kuppingercole ANALYSTS

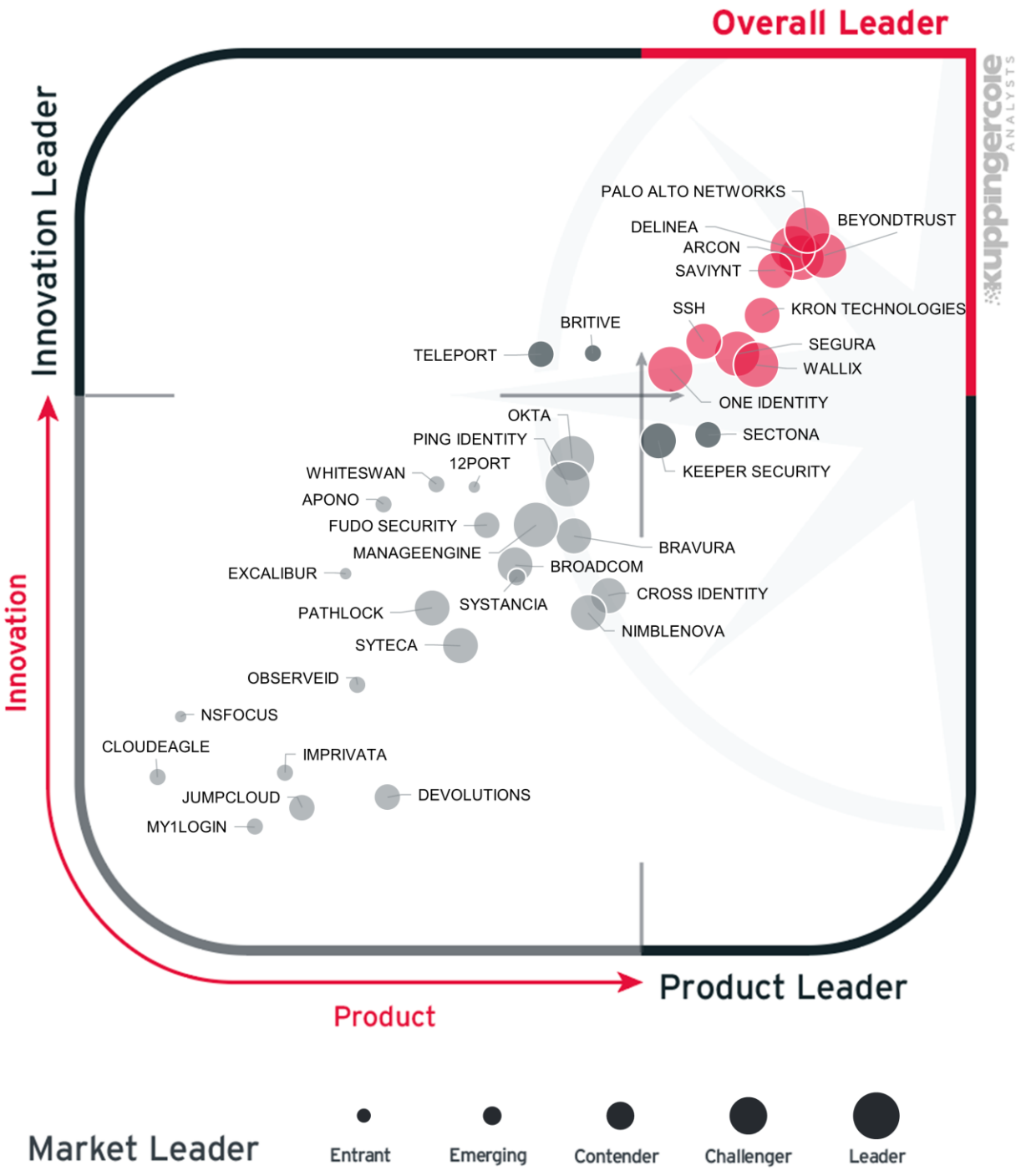
Leadership Compass Privileged Access Management (PAM)

Alejandro Leal

May 18, 2026

Leadership Compass

Privileged Access Management



This KuppingerCole Leadership Compass provides an overview of the leading vendors in the Privileged Access Management (PAM) market, assessing their innovation, product capabilities, and market presence. PAM solutions enable organizations to control, manage, and monitor privileged access across endpoints, servers, applications, and increasingly, cloud and hybrid environments. This includes not only human administrators but also Non-Human Identities (NHIs), including automated workloads and emerging agentic Artificial Intelligence (AI). The evaluated products range from core capabilities such as vaulting and session management to more advanced features like Just-in-Time (JIT) access, secrets management, Cloud Infrastructure and Entitlement Management (CIEM), and the enforcement of Zero Standing Privileges (ZSP) to reduce persistent risk.

Contents

Executive Summary

Privilege in the enterprise should not be understood merely as access granted to a small set of administrative accounts, but as the ability of any identity to perform actions that affect systems, security controls, infrastructure, or other identities. In this sense, privilege is defined less by who holds a specific account and more by what an identity is capable of doing within an environment. This definition shifts the focus of PAM from managing privileged accounts to controlling and governing privileged actions across an environment.

Historically, privileged access was associated primarily with human administrators responsible for maintaining servers, networks, and enterprise applications. That model no longer reflects how organizations operate today. Privilege now extends to AI agents, service accounts, automation pipelines, Application Programming Interfaces (APIs), workloads, and other machine-driven processes that execute operational tasks continuously. In many organizations, these NHIs significantly outnumber human users. Because they often run unattended and operate with broad permissions, they represent a substantial portion of the privileged activity occurring inside enterprise environments.

At the same time, enterprise infrastructure has become more distributed and dynamic. Access rights are no longer concentrated in static administrator accounts but are dispersed across identities, roles, tokens, policies, and application entitlements. Cloud platforms, Software as a Service (SaaS) applications, containerized workloads, and API-driven services create environments where privileges can be granted, modified, or removed in real time as systems are created, scaled, or decommissioned. Privilege therefore becomes a fluid set of capabilities distributed across identities and services rather than a fixed attribute assigned to a specific account.

These changes have expanded the scope of PAM. Traditional PAM solutions focused primarily on credential vaulting, password rotation, and administrative session monitoring. While these functions remain important, they address only a portion of the privileged activity taking place across enterprise infrastructure. Modern PAM solutions extend these capabilities with broader mechanisms for discovering privileged identities, managing credentials and secrets, enforcing policy-driven authorization, providing visibility across environments, leveraging AI and Machine Learning (ML), enabling JIT access, and monitoring privileged actions across systems and services.

Together, these controls support the principle of least privilege by limiting standing permissions and ensuring that elevated access is granted only when required. This is especially critical for AI agents, which typically operate with legitimate credentials and inherited permissions, making dynamic, context-based privilege enforcement at the point of action far more important than authentication alone. Therefore, reducing persistent administrative rights helps minimize the potential impact of compromised accounts or credentials and limits how far an attacker can move once inside an environment.

As identity increasingly becomes the primary control boundary within distributed infrastructures, the management of privilege takes on a central role in enterprise security. PAM solutions provide the mechanisms for governing the most powerful permissions within an organization, ensuring that elevated capabilities, whether exercised by people, machines, or automated processes, are controlled, monitored, and fully auditable.

To better understand the fundamental principles this report is based on, please refer to KuppingerCole's Research Methodology.

Key Findings

- Privilege is increasingly defined by what an identity can do rather than the account it holds. This shifts PAM toward controlling actions rather than managing accounts.
- Demand continues to grow as privileged access remains a primary attack vector. At the same time, new vendors are entering the market to address niche PAM and CIEM use cases.
- PAM is moving beyond password vaulting and session monitoring toward securing hybrid, cloud-native, and machine-driven environments, reflecting the growing role of applications and automated workloads in privileged operations.
- PAM is no longer a standalone domain but part of a broader identity security fabric. This shift is intensifying competition across the market.
- The boundaries between PAM and adjacent identity disciplines are blurring. Vendors are integrating capabilities such as JIT access, threat detection, secrets management, and cloud entitlement controls.
- The convergence of PAM and Identity Governance and Administration (IGA) reflects a shift toward continuous control over how access is granted and used. Governance and enforcement are increasingly happening in real time.
- Key challenges for large organizations include securing NHIs, identifying truly privileged access, managing cloud entitlements, and implementing JIT access. These issues are particularly amplified in complex, dynamic environments.
- SMB-focused vendors are gaining traction with simpler, modular PAM solutions that offer faster deployment and lower complexity. This aligns with organizations that still view PAM as a foundational capability.
- Deployment flexibility remains critical, particularly in regulated and data-sensitive sectors. Vendors are therefore offering a range of deployment models to meet diverse requirements.

Market Analysis

The PAM market is currently undergoing a period of rapid expansion and structural change. Demand continues to grow as organizations recognize that privileged access remains one of the most common pathways for cyberattacks. New vendors enter the PAM market each year, looking to fill niche demands for PAM and CIEM. Additionally, traditional Identity Providers (IdPs) are looking to generate returns in the PAM market, and there is additional

interest from private equity and venture capital investors. KuppingerCole analysts believe there is significant room for growth in this market as it continues to change.

At the same time, the market is evolving beyond its historical focus on vaulting administrator passwords and monitoring privileged sessions. PAM solutions increasingly address hybrid infrastructure, cloud-native environments, and machine-driven access, reflecting the reality that privileged operations are now performed by a mix of humans, applications, and automated workloads. In addition, the boundaries between PAM and adjacent identity disciplines are becoming less distinct. Vendors are responding by integrating capabilities such as JIT access, secrets management, cloud entitlement controls, and deeper integration with identity governance and threat detection systems.

PAM is therefore no longer isolated from the broader identity ecosystem but increasingly functions as part of an integrated identity security fabric. This evolution has also intensified competition. The market now includes established PAM specialists, large cybersecurity platforms, and newer cloud-native challengers, with consolidation and acquisitions reshaping the landscape as identity security becomes a strategic control plane for enterprise defense.

Moreover, the increasing convergence between PAM and IGA illustrates how identity security is shifting toward continuous control over how access is granted, exercised, and reviewed. Historically, IGA governed the lifecycle of access rights through approval workflows and certification processes, while PAM focused on protecting privileged credentials and monitoring administrative sessions. As organizations rely more heavily on automation, cloud services, and machine-driven operations, these distinctions become less clear. Modern identity programs require governance at the moment privileged access is granted as well as real-time control and monitoring when that access is used.

Of course, the maturity and priorities of PAM deployments vary significantly across organizations. Large enterprises are increasingly adopting modern PAM architectures that address machine identities, AI-driven automation, and complex cloud entitlements. Many of these large organizations struggle with:

- Securing NHIs
- Gaining visibility into what access is truly privileged
- Managing cloud entitlements effectively
- Implementing JIT access to reduce standing administrative privileges
- Controlling privilege sprawl across SaaS and multi-cloud environments
- Discovering unmanaged or orphaned privileged accounts and credentials
- Enforcing least privilege consistently across dynamic infrastructure and development environments

However, most vendors developing these advanced capabilities primarily target large enterprises with mature security programs. For many Small and Medium Businesses (SMBs), the immediate priority remains far more foundational: achieving time-to-value and implementing the basic controls that reduce risk quickly. As a result, many SMB-focused vendors have gained traction by offering simpler, modular PAM solutions with lower operational complexity, faster deployment cycles, and clearer licensing models, addressing

the reality that for many organizations PAM is still a foundational security capability rather than an advanced identity security control plane.

From an analyst perspective, the key tension shaping the market is the balance between traditional PAM fundamentals, vaulting, credential rotation, and session oversight, and newer capabilities required to manage machine identities, automation, and ephemeral cloud infrastructure. While large enterprises increasingly demand advanced privilege governance across dynamic environments, many organizations are still focused on solving foundational problems: discovering privileged access, reducing standing permissions, and enforcing least privilege consistently across systems.

Delivery Models

Deployment flexibility remains critical, especially in highly regulated or data sovereignty-sensitive sectors. As a result, PAM vendors offer a variety of deployment models to suit different organizational needs. These models include Fully Hosted SaaS, On-Premises Self-Hosted, Public Cloud Self-Hosted SaaS, Private Cloud Self-Hosted SaaS, Appliance Self-Hosted, or a Hybrid Cloud/On-Premises Vault option. Additionally, some vendors may provide more specialized deployment configurations.

When considering product offerings, it is important to determine whether the vendor provides a fully integrated suite or a set of integrated products or services. Options include a single product, service, or platform; multiple products or services offered in a suite; or functionality that is partially provided through third-party products or services. Other configurations may also be available depending on the vendor.

The deployment of products can vary significantly. Some are installed as software on the customer’s premises, while others may be deployed as an appliance on-site. Additionally, there are options to deploy the product as a cloud service or as a managed service, depending on the organization’s preferences and infrastructure.

Finally, it is worth noting whether the solution operates on a microservices architecture, which can be particularly relevant for those considering On-Premises Self-Hosted deployment models.

Required Capabilities

This Leadership Compass analyzes which PAM offerings in the market are best suited to enabling the following capabilities:

- Privileged Account and Identity Lifecycle Management
- Privilege Elevation and Delegation Access Management
- Dashboarding and Analytics
- CIEM capabilities

- Authentication
- DevOps Support
- Credential, Secrets, and Key Management
- Ephemeral Credential Support
- Platform and System Integration Support
- Privileged Session Management (PSM)
- Session Recording and Monitoring (SRM)
- Endpoint Privilege Management (EPM)
- Privileged User Entity Behavior Analytics (PUEBA)
- JIT Provisioning
- Fine Grained Access Control
- Administration Support
- Product Integrations
- Quality Assurance and Professional Services

We expect solutions to cover most of these capabilities, and in addition to delivering functionality to support them, must also meet our requirements for deployment and interoperability with other security tools.

Deployment can be on-prem, in the cloud, or hybrid, but solutions that provide the most flexibility in deployment options and the best coverage of modern IT environments will score more highly.

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

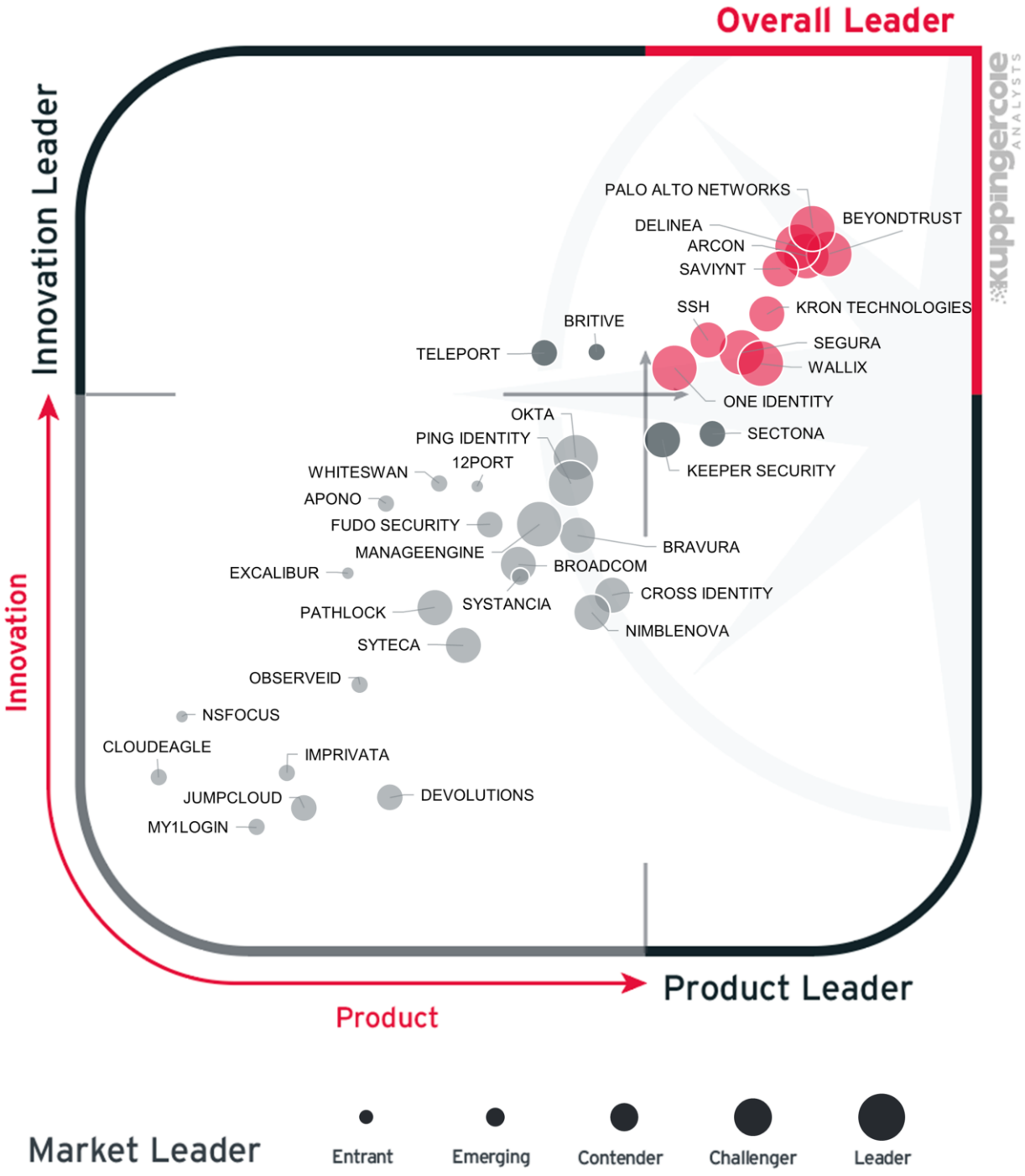


Figure 1: Overall Leadership in the PAM market

The Combined Leadership chart provides insights into Product, Innovation, and Market Leadership. Vendors that obtained both Product and Market Leadership are displayed in the upper right quadrant. The position in Market Leadership is indicated via the size of the bubbles. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and its products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

The Overall Leadership view highlights a group of vendors that combine strong product depth with sustained innovation, positioning them to address both traditional PAM requirements and emerging identity security challenges. At the forefront are Idira, Delinea, BeyondTrust, ARCON, and Saviynt, which demonstrate leadership across product capabilities and innovation. These vendors provide comprehensive PAM platforms covering credential and secrets management, session monitoring, EPM, and increasingly cloud-native and machine-driven access. Closely behind, we see Kron Technologies, SSH, Segura, WALLIX, and One Identity.

Innovative challengers such as Teleport and Britive are redefining how privileged access is delivered. While these vendors may not yet match the scale of the leaders, they are shaping the future direction of PAM, particularly for cloud-native environments and emerging agentic identity models. Identity platform vendors such as Okta and Ping Identity are expanding into PAM, often through acquisitions and platform convergence strategies. However, their PAM capabilities are still evolving compared to more specialized vendors.

A distinct segment of the market is driven by vendors targeting SMBs, such as NSFOCUS, nimbleNOVA, and Devolutions, which prioritize simplicity, rapid deployment, and lower operational overhead. While these vendors increasingly support cloud-native environments and NHI use cases, they primarily address organizations focused on establishing foundational PAM capabilities before expanding into more advanced privilege management models. Regional dynamics are also visible, with European vendors such as Excalibur, Systancia, My1Login, and Fudo Security gaining traction, particularly in sovereignty-sensitive environments. These vendors often differentiate through local compliance alignment, data residency, and support for regulated industries, making them attractive in public sector and critical infrastructure contexts.

Finally, a new generation of younger and innovative vendors, including 12Port, CloudEagle, Apono, and Whiteswan, is emerging with focused and differentiated approaches to PAM. These companies often target specific gaps, such as agentless access brokering, SaaS access governance, context-based decision engine, or identity threat detection, and bring fresh perspectives to privilege management. While still early in their growth, they highlight how the PAM market continues to evolve toward more granular, context-aware, and automated access control models.

Product Leadership

Product Leadership is the first specific category examined below. This view is based on the presence and completeness of required features as defined in the required capabilities section above. It provides a unidimensional, linear perspective, with the Product Leaders to the right. The best positioned vendors in this category are to the far right.

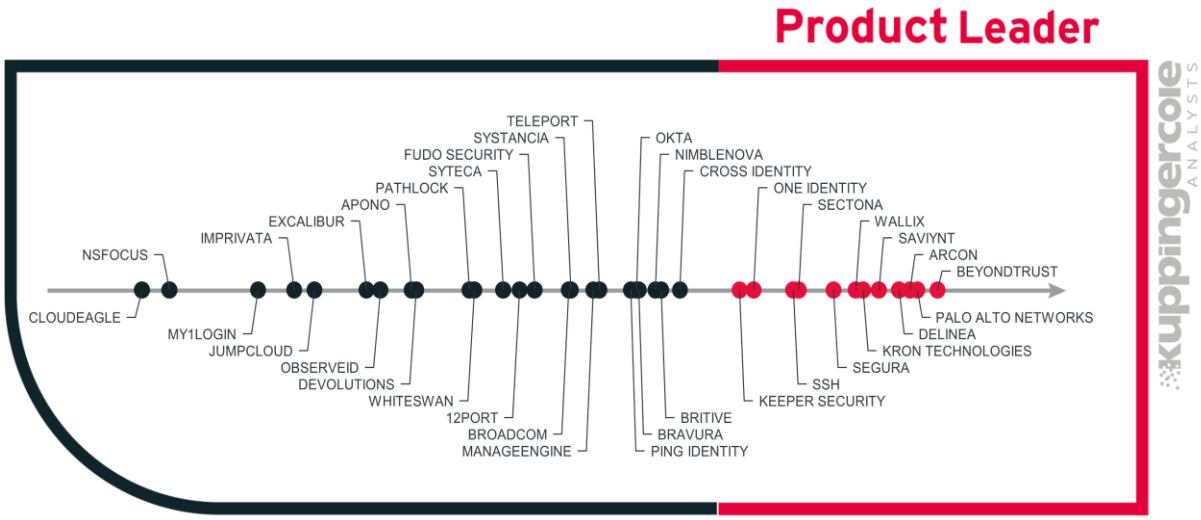


Figure 2: Product Leadership in the PAM market

The Product Leaders in PAM are those vendors that deliver broad, consistent, and well-integrated coverage across both foundational and advanced capabilities, enabling them to support a wide range of enterprise use cases. These solutions typically combine strong performance in credential and secrets management, session management and monitoring, EPM, and policy-driven access control, while also extending into cloud-native environments, DevOps workflows, and identity discovery. Product Leaders distinguish themselves through depth of functionality, scalability, and the ability to operate across hybrid infrastructures, making them suitable for large and complex deployments where multiple privileged access scenarios must be addressed within a unified platform.

Vendors positioned outside the leadership segment, in the Challenger category, often demonstrate strength in specific areas or targeted use cases, but may lack the same level of completeness or integration across the full PAM capability spectrum. Common gaps include limited support for cloud-native and DevOps environments, weaker EPM, less mature identity discovery and visibility, or insufficient policy-driven and context-aware access controls. In some cases, these solutions may also lack tight integration with adjacent systems such as identity governance, access management, or threat detection and response platforms, which are increasingly important in modern identity security architectures.

That said, Challenger vendors can still provide strong value, particularly for organizations with focused requirements, specific infrastructure constraints, or a need for faster

deployment and reduced complexity. In these cases, selecting a solution that excels in a defined area may be more appropriate than adopting a fully integrated platform.

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is a key capability in all IT market segments. Customers require this to meet evolving and even emerging business requirements. Innovation is not about delivering constant new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. It provides a unidimensional, linear perspective, with the Product Leaders to the right. The best positioned vendors in this category are to the far right.

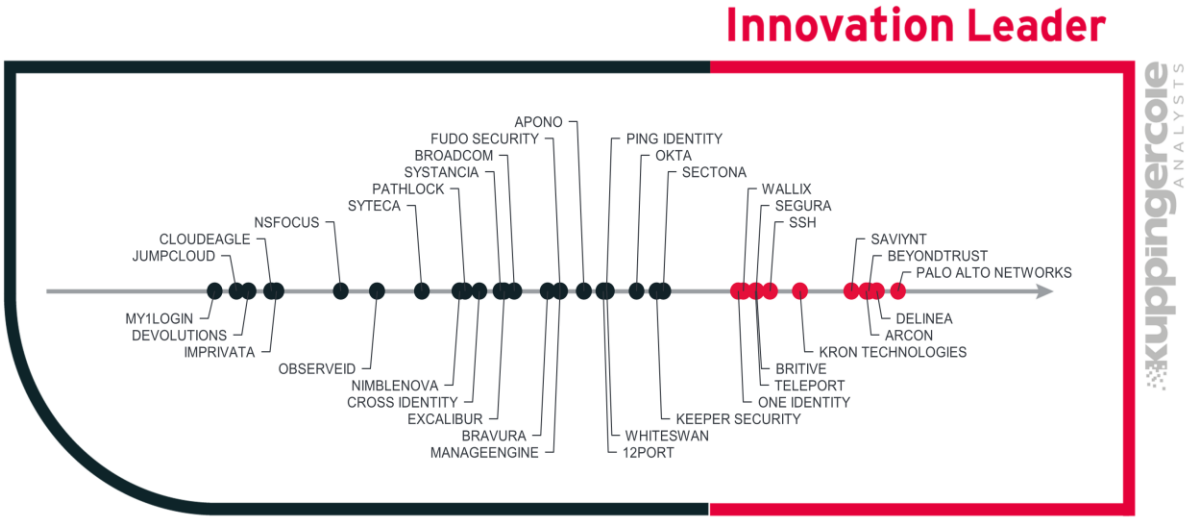


Figure 3: Innovation Leadership in the PAM market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

For the 2026 LC PAM, the Innovation Leadership view highlights a market undergoing a clear shift from traditional, credential-centric models to dynamic, policy-driven privilege enforcement across cloud-native and machine-driven environments. Leading vendors such as Idira, Delinea, BeyondTrust, ARCON, and Saviynt continue to anchor the market while evolving toward broader identity-centric control planes. At the same time, a new wave of innovation, driven by vendors like Kron Technologies, SSH, Britive, Segura, Teleport, and One Identity, are accelerating the adoption of short-lived credentials, JIT access, and granular, policy-based entitlement control, particularly for cloud-native architectures and emerging agentic identity models.

Market Leadership

This chart shows the market strength of vendors plotted on the horizontal axis. The chart divides vendors into five categories Leaders, Challengers, Contenders, Emerging, and Entrants. The Market Leaders, shown to the right of the chart and colored red, are those with market dominance and high influence. Market Challengers, shown to the left of leaders and colored black, are strong competitors with significant market presence and growth potential. Contenders, shown in in grey, are solid players with a stable position and reliable offerings. Emerging vendors with a growing presence and the potential for further market impact are colored light grey. Entrants, shown to the left of the chart, are newcomers or smaller players just beginning to establish market presence.

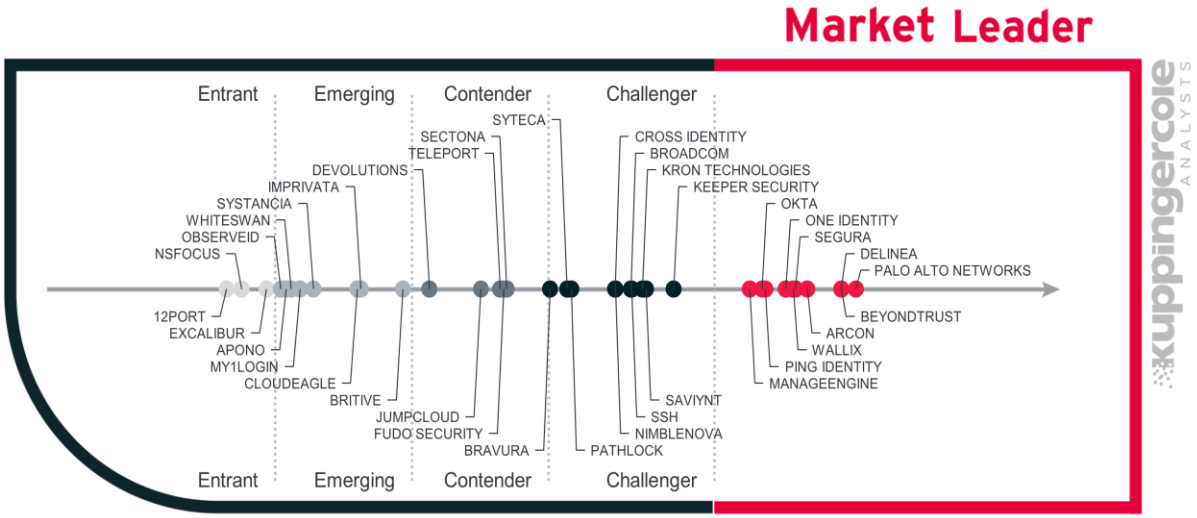


Figure 4: Market Leaders in the PAM Market

Market Leaders, positioned on the far right, include Idira, Delinea, BeyondTrust, ARCON, Segura, One Identity, WALLIX, Ping Identity, Okta, and ManageEngine. These vendors demonstrate strong enterprise adoption, broad capability coverage across traditional and modern use cases, global coverage, and the ability to operate at scale in complex, hybrid environments. Their positioning reflects mature offerings that span credential management, session control, and increasingly cloud and machine access use cases.

Challengers, located just to the left of the leaders, include vendors such as Keeper Security, Kron Technologies, Saviynt, Broadcom, SSH, Cross Identity, and nimbleNOVA. These vendors show solid market traction and expanding capabilities but may be more specialized, regionally focused, or still evolving toward full platform maturity. Many are strengthening their PAM capabilities through convergence with Identity and Access Management (IAM), IGA, or cloud security.

Contenders, and other mid-tier players, demonstrate stable offerings and credible execution within defined segments. These vendors often address specific enterprise requirements or regional markets effectively but may lack the global scale, ecosystem depth, or breadth of functionality seen in the leader segment.

Emerging vendors represent a dynamic and innovative segment of the market. These players often focus on modern use cases, including cloud-native access, developer-centric workflows, and machine identity management. While they show strong growth potential, their market presence and enterprise penetration are still developing.

Finally, Entrants are early-stage or niche providers. These vendors typically target specific use cases such as healthcare access, SaaS governance, or lightweight PAM deployments, and are in the process of establishing broader market relevance.

Overall, the market reflects a dual dynamic: strong demand for traditional PAM capabilities continues to anchor the leader segment, while innovation is increasingly driven by emerging vendors addressing cloud-native, machine-driven, and developer-centric access models.

Product/Vendor Evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider Graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For this market segment, we look at the following categories:

Just In Time Access –This category evaluates the vendor's capability to provide secure, on-demand access to privileged resources, which is activated only when needed, thereby minimizing the risks associated with prolonged or unnecessary access.

Session Management & Monitoring – This evaluates the vendor’s capabilities to establish, monitor, record, and control privileged sessions. It includes real-time session oversight, activity logging, session recording and playback, and the ability to intervene or terminate sessions to ensure accountability, auditability, and rapid incident response.

Credentials, Secrets, & Key Management – This measures the vendor’s ability to securely store, manage, and rotate privileged credentials, including passwords, SSH keys, API tokens, and certificates. It includes vaulting, automated rotation, secure retrieval, and support for both human and machine credentials across hybrid environments.

AI/ML Assistance – This evaluates the vendor’s integration of AI and ML to enhance system functionalities, such as automating processes, usability, threat detection, predicting potential issues, and improving operational efficiency.

Endpoint Privilege Management (EPM) – This evaluates the vendor’s ability to control and enforce least privilege on endpoints and servers by removing standing administrative rights and enabling policy-based privilege elevation. It includes capabilities such as application-level elevation, command control, and cross-platform support (Windows, macOS, Linux) to manage privileged actions at the device level.

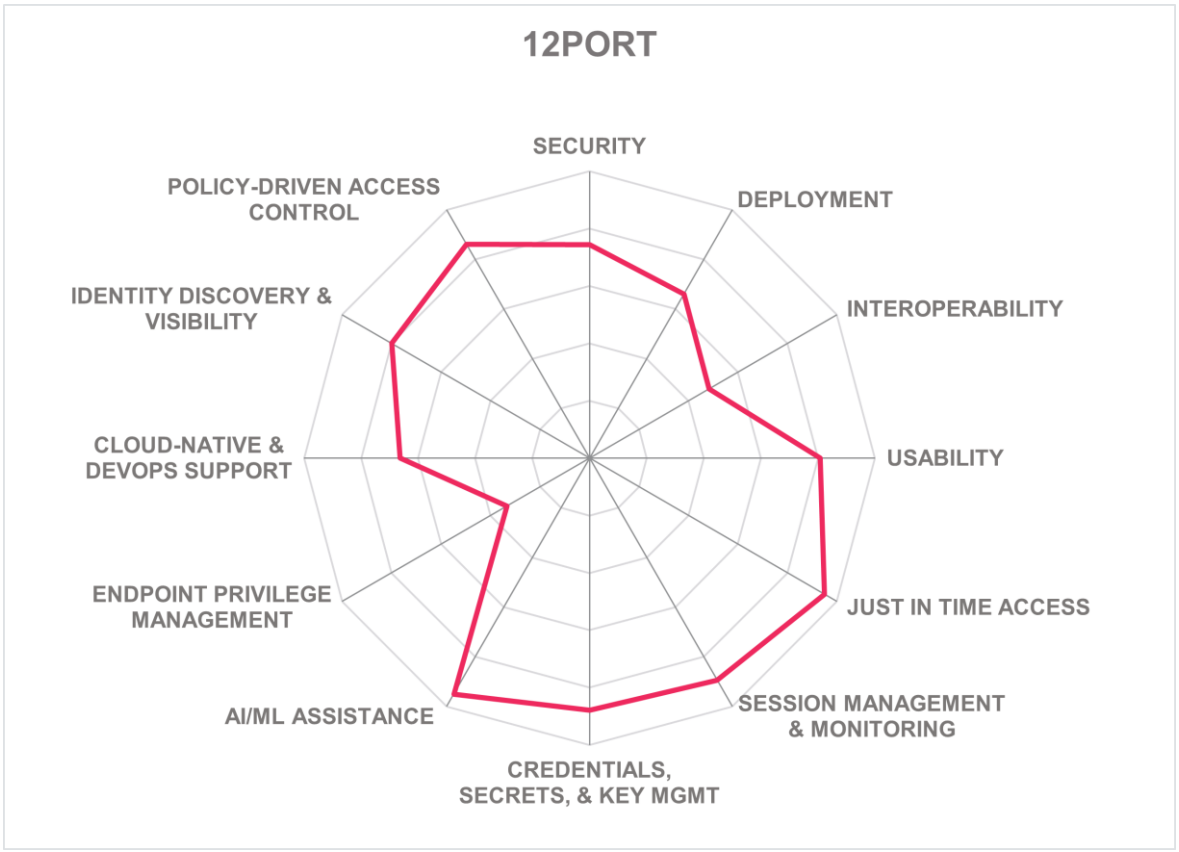
Cloud-Native & DevOps Support – This assesses the vendor’s ability to secure privileged access across cloud and DevOps environments, including infrastructure-as-code, containers, and Continuous Integration and Continuous Delivery (CI/CD) pipelines. It covers integration with cloud platforms, support for dynamic and ephemeral workloads, and the management of privileges in modern, API-driven and automated environments.

Identity Discovery & Visibility – This evaluates the vendor’s ability to continuously discover, inventory, and provide visibility into identities, credentials, and access relationships across systems, including users, service accounts, workloads, and tokens. It ensures

organizations can identify where privileged access exists, understand how it is used, and maintain ongoing oversight of access across hybrid and cloud environments.

Policy-Driven Privileged Access Control – This assesses the vendor's ability to enforce fine-grained, context-aware policies that govern when and how privileged access is granted. It includes JIT access, approval workflows, and dynamic authorization based on factors such as user, device, location, and risk, ensuring that privileged actions are tightly controlled and aligned with least privilege principles.

12Port – 12Port PAM



12Port is a privately held self-funded vendor headquartered in Eagleview, Pennsylvania, in the US. Founded in 2024, 12Port focuses on PAM for mid-market and large enterprise customers. Its PAM platform brings together vaulting, brokered access, workflow controls, and audit capabilities in a software-based product designed for straightforward deployment and phased adoption. The solution is available through a wide set of delivery models, including self-hosted on premises, public or private cloud, appliance-based deployments, Managed Service Provider (MSP)-hosted SaaS, and a mixed vault model for organizations that need greater control over credential storage. It supports high availability, disaster recovery, multi-site operation, and multitenancy, which also makes it suitable for service providers. As a relatively new entrant in this market, it is not surprising that 12Port has not obtained security certifications yet. Licensing is per user. The company's current customer base is concentrated in North America, with growing activity in Europe, Middle East, and Africa (EMEA).

12Port combines vault-centric and session-centric controls in one product, allowing organizations either to broker privileged access without exposing credentials or to support controlled credential checkout when that remains necessary. Passwords, SSH keys, API keys, tokens, certificates, and other secrets are stored in the vault under role-based controls, policy enforcement, and full audit logging. Privileged access is mediated through brokered via Web or Native clients for Remote Desktop Protocol (RDP), SSH, PowerShell, and HTTPS sessions with credential injection, while approvals, MFA, and separation of duties help constrain misuse. The platform also addresses third-party access well, with policy-driven workflows that make vendor access more governable and easier to audit. Its agentless design differentiates it from some of its competitors. Discovery includes imports from sources such as Lightweight Directory Access Protocol (LDAP), Microsoft Entra ID, Amazon Web Services (AWS), VMware, and CSV, along with privileged account discovery on Windows endpoints; however, it relies on scheduled scans rather than continuous, real-time discovery. 12Port integrates with IdPs such as Microsoft Entra ID, Okta, Ping Identity, and OneLogin.

Dashboards and reports span sessions, access rights, and workflow activity, with executive and audit views as well as exportable reporting for compliance processes. The Assets Access Report is useful because it shows who can access which assets and how those permissions were granted. The platform integrates with common authentication providers, directory services, and MFA tools, while Representational State Transfer (REST) APIs enable onboarding and workflow integration. For infrastructure coverage, 12Port supports environments across AWS, Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle, VMware, and selected OT and Industrial Control Systems (ICS). JIT access is enforced through time-bound action requests, approval workflows, and per-asset access profiles. Session monitoring includes recording, command-level activity indexing, and policy controls that can restrict commands, terminate sessions, revoke temporary privileges, or block users. Session Intelligence extends this with baseline analysis and configurable AI-assisted review. In addition, 12Port supports AI agent integration through an MCP (Model Context Protocol) server, which provides a secure and standardized interface for AI-driven processes to discover authorized data sources, request access through approval workflows, and obtain credentials for connecting to external systems under controlled policy enforcement. Credential and secret lifecycle management is also solid, including onboarding, policy-based issuance, automated rotation, revocation, and replacement. 12Port also integrates with IT Service Management (ITSM) tools such as ServiceNow and JIRA. However, the solution lacks EPM features and does not currently support third-party vault interoperability. Additionally, CI/CD support remains limited to API-based automation without deeper pipeline integration capabilities.12Port is still a young company, but the product already shows a degree of completeness that is uncommon for a vendor at this stage. Its strongest innovations lie in the combination of agentless access brokering, workflow-driven control, and AI-assisted session review that can support both investigation and immediate action. Nevertheless, as a relatively new entrant, the company has a limited track record and a less mature partner ecosystem compared to more established competitors. 12Port appears well suited to organizations that want broad PAM capability, flexible deployment, and tighter control over privileged sessions and secrets without the operational weight of older platforms.

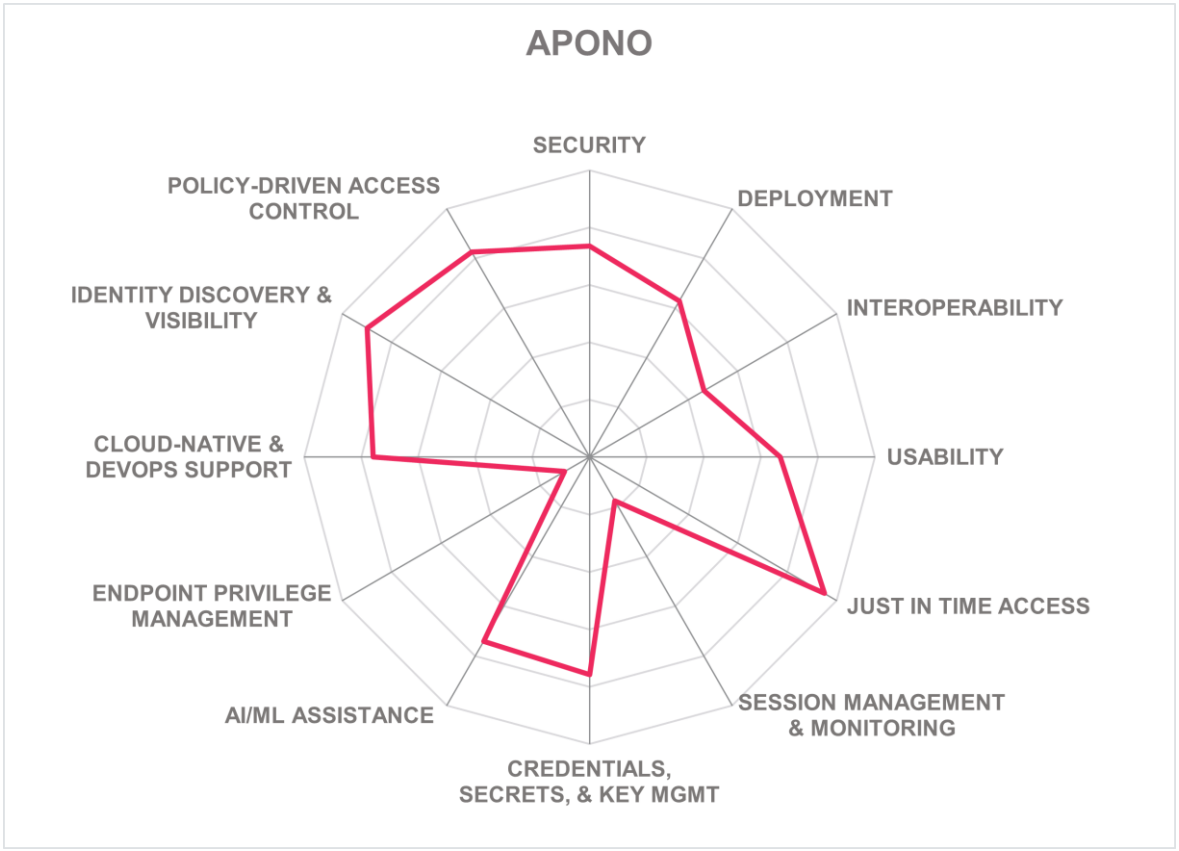
Strengths

- Agentless architecture across web and native access
- Well-developed vaulting for passwords, keys, and secrets
- Useful workflow-driven JIT access controls
- Full REST API including MCP server for AI Agents
- Good session monitoring with actionable policy enforcement
- Multitenant design suits MSSP and service provider models
- AI-assisted session analysis and review
- Fully integrated, unified platform specifically designed for cloud-native workload security

Challenges

- New market entrant with limited track record
- Channel-led growth may take time to mature
- No traditional EPM capability
- No support for third-party vault interoperability
- Limited CI/CD depth beyond core API-based automation
- Lack of key security certifications

Apono – Apono Privilege Cloud Platform



Founded in 2022 and headquartered in New York, in the US, with an office in Tel Aviv, Israel, Apono is a privately held company focused on privileged access for cloud-centric and hybrid environments. Its access management platform has separate modules for legacy infrastructure and cloud environments, and is delivered primarily as a SaaS offering, with options spanning fully hosted SaaS, self-hosted public or private cloud SaaS, and a vault option for organizations that require part of the control plane to remain closer to their own infrastructure. It has SOC 2 Type II and GDPR security certifications. Licensing is modular and based on the number of identities under management. Apono's current focus is on mid-market and emerging enterprise organizations, particularly in North America, with growing activity in EMEA and Asia-Pacific (APAC).

Apono's platform takes a ZSP approach to both humans and AI agents. It is designed to replace persistent access with JIT, policy-controlled access across cloud infrastructure, databases, Kubernetes, servers, and selected developer-facing systems. Its central differentiator is a context-based decision engine that evaluates user attributes, target

resources, and environmental signals at request time, then provisions access only for the task at hand. This is paired with dynamic role creation, allowing permissions to be assembled on demand rather than pre-built and maintained as static roles. Apono also introduces access scopes, which are saved and self-updating resource groupings derived from discovery and filtering. As environments change, newly discovered resources are brought into existing guardrails automatically. This is a useful idea in organizations where cloud sprawl and frequent infrastructure changes tend to outpace manual policy upkeep. In addition, Apono integrates with IdPs such as Okta, Ping Identity, JumpCloud, GCP, and Microsoft Entra ID.

Apono supports discovery of privileged users and service accounts across AWS, Azure, and GCP, with CIEM functions that identify standing, dormant, and overprivileged access and recommend corrective action. JIT access is available for humans and NHIs through a lightweight connector deployed in the customer environment, avoiding changes to existing user workflows. Access requests can be initiated through Slack, Teams, command-line interface (CLI), Terraform, APIs, or MCP-enabled LLM workflows. Apono supports user self-service workflows and integrates with ITSM platforms such as ServiceNow and Jira. The platform also supports ephemeral credentials, including SSH certificates, Kubernetes CA credentials, and database credentials, with automated rotation based on time, event, policy, or risk. Dashboards show access activity, anomalies, integrations in use, and attack surface reduction, though customization is limited and there is no real-time threat alerting. Built-in reports map relationships between identities and the systems, accounts, and privileged resources they can reach, which is useful for both internal review and audit preparation. Session auditing is present, but full session recording, playback, monitoring, and review remain absent. Moreover, EPM, OT and ICS support, and full DevOps secrets lifecycle coverage are not currently available.

Apono’s recent product direction is especially interesting where agentic usage is beginning to intersect with privilege control. The platform uses Generative AI (GenAI) to help users formulate requests, create queries and policies, and support copilot-style workflows through MCP servers for both end users and administrators. It also extends policy controls to autonomous AI-driven access requests using the same ZSP approach, adding visibility and intent-based guardrails where many organizations still lack a coherent operating model. That said, Apono remains more focused on cloud privilege orchestration than on the broader range of traditional PAM controls, and some buyers will still expect deeper session monitoring capabilities and broader endpoint coverage. Even so, the product shows a clear point of view: reduce persistent privilege, keep access decisions close to operational context, and let developers and operators work from the tools they already use. Apono is well suited to organizations that want cloud-focused PAM with strong JIT access controls and less administrative drag.

Strengths

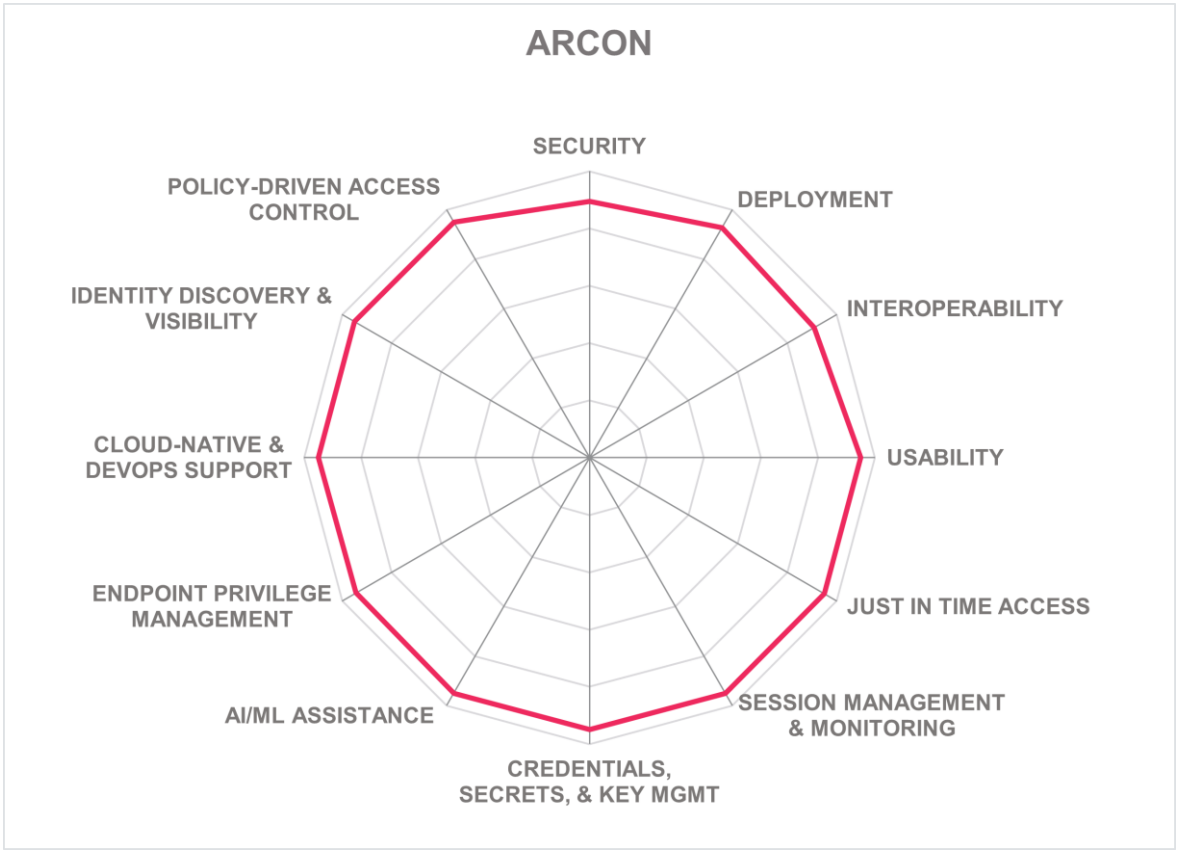
- Dynamic JIT access across major cloud platforms
- Context-based access decisions reduce standing privilege significantly
- Access scopes adapt automatically to infrastructure changes
- Broad integration with developer and ITSM workflows

- Ephemeral credential support for humans and NHIs
- Granular cloud and database entitlement control
- Useful CIEM visibility for dormant and excessive access
- GenAI improves request and policy creation

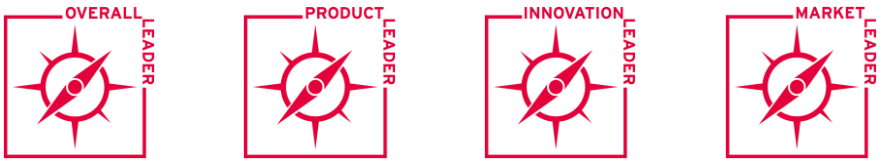
Challenges

- Limited brand recognition outside North America and Israel
- Smaller partner ecosystem compared with competitors
- Session recording and playback are not available
- Dashboards lack customization and real-time threat alerting
- No full secrets lifecycle support for DevOps use cases
- EPM and OT/ICS support missing

ARCON – ARCON PAM



Leadership



With headquarters in Mumbai, India, ARCON is a privately held company focused on identity security and PAM. The company has built a presence across North America, EMEA, APAC, and Latin America (LATAM), serving mid-market and large enterprises across sectors such as banking, government, telecom, and manufacturing. ARCON's core offering is its converged PAM platform, which integrates privileged access, identity governance, and analytics into a unified control plane, complemented by ARCON Digital Vault for centralized secrets, credentials, and key management. The solution is delivered across multiple deployment models, including on-premises, SaaS, appliance-based, and MSP-hosted options, with consistent functionality across environments. ARCON states that it has

achieved certification for the International Organization for Standardization's Information Security Management Systems standard (ISO 27001) and SOC 2 Type II. Licensing is based on users, time periods, and nodes, supporting a range of enterprise deployment scenarios.

ARCON's solution aims to govern human and NHIs, including service accounts, APIs, certificates, and automation workloads. Privileged access is brokered through secure gateways using ephemeral credentials and time-bound access, enforcing ZSP. ARCON Digital Vault plays a central role by securing credentials, secrets, API keys, and cryptographic keys with automated rotation and lifecycle governance, while integrating with external Hardware Security Modules (HSMs) and Key Management Service (KMS) systems. The platform emphasizes policy-driven access tied to identity context, asset criticality, and operational intent. A distinguishing aspect is its approach to session intelligence, where activity is not only recorded but interpreted through intent-driven analysis, allowing organizations to understand what actions were performed and why, improving auditability and reducing reliance on manual session reviews. Dynamic application and device binding enforces execution of applications only through PAM-controlled workflows by linking user identity, endpoint, and application via one-time tokens, strengthening endpoint security and access control. ARCON integrates with IdPs such as Microsoft Entra ID, Okta, Ping Identity, AWS, GCP, OneLogin, and 1Kosmos.

Session management also includes full monitoring of commands, keystrokes, and queries, with correlation between textual logs and video playback. ARCON supports JIT access through time-bound provisioning and automatic de-provisioning, with continuous evaluation during sessions based on risk signals. AI/ML capabilities enable the detection of anomalous privileged activity through behavioral profiling and risk scoring. The platform provides detailed dashboards with entity-level visibility and drill-down capabilities, complemented by extensive reporting across access, governance, and security domains. Moreover, the solution allows for direct integration with response workflows for Identity Threat Detection and Response (ITDR) use cases, including session termination, access revocation, and step-up authentication. EPM is integrated, allowing controlled elevation and enforcement of application-level restrictions tied to PAM workflows. Support extends to cloud platforms, DevOps pipelines, APIs, and OT environments, providing broad coverage across infrastructure types.

ARCON's platform reflects a consistent effort to unify access control, governance, and analytics within a single system, with particular attention to machine identities and operational workflows. Its use of internally developed AI models allows organizations to maintain control over sensitive data while still benefiting from advanced analytics and contextual insights. The platform supports a wide range of environments, including cloud infrastructure, DevOps pipelines, APIs, and OT systems, making it applicable to infrastructure-heavy and regulated organizations. With an established customer base and presence across multiple regions, ARCON is positioned for organizations seeking a consolidated approach to privileged identity security that extends beyond traditional vaulting into identity-driven monitoring and response.

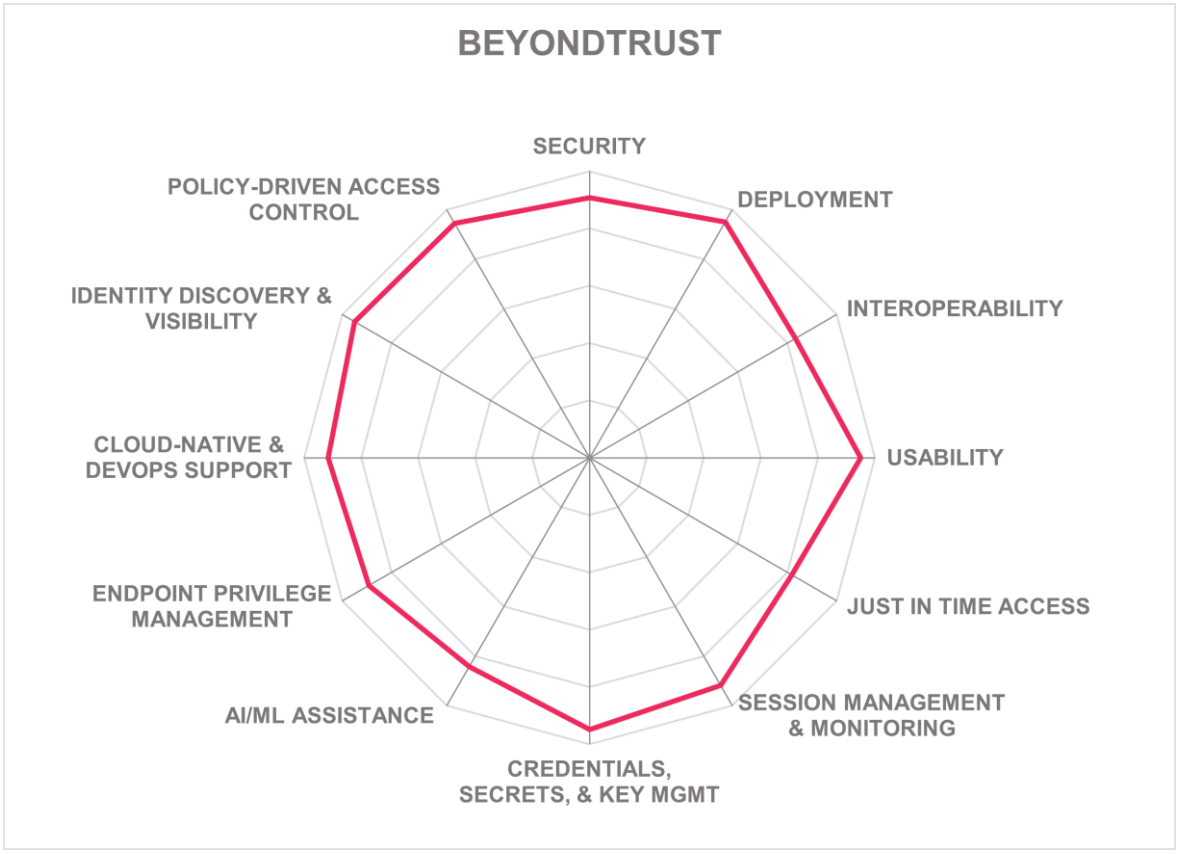
Strengths

- Good coverage for machine and NHIs
- Intent-based session analysis improves investigation efficiency
- Direct integration with ITDR response workflows
- AI/ML-driven risk scoring and behavioral analytics
- Granular session monitoring with precise forensic capabilities
- Policy-driven JIT access enforcement
- Dynamic application and device binding enforces strict control over application execution on endpoints
- Centralized control across privileged access, identity governance, and secrets management reduces operational fragmentation

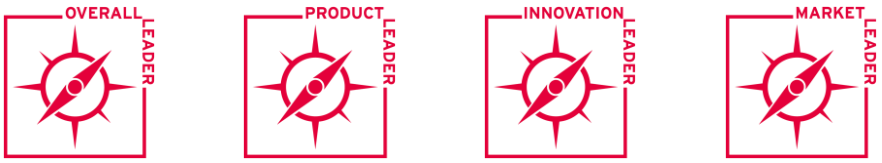
Challenges

- FedRAMP and other certifications could improve appeal in US public sector
- Platform scope may increase implementation complexity, but its modular and phased deployment approach allows organizations to start with only the necessary components and expand over time

BeyondTrust – Pathfinder



Leadership



Founded in 2003 and headquartered in Johns Creek, Georgia, in the US, BeyondTrust is a long-established vendor in privileged access and identity security. Privately held by Francisco Partners and Clearlake Capital, the company has broadened its PAM strategy around the BeyondTrust Pathfinder platform. Pathfinder acts as the unifying platform that brings together BeyondTrust's identity security capabilities across PAM, ITDR, CIEM, and broader identity governance. Within this platform, BeyondTrust's PAM portfolio is centered on Password Safe, Privileged Remote Access, Identity Security Insights, EPM, and Entitle. Deployment flexibility is one of BeyondTrust's main attributes: the platform is available through virtual appliances for Windows and Linux, self-hosted deployments (on-premises

and private cloud), hosted SaaS, appliance-based options, MSP delivery, and vault options for mixed environments. Licensing spans per user, per node, per server, per appliance, time-based, fixed-cost, and personnel-based models. BeyondTrust is certified under ISO 27001/27701, ISO 15408 (Common Criteria), and SOC 2 Type II compliant. It is also authorized under FedRAMP and aligns with FIPS-related requirements, and PCI DSS. The company targets organizations of all sizes across sectors including critical infrastructure, healthcare, utilities, and industrial environments.

Pathfinder and Identity Security Insights extend that idea by mapping what BeyondTrust calls true privilege, showing how privilege paths form across Microsoft Active Directory and Entra ID, cloud platforms, SaaS, endpoints, and NHIs. This gives the platform a broader field of view than traditional vault-first PAM. It can discover privileged accounts, service accounts, secrets, roles, policies, and privilege relationships, then connect those findings to risk scoring and actionable remediation. However, it does not extend to detecting hard-coded credentials in scripts or cleartext credentials within configuration files. BeyondTrust also pushes further into AI agent governance, offering discovery, privilege mapping, and risk assessment for agents in Azure, Copilot, AWS, GCP, Google Vertex, OpenAI, Salesforce, and ServiceNow. Additionally, BeyondTrust supports OT environments by enabling secure remote access, credential management, and policy-based least privilege controls for industrial systems, including legacy and non-routable assets. It also integrates with IdPs such as Microsoft Entra ID, Okta, JumpCloud, OneLogin, and Google Workspace.

BeyondTrust delivers a broad functional set across core PAM and adjacent privilege controls. Pathfinder provides configurable dashboards for high-risk accounts, identity threats, secrets, NHI and AI identities, MITRE ATT&CK®, NIST 800-53, and cloud identity risk, supported by drill-down reporting, scheduled exports, and executive Key Performance Indicators (KPIs). Session management is mature, with monitoring, recording, keystroke logging, and session termination for RDP, SSH, HTTPS, Virtual Network Computing (VNC), SQL, and mixed IT and OT access scenarios. Its vaulting and secrets capabilities cover passwords, SSH keys, X.509 certificates, and integrations with external secret stores such as AWS Secrets and HashiCorp, while Secrets Safe supports API-driven automation and scheduled rotation for DevOps use cases. BeyondTrust also supports JIT and ephemeral access in several forms, including time-bound entitlements, single-use credentials, short-lived certificates for SSH access, temporary admin elevation, and ephemeral account provisioning. EPM extends least-privilege controls across Windows, macOS, Unix, and Linux. On the cloud and DevOps side, the platform supports SaaS services, REST APIs, webhooks, policy-based workflows, and CI/CD tooling such as Jenkins, GitHub, GitLab, Kubernetes, Terraform, and Ansible.

A distinguishing part of BeyondTrust’s recent evolution is the way it combines privilege control with identity analytics rather than treating these as separate domains. Identity Security Insights applies AI and ML to normalize identity data, reduce noise, and produce detections and recommendations with useful context. That same analytical model now extends into AI agents, machine identities, and cross-domain privilege relationships, giving customers a better picture of who or what can reach sensitive systems and secrets. The company also continues to show practical strength in regulated and operationally complex environments, particularly where IT, OT, remote vendor access, and cloud entitlements

intersect. BeyondTrust remains strongest in North America, but its footprint is growing in EMEA, APAC, and LATAM. It is particularly well suited for organizations that want broad PAM coverage tied to identity visibility, JIT controls, and strong support for heterogeneous enterprise environments.

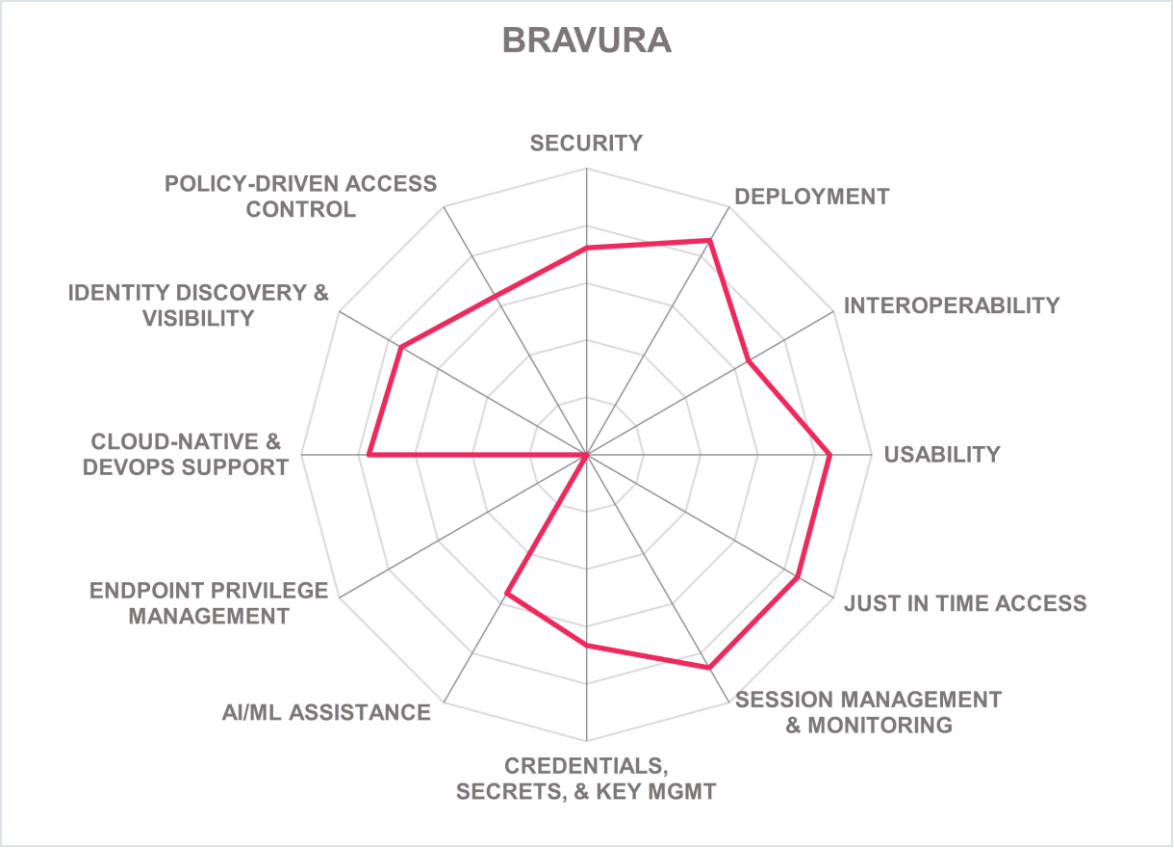
Strengths

- Broad PAM security coverage across human and NHIs, including AI agents
- Advanced JIT and ephemeral access capabilities
- Mature session monitoring for IT and OT
- Cross-domain privilege graph improves risk visibility
- Extensive integrations across identity and DevOps ecosystems
- Robust secrets, key, and certificate management
- Useful dashboards and compliance-aligned reporting
- EPM extends least-privilege control across major operating systems
- Unified visibility and analysis of the entire environment, including on-premises systems, AD, cloud IDPs, CSPs, and SaaS applications

Challenges

- Lack of application sandboxing capabilities
- European certification coverage remains limited
- Breadth of capabilities may require careful product scoping

Bravura Security – Bravura Security Fabric



Headquartered in Calgary, Alberta, in Canada, Bravura Security is a privately held vendor with a long presence in identity and privileged access. Its PAM offering, Bravura Privilege, is delivered as part of the broader Bravura Security Fabric, a unified platform that also includes identity and governance capabilities. The product is available as fully hosted SaaS, MSP hosted SaaS, self-hosted deployments in public or private cloud, on premises, and mixed vault arrangements spanning cloud and on premises environments. Bravura Security has SOC 2 Type II certification for its SaaS service, though it lacks certification for ISO 27001. Licensing is offered through per server, per transaction, per user, and fixed-cost models. The company targets mid-market organizations and large enterprises across sectors such as manufacturing, higher education, financial services, and healthcare.

Bravura Privilege is best understood not as an isolated PAM tool, but as part of a broader identity fabric where privileged access can be tied directly to identity lifecycle, governance, and policy. That architectural choice is one of its main differentiators. Rather than treating vaulting as the center of gravity, Bravura Security places equal weight on automation, managed-system integration, and policy-governed access flows. The platform supports

encrypted vaulting, password randomization and rotation, controlled disclosure, and brokered access that keeps credentials hidden from users where required. It manages privileged passwords and accounts for human and non-human access paths, including service accounts, while also supporting vault-only storage for secrets that cannot be rotated automatically. The solution supports JIT by granting time-bound privileged capability only for the approved window, using multiple methods so customers can choose the least-privilege approach per use case. JIT can also be applied to personal admin accounts, ephemeral accounts, shared accounts, and high-level built-in administrative accounts using request/approval policy, strong controls on disclosure, and auditing. The Bravura Security Fabric also integrates with IdPs such as Okta, Microsoft Entra ID, Ping Identity, SecureAuth, and Keycloak.

The platform provides mature operational coverage in several important PAM areas. It includes interactive dashboards, graphical summary reporting, and more than 180 built-in reports, including relationship-based reporting on users, groups, systems, and privileged accounts. Session management is one of the stronger parts of the product: Bravura Privilege records screen activity, keyboard input, and related telemetry, supports real-time and after-the-fact playback, allows authorized reviewers to search and replay sessions, and can disconnect sessions when monitoring is interrupted or specific alert conditions are met. Credential handling is also well developed, with encrypted vaulting, scheduled and event-driven password rotation, service account orchestration, and API-based secret retrieval for automation use cases. For cloud and infrastructure coverage, Bravura supports major cloud platforms including AWS, Azure, GCP, Oracle, Alibaba Cloud, IBM Cloud, VMware Cloud, OVH Cloud, and Rackspace, while also extending to network devices, legacy systems, and OT environments through native and scriptable connectors. Discovery goes beyond accounts, covering entitlements, service dependencies, local groups, scheduled jobs, IIS components, DCOM objects, and SSH trust relationships. The product also benefits from close alignment with IAM and IGA processes inside the same platform. It does not support PUEBA, which limits its ability to add behavior-driven analytics to privileged activity. It also lacks EPM, dedicated DevOps-oriented secrets management, certificate-based authentication for users and machine identities, and broader key management functions.

Bravura Security's recent direction shows a vendor modernizing with purpose rather than chasing feature inflation. Its migration from IdentityServer4 to OpenIddict improves long-term interoperability and brings the platform into line with current OAuth 2.1 and OpenID Connect (OIDC) expectations. The ongoing React-based interface rebuild, including widget-driven dashboards and better accessibility, should also improve day-to-day administration. Bravura Security does not currently use ML in the product, but it has taken a practical "bring your own AI" route, aligning its APIs and planned MCP server with external AI platforms for analytics, reporting, and administrative assistance. With customer presence across North America, EMEA, APAC, and LATAM, Bravura Security has clear relevance for enterprises that want PAM tied closely to governance, identity workflows, and broad connector coverage, especially in complex environments where legacy systems still matter.

Strengths

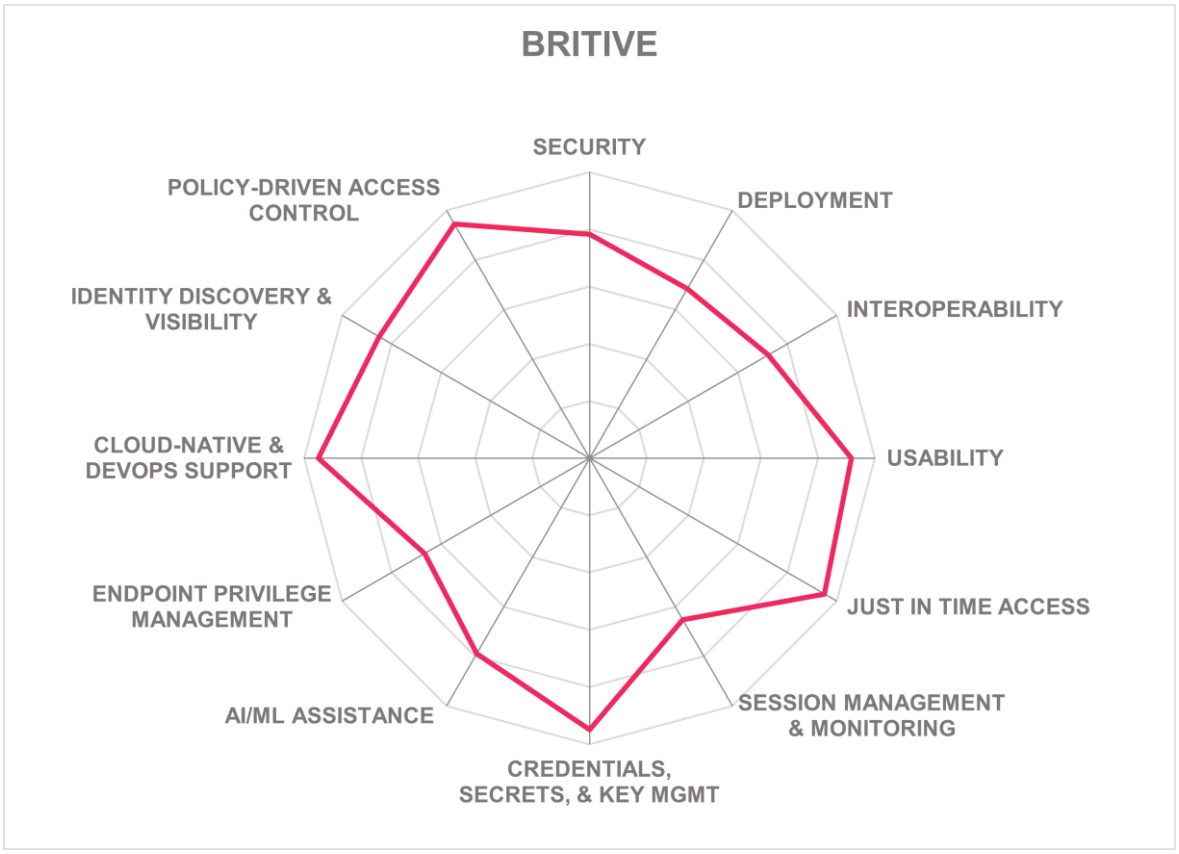
- Deeply integrated PAM and IGA within a single operational platform

- Good JIT support through multiple access methods
- Excellent connector coverage across legacy and cloud systems
- Mature session recording and replay capabilities
- Broad discovery beyond simple account enumeration
- Deep visibility into privileged access across cloud environments and enforces access policies effectively
- Bravura Safe enhances the platform by providing zero-knowledge credential vaulting, compromised password alerts, and secure secret sharing

Challenges

- No EPM capabilities
- No PUEBA for behavioral analysis of privileged activity
- Limited dedicated DevOps secrets functionality
- Lacks ISO 27001 certification
- No native ML-driven analytics today

Britive – Britive Cloud Identity Security Platform



Leadership

Established in 2018 and headquartered in Glendale, California, in the US, Britive is a privately held company focused on PAM with an emphasis on cloud-first environments. Its core offering, the Britive Cloud Identity Security Platform, is designed as a unified control plane for managing privileged access across human, NHIs, and agentic identities. Delivered primarily as a SaaS application with both multitenant and dedicated deployment options, the platform extends into private environments through its Access Broker component. Britive is SOC 2 Type II compliant. Licensing is subscription-based, priced per managed identity. The company targets mid-market and large enterprises, particularly those with strong cloud

adoption, with most customers located in North America and a growing presence in the APAC.

