# Magic Quadrant for Privileged Access Management

Published 4 August 2020 - ID G00381092 - 55 min read

By Analysts Felix Gaehtgens, Abhyuday Data, Michael Kelley

The PAM market continues to mature with accelerated adoption. Many vendors focus on advanced features like just-in-time PAM, secrets management and cloud capabilities, even when their tools are not yet mature in some basic PAM capabilities, such as account discovery and service account management.

## Strategic Planning Assumptions

By 2024, 50% of organizations will have implemented a just in time (JIT) privileged access model, which eliminates standing privileges, experiencing 80% fewer privileged breaches than those that don't.

By 2024, 65% of organizations that use privileged task automation features will save 40% on staff costs for IT operations for IaaS and PaaS, and will experience 70% fewer breaches than those that don't.

## Market Definition/Description

Gartner defines the privileged access management (PAM) market as tools that offer one or more of these features:

- Discover, manage and govern privileged accounts (i.e., accounts with superuser/administrator privileges) on multiple systems and applications.
- Control access to privileged accounts, including shared and emergency access.
- Randomize, manage and vault credentials (password, keys, etc.) for administrative, service and application accounts.
- Provide single sign-on (SSO) for privileged access to prevent credentials from being revealed.
- Control, filter and orchestrate privileged commands, actions and tasks.
- Manage and broker credentials to applications, services and devices to avoid exposure.
- Monitor, record, audit and analyze privileged access, sessions and actions.

Gartner covers three distinct tool categories that have evolved as the predominant focus for security and risk management (SRM) and other IT leaders considering investment in 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 credential injection, and full session recording. Passwords and other credentials for privileged accounts are actively managed, such as being changed 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 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, the latter in the form of allowing 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. PEDM tools can optionally also provide file integrity monitoring features.

- **Secrets management:** Credentials (such as passwords, OAuth tokens, SSH keys, etc.) 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 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.

Vendors covered in this Magic Quadrant must provide a fully functional PASM product. A vendor might also provide PEDM or secrets management tools. In the Vendor Strengths and Cautions section, for each vendor we comment on the quality of individual product components, and use terms such as “well above average,” “above average,” “average,” “below average” and “well below average.” The average for a particular component refers to the average score for all vendors evaluated in this research for that component. Please refer to the entry for Product or Service in the Evaluation Criteria section for a full description of these components and what was evaluated.

## Magic Quadrant

Figure 1. Magic Quadrant for Privileged Access Management


Source: Gartner (August 2020)

## Vendor Strengths and Cautions

### ARCON

ARCON is a Challenger in this Magic Quadrant; in the last iteration of this research, it was a Niche Player.

Its ARCON Privileged Access Management product is delivered as an appliance, software, or SaaS, and provides vaulting and session management (PASM) capabilities, and PEDM functionality for Windows and UNIX/Linux. ARCON's operations are mostly focused on the Asia/Pacific region and EMEA.

ARCON continues to invest heavily in analytics, a SaaS offering and in making its solution more scalable.

#### Strengths

- **Support:** The vendor does not differentiate between different tiers for technical support. It offers 24/7 support to all clients as the base support offering. Support pricing is based on a percentage of license spend, which, at 18%, stands well below other vendors' rates.
- **Product:** ARCON's offering has many differentiating features not commonly found with other vendors, such as the ability to filter SQL commands, logging SQL for database administrator access and file integrity monitoring for both Windows and UNIX/Linux.
- **Product/Scalability:** With the recently released secure gateway module, ARCON provides significantly better and easier scalability than most other vendors that use session proxy approaches.
- **Pricing:** The vendor offers a mix of pricing and licensing models, including both perpetual and subscription-based, along with a consumption-driven model available to managed service providers. Pricing is below the industry average — in some cases, well below — for a series of pricing scenarios evaluated by Gartner.

### Cautions

- **Product:** ARCON's PAM solution works best when the vendor's specialized client access tools are used. It is possible to use third-party or operating-system-native RDP and SSH access tools, but this is not as seamless as with most other PAM solutions.
- **Product:** While ARCON does support application allow/deny/isolate controls, application sandboxing is not supported.
- **Geographic Strategy:** While ARCON has begun making marketing investments and has begun to secure distribution channels in other regions, it has only a limited market profile outside of its core regional markets of the Asia/Pacific region and the Middle East.
- **Viability:** Although ARCON was able to grow its number of customers as compared to last year, its operating margin and cash on hand are relatively low compared to its competitors analyzed in this Magic Quadrant.

## BeyondTrust

BeyondTrust is a Leader in this Magic Quadrant; in the last iteration of this research, it was a Leader.

It offers PASM capabilities with Password Safe as software or as an appliance, and Cloud Vault via SaaS. PEDM capabilities are provided through Privilege Management for Windows and Mac, and Privilege Management for UNIX and Linux.

Its operations are geographically diversified. BeyondTrust is still integrating its portfolio of multiple acquisitions made in 2018.

### Strengths

- **Product:** BeyondTrust offers a solution called Privileged Remote Access (PRA) that provides a mature and easy-to-deploy solution for supporting administrators (including third-party users) that require remote privileged access.
- **Product:** BeyondTrust's offering has many differentiating features not commonly found with other vendors, such as file integrity monitoring for UNIX/Linux and Windows, trusted application protection, which provides protection for critical applications such as browsers, and a mature remote execution capability for remotely running administrative commands.
- **Product:** BeyondTrust's PAM products stand out in analytics and reporting functionalities, which include an extensive list of preconfigured reporting templates and visualization dashboards. The platform also allows administrators to create their own custom dashboards from predefined templates.
- **Product:** In clustering situations, administrators can tune Password Safe for performance by assigning roles to specific servers to balance loads across the cluster.

