

TEC

**The Experts
Conference**

SPONSORED BY  Quest

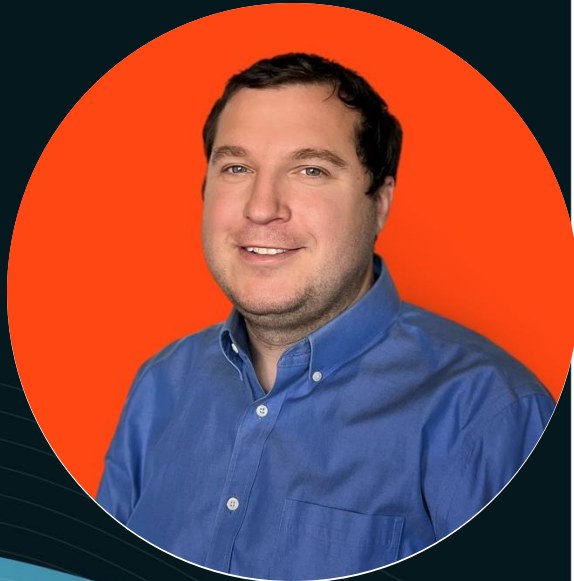
Protecting the Keyboard: Ingredients of a Successful PAW Program

Brian Desmond



TEC

The Experts
Conference
Sponsored by Quest®



About Brian

Brian is a Principal at Ravenswood Technology Group. At Ravenswood, Brian helps commercial enterprise and higher education customers solve problems surrounding Enterprise Mobility, Active Directory, Identity Management, and Office 365. 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. You can often find Brian speaking at conferences and events worldwide.