Britive's approach to PAM centers on eliminating standing privileges rather than managing them more efficiently. The platform delivers JIT, ephemeral access by dynamically creating and assigning permissions at the moment of need, then removing them once the defined policy evaluation result expires. This extends beyond human users to include service accounts, CI/CD workloads, and AI-driven identities, all governed under a single policy model. Unlike traditional vault-centric approaches, Britive reduces reliance on static credentials by generating short-lived access paths directly within target systems. Its API-first and agentless design allows direct integration with cloud providers, SaaS platforms, and infrastructure services without relying on proxies, though in practice this approach may require customers to configure integrations more actively compared to solutions that provide pre-built connectors. The platform integrates with existing identity providers such as Okta, Ping Identity, Microsoft Entra ID, Idira, and OneLogin for authentication, focusing instead on authorization and permission delivery. This separation allows organizations to retain their existing IAM stack while introducing fine-grained, time-bound privilege control across diverse environments.

Privileged access is enforced through policy-driven workflows, including approval chains, ITSM integration, and contextual controls such as time-of-day or ticket validation. The platform provides centralized dashboards and reporting capabilities that aggregate identity activity, entitlement usage, and audit trails into a single interface. Session management is supported through policy-based recording and monitoring of SSH, RDP, and Kubernetes sessions, with playback and termination capabilities tied to privilege levels. Credential and secret management is handled through an integrated vault supporting generation, rotation, versioning, and ephemeral credential issuance. Identity discovery spans both cloud and traditional systems, using native integrations and the Access Broker to identify accounts, entitlements, and drift. No EPM capabilities are provided natively, but Britive integrates directly with common EPM solutions such as Microsoft Intune. The platform also extends to DevOps workflows, offering Terraform-based configuration and policy enforcement within pipelines.

Britive continues to expand into areas shaped by AI-driven operations, introducing capabilities such as policy-controlled impersonation for agentic identities and an MCP server that enables secure interaction between AI agents and enterprise resources. These features allow AI-driven workflows to request and obtain privileges within defined boundaries, maintaining auditability and reducing overprivileged access. The platform's coverage across cloud infrastructure, SaaS, and legacy systems reflects a deliberate effort to unify privilege management under a single model rather than extending legacy PAM constructs. Britive is well suited for organizations seeking to reduce standing privileges, simplify access control across identity types, and align PAM strategies with cloud and DevOps operating models.

Strengths

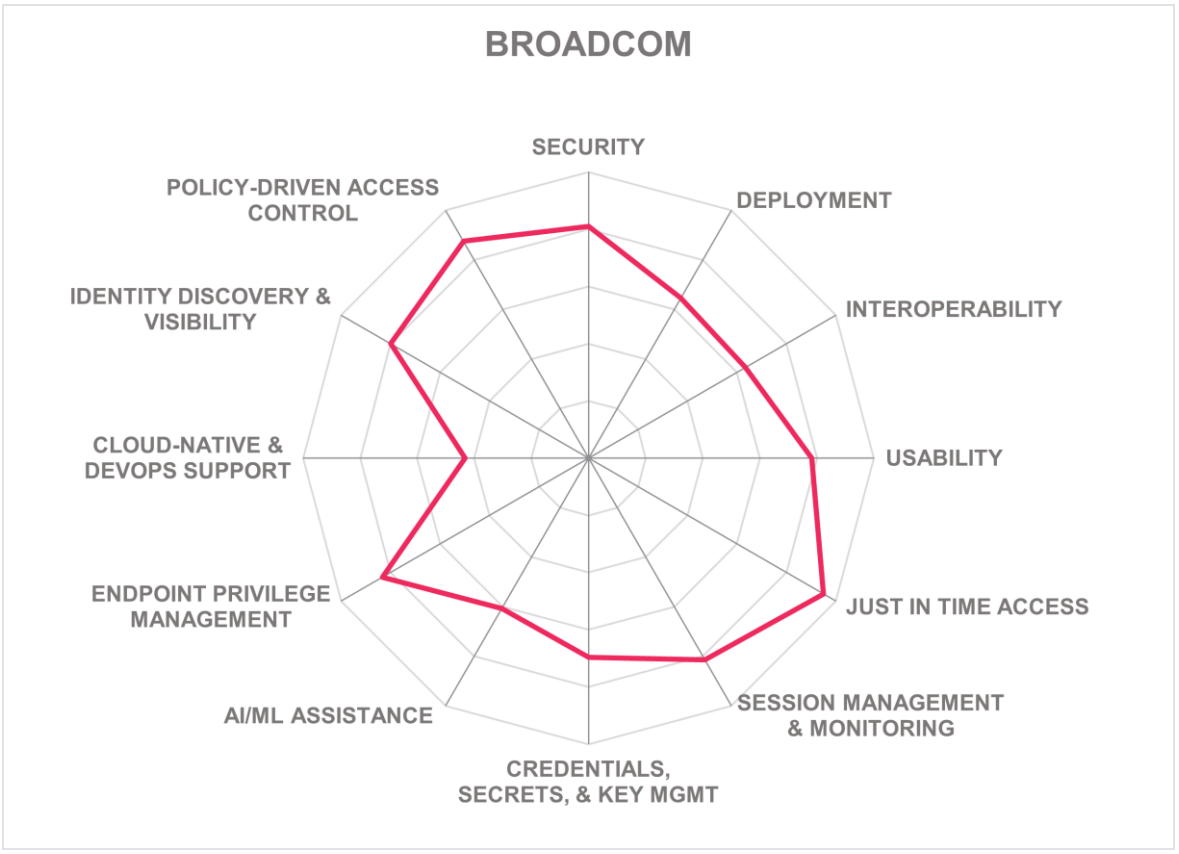
- Unified control plane for all identity types
- True ephemeral JIT privilege model

- Agentless and API-first architecture simplifies deployment
- Extensive integration with CI/CD and DevOps workflows
- Policy-driven access with granular entitlement control
- Support for agentic identity and AI workflows
- Access Broker extends cloud-native JIT permissions to cloud-first, hybrid on-prem, and private cloud environments

Challenges

- Limited support for ML-based anomaly detection
- No support for PUEBA capabilities
- No native EPM features
- Lacks ISO 27001 certification
- Limited market presence outside North America

Broadcom – Symantec PAM



Headquartered in Palo Alto, California, in the US, Broadcom traces the roots of its security portfolio to earlier technology lineages that stretch back decades. Through its Symantec division, the company delivers Symantec PAM, a long-established offering for PAM aimed primarily at large enterprises. The solution is available across a wide range of deployment models, including self-hosted on premises, public and private cloud, appliance-based delivery, virtual appliance, MSP-hosted SaaS, and vault options for distributed environments. Broadcom does not host Symantec PAM itself as SaaS, however. Symantec PAM is a unified product that includes credential vaulting, session recording, threat analytics, fine-grained access control, app-to-app password management, secrets management, and server control agents, while some capabilities can also be licensed separately. Pricing options include per user, per device, and bundled options using a subscription model. Broadcom serves customers across North America, EMEA, APAC, and LATAM.

Symantec PAM's core value lies in bringing multiple PAM controls into one interface so that credential management, access enforcement, session oversight, secrets handling, and threat analytics do not operate as disconnected functions. The platform protects privileged human accounts, application-to-application access, SSH keys, and a growing set of machine identities, while also extending to keys and secrets used across infrastructure and

operations. Broadcom places particular weight on fine-grained access control, an area where the product has long had depth, and this remains a meaningful differentiator for organizations that need tighter policy enforcement across heterogeneous systems. Its out-of-the-box integration with VMware Virtual Cloud Foundation (VCF) also adds practical value for organizations securing administrative access within private cloud estates. Broadcom integrates with IdPs such as Okta and Microsoft Entra ID.

Broadcom has a broad PAM capability set and, in several areas, shows particular maturity. Dashboards are customizable and provide real-time alerting for privileged access threats and drill-down capabilities for investigation. The types of reports that can be generated include manual, scheduled, real-time and GRC-related reports, which supports audit and operational review, especially for medium- and high-risk activities flagged by threat analytics. Symantec PAM integrates with external systems through REST APIs, System for Cross-domain Identity Management (SCIM), CLIs, and out-of-the-box connections to Broadcom's Identity Security Platform, VMware VCF, and identity governance tools such as SailPoint and Symantec Identity Governance. These integrations also enable JIT provisioning, either through governance workflows, imported directory group membership, or proprietary API-driven processes. Session management features include session recording, terminal text capture, selective recording modes, and the ability to halt sessions when risk increases. Broadcom also works with OT, ICS, network devices, and other non-traditional endpoints. It controls and audits third-party vendor access to ICS networks and provides a single admin console for both IT and OT resources. On the secrets side, Symantec PAM can import, store, rotate, revoke, and decommission secrets, as well as generate and distribute SSH keys, though it does not support dynamic secrets. Discovery extends beyond human credentials to machine identities through embedded network scanning and certificate discovery tools.

Broadcom is currently investing in areas that align with where PAM demand is moving, particularly machine identity discovery and monitoring, platform modernization through its Identity Security Platform, and stronger alignment with private cloud environments. Its new machine discovery and monitoring capability adds visibility into certificates and other NHIs. The company is also exploring AI-assisted use cases for policy creation and analysis, though these efforts are on the roadmap. Symantec PAM has proven fit for large enterprises, regulated sectors, and organizations with complex infrastructure that need broad PAM coverage, mature session controls, and strong policy enforcement under one administrative framework.

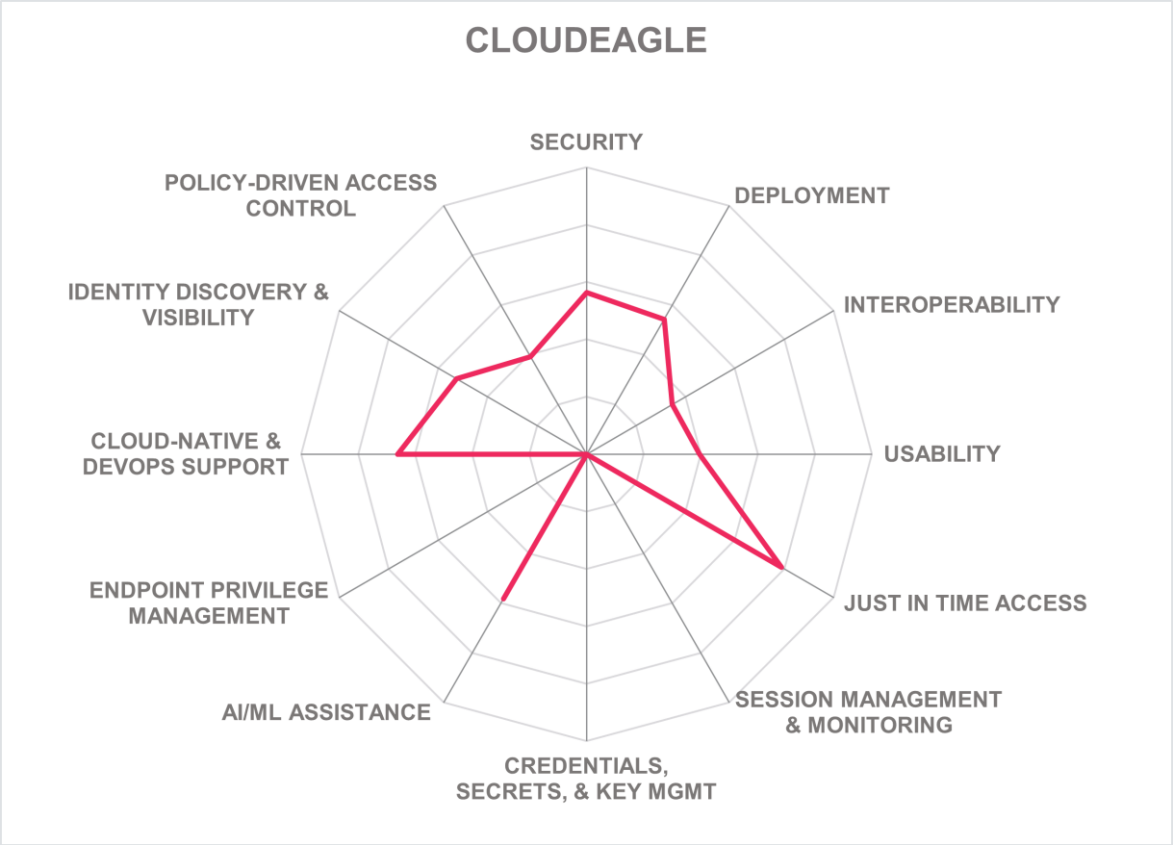
Strengths

- Unified interface across core PAM capabilities
- Deep fine-grained access control capabilities
- Feature-rich session recording and monitoring functions
- Good support for OT and ICS systems
- Machine identity discovery adds useful visibility
- Turnkey VMware VCF integration for private clouds
- Supports JIT provisioning via integration with Identity Governance solutions

Challenges

- No support for dynamic secrets
- No cross-account access visualization in dashboards
- Lacks pipeline-driven secrets lifecycle automation
- No policy-based privilege escalation for CI/CD processes
- Broadcom does not host Symantec PAM as SaaS

CloudEagle – CloudEagle.ai



Founded in 2021 and headquartered in Palo Alto, California, in the US, CloudEagle is a private company focused on SaaS governance, spend management, and access operations. Its core offering, CloudEagle.ai, sits adjacent to PAM rather than within the traditional category, but it covers several access governance use cases that matter in privileged SaaS contexts. The platform is delivered primarily as a fully hosted, multitenant SaaS service, with support for virtual appliance deployment. Managed services are available through in-house customer success teams and consultants. CloudEagle is ISO 27001 and SOC 2 Type II compliant. Licensing is based on employee bucket ranges. The company targets mid-sized and mid-market organizations, mainly in North America and EMEA, with a smaller but growing presence in APAC and LATAM.

CloudEagle has more than 500 direct integrations with applications. It builds a system of record for applications, identities, licenses, roles, permissions, and usage across SaaS environments. It governs access to privileged roles within business applications, showing who has elevated permissions, how those permissions were assigned, whether they are still being used, and when they should be removed. Time-bound access is a particularly relevant capability here: employees can request access to an application for a limited duration, approvals can be routed through defined stakeholders, and access is automatically revoked

when the approved time window ends. This reduces standing privilege in SaaS applications, even if the platform does not vault credentials, broker sessions, or manage secrets.

CloudEagle integrates with identity providers such as Microsoft Entra ID and Okta, and it can synchronize with ITSM and workflow systems, including bi-directional ticket updates. The platform provides customizable dashboards and reports that map identities to SaaS applications, roles, permissions, access review status, and license activity. It also supports guided access reviews, evidence generation, and workflow-driven deprovisioning when reviewers reject access or identify inactive users. Its coverage extends across SaaS and major public cloud platforms such as AWS, Azure, GCP, and Alibaba Cloud, though this should be understood as only governance visibility and orchestration around cloud services rather than infrastructure PAM. Smart Workflows, no-code automation, and EagleEye add useful assistance through predictive suggestions, contextual automation, Natural Language Process (NLP)-based interaction, and one-click actions. However, several core PAM functions are absent: there is no password vaulting, no secrets or key management, no certificate lifecycle management, no privileged session recording, no EPM, no ephemeral credentials, and no support for CI/CD or DevOps pipeline use cases.

CloudEagle is best understood as a SaaS access governance platform with partial overlap into PAM-related use cases, especially where organizations need better control over privileged roles inside SaaS applications and stronger discipline around approvals, access reviews, and offboarding. Its strongest features come from combining discovery, workflow automation, and audit-ready evidence in a way that reduces manual work and access review fatigue. The breadth of integration coverage is also meaningful, particularly in environments where identity, finance, procurement, and IT operations all shape who gets access to what. Still, CloudEagle does not address the foundational controls expected from full PAM platforms, and buyers should not treat it as a substitute for vaulting, session control, or secrets protection. CloudEagle fits organizations that want to govern SaaS access more rigorously and reduce standing privilege in business applications without introducing heavy operational overhead.

Strengths

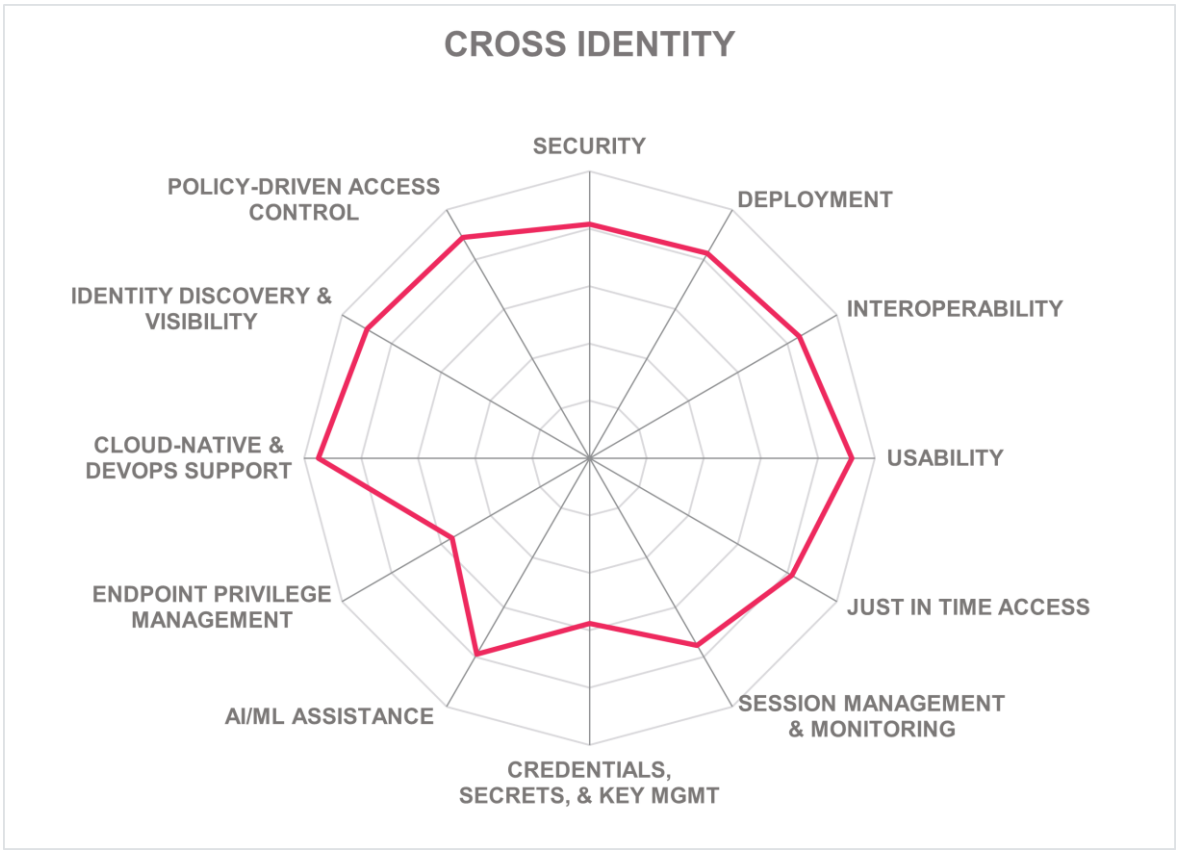
- Broad SaaS integration coverage across business systems
- Useful time-bound access for SaaS entitlements
- Effective onboarding and offboarding automation
- Guided access reviews with evidence generation
- Good visibility into SaaS roles and permissions
- No-code workflows reduce administrative effort
- Combines governance, procurement, and license insights
- Centralized catalog improves approval consistency

Challenges

- Not a full PAM platform
- Small partner ecosystem compared to other vendors
- No password vaulting, or secrets, key, or certificate management

- No session recording or session brokering
- No EPM capabilities and no support for CI/CD or DevOps pipeline use cases.
- Limited to SaaS-centric privileged access scenarios
- SaaS only solution

Cross Identity – Cross Identity



Cross Identity (formerly Ilantus Technologies) was founded in 2000. Its US headquarters are located in Schaumburg, Illinois, and it has significant operations in Bangalore, India. The company has long focused on identity-centric security. Cross Identity is a unified platform spanning IGA, Access Management, Customer IAM (CIAM), and PAM. For PAM, the platform goes beyond password vaulting and session control by tying privileged access to governance, analytics, and risk evaluation. It is available through a broad set of deployment models, including self-hosted software, appliance and virtual appliance options, fully hosted SaaS, MSP-hosted SaaS, and vault options for mixed infrastructures. Cross Identity also offers a consumption-based licensing model. The platform has certifications for ISO 27001 and SOC 2 Type II. The company primarily targets mid-market organizations and has established presence in North America and APAC while expanding into EMEA and LATAM. In addition, Cross Identity also offers a separate converged PAM solution, nimbleNOVA, designed to give smaller and mid-market organizations a broader identity security capability; this solution is covered in a dedicated chapter within this Leadership Compass.

Cross Identity connects privileged sessions, entitlements, approvals, and threat signals into a broader control plane rather than treating PAM as a vault with a gateway attached. The platform protects privileged users, service accounts, application-linked privileged identities,

and other machine accounts that interact with business systems, databases, and infrastructure. Vaulting covers passwords, credentials, and secrets, while session monitoring and privilege elevation are tied to policy and contextual risk. A key differentiator is the way the platform evaluates privileged access requests using factors such as user behavior, origin, asset criticality, compliance relevance, and contextual signals before approving or restricting access. This gives Cross Identity a more adaptive operating model than products that rely mainly on static rules. Cross Identity integrates with multiple IdPs, such as Microsoft Entra ID, Ping Identity, Okta, Keycloak, OneLogin, and Idira.

Cross Identity delivers a broad PAM feature set with particular strength in JIT privilege elevation, identity visibility, and policy-driven control. Temporary elevated access can be granted based on approvals, policy conditions, risk scores, device posture, geolocation, and time of request, then removed automatically when the task or time window ends. Session monitoring supports SSH, RDP, web administrative consoles, and proxied database sessions, with alerting for failed access attempts, restricted commands, privilege escalation, file transfers, and policy violations. The platform also supports session recording, automated credential rotation, and temporary credential injection for approved tasks. Discovery covers privileged accounts, service accounts, scripts, and configuration files containing cleartext credentials through continuous scanning. Dashboards provide cross-account access visibility, threat alerts, and drill-down investigation. Reporting is another strong area, with natural language interaction enabling users to generate reports and ML-powered analytics through conversational prompts. Cross Identity also extends into CIEM by continuously mapping permissions across major cloud platforms and surfacing excessive or risky entitlements, supported by remediation workflows and integrations across common APIs and CI/CD tooling. EPM is supported for Windows, with application allow-listing, while privileged behavior analytics currently support Windows and Linux systems. Additionally, the solution provides emergency access workflows including approval-bypass escalation paths, emergency account unlock, and out-of-band access request channels designed for crisis scenarios. The Threat Intelligence module provides centralized monitoring across identity systems and endpoints, with a strong focus on detecting privilege escalation risks. It identifies accounts with elevated group memberships, such as Domain or Enterprise Admins, where compromise could lead to full domain control, especially when combined with weak credential policies.

Cross Identity presents a more expansive view of PAM, one that connects vaulting, elevation, monitoring, governance, and identity threat protection into a common framework. Its use of ML and GenAI is particularly relevant where access reviews, role mining, reporting, and analytics have become too labor-intensive to manage manually. GenAI-created summaries, natural language queries for reporting, and contextual guidance for reviewers make the platform more usable without reducing its technical depth. At the same time, some limits remain. The absence of a dedicated ephemeral secrets engine, full OT and ICS coverage, and deeper searchability within session recordings narrows its fit for some operational environments. Even so, Cross Identity offers a coherent platform for organizations that want PAM tied closely to governance and risk rather than treated as a separate security island.

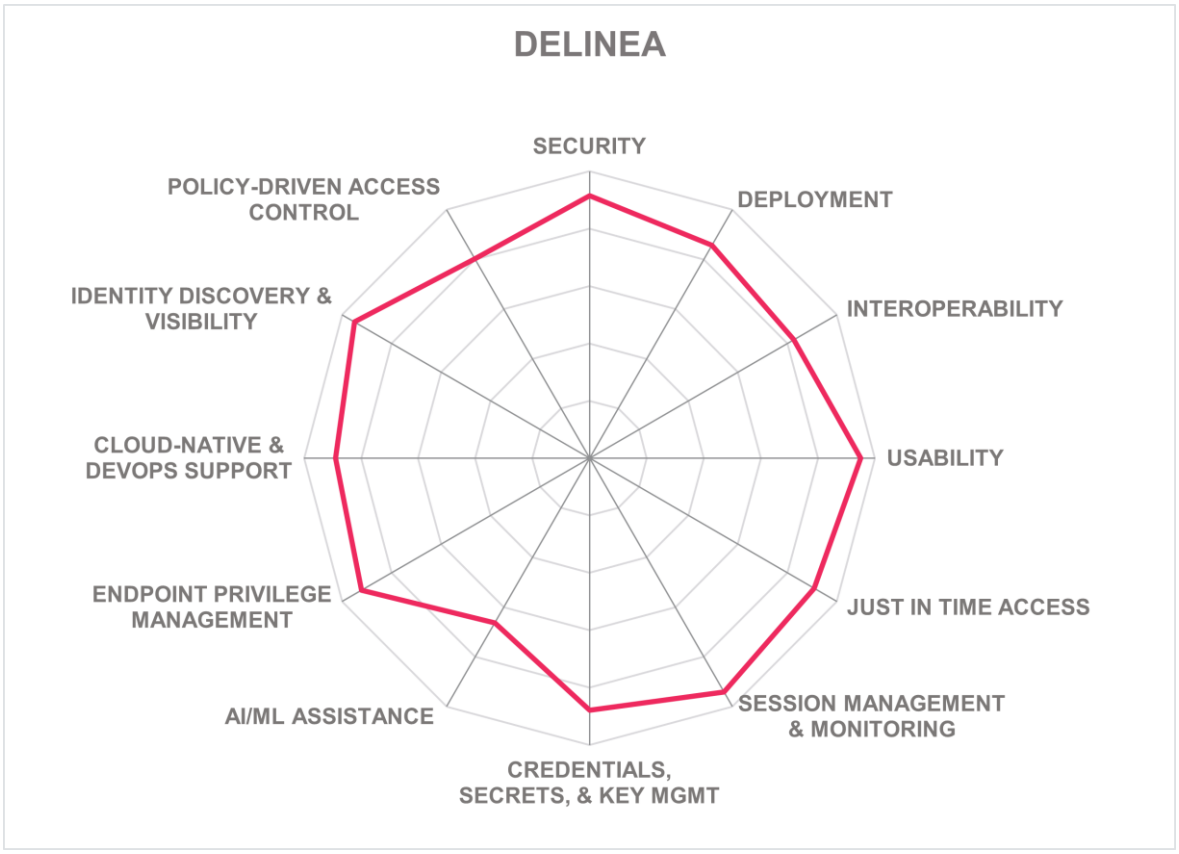
Strengths

- Unified platform provides PAM, IGA, AM, and CIAM capabilities
- Context-aware JIT privilege elevation
- Granular policy-driven access and approval controls
- Integrated session monitoring and recording capabilities
- Continuous discovery of privileged accounts and exposures
- ITDR-linked risk scoring strengthens privileged access decisions and response
- GenAI assistance for reviews and analytics
- CIEM capabilities tied to governance and PAM

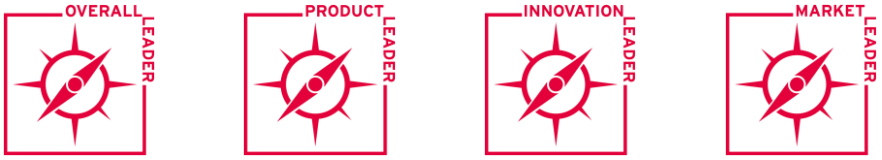
Challenges

- Session recordings currently lack deep search capabilities
- EPM support does not cover macOS, but enhancements are on the roadmap
- No support for a dedicated ephemeral secrets engine, but improvements are on the roadmap
- No OT/ICS coverage, but it integrates with OT-native platforms (such as Claroty and Nozomi Networks) via APIs

Delinea – Delinea Platform



Leadership



Established in 2004 and headquartered in San Francisco, California, in the US, Delinea is a private company focused on identity security, with a long-established presence in the PAM market. Its portfolio centers on the Delinea Platform, a cloud-native offering that brings together Secret Server, Privileged Remote Access, Privilege Control for Servers, Identity Threat Protection, Continuous Identity Discovery, analytics, and related controls for privileged access and identity risk. The company delivers the platform through fully hosted SaaS, MSP-hosted SaaS, public and private cloud self-hosted models, on-premises deployments, hybrid vault options, and virtual appliances. Delinea supports standards such as FIPS 140-2 and maintains certifications including ISO 27001 and SOC 2 Type II.

Licensing is based on users, servers, and workstations. It serves mid-market and large enterprises across North America, EMEA, APAC, and LATAM. In March 2026, Delinea acquired StrongDM. This acquisition will help Delinea modernize and broaden its PAM strategy. This shift is from traditional privileged access toward cloud-native, developer-friendly, and policy-driven, real-time authorization across human, machine, and emerging AI-agent use cases. However, integration work lies ahead.

Delinea's platform combines vaulting, credential rotation, session control, remote access, and granular elevation with continuous discovery and analysis. Secret Server handles privileged credentials, service accounts, SSH keys, and cryptographic material with automated rotation, dependency updates, credential injection, optional HSM and KMS integration, and support for native cloud vault governance. Privilege Control for Servers extends JIT and just-enough privilege to Windows, Linux, and Unix with identity consolidation via AD Bridging on *nix systems, while Delinea Privileged Remote Access provides VPN-less access for IT staff as well as federated authentication to third parties. A particularly relevant differentiator is Delinea's approach of treating discovery, posture analysis, and control as part of a single continuum. With the StrongDM acquisition, Delinea expands beyond traditional vault-centric PAM toward a more modern approach incorporating secretless, ephemeral, and zero-standing privilege access models, while maintaining integration with existing vault solutions. Delinea integrates with Microsoft Entra ID, Okta, Active Directory, Azure, AWS, GCP, Ping Identity, and other sources, as well as supporting custom extensibility for discovery. Delinea is also capable of discovering cloud native vaults and provide governance over those vaults. This allows developers to use native tools while giving the identity and security teams centralized visibility and governance over those secrets.

Reports provide detailed audit trails for privileged activity, compliance support, and forensic review. Delinea provides dashboards for privileged identities, access paths, risk scoring, posture findings, and activity views, with growing support for customer-defined dashboards and deeper identity graph exploration. Integration coverage is broad, spanning IAM and CIAM-adjacent systems through SAML, OIDC, LDAP, Kerberos, SCIM, REST, Simple Object Access Protocol (SOAP), JavaScript Object Notation Remote Procedure Call (JSON-RPC), and webhooks, plus out-of-the-box support for a long list of IdPs, SaaS services, and cloud platforms. JIT access is one of Delinea's strongest areas, covering credentials, workstation admin rights, granular server privilege elevation and now with the StrongDM acquisition, granular JIT for Databases, Kubernetes environments, cloud consoles as well as traditional server infrastructure. This is all done with policy-based approvals and integration into systems such as ServiceNow and SailPoint. The platform also supports ephemeral credentials, session checkout with automatic rotation, session monitoring through multiple recording methods, and EPM for Windows, Linux, and macOS. Delinea's approach to AI can be split into two categories: using AI to make the product easier to use and more efficient and secondly helping customers adopt AI. For example, Iris AI Auditing summarizes and tags session recordings while identifying anomalies, AI Authorization evaluates elevation requests using context and ticketing data, and natural language querying helps users both configure the product as well as work with the identity graph without learning a complex query language. On the other hand, for customers' own AI environments, Delinea helps with

discovery of AI Agents in the cloud, AI tools on workstations and provides access for AI agents to private resources without granting credentials to those agents.

Delinea's recent work suggests a vendor that is trying to widen PAM into a broader identity security control plane without losing sight of their core competencies. The combination of Continuous Identity Discovery, ITDR, CIEM, server and workstation privilege control, and AI-assisted analysis gives the platform a wider scope than traditional vault-centric PAM. The use of AI is more concrete than cosmetic, particularly in session review, contextual authorization, and identity graph interrogation, though some of the more ambitious co-pilot and action-taking functions are still developing. The StrongDM acquisition materially expands Delinea's JIT reach into databases, containers, and cloud consoles, which fits well with its ZSP direction. StrongDM also brings additional capabilities for agentic AI control. Delinea is well suited for regulated sectors, large enterprises, and organizations with mixed infrastructure that need PAM controls broad enough to cover legacy systems, cloud services, workforce devices, Agentic AI, and machine identities without fragmenting administration.

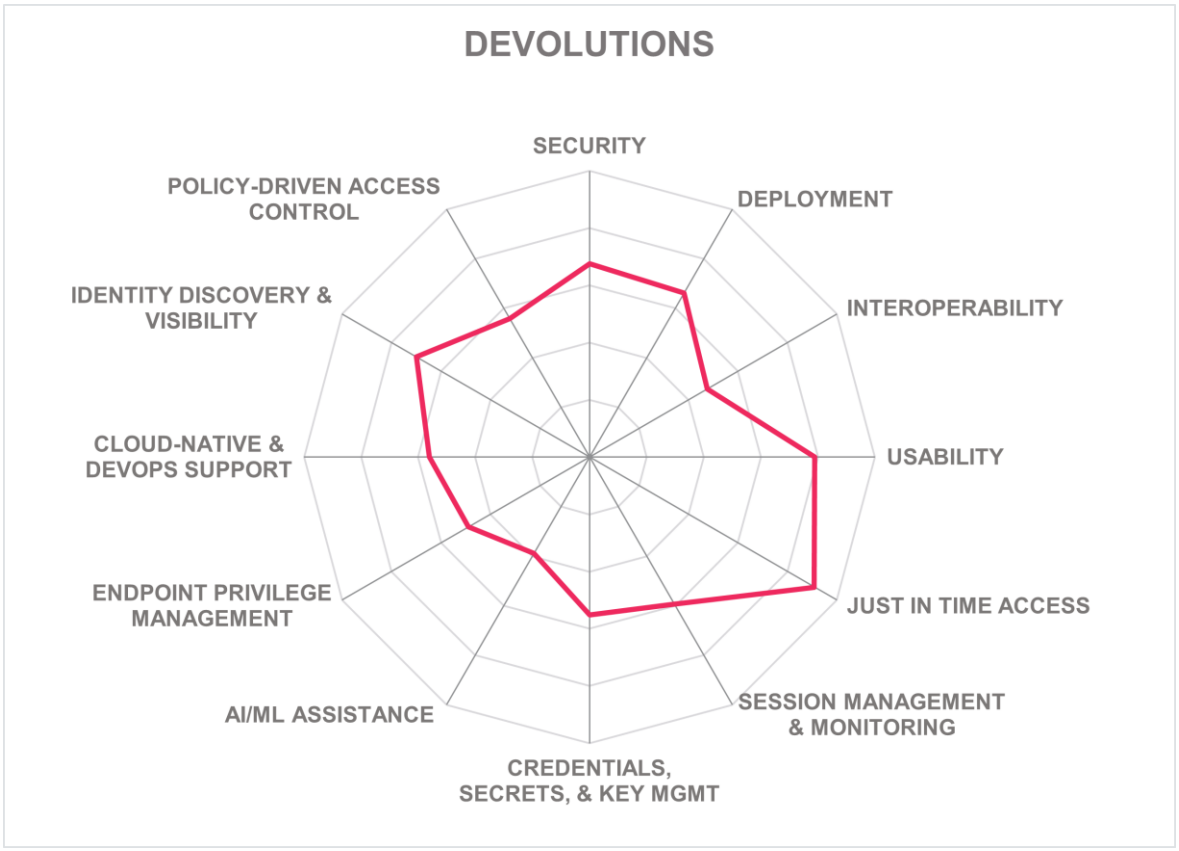
Strengths

- Advanced JIT and just-enough privilege controls
- EPM support for Windows, Linux, and macOS
- Continuous identity discovery feeds posture and threat analysis
- Session monitoring includes AI-assisted review and anomaly detection
- Governance includes native cloud vaults and third-party vaults
- Good support for contractors and federated privileged access
- Facilitates the transition from full admin accounts to least privilege, promoting a zero standing privilege state

Challenges

- Platform breadth may introduce perceived complexity, although feature exposure is typically aligned to what customers have purchased and deployed.
- DevOps Secrets Vault is not yet fully integrated

Devolutions – Devolutions PAM



Headquartered in Lavaltrie, Quebec, in Canada, Devolutions was founded in 2010. The company is a privately held vendor serving SMBs and mid-market organizations. Its PAM offering combines the Devolutions PAM module with Remote Desktop Manager, Devolutions Gateway, Devolutions Launcher, and Devolutions Workspace. The solution is available through self-hosted on-premises deployments, self-hosted public or private cloud SaaS, fully hosted SaaS, virtual appliance form factors, and mixed vaulting scenarios that combine on-premises and cloud components. It is not built on a microservices architecture. Licensing is subscription-based, per user, with published package pricing and one- or three-year terms billed annually. Devolutions has achieved SOC 2 Type II and ISO 27001/27701. Its strongest presence is in EMEA, though the company is also expanding across North America, APAC, and LATAM.

Devolutions covers privileged account discovery, password and secret vaulting, automated rotation, approval-based access, brokered session launch, and JIT elevation. Credentials are injected at session time, so users do not need to see or handle them directly. This is particularly relevant for service accounts, contractors, and external vendors, where Devolutions offers a separate identity layer when customers do not want to expose their

primary identity infrastructure. The platform reflects a practical design approach, emphasizing usability, faster deployment, and the reduction of standing privileges, particularly suited to SMBs, while avoiding unnecessary administrative complexity. Devolutions integrates with Microsoft Entra ID, Okta, and PingOne.