### Cautions

- **Product:** BeyondTrust lacks an SDK for Password Safe that could be used by clients to create custom connectors for password rotation; it offers only a CLI interface that leverages SSH or Telnet for this purpose. This makes it more difficult to integrate with external systems when BeyondTrust does not ship a connector out of the box.
- **Product:** BeyondTrust is the only Leader in this Magic Quadrant that does not yet ship a fully featured SaaS-based PAM solution.
- **Product:** Password Safe includes a self-contained data store for simple deployment configurations, but this is insufficient for enterprise deployments with uncompromising high-availability and disaster recovery needs. For those needs, an optional configuration mechanism is available that relies on Microsoft SQL Server Always On as a data store.
- **Customer Experience/Sales Execution:** Several acquisitions and subsequent consolidation has disrupted customer support; and client interest in purchasing BeyondTrust's PAM solutions dropped in 2019. While new sales have since bounced back, it is too early to tell at publication time whether customer satisfaction for support has fully recovered.

## Broadcom (Symantec)

Symantec is a Niche Player in this Magic Quadrant; in the last iteration of this research, it was a Leader (covered as CA Technologies).

The PASM portion of the solution is provided by Symantec Privileged Access Manager, available in a hardened appliance or virtual image. PEDM services are provided by the Privileged Access Manager Server Control product, an agent-based solution. AAPM agents are also available.

The vendor's operations are geographically diversified. The solution was previously available from CA Technologies before its acquisition by Broadcom, and it has recently moved to Broadcom's Symantec Enterprise Division.

### Strengths

- **Product:** Privileged Access Manager has very efficient and scalable PSM capabilities that can handle more simultaneous connections than most other products evaluated.
- **Product:** The solution has a good range of PEDM support for Windows and UNIX/Linux with excellent feature sets, including file integrity monitoring.
- **Product:** The solution has many enterprise-grade features, such as a special Java Database Connectivity (JDBC) driver for database connection management — not commonly found in other solutions — and unique support for Amazon Web Services (AWS) JIT privilege filtering and WAN-based clustering.
- **Pricing:** The solution is priced competitively, with almost all pricing scenarios below — and sometimes well below — the average for the market as a whole.

### Cautions

- **Operations:** The acquisition of CA Technologies by Broadcom has not gone well for some customers outside Broadcom's top 1,000 global accounts, who have complained about inconsistent support and engagement from the vendor since the last iteration of this Magic Quadrant. The PAM solution has been placed into the Symantec Enterprise Division and customer feedback seems to have stabilized for now.
- **Product:** Although Symantec now provides an alternative to the use of an unsecure Java plug-in for its Client Manager tunneling solution, Symantec still supports, and now stands out as the sole vendor still using, this legacy technology, after several other vendors eliminated the use of it since the last iteration of this Magic Quadrant.
- **Product/Product Strategy:** Symantec has no SaaS offering for its PAM solution and does not have one on its roadmap.
- **Product:** For complex service account credential management, Symantec leans on its Custom Connector Framework, but in several cases this places the burden on the customer to develop custom connectors where other vendors would offer out-of-the-box connectors.

## Centrify

Centrify is a Leader in this Magic Quadrant; in the last iteration of this research, it was a Leader.

Its Centrify Privileged Access Service solution is mainly focused on SaaS-based PASM, while Centrify Privilege Elevation Service has PEDM capabilities. Centrify also offers UNIX/Linux support and Active Directory (AD) bridging through the Centrify Authentication Service. Its

operations are mostly focused on the Americas and Europe. Centrify was traditionally AD-centric, but can now use other directory servers.

#### Strengths

- **Product:** Centrify includes a full SaaS-based remote privileged access solution, making client-installed software such as VPN solutions unnecessary.
- **Customer Experience:** All manuals are available online without requiring registration. Additionally, Centrify offers a free service called Centrify Health Check — a one-day consulting program for assessing the maturity of a PAM program and determining next steps.
- **Product:** Centrify offers a mature and feature-rich AD bridging capability for UNIX/Linux that includes features like file integrity monitoring as part of its Privilege Elevation Service.
- **Product Strategy:** Centrify has a good roadmap with a strong pipeline for new functionality. Deployment and licensing options are already diverse and flexible, and include cloud, on-premises and SaaS-based arrangements, along with metered, perpetual and subscription-based pricing.

#### Cautions

- **Pricing:** Centrify's pricing is above — and in many cases, well above — the market averages for most of the evaluated PAM scenarios, for both software and SaaS offerings.
- **Product:** Service account and credential management capabilities are average at best. There is a lack of depth in support for complex service account management, such as preactions/postactions or checking whether account credentials have changed. However, there is an SDK for writing custom credential rotation connectors.
- **Product:** System discovery is mostly limited to AD and network scanning. Privileged account discovery capabilities are rudimentary and mostly focused on AD discovery.
- **Product:** There is no PEDM support for macOS, nor is sandboxing and application allow/deny/isolate controls supported for applications in Windows.

### CyberArk

CyberArk is a Leader in this Magic Quadrant; in the last iteration of this research it was a Leader.

Its Privileged Access Security (PAS) solution offers PASM capabilities as software or SaaS. For PEDM, CyberArk offers Endpoint Privilege Manager (EPM) for Windows and Mac, and On-Demand Privileges Manager (OPM) for UNIX/Linux. Application Access Manager offers secrets management. CyberArk's operations are geographically diversified. In May 2020, CyberArk branched out into access management by acquiring Idaptive.

#### Strengths

- **Success in the PAM Market:** CyberArk has a long-standing history in the PAM space and the brand is very well-known. Almost all Gartner clients researching PAM products are including CyberArk on their list of vendors to evaluate.
- **Product Strategy:** CyberArk has a broad set of capabilities to serve the vast majority of PAM needs. The product set is very mature and is able to address difficult scenarios and edge cases.
- **Innovation:** CyberArk has a history of trendsetting innovations; this past year, it developed a novel "secretless" broker to expand the capabilities of its secrets management tool and a full SaaS-based remote privileged access solution called Alero, making customer-installed remote-access software such as VPN solutions unnecessary.
- **Product:** SQL logging and filtering for database administrators is supported as a Privileged Session Manager extension for Toad and Oracle SQL Plus.

