Magic Quadrant for Privileged Access Management

Published 5 September 2023 - ID G00776445 - 61 min read

By Felix Gaehtgens, James Hoover, **and 3 more**

PAM products are now mainstream, but organizations struggle with adoption beyond the basic controls, which some vendors address better than others. Support for account discovery and machine identity management, pricing and licensing terms also continue to be uneven. HashiCorp enters the PAM space.

Market Definition/Description

Gartner defines privileged access management (PAM) as tools that manage and protect accounts, credentials and commands that offer an elevated level of technical access, that is, administer or configure systems and applications. Available as software, SaaS or hardware appliances, PAM tools manage privileged access for 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): Vaulting of privileged account credentials, and session management for privileged usersPrivilege elevation and delegation management (PEDM): Host-based agents that provide command; filtering and privilege elevation for users on macOS, UNIX/Linux and Windows. Secrets management: Specialized vault focused on managing credentials for software and workloads. Cloud infrastructure entitlement management (CIEM): Management of entitlements used in cloud service provider (CSP) infrastructure.

Privileged access is access beyond the level granted to normal business users. It allows users to override existing access controls, change security configurations, or make changes affecting multiple users or systems. Privileged access can create, modify and delete IT infrastructure, along with company data contained in that infrastructure, so it carries catastrophic risk. Managing privileged access is thus a critical security function for every organization. Regular user access controls cannot effectively manage privileged access, so special procedures and tools are required. PAM tools roughly fall into two categories: those that focus on privileged accounts and those that focus on privileged commands.

PAM tools focused on privileged accounts help organizations discover privileged accounts used by people and machines. The 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 zero-trust remote access through session control mechanisms to enable privileged account use without disclosing their credentials. For noninteractive accounts used by machines, PAM tools secure the handling of privileged credentials so that they are not exposed at rest. This often requires collaboration from (and changes to) applications and code. Typical examples of machine accounts are service accounts and automation accounts used for DevOps and modern cloud development use cases.

The second category of PAM tools provides 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.

All PAM tools provide visibility and observability into privileged account and command usage by tracking and recording privileged access for auditing. This can include detailed session recording to help understand not only who used which privileged account when, but also what they were doing.

The combination of technical controls provided by PAM tools can implement just-in-time privilege management to enforce the principle of least privilege: Users must have only the minimum level of privilege for just the time needed to accomplish a specific objective.

The must-have capabilities for PAM are:

- Offering 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 (i.e., system administrators, operators, help desk staff, and so on) on a temporary basis.

Standard capabilities include:

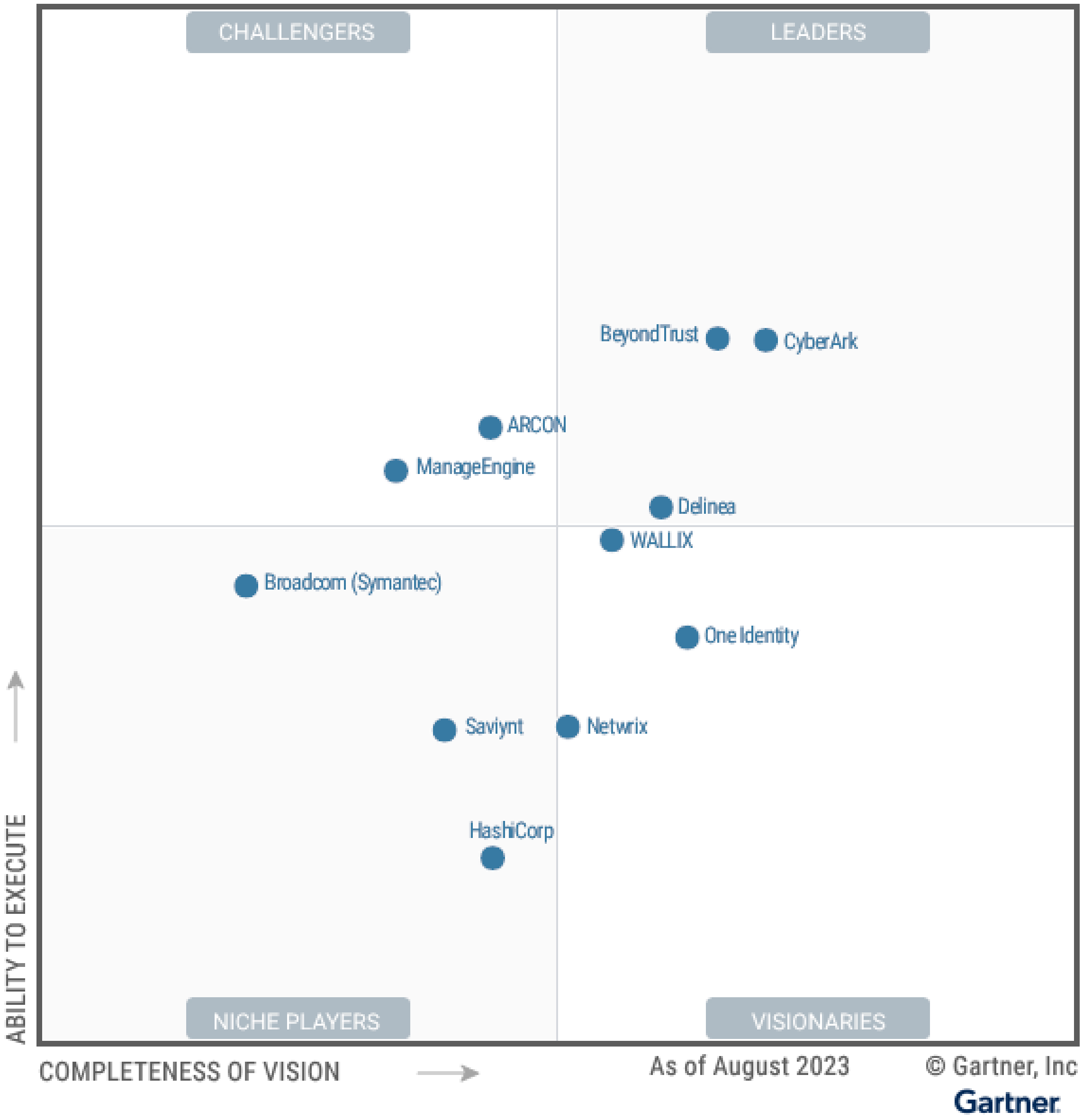
- Credential vaulting and management for privileged accounts.
- Agent-based controlled privilege elevation for commands executed on Windows, UNIX/Linux or macOS operating systems.
- Privileged account discovery across multiple systems, applications and cloud infrastructure providers.
- Management, monitoring, recording, and remote access for privileged sessions.
- Auditing capabilities to ascertain who used what privileged access when and where.

