

63-51 / Emerging Technologies

May 2025



Introduction

PAM solutions

Goal

To protect privileged accounts from misuse and compromise by ensuring strict control, complete visibility, and traceability of access to critical systems within an organization.

- Reduce the attack surface from internal and external cyber threats
- Ensure compliance with standards (ISO 27001, GDPR, PCI DSS, etc.)
- Minimize the impact of breaches by restricting access

Target

All privileged accounts that could cause significant harm if misused or compromised:

- System and network administrators
- Root accounts (Linux/Unix)
- Critical service accounts
- DevOps accounts (CI/CD pipelines, APIs, cloud infrastructure)
- Temporary privileged users (e.g., consultants)

Scope

Covers the full lifecycle of privileged access, including:

- Credential management: storing, encrypting, and rotating passwords
- Session recording and monitoring
- Just-in-Time (JIT) access for specific tasks
- Role-Based Access Control (RBAC)
- MFA and Zero Trust integration
- Compatibility with DevOps tools, SaaS, cloud, and hybrid infrastructure ³

Why Pam Matters?



A Short History of PAM

PAM solutions emerged in the 2000s

Organizations faced increasing threats linked to privileged accounts

Traditional tools like Active Directory lacked fine-grained controls

Dedicated PAM platforms to secure admin access

Hybrid and cloud environments

Privilege Escalation & Critical Account Risks

Attackers often target:

- **Local Administrator Accounts** (reused passwords across devices)
- **Domain Admin Accounts** (full Active Directory control)
- **Service Accounts** (undocumented, non-expiring, unmonitored)

Common techniques:

- Credential dumping (e.g., Mimikatz)
- Lateral movement
- Golden Ticket attacks (Kerberos ticket forging)
- Shadow Admins (hidden high-privilege accounts)

Major Recent Breaches

Tesla Data Leak (2023 & 2025)

Two former employees leaked over 100 GB of PII, including Social Security numbers, bank details, and in-car recordings.

In 2025, a website called *DogeQuest* displayed personal Tesla user data on a live map.

These incidents highlight the danger of poorly controlled internal access.

Major Recent Breaches

Dropbox Sign Breach (2024)

A threat actor accessed the production backend of Dropbox Sign through an automated system configuration tool.

Stolen data included:

Customer emails, usernames, and phone numbers

Hashed passwords, API keys, OAuth tokens

Multi-factor authentication data

The breach emphasizes the need for strong access controls and real-time monitoring of backend systems.

How PAM Mitigates These Risks

**Removes standing
privileges** using
Just-in-Time
access

**Centralized
credential vault**
eliminates local
password storage

**Full session
recording** for
accountability
(SSH/RDP)

**Automated
password rotation**
to prevent reuse

**Approval
workflows and
MFA** to control
high-risk access

**Audit &
Monitoring**

The chosen solution



Small Market Analysis: Leaders and Alternatives

Gartner Magic Quadrant (Aug 2024) – shown in background

Leaders: CyberArk, BeyondTrust, Delinea

Challengers: ARCON, **ManageEngine (PAM360)**

Visionaries: WALLIX, One Identity

Niche Players: Broadcom (Symantec), Netwrix

ManageEngine PAM360 is positioned as a Challenger, showing growing maturity in execution with a strong vision for integrated, cloud-compatible PAM solutions.

Figure 1: Magic Quadrant for Privileged Access Management



Why We Didn't Choose CyberArk or BeyondTrust

Solution	Strengths	Limitations for Our PoC
CyberArk	Industry leader, comprehensive, robust	Too complex and costly for a student PoC or small-scale testing
BeyondTrust	Great balance of usability and control	Professional license required, more complex to deploy
JumpServer	Open-source, multi-protocol, lightweight	Less polished UI, limited scalability, fewer enterprise features

Why PAM360 Was the Best Fit

- Full license provided by our partner Kidan
- Native integration with Azure AD, RDP, SSH, Linux
- Ready-to-use compliance templates (ISO 27001, GDPR, PCI DSS)

PAM360 → complete and realistic platform

Strategic Partnership with Kidan

Thanks to Kidan.co, official ManageEngine partner in Switzerland:

- We received a full-featured PAM360 license
- Gained professional-level documentation and support
- Opportunity for future collaboration (internship, projects, company training)
- This transformed our project into a market-relevant experience, aligned with real business needs.

