A buyers guide to securing the production stack

The Cyber Hut

Contents

Executive summary

Modern production infrastructure has outpaced traditional Privileged Access Management (PAM), leading to an increase in the identity attack surface along with significant operational drag. Traditional, on-premises, vault-centric PAM systems, which were designed for a small, static set of accounts, can no longer manage the breadth of modern systems, protocols, and identity types, including human, non-human, and agentic identities. This complexity results in over-provisioned, standing privileges and slow, manual access workflows that frustrate developers and increase risk.

This guide outlines a strategic shift from legacy, isolated PAM to an Identity-Native, API-first model that supports a decoupled, "zero-touch" production access environment.

Capabilities in this modern approach leverage:

- **Just-in-Time (JIT) access and Zero Standing Privilege (ZSP)**: JIT allows identities to request access only when needed, and only for as long as needed, which is critical for minimizing the identity attack surface and enforcing a least-privilege policy.

- **Broad, consistent coverage**: A modern privileged access platform must cover the full spectrum of high-risk assets, including cloud consoles, databases, Kubernetes and code repositories, and all identity types, particularly non-human identities (NHIs) which often hold unchecked privileged access.

By adopting this approach, organizations can achieve a more dynamic and responsive security posture that delivers measurable impact across three core areas:

1. **Improved security and compliance** by eliminating standing access, enforcing least privilege proactively, and simplifying audits with real-time session recording.

2. **Increased developer velocity** by automating access orchestration and embedding JIT workflows directly into tools like Slack and CLI, increasing developer adoption and cutting Mean Time To Access (MTTA) from hours to minutes.

3. **Reduced operational overhead** by automating manual access provisioning and de-provisioning, allowing Security Operations (SecOps) and IAM teams to focus on critical threats, with continuous governance a possibility.

This Buyer's Guide provides security and operations leaders with the necessary framework to understand their current state, analyze migration pain points, and select a modern access management solution that improves both security assurance and employee productivity.

Introduction

Why Privileged Access Management needs to evolve

- **Early PAM (On-Premises):** Focused on a small, static set of accounts and functions, mainly using password vaulting and session management for Unix systems. It relied on role-based association and was under the near full-control of administrators due to being on-premises.

- **The rise of Cloud:** The adoption of cloud computing brought fundamental changes, increasing the volume and variety of systems and identities needing integration. This required new access methods (e.g., CLI, certificates, bastion hosts), protocols, that are solely reliant on the network along with a broader adoption of policy-based access control to support scalable PAM platforms.

- **The new era (convergence):** Modern PAM is moving beyond scalable and policy-centric approaches to embrace ephemeral, dynamic, and Just-in-Time (JIT) access for all users, not just human ones.

Emerging needs

- More systems and accounts in a hybrid deployment landscape.

- Ephemerality with respect to credentials, permissions, and access grants.

- DevOps and SecDevOps workflows (e.g., infrastructure management as code).

- Simple access approvals using modern chatops and mobile patterns.

- Runtime management capable of complex intent analysis to distinguish between classic insider threats and advanced state actors.

- Continuous data governance (permissions, policy) and post-access monitoring and audit, especially with the rise of AI-based systems.

The document, "Defining and Securing Privileged Access in Modern Environments," is the second in a three-part series on modern Privileged Access Management (PAM).

Key capabilities for the new PAM era

- **Risk Evolution:** High-risk systems have broadened to include cloud infrastructure, SaaS, API-fronted control planes, and dev-centric everything-as-code.
- **Isolation to integration:** Managing this mesh of resources requires moving away from isolated components to a conceptual, dynamic approach that treats **risk as a spectrum** and integrates least privilege, just-in-time access, and strong attribution.
- **The Cloud complication:** Cloud environments introduce varying shared responsibility models, different system types, and a wider range of users (including non-technical managers and microservices engineers).
- **Focus on productivity:** Modern PAM must not interfere with employee productivity. The concept of **Mean Time to Access (MTTA)** as a key metric alongside standard cyber metrics like MTTD and MTTR, focusing on efficiency optimization for access request, credential issuance, and just-in-time processing for all users (humans, services, engineers, and developers).
- **Zero touch access:** The strategic goal is to achieve "zero touch" access management by **decoupling and centralizing policy** for privileged systems. This identity-centric approach allows organizations to consistently and repeatedly add new high-risk resources with limited proprietary controls, ultimately improving developer/engineer productivity and security assurance.

Use Cases

Actor	Aim	Success
Developer/SRE	Gain secure, just-in-time (JIT) access to a high-risk production system (e.g., Kubernetes, database, cloud console) to perform a task or resolve an incident.	Access is granted instantly through a frictionless, embedded workflow (e.g., Slack or CLI), and the Mean Time to Access (MTTA) is cut from hours to minutes.
Security Operations (SecOps)	Eliminate security vulnerabilities created by standing privileges and over-provisioned access across cloud environments.	Zero Standing Privilege (ZSP) is enforced by default. The identity attack surface is minimized, and risk is reduced by ensuring access is ephemeral and only granted when actively needed.
IAM/GRC team	Simplify compliance audits and ensure accountability for all privileged activity, including human and non-human access.	Auditability is ensured without shared accounts, and session recording/monitoring tied directly back to the Identity Provider (IdP). Compliance is simplified (SOC 2, ISO 27001) with automated attestations and immutable logs.
DevOps/ Cloud engineer	Securely manage the lifecycle and privileged access for Non-Human Identities (NHIs) such as service accounts, bots, and AI agents.	The platform provides governance for NHIs (like AWS IAM roles), supporting NHI lifecycle management from creation to ephemeral access tokens, which eliminates the risk of hardcoded credentials
Infrastructure administrator	Migrate from a legacy, vault-centric Privileged Access Management (PAM) solution to a cloud-native, API-first architecture.	The organization achieves a future-proof, easier-to-deploy solution that removes operational drag and provides additional functionality like cloud-native access.

Capabilities and Market Considerations

Functional Capabilities

Category	Capability description	Market considerations
Inventory	An ability to understand the existing high risk and privileged access landscape. This will include systems, identities, accounts, workflow processes, Jira ticketing flows and the various stakeholders involved.	• Understand access elevation flows • Leverage ticketing systems to understand requests, approvals, rejections, time to fulfill • Support for human and non-human identities such as services, lambda functions, infrastructure, workloads etc • Understand both cloud (CSP, SaaS) and hybrid systems
Vulnerability discovery	Understand existing high risk access to a broad array of systems and services and in turn be able to prioritize, triage and treat with countermeasures.	• Identify unused access (e.g. 90 days) • Identify static access • Identify static credentials • Identify non-human/services without accountable owners • Identify permissions that have not been removed from accounts • Identify shared accounts
Just in Time (JIT) access	Develop a strategy that removes statically assigned permissions and credentials with one that is dynamically inline with context, risk and request status.	• Assign permissions to users based on request and approval flows • Assign credentials to users based on a request and approval flows • Request and approval flows to be time based • Request and approval flows to be based on contextual aware policies (e.g. user is in the on call team)

Capabilities and Market Considerations

Functional Capabilities

Category	Capability description	Market considerations
Policy management	Develop organisational and system wide capabilities to enforce security controls, improve reporting and support continuous compliance.	• Automatically remove unused access • Identify and automate notifications of high risk • Identify and automate cleanup and removal of excess permissions and unused accounts • Automate credential and token rotation when revocation is not possible • Automate credential and token revocation
Rotation management	Strategic migration to ephemeral permissions, credentials and associations. Movement away from hard coded credentials, long-lived credentials and keys and accounts with long time standing permissions associations.	• Implementation of short-lived tokens and credentials • Auto-expirty of tokens and credentials

Capabilities and market considerations

Non-Functional Capabilities

Category	Capability description	Market considerations
Dashboarding	Central ability to view privileged landscapes, composite risk analysis and support data distribution to a range of stakeholders.	• Ability to view number of systems and identities under management • Quickly heat map high risk • Top-line view of key metrics such as time to access, time to approve, number of requests, rejections, etc.
Integrations	Modern privileged access management should cover a range of systems and services that covers on-prem, cloud service provider, SaaS, human and non-human identity types.	• Strong breadth and depth of out of the box integrations • API-first approach to ingesting data • Cloud: AWS, GCP, Azure, K8 • Logs: SIEM, UEBA • Notifications: Slack, Email, Jira • IDPs • Repositories Eg Github • Ability to extend and expand integration profile without considerable effort
Scalability and elasticity	As the PAM platform becomes critical to risk reduction and improvements to the mean time to access, it must not be limited by the number of systems, identities and accounts under management.	• Internet scale • An ability to grow based on request demand • An ability to be resilient to known attacks
Usability	As the PAM platform becomes critical to risk reduction and improvements to the mean time to access, it must not be limited by the number of systems, identities and accounts under management.	• Out of the box integration for an array of business operational tools • Email functions • Chatops and messaging integration • Ticketing and IT service management platforms

Recommendations and getting started

First 30 days	First 45 days	First 90 days
• Identify high risk systems that have high friction workflows and long mean time to access • Identify location of hard coded and static credentials • Identify permissions that are statically assigned to accounts • Identify accounts with potential over permissioning • Identify shared accounts usage • Build a roadmap for privileged systems to integrate	• Build out access baselines for privileged systems policy design • Build out policies to manage exceptions and human in the loop approvals • Build out effective success communications plan to help improve business case and engage stakeholders—e.g. capturing time to access improvements, UX happiness changes	• Automation of simple access-request approval workflows • Automation of credential issuance and rotation • Automation of access removal • Build out strategic reporting for standing access, time to access, high risk workflows to allow continual roll out of platform capabilities

The Cyber Hut opinion in this document represents the view at the time of writing. Recommendations, comment and opinion is subject to change as market conditions and product maturity alters. The Cyber Hut does not provide legal or financial advice.

The Cyber Hut shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

The Cyber Hut provides impartial and neutral commentary on technology within the identity and security communities - helping buyers and investors understand the complexities with respect to technology, concepts and market patterns.

The Cyber Hut was founded in 2021 to provide a range of training, advisory, market analysis and research services covering the emerging technologies within the identity and security industries.

For further information, please contact **info@thecyberhut.com.**

The Cyber Hut

P0 SECURITY

Contact Us

Email: info@p0.dev
Web: www.p0.dev

P0 Security is the unified access privilege platform built for modern cloud infrastructure. Where legacy IAM, PAM, and IGA tools fall short—particularly around non-human identities, ephemeral infrastructure and developer velocity—P0 delivers orchestration and governance, visibility and risk posture across all cloud environments.

With an agentless, API-native architecture, P0 helps teams enforce least privilege by default through short-lived, just-in-time access for both human and machine identities. Security and platform teams rely on P0 to reduce blast radius, streamline audits and eliminate manual provisioning without slowing down development.

P0 is trusted by leading organizations in fintech, healthcare, AI, and cloud-native tech, with full enterprise deployments completed in under 60 days. Learn more at www.p0security.dev.

Copyright © 2026 P0 Security

CH-BGProdStk_010626