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.
- Just-in-time privilege management to reduce the time and scope that a user is granted a privilege to the minimum possible.
- 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 the ARCON PAM Enterprise for privileged account and session management, and ARCON EPM for privileged elevation and delegation management. ARCON also offers several additional products and modules, including secrets management and application-to-application password management (AAPM), connectors to DevOps infrastructure tools, and cloud infrastructure entitlement management (CIEM). Its operations are mostly focused in APAC and EMEA, although the vendor is expanding its base in the U.S. ARCON is one of a few PAM vendors that also has a technically differentiated offering for operational technologies (OT). Roadmap items this year are focused on making PAM easier to use and providing additional convergence with the vendor's other identity and access management (IAM) tools.

Strengths

- Product: ARCON's offering is the most capable of all vendors evaluated, with every capability evaluated above — and often well-above — the average.
- Pricing: ARCON's pricing is competitive. In most pricing scenarios, especially around PASM, ARCON is more affordable than other vendor offerings in this research. In AAPM and PEDM scenarios, pricing is around average and sometimes higher than average, especially for its software offering.
- Customer experience: ARCON staffs its customer relationship management team with customer success managers for each customer. Even the most basic support package offers 24/7 support.
- Market responsiveness: Since last year's Magic Quadrant, ARCON introduced additional capabilities for collaboration in session management and incident management. It also introduced starter kits that simplify adoption of the product.

Cautions

- Product: The most common complaint Gartner heard from ARCON's clients is related to the overall user interface. Some also mentioned session management performance and the overall upgrade process.
- Marketing and sales: ARCON is lagging behind Leaders in this research in marketing and sales efforts to gain new customers.
- Geographic strategy: ARCON's footprint in the Americas is small, with only a few deployments.
- Product roadmap: ARCON's product roadmap is mostly focused on convergence with its own IAM products, as opposed to focusing on innovation in core PAM functionality (like simplifying implementations with toolkits).

BeyondTrust

BeyondTrust is a Leader in this Magic Quadrant. PASM services are provided by two products, Password Safe (PS) and Privileged Remote Access (PRA), both available as SaaS, or software as a hardware or virtual appliance. Those two products are sold separately, but BeyondTrust now offers them in a bundle called Total PASM, and

Gartner has evaluated it as such. PEDM functionality is provided by its Privilege Management products, which are available as software (UNIX/Linux, macOS and Windows) and SaaS (for macOS and Windows). BeyondTrust also provides Active Directory (AD) bridging tools as software. Secrets management used to be a stand-alone product but has now been bundled into Total PASM. BeyondTrust also offers CIEM functionality with its Cloud Privilege Broker tool. BeyondTrust customers are geographically diversified, with large concentrations in North America and Europe.

Strengths

- Product strategy: The bundle of PS and PRA provides strong capabilities, especially in the areas of account discovery and onboarding, privileged session management and remote access. However, the same is not true if only one of those products is deployed: PRA is focused on privileged session management, which the stand-alone version of PS is not strong in.
- Product: BeyondTrust is best in class for UNIX/Linux and macOS PEDM, and a top performer for Windows PEDM. For the Total PASM bundle, clients comment favorably on discovery capabilities, smart rules, and ease of use.
- Customer experience: BeyondTrust is very engaged with its customers, with multiple teams from customer success to technical support.
- Market responsiveness: BeyondTrust has added zero trust network access (ZTNA) capabilities to its PRA product, and now offers a capable IT infrastructure access tool for developers and engineers. It also added more tools to help customers measure their PAM maturity levels.

Cautions

- Product: For workload identity and secrets management, BeyondTrust continues to disappoint, with little innovation and lacks support for native authentication methods and integration with DevOps technologies.
- Offering strategy: Roadmap items for BeyondTrust are less focused on needed improvements in core PAM capabilities such as just in time (JIT) use cases, and more focused on edge cases like CIEM and managing passwords for business users.
- Product: Clients point out a cumbersome upgrade process for software versions.
- Pricing: BeyondTrust’s pricing remains higher than the market average, especially for its software PAM offerings.

Broadcom (Symantec)

Broadcom (Symantec) is a Niche Player in this Magic Quadrant. Broadcom is a large software company, offering a PAM solution that has been rebranded multiple times and is now offered under the Symantec banner. Symantec offers PASM functionality through a product called Symantec Privileged Access Management, which is available as a virtual or hardware appliance. Its PEDM product, called Symantec Privileged Access Management Server Control, is only available as software. Broadcom also offers an AAPM tool and an analytics tool, but does not offer CIEM. Symantec has significant customer populations in North America, EMEA and APAC, and has introduced basic secrets management functionality since last year's Magic Quadrant.

