Magic Quadrant for Privileged Access Management

9 September 2024 - ID G00802036 - 64 min read

By Abhyuday Data, Michael Kelley, **and 3 more**

PAM products are now mainstream. Many vendors added advanced functionalities in the past year either through native product expansions or through strategic acquisitions. IAM leaders should focus assessment on the advanced 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 four distinct tool categories for PAM tools: privileged account and session management (PASM), privilege elevation and delegation management (PEDM), secrets management, and cloud infrastructure entitlement management (CIEM).

Privileged access is access beyond the normal level granted to business users. It allows users to override existing access controls, change security configurations, or make changes affecting multiple users or systems. Because 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. Users with a normal level of access control cannot effectively manage privileged access, so a specific set of procedures and tools is required. PAM tools focus on either privileged accounts or privileged commands.

PAM tools help organizations discover privileged accounts used by people 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 provide visibility and control into privileged account and command usage by tracking and recording privileged access for auditing. 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.

Must-Have Capabilities

The must-have capabilities 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 users (e.g., system administrators, operators and help desk staff) on a temporary basis

- Credential vaulting and management for privileged accounts

Standard Capabilities

Standard capabilities include:

- Privileged account discovery across multiple systems, applications and cloud infrastructure providers

- Agent-based controlled privilege elevation for commands executed on Windows, UNIX/Linux or macOS operating systems

- Management, monitoring, recording and remote access for privileged sessions

- Auditing capabilities to ascertain who used what privileged access when and where

- Just-in-time privilege management, which reduces the time and scope for which a user is granted privileged access
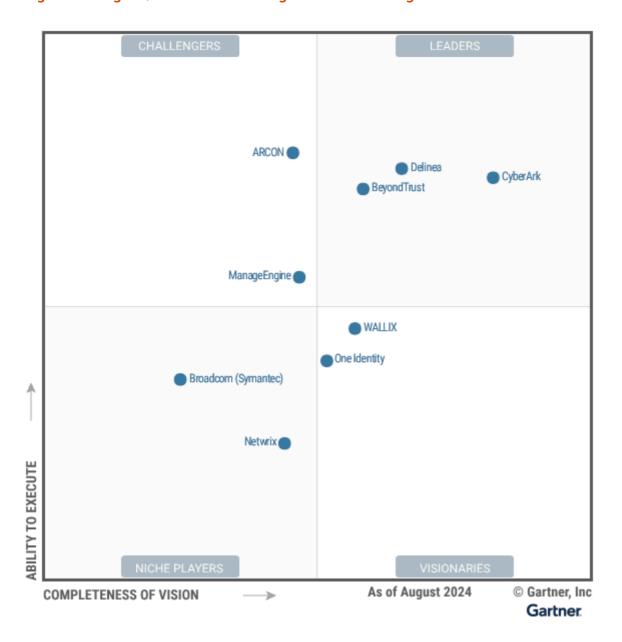
Optional Capabilities

Optional capabilities include:

- Secrets management for applications and services

- Privileged account life cycle management and remote privileged access for vendors, service providers and other external users that require technical access

- Cloud infrastructure entitlement management (CIEM) and discovery

Magic Quadrant

Figure 1: Magic Quadrant for Privileged Access Management

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 also offers several additional products and modules, including secrets management and application-to-application password management (AAPM), remote privileged access management (RPAM), connectors to DevOps infrastructure tools, and cloud infrastructure entitlement management (CIEM). Its operations are mostly focused in APAC and EMEA, although the vendor is steadily expanding its base in the U.S. Roadmap items since the last Magic Quadrant include zero-trust network access (ZTNA) enhancements for RPAM scenarios and improvements in operational efficiency of privileged activities through AI enhancements.

Strengths

- **Product**: ARCON's offering is the most capable of all vendors evaluated, with every capability evaluated above — and often well-above — the average. Two core features where Arcon scores the highest are account discovery and just-in-time (JIT) PAM; Arcon demonstrated notable improvements in the ephemeral credential JIT use case.

- **Pricing**: ARCON's pricing is competitive. In most pricing scenarios, especially for PASM, ARCON is more affordable than other vendor offerings in this research. In PEDM and secrets management scenarios, pricing is around average and sometimes higher than average, especially for its software offering.

- **Customer experience**: ARCON excels in customer experience, earning one of the highest scores in this research. 24/7 support is included for all customers, a technical account manager is available at no additional cost as well as a complimentary product training program.

- **Overall Viability:** ARCON's PAM customer growth in the last fiscal year was one of the highest among the vendors evaluated in this research.

Cautions

- **Product**: Arcon provides limited out of the box (OOTB) preconfigured integration with IT service management (ITSM) tools, or the kind of identity governance and administration (IGA) tools compared to other vendors included in this research.

- **Market responsiveness**: Arcon did not demonstrate response to evolving market dynamics for new regulations or legislations this year like NIS 2 and the Digital Operational Resilience Act (DORA).

- **Geographical strategy:** Though ARCON is trying to expand its customer base in the U.S., it currently lags behind other vendors within this Magic Quadrant, in terms of prominent presence in the Americas and Europe.

- **Sales strategy:** Arcon's channel partner network has limited global penetration compared to most other vendors included in this research.

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 secrets management functionality. PS and PRA are also sold separately, with each available as SaaS, software and appliance (hardware or virtual). PEDM functionality is provided by BeyondTrust's Privilege Management products for UNIX/Linux, macOS and Windows, which are available as software and SaaS. CIEM functionality is provided through Identity Security Insights and Entitle (SaaS only, which also provides JIT features), a recent acquisition earlier in 2024. BeyondTrust customers are geographically diversified, with large concentrations in North America and Europe. Roadmap items since the last Magic Quadrant include enhancements to Identity

Security Insights, additional JIT functions, and adding database proxying for MySQL and PostGres.

Strengths

- **Product:** BeyondTrust is best in class for UNIX/Linux and macOS PEDM, and a top performer for Windows PEDM, including strong methods for application controls. For the Total PASM bundle, clients comment favorably on discovery features, smart rules and ease of use.

