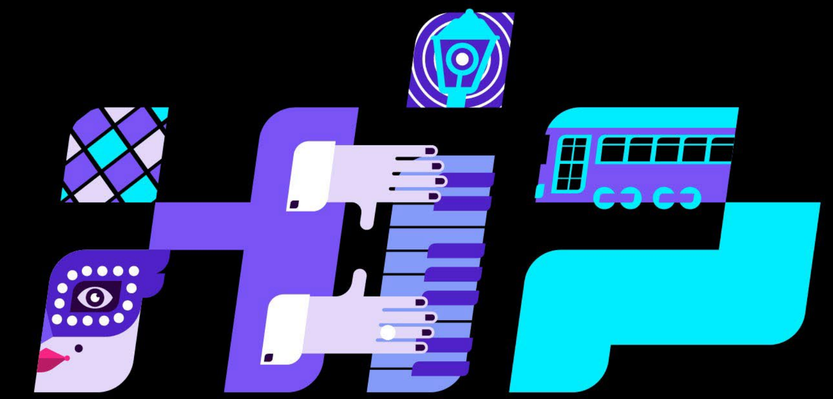
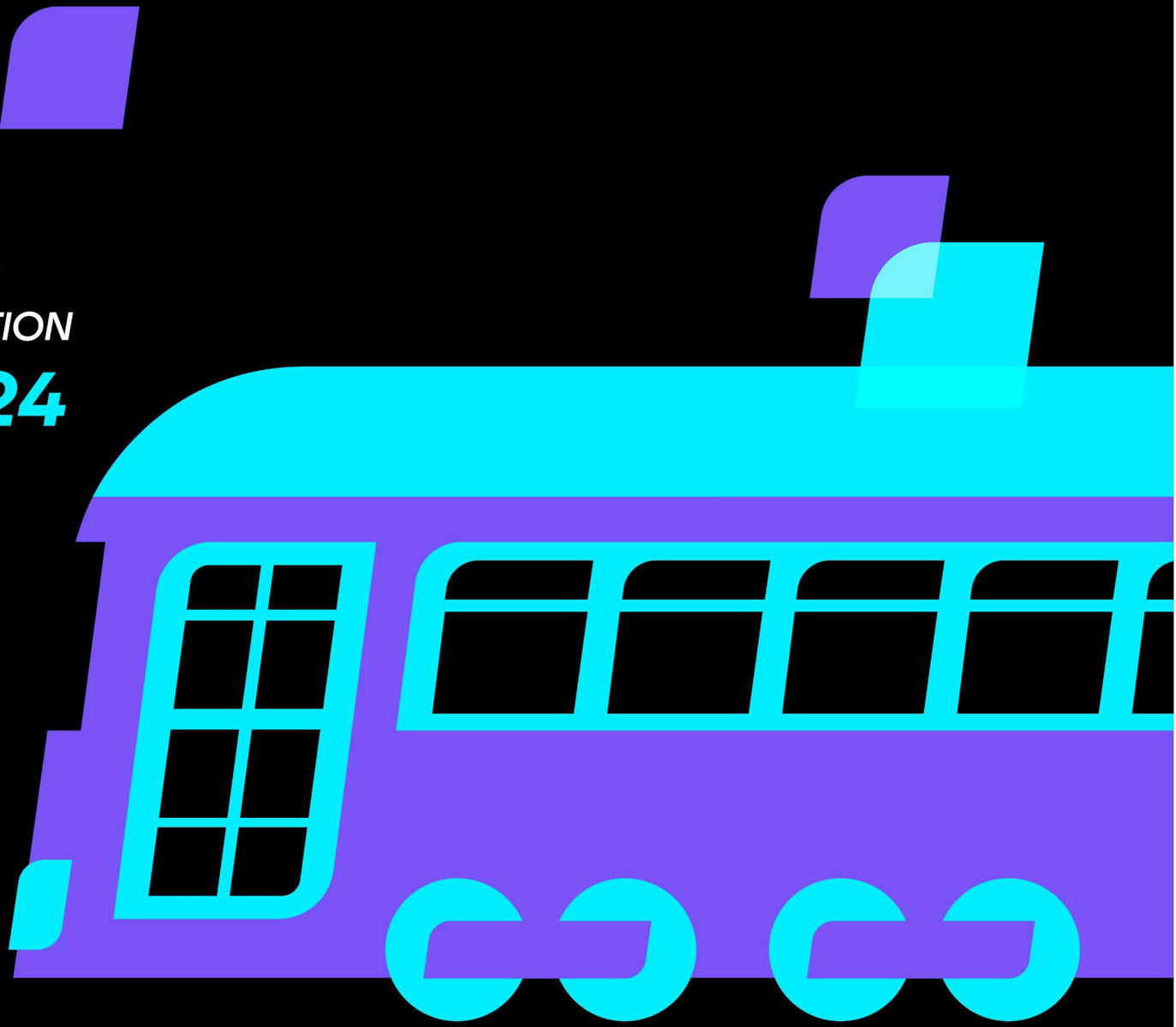