The solution provides dashboards and administrative reports, including ad hoc, manual, and scheduled reports, as well as GRC-related reports. It also provides audit trails and evidence generation for access reviews, though it does not model identity-to-resource relationships in the same way as some graph-oriented platforms. Interoperability extends across Active Directory, Windows, Linux and Unix systems, SQL Server, VMware environments, and major cloud platforms including AWS, Azure, and Google Cloud. Support also includes SSH-based network devices, as well as selected OT and non-traditional environments through the Gateway and custom provider framework. JIT access is handled through RBAC, approval workflows, time-bound elevation, and credential brokering, with full logging of requests, approvals, and use. With session management, administrators can observe and review active RDP, VNC, and SSH sessions through recorded playback tied to approvals and audit events. Devolutions also supports password and SSH key vaulting, rotation, and controlled distribution, but it is not a full KMS, does not provide dynamic secrets, and offers only limited DevOps and CIEM support. EPM is present through JIT local admin elevation, but without application allow-listing or deep endpoint control. There is no PUEBA capability, and AI support remains limited by design.

Devolutions' approach reflects a deliberate focus on usability and accessibility, particularly for teams without dedicated PAM specialists. Recent developments around SaaS capabilities, contractor access models, and initial steps toward cloud entitlement management indicate an attempt to extend coverage into adjacent areas. However, these areas are still evolving and do not yet reach the level of maturity or breadth seen in more established enterprise-focused platforms. Devolutions does not have ML or GenAI capabilities, and that may suit buyers who are more interested in reliable controls than in speculative analytics. Devolutions aims to provide SMBs, mid-sized enterprises, and operationally constrained IT teams with a PAM solution that is easier to deploy, easier to price, and easier to maintain than many of its larger competitors.

Strengths

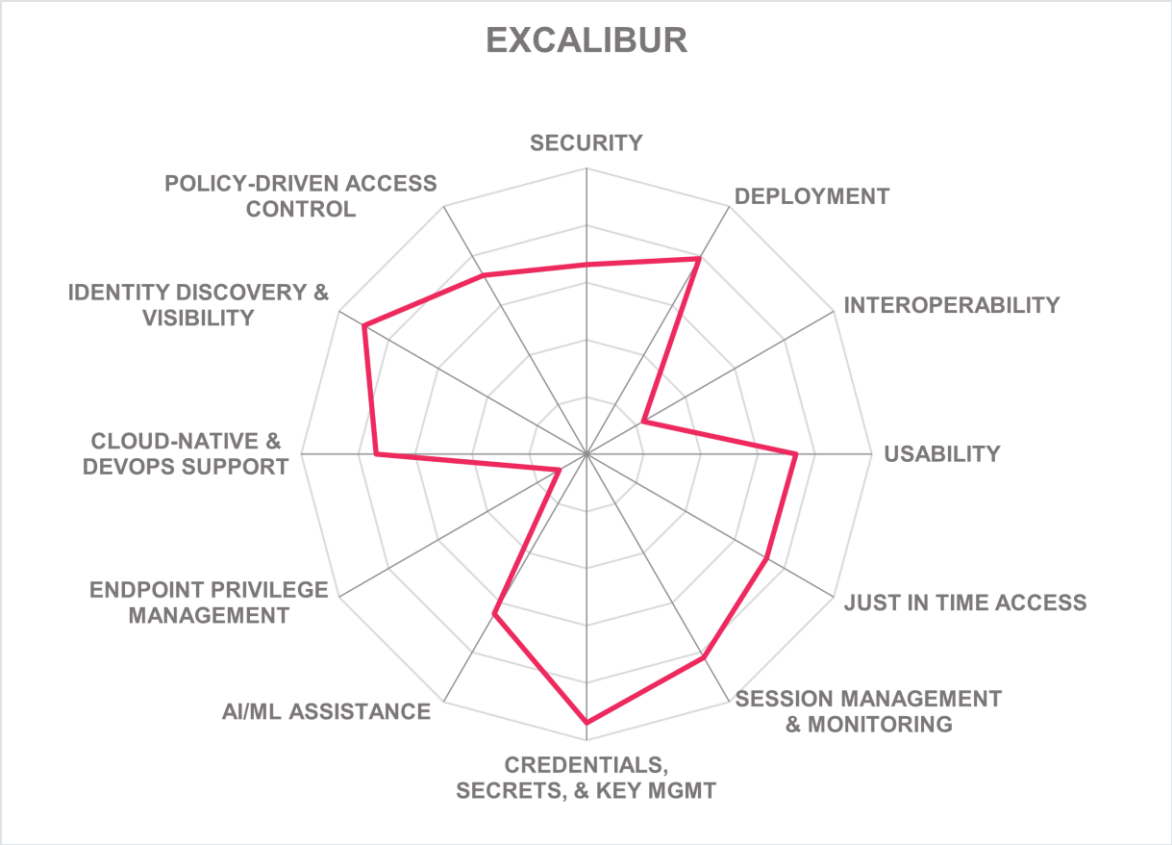
- Well suited for SMBs
- Integrated vaulting, brokering, and remote access
- Good contractor and third-party access support
- Solid JIT elevation and approval workflows
- Good coverage for Windows, Linux, and databases
- Session recording with useful playback capabilities
- Transparent subscription pricing by package

Challenges

- Integrations with IdPs beyond Microsoft Entra ID would be useful
- No PUEBA or advanced behavioral analytics

- Limited DevOps and CIEM support
- No certificate lifecycle management
- Lack of ML and GenAI capabilities
- Limited EPM depth beyond elevation
- SaaS feature parity still maturing

Excalibur – Streamed Access Management



Founded in 2016 and headquartered in Poprad, Slovakia, Excalibur is a European vendor with a distinct view of privileged access. Excalibur supports on-premises, private or public cloud self-hosted deployments, fully hosted SaaS, MSP-hosted SaaS, and multitenant service models. Licensing is per user. The company states that SOC 2 Type II certification is on the roadmap. Excalibur targets mid-market and large organizations, especially those with regulatory pressure, public-sector requirements, or sovereignty concerns. Its market presence is currently limited to EMEA.

Excalibur's solution is built around the concept of Streamed Access Management (SAM), a unified platform that combines PAM, smartphone-centric passwordless MFA, and secure remote connectivity through a single browser-based interface. Excalibur's differentiator is architectural. The product treats the endpoint and the user interaction layer as the primary risk surface, while the protected application remains inside an isolation layer. This gives the platform an unusual posture in PAM, one that overlaps with secure remote access, browser isolation, and in some cases VDI replacement. Privileged access is handled through streamed sessions, credential injection, policy enforcement, and session oversight rather than by handing direct network-level access to the user. Credentials configured in PAM

targets are stored as encrypted values with two-layer encryption and can be rotated automatically for supported scenarios. For streamed privileged-access sessions, particularly in web-based administrative and operational workflows, Excalibur applies real-time GenAI-driven contextual analysis to evaluate user actions before they reach the protected application. The system focuses on workflows where intent and context matter more than simple syntax validation, including privileged administration, IAM changes, financial approvals, sensitive data handling, support operations, and developer-oriented activities. This makes the product less about vault-centric administration and more about governing interactive privileged behavior as it unfolds.

Excalibur provides customizable dashboards with cross-account access visualization and real-time threat alerts, alongside reporting suited to audit and compliance use cases. It integrates with Active Directory and Microsoft Entra ID and other LDAP-enabled directories, supports SIEM and ticketing connectivity, and exposes a full REST API for third-party integration and workflow automation. Session management is central: sessions can be monitored, recorded, replayed, searched, and governed through policy. Credential handling is solid, with encrypted storage, credential injection, and automated password rotation. However, important gaps remain, including limited EPM capabilities and a comparatively small market presence outside its core regional focus.

Excalibur takes a different approach in this market by shifting privileged access control away from direct endpoint interaction and into a streamed, isolated access layer. Its architecture, support for large numbers of concurrent sessions on commodity infrastructure, and real-time AI-based session governance make it particularly relevant for web-based administrative use cases. Its emphasis on European delivery and absence of U.S. operational dependence may also resonate in sovereignty-sensitive sectors. Excalibur appears best suited for EU organizations that value interactive session control, evidentiary audit, and architectural containment over breadth of traditional PAM coverage.

Strengths

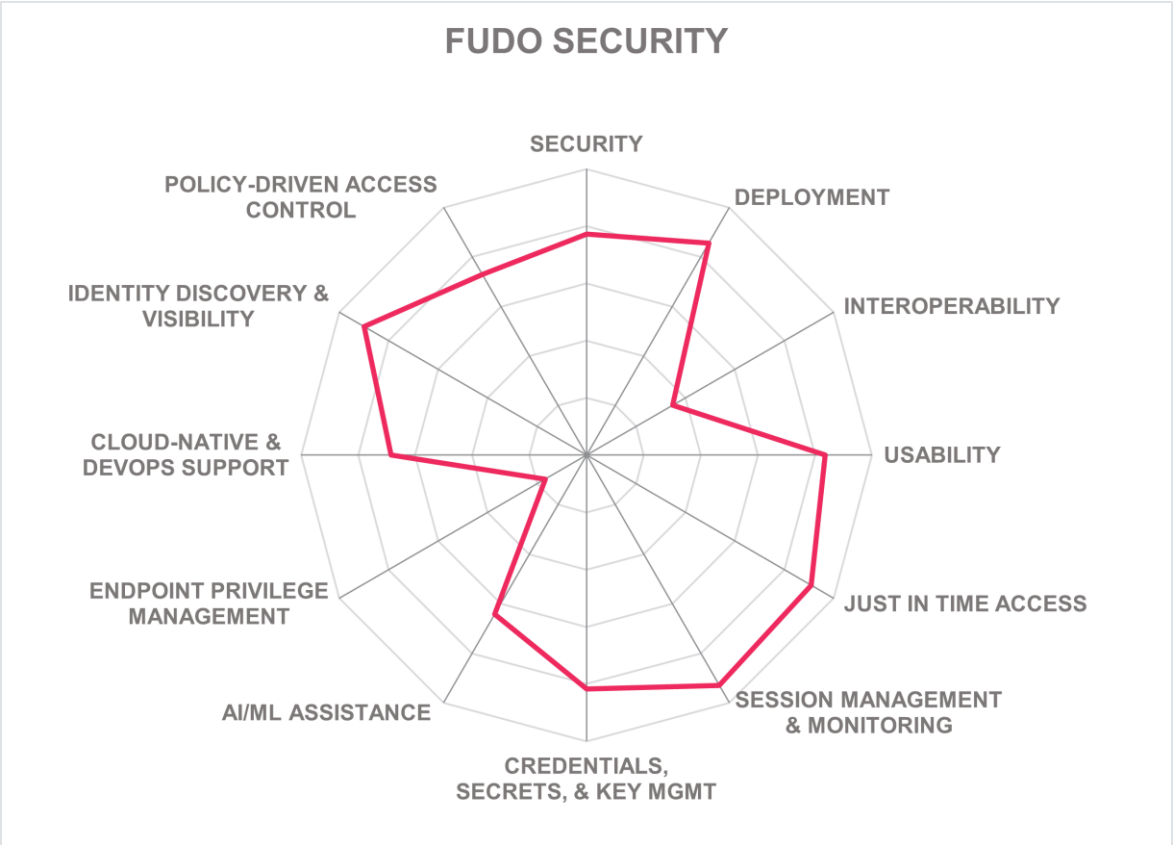
- European vendor with sovereignty-focused positioning
- Distinct streamed access architecture with an isolation layer between the endpoint and the protected target
- Granular control for all supported target types
- Inline AI oversight with pre-execution analysis and post-session investigation capabilities
- Encrypted credential storage and automated rotation
- Customizable dashboards and audit-oriented reporting
- Four-eyes approval with policy-driven escalation
- Integrated PAM and MFA in a passwordless, mobile-based solution

Challenges

- Small market presence and partner ecosystem
- Limited EPM features

- Out-of-the-box pre-configured connectors limited to Microsoft AD and Entra ID; SAML and other LDAP-enabled directories are supported via configuration

Fudo Security – Fudo Enterprise and Fudo ShareAccess



Fudo Security is a European vendor based in Warsaw, Poland, that focuses on PAM and secure remote access. Its core offering consists of Fudo Enterprise, the company's PAM platform, and Fudo ShareAccess, a SaaS-based service for managing external service provider organizations. Fudo Enterprise can be deployed on-premises by customers, using virtual and hardware appliances, and supports mixed deployment scenarios. Fudo Security hosts it as SaaS, and some MSSPs host it as SaaS as well. Licensing is available in both subscription and perpetual forms, with pricing based on numbers of either on monitored systems or privileged users. Fudo is currently pursuing ISO 27001 certification and SOC 2 Type II attestation in 2026. The company mainly targets medium-sized and mid-market organizations in EMEA and North America, with particular relevance for critical infrastructure, industrial organizations, and defense-related environments.

Fudo Enterprise controls privileged access through a proxy and reverse proxy model that separates users from target systems and keeps privileged credentials out of direct user hands. The platform authenticates users through third-party MFA options and external identity providers such as Microsoft Entra ID, Okta, and any other provider that supports LDAP, OIDC, and Remote Authentication Dial-In User Service (RADIUS); it then maps them to authorized targets, accounts, and policies. Privileged credentials, passwords, SSH keys,

certificates, and other sensitive secrets are vaulted and distributed only at the moment of access, which reduces standing privilege and limits credential exposure. This applies to both human and NHIs, with support for short-lived credentials and policy-scoped access. A distinguishing element is Fudo's behavioral biometric analysis of users during sessions, including mouse dynamics, keyboard patterns, and command semantics, which allows the platform to detect session hijacking or misuse even after authentication has succeeded. Fudo ShareAccess adds a useful layer for fast onboarding and controlled access for third parties without burdening internal teams with slow manual provisioning.

Intuitive dashboards and reporting are included, with real-time visibility into concurrent sessions, suspicious activity, account usage, and policy events. Session management features include live session monitoring, video replay, searchable Optical Character Recognition (OCR) for recorded sessions, session sharing, administrative intervention, and interactive control, including pausing or terminating suspicious activity. JIT access is handled through request-based workflows that can be approved through the admin console or mobile app, with support for immediate or scheduled access and granular policy controls. Fudo also covers centralized credential, secret, and key management through its integrated vault, including generation, rotation, checkout, expiration, revocation, and auditing. Support extends across enterprise IT, cloud infrastructure, OT/ICS, network devices, and other non-traditional endpoints. AI assistance is applied to behavioral analysis, threat scoring, and GenAI-generated summaries for SSH and RDP sessions. The product also supports policy-driven access controls, connection-layer privileged user behavior analytics, and REST-based integration with SIEM, SOC, MFA, and related systems. It does not currently provide EPM features.

Fudo's internal architecture relies on process isolation, sandboxing through Capsicum, encryption at multiple layers, and trusted timestamping for evidentiary session integrity. Fudo's AI capabilities focus on session integrity, behavioral drift, and operator accountability rather than loose automation promises. The company's fit is for organizations that prioritize secure remote administration, third-party access control, detailed session oversight, and support for industrial or regulated environments. Fudo Security is a solid option for buyers seeking an agentless PAM platform with strong session intelligence and a distinct European design approach.

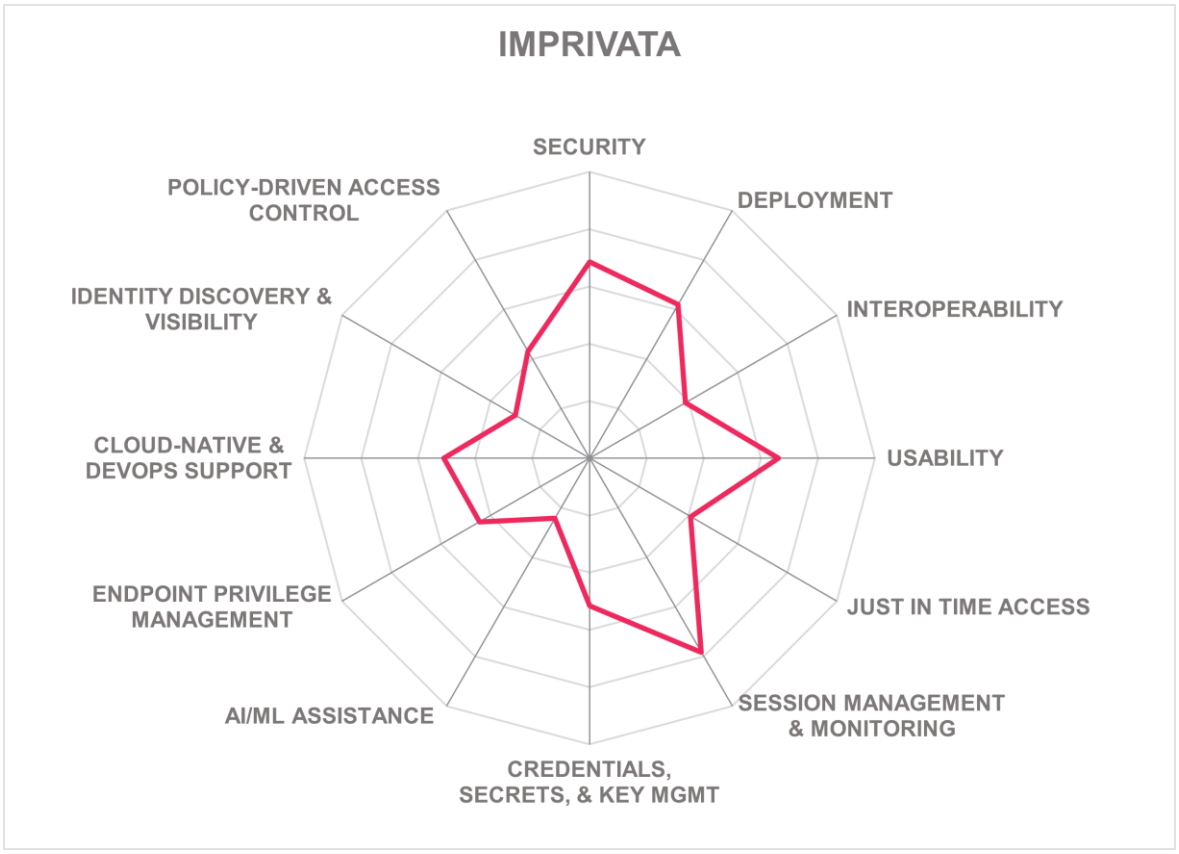
Strengths

- European vendor with sovereignty-focused positioning
- Mature session recording and live intervention capabilities
- Behavioral biometrics strengthen post-login assurance
- Agentless and clientless deployment reduces operational friction
- Broad support for third-party remote access
- Integrated vault supports human and machine identities
- Good coverage for OT and industrial environments
- Granular JIT access request workflows
- Internal platform security architecture is well designed

Challenges

- Smaller global footprint than larger PAM vendors
- No EPM capabilities
- Lacks security certifications today

Imprivata – Privileged Access



Imprivata is a private company headquartered in Waltham, Massachusetts, in the US. It is best known for its secure access management solutions in healthcare and other mission-critical sectors. However, its Privileged Access offering is not confined to those areas. The product is delivered as on-premises self-hosted software, private cloud self-hosted, self-hosted appliances, or fully hosted SaaS, with feature consistency across deployment models. It does not run on a microservices architecture. Licensing is per user for traditional PAM use cases and per vendor company for third-party access. Security and certifications include ISO 27001/27701, SOC 2 Type II, and UK Cyber Essentials Plus. Imprivata primarily targets organizations of all sizes in North America, with a growing presence in EMEA and APAC. Relevant acquisitions include SecureLink in 2022 and Verosint in 2025.

Imprivata Privileged Access is built around the idea that privileged access is not limited to internal administrators logging into servers. The platform was designed from the outset with Remote PAM as a core requirement, which gives it a broader operational scope than many PAM products that were later extended for third-party access. It supports any TCP or UDP protocol across any host, allowing organizations to manage internal privileged users, external vendors, and customer-facing remote support scenarios from one control plane.

Credential handling includes vaulting, controlled check-out, credential injection, and password rotation triggered manually, on schedule, or after specific events. Access is granted through granular permissions, delegated approvals, and time-limited policies that align well with least-privilege objectives. A distinctive element is the Nexus model, which enables enterprises and vendors to establish controlled trust relationships while maintaining unified authentication, approvals, and audit records within a single system. Imprivata integrates with Microsoft Entra ID, Okta, Auth0, Active Directory Federation Services (AD FS), and Ping Identity.

Session activity is captured at the appliance level, which supports a tamper-resistant audit trail across supported protocols and avoids dependence on endpoint-side agents for recording. For RDP and VNC sessions, Imprivata supports DVR-style recording, while SSH activity can be logged in text form; key logging, event-based recording, and notifications on session start and end are also supported. Imprivata does not provide a single-pane administrative dashboard, but it does deliver out-of-the-box reporting views, on-demand reports, and scheduled reports, and can forward events such as user creation and session activity to Syslog or SIEM tools. The REST API exposes all User Interface (UI) functionality, enabling administrative automation, audited endpoint access, credential rotation, and check-out workflows. Cloud coverage is broad, with support for Azure, AWS, GCP, IBM Cloud, Alibaba Cloud, OVHcloud, and VMware Cloud. The product also supports JIT access through approval-based, time-limited access to applications and secrets, plus credential rotation for both human and machine identities. EPM extends to Windows, Linux, and macOS, including application and command sandboxing. The platform now also includes Agentic Identity Management, which extends PAM-style controls to AI agents and treats them as managed privileged identities within the same control plane. In practice, that means organizations can apply the same access controls, approvals, credential protections, monitoring, and auditability used for human users to agentic workloads. Through Local MCP, Imprivata can broker scoped and tunneled access to legacy and on-premises systems that lack modern APIs or native AI integrations. The forthcoming MCP Gateway is designed to centralize management, policy enforcement, and auditing for agent connections across both cloud-based and local MCP environments. This allows AI users to access required systems without stepping outside existing governance and audit models.

The company has improved usability with a modernized interface and HTML5 access for common protocols. Its newer PUEBA capability, brought in through the Verosint ITDR acquisition, is intended to evaluate risk across all identities, applies adaptive response during authentication, credential access and session activity, and enables monitors which can be used to proactively disable an account and notify admins if risk warrants. That broad identity focus could become more relevant as PAM and ITDR continue to overlap. Still, some gaps remain: no dedicated DevOps or CI/CD module and no support for ephemeral machine-to-machine secrets. Even so, Imprivata presents a solid alternative for organizations that want one platform for internal privileged access, third-party access, and remote support, particularly in regulated environments where audit quality and deployment flexibility carry real weight.

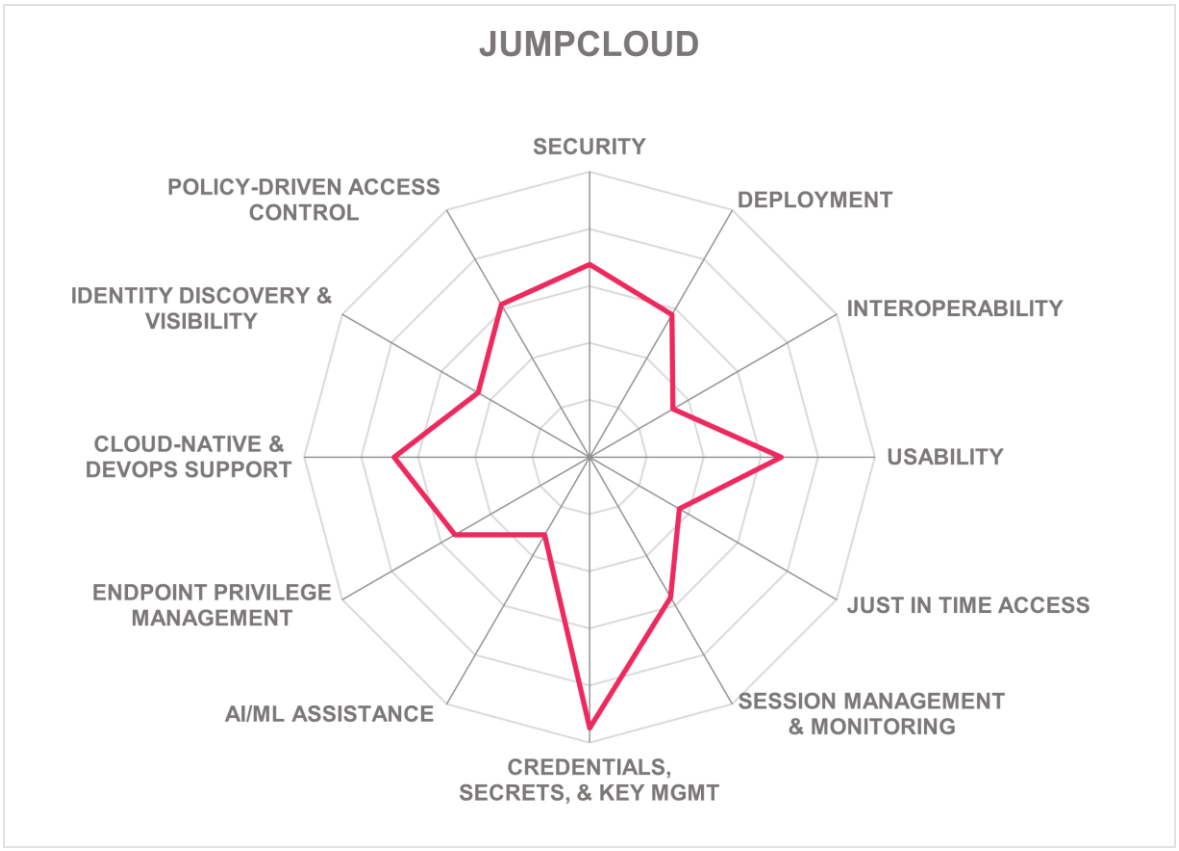
Strengths

- Broad support for TCP and UDP protocols
- Centralized control through Nexus connectivity model
- Extensive third-party and vendor access capabilities
- Tamper-resistant auditing from the appliance layer
- Comprehensive credential injection, check-out, and rotation
- Native ITDR capabilities across privileged workflows
- Supports privileged identity access across a wide range of cloud infrastructures

Challenges

- No single-pane administrative dashboard
- OT, ICS, or SCADA coverage relies on direct configuration of service definitions for endpoints in these environments or jumpboxes
- No dedicated DevOps or CI/CD module
- Features leveraging AI/ML are currently limited to modeling and response within ITDR with broader use on the roadmap.

JumpCloud – JumpCloud Platform



Founded in 2014, JumpCloud is a private company headquartered in Louisville, Colorado in the US. Its PAM capabilities are delivered as part of the JumpCloud Platform, which combines privileged access controls with broader IAM and endpoint management functions. The solution is available as public cloud SaaS. JumpCloud follows a per-user licensing model. The platform is certified ISO 27001 and SOC 2 Type II attested. JumpCloud's targets the mid-market, though it addresses organizations of varied size across sectors, with strongest presence in North America and growing traction in EMEA, APAC, and LATAM.

JumpCloud approaches PAM less as a standalone vault and more as an extension of a broader identity and access fabric. Rather than limiting privileged access to servers, databases, and a narrow set of administrative systems, the platform extends control to web-based assets through its private browsing model built on remote browser isolation. This allows privileged sessions to be mediated without exposing direct access paths and, when implemented broadly, reduces lateral movement and can remove dependence on VPNs for certain access scenarios. The solution also obscures credentials from end users while still granting access through controlled sessions, combining password generation, rotation, and secure brokering. This is a pragmatic design choice. It shifts the emphasis away from users

handling secrets and toward tightly managed session-based access. The broader value proposition lies in simplicity of deployment, tighter linkage with IAM and device context, and a more accessible operating model for mid-sized organizations that want PAM without the overhead of older architectures.

The platform includes modern dashboards for visibility into approval requests, session recordings, and privileged access activity, though dashboard customization remains limited. Reporting is supported, including reporting on cloud permissions, and reports can be generated on demand, created manually, or scheduled for automated delivery. Session management covers SSH, FTP/SFTP, RDP, databases, and browser-based access, with recording, playback, and audit trails, while database sessions can also be governed through blocking rules and immediate session termination by administrators. For credentials and secrets, JumpCloud provides vaulting, password rotation, password obfuscation, and a dedicated secrets vault for DevOps, automation, and machine identities. It also supports ephemeral short-lived secrets for pipeline runs and automated tasks. EPM is another strength, covering Windows, macOS, and Linux, with sandboxing, allow-listing, and integrity checks after elevation. The platform also benefits from integration with JumpCloud's IAM and device management capabilities. AI agent handling is on the roadmap. However, the solution currently lacks account discovery capabilities, OT/ICS support, PUEBA, customizable dashboards, and deeper command-level session analytics.

JumpCloud's more interesting direction lies in how it is combining PAM with the rest of its platform rather than treating privileged access as an isolated control point. That includes the use of ML and GenAI to improve usability, streamline reporting, and support administrative workflows, while taking a measured approach to automation in access-sensitive scenarios. The solution will appeal most to organizations that want PAM tied closely to identity and device context, value ease of deployment, and prefer a more operationally manageable alternative to heavier legacy platforms.

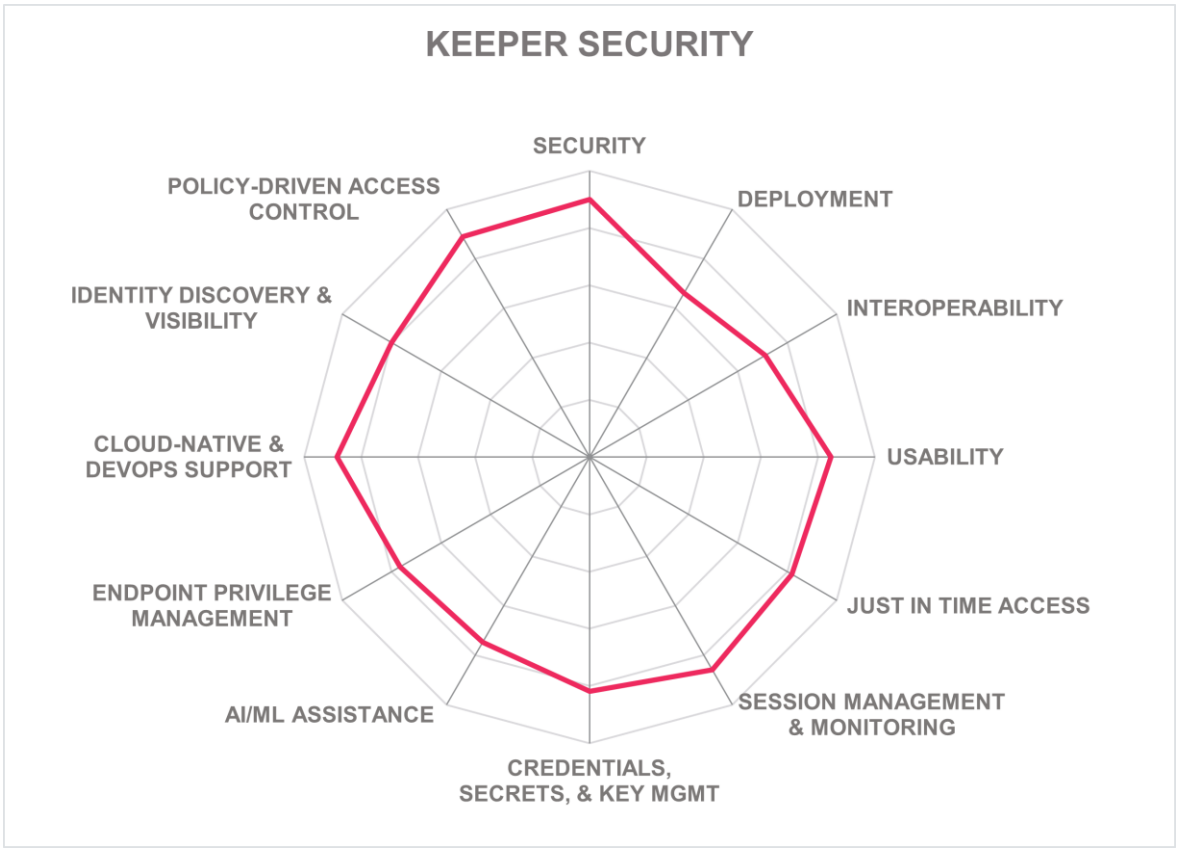
Strengths

- Private browsing extends PAM to web-based assets
- Good integration with IAM and device management
- Credential obfuscation reduces user exposure to secrets
- Ephemeral secrets support DevOps and automation use cases
- Broad EPM across major operating systems
- VPN-less access model reduces friction and cost
- Session recording and audit coverage across multiple protocols

Challenges

- No account discovery capabilities
- Dashboard customization is limited
- No PUEBA support
- No command-level session search indexing
- Granular privilege elevation controls remain limited
- More connectors for IdPs and SaaS apps would be useful

Keeper Security – KeeperPAM



Leadership

Keeper Security was founded in 2011. The company is based in Chicago, Illinois, in the US and is privately held. Its PAM offering, KeeperPAM, builds on the vendor's earlier strength in password management and extends it into a broader privileged access platform. KeeperPAM is delivered primarily as a fully hosted, multitenant SaaS service, with hybrid deployment components such as customer-controlled gateways and connectors for internal systems, directory services, and network-restricted resources. The architecture follows a zero-knowledge model in which sensitive data is encrypted client-side and cryptographic keys remain under customer control. Keeper is ISO/IEC 27001/27017/27018 certified, SOC 2 Type II attested, and US FedRAMP Class D (High) certified. Its crypto modules are FIPS

140-3 validated and utilized Kyber-based Quantum-Resistant Cryptography (QRC) to protect against future quantum computing threats. Licensing is per user for both KeeperPAM and Keeper Password Manager. The company targets small, medium, mid-market, and large enterprises.

KeeperPAM provides a broad set of privileged access capabilities that span credential vaulting, secrets management, remote access, session control, and endpoint privilege management. The platform supports privileged access for human users, service accounts, NHIs, and emerging AI-driven use cases through a common administrative framework. Privileged access can be granted through passwordless, zero-trust encrypted sessions launched directly from the vault, with credentials injected at runtime rather than exposed to users. The platform supports static credentials where needed, but places greater value on short-lived access, ephemeral accounts, and session-based privilege assignment that reduce standing exposure. Keeper's zero-knowledge design remains one of its main differentiators, especially in regulated sectors. Another is its browser isolation capability, built by the original creators of Apache Guacamole, which provides isolated access to internal and cloud-based web applications through an encrypted tunnel inside the vault. Keeper integrates with multiple IdPs, including Microsoft Entra ID, AWS, Google Workspace, Okta, OneLogin, Ping Identity, RSA, SecureAuth, and JumpCloud.

The admin console includes built-in dashboards, preconfigured reports, immutable audit records, and optional SIEM or syslog integration for centralized monitoring. Cloud and infrastructure coverage spans AWS, Azure, GCP, Alibaba Cloud, IBM Cloud, Salesforce, VMware Cloud, and other platforms, while DevOps support is delivered through Keeper Secrets Manager, APIs, SDKs, and integrations for CI/CD and automation workflows. The platform supports agentless session management for SSH, RDP, databases, web applications, and tunneled access, with graphical and text-based session recordings. JIT access is implemented through time-bound privileged sessions, injected credentials, and temporary privileged accounts, while discovery identifies accounts, resources, and service-account relationships through a gateway-based model. EPM extends policy-based elevation, MFA, approvals, and least-privilege enforcement across Windows, macOS, and Linux. In addition, the solution incorporates PUEBA by turning risk signals into immediate actions and by generating encrypted session summaries for audits.

KeeperAI adds real-time, policy-driven analysis of privileged sessions at the PAM gateway layer, classifies risk, generates encrypted session summaries, and can automatically terminate suspicious activity. This gives Keeper a stronger response posture than vendors that limit session monitoring to recording and later review. The company is also extending GenAI into administrative areas such as reporting, policy generation, and user management through Keeper Commander. Additional engineering depth is visible in areas such as remote browser isolation, zero-trust encrypted SaaS sessions, and Forcefield technology for protecting sensitive applications and processes on Windows against memory scraping and credential harvesting. KeeperPAM is well suited for organizations that want broad PAM functionality in a unified SaaS platform without inheriting the operational burden of more fragmented deployments.