- **Customer experience:** BeyondTrust scores high for customer experience where it boasts customer support teams with a wide range of expertise. Every customer is assigned an account team that includes different levels of support, from customer success managers to technical professionals.

- **Product strategy:** The bundle of PS and PRA provides strong account discovery and onboarding, privileged session management and remote access features. However, the same is not true if only one of those products is deployed: PRA is focused on privileged session management, but the stand-alone version of PS is not strong here.

- **Product and operations:** Improvements in ease of deployments include analytics with correlation of identity data from identity providers (IdPs) and cloud infrastructure platforms (CIPs). Also, customers have flexibility to schedule updates when using BeyondTrust's SaaS solution. It also offers extensive out-of-the-box ITSM and other adjacent system integrations.

Cautions

- **Product:** Despite BeyondTrust's above-average performance in account discovery mechanisms for operating systems accounts, it is trailing behind some of the other vendors in this research due to its lack of discovery for shadow admin accounts and private Secure Shell keys.

- **Pricing:** BeyondTrust's pricing remains higher than the market average, especially for its software PAM offerings. Enhanced JIT functionality requires the purchase of an additional product, Entitle, which further escalates costs.

- **Product:** BeyondTrust's offering for workload identity and secrets management provides only rudimentary capabilities, although it is included without extra charge for all clients that purchase Password Safe stand-alone or as part of the Total PASM bundle.

- **Reporting and auditing:** BeyondTrust continues to lack the ability to provide information for troubleshooting and guidance to resolve issues beyond just logging, and its provision of relevant health reporting in customer environments is immature for administrative reporting and auditing purposes.

Broadcom (Symantec)

Broadcom (Symantec) is a Niche Player in this Magic Quadrant. Its PAM product is Symantec Privileged Access Management, which is available as a virtual or hardware appliance, and includes PASM, PEDM, AAPM and secrets management bundled together. Broadcom does not

offer CIEM. Broadcom has significant customer populations in North America, EMEA and APAC. Roadmap items since the last Magic Quadrant include minor improvements to existing functionality, like discovery and secrets management, as well as the introduction of a new browser-based PAM gateway.

Broadcom did not respond to requests for supplemental information. Gartner's analysis is therefore based on other credible sources.

Strengths

- **Product:** Broadcom offers a very competitive PEDM product for Windows and UNIX/Linux. Its performance and scalability, availability and recoverability capabilities are strong for PASM, including excellent clustering and high-availability features that support the addition of nodes without having to take a cluster down.

- **Pricing:** Symantec PAM is priced competitively, with almost all scenario pricing below — and sometimes well below — the average for the market as a whole. In addition, Broadcom offers its top clients portfolio license agreements, which may offer additional savings.

- **Geographic strategy:** Broadcom maintains a strong global presence and continues to offer dedicated support to its PAM clients in different regions.

- **Product:** Broadcom scores above average for performance and availability features. It offers robust support for very large PAM implementations with a streamlined approach to scale up proxies, jump boxes or bastion servers, and it can support a large number of concurrent sessions for enterprise scalability.

Cautions

- **Marketing strategy and execution:** Given that Broadcom is focused on its top customers, market strategy and execution is relatively weaker than other vendors evaluated in this research. Broadcom has few media or marketing channels to promote its PAM products to gain new customers.

- **Product:** For complex service account credential management, Broadcom customers still have to develop custom connectors, whereas other vendors offer out-of-the-box connectors. Privilege credential management and JIT PAM were also less mature compared to other vendors evaluated in this research.

- **Innovation/roadmap:** Broadcom innovations since the last publication of this Magic Quadrant were limited to minor incremental enhancements of existing products like new dashboards and additional API functions.

- **Product strategy:** Broadcom is the only vendor in this Magic Quadrant that has not yet provided, developed or roadmapped a SaaS offering for its PAM product.

CyberArk

CyberArk is a Leader in this Magic Quadrant. It offers PASM functionality with Privileged Access Manager (SaaS or software), PEDM functionality with its Endpoint Privilege Manager for Windows, Linux and macOS (SaaS), On-Demand Privileges Manager (OPM) for AIX and Solaris (software). Secrets management and AAPM features are offered with Conjur (SaaS or software) and Secrets Hub (SaaS). It also offers a remote PAM tool called Vendor Privileged Access Manager (SaaS). CIEM functionality is now provided through its Secure Cloud Access (SCA) product (SaaS), which was previously delivered stand-alone through Cloud Entitlements Manager. CyberArk's operations and customer base are geographically diversified. Roadmap items since the last Magic Quadrant include identity (Active Directory) bridging for Linux and macOS, as well as a hybrid architecture support to accommodate self-managed systems in its SaaS deployment model.

Strengths

- **Product:** CyberArk's PAM solution is mature and highly capable across the various use cases evaluated, mainly PASM, Windows PEDM, workload identity and secrets management.

- **Market responsiveness:** CyberArk has invested heavily in workload identity and secrets management for the past few years. The outcome is a broad set of technical capabilities that can address client needs across virtually every scenario evaluated.

- **Geographical strategy:** CyberArk has a robust global presence with its customers spread all across the globe.

- **Innovation:** CyberArk has delivered a number of significant updates since last year's Magic Quadrant, such as improving group-membership-based JIT, and adding native database access through its Dynamic Privileged Access (DPA) module.

Cautions

- **Product:** Configuration and management of the self-hosted components of CyberArk's PAM solution are usually complex. There have been some improvements to the upgrade process, but major upgrades may require extensive vendor support.

- **Pricing:** A common complaint from clients is about cost — CyberArk's products are among the most expensive on the market — and it no longer offers additional discounting for customers who opt for a multiyear deal over a one-year deal.

- **Customer experience:** While customer experience is still overall positive, CyberArk customers identify customer support and timely responsiveness as areas the vendor could improve.

- **PEDM:** File integrity monitoring for UNIX/Linux, as well as centralized sudo management, are limited compared to other leaders. Native AD bridging is available only for OPM (which is no longer sold for Linux). CyberArk does not support the application of Windows group policy objects (GPOs) for UNIX/Linux and macOS.

