SACR®

THE EVOLUTION OF THE PRIVILEGED ACCESS MANAGEMENT (PAM) MARKET & THE NEW COMPETITIVE LANDSCAPE

FRANCIS ODUM

PO SECURITY

Research

We explore the newest frontiers of cybersecurity.

Whether you're looking at emerging vendors, evolving threats, or shifting architectures, our timely, opinionated insights help modern security leaders make smarter, faster decisions.

About Software Analyst Cybersecurity Research

SACR is a modern research and advisory firm built for today's cybersecurity leaders. We deliver in-depth, timely analysis across SOC operations, Identity, Network, Cloud, Application Security, Data, and AI Security; equipping CISOs, security teams, founders, investors, and practitioners with the insight they need to navigate high-stakes decisions.

With an engaged community of over **80,000** readers and followers, SACR connects with a global network of cybersecurity decision-makers and innovators. Our access to leaders across categories and industries gives us a direct line to the conversations shaping the market. By pairing these insights with rigorous technical analysis and continuous market tracking, we produce research that is both data-driven and grounded in the realities of modern security operations.

Whether you're seeking clarity on emerging technologies, evaluating vendors, or tracking market shifts, SACR delivers trusted, independent research designed to help you see clearly and decide with confidence.

Author

- **Francis Odum** is the Founder/CEO of the Software Analyst Cyber Research, where he leads the firm's research and engagement with cybersecurity leaders.

Table of Contents

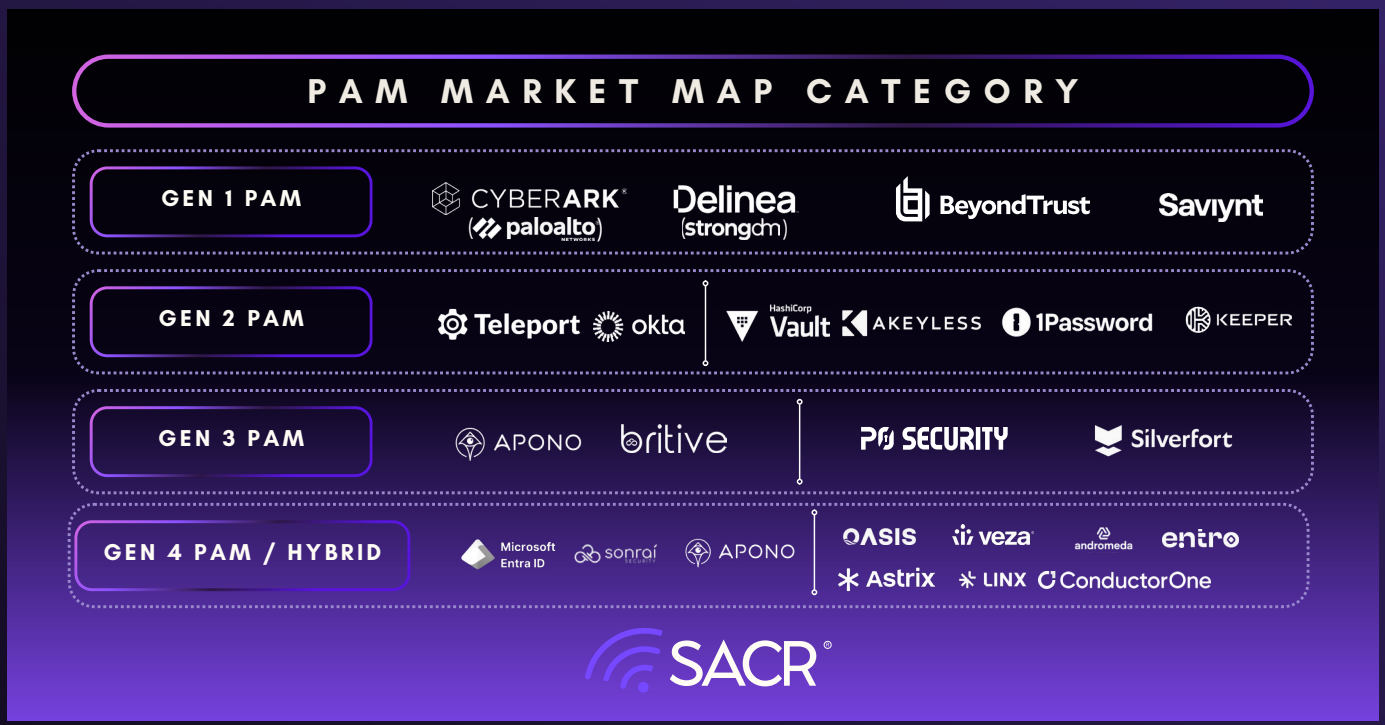
Introductory Blurb

As Identity becomes central to agentic security, Privileged Access Management (PAM) is undergoing a structural shift. It is currently an underlooked category which deserves more attention as we prepare for an identity centric agentic stack.

Our opinion is that privileged access will be central to how humans, agents, and machines (NHIs) evolve within the future identity stack. The acquisitions we have witnessed over the past 12 months have been reinforced by decisive market activity. Palo Alto Networks' $25B acquisition of CyberArk reflects a clear recognition that identity and privilege are now foundational to platform agentic security. Palo Alto Networks had many opportunities across this ecosystem, but chose to go with the PAM route.

Subsequently, we've seen other minor acquisitions such as Okta's acquisition of Axiom. We also saw Delinea's acquisition of StrongDM two weeks ago signal a move toward just-in-time, runtime-aware access for cloud and developer environments. We've recently seen vendors such as Silverfort (PAM), 1Password vaulting and Keeper PAS continue to push for more privilege access products.

See market breakdown below:



SACR's View Of The Modern Identity Security Stack

To better understand this framework, it's crucial to understand how SACR thinks about the identity ecosystem. In today's cloud-first and identity-driven environments, **identity security has become the new perimeter.** The image below outlines the core pillars of a modern **Identity Security Framework,** illustrating how organizations must govern access across both human and machine users.

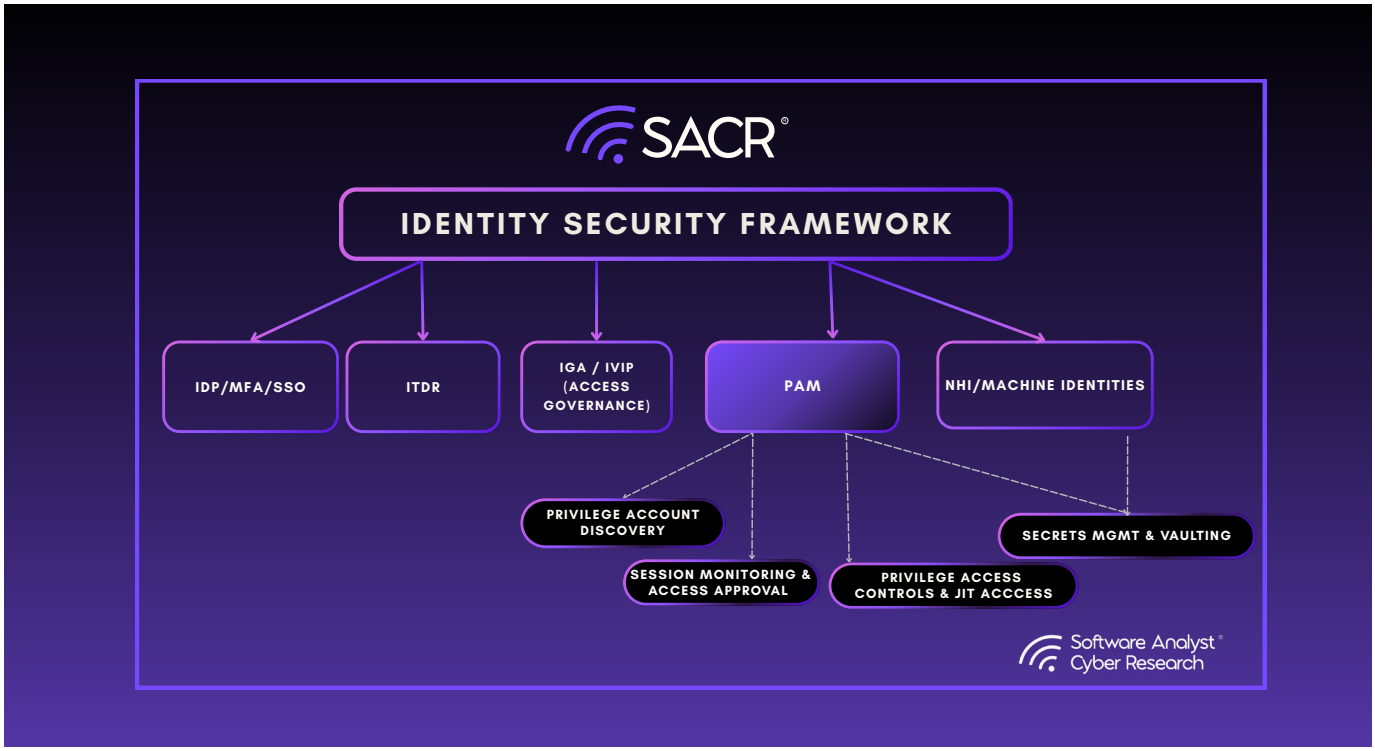
At the center is **Privileged Access Management (PAM).** Its the hardest capability to build in *identity security relative to others*. We believe PAM will be central to managing agent identity, as its the function responsible for securing the most sensitive and high-impact permissions across your environment. Surrounding PAM are adjacent pillars:

- **IDP/MFA/SSO,** which authenticate users and enable secure logins.
- **ITDR** (Identity Threat Detection & Response), focused on detecting identity-based threats in real time,
- **IGA/IVIP,** which handles visibility into all identities (IVIP) and IGA focuses on governance, access reviews, and joiner/mover/leaver flows.
- **NHI (Non-Human Identities),** which includes service accounts, workloads, bots, and API keys. It is important to realize there is a separation or distinction of NHIs vs agents.

Within PAM itself, we break SACR down into four essential components**:**

1. **Privileged Account Discovery:** Find what powerful access exists
2. **Secrets Management & Vaulting:** Store credentials safely
3. **Privileged Access Controls & JIT Access**: Enforce who gets access, when, and how
4. **Session Monitoring & Access Approval:** Observe usage and add checks before granting access

These building blocks work together to enforce least privilege, prevent unauthorized escalation, and contain the blast radius of breaches. The rest of this report will dive deeper into this PAM pillar and, hopefully, provide context for all readers. We provide a foundation breakdown much more in the report.



Defining Privileged Access Management (PAM) in the Modern Enterprise

Privileged Access Management is the identity security discipline focused on protecting, governing, and monitoring access to the most sensitive systems and actions within an environment.

A privileged account is any account that can

- Change systems
- Access sensitive data
- Create or delete users
- Shut things down
- Override security controls

Privileged accounts span

- Domain controllers and directory services
- Administrative access to databases, applications, and operating systems
- Public and private cloud IAM permissions
- Network and infrastructure devices
- DevOps secrets, API keys, tokens, and service accounts

Historically, PAM was synonymous with IT administrators and shared root credentials. Today, privilege has expanded dramatically in breadth (more identities) and depth (more powerful actions). Broadly, the move to the cloud has expanded access across the enterprise. We have seen an expansion in developers becoming more admins of critical infrastructure.

Foundational components

The core components of a PAM suite

1. **Privileged Account Discovery:** The goal is to identify all privileged accounts across systems, networks, applications, and cloud platforms. There is also another auditlogging and compliance where before you can protectprivileged access, you need to *find it and track it.* This pillar handles account discovery, continuous inventory, detailed activity logs, and compliance reporting. It ensures that security teams have the insights to detect risks and prove controls are working.
2. **Credential Vaulting / Rotation:** This pillar stores privileged credentials in a secure and encrypted vault accessible only to authorized users or systems. This pillar focuses on protecting the actual *secrets*: passwords, SSH keys, tokens, and certificates. Credentials are stored in secure vaults, rotated frequently, and retrieved securely without exposing them to users. This reduces the risk of theft, reuse, or unmanaged sprawl.
3. **Access Control & Least Privilege:** This category covers Access control, Just-in-Time (JIT) Access and Approval Workflows. It enforce *who gets access, when, and under what conditions*. The goal is to eliminate standing privileges and instead issue temporary access based on need and context, often requiring manager or peer approval. It's the core of Zero Trust and minimizes exposure.
4. **Session Management and Monitoring:** Once privileged access is granted, this pillar ensures *real-time visibility* and oversight of what users do with that power. This includes logging, monitoring, session recording, and if needed, termination of live sessions. It's crucial for incident response and auditability.

Core Actionable Summary for Readers

Setting the context for PAM, if you only had a few minutes to read the report. Here are the core takeaways:

1. **Consolidation Has Made Privileged Access a Board-Level Control, not a Point Solution. We highlighted this in our report last year.** Palo Alto Networks' acquisition of CyberArk is not simply another large security deal; it is a signal that privileged access has moved to a foundational layer of enterprise security architecture. Platform security vendors do not spend $25B to fill feature gaps, they do it to control a control plane. By embedding privileged identity telemetry into network, endpoint, and SOC workflows, Palo Alto is effectively asserting that identity-driven privilege enforcement must operate at the same level of priority as threat detection and response. For CISOs, the implication is clear: privileged access is no longer a standalone IAM decision or a compliance checkbox. It is becoming inseparable from how organizations detect, contain, and respond to breaches. This acquisition has created a gap, opening the door for new vendors like Britive, Apono, Teleport and P0 Security.

2. **Machine and Agentic Identities Are Now the Fastest-Growing Privileged Users and the Least Governed:** The definition of identities is expanding more and more. The most significant expansion of privilege in modern environments is no longer human administrators, but non-human identities: service accounts, API keys, workloads, automation, and increasingly autonomous AI agents. These identities already outnumber humans by orders of magnitude, and unlike people, they operate continuously, at machine speed, and often with broad, implicit permissions. AI agents amplify this risk further by introducing non-deterministic behavior, an agent granted access to "optimize infrastructure" may legitimately modify or delete production systems if guardrails are weak or misinterpreted.

3. **The Evolution of Privileged Identity:** Enterprise security has undergone a structural inversion over the last two decades. Where trust was once anchored to a hardened network perimeter, modern environments have dissolved those boundaries through cloud computing, SaaS adoption, automation scripts, and an API-driven infrastructure. The perimeter no longer meaningfully exists. Identity is now the only consistent boundary. Across any organization, certain users and accounts hold elevated permissions over systems, infrastructure, data, and configurations effectively the "keys to the kingdom." These privileged identities now include not only IT administrators, but developers, cloud engineers, service accounts, APIs, workloads, and increasingly, autonomous AI agents. This is a crucial contrast that is changing PAM.

4. **Cloud and Ephemeral Infrastructure Have Made Standing Privilege Structurally Unsustainable:** Cloud has fundamentally broken the assumptions that traditional PAM was built on. Infrastructure is now created and destroyed in minutes, access requirements change continuously, and policy defined through static roles cannot keep pace without creating excessive risk or operational drag. Standing privilege like long-lived permissions granted has become one of the most common root causes of cloud security incidents. In this environment, the question is no longer whether an organization will experience privilege misuse, but whether it can limit the blast radius when it happens. Modern PAM is shifting from credential storage to real-time authorization: provisioning access only when needed, enforcing it in context, and revoking it automatically. Organizations that fail to make this transition are not merely behind the curve; they are operating with an access model that is incompatible with the speed and volatility of their own infrastructure.

How PAM is Slowly Evolving In 2026

This new parameter shift, where identity security becomes the 'parameter,' is new for many practitioners. What was once a discipline centred on on-prem session control and credential vaulting is now evolving into a core access control layer responsible for enforcing contextual access decisions, continuous verification, and eliminating standing privileges across increasingly dynamic environments

As a result, the baseline for PAM has materially changed. Just-in-time (JIT) access, remote privileged access, secrets management, and automation are no longer differentiators; they have become stakes. Buyers are increasingly evaluating PAM platforms based on their ability to enforce least privilege in real time, integrate with identity and infrastructure signals, and operate effectively across hybrid, cloud-native, and SaaS environments.

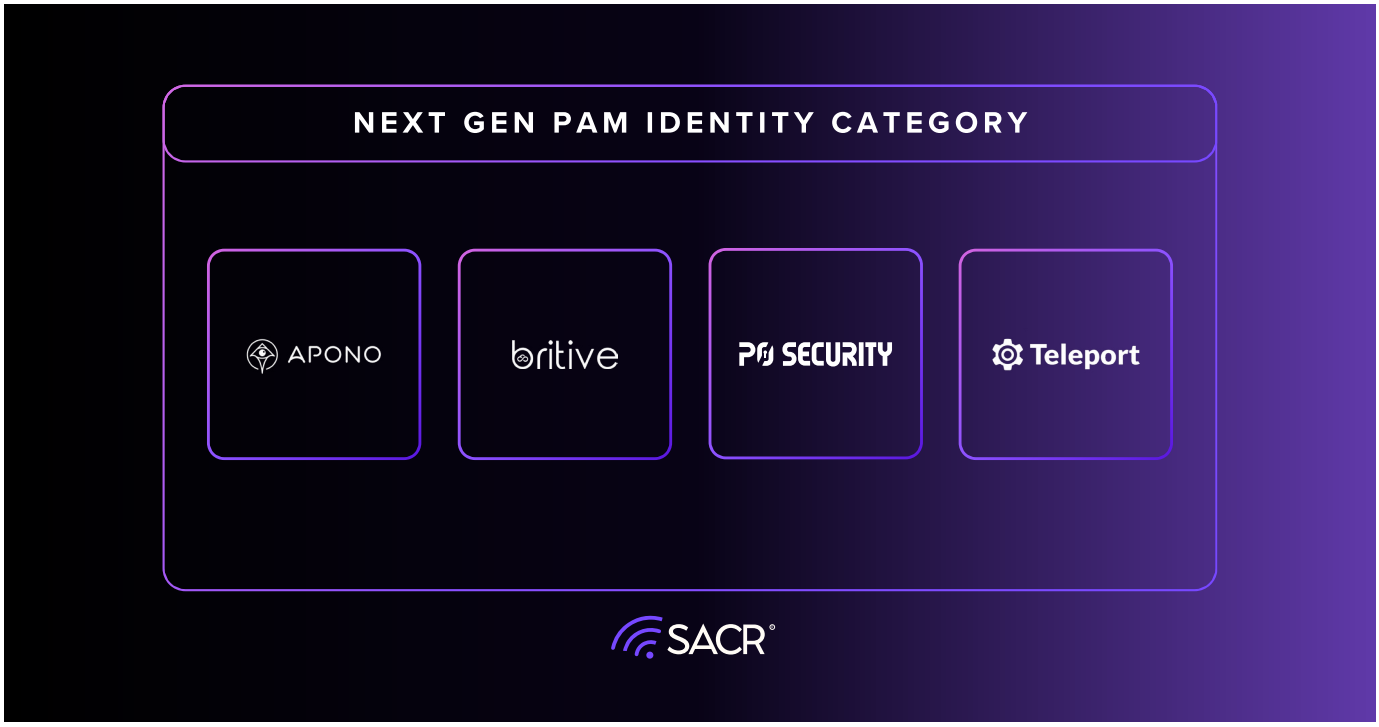
However, the most consequential force reshaping PAM is not cloud adoption or Zero Trust alone, as we've seen in recent years. Agentic AI is now redefining the nature of privileged access itself. The scope of identity has expanded well beyond human administrators to include non-human identities like service accounts and agents that operate with elevated permissions. This expansion in identities and privileged access is exposing a critical gap.

Traditional PAM architectures, which were designed for human-centric access and static infrastructure, are increasingly misaligned with these new identities.

For CISOs and investors alike, the next phase of PAM will be determined by which platforms can govern human, machine, and AI identities at runtime, enforce privilege dynamically, and scale trust decisions in systems where access is transient and constantly changing.

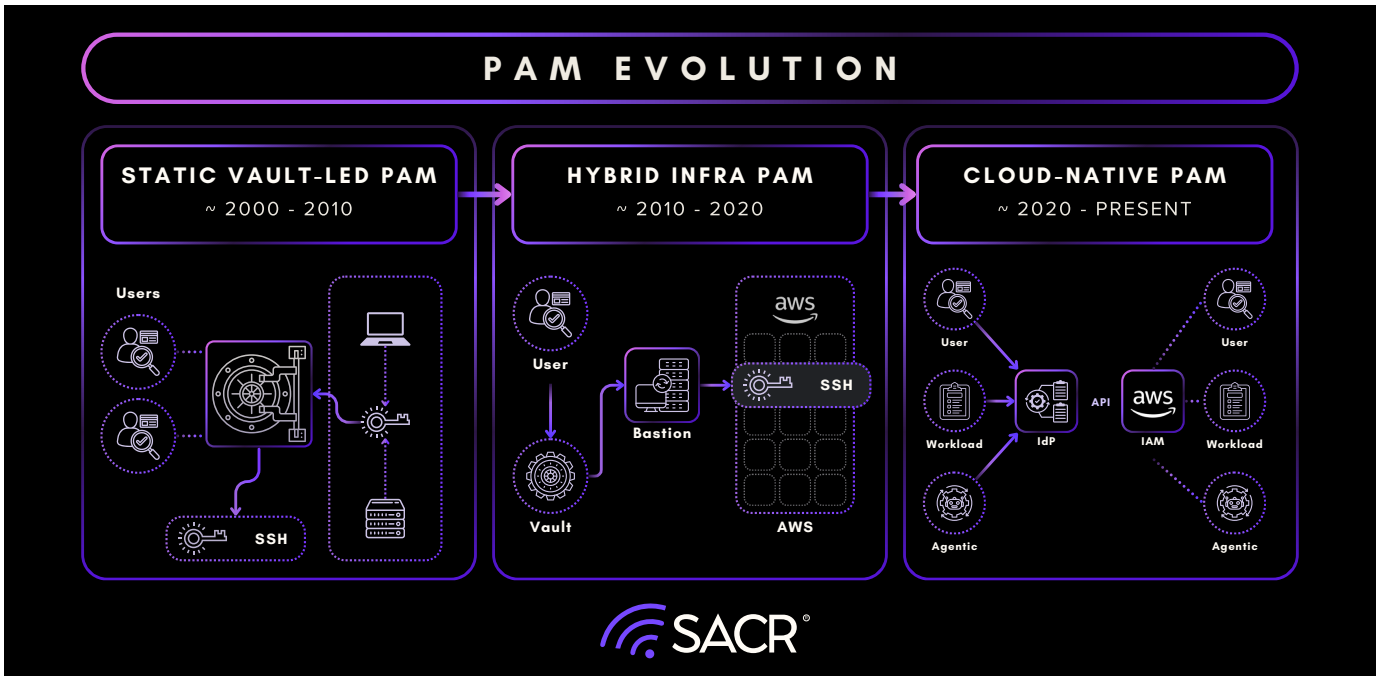
This report examines how the evolving PAM market has hit an inflection point for 2026, what it signals about the future of identity security, and which architectural approaches are likely to define the next generation of privileged access control. We selected the following players based on their next-gen PAM criterion and partnered with them to produce this research report for the community. The four vendors do not represent the entire market for next-gen players but they have representative key use-cases that help us illustrate how PAM is evolving for the cloud and agentic world.

1. Apono
2. Britive
3. P0 Security
4. Teleport



The History & Evolution of PAM

PAM suites then evolved over the years as more applications and infrastructure shifted from on-premise environments to public cloud environments. As we think about PAM, it has changed over the years from an on-prem-centric ecosystem to cloud-centric view. More readings can be found here.



Phase 1: The Vault-Centric Era (Static Infrastructure, Static Secrets)

The PAM market emerged in the early 2000s alongside large on-premise data centers. Infrastructure was static, credentials were long-lived, and administrative access was often shared and poorly documented.

High-profile breaches exposed the fragility of this model. The 2014 Sony Pictures breach where attackers discovered a literal folder named "Passwords" containing privileged credentials became a defining moment for the category. Adoption accelerated rapidly, coinciding with CyberArk's IPO and the market's transition from niche to mission-critical.

Core architectural components of this era included:

- Secure password vaults
- Privileged session management and recording
- Application identity and service account credential storage
- Threat analytics focused on anomalous privileged behavior

This model dramatically reduced risk in static environments but introduced friction. Manual password checkout workflows often failed to scale, leading to shadow accounts and policy bypasses.

Phase 2: The Hybrid Cloud PAM Era (Session Governance at Scale)

As enterprises migrated to public cloud and virtualized infrastructure, the assumptions underlying vault-centric PAM began to break down. Ephemeral virtual machines, autoscaling workloads, CI/CD pipelines, and SaaS platforms caused an explosion in privileged credentials which many teams refer to as secret sprawl.

PAM platforms expanded to address this hybrid reality:

- DevOps and secrets management
- Endpoint privilege management
- Cloud privilege and entitlement management
- Bastion-based session mediation for SSH, RDP, and web access

Despite architectural change, market leadership remained stable. CyberArk and BeyondTrust retained dominance, while Centrify and Thycotic merged to form Delinea. At the same time, DevOps-native players like HashiCorp carved out a strong position around secrets management. The core limitation persisted: static roles and long-lived permissions do not align with infrastructure that changes by the minute.

Cloud Introduced Complexities Around Managing Ephemeral and Dynamic Privileged Access

The scale and volatility of modern cloud environments have fundamentally changed the requirements for privileged access management. Infrastructure is no longer composed of long-lived assets with predictable access patterns; instead, thousands of resources, virtual machines, containers, serverless functions, and cloud services are created, modified, and destroyed on a continuous basis.

In this context, access models built on static roles and pre-defined permissions become operationally unmanageable. Roles require constant updates, new resources must be manually onboarded, and permissions frequently lag behind the actual state of the environment, creating both security gaps and administrative overhead.

To be effective in cloud-native environments, privileged access must shift from static entitlement management to dynamic, context-aware authorization. This requires continuous, real-time discovery of infrastructure and identities, coupled with policies that evaluate access requests based on attributes such as workload context, environment, risk signals, and business intent at the time of use. Privilege must be provisioned just-in-time, scoped narrowly to the specific task or resource, and automatically revoked once the task is complete. Solutions that cannot adapt to infrastructure as it comes online without manual intervention; do not reduce risk; they simply introduce friction and complexity that teams will eventually work around.

As a result, defining privileged access policy through Infrastructure as Code (IaC) is becoming a practical requirement rather than a best practice for organizations operating at scale. Security and access controls must be versioned, automated, and deployed alongside infrastructure changes to remain effective. These requirements are increasingly driven not only by security teams, but also by platform, cloud, and DevOps engineers who are responsible for day-to-day operations and uptime. In environments where velocity is a competitive necessity, privileged access solutions must enforce control without impeding delivery: otherwise, they will be bypassed, undermining both security and governance.

Phase 3: The Zero Standing Privilege for AI Agents Era (Authorization Over Authentication)

The most significant shift underway is the transition from standing privilege to ephemeral, just-in-time authorization continuously in cloud environments and increasingly for AI agents.

In cloud-native environments, privileged access is less about logging into servers and more about executing API calls that mutate infrastructure state. Modern PAM architectures integrate directly with identity providers and cloud control planes, provisioning temporary credentials only when required and revoking them automatically upon task completion.

This Zero Standing Privilege (ZSP) model reduces the blast radius, eliminates permanent secrets, and aligns access with real-time context. Newer entrants argue that managing secrets indefinitely is an anti-pattern, the real solution is eliminating the need for secrets altogether. Importantly, this is not yet the norm. Most enterprises remain hybrid, and vault-based PAM will remain essential for years. The market is not replacing legacy PAM, it is layering dynamic authorization on top of it.

The Expansion of Privilege From Humans to Machines

The complexity of human identity roles requires newer PAM solutions

The breadth and depth of access that engineers need to complete their work in the cloud have created a new attack surface for security teams to manage. This new class of privileged account presents two critical challenges for PAM: unprecedented scale, with exponentially more privileged accounts to manage; and heightened expectations regarding user experience. Unlike traditional privileged users, today's developers represent a large population whose productivity directly impacts business outcomes, making friction intolerable. As a result, we regularly speak with CISOs who are as concerned with their team being viewed internally as business enablers as they are with addressing risk: an outcome that is often incompatible with traditional approaches to privileged access. We've also seen the scope of privileged access projects shift to include many stakeholders not typically associated with the category, including cloud security, platform security, DevOps, and even engineering leadership.These dynamics have redefined what organizations need and expect from PAM solutions: robust self-service capabilities, developer-friendly workflows, and the ability to secure access without impeding velocity.

Machines & Agents Evolving The Market

Identity security is increasingly bifurcated into human and non-human (machine) identities. While the number of human users has stabilized, machine identities: service accounts, API keys, tokens, certificates, workloads are growing exponentially. Most organizations already manage 40–50x more non-human identities than human ones, yet visibility and governance lag far behind. High-profile breaches at Okta, JumpCloud, and others have demonstrated that poorly managed machine identities represent a systemic risk. Machine identity security has evolved from SSH key management into a broader discipline encompassing:

1. Discovery and inventory
2. Lifecycle management
3. Secret rotation and certificate management
4. Behavioral detection and response

As PAM expanded into DevOps and secrets management, its boundaries increasingly overlapped with machine identity platforms such as Venafi and emerging startups focused exclusively on this problem.

The Future of PAM: The Rise of Agentic AI & the Redefinition of Privilege With Agents

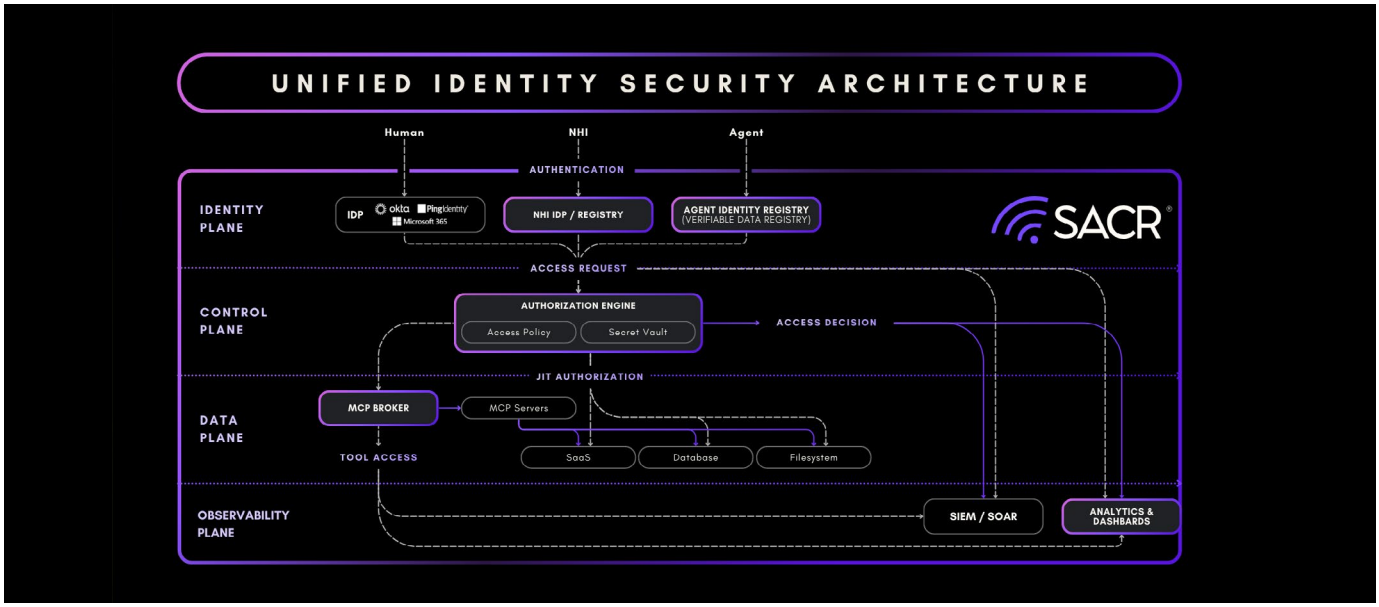
AI agents represent a new class of privileged identity. When we compare them to traditional service accounts, agentic systems can reason, plan, and execute multi-step actions across domains. If compromised via prompt injection or model manipulation, these agents become high-speed insider threats. Organizations that have already operationalized just-in-time access, session auditing, and dynamic policy enforcement for humans are structurally better positioned to govern AI agents.