HYBRID
IDENTITY
PROTECTION

conf24

NEW ORLEANS



Protecting the Keyboard: Ingredients of a Successful PAW Program

Brian Desmond

Ravenswood Technology Group, LLC

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

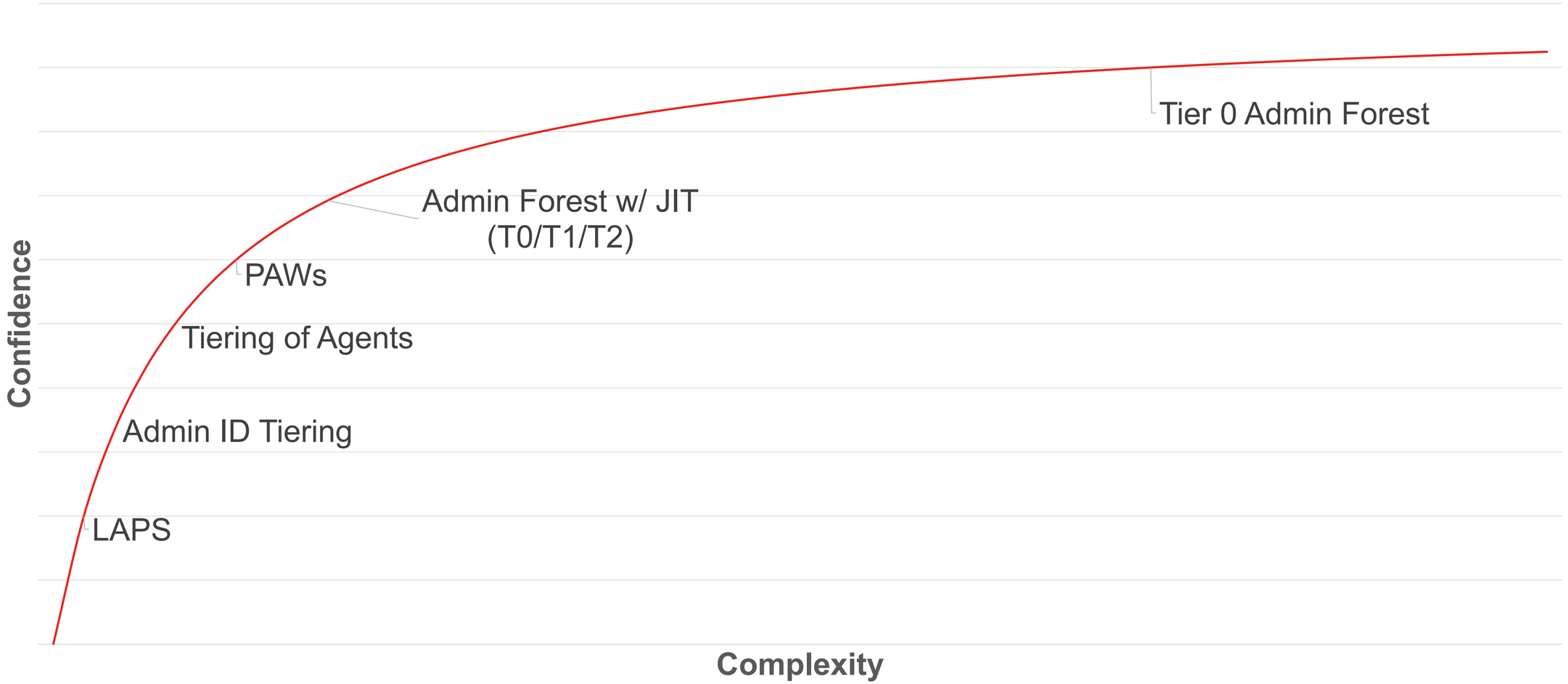
Brian Desmond

Principal, Ravenswood Technology Group, LLC

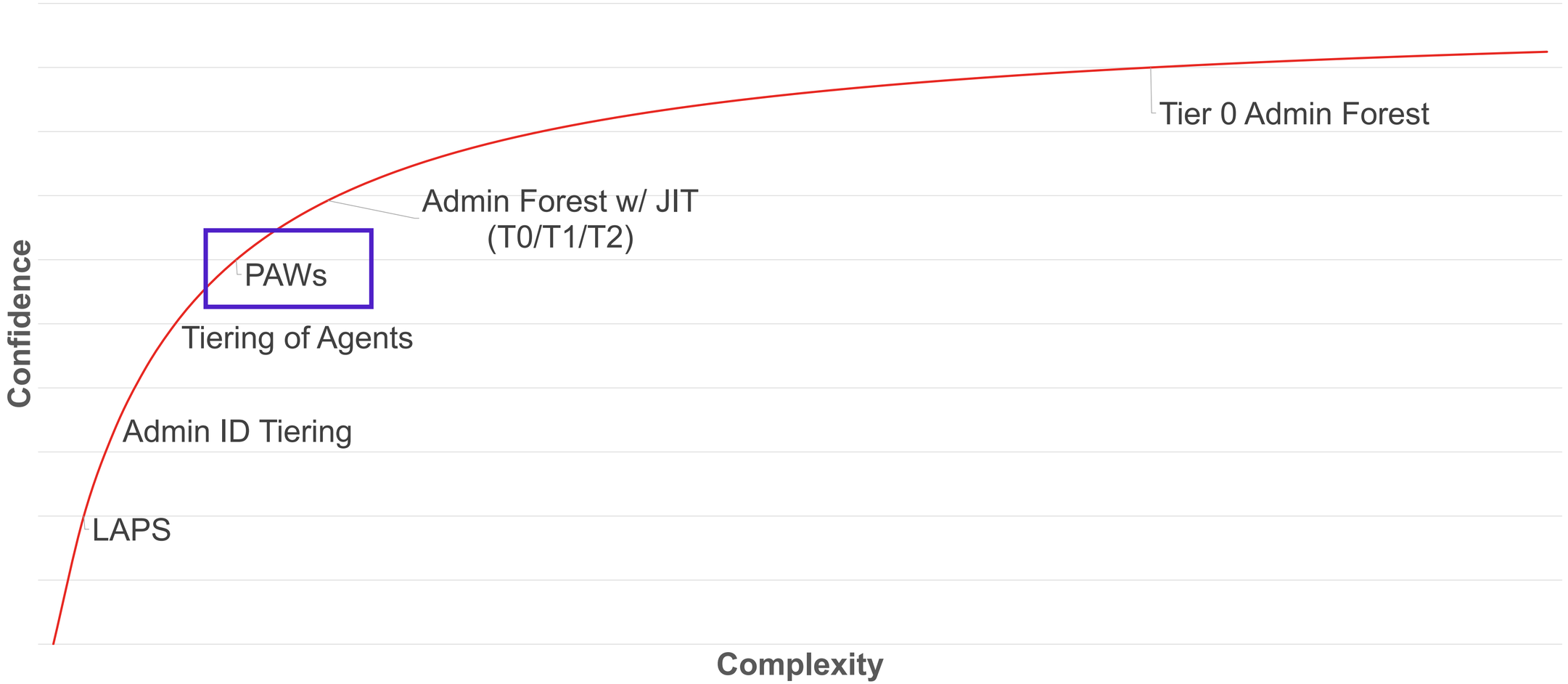
At Ravenswood, Brian helps commercial enterprise and higher education customers solve problems surrounding Active Directory, Identity, Security, and Compliance. Brian was recognized annually as a Microsoft MVP for Identity and Access Management for 15 years for his contributions to the Microsoft technical communities at large. Brian is the author of *Active Directory, 5th Edition* published by O'Reilly as well as a frequent contributor to leading industry publications.