Strengths

- Product: Symantec offers a very competitive PEDM product for Windows, UNIX/Linux and mainframe clients. 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's PAM offering 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.
- Vertical industry strategy: Symantec supports a very diverse set of market verticals, including the public sector, with its PAM tool.
- Geographic strategy: Symantec's customer base is very diverse in terms of regions, and the company has an established global support structure.

Cautions

- Product: For complex service account credential management, Symantec relies on its Custom Connector Framework. This means that customers sometimes 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 the market.
- Customer experience: Broadcom scored lowest of all included vendors in client ratings for customer support. Customers complain about resolution times for service incidents, especially after escalations.

- Product strategy: While every other vendor in this Magic Quadrant provides (or is developing) SaaS capabilities, Broadcom has not as yet roadmapped a SaaS offering for its PAM product.
- Business model: Broadcom’s direct customer relationship focus is on its top 1,000 customers. Other clients are being offloaded to Broadcom’s partner channel.

CyberArk

CyberArk is a Leader in this Magic Quadrant. CyberArk patented vault technology over two decades ago, and was the first PAM vendor to introduce both secrets management and CIEM functionality to its portfolio. CyberArk offers PASM functionality with Privileged Access Manager (SaaS or software), PEDM functionality with its Endpoint Privilege Manager for Windows, UNIX/Linux and macOS (SaaS or software), secrets management and AAPM with Conjur and CIEM functionality with Cloud Entitlements Manager. It also offers a remote PAM tool called Vendor Privileged Access Manager. CyberArk’s operations and customer base are geographically diversified.

Strengths

- Product: CyberArk has a large partner ecosystem, and has delivered many connectors and integrations with adjacent technologies, such as IT service management (ITSM) and identify governance and administration (IGA) tools. CyberArk’s PAM products are some of the most mature in the market. It rates high for workload identity and secrets management, credential management, logging and reporting, adjacent technology integrations and automation, and CIEM.
- Overall viability: CyberArk continues to have the largest share of the PAM market. Customer and revenue growth continued to be strong since the publication of the last Magic Quadrant.
- Innovation: CyberArk has delivered a number of significant updates since last year’s Magic Quadrant, such as integrating its secrets manager with Amazon Web Services (AWS), and extending JIT functionality to cover more use cases.
- Market responsiveness: CyberArk added a feature called transparent secrets management — an enhancement for its secrets management, which allows secrets to be managed across both CyberArk and AWS secrets vaults.

Cautions

- Product: CyberArk’s PASM software remains difficult to manage and upgrade, including those on-premises bridge components that are required even for SaaS. Disaster recovery — especially failover support — is brittle, relies on manual processes and has been a source of customer complaints for a long time.
- Pricing: A common complaint from clients is about cost — CyberArk’s products are among the most expensive on the market. Clients will often require multiple products offered in different editions that are licensed separately. This makes it more complicated to select and size the right solution and predict costs, especially for multiyear deals.
- Offering strategy: For several years, CyberArk has roadmapped improvements for its aging PSM functionality — especially to increase performance and throughput — but has not yet delivered.
- Technical support: While customer experience is still positive overall, CyberArk is rated by customers in the lowest quartile for quality of technical support.

Delinea

Delinea is a Leader in this Magic Quadrant. PASM functionality is covered by the Secret Server product. Privilege Manager covers Windows and macOS PEDM. PEDM for UNIX/Linux is sold as Server PAM, Authentication Service products and AD bridging tools, available as software or SaaS. DevOps Secrets Vault is the secrets management product. A combination of these products is available through the integrated Delinea Platform (SaaS only). While there are some basic CIEM capabilities, no stand-alone CIEM product is currently offered, but one is roadmapped. Delinea’s operations are geographically diversified, although most of its clients are in North America, followed by Europe. The vendor plans to strengthen its Delinea Platform by development of common capabilities and further integration of additional products within the platform.

Strengths

- Product: Delinea has consolidated its PASM SaaS platform into three editions: Essentials, Standard and Enterprise. The last two editions notably also include licenses for a limited number of PEDM functions for servers and workstations. Delinea has a very competent PEDM offering for UNIX/Linux that scored among the top vendors of those evaluated.
- Customer experience: Clients consistently mention ease of use as one of the aspects that they like most about Secret Server and Privilege Manager.

- Offering strategy: Delinea is one of the first PAM vendors with plans to adopt two standards to help with interoperability: Secure Production Identity Framework for Everyone (SPIFFE) for PAM for machines, and elements of Open Policy Agent (OPA) for policy creation. It also plans to introduce functionality to manage Delinea and other on-premises vaults with a single management console.
- Sales/geographic strategy: Delinea recently restructured its go-to-market organization, enabling it to refocus resources and efforts. Additionally, Delinea has expanded its sales, engineering and customer success functions.

Cautions

- Product: Delinea continues to lag behind other Leaders in some capabilities. RDP session management with keystrokes and metadata recording requires installation of local agents on target servers, which most other vendors don’t require. Secret Server also lags behind other Leaders in support for advanced service account and credential management scenarios, and is especially brittle on local systems that are not permanently connected.
- Product strategy: Delinea has a strategy to present Secret Server as a “simple to deploy and use” solution. However, several fairly common requirements need customization through PowerShell, placing an additional burden on clients.
- Business model: Delinea is developing significant new capabilities to be delivered as SaaS-only, leading to an increased disparity in functionality between its SaaS and on-premises offerings.
- Operations: Overall, Delinea continued to shrink slightly in terms of employee count. The company has added some staff to R&D, but it still has the lowest ratio of employee population devoted to PAM R&D of all three Leaders in this research.

