Magic Quadrant for Privileged Access Management

13 October 2025 - ID G00823931 - 61 min read

By Abhyuday Data, Paul Mezzera, and 3 more

The PAM market is evolving to meet the demands of managing privileged access for machines, cloud environments and, at the same time, securing traditional privileged access risks. IAM leaders should focus on the features that differentiate vendors in this market.

Market Definition/Description

Gartner defines privileged access management (PAM) as tools that provide an elevated level of technical access through the management and protection of accounts, credentials and commands, which are used to administer or configure systems and applications. PAM tools — available as software, SaaS or hardware appliances — manage privileged access for both people (system administrators and others) and machines (systems or applications). Gartner defines five distinct tool categories for PAM tools: privileged account and session management (PASM), privilege elevation and delegation management (PEDM), secrets management, cloud infrastructure entitlement management (CIEM) and remote PAM (RPAM).

Privileged access is access beyond the normal level granted to both human and machine accounts. It allows users to override existing access controls, change security configurations, or make changes affecting multiple users or systems. As privileged access can create, modify and delete IT infrastructure, along with company data contained in that infrastructure, it presents catastrophic risk. Managing privileged access is thus a critical security function for every organization and requires a specific set of procedures and tools. PAM tools focus on either privileged accounts or privileged commands.

PAM tools help organizations discover and onboard privileged accounts used by humans and machines. PAM tools secure these accounts by rotating and vaulting their credentials (e.g., passwords, keys), and brokering delegated access to them in a controlled manner. For interactive accounts used by people, PAM tools help provide multifactor authentication and explicit trust remote access through session control mechanisms to enable privileged account use without revealing credentials. For noninteractive accounts used by machines, PAM tools secure the handling of privileged credentials so that they are not exposed at rest.

PAM tools also provide command control by allowing only specific actions to be executed, and can optionally elevate a user's privileges temporarily to allow the execution of commands in a privileged context.

PAM tools offer visibility and control over the usage of privileged accounts and commands by tracking and recording privileged access for auditing purposes. This includes detailed session recording to help understand not only who used which privileged account and when, but also what they were doing. The controls provided by PAM tools can implement just-in-time privilege management to enforce the principle of least privilege — users must have the right level of access to the right resource for the right reason, at the right time.

Mandatory Features

The mandatory features for PAM are:

- Centralized management and enforcement of privileged access by controlling either access to privileged accounts and credentials or execution of privileged commands (or both)
- Managing and brokering privileged access to authorized human users (e.g., system administrators, operators and help desk staff) and authorized machines (e.g., systems, applications, workloads etc.) on a temporary basis
- Account discovery and onboarding of privileged accounts across multiple systems, applications and cloud infrastructure providers
- Vaulting, rotation and management of privileged credentials
- Management, monitoring, recording and auditing for privileged sessions, including remote privileged sessions

- Role-based administration, including centralized policy management for controlling access to credentials and privileged actions, when applicable
- Just-in-time privilege management, which reduces the time and scope for which a user is granted privileged access

Common Features

Common features for PAM include:

- Agent-based controlled privilege elevation for commands executed on Windows, UNIX/Linux or macOS operating systems.
- Secrets management for workloads including applications, services, containers, scripts and VMs.
- Privileged account life cycle management for humans and machines.
- Cloud infrastructure entitlement management (CIEM).
- Identity administration including federation and authorization capabilities to secure remote privileged access for third-party external IT staff, including vendors, service providers and other external users that require technical access.
- Automating multistep, repetitive and routine tasks related to privileged operations that are orchestrated and/or executed over a range of systems, while providing guardrails by checking against defined policies and settings.
- Zero standing privileges (ZSP) where users are not elevated to a preexisting privileged account or privileged role as a just-in-time (JIT) approach, but rather net-new permissions and roles are created when a privileged user needs access. Those permissions are then deleted after a time-bound session.
- Analyzing privilege patterns, misconfigurations, access behaviors, and anomalies for privileged threat detection and response.

Magic Quadrant

Figure 1: Magic Quadrant for Privileged Access Management

Gartner

Vendor Strengths and Cautions

ARCON

ARCON is a Challenger in this Magic Quadrant. Its PAM offering consists of ARCON PAM Enterprise for privileged account and session management (PASM), and ARCON EPM for privileged elevation and delegation management (PEDM). Both are available as software and SaaS. ARCON offers several additional PAM products and modules, including remote privileged access management (RPAM), secrets management, cloud infrastructure entitlement management (CIEM) and connectors to DevOps infrastructure tools.

ARCON has a strong presence in Asia/Pacific and EMEA, although it considerably increased its customer base in North America last year. Recent roadmap updates include AI-driven policy recommendations for improved operational efficiency, enhanced support for operational technology (OT) and cyber-physical system (CPS) use cases, and expanding PAM for machines capabilities.

Strengths

- **Product:** ARCON's offering is among the most capable of all those evaluated, with every capability evaluated as good — and often excellent. It is also a top performer for two core features: privileged credential management and CIEM.
- **Customer experience:** ARCON excels in support services, offering three levels of support and providing a dedicated technical account manager and customer success manager for all support levels at no additional cost.
- **Pricing:** Even though ARCON increased its pricing last year, it is still competitive. In most pricing scenarios — especially for PASM — ARCON's offerings are more affordable than those of other vendors in this research. In PEDM and secrets management scenarios, pricing is around average and sometimes higher than average, especially for its software offering.
- **Innovation:** With the introduction of ARCON.ai, ARCON can review privileged sessions, analyze abnormal activities and generate actionable summaries.

Cautions

- **Product:** ARCON provides limited out-of-the-box preconfigured integration with IT service management (ITSM) tools and identity governance and administration (IGA) tools, compared with other vendors in this research.
- **Market understanding:** ARCON does not offer support for a customer advisory board, which Gartner believes is critical for obtaining timely and honest customer feedback.
- **Operations:** ARCON lacks regulatory certifications that are common among other vendors in this Magic Quadrant, such as FedRAMP and FIPS.
- **Geographical strategy:** ARCON has a limited presence in the Americas and Europe, including limited channel partner support, compared with other PAM vendors.

BeyondTrust

BeyondTrust is a Leader in this Magic Quadrant. Its PAM offering consists of the Total PASM product, which bundles together Password Safe (PS) for PASM, Privileged Remote Access (PRA) for RPAM, and workload identity and secrets management. PS and PRA are also sold separately, with each available as SaaS, software and appliance (hardware or virtual). PEDM functionality is provided by Endpoint Privilege Management products for UNIX/Linux, macOS and Windows, which are available as software and SaaS. Last year, BeyondTrust also introduced a consolidated platform-based offering, called Pathfinder.

BeyondTrust's customer base is geographically diverse, with significant concentrations in North America and Europe. Recent roadmap updates include PAM controls for agentic-AI-based identities and a unified command line interface (CLI) for the Pathfinder platform to improve developer experience and security.

Strengths

- **Product:** BeyondTrust continues to offer some of the strongest capabilities for RPAM and JIT PAM. It is also a top performer for CIEM capabilities evaluated in this research.
- **Pricing:** Last year, BeyondTrust launched Essentials, Plus and Flex bundles within its Pathfinder platform, resulting in SaaS pricing below market averages for several scenarios. However, its overall software pricing remains above the market average.
- **Sales strategy:** BeyondTrust leverages a strong global channel partner network and strategic initiatives — including multiyear discounts, competitive upgrade programs, complementary assessments, and effective cross-selling of its Pathfinder platform — to enhance market reach and drive sales growth.
- **Market understanding:** BeyondTrust engages with its customers in a variety of ways, including support for both customer and partner advisory boards, which Gartner believes are critical for timely and honest customer feedback. The company also offers several levels of training, including some unpaid and paid training.

