Magic Quadrant for Privileged Access Management

Published 19 July 2021 - ID G00734652 - 50 min read

By Felix Gaehtgens, Abhyuday Data, and 2 more

The past year has seen intense focus on remote privileged access and secrets management. Several smaller vendors now have more capable and less expensive offerings than large, established PAM vendors. PAM is a mature market, and SRM leaders should cast their nets wide to look for potential products.

Market Definition/Description

Gartner defines the privileged access management (PAM) market as a foundational security technology to protect accounts, credentials and operations that offer an elevated ("privileged") level of access. Privileged access differs from "normal" access because it may allow security or maintenance functions, system- or application-wide configuration changes, or the bypassing of established security controls through superuser access. PAM tools control privileged access for machines (systems or applications) for internal or machine-to-machine communication, and for people who administer or configure systems and applications.

The core capabilities of PAM include:

- ***Discovery of privileged accounts across multiple systems, infrastructure and applications***
- ***Credential management for privileged accounts***
- ***Delegation of access to privileged accounts***
- ***Session establishment, management, monitoring and recording for interactive privileged access***
- ***Controlled elevation of commands***

Optional capabilities of PAM include:

- ***Secrets management for applications, service and devices***
- ***Privileged task automation (PTA)***
- ***Remote privileged access for workforce and external users***

Gartner covers three distinct tool categories that have evolved as the predominant focus for security and risk management (SRM) 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 on occurrence of specific events. PASM solutions can also manage (rotate) credentials for service accounts.***
- ***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) and privilege elevation for servers, 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). For UNIX/Linux PEDM tools, directory bridging functionality is often included to allow users to log into UNIX/Linux systems with their Active Directory (AD) credentials. Command control through session monitoring (i.e., command filtering on Secure Shell [SSH] sessions) is explicitly excluded from this definition, because the point of control is less reliable.

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

Magic Quadrant

Figure 1: Magic Quadrant for Privileged Access Management

Source: Gartner (July 2021)

Vendor Strengths and Cautions

ARCON

ARCON is a Leader in this Magic Quadrant. Its ARCON Privileged Access Management product is delivered as an appliance, software or SaaS, and provides vaulting and PASM capabilities, PEDM functionality for Windows and UNIX/Linux, and secrets management.

ARCON's operations are mostly in Asia/Pacific and EMEA.

ARCON is focused on closing the gap with other vendors with a full SaaS-based offering and improving its features to support the Internet of Things (IoT) and operational technology (OT).

Strengths

- ***Innovation: ARCON's product development has made great progress since our evaluation for the 2020 edition of this Magic Quadrant, aided by major investment. ARCON has an aggressive roadmap that features additional support for OT and the IoT, as well as governance for bots, additional robotic process automation (RPA) integrations, and support for managing privileged access for DevOps tools.***
- ***Support: ARCON does not differentiate between different tiers for technical support. It offers 24/7 support to all clients as its base support offering.***
- ***Software pricing: ARCON's software offering is priced below the industry average for most of the pricing scenarios evaluated. However, ARCON charges both for the number of users and for the number of target systems, which may mean costs escalate when one of the metrics changes substantially.***
- ***Customer experience: ARCON's offering has been awarded a Customers' Choice distinction on Gartner's Peer Insights platform. Customers have shared positive feedback about the product's ease of integration and rapid deployment functionalities.***

Cautions

- ***Geographic strategy: Awareness of ARCON is limited outside its core markets of Asia/Pacific and EMEA, even though the company has a local presence and actively sells its products outside those regions.***
- ***Product integration: ARCON relies mostly on customers to develop their integrations into other adjacent systems through its APIs, rather than delivering premade integrations as part of the product.***
- ***Product: For users who prefer not to use ARCON's client tools, privileged access can be provided through a web interface instead, but this requires an ActiveX or an obsolete Java plug-in.***
- ***SaaS pricing/operations: ARCON's pricing is above average for the SaaS offering in most scenarios evaluated. Unlike most vendors that offer a PAM product as a service, ARCON does not have SOC Type 2 certification yet.***

BeyondTrust

BeyondTrust is a Leader in this Magic Quadrant. It offers PASM capabilities within its Password Safe offering, as software, a physical or virtual appliance, or as SaaS.