PAM 360's SWOT

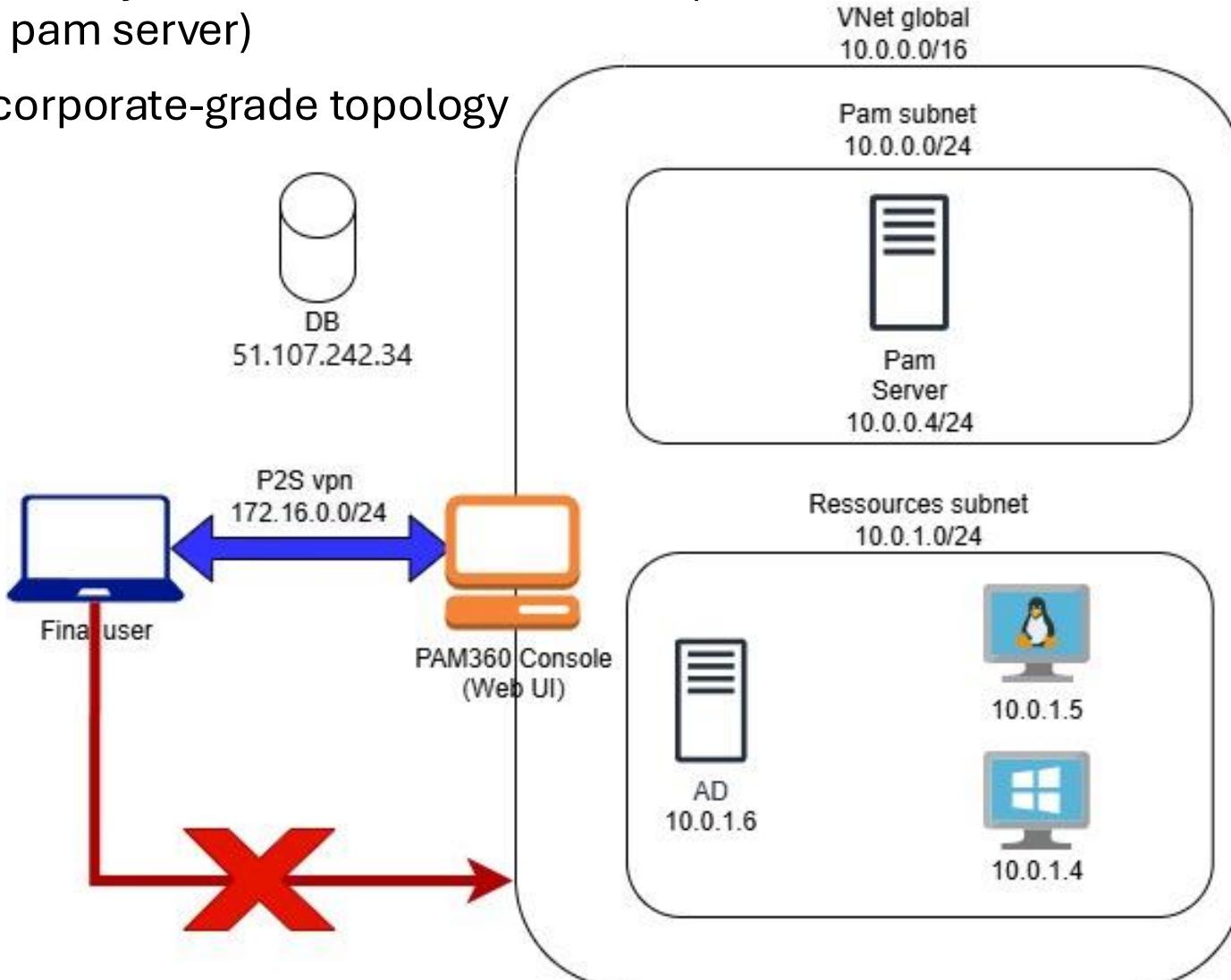


Architecture

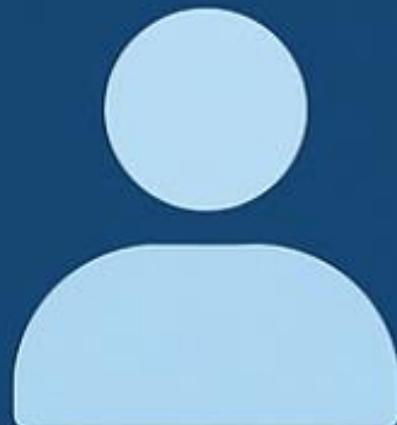


Overview of Our Lab Architecture

- Hosted on Azure
- 2 subnets: Management and Resources
- PAM360 as the central control point
- VPN access only leads to PAM360 Console (no direct resource access or pam server)
- Realistic corporate-grade topology



Core module implementation



Core PAM Modules Implemented in Our PoC

Privileged Account & Credential Vaulting

→ Centralized and encrypted password storage,
auto-rotation

Privileged Session Management

→ Monitored RDP/SSH sessions, with full playback
and live oversight

Access Workflow Control

→ Role-based access approval, request → approval
→ checkout → audit

Audit & Compliance

→ Detailed audit logs, reports aligned with ISO
27001 / GDPR

VPN – Secure Access

Assignment

Dynamic Static

Enable active-active mode *

Enabled Disabled

Configure BGP ASN *

Enabled Disabled

Once your VPN gateway is deployed correctly

The screenshot shows the configuration interface for a virtual network gateway named 'VpnPam'. On the left, there are several configuration options: 'Address pool *' set to '172.16.1.0/24', 'Tunnel type' set to 'IKEv2 and SSTP (SSL)', 'IPsec / IKE policy' set to 'Default', and 'Authentication type' set to 'Azure certificate'. Below these is a section for 'Root certificates' with a table:

Name	Public certificate data
VpnPam	MIIC7TCCAdWgAwIBAgIQA63o4iJKIRC2NHVcTStOT... ...

