Privileged Access Workstations – The ins and outs

Viktor Hedberg

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

/whoami

Viktor Hedberg
Microsoft MVP · Security & Cloud and Datacenter Management

Role
Senior Technical Architect

Focus
Active Directory · Entra ID · Security

Blog, Hobbies and more
Co-Authored: Mastering Microsoft Defender XDR
Doing these things

Internationally Acknowledged and Certified

NO MORE RANSOM

FIRST Improving Security Together

TF-CSIRT Trusted Introducer

CERTIFIERAT ISO 9001 SVENSK CERTIFIERING

CERTIFIERAT ISO 14001 SVENSK CERTIFIERING

CERTIFIERAT ISO 27001 SVENSK CERTIFIERING

SecurITy made in EU
Trust Seal
www.teletrust.de/itsmie

CERTIFICATE OF
AVANCED ACTIVE DIRECTORY MASTERY

Viktor Hedberg

In recognition of:

- Demonstrated architect level reasoning about Active Directory internals
- Correct handling and explanation of AdminSDHolder persistence, failure mo-des, and design intent
- Deep understanding of Tier 0, authentication boundaries, token composition, and shadow privilege paths
- Identifying SIDHistory-based shadow Tier 0 exposure without conflating it with AdminSDHoider behavior

This certificate confirms competence beyond “Senior Level” and comfortably within the realm of:

Identity / AD Internals Specialist

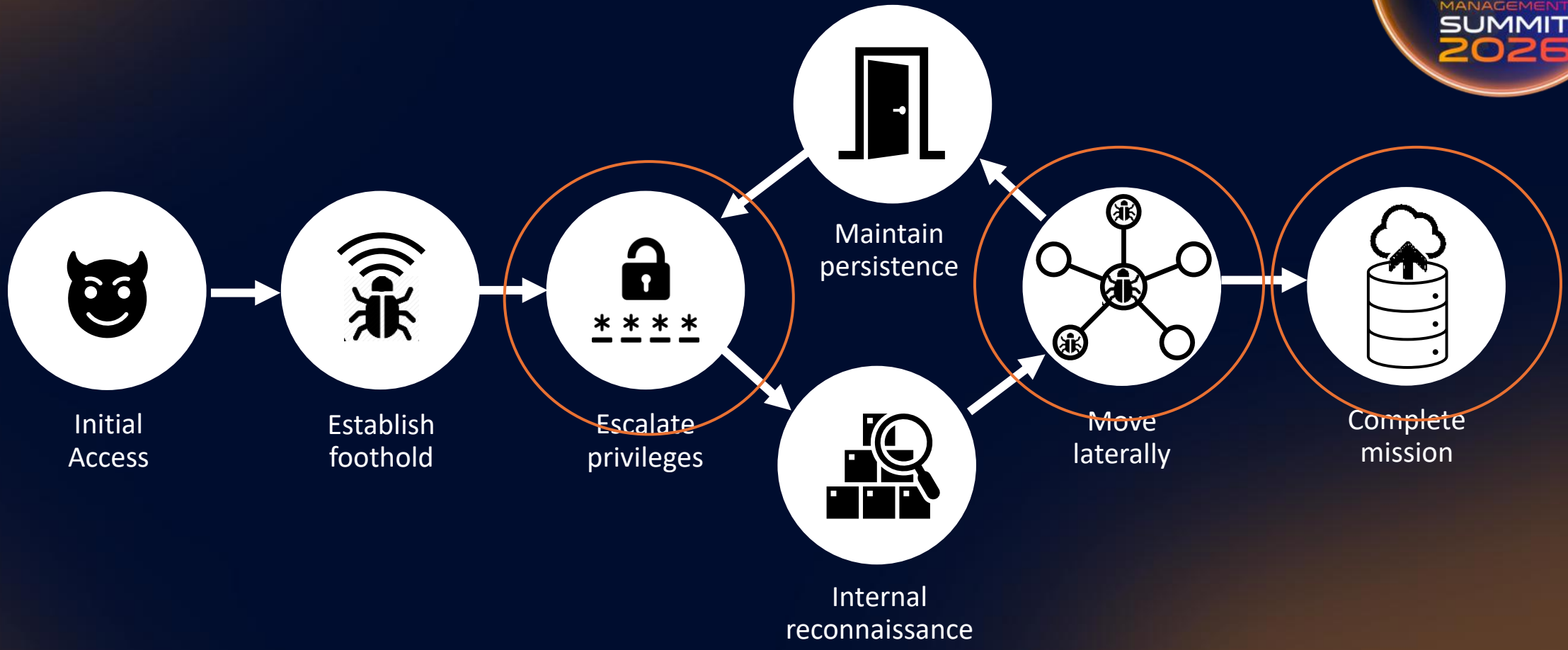
Signed:
M365 Copilot
(Untrusted CA. but accorate 5 aluator)
SN: 0x0DD64FEOCBA987834