It also offers a secrets management product, DevOps Secrets Safe, as software. PEDM capabilities are provided through Privilege Management for Windows, Privilege Management for Mac, and Privilege Management for UNIX and Linux.

BeyondTrust also has several additional products that overlap with its PAM offering, which are not evaluated in this Magic Quadrant: an actively marketed PASM product called Privileged Remote Access and two legacy products that are supported but not actively marketed (a PASM product called Privileged Identity and a PEDM product called PowerBroker for Windows).

BeyondTrust's operations are geographically diversified.

BeyondTrust is working on adding cloud infrastructure entitlement management (CIEM) features.

Strengths

- *Account discovery: Excellent account discovery features are available through a BeyondInsight add-on that is included with BeyondTrust's PAM products.*
- *UNIX and Linux: BeyondTrust's Privilege Management for UNIX and Linux is a best-in-class offering for UNIX and Linux PEDM. It has a rich set of capabilities to support all evaluated use cases.*
- *Dashboards/reporting: BeyondTrust's PAM products stand out for their reporting functionality, which includes an extensive list of preconfigured reporting templates and visualization dashboards. The platform also enables administrators to create their own custom dashboards from predefined templates.*
- *Windows application control: Application controls in the BeyondTrust Privilege Management for Windows tool are very strong, with an extensive list of criteria for identifying and controlling access to applications. Additionally, the Privilege Management for Mac tool provides a comprehensive set of application controls for macOS.*

Cautions

- *Product strategy: BeyondTrust has three overlapping products for PASM: Password Safe, Privileged Remote Access and Privileged Identity, although the last one is a legacy product that is no longer sold to new customers. BeyondTrust has not managed to fulfill its roadmap intention to merge the products' functionality after more than two years.*
- *Pricing: BeyondTrust allows clients to choose either a per user or a per target licensing model for Password Safe that, by itself, would offer flexibility. However, unlike other vendors, BeyondTrust imposes a limit on the number of target systems for the per user licensing model.*
- *Product: Password Safe is weak in terms of service account management and lacks an SDK that clients could use to create custom connectors for password rotation. For that purpose, it offers only a command line interface that leverages SSH or Telnet. This reduces scalability and makes it more difficult to integrate with external systems when BeyondTrust does not ship a connector with its product.*
- *Adoption rate in PAM market: Although BeyondTrust has been very successful at selling its less-capable Privileged Remote Access product, which is focused*

on midsize enterprises and remote access use cases, adoption of Password Safe has fallen behind that of its main competitors in terms of growth.

Broadcom (Symantec)

Broadcom (Symantec) is a Niche Player in this Magic Quadrant. It sells a product called Symantec Privileged Access Management that offers PASM, as well as PEDM capabilities for UNIX, Linux and Windows. The product is available as a hardened appliance either on dedicated physical hardware or as a virtual image in multiple formats.

This vendor's operations are geographically diversified.

Symantec previously sold its PEDM product separately under the name PAM Server Control. Symantec is planning to strengthen its app2app capabilities.

Strengths

- *Scalability: Symantec Privileged Access Management has very efficient and scalable session management. It can handle many simultaneous connections with low hardware requirements.*
- *Pricing: Symantec's PAM offering is priced competitively, with almost all pricing scenarios below — and sometimes well below — the average for the market as a whole. In Symantec's case, Gartner evaluated list and street pricing for clients without a portfolio license agreement.*
- *PEDM: Symantec has a good range of PEDM support for Windows, UNIX and Linux, with excellent feature sets that include file integrity monitoring.*
- *Clustering: Symantec's product has excellent clustering and high-availability features that support the addition of nodes without having to take a cluster down.*

Cautions

- *Absence of SaaS: Symantec does not have a SaaS offering for its PAM solution, nor does it plan to offer one.*
- *Connectors: For complex service account credential management, Symantec relies on its Custom Connector Framework, but this means that customers sometimes have to develop custom connectors, whereas other vendors offer out-of-the-box connectors.*
- *Privileged task automation: Symantec's PTA capabilities are basic. For most of the evaluated PTA scenarios, Symantec points toward its APIs, which requires customers to develop their own automations.*
- *Innovation: Although Symantec's innovation has focused on making its products easier to deploy, overall the vendor has fallen behind most other vendors in this Magic Quadrant in terms of differentiating innovations.*

Centrify

Centrify is a Leader in this Magic Quadrant. The Centrify Privileged Access Service is available as SaaS and focused on PASM, whereas Centrify Privilege Elevation Service has PEDM capabilities. The vendor also offers directory bridging through the Centrify Authentication Service.