#### Cautions

- **Product:** Privileged Session Manager is very powerful, but resource-hungry, and could be a potential bottleneck that requires powerful hardware and careful planning to perform adequately.
- **Customer Experience:** The software version of PAS is not easily installable or upgradable without help from CyberArk's professional services.
- **Product:** Unlike other vendors' solutions that offer AD bridging, OPM does not offer full-feature Kerberos integration or group policy support for UNIX/Linux.
- **Product Strategy:** While CyberArk's stated intention is to achieve parity between its on-premises and SaaS-based solutions, Privileged Threat Analytics is not part of the CyberArk PAS SaaS offering, although it is part of the PAS software version.

### Hitachi ID Systems

Hitachi ID Systems is a Challenger in this Magic Quadrant; in the last iteration of this research, it was a Niche Player.

Its Privileged Access Manager (HIPAM) software product is focused on PASM and can be deployed in data centers or in AWS private clouds. The vendor does not offer a PEDM solution at this time. Its operations are mostly focused on North America and Europe. Hitachi ID Systems is currently focused on making a full SaaS version available and enhancing its session monitoring capabilities.

#### Strengths

- **Product:** The solution has excellent discovery, credential management and automation capabilities. Also, it has a wealth of additional useful features that are not usually found in

competing PAM products, such as SSH key trust mapping and analysis, or the ability to scrub confidential data from session recordings.

- **Product:** Hitachi ID Systems supports the unique JIT approach to dynamically assign AWS console login accounts through credential injections into AWS roles.
- **Product Strategy:** All features are included in the base product, and the vendor has a track record of including new capabilities as part of upgrades, rather than breaking them out into separate products and charging for them separately.
- **Product:** Unlike most other vendors that require vulnerable API keys to be stored by applications, Hitachi ID Systems' AAPM uses special agent-based application fingerprinting and automatically rotates one-time keys. This method can effectively eliminate any static credentials from applications or scripts.

#### Cautions

- **Product Roadmap:** Hitachi ID Systems does not yet have a pure SaaS offering, although it offers its solution hosted on AWS and managed by the vendor.
- **Geographic Strategy:** The vendor conducts the bulk of its business in North America and Europe, where direct support is concentrated. Customers in other regions must rely on support and services coordinated through those regions, and via partners in the Asia/Pacific region (India and Japan).
- **Product:** Hitachi ID Systems does not offer PEDM, but has roadmapped adding this capability.
- **Pricing:** Pricing is based on the number of target devices under management, and runs above the industry average for a series of pricing scenarios. Per-user-based pricing is also available; however, programmatic API features are disabled for customers that choose that price model. Hitachi ID Systems also charges a base activation charge, or "vault fee," for all customers, allowing them to run as many replicas of a single database as required for operational, development and testing purposes.

### Krontech

Krontech is a Niche Player in this Magic Quadrant.

Its Single Connect tool is delivered as software and focused on PASM capabilities, also including limited UNIX/Linux PEDM functionality. Its operations are mostly focused on Europe and North America. Krontech plans to expand its single-tenant SaaS-based PAM solution called Private PAM as a Service, and to focus on discovery and onboarding for IaaS platforms and database PAM.

#### Strengths

- **Product:** Krontech goes further than other PAM vendors in supporting extensive SQL filtering and data masking controls for monitoring and controlling privileged database access.

- **Product:** Single Connect provides full optical character recognition (OCR) for captured graphical sessions, allowing auditors to search for artifacts displayed on screens during activity that would otherwise be difficult to find.
- **Product:** Single Connect has been built for use in large environments and has a highly scalable architecture that supports massive parallel credential rotation.
- **Innovation:** Krontech has developed a multitenancy feature for its solution. This gives the customer the ability essentially to provide PAM as a service for various groups requiring PAM services, inside or outside the company, but with isolation established between those groups.

### Cautions

- **Product Strategy:** Krontech has lightweight PEDM for UNIX/Linux, but does not support application allow controls, sandboxing, or file integrity monitoring.
- **Product:** Single Connect is well below average in capabilities for secrets management, and does not integrate with any DevOps tool out of the box.
- **Integration:** While Single Connect ships with a built-in multifactor authentication (MFA) module, integration with external MFA providers is limited to Cisco Duo and Okta; no integration with other MFA vendors is available.
- **Pricing:** The cost evaluated for most PAM scenarios is above the industry averages.

## ManageEngine

ManageEngine is a Niche Player in this Magic Quadrant; in the last iteration of this research, it was a Niche Player.

Its PAM360 solution is broadly focused on PASM capabilities with SSH key and SSL certificate management capabilities. Another product, Access Manager Plus, provides stand-alone remote access for privileged users. ManageEngine does not offer PEDM capabilities. ManageEngine's operations are geographically diversified. PAM360 includes and extends capabilities from Password Manager Pro, ManageEngine's previous PAM solution.

### Strengths

**Product:** PAM360 comes with SSH key and SSL certificate management capabilities out of the box.

**Product:** ManageEngine sells a managed service provider version of PAM360 for use with managed service providers that require managing privileged access to multiple customers.

**Customer Experience:** All manuals for PAM360 are available online without requiring registration.

**Pricing:** ManageEngine's pricing for the scenarios it supports consistently undercuts competitors.

### Cautions

**Product:** PAM360 is a new offering with enhanced features, but shares the same code base and limitations of Password Manager Pro. Access works exclusively through a web-based client access interface that has an HTML5-based RDP and SSH client — customers cannot use their own RDP or SSH access tools.

**Product:** Credential management capabilities are below average, with advanced service and software account credential rotation methods unsupported. However, there is an SDK for writing custom credential rotation connectors.

**Product:** Privileged task automation features are almost entirely absent.

**Product/Product Strategy:** ManageEngine does not offer PEDM capabilities; however, they have been roadmapped.

## One Identity

One Identity is a Visionary in this Magic Quadrant; in the last iteration of this research, it was a Visionary.