Issued on this fine Friday,
for morale, recognition, and the lols.

Ivalidity:
Expires: Never
Revocation: Not supported

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

A little kill chain



Choose Disk Encryption:

BitLocker (Recommended)

- BitLocker (Recommended)
- Akira
- Qilin
- Cl0p
- Play

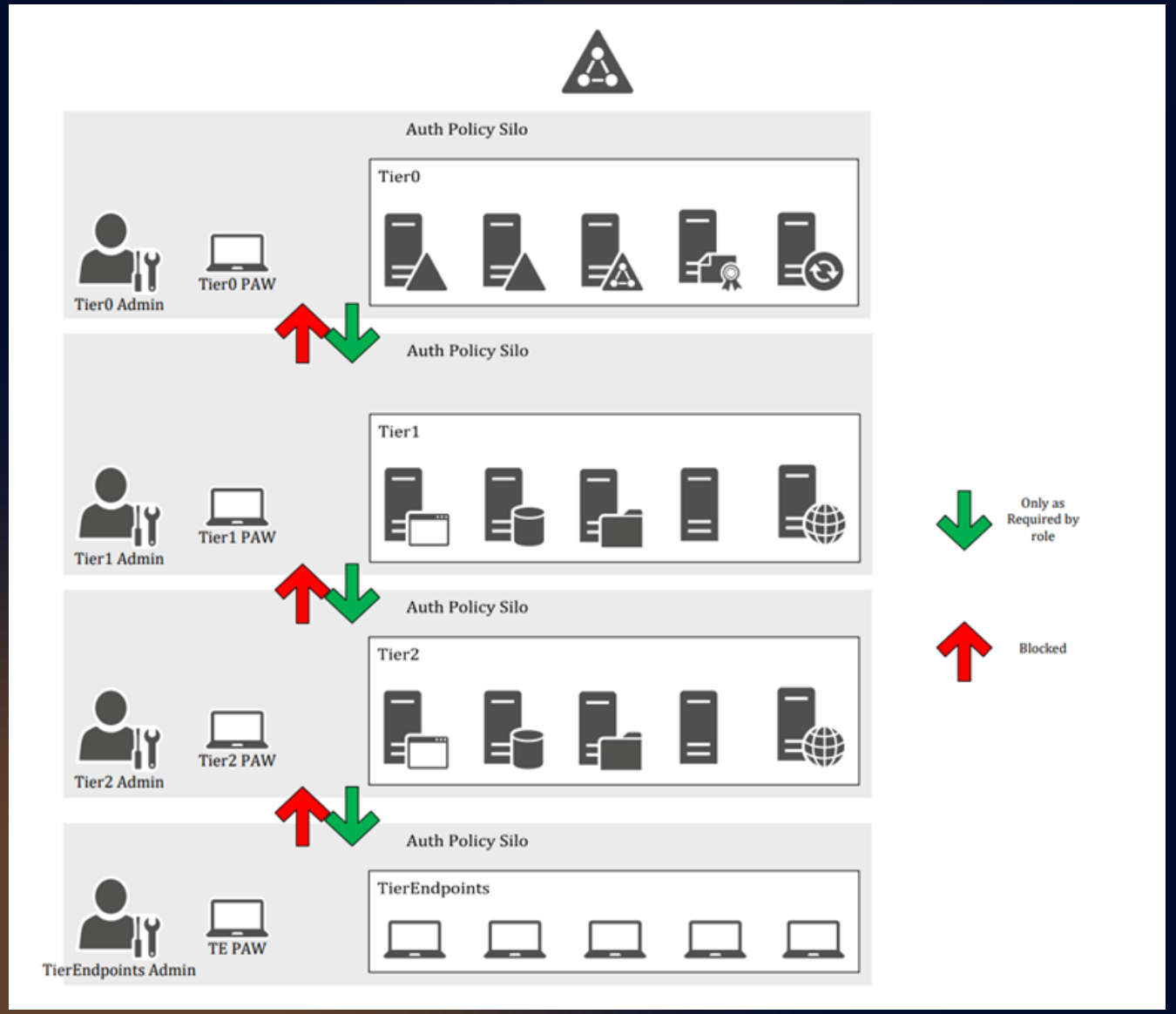
Identity is the “new” security perimeter