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 CIEM functionality bundled together. Stand-alone options include Secret Server for PASM (SaaS or software), PEDM with Privilege Manager (SaaS or software, Windows and macOS endpoints) and Server Suite (UNIX/Linux endpoints).

DevOps Secrets Vault is the secrets management product. Delinea acquired Authomize earlier in 2024, which enhances its existing CIEM capabilities, and FastPath (also in early 2024) which, according to Delinea, will bring enhancements to JIT and life cycle management features. Delinea's operations are geographically diversified, although most of its clients are in North America, followed by Europe. Roadmap items since the last Magic Quadrant include expansion of CIEM features to CSPs and SaaS apps, and the ability to manage other CSP-native and third-party vaults for secrets management enhancements.

Strengths

- **Product:** Delinea has a very competent PEDM offering for UNIX/Linux that scored among the top vendors of those evaluated.

- **Overall Viability:** Delinea's revenue and customer count growth was one of the highest among all vendors included in this research.

- **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.

- **Geographical strategy:** Delinea has built a strong geographical presence and intends to enhance its global customer reach by strengthening local operational support in APAC, Japan and LATAM.

Cautions

- **Product:** Remote Desktop Protocol (RDP) video session metadata recording requires installation of local agents on target servers, which most other evaluated vendors don't require.

- **Pricing:** Although Delinea introduced a new pricing model to consolidate all of its SaaS products into a bundled offering, pricing evaluated for a series of scenarios in this research is uneven. Pricing for small and midsize scenarios is below the market average, and pricing for large-size scenarios is above the market average. Windows PEDM pricing is one of the highest compared to alternatives.

- **Product strategy:** Delinea has a strategy to present Secret Server as a "simple to deploy and use" solution and its marketplace for available OOTB integrations grew last year. However, several requirements still need customization through PowerShell, placing an additional burden on customers. Many customers have highlighted the need for improvement in technical support response times.

- **Operations:** Delinea recently made two major acquisitions (Authomize and Fastpath), and made a large number of changes to its executive team, which may cause some inconsistencies in execution until the dust settles.

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 its PAM product, PAM360. PAM360 offers PASM, PEDM, AAPM and some secrets management functionality bundled together as software only. It also offers Application Control Plus for endpoint privilege management and application control functionality. ManageEngine does not currently offer CIEM functionality. ManageEngine's operations are geographically diversified. Roadmap items since the last Magic Quadrant include the introduction of a SaaS version of the PAM product and CIEM capabilities along with enhancement to privileged task automation functionality.

Strengths
- **Pricing:** ManageEngine pricing is consistently less than market averages. 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).

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

- **Vertical strategy roadmap:** ManageEngine is committed to improving its support for government-specific needs. As part of its plan, it is working on a specialized version of its PAM360 product that will include controls tailored to meet the unique requirements of government clients.

- **Business Model:** ManageEngine claims to invest over 50% of its revenue into R&D initiatives, but has a product roadmap designed to catch up on product capabilities, as well as to stand out in other areas such as managing privileged access for IoT/OT devices.

Cautions
- **Product:** ManageEngine's JIT PAM capabilities are immature compared to other vendors. There were no improvements in session management and in out-of-the-box connectors for adjacent system integrations including IGA, which is a common integration among PAM vendors.

- **Product strategy:** ManageEngine still does not offer a SaaS version of its PAM product, but this is included in its roadmap.

- **Operations:** ManageEngine lacks certifications that are common among other vendors, such as Federal Information Processing Standards (FIPS), a focus on encryption, or the Common Criteria standards.

- **Product strategy:** ManageEngine's roadmap does not address long-standing product gaps compared to the market. PAM360 is below the average of vendors evaluated for privileged credential management, workload identity and secrets management, and UNIX/Linux PEDM.

Netwrix

Netwrix is a Niche Player in this Magic Quadrant. Its PAM offering consists of Privilege Secure for Access Management for PASM and secrets management functionality, and Privilege Secure for Endpoints (aka PolicyPak) for PEDM functionality. Netwrix's PAM products are available only as software. It does not currently offer CIEM functionality. Netwrix's customers are primarily concentrated in North America and Europe. Roadmap items since the last Magic Quadrant include the addition of a VPN-less RPAM product, enhancements to protocol filtering, and detection of sensitive data on an endpoint to control authorization for endpoints.

Strengths

- **Product:** JIT privileged access functionality is among the most capable of all vendors evaluated. Privileged session management and Windows PEDM functionality is also competitive.

- **Innovation:** Netwrix had one of the highest scores for innovation in this research. Notable innovations since the last Magic Quadrant include a JIT approach for database access, and new health checks for privileged access review and auditing.

- **Marketing understanding:** Netwrix has a unique angle on the PAM market with a bring-your-own-vault approach, allowing the company to position itself as an enhancement to existing PAM tools as opposed to just a replacement for those tools.

- **Marketing execution:** Netwrix has developed a solid narrative around its brand and specifically targets its marketing toward the benefits of zero standing privileges, rapid deployment and ease of use.

Cautions

- **Product:** Apart from JIT privileged management, Netwrix's offering underperforms in most other evaluated technical capabilities, and is especially weak in privileged credential management and remote access.

- **Pricing:** Netwrix is priced above the market average compared to other vendors included in this research, across multiple pricing scenarios.

- **Product strategy:** Netwrix still does not offer a SaaS version of its PAM products and it pushed a few roadmap items planned for 2024 to 2025, which includes promised out-of-the-box integration with ITSM tools.

- **Overall viability:** Netwrix's PAM revenue and customer count growth in the last fiscal year were some of the lowest among the vendors evaluated in this research.