Its PASM solution is provided by two products: One Identity Safeguard for Privileged Passwords and One Identity Safeguard for Privileged Sessions. Both solutions are available as a hardware or virtual appliance. Privileged Access Suite for UNIX and Privilege Manager for Windows provide PEDM capabilities. One Identity's operations are geographically diversified, and the vendor is developing SaaS-based PAM capabilities.

### Strengths

- **Product:** One Identity Safeguard for Privileged Sessions can provide full OCR for captured graphical sessions, allowing auditors to search for artifacts displayed on screens during activity that would otherwise be difficult to find.
- **Product:** One Identity's PAM offering features comprehensive and well-thought-out API and SDK capabilities, as well as enhanced SQL database access controls, including Azure SQL.
- **Integration:** One Identity has strong support for sudo functionality on UNIX/Linux, and clients who require both IGA and PAM functionality can take advantage of One Identity's products in both spaces.
- **Product:** One Identity Safeguard for Privileged Analytics stands out from other solutions by using machine learning to analyze not just privileged access attempts, but also complete session activity, including commands. Passive biometric analysis can be used to detect unauthorized use through keystroke dynamics.

Cautions

- **Product:** One Identity does not yet have a full-featured SaaS version of its Safeguard solutions.
- **Pricing:** The pricing in the scenarios evaluated by Gartner tend to be somewhat above average.
- **Product:** One Identity Safeguard's privileged task automation capabilities are limited, with the available APIs providing no support to automate file management, delegated approvals or governance tasks.
- **Product:** While One Identity Safeguard's service account management capabilities have improved since the last iteration of this research, they remain average, with some advanced features requiring the creation of custom system connector logic.

### senhasegura

Senhasegura is a Challenger in this Magic Quadrant; in the last iteration of this research, it was a Visionary.

Its PAM solution consists of many modules in four product families: Privileged Identity, Privileged Access, Privileged Change Audit and Privileged Infrastructure. The products provide PASM and PEDM capabilities, and secrets management. Senhasegura's operations are mostly focused on Latin America and EMEA. The vendor is focused on expanding its DevOps tools integration and analytics capabilities.

Strengths

- **Product:** The vendor's discovery and account mapping capabilities stand out from most other vendors evaluated in this research because of the sheer number of predefined connectors and advanced features such as scanning authorized_keys and sudoers files.
- **Product Strategy:** Senhasegura is fast in bringing new features to market and has shown a number of differentiating innovations in the past year, such as discovery tasks for containers and access control for the Kubernetes management API. The vendor also has a solid roadmap for additional secrets management, fraud detection and response.
- **Product:** Sizing guidelines indicate that the RDP proxy function is very efficient, supporting more than 1,000 simultaneous connections on a high-end hardware appliance.
- **Brand:** It has established itself as the "brand to beat" in the Latin American market, with strong local support and distribution, in contrast to many other vendors by which Latin America is either overlooked or not well-supported.

Cautions

- **Product Strategy:** Senhasegura has the least amount of documentation, by far, for any vendor evaluated in this Magic Quadrant. Many features and connectors are only listed and not documented. This issue was already documented in the last iteration of this research.

- **Product:** Many features and functionality are available through scripting, but this places the burden on the customer to create them, as opposed to offering out-of-the-box functionality.
- **Pricing:** The vendor's method of licensing revolves around an a la carte approach that requires its clients to buy many different modules and closely track usage. While overall prices are just about average compared to market norms, this requires true-ups of license alignments at license renewal time.
- **Product:** Senhasegura does not support standards-based SSO interactions for users, and MFA capabilities are limited to TOTP standard support (for one-time password authenticator apps from Google, Microsoft and others), as well as support for a single vendor — Dell Technologies (RSA).

### Thycotic

Thycotic is a Leader in this Magic Quadrant; in the last iteration of this research, it was a Visionary.

Its Secret Server Platinum solution is broadly focused on PASM capabilities and is available as software or SaaS. In addition, its Privilege Manager offers PEDM capabilities for Windows and macOS. Thycotic also offers secrets management. Its operations are geographically diversified. In 2020, Thycotic acquired Onion ID to expand its privileged access controls for IaaS, SaaS and database platforms.

#### Strengths

- **Customer Experience:** Clients continue to be positive about the vendor's technical support, the user-friendly UI, and the ease of installation and configuration. In addition, manuals are available online without requiring registration.
- **Product Strategy:** The acquisition of Onion ID puts Thycotic in a strong position to compete in the field of PAM for IaaS, SaaS and databases, which is underserved by most PAM vendors.
- **Product:** To address complexity and disruption of upgrades for PAM tools, Thycotic developed a zero downtime upgrade process, able to provide continuous access to the tool, even during system upgrades.
- **Innovation:** Identity life cycle management for privileged accounts has been a gap for many PAM tools. Thycotic has added simple identity administration functionality for tracking identity life cycles for privileged accounts such as service accounts.

#### Cautions

- **Product:** Many features and functionality are available through scripting rather than offered out of the box, but this places the burden on the customer to create them. There is no built-in privileged task automation functionality; instead, Thycotic relies on integrations with robotic process automation (RPA) tools to automate limited repetitive tasks.

- **Product/Product Strategy:** Service account management remains below average since the last iteration of this research, with support for more complex service account credential management absent and not on the roadmap.
- **Pricing:** Pricing is uneven for the SaaS offering, with different pricing scenarios set at either above or below market averages compared to other vendors offering SaaS-delivered PAM. Consideration of competitive bids and the functionality provided is necessary to ensure receiving the best price.
- **Product:** Thycotic's Windows PEDM solution does not offer file integrity monitoring.

### WALLIX

WALLIX is a Niche Player in this Magic Quadrant; in the last iteration of this research, it was a Niche Player.

Its WALLIX Bastion product line is available as software, or as an appliance (virtual or physical) focused on PASM. AAPM and PEDM capabilities for Windows are also available as software. WALLIX's operations are mostly focused on EMEA and North America. It is currently investing in a SaaS-based PAM solution and JIT features.