HashiCorp

HashiCorp is a Niche Player in this Magic Quadrant. The company offers a combination of its two products, Vault and Boundary for PAM. Vault covers machine identity and secrets management. Boundary provides PASM capabilities that focus on privileged session management and remote access capability with zero trust controls in combination with Vault. Both products are available as software or as a service within its HashiCorp Cloud Platform (HCP). While Vault is the subject of a significant majority of Gartner client inquiries for secrets management products, Boundary is a new offering that has allowed HashiCorp to be included for the first time in this Magic Quadrant.

HashiCorp has a significant customer base across all major market regions and is planning to add session recording, catching up with the rest of the market, and offering a self-managed (on-premises) version of Boundary. HashiCorp acquired BluBracket in June 2023, which brings secrets scanning capabilities.

Strengths

- Product and market presence: HashiCorp has the highest market share for stand-alone secrets management. Its Vault product scores among the top of all products evaluated for that capability.
- Marketing execution: HashiCorp demonstrates a keen understanding of its brand and the target personas to which it sells, including practitioners, application developers and DevOps teams.
- Customer enablement: HashiCorp offers a vast library of free resources, documentation and tutorials that is very popular and provides excellent self-paced training.
- Customer experience: Customer comments on HashiCorp Vault express an appreciation of its encryption capabilities and praise its ease of integration.

Cautions

- Product: Boundary is a new offering and still lacks many of the features and capabilities commonly found in more mature PAM products, such as privileged account life cycle management, discovery and credential management. Its session management capabilities are below the average of what is offered by other included vendors.
- Pricing: Customers mention the high cost of HashiCorp Vault as the main drawback and customers score HashiCorp lowest of all vendors for pricing and contract flexibility. In addition, pricing for Boundary is unusual, as HashiCorp charges customers on the basis of “sessions per month,” unlike any other vendor in this market that charges on a per-user or per-asset basis.
- Operations: HashiCorp laid off approximately 8% of its workforce in June 2023.
- Market responsiveness: HashiCorp’s PAM maturity model is less focused on long-term success with mitigating the risk of PAM in traditional corporate environments, and more focused on management of privileged access for DevOps use cases and a cloud operating model.

ManageEngine

ManageEngine is a Challenger in this Magic Quadrant. ManageEngine is a division of Zoho Corp., which has been in existence since 1996. ManageEngine produces a number of enterprise management software tools, including its PAM product, PAM360. That product delivers PASM and Windows PEDM functionality as software only. A less featured version of the product is also available, called Password Manager Pro. Gartner's evaluation is based on the capabilities of PAM360. Basic secrets management functionality is also a part of the PAM360 product, but it does not currently offer CIEM functionality, although that is on its roadmap. ManageEngine's operations are geographically diversified. ManageEngine has roadmapped privileged task automation capabilities and an access review process for privileged accounts.

Strengths

- Product: PAM360's discovery capabilities are extensive, offering a wide range of scanning tools for finding privileged accounts on systems, databases, infrastructure and networks. Ease of deployment, administration and maintenance are areas in which ManageEngine is strong.
- Pricing: ManageEngine pricing is now consistently less than market averages. It offers a distinct pricing model where PAM360 is licensed based on the number of PAM tool administrators (and not the number of privileged users who would like to perform administrative tasks on the target systems).
- Product strategy: ManageEngine sells a version of PAM360 for use with managed service providers that require managing privileged access to multiple customers.
- Geographic market strategy: ManageEngine is well-represented across the globe, with customer concentrations in North America, Asia/Pacific, EMEA and Latin America.

Cautions

- Product: PAM360 supports multiple connection mechanisms, including proxying, but full session management and recording is only supported through an HTML5 browser session emulation, which is resource-intensive and less scalable.
- Innovation: New product introductions since last year's Magic Quadrant were limited to feature enhancements and catch-ups in the market.
- Market understanding: While ManageEngine recognizes market trends toward cloud adoption and integration with DevOps, it still has to catch up by offering a SaaS-based solution and building out its secrets management capabilities.

- 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 Windows PEDM.

Netwrix

Netwrix is a Visionary in this Magic Quadrant. It was founded in 2006, and is known for its auditing and compliance software products. In 2022, Netwrix acquired Remediant, and merged its PAM offering with capabilities from SbPAM, which Netwrix gained through the acquisition of Stealthbits in 2021. Its PAM solution includes Privilege Secure for Access Management, its PASM product, which is available as software. Netwrix also offers Privilege Secure for Endpoint (aka PolicyPak), a Windows PEDM product that is available as software or SaaS. Neither secrets management nor CIEM functionality are supported. Netwrix customers are primarily concentrated in North America and Europe. Netwrix has additional SaaS-based discovery capabilities and new functionality for remote PAM use cases on its roadmap.

Strengths

- Product: JIT privileged access functionality is among the most capable of all vendors evaluated. The Windows PEDM product is also competitive.
- 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.
- Market responsiveness: Since last year’s Magic Quadrant, Netwrix introduced a comprehensive maturity program, helping customers measure and plan the maturity of their PAM practices, and it offers a zero-standing-privileges approach for database access.
- 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.

Cautions

- Product: For account discovery and onboarding, and credential management, Netwrix does the basics well, but has very limited support for advanced scenarios involving nonstandard service accounts, shadow admin accounts or Secure Shell (SSH) keys.

