THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Privileged Access – The Crown Jewel of Breaches

Industry coverage highlights that the majority of high-impact data breaches begin with the compromise of privileged credentials. Protecting these accounts is the single most effective way to reduce breach scope.

→ Privileged accounts hold the keys to critical systems and data.

→ Attackers prioritize them for lateral movement and persistence.

CONTROL FRAMEWORK

1 Discover All Privileged Assets

Map every privileged account, service-level credential, and admin-enabled application across on-prem, cloud and SaaS environments.
Continuous discovery prevents hidden backdoors.

- → Automated inventory of local admin, domain admin, and service accounts.
- → Include cloud IAM roles and API keys.

CONTROL FRAMEWORK

2 Enforce Least-Privilege Access

Apply just-in-time (JIT) elevation and role-based policies so users receive only the permissions needed for a specific task and for a limited time.

→ Dynamic approval workflows.

→ Automatic revocation after task completion.

CONTROL FRAMEWORK

3 Centralize Credential Vaulting

Store privileged passwords, SSH keys and API secrets in an encrypted vault with automated rotation and access logging.

→ Zero-knowledge storage protects vault master keys.

→ Rotation policies reduce credential reuse.

CONTROL FRAMEWORK

4 Monitor Sessions & Apply Real-Time Analytics

Record privileged sessions, apply behavior analytics, and trigger alerts on anomalous commands or lateral movement.

→ Full-screen video replay for forensic review.

→ AI-driven risk scoring flags risky activity.

CONTROL FRAMEWORK

5 Integrate PAM with Enterprise IAM & Zero Trust

Connect the PAM platform to directory services, SSO, and Zero-Trust network access controls to enforce consistent identity policies across all workloads.

→ Single source of truth for privileged identity attributes.

→ Conditional access based on device posture and risk score.

EXECUTIVE TAKEAWAY

Executive Takeaway

A unified PAM architecture—discovery, least-privilege enforcement, vaulting, session control, analytics, and IAM integration—creates a hardened privileged-identity perimeter, reduces breach impact, and satisfies audit requirements.

→ Start with inventory; expand to JIT and vaulting.

→ Layer monitoring and analytics for rapid detection.

→ Tie PAM into existing IAM and Zero-Trust frameworks.