KPMG

Privileged identity security

The evolution of PAM and its modern relevance

The landscape of **privileged access management (PAM)** has notably evolved in recent years. The traditional definition of what constitutes 'privileged access' has vastly expanded, requiring new capabilities to protect systems, applications, and identities. To protect critical organizational assets, PAM programs should evolve in parallel. To do so, it's essential to first understand some of the core drivers of this shift:

Key change drivers:

1. **New Identities**
   A rise in new human, machine, and third-party identities supporting organizational IT and developer capabilities introduce complexity to the overall identity landscape, emphasizing the need for modern privilege controls
2. **Expansion of cloud resources**
   Cloud adoption has fundamentally transformed operational norms. Privileged accounts were previously restricted to on-prem systems bound by clear network perimeters. These perimeters are now fluid, with privileged access extending beyond conventional domains to dynamic workloads, databases, and containers, growing the attack surface as a result.
3. **Artificial Intelligence (AI)**
   AI is at the forefront of next-gen digital capabilities. The swift rate of change propelled by AI is not only driving technological progress but is intensifying the need for robust access controls to maintain integrity of IT assets amidst an expanding threat landscape.
4. **New attack vectors**
   Evolving adversary capabilities and methodologies are largely due to sophisticated tools and technologies that call for more robust counteractions.

Considering these catalysts, the traditional approach to PAM – while still critical on its own – must evolve to address the modern technology and threat landscape.

Industry insights

#1	Machine identities are the #1 driver of identity growth[1]
61%	Organizations that define a privileged user as human-only [1]
84%	Of organizations will use three or more Cloud Service Providers [1]
94%	Organizations that experienced an identity related breach at least once [1]
68%	Of breaches involved a human element [3]
$4.88M	2024 global average total cost of data breach, 10% increase from 2023 [2]
292	Average days to identify and contain breaches involving stolen credentials, the longest of any attack vector [2]

1 = CyberArk 2024 Identity Security Threat Landscape Report
2 = IBM Security 2024 Cost of a Data Breach Report
3 = Verizon Data Breach Investigations Report

Common PAM challenges in a modern enterprise

01

Program scope

Privileged access and identity security programs should be expanded to secure critical environments, such as cloud application and workloads. This often includes the deployment of new capabilities across complex ecosystems.

02

SaaS migration

Migrating to SaaS solutions and leveraging modern session management capabilities can help reduce footprint and scale faster. However, intricate planning and execution is needed to ensure a seamless transition.

03

Artificial intelligence

AI can help automate account lifecycle management, discovery, onboarding, certifications, and more. The introduction of AI does not come without major considerations such as privacy, security, and compliance.

04

Expansion of identities

Extending solutions to new identities including cloud operations, developers, and privileged business users should be methodical to garner quick-wins and ensure high-priority use cases are addressed.

05

Implementation complexity

Managing multiple solutions across different vendors introduces complexity that can hinder progress and limit the holistic coverage of identity security controls.

While traditional PAM capabilities remain critical to the enterprise, the scale and complexity of modern ecosystems introduce challenges that call for a more expansive approach. As this landscape evolves, organizations and program leaders can reimagine their ways of working and capabilities to safeguard their people, processes, and technologies. Modern PAM presents new opportunities to improve security posture while simplifying operations.

A new era of privilege controls

AI-Driven behavior analysis & AI Agents

It is increasingly common for modern tooling to leverage AI to identify patterns that deviate from baselines and AI agents that perform various tasks. Organizations should be ready to embrace AI-driven solutions and agents, as they present an opportunity to enable a view of the privilege landscape and introduce actionable insights from various datapoints. At the same time, organizations should be ready to address identity security risks posed by AI Agents.

Just-in-time & Ephemeral access

PAM solutions now provide dynamic privilege controls to enable enforceable zero standing privilege and just-enough-access (ZSP & JEA). Ephemeral access, which grants temporary, short-lived permissions within APIs and source code, is also a key component. These dynamic controls have become critical elements in addressing the increasingly fluid nature of access and mitigating risks.

Integrations & scalability

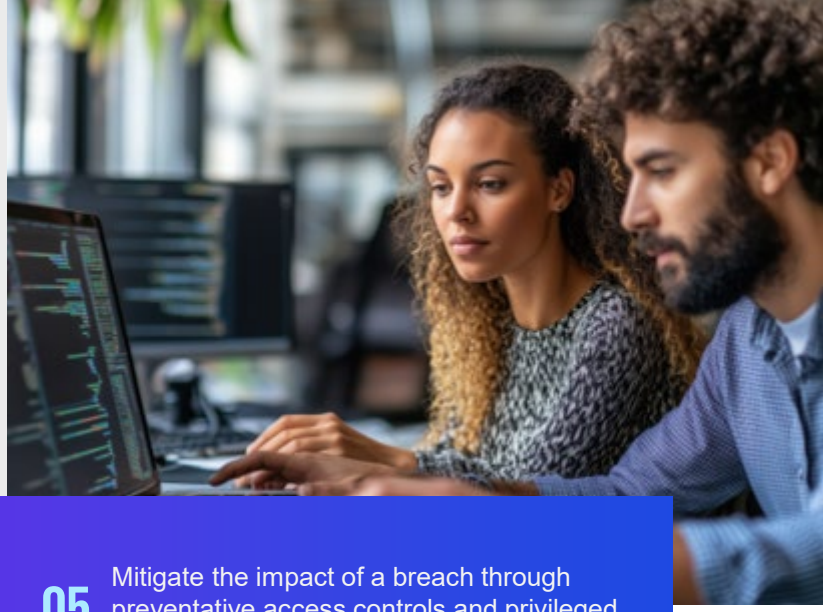
Orienting your organization's program to recognize the increased footprint cloud-based services and third-party integrations is critical in protecting high-value assets. IT leaders should consider shifting their approach from a segmented, on-premises focused mindset to a unified strategy that spans cloud, on-prem, and hybrid systems.