#### Strengths

- **Product:** WALLIX Bastion can provide full OCR for captured graphical sessions, allowing auditors to search for artifacts displayed on screens during activity that would otherwise be difficult to find.
- **Product Strategy:** WALLIX has recently acquired Simarks and with it a capable Windows PEDM solution. Its roadmap emphasizes a scalable, distributed architecture across cloud providers and data centers.
- **Product:** Unlike most other vendors that require vulnerable API keys to be stored by applications, the vendor's AAPM uses comprehensive agent-based application fingerprinting. This method can effectively eliminate any static credentials from applications or scripts.
- **Industry Strategy:** WALLIX offers connectors for certain industrial control systems and operational technology systems. It has a partnership with Schneider Electric, and recent innovations include direct connection brokering and filtering from technicians' remote workstations to a PLC for industrial control systems.

#### Cautions

- **Product/Product Strategy:** Apart from the solid AAPM capabilities mentioned above, service account management remains below average since the last iteration of this research, with support for more complex service account credential management absent and not on the roadmap.

- **Product:** From a high-availability perspective, the WALLIX Bastion active/passive type cluster does not have a load balancing function.
- **Product:** Automation is below average — an API is available, and there is documentation on how to integrate with some DevOps tools, but few features for privileged task automation exist.
- **Pricing:** Pricing is uneven, with smaller scenarios being closer to market averages, whereas larger and more complex deals tend to be priced above market averages.

### 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

- Krontech
- The Symantec brand of Broadcom appears for the first time in this Magic Quadrant; however, the vendor was covered in the previous iteration as CA Technologies.

#### Dropped

- **Fudo Security** was a Niche Player in the last iteration of this Magic Quadrant. Its solution is focused on privileged session management, but also has analytics and vaulting capabilities. Fudo Security did not meet the elevated inclusion criteria for minimum growth and customers in this iteration.
- **Micro Focus** was a Niche Player in the last iteration of this Magic Quadrant. Its NetIQ Privileged Account Manager provides PASM and PEDM functionality with optional agents for Windows and UNIX/Linux platforms for fine-grained command control PEDM. Micro Focus did not meet the elevated inclusion criteria for minimum growth and customers in this iteration.
- **Osirium** was a Niche Player in the last iteration of this Magic Quadrant. Its solution is focused on privileged task automation with advanced analytics and vaulting capabilities. Osirium did not meet the elevated inclusion criteria for minimum growth and customers in this iteration.

## Inclusion and Exclusion Criteria

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

**Mandatory:** Privileged account and session management. Vendors that do not provide this function will not be included in the Magic Quadrant for Privileged Access Management.

**Optionally**, a vendor may also offer:

- Privileged elevation and delegation management for UNIX/Linux and/or Windows operating systems
- Secrets management

The vendor's solution must meet the following **minimum capabilities** as of 31 January 2020:

- A secured, hardened and highly available vault for storing credentials and secrets
- Tools to discover, map and report privileged accounts on multiple systems, applications and devices
- Tools to automatically randomize, rotate and manage credentials for system, administrative, service, database, device and application 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
- Tools to allow a privileged session to be automatically established using protocols such as SSH, RDP or HTTPS without revealing credentials to the user
- Features must exist to fully record and review sessions, as well as manage live sessions by allowing them to be accompanied or terminated
- Tools that broker credentials to software, thereby allowing the elimination of clear-text credentials in configuration files or scripts
- Support for role-based administration including centralized policy management for controlling access to credentials, and privileged actions
- Analytics and reporting of privileged accounts and their use (for example, discovering unauthorized use of privileged credentials or reporting on unusual activities)
- Underlying architecture for the above, including connector architecture
- Products must be marketed, sold and deployed for use with customer production environments for purposes consistent with objectives of PAM

To further qualify for inclusion in the 2020 PAM Magic Quadrant, the respective vendors must meet the following criteria:

- Revenue:
  - Have booked a total revenue of at least $7.5 million for PAM products and subscriptions (inclusive of maintenance revenue, but excluding professional services revenue) for any period of 12 consecutive months (fiscal year) between 1 March 2018 and 31 December 2019.

  Or

  - Have booked a total revenue of at least $5 million for PAM products and subscriptions (inclusive of maintenance revenue, but excluding professional services revenue) for any period of 12 consecutive months (fiscal year) between 1 March 2018 and 31 December 2019 and 25% year-over-year revenue growth.

- Deployment:
  - Have at least 125 distinct customers for PAM products and subscriptions (i.e., “net logos,” meaning different business units or dependencies of the same company should not be counted as separate customers).

  Or

  - Have at least 80 distinct customers for PAM products and subscriptions and 20% year-over-year growth in number of customers.

- Geography: Vendors must compete in at least two of the five major regional markets (North America; Latin America, including Mexico; Europe; the Middle East and Africa; and the Asia/Pacific region, including Australia and New Zealand, and Japan). This condition would be met if a vendor has no more than 90% or 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 industry verticals.
- Positioning: Market their products for use consistent with PAM.

# 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 access governance:** This capability provides features and functions to formally manage privilege assignment, periodically review and certify privileged access, and ensure segregation of duties based on a set of policies.

- **Account discovery and onboarding:** This capability provides features to discover, identify and onboard privileged accounts, including the ability to support periodic, ad hoc or continuous discovery scans. This also includes the ability to automatically discover target services, and systems (including virtual machines) for further 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. These functions require the ability to access the PAM tool through a web console or API at minimum.

- **Privileged session management:** This capability provides session establishment, management, recording and playback, real-time monitoring, protocol-based command filtering, and session separation for privileged access sessions. This 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. This capability may also involve restrictions, such as allow/deny of certain types of commands and functions while logged into the target system.

- **Secrets management:** This capability provides the ability to manage access to credentials (such as password, OAuth tokens, SSH keys, etc.) 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 (e.g., via 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. In combination, these functions support secrets management for dynamic environments, and provide support for RPA platforms.