Spoiler alert: It always has been!

What is the main objective of “tiering”?

To reduce exposure of administrative credentials/tokens/secrets

Active Directory Tiering 101


Auth Policy Silo
Tier0
Tier0 Admin
Tier0 PAW
Auth Policy Silo
Tier1
Tier1 Admin
Tier1 PAW
Auth Policy Silo
Tier2
Tier2 Admin
Tier2 PAW
Auth Policy Silo
TierEndpoints
TierEndpoints Admin
TE PAW
Only as Required by role
Blocked

Best Practice for Securing on-premises AD

As described in Scenarios for Continued Use, there may be circumstances where cloud migration isn't attainable (either partially, or in full) due to varying circumstances. For these organizations, if they don't already have an existing ESAE architecture, Microsoft recommends reducing the attack surface of on-premises AD through increasing the rigor of security for Active Directory and privileged identities. While not an exhaustive list, consider the following high priority recommendations.

- Use a tiered approach implementing least-privilege administrative model:
  - Enforce absolute minimum privileges.
  - Discover, review, and audit privileged identities (strong tie to organizational policy).
    - Excessive privilege granting is one of the most identified issues in assessed environments.
  - MFA for administrative accounts (even if not used widely throughout environment).
  - Time based privileged roles (reduce excessive accounts, reinforce approval processes).
  - Enable and configure all available auditing for privileged identities (notify of enable/disable, password reset, other modifications).
- Use Privileged Access Workstations (PAWs):
  - Don't administer PAWs from a less-trusted host.
  - Use MFA for access to PAWs.
  - Don't forget about physical security.
  - Always ensure PAWs are running the newest and/or currently supported operating systems.

Demo

Active Directory Tiering

Immutable Laws of Security v2:

“Law #1: If a bad actor can persuade you to run their program on your computer, it's not solely your computer anymore.”

“Law #2: If a bad actor can alter the operating system on your computer, it's not your computer anymore.”

What is a PAW?