A modal dialog box titled 'PAM_Network' is displayed in the center, showing the text 'Azure VPN' with a connection status message: 'Cliquez sur Connexion pour démarrer la connexion. Cliquez sur Annuler pour travailler hors connexion.' At the bottom of the dialog are three buttons: 'Conneter', 'Annuler', and 'Propriétés'.

Address pool is for the ip that will be dynamically associated to your computer when initiating a vpn connection

Tunnel type → choose IKEv2 and SSTP so that you can use it on windows and MAC devices



Taper ici pour rechercher



10:31

FRA

150

Screenpresso.com

Discover Resources

ManageEngine PAM360

10.0.0.4:8282/PassTrixMain.cc#/PasswordFullView/PasswordMainView

Trial period valid till Jun 10, 2025

Request: Personalized demo More admins Sales quote Contact us

ManageEngine PAM360

Search

All My Passwords

Resources Passwords

Add Resource Discover Resources Resource Types Resource Actions Export

Showing 1 - 7 Total Count prev Page 1 next 25 50 75 100

	Resource Name	Description	Type	DNS Name	Department	Location	URL	Trust Score	Resource Actions	Remote Connection
<input type="checkbox"/>	AzureDb	protectdbser...	...	N/A	N/A
<input type="checkbox"/>	Domain Adm...	Resource imp...	...	Domain Ad...	N/A
<input type="checkbox"/>	Domain Users	Resource imp...	...	Domain Users	N/A
<input type="checkbox"/>	Enterprise A...	Resource imp...	...	Enterprise A...	N/A
<input type="checkbox"/>	PAMPOC - D...	Resource imp...	...	ADPAM	N/A
<input type="checkbox"/>	TOTPTest	totpsite-fqh...	...	https...	N/A	N/A
<input type="checkbox"/>	vmwindows	Added By Ag...	...	vmwindows	100%	100%