bdesmond@ravenswoodtechnology.com
www.ravenswoodtechnology.com



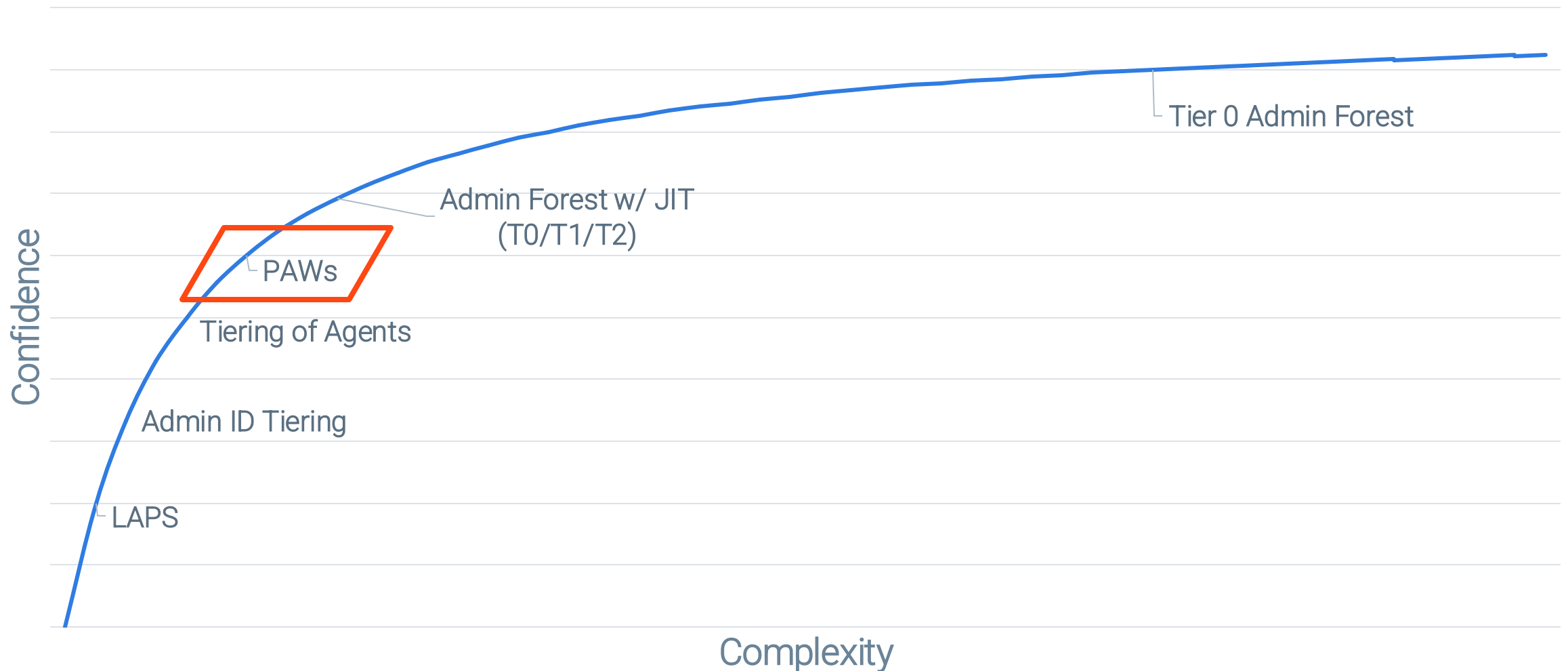
AGENDA

 What is a Privileged Access Workstation (PAW)?

 What Goes Into a PAW?

 What Implementation Looks Like

PRIVILEGED ACCESS PROTECTION: COMPLEXITY VS REWARD



CREDENTIAL THEFT IS A GROWING THREAT

Identity and network access is the foundation of modern cybersecurity, with **66% of attacks involving compromised identities**

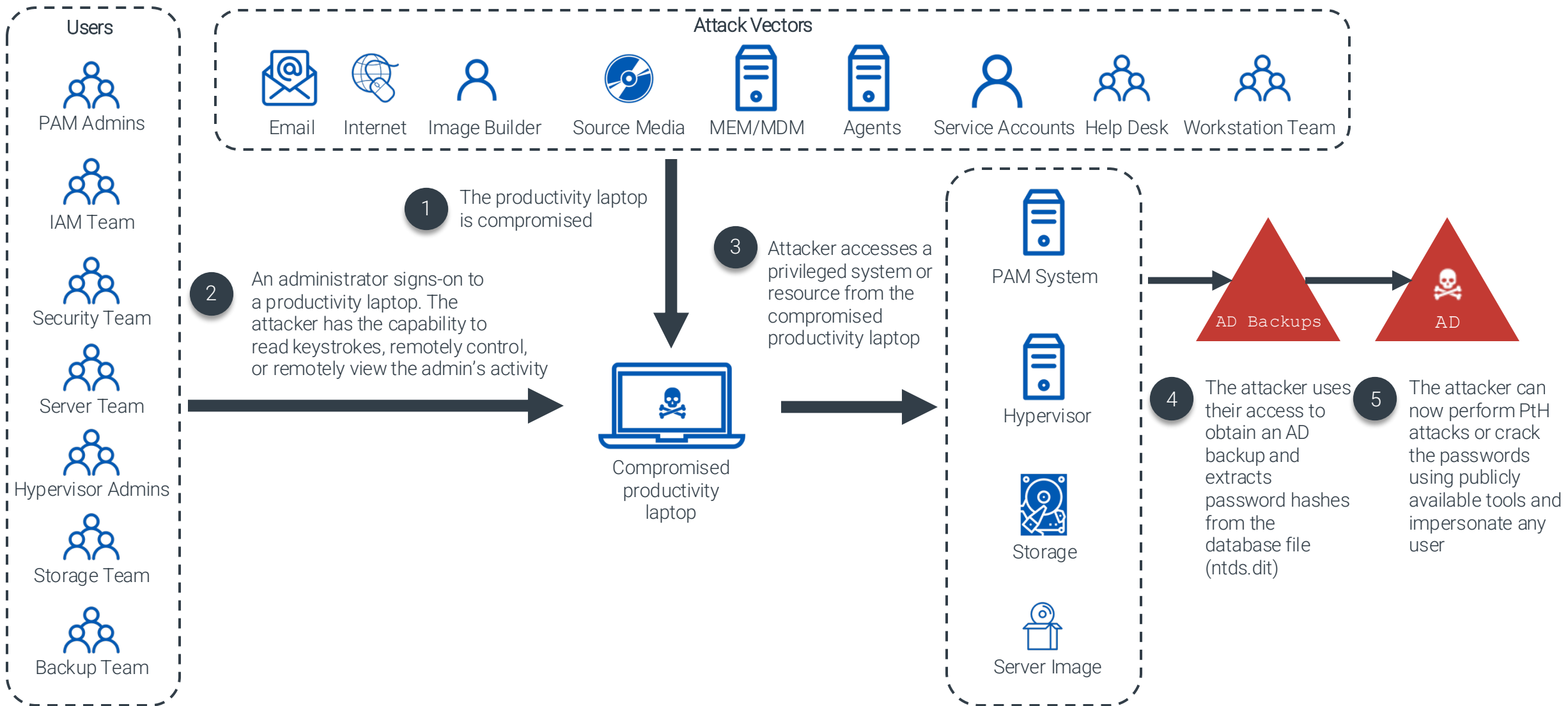
- STATE OF MULTICLOUD RISK REPORT

A compromised admin account can lead to:

- ✗ Unauthorized access to sensitive data & critical systems
- ✗ Data breaches & financial loss
- ✗ Business disruption



PRODUCTIVITY COMPUTER ATTACK VECTORS

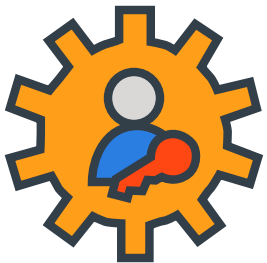


WHY PRIVILEGED ACCESS WORKSTATIONS?



Productivity machines increase vulnerability to attacks:

- Administrators who do not use PAWs perform sensitive tasks on general-purpose workstations, which are more susceptible to compromise.
- Using privileged accounts on unsecured machines increases the risk of credential theft through keylogging, phishing, and malware.



Malicious activities may blend into regular daily user operations, delaying remediation:

- Consider the volume of activities across all productivity machines compared to carefully monitoring a few special machines for administrative purposes only.

WHAT IS A PAW?



Dedicated & hardened device

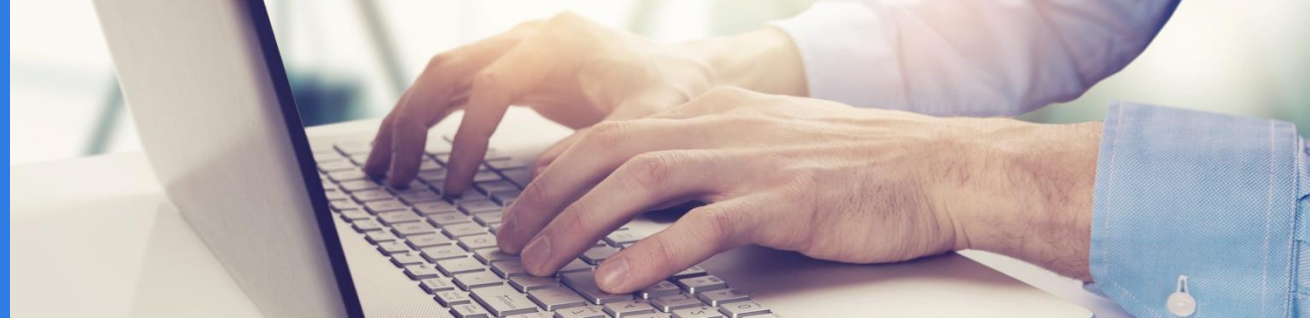
- ✓ Used exclusively for accessing sensitive systems
- ✓ Delivers a known-good, clean keyboard for performing privileged or sensitive tasks



Secure environment

- ✓ Isolates privileged accounts from common cyber threats
- ✓ Protects against phishing, malware, and credential theft
- ✓ Prevents administrators from making poor choices that expose credentials and access

PRIMARY USE CASE: IT ADMINISTRATOR ACCESS



Role of IT Administrator

- Manages domain controllers
- Ensures critical infrastructure protection



Privileged Access Workstation (PAW)

- Used for secure management
- Restricts access to authorized environments
- Prevents execution of unauthorized applications



Security Measures

- Protection from keyloggers
- Protection from malware

What Goes Into a PAW?

