KEEPER®

Securing Privileged Access

The Key to Modern Enterprise Defense

Introduction

In today's digitally connected world, organizations rely on a diverse network of users, applications and infrastructure to operate efficiently and securely. As that network expands across cloud, hybrid and multi-vendor environments, managing privileged access has become increasingly complex, and more critical.

At the same time, attackers continue to leverage sophisticated campaigns targeting credentials, not just to gain initial access, but to escalate privileges, bypass detection and take control of sensitive systems. This places greater responsibility on organizations to ensure that the right individuals have access to the right systems and the right data at the right time.

Privileged Access Management (PAM) helps address this challenge by enabling organizations to control, monitor and restrict access to critical infrastructure. However, as environments evolve with cloud adoption, remote work and growing automation, traditional access controls often struggle to keep pace.

To better understand how organizations are defending modern environments, Keeper Security conducted a global survey of 4,000 IT and security professionals at organizations with 250 or more employees. This report highlights their perspectives on PAM: the motivations driving adoption, the obstacles to effective deployment and the features considered essential for securing access in today's dynamic operating environments.

Why Organizations Are Turning to PAM

The primary function of PAM is to assist organizations in managing accounts with elevated access. These accounts – used by administrators, service applications and automation tools – can unlock broad system permissions. If misused or compromised, the consequences can be significant.

The Top Reasons Organizations Say They Adopted PAM

Protection against credential theft and cyber threats

69%

Secure access to cloud and hybrid environments

65%

Meeting compliance requirements

60%

Securing service accounts

54%

Providing secure remote access for third parties

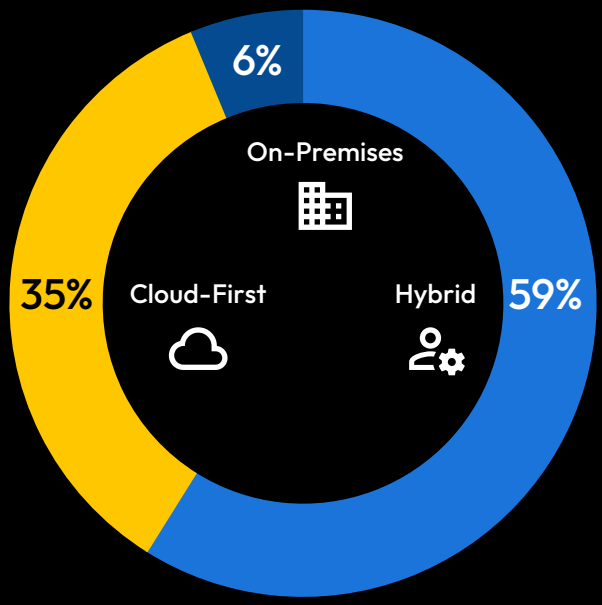
53%

These priorities reflect a strong understanding of PAM's value to the enterprises, for both security and operations.

Shifting Infrastructure, Expanding Risk

The IT landscape has changed dramatically in the past decade with new technologies introduced daily. As the traditional castle and moat approach to network security is now all but obsolete, our research shows the majority of organizations find themselves operating in hybrid environments.

This multi-environment reality increases the complexity of managing privileged access. Privileged accounts must be secured, not only on traditional on-prem servers, but also across cloud platforms, SaaS applications, developer tools and diverse remote endpoints. Each environment introduces unique risks and requires tailored controls to ensure sensitive systems remain protected. As organizations continue to embrace cloud and hybrid models, the perimeter for privileged access expands beyond the network boundary – demanding a more nuanced and adaptable approach to access management.

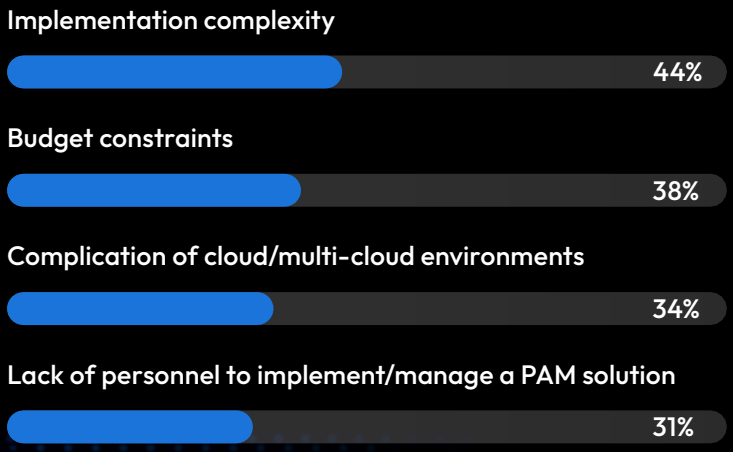


> Every system, whether in the cloud, on-prem or remote, is a potential entry point that necessitates adaptive and secure controls to defend against modern threats
>
> – **Darren Guccione**, CEO & Co-founder Keeper Security Inc.

Navigating PAM Adoption

While 86% of respondents agree that their organizations would benefit from a PAM solution, many still face practical and organizational challenges that can hinder implementation and limit its effectiveness.

Top Barriers Keeping Organizations From Fully Implementing PAM



Challenges don't necessarily end after initial deployment. Among those with some form of PAM in place, many encounter difficulties in scaling and operationalizing their solution.

Key Obstacles Reported by Organizations Post-PAM Deployment

These findings highlight the importance of choosing a PAM solution that is flexible, easy to deploy and built to integrate seamlessly with existing infrastructure. Success is also dependent on organizational alignment and ensuring the right support is in place across both technical and business teams.

What Effective PAM Looks Like

When implemented effectively, PAM delivers measurable security and operational gains across the enterprise, with users reporting better data protection, efficiency and reduced cyber incidents, among other benefits. Organizations that have adopted PAM report significant improvements well beyond improved access controls.

According to respondents who have fully implemented PAM

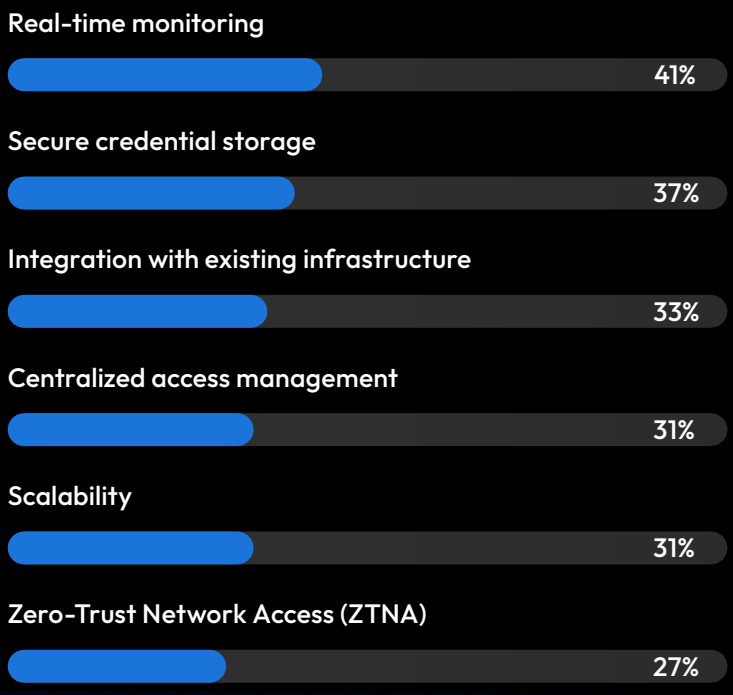
- **53%** Improved protection of sensitive data
- **50%** Saw greater efficiency in managing privileged credentials
- **49%** Enhanced security for remote connections to infrastructure
- **49%** Reduced security incidents tied to privilege misuse
- **48%** Gained better visibility and control over privileged accounts
- **47%** Reduced IT help desk burden tied to manual credential management
- **47%** Strengthened their compliance posture
- **40%** Streamlined access request and approval workflows

These outcomes demonstrate that modern PAM doesn't just mitigate risk – it improves agility, reduces overhead and helps organizations align security with operational goals.

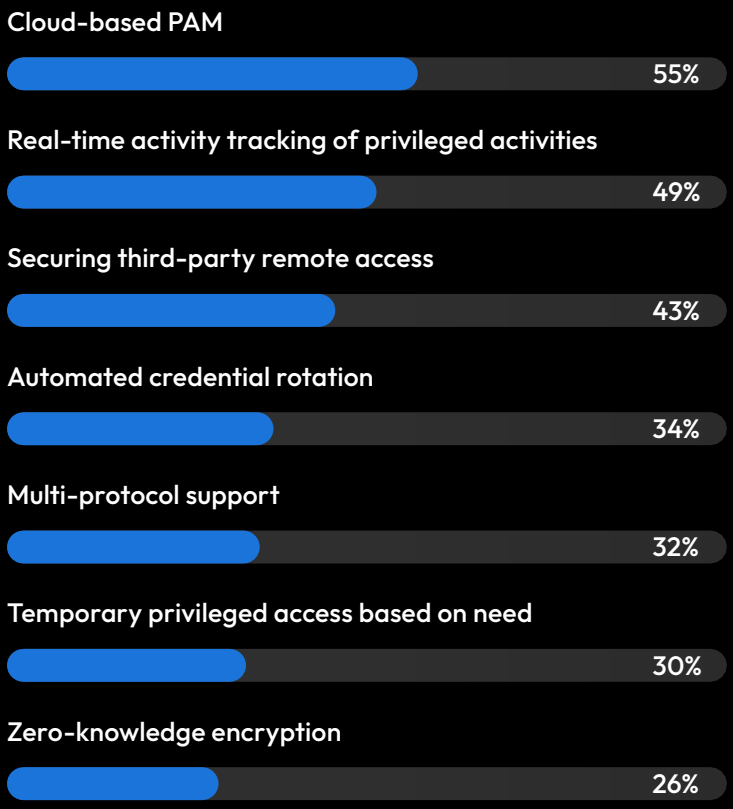
PAM Features That Matter Most

As organizations grow more cloud-centric, they need features that reflect modern workflows and architectures. Among those using PAM in cloud and hybrid environments, the most valued capabilities include:

Top Cloud/Hybrid Environment Features



When asked to name the most critical PAM features overall, respondents pointed to



These findings reinforce a shift toward cloud-native, flexible platforms that offer strong security without sacrificing usability. In contrast, traditional on-premises PAM solutions require significant upfront investment, while lacking the scalability and flexibility of cloud-based alternatives, making them less suited to cloud and hybrid environments.

Why Education Still Matters

Technology ≠ Awareness

Even with PAM tools in place, human factors can introduce risk. A strong security posture requires both the right systems and the right behaviors.

Organizations audit privileged accounts monthly or more often

37%

Audit annually or less, risking standing permissions and unchecked access

13%

Non-PAM users rely on shared spreadsheets for storing credentials

8%

Still have hardcoded credentials

5%

Have no formal credential management system in place

5%

Without regular training, strong access policies and cultural reinforcement, even well-resourced organizations may revert to risky practices. Educating teams on why certain behaviors, like hardcoding credentials or skipping regular audits, create risk is essential to widespread adoption. When people understand not just the “how” but the “why” of secure access management, they’re more likely to use PAM tools effectively.

Aligning technology with education helps close the gap between control in theory and security in practice.

What's Next for PAM?

As security threats evolve, so too must the tools used to defend against them. IT and security leaders around the globe identified the following trends as important to the future of PAM:

AI-powered security analytics to detect anomalies in privileged access

72%

Wider adoption of cloud-native PAM solutions

60%

Simplified user experiences to reduce friction and improve adoption

56%

Stronger integration with zero-trust architectures

56%

This points to a future where PAM is not only more powerful, but also more accessible – enabling organizations of all sizes to safeguard privileged access and adopt emerging technologies without overburdening teams.

Final Thought: Control Builds Confidence

In a security landscape where identities outnumber devices and access can be granted from anywhere, at any time, controlling privileged accounts is foundational to protecting critical systems and data. Privileged access management enables organizations to shift from reactive defense to proactive control. By combining credential storage, role-based access and real-time monitoring, modern PAM solutions help reduce risk and improve operational resilience.

Methodology

This research was conducted by Keeper Security in partnership with the independent research firm OnePoll. The study surveyed 4,000 IT and security decision-makers at organizations with 250 or more employees across the United States, United Kingdom, France, Germany, Japan, Australia, New Zealand and Singapore. Fieldwork was conducted online between March 25 and April 11, 2025.

> Access can happen anywhere and PAM ensures it happens securely. It's how organizations manage, monitor and protect what matters most.
>
> – **Darren Guccione**, CEO & Co-founder Keeper Security Inc.

About Keeper Security

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organizations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access, endpoint privilege management and remote browser isolation. By combining these critical identity and access management components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met. Learn how Keeper can defend your organization against today's cyber threats at KeeperSecurity.com.