New

Cloud Entitlements

SSH Keys

Certificates

Users

Admin

Audit

ManageEngine PAM360

ACME Providers

25 Screenpress.com

File Share & Session Recording

ManageEngine PAM360 10.0.0.4:8282/PassTrixMain.cc#/ConnectionView Trial period valid till Jun 10, 2025 Request : Personalized demo More admins Sales quote Contact us

ManageEngine PAM360 Search Facing problems in launching remote connections?

Dashboard Resources Groups Connections Cloud Entitlements SSH Keys Certificates Users Admin Audit

Remote Connections All My Connections Owned and Managed Favorites Recently Accessed Web App Connections HTTPS Gateway Connections Secure File Transfer

▶ Folders

◀ Resource Groups Computers@PAMPOC PAMPOC\Administrators PAMPOC\Domain Computers PAMPOC\Users

◀ Default Groups admin's Default Group

Resources Accounts Domain Accounts Local Accounts

PAMPOC - Domain Controller

Search Accounts

adminhevs adurand dydy jojo mama nana

Taper ici pour rechercher

10:43 15/06/2024 Screenpresso.com

Access Policy

ManageEngine PAM360 x + 10.0.0.4:8282/PassTrixMain.cc#/PasswordFullView/PasswordMainView ☆ ! ? ...

Trial period valid till Jun 10, 2025 Request: Personalized demo More admins Sales quote Contact us

ManageEngine PAM360 Search Facing problems in launching remote connections?

Dashboard **Resources** **Groups** **Connections** **New Cloud Entitlements** **SSH Keys** **Certificates** **User** **Admin** **Audit**

Password Explorer All My Passwords ← All My Passwords

Resources **Passwords** Add Resource Discover Resources Resource Types Resource Actions Export

Showing 1 - 8 Total Count < prev Page 1 next > 25 50 75 100

<input type="checkbox"/>	Resource Name	Description	Type	DNS Name	Department	Location	URL	Trust Score	Resource Actions	Remote Connection
<input type="checkbox"/>	AzureDb	protectdbser...	...	N/A
<input type="checkbox"/>	Domain Adm...	Resource imp...	...	Domain Ad...
<input type="checkbox"/>	Domain Users	Resource imp...	...	Domain Users
<input type="checkbox"/>	Enterprise A...	Resource imp...	...	Enterprise A...
<input type="checkbox"/>	PAMPOC - D...	Resource imp...	...	ADPAM
<input type="checkbox"/>	TOTPTest	totpsite-fqh...	...	https...	N/A
<input type="checkbox"/>	vmlinux.inte...	Added from r...	Li...	vmlinux.inte...	Department	Location	...	N/A
<input type="checkbox"/>	vmwindows - ...	Added By Ag...	...	vmwindows	100%

Taper ici pour rechercher Windows Taskbar Icons 11:48 15.0% Screenpresso.com

Remote App Access

ManageEngine PAM360

10.0.0.4:8282/PassTrixMain.cc#/AuditQuickView/RecordedSession

Trial period valid till Jun 10, 2025

Request : Personalized demo More admins Sales quote Contact us

ManageEngine PAM360 Search Facing problems in recorded sessions playback?

