Mastering the Privileged Access Workstation: Secure by Design

Anders Ahl & Nickolaj Andersen

Anders Ahl

Anders Ahl

Role
Product Owner UEM & PAW

Focus
Intune · Windows Client · Security

Blog, Hobbies and more
Sportscars (Italian, preferably red)
MSEndpointMgr.com

Nickolaj Andersen

Microsoft® Most Valuable Professional

Nickolaj Andersen
Microsoft MVP · Security & Azure

Role
Senior Architect End User Computing

Focus
Intune · Windows 365 · Automation · Azure

Blog, Hobbies and more
F1 · MSEndpointMgr.com

Agenda

- What, why and how
- Design considerations
- Supply chain security
- Provision and manage devices
- Hardening policies

What, why and how

What is a Privileged Access Workstation and why would you need one?

PAW, SAW – key differences, or?

Privileged Access Workstation (PAW)

- Highest security tier for extremely sensitive / Tier 0 roles
- Dedicated to high-impact administrative tasks with maximum isolation
- Strictest controls: no email, no web browsing, minimal attack surface
- Often a physical device; designed for roles where compromise has material organizational impact

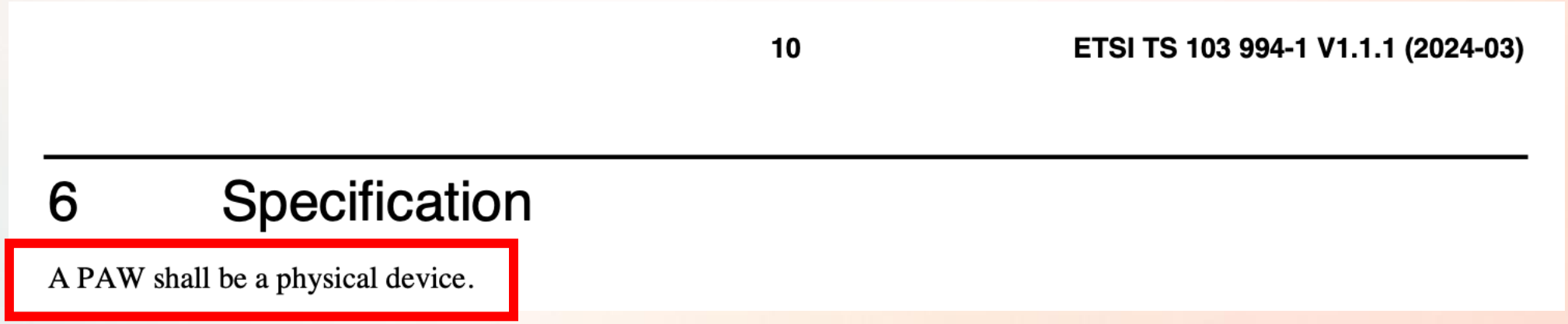
Secure Access Workstation (SAW)

- Secure Admin Workstation Hardened workstation for sensitive administrative tasks (typically medium-to-high risk)
- Strong security with focus on overall lockdown and compliance
- May allow limited productivity in some implementations; often virtual
- Broader use for general privileged operations compared to PAW

Industry consensus:
The terms are often used interchangeably or as near-synonyms. Many sources explicitly state there is no strict, universally mandated difference, organizations may adopt one term or the other based on preference or slight emphasis.

What are you going to use it for?

- Your usage areas for a ‘Privileged Access Workstation’ dictates the defintion and level of security hardening
- Depending on your own definition, start by answering this:
  - Should a PAW be physical or virtual?



10 ETSI TS 103 994-1 V1.1.1 (2024-03)

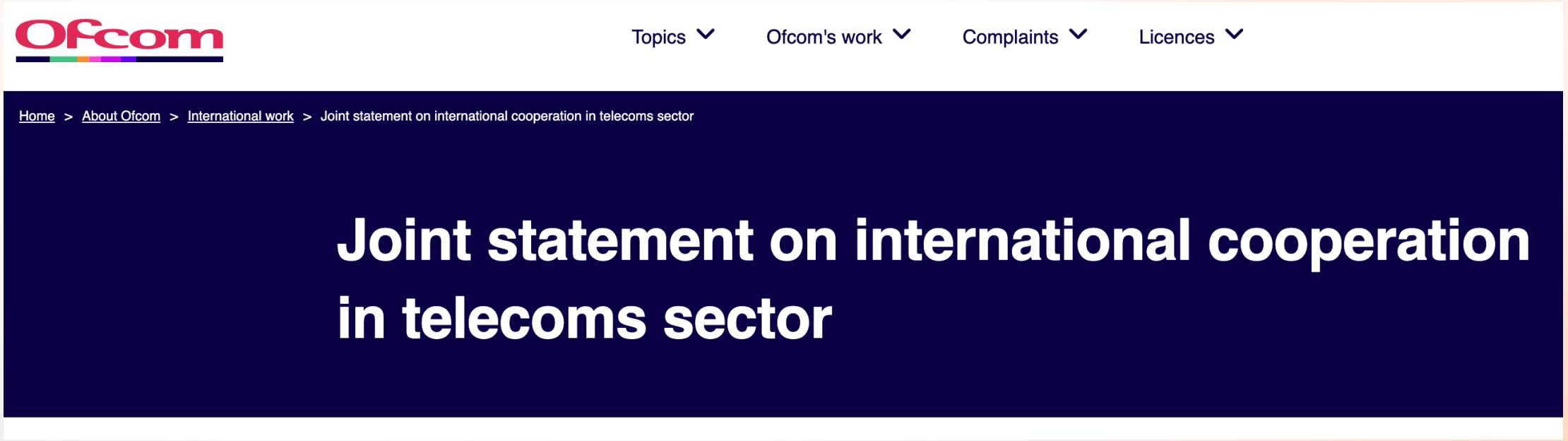
6 Specification

A PAW shall be a physical device.

