THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Why PAM is a Critical Control in 2026

Privileged credential abuse remains the top vector for data breaches. Modern attackers exploit cloud APIs, DevOps pipelines and remote work tools, making traditional password vaults insufficient.

- → Credential theft leads to lateral movement and ransomware escalation
- → Hybrid workloads increase the attack surface for privileged accounts
- → Zero-Trust mandates continuous verification of privileged actions

CONTROL FRAMEWORK

Core Evaluation Criteria for 2026 PAM

Select platforms that meet these architectural pillars:

→ Zero-Trust session isolation and just-in-time access

→ API-first design for DevOps and cloud integrations

→ AI-driven anomaly detection on privileged activity

→ Native support for multi-cloud (AWS, Azure, GCP) and on-prem

→ Scalable secret rotation and audit logging

CONTROL FRAMEWORK

Enterprise-Grade Leaders

These platforms dominate large-scale deployments and offer deep integrations with SIEM, IAM and identity governance suites.

- → CyberArk Privileged Access Security – comprehensive vault, session recording and threat analytics
- → BeyondTrust Privilege Management – unified password, session and endpoint protection
- → Delinea Secret Server (formerly Thycotic) – rapid deployment, granular policy engine

CONTROL FRAMEWORK

Cloud-Native PAM Services

Built directly into public cloud platforms, these services provide seamless privilege elevation without extra infrastructure.

→ Azure AD Privileged Identity Management – just-in-time role activation and access reviews

→ AWS IAM Access Analyzer – automated detection of over-privileged policies and temporary credentials

→ Google Cloud Privileged Access Manager – fine-grained, time-bound access to GCP resources

CONTROL FRAMEWORK

Hybrid & Open-Source Options

Flexible solutions that bridge on-prem and cloud, often with extensible APIs for custom workflows.

- → HashiCorp Vault – secret storage, dynamic credentials and policy-as-code
- → IBM Security Verify Privilege Vault – integrated with IBM Cloud Pak and QRadar
- → ManageEngine PAM360 – centralized dashboard for on-prem, SaaS and cloud assets

CONTROL FRAMEWORK

AI-Driven and Emerging PAM Platforms

Next-generation offerings that leverage machine learning to predict risky privileged behavior and automate remediation.

→ One Identity Safeguard – real-time risk scoring of privileged sessions

→ Centrify Privilege Cloud (now Delinea) – adaptive access based on user risk profile

→ Delinea Secret Server – AI-powered secret discovery and rotation recommendations

EXECUTIVE TAKEAWAY

Executive Takeaway

Build a PAM architecture that layers enterprise-grade vaults, cloud-native services and AI analytics. Prioritize zero-trust session control, automated secret rotation and unified audit across all environments to stay ahead of privileged-credential attacks.

→ Deploy a core vault (CyberArk, BeyondTrust or Delinea) for high-value assets

→ Extend with native cloud PAM for elastic workloads

→ Add AI risk engines (One Identity, Centrify) for continuous threat detection