- Customer experience: Netwrix does not offer fixed-price and scope-implementation packages beyond a simple one-day “jump-start” package with an additional customized professional services engagement. On-site training is also only available through the procurement of professional services.
- Pricing: Since last year’s Magic Quadrant, Netwrix’s pricing has been simplified for its new offering; however, it is priced above average compared with the market, across multiple pricing scenarios.
- Business strategy: Netwrix acquired four companies in 2022, among them Remediant, which is now part of Netwrix’s PAM offering. While PAM product integration has made quick and large strides, the overall rapid pace of these acquisitions may create some distraction.

One Identity

One Identity is a Visionary in this Magic Quadrant. One Identity (part of Quest Software) provides PASM functionality with its Safeguard product, available through either software, hardware or SaaS; software-based PEDM functionality with Privilege Manager (for Windows, UNIX/Linux and macOS); and Safeguard authentication services for AD bridging functionality. It also offers a tool called Safeguard Secrets Vault/Broker that is not a secrets manager by itself, but acts as a frontend to other vaults and secrets managers. One Identity does not offer a CIEM product, but can provide some CIEM functionality with an adjacent IGA product. One Identity’s operations are geographically diversified. This year, One Identity introduced a remote PAM tool, SafeGuard Remote Access, for vendors and business partners.

Strengths

- Product: One Identity received one of the highest scores in the market for privileged session management and remote access, and for PEDM for UNIX/Linux and macOS.
- Customer experience: One Identity scored well in customer experience, assigning an account manager and a success manager to each One Identity account.
- Product: Customers consistently call out the ease of use and deployment for One Identity’s Safeguard products.
- Sales and geographic strategy: One Identity has new sales strategies focusing on improved partner assets. Due to a revamped vendor-to-partner information delivery system, providing immediate on-demand updates and release information, it has seen

an uptick in new partners. If executed properly, this could lead the product revenue back to growth.

Cautions

- Viability: One Identity's PAM revenue has hardly grown over the last year.
- Operations: The vendor has gone through significant changes in its executive team over the last year.
- Offering strategy: This year, One Identity's roadmap is less focused on core PAM improvements like JIT use cases. It is more focused on catch-up items, such as enhancing its privileged account discovery capabilities and adding System for Cross-Domain Identity Management (SCIM) support to simplify managing users for the PAM tool.
- 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, Active Roles is required for JIT privileged access, and the One Identity IGA tool is required to expand life cycle management and auditing.

Saviynt

Saviynt is a Niche Player in this Magic Quadrant. Saviynt was established in 2015 to bring a SaaS-based IGA tool to the market and, in 2019, Cloud Privileged Access Management (CPAM) was released. CPAM is a PASM product only available as SaaS or privately managed on infrastructure as a service (IaaS) platforms like AWS, Microsoft Azure and Google Cloud Platform (GCP). CIEM functionality is also only available as a SaaS option. PEDM functionality is not currently available. Saviynt customers are primarily concentrated in North America and Europe, and in smaller numbers in APAC. Saviynt plans to expand secrets management with native functionality and to add new tools to help track and manage access by machine accounts.

Strengths

- Product: Saviynt does well in the areas of privileged account life cycle management, account discovery and onboarding, ease of deployment, administration and maintenance, adjacent system integration performance and scalability, availability, and recoverability, and CIEM functionality.

- Product: Unique to Saviynt, CPAM users get Saviynt IGA functionality for all licensed privileged users at no additional cost.
- Customer experience: Customers consistently called out appreciation for advanced features such as threat monitoring and comprehensive JIT privilege management.
- Business model and operations: Saviynt scored well for its business model, landing new funding in the past year, and achieving FedRAMP authorization (moderate) for CPAM. It also aspires to expand its global footprint.

Cautions

- Product: Saviynt's session management capabilities are below average, lacking specialized controls for databases and file transfers. In addition, its CPAM product leverages a built-in, open-source version of HashiCorp's Vault, which places an additional burden on its operation when the solution is privately managed.
- Pricing: Saviynt's pricing is consistently among the highest of the vendors in this Magic Quadrant across multiple pricing scenarios.
- Market responsiveness: The broader PAM market addresses continuous client interest in host-based PEDM tools for UNIX/Linux and Windows, however, Saviynt does not and does not have them roadmapped.
- Product strategy: Saviynt still lacks native secrets management capabilities, although they are roadmapped.

WALLIX

WALLIX is a Visionary in this Magic Quadrant. Founded in France in 2003, WALLIX introduced its PAM product in 2007. WALLIX Bastion provides PASM functionality, and is available as software, a virtual appliance or as a managed service. WALLIX BestSafe provides PEDM functionality, and is available as software only. WALLIX also offers a SaaS-based service for remote access PAM. WALLIX does not provide CIEM functionality, and does not have it roadmapped. Customers are primarily found in EMEA, with a few located in North America. The company has invested heavily to attract and support customers that use industrial controls systems and operational technologies.

Strengths

- Product: WALLIX offers a mature and feature-rich session management product and has extensive capabilities for filtering session controls, recording and live session auditing. It also evaluated well for adjacent system integration and has advanced capabilities for managing file transfers, including the ability to authorize inbound and outgoing transfers through workflows, and automatic scanning of files.

- Product: WALLIX has a best-in-class tool for OT/process control networks with the ability to tunnel through proprietary OT protocols.
- Pricing: Pricing is highly competitive, with quotes below the average for all evaluated scenarios.
- Customer experience: Clients often highlight efficient and timely support, and also comment positively on the solution’s ease of use.

Cautions

- 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 as it is focused mostly on AD scanning.
- Operations: While the overall number of employees remained essentially the same, Gartner has noted a reduced number of staff devoted to R&D compared to last year.
- Product strategy: SaaS versions of the Bastion and BestSafe products have been on the roadmap for several years now, and investments in PAM seem to be mainly focused on expanding the functionality of the OT PAM offering.
- Geographic strategy: Although WALLIX is popular in EMEA, its footprint in other regions is still small.