PRIORITIZE CLEAN SOURCE PRINCIPLE



By:

- Hardware acquisition
- Base operating system installation
- Software packages
- External control points

Protects Against:

- ✓ Laptop image compromise during build by downloading OS, software, etc. from an insecure environment
- ✓ Compromised pre-built images re-used for every deployment

CLEAN SOURCE PRINCIPLE



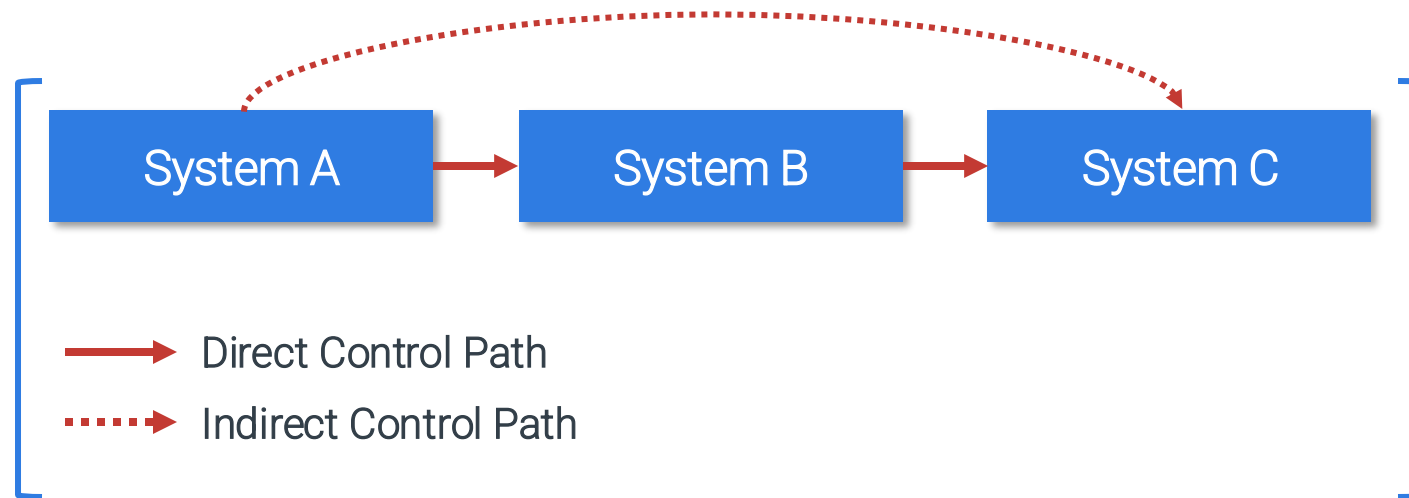
The clean source principle is crucial in securing Tier 0 since every system in the control path can be used to modify a Tier 0 asset and result in widespread impact.



The clean source principle dictates that any security-related dependency of a system must be managed to the same level of assurance. Put another way, given three systems below called A, B, and C, if A controls B and B controls C, A also transitively controls C. To adhere to the clean source principle, if system C is a Tier 0 asset, systems A and B must also be Tier 0 assets.



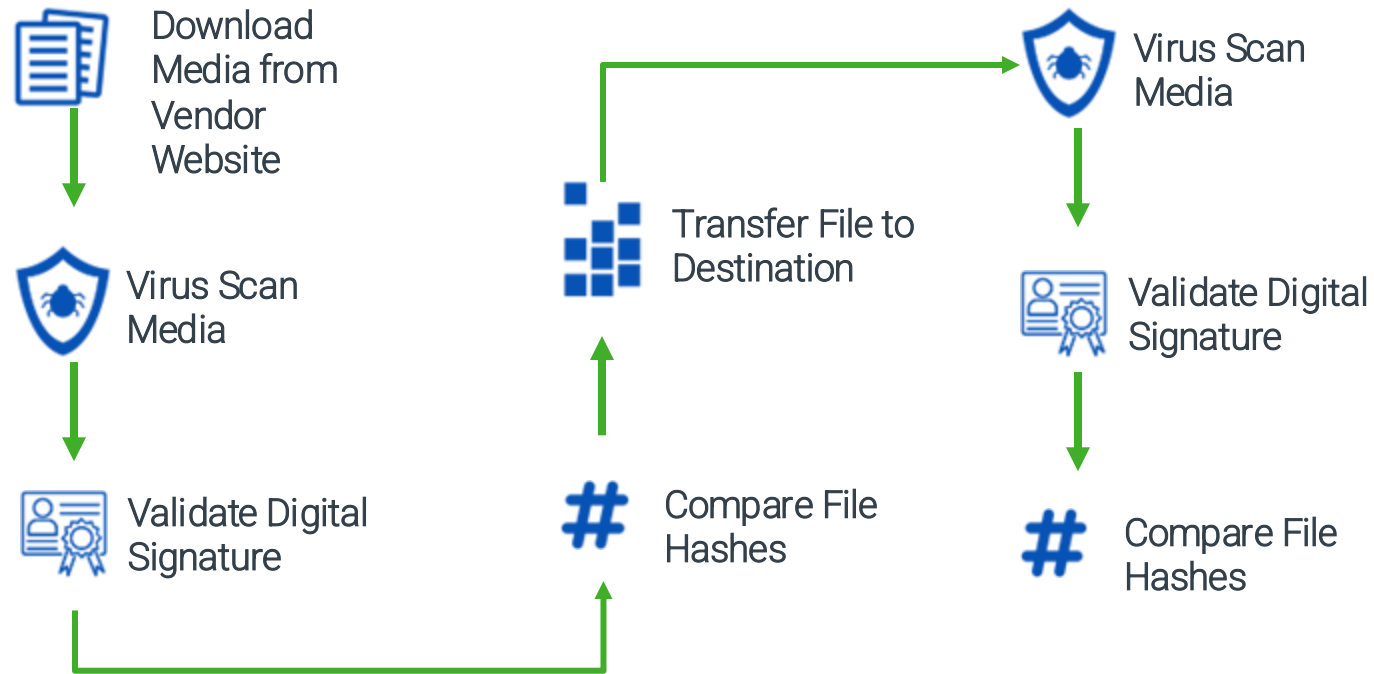
The Tier 0 forest should be built using the clean source principle, using Privileged Access Workstations (PAWs) and following the clean source media process. Ongoing management of Tier 0 should only be performed with PAWs.