Centrify's operations are mostly focused on the Americas and Europe.

Centrify was traditionally AD-centric, but its technology can now be used with other directory servers.

In early 2021, after the cutoff date for this research, Centrify was acquired by TPG, a private equity firm, and announced a merger with Thycotic (a vendor evaluated separately in this Magic Quadrant). Gartner's evaluation of Centrify in this Magic Quadrant reflects its position before the acquisition and merger.

Strengths

- *Directory bridging: Centrify offers best-in-class directory bridging capability for UNIX and Linux, and accommodates complex AD configurations.*
- *Customer experience: Centrify's customers rate it highly for support, and the vendor makes extensive support and training programs available. All manuals are accessible online without registration.*
- *Integration: Centrify offers mature APIs and has many out-of-the box integrations with other security tools, as well as with DevOps, RPA and IT service management (ITSM) tools.*
- *Machine authentication: A feature called Delegated Machine Credentials simplifies the authentication process for machine identities. It also provides a secure, contained approach for machine-to-machine authentication without requiring direct access by applications to cleartext credentials.*

Cautions

- *Discovery and service account management: Centrify's privileged account discovery and service account management capabilities are basic. Only the most common credential rotation scenarios are supported out of the box, which means clients have to use scripting to support more advanced scenarios.*
- *macOS: Centrify offers no PEDM support for macOS, nor is sandboxing supported for Windows applications.*
- *Product strategy: With the merger of Centrify and Thycotic, product lines, channels and departments are likely to be consolidated. Clients are advised to seek clarity on the vendor's product strategy and roadmap before any major purchase.*
- *Operations: Centrify is the only vendor in this Magic Quadrant that has fewer staff than since our evaluation for the 2020 edition of this Magic Quadrant.*

CyberArk

CyberArk is a Leader in this Magic Quadrant. Its Privileged Access Manager product offers PASM capabilities as software or SaaS. For PEDM, CyberArk offers Endpoint Privilege Manager (EPM) for Windows and Mac as SaaS, and On-Demand Privileges Manager (OPM) for UNIX and Linux as software. Secrets management is offered via a software product called Secrets Manager, which includes technology acquired from Conjur.

CyberArk's operations are geographically diversified.

CyberArk plans to build new capabilities for extending just-in-time (JIT) access methods to virtual machines and cloud services. It also plans to build new features for controlling and monitoring access to web applications.

Strengths

- ***Success in PAM market: CyberArk remains the biggest PAM brand, with a long history in this sector, a wide geographic reach and the largest share of the PAM market. Most Gartner clients researching PAM products include CyberArk on their list of vendors to evaluate.***
- ***Innovation: CyberArk has a history of being first to deliver innovations to the market. At present, it is the only PAM vendor offering CIEM functionality.***
- ***Integration: CyberArk has a large partner ecosystem, and has delivered many connectors and integrations with adjacent technologies, such as ITSM and identity governance and administration (IGA) tools.***
- ***Product: CyberArk is able to support complex use cases and its PAM products receive consistently high scores in Gartner's technical evaluations.***

Cautions

- ***Customer experience: CyberArk customers have shared concerns with Gartner about poor ease of use and difficulty of deployment for the software version of the product, to the extent of reporting that even software upgrades often require professional services. Rather than fixing these issues, CyberArk is urging existing and prospective clients to move to the SaaS versions of its products.***
- ***Pricing: CyberArk's products are among the most expensive on the market. Additionally, CyberArk has discontinued the software version of its Windows EPM product, forcing all clients to subscribe to a SaaS model over time.***
- ***High availability: CyberArk's disaster recovery and high-availability features are complex to set up and operate. Disaster recovery, especially failback support, is brittle, relies on manual processes and has been a source of customer complaints for a long time.***
- ***UNIX and Linux: CyberArk's PEDM and directory-bridging capabilities for UNIX and Linux are inferior to those of its main competitors, both in terms of deep control mechanisms on a system call basis and the ability to support more complex AD configurations.***

Krontech

Krontech is a Niche Player in this Magic Quadrant. It sells multiple products as software under the Ironsphere 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's operations are mostly focused on Europe and North America.

