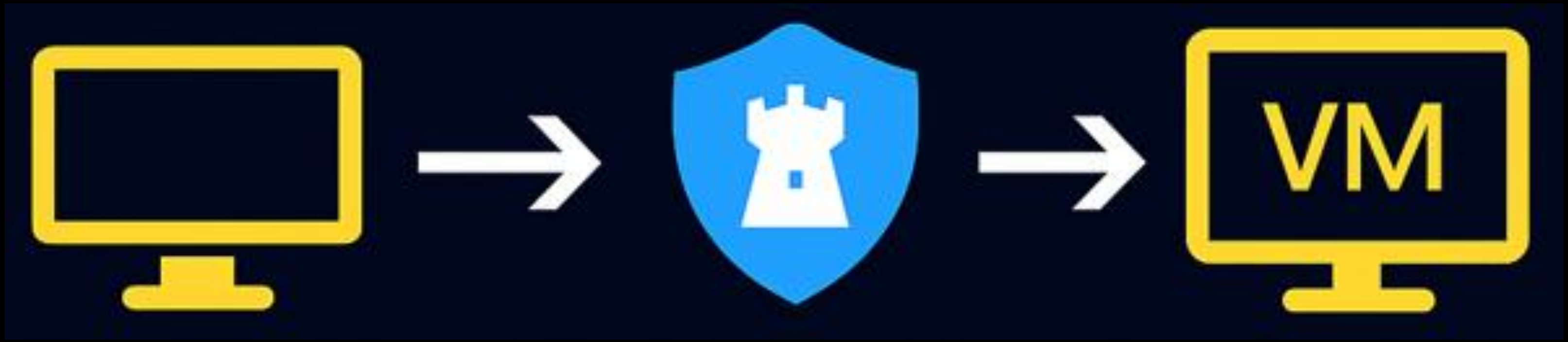
Privileged Access Workstations (PAW) + Azure Bastion Securing Administrative Access in the Cloud

Microsoft CERTIFIED EXPERT

#PerparimLabs | Microsoft Entra | Azure Security | Zero Trust



PerparimLabs

Why Administrative Access Must Be Protected

- Admin accounts are the biggest target in cyberattacks
- Compromised admin → full environment compromise
- Zero Trust requires verifying both **identity and device**

PerparimLabs

What Is a Privileged Access Workstation (PAW)?

- A hardened, isolated device for high-risk admin tasks
- Designed for Zero Trust administrative operations
- Strictly separated from daily user activities (email, browsing)

PerparimLabs

PAW Security Layers

Four security layers that make PAWs Zero Trust–ready

Four mini-sections:

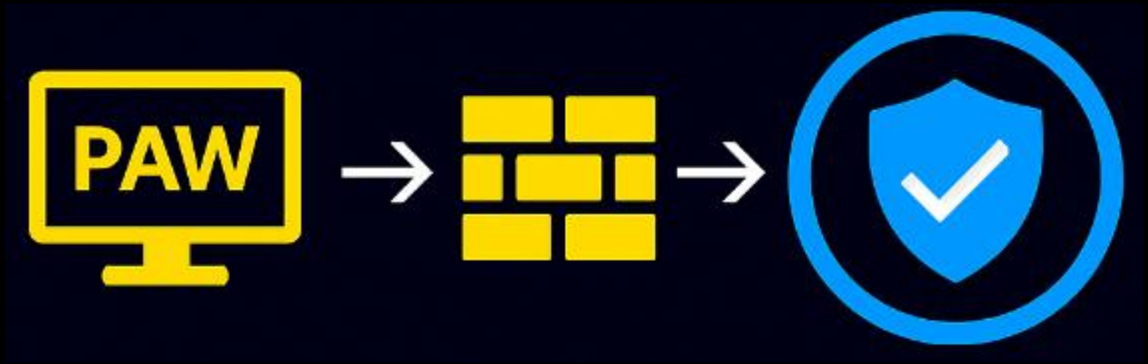
- **Hardware Root of Trust**
- **Secure OS Baseline (Intune)**
- **Microsoft Defender for Endpoint**
- **Conditional Access device posture checks**

Why PAWs Matter

- Reduce attack surface
- Prevent lateral movement
- Stop malware/keylogging against admins
- Enforce least privilege
- Align with Zero Trust architecture

Hybrid PAW Architecture

- On-prem → perimeter network (DMZ) → jump host
- Admin workstation → secure access path
- No direct access to servers



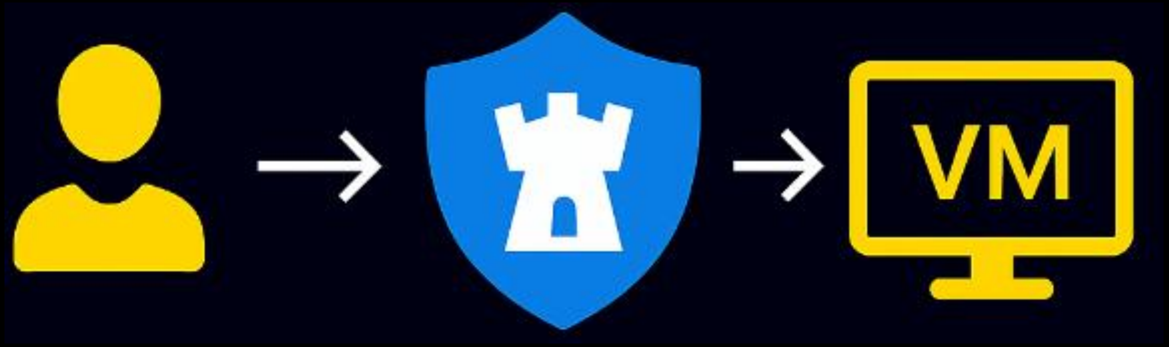
Hybrid Privileged Access Flow (PAW → DMZ → Jump Host → Servers)

PerparimLabs

Azure Bastion Overview

Secure admin access without exposing public RDP/SSH.