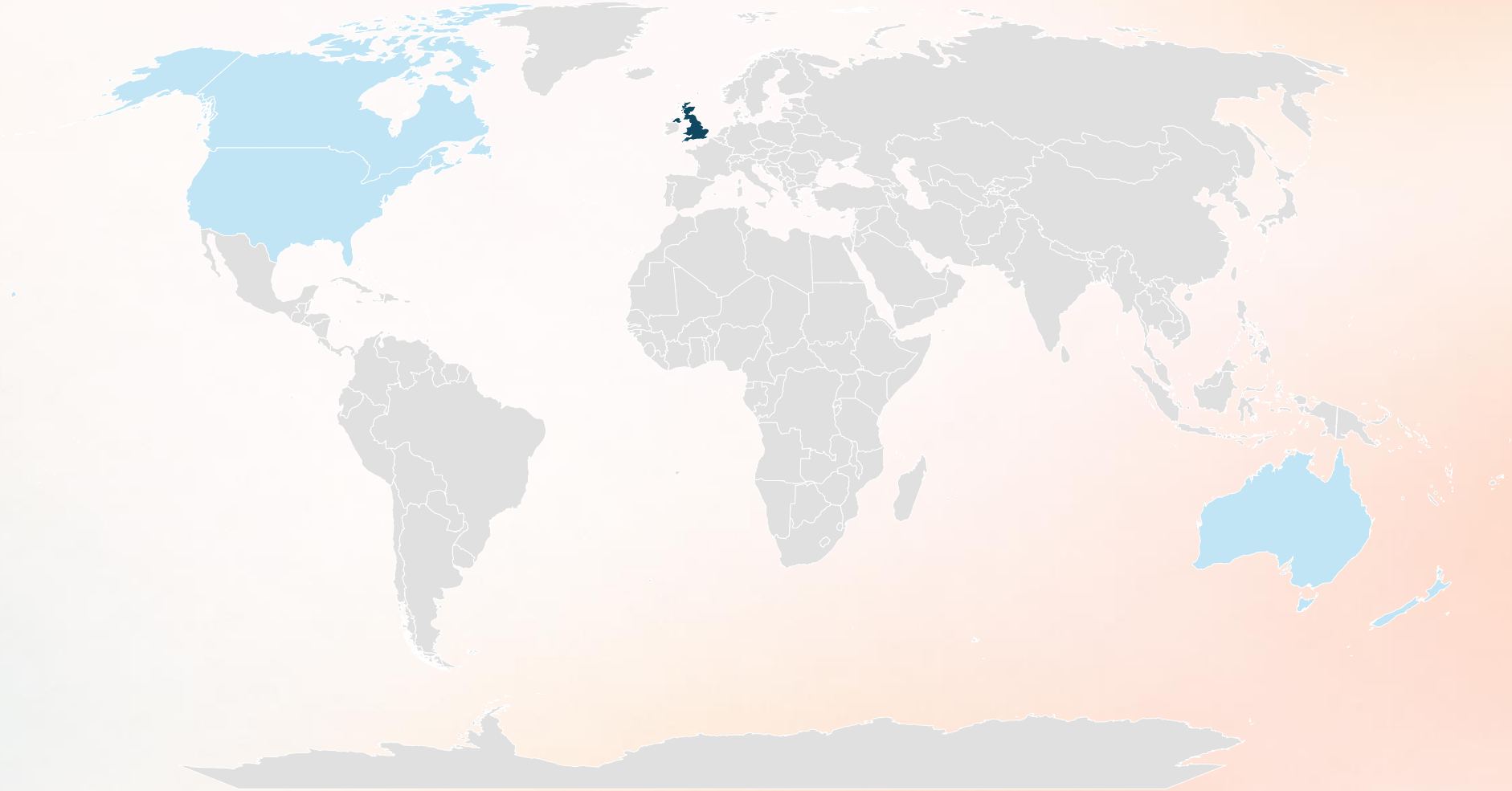
TSA Regulation family

- **TSA – Telecommunications Security Act**
  - Primary legislation - Set by *UK Parliament / DSIT* (Department for Science, Innovation & Technology).
- **TSR – Telecom Security Requirements**
  - Secondary legislation made *under the authority of the TSA*.
  - Drafted and shaped by DSIT, with technical input from NCSC.
- **NCSC – National Cyber Security Centre**
  - Provides expert technical guidance, best practices, and input to DSIT and Ofcom.
  - Does not enforce and does not decide compliance.
- **ETSI (European Telecommunications Standards Institute) – Standards Body**
  - Produces international technical standards that influence the detailed content of the TSR and Code of Practice.
- **Ofcom – Regulator**
  - Enforces the TSA and TSR.
  - Conducts audits, demands evidence, and issues penalties.

Is this for UK Only?



Is this for UK Only?