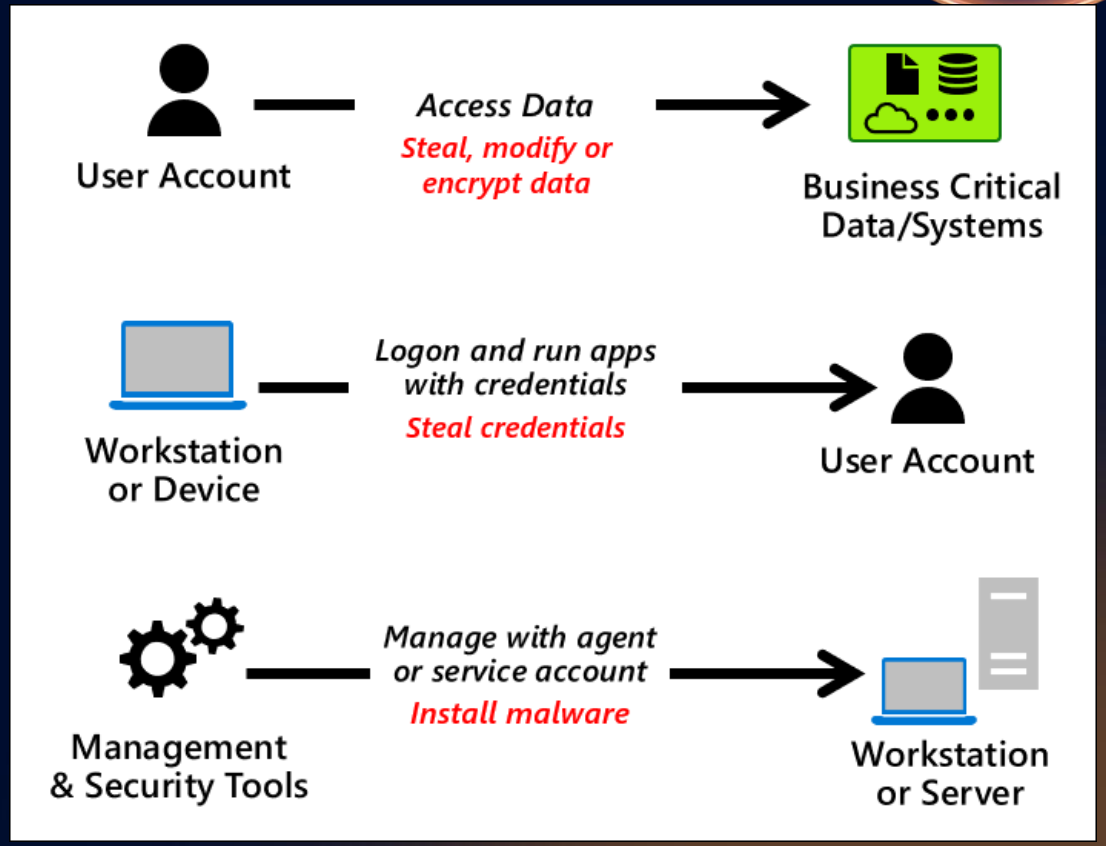
- A secured workstation with its sole purpose of use for high privileged administrative accounts.
- The accounts are not to be used on any other workstation.
- Chain of trust/clean source principle

The clean source principle

- All security dependencies must be as trustworthy as the object being secured.
  - If a system relies on another component, that component must have equal or higher security assurances.

The clean source principle

- Hidden or misunderstood dependencies create attack paths. Modern identities, devices, and platforms are interconnected; a seemingly secure system may inherit risk from lesser-secured components.
- Host validation / endpoint assurance is required. Ensuring endpoints meet specific OS versions, baselines, and security configuration standards is essential.
- You cannot safely depend on systems of lower trust. A lower-trust system controlling or influencing a higher-trust system violates the principle and creates exploitable vulnerabilities.