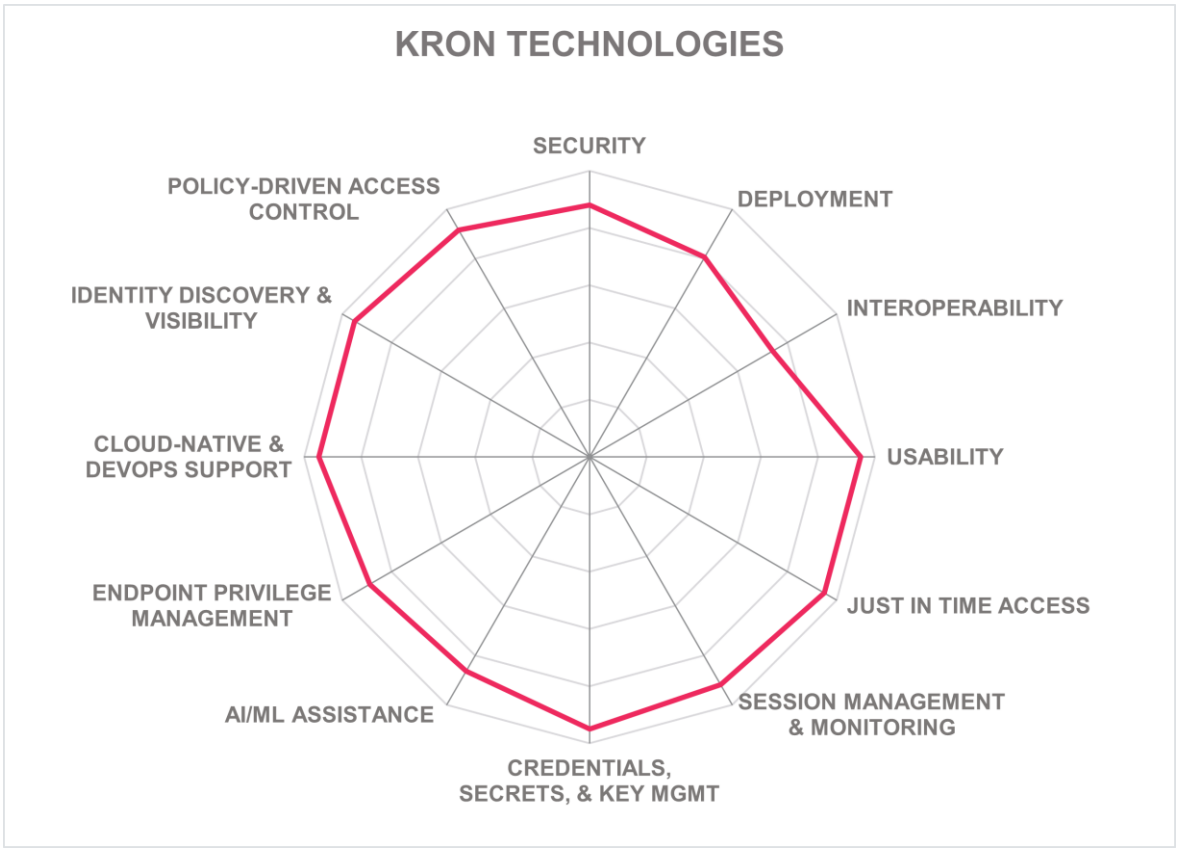
Strengths

- Zero-knowledge architecture reduces provider-side exposure
- Broad PAM coverage in one management plane
- Good identity provider and directory integration
- Agentless privileged session access for many resources
- Built-in reporting and immutable audit trails
- Solid support for secrets and DevOps workflows
- Real-time AI-driven session monitoring and termination
- Supports ephemeral accounts and time-bound access
- Remote browser isolation protects web application access
- Multiple security certifications

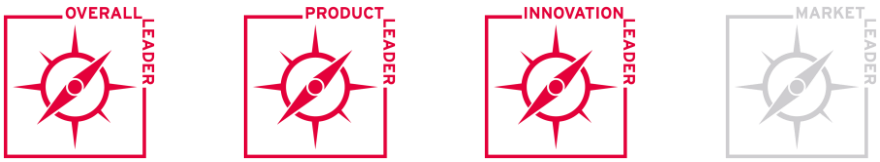
Challenges

- No discovery of privilege use in scripts
- No endpoint application or command sandboxing
- Limited support for automated cryptographic key lifecycle management
- JIT credential issuance remains incomplete, but improvements are on the roadmap

Kron Technologies – Kron PAM



Leadership



Established in 2007 and headquartered in Istanbul, Turkey, Kron Technologies is a publicly traded company with a growing presence beyond its home market. The company has built a solid footprint across EMEA and APAC, while also expanding into North America, Central Asia, and parts of LATAM. Its PAM offering, Kron PAM, is aimed at mid-market, medium-sized, and large enterprises, with customers across finance, insurance, telecom, energy, defense, and other regulated sectors. The platform is available in several delivery models, including on-premises self-hosted, public and private cloud self-hosted SaaS, fully hosted SaaS, MSP-hosted SaaS, virtual appliance, and vault options spanning mixed environments. Kron PAM does not use a microservices architecture, but it does support multitenancy,

which is particularly relevant for MSSPs and MSPs. Licensing is available per user, per node, and per time period. The company is ISO 27001 certified, but SOC 2 Type II attestation remains in progress.

At its core, the platform combines centralized vaulting, automated credential rotation, approval-driven access, and policy-based authorization across servers, databases, network devices, applications, and NHIs. One of its more interesting characteristics is the breadth of identity coverage, extending from administrators and third parties to scripts, service accounts, applications, APIs, scripts, and bots, CI/CD workflows, and AI-driven service use cases. The solution places particular emphasis on removing hard-coded credentials from source code, configuration files, and operational tooling through APIs, SDKs, plugins, and agent-based delivery where needed. Secure remote access is handled without requiring traditional VPN dependence, while time-bound access, step-up authentication, and session brokering reduce exposure to standing privileges. The solution integrates with Microsoft Entra ID, Okta, Ping Identity, and Keycloak.

The platform delivers broad functional coverage across the areas expected from a full PAM suite. Kron PAM provides dashboards with visibility into users, devices, vaulted accounts, MFA usage, discovered privileged accounts, and anomaly signals, alongside roughly 20 predefined compliance reports and customer-defined reporting options with scheduling support. Its integration model is broad, covering directories, identity providers, SIEM, SOAR, ITSM, cloud platforms, and CI/CD tooling through REST, SOAP, JSON-RPC, XML-RPC, and Google Remote Procedure Call (gRPC) APIs, though webhook support is absent. Kron PAM supports deployment and device inventory discovery across IBM Cloud, Alibaba Cloud, and VMware environments. However, its CIEM capabilities, specifically entitlement discovery, risk scoring, and remediation recommendations, are currently limited to AWS, Azure, and GCP. JIT access is handled through time-bound approvals, ephemeral credentials, short-lived secrets, and session brokering. Session management is extensive across SSH, Telnet, RDP, VNC, HTTPS, SQL, SFTP, and TCP/IP-based legacy protocols, with command control, OCR-supported indexing for graphical sessions, and real-time monitoring. Kron also supports EPM for Windows, Linux, and macOS, policy-driven access control, privileged behavior analytics, and key and secrets lifecycle management for both enterprise and DevOps use cases. Additionally, the solution supports privileged access control for network devices and OT/ICS environments through SSH, Telnet, and RDP, while extending coverage to native industrial protocols such as Modbus and Profibus via a TCP/IP proxy.

Kron PAM’s differentiation comes from the combination of multitenancy, database access control with dynamic data masking, secure remote access for third parties, coverage for OT and legacy protocols, and support for NHIs and automation workflows. The company has also started to extend the product with ML for anomaly detection, usability, and cyber threat identification, while GenAI is being used for query creation and administrative assistance. That said, the use of AI still appears to be at an earlier stage when it comes to remediation depth. Kron PAM is a solid alternative for organizations that need broad PAM coverage, strong deployment flexibility, and support for regulated, operationally diverse, and OT/ICS environments.

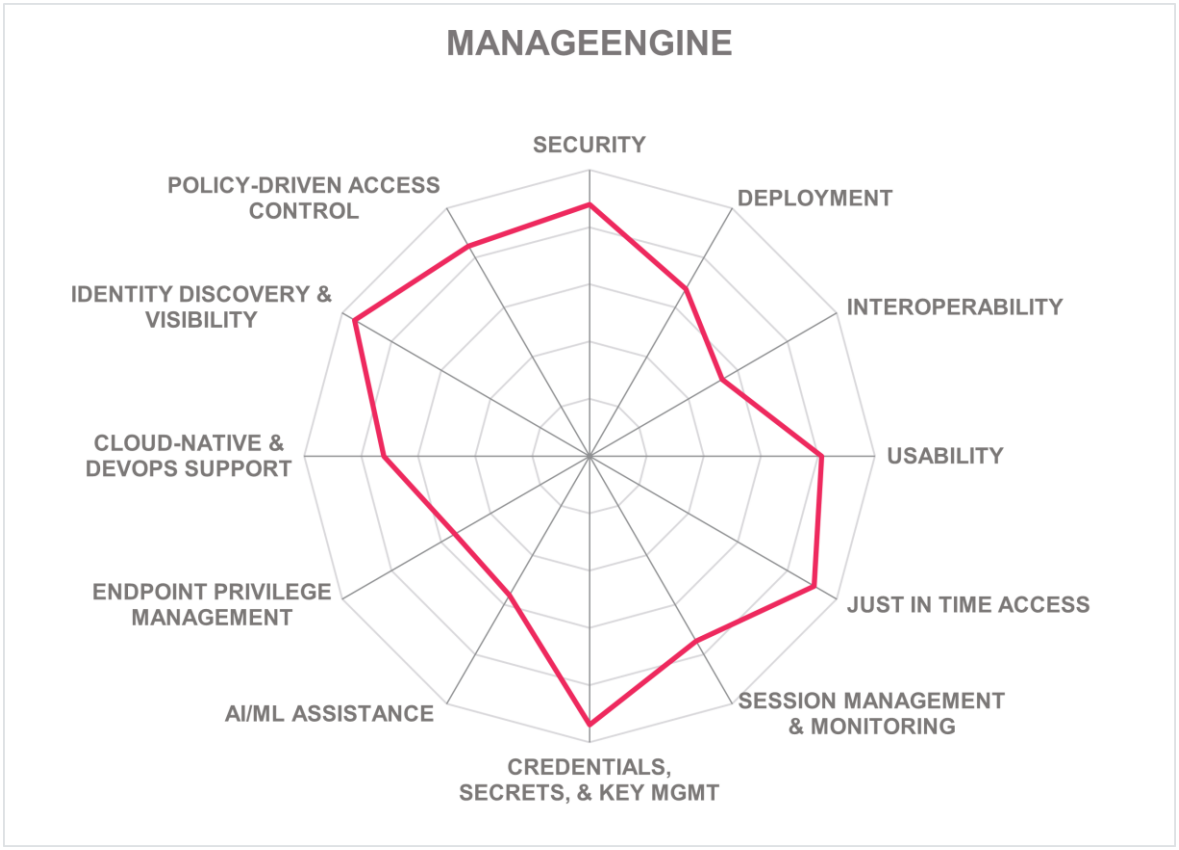
Strengths

- AI and ML used for anomaly and threat detection
- Established presence in Central Asia and Latin America
- Broad PAM coverage across human and NHIs
- Advanced session control across diverse protocols
- Useful database access controls with dynamic masking
- Good support for OT and legacy environments
- JIT access with ephemeral credential options
- Wide cloud and CI/CD integration coverage
- Does not require agents on endpoints, simplifying deployment and maintenance

Challenges

- Webhook support is not available
- ISO 27001 and SOC 2 Type II still pending
- AI remediation capabilities remain limited
- No support for application sandboxing

ManageEngine – PAM360



Leadership

ManageEngine, a division of Zoho Corporation, was founded in 2002 and is headquartered in Pleasanton, California, in the US. It offers a broad portfolio of IT management and security solutions. Its offerings span IT help desk, patch and vulnerability management, SIEM, MDM, IGA, PAM, ITDR, analytics, and low-code development tools. Its PAM portfolio consists of four products: PAM360, Password Manager Pro, Key Manager Plus, and Access Manager Plus. ManageEngine's PAM360 brings together the core capabilities of the other offerings while adding broader enterprise functionality. PAM360 is delivered through on-premises self-hosted deployments, customer-managed deployments in public cloud environments, virtual appliance options, and a vault-based architecture that enables separation of application and

vault components. It also supports multitenancy through an MSP edition with customer data segmentation. It is not hosted as SaaS by the vendor. Licensing is based on the number of administrative users, with no cap on end users or managed endpoints. The platform is certified to ISO 27001 and UK Cyber Essentials Plus. It has also been attested to SOC 2 Type II requirements. ManageEngine targets medium-sized organizations, mid-market customers, and large enterprises across North America, EMEA, APAC, and LATAM.

PAM360 discovers privileged identities across Microsoft Windows (AD and Entra ID), Linux, databases, cloud environments, and network infrastructure, and then brings them into a centralized vault for governance, rotation, and controlled use. Beyond privileged passwords, it manages SSH keys, certificates, encryption keys, tokens, and other non-human access artifacts, reflecting a wider view of privileged identity. One of its more distinctive elements is the inclusion of certificate lifecycle management as a native PAM function rather than as a separate adjacent tool. PAM360 also applies a dynamic trust-score model to access decisions, using real-time signals from users and devices to grant, restrict, or deny access. The platform's breadth is strengthened further by its ties to the wider ManageEngine portfolio, particularly for analytics, anomaly detection, response, and event correlation. It also integrates with IdPs such as Broadcom SiteMinder, IBM Security Verify, Microsoft Entra ID, Okta, One Identity, and Ping Identity.

Dashboards provide visibility into password activity, user activity, key usage, and security events, while reporting is broad, with compliance-ready reports and customizable query-based reporting for more granular analysis. Session management is delivered through browser-based access and native thick-client support, with recording for web, SSH, RDP, VNC, and supported database sessions, alongside command filtering and application control. The platform supports JIT elevation for Windows and Linux, including time-bound privilege elevation for local and domain accounts, self-service elevation for approved applications, and command-level control in Linux environments. Secrets, certificates, SSH keys, and encryption keys are vaulted centrally and rotated automatically, with HSM and Azure Key Vault integration available. For cloud environments, the CIEM module provides visibility into AWS and Azure entitlements, identifies shadow admin risk and inactive access, and can apply AI-generated least-privilege remediation policies. PAM360 also supports APIs, SDKs, CI/CD integrations, privileged task automation, and policy-driven access controls based on dynamic trust scoring. EPM, however, is limited to Windows. However, coverage for OT and ICS environments remains limited, webhook support is not yet available though planned, and the platform's monolithic architecture may constrain scalability and modular extensibility in more distributed deployments.

PAM360's main appeal lies in how much functionality ManageEngine has assembled into a single installable platform without making deployment overly demanding. The product can be adopted in a phased way, starting with vaulting and session control, then extending into task orchestration, CIEM, privilege elevation, and workflow automation. ManageEngine has also started to bring GenAI into practical areas, particularly session summarization and policy guidance for cloud entitlements. PAM360 is particularly well suited for organizations that are already ManageEngine customers as well as organizations that want to consolidate privileged account governance, session control, certificate management, and automation into one platform.

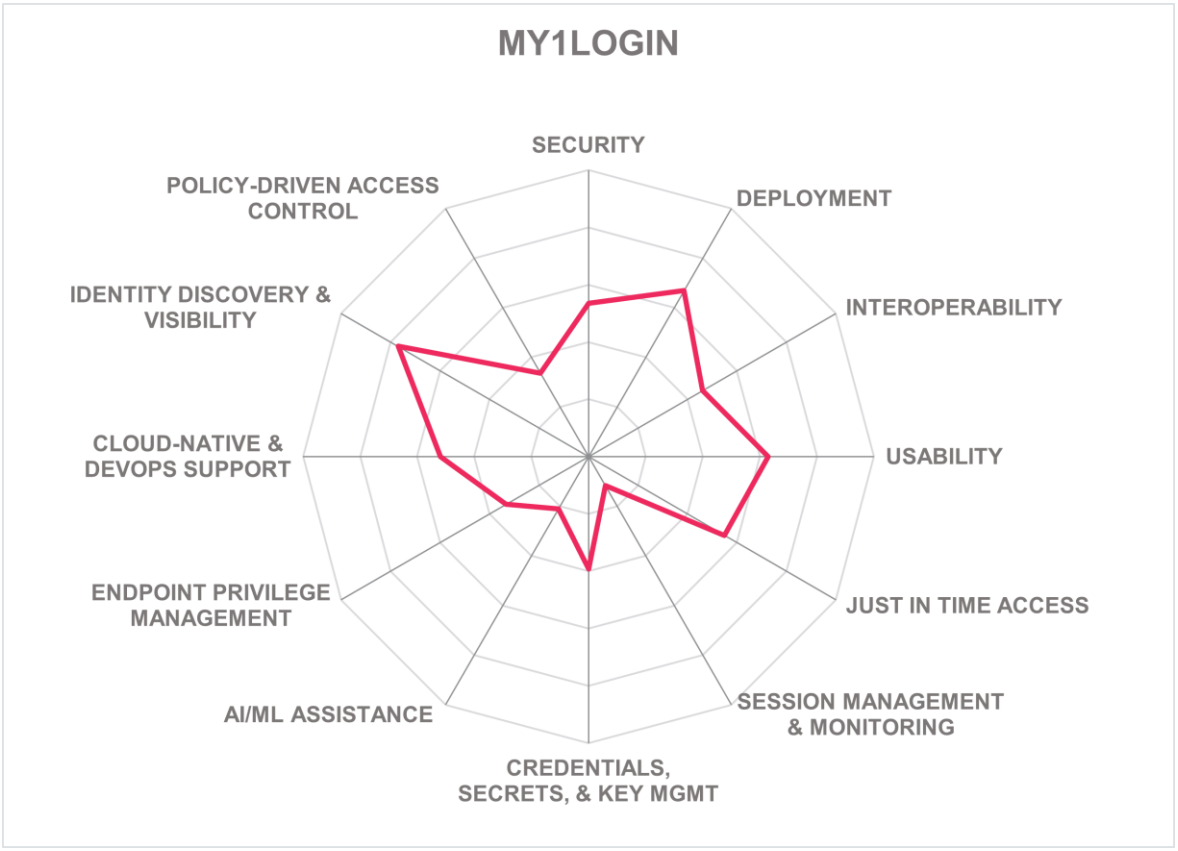
Strengths

- Modular suite covering IAM, PAM, SIEM, and ITDR
- Native certificate lifecycle management included
- Admin-based licensing favors large estates
- Strong JIT access controls
- Useful automation for privileged workflows
- Good support for secrets and key management
- Wide integration across ManageEngine portfolio
- Practical use of GenAI for session summarization and policy guidance

Challenges

- EPM is Windows-only
- OT and ICS support remains limited
- CIEM breadth is still expanding
- No Webhook support yet, but on the roadmap
- Operates on a monolithic architecture rather than a microservices-based framework, which may limit scalability and modularity
- Not hosted as SaaS

My1Login – My1Login Enterprise Identity and Access Management



Founded in 2007 and headquartered in London, UK, My1Login is a privately held vendor focused on enterprise IAM with a particular emphasis on authentication and access control policies. Its My1Login Enterprise IAM offering combines enterprise password management, privileged access controls for shared and individual accounts, and SSO for both modern and legacy applications. The solution is delivered through fully hosted SaaS, self-hosted public cloud SaaS, a virtual appliance, and a hybrid vault option that keeps sensitive encryption operations within the customer's environment. It is not built on a microservices architecture. My1Login's 256-bit Advanced Encryption Standard (AES) encryption model is built around a zero-knowledge design in which encryption keys remain inside the customer perimeter. The company currently lacks standard security certifications, but they report that they are working toward ISO 27001. Licensing is available per user per time period. The company primarily targets medium and mid-market organizations in the UK and selected European markets.

My1Login's platform detects external application usage, identifies shadow IT, and enables administrators to determine when credentials should be captured, vaulted, and governed by policy. Once enrolled, credentials are associated with the user's corporate identity and can

be released for future access without exposing the underlying password. However, the solution is currently limited to human user accounts. My1Login also supports shared account password management with granular permissions for reading, updating, onward sharing, deletion, and ownership transfer. The vendor's Zero Login and Zero UI capabilities eliminate the need for separate authentication steps or interaction with a vault by inheriting authentication from the user's existing enterprise session and operating transparently in the background, enabling silent authentication and automatic credential injection directly within applications without requiring users to view or manage credentials. The platform interoperates closely with Microsoft AD and Entra ID for synchronization, deprovisioning, suspension, and group-based policy enforcement. It supports SAML and OIDC for SSO, while its patented form-finder extends access control to credential-based web applications without requiring APIs or custom integration work for every target system.

My1Login also supports temporal sharing and policy-based JIT provisioning tied to directory group membership, including use cases for least-privilege access and selected DevOps workflows. Dashboards provide centralized visibility into cross-account access and cloud application usage, including shadow IT detection, but they are not customizable and do not provide real-time threat alerting. Support extends across AWS, Azure, GCP, Oracle, IBM Cloud, VMware, Salesforce, SAP, and related environments. EPM is available for Windows and macOS, including application filtering and allow-listing, but without broader privilege elevation depth. Also, the solution does not provide PUEBA features, session recording or monitoring capabilities, nor broader credential lifecycle management across all secret types.

My1Login provides a pragmatic approach for organizations seeking tighter control over password-based access without the overhead of a full PAM deployment. However, the company has limited partner ecosystem and market awareness outside of Europe. Its architecture and deployment model make it especially relevant where enterprises need faster rollout, reduced user friction, and better governance over third-party and cloud application access. The zero-knowledge vault model, broad compatibility with applications that lack modern federation, and emphasis on silent background operation give it a point of differentiation. At the same time, the platform remains more focused on controlled access and credential abstraction than on the broader control, monitoring, and analytics capabilities typically associated with traditional PAM solutions. Overall, My1Login is well suited to mid-market and enterprise organizations seeking practical password control, strong directory integration, and low-friction privileged access across mixed application estates.

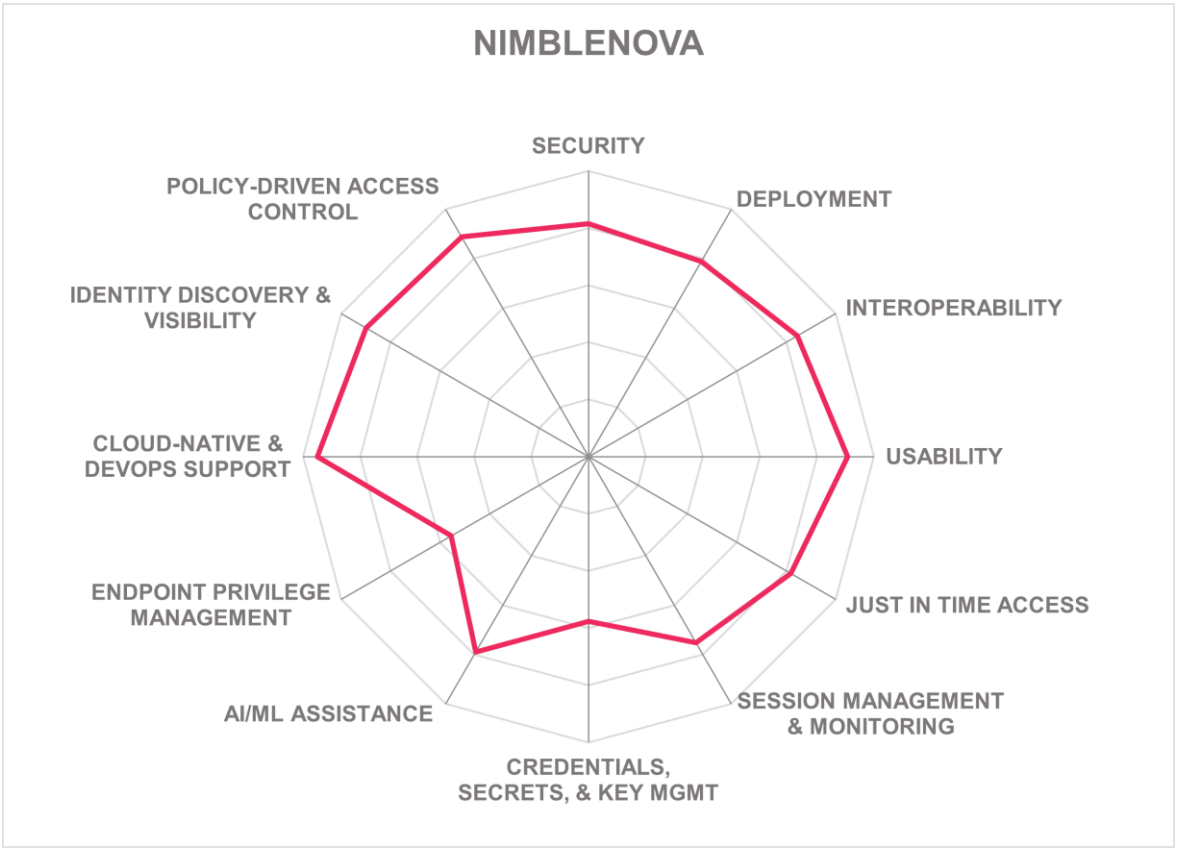
Strengths

- Zero-knowledge encryption model limits vendor-side exposure
- Zero Login and Zero UI capabilities reduce user friction
- Good support for legacy application SSO
- Granular shared account permission controls
- Good directory synchronization with Microsoft AD and Entra ID
- Shadow IT discovery adds useful visibility
- Temporal access policies support controlled credential release
- Flexible deployment options suit varied customer needs

Challenges

- Limited market visibility outside of Europe
- Pending ISO 27001 and SOC 2 Type II
- Small partner ecosystem compared to other vendors
- No session recording or playback
- Dashboards lack customization options
- Limited credential lifecycle management breadth
- No PUEBA capabilities or NHIs coverage

nimbleNOVA – nimbleNOVA



Cross Identity introduced its nimbleNOVA converged identity security platform in 2025, specifically designed to give smaller and mid-market organizations a broader identity security capability without forcing them to assemble and manage multiple separate tools. Cross Identity itself, which produces nimbleNOVA, was founded in 2017 and is headquartered in Schaumburg, Illinois, US. with significant operations and focus on Indian markets. The solution brings governance, privileged access, and identity security into one system, with deployment options that include fully hosted SaaS, MSP-hosted SaaS, virtual appliance, and fully customer-managed installations for organizations with strict control or residency requirements. Licensing is based on numbers of users and transactions. The platform is ISO/IEC 27001, and SOC 2 Type II certified. Geographical coverage includes North America, EMEA, APAC, and LATAM.

nimbleNOVA combines password vaulting, access governance, risk-based access, session isolation, and cloud entitlement visibility, enabling privilege to be evaluated in context rather than granted as a static entitlement. It supports privileged users, service accounts, NHIs, application accounts, API keys, certificates, SSH keys, and other credential types, with lifecycle management and automated rotation based on time, policy, events, or risk triggers. The platform also allows organizations to define what constitutes privileged access, which is particularly relevant in environments such as smaller businesses, where roles are fluid and access tends to accumulate over time. Additionally, the platform provides customizable dashboards with drill-down analysis, persona-specific views, and reporting that can be generated through natural language prompts. The solution integrates with multiple IdPs, such as Microsoft Entra ID, Ping Identity, Okta, Keycloak, OneLogin, and Idira.

Its PAM coverage includes JIT elevation with time-bound access, workflow-driven approvals, automatic revocation, and dynamic policy decisions based on identity attributes, device posture, geolocation, request timing, and risk score. Session management is well developed, covering SSH, RDP, web administrative consoles, and proxied database sessions, with recording and alerts for restricted commands, file transfers, escalation attempts, failed access, and policy violations. Credential and secrets management spans local and hosted infrastructure, with support for passwords, SSH keys, API tokens, and certificates. Cloud infrastructure support includes AWS, Azure, GCP, Oracle, IBM Cloud, Alibaba Cloud, SAP, Salesforce, OVH Cloud, and VMware. PUEBA adds behavioral visibility for privileged activity across supported Windows and Linux environments, helping identify suspicious patterns and higher-risk actions during privileged use. EPM is available for Windows endpoints, where it supports privilege elevation controls and application filtering to reduce local admin exposure. Integration support is extensive, with REST, SCIM, LDAP, SOAP, GraphQL, gRPC, JSON-RPC, Extensible Markup Language Remote Procedure Call (XML-RPC), and webhooks, plus SIEM interoperability. The use of ML and GenAI for role mining, access reviews, analytics, and report generation adds helpful operational support, but the product does not support ephemeral secrets, OT or ICS coverage, or JIT admin provisioning for endpoints. Also, break-glass access to vaulted credentials is not currently supported.

The platform’s integration of access governance, session control, and entitlement visibility enables organizations to move away from fragmented oversight toward a more coherent view of privilege across users, services, and infrastructure. Its support for both human and NHIs, along with flexible privilege definitions, addresses environments where access boundaries are less formal and roles change frequently. nimbleNOVA will appeal most to small and mid-market organizations that need broad PAM and identity security coverage in one product and want stronger control over privilege without managing a pile of separate tools.

Strengths

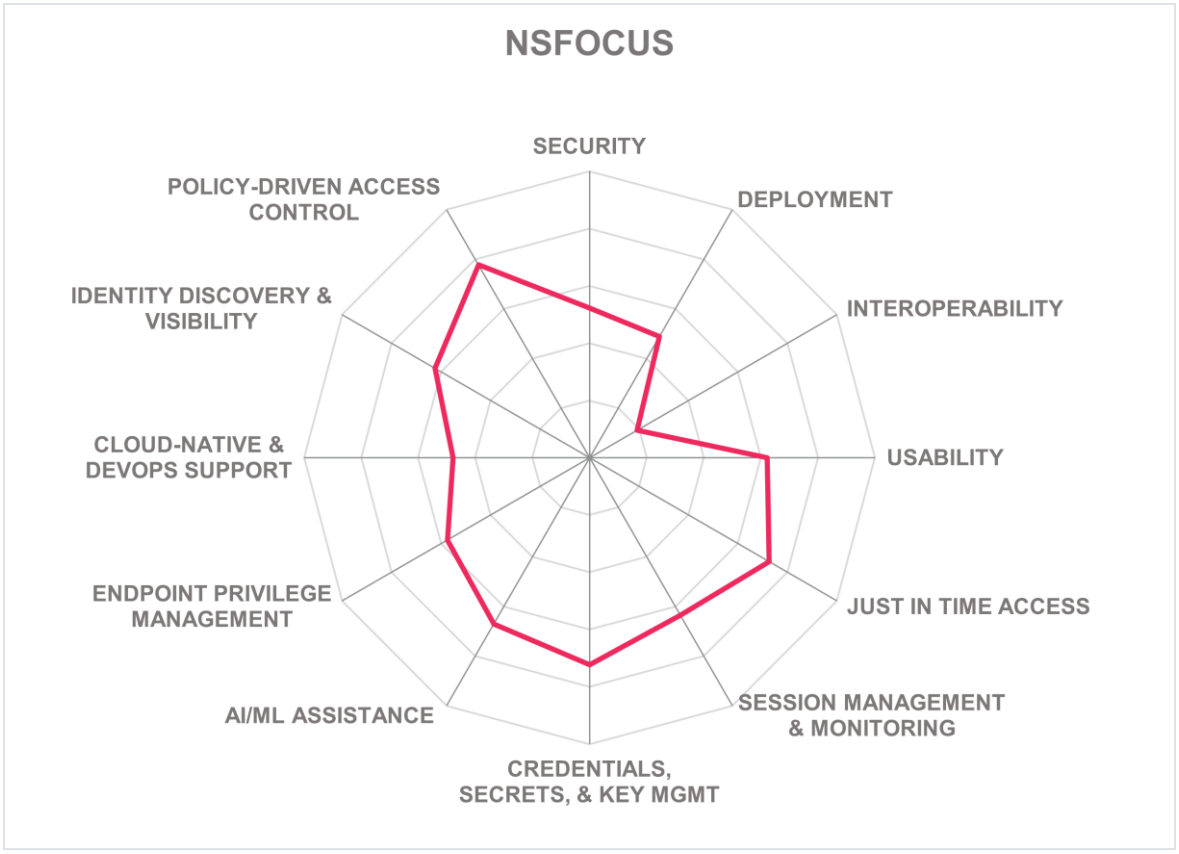
- Converged PAM, governance, and identity security approach
- Context-aware JIT access with risk-based checks
- Broad credential and secrets lifecycle management
- Good cloud entitlement visibility across major providers
- Custom dashboards with persona-based views

- Natural language reporting and analytics support
- Broad compliance coverage and multi-environment support
- Session recording and policy-based control are well developed

Challenges

- No support for ephemeral secrets issuance
- Break-glass access to vaulted credentials is not supported
- Lack of OT/ICS coverage
- EPM limited to Windows
- No JIT provisioning for endpoints or CI/CD pipeline-driven access

NSFOCUS – NSFOCUS Operational Security Management System



NSFOCUS is an established provider of internet and application security solutions with over two decades of industry experience. The company operates globally with more than 3,000 employees, dual headquarters in Beijing, China, and an international presence spanning over 50 offices, including its international business division in Milpitas, California. Its customer base includes several of the world's largest telecommunications providers and financial institutions. Its PAM-related offering, NSFOCUS Operational Security Management System, centers on the NSFOCUS Bastion Host which is a broader IAM platform that combines privileged access controls, access management, and zero trust elements. The product is available as appliance self-hosted, virtual appliance, fully hosted SaaS, and deployments with vault options across hosted and local environments. It does not use a microservices architecture. NSFOCUS aligns the platform with Chinese compliance requirements, including domestic cryptographic algorithm standards, the Commercial Secret Cryptographic Product Certification Certificate, and the national standard for operation and maintenance security management products. It does not have ISO 27001 or SOC 2 Type II certifications. Pricing is based on managed assets and device performance tiers. NSFOCUS

mainly targets small and mid-sized organizations in China, particularly in government, energy, education, science and technology, culture, and healthcare.

At its core, the platform delivers a 4A model that has account, authentication, authorization, and audit a single control plane for privileged operations. The emphasis is on centralized management of primary and secondary accounts, fine-grained command control, and traceable access to sensitive systems. NSFOCUS takes a practical approach to privileged access by combining bastion host capabilities with dynamic authorization, work-order approval, and what it describes as a zero-permission baseline. Access is granted only after approval and only for the approved scope and duration, after which rights are revoked. The product supports privileged access for human and NHIs, including machine identities used in automation scenarios. Vaulting covers passwords and privileged account credentials, with encrypted storage, policy-based complexity and validity controls, proxy login for supported targets, and check-in/check-out processes for high-privilege use. A useful differentiator is its fit for the domestic Chinese technology stack, including support for local CPUs, operating systems, and databases. NSFOCUS does not integrate with any IdP.

NSFOCUS provides built-in dashboards that visualize cross-account access relationships and surface real-time alerts tied to privileged activity, though dashboard customization is limited. Reporting is built in and maps identities to the systems, accounts, and privileged resources they can access. Session management is one of the stronger parts of the product: the platform brokers and records RDP, SSH, Telnet, FTP/SFTP, Session Control Protocol (SCP), Transparent Network Substrate (TNS), VNC, X11, and web-based sessions, while supporting screen recording, application logging, and screen scraping for detailed audit trails. JIT access is implemented through work orders and vault mode, where a user requests time-bound access to a specific device and account, approval is granted in real time, and permissions are automatically withdrawn after the session. The product also supports ephemeral credential issuance for both human and NHIs, especially for DevOps and automated processes, backed by a dedicated secrets vault and a hardware-based encryption card for key management. Additional capabilities include automatic password rotation, limited standing-account discovery, command filtering, policy-based privilege escalation for automated workflows, REST APIs, cloud privilege governance for Alibaba Cloud, and EPM support for Windows, macOS, and Galaxy Kylin/UOS. GenAI is used to create queries, while ML is applied to detect abnormal activities and suspicious accounts such as ghost and idle accounts.

NSFOCUS combines core bastion host functions with compliance-driven controls, session oversight, workflow-based approvals, and increasing use of AI to improve detection and usability. The product is especially relevant for Chinese organizations that need privileged access control aligned with local regulations and domestic infrastructure requirements, and for buyers that prefer an integrated approach instead of stitching together multiple specialized tools. However, the solution is unlikely to meet the needs of organizations outside of China.