Design considerations

What to keep in mind when architecting a Privileged Access Workstation

Privileged Access security levels

Privileged Security

Highest privileged access with restricted attack surface

Specialized Security

Used for highly privileged access with restricted attack surface

Enterprise Security

Baseline security for corporate assets & starting point for security

Privileged Access security levels

Privileged Security

Highly privileged access with restricted attack surface

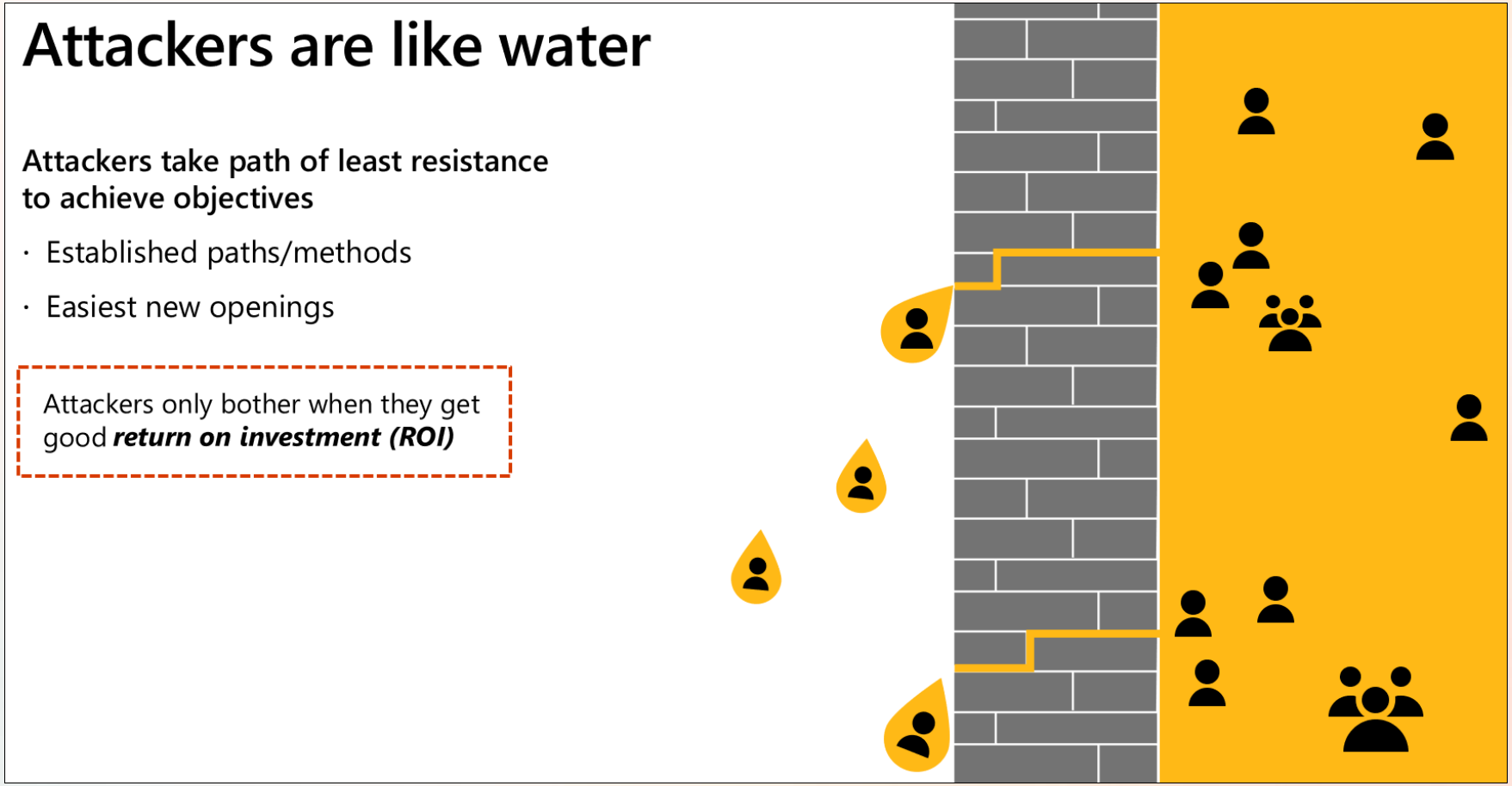
Specialized Security

Used for highly privileged access with restricted attack surface

Enterprise Security

Baseline security for corporate assets & starting point for security

Attackers are like water



PAW Design principles

Restricted Internet access
Locked down internet access to allow-listed domains for management purposes

Locked down environment
Increased levels of policy-based restrictions within the operating system

Allow-listed application control
Limited set of approved and signed applications reduces security risks and attack vectors

Always-on VPN
Allows for secured and managed access to highly sensitive management zones to serve customer environments

Highly restricted and secure
Adopts industry standards of hardened operating system security policies

Provisioning
Strict provisioning performed by personnel in restricted areas ensures procedural compliance