Krontech's roadmap includes plans to extend its capabilities for Windows PEDM and to develop extensive PAM capabilities for IoT devices, including agent-based capabilities for Linux IoT devices.

Strengths

- ***Scalability: Krontech is well-positioned for large, heterogeneous environments, such as those of telcos, and has a highly scalable architecture that supports massively parallel credential rotation.***

- ***Database controls: Krontech goes further than other PAM vendors by supporting extensive SQL filtering and data-masking controls for monitoring and controlling privileged database access.***
- ***Session auditing: Krontech provides full optical character recognition (OCR) for captured graphical sessions, enabling auditors to search for artifacts, displayed on screens during activity, that would otherwise be difficult to find.***
- ***Service provider offering: Krontech has developed a multitenancy feature for its solution that it offers directly to customers, in contrast to other vendors. This gives service provider customers the ability to provide PAM as a service for various groups requiring PAM services, inside or outside a company, but with isolation established between those groups.***

Cautions

- ***Pricing: For most of the PAM scenarios evaluated for this Magic Quadrant, Krontech's offerings cost more than the industry average.***
- ***PEDM: Krontech offers only basic PEDM functionality for UNIX, Linux and Windows, and none at all for macOS. Nor does it support application allow/deny controls, sandboxing or file integrity monitoring.***
- ***Cloud operations: Krontech has no SOC 2 Type 2 or ISO 27001 certification, even though it offers some of its solutions as a service.***
- ***Integration: Although Krontech ships a built-in multifactor authentication (MFA) module, integration with external MFA providers is limited to Cisco (Duo), Okta and RSA. No integration with other MFA vendors is available.***

One Identity

One Identity, a Quest Software business, is a Leader in this Magic Quadrant. Its PASM solution, One Identity Safeguard, comprises three modules called Safeguard for Privileged Passwords, Safeguard for Privileged Sessions and Safeguard for Privileged Analytics. The solution is available within a hardware or software appliance, or as SaaS. One Identity also offers PEDM for UNIX and Linux via software called Privilege Manager for UNIX, in addition to an alternative product that integrates with the native UNIX/Linux sudo tool, called Safeguard for Sudo. PEDM for Windows is also available via software called Privilege Manager for Windows.

One Identity's operations are geographically diversified.

One Identity plans to close gaps with other leading solutions for SaaS-based remote privileged access, and to extend its offering for sudo.

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.***
- ***Integration: With Safeguard for Sudo, One Identity provides strong support for sudo functionality on UNIX and Linux at a lower price than, and as an alternative to, Privilege Manager for UNIX.***
- ***Analytics and session auditing: 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 behavioral biometric analysis can detect unauthorized use through keystroke dynamics.

- *Market understanding: One Identity understands, and has a strategy to solve, the problem of how to detect hard-to-find embedded Windows service accounts, although this requires the purchase of additional tools, such as Quest Change Auditor and Quest Enterprise Reporter.*

Cautions

- *Service account management: One Identity Safeguard's service account management capabilities are basic. Some advanced features require the creation of custom system connector logic.*
- *Deployment: One Identity's on-premises PASM product is distributed over two different appliances, each using an entirely different technology stack.*
- *Pricing: Pricing for One Identity products is uneven. Smaller clients with less complex scenarios profit from a solution that costs less than the industry average, but costs for larger, more complex scenarios tend to exceed the average. Large enterprises, or those that plan to grow their deployments significantly over time (both in size and functionality) should carefully examine projected costs.*
- *Product strategy: One Identity requires the purchase of additional products, such as Active Roles, to support JIT PAM and privileged identity governance and administration use cases that other vendors support with their main PASM product.*

senhasegura

Senhasegura is a Challenger in this Magic Quadrant. Its PASM product, senhasegura PAM Core, is available as software or as a service. PEDM for Windows and Linux is available in a software offering called senhasegura.Go. Secrets management is sold as software or as a service under the name DevOps Secrets Management.

