

PRIVILEGED ACCESS MANAGEMENT.



Every admin credential, service account, and root password is a high-value target — **and standing privileged access is often the shortest path from one compromised login to full domain control.** PAM replaces persistent admin rights with vaulted, time-bound, monitored elevation.

- CREDENTIAL VAULTING
- JUST-IN-TIME ELEVATION
- SESSION RECORDING
- BREAK-GLASS ACCESS

01 THE MECHANISM

Credential Vaulting
Storing privileged passwords and keys in an **encrypted vault, checked out on demand** rather than known or shared.

Just-in-Time Elevation
Granting admin rights **only for the duration of an approved task**, then automatically revoking them.

Session Monitoring
Recording and auditing **privileged sessions in real time** to detect misuse as it happens.

02 THE FLOW

The Elevation Cycle PER REQUEST

1

An admin requests elevated access to a specific system for a **defined task and time window**.

2

The vault checks out a rotated credential or issues a short-lived token — **the human never sees the static password**.

3

The session is **recorded and monitored**; access expires automatically when the window closes.

The Emergency Cycle BREAK-GLASS

1

A break-glass account is used **only when normal elevation channels are unavailable** during an incident.

2

Use of the credential triggers an **immediate, mandatory alert** to security and IT leadership.

3

The credential is **rotated immediately after use**, regardless of whether the emergency was legitimate.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Credential Vaulting & Rotation	Stores and automatically rotates privileged passwords, keys, and secrets.
Just-in-Time Access	Grants elevated rights only for the task duration, then revokes automatically.
Session Recording & Auditing	Captures privileged sessions for real-time review and forensic replay.
Service & Machine Account Governance	Extends the same vaulting and rotation discipline to non-human accounts.

04 PRIVILEGED ACCESS APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Shared Local Admin Passwords	No	One compromised credential grants admin access across every machine that shares it.
Standing Domain Admin Rights	No	Persistent elevated access sits exploitable long after any task requiring it ends.
Unmonitored Service Accounts	No	Machine credentials often outlive their original purpose with no owner reviewing them.
Manual Password Rotation	No	Rotation lapses the moment it depends on someone remembering to do it.
Combined PAM Program (Vaulting + JIT + Governance)	Yes	Removes standing privilege and makes every elevated action time-bound and auditable.

PRIVILEGED ACCESS.

VAULT · ELEVATE · MONITOR

05 PROGRAM OPERATIONS

Standing privilege is the single biggest lever attackers pull. Removing it does more than almost any other single control.

Service accounts are often the least governed identities. They rarely get reviewed like human accounts do.

Recordings only have value if someone reviews the alerts. Recording without monitoring is just storage.

Break-glass access must be rare and loud. If emergency access is used quietly and often, the process has failed.

06 CONTROL MAPPING

NIST SP 800-53 (AC-6)

Least privilege and privileged account management controls.

CIS CONTROLS V8.1

Account management safeguards including privileged account inventory.

PCI DSS V4.0

Requirements for **unique, monitored access** to cardholder data environments.

NIST CSF 2.0

Protect function coverage for identity and access management.

07 WHAT THIS DOES NOT SOLVE

A compromised vault itself

The vault becomes the **highest-value target** once privileged credentials centralize there.

Approval fatigue on elevation requests

Reviewers who rubber-stamp every request **remove the control's real value**.

Legacy systems that can't support vaulting

Some hardware and applications still require **hardcoded or shared credentials**.

Malicious use of legitimate access

A properly authorized session **can still be used to cause harm**.

08 MYTHS VS. REALITY

MYTH	REALITY
"PAM is just a password vault."	Vaulting is one piece; session monitoring and JIT elevation matter just as much.
MYTH	REALITY
"Only human admins need PAM."	Service and machine accounts often hold more standing privilege than people do.
MYTH	REALITY
"Break-glass accounts are a backup plan, not a risk."	An unused but unmonitored break-glass account is itself an attack target .
MYTH	REALITY
"Session recording alone prevents misuse."	Recording without active review only creates evidence after the damage is done .
MYTH	REALITY
"Rotating passwords quarterly is enough."	Static rotation cycles leave a wide window; JIT and automatic rotation close it.

09 SPEAK THE PROGRAM — KEY TERMS

PAM

The systems and practices that **vault, elevate, and monitor** high-privilege accounts and credentials.

CREDENTIAL VAULTING

Storing privileged secrets in an encrypted repository, **checked out on demand** instead of memorized or shared.

JUST-IN-TIME (JIT) ELEVATION

Granting privileged access **only for the duration** of an approved task.

BREAK-GLASS ACCESS

An emergency credential used **only when normal elevation channels are unavailable**.

SESSION RECORDING

Capturing a privileged session's activity for **real-time review** and **audit replay**.

SERVICE ACCOUNT

A non-human account used by an application or process, **often holding standing privilege**.