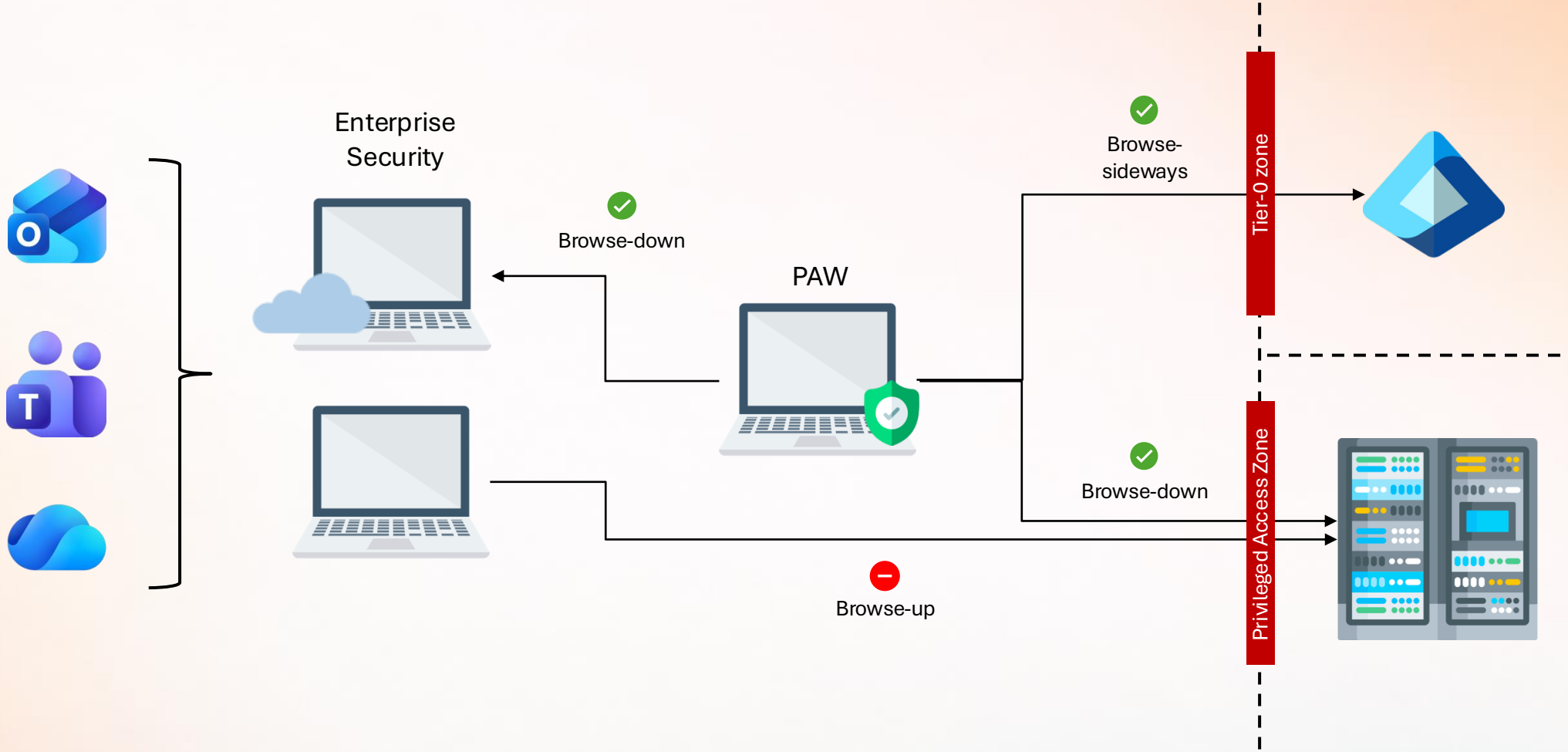
Hardware Procurement
Dedicated vendor SKU ensures hardware specific requirements and supply chain security

User authentication
Dedicated user account for device sign-in and network connectivity authorization

Device Compliance
Device compliance evaluation using Microsoft Intune

Update management
Leverage smaller, incremental updates with higher release cadence to ensure client platform is up-to-date and secure

Browse-down, Sideways and Browse-Up



Why an Isolated Entra ID Tenant is the Right Choice for Tier-0 Privileged Access

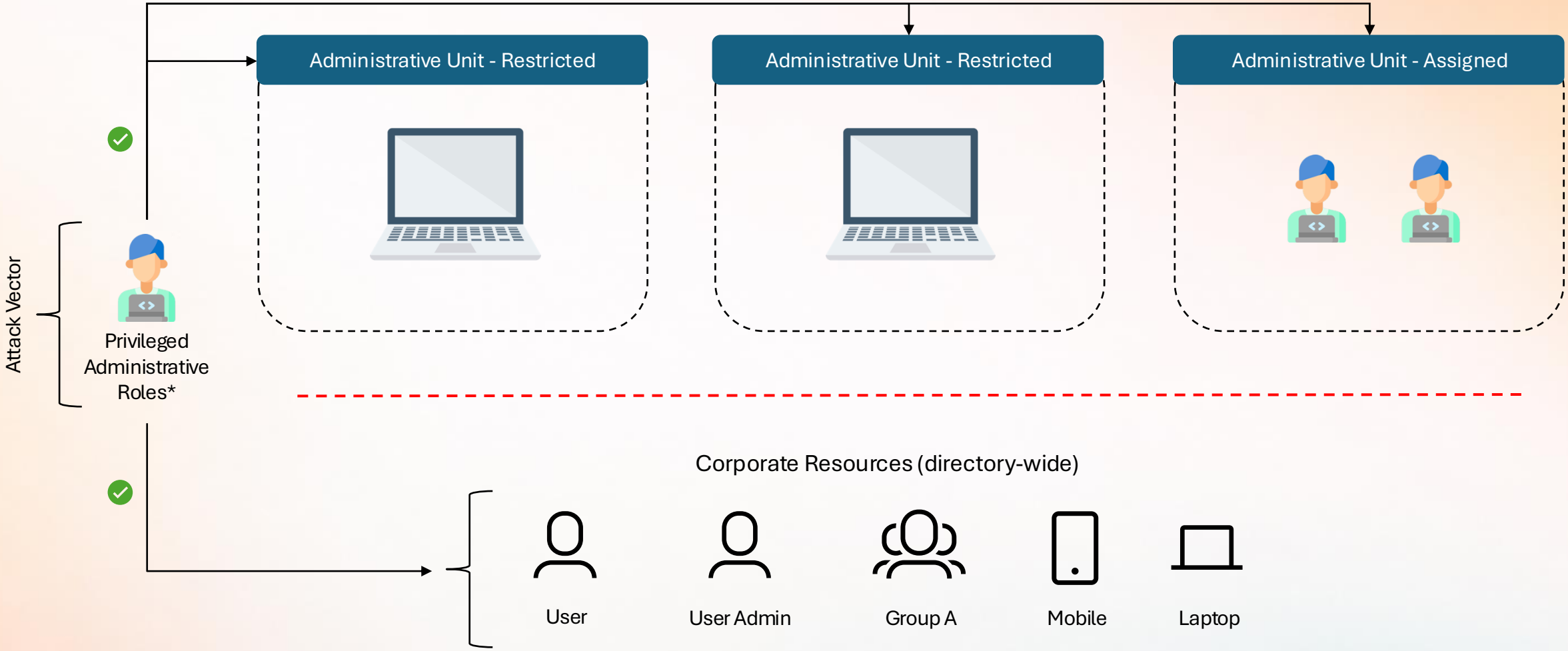
Limitations of Administrative Units in Entra ID

- Entra ID has **no Organizational Unit (OU) structure** like Active Directory
  - Administrative Units are **not equivalent** to OUs in functionality or strength
- AUs provide **auditability and friction control only**
  - They are **not** an impenetrable security boundary
- When used as the **sole** protection layer for privileged accounts in a PAW design:
  - A single Global Admin / Privileged Role Admin (GA/PRA) credential compromise is enough to:
  - Remove the privileged account from the restricted AU (**stripping all protection**)
  - Modify the account freely (reset password, change MFA methods, etc.)

Dedicated “Privileged Access” Entra ID Tenant

- **Robust Isolation**
  - Completely isolates company-managed PAWs from corporate identities and trust boundaries
  - Secures Tier-0 management zones and customer infrastructure access
  - Simplifies Conditional Access policy deployment
- **Stronger Compliance & Auditability**
  - Ensures TSA compliance for PAW connections to destination networks via specialized management zones
  - Delivers clear, unambiguous compliance evidence for PAW-to-access platform connections (CoP 5.2.11)
  - Provides the level of isolation and auditability that Administrative Units **cannot** achieve

Administrative Units may sound like a great idea, but does it meet the requirements in all scenarios?

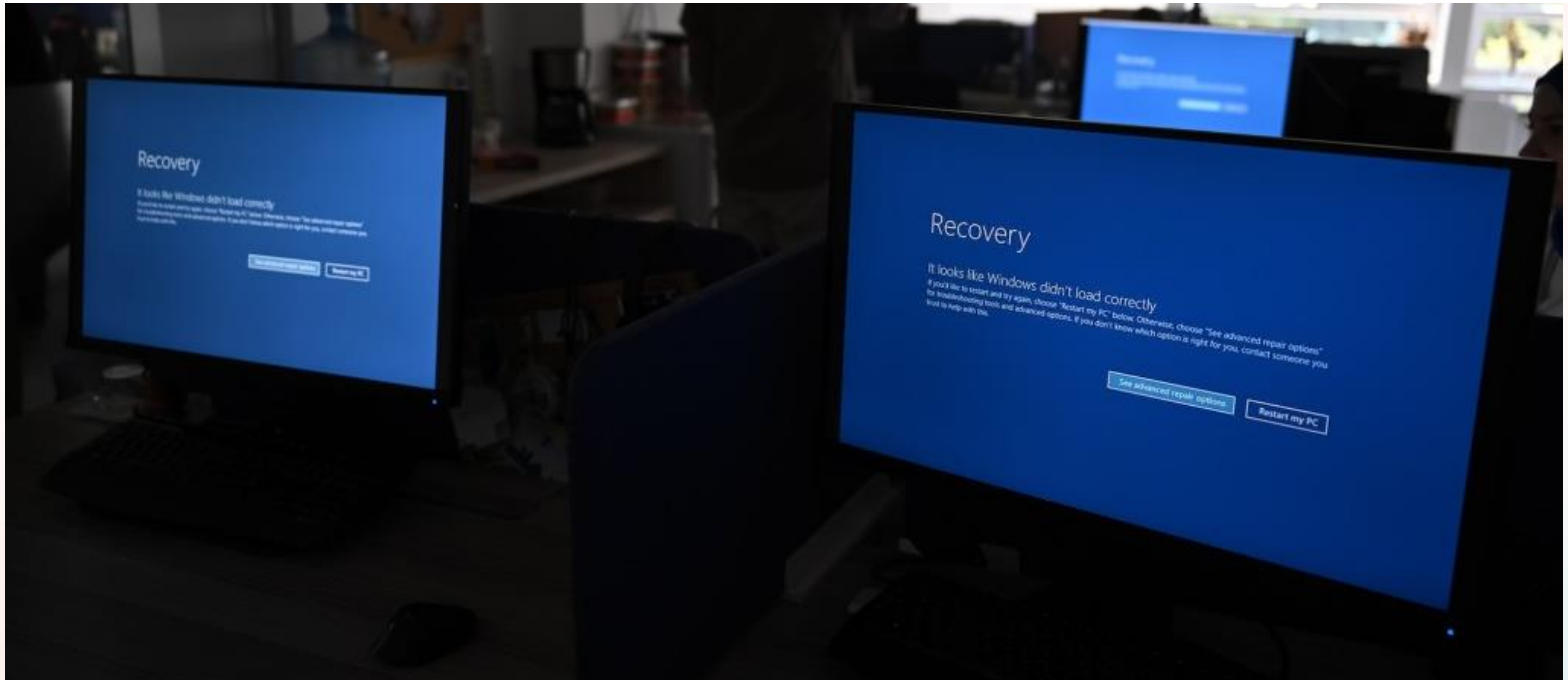


*) Global Administrators and Privileged Role Administrators

Importance of protecting highly privileged accounts

The US-based medical device manufacturer, **Stryker**, recently made headlines around the world in relation to a cybersecurity incident they suffered. As a short recap of the key facts:

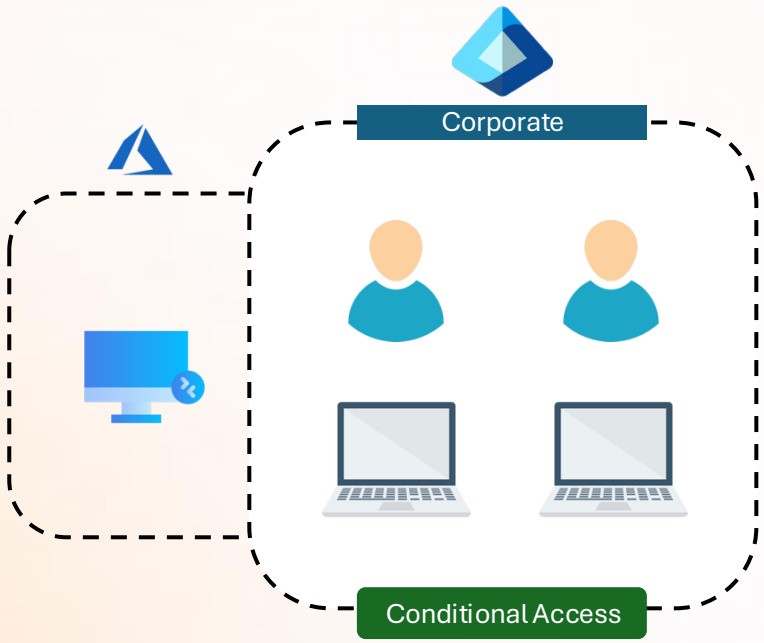
- On March 11, 2026, Stryker was reportedly breached by an Iran-linked hacktivist group, Handala.
- Handala purportedly breached a Global Administrator account in the Stryker Microsoft 365 (**M365**) IT environment and proceeded to wipe 200k+ Stryker devices!
- This resulted in global outage across internal systems and also affected medical devices across the global.



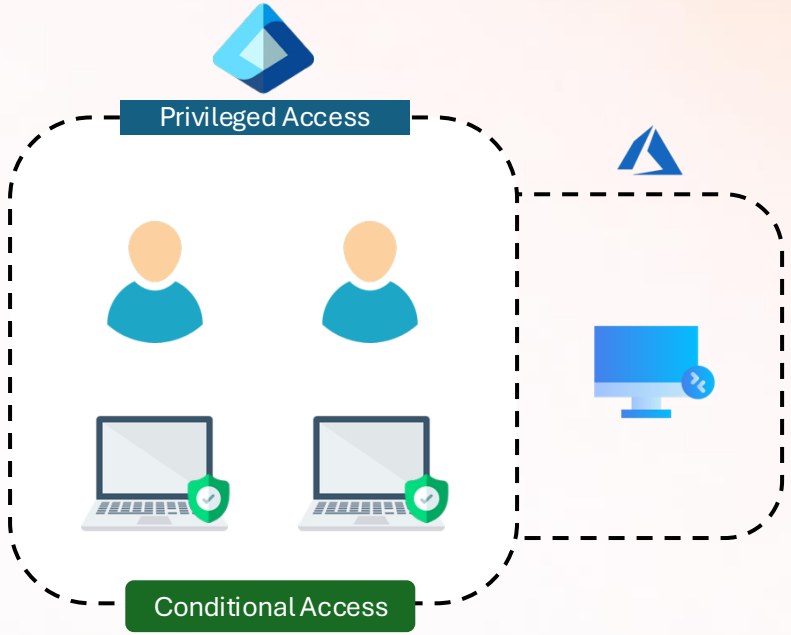
Demo

Administrative Units

High-level overview using tenant isolation



Tenant boundary



Corporate environments usually have years of investments into configuration, management planes

Privileged Access tenant reduces the attack vector with minimal privileged accounts necessary, a PAW is required for management tasks and security keys are enforced for authentication

Supply chain security

Manufacturing and transport, following a clean source principle

Manufacturing and supply chain security with trusted components

Components assembled into finished units. Verified integrity with **Virtualization Based BIOS Protection** activation, using hypervisor tech to isolate and validate boot processes against tampering

Manufacturing process embeds robust hardware-backed protections to combat threats like tampering and grey-market infiltration and spotlights early-stage defenses against physical intrusions, malicious implants, and counterfeit parts, ensuring seamless integrity from factory assembly to end-user delivery

Delivery through air and with ground transportation to provisioning centers

Parcel inspection & firmware tamper protection verification

Office

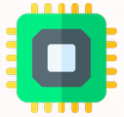
Parcel inspection & firmware tamper protection verification

Office

Secure parcel delivery from hardware factory

Video surveillance of individuals entering the restricted area including special keycard access

Ocular seal inspection of delivered parcels with hardware performed by authorized personnel



Firmware logs inspection prevents hardware-based tamper protection and supply-chain attacks

Device certificate verification and device provisioning and decommissioning activities

Authorized personnel

Unauthorized personnel

Tamper protection

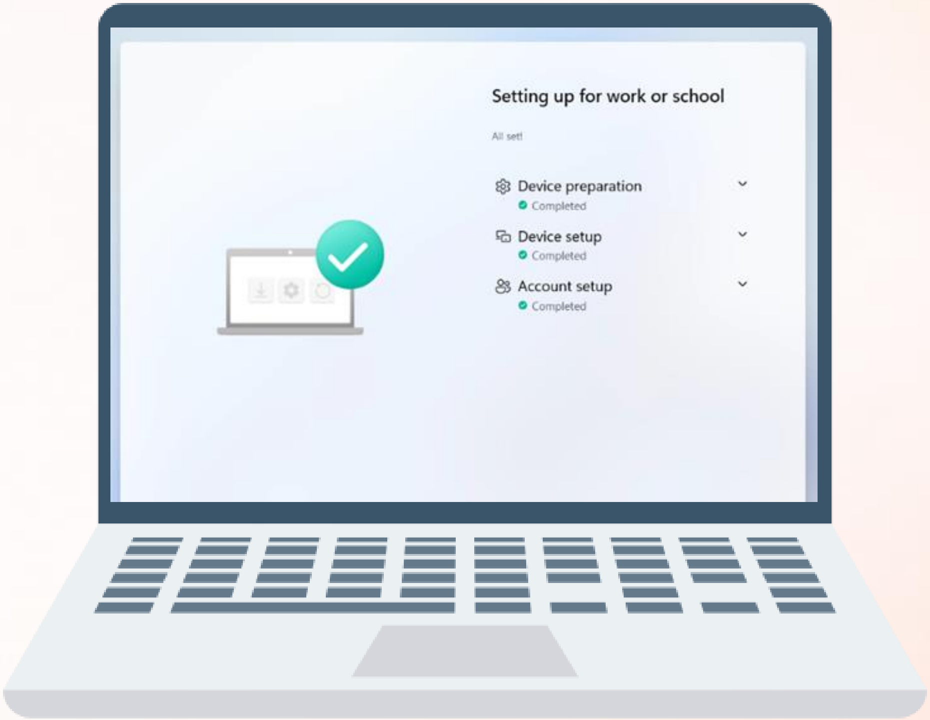
Programmatically verify device integrity

Provision & manage devices

Autopilot pre-provisioning enables technician and end user phases

Provisioning – Technician flow

Authorized technician uses a PAW device with specialized access and software available to initiate provisioning of new devices



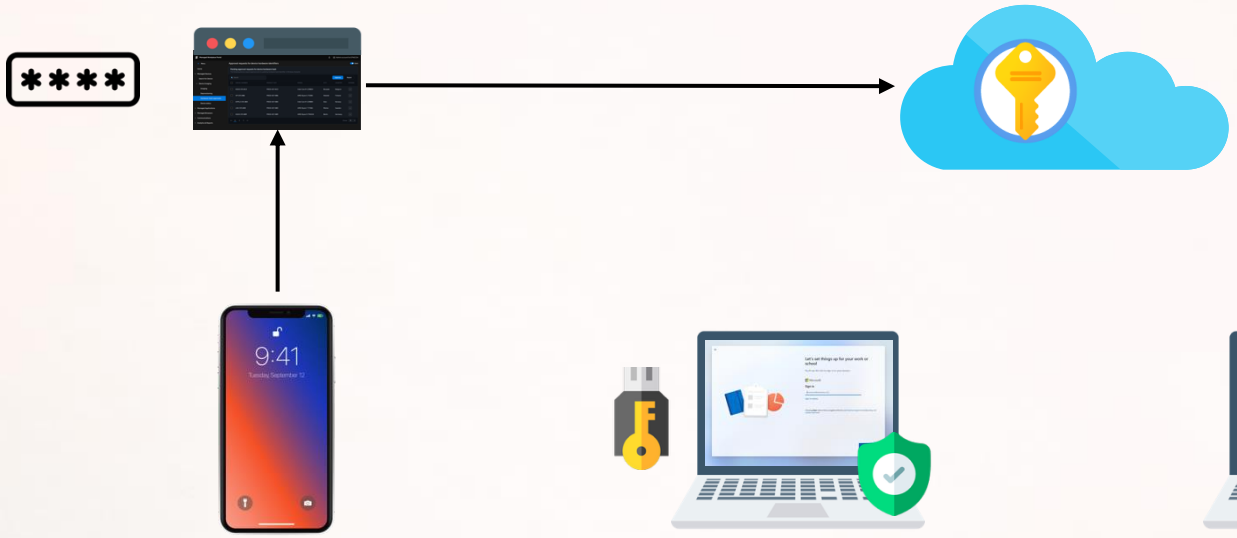
After device is successfully imaged, provisioning through USB is initialized, and all security hardening and configuration is applied

Unmanaged devices are initiated for Autopilot pre-provisioning using boot into specialized provisioning software running Windows PE, establishing a provisioning session that must be authorized by the technician – ensuring two step verification

Demo

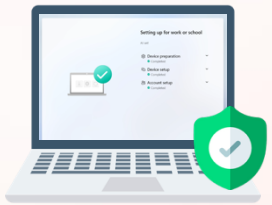
Custom hardware key pre-registration

Provisioning – User flow



User retrieves security key PIN from portal using TAP sent to corporate email during security key provisioning

User opts to sign-in using security key, during device registration and enrollment



User-provisioning phase completes with any remaining policies to be applied or app updates

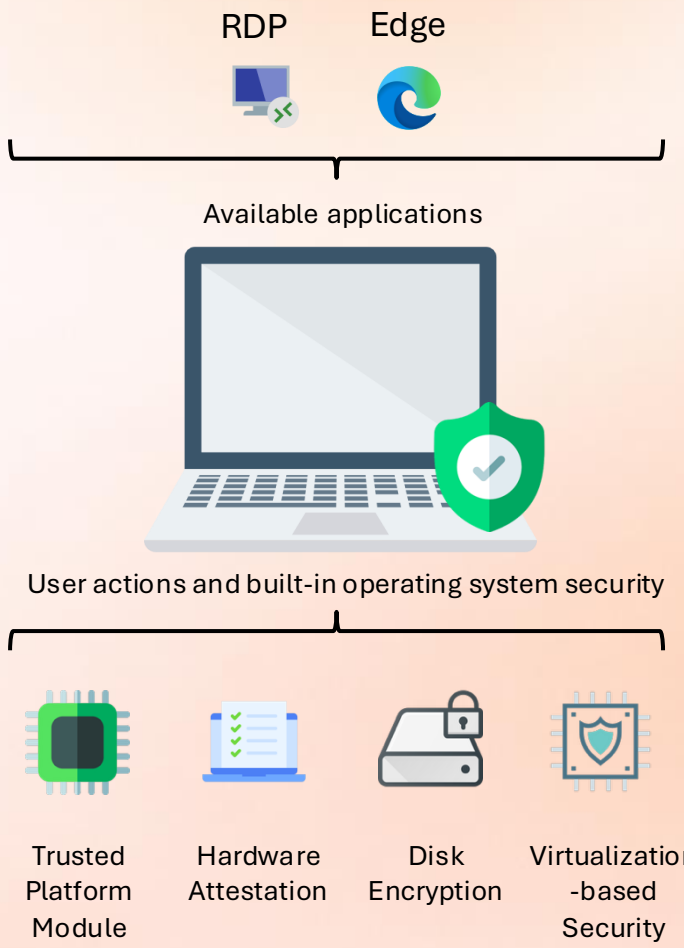
Device registration and enrollment completes; Privileged Access Workstation is provisioned and ready to use

Hardening policies

What is in the box? App Control for Business, Security Baselines, restricting internet access etc.