However, the effective deployment of AI and agents require access to sensitive internal systems, data, and infrastructure — and a majority of organizations remain uncertain about how to enable that access safely. Recent research indicates that a significant portion of IT leaders lack confidence in their ability to govern AI interactions with proprietary data, highlighting a growing gap between AI ambition and access control maturity. For many enterprises, even achieving zero standing privilege for human users remains an aspirational goal; extending privilege safely to non-deterministic AI agents introduces a materially higher level of risk.

Agentic identity is still an emerging domain, but customer sentiment is converging around a clear conclusion: privileged access maturity is a prerequisite for agentic AI adoption, not a downstream enhancement. AI agents operate continuously, execute multi-step actions, and can affect production environments at machine speed. Without just-in-time access, real-time authorization, session-level auditing, and anomaly detection, these agents effectively function as high-velocity privileged insiders. Organizations that have already operationalized these controls for human users are structurally better positioned to apply the same governance patterns to autonomous systems.

Additionally, AI co-pilots that inherit or "piggyback" on human access rights significantly expand the attack surface in environments with weak privilege boundaries. In such cases, compromise of a single identity can cascade across human and machine workflows.

Forward-looking CISOs are responding by treating PAM as a foundational control for AI readiness. We broadly believe that investing now in deep visibility into sensitive resources, enforcing automated and context-aware permissions, and aligning privileged access decisions with business intent. This groundwork will ultimately determine whether AI becomes a controlled force multiplier or an ungoverned source of systemic risk.



Future Themes To Watch

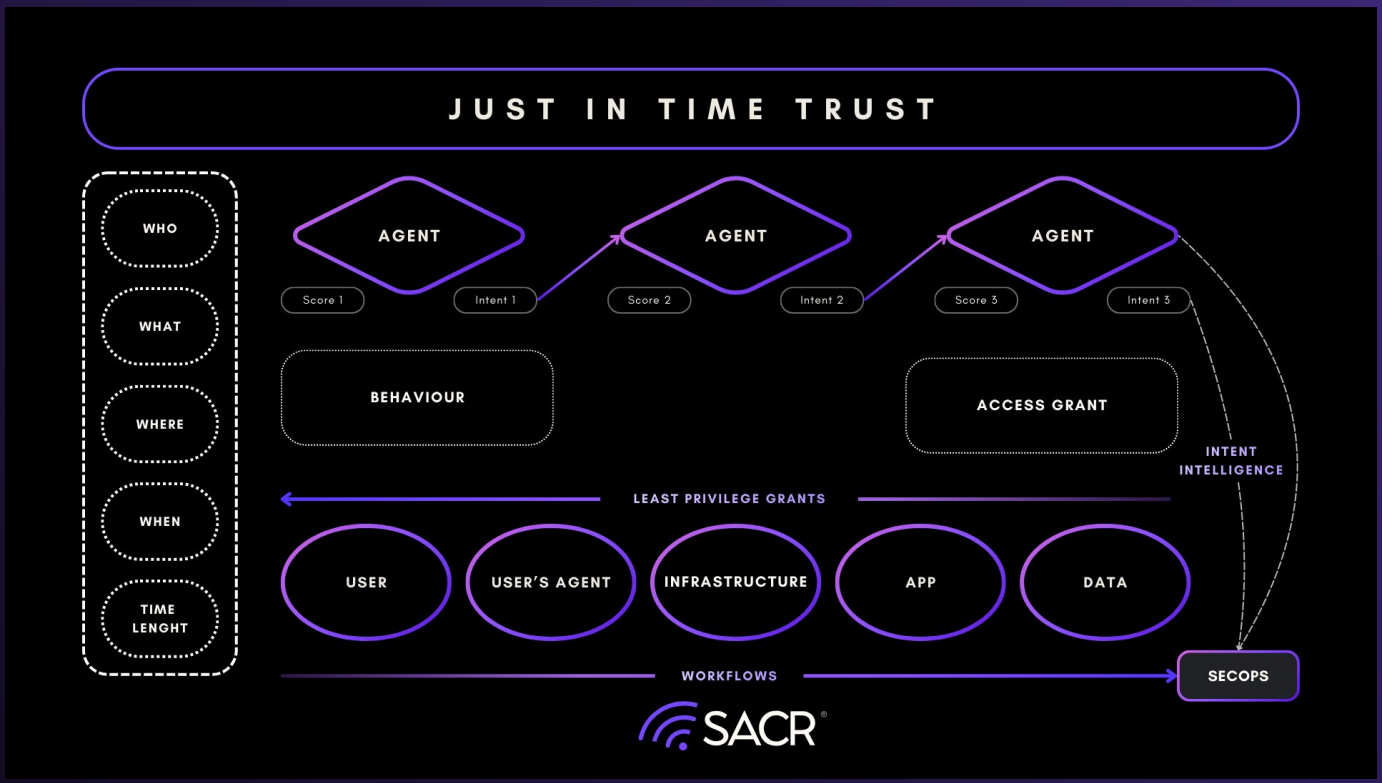
The Rise of Just-in-Time Trust (JIT Trust)

Just-in-Time Trust (JIT Trust) represents the next evolutionary step beyond Zero Trust Architecture (ZTA). It emerges as a unified identity control layer designed for the speed of modern threats and the rise of autonomous, agentic systems and AI agents. Where Zero Trust redefined *who* can access *what*, JIT Trust redefines *how long*, *under what conditions*, and *for what exact purpose* access exists. Unified identity systems, stronger authentication, and just-in-time access must be contextually aware of intent.

At its core, JIT Trust treats access as a continuously evaluated, ephemeral resource rather than a static entitlement. Long-lived credentials and standing privileges are replaced with temporary, self-destructing Ephemeral Access Grants and short-lived, certificate-based authentication. These grants are narrowly scoped to the precise resources and actions required for a specific human, machine, or agentic task.

JIT Trust moves beyond traditional authentication toward continuous authorization grounded in behavioral and intent-based signals. Rather than validating identity once at login, the system continuously monitors an entity's intent and behavior: the digital signals generated through AI prompts, tool usage, API calls, and execution patterns to dynamically assess risk and derive trust in real time. When behavior deviates from an established baseline or intent shifts unexpectedly, the system initiates a graduated response: privileges can be reduced, entitlements constrained, or access suspended entirely.

This model establishes Continuous Adaptive Trust (CAT): a control framework where trust is not assumed, but continuously earned and recalibrated. The result is a dramatically reduced attack surface, tighter blast-radius containment, and an access model that aligns with environments defined by automation, ephemerality, and machine-speed execution.