bdesmond@ravenswoodtechnology.com www.ravenswoodtechnology.com

Privileged Access Protection: Complexity vs Reward



Privileged Access Protection: Complexity vs Reward



Privileged Access Workstations & JIT Access

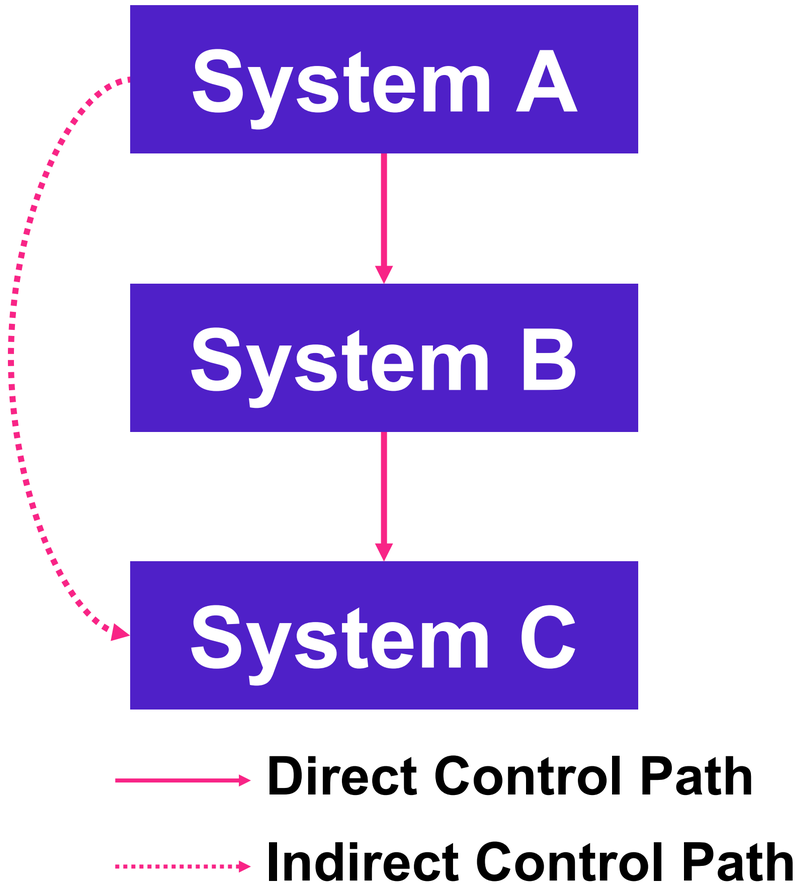
Privileged Access Workstations

- Deliver a known-good, clean keyboard for performing privileged or sensitive tasks
- Isolate sensitive accounts and processes from the risk of a compromised workstation
- Prevent administrators from making poor choices that expose credentials and access

Just-in-Time Access

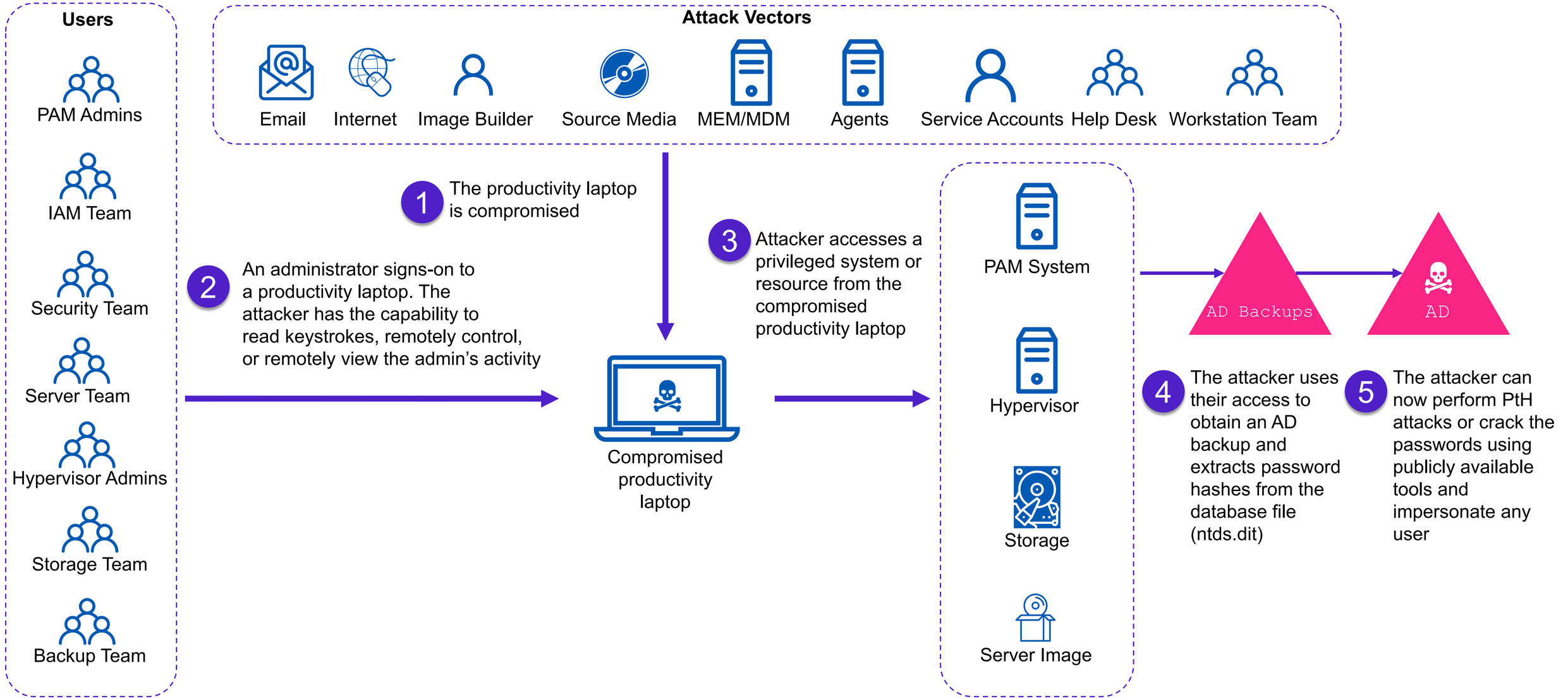
- Eliminate standing privileged access to systems
- Mitigate the risk of persistent credential theft
- Layer intermediate controls on gaining privileged access
- Gain insight on who is *actually* using access and when