Operating system security aspects

- **Secure Boot & Trusted Platform Module (TPM)**
  - Secure Boot ensures only trusted firmware and OS load, verified by TPM, a hardware chip that stores cryptographic keys for secure attestation and encryption
- **BitLocker Disk Encryption**
  - Protects data at rest by encrypting the entire disk, requiring TPM or a key for access
- **Hardware Attestation**
  - Verifies device compliance with security policies through TPM-backed cryptographic proof, ensuring only trusted devices access privileged zones
- **No Local Admin Rights**
  - Restricts user privileges to prevent unauthorized system changes
- **Virtualization-Based Security (VBS)**
  - Isolates critical security processes in a virtualized environment, protecting against kernel-level attacks
- **Available Applications**
  - Strictly limited to pre-approved, essential tools required for privileged tasks, reducing attack surface
- **Firewall configurations**
  - Inbound and outbound restricted policy, allowing only connectivity towards SASE solutions



Remote OTA capabilities

- OEM proprietary hardware built-in features using global cellular and GPS technology provides highly accurate location information and continues to function even if the PC is turned off
- **Find:**
  - Locate and obtains position of a Privileged Access Workstation in real-time
- **Lock:**
  - Disable a Privileged Access Workstation to prevent unwanted access in case a device is lost or stolen
- **Erase:**
  - Wipe the primary hard drive of a Privileged Access Workstation if it's lost or stolen

Security baseline configuration

- CIS Windows 11 Intune v4.0.0
  - Easily import .json files directly to Settings Catalog policies
  - Document deviations from the framework (not everything is applicable)

Demo

Security Baseline recommendations

App Control for Business - Microsoft trust templates (Allow)

- Start with a Microsoft provided template:
  - Default Windows Mode
    - Trust the OS
    - DefaultWindows_*.xml
  - Allow Microsoft Mode
    - Trust Microsoft
    - AllowMicrosoft.xml
  - Signed & Reputable Mode
    - 3rd-party software via Microsoft Defender ISG

Example Base Policy	Description	Where it can be found
DefaultWindows_*.xml	This example policy is available in both audit and enforced mode. It includes rules to allow Windows, third-party hardware and software kernel drivers, and Windows Store apps. Used as the basis for the Microsoft Intune product family policies.	%OSDrive%\Windows\sche %ProgramFiles%\Windows\
AllowMicrosoft.xml	This example policy includes the rules from DefaultWindows and adds rules to trust apps signed by the Microsoft product root certificate.	%OSDrive%\Windows\sche %ProgramFiles%\Windows\
AllowAll.xml	This example policy is useful when creating a blocklist. All block policies should include rules allowing all other code to run and then add the DENY rules for your organization's needs.	%OSDrive%\Windows\sche

App Control for Business

Application Control in the Real World: Deep Dive into Structure, Signing, and Deployment

Friday April 24, 2026 13:45 - 14:45 CEST

Louis Armand 1

Application Control for Business (ACfB) is one of the most powerful security layers in Windows, but implementing it at scale is far from trivial. In this deep dive, we'll go beyond the basics and dissect the ACfB policy structure, explore common pitfalls (think app GUID mismatches, XML syntax quirks, and supplemental policy chaos), and uncover why the "simple" act of signing your policies can completely derail your deployment strategy.

We'll walk through the end-to-end signing process, with special focus on Azure Trusted Signing Services, how it works, what to trust, and how to integrate it into automated pipelines without breaking your rollout. All of this will be framed in the context of Privileged Access Workstations (PAWs), but the principles apply equally to broader enterprise scenarios. We'll also show how to scale up or peel back security layers for less restrictive environments while maintaining operational efficiency.
Expect real-world lessons, live demos, and battle-tested best practices that will help you avoid costly mistakes and build a robust ACfB implementation strategy.

Make sure your expectations meet your requirements – ask yourself these questions

- **What are you securing?**
  - Scope: Which privileged tiers/roles are in scope, Tier 0 / Domain Admins / Enterprise Admins, cloud global admins, specific high-value assets like domain controllers, Entra ID Connect servers, or crown-jewel applications?
- **Are you bound to any legislative requirements?**
  - Compliance: GDPR, HIPAA, PCI-DSS, SOX, NIS2, DORA, or sector-specific rules that mandate privileged access controls, auditing, or separation of duties?
- **What is your current threat model and privileged access risk?**
  - Realistic risks: credential theft, pass-the-hash, lateral movement, supply-chain attacks, insider threats, or nation-state persistence?
- **Who will use the PAW and what specific tasks will they perform?**
  - Number of users, daily workflows, and whether they need simultaneous access to regular productivity tools
- **Will you use dedicated physical hardware, virtual machines, or cloud-based PAWs?**
  - Hardware vs. virtual/cloud decision drives isolation, performance, and cost

Wrapping things up

Is Intune ready to fully support managing a PAW?

Final demo

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

robopack

numecent

Microsoft

eido

Rimo3

Please rate this session on Sched.com

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

Thanks!