Cautions

- **Product:** BeyondTrust continues to lack maturity for workload identity and secrets management capabilities. Most authentication methods evaluated are roadmapped and there is no support for managing third-party secrets managers.

- **Innovation:** BeyondTrust's technical innovations since the last Magic Quadrant release are limited to foundational platform unification and integration efforts. Moreover, it lags behind other Leaders in offering GenAI approaches for analyzing session recordings.
- **Technical support:** BeyondTrust only offers one level of support for its customers, which has been identified as an area for improvement based on customer feedback.
- **Customer experience:** While BeyondTrust scores well for customer experience, many Gartner clients indicate that the initial setup and configuration of its software products is often complex and time-consuming, compared with other vendors. User interface and navigation have also been identified as areas for improvement based on customer feedback.

CyberArk

CyberArk is a Leader in this Magic Quadrant. It offers PASM functionality with Privilege Cloud, available as SaaS, and PAM Self-Hosted, which is available as software. CyberArk offers PEDM functionality with its Endpoint Privilege Manager for Windows, Linux and macOS (SaaS), and its On-Demand Privileges Manager (OPM) for AIX and Solaris (software). PAM for machines functionality is offered through Conjur (SaaS or software), Secrets Hub (SaaS) and Venafi (acquired in October 2024), which provides certificate life cycle management and SSH key management for machines (specifically workloads). CyberArk also offers Vendor Privileged Access Manager (SaaS) for RPAM and Secure Cloud Access (SaaS) for JIT access to cloud resources.

CyberArk's operations and customer base are geographically diversified across the globe. Recent roadmap updates include addressing AI agent threats, securing machine identities and expanding discovery capabilities.

As of July 2025, Palo Alto Networks has agreed to acquire CyberArk.

Strengths

- **Product:** CyberArk is best in class for workload identity and secrets management and Windows PEDM capabilities. It is also mature and highly capable across the various other product capabilities evaluated.
- **Innovation:** CyberArk has introduced CORA AI, which offers capabilities such as session summaries, secret anomaly detection, policy recommendations and rule suggestions, along with improvements to its secrets management capabilities.

- **Market understanding:** Besides leaning on customer surveys, CyberArk supports a customer advisory board, as well as research and innovation labs that include red team and threat researchers.
- **Geographical and vertical strategy:** CyberArk's ongoing regional investments and localized delivery capabilities support its ability to serve organizations in different geographic and cultural contexts. Moreover, CyberArk's broad customer base and strong partnerships support its growth, especially as it expands offerings for highly regulated sectors like public and financial service.

Cautions

- **Product:** While CyberArk supports privilege elevation for UNIX and Linux, it requires a different product for each and lacks feature parity between the two.
- **Pricing:** A common complaint that Gartner hears from clients is about cost — CyberArk's products are among the most expensive on the PAM market — and the company still does not offer additional discounts for customers that opt for a multiyear deal over a one-year deal.
- **Sales execution:** Following Palo Alto Networks' acquisition of CyberArk, changes in branding, sales channels, and go-to-market messaging may result in confusion for both existing and prospective clients. Uncertainty about the level/extent of integration with Palo Alto's existing security offerings may also introduce new complexity.
- **Customer experience:** Gartner clients identify customer support, initial setup complexities and upgrades for PAM Self-Hosted as areas in which CyberArk could improve.

Delinea

Delinea is a Leader in this Magic Quadrant. Its PAM offering consists of the Delinea Platform product, available as SaaS, which includes PASM, PEDM, RPAM and PAM for machines functionality bundled together. Stand-alone options include Secret Server for PASM (SaaS or software), PEDM with Privilege Manager (SaaS or software, Windows and macOS desktops), Server Suite (UNIX/Linux and windows servers), and DevOps Secrets Vault for workload identity and secrets management (SaaS).

Delinea's operations are geographically diversified, although most of its clients are in North America, followed by Europe. Recent roadmap updates include multicloud credential governance, expanding PAM for machines capabilities, OT/CPS enhancements such as unified IT/OT access governance, and the addition of VNC support for RPAM to, in turn, support GUI Linux interfaces.

Strengths

- **Product:** Delinea continues to be one of the top performers for UNIX/Linux PEDM. It also offers strong capabilities for workload identity and secrets management, CIEM and privileged credential management.
- **Technical support:** Delinea offers four different levels of support and paid training. It also offers a well-sought-out strategy for incorporating customer feedback via customer surveys and through the support of a customer advisory board.
- **Customer experience:** Delinea's customers consistently commend the user-friendly nature of its products. It offers unified engines and connectors to a single management plane and comprehensive coverage on health reporting.
- **Innovation:** Delinea has introduced a runtime AI authorization agent that can use identity and risk context to automate and enable policy-driven access decision making for cloud environments — a feature that differentiates it from other vendors in this research.

Cautions

- **Product:** Delinea continues to have less mature capabilities to address requirements for RPAM, compared with other vendors in this Magic Quadrant. It currently lacks advanced features like self-service registration and multiuser collaboration, and the ability to create on-demand, one-time access tokens that can be sent to an external identity to join remote privileged sessions.
- **Pricing:** Delinea's pricing for a series of scenarios evaluated in this research is uneven. Its pricing for small and midsize scenarios is below the market average, while its pricing for large-size scenarios is above the market average. Delinea's PEDM pricing is one of the highest in this evaluation.
- **Product strategy:** Several product requirements around privileged credential management and account discovery still need customization through Microsoft PowerShell, which places an additional burden on Delinea customers.

- **Overall viability:** Delinea's revenue growth rate has slowed down from the previous year. In addition, growth in sales and marketing investments has also moderated.

Keeper Security

Keeper Security (Keeper) is a Niche Player in this Magic Quadrant. Its PAM offering consists of KeeperPAM for PASM and RPAM, Keeper Secrets Manager (KSM) for PAM for machines, and Endpoint Privilege Manager for PEDM. All of these products are either available as software or SaaS. The company also offers Keeper Security Government Cloud (KSGC) — a FedRAMP- and StateRAMP-authorized product for public sector entities.

Keeper's operations are mostly focused in North America and Europe. Recent roadmap updates have been limited, with enhancements to database privileged access being the main addition.

Strengths

- **Product:** Workload identity and secrets management capabilities are key strengths in Keeper's PAM offering. It offers comprehensive support for visibility into, and synchronizations with, all major cloud service providers, as well as integration with Oracle Key Vault.
- **Technical support:** Keeper offers four different levels of support to choose from and, somewhat uniquely, includes training costs for each support level. Keeper leverages customer feedback surveys, but has not yet developed a customer advisory board.
- **Innovation:** Keeper has introduced agentic AI approaches to analyze recorded sessions and provide actionable summaries, but the functionality is only available for SSH.
- **Market responsiveness:** Keeper has been responding positively to market dynamics. Examples of this include its browser-based PAM capabilities and its ability to respond to regulations such as FedRAMP, FIPS and SOC 2.

Cautions

- **Product:** Apart from workload identity, secrets management and remote access, Keeper's offering underperforms in most other evaluated technical capabilities, and is especially weak in privileged account discovery and privileged credential management.
- **Product strategy:** Keeper Security's recent roadmap items are mostly focused on tactical improvements, with no new differentiating functionality compared with other vendors

evaluated. Moreover, Keeper's SaaS offering is not available for hosting in Latin America, the Middle East and Africa.

- **Pricing:** Keeper's pricing for a series of scenarios evaluated in this research is higher than the market average.

- **Sales strategy:** Keeper benefits from established channel partner support in North America and Europe; however, its presence in other regions remains nascent. Additionally, its sales strategies are relatively generic and lack the robustness seen in competitors, which may limit its effectiveness in driving growth outside its core markets.

ManageEngine

ManageEngine is a Challenger in this Magic Quadrant. ManageEngine is a division of Zoho Corporation, which offers a number of enterprise management software tools, including ManageEngine's PAM product, PAM360. PAM360 offers PASM, PEDM and some PAM for machines functionality bundled together as software-only. It also offers Application Control Plus, available as software, for endpoint privilege management and application control functionality.

ManageEngine's operations are geographically diverse. Recent roadmap updates include a new SaaS PAM offering, privileged access management for AI agents, and enhanced threat analytics.

Strengths

- **Product:** ManageEngine offers an effective PAM "break glass" functionality, making privileged passwords available through an encrypted HTML file approach, which can be stored locally or pushed automatically to Dropbox, Box and S3 buckets using its offline access/cloud integration function.

- **Technical support:** ManageEngine offers three different levels of support to choose from, as well as both free and paid training options. It leverages customer feedback surveys, but has not yet developed a customer advisory board.

- **Pricing:** ManageEngine pricing is consistently less than the market average. It offers a distinctive pricing model based on the number of PAM tool administrators (and not the number of privileged users who perform administrative tasks on the target systems).

- **Innovation:** ManageEngine has added a task automation module to orchestrate privileged access workflows, a new dashboard for security and health status reporting, and OpenAI

integration to automatically generate summaries of recorded SSH sessions.

Cautions

- **Product:** PAM360 cannot block recording of passwords in the recorded connections, thereby not offering any approach to avoid logging passwords in a session log. Moreover, its RPAM capabilities are fairly immature relative to those of other vendors in this research.
- **Operations:** ManageEngine lacks certifications that are common among the leading vendors in this Magic Quadrant, such as FedRAMP, FIPS and Common Criteria standards.
- **Product strategy:** ManageEngine's roadmap does not address long-standing product gaps compared with the market. PAM360 still has poor scores for JIT privileged access, workload identity and secrets management, privileged life cycle management and CIEM.
- **Business model:** ManageEngine still does not offer a SaaS version of its PAM product, but this is included in its roadmap.

Netwrix

Netwrix is a Niche Player in this Magic Quadrant. Its PAM offering consists of Netwrix Privilege Secure for Access Management for PASM and some PAM for machines functionality; and Netwrix Privilege Secure for Endpoints (formerly PolicyPak) for PEDM functionality. Netwrix's PAM products are available only as software.

Netwrix's customers are primarily concentrated in North America and Europe. Recent roadmap updates include introducing a SaaS offering. Other roadmap items are less focused on the PAM market specifically.

Strengths

- **Product:** JIT privileged access functionality is the top-performing capability for Netwrix, with support for all JIT methods evaluated. The product's privileged session management, remote PAM and Windows PEDM functionality are also competitive.
- **Technical support:** Netwrix only offers two support levels to choose from, but all training is free. It offers multiple customer engagement strategies, but no support for a customer advisory board.

- **Business model:** Netwrix offers a bring-your-own-vault model, allowing the company to position itself as an enhancement to existing PAM tools, as opposed to just a replacement for those tools.
- **Customer experience:** Overall customer experience is positive for Netwrix, with its customers praising the ease of use and ease of deployment aspect of Netwrix's PAM product.

Cautions

- **Product:** While Netwrix is one of the top performers for JIT privileged access, its offering underperforms in most other evaluated technical capabilities, and is especially weak in privileged credential management and workload identity and secrets management.
- **Pricing:** Netwrix is priced above the market average across multiple pricing scenarios.
- **Operations:** Netwrix lacks certifications that are common among other vendors in this Magic Quadrant, such as FIPS and Common Criteria standards. Moreover, it experienced a lot of major leadership changes last year.
- **Product strategy:** Netwrix still does not offer a SaaS version of its PAM products and it has pushed a few roadmap items planned for 2025 back to 2026, including SSH key discovery and promised out-of-the-box integration with ITSM tools.

One Identity

One Identity is a Visionary in this Magic Quadrant. One Identity (part of Quest Software) provides PASM functionality with its One Identity Safeguard product, available as software, hardware or SaaS. It offers software-based PEDM functionality with Safeguard Privilege Manager (for Windows); Safeguard for Sudo (for UNIX/Linux); and Safeguard Remote Access and PAM Essentials, available as SaaS, for RPAM. One Identity also offers Safeguard Secrets Broker Vault for some PAM for machines functionality, and One Identity Cloud PAM Essentials — a SaaS lightweight PASM product targeted at SMB customers.

One Identity's operations are geographically diversified. Recent roadmap updates include SaaS PEDM capabilities and AI-driven PAM deployment and configuration features.

Strengths

- **Product:** One Identity received some of the highest scores in this evaluation for privileged session management and for PEDM for UNIX/Linux and macOS.

- **Technical support:** One Identity offers four different levels of support and paid training. It offers multiple approaches for customer feedback. Its PAM solution received praise from customers for its user interface (UI), deployment process and management features.
- **Innovation:** One Identity Cloud PAM Essentials has added search capabilities powered by Azure AI, enabling searches through session recordings using natural language models. It has also introduced an AI-based UI to facilitate administrative tasks.
- **Pricing:** One Identity's pricing for a series of pricing scenarios evaluated is below the market average, especially for its SaaS PAM offerings.

Cautions

- **Product:** Apart from privileged session management and UNIX/Linux and macOS PEDM, One Identity either scores fair or just good for most other evaluated technical capabilities.
- **Overall viability:** One Identity had some of the lowest revenue growth for its PAM products among vendors evaluated in this research during the last fiscal year.
- **Operations:** In recent years, One Identity has continued to shrink in terms of dedicated staff focused on its PAM product portfolio. The company has shifted to a channel-first model, which is in line with its employee retention rate being the lowest of vendors evaluated in this research.
- **User experience:** One Identity still offers separate interfaces for its PASM, PEDM, RPAM, CIEM and secrets management tools.

Saviynt

Saviynt is a Challenger in this Magic Quadrant. Its PAM offering is part of Saviynt Identity Cloud, available as SaaS, and offered in Pro or Essentials packages. The Pro package includes all required PAM capabilities for PASM, PEDM, RPAM and PAM for machines. PAM Essentials is a lightweight version sold for lightweight PAM scenarios.

Saviynt's operations are mostly focused in North America and Europe, although the vendor is steadily expanding its base in the Asia/Pacific market. Recent roadmap updates include AI-driven PAM deployment enhancements and building a decentralized framework for federated PAM scenarios.

Strengths

- **Product:** Saviynt is a top performer for privileged identity life cycle management, CIEM, and auditing and threat protection. Its privileged accounts discovery, JIT privileged access and secrets management capabilities are also competitive.
- **Product strategy:** Saviynt claims to invest a substantial part of its revenue in R&D initiatives for its PAM product, resulting in strong roadmap items such as AI-enabled autonomous onboarding for PAM.
- **Operations:** Saviynt's PAM offering is certified for most of the relevant certifications, including FedRAMP.
- **Business model:** Saviynt launched a free certification program that aims to train 100,000 students and professionals by 2026 in the fundamentals of IAM, and to explore how AI and machine learning are reshaping cybersecurity.

Cautions

- **Product:** Saviynt offers PEDM for Windows and Linux only, but those capabilities are relatively immature compared with other vendors. UNIX and macOS PEDM capabilities are not supported. Moreover, Saviynt does not offer a native "break glass" capability.
- **Pricing:** Saviynt's pricing for a series of scenarios evaluated is uneven. Pricing for small and midsize scenarios is above the market average, while its pricing for large-size scenarios is around the market average.
- **Technical support:** Savyint offers three levels of support, and while some training is free, premium training is paid and appears more expensive than other alternatives.
- **Product strategy:** Saviynt does not have any additional capabilities for PAM services to CPS on its roadmap.

Segura

Segura is a Challenger in this Magic Quadrant. Its PAM offering consists of PAM Core, available as software or SaaS, for PASM; Endpoint Privilege Manager (EPM), available as software, for PEDM; Domum Remote Access, available as SaaS, for RPAM; and DevOps Secret Manager (DSM), available as software or SaaS, for PAM for machines.

Segura's customers are primarily concentrated in Latin America, followed by Europe and some footprint in Asia/Pacific and North America. Roadmap items include unifying

privileged policy enforcement and session controls in a single control plane from various PAM tools.

In April 2025, Senhasegura underwent a rebranding exercise and changed its name to Segura.

Strengths

- **Product:** Segura is one of the top performers for account discovery and onboarding, privileged credential management and privileged life cycle management capabilities. Other capabilities are also competitive.
- **Technical support:** Segura offers three levels of support, with free training available. It collects various customer inputs for product improvement, but does not have a customer advisory board.
- **Innovation:** Segura introduced a universal bridge — called Quantum Connector — to connect its PAM product to cloud, OT, IoT, CPS and on-premises systems. Based on quantum-resistant encryption, this bridge will help customers remove custom connector sprawl, enable faster deployments, and ensure centralized monitoring and compliance.
- **Overall viability:** Segura's PAM customer growth in the last fiscal year was one of the highest among vendors evaluated in this research.

Cautions

- **Product:** Segura is relatively weak compared with most other vendors in remote privileged access and JIT privileged access capabilities.
- **Pricing:** Segura's pricing for a series of scenarios evaluated in this research is above the market average, for both its software and SaaS products.
- **Operations:** Segura experienced a lot of major leadership changes last year. Moreover, it lacks certifications such as FedRAMP, FIPS and Common Criteria standards.
- **Geographical strategy:** Although Segura expanded its customer base considerably in other geographies apart from Latin America, it currently lags behind most other vendors within this Magic Quadrant in terms of prominent presence in North America and Europe.

StrongDM

StrongDM is a Niche Player in this Magic Quadrant. It offers PASM, RPAM and PAM for machines capabilities through its StrongDM Enterprise offering, which is only available as SaaS. StrongDM does not offer PEDM and CIEM functionality.

StrongDM's operations are mostly focused in North America, although the vendor is slowly expanding its base in Europe. Recent roadmap updates include improvements in operational efficiency of privileged activities using AI agents, expanded PAM capabilities for SaaS applications and identity providers (IdPs), and the addition of privileged threat detection capabilities.

Strengths

- **Product:** StrongDM excels in JIT privileged access capabilities, supporting granular access to cloud provider services such as Amazon Relational Database Service, Google Kubernetes Engine, and Azure Virtual Machines.
- **Technical support:** StrongDM offers four levels of support, including a basic free option and a mix of paid and free training. It leverages a number of options for customer feedback, including customer surveys and a customer advisory board.
- **Innovation:** StrongDM was evaluated as excellent in terms of innovation, with notable innovative achievements including fine-grained access controls for SQL statements (initially PostgreSQL). This enables enforcement of data layer controls and facilitates compliance without requiring modification of database permissions. StrongDM also invests significant resources for R&D as a percentage of its budget.
- **Customer experience:** Overall customer experience with StrongDM is positive. Many customers praise the ease of implementation, use and administration of the StrongDM offering.

Cautions

- **Product:** Aside from JIT privileged access, StrongDM underperforms in other technical areas, especially privileged account discovery, session management and credential management.
- **Pricing:** StrongDM's pricing for a series of scenarios evaluated is one of the highest relative to competitors in this research.
- **Operations:** StrongDM lacks common certifications such as FedRAMP, FIPS, ISO 27001 and Common Criteria standards.

- **Geographic strategy:** StrongDM's customer base is primarily concentrated in North America. While the company is expanding its presence in Europe, Asia/Pacific, the Middle East and Latin America, sales and support coverage in these regions may not be as extensive as in its core market.

WALLIX

WALLIX is a Visionary in this Magic Quadrant. Its PAM offering consists of WALLIX Bastion, available as software; and WALLIX One PAM, available as SaaS, for PASM and PAM for machines functionality. PEDM functionality is provided under WALLIX PAM, which is available as software. WALLIX also offers WALLIX One Remote Access, available as SaaS, for RPAM.

WALLIX customers are primarily in EMEA, with some in North America, the Middle East and Africa. The company has invested heavily to attract and support customers that use CPS. Recent roadmap updates include a consolidated platform offering for its different PAM products. Other roadmap items are mostly catch-up features, such as privileged threat detection and CIEM integration.

Strengths

- **Product:** WALLIX has a key strength in privileged remote access, with WALLIX One Remote Access supporting any session management protocol. It also demonstrates significant capability in CPS PAM scenarios.
- **Technical support:** WALLIX offers two levels of support, along with paid training. It regularly engages customers for feedback and supports a customer advisory board.
- **Vertical strategy:** WALLIX maintains a strong presence across diverse industry verticals, including manufacturing, financial services and the public sector. Its robust PAM for CPS strategy effectively positions the company to address the specific needs of manufacturing and wholesale retail organizations.
- **Customer experience:** Clients often highlight efficient and timely support, and also comment positively on the solution's ease of use.

Cautions

- **Product:** WALLIX lacks password rotation connectors for most noninteractive accounts, has limited account discovery focused on Active Directory, and its JIT PAM capabilities remain immature and reliant on workflow/ITSM integrations.

- **Sales execution:** Of all the vendors offering SaaS deployment models, WALLIX has the weakest SaaS sales execution. It closed the lowest number of SaaS deals compared with other vendors, and the majority of its customers still implement WALLIX's PAM products on-premises.
- **Pricing:** Pricing continues to be uneven for WALLIX. Pricing for small and midsize scenarios is below the market average, while its pricing for large-size scenarios is above the market average.
- **Operations:** WALLIX lacks certifications that are common among other vendors, such as FedRAMP, SOC 2, FIPS and Common Criteria standards.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Keeper Security
- Saviynt
- Segura
- StrongDM

Dropped

- Broadcom (Symantec) was dropped as it did not meet the CII requirement of business and financial performance inclusion criteria.

Inclusion and Exclusion Criteria

The criteria listed here represent the specific attributes that analysts believe are necessary for inclusion in this research. To qualify for inclusion, vendors were required to provide a solution that satisfied the following inclusion criteria:

In terms of technical inclusion criteria, each vendor's solution had to meet all mandatory features for PAM and at least five out of eight common features, as of 19 May 2025.

The mandatory features for inclusion are:

- Centralized management and enforcement of privileged access by controlling either access to privileged accounts and credentials or execution of privileged commands (or both).
- Brokering privileged access to authorized human users (e.g., system administrators, operators and help desk staff) and authorized machines (e.g., systems, applications, workloads) on a temporary basis.
- Account discovery and onboarding of privileged accounts across multiple systems, applications and cloud infrastructure providers.
- Vaulting, rotation and management for privileged accounts, specifically:
  - A secured, hardened and highly available vault for storing credentials and secrets.
  - Tools to automatically randomize, rotate and manage credentials for privileged accounts.
  - Tools to manage the end-to-end process of requesting access through user interfaces by privileged users with approval workflows.
  - User interfaces to check out privileged credentials.
  - Injection of credentials in privileged sessions, including remote privileged sessions (e.g., RDP, SSH).
- Management, monitoring, recording and auditing for privileged sessions, including remote privileged sessions by allowing a privileged session to be automatically established using protocols such as SSH, RDP or HTTPS without revealing credentials to the user.