Clean Source Principle



- If “System C” is in Tier 0, then all upstream control paths must operate at the same level of assurance
- This extends to agents and management tools
- Clean Source also creates the need for privileged access workstations (PAWs)

Productivity Computer Attack Vectors



Privileged Access Workstation Ingredients

Users are “standard” users, not local admins

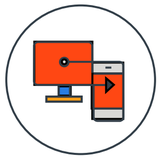
Managed by Tier 0 admins

Internet access is restricted

Conditional Access policies can be used to constrain Azure & Entra roles to a PAW

Apps only deployed using management stack

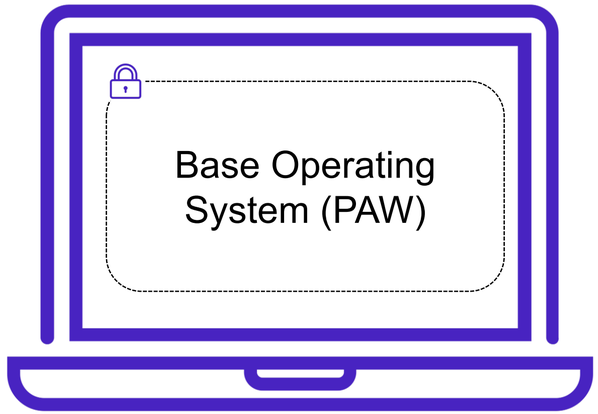
App Control – Enforce kernel mode drivers (user mode is also possible)



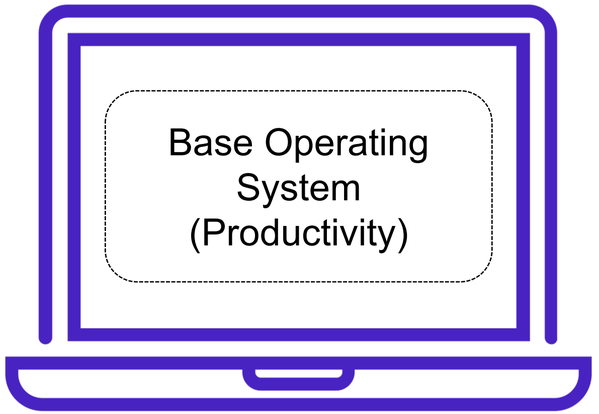
Unnecessary apps are removed

Physical security is important!