Senhasegura's operations are mostly in Latin America and Europe.

Senhasegura plans to use AI for sensitive data analysis in automation scripts and source code, and to add CIEM features.

Strengths

- *Innovation: Senhasegura has rapidly improved its capabilities and delivered many new product features over the past year. It now has one of the most technically advanced PAM solutions.*
- *Product: Senhasegura is best in class for account discovery and onboarding, and for privileged task automation.*
- *Pricing: Senhasegura's pricing is highly competitive, with quotes for pricing scenarios below the average for all evaluated scenarios.*
- *Customer experience: Senhasegura's offering has been awarded a Customers' Choice distinction on Gartner's Peer Insights platform. Customers have shared positive feedback about its ease of use, user-friendly interface and rapid deployment functionalities.*

Cautions

- ***Professional services: Senhasegura has the smallest professional services team of any vendor in this Magic Quadrant. This limits its ability to support deployments by clients who prefer the vendor to deliver services.***
- ***Operations: Senhasegura offers its products as SaaS, but does not have SOC 2 Type 2 or ISO 27001 certification.***
- ***Geographic strategy: Although senhasegura is very popular in Latin America, its footprint in North America and EMEA is much smaller.***
- ***Product strategy: Despite a marked improvement since our evaluation for the prior edition of this Magic Quadrant, senhasegura still has the least documentation of any vendor evaluated.***

Thycotic

Thycotic is a Leader in this Magic Quadrant. Its Secret Server product is focused on PASM capabilities and available as software or SaaS. Gartner only evaluated the Platinum edition of Secret Server. In addition, its Privilege Manager offers PEDM capabilities for Windows, Linux and macOS. Thycotic also offers secrets management as SaaS under the name DevOps Secrets Vault.

Thycotic's operations are geographically diversified.

In early 2021, after the cutoff date for this research, Thycotic was acquired by the private equity firm TPG and announced a merger with Centrify (a vendor evaluated separately in this Magic Quadrant). Gartner's evaluation of Thycotic reflects its position before the acquisition and merger.

Strengths

- ***Privileged account life cycle management: Unlike most other vendors in this Magic Quadrant, Thycotic offers in-depth identity life cycle management for service accounts, although this requires the purchase of a separate tool, Thycotic Account Lifecycle Manager.***
- ***Viability/sales execution: Thycotic is one of the fastest-growing vendors in this Magic Quadrant, and is frequently evaluated by Gartner clients.***
- ***Innovation: Thycotic has delivered many new features in the past year. These include automated remediation for defined events (such as automatically alerting and disabling of users that have obtained administrator rights outside the PAM system), web session recording and extension of its secrets management capabilities.***
- ***Product strategy: Thycotic sells add-on products to extend privileged access controls to web consoles (Cloud Access Controller) and databases (Database Access Controller) with extensive filtering capabilities.***

Cautions

- ***Pricing: Thycotic's pricing is consistently among the highest of the vendors in this Magic Quadrant, across multiple pricing scenarios. There is a hard limit of 10,000 secrets (regardless of the number of users licensed) for Secret Server Cloud (but not for the on-premises version). Additional capacity for secrets requires additional payment.***
- ***Product: Thycotic relies heavily on scripting. It leaves it to customers to develop, or pay Thycotic's professional services to develop, capabilities through customizations that other vendors offer out of the box.***

- ***Product strategy: With the merger of Centrify and Thycotic, product lines, channels and departments are likely to be consolidated. Clients are advised to seek clarity on the vendor's product strategy and roadmap before any major purchase.***
- ***PEDM: Thycotic Privilege Manager does not offer file integrity monitoring.***

WALLIX

WALLIX is a Challenger in this Magic Quadrant. The WALLIX Bastion PAM solution provides PASM capabilities and is available as software or SaaS. In addition, PEDM capabilities for Windows, UNIX and Linux are available as software under the name WALLIX BestSafe.

WALLIX's operations are mostly focused in EMEA and North America.

WALLIX plans to extend and diversify its cloud offering.

Strengths

- ***Session management: WALLIX Bastion is an excellent fit for organizations that are primarily looking for session management and recording. It 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.***
- ***Ease of deployment: WALLIX Bastion is simple to deploy and comes in several form factors, including prebuilt virtual images. The solution features good disaster recovery and high-availability capabilities.***
- ***Pricing: WALLIX's pricing tends to be competitive. Smaller clients with less complex scenarios profit from a solution that costs less than the industry average. Pricing for larger, more complex scenarios tends to be similar to that of WALLIX's main competitors. However, large enterprises, or those that plan to grow their deployments significantly over time (both in size and added functionality) should carefully examine projected costs.***
- ***Secrets management: Unlike most other vendors that require vulnerable API keys to be stored by applications, WALLIX's AAPM uses comprehensive agent-based application fingerprinting. This method can effectively eliminate any static credentials from applications or scripts.***

Cautions

- ***Credential rotation: WALLIX's service account management is below average, with support for complex service account credential management absent (and not on the vendor's roadmap).***
- ***Discovery: Account discovery features are limited and focus mostly on AD scanning.***
- ***UNIX and Linux: WALLIX BestSafe does not support macOS and has only basic PEDM functionality for UNIX and Linux. It does not support application allow/deny controls or sandboxing, or file integrity monitoring.***
- ***Geographic strategy: Although WALLIX is popular in EMEA, its footprint in other regions is 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

None

Dropped

- *Hitachi ID Systems sells a PASM solution called Bravura Privilege as software or as a managed service. It did not meet this Magic Quadrant's requirement for agent-based PEDM for UNIX, Linux or Windows. The vendor did not deliver PEDM functionality by the cutoff date for this Magic Quadrant.*
- *ManageEngine sells Password Manager Pro, a basic PASM solution, and PAM360, which builds on Password Manager Pro but focuses on more advanced capabilities and includes SSH key and Secure Sockets Layer (SSL) certificate management capabilities. Another product, Access Manager Plus, provides stand-alone remote access for privileged users. ManageEngine has been dropped because, although it offers a basic application control agent for Windows called Application Control Plus, that product did not fulfill the minimum requirement for PEDM capabilities by the cutoff date for this Magic Quadrant.*

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 (PASM). Vendors that do not provide this function will not be included in the Magic Quadrant for Privileged Access Management.*
- *Mandatory: Privileged elevation and delegation management (PEDM) by host-based agents for UNIX/Linux and/or Windows operating systems.*
- *Optionally, a vendor may also offer secrets management.*

The vendor's solution must meet the following minimum capabilities as of 31 January 2021:

- *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.*

- ***Host-based PEDM tools that provide command control (filtering) and privilege elevation, by 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, or group elevation tools, are explicitly excluded from this definition.***
- ***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.***
- ***All tools and features to be considered must be fully documented, including the documentation of the configuration (if applicable), as well as 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.***

To further qualify for inclusion in the 2021 PAM Magic Quadrant, the respective vendors must meet the following criteria:

- ***Revenue:***
    - ***Have booked a total revenue of at least $9 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 2019 and 31 December 2020, or***
    - ***Have booked a total revenue of at least $7 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 2019 and 31 December 2020 and 25% year-over-year revenue growth.***
- ***Deployment:***
    - ***Have at least 150 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 a separate customer), or***
    - ***Have at least 120 distinct customers for PAM products and subscriptions and 25% 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; 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.***

With respect to the previous year's Magic Quadrant, the minimum revenue and customer counts for inclusion were increased in line with market forecasts. Also, a PAM vendor had to offer at least one agent-based PEDM product, either for UNIX/Linux or for Windows (in last year's evaluation, this was optional). This is because agent-based PEDM solutions provide a more granular and deeper control surface for command control and system call monitoring (such as file integrity monitoring, or detecting changes that administrators or scripts may make to configuration files). Also, all vendors covered in last year's Magic Quadrant analysis either already had PEDM tools or mentioned plans to deliver them on the near-term roadmap.

Honorable Mentions

Fudo Security sells Fudo PAM, a PASM product with advanced session management capabilities, including AI-based behