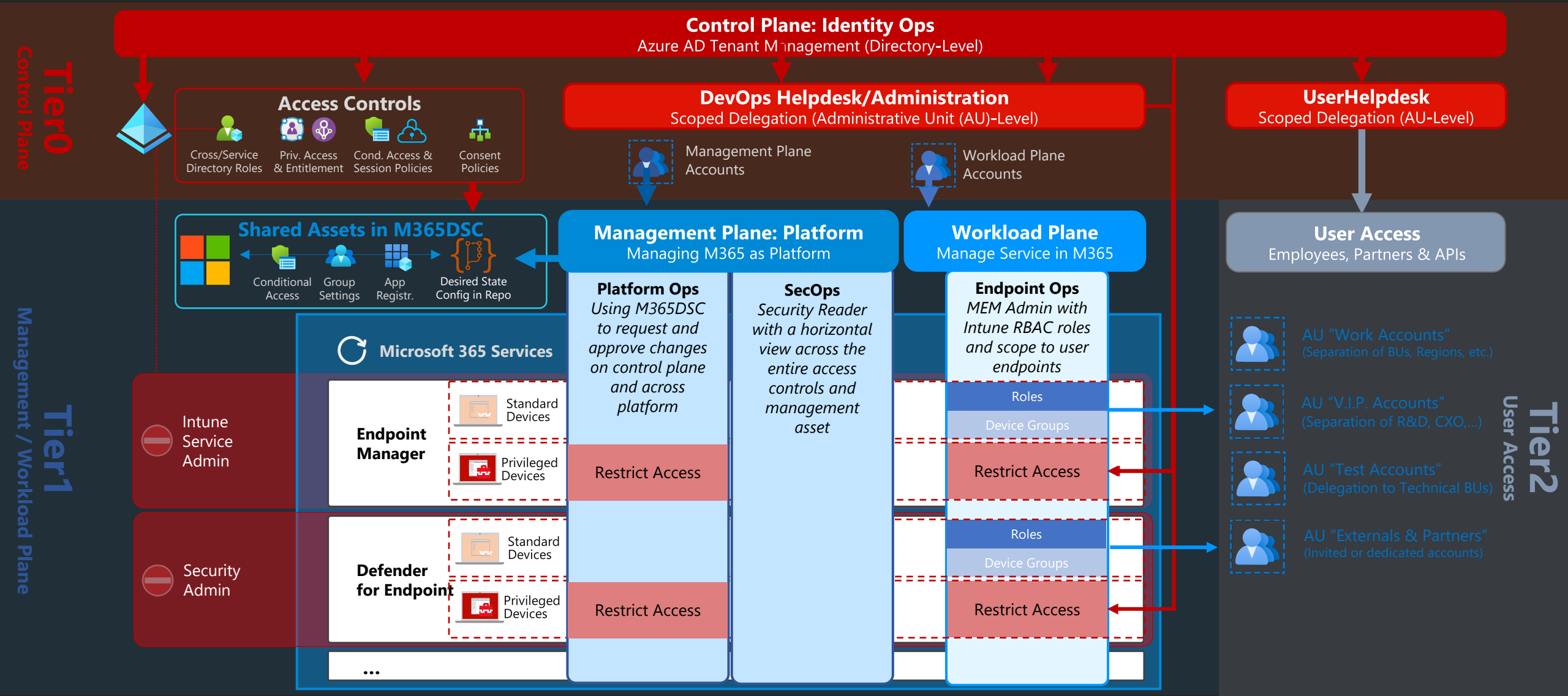
NORDIC — VIRTUAL SUMMIT —



Protection of Privileged Access

EAM solution approach in M365

NORDIC — VIRTUAL SUMMIT —



Protection of Privileged Access

Live Demo: RBAC of Azure AD Roles

NORDIC
– VIRTUAL SUMMIT –

- Administrative Units (AUs)
- Role-Assignable Groups and Privileged Access Groups (PAG)
- Entitlement Management and Access Package