Standalone PAW

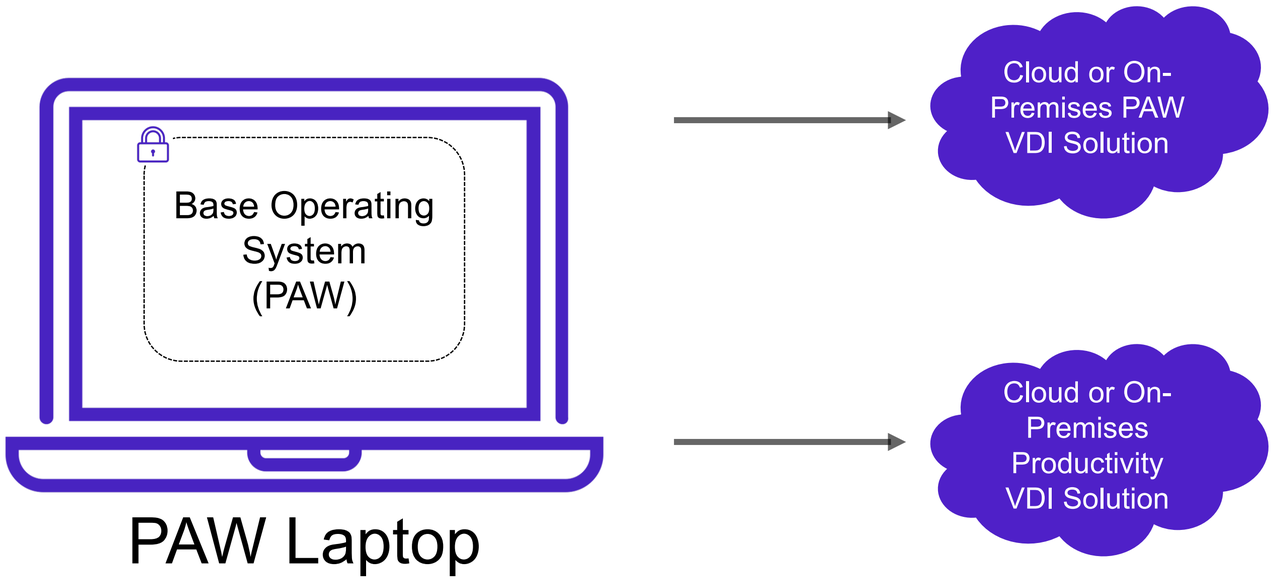


PAW Laptop

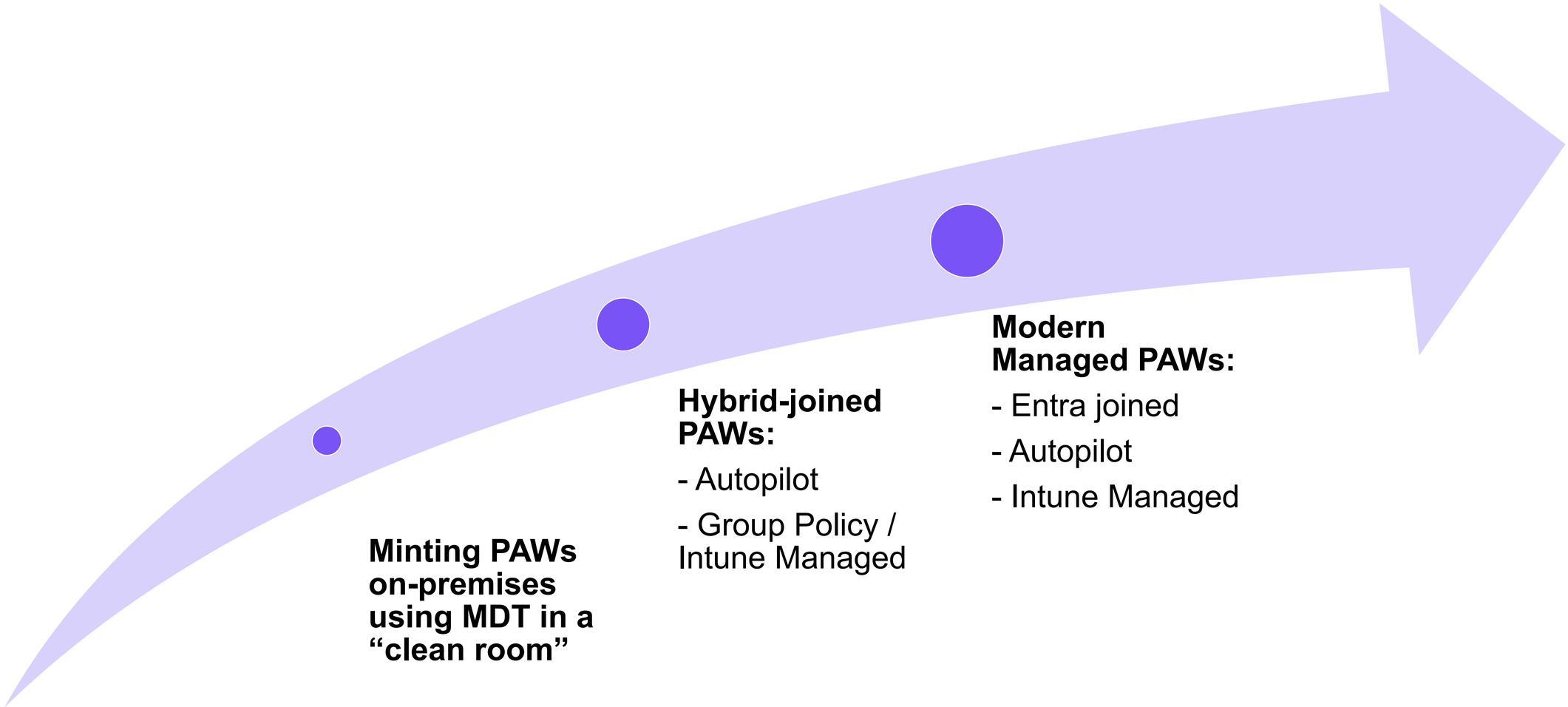


Productivity Laptop

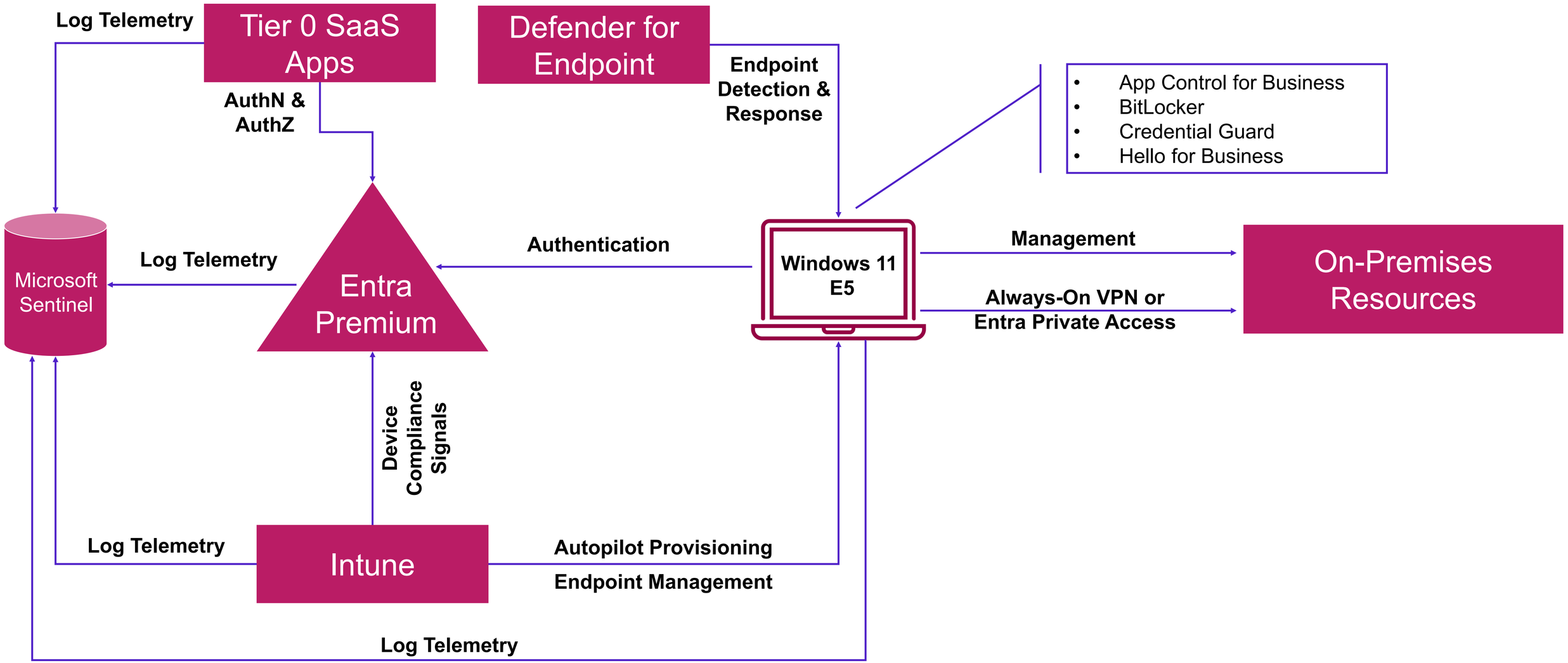
Hardened VDI Client



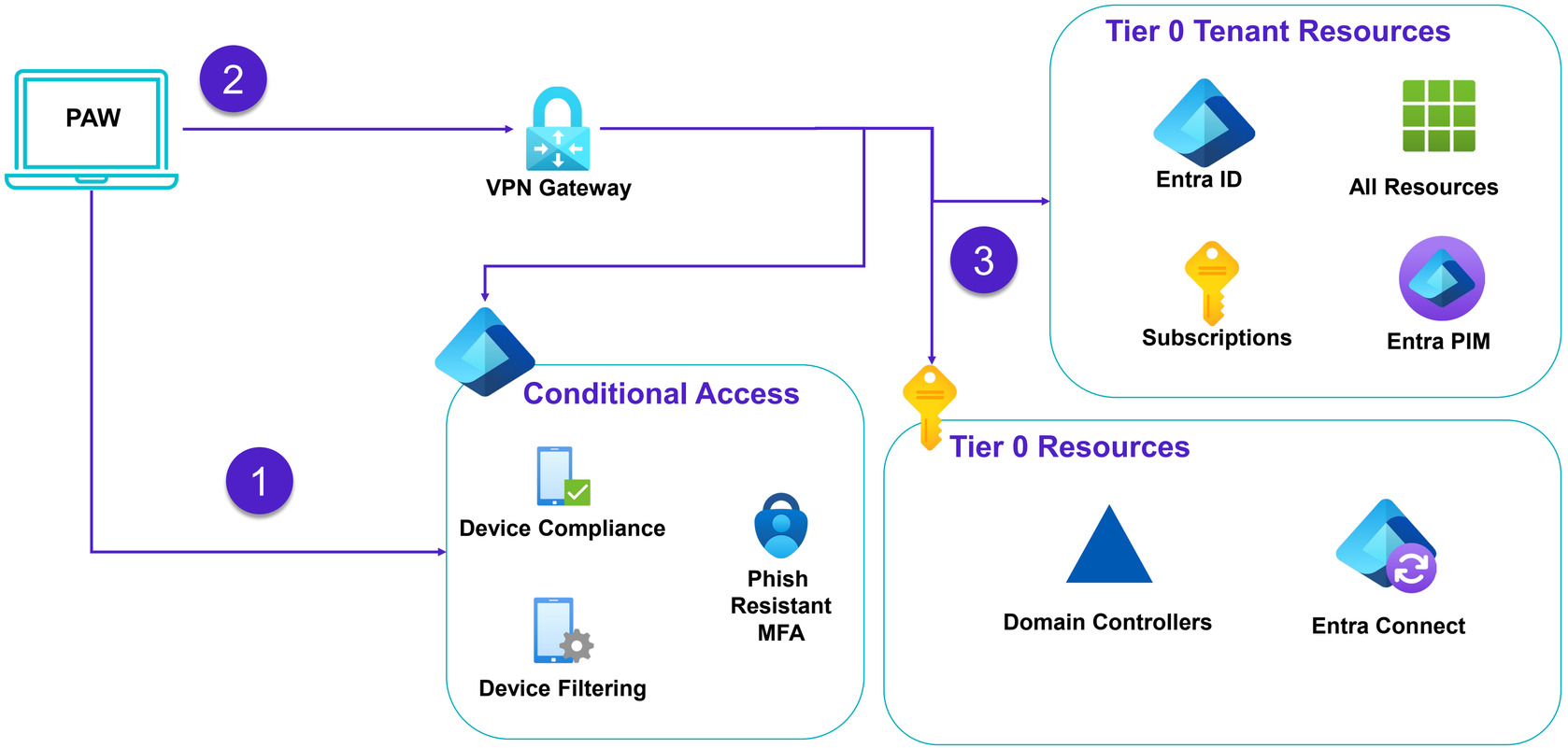
PAW Deployment Evolution



Modern Managed PAW Ecosystem



VPN-Based Networking



Step	Task
1.	User logs on to the PAW using Windows Hello for Business with a FIDO2 key. The