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

- HashiCorp

Dropped

- Bravura Security (Hitachi ID) was dropped from this year’s Magic Quadrant because it did not meet the inclusion criteria for $25 million in annual revenue.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for vendors to have to be in this Magic Quadrant. To qualify for inclusion, vendors must provide a solution that satisfies the following technical criteria.

The vendor’s solution must meet at least three out of five categories as of 12 April 2023, which are:

- Credential vaulting for privileged accounts, including:
    - 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.
- Session management and remote access capabilities, including:
    - Allowing a privileged session to be automatically established using protocols such as SSH, RDP or HTTPS without revealing credentials to the user.
- Secrets management, including:
    - Tools that broker credentials to software, thereby allowing the elimination of clear-text credentials from configuration files or scripts.
- Agent-based controlled privilege elevation for Windows, UNIX/Linux or macOS.
- Cloud infrastructure entitlement management, including:
    - Support for at least two of the following cloud infrastructure and platform services: AWS, Microsoft Azure GCP.

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: 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 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 the 2023 PAM Magic Quadrant, the respective vendors must also meet one of the following criterion:

- Have booked total revenue of at least $25 million in FY22* for core PAM capability products and subscriptions (inclusive of maintenance revenue, but excluding professional services, consulting and any SI support revenues), OR
- Have a minimum of 1,000 paying customers (“unique client logos”) that have acquired the vendor’s PAM tools that cover the entirety of core PAM capabilities, OR
- Rank in the top 10 vendors in Gartner’s Customer Interest Indicator for Privileged Access Management compiled by Gartner Secondary Research Service for the PAM market in March 2023.**

* Annual revenue and customer numbers, as applicable to criteria A and B, imply revenue or total number of customers as of 2022 from PAM software licensing and subscription only. This does not include professional services, free trial users and other non-PAM software licenses such as enterprise or personal password management or access management. Calendar year 2022 is considered if total revenue for FY22 is not available. SaaS subscription includes contract value (CV) for a calendar year but excludes any services included in an annual contract. For multiyear contracts, only the CV for the first 12 months is considered. All revenue is converted as USD constant

currency to neutralize the effect that foreign exchange rates can have on revenue. The default accounting standard is generally accepted accounting principles (GAAP).

** For the 2023 PAM Magic Quadrant, Gartner has calculated an overall customer interest indicator (CII) for PAM vendors based on a combination of factors that demonstrate customer sentiment, customer engagement and customer interest.

Honorable Mentions

Apono offers a service under the same name that is focused on brokering JIT privileged access to cloud resources for developers and administrators. It uses contextual automated authorization policy and workflows to determine whether access can be granted and if approvals are required. Apono also helps visualize cloud and Kubernetes RBAC authorizations. Apono did not meet the inclusion criteria for revenue.

Bravura Security (formerly Hitachi ID) offers PASM functionality through the Bravura Privilege product, a software-delivered PAM tool with solid capabilities for discovery and credential management, including out-of-the-box connectors for service accounts. Bravura Security did not meet the inclusion criteria for revenue.

Fudo Security sells Fudo Privileged Access Management (PAM), a PASM product with advanced session management capabilities. These include AI-based behavioral analytics, leveraging mouse movement, keyboard typing, and command analysis to detect and mitigate threats. Fudo Security did not meet the inclusion criteria for revenue.

Imprivata sells Privileged Access Management, a PASM solution that also features several protocol-level proxies — RDP, SSH, SQL, HTTP(s) and AWS CLI — that support filtering for common remote access protocols and databases. Imprivata did not meet this Magic Quadrant’s inclusion criteria for revenue.

Kron Technologies sells multiple products as software under the Kron PAM brand that offer PASM capabilities as well as PEDM capabilities for UNIX/Linux and Windows. Several capabilities are also available “as a service” under the Cloud PAM brand. Krontech did not meet the inclusion criteria for revenue.

Microsoft offers several PAM features in its offerings. Microsoft Entra ID P2 (formerly Azure Active Directory Premium P2) contains a privileged identity management (PIM) capability 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. A similar mechanism is available for Microsoft 365. Microsoft Entra Permissions Management is a CIEM solution that supports the Azure, AWS and GCP IaaS platforms. In addition, Microsoft offers a Local Administrator Password Solution (LAPS) that stores passwords for local administrator accounts in Active Directory and makes them available to administrators upon approval. Microsoft has also recently (April 2023) released Microsoft Intune Endpoint Privilege Management, with Windows PEDM capabilities as part of the Microsoft Intune Suite and as an add-on to any plan that includes Intune P1. Although it supports some aspects of PAM, Microsoft did not meet the technical inclusion criteria.

Sectona has a PAM offering called Sectona Security Platform, which is only available as software. Sectona offers PASM capabilities, PEDM capabilities for Windows and a remote access functionality on the same platform. Sectona targets the midsize and large enterprise market with a competitive license model. Sectona did not meet the inclusion criteria for revenue.

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. senhasegura did not meet the inclusion criteria for revenue.

StrongDM provides a SaaS-based solution 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. StrongDM did not meet the inclusion criteria for revenue.

Teleport takes a different approach to PAM in multicloud scenarios. Instead of relying on managing credentials, it enforces strictly identity-based access by creating a virtual privileged access mesh and targeting four main access use cases: SSH, Kubernetes, web applications and databases. Teleport did not meet the inclusion criteria for revenue.