Audit

Resource Audit

Active Privileged Sessions

Recorded Server Connections

Recorded Website Connections

Keys Audit

Certificate Audit

Cloud Entitlements

New

SSH Keys

Certificates

Users

Task Audit

Privileged Task Automation

Configure Session Recording

Audit Actions

Showing 1 - 25 of 134

Resource Name	User Account	Operated By	IP Address	Status	Time Stamp	Reason	Play	Activity Logs	Chat Log	Delete
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:43 AM	Retrieved b...	▶	⚙️	-	🗑
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:42 AM	Retrieved b...	▶	⚙️	-	🗑
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:41 AM	Retrieved b...	▶	⚙️	-	🗑
PAMPOC - Domain Con...	dydy	admin	172.16.1.130	Succ...	May 15, 2025 08:40 AM	Retrieved b...	▶	⚙️	-	🗑
PAMPOC - Domain Con...	dydy	admin	172.16.1.130	Succ...	May 15, 2025 08:38 AM	Retrieved b...	▶	⚙️	-	🗑
PAMPOC - Domain Con...	dydy	admin	172.16.1.130	Succ...	May 15, 2025 08:38 AM	Retrieved b...	▶	⚙️	-	🗑
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 08:36 AM	Retrieved b...	▶	⚙️	-	🗑
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 08:33 AM	Retrieved b...	▶	⚙️	-	🗑
PAMPOC - Domain Con...	adminhevs	admin	172.16.1.130	Succ...	May 15, 2025 08:09 AM	Retrieved b...	▶	⚙️	-	🗑
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 08:09 AM	Retrieved b...	▶	⚙️	-	🗑
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 07:33 AM	Retrieved b...	▶	⚙️	-	🗑
vmwindows - Agent1	dylsan	admin	172.16.1.130	Succ...	May 15, 2025 07:25 AM	Retrieved b...	▶	⚙️	-	🗑

Taper ici pour rechercher

Windows Taskbar icons: File Explorer, Microsoft Edge, Word, Excel, Powerpoint, Firefox, Internet Explorer, Task View, Settings, Task Manager, File History, Taux... (Network Speed), Volume, Battery, F148, 15:00, Screenpresso.com

Remote App Access

The screenshot shows the ManageEngine PAM360 web application interface. The top navigation bar includes the title "ManageEngine PAM360", a trial period message ("Trial period valid till Jun 10, 2025"), and links for "Personalized demo", "More admins", "Sales quote", and "Contact us". The main dashboard features a search bar and a sidebar with navigation icons for Dashboard, Resources, Groups, Connections, Cloud Entitlements (highlighted with a yellow "New" badge), SSH Keys, Certificates, Users, Admin (highlighted in dark blue), and Audit.

The main content area is divided into several cards:

- Authentication**: Includes Active Directory, Microsoft Entra ID, LDAP, SAML Single Sign-On, RADIUS, Smart Card / PKI / Certificate, Two-Factor Authentication, and Super Administrators.
- Resource Config**: Includes Discover Resources, Password Policies, Resource Additional Fields, Account Additional Fields, Resource Types, and JDBC Properties.
- Zero Trust**: Includes Configuration, Trust Score, Access Policy, and Conflict Resolver.
- Customization**: Includes Roles, Password Reset Listener, Auto Logon Helper, Rebrand, Email Templates, Message Templates, Password Reset Plugin, and SSH Command Sets.
- Settings**: Includes Log Level, Export / Offline Access, Mail Server Settings, and Proxy Server.
- Connections**: Includes RemoteApp, Gateway Server Settings, Session Configuration, and Landing Servers.
- Privilege Elevation**: Includes Allowed Apps/Scripts, Manage Commands, and Application Control.
- SSH/SSL Config**: Includes Schedules, SSH Policy Configuration, Notification Settings, and Certificate Sharing.

At the bottom, there is a search bar ("Taper ici pour rechercher") and a taskbar with various application icons. A small orange circular icon with an equals sign is located in the bottom right corner.

Secure Command SSH

ManageEngine PAM360

10.0.0.4:8282/PassTrixMain.cc#/admin/adminMain

Trial period valid till Jun 10, 2025

Request : Personalized demo More admins Sales quote Contact us

Importing Domain Accounts...