PAW connects to Entra ID and is checked against CA policies for device compliance.
2.	If a FIDO2 logon occurred, the PAW connects to VPN
3.	The PAW can then be used to manage Tier 0 resources (Entra Connect, Active Directory, Entra ID, etc.)

Unboxing the PAW Device

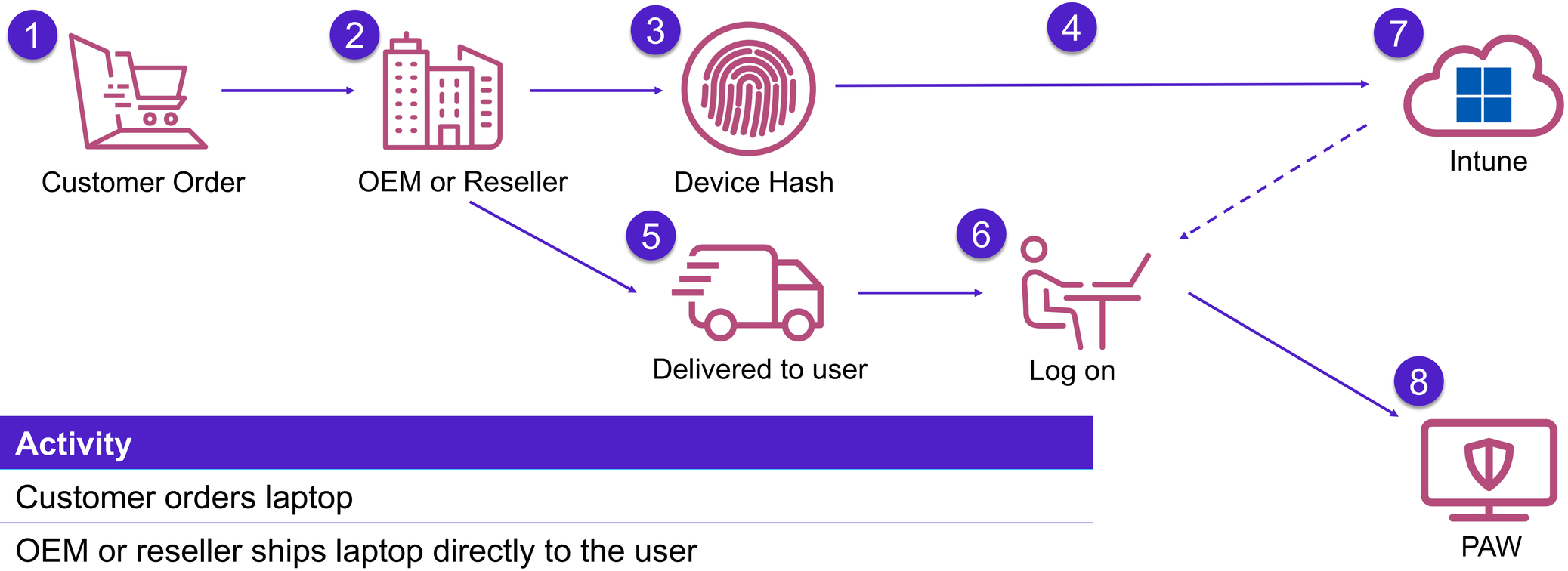
Laptops that ultimately become PAWs are shipped directly to the end user or to a trusted office location