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 through either software, hardware or SaaS; software-based PEDM functionality with Safeguard Privilege Manager (for Windows and macOS); Safeguard for Sudo (for UNIX/Linux) and Safeguard Remote Access, available as SaaS, for RPAM. It also offers a tool called Safeguard Secrets Broker Vault that is not a secrets manager in itself, but acts as a front end to other vaults and secrets managers. One Identity does not offer a CIEM product, but can provide some CIEM functionality with an adjacent identity governance and administration (IGA) product. Since the last Magic Quadrant, One Identity also introduced One Identity Cloud PAM Essentials, a SaaS lightweight PASM product targeted for SMB customers. One Identity's operations are geographically diversified. Roadmap items since the last Magic Quadrant include enhancements to VPN-less remote access for cloud infrastructure components.

Strengths

- **Product:** One Identity received some of the highest scores in the market for privileged session management, account discovery and onboarding, and for PEDM for UNIX/Linux and macOS.

- **Customer experience:** One Identity's PAM solution receives praise from customers for its user interface, deployment process and management features.

- **Innovation:** One Identity scores above average for innovation, which includes a new lightweight PAM SaaS-based offering for midsize enterprises and enhancements to its existing remote PAM features.

- **Sales and geographic strategy:** One Identity scores above average for sales and geographic strategy. It offers an extensive channel partner network across the globe due to a revamped vendor-to-partner information delivery system, providing immediate on-demand updates and release information. It has also seen an uptick in new partners.

Cautions

- **Product bundling/packaging:** Clients looking for a single tool for comprehensive PAM functionality, may find One Identity's strategy confusing. One Identity's core PAM tool is dependent on additional One Identity products for extending functionality. For example, One Identity IGA tool is required to expand life cycle management and auditing, and to provide CIEM functionality, and Active Roles is required for extending JIT functionality, such as mapping network drives.

- **Pricing:** One Identity's pricing remains higher than the market average, especially for its SaaS PAM offerings.

- **User experience:** One Identity offers only separate interfaces for its PASM, PEDM, RPAM, CIEM and secrets management tools.

- **Overall viability:** One Identity had some of the lowest revenue and customer count growth among the vendors evaluated in this research for its PAM products in the last fiscal year.

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 AAPM functionality. PEDM functionality is provided under WALLIX PAM. It also offers WALLIX One Remote Access, available as SaaS, for RPAM. WALLIX does not offer a CIEM product, but can provide some CIEM functionality with an adjacent IGA product. WALLIX customers are primarily in EMEA, with some in North America, Middle East and Africa. The company has invested heavily to attract and support customers that use cyber-physical systems (CPS). Roadmap items since the last Magic Quadrant include a centralized control for dashboarding, configuration and administration for its customers, improvements to secrets management, and a new functionality for tunneling in OT environments.

Strengths

- **Product:** WALLIX received one of the highest scores in the market for privileged remote access and session management. For RPAM, its WALLIX One Remote Access is one of the strongest in the market offering support for all major session management protocols including universal tunneling through TCP. Identity administration, authorization, session collaboration and file transfer capabilities for remote privileged scenarios are also mature.

- **Vertical industry strategy:** WALLIX stands out with one of the highest scores for its vertical strategy, demonstrating a significant presence across a wide range of industry verticals (with best-in-class support for operational technology and industry control systems), as well as manufacturing, banking, securities and insurance, and government.

- **Product:** WALLIX offers a meaningful PAM break-glass approach where it can run a scheduled task to send break-glass credentials over encrypted emails periodically.

- **Customer experience:** Clients often highlight efficient and timely support, and also comment positively on the solution's ease of use.

Cautions

- **Pricing:** WALLIX changed its pricing model in 2024 and increased the price of its PAM products. As a result, its pricing is consistently above market averages compared to competitors across various pricing scenarios evaluated in this research.

- **Product:** WALLIX continues to lack password rotation connectors for most noninteractive machine and service account scenarios, and has no plans to address this shortcoming. WALLIX also has limited account discovery features (it is focused mostly on active directory scanning) and has stopped offering them as a separate tool for free download.

- **Geographic strategy:** WALLIX has a strong presence in Europe, but its geographical expansion is nascent in comparison to other vendors in this research.

- **Product:** WALLIX has relatively immature JIT PAM capabilities, where it is still dependent on workflow/ITSM integrations.

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

No vendors were added.

Dropped

- HashiCorp was dropped as it did not meet the technical inclusion criteria.

- Saviynt was dropped as it did not meet the 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 are required to provide a solution that satisfies the following technical product criteria:

For technical inclusion criteria, the vendor's solution must meet all must-have capabilities and at least four out of five of the standard capabilities as of 17 April 2024.

The must-have capabilities 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 users (e.g., system administrators, operators and help desk staff) on a temporary basis

- Credential vaulting and management for privileged accounts

  - 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.

Standard capabilities include:

- Privileged account discovery across multiple systems, applications and cloud infrastructure providers.

- Agent-based controlled privilege elevation for commands executed on Windows, UNIX/Linux or macOS operating systems.

- Management, monitoring, recording and remote access for privileged sessions allows a privileged session to be automatically established using protocols such as SSH, RDP or HTTPS without revealing credentials to the user.

- Auditing capabilities to ascertain who used what privileged access when and where.

- Just-in-time privilege management, which reduces the time and scope for which a user is granted privileged access.

In addition, tools must meet all of the following requirements:

- Offer support for role-based administration, including centralized policy management for controlling access to credentials and privileged actions, when applicable.

- 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, but not documented) cannot be considered.

- Geography: 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 condition would be met if a vendor has no more than 90% of its client base in one particular region.

- Intellectual property: Sell and support their own PAM product or service developed in-house, rather than offer as a reseller or third-party provider.

- Verticals: Have sold their PAM product or service to customers in different verticals or industries.

- Positioning: Market their products for use consistent with PAM.

To further qualify for inclusion in this research, the respective vendors must also meet the following business and financial performance criteria:

1. 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. Data inputs used to calculate PAM customer interest include a balanced set of measures:

1. Gartner end-user inquiry volume per vendor

2. Gartner.com search data

3. Gartner Peer Insights competitor mentions

4. Google trends data

5. Social media analysis

6. Web traffic analysis

2. Have booked total revenue of at least $25 million in FY23 for core PAM capability products and subscriptions (inclusive of maintenance revenue, but excluding professional services, consulting, and any SI support revenue) 'OR' have a minimum of 1,100 paying customers ("unique client logos") that have acquired the vendor's PAM tools that cover the entirety of core PAM capabilities.