Protection of Privileged Access

Key takeaways

NORDIC
– VIRTUAL SUMMIT –

Privileged Ident

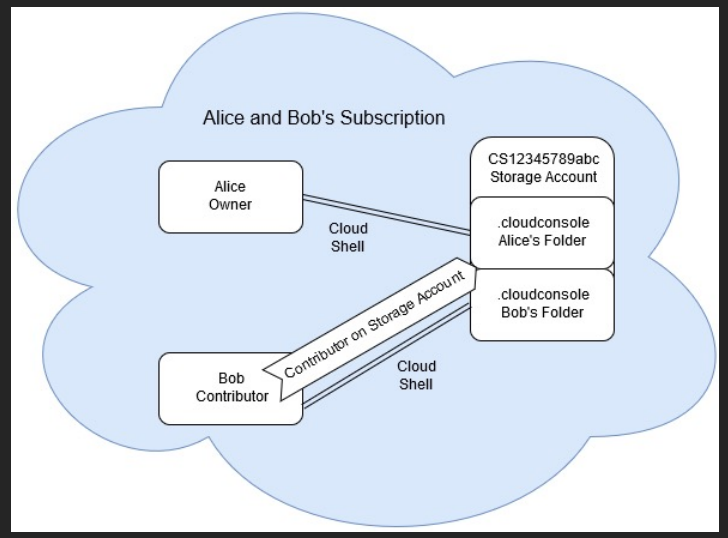
- Separated/isolated acc
  from "productive" task
- Strong and passwordle
  authentication options
- Conditional Access Pol
  protect authorization p
  interfaces/intermediari
- MCAS and Azure Senti
  detect suspicious even
  and audit privileged ac

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)

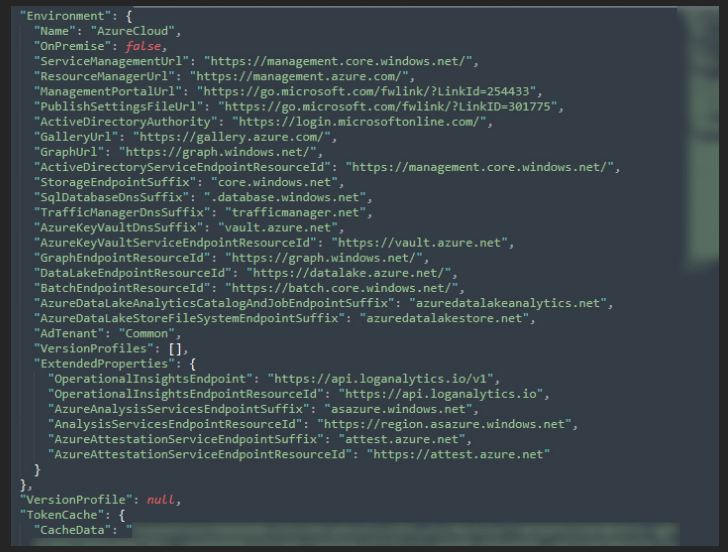
Protection of Privileged Access

Privileged Escalation (Intermediaries)



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

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



Dumping from PowerShell Memory
(Blog post by R.J. McDown)