Dashboard

Resources

Groups

Connections

New Cloud Entitlements

SSH Keys

Certificates

Users

Admin

Audit

ManageEngine PAM360

Search

Search term

Authentication

- Active Directory
- Microsoft Entra ID
- LDAP
- SAML Single Sign-On
- RADIUS
- Smart Card / PKI / Certificate
- Two-Factor Authentication
- Super Administrators

Resource Config

- Discover Resources
- Password Policies
- Resource Additional Fields
- Account Additional Fields
- Resource Types
- JDBC Properties

Zero Trust

- Configuration
- Trust Score
- Access Policy
- Conflict Resolver

Customization

- Roles
- Password Reset Listener
- Auto Logon Helper
- Rebrand
- Email Templates
- Message Templates
- Password Reset Plugin
- SSH Command Sets

Settings

- Log Level
- Export / Offline Access
- Mail Server Settings
- Proxy Server

Connections

- RemoteApp
- Gateway Server Settings
- Session Configuration
- Landing Servers

Privilege Elevation

- Allowed Apps/Scripts
- Manage Commands
- Application Control

SSH/SSL Config

- Schedules
- SSH Policy Configuration
- Notification Settings
- Certificate Sharing

ACME Providers

https://localhost:8282/PassTrixMain.cc#/admin/ContainerPlatforms

Screenpresso.com

30



Challenges, learnings and conclusion

What We Learned from the Project

The **complexity of secure privileged access**: understanding vaulting, session isolation, JiT, and least privilege logic.

How to configure a **VPN gateway and restrict direct access** through NSG rules.

Full deployment of a **realistic PAM solution** (PAM360) including:

Understand Zero Trust Framework and how to implement it

MFA

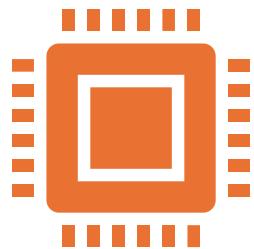
Session recording

SSH/RDP access brokerage

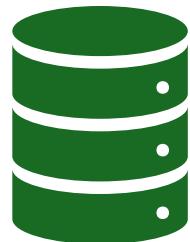
Password rotation

Certificate integration

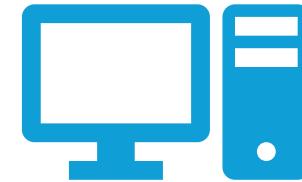
What challenge have we met?



VPN + certificate setup was the most technical part (cert generation, .pfx/.cer, P2S configuration)