Honorable Mentions

- **Bravura Security** (formerly Hitachi ID) sells PASM functionality through the Bravura Privilege product, a software-delivered PAM tool with solid discovery and credential management, including out-of-the-box connectors for service accounts. It does not offer any PEDM features. Bravura Security did not meet the business/financial performance inclusion criteria.

- **Fortinet** sells FortiPAM for PASM and FortiSRA for RPAM. FortiPAM is available both as a virtual machine and a hardware appliance, while FortiSRA is only available as a virtual machine. Its session management is relatively more mature than its other PAM features. It also offers ZTNA type capabilities to its PAM customers at no additional cost. Fortinet did not meet the business and financial performance inclusion criteria.

- **HashiCorp** sells Boundary for PASM and RPAM and Vault for machine identity and secrets management. Both products are available as self-managed software or as a service within its HashiCorp Cloud Platform (HCP). HashiCorp is a well-known player in the secrets management market, and clients share positive feedback about the Vault product. HashiCorp did not meet the technical inclusion criteria.

- **Keeper Security** sells a platform solution called Zero-Trust Keeper PAM, which consists of Keeper Password Manager, a Workforce Password Management (WPM) tool, in combination with Keeper Connection Manager for Privileged Account and Session Management (PASM) use case, and Keeper Secrets Manager for secrets management use case. Keeper Security's session management is relatively more mature than its other PAM features. Keeper Security has a good reputation in the WPM market and it still markets and sells its products primarily in that space. Keeper Security did not meet the technical inclusion criteria.

- **Microsoft** sells several PAM features in its offerings. Microsoft Entra ID P2 includes privileged identity management (PIM) that is focused on JIT elevation of privileged sessions upon

approval for roles in Microsoft Entra ID and Azure infrastructure, and group-based access to IaaS, PaaS and SaaS resources. Microsoft Entra Permissions Management is a CIEM solution that supports the GCP, AWS and Azure IaaS platforms. In addition, Microsoft offers a local administrator password solution (LAPS) that stores passwords for local administrator accounts in on-premises Active Directory, and makes them available to administrators upon approval. Microsoft has also introduced 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** recently introduced its PAM product, Okta Privileged Access, which is focused on brokering privileged sessions to authorized users with a JIT approach. It also offers vaulting, session management/recording for standard PASM scenarios, and the ability to discover entitlements in cloud infrastructures. Okta did not meet the business and financial performance inclusion criteria

- **Saviynt** sells its PAM product as part of its Saviynt Identity Cloud platform. Saviynt PAM is available as SaaS or privately managed on infrastructure as a service (IaaS) platform like AWS, GCP and Azure or as a virtual appliance. It primarily offers PASM and CIEM and has recently added RPAM and some native secrets management functionalities. Saviynt is a well-known player in the IGA market and Saviynt PAM users get Saviynt IGA and CIEM functionality for all licensed users at no additional cost. Saviynt did not meet the business and financial performance inclusion criteria.

- **senhasegura** offers a PASM product, senhasegura PAM Core, available as software or as a service. PEDM for Windows and Linux is available in a software offering called GO Endpoint Manager. Secrets management is sold as software or as a service under the name DevOps Secrets Management. senhasegura also offers a CIEM product under the name senhasegura Cloud Entitlements and RPAM product as Domum Remote Access. senhasegura offers robust PAM for many scenarios, but did not meet the business and financial performance inclusion criteria.

- **StrongDM** provides a SaaS-based solution, Zero Trust PAM, focused on brokering privileged sessions to authorized users with a JIT approach. It also features vendor remote access, and easy authorization functions through contextualized workflows and policy-based access controls. StrongDM did not meet the business and financial performance inclusion criteria.

- **Teleport** sells Teleport Access Platform, which is an alternative to PAM 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 accounts accessing SSH, Kubernetes, web applications,databases, Windows desktops and cloud consoles. Teleport did not meet the technical inclusion criteria.

Evaluation Criteria

Ability to Execute

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

- **Privileged account life cycle management:** Features to manage the full life cycle of privileged accounts, including: creation of privileged accounts and handling of discovered accounts, assignment and management of ownership and usage, account decommissioning, and the ability to review and certify privileged accounts.

- **Account discovery and onboarding:** 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, systems (including virtual machines), for further discovering privileged accounts contained on them.

- **Privileged credential management:** 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.

- **Privileged session management:** 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.

- **Privileged remote access:** Features for VPN-less secure remote privileged access scenarios including credential management, session brokering, session recording and auditing, life cycle management, file transfers, 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, multiuser session collaboration, sponsorship and delegated administration, identity federation and access requests for remote privileged users.

- **Workload identity and secrets management:** Features that enable management and brokering of access to credentials (such as passwords, OAuth tokens and SSH keys) for nonhuman use cases, such as machines, applications, services, scripts, processes and DevOps pipelines. It includes the ability to generate, vault, rotate and provide a credential to nonhuman entities (for example, via an API). It also includes the ability to broker trust between different nonhuman entities for the purpose of exchanging secrets, and to manage authorizations and related functions. It includes the optional ability to establish trust with a nonhuman entity 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 secrets management for dynamic environments and robotic process automation platforms. This also includes optional analytics to determine

1/21/25, 6:06 PM

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

- **UNIX/Linux privilege elevation and delegation management**: Features to provide host-based functions 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.

- **Windows privilege elevation and delegation management**: Features to provide host-based functions 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 an 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 (at a kernel or process level). Level of support may vary by platform (Windows).

- **Ease of deployment, maintenance and adjacent system integration:** This includes functions and features that simplify the deployment of the PAM solution while ensuring ease of administration and maintenance. This also requires the ability to provide functions and features to integrate and interact with adjacent security and service management. 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

  - Vulnerability management

- **Performance and availability:** This includes functions and features that track performance and provide granular authorization capabilities (e.g., role-based access control) to the PAM tool. It also provides functionality that allows the PAM tool to provide redundancy for disaster recovery (DR) or business continuity (BC) 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 (for when the PAM tool is not available) in the case of self-managed tools. This capability further provides the ability to rapidly scale the product for on-demand requirements.