Strengths

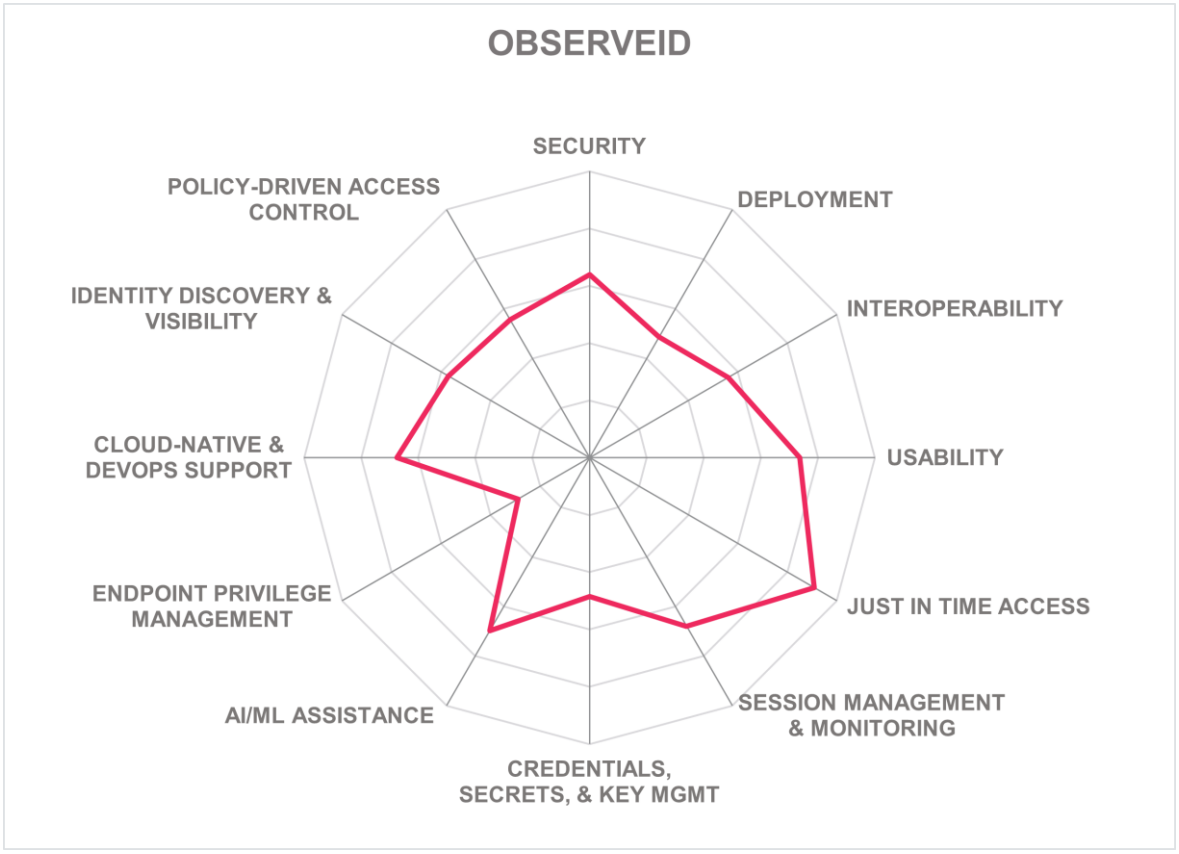
- Deep alignment with Chinese compliance requirements

- Granular command-level privileged control
- Solid session monitoring and recording coverage
- JIT access with approval workflows
- Hardware-backed key management for secrets protection
- Support for machine identities and DevOps secrets
- Deep compatibility with domestic Chinese technology stacks
- Bastion host deployment minimizes disruption to existing network architecture

Challenges

- Limited presence outside the Chinese market
- Cloud support is narrow and Alibaba-focused
- Dashboard customization is limited
- No OT or ICS coverage
- Lacks PUEBA capabilities
- No integrations with IdPs

ObserveID – ObserveID Converged Identity Security Platform



ObserveID is an emerging provider in the IAM space. Headquartered in Aliso Viejo, California, with additional operations in India, ObserveID was founded in 2021 as a spin-off from Guardian Technology, an established Managed Services Provider (MSP). Its ObserveID Converged Identity Security Platform brings together IAM, IGA, PAM, CIEM, (Identity Visibility and Intelligence Platform (IVIP), and what the company describes as IVOP (Identity Visibility and Observability Platform) in a single interface. The product is delivered through several models, including fully hosted SaaS, public cloud self-hosted SaaS, private cloud self-hosted SaaS, MSP-hosted SaaS, and Bring Your Own Cloud (BYOC) options for AWS, Azure, Rackspace, and Oracle private cloud environments. ObserveID asserts ISO 27001 and SOC 2 Type II attestation. Licensing is subscription-based and priced per identity. The company targets medium-sized organizations, the mid-market, and larger enterprises, with most customer traction in North America and a growing presence in EMEA, APAC, and LATAM.

The platform centralizes identities, entitlements, policies, activity logs, and privileged resources into what is effectively a unified identity data layer, allowing analytics, reporting,

and access decisions to draw from the same context. On the PAM side, the solution supports password vaulting, automated password rotation, time-bound JIT access, and privileged account unlock workflows tied to approvals and audit trails. ObserveID also supports temporary access for both human and NHIs, with credentials that can be issued, rotated, revoked, and retired based on policy, events, time, or risk signals. A particularly interesting capability is support for switching multi-persona logins, where a user's profile and effective access can change dynamically according to role, task, or time of day. That is a practical feature for sectors such as healthcare, hospitality, and education, where role fluidity is common and static access models often fail. It integrates with multiple IdPs, including Microsoft Entra ID, Okta, Ping Identity, Duo, and more.

The platform provides configurable dashboards tailored to role and responsibility, which is important in a product that spans administrators, auditors, managers, and end users. Reporting is one of the stronger parts of the offering: built-in reports map relationships among identities, systems, accounts, and privileged resources, while GenAI is used for custom reports and user access reviews. ObserveID's OBI framework adds AI-driven analytics, alerting, and remediation workflows when anomalous activity is detected, with ML used to identify abnormal behavior and risk shifts. The PAM feature set includes session monitoring and recording across protocols such as SSH, RDP, VNC, X11, Telnet, SCP, and FTP/SFTP, with support for key logging, screen scraping, DVR-style capture, and event-based recording. JIT access is policy-driven, time-bound, and can be auto-approved under predefined rules. The platform also covers on-premises systems, SaaS, public cloud services, OT, ICS, and network devices, while CIEM capabilities extend visibility across AWS, Azure, GCP, and Oracle Cloud Infrastructure (OCI) with recommendations and automated posture actions. Support for Jenkins, GitHub, and Atlassian adds relevance for DevOps-oriented environments, although it does not extend to privilege escalation controls within CI/CD pipelines.

ObserveID's PAM capabilities focus on controlling and limiting privileged access through time-bound usage and enforced workflows. It provides a converged platform that can coexist with existing investments when full replacement is unrealistic. In addition, the company's AI work appears more structural than cosmetic, especially given its emphasis on customer-specific models, connector creation, analytics, and workflow support rather than a simple chatbot layer. ObserveID appears well suited for organizations that want broad identity security coverage, observability, and a more unified operating model without giving up deployment flexibility.

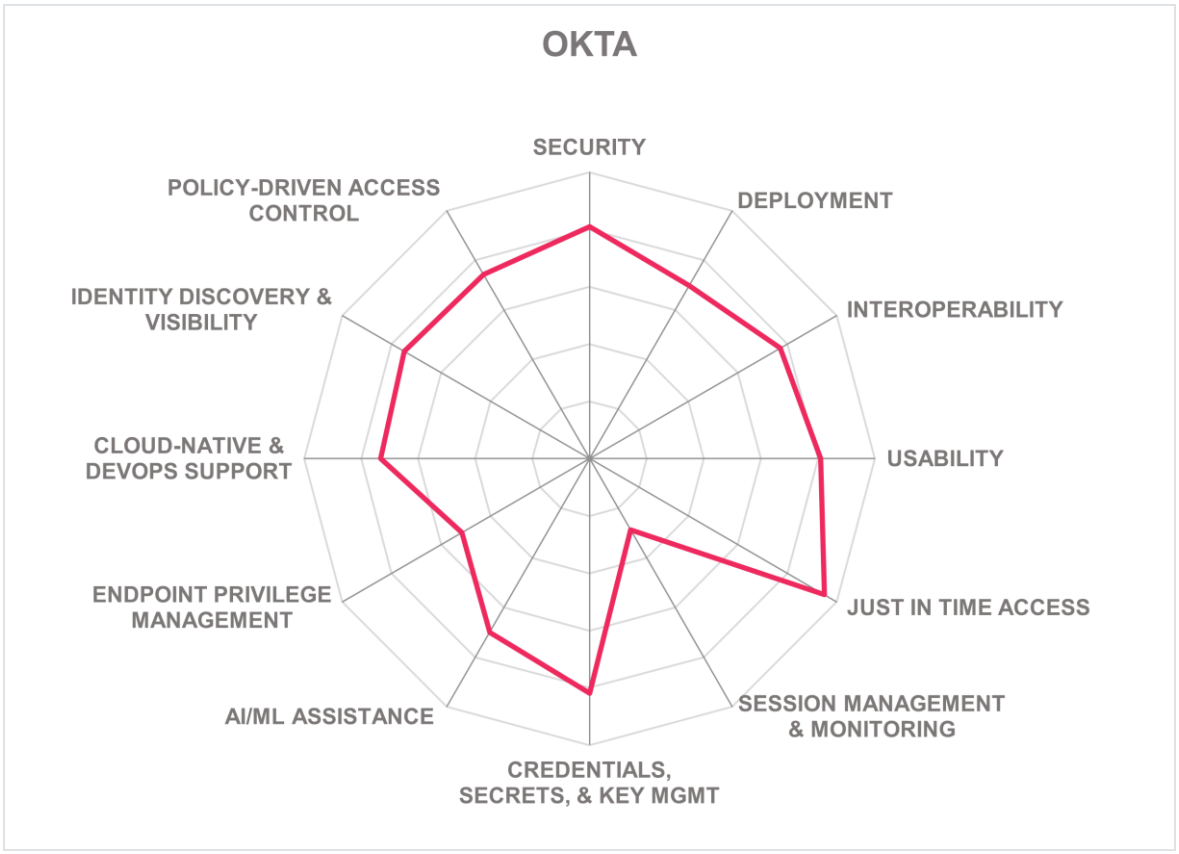
Strengths

- Unified IAM, IGA, PAM, CIEM, and IVOP approach
- Broad PAM coverage across diverse environments
- Time-bound JIT access with automatic expiration
- Flexible deployment and BYOC options
- Configurable dashboards for different user roles
- AI-assisted reporting and access reviews
- Session recording across many protocols
- Extensive prebuilt Application Connector Library for simplified integrations

Challenges

- Limited market maturity compared with established PAM vendors
- No dedicated DevOps secrets vault
- No command filtering for CLI sessions
- Scheduled rather than continuous account discovery
- EPM lacks application allow-listing and sandboxing

Okta – Okta Privileged Access (OPA)



Leadership

Headquartered in San Francisco, California, Okta has established its cloud identity platform as a significant player in workforce and customer identity management. Okta has expanded its identity portfolio through several strategic acquisitions, including Axiom Security, a modern, identity-centric PAM solution built for cloud, SaaS, and database environments. Axiom's technology is integrated into Okta Privileged Access (OPA) solution. While Okta's primary customer base remains heavily represented in North America, its focus has been global for some time, reflected in expanded international sales teams and region-specific initiatives. OPA is delivered as a multitenant SaaS offering, supported by lightweight agents and gateways, with public cloud deployment options. Pricing is based per resource, where a

resource can be a principal accessing OPA, including human users or workloads, or can be target systems and accounts that are under management within OPA. The Okta Platform has multiple security certifications which can be viewed at https://security.okta.com. Okta primarily targets mid-sized and large enterprises across regulated and general commercial sectors.

OPA focuses on eliminating standing privileges by issuing short-lived certificates, provisioning user accounts and entitlements only at the time of access and enforcing time-bound checkout with automatic credential rotation for systems that still require static credentials. For Linux and Windows servers, access is established using short-lived certificates issued on demand. For systems where static credentials remain necessary, the platform provides a centralized vault for local server accounts, Active Directory accounts, Okta admin accounts, and SaaS service accounts, and database accounts with automated rotation and controlled checkout. Access is governed through contextual policies that incorporate device posture, network conditions, and risk signals, and can require phishing-resistant MFA or approval workflows. Users submit JIT access, while approval flows can be handled directly in collaboration tools such as Slack or Microsoft Teams. Okta integrates with several IdPs, including Microsoft Entra ID, Ping Identity, and Google Workspace.

From a capability standpoint, Okta delivers a broad PAM feature set, though with some limitations in depth. The platform provides centralized visibility through dashboards and a consolidated system log that captures all privileged and identity-related activity. However, dashboards lack customization and detailed drill-down capabilities, and reporting does not fully map relationships between identities and privileged resources. Discovery and visibility are extended through Okta's Identity Security Posture Management (ISPM) capability, which identifies stale accounts, API keys, and service identities, prioritizes risks, and supports remediation workflows. JIT access is implemented through multiple mechanisms: for infrastructure access, short-lived certificates are issued after authentication and policy evaluation for SSH and RDP sessions, while for Active Directory and SaaS accounts, access is granted through time-bound checkout models with automatic credential rotation upon check-in or expiration. Secrets and key management combine secure vaulting with granular policies and automated rotation. Session recording is available for SSH and RDP sessions, but it lacks advanced monitoring, indexed activity search, and deeper analysis features. API support is limited to REST. Currently, the solution does not address OT, ICS, network devices, or non-traditional endpoints, nor does it include PUEBA or EPM capabilities.

Okta's direction reflects a shift toward managing NHIs and AI-driven workloads within the same control framework as human users. Okta is also developing capabilities to secure AI workloads through offerings such as Okta for AI Agents that allows you to discover, onboard, and protect agents. OPA is best suited for organizations already invested in the Okta platform that want to extend existing identity policies, risk signals, and integrations into privileged access without introducing a separate PAM control plane.

Strengths

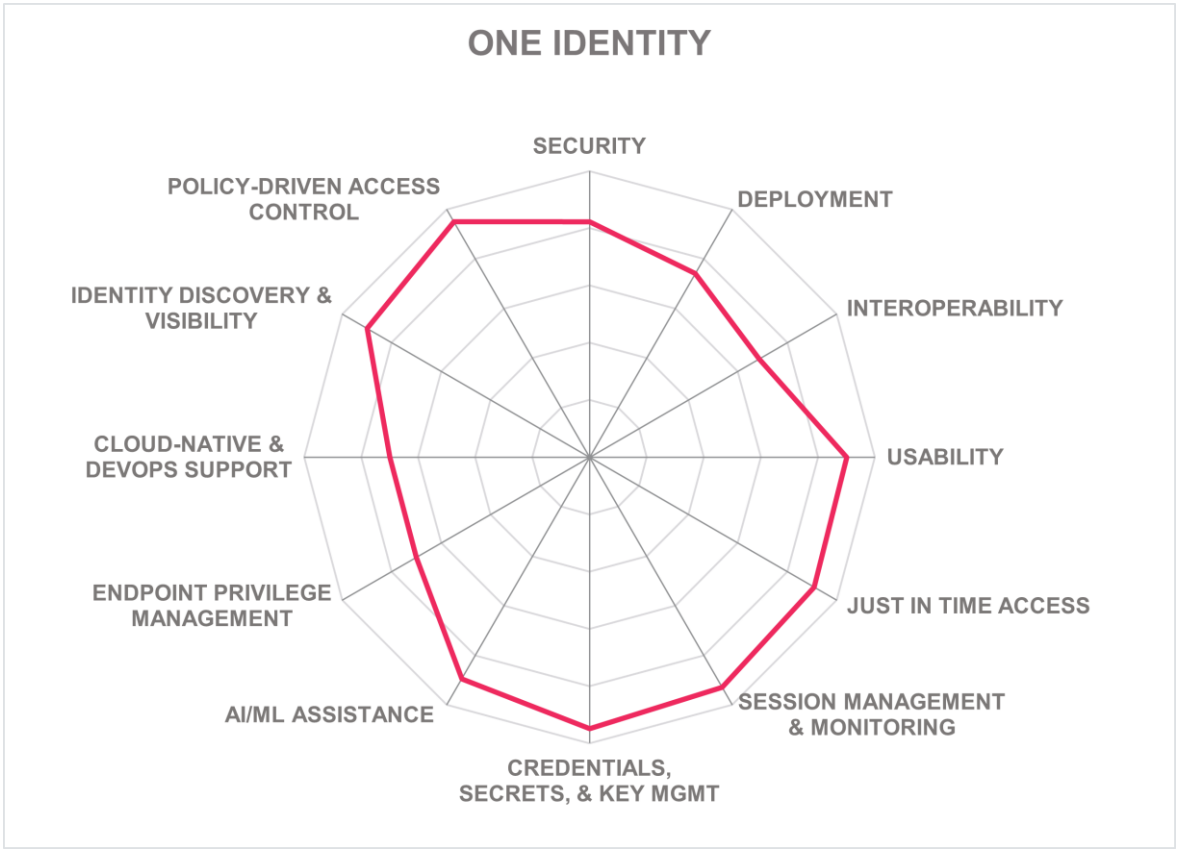
- Extensive partner and connector ecosystem
- Advanced JIT access using ephemeral certificates

- Secure vaulting with automated password rotation
- Effective discovery of stale accounts and service identities
- Context-aware access policies with risk-based controls
- Collaboration-based approval workflows reduce operational friction
- Unified audit trail across identity and privileged activities
- Approval flows can be integrated with Slack and Microsoft Teams

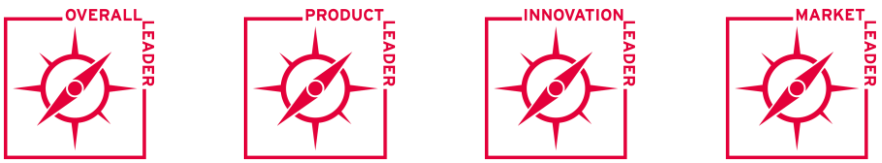
Challenges

- No PUEBA capabilities in the current offering
- Limited support for OT/ICS and legacy network systems
- Support for NHI privilege management is still maturing
- Database and Kubernetes access capabilities are still evolving, but improvements are on the roadmap
- Okta does not provide traditional EPM capabilities
- Session recording needs enhancement

One Identity – One Identity Safeguard Suite



Leadership



One Identity is a long-established identity security vendor with broad reach across North America, EMEA, APAC, and LATAM. Its PAM offering is the Safeguard portfolio, within a wider platform that brings together PAM, IGA, IAM, and Active Directory management. The portfolio includes One Identity Safeguard Suite, Identity Manager, and OneLogin, the latter acquired in 2021 to support a more unified identity approach. Safeguard On-Demand is One Identity's SaaS-based PAM offering within the One Identity Cloud, designed to deliver core privileged access capabilities with simplified deployment and management. It is available through self-hosted and fully hosted SaaS models, public or private cloud deployments, and physical or virtual appliances. The company also supports clustered high availability and

disaster recovery through a shared architecture. One Identity has achieved SOC 2 Type II attestation and ISO 27001 certification. Pricing options are per user, time period, appliance, and server. The company serves medium-sized organizations through large enterprises.

CIEM capabilities support discovery and visibility into infrastructure, objects, access by user and resource across Azure. AWS and GCP integrations are on the roadmap to broaden their CIEM capabilities across other cloud platforms. It also supports policy and anomaly detection through orphaned privileges, infrastructure without owners, mapping of identities with inappropriate access by geography and role. Access request and attestation/recertification of infrastructure access and entitlement mapping are included. The solution combines vaulting, session management, analytics, Unix and Linux privilege delegation, Active Directory bridging, EPM, and DevOps secrets brokering. Its JIT model is particularly strong: standing accounts can remain disabled until needed, then be enabled, added to the right group, used for the approved task, and removed or deactivated afterward. One Identity integrates with IdPs such as Microsoft Entra ID, Okta, and Ping Identity.

One Identity provides dashboards, reporting, and near real-time analytics, with plans to expand compliance-focused reporting and audit readiness views. Its session management is a major strength: agentless transparent proxying routes privileged sessions through an intermediary gateway that captures and interprets all traffic in real time, enabling full recording, searchable playback, and immediate enforcement of controls such as command restriction or session termination while activity is still in transit. OCR, free-text search, metadata inspection, keystroke analysis, and behavioral biometrics such as typing dynamics and mouse movement analysis enable detailed monitoring and risk analysis during privileged sessions. Credential, secrets, key, and certificate management are covered through vaulting, certificate workflows, and a DevOps secrets broker that can push to or pull from external vaults. Additionally, Safeguard supports Certificate Signing Requests (CSRs), allowing for integration with existing certificate issuance processes. Cloud coverage includes Azure, AWS, GCP, SAP, Salesforce, Oracle, and VMware. The platform also supports EPM for Windows, macOS, and Linux.

AI/ML is present in behavioral analytics and risk scoring, with broader AI capabilities still emerging and focused on usability and automation, rather than being a core differentiator of the PAM engine itself. One Identity is well suited to organizations that want mature PAM capabilities with Unix and Active Directory depth, broad session control, and a credible path toward privilege governance rather than PAM as a silo.

Strengths

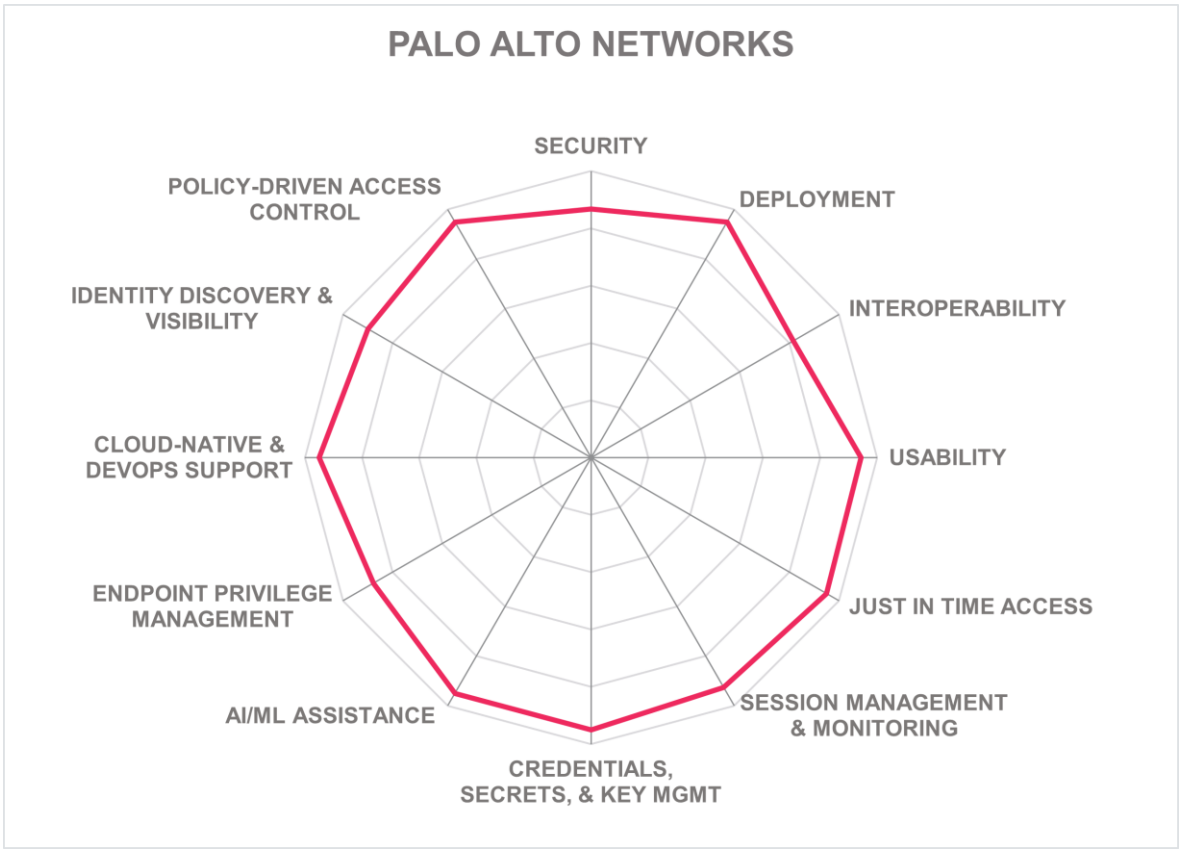
- Global partner ecosystem
- Broad PAM, IGA, and IAM integration
- Deep Unix, Linux, and Active Directory coverage
- Mature JIT privileged access workflows
- Advanced secrets, certificate, and DevOps support
- Behavioral analytics adds context to session monitoring
- Runs on multiple types of architectures including microservices, traditional monolithic client/server, and web services architectures

- Supports discovery and visibility into infrastructure, objects, and access by user and resource

Challenges

- CIEM depth remains limited to Azure, but AWS and GCP are on the roadmap
- Machine Identity roadmap continues to evolve, with broader inventory and governance capabilities still developing
- ML/AI capabilities continue to evolve and innovate
- Some advanced capabilities may need additional One Identity products
- While PAM Essentials accelerated Safeguard modernization, strategic focus has shifted to Safeguard On-Demand

Palo Alto Networks (formerly CyberArk) – The Idira Identity Security Platform



Leadership

Founded in 1999 and headquartered in Israel and the US, CyberArk is widely recognized as a long-standing provider in the PAM space. The company has built a global presence across North America, EMEA, and APAC, with a focus on large and mid-sized organizations in regulated and security-sensitive industries. Its portfolio is anchored in the newly-launched Idira CyberArk Identity Security Platform, which includes Privilege Access Management, Endpoint Privilege Manager, Secure Cloud Access, Secrets Manager, and Secure

Infrastructure Access. The platform is delivered through flexible deployment models, including SaaS, self-hosted, and managed service options. Idira CyberArk supports standards such as ISO 27001/27017/27018, SOC 2 Type II, and US FedRAMP High. Licensing is based on numbers of users, servers, and workstations. In early 2026, CyberArk was acquired by Palo Alto Networks, rebranding and launching as the Idira Identity Platform, further extending its reach into broader identity, network and security operations.

Idira's approach to PAM centers on eliminating standing privileges across human, machine, and AI identities. The platform enforces ZSP through JIT access, where privileges are dynamically created at session start and revoked immediately after use. For human users, ephemeral accounts are provisioned for Windows, Linux, database, macOS, and Kubernetes access, with attribute-based policies governing scope and duration. Credentials are vaulted and never exposed to endpoints, with session brokering ensuring isolation. For machine identities and workloads, Idira generates short-lived secrets and certificates, including the Secure Production Identity Framework For Everyone (SPIFFE)-based identities for cloud-native environments. This unified model extends to AI agents, treating them as first-class identities with controlled, auditable access. The platform's breadth across identity types, combined with credential abstraction and ephemeral access models, reflects a shift away from static privilege assignment toward contextual, time-bound access control. While Idira provides an IAM solution, it also integrates with IdPs such as Okta, Microsoft Entra ID, Ping Identity, JumpCloud, and OneLogin.

Discovery capabilities identify privileged accounts, entitlements, secrets, and workload identities across hybrid infrastructure, SaaS applications, and cloud environments, feeding into risk-based remediation workflows. Idira provides centralized dashboards and reporting through a unified control plane, offering visibility into privileged sessions, risk indicators, and compliance posture. Session management includes full recording, monitoring, and forensic playback, with credential injection ensuring that sensitive data is never exposed. JIT access is enforced through policy-driven workflows that evaluate identity, device, and contextual risk before granting ephemeral privileges. EPM delivers granular control over application execution and elevation across Windows, macOS, and Linux, including step-up authentication and ransomware protection. Secrets and key management extend into DevOps pipelines, integrating with tools such as Jenkins and Terraform. AI-driven analytics support threat detection and response, with automated remediation actions orchestrated through built-in workflows or external integrations. PUEBA capabilities analyze anomalous behavior across sessions, credentials, and access patterns to detect misuse.

The Idira platform has expanded to address emerging identity challenges, including machine identities, cloud entitlements, and AI-driven workloads. The introduction of Secure AI Agents reflects this direction, extending privilege controls to autonomous systems while maintaining auditability and governance. The platform's integration ecosystem, with over 1,000 connectors, supports interoperability with Security Information and Event Management (SIEM), XDR, ITSM, IAM, IGA, and cloud platforms. Its global footprint and flexible deployment options allow organizations to align with regional data requirements, including European data residency needs. With the added capabilities from Palo Alto Networks, particularly in telemetry and response, Idira CyberArk is positioned to connect identity security more closely with broader security operations. Palo Alto Networks (formerly

CyberArk) remains a strong fit for large enterprises and regulated sectors that require comprehensive privilege control across diverse identity types and infrastructure.

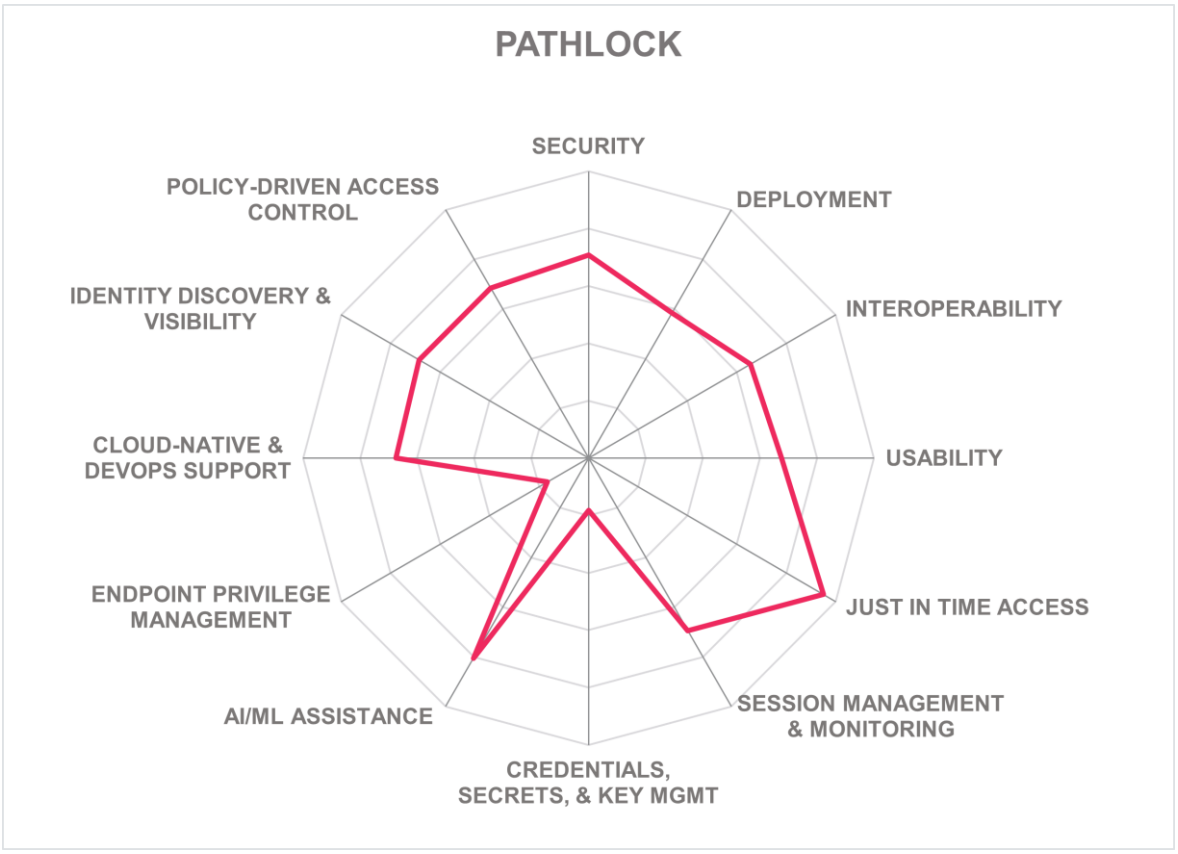
Strengths

- Broad coverage across human, machine, and AI identities
- Extensive integration ecosystem with 1000+ connectors
- Excellent session monitoring and recording capabilities
- Advanced secrets management for DevOps and cloud workloads
- Support for multi-platform EPM
- Unified platform for governance and privilege control
- Comprehensive discovery and identity visibility capabilities
- Implements ZSP to reduce identity-related risks and provides CIEM capabilities as part of Secure Cloud Access

Challenges

- Dashboards lack customization and flexible reporting options
- API session monitoring capabilities remain limited
- Comprehensive platform may require operational maturity to fully leverage
- AI agent security is a rapidly evolving area where Idira’s capabilities continue to expand
- Extensive ZSP and JIT customization enables tailored enforcement, yet this breadth requires mature policy design

Pathlock – Pathlock Cloud



Established in 2004 and headquartered in Denver, Colorado, Pathlock is a private company that approaches PAM from a different angle than most vendors in this report. Its relevant offering here is Pathlock Cloud. Deployment options include fully hosted SaaS and self-hosted installations, with SaaS delivered in a single-tenant model. Licensing is modular across its portfolios and is based primarily on the number of users in the customer's Enterprise Resource Planning (ERP) estate, not on the number of users accessing the reporting environment itself. Pathlock achieved SOC 2 Type II attestation and ISO 27001 certification. The company targets medium, mid-market, and large organizations. Coverage includes North America, EMEA, APAC, and a smaller footprint in LATAM.

Pathlock's approach differs from traditional PAM models in that it does not center on credential vaulting, password rotation, or session proxying. Instead, it focuses on the application layer, examining how privileged access is used within business systems such as SAP, Oracle, Microsoft Dynamics, Salesforce, and Workday. Privileged access is governed through policy-based, time-bound workflows that include approvals, segregation-of-duties checks, and contextual risk analysis prior to provisioning. Access can be requested, approved, granted temporarily, and revoked automatically. The emphasis is on controlling

and verifying elevated activity within business-critical applications, particularly where auditability and financial integrity are key requirements. Rather than relying on screen recordings or keystroke capture, the platform analyzes application and security logs to reconstruct user actions, compare them against the original justification for access, and attribute activity to individual users. Workflow configuration allows self-service requests, approvals, access reviews, policy enforcement, and remediation. Pathlock integrates with IdPs such as Microsoft Entra ID, Okta, Ping Identity, OneLogin, Google Workspace, and IBM Security Verify, as well as major business applications, through REST APIs, syslog, and webhooks support. It provides JIT provisioning for human users, especially in enterprise and SaaS applications, where elevated rights are granted for a defined window and then removed automatically. Governance for NHIs remains limited, but enhancements are on the roadmap. Mature dashboards with customization and drill-down capabilities are included, along with built-in reporting that maps identities to systems, accounts, privileged resources, and more. Pathlock also offers governance-driven monitoring for emergency and privileged sessions, including session start and end events, policy violations, and sensitive application changes. Discovery is identity- and application-centric, surfacing users, roles, entitlements, standing access, and risky combinations inside connected systems. Pathlock also includes PUEBA capabilities, though these are business-context and policy driven rather than full UEBA. By contrast, it does not provide credential vaulting, secrets lifecycle management, ephemeral credentials, key management, EPM, or protocol-level session recording. This reflects a deliberate architectural choice: Pathlock governs privileged access and activity at the application and identity layer, leaving infrastructure-level credential management, session brokering, and secrets handling to dedicated PAM and security platforms.

Pathlock's more interesting contribution is conceptual as much as technical. It applies identity governance discipline to privileged access in business systems where traditional PAM tools often have limited depth. It uses ML to improve usability and detect abnormal activity, with GenAI for policy creation, workflow building, and integration authoring. This is not a direct replacement for traditional PAM solutions, and Pathlock itself does not present it that way. It is better viewed as a complementary control layer for organizations that need tighter oversight of elevated access inside ERP, finance, HR, and other transaction-heavy applications. Pathlock is a good fit for enterprises that treat privileged activity in business applications as an audit, fraud, and compliance problem as much as a security one.

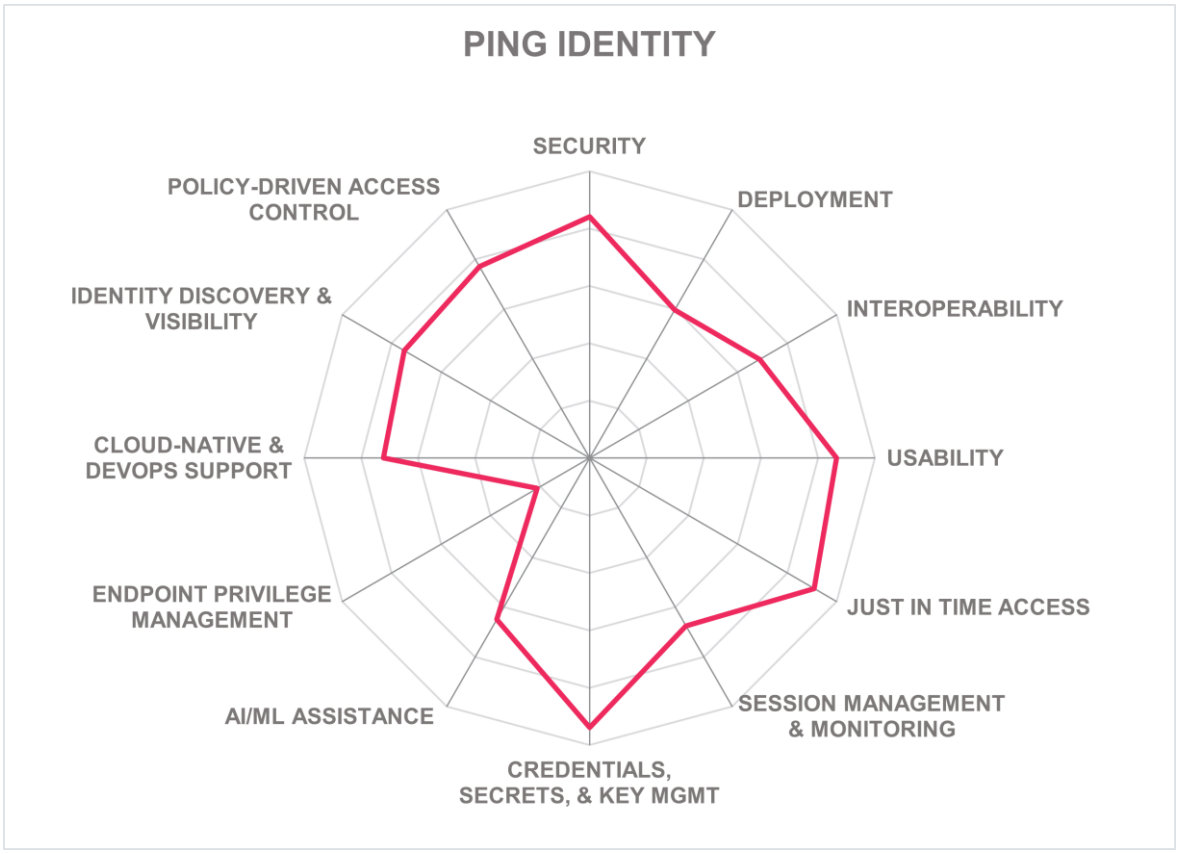
Strengths

- Application-centric approach to privileged access
- Good support for ERP-focused JIT access
- Detailed auditability for elevated business activity
- Useful Segregation of Duties risk analysis
- Customizable dashboards with drill-down investigation
- Broad enterprise application integration coverage
- Workflow-driven approvals and automatic revocation
- Clear differentiation from infrastructure PAM tools

Challenges

- Not a full traditional PAM suite
- Limited NHI coverage, but on the roadmap
- PUEBA capabilities lack full UEBA depth and analytics
- No credential vaulting, secrets lifecycle, or ephemeral credentials
- No protocol-level session recording capabilities
- Missing EPM capabilities

Ping Identity – Ping Identity Platform



Leadership

Ping Identity was founded in 2002 and is based in Denver, Colorado, in the US. The company is a long-established identity vendor whose portfolio spans access management, identity governance, fraud and risk controls, and privileged access. Its PAM offering, PingOne Privilege, reflects this broader identity focus and operates less as a traditional vault product and more as a privileged access layer built around identity, device trust, and session control. The service is delivered as a fully hosted SaaS offering. A Privilege Gateway can be deployed privately or publicly depending on customer requirements, allowing secure brokering of privileged sessions without major infrastructure change. The licensing model is based on the number of resources managed by PingOne Privilege. Ping Identity holds

certifications for ISO 27001, 27017, and 27018 and has SOC 2 Type II attestation The company targets organizations of all sizes, primarily in North America, with growing presence in EMEA, APAC, and LATAM. Recent acquisitions include Procyon and Keyless.