The laptop’s OEM box and outer shipping box and sealing tape is left intact. This helps assure that the device has not been tampered with.

The PAW user sets up their own PAW using Windows Autopilot

PAW users are configured as standard users, not local administrators

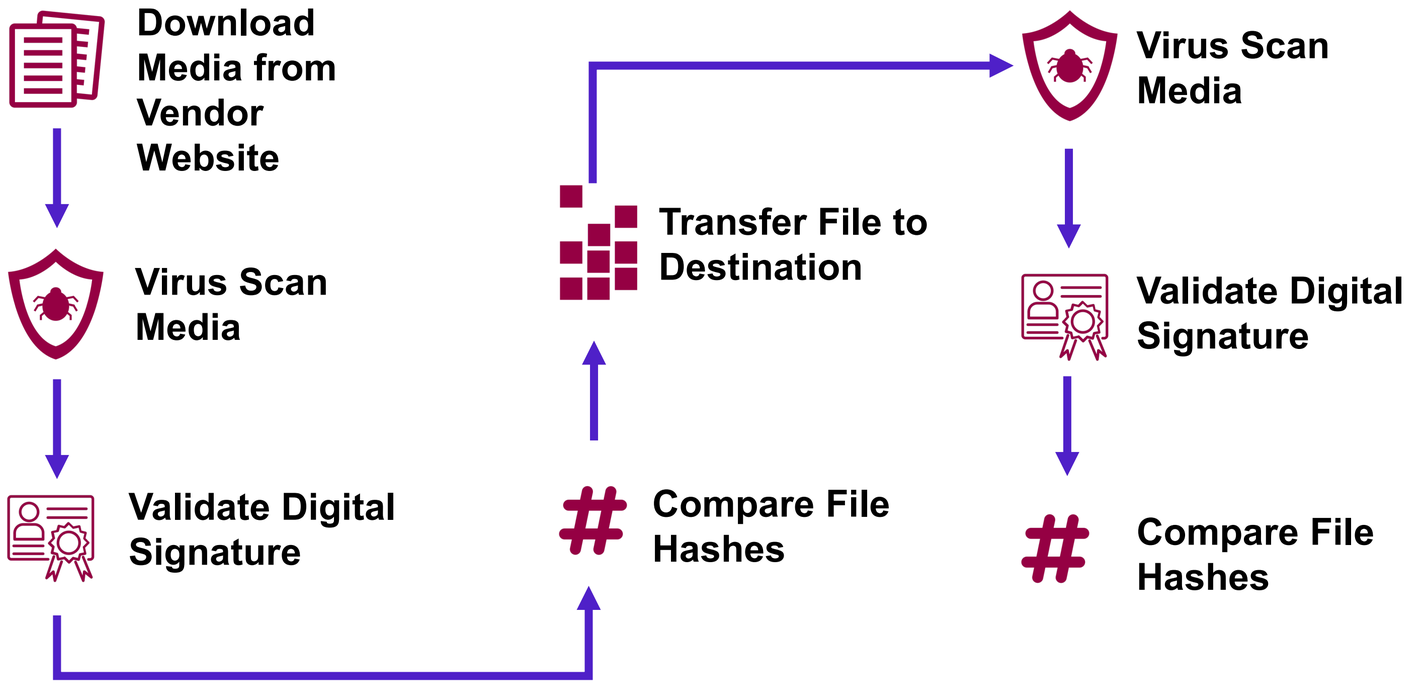
Entra-joined PAW Provisioning Process



Step	Activity
1.	Customer orders laptop
2.	OEM or reseller ships laptop directly to the user
3.	The device hash for the laptop is obtained from the OEM or reseller
4.	The device hash is uploaded to Intune
5.	The laptop is delivered to the admin’s home or office
6.	User logs on to the laptop
7.	Autopilot configures the laptop with the configuration in Intune
8.	The PAW is ready for use

Clean Source Media

Ensuring that the source media (installation files, drivers, operating system, software packages, etc.) is clean is critical. Typically, media must be obtained from a vendor's website and then transferred into the Tier 0 environment.



Validating the File Hash

Vendor supplied file hash

- You should compare the vendor-provided file hash for downloaded files to help ensure that the file has not been tampered with since creation by the vendor
- For example, the file hash provided by Microsoft for the April 2024 Windows Server 2022 ISO file is available in their download site:

Released: 4/16/2024

SHA256: 7F41D603224E8A0BF34BA957D3ABF0A02437AB75000DD758B5CE3F050963E91F

File name: en-us_windows_server_2022_updated_april_2024_x64_dvd_164349f3.iso

Check the file hash

- Download the file and run “Get-FileHash,” supplying the following parameters
  - -Path (the path to the file in which to obtain the file hash
  - -Algorithm (the algorithm to use)

Example command:

```
Get-FileHash -Path "C:\Temp\en-us_windows_server_2022_updated_april_2024_x64_dvd_164349f3.iso" -Algorithm SHA256
```