- **Just in time (JIT) PAM methods**: Features to provide 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, or the use of ephemeral accounts or security tokens. JIT PAM focuses on compliance with the principle of least privilege and subsequently achieving zero standing privileges for PAM access.

- **Cloud infrastructure entitlement management (CIEM)**: Features to manage 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 tools use analytics, machine learning (ML) and other methods to detect anomalies in account entitlements, like 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 AliCloud, Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure.

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 to continue to offer and invest in its PAM product, continue offering the product, and continue advancing the state of the art within the organization's portfolio of PAM products. Factors considered include the overall financial health of the organization based on overall size, its profitability and its liquidity. A vendor's viability in the PAM market is also evaluated 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. Vendors were evaluated on how they measure the

maturity of a PAM implementation, and how they have 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 vendors measured the impact of their 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 included 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 has passed since the initial deployment. Methods to measure and incorporate customer satisfaction and feedback into existing processes were also 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, internal processes as well as availability (in terms of uptime) for SaaS-based offerings.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Product or Service	Medium

Evaluation Criteria ↓	Weighting ↓
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	Medium
Operations	Low

Source: Gartner (September 2024)

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 identify market trends and changes.

Marketing strategy: Evaluates whether a vendor's messaging is clear and differentiating, while being consistently communicated internally, and 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 a 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, a vendor's ability to enable its sales force, both internally and externally, was evaluated.

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 will offer value for customers and will differentiate a vendor's 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, a vendor's ability to establish and maintain partnerships (with adjacent technologies, value-added resellers and systems integrators) was reviewed, along with its ability to leverage them as part of an overall business plan. In addition, 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 (sales and product development, for example), 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 sizes of organizations; the vendor's understanding of the varying needs and requirements 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 (supporting processes and implementation programs, for example) 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. Vendors were evaluated on their presence in international markets, and changes that support the spread of their 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.

Table 2: Completeness of Vision Evaluation Criteria

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

Source: Gartner (September 2024)

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. 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, a limited investment in PAM, or a geographically limited footprint. Or they may focus on other factors that inhibit them from providing a broader set of capabilities to enterprises. However, this does not reflect negatively on the vendor's value in the more narrowly focused service spectrum. Niche Players can be very effective in their area of focus.

Context

Pricing and Negotiation Guidance

There are a number of considerations when it comes to pricing. First is the license model for different PAM tools — PASM, PEDM, RPAM, secrets management and CIEM:

- PASM tools are primarily sold on a per-privileged-user license model. A "privileged user" here means a person that can be granted privileged access to one or many target accounts. RPAM tools are primarily sold on a per-remote-privileged-user model. PASM and RPAM tools are typically not licensed on the basis of the number of privileged accounts on target systems. However, some vendors offer their PASM and RPAM tools on a per-asset (i.e., target system) license model or a combination of per-user and per-asset license model.

- PEDM tools are primarily sold in a per-asset license model.

- Secrets management tools are mostly sold on the basis of the number of "users" (where each user is an application with its distinct account in the secrets manager), or per-application clusters, workloads or secrets.

- CIEM tools are sold in a per-managed-target (cloud tenant) or per-SaaS-application model.

Second, from a delivery options perspective, many PAM vendors now provide a SaaS delivery option for their tools. These options are largely licensed on a per-privileged-user or per-asset-license basis, with an annual subscription. Several PAM vendors have stopped offering perpetual licensing for their products in the last two years, and are selling software only on a subscription basis. However, some of those vendors have started offering perpetual licenses again after losing opportunities.

Some vendor licenses are based on privileged users, some are based on assets, and some will license both. If both options are available, consider licensing based on whichever component is projected to change less in your environment. If the number of users is projected to change less, license your users. If the number of targets is projected to change less, license your targets. Due to evolving architectures, most organizations will find that the number of users tends to change less.

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 to 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 — can take 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.

IAM leaders responsible for choosing a PAM solution should use some general negotiation tips, as listed below:

- **Acquire licenses needed for the current volume:** Negotiations for potential future license increase should be done upfront, to take advantage of potential discounts for higher volume numbers as they happen, and to limit uplifts when the contract is extended. Once a contract has been signed, and the base product has been deployed, the vendor's incentive to offer discounts for additional licenses is drastically reduced. Negotiate discounts on the basis of the length of the term. Three years has become the standard, but there are exceptions being accepted for shorter terms. Contracts longer than three years should only be considered if significant discounts are offered. Look for volume discounts on individual products based on term length, number of products bought, and volume for which the products are being bought to get effective pricing.

- **Leverage third-party advice, such as Gartner BuySmart, before signing contracts:** Contracts and proposals grow more complex every year. Vendors introduce new pricing, licensing models, maintenance options and audit clauses every day. Unless one has day-to-day market visibility, it is nearly impossible to keep up.

- **Review vendor packaging deals:** To address your PAM requirements and get effective volume discounts on each product, look for pricing breakdowns for the individual products or modules to be bought. Be wary of "all-inclusive package pricing" that does not individually list the price for each component. Experience has shown that it is virtually impossible to drop an unused component later on. Always consider the latest bundled packages, and do not just renew existing toolsets. Don't expect the vendor or value-added reseller (VAR) to suggest lower-cost or more-inclusive packages unprompted.

- **Start renewal negotiations early:** If negotiations are stuck, switching vendors and products may be an alternative, but only if there is enough time. Gartner recommends renewal negotiations should begin at least six months before the contract expiration date, and earlier for complex or larger installations. This will provide enough time for competitive bidding and migration planning, if desired. Late renewal negotiations shift the advantage to the incumbent vendor, because there is not enough time to seriously consider switching to an alternative.