- Offer role-based administration, including centralized policy management for controlling access to credentials, and privileged actions, when applicable.
- Just-in-time (JIT) privilege management, which reduces the time and scope for which a user is granted privileged access.

The common features for inclusion are:

- Agent-based controlled privilege elevation for commands executed on Windows, UNIX/Linux or macOS operating systems.
- Secrets management for workloads, including applications, services, containers, scripts and virtual machines.
- Privileged account life cycle management for humans and machines.
- Cloud infrastructure entitlement management (CIEM).
- Identity administration, including federation and authorization capabilities to secure remote privileged access for third-party external IT staff, such as vendors, service providers and other external users that require technical access.
- Automating multistep, repetitive and routine tasks related to privileged operations that are orchestrated and/or executed over a range of systems, while providing guardrails by checking against defined policies and settings.
- Zero standing privileges (ZSP) where users are not elevated to a pre-existing privileged account or privileged role as a JIT approach, but rather net new permissions and roles are created when a privileged user needs access. Those permissions are deleted after a time-bound session.
- Analyzing privilege patterns, misconfigurations, access behaviors, and anomalies for privileged threat detection and response.

In addition, tools had to meet all of the following requirements:

- Be marketed, sold and deployed for use with customer production environments for purposes consistent with objectives of PAM.
- Be fully documented, for the entirety of features, including the documentation of the configuration (if applicable) and the use of the feature. Features that are not documented, or that are merely listed or referenced in passing, cannot be considered.

- Geography: Vendors must compete in at least two of the four major regional markets (North America; Latin America, including Mexico; Europe, the Middle East and Africa; Asia/Pacific, including ANZ). This criterion is considered met if a vendor has no more than 90% of its client base in one particular region.
- Intellectual property: Sell and support its own PAM product or service developed in-house, rather than offered as a reseller or third-party provider.
- Verticals: Have sold its PAM product or service to customers in different verticals or industries.
- Positioning: Markets its products for use consistent with PAM.

To further qualify for inclusion in the 2025 PAM Magic Quadrant, each vendor was also required to meet the following business performance criteria:

- Rank in the Top 15 for the Customer Interest Indicator (CII), as defined by Gartner. CII was calculated using a weighted mix of internal and external inputs that reflect Gartner client interest, vendor customer engagement, and vendor customer sentiment from 1 Apr 2024 through 31 Mar 2025. Data inputs used to calculate PAM customer interest include a balanced set of measures:
  - Gartner end-user inquiry volume per vendor
  - **Gartner.com** search data
  - Gartner Peer Insights competitor mentions
  - Google trends data
  - Social media analysis
  - Web traffic analysis
- Have booked total revenue of at least $30 million USD in FY24 for core PAM capability products and subscriptions (inclusive of maintenance revenue, but excluding professional services, consulting, and any systems integration support revenue); or, have a minimum of 1,200 paying customers (“unique client logos”) that have acquired the vendor’s PAM tools that cover the entirety of core PAM capabilities.

Honorable Mentions

- **Broadcom** sells Symantec Privileged Access Management, which is available as a virtual appliance for on-premises or in the cloud, and includes PASM, PEDM and PAM for machines capabilities bundled together. Broadcom did not meet the Customer Interest Indicator (CII) cut-off, as defined by Gartner, which is part of the broader business performance criteria for inclusion in this Magic Quadrant.

- **Devolutions** sells Devolutions PAM, which is available both as software and as SaaS for PASM, RPAM and some PAM for machines capabilities. It does not offer PEDM capabilities. Devolutions did not meet the business performance criteria for inclusion.

- **Fortinet** sells FortiPAM for PASM and RPAM. FortiPAM is available both as a virtual machine and a hardware appliance. Fortinet also offers zero-trust network access (ZTNA)-type capabilities embedded in its PAM product. Fortinet did not meet the business performance inclusion criteria.

- **IBM (HashiCorp)** sells Boundary for PASM and RPAM, and Vault for PAM for machines capabilities. IBM acquired HashiCorp in February 2025 and offers both products as self-managed software or as SaaS within the HashiCorp Cloud Platform (HCP). IBM (HashiCorp) did not meet the technical inclusion criteria.

- **Microsoft** sells several PAM features in its offerings. Microsoft Entra ID P2 includes privileged identity management (PIM), which is focused on JIT elevation of privileged sessions upon approval for roles in Microsoft Entra ID and Azure infrastructure, as well as group-based access to IaaS, PaaS and SaaS resources. Microsoft also offers a local administrator password solution (LAPS), which stores passwords for local administrator accounts in on-premises Active Directory and makes them available to administrators upon approval. In addition, Microsoft offers Windows PEDM features with Microsoft Intune Endpoint Privilege Management as part of the Microsoft Intune Suite, and as an add-on to any plan that includes Intune P1 or higher. Although it supports some aspects of PAM, Microsoft did not meet the technical inclusion criteria.

- **Okta** sells Okta Privileged Access, which provides JIT access to servers, secures access for privileged accounts across Active Directory and SaaS accounts, and offers a vault for secrets management. Okta did not meet the technical and business performance inclusion criteria.

- **SSH Communications Security** sells PrivX PAM, which is available both as software and as SaaS for PASM, PEDM, RPAM and some PAM for machines capabilities. It also offers

capabilities to adaptively address PAM CPS scenarios and provides ZTNA-type capabilities to its PAM customers without changes to existing infrastructure. SSH did not meet the business performance inclusion criteria.

- **Sectona** sells Sectona Security Platform, which is only available as software for PASM, PEDM, RPAM and some PAM for machines capabilities. Sectona targets the large enterprise and midsize market with a competitive license model. Sectona did not meet the business performance inclusion criteria.

- **Teleport** sells Teleport Infrastructure Identity Platform for cloud-native and multicloud infrastructure scenarios. Instead of relying on managing credentials, it enforces strictly identity-based access by creating a virtual privileged access mesh for identities accessing SSH, Kubernetes, web applications, databases, Windows desktops, cloud consoles, GitHub and MCP servers. Teleport did not meet the technical inclusion criteria.

- **Xage Security** sells Xage Extended PAM (XPAM), which is available both as software and SaaS for mainly PASM and RPAM scenarios. Xage Security includes ZTNA-type controls embedded in its PAM offering and is primarily used for JIT PAM and CPS protection scenarios. Xage Security did not meet the technical and business performance inclusion criteria.

Evaluation Criteria

Ability to Execute

Product or service: Evaluates core products offered by the vendor that compete in or serve the defined market. This includes current product capabilities, quality, feature sets and documentation in multiple product categories:

1. **Privileged account life cycle management:** This capability includes features to manage the full life cycle of privileged accounts, such as creation of privileged accounts and handling of discovered accounts, assignment, and management of ownership and usage, including granular administration-time authorization controls (i.e., RBAC). It also includes account decommissioning and the ability to review and certify privileged accounts.

2. **Account discovery and onboarding:** This capability includes features to discover, identify and onboard privileged accounts, including the ability to support periodic, ad hoc or continuous discovery scans. This also includes the ability to automatically discover target

services and systems (including virtual machines) for further discovery of privileged accounts contained on them.

3. **Privileged credential management:** This capability includes features to manage and protect system- and enterprise-defined privileged account credentials or secrets (including SSH keys). It includes generation, vaulting, rotation and retrieval for interactive access to these credentials by individuals. It also includes rotation of service and software accounts (i.e., embedded accounts) on target systems.

4. **Privileged session management:** This capability includes features for session establishment, management, recording and playback, real-time monitoring, protocol-based command filtering and session separation for privileged access sessions. Included are functions to manage an interactive session with the PAM tool, from check-out of a credential to check-in of that credential, although in normal cases the credential is not disclosed to the user.

5. **Privileged remote access:** This capability includes features for VPN-less secure remote privileged access scenarios, including credential management, session brokering, session recording and auditing, life cycle management, built-in MFA, JIT access, and enforcement of least privilege principles of remote privileged users. Additionally, it includes the optional capabilities for self-service registration and profile management, sponsorship and delegated administration, identity federation and access requests for remote privileged users.

6. **Workload identity and secrets management:** This capability enables management and brokering of access to credentials (e.g., passwords, OAuth tokens and SSH keys) for machines, such as workloads, devices, applications, services, scripts, processes and DevOps pipelines.
   It includes the ability to generate, vault, rotate and provide a credential to machines (for example, via an API). It also includes the ability to broker trust between different machines for the purpose of exchanging secrets, and to manage authorizations and related functions.
   Additionally, it includes the optional ability to establish trust with a machine without requiring a credential by using other mechanisms of recognition (including zero-factor authentication).
   IaaS/PaaS identities can also be used to establish trust with the vault. In combination, these functions support both secrets management for dynamic environments and robotic process automation platforms. This capability also includes optional analytics to

determine whether machine accounts are potentially abused or no longer in use, and the management of secrets in other secrets management products.

7. **UNIX/Linux privilege elevation and delegation management:** This capability provides host-based functions and features for enforcing policies to allow authorized commands or applications to run under elevated privileges. These features must execute on the actual operating system (kernel or process level). Level of support may vary by platform (UNIX/Linux and macOS). This capability can also provide Active Directory (AD) bridging, which applies AD controls to Linux/UNIX systems, including the ability to authenticate to these systems with AD credentials, and pass through GPO policies. This also covers file integrity monitoring and sudo controls.

8. **Windows privilege elevation and delegation management:** This capability provides host-based functions and features for enforcing policies to allow authorized commands or applications to run under elevated privileges. Administrators will log in using an unprivileged account and elevate the privilege as needed. Any command that needs additional privilege would have to pass through those tools, in effect preventing administrators from carrying out unsafe activities. These features must execute on the actual operating system (kernel or process level). Level of support may vary by platform (Windows).

9. **Ease of deployment, maintenance and adjacent system integration:** This capability provides functions and features to simplify the deployment of the PAM solution while ensuring ease of administration and maintenance. It requires the ability to provide functions and features to integrate and interact with adjacent security and service management features. These systems include identity governance and administration (IGA), single sign-on (SSO), multifactor authentication (MFA), enterprise directories, support for flexible connector and integration frameworks, general API access, integration with IT service management (ITSM) systems, security information and event management (SIEM) systems, and vulnerability management.

10. **Performance and availability:** This capability provides functions and features that track performance and availability of the PAM tool, including those that allow the PAM tool to provide redundancy for disaster recovery or business continuity purposes and ensure availability, recoverability and scalability. This is handled through SaaS architecture, or through native or third-party mechanisms for load balancing and “break glass” credential retrieval (when the PAM tool is not available) in the case of self-managed tools.

Additionally, this capability enables rapid scaling of the product to meet on-demand requirements.

11. **Just-in-time PAM methods:** This capability provides on-demand privileged access without the requirement of shared accounts carrying standing privileges. Typically, this involves nonprivileged accounts being granted appropriate privileges on a time bound basis. Common methods for achieving this can be: use of PEDM approaches; use of temporary and on-demand group membership; and the use of ephemeral accounts or security tokens. This capability is focused on compliance with the principle of least privilege and, subsequently, achieving zero standing privileges (ZSP) for PAM access.

12. **Cloud infrastructure entitlement management (CIEM):** This capability manages cloud access risks via admin-time controls for the governance of entitlements in (multi)cloud infrastructure environments (IaaS). Privileged entitlements define access to cloud resources, service access privileges and cloud management permissions. CIEM uses analytics, machine learning and other methods to detect anomalies in account entitlements, such as accumulation of privileges, and dormant and unnecessary permissions. CIEM enables enforcement and remediation of least privilege approaches by recommending and deploying policies. Most CIEM tools provide integrations with key IaaS platforms, such as Amazon Web Services, Google Cloud Platform and Microsoft Azure.

13. **Privileged access auditing and threat detection:** This capability enables auditing by capturing detailed logs of privileged access. These include requests, approvals or denials, login/logout times, policy violations, failed access attempts, file transfers and changes to configurations or data to maintain audit trails for security monitoring, forensic investigations and compliance auditing. It also enables threat detection by monitoring and analyzing privileged account activities, including detecting anomalies and suspicious behavior, such as unusual access patterns or unauthorized changes, and trigger alerts for potential security threats. Additionally, it provides risk assessment features that evaluate the security posture of privileged accounts and suggest remediation actions to mitigate vulnerabilities.

Overall viability: Includes an assessment of the organization's overall financial health, and the financial and practical success of the business unit. Also included is the likelihood of the individual business unit continuing to offer and invest in its PAM product, as well as advance the state of the art within the organization's portfolio of PAM products. We factored in the overall financial health of the organization based on overall size, its profitability and its

liquidity. We also evaluated each vendor's viability in the PAM market by examining the extent to which PAM sales contribute to overall revenue, customer retention and growth in PAM revenue, and the number of new customers.

Sales execution/pricing: Evaluates the PAM provider's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel. Factors evaluated include the manner in which the vendor supports customers in the sales process, utilization of direct and indirect channels, and pricing.

Pricing was more heavily weighted than other factors in this category, and included an evaluation of pricing models and their flexibility, and actual price performance. Vendors were asked to provide their best pricing for a series of six predefined configurations of increasing complexity and scale. Scores were then assigned based on whether a specific vendor's price for a configuration was well-below, below, on par with, above or well-above the industry average, as determined by standard statistical measures (see Note 1).

Market responsiveness/record: Evaluates a vendor's ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness to changing market demands. Each vendor was evaluated on how it measures the maturity of a PAM implementation, and how it has reacted within the past 12 months to the emerging needs of customers, evolving regulations and competitor activities. This criterion also considers the provider's history of responsiveness to changing market demands.

Marketing execution: Assesses the clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This "mind share" can be driven by a combination of publicity, promotional activity, thought leadership, social media, referrals and sales activities. Marketing activities and messaging were evaluated by looking at recent campaigns and their ability to make the vendor stand out from the pack, as well as how each vendor measured the impact of its own marketing activities. A vendor's ability to promote itself through the press, conferences and other avenues was scored not just by the quantity, but also by the substance of the material and the thought leadership demonstrated. Brand depth and equity was another area of

consideration, looking for how a vendor builds and maintains its brand globally. Attention was also given to how the vendor uses its brand to attract buyers.

Customer experience: Evaluates the products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. This includes quality supplier/buyer interactions, technical support and account support. This may also include ancillary tools, customer support programs, availability of user groups and service-level agreements. Factors evaluated include customer relationships and services. We specifically focused on those that add value to the client (rather than adding the ability to upsell to the vendor). Among these, we also evaluated standardized professional services packages and other tools provided to customers for starting their journey, and helping them mature further, after some time had passed since the initial deployment. Methods to measure and incorporate customer satisfaction and feedback into existing processes were evaluated. We also took direct customer feedback into consideration using Gartner Peer Insights data, other Gartner client feedback and other sources.

Operations: Assesses the ability of the organization to meet goals and commitments. Factors include the overall size and quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently. We also evaluated organizational changes, certifications and internal processes, as well as availability (in terms of uptime) for SaaS-based offerings.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium

Evaluation Criteria	*Weighting*
Customer Experience	Medium
Operations	Low

Source: Gartner (October 2025)

Completeness of Vision

Market understanding: Assesses the ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their market — that listen to and understand customer demands, and can shape or enhance market changes with their added vision — scored well in this criterion. We evaluated the methodology and input to a vendor's market research programs, its understanding of buyers and their needs, an understanding of the competitive landscape and differentiators, and its ability to identif market trends and changes.

Marketing strategy: Evaluates whether a vendor's messaging is clear and differentiating, consistently communicated internally, and effectively externalized through social media, advertising, customer programs and positioning statements. Vendor communications plans were evaluated for raising awareness of the need for PAM initiatives, as well as the vendor's PAM products. Each vendor's marketing organization was also evaluated to determine if its makeup enables it to stay competitive when compared with other vendors in the space. We also evaluated each vendor's planned use of media to communicate its message.

Sales strategy: Examines the soundness of the vendor's sales strategy in terms of use of appropriate networks. These include direct and indirect sales, and partners that extend the scope and depth of market reach, expertise, technologies, services and the vendor's customer base. We also looked at the use of multiple channels to drive sales through direct and indirect sales. Lastly, we evaluated each vendor's ability to enable its sales force, both internally and externally.

Offering (product) strategy: Evaluates an approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements. An evaluation of the three most important features on a

vendor's roadmap was weighted heavily. We also measured vendors' plans to meet customer selection criteria, plans to catch up with competitors, and aspects of the vendor's product strategy that offer customer value and differentiate its offering from those of its competitors.

Business model: Emphasis was given to the design, logic and execution of the organization's business proposition to achieve continued success. We evaluated a cogent understanding of competitive strengths and weaknesses, recent company milestones and the path to further growth. In addition, we reviewed each vendor's ability to establish and maintain partnerships (with adjacent technologies, value-added resellers and system integrators), along with its ability to leverage them as part of an overall business plan. Finally, we evaluated the ease of doing business with the vendor from a customer's perspective.

Vertical/industry strategy: Assesses the vendor's strategy to direct resources (for example, sales and product development), skills and offerings to meet the specific needs of individual market segments, including midsize enterprises, service providers and verticals. Factors evaluated include the applicability of the offering to specific verticals, industries and organization sizes; the vendor's understanding of the varying needs of those segments; and the vendor's overall vertical strategy, including planned changes.

Innovation: Evaluates the direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes. We evaluated the ability of the vendor to deliver both technical and nontechnical innovations (for example, supporting processes and implementation programs) that advance the ability of buyers to better control, monitor and manage privileged users and credentials, and which meaningfully differentiate the products.

Geographic strategy: Assesses the vendor's strategy and ability to direct resources, skills and offerings to meet the specific needs of geographies outside its "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market. Each vendor was evaluated on its presence in international markets, and changes that support the spread of its products and services into other geographies. We also evaluated strategies for expanding global sales and support reach, internationalization support within products, and the ready availability of support and services in distinct geographies.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	Medium
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	High

Source: Gartner (October 2025)

Quadrant Descriptions

Leaders

PAM Leaders deliver a comprehensive toolset for administration of privileged access. These vendors have successfully built a significant installed customer base and revenue stream, and have high viability ratings and robust revenue growth. Leaders also show evidence of superior vision and execution for anticipated requirements related to technology, methodology or means of delivery. Leaders typically demonstrate customer satisfaction with PAM capabilities and/or related service and support.

Challengers

Challengers deliver a relatively strong set of PAM features. Some have major clients using their PAM solution. Challengers also show strong execution, and most have significant sales

and brand presence within a particular region or industry. However, Challengers may not have the means (such as budget, personnel, geographic presence or visibility) to execute in the same way as Leaders. Due to their smaller size, there may be initial concerns among some potential buyers regarding long-term viability.

Challengers have not yet demonstrated the same feature completeness or maturity, scale of deployment or vision for PAM as Leaders. Rather, their vision and execution for technology, methodology and/or means of delivery tend to be more focused on — or restricted to — specific platforms, geographies or services.

Visionaries

Visionaries provide products that meet many PAM client requirements. Visionaries are noted for their innovative approaches to PAM technologies, methodologies and/or means of delivery. They may have unique features, and may be focused on a specific industry or set of use cases, more so than vendors in other quadrants. While Visionaries can influence the direction of technological development in the market, they may not yet demonstrate a consistent track record of execution and often lack market share. Visionaries are often innovation leaders in maturing markets such as PAM, and enterprises that seek the latest solutions often look to Visionaries.

Niche Players

Niche Players provide PAM technology that is a good match for specific PAM use cases or methodologies. They may focus on specific industries or customer segments, and can actually outperform many competitors. They may focus their PAM features primarily on a specific use case, technology stack and/or infrastructure. Vendors in this quadrant often have a small installed base, a focus on specific customer segments, or a geographically limited footprint. Niche Players may also focus on other factors that inhibit them from providing a broader set of capabilities to enterprises. However, this does not reflect negatively on their value in the more narrowly focused service spectrum. Niche Players can be very effective in their area of focus.

Context

The goal of any Magic Quadrant is to provide a level view of comparable products (size, capability and corporate structure) to address the demands of a wide variety of buyers. Not

every company's requirements are identical. We encourage clients to review the accompanying **Critical Capabilities for Privileged Access Management** to review use-case and functionality requirements, and the Magic Quadrant to align industry expertise, vision, technology and cost requirements with the right vendor, regardless of whichever quadrant that vendor is in.

To lay a foundation for PAM success, organizations should start by investing in core PAM tool capabilities — such as privileged account discovery, credential management, session management/recording and MFA integration — for future-proof deployments. Furthermore, they should clearly define use cases, customization and scalability needs to match the right solution — whether PASM, PEDM, RPAM or PAM for machines — with targeted extensions to mature their PAM implementations.

Based on this research, Gartner continues to see more vendors offering a SaaS option for PAM implementations. This year, of the 12 vendors included in the research, 10 have a SaaS option and the remaining two have it in their roadmap. Many clients need to secure privileged access in their private and public cloud infrastructure, and we have seen the PAM market respond to this concern with new tools. The majority of the included vendors offer a secrets management tool for developer use cases, and the others have developed some basic secrets management features in their products. In addition, we have seen six vendors offering a CIEM tool, with some adding CIEM to their portfolios through acquisitions.

As the PAM market evolves with maturity in workload identity, secrets management and other PAM for machines capabilities, buyers must take a strategic approach to maximize value and minimize risk. Inadequate security for machines — especially workloads — poses significant security risks, given the extensive access and privileges provided to machine identity actors. PAM tools can help manage credentials for legacy service accounts and rotate service account credentials. They often provide some discovery capabilities for workload types of machine accounts. PAM tools also come with a vault that can be used to store credentials. However, the vaulting approach is not optimized for machine-to-machine use cases, which can be better addressed with secrets management capabilities, as part of PAM tools or with stand-alone secrets management tools. That said, several PAM vendors also sell stand-alone secrets management tools.