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 includes the ability to automatically discover target services and systems (including virtual machines) for further discovering privileged accounts contained on them.
- Privileged credential management: This capability provides core features and functions 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 and remote access: This capability provides session establishment, management, recording and playback, real-time monitoring, protocol-based command filtering, and session separation for privileged access sessions. It includes 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, this credential is not disclosed to the user. It also includes VPN-less secure remote privileged access capabilities.
- Workload identity and secrets management: This capability provides the ability to manage access to credentials (such as passwords, OAuth tokens and SSH keys) for nonhuman use cases such as machines, applications, services, scripts, processes and DevSecOps pipelines. It includes the ability to generate, vault, rotate and provide a credential to nonhuman entities (via an API, for example). 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. Additionally, 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 support robotic

process automation platforms. This capability also includes optional analytics to determine whether workload accounts are potentially abused or no longer in use, and the management of secrets in other secrets management products.

- Privilege elevation and delegation for UNIX/Linux: 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.
- Privilege elevation and delegation for Windows: This capability provides host-based functions and features for enforcing policies on Windows systems that implement application allow/deny/isolate controls, and to permit 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 these tools, preventing administrators from carrying out unsafe activities. These features must execute on the actual operating system (kernel or process level). Windows PEDM tools can optionally also provide file integrity monitoring features.
- Ease of deployment, administration and maintenance, 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 also requires the ability to provide functions and features to integrate and interact with adjacent security and service management capabilities. 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 ITSM systems, security information and event management (SIEM) systems, and vulnerability management.
- Scalability, authorization, availability and recoverability: This capability provides functions and features that track performance, and provide granular authorization capabilities, (RBAC) to the PAM tool. This capability also provides functionality that allows the PAM tool to provide redundancy for disaster recovery or business continuity purposes through SaaS architecture, or through native or third-party mechanisms for load balancing and “break glass” features in the case of self-managed tools. This

capability further provides the ability to rapidly scale the product for on-demand requirements.

- JIT 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. This capability is focused on compliance with the principle of least privilege and subsequently achieving zero standing privileges (ZSPs) for PAM access. JIT use cases include the ability to:
  - Dynamically add and remove users from security groups
  - Create and use ephemeral tokens
  - Unlock privileged accounts for a limited time and then lock them again
  - Create and delete privileged accounts on demand
- Cloud infrastructure entitlement management: 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 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, AWS, 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, profitability and 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: This 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.

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 emerging needs of customers, evolving regulations and competitor activities.

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 impact of marketing activities. The vendors' ability to promote themselves 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 upsell capabilities 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 and other Gartner client feedback.

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 (uptime) for SaaS-based offerings.

Table 1: Ability to Execute Evaluation Criteria

Enlarge Table

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

Evaluation Criteria	Weighting
Operations	Low

Source: Gartner (September 2023)

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 privileged access management 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 the “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

Enlarge Table

Evaluation Criteria	Weighting
Market Understanding	Medium
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 2023)

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 and 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

Expanded Drivers for PAM

For the second 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, 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 of first-time PAM purchases that would have otherwise not happened at this time.

Remote PAM Use Cases

Many clients are interested in the role that PAM plays for their remote vendors, contractors and other external technicians.[2] Even prior to global lockdowns from the COVID-19 pandemic, clients had concerns about how remote access played into their PAM strategy. Outsourcing core IT services has long been a common practice in the market. This encompasses server administration and database administration, and especially supporting the unique requirements of process control environments in critical infrastructure (industrial control systems/SCADA) and similar environments. In terms of remote access for external technicians, many organizations historically accepted the risk of providing VPN access to support these use cases. However, using only VPNs to enable and control remote privileged access leaves significant security gaps that have been exploited.[3]

To address these security concerns, interest in and adoption of remote PAM tools have grown. Beyond the initial remote PAM tools from BeyondTrust (Privileged Remote Access) and SecureLink (now part of Imprivata), we have seen CyberArk (Alero), One Identity (SafeGuard remote access) and other PAM vendors introduce remote PAM tools. WALLIX has produced very capable tools for managing PAM in those challenging process control environments. The same vendors introduced functionality similar to zero-trust network access tools in their remote PAM tools, going beyond simple SSH and RDP access to allow tools on a remote workstation to function in the client environment.

In addition, we have seen tools introduced into the market that are focused on the use case of managing remote privileged access for developers and engineers to cloud infrastructure, specifically to support DevOps initiatives. To make this process much simpler and easy to implement and manage, HashiCorp, as well as our honorable mentions, Apono, Teleport and StrongDM, offer specialized tools that enable remote access. These tools also allow organizations to implement controls that manage and apply policy to those privileged access use cases.

How should these trends affect organizations' thinking about vendor selection for PAM? Remote access and DevOps-driven use cases such as the ones mentioned above are easiest to address with a focused solution. However, these focused solutions usually lack depth around general-purpose PAM controls (such as those provided by vendors in this Magic Quadrant).

To make the best decision for your organization, balance the priorities of a DevOps- or remote-access-focused solution versus a general PAM approach by keeping in mind that:

- Focused solutions may eventually mature to include broader, more general PAM requirements.
- General PAM vendors have already added, or are in the process of adding, specialized features to support the focused use cases described (usually as separate modules at extra cost).

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. We expect the need for endpoint PAM to continue to grow, especially for work-from-home use cases. 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) buying PEDM from PAM vendors for endpoint use cases.

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

PAM is hard, not only 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 balance cost, operational impact and security is to take a risk-adjusted approach to PAM practices.

For example, if a significant part of 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 that addresses 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.

Password Management Tools and PAM

Password management (PM) tools designed to simplify application login for all users should not be confused with PAM tools, and should not be used to manage privileged access. More than 50 vendors offer PM tools, among which the most mentioned are 1Password, Bitwarden, Dashlane, LastPass, NoPassword (acquired by LogMeIn), and Siber Systems (RoboForm).