PAM Market Ecosystem

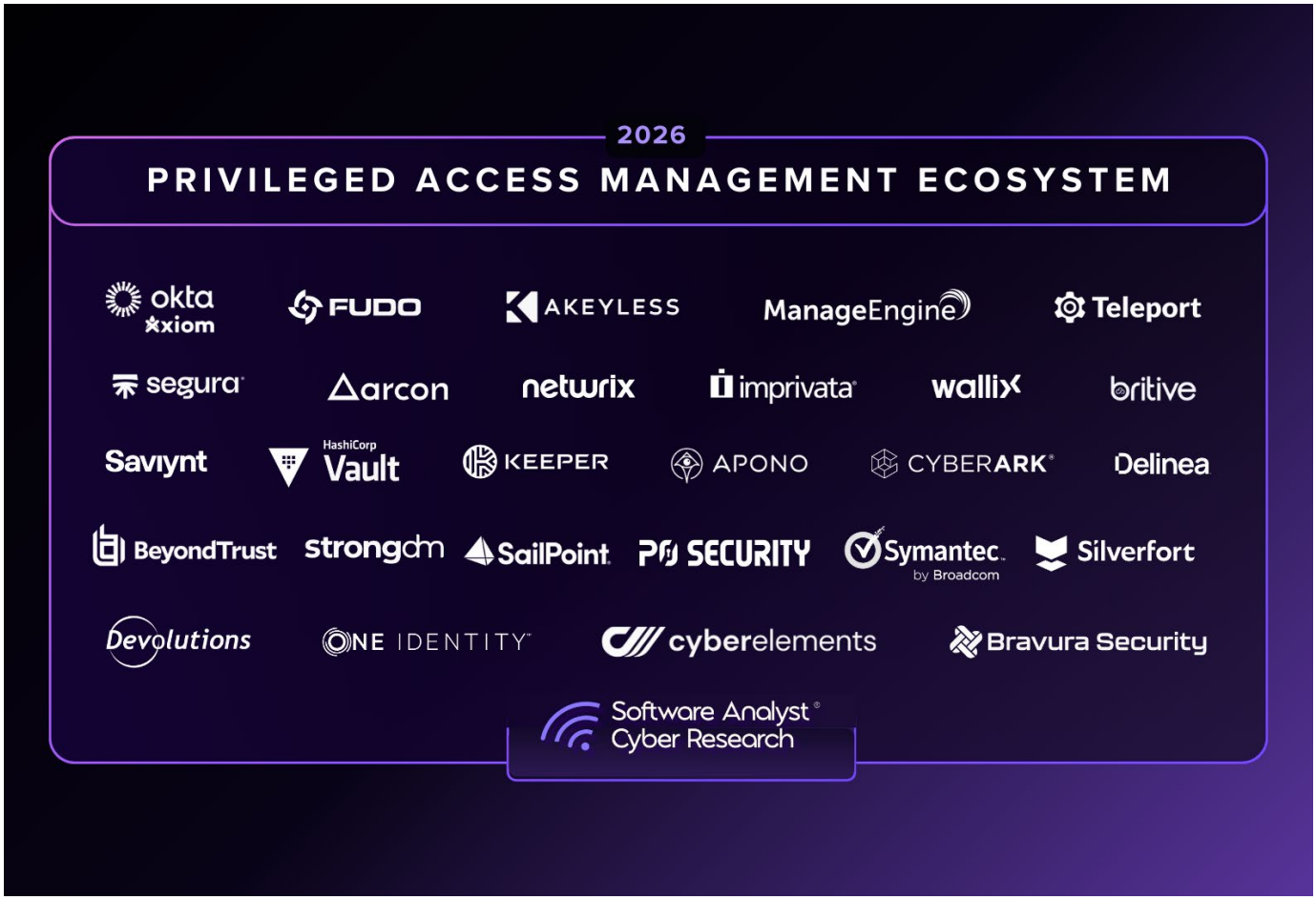
This landscape illustrates a Privileged Access Management (PAM) market that has expanded well beyond its historical roots in password vaulting and session control. What was once a narrow category dominated by a handful of incumbents has evolved into a broad ecosystem spanning identity providers, secrets management, cloud-native access platforms, developer-centric tools, and emerging authorization layers.

The presence of legacy leaders such as CyberArk, Delinea, and BeyondTrust alongside newer cloud- and API-native players like Apono, Britive, Teleport, StrongDM and P0 security reflects a market in transition rather than replacement. Incumbents continue to anchor regulated and hybrid environments, while newer entrants are redefining PAM around just-in-time access, zero standing privilege, and runtime authorization aligned with cloud and DevOps workflows. At the same time, adjacent identity vendors including Okta, SailPoint, and One Identity underscore the growing convergence between PAM, IAM, IGA, and identity threat detection.

Collectively, this ecosystem signals that PAM is no longer a point solution but a foundational control layer within the modern identity stack. As non-human identities, automation, and agentic systems proliferate, the market is shifting toward platforms that can enforce privilege dynamically, at scale, and in context positioning PAM as a central pillar of enterprise security architecture heading into 2026.

Based on our extensive work, we want to dive into next-gen platforms that are set to capitalize on the next evolution of cloud and agentic PAM architecture. They include:

1. Apono
2. Britive
3. P0 Security
4. Teleport




PT SECURITY

P0 Security

Executive Summary

P0 Security is a cloud-based Privileged Access Management (PAM) platform designed to address the challenges of hyper-fragmented, cloud-native environments by shifting the focus from credential vaulting to identity-native authorization. The platform is notably modern compared to earlier traditional "heavy" PAM solutions that rely on bastions and vaults.

P0 Security utilizes an API-led orchestration layer to enforce Zero Standing Privilege (ZSP) at scale. By integrating directly with existing Identity Providers (IdPs) such as Okta or Entra ID, P0 provisions Just-in-Time (JIT) and Just-Enough Privilege (JEP) access for human users, workloads, and AI agents across multi-cloud and hybrid infrastructure.

Core Architectural Philosophy

Similar to other players discussed, P0 Security's differentiation is rooted in its provisioning access and identity-centric approach, which aims to secure the business without interrupting developer velocity.

Based on our analysis, its core differentiation lies in SSH (Secure Shell) and RDP (Remote Desktop Protocol) access tied directly to corporate identity, both of which are commonly used to remotely control servers or computers.

