Prepared for

KEEPER

Beyond the Vault:

Elevating Privileged Access Management in the Modern Enterprise

July 2025 EMA White Paper
By **Ken Buckler, CASP;** Research Director
Information Security, Risk, and Compliance Management

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Introduction

In an era of relentless cyber threats and rapid digital transformation, privileged access management (PAM) emerged as a foundational security discipline. Today's enterprises demand more than credential vaulting; they require a comprehensive framework that protects critical assets, enforces least-privilege access, and integrates seamlessly across on-premises and cloud environments.

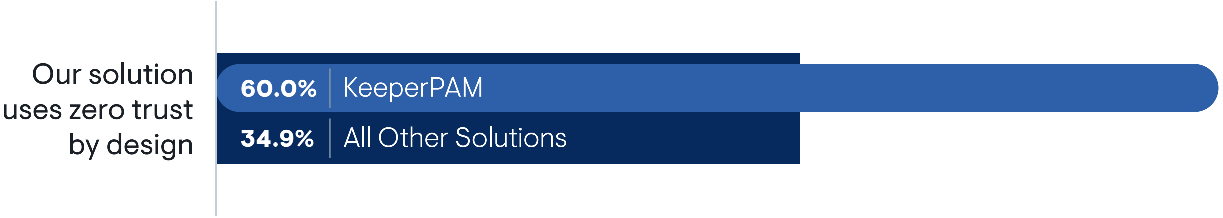
Effective PAM begins with robust identity-proofing and multi-factor authentication to combine hardware tokens, mobile approvals, and biometric checks backed by end-to-end encryption and zero-knowledge security. Fine-grained, role-based controls and just-in-time provisioning within a zero-trust architecture ensure that users receive the minimum privileges necessary, dramatically reducing breach impact. Simultaneously, audit logs capture every privileged session, from commands executed to visual replays and session duration. The audit logs then feed automated compliance engines that align practices with HIPAA, SOX, and PCI DSS standards, while recertification campaigns eliminate orphaned or excessive accounts.

Seamless integration with cloud services and existing tools is essential. Credential injection into scripts, pipelines, and remote-access gateways maintains user productivity without sacrificing oversight. Advanced behavioural analytics and agentic AI then elevate PAM to an active defence. Real-time alerts and actions can terminate threats and revoke privileges instantly. Extending these controls to third parties through time and device-bound sharing, automatic password rotation, and strict approval workflows further mitigates contractor and supply chain risks.

In this white paper, we will examine the challenges organisations face in fulfilling these PAM priorities and evaluate how Keeper Security's KeeperPAM platform stacks up against the wider industry.

Zero Trust by Design

Zero Trust and Zero Knowledge



Embedding zero-trust principles from the ground up is no longer optional for privileged access management – it's imperative. A "zero trust by design" framework treats every request for elevated privileges as inherently untrusted, requiring continuous verification, strict segmentation, and least-privilege enforcement. By shifting from static, all-powerful credentials to ephemeral, context-aware access tokens, organisations can dramatically reduce the attack surface and limit lateral movement in the event of a breach. With zero trust by design, every access decision considers user identity, device posture, location, time of day, and behavioural context. Just-in-time provisioning ensures that privileged rights are granted only for the exact duration needed and automatically revoked afterward. Fine-grained, role-based access controls minimise over-permissioning, while multi-factor authentication and continuous session monitoring guard against credential compromise and insider threats.

"[When it comes to privileged access management, our priorities are] integration with zero trust architecture and continuous validation framework."
- IT Director, 500-749 employees, using KeeperPAM

Keeper's zero-knowledge approach to product design further enhances this approach, which ensures that all encryption and decryption happen locally on your device – only ciphertext ever travels to Keeper's cloud. A master password and any derived key material never leave a chosen device, meaning Keeper's servers cannot access or store unencrypted data or the keys that protect it. Even if their infrastructure were breached, attackers would only obtain an unreadable string of characters, guaranteeing true end-to-end confidentiality.