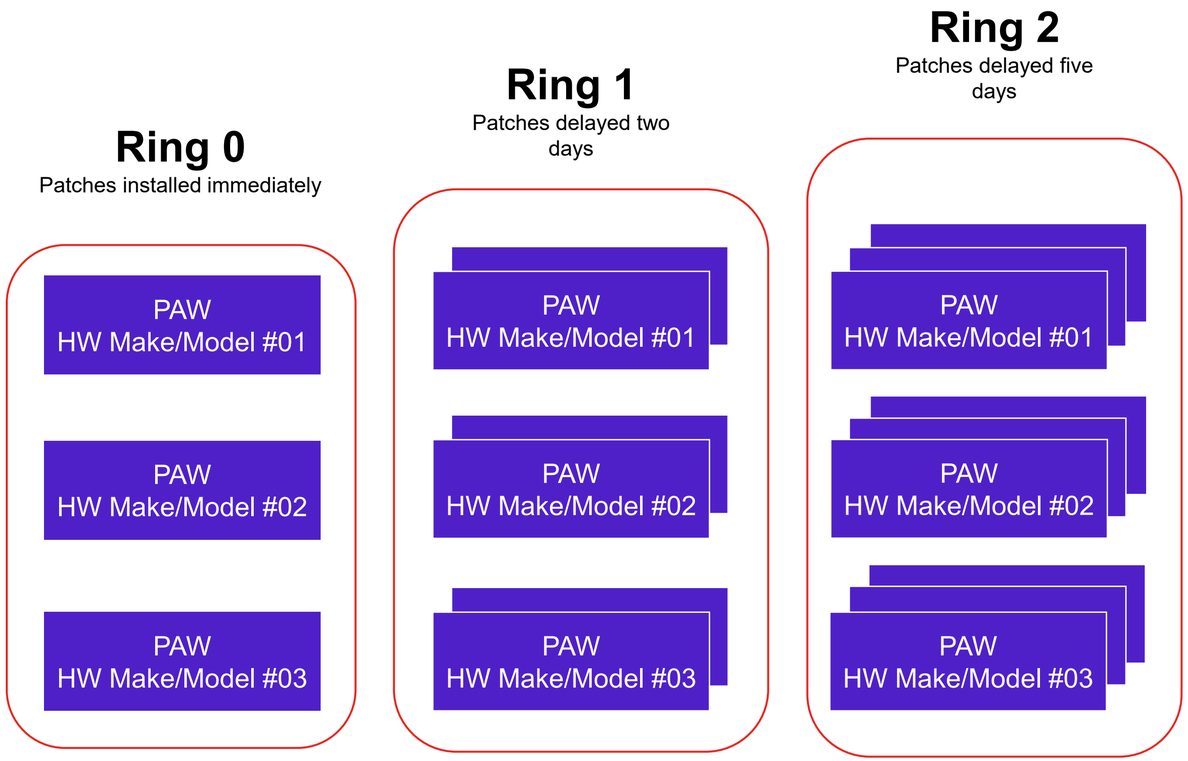
Result:

```
PS C:\Temp> Get-FileHash -Path "C:\Temp\en-us_windows_server_2022_updated_april_2024_x64_dvd_164349f3.iso" -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          7F41D603224E8A0BF34BA957D3ABF0A02437AB75000DD758B5CE3F050963E91F       C:\Temp\en-us_windows_server_2022_upd
```

Patch Management

- PAW patching is performed using Windows Update for Business
- The PAWs are separated into three patch rings
- Patch rings are configured within Microsoft Intune; each with different delay periods. This gives administrators a chance to address issues prior to all PAWs being affected by an update.



Removing Extra Stuff

Windows 11 comes with various preinstalled apps that are not necessary for a PAW. Removing unnecessary apps reduces the attack surface.

- ❑ WindowsMaps
- ❑ Clipchamp
- ❑ 549981C3F5F10
- ❑ BingNews
- ❑ BingWeather
- ❑ GamingApp
- ❑ GetHelp
- ❑ Getstarted
- ❑ MicrosoftOfficeHub
- ❑ MicrosoftSolitaireCollection
- ❑ MicrosoftStickyNotes
- ❑ OneDriveSync
- ❑ Paint
- ❑ People
- ❑ PowerAutomateDesktop
- ❑ Todos
- ❑ Windows.Photos
- ❑ WindowsCalculator
- ❑ WindowsCamera
- ❑ Windowscommunicationsapps
- ❑ WindowsFeedbackHub
- ❑ WindowsSoundRecorder
- ❑ WindowsStore
- ❑ WindowsTerminal
- ❑ Xbox.TCUI
- ❑ XboxApp
- ❑ XboxGameCallableUI
- ❑ XboxGameOverlay
- ❑ XboxGamingOverlay
- ❑ XboxIdentityProvider
- ❑ XboxSpeechToTextOverlay
- ❑ YourPhone
- ❑ ZuneMusic
- ❑ ZuneVideo
- ❑ QuickAssist
- ❑ Windows365
- ❑ MicrosoftFamily
- ❑ MicrosoftTeams
- ❑ MSTeams
- ❑ Copilot
- ❑ WindowsAlarms
- ❑ OneConnect

App and Binary Whitelisting

- Multiple past Windows components have consolidated into App Control
- Whitelist user-mode and/or kernel-mode binaries and scripts
- Combine app control manifest with code signing to make policies highly tamper-resistant
- Testing and release management processes become especially important as you deploy App Control

Network / Internet Isolation

- Your PAWs should not be used to browse the Internet
- Cloud management portals negate this fundamental assumption
- Block by default and whitelist approved destinations
  - Proxy PAC file
  - Entra Global Secure Access
  - SASE Solutions like Z-Scaler
- Think about how you will connect PAWs to on-premises networks
  - VPN
  - Entra Private Access
  - SASE Solutions
  - Virtual Desktop Infrastructure

Support and File Sharing

Microsoft Teams is used to collaborate within Tier 0 and in limited (and restricted) cases, with the non-Tier 0 environment. It is installed on the PAWs and used for screen sharing, chat, and file transfer.

Screen sharing

Screen sharing can aid in the resolution of issues by allowing team members to quickly convey the configuration and symptoms being experienced

Chat

Text and screen captures sometimes need to be shared with support personnel for troubleshooting and for documentation purposes

File Transfer

Application installation files, agents, infrastructure code, and log files need to be transferred into and out of the Tier 0 environment

Wrap-Up

- PAWs are a critical component for safely managing critical infrastructure
- Your PAW architecture needs to respect clean source to be an effective control
- Managing a PAW deployment often creates requirements for a new set of skills in an identity / security team

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Questions?