Just in Time Privilege (JITP) Tools (PAM Alternatives)

Gartner is witnessing an increasing traction for this new class of tools in the PAM space as companies seek to mitigate the risk of privileged access. The reason for their popularity is because they address much of the visibility and discipline of PAM, while providing an easy and frictionless user experience. While JITP tools are closely adjacent to both PAM and RPAM tools, they have some unique features that make them different:

- **Usability:** These are agent-based tools, meaning that interacting with them is automatic. No more logging into a PAM tool to check out an account, simply launch a privileged RDP, HTML, or SSH session, (along with MFA authentication), and the tool takes care of the privilege elevation and activity logging according to an organization-defined policy.

- **Users:** While traditional IT administrators are still a better audience for conventional PAM tools due to the flexibility of the integration patterns and the far higher number of use cases for privileged access, developers, engineers, and other IT specialists are the primary targets for JITP tools. While these tools can likely serve remote contractors and vendors, they are primarily being marketed for internal IT staff. Traditional PAM tools require integrations with any device or piece of software requiring controlled privileged access. However, due to the more limited use patterns of developers and other IT specialists, the integration surface for JITP tools is also more limited, significantly reducing the implementation and onboarding time.

While JITP tools are also lacking features like vaulting and credential rotation compared to either PAM or RPAM tools, they do what they do very efficiently. It is that efficiency in both implementation and use that is driving their popularity.

Note that Gartner does not recommend solely using a JITP tool to mitigate PAM risk, as the vast majority of environments will have requirements (the existence of local admin or root, for example) that will require additional, traditional PAM capabilities like vaulting and credential rotations. However, clients should investigate their need for privileged access and factor in the use of JITP tools. Sample vendors include Apono, Okta, SSH.com, StrongDM and Teleport and some others.

Expanded Drivers for PAM

For the third year in a row, a significant minority of clients are telling Gartner that cybersecurity insurers require clients to have a strategy for managing privileges in their environment. This adds to the traditional drivers for PAM, which are 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 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.

Endpoint PAM

Malware and especially ransomware have been particularly impactful and costly for the market over the past couple of years. In this year's PAM research, we have expanded the topics covered to PAM for endpoints. We evaluated the capabilities provided for developing allow/deny policy templates for different types of users, and whether the tool for servers is truly different from the tool for endpoints. Endpoint PAM is a mature market that continues to grow. Adjacent markets, like endpoint protection platforms and unified endpoint management, sometimes offer PAM features in the form of endpoint privilege management. These can potentially be a replacement for (or alternative to) PEDM tools from PAM vendors for endpoint use cases.

Applying a Risk-Based, or Minimum Effective, Security Model to PAM

PAM is hard due to many disparate use cases and different types of privileges, such as accounts and entitlements, across an organization's IT landscape. PAM also introduces friction to user communities because it changes the way they access systems. The best way to mitigate this impact — and to balance cost, operational impact and security — is to take a risk-adjusted approach to PAM practices.

For example, if a significant part of an intellectual property is contained on Linux servers, and yet spending and effort are primarily devoted to Windows servers, that would indicate an out-of-balance PAM approach. If the biggest risk of exposure is regulated data, like personally identifiable or personal health information, but the biggest spend and efforts are focused on the service desk, that might also indicate an out-of-balance approach to PAM.

To take a risk-adjusted approach to PAM, first conduct in-depth account discovery across all PAM use cases, for all kinds of users (human and machine) and for all environments (on-premises, IaaS and SaaS). From that comprehensive discovery and categorization of PAM use cases, begin assigning risk for access, from the most risky to the least risky. Then construct a PAM practice, as part of a broader IAM program, that focuses on the use cases that introduce the most risk to the business. Remember, sometimes getting to 80% to 90% of risk mitigation is okay, especially if getting the last 10% to 20% requires spending double what has already been spent, but does not result in a corresponding security benefit for the business.

Workforce Password Management Tools and PAM

Workforce password management tools (WPM) focus on providing a secure password storage system. These tools are concerned with protecting passwords, not privileges. WPM tools are designed to simplify application login for the general workforce by creating, storing and retrieving passwords, while giving organizations more control and visibility over password usage across the organization. Access to these tools requires a master password or a FIDO2 security key (or where possible integration with a single sign-on [SSO] solution, such as an access management [AM] tool). There are many vendors in this market, among which the ones most often cited in client interactions include: 1Password, Bitwarden, Dashlane and LastPass. However, WPMs should not be confused with PAM tools, and should not be used to manage privileged access (see Innovation Insight: Workforce Password Management Tools).

While WPM tools can programmatically generate, store and retrieve passwords, and in some use cases share passwords between vaults, they lack the robust security features needed to manage and control privileged access. PAM tools on the other hand, are designed to protect and manage access (not just passwords) for privileged accounts specifically, ensuring that privileged access is tightly governed.

Notably, WPM tools fall short in the following areas:

- They do not provide features to discover, map and report privileged accounts on multiple systems, applications and devices.

- They cannot manage credentials for service accounts, such as noninteractive accounts used to run services, applications and scripts.

- They do not provide JIT elevation features, and generally do not manage privileged entitlements.

- They do not allow a privileged session to be automatically established using protocols such as SSH, RDP or HTTPS without revealing credentials to the user. In some cases, they provide minimal capabilities such as injecting credentials into a web form.

- They cannot fully record and allow auditors to review sessions, nor manage live sessions by allowing them to be accompanied or terminated.

- They cannot broker credentials to software, thereby allowing the elimination of clear-text credentials in configuration files or scripts.

- They lack analytics and reporting of privileged accounts and their use (for example, discovering unauthorized use of privileged credentials or reporting on unusual activities).

Market Overview

Gartner's expanded definitions of the five distinct tool categories for PAM tools:

- **Privileged account and session management (PASM):** Privileged accounts are protected by vaulting their credentials. Access to those accounts is then brokered for human users, services and applications. Privileged session management (PSM) functions establish sessions with possible privileged credentials' injection into sessions, and full session recording. Passwords and other credentials for privileged accounts are actively managed, such as being changed at definable intervals or after specific events. Optionally, PASM solutions can also provide application-to-application password management (AAPM) and/or zero-install remote privileged access features for IT staff and third parties that do not require a VPN.