- Secure RDP/SSH over HTTPS
- No public IP on VMs
- Prevent exposed RDP attacks
- Fully integrated with Azure Portal

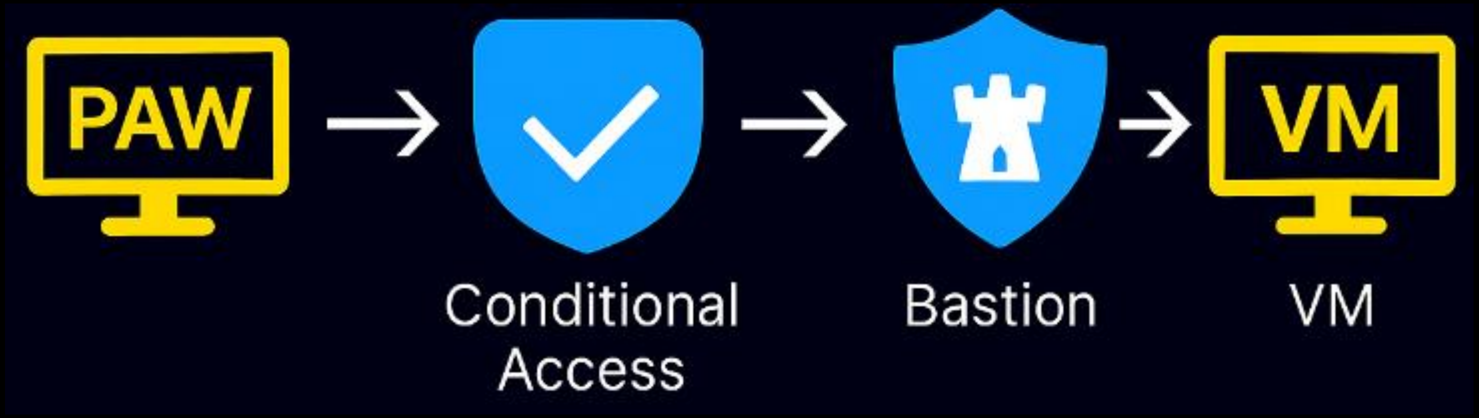


PerparimLabs

PAW + Azure Bastion Together

This is the Zero Trust administrative access path.

- PAW provides secure device + identity
- Bastion provides secure access path
- Combined = hardened Zero Trust admin access
- Prevents credential theft + remote exploitation



PerparimLabs

End-to-End Access Flow

Numbered sequence:

1️⃣ Admin signs into PAW

2️⃣ Conditional Access enforces MFA + device compliance
3️⃣ PAW verified by Defender + Intune
4️⃣ Admin connects to VM using Azure Bastion
5️⃣ VM accessed over secure HTTPS session

6️⃣ No public exposure of privileged endpoints

Security Benefits

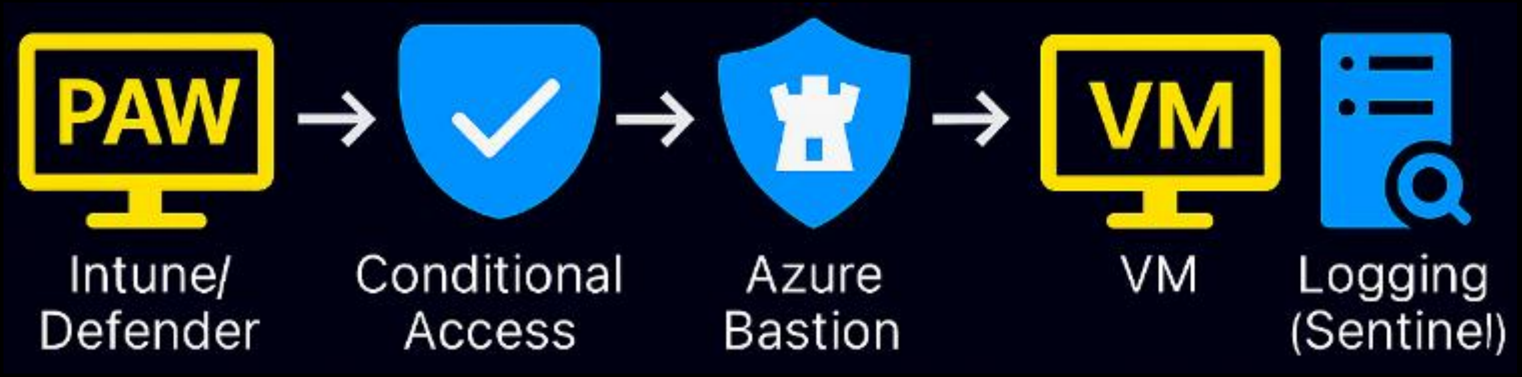
✓ Eliminates exposed RDP endpoints completely
✓ Provides isolation for admin tasks
✓ Reduces credential theft
✓ Supports Zero Trust enforcement
✓ Enables secure remote administration

Business Impact

- Stronger compliance posture
- Prevents catastrophic admin compromise
- Improves operational security
- Reduces attack surface across hybrid/cloud environments

PerparimLabs

Privileged Access Workstation + Azure Bastion Architecture



PerparimLabs

When to Use PAWs

- Domain / cloud administrators
- Privileged identities
- Sensitive workloads
- Security-critical environments
- Hybrid or cloud-only organizations

Summary

- PAWs protect admins
- Bastion protects access paths
- Combined = Zero Trust administrative security
- Applicable across hybrid and Azure environments