Cached Tokens by PowerShell Modules
for Azure (AD) Management

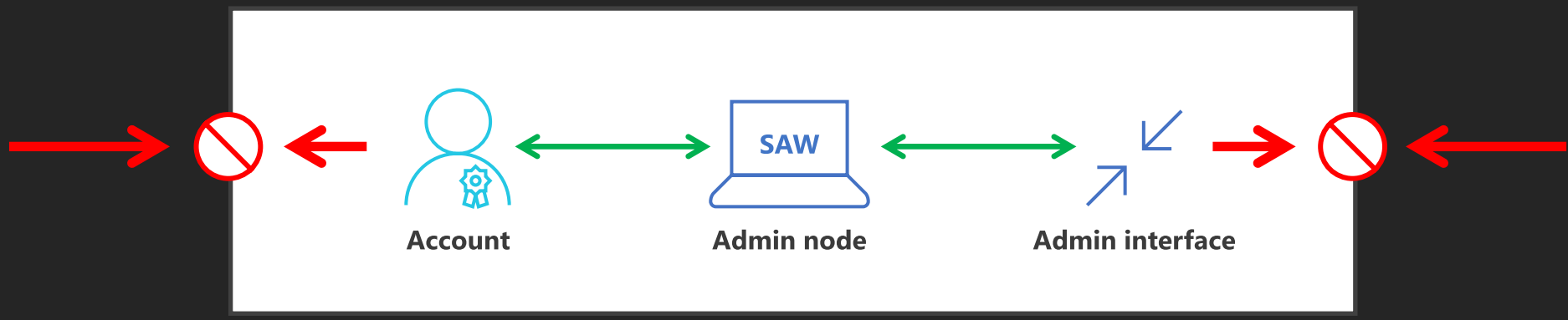
NORDIC
– VIRTUAL SUMMIT –

Access from Secure Admin Workstations

Improve privileged security by using hardened endpoints

Access from Secure Admin Workstations

Foundation of SAW



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

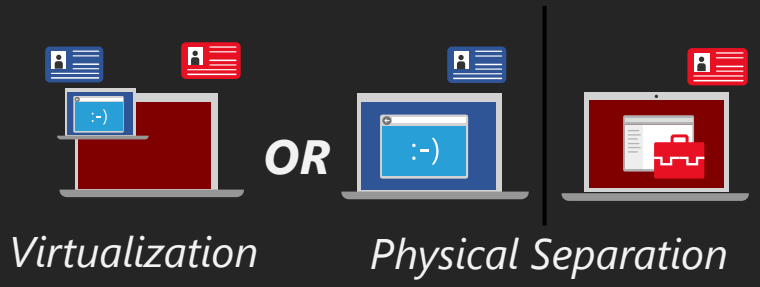


Image source: "Microsoft CISO Workshop_4a - Threat Protection Strategy"

Protection of Privileged Access

Live Demo

NORDIC
– VIRTUAL SUMMIT –

- SAW template from Microsoft
- Windows Logon with FIDO2
- “My Access” Portal for Request and Approval

Securing your privileged identity & access in Azure AD
Key takeaways

NORDIC
– VIRTUAL SUMMIT –

Privileged Identity

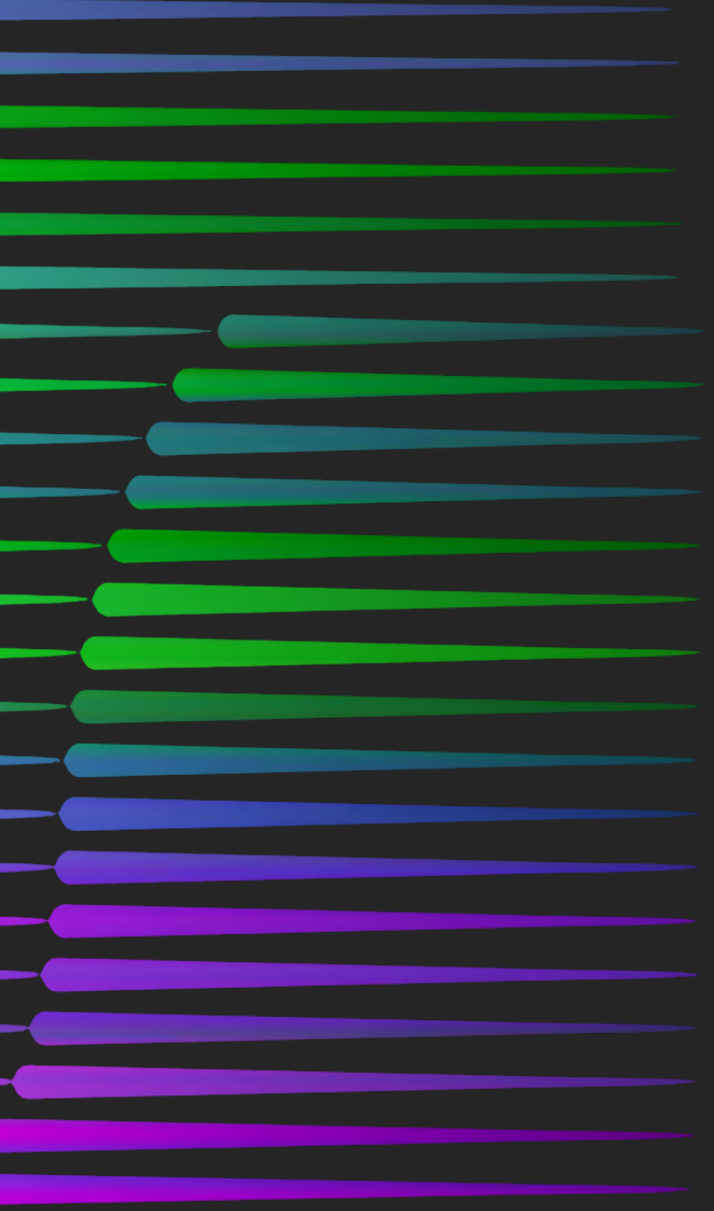
- Separated/isolated accounts from “productive tasks”
- Strong and passwordless authentication options
- Protected authorization paths to priv. interfaces/intermediaries by Conditional Access & MCAS
- Using MCAS & Azure Sentinel to detect suspicious events, monitor and audit privileged access

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 Workstation

- 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



Thank You!
Q&A

- Twitter: @Thomas_Live
- www.cloud-architekt.net

NORDIC — VIRTUAL SUMMIT —