Rather than exposing standing credentials to administrators, developers, and other privileged users, PingOne Privilege issues JIT access to cloud and infrastructure resources at the point of use. The result is a model centered on ephemeral access, ZSP, and native tool usage rather than traditional vault-based credential retrieval. PingOne Privilege supports AWS, Azure, and GCP, as well as SSH, RDP, databases, Kubernetes, and cloud consoles. It can generate short-lived roles, tokens, and SSH certificates for both human and workload identities, while remaining vault-agnostic through integrations with external vaults such as HashiCorp and AWS Secrets Manager. This gives the product a distinct profile for organizations that want to reduce credential sprawl without forcing administrators into cumbersome workflows. PingOne Privilege integrates with any standards-based IdP supporting SAML, OIDC, or SCIM, including PingFederate, Okta, and Microsoft.

PingOne Privilege offers a well-developed set of PAM capabilities tied closely to privileged session control and cloud entitlement visibility. Through Identity Analyzer, PingOne Privilege continuously discovers cloud identities, roles, permissions, inheritance paths, and unused access across AWS, Azure, and GCP, helping teams identify excessive privileges and hidden exposure. Its dashboard provides identity-centric operational and security visibility across users, devices, resources, and access activity, while audit trails, session recordings, and entitlement reports support compliance and access reviews. Session monitoring covers SSH, RDP, and database CLI sessions, with real-time alerting for elevated commands, sensitive resource access, and policy violations. Policy-driven workflows are available through a self-service portal and integrations with Slack, Jira, ServiceNow, and Microsoft Teams. PingOne Privilege is complemented by PingOne Protect, which applies ML to evaluate user behavior, device posture, and contextual risk. These risk signals inform access decisions and enable continuous authorization and PUEBA within privileged sessions. EPM capabilities are not included. In addition, there is currently no support for OT or ICS environments.

PingOne Privilege reflects an identity-centric approach to privileged access management that reduces reliance on broad, persistent administrative access and traditional vault-based models. Its strongest qualities lie in JIT access, native cloud control, policy-driven approvals, and hardware-bound assurance tied to user and device trust. However, product maturity is still evolving compared to established PAM solutions. The product is especially relevant for enterprises with substantial hybrid infrastructure, DevOps activity, and existing investments in identity orchestration or governance that can be connected into a broader control plane. At the same time, its emphasis is on infrastructure and cloud privileged access rather than endpoint privilege or industrial environments. Ping Identity provides a strong solution for enterprises seeking PAM that aligns more closely with identity, Zero Trust, and least-privilege enforcement than with traditional credential handling.

Strengths

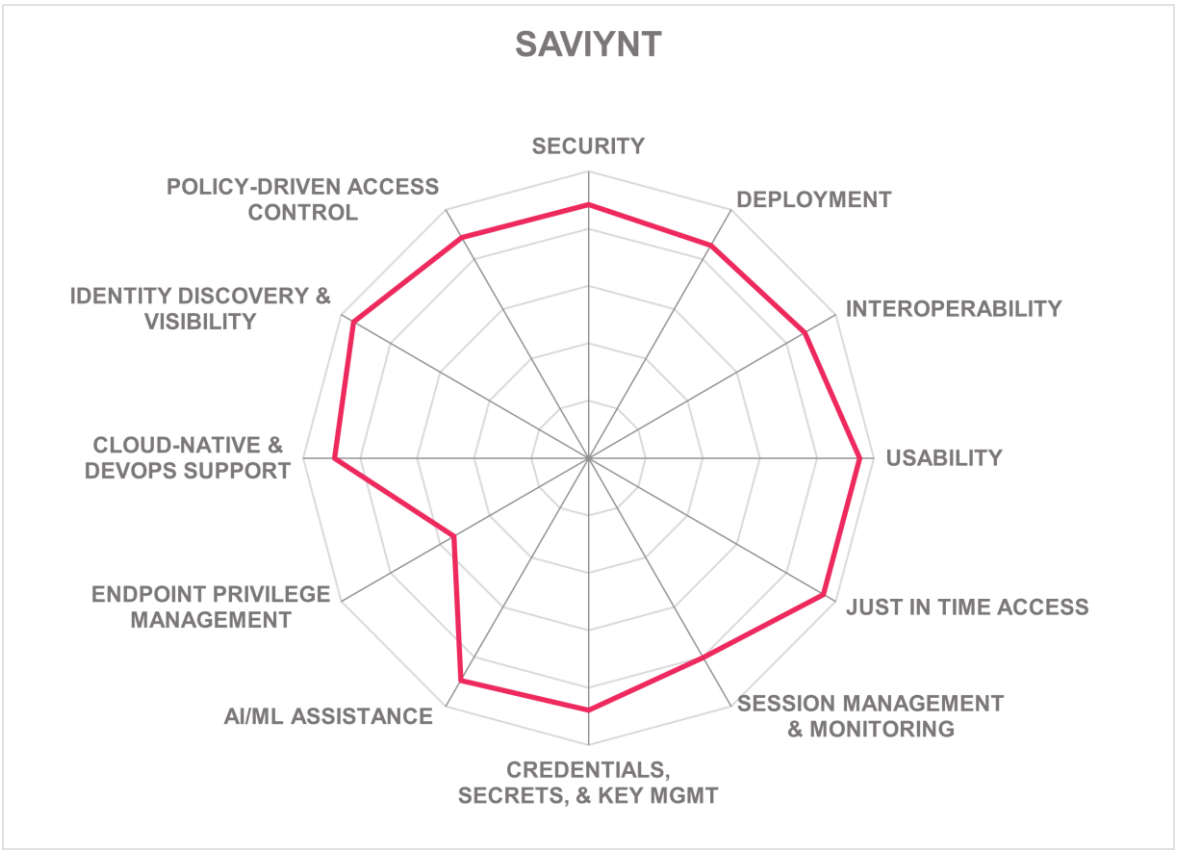
- Global partner ecosystem

- Identity-centric analytics with entitlement visibility
- Advanced JIT access across cloud and infrastructure
- Ephemeral credentials reduce standing privilege exposure
- Works with native admin and developer tools
- Continuous authorization using contextual risk signals
- Solid session monitoring and audit visibility
- Built-in CIEM through Identity Analyzer

Challenges

- Product maturity still evolving compared to established PAM vendors
- No native EPM capabilities
- No support for OT or ICS environments
- Break-glass depends on external vault integration
- No proprietary secrets vault included

Saviynt – Saviynt Identity Cloud



Leadership

Saviynt, founded in 2011 and headquartered in El Segundo, California, in the US, delivers a unified cloud-based identity security platform designed to meet the requirements of large enterprises and mid-market organizations. The company's flagship product, Saviynt Identity Cloud, contains IGA, PAM, access governance, ISPM, ITDR, and Identity Security for AI capabilities. Offered under a per-user licensing model, the platform is available as SaaS, a virtual appliance, or a container-based deployment, and supports on-premises, public and private cloud, and MSP-hosted environments. Saviynt is ISO 27001, UK Cyber Essentials Plus and PCI DSS certified, SOC 2 Type II attested, and US FedRAMP Class C (Moderate)

certified. The company targets mid-market and large organizations primarily in North America and EMEA, but with traction in APAC and LATAM.

The solution covers human and NHIs, including service accounts, machine identities, application credentials, cloud access keys, SSH keys, certificates, API tokens, hard-coded secrets, and AI agents. Its vault supports secure storage, controlled distribution, rotation, and lifecycle management for credentials, secrets, and encryption keys, while also integrating with external KMS services such as AWS KMS and Azure Key Vault. Saviynt's JIT Access extends time-bound elevation beyond traditional administrators to broader business populations, while Embedded Identity Verification adds remote onboarding controls for third parties and other untrusted or short-lived users. Saviynt also offers broad infrastructure coverage across AWS, Azure, GCP, Oracle, IBM Cloud, Salesforce, SAP, VMware, OVH Cloud, and other environments, with REST as the supported API model. Saviynt integrates with Microsoft Entra ID, Okta, Auth0, Ping Identity, AWS IAM Identity Center, Google Workspace, and SecureAuth.

Its cloud entitlement capabilities provide entitlement discovery, centralized visibility, policy enforcement, compliance monitoring, and unified governance across SaaS, IaaS, PaaS, and on-premises services. The platform provides mature dashboards and reporting, including customizable visualizations for operational and audit use cases. Supported report types include automated, real-time, machine learning-driven, ad hoc, manual, and GRC-related reports. Saviynt supports ephemeral account creation across databases, Active Directory, and other systems. It also supports credential checkout, credential injection, and token-based access, with automatic revocation after the approved period. Session management includes recorded connections for Telnet, SSH, FTP/SFTP, RDP, SCP, TNS, and VNC, with linked event logs to provide fuller activity context. EPM is supported for Windows and Linux systems, but not for macOS. PUEBA monitors activity across infrastructure, cloud platforms, containers, databases, and enterprise applications by analyzing session activity and audit logs. However, the platform does not support step-up authentication based on user location or network context. Discovery is continuous and identity-first, correlating privileged access to ownership, usage, and business context across servers, databases, SaaS, containers, CI/CD artifacts, and OT/ICS-related remote access scenarios.

Saviynt incorporates AI capabilities across the platform, including ML for recommending recurring report actions and GenAI-driven features such as query creation, agent-assisted onboarding, MCP, and Saviynt Co-Pilot. Its ISPM capabilities add further value by prioritizing remediation tasks through risk and trust scoring, including PAM-related KPIs. Overall, Saviynt is a strong fit for organizations that want PAM tied closely to governance, identity context, and time-bound access control across diverse enterprise environments.

Strengths

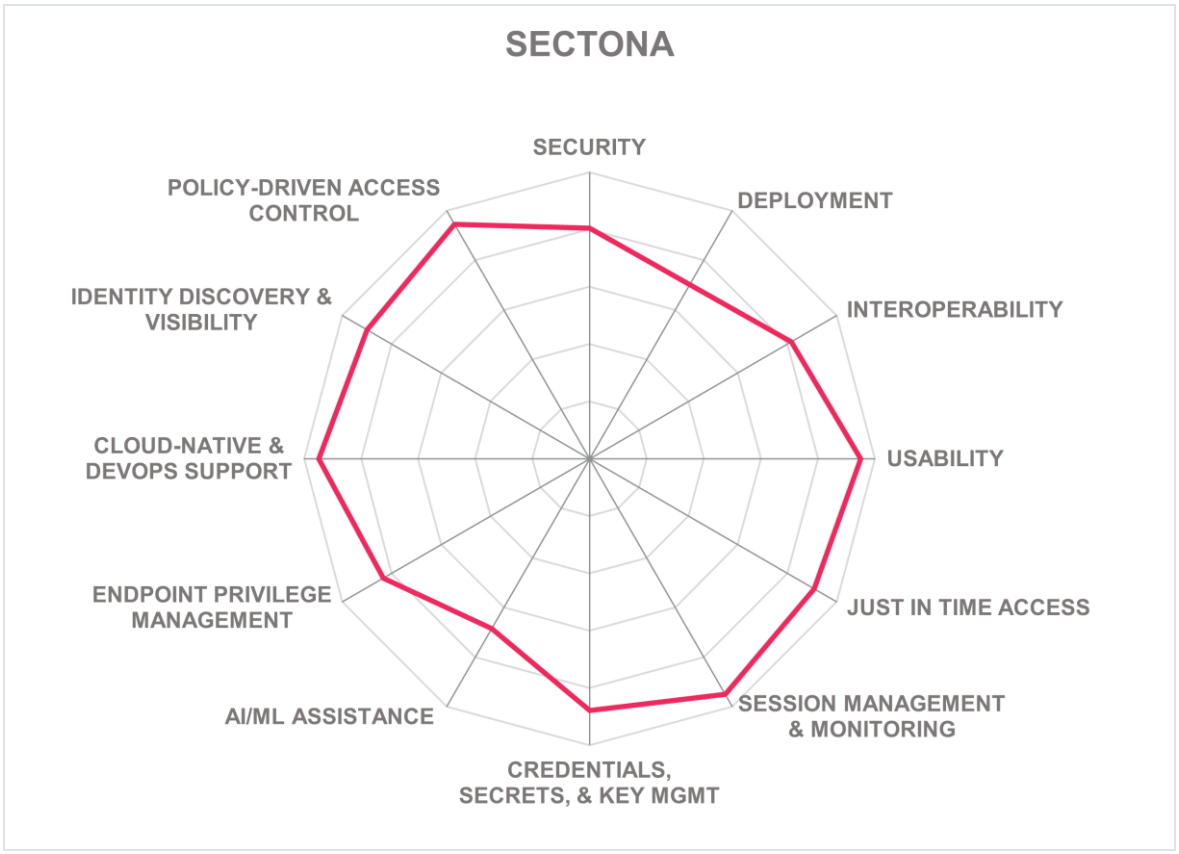
- Unified PAM and IGA architecture
- JIT access extended to non-admin business users
- ISPM prioritizes PAM risks with trust scoring
- Embedded identity verification for external PAM onboarding
- Continuous discovery of secrets across CI/CD artifacts

- Support for ephemeral accounts across multiple access models
- Wide infrastructure and cloud service coverage
- Continuous discovery with business context correlation

Challenges

- No macOS support for EPM
- No step-up authentication based on user location or network context

Sectona – Sectona Security Platform



Leadership

Sectona, founded in 2017 and headquartered in Mumbai, India, is a PAM specialist focused on privileged and remote access control across enterprise infrastructure. Its core offering centers on Sectona PAM and Sectona EPM, with Cloud Access Management (CAM) and related governance functions brought together through the broader Sectona Security Platform. The platform is designed as a unified control plane for privileged access rather than a collection of loosely connected modules, which is an important distinction in a market still shaped by product sprawl and acquired feature sets. Sectona supports a wide range of delivery models, including on-premises, an appliance, a virtual appliance, self-hosted public and private cloud, fully hosted SaaS, MSP-hosted SaaS, and vault options across mixed

environments. The platform supports REST, SOAP, and webhooks. Sectona is ISO 27001 certified, and SOC 2 Type II attestation is on the roadmap. Licensing is based on number of users for PAM and CAM. EPM licensing is based on the number of endpoints/workstations. Sectona's main focus is mid-market and large organizations in EMEA, APAC, North America, and Latin America.

The platform is designed to cover privileged access for human users, machine identities, and increasingly automated workflows. Vaulting covers passwords, SSH keys, API keys, certificates, and tokens, with policy controls, encrypted storage, credential brokering, and automated rotation based on time or event triggers. Secrets can also be revoked immediately and decommissioned when systems are retired. However, the platform does not provide native discovery of existing certificates, nor does it track certificate expiration or remediation workflows for expiring certificates. The solution supports standing privilege management alongside controlled elevation and remote access, while also extending into cloud entitlements and endpoint privilege control from the same console. Sectona reduces reliance on layered jump-server architectures and external database management by embedding access control, session brokering, and vault operations within a unified platform, limiting the need for multiple intermediary systems and separate database administration layers. Its inline database proxy for MySQL, MariaDB, and Microsoft SQL is designed to preserve a more native user experience, while the SaaS version of the Sectona Security Platform is intended to reduce infrastructure overhead on the customer side.

Sectona provides customizable dashboards and detailed reporting, including visibility into policy violations, access activity, compliance issues, and cloud permissions. Its session management is extensive, supporting Telnet, SSH, FTP, SFTP, RDP, SCP, TNS, VNC, and X11, with session recording through key logging, DVR, application logging, and screen scraping. It also captures lower-level activity and can trigger alerts for events such as critical command execution, leapfrogging, copied files, unusual account activity, or specific text strings entered during a session. These controls are paired with built-in risk scoring and analytics that assign composite risk to sessions. The platform incorporates PUEBA, combining user behavior analytics and threat analytics across operating systems, databases, network devices, and SaaS systems, enabling detection of abnormal user activity, anomalous access patterns, and high-risk behavior during privileged sessions. Sectona also supports scheduled and continuous discovery of privileged users, service accounts, scripts, and configuration files with privileged use. Its cloud support spans AWS, Azure, GCP, Oracle, IBM Cloud, Rackspace, and VMware. CIEM capabilities within the platform address risky entitlements and misconfigurations, while CAM adds dynamic RBAC, ephemeral console access, and JIT methods for human users, machine identities, and CI/CD workflows. EPM support extends across Windows, macOS, and Linux.

Sectona's use of ML for usability improvements, abnormal activity detection, and cyber threat identification adds analytical depth, though the platform's innovation is more architectural and operational than high-visibility feature innovation. The single-console model, native database proxy approach, and broad support for infrastructure, cloud, OT, ICS, and non-traditional endpoints reflect a distinct architectural approach. However, some gaps remain, particularly in certificate discovery and lifecycle management for existing certificates and the use of GenAI remains limited. Sectona is best suited to mid-sized and

large enterprises, especially those with mixed infrastructure, distributed administrator populations, and a need to manage privileged access across operations, engineering, and cloud teams.

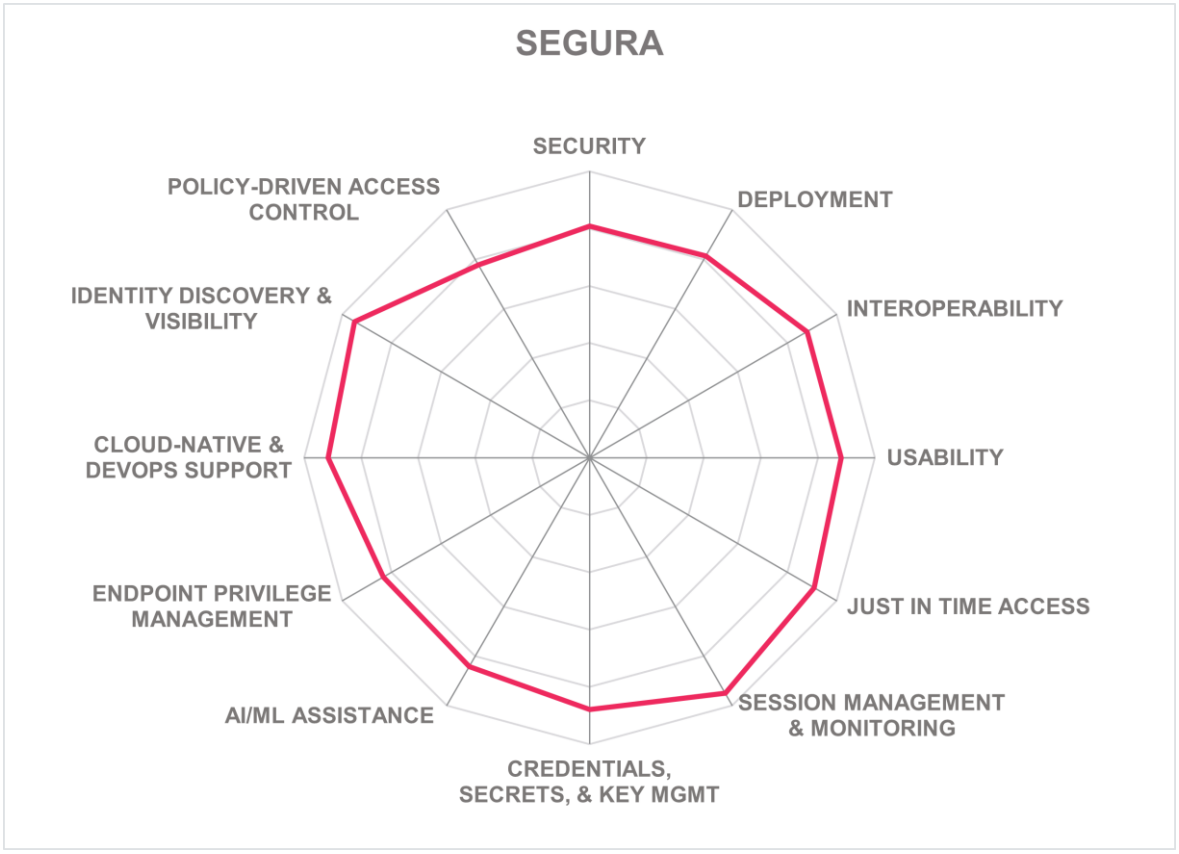
Strengths

- Continuous discovery of privileged identities and assets
- Broad deployment choice across hosted and self-hosted models
- Extensive session recording and monitoring depth
- Inline database proxy preserves native access experience
- Customizable dashboards and detailed compliance reporting
- Integrated PUEBA with risk scoring and analytics
- Good support for OT/ICS environments

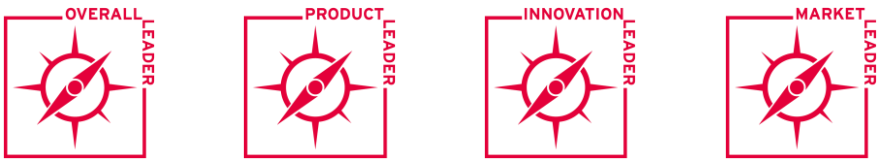
Challenges

- SOC 2 Type II still in progress
- Limited lifecycle visibility for existing certificates
- GenAI features are limited, but improvements are on the roadmap

Segura – Segura 360° Privilege Platform



Leadership



Segura, founded in 2001 and headquartered in São Paulo, Brazil, delivers a broad range of privileged access and identity security solutions under its Segura 360° Privilege Platform. Formerly known as senhasegura, the company has evolved into a recognized provider of PAM, CIEM, Certificate Lifecycle Management (CLM), and ITDR capabilities. Segura supports deployment across on-premises and public and private cloud environments, with delivery available as SaaS, a managed service, a hardware appliance, or container-based form factors. Licensing is based on the number or users and nodes. Segura's sweet spot is small and medium size organizations. Its historical strength lies in LATAM, which now accounts for approximately 45% of its customer base, reflecting a shift toward a more

balanced global presence. This change is driven by sustained expansion in EMEA and APAC, supported by localized go-to-market efforts, regional Centers of Excellence, and an extended partner network, alongside gradual growth in North America. The solution supports REST, gRPC, and webhooks for integration, and authentication and authorization standards such as OAuth 2.0, OIDC, SAML, and JSON Web Tokens (JWT). It is also certified ISO 27001 and SOC 2 Type II attested.

Segura's platform secures privileged access for human and NHIs across systems, databases, applications, cloud services, and operational environments, while also governing credentials, secrets, tokens, and certificates from a single control plane. Segura automatically discovers, inventories, and classifies privileged accounts across infrastructure, cloud, SaaS, DevOps, containers, and OT, including service accounts, shared accounts, shadow admins, and automation identities. Segura also brings machine identity management and certificate lifecycle management into the same platform, which is a sensible direction given how quickly certificates, keys, and service identities have become operational dependencies rather than niche concerns. Its CIEM capabilities reinforce that broader approach by identifying excessive permissions, mapping access relationships, and supporting remediation of overprivileged cloud identities. Segura supports integration with IdPs using standards such as SAML and OIDC and integrates with directory and authentication services via Lightweight Directory Access Protocol Secure (LDAPS), Terminal Access Controller Access-Control System Plus (TACACS+), Kerberos, and RADIUS. Certified integrations include Active Directory, Microsoft Entra ID, Google Workspace, authID, Keycloak, Okta, and ProID.

Reporting is supported through detailed audit trails, access histories, forensic logs, and session records, with integration into external SIEM tooling where needed. Segura provides broad cloud coverage across AWS, Azure, GCP, Oracle Cloud, and other platforms, while also supporting network devices, OT/ICS systems through agentless access, credential control, and session oversight. The platform also includes built-in dashboards, analytics, and alerting for security, operations, audit, and executive stakeholders, with visibility into privileged activity, policy enforcement, and risk exposure. JIT access is handled through time-bound elevation, temporary group membership, one-time-use tokens, ephemeral secrets, and automatic revocation, helping reduce standing privilege across both users and automation. Session management includes video recording, OCR-based indexing, command search, file transfer logging, real-time monitoring, and active intervention controls such as blocking or terminating sessions. Credentials, secrets, keys, and certificates are managed natively through centralized vaulting, rotation, distribution, versioning, and full auditability. EPM extends to Windows, macOS, Solaris, AIX, Red Hat, SUSE, Ubuntu, and CentOS Linux. Segura also embeds PUEBA and augments that further through Continuous Identification, which evaluates behavior during active sessions and can trigger adaptive controls, alerts, or session blocking when activity diverges from expected patterns. Segura is continuing to evolve toward deeper policy-as-code frameworks and more advanced CI/CD-native enforcement models.

Segura's recent product direction reflects a shift from traditional PAM toward a broader privileged identity platform, with increased emphasis on embedding intelligence into operational workflows. Segura Intelligence applies ML and GenAI to session analysis,

anomaly detection, policy recommendations, and remediation guidance. In Segura's CIEM module, GenAI is used to analyze attack paths and recommend remediation scripts, which gives administrators a more direct route from visibility to action. Another element worth noting is the introduction of post-quantum cryptography (PQC) support within the Network Connector, which establishes a secure communication channel between the platform and isolated environments using a hybrid cryptographic model. That remains uncommon in this market and suggests a forward-looking product strategy. Segura is a good fit for small and mid-sized organizations, as well as selected larger enterprises, that want broad PAM coverage, strong session control, and an offering that ties privileged access, secrets, certificates, and machine identities into a more unified operational model. However, some advanced features may exceed needs of smaller organizations.

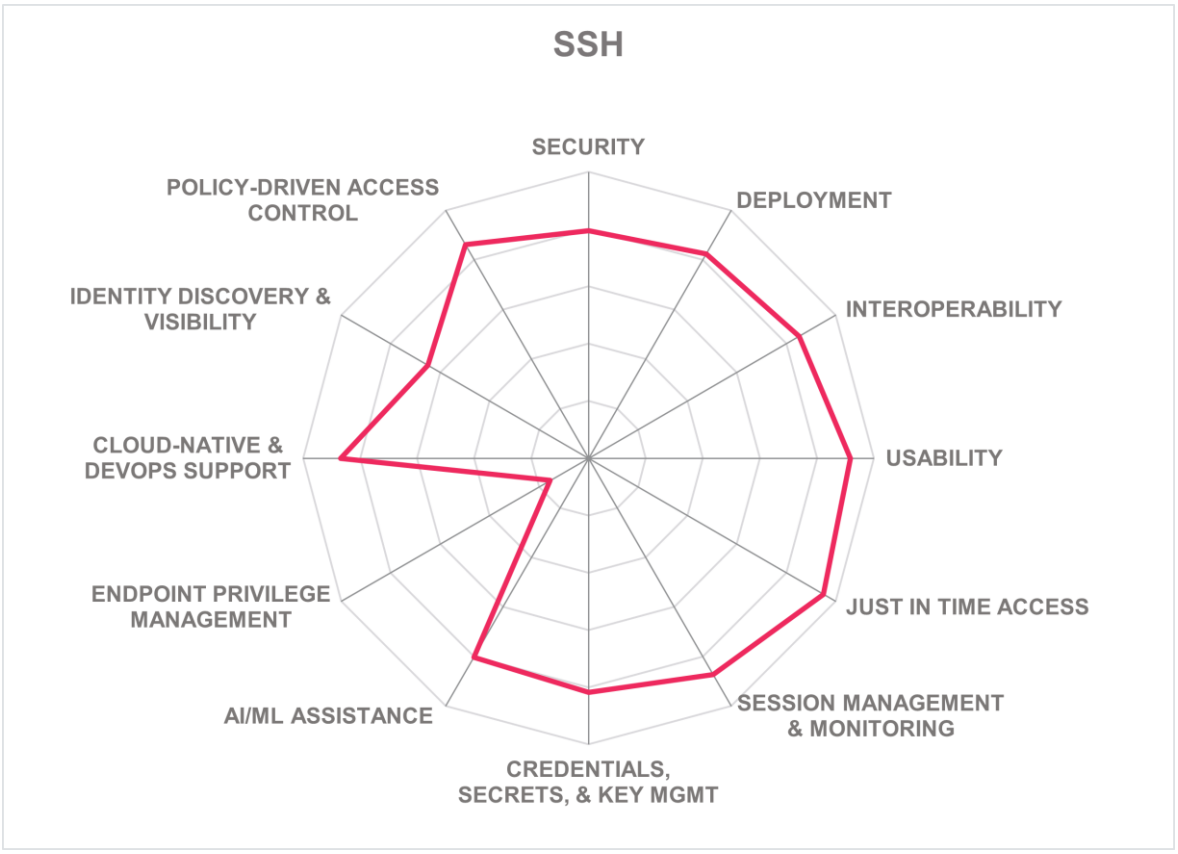
Strengths

- Integrated PAM, CIEM, CLM, and ITDR platform approach
- Comprehensive discovery across privileged human and machine identities
- Deep session monitoring and forensic audit capabilities
- Useful JIT access controls across multiple environments
- Agentless support for OT, ICS, and network systems
- Continuous Identification strengthens insider threat detection
- GenAI supports remediation and policy guidance
- PQC support is ahead of many competitors

Challenges

- Recent rebranding may cause market confusion
- Limited policy-as-code support for DevOps workflows
- Advanced features may exceed needs of smaller organizations
- Segura is continuing to evolve toward deeper native secret lifecycle automation tied directly to CI/CD pipeline events and ephemeral runtime workflows

SSH – PrivX



Leadership

Established in 1995 and headquartered in Helsinki, Finland, SSH is one of the longer-established vendors in this market and remains closely associated with secure access and SSH security. Its PAM offering is centered on PrivX, including its SSH key management and automation microservice. In 2025, Leonardo S.p.A became the company's largest shareholder, giving SSH added weight in sectors where sovereignty, defense, and critical infrastructure concerns shape technology decisions. PrivX is delivered through a wide set of models, including self-hosted deployments on physical or virtual infrastructure, public or private cloud deployments, SaaS through partners, virtual appliance options, and MSP-hosted services. The product supports automated deployment and maintenance through

Terraform, Ansible, APIs, and Kubernetes tooling. SSH supports FIPS 140-3 validated cryptographic modules and is ISO 27001 certified. Licensing costs are calculated per-user, per-period, per-node, and actor-plus-target models. The company mainly targets large organizations, while also addressing selected mid-market and smaller enterprise use cases.

PrivX provides role-based access control, passwordless ZSP, JIT access through ephemeral certificates for both human and NHIs. SSH's position is particularly strong in environments where SSH key sprawl has become a security and operational problem. PrivX can vault passwords and other secrets when needed, but its more distinctive value lies in managing, auditing, rotating, and gradually replacing SSH key-based access with certificate-based authentication. The product integrates with existing identity providers such as Microsoft Entra ID, Okta, and Google Workspace. It supports MFA and adds phishing-resistant assurance through the PrivX Authorizer mobile application, which continuously verifies user validity and device posture during sessions. For highly sensitive connections, SSH also brings quantum-safe cryptography into the PAM discussion in a way few vendors currently do.

Reporting is useful for access review and policy analysis, though detailed reporting on cloud permissions remains less developed. PrivX offers mature and customizable dashboards, along with built-in reports that map identities to the privileged resources they can reach. The platform integrates with existing IAM and IGA systems, supports SSO, and extends to broad cloud coverage across AWS, Microsoft Azure, GCP, Oracle, IBM Cloud, Alibaba Cloud, Salesforce, SAP, Nutanix, OpenStack, VMware, and others. Its support for JIT access is well developed: roles are calculated from identity sources at the moment of access and refreshed regularly, allowing privileges to change in line with policy, risk, and user state. Session management is another strong area, with monitoring and recording for SSH, RDP, HTTPS, FTP, SFTP, SCP, VNC, and X11, plus event-based recording and command-level indexing for activity search. Secrets and key management are also central capabilities. PrivX can vault secrets, discover accounts and hosts, and provide full life cycle management for SSH keys, though not for every credential type. ML-based analytics support abnormality detection, while GenAI is being used to improve usability, queries, policies, and configuration tasks. In addition, PrivX OT extends SSH's PAM capabilities into industrial environments by providing centralized, policy-driven access management for both modern and legacy ICS systems, supporting just-in-time and least-privilege access across IT and OT protocols while enabling secure remote operations, session monitoring, and regulatory alignment without relying on traditional VPN-based approaches.

Its agentless model, browser-based access, and certificate-based approach position the platform as a practical option for organizations seeking tighter control over privileged access. However, some limitations remain. Discovery is based on scheduled rather than continuous scans and the discovery component is not included in the base PAM license. There are also no EPM features. Even so, SSH presents a thoughtful PAM offering for organizations that want to move from vaulted credentials toward short-lived, policy-driven access with unusually strong SSH key governance and credible quantum-safe capabilities.

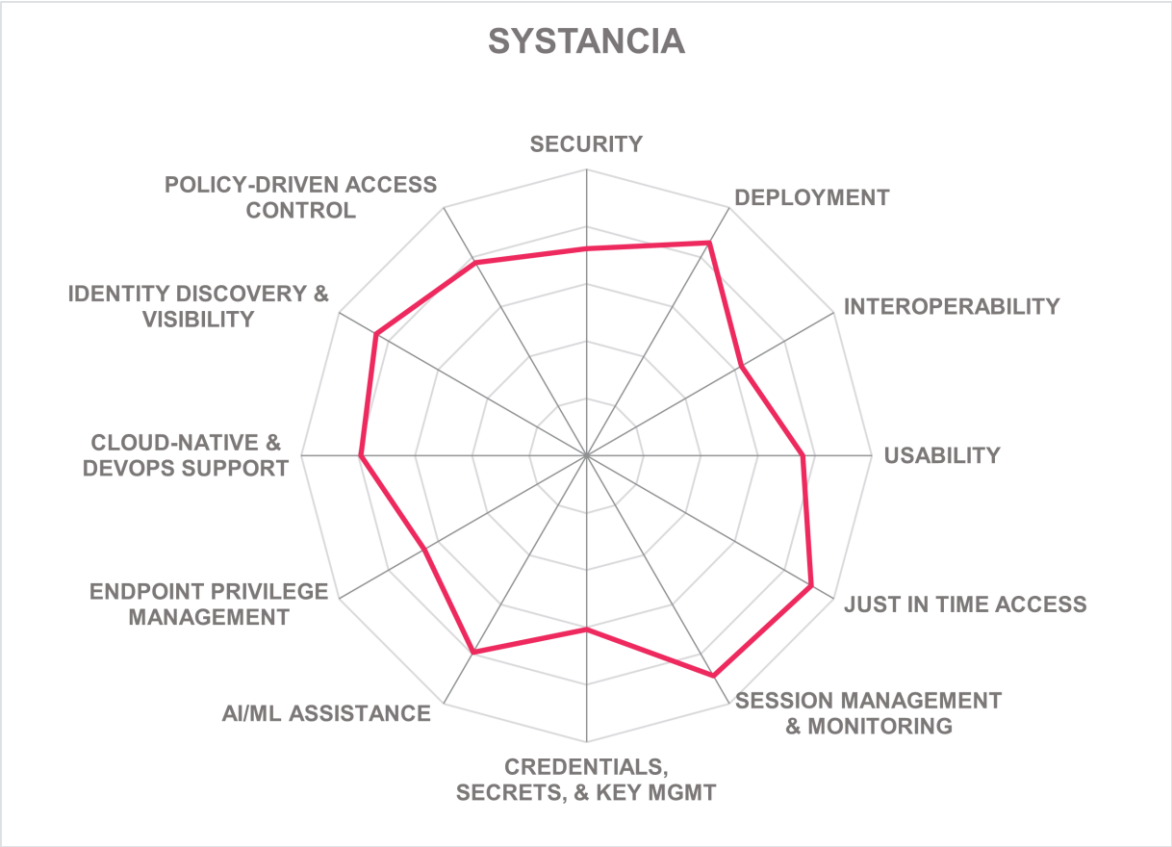
Strengths

- Robust passwordless ZSP model
- Advanced SSH key discovery and remediation
- Broad session monitoring and recording coverage
- Quantum-safe cryptography support
- Agentless access reduces operational friction
- Strong fit for sovereignty-sensitive deployments
- Good cloud and CI/CD integration breadth
- Offers detailed logs and real-time monitoring of all JIT provisioning events

Challenges

- No EPM coverage
- Discovery relies on scheduled scans, continuous scans not available
- Discovery tool not included in base license

Systancia – cyberelements



Systancia is a software vendor specializing in secure remote access and workspace solutions based in Sausheim, France. Founded in 1998 and originally focusing on Virtual Desktop Infrastructure (VDI), the company has expanded into IAM and Zero Trust Access solutions through later acquisitions and now positions cyberelements as a broader platform spanning IAM, Zero Trust Access, and PAM. The product is delivered both as SaaS and as self-hosted software, with support for public and private cloud, appliance and virtual appliance models, MSP-hosted delivery, and on-premises deployments. It also supports a server-side vault option for customers that want tighter control over secrets. Subscription pricing is based on active users rather than named accounts. Systancia also benefits from the European sovereignty discussion, and its support for SecNumCloud-aligned hosting expectations and ISO 27001 work in progress will matter to regulated EU customers. However, SOC 2 Type II attestation is still pending. The company primarily targets organizations across EMEA, from mid-sized businesses to larger enterprises.

cyberelements combines privileged session management, password and SSH key handling, clientless access, remote access, and IAM functions within a single platform. This allows Systancia to support use cases that move beyond conventional administrator access,

including third parties, business users, contractors, and external service providers. Resources are obscured from direct Internet exposure, connections are opened only when needed through volatile ports, and traffic between components can be encrypted with customer-held keys, limiting vendor visibility into data flows. Systancia also avoids exposing authentication secrets where possible through plugin-less web SSO injection with the vault on the server side. The solution integrates with IdPs, including Microsoft Entra ID and any SAML compatible provider.