- **Privilege elevation and delegation management (PEDM):** Specific privileges are granted on the managed system by host-based agents to logged-in users. PEDM tools provide host-based command control (filtering), application allow/deny/isolate controls, and/or privilege elevation which allows particular commands to be run with a higher level of privileges. PEDM tools must execute on the actual operating system (kernel or process level). Command control through protocol filtering is explicitly excluded from this definition, because the point of control is less reliable. Optionally, PEDM tools can also provide file integrity monitoring features.

- **Remote privileged access management (RPAM):** RPAM tools enable access for remote privileged users through session brokering, credential injection/vaulting and strong authentication capabilities, which mitigate many of the risks of unmanaged devices employed by those users. These tools also provide controls for establishing, monitoring and recording remote privileged sessions to specific targets and eliminate the need for VPN and provide more secure access to critical systems. The tools also enable alignment with zero-trust architectures, because there is no implicit trust in corporate networks or endpoint devices. Most stand-alone RPAM tools offer multifactor authentication (MFA) features to provide effective protection against account takeover (ATO) threats.

- **Secrets management:** Credentials (such as passwords, OAuth tokens and Secure Shell [SSH] keys) and secrets for software and machines are programmatically managed, stored and retrieved through APIs and software development kits (SDKs). Trust is established and brokered for the purpose of exchanging secrets and to manage authorizations and related functions between different nonhuman entities such as machines, containers, applications, services, scripts, processes and DevSecOps pipelines. Secrets management is often used in dynamic and agile environments such as IaaS, PaaS and container management platforms.

- **Cloud infrastructure entitlement management (CIEM):** An adjacent cloud security area, CIEM offerings provide administration time controls for the governance of entitlements in hybrid and multicloud IaaS. This helps mitigate identity risks associated with permissions to virtual infrastructure (IaaS). CIEM solutions typically use analytics, machine learning (ML) and other methods to detect anomalies in account entitlements, like accumulation of privileges, and dormant and unnecessary entitlements. CIEM provides remediation and enforcement of least privilege approaches in cloud infrastructures.

Market Size and Drivers

Gartner estimates that the PAM market revenue for 2024 will amount to $2.37 billion, representing a growth rate of 10% over 2023. The market will continue to witness expansion, although growth is expected to taper off in the coming two to three years (see Forecast Analysis: Information Security and Risk Management, Worldwide).

Growth continues to be driven by the 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] In addition, regulations, the accelerated migration to cloud, automation enablement for DevOps, the blurring of enterprise security perimeters and the overall increase in the number of cyberattacks contribute to the growth of PAM adoption. Also, 15% to 25% of Gartner clients that evaluate PAM tools for first-time purchase, state that they are doing so because their cybersecurity insurance requires the deployment of such tools.

The PAM market also continues to profit from interest in remote access for vendors and remote external IT staff. Enabling privileged remote access using PAM tools (rather than pure-play remote access tools without privileged controls) is the recommended best practice to meet requirements and mitigate security risks. This has resulted in increased sales of dedicated RPAM tools. Vendors, accordingly, have prioritized development of remote access over other features.

Another interest is in secrets management, which brings PAM additional buyers (software development and cloud operations).

Small and midsize businesses (SMBs) face the same challenges as large and midsize enterprises — albeit on a smaller scale. PAM adoption has reached maturity for large and midsize enterprises, and vendors are now increasing their focus on SMBs as they increasingly realize the criticality of PAM implementations. With this evolution, Gartner is seeing a shift toward the adoption of SaaS solutions, albeit with regional variations and, in some cases, managed service offerings.

Many early adopters of PAM — the large enterprises — are looking to increase their PAM maturity to extend beyond basic use cases. To address these advanced needs, vendors have made further investments in capabilities such as secrets management, JIT PAM, privileged threat detection and reporting of privileged activities and management of privileges in multicloud environments. For some of these capabilities, PAM vendors also face stiff competition from vendors outside the

core PAM market, such as those that offer stand-alone secrets management, RPAM or CIEM products.

Market Dynamics

We continue to see more vendors offering a SaaS option. This year, of the nine vendors included in the research, six have a SaaS option, and one has it in its roadmap. Two vendors have no current or planned SaaS option.

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. Five of the nine included vendors offer a secrets management tool for developer use cases, and the other four have developed some basic secrets management features in their products. In addition, we have seen four vendors offering a CIEM tool, with some adding CIEM in its portfolio through acquisitions, like Delinea acquiring Authomize. Two out of the four offering CIEM have some CIEM capabilities included within their broader PAM solution, and two are currently roadmapping the capability.

Geographic and Vertical Trends

North America and Europe remain the primary markets for PAM products. However, the APAC region has exhibited increased interest and sales. Global enterprise vendors — such as Broadcom (Symantec), CyberArk and, somewhat aspirationally at the moment, BeyondTrust and Delinea — are increasingly attempting to extend their geographic reach to all regions. Once there, they'll be met by strong regional vendors: ARCON in the Middle East and APAC, senhasegura in Latin America, and WALLIX in Europe. While 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 CPS (cyber-physical systems). Examples include companies in the utilities and energy sectors, and hospitals. These organizations need to secure privileged access to their supervisory control and data acquisition (SCADA) and OT devices, and require preconfigured connectors to popular OT systems.

Evidence

[1] We have ample anecdotal evidence from clients that cybersecurity insurers either raise premiums in the absence of a deployed PAM tool, or will refuse the insurance altogether (see also How to qualify for cybersecurity insurance, Expert Insights.

[2] Verizon's 2024 Data Breach Investigations Report, for example, lists stolen credentials and privilege misuse as contributing factors in many breaches covered in the report.

Note 1: Pricing

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 two highest price points (out of nine vendors).

- **Well-below average** includes the two lowest price points.

- **Above average** are prices above the average price point but below the two highest prices.

- **Below average** is below the average price point, but above well-below price points.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor'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.

Market Responsiveness/Record: 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.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

About   Careers   Newsroom   Policies   Site Index   IT Glossary   Gartner Blog Network   Contact   Send Feedback

Gartner