Thus, increased emphasis was placed on PAM for machines scenarios in this year's research, considering both product and nonproduct criteria. Specifically, from a product functionality standpoint, we introduced a new product use case, referred to as "PAM for machines." This use case focuses on securing the growing population of accounts and privileged

entitlements used by machines, including workloads and devices. From a functionality standpoint, increased emphasis was placed on:

- Workload identity and secrets management capabilities of the PAM tool, including:
  - A secret manager, which includes a secure and encrypted vault, that supports various types of authentication methods for machines.
  - Capabilities to programmatically issue, store, retrieve, rotate and manage secrets (such as keys, passwords, OAuth client credentials and certificates) for workloads (such as containers, applications, services, scripts, processes, DevOps pipelines and AI agents).
  - Capabilities provided through APIs, command-line interfaces (CLIs) and software development kits (SDKs).
  - Capabilities to discover and provide visibility and synchronization across various secrets vaults (both on-premises and cloud native).
- CIEM capabilities to analyze and manage identities, access policies and permissions, primarily for workloads and machines, across hybrid and multicloud infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) environments.
- Capabilities to continuously monitor the usage of credentials used by machines.
- Certificate life cycle management and SSH key management capabilities.

These capabilities can be delivered through stand-alone tools or embedded in the existing tools of the PAM vendor portfolio, which can be available as software or SaaS. Vendors were scored on their functionality for providing the above-mentioned PAM for machines capabilities, as well as their ability to support multiple types of secrets, integrate with secrets managers and cover multiple cloud infrastructures.

Also, given the emergence of generative AI tools, Gartner has observed PAM tools beginning to incorporate capabilities such as leveraging natural language interaction with key PAM functions and data. Examples include access to technical documentation, enhanced reporting and audit simulation capabilities, and automated session recording analysis. In addition, PAM vendors are introducing capabilities for enhanced threat detection. For example, determining suspicious behaviors in real time and leveraging agentic AI to learn and reason for potential corrective actions. These capabilities are nascent but will become

key differentiators in the coming years, including the capability to discover and manage the privileged access of AI agents.

Another consideration for PAM buyers should be on pricing of PAM tools and contract negotiations with their chosen or prospect PAM vendor. When negotiating SaaS or software subscription contracts, be very aware of what may happen once the contract terminates. Gartner has noticed that special discounts granted for the duration of one contract will no longer be granted at the time of an extension, forcing an organization to pay significantly more to continue using the solution. Also, vendors tend to update their pricing models from time to time, and have in some cases forced organizations to renew their subscriptions at a rate that is unfavorable compared with the previous contract. Consider negotiating maximum uplifts in the initial contract to cover the scenario when the current contract expires.

Proofs of concept and other vendor negotiations can take several months. An initial implementation of a PAM tool can take up to two months, with implementation of basic controls — especially PASM for human privileged account use cases — taking up to three months, depending on the complexity of the environment. Once these steps are complete, estimate timelines per use case or functional group until all PAM access is managed by the tool.

Market Overview

Vendor technology in the PAM market is more evolutionary than revolutionary. Although PAM tools are still hard to implement, the base technology — including core PAM capabilities around PASM, PEDM and RPAM — is fairly mature and the industry (vendors and customers) have a good understanding of its capabilities and usage.

However, the market continues to face notable challenges. Buyer maturity remains relatively low, solution differentiation for advanced use cases such as PAM for machines is unclear and more nuanced, with many providers struggling to differentiate their solutions, and the competitive landscape is crowded. These challenges complicate vendor positioning and customer decision making. In response, many vendors are repositioning as identity and access management (IAM) platform providers and rearchitecting their product portfolios to incorporate adjacent capabilities from other IAM markets.

Market evolution: The market has evolved over the past year, driven by end-user needs and advances in product capabilities. Apart from regulatory compliance, the main drivers of product capability expansion are accelerated migration to cloud, automation enablement for DevOps, the blurring of enterprise security perimeters, and a heightened need to discover and respond to privileged access threats given the rise in the number of cyberattacks. These drivers have contributed to expanded capabilities for remote PAM, secrets management, PEDM and PAM for machines scenarios.
PAM buyers show increased interest in securing remote privileged access for vendors and remote external IT staff. Other PAM buyers — such as software development and cloud operations teams — are struggling to impose stronger PAM controls to secure privileged access in DevOps and cloud infrastructures, leading to increased emphasis on secrets management capabilities. With the rise of machine IAM, PAM buyers show accelerated interest in securing privileged access associated with machine identities.

Market drivers: As in previous years, a significant minority (15%-25%) of clients are telling Gartner that cybersecurity insurers require them to have a strategy for managing privileges in their environment. This adds to the traditional drivers for PAM: security, regulatory compliance and audit.

Insurers often require organizations to deploy a PAM tool, along with MFA for administrative access, to mitigate the risk of breaches and malware events. [1] Clients should expect cybersecurity insurers to continue to scrutinize how privileged access is managed, in return for an insurance policy or lower premiums. This requirement is directly responsible for a significant minority (approximately 15% to 25%) of first-time PAM purchases that would have otherwise not happened at this time.

Market size: The growth of the privileged access management market continues to be driven by increasing awareness among security and identity leaders regarding the critical need for PAM solutions. Several high-profile breaches have been linked to compromised privileged account credentials and privilege abuse. [2] Gartner estimates that PAM market revenue for 2025 will amount to $3.25 billion, representing a growth rate of 12% over 2024. The market will continue to witness expansion, although growth is expected to taper off in the coming two to three years (see **Forecast: Information Security, Worldwide, 2023-2029, 3Q25 Update**).

Geographic and vertical trends: North America and Europe remain the primary markets for PAM products. However, the Asia/Pacific and Middle East regions have exhibited increased

interest and sales. Global enterprise vendors — such as CyberArk and, to some extent, BeyondTrust, Delinea, One Identity and ManageEngine — are increasingly attempting to extend their geographic reach into all regions. Once there, they'll be met by strong regional vendors: Segura in Latin America and WALLIX in Europe. While relatively smaller in size, these vendors have been able to take advantage of their local knowledge and relationships, language and close proximity to customers.

Diversified financial services (including banking, securities and insurance) — along with communications, media and services, and government — remain the primary industry verticals acquiring PAM solutions. This is unsurprising, given the high degree of risk and the heavy compliance load these industries face, as well as audit requirements. However, PAM is increasingly a horizontal solution. An emerging need from a vertical standpoint is for specific features for organizations using the Internet of Things (IoT) and cyber-physical systems (CPS).

See the Evaluation Criteria and Note 1 on pricing information (at the end of this research) for detailed explanations of terms used and other important information you will need to make the most of this Magic Quadrant.

Acronym Key and Glossary Terms

AD	Active Directory
CIEM	cloud infrastructure entitlement management
CLI	command-line interface
CPS	cyber-physical systems
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
GPO	Group Policy Object

IGA	identity governance and administration
IaaS	infrastructure as a service
IoT	Internet of Things
ITSM	IT service management
JIT	just in time
MFA	multifactor authentication
OT	operational technology
PaaS	platform as a service
PAM	privileged access management
PASM	privileged account and session management
PEDM	privilege elevation and delegation management
RPAM	remote privileged access management
SaaS	software as a service
SDK	software development kit
SIEM	security information and event management
SOC 2	System and Organization Controls 2

SSH	Secure Shell
SSO	single sign-on
UI	user interface
VNC	virtual network computing
ZSP	zero standing privileges
ZTNA	zero-trust network access

⊕ Evidence

Note 1: Pricing Information

We comment on the pricing of individual products based on a relative scale, using terms such as “well-above average,” “above average,” “average,” “below average” and “well-below average.” In each pricing scenario, the average is the mean/median value of the pricing for all vendors evaluated in this research:

- **Well-above average** includes the three highest price points (out of 12 vendors).
- **Well-below average** includes the three lowest price points.
- **Above average** are prices above the average price point, but below the three highest prices.
- **Below average** is below the average price point, but above well-below price points.

⊕ Evaluation Criteria Definitions