These tools can share passwords between vaults for teams, require a master password for accessing the vault, and generate unique and complex passwords. However, none of these things make them PAM tools. Specifically, password management 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 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 four 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 through the PAM tool. Privileged session management (PSM) functions establish sessions, usually with credential injection and full-session recording. Passwords and other credentials like certificates and tokens for privileged accounts are actively managed (for example, being rotated at definable intervals or upon occurrence of specific events). PASM solutions can optionally also provide application-to-application password management (AAPM) and/or zero-install remote privileged access features for external IT staff and third parties that do not require a VPN.
- Privilege elevation and delegation management (PEDM): Host-based agents on the managed system grant specific privileges to logged-in users. PEDM tools provide host-based command control (filtering), application allow/deny/isolate controls and/or privilege elevation, which enables particular processes to be run with a higher level of privileges. PEDM tools must execute on the actual operating system (at a kernel or process level). Command control through protocol filtering is explicitly excluded from this definition because the point of control is less reliable. PEDM tools can optionally also provide application controls and file integrity monitoring features. PEDM tools are often a mandatory requirement for regulated industries and where compliance with PCI-DSS, SOX and other regulatory and financial controls are stipulated. Defense and government environments also often mandate the removal of local admin privileges.

- Secrets management: Credentials (such as passwords, OAuth tokens and SSH keys) and secrets for software and machines, are programmatically managed, stored, and retrieved through APIs and SDKs. Trust is established and brokered for the purpose of exchanging secrets and to manage authorizations and related functions between different nonhuman entities like 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. Secrets management products can also provide AAPM.
- Cloud infrastructure entitlement management (CIEM): CIEM offerings are specialized, identity-centric SaaS solutions that focus on managing cloud access risks via administration-time controls governing entitlements in hybrid and multicloud IaaS. They typically use analytics, machine learning (ML) or other methods to detect anomalies in account entitlements, like accumulation of privileges, or dormant and unnecessary entitlements. CIEM ideally provides remediation of excessive permissions, and enforcement of least-privilege approaches in cloud infrastructures.

Market Size and Drivers

Gartner estimates that the PAM market revenue for 2023 will amount to $2.12 billion, representing a growth rate of 13.6% over 2022. 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 and Risk Management, Worldwide, 2021-2027, 2Q23 Update).

The growth continues to be driven by the increasing awareness among security leaders regarding the critical need for PAM solutions. Several high-profile breaches have been linked to compromised privileged account credentials and privilege abuse.[4] In addition, regulations, the accelerated migration to cloud, the blurring of enterprise security perimeters and the overall increase in the number of cyberattacks contribute to the growth of PAM adoption. Also, 10% to 20% of Gartner clients that evaluate PAM tools for first-time purchase, state 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 staff. Use of PAM tools to enable privileged remote access (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 remote-access-focused products. Vendors, accordingly, have prioritized development of remote access capabilities over other features. Another interest is in secrets management, which brings PAM additional buyers (software development and cloud operations).

The aforementioned drivers of PAM solutions have not been restricted to the large and midsize enterprises; small and midsize businesses (SMBs) face the same challenges — albeit on a smaller scale. PAM adoption has reached maturity for large and midsize enterprises, and the focus is now expanding to SMBs as they increasingly realize the criticality of PAM implementations. With this evolution, we are seeing a shift toward the adoption of SaaS-based 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 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, remote access or CIEM products. Some of these vendors have evolved their offerings to start competing in the general PAM space (an example of this is HashiCorp, included for the first time in this Magic Quadrant).

Market Dynamics

We continue to see more vendors offering a SaaS option. This year, of the 11 vendors included in the research, eight have a SaaS option, and two are developing one. Only one vendor has no current or planned SaaS option. Several PAM vendors 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.

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 11 included vendors offer a secrets management tool for developer use cases, and the other six have developed some basic secrets management features in their products. In addition, we have seen four vendors offering a CIEM tool, two offering some CIEM capabilities included within their broader PAM solution, and two roadmapping the capability.

Competition in the PAM market remains intense owing to the presence of a large number of players. Newer players are rapidly ramping up their portfolio to better compete in the space. The 2022 acquisition of Remediant by Netwrix and the 2023 acquisition of BluBracket by HashiCorp are notable examples.

Geographic and Vertical Trends

North America and Europe remain the primary markets for PAM products, comprising 51% and 27% of the overall global market, respectively. However, the broader 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 the APAC region, Senhasegura in Latin America, and WALLIX and Kron Technologies in Europe. While smaller in size, these firms 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 OT. 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.

Large insurance brokerages point to the same, such as Cyber Insurance Market Overview: Fourth Quarter 2021, Marsh.

[2] In inquiries, clients consistently mention requirements to support remote privileged access by external user populations such as vendors, consultants, outsourcers and other business partners. Virtually every client RFP document for PAM includes questions regarding these capabilities.

[3] Traditional remote access solutions like virtual private networks (VPNs) do not address the challenges of remote privileged access such as strong authentication, governance and fine-grained visibility of authorized privileged accounts. VPNs are therefore not the best solution for securing remote privileged access for external users like third-party vendors, service providers and external IT staff. A more detailed discussion of the security gaps and issues found with VPN-based remote privileged access, and better ways of managing remote privileged access can be found in Securing Remote Privileged Access for External Users.

[4] Verizon’s 2023 Data Breach Investigations Report, for example, lists stolen credentials and privilege misuse as contributing factors in many breaches covered in the report.

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.

IS THIS CONTENT HELPFUL TO YOU?

It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.