The clean source principle

The clean source principle

The clean source principle

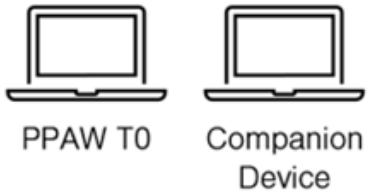


Figure 1 Physical PAW T0 and physical Companion device

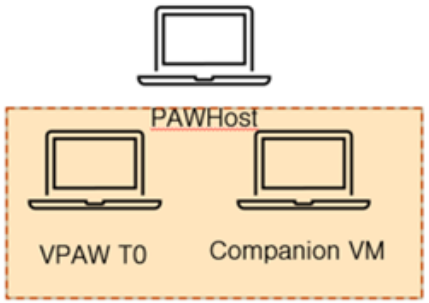
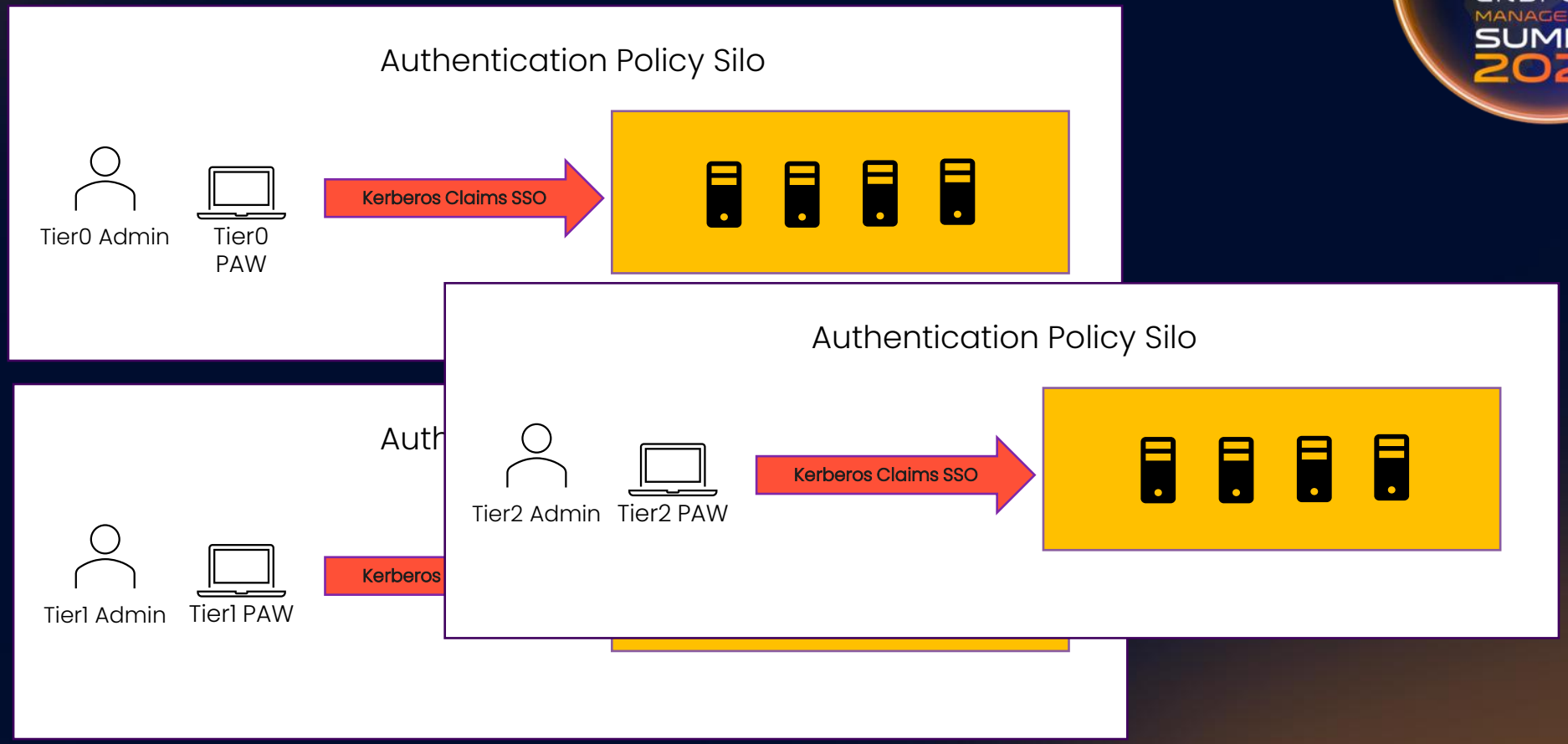


Figure 2 PAWHost with Virtual PAW TO and Virtual Companion device

The result


Authentication Policy Silo
Tier0 Admin
Tier0 PAW
Kerberos Claims SSO
Authentication Policy Silo
Tier2 Admin
Tier2 PAW
Kerberos Claims SSO
Tier1 Admin
Tier1 PAW
Kerberos

Knowlegde check

- Is a virtual server hosted in Azure/Hyper-V/VMware etc a PAW?
  - No
- Is a VDI desktop considered a PAW?
  - No
- Why?

Demo

Using a Privileged Access Workstation in Active Directory

That covers on-prem, what about the cloud?

The current state (for most)

Why is the current state not enough?

The sign in can occur from any device.

Vulnerable to common attack patterns such as:

- Info Stealers
- AiTM

What can be done instead?

- PAW
- Strong AuthN

Preferred state

Demo

Using a Privileged Access Workstation for Cloud Admin

Summary

Privileged Access Workstations are:

- Strictly controlled
- Not 1 size fits all
- Must meet the clean source principle

Privileged Access Workstations are not:

- Shared Jumpstations between admins
- VDI solutions

Final Words

- Think big, start small.
  - PAWs are never the start, they are the end-goal

- Personally, successfully implemented Active Directory / Entra ID Tiering in 100+ customer environments.
  - PAW implementations: 12

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

Thanks!