Rapid automation

Modern PAM approaches often involve workflows automation to eliminate overhead associated with granting, modifying, and removing access rights. Automation helps streamline operations, mitigate human error, and swiftly adjust to growing business needs. It's become apparent that these features are not merely add-ons but are a core component of a mature PAM program.

Modern privileged access – what does "good" look like?

At the core of this evolution is a transition from traditional credential vaulting controls to dynamic, zero standing privilege, and just-enough-access models, all while continuing to extend compensating controls across the broader IAM ecosystem. By partnering with CyberArk, KPMG can assist organizations to elevate their PAM programs across people, processes, and defining how to maximize value from technology investments.



01 Define a clear strategy for implementing and enhancing privilege controls based on organizational processes, technologies, and business goals.

02 Enable insight into critical organizational assets, identities, and data.

03 Manage privileged access risk across multiple enterprise ecosystems, platforms, and systems.

04 Efficient and thorough discovery, cataloging, and classification of privileged identities.

05 Mitigate the impact of a breach through preventative access controls and privileged entitlement management.

06 Adapt to new and evolving compliance regulations and requirements.

07 Evolve with changing business requirements and objectives.

Journey to transformation success

Navigating the intricacies of the modern PAM landscape necessitates a well-considered transformation. With KPMG's guidance, your organization can confidently embrace the latest evolutions.

Deep understanding of privileged access objectives

Understanding the appropriate risk-based requirements for privileged access management tailored to your specific technology stack, organization, and industry.

Technology enhancement

Making PAM a reality starts with gaining visibility of critical assets, systems, and identities by utilizing a technology-enabled approach to automate discovery and generate prioritized, actionable recommendations.

Alignment with changing business needs

An effective modern PAM program should be made in partnership with the overall business vision, tailored to organizational objective, and aligned to broader IT goals.

Tailored capability framework

Privileged access is not one-size-fits-all – it is crucial to tailor your PAM capabilities and controls to meet your specific needs and align with organizational processes, technologies, and operating models.

KPMG services across modern PAM features

KPMG's privileged access management services focus on protecting access to all identities as they access critical digital assets and infrastructure. In our experience, PAM programs should encompass and address a combination of identity security challenges from governance and strategy to monitoring and end user training.

Strategy & Governance	Establish a privileged access management strategy to secure privileged identities from internal and external threat vectors.	**KPIs & Adoption Strategy** Custom Key Metrics Reporting Capabilities Adoption Strategy
Discovery	Discover and classify identities based on risk-level, priority, system criticality, and other organizational factors.	**Infrastructure Scanning** Automated Discovery & Onboarding Cloud Entitlement & Account Scanning
Identity Management	Formally define policies, roles, and responsibilities for managing privileged access.	**PAM RBAC & ABAC Policies** Automated Workflows & Processes Identity Provisioning & Lifecycle Management
Protection	Implement runtime controls to secure privileged identities, their credentials, and their users.	**Zero Standing Privilege & Just-in-Time Access** Automated Credential Rotation MFA & Conditional Access Secrets Management Endpoint Privilege Management
Monitoring	Monitor for privilege misuse and analyze user activities for rapid, actionable alerts.	**Session Isolation & Recording (Multi-Environment)** Activity Auditing & Alerts Third-Party SIEM Integration
Training & Awareness	Educate stakeholders on the risks of unmanaged privileged access and benefits realized as part of a successful PAM program.	**Technical Training & Resources**

Why KPMG?

01

Global footprint

KPMG employs more than 219,000 professionals in 147 countries and territories. Our team of cybersecurity professionals have extensive knowledge and offer a global multidisciplinary view of cyber risk, helping drive security throughout your organization.

02

Strategic ecosystems

Leveraging our experience with the CyberArk suite of products, KPMG brings market-leading offerings including an automated and integrated approach for securing privileged accounts and digital assets for our clients.

03

Experience deploying PAM programs

KPMG became a Platinum Partner with CyberArk in 2011 and the 2023 recipient of the CyberArk Global Systems Integrator (GSI) Partner of the Year award. With over 14 years of experience delivering 50+ PAM transformation engagements, our team brings deep subject matter experience across domains, including strategy, implementation, operations automation, and managed services.

04

Cross-skilled teams

The KPMG Cyber team consists of over 6,000 professionals globally including more than 100 individuals trained on CyberArk technologies. These professionals bring a distinctive combination of technical know-how, business knowledge, and creative problem solving to help defend and advance businesses.

Contact us

Hemal Shah
IAM Offering Lead
Cybersecurity & Tech Risk
E: hpshah@kpmg.com

Adam White
PAM Offering Lead
Cybersecurity & Tech Risk
E: arwhite@kpmg.com

Mike Hatjiyannis
IGA Offering Lead
Cybersecurity & Tech Risk
E: mhatjiyannis@kpmg.com

Stephen Ballard
Manager
Cybersecurity & Tech Risk
E: stephenballard@kpmg.com

Learn about us: **kpmg.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.