CLEAN SOURCE MEDIA



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



REDUCE THE ATTACK SURFACE



By:

- Removing unnecessary software & agents
- Using advanced Windows security features to harden the operating system
- Removing local administrator access to PAWs

Protects Against:

- ✓ Vulnerabilities in unnecessary software packages
- ✓ Exploitable parts of Windows
- ✓ Elevation of privileges and limiting potential attacks

ISOLATE PAWS FROM THREAT VECTORS



By:

- Preventing unauthorized Internet access
- Tunneling through trusted networks/endpoints only
- Isolating PAWs from untrusted files and code

Protects Against:

- ✓ Accessing malicious content online
- ✓ Man-in-the-middle attacks
- ✓ Running malicious code or compromised files

COMPARING PRODUCTIVITY AND PAW DEVICES

	Productivity	PAW
Secure boot	✓	✓
Credential Guard	✓	✓
TPM 2.0	✓	✓
BitLocker encryption	✓	✓
WHfB	✓	✓
Intune Security Baselines	✓	✓
Remove Admin rights	Some	✓
URLs restricted	Some	✓
AppLocker (application execution control)		✓
Applications only installed by Intune		✓
App Control for Business		✓
Windows Firewall – Outbound traffic blocked by default		✓

MANDATE PAW USAGE



By:

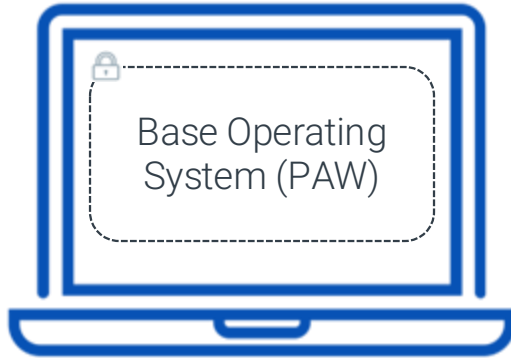
- Ensuring administrators use PAWs exclusively for managing high-value assets and privileged credentials
- Leveraging conditional access policies to mandate PAWs for cloud-management tasks
- Isolating network access to require a PAW to connect to critical systems

Protects Against:

- ✓ Insecure or compromised workstations used to manage high-value assets
- ✓ Cloud-management tasks performed from insecure workstations
- ✓ Attacks from non-management devices to critical systems

