THE BIGGEST RISKS OF OPERATING WITHOUT PAM

The impact of unmanaged privileged access extends far beyond cybersecurity. Security incidents involving privileged accounts can disrupt operations, damage customer trust, and create significant financial losses.

Even a single compromised privileged account can result in:

- SYSTEM OUTAGES
- DATA BREACHES
- RANSOMWARE ATTACKS
- LOSS OF INTELLECTUAL PROPERTY
- FINANCIAL LOSSES
- BUSINESS INTERRUPTION
- REPUTATIONAL DAMAGE

As organizations become more digitally connected, the operational risk associated with privileged access continues to grow.

1 UNCONTROLLED ACCESS CREATES SECURITY VULNERABILITIES

Without centralized PAM controls, organizations often lose visibility over who has access to critical systems and how these privileges are being used. Over time, excessive permissions, shared administrator accounts, and forgotten credentials accumulate across the environment.

THIS LACK OF CONTROL INCREASES THE RISK OF:

- Unauthorized access to sensitive systems
- Insider threats and privilege misuse
- Credential theft and lateral movement
- Human errors caused by excessive permissions
- Compromised administrator accounts

Attackers specifically target privileged credentials because they provide direct access to critical infrastructure and valuable business data.

2 INCREASING COMPLEXITY IN MODERN IT ENVIRONMENTS

Today's organizations operate across hybrid infrastructures that combine on-premises systems, cloud platforms, SaaS applications, remote access technologies, and third-party services. Managing privileged access across these interconnected environments without centralized PAM becomes increasingly difficult.

The result is often **fragmented visibility, orphaned accounts, unmanaged credentials, and growing security blind spots.** As digital ecosystems expand, the complexity of privileged access management grows with them.

3 INCREASED RISK OF CREDENTIAL THEFT

Privileged credentials are prime targets for phishing attacks, malware, ransomware, and credential dumping. When passwords are stored in spreadsheets, local files, browser extensions, or unmanaged vaults, attackers can easily steal them.

Once privileged credentials are compromised, attackers can disable security controls, deploy ransomware, access confidential information, move laterally across systems and disrupt business operations. Organizations without PAM often discover breaches only after **significant damage has already occurred.**

4 INSIDER THREATS AND HUMAN ERROR

Not every security incident is caused by external attackers. Employees with excessive privileges can intentionally or accidentally create significant damage. Misconfigured systems, unauthorized changes, accidental deletions, or improper access approvals can all impact operational continuity.

PAM HELPS REDUCE INSIDER RISKS BY:

- Enforcing least-privilege access
- Restricting unnecessary permissions
- Monitoring privileged sessions
- Recording administrative activities (REC)
- Automating approval workflows

This significantly improves security visibility and accountability.

5 COMPLIANCE AND AUDIT CHALLENGES

Regulatory frameworks such as NIS2, DORA, GDPR, ISO 27001, and many industry-specific standards increasingly require organizations to implement strict access controls, monitor privileged activities, and maintain detailed audit trails.

Without PAM, demonstrating compliance becomes significantly more difficult.

Organizations may face failed audits, regulatory penalties, and increased legal and operational risk.

- Lack of accountability for privileged actions.
- Insufficient monitoring of sensitive systems.
- A lack of visibility into privileged activities also limits incident **response capabilities during** security investigations.

PAM IS NOT OPTIONAL. IT'S ESSENTIAL.

Protect your critical systems, reduce risk, and strengthen your security posture with Privileged Access Management.