Session management covers protocols such as SSH, RDP, Telnet, VNC, X11, SCP, FTP/SFTP, and others, with recording options including key logging, DVR, and application logging. Systancia adds AI-based analysis of recorded sessions through Lens, which scores both how closely a session matched its declared task and whether actions aligned with expected security practices. JIT access is supported through workflow-based policy enforcement and through ephemeral accounts created and removed around the session, particularly where PAM and IGA are used together. The platform also supports ephemeral secrets and short-lived credentials for human and NHIs. Coverage extends to major cloud platforms, OT/ICS environments, and network devices. Identity discovery enables automated discovery of machines, privileged accounts, user accounts, and SSH keys through integrated scanning and centralized visibility features. EPM capabilities for Windows and macOS add workstation integrity controls during privileged sessions, including restrictions on processes, file transfer, USB use, and local rights. However, EPM support for Linux is missing. The solution provides customizable dashboards with cross-account visibility and real-time alerting, alongside reporting and search capabilities that are particularly useful for investigations. Additionally, PUEBA is addressed through ML-driven analysis of user activity and session recordings, combining behavioral patterns, contextual signals, and task-based validation to produce risk scores that reflect both user intent and adherence to expected actions.

Systancia's use of ML for behavioral authentication, user-context analysis, and video-based risk scoring provide a point of differentiation, even if GenAI remains on the roadmap. Systancia appears especially well suited to organizations that want privileged access, remote access, and identity controls in one platform, with a preference for zero trust enforcement, EU sovereignty-aware deployment options, and strong support for third-party and operational access scenarios.

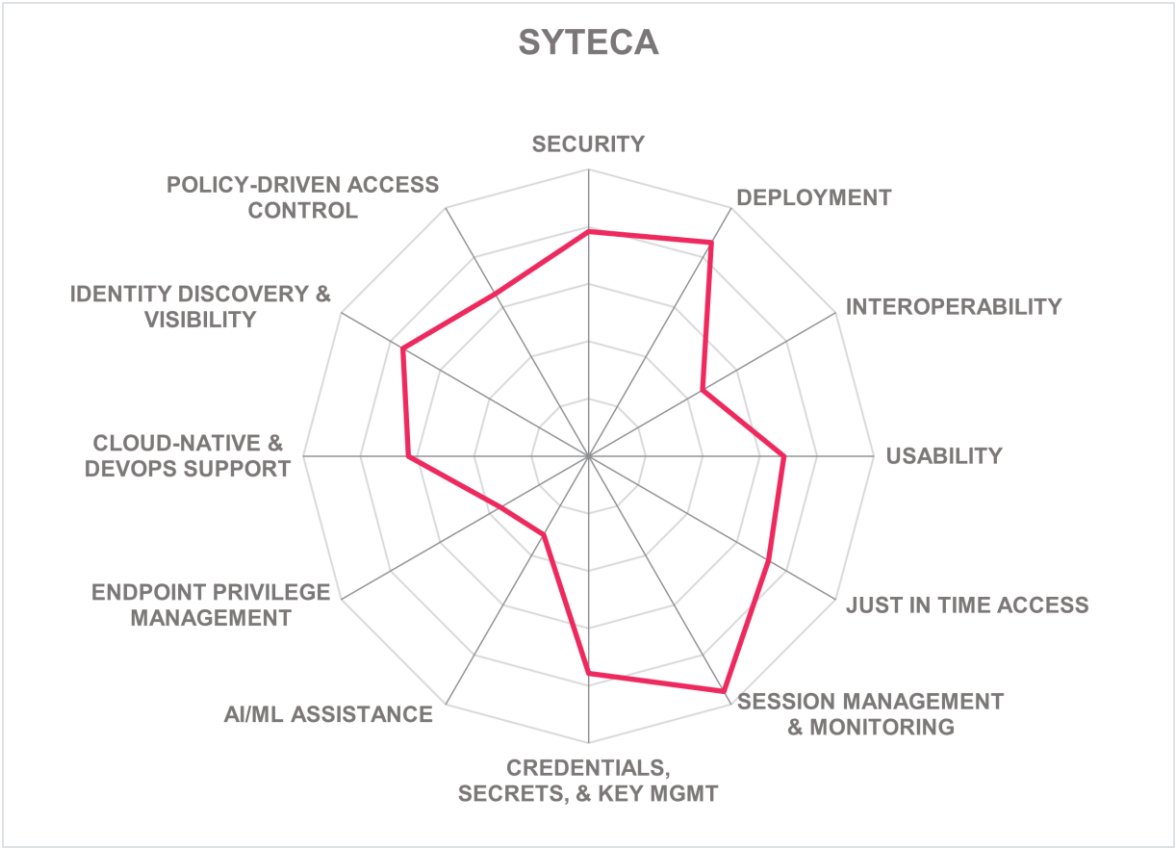
Strengths

- Good support for third-party privileged access
- PUEBA combines behavioral, contextual, and session-based risk scoring
- Support for contractors and external workforce scenarios
- AI-based session analysis adds useful context
- Broad support for cloud and OT environments
- European data privacy regulatory compliance alignment
- Use of ML for behavioral authentication, user-context analysis, and video-based risk scoring
- Consistent Zero Trust model applied to PAM, remote access, and IAM functions

Challenges

- Limited market visibility outside EMEA
- EPM support for Linux is not present
- GenAI capabilities are not yet available, but improvements are on the roadmap
- ISO 27001 certification and SOC 2 Type II attestation still in progress

Syteca – The Syteca Platform



Syteca, formerly Ekran System, was founded in 2013. The company is based in Needham, Massachusetts. Syteca's PAM solution combines privileged access control, session visibility, and built-in ITDR in a single product, with an emphasis on what happens after access is granted rather than ending control at authentication. Syteca supports a wide range of deployment models, including self-hosted on-premises, customer-controlled public and private cloud, fully hosted SaaS, MSP-hosted SaaS, appliance, and virtual appliance options. It does not run on a microservices architecture, but it supports high availability, disaster recovery, load balancing, and multitenant deployments. The platform is ISO 27001 certified, but SOC 2 Type II remains in progress. The licensing model is per user, per time period, per node, and per server. Syteca targets organizations of all sizes, particularly across EMEA and APAC, while expanding in North America and LATAM.

Syteca's ITDR capabilities extend detection and control directly into privileged sessions, using rule-based analysis to identify risky commands, abnormal behavior, and credential misuse. By correlating in-session actions with predefined policies and contextual signals, the platform can identify patterns associated with misuse, lateral movement, or unauthorized escalation. Privileged access is governed through role-based permissions, approval

workflows, MFA, endpoint verification, encrypted credential vaulting, and automated password rotation. JIT access reduces standing privilege, while credential injection and passwordless access patterns limit exposure of secrets to users. The platform provides deep discovery across Microsoft Active Directory and Entra ID, Okta, ForgeRock, and Keycloak. Automated response actions can be triggered based on detected behavior, while SIEM integrations allow events to flow to existing security infrastructure. API support includes REST and webhooks.

In addition, the platform provides real-time dashboards for privileged access monitoring with alert-driven drill-down capabilities, though customization options remain limited and there is no visualization of relationships between identities and resources. Reporting is supported through audit logs, forensic evidence export, and integration with external tools such as Microsoft Power BI. Cloud coverage includes AWS, Azure, GCP, Oracle Cloud, Alibaba Cloud, IBM Cloud, and VMware environments. The platform also supports privileged access management to network devices. Session management includes full session recording, live monitoring, indexed metadata, command capture, and searchable session activity across Windows, Linux, macOS, RDP, SSH, and browser-based sessions, including jump server scenarios. Sensitive data masking and pseudonymization enable privacy-aware monitoring. Syteca does not currently provide PUEBA, but it offers CI/CD pipeline integration via Syteca Application Credentials Broker (ACB), enabling automated secret retrieval and API-based management. EPM capabilities monitors privilege escalation against policies on endpoints.

Features such as the Web Connection Manager for agentless browser-based access, advanced Linux privileged session monitoring, and privacy-aware recording highlight additional capabilities in session control and access management. The platform embeds detection and response capabilities directly within privileged access controls and session monitoring, allowing security teams to identify and act on suspicious activity without relying on separate analytics layers or additional tooling. GenAI capabilities are limited, while current detection relies on rule-based analysis and predefined activity patterns. Syteca is well suited for organizations that prioritize session-level visibility, auditability, and control in their privileged access strategy.

Strengths

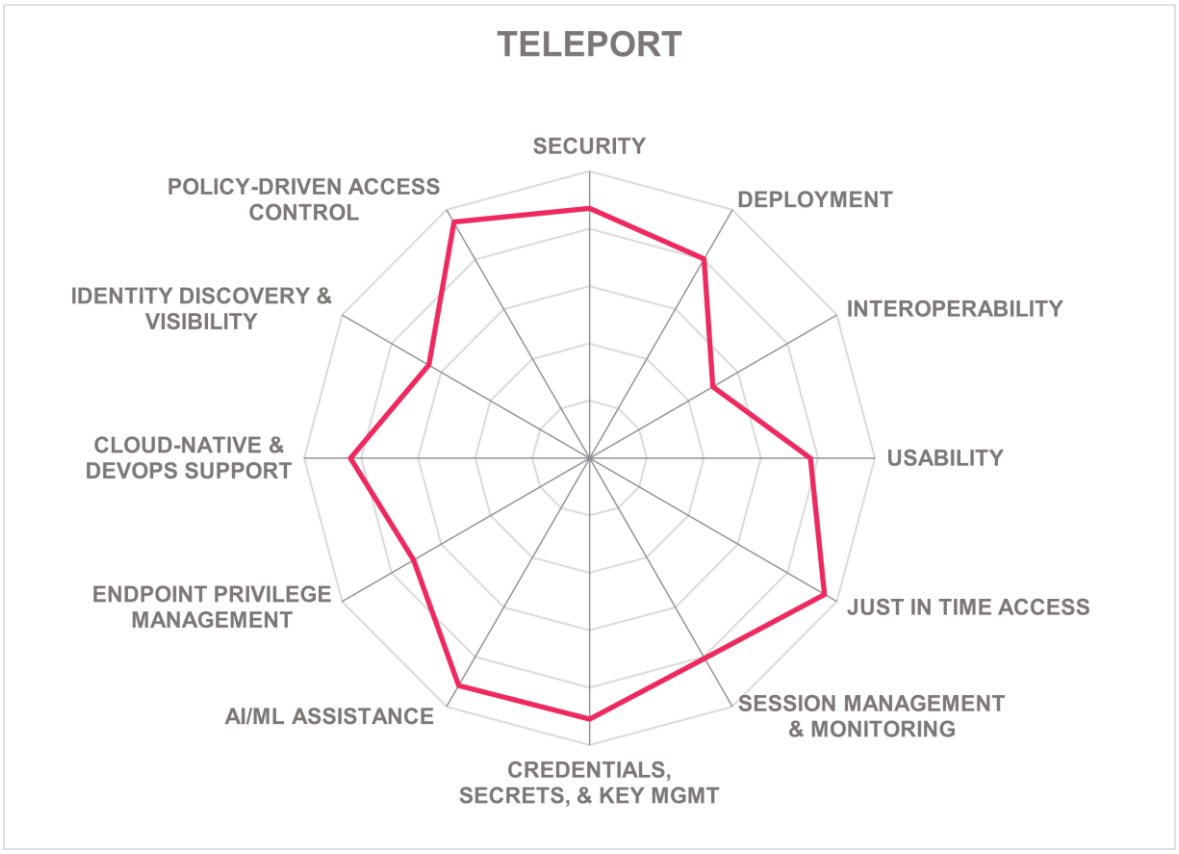
- ITDR-centric PAM approach enhances post-access visibility
- Provides extensive auditing features to track and manage user actions
- Granular session monitoring across multiple operating systems
- Web Connection Manager enables agentless browser-based access
- Sensitive data masking supports privacy-aware investigations
- Deep discovery of privileged and service account dependencies
- Advanced Linux privileged session monitoring capabilities

Challenges

- Limited dashboard customization options
- No CI/CD pipeline integration support
- Additional integrations with major IdPs would be useful

- Privilege elevation functionality not yet fully available
- No PUEBA capabilities
- GenAI capabilities are still maturing

Teleport – Teleport Infrastructure Identity Platform



Leadership

Founded in 2015 and headquartered in Oakland, California, Teleport is an AI infrastructure identity company focused on modernizing identity, access, and policy across infrastructure. Its Teleport Infrastructure Identity Platform brings access, governance, and identity security into a single control plane for servers, Kubernetes clusters, databases, Windows desktops, internal web applications, cloud consoles, Git repositories, and MCP servers. The platform is delivered through a wide range of models, including self-hosted deployments, managed SaaS, MSP-hosted services, and mixed deployments. Teleport uses FIPS 140-3 compliant modules. It is ISO 27001 certified and SOC 2 Type II attested. Licensing is based on monthly active users and protected resources. The company targets organizations of varying

size, with particular resonance among engineering-driven enterprises, regulated sectors, and firms operating distributed infrastructure and infrastructure at scale.

Teleport's central differentiator is that it replaces passwords, SSH keys, API tokens, and other long-lived secrets with short-lived X.509 certificates and JWTs tied to verified human, machine, workload, device, or agentic identity. The platform is centered on cryptographic identity, ZSP, and ephemeral access rather than credential storage and rotation as the primary control model. Device Trust adds hardware-bound verification, while MFA reinforce access decisions through WebAuthn-based authentication. Teleport's Machine ID capability extends this approach to CI/CD pipelines, microservices, and containers, including support for SPIFFE Verifiable Identity Document (SPIFFE/SVID)-based workload identity. In addition, the platform integrates broadly with enterprise IAM and access infrastructure, including Okta, Microsoft Entra, Google Workspace, GitHub, Active Directory, Auth0, and generic SAML and OIDC providers, as well as ChatOps and ITSM tools such as Slack, Teams, Jira, PagerDuty, ServiceNow, Mattermost, and Opsgenie.

Teleport supports public cloud platforms such as AWS, Azure, GCP, and Oracle, and it also provides monitored privileged access to OT/ICS systems. JIT access is implemented through temporary role or resource access requests, peer approval workflows, automatic approvals tied to operational context, and automatic expiration. For session management, Teleport covers SSH, Kubernetes, database, desktop, application, and LLM sessions with recording and playback, query-level visibility, and AI-assisted summaries, with live session viewing capabilities for SSH, Kubernetes, desktop, and database sessions. It also adds ML-based risk scoring, real-time activity views, access graph analysis, and behavioral signals such as impossible travel. Although access adjustments cannot be automatically triggered by changes in user behavior, invoked session termination will suspend sessions and privileges across all infrastructure. Teleport provides mature dashboarding and built-in reporting, including views that map relationships between identities and the systems or privileged resources they can reach. The graph can be explored dynamically by identity or resource, with the reporting model being useful for audits and access reviews. It does not have EPM capabilities.

Teleport is extending its infrastructure identity model to address emerging AI-related use cases. Capabilities such as Secure MCP, the Teleport Agentic Identity Framework, and AI Session Summaries reflect the incorporation of agentic systems into existing identity and access control models rather than treating them as a separate category. This aligns with a broader shift where organizations must manage not only privileged human access, but also automation, delegated actions, and machine-driven workflows. Teleport is particularly well suited to organizations that want to reduce credential sprawl, simplify privileged access across heterogeneous infrastructure, and move beyond a vault-centric view of PAM without giving up auditability or control.

Strengths

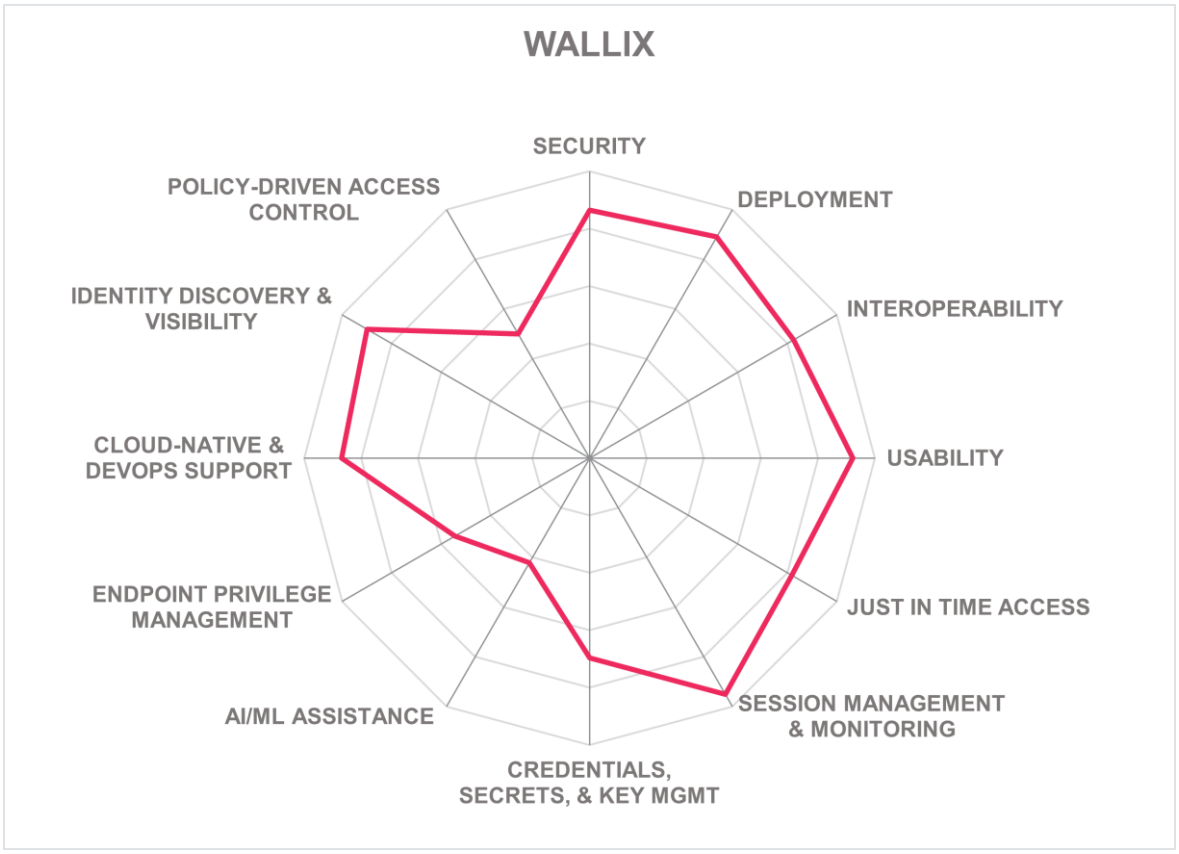
- Eliminates long-lived credentials with short-lived certificates
- Advanced JIT and ZSP model
- Broad support for Kubernetes, databases, and cloud consoles

- Machine ID fits CI/CD, workload, and agentic identity use cases
- Access Graph improves visibility into privileged pathways
- Secure MCP supports emerging AI access scenarios
- Agentic Identity Framework addresses delegated AI identity, Access, and Security
- AI Session Summaries reduce audit review effort
- Supports OT/ICS use cases

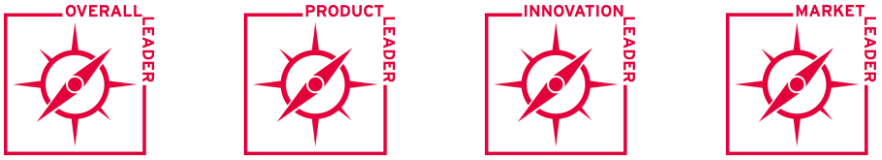
Challenges

- No traditional secrets vault for buyers expecting one
- EPM capabilities are not present
- Access adjustments cannot be automatically triggered by changes in user behavior; however, sessions and privileges can be terminated simultaneously across all infrastructure

WALLIX –WALLIX PAM and WALLIX One



Leadership



Founded in 2003 and headquartered in Paris, France, WALLIX has built its position in privileged access management from a European security perspective, with particular traction in regulated and operationally sensitive environments. The company's WALLIX PAM offering brings together WALLIX Bastion, Access Manager, Privilege Elevation and Delegation Management (PEDM), Web Session Manager, Application to Application Password Manager (AAPM), and related capabilities under an integrated suite. WALLIX One extends the portfolio with SaaS-delivered vaulting, remote access, managed PAM, and a centralized administration console. The platform is available through a wide set of deployment models, including self-hosted on premises, public and private cloud, appliance, virtual appliance, fully

hosted SaaS, MSP-hosted SaaS, and mixed deployment options. Licensing is offered as yearly subscription or perpetual, with metrics based on users or resources. WALLIX is ISO/IEC 27001:2022 certified and holds BSI BSZ (Beschleunigte Sicherheitszertifizierung) certification, awarded by the German Federal Office for Information Security (BSI) in September 2025 for its PAM solution (version 12.0.14). Under a mutual recognition agreement between BSI and ANSSI, this certification is recognized by the French National Agency for the Security of Information Systems (ANSSI) as equivalent to a CSPN (Certification de Sécurité de Premier Niveau) certificate. Its customer base spans organizations of all sizes across industries such as energy, transport, banking, manufacturing, government, and critical infrastructure.

WALLIX PAM is centered on controlled, auditable access to privileged accounts, systems, and sessions across IT and OT. WALLIX Bastion provides password vaulting, session brokering, recording, credential injection, approval-based access, and secret rotation through an agentless proxy architecture. The suite supports shared administrative accounts, privileged users, external contractors, service accounts, application credentials, and an expanding set of NHIs. The solution's newer Web Session Manager applies browser isolation functions to PAM, allowing secure access to web targets from standard browsers while preserving session control and recording. The Universal Tunneling with Seamless Connection supports complex access scenarios, including OT targets and fat-client applications, without requiring admin rights or workstation reconfiguration. It operates by routing sessions through the Bastion, which centrally manages protocols, credential injection, and session control while transparently handling multi-port and non-standard communications. It integrates with IdP such as Microsoft Entra ID, Okta, Wallix IDaaS, Ping Identity, Google Workspace, OneLogin, and more.

Dashboards are mature and usable, with drill-down for investigation, while reporting enables the building of custom entitlement queries and mapping of identities to systems, accounts, and privileged resources. For session management, RDP and SSH sessions are recorded for replay, transcript generation, with rich metadata. It can record TCP-based sessions, which enable monitoring of OT/ICS environments. WALLIX supports secure access to legacy OT systems using agentless methods such as jump servers and session brokers. Real-time alerts can flag unauthorized patterns, lateral movement, and specific process launches. Credential and secret management are also well developed, with centralized storage, automatic rotation, SSH key lifecycle handling, and more than 20 rotation plugins for common operating systems, directories, databases, firewalls, hypervisors, and infrastructure devices. JIT access is implemented through structured request and approval workflows tied to duration, ticketing, and justification, with support for machine-driven validation through ITSM tools such as ServiceNow. WALLIX also supports ephemeral SSH certificates and separate vaults for dedicated DevOps environments, though ephemeral access beyond SSH certificates remains limited. Discovery capabilities are present, but they can only be scheduled or triggered manually, rather than continuous. The solution does not provide PUEBA today, which narrows its analytical depth in comparison with vendors that already combine privileged control with behavioral privilege analytics. Cloud coverage includes major providers, but broader CIEM and some JIT use cases outside Azure rely on partner technology.

WALLIX's direction is increasingly shaped by centralized administration, broader secret management, and more contextual control over privileged access. WALLIX One Console gives administrators a single place to manage distributed deployments, reduce duplication, and push policy consistently across environments. The roadmap also points toward deeper analytics, ML and AI features, risk scoring, and more predictive access decisions. WALLIX is particularly relevant for organizations that need European assurance and OT support. The solution has a proven track record and could be a good alternative for enterprises, public sector bodies, and critical infrastructure operators who want controlled privileged access across IT and OT. This is especially true when sovereignty, auditability, and operational flexibility are as important as feature breadth.

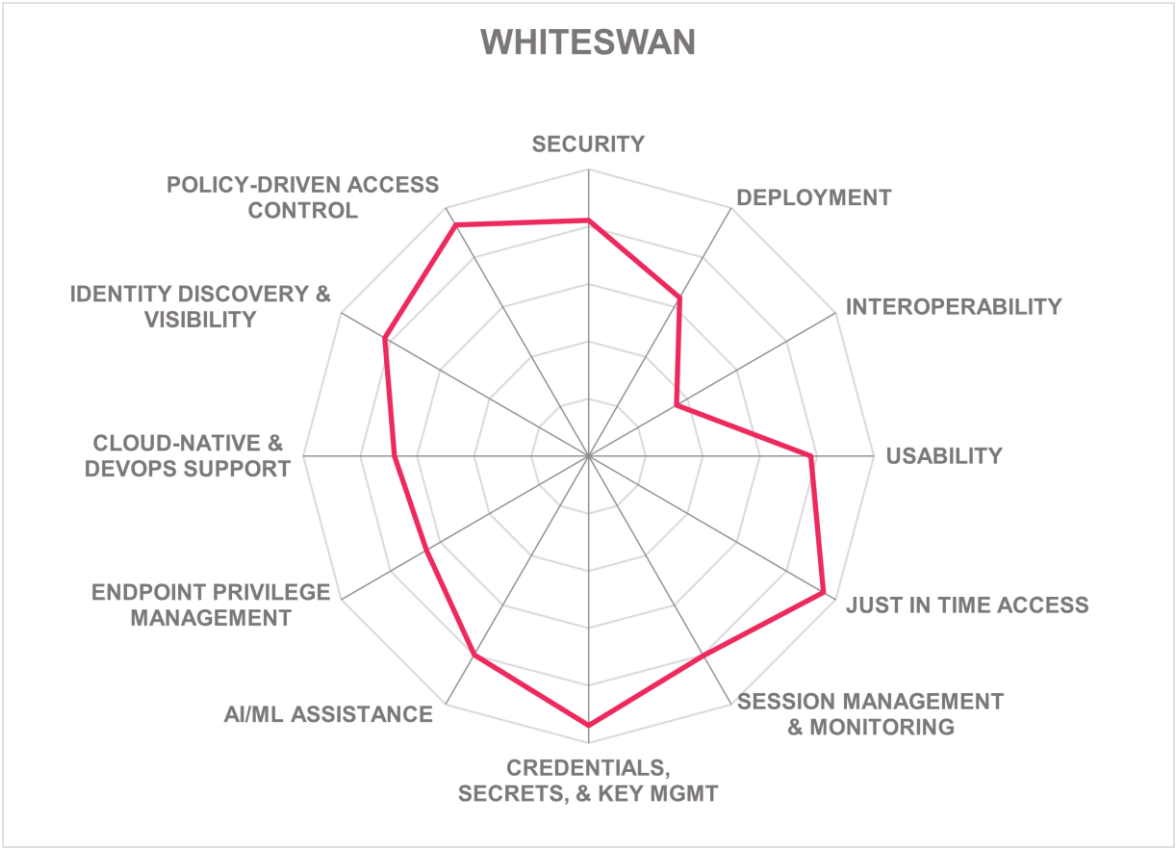
Strengths

- Agentless session management reduces deployment friction
- Extensive support for OT and industrial access scenarios
- Web Session Manager secures browser-based privileged access
- Universal Tunneling handles complex target connectivity
- Credential and secret management are well developed
- Extensive session recording, metadata, and alerting
- Deep alignment with European sovereignty requirements

Challenges

- Discovery is scheduled or manual, not continuous
- Advanced AI and ML capabilities remain largely roadmap items
- Broader CIEM coverage requires partner technology
- No PUEBA capabilities available today
- Ephemeral access support remains limited to SSH certificates

Whiteswan – Whiteswan Identity Security Platform



Whiteswan, established in 2023 and headquartered in San Mateo, California, US, delivers the Whiteswan Identity Security Platform, a PAM offering that has expanded quickly from endpoint controls into a broader privilege and identity security platform. The company targets mid-market and medium-sized organizations, with its strongest presence in APAC and growing traction in North America and EMEA. The platform is available through a wide range of deployment models, including self-hosted software, appliance and virtual appliance options, and vault deployments spanning public and private environments. Whiteswan hosts it as SaaS, and some MSPs use it also. Licensing is primarily per user per year, while endpoint PAM is priced per device. Whiteswan has not yet obtained SOC 2 Type II, ISO 27001, or other certifications yet.

Whiteswan's value proposition rests on a ZSP model that combines JIT access, ITDR, and session control across human and NHIs. The platform supports privileged access for endpoints, servers, Active Directory, cloud resources, SaaS applications, CI/CD workflows, service accounts, and other machine identities. Their mesh-based trusted access model removes the need for traditional jump boxes while still allowing organizations to control and monitor SSH, RDP, and SaaS access, by establishing direct, encrypted connections

between users and target systems through distributed agents rather than routing traffic through a central intermediary. For secrets management, Whiteswan uses OpenBao as the backend for a full vault that supports secret storage, scoped access, visibility into usage, and automated rotation triggered by time, events, policy, or risk. It also issues ephemeral credentials and tokens for both human and NHIs. It integrates with IdPs such as Microsoft Active Directory and Entra ID, Okta, OneLogin, Ping Identity, and Google Workspace. The platform supports REST APIs and webhooks for integration.

The solution provides customizable dashboards with real-time threat visibility, including cross-account access views and identification of overpermissioned entities, and audit reports for compliance are available. Whiteswan integrates with GitLab and GitHub and extends privileged controls into CI/CD workflows by applying policy-based privilege escalation and JIT access for automated processes, though it does not support policy-as-code. Its cloud coverage includes AWS, Azure, GCP, Oracle, and OVH Cloud, and it also supports OT/ICS, and network devices. Discovery capabilities include continuous scanning, detailed identification of shadow accounts and privileged users in Linux environments, and network-wide visibility through a built-in scanning tool. Session monitoring spans Windows and Linux environments, with recording for SSH, RDP, Telnet, VNC, and related protocols and the ability to terminate sessions or block commands in real time. However, there is limited full-text search across session recordings. Privilege elevation and delegation are supported across Windows and Linux systems, though the platform does not extend to kernel-level or system service-level interception of privileged actions. The platform also incorporates PUEBA to identify shadow administrators, track service account activity, and detect behavioral anomalies in Active Directory environments.

A distinguishing feature of Whiteswan is the way it brings PAM and ITDR together rather than treating them as separate products. Its Active Directory, endpoint, and cloud threat detection components work with native enforcement controls, while ML detection models find suspicious activity. That design can reduce turnaround time for detection and response and reflects a more integrated approach to privilege security. The platform also uses GenAI to assist with policy creation and query generation. Whiteswan adds further differentiation through quantum-safe cryptography and RPA-based vision agents for enrolling SaaS portals and injecting passwords. Overall, Whiteswan appears best suited to mid-market organizations seeking a unified PAM platform with strong JIT controls, broad identity coverage, and tighter linkage between visibility and enforcement.

Strengths

- ZSP design across multiple environments
- Broad coverage for human and NHIs
- Multi-cloud JIT access capabilities
- Entitlement discovery and removal of over-privileges
- Integrated PAM and ITDR solution
- Real-time session monitoring and command control
- Customizable dashboards and ready-made reports
- ML detection improves response speed

Challenges

- Small vendor with a small partner ecosystem compared to competitors
- No major security certifications yet
- Limited full-text search across session recordings
- No kernel-level privileged action interception
- Mid-market focus may limit large enterprise reach

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless offer a significant contribution to the market space.

Admin By Request

Admin By Request was founded in 2017. While the company has a primary US office in San Francisco, it was founded and maintains its main development headquarters in Denmark. The company provides a combined EPM and PAM solution focused on removing standing administrative rights and enabling controlled privilege elevation. Its platform emphasizes simplicity, offering features such as JIT privilege access, application control, and secure remote access in a lightweight deployment model.

Why worth watching: The vendor targets the underserved mid-market with a low-complexity approach to privilege management, which contrasts with more traditional, heavier PAM platforms. Its focus on usability and rapid deployment aligns with growing demand for pragmatic PAM adoption.

HashiCorp (IBM)

Founded in 2012 and headquartered in San Francisco, US, HashiCorp develops infrastructure automation and security tools for multi-cloud environments, with HashiCorp Vault serving as its core secrets management and machine identity protection solution. Vault enables organizations to secure, store, and control access to credentials, tokens, and encryption keys across dynamic, cloud-native environments.

Why worth watching: Its strong position in DevOps and cloud-native ecosystems makes it highly relevant as PAM expands toward secrets management and machine identities. Integration into IBM may further extend its enterprise reach and influence in hybrid cloud security architectures.

Netwrix

Founded in 2006 and headquartered in Frisco, Texas, US, Netwrix offers Privilege Secure, a PAM solution focused on eliminating standing privileges through JIT access and enforcing least privilege across IT environments. The platform includes session monitoring and behavioral controls to reduce lateral movement and mitigate ransomware risks.

Why worth watching: Netwrix is evolving from a governance and audit-focused vendor into a broader identity security provider, with PAM as a central pillar. Its pragmatic, risk-reduction-focused approach may resonate with organizations seeking faster time-to-value.

OpenText (including Micro Focus portfolio)

Founded in 1995 and based in Waterloo, Ontario, Canada, OpenText provides a broad enterprise software portfolio spanning information management, cybersecurity, and cloud services, including PAM capabilities inherited from the Micro Focus acquisition. Its PAM offerings are typically part of a wider identity and security stack designed for large, complex enterprise environments.

Why worth watching: The combination of legacy Micro Focus capabilities with OpenText's broader platform strategy could reshape its positioning in IAM and PAM. Its scale and installed base provide an opportunity to embed PAM into larger security and governance initiatives.

P0 Security

P0 Security provides an identity-centric platform that combines PAM, identity governance, and cloud entitlement management capabilities. The platform focuses on managing privileged access for human, non-human, and AI identities across hybrid and cloud environments through just-in-time access controls and continuous visibility into permissions and entitlements.

Why worth watching: P0 Security reflects the broader market shift toward converged identity security platforms and ZSP models. Its focus on API-driven orchestration and securing non-human and AI identities aligns with emerging enterprise requirements in cloud-native environments.

SailPoint

Founded in 2005 and based in Austin, Texas, US, SailPoint is a leading provider of IGA and cloud identity security, with capabilities that extend into managing privileged access through entitlement governance and JIT access controls. Its platform provides visibility and policy enforcement across cloud infrastructure and SaaS environments.

Why worth watching: As PAM increasingly converges with identity governance and CIEM, SailPoint is well positioned to influence this intersection. Its AI-driven analytics and strong governance foundation may appeal to organizations prioritizing identity-centric security models.

Silverfort

Silverfort, founded in 2016 and headquartered in Tel Aviv, Israel, delivers a privilege access security approach that operates at the authentication layer, enabling discovery, enforcement of least privilege, and JIT access without relying on traditional vault-based architectures. It extends protection to users, service accounts, and other NHIs across hybrid environments.

Why worth watching: Its "vaultless" approach challenges traditional PAM architectures and addresses gaps in coverage, particularly for non-human and distributed identities. This

architectural shift aligns with evolving enterprise environments and may drive disruption in the PAM market.

Soffid

Based in Spain and established in 2013, Soffid provides an open-source-based IAM platform that integrates IGA, access management, and PAM capabilities into a single converged solution. Its PAM functionality supports the management of both human and non-human privileged accounts, with a focus on visibility, control, and compliance.

Why worth watching: Its open-source roots and integrated platform approach differentiate it from more siloed vendors. Strong traction in EMEA and LATAM suggests potential for broader expansion, particularly among organizations seeking flexible and cost-effective IAM solutions.

Related Research

Leadership Compass: Access Management
Leadership Compass: Cloud Infrastructure & Entitlement Management (CIEM)
Leadership Compass: Identity Threat Detection and Response (ITDR)
Leadership Compass: Non-Human Identity Management
Research Compass: Identity and Access Management 2026
Advisory Note: NHI and CIEM: Beyond Point Solutions towards Strategy
Whitepaper: The Role of Identity Fabrics in Modern IAM
Whitepaper: Navigating the Future of Authentication in the Age of AI and Deepfakes
Buyer's Compass: Cloud Infrastructure Entitlement Management (CIEM)
Buyer's Compass: Privileged Access Management (PAM)

Copyright

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com..