PAW MODELS

Standalone PAW

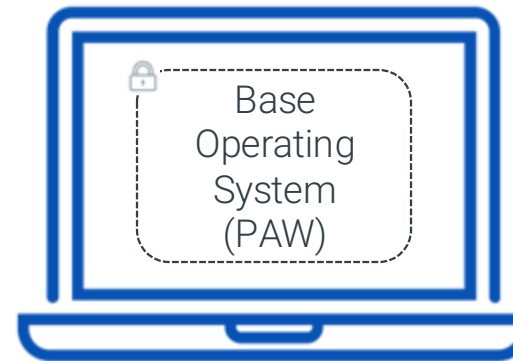


PAW Laptop



Productivity Laptop

Hardened VDI Client

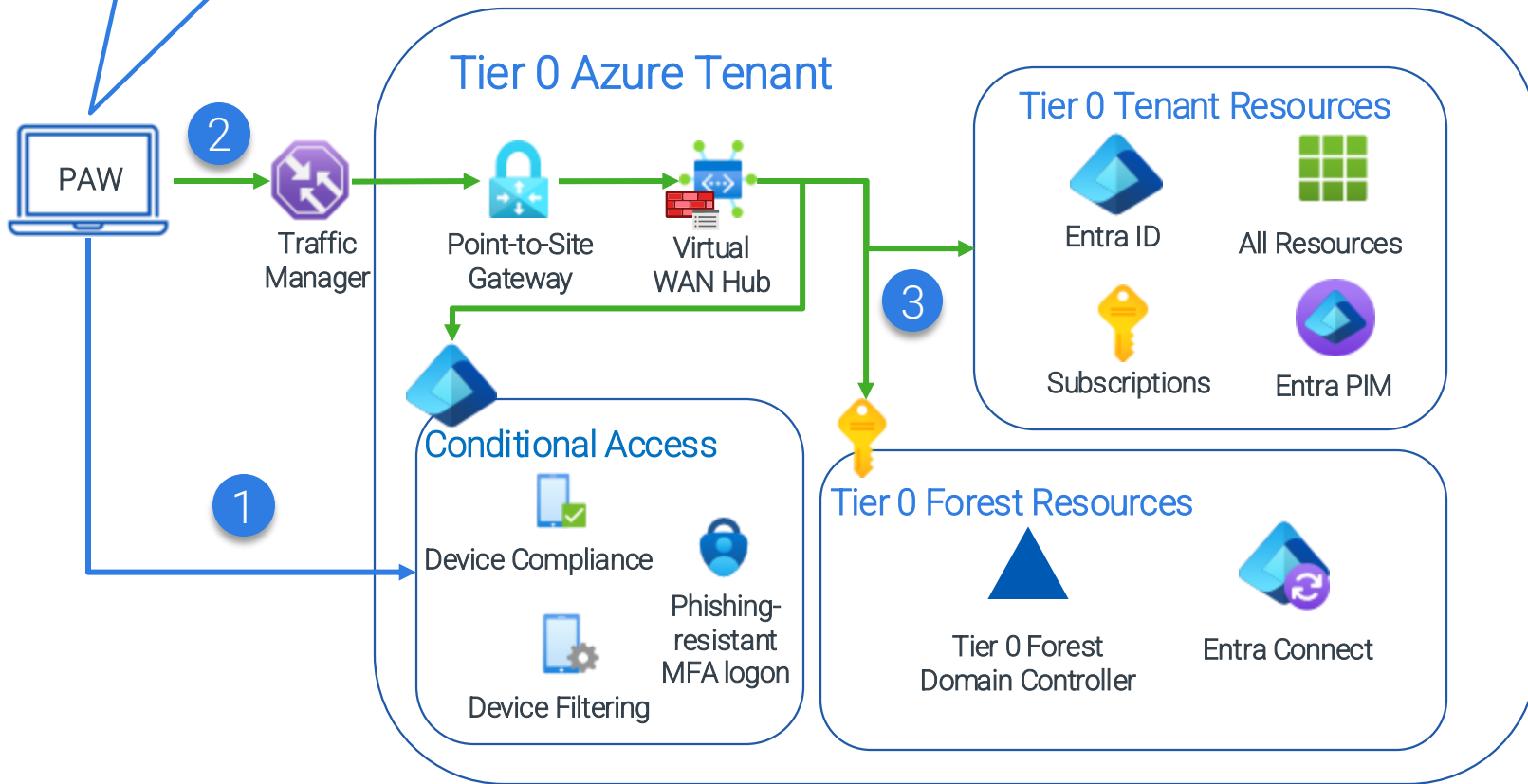


PAW Laptop



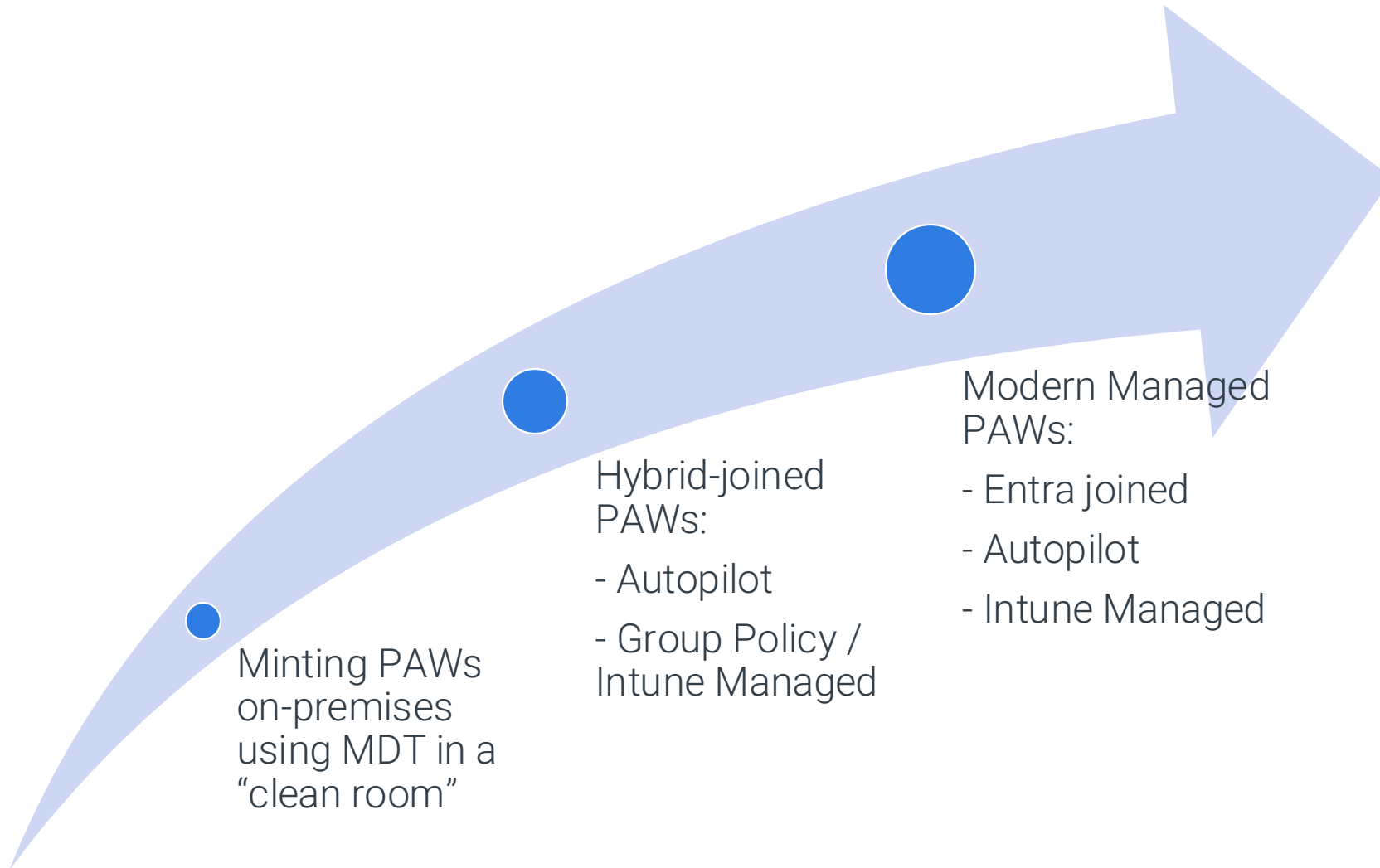
SUPPORTING INFRASTRUCTURE DESIGN

- Windows 11 Enterprise
- Entra joined to the Tier 0 Tenant
- Internet browsing restricted
- Logon to PAW with a standard user account (not privileged on PAW)