- **Logging and reporting:** This capability provides the ability to record all single events, including changes and operations, as part of the PAM operation. A single event is based on user, time, date and location, and is processed with other events via correlation in a logical order. This is to monitor and determine the root cause of risk events and identify unauthorized access. This also provides features required for auditing and reporting of the event database, including prebuilt reports and support for ad hoc reports. Event data must also include information from privileged sessions. This capability also provides analytics (using machine learning) on privileged account activities to detect and flag anomalies, including baselining, risk scoring and alerting. The objective is to better identify lagging and leading indicators that identify privileged access anomalies to trigger automated countermeasures in response to alerts.

- **Privileged task automation:** This capability provides functions and features for automating multistep, repetitive tasks related to privileged operations that are orchestrated and/or executed over a range of systems. This capability uses extensible libraries of preconfigured privileged operations for common IT systems and devices. It can orchestrate back and forth between different activities and ask for more information as needed, while providing guard rails by checking input against policies and settings.

- **Privilege elevation and delegation:** This capability provides host-based functions and features for enforcing policies 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, in effect preventing administrators from carrying out unsafe activities. These features must execute on the actual operating system (kernel or process level). Level of support may vary by platform (i.e., Windows, UNIX/Linux and Mac). PEDM tools can optionally also provide file integrity monitoring features.

- **Adjacent system integration:** This capability 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), SSO, MFA, enterprise directories, support for flexible connector and integration frameworks, general API access, integration with IT service management (ITSM) systems, security information and event management (SIEM) systems, and vulnerability management.

- **Ease of deployment, performance:** This capability provides functions and features to simplify the deployment of the PAM solution while ensuring availability, recoverability, performance and scalability.

- **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. 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. 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 AD groups
  - Dynamically provide time-limited access to privileged accounts
  - PEDM functionality through on-demand privilege elevation
  - The ability for on-demand creation and deletion of privileged accounts
  - The ability to create and use ephemeral tokens

- The ability for on-demand access to SaaS control panels such as AWS

**Overall Viability:** Includes an assessment of the overall organization's 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 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 success 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, which was more heavily weighted than other factors in this category, 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 14 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, average, above or well above the industry average, as determined by standard statistical measures.

**Market Responsiveness/Record:** Evaluates the 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 in 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 or 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. In addition, the organization's ability to respond to rapidly changing shifts was reviewed. 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. Specifically, this includes

quality supplier/buyer interactions, technical support or account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc. 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). Methods to measure and incorporate customer satisfaction and feedback into existing processes were also evaluated. We highly weighed direct customer feedback with a mix of customer feedback from vendor-supplied references (if provided), 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 and internal processes.

**Table 1: Ability to Execute Evaluation Criteria**

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

Source: Gartner (August 2020)

## 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 — would score well in this criterion. We evaluated the methodology and input to vendors' market research programs, and vendors' 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. Vendors' marketing activities, communications plans and brand awareness campaigns were evaluated, as well as the use of media. A vendor's marketing organization itself was also evaluated to determine if its makeup enables it to stay competitive when compared to other vendors in the space. Factors such as staff size and use of external components were evaluated.

**Sales Strategy:** Examines the soundness of the vendor's sales strategy that uses the appropriate networks, including: direct and indirect sales, marketing, service and communication and partners that extend the scope and depth of market reach, expertise, technologies, services and their customer base. We evaluated a vendor's understanding of its buyers and possibly the unique buyers it targets. We also looked at its 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' future plans to meet customers' selection criteria, and evaluate software development practices, and participation in industry or standards organizations.

**Business Model:** Emphasis is 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 (technology, VAR, SI) was reviewed, along with its ability to leverage them as part of an overall business plan.

**Vertical/Industry Strategy:** Assesses the vendor's strategy to direct resources (sales, product, development), skills and offerings to meet the specific needs of individual market segments, including midsize enterprises, service providers and verticals. Factors evaluated include the applicability of the offering to specific verticals, industries and 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 (i.e., supporting processes, implementation programs, etc.) that advance the ability of buyers to better control, monitor and manage privileged users and credentials, and which meaningfully differentiate the products. Technical and nontechnical innovations over the last 18 months were heavily weighted. We also evaluated foundational advancements (older than 18 months) made over the lifetime of the product.

**Geographic Strategy:** Assesses the vendor's strategy and ability to direct resources, skills and offerings to meet 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

| 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 (August 2020)

## 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. However, Challengers have not yet demonstrated the feature completeness, scale of deployment or vision for PAM that Leaders have. 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. Clients of Challengers are relatively satisfied, but ask for additional PAM features as they mature.

### Visionaries

Vendors in the Visionaries quadrant provide products that meet many PAM client requirements, but may not have the means (such as budget, personnel, geographic presence, visibility and so on) to execute as Leaders do. Due to smaller size, there may be initial concerns among some potential buyers regarding long-term viability. Visionaries are noted for their innovative approach to PAM technology, methodology and/or means of delivery. They often may have unique features, and may be focused on a specific industry or specific set of use cases, more so than others. Visionaries are often the technology leaders in evolving 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 methodology. 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 vendor's applications, data and/or infrastructure. Vendors in this quadrant often have a small installed base, a limited investment in PAM, a geographically limited footprint or other factors that inhibit providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in this quadrant. However, this does not reflect negatively on the vendor's value in the more narrowly focused service spectrum. Niche solutions can be very effective in their area of focus.

## Context

Before any selection of a PAM tool, buyers must define their vision for their PAM practice, including which practices and policies they believe are required for managing privileged access in their unique environment. There are two possible overall strategies to follow. In the first, privileged access practices drive the organization; this is a response driven strategy and not ideal. The second approach is the ideal path: Organizations proactively drive their privileged access practice by using comprehensive discovery practices to understand what privileged access exists in their environment, and then by defining how privileged access will happen.

There are some fundamental concepts that can inform this latter approach to PAM, beginning with the principle of least privilege. The elusive target of any PAM program is to ensure that the right person has access to the right resource at the right level at the right time. This target is elusive because neither process nor tools alone can help an organization meet that target; it requires a combination of both, applied at the appropriate levels. When good processes and practices are enforced by an effective tool, organizations begin to see success in their PAM goals.

In terms of process and practices, borrow heavily from Gartner's four pillars of PAM:

- Track and secure every privileged account.

Govern and control access.

Record and audit privileged activity.

Operationalize privileged tasks.

**Track and secure every privileged account.** Buyers can't manage or control what they don't know about, so focus efforts on discovery for all accounts, users of those accounts (remembering that users include software and service accounts) and understanding what resources those accounts are accessing. Discovery processes must be ongoing and comprehensive, meaning discovery of all privileged access, whether in the data center or in the cloud, and whether the user is a person, software or a machine. Unaccounted privileged access carries significant risk and breaches policies. While audits can help with visibility, some privileged accounts may exist for just a short time and may not be seen by audits. For this reason, a continuous discovery process is essential. Discovery is a complex, but fundamental, part of succeeding with PAM, and there is considerable variety in levels of capability for discovery from PAM vendors. Success in discovering all privileged accounts, including service accounts, both inside and outside of AD, is foundational to a PAM program.

**Govern and control access.** Develop or acquire an effective identity governance program for PAM access to ensure that all changes in accounts, systems and access are accounted for. Leaders must decide which kind of control they can be successful in capturing now, and which they want to forecast. For example, start with password vaulting for human users, then move to service accounts and application-to-application access. Next, move to enabling access that does not require standing (always-on) access — things like automation, normal users running scripts with privileged access and workflow processes for requesting JIT access.

Expanding use cases for JIT access is a fundamental part of governing privileged access, and a necessary step on the journey to ZSPs. It is based on the principle that access is granted only for a short period of need and then removed. While this is true for all PASM solutions that can broker access to a privileged account and then remove access to that account, JIT goes deeper. For example, JIT can allow elevated permissions to be attached to an account — personal or privileged — for a short period. Or, JIT can grant time-limited access to privileges through access to the vault, or though access to temporary accounts (created on the fly and then removed after use), or through access to ephemeral mechanisms like one-time, one-use tokens.

Each step down this path to JIT and ZSP takes your organization closer to fully implementing the principle of least privilege.

**Record and audit privileged activity.** Even the most effective PAM programs can have gaps; you must have visibility for any access or change that slips through, or around, your discovery process. Scrutinize vendors not just for whether they can record sessions, but also for how easy it is to quickly and effectively review activity. Extensive time spent reviewing session recordings can be mind-numbing and cause ineffective results, and some vendors differentiate their products by providing users with tools to more easily find unusual activity in logs and recordings.

Security and risk management leaders should not limit their visibility to what is provided in the PAM tool; security infrastructure that is devoted to logging, monitoring and analytics must be a part of this effort. Mature SIEM tools will give visibility for use of privileged access. While several PAM vendors offer a "UEBA-like" feature, if an enterprise UEBA platform is available, then outputting the PAM logs to that tool carries additional potential for discovery of anomalous activity.

**Operationalize privileged tasks.** Start adding real business value to the security value of a PAM program by working to find opportunities to automate, script and integrate with other enterprise systems, such as identity governance and administration (IGA), orchestration, and workflow platforms. The goal will be to move beyond the legacy functions of PAM, such as password vaulting and session recording, into the next-generation functions of ZSP, and little to no human interaction for support of privileged task execution.

These four pillars of PAM describe the best practices for a comprehensive approach to a PAM practice, but leaders must have a strategy for the progressions of PAM maturity, and must select a PAM tool that can best help them mature their PAM practice.

## Considerations for Achieving PAM Maturity

- *Breadth*
  - Unfortunately, many organizations hit a wall with their PAM practice before comprehensive protection has been implemented. PAM is a challenging road, and the principle of least privilege is best understood as a journey as opposed to a destination. While it is advisable to begin with simple PAM use cases like Windows servers and UNIX/Linux servers, Identity and access management (IAM) leaders should expect to support a comprehensive array of approaches to PAM methodologies and technologies in their environment. Nearly every piece of software installed in the environment, whether in traditional data centers or in public and private clouds, and every device, whether physical or virtual, must be accounted for with a PAM practice. New use cases like DevOps, continuous integration/continuous development (CI/CD) and other line-of-business applications often fall outside the classical purview of IAM leaders, yet each of these use new cases must have a defined strategy from a PAM perspective.
    - Expand use cases to include new PAM challenges coming from SaaS platforms like Office 365 and Salesforce; IaaS and PaaS platforms like AWS and Azure; and DevOps coverage, including community code platforms and container technologies. Several vendors are offering secrets management functionality, but there is a wide range of maturity for these solutions in the market, and accurate requirements analysis is necessary in this area.
    - For critical remote privileged access for contractors and consultants, several PAM vendors are providing web-based mechanisms, offering a secure approach for giving support teams access to systems without leveraging VPN or other remote access technologies.

- Leverage automation and software controls for as many PAM use cases as possible to increase security, reliability and availability of infrastructure. Migrate manual execution of privileged tasks into automated execution of privileged tasks.

- *Depth*
  - Vaulting and session management are basic PAM needs, but are only the starting point for a mature PAM practice. Given the breadth of PAM use cases, leaning solely on basic PAM approaches is a recipe for failure. Target vendors that are working to innovate new PAM approaches, providing competent core PAM capabilities today, while working toward new capabilities needed in the future. Examples of innovation in PAM markets include:
    - Supporting JIT access to mitigate the risk of privileges held by PAM accounts, and to ZSP to mitigate the existence of PAM accounts.
    - Discovery, provisioning and workflow integrations with other enterprise systems like CMDBs, ITSM, IGA, and SIEM.
    - Secure access, since PAM access provides access to the enterprise's most critical assets and data, single-factor authentication is totally inappropriate for accessing PAM credentials; instead, MFA must be required for PAM access. Organizations looking for a PAM tool must ensure that the tool they select will accommodate a third-party, or include a built-in, MFA capability that provides a higher level of security. See "Market Guide for User Authentication" for additional guidance. Leverage identity corroboration techniques like mobile push, public key tokens and other methods, such as biometrics.
    - In addition, more PAM vendors are providing UEBA capabilities that detect when unauthorized use through impersonation, or when session hijacking has taken place.
    - While secrets management is a quickly maturing approach for machine-to-machine authentication, new approaches like Spiffe offer promise through identification of machines to establish trust without exchanging secrets. This technology is still new, but should be monitored as a potential long-term disruption for secrets management in DevOps scenarios.

- *Availability:*
  - As the PAM capability is expanded to all privileged access in the enterprise, reliability and uptime of systems will now depend on the availability of the PAM solution. Key considerations for discussion with PAM vendors include redundancy, high availability, time to recovery and a "break glass" capability, which gives you emergency access to your privileged accounts and passwords when the PAM system is unavailable.

- *Culture:*

- Many IT administrators can see PAM as a threat to their authority, or an indication of lack of trust in their competency. In addition, the adoption of PAM is challenging for even the most enthusiastic participant, creating further friction for adoption. Leaders should not underestimate the organizational change management impact of a PAM practice. Communications that target key user populations with a clear, unified message are crucial for adoption. Leaders should have a strategy for executive sponsorship and clear communications that succinctly point out the "why" for a beginning or expanding PAM practice. Use technical approaches such as selecting a PAM tool to enable administrators to leverage remote access tools that they are familiar with and enhance their productivity. In addition, select PAM products that leverage automation and scripting to execute privileged tasks, rather than granting full operating system or application access, which will also help minimize disruption for users by reducing the amount of tasks for which they are responsible.

# Market Overview

## Market Size and Drivers

Gartner estimates the PAM market revenue for the vendors covered in this Magic Quadrant exceeded $1.4 billion in 2019, representing growth of 18% over 2018. The market is expected to continue to grow (see "Forecast: Information Security and Risk Management, Worldwide, 2018-2024, 1Q20 Update"). Readers, particularly Invest clients, are cautioned not to interpret this revenue estimate as accounting for all PAM products and services available in the market. Numerous vendors that could not be included in this Magic Quadrant can meet at least partial requirements — for example, providing only session management capabilities.

Emerging market forces are driving the criticality of effective PAM. First, the security control plane has been subtly shifting from network to endpoint to identity. Second, the explosion of cloud services has driven proliferation of privileged accounts and credentials to a state that, for most organizations, is unmanageable without processes and tools. The recent challenges posed by the impact of COVID-19 will not slow the growth of PAM significantly in the near term, especially as organizations are seeking to provide remote privileged access to IT workers. Indeed, during the first half of 2020, PAM purchasing does not seem to have been much affected by the COVID-19 crisis, according to anecdotal discussions with Gartner clients and the steady stream of PAM proposal review requests from Gartner clients.

Specific influencing factors driving growth in the market include:

- Organizations seeking to mitigate the risk of breaches and insider threats, which are often associated with stolen, compromised or misused privileged credentials
- A growing number of regulatory and compliance mandates that require, explicitly or implicitly, controls over privileged users and the protection of privileged credentials
- Failed audits, as auditors continue to understand the criticality of controlling and monitoring privileged user activity, and cite the absence or inadequacy of such controls as findings

- Sudden shift of remote work for privileged users due to the COVID-19 pandemic

Other factors contributing to growing use of PAM tools include:

- The need to grant and control privileged access to third parties, such as vendors, contractors, service providers and business partners, which has proliferated the adoption of remote privileged access features from PAM tools
- Evolving PAM capabilities to manage all types of secrets in an organization's environment
- A desire to increase the operational efficiency of administrators and operators
- Providing support for an overall security strategy

## Market Dynamics

Although the market continues to be served by a large number of vendors, and remains extremely competitive, signs of continued consolidation are readily visible.

The following acquisitions, mergers and business restructuring are noteworthy:

After Broadcom completed the acquisition of CA Technologies, its PAM solutions (together with other IAM solutions) were integrated into Broadcom's Symantec division.

Thycotic acquired Onion ID, a specialist PAM vendor focusing on PAM for databases and SaaS.

Okta acquired ScaleFT, a PAM specialist focusing on brokering SSH connections.

CyberArk acquired Idaptive, a SaaS-based access management vendor.

WALLIX acquired Simarks, a Spanish company specializing in Windows PEDM tools.

## Geographic and Vertical Trends

Across the world, North America and Europe still remain the primary markets for PAM products. However, other regions — particularly the broader Asia/Pacific region and Latin America — exhibited increased interest and sales. Vendors have continued to split into two groups. Global, enterprise vendors — such as Broadcom (Symantec), CyberArk and, somewhat aspirationally at the moment, BeyondTrust, Centrify and Thycotic — are increasingly attempting to diversify their geographic reach to extend to all regions. Once there, they're met by strong regional vendors: ARCON in the EMEA and the Asia/Pacific region, ManageEngine in southeast Asia, senhasegura in Latin America, and WALLIX and Krontech in Europe. While smaller in size, these firms have been able to leverage local knowledge and relationships, language, and close proximity to customers to their advantage.

Diversified financial services (banking, securities and insurance) — along with communications, media and services, and, increasingly, manufacturing and government— remain the primary

industry verticals acquiring PAM solutions. This is unsurprising, given the high degree of both risk and the heavy compliance load faced by these industries, as well as auditor requirements. However, data suggests that PAM is becoming more of a horizontal solution, with increasing demand from healthcare; manufacturing and natural resources; utilities; and technology firms. The focus of PAM is shifting from large enterprises alone to the increased demand among midsize enterprises, and even some small and midsize businesses.

## 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.