Historically, accessing servers via SSH or RDP required:

- Shared admin accounts (e.g., "root" or "Administrator") used by multiple people
- SSH keys or passwords managed separately from corporate identity
- Static credentials stored in password vaults or shared across teams

These approaches created issues around traceability, credential sprawl, and security gaps. P0 Security's approach removes shared accounts and static credentials, ensuring that every remote session is tied directly to an established corporate identity (the same identity used for Active Directory, Gmail, Slack, or Okta).

This capability continues to be central to the platform. Developers authenticate via corporate IdP credentials with no shared admin accounts, no SSH key management, and no secondary credentials. Every session is tied to an individual identity with full audit trails. This identity-native authorization method ensures every session is tied directly back to the corporate IdP identity rather than relying on shadow accounts or shared static credentials. The focus is more on removing friction for developers, governance overhead for security and the costs of heavy infrastructure maintenance.

Detailed Capability Analysis

The following analysis examines P0 Security's technical capabilities, focusing on how their "Identity-Native" architecture addresses the "last mile" of privileged access in cloud-native and hybrid environments.

Just-Enough and Just-in-Time Server Access

A primary differentiator for P0 is its bastionless JIT SSH capability, which challenges the traditional vault-and-proxy model. By eliminating static credentials and shared admin accounts, the platform replaces long-lived SSH keys with short-lived, identity-based access tied directly to the corporate Identity Provider (IdP).

From a practitioner's perspective, this removes a common bottleneck in legacy systems. Users request access through lightweight ChatOps workflows (Slack or Teams) or a CLI wrapper. Upon approval, P0 provisions a short-lived and tightly scoped IAM role or native entitlement. Sessions are automatically terminated upon expiry or manual revocation, ensuring no "shadow accounts" or standing privileges persist once the task is complete.

Granular Scoping for Code, Data Stores and Entitlements

P0 Security provides specialized depth for modern production stacks, particularly within Kubernetes (EKS, GKE, AKS) and high-scale data stores like Snowflake and Postgres. In Kubernetes environments, the platform moves beyond broad cluster-level access to allow "task-specific scoping" at the namespace or even individual pod level. This allows developers to "exec" into specific containers for troubleshooting

without being granted cluster-wide permissions that could expand the blast radius. Similarly, for database resources, the platform can provision granular access down to the ability to run specific queries rather than granting broad, standing role permissions, effectively delivering "just-enough-privilege" (JEP) as the operational default.

The "Closed-Loop" Privilege Governance

To move an organization toward a Zero Standing Privilege (ZSP) target state, P0 includes a posture product designed to identify and quantify privilege-related risk in real time. This "closed-loop" system identifies unused or excessive privileges such as role bindings that have not been exercised in 90 days and provides security teams with actionable instructions or automated JIT policies to remediate those risks. Beyond a one-time cleanup, the platform performs continuous monitoring for "drift," where access patterns deviate from defined guardrails. By surfacing these over-permissioned roles and automatically converting them into policy-driven, time-bound controls, P0 enables enterprises to transition from a reactive static defense to a dynamic, authorization-centric security model.

Analyst Perspective: Practitioner Considerations

1. **Bring Your Own Identity (BYOI) Architecture:** P0 emphasizes a pure authorization model with no infrastructure deployment. It leverages existing IdPs (Okta, Active Directory) and native cloud APIs to auto-discover resources and provision Just-in-Time access. No agents, proxies, or bastions are required. All activity ties directly back to corporate identity without cross-system correlation.
2. **Access Graph:** The platform builds a contextual visualization of all access paths, patterns, and relationships between users, machine identities, and resources. This allows security teams to identify risky "lurking" privileges that traditional tools often miss.
3. **Proxy-Free Deployment:** Because P0 operates as an orchestration layer outside the direct data path, it auto-discovers privileged resources via APIs without requiring the deployment of proxies or jump-hosts. This minimizes downtime risk and simplifies operations for hybrid enterprises.

Strengths

Policy-Based JIT Provisioning

P0 has good cloud-based JIT access scoping down to individual S3 bucket folders, specific database roles, or even single queries without broader role permissions. Configurable time windows, approval workflows (including auto-approval based on conditions like PagerDuty escalations), and dynamic IAM role creation with precise permissions.

Since P0 started with building cloud-based access governance controls, they have a good base of built-in cloud security posture management (CSPM) features that identifies unused standing privileges and role bindings (90+ days unused), then provides both remediation instructions and one-click conversion to JIT policies. This we believe helps customers achieve zero standing privileges by showing where unused access exists and automatically migrating identities to the JIT model.

Zero-Friction Developer UX: Native ChatOps (Slack/Teams) and CLI integrations drive high adoption among engineers.

Hybrid Maturity: While P0 announced hybrid/on-prem support (SSH/RDP) in late 2025, it remains a cloud-first platform compared to decades-old legacy incumbents.

Identity Lineage: Tying every action to a "real" IdP identity simplifies audits and removes the correlation overhead of shared accounts.

Direct Critical Path: P0 positions its API-led orchestration as being "outside the critical path" to reduce downtime risk, though it remains a critical control point.

Cost Efficiency: Eliminating the need for vaults, bastions, and shadow accounts reduces infrastructure and governance overhead.

Things To Watch

For a “hybrid” enterprise with significant on-prem stacks, P0 lacks the decades of hardened connectors required to manage privilege for non-API-driven legacy hardware that cannot easily adopt a just-in-time (JIT) workflow. Legacy market leaders like CyberArk maintain a massive catalog of out-of-the-box integrations for “long-tail” infrastructure, including Mainframes, AS400, and Industrial Control Systems (OT/ICS).

P0 Security has an architecture that is predominantly API-led. While their historical focus has been on cloud servers and databases, recent months have seen an expansion of support to include traditional on-prem servers and databases. This deepening of capability will further extend to Active Directory in late 2025.

Broadly, compared to vendors like CyberArk’s Digital Vault, which provides policy-based rotation for nearly any credential type, P0 is a “authorization control plane” optimized for modern production stacks (K8s, Snowflake, AWS). However, we see P0 as being a strong complementary fit for large enterprises wanting a combination of both capabilities bolted into one stack.

Conclusion

In summary, P0 Security is a good choice for enterprises looking to modernize their PAM stack specifically for ephemeral clouds and Kubernetes environments where legacy tools often struggle. It is a complementary fit to vendors with strong on-prem systems. Broadly, we see P0 has having a complementary capability alongside companies that have vendors like CyberArk. P0 shines very well for developer-heavy, cloud environments that typically have strong and simple authentication controls around SSH and data store demos, where teams can achieve total session auditability without shared keys or complex proxy infrastructure.

Software Analyst®
Cyber Research

business personal

softwareanalyst.io

SACR®

Trusted research. Sharp insights. Real conversation.

CISO	VENDOR
SECURITY TEAMS	INVESTORS