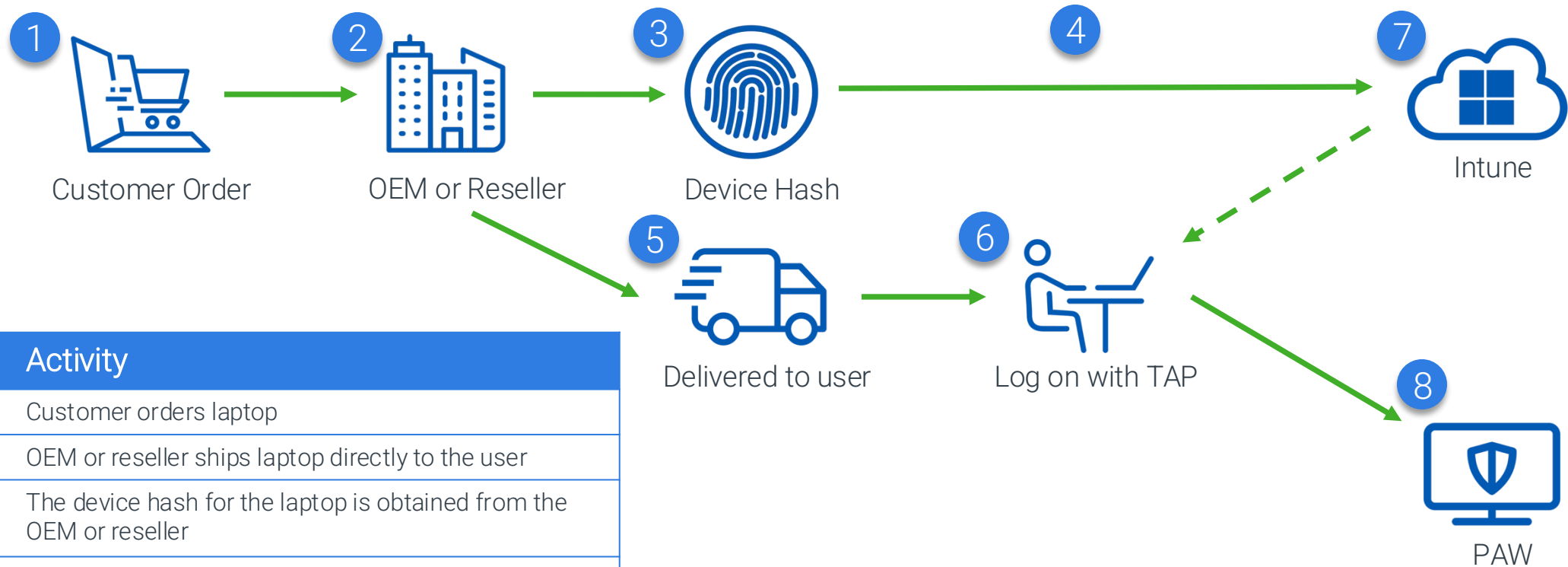


Step	Description
1.	User logs on to the PAW using Windows Hello for Business (using a FIDO2 key). The PAW connects to Entra ID and is checked against CA policies for device compliance and device filters.
2.	If Windows Hello for Business or FIDO2 logon occurred, the PAW connects to VPN
3.	The PAW can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

EVOLVING ESTABLISHED PAW PROGRAMS



PAW PROVISIONING PROCESS – ENTRA JOINED



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 user's home or office
6.	User logs on to the laptop with a Temporary Access Pass (TAP)
7.	Autopilot configures the laptop with the configuration in Intune
8.	The PAW is ready for use

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

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
- Windowscommunicationsa
pps
- 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



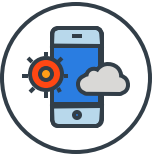
TO SUM IT UP... SECURING PAWS



Users are “standard” users, not local admins



Managed by Tier 0 admins (manage across tier or managed down, never up)



Internet access is restricted



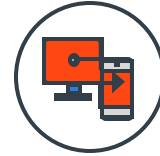
Conditional Access policies can be used to restrict Azure roles to require a PAW



Apps only deployed using Intune



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



Unnecessary apps are removed




Physical security is important!


A FEW QUESTIONS TO ASK




- ✓ Do you have specific preferences or requirements for a secondary device to support Privileged Access Workstations (PAWs)? For instance, are your administrators open to having two devices, or would they prefer a model where a VDI is used as their 'productivity' machine?
- ✓ What is the total number of administrators who will be operating within the PAW environment?
- ✓ Which applications or tools are essential for the administrators to perform their tasks effectively?

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

THANK YOU!