Understanding and enforcing **Zero Trust logic** across multiple subnets



Remote connections in general (RDP, SSH, ...) due to a lack of logs

What's Next? – Maturity Model and Next Steps

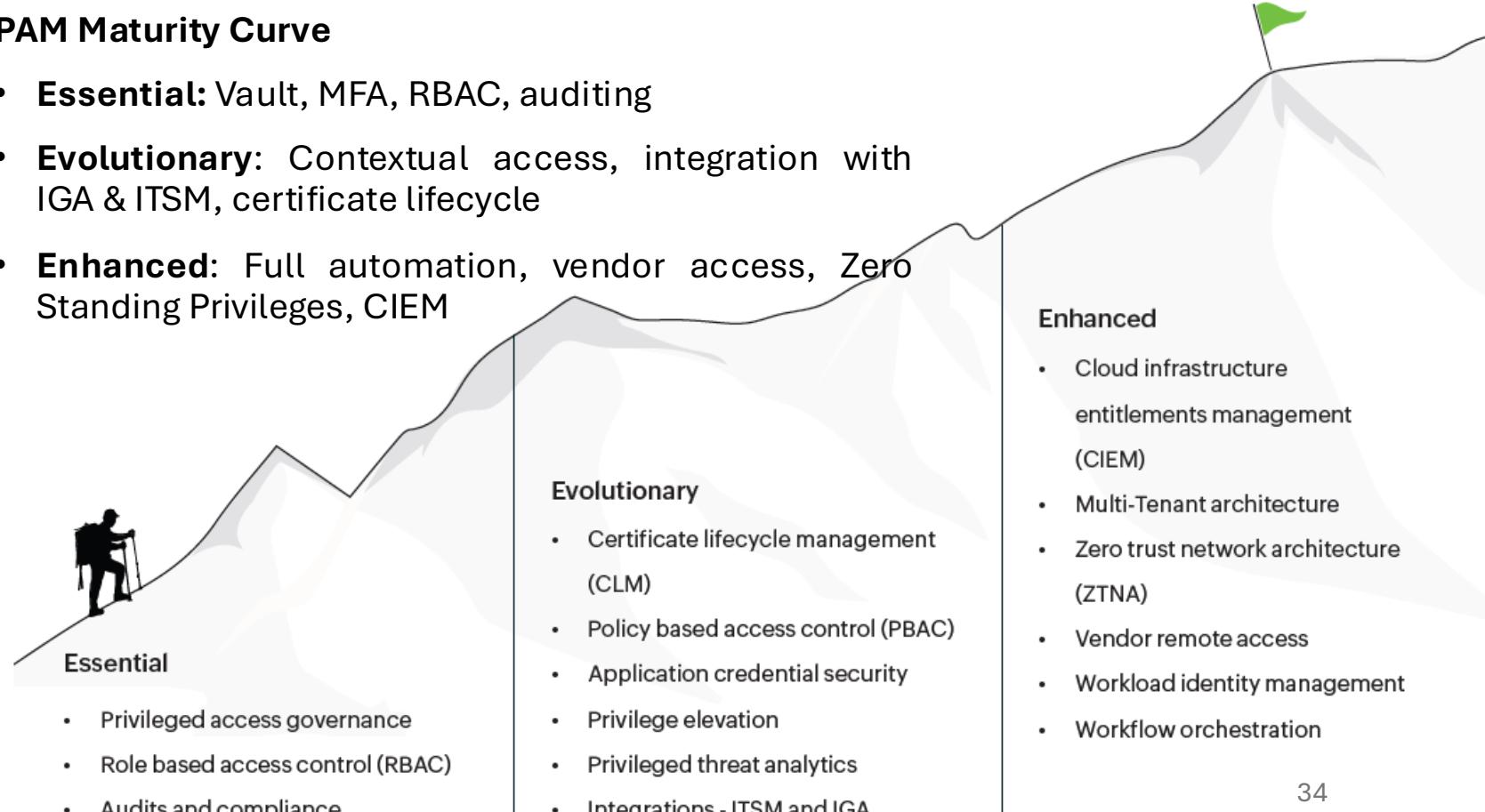
Recommendations

- Move toward **JIT (Just-in-Time)** and **PBAC** (Policy-Based Access Control)
- Enhance automation: Credential lifecycle, session termination
- Integrate **DevOps, CI/CD tools**, or third-party app credentials
- Strengthen monitoring with **SIEM integration (Azure Sentinel)**

ManageEngine

PAM Maturity Curve

- **Essential:** Vault, MFA, RBAC, auditing
- **Evolutionary:** Contextual access, integration with IGA & ITSM, certificate lifecycle
- **Enhanced:** Full automation, vendor access, Zero Standing Privileges, CIEM



Conclusion: What PAM360 Taught Us

Privileged access is one of the most critical risks in modern infrastructure. Through this project, we deployed and tested PAM360 in a realistic Azure environment, applying key cybersecurity principles like:

- Least privilege
- Just-in-Time access
- Zero Trust enforcement

Key takeaway:

- PAM360 proved to be a professional-grade solution that is also well-suited for education and experimentation.
- This PoC helped us understand real-world privileged access risks and defenses.

Questions ?