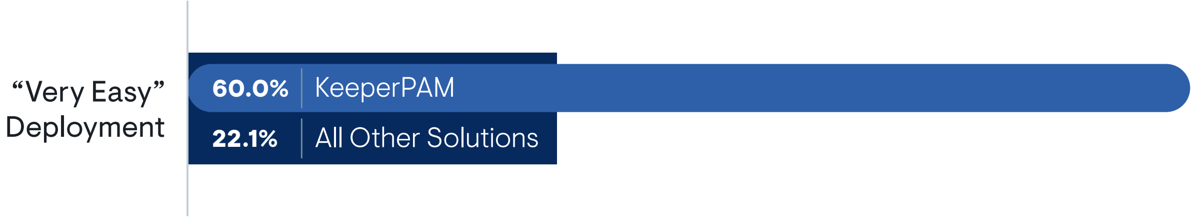
Survey data underscores the impact of this approach: 60% of Keeper Security users regard their PAM implementation as "zero knowledge" and "zero trust by design," compared with just 34.9% of users of all other vendors. This gap reflects a proactive security posture – Keeper customers emphasise continuous validation, elimination of shared accounts, and automated privilege lifecycle management – versus a more reactive, compliance-driven mindset elsewhere.

Zero-trust PAM also accelerates compliance and audit readiness. Every privileged session is logged end to end – complete with commands executed, visual replay, and duration metrics – feeding automated compliance engines aligned to HIPAA, SOX, and PCI DSS requirements. In practice, organisations that bake zero trust into their PAM architectures not only strengthen their defences, but also streamline operations, reduce costs associated with orphaned accounts, and demonstrate measurable improvements in breach containment.

Ultimately, Keeper's zero-knowledge approach and zero-trust design transforms privileged access from a potential liability into a controlled, verifiable process – one that adapts in real time to evolving risks and ensures that critical systems remain secure, compliant, and resilient.

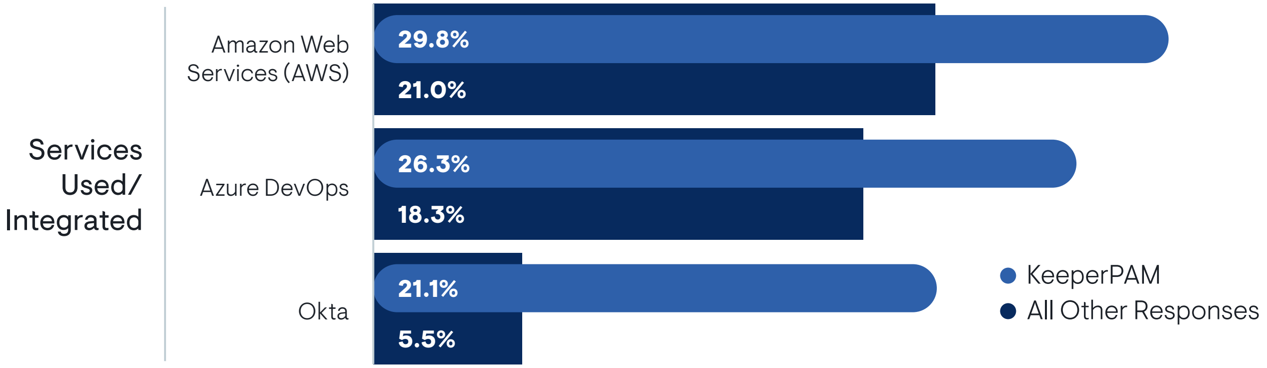
Ease of Deployment, Configuration, and Integrations

There is no "Easy Button," but Keeper Comes Close



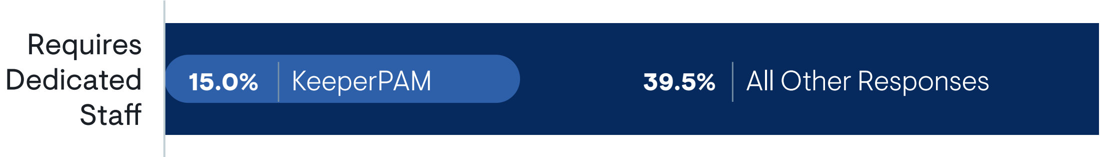
Ease of deployment, configuration, and integration can make or break a PAM project's ROI. According to EMA's survey, 60% of Keeper Security customers rated initial deployment as "very easy," compared to just 22.1% of users on other PAM platforms. Conversely, 10% of all other solutions' customers called deployment "somewhat difficult" or "very difficult," a pain point entirely absent among KeeperPAM users. Migrating legacy, on-prem PAM tools to the cloud still trips up 39% of organisations – a complexity Keeper's cloud native architecture sidesteps. Integration hurdles plague 11% of non-Keeper deployments, in which proprietary connectors and manual scripts are often required to tie into SIEM, ticketing, or DevOps pipelines. KeeperPAM's modular APIs, plug-and-play connectors, and seamless cloud orchestration accelerate time to value and minimise operational friction.

Plays Well with Others



Seamless integrations are a cornerstone of any modern PAM strategy, and Keeper leads the pack here as well. Out-of-the-box connectors and APIs enable rapid, bidirectional integration with core platforms – whether you're spinning up EC2 instances in Amazon Web Services, automating pipelines in Azure DevOps, or centralising authentication through Okta. KeeperPAM users report far higher adoption of these integrations compared to other PAM solutions, eliminating the need for time-consuming custom scripting or manual connector maintenance. By embedding privileged credential injection directly into your CI/CD workflows, cloud consoles, and identity providers, KeeperPAM minimises friction, drives developer productivity, and ensures secrets remain protected at every layer.

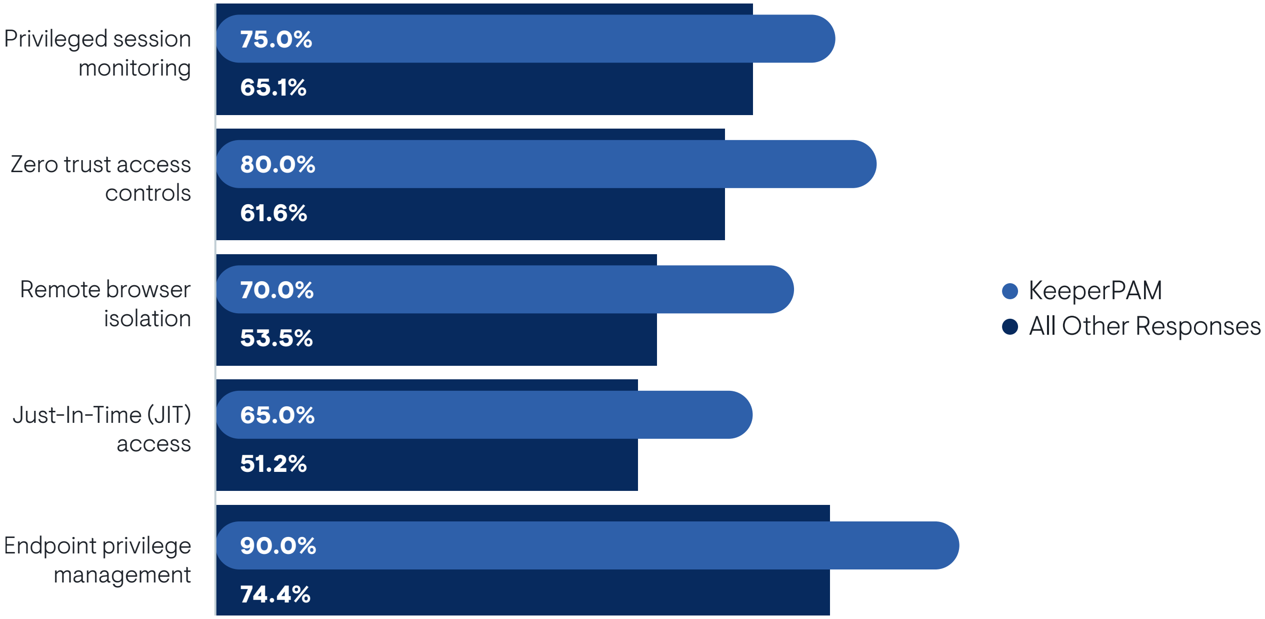
Doing More with Less Staff



Staffing requirements for PAM implementations vary widely by platform. Only 15% of Keeper Security customers report needing dedicated personnel to manage deployment, configuration, and integration, thanks to Keeper's intuitive user interface, guided setup wizards, and comprehensive documentation. By contrast, 39.5% of organisations using other PAM solutions require one or more full-time administrators to keep their environments running. Those teams often juggle complex on-prem appliance maintenance, bespoke scripting, and manual connector updates, driving up headcount and stretching existing IT resources. Keeper's cloud native design and self-service tooling minimise reliance on specialised skill sets. Administrators can onboard new systems, adjust privilege policies, and integrate with SIEM or DevOps pipelines without heavy customisation. Ultimately, lower staffing overhead translates into faster rollouts and more sustainable, affordable long-term operations.

Beyond Password and Secrets Management

Advanced PAM Capabilities



Modern PAM demands far more than vaulting credentials – it requires a rich feature set that actively defends, monitors, and adapts to evolving threats. KeeperPAM stands out by delivering advanced capabilities many legacy vendors simply don't offer or implement at scale. Privileged session monitoring, for example, is critical for capturing every keystroke, command, and visual replay of high-risk activities. Keeper customers leverage this feature more frequently than peers, enabling real-time threat detection and forensic analysis.

"Using PAM strengthens our data integrity and our reputation."
- VP Development/Engineering, 1,000-2,499 employees, using KeeperPAM

Zero-trust network access extends least-privilege principles beyond passwords to every access request. Keeper embeds contextual policy checks – device posture, location, time, and behavioural baselines – ensuring that even authenticated sessions remain under continuous scrutiny. This granular gating of privileged operations dramatically reduces the potential window of exposure compared to static, all-or-nothing models.

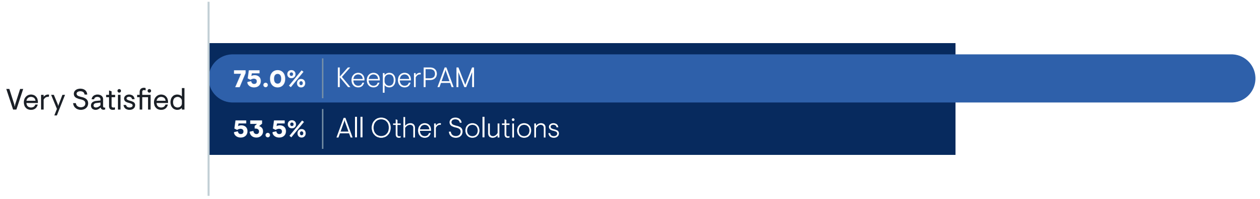
Remote browser isolation (RBI) is another area where Keeper outpaces competitors. By proxying administrative consoles through isolated, secure browsers, organisations eliminate direct endpoint access for third parties and contractors, effectively quarantining potential malware or credential theft. Few other PAM solutions integrate RBI so seamlessly, instead forcing manual workarounds that undermine both security and user experience.

Just-in-time provisioning and automated privilege lifecycle management round out Keeper's advanced toolkit. Temporary, time-bound elevation prevents standing high-privilege accounts from accumulating, while automatic deprovisioning and recertification campaigns ensure adherence to compliance mandates without manual overhead. Finally, endpoint privilege management – removing local admin rights while granting scoped privileges on demand – protects against both external attacks and insider misuse.

By looking beyond passwords and secrets, Keeper transforms PAM into an active defence platform: one that anticipates attacks, enforces zero trust at every layer, and delivers the advanced controls today's complex environments demand.

Overall Satisfaction

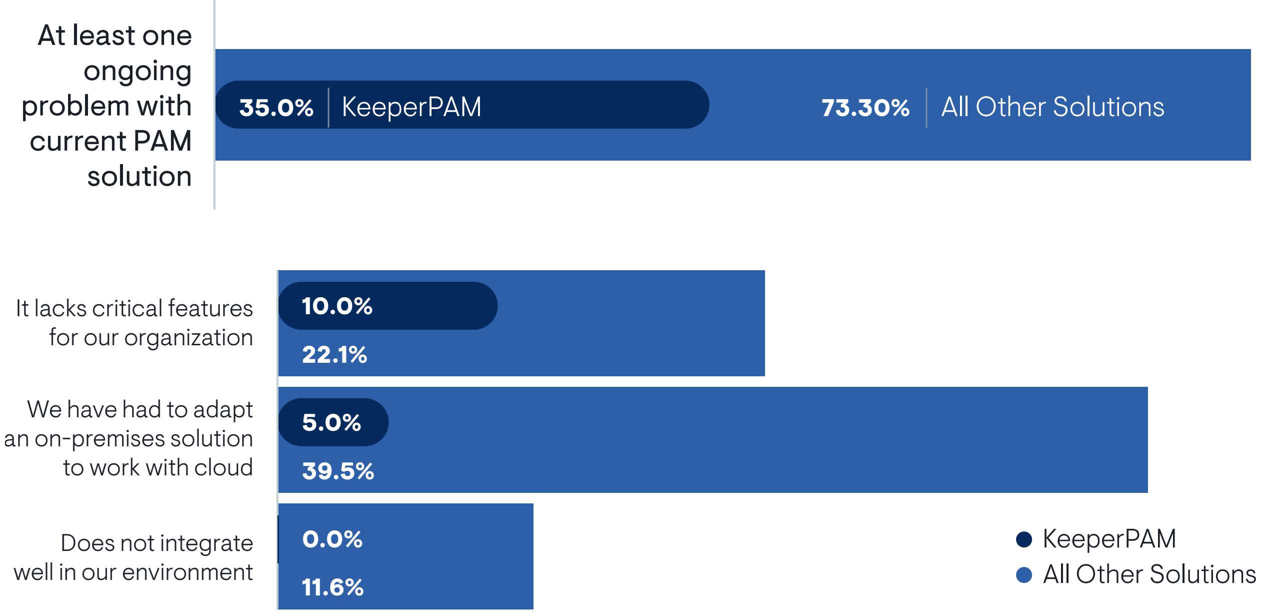
Does Your PAM Solution Weather the Storm?



Customer satisfaction is the ultimate barometer of a PAM solution's value and longevity. When 5% of organisations using other platforms are actively searching for a replacement, it signals critical gaps in reliability, usability, and/or support. By contrast, no Keeper Security users reported plans to ditch their PAM tool, underscoring Keeper's ability to meet evolving security and operational needs.

Moreover, 75% of Keeper customers describe themselves as "very satisfied" overall – far outpacing the 53.5% "very satisfied" rating among users of competing vendors. High satisfaction correlates with faster adoption, more effective risk reduction, and lower total cost of ownership, as pleased teams invest in deeper integrations and more advanced features. In a landscape where privileged access is continually targeted, choosing a platform that delights its users is not just nice to have – it's mission-critical.

Features and Integrations are Critical Pain Points



Despite their critical role, many PAM deployments struggle with persistent roadblocks. Seventy-three percent of organisations using non-Keeper solutions report at least one significant challenge, compared to just 35% of Keeper customers. Common pain points include missing essential capabilities – forcing teams to bolt on third-party tools – poor integration into existing infrastructure, and the headache of retrofitting on-premises platforms to support cloud environments. KeeperPAM users experience these issues far less frequently, thanks to its comprehensive feature set, native cloud-first architecture, and extensive library of connectors. By minimising gaps in functionality and simplifying hybrid deployments, Keeper not only accelerates time to value, but also reduces the burden of troubleshooting and workarounds, freeing security teams to focus on proactive risk mitigation rather than firefighting legacy limitations.

Better Solution, Better Priorities

Other PAM Implementations Fail to Live Up to Potential

Priority Area	Keeper Customers	Other PAM Solutions
Authentication	Continuous, zero trust	Role-based, MFA
Credential Management	Eliminate static/shared credentials	Basic control and monitor access
Training	Explicit priority	Not emphasized
Automation	Risk mitigation focus (because the process is already efficient)	Process efficiency focus
Compliance	Credential misuse & audit focus	Minimum regulatory compliance

Keeper Security empowers organisations to move from a maintenance-mode, compliance-driven stance to a proactive, security-first posture. KeeperPAM customers eliminate static and insecurely shared credentials through a zero-knowledge vaulting engine that issues ephemeral, least-privilege secrets, dramatically reducing both external attack vectors and insider abuse compared to traditional vault-only approaches. Continuous authentication and zero-trust access controls – including device health checks, geolocation, and behavioural analytics – ensure that every session remains under scrutiny long after a one-time MFA prompt, making it virtually impossible for attackers to exploit stolen credentials undetected. Keeper's risk-centric automation tackles the entire privilege lifecycle – from discovery and onboarding to automatic rotation and deprovisioning – preventing credential sprawl and orphaned accounts, whereas many other solutions simply automate approval workflows or compliance reporting. Importantly, Keeper customers explicitly integrate staff training and awareness as a core security control, recognising that human factors are as crucial as technology in driving adoption and preventing risky workarounds.

"I believe constant monitoring of privileged accounts helps me sleep better at night."
– VP Development/Engineering, 2,500-4,999 employees, using KeeperPAM

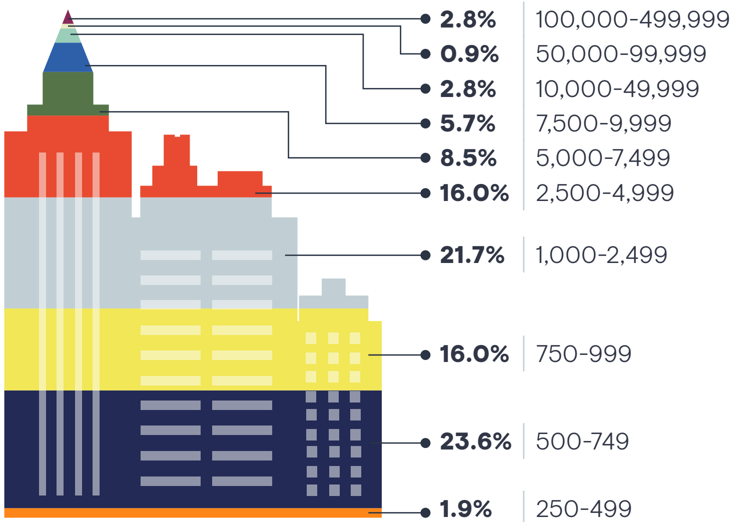
In contrast, users of other PAM tools often emphasise traditional controls, such as role-based access, post-access auditing, and operational efficiency, reflecting a reactive mindset that struggles with feature gaps, brittle integrations, and the complexity of retrofitting on-premises solutions for the cloud. Keeper's cloud native architecture and extensive library of plug-and-play connectors eliminate these headaches, enabling rapid integration with SIEM platforms, identity providers like Okta, and CI/CD pipelines in AWS or Azure DevOps. Advanced capabilities including privileged session monitoring, remote browser isolation, just-in-time provisioning, and endpoint privilege management are all native to Keeper, reducing deployment friction and ongoing staffing demands.

By combining these next-generation features with a seamless user experience, Keeper equips security teams to anticipate threats, enforce continuous protection, and truly harden their privileged access environment.

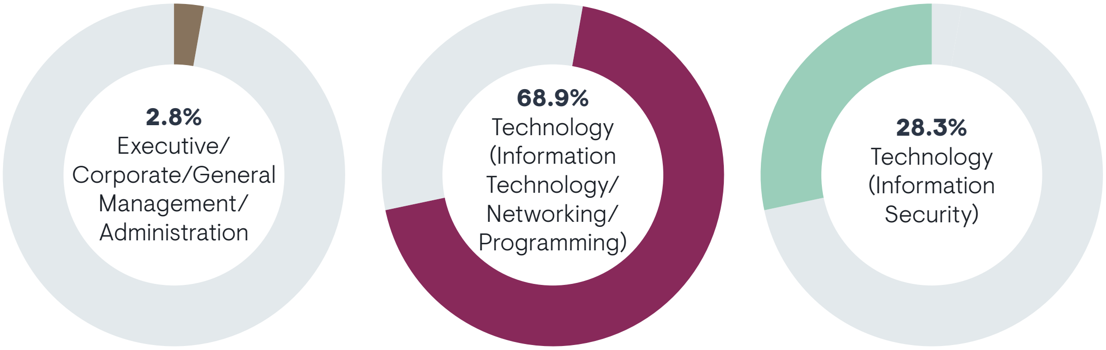
Methodology

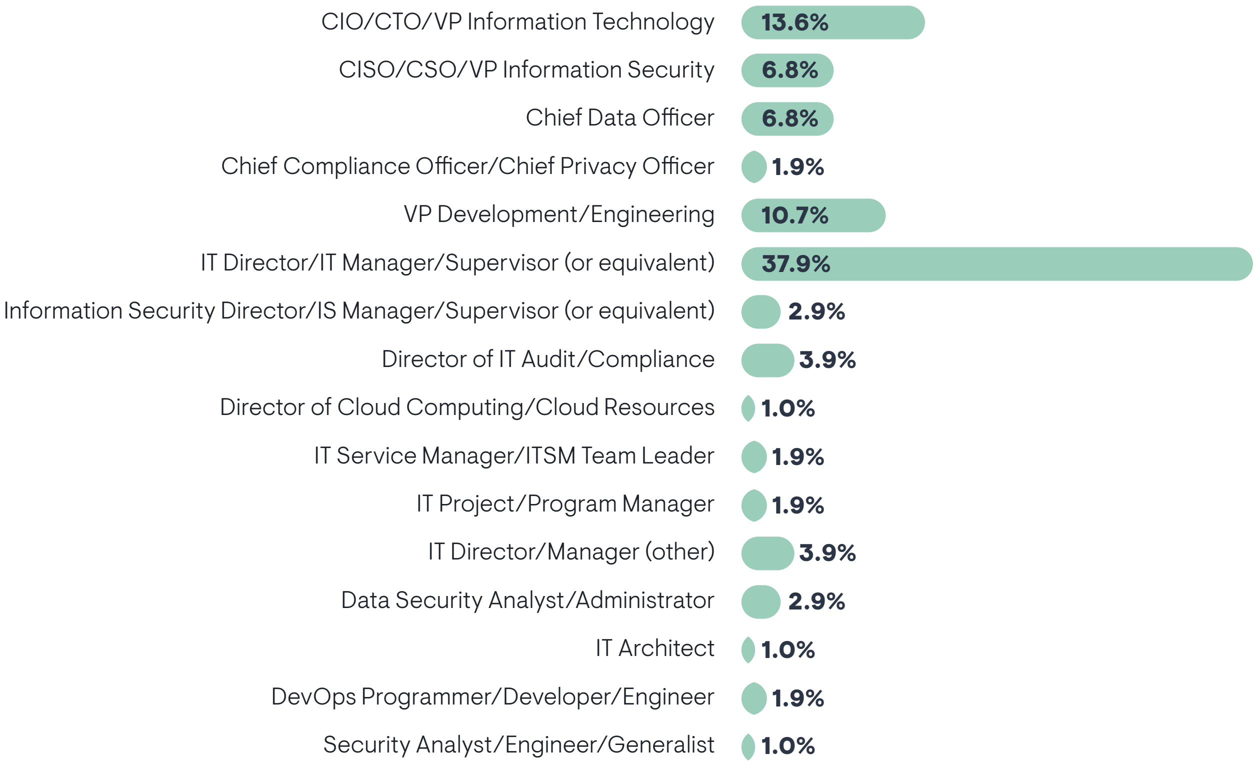
Total of 106 professionals using BeyondTrust, CyberArk, Delinea, Devolutions, Keeper Security, ManageEngine, One Identity, or StrongDM as of June 2025. All data in this white paper is based upon the survey responses and open-ended answers regarding privileged access management priorities and challenges in the enterprise.

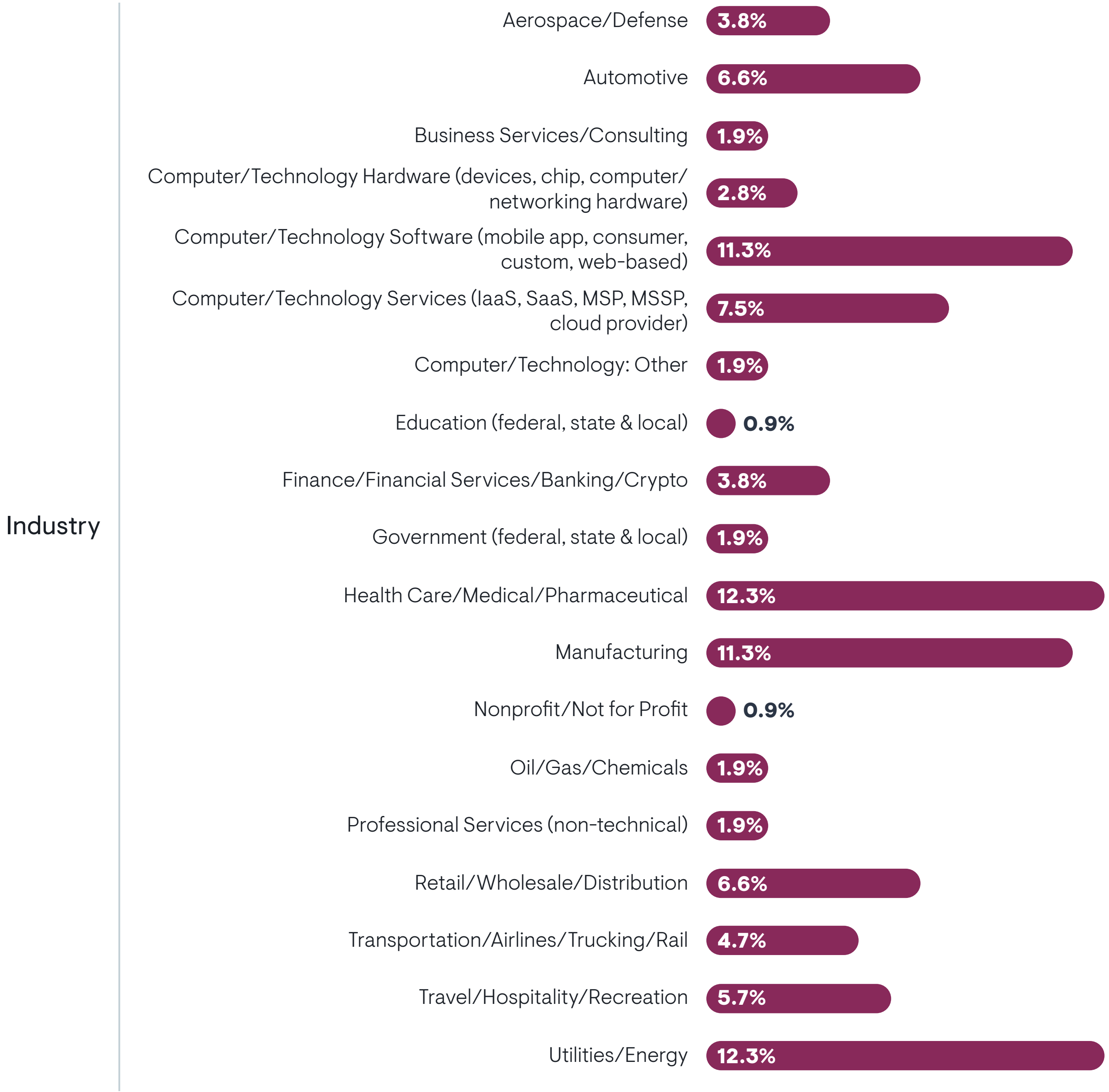
Organization Size



Respondent Role




CIO/CTO/VP Information Technology
13.6%
CISO/CSO/VP Information Security
6.8%
Chief Data Officer
6.8%
Chief Compliance Officer/Chief Privacy Officer
1.9%
VP Development/Engineering
10.7%
IT Director/IT Manager/Supervisor (or equivalent)
37.9%
Information Security Director/IS Manager/Supervisor (or equivalent)
2.9%
Director of IT Audit/Compliance
3.9%
Director of Cloud Computing/Cloud Resources
1.0%
IT Service Manager/ITSM Team Leader
1.9%
IT Project/Program Manager
1.9%
IT Director/Manager (other)
3.9%
Data Security Analyst/Administrator
2.9%
IT Architect
1.0%
DevOps Programmer/Developer/Engineer
1.9%
Security Analyst/Engineer/Generalist
1.0%


Industry
Aerospace/Defense 3.8%
Automotive 6.6%
Business Services/Consulting 1.9%
Computer/Technology Hardware (devices, chip, computer/networking hardware) 2.8%
Computer/Technology Software (mobile app, consumer, custom, web-based) 11.3%
Computer/Technology Services (IaaS, SaaS, MSP, MSSP, cloud provider) 7.5%
Computer/Technology: Other 1.9%
Education (federal, state & local) 0.9%
Finance/Financial Services/Banking/Crypto 3.8%
Government (federal, state & local) 1.9%
Health Care/Medical/Pharmaceutical 12.3%
Manufacturing 11.3%
Nonprofit/Not for Profit 0.9%
Oil/Gas/Chemicals 1.9%
Professional Services (non-technical) 1.9%
Retail/Wholesale/Distribution 6.6%
Transportation/Airlines/Trucking/Rail 4.7%
Travel/Hospitality/Recreation 5.7%
Utilities/Energy 12.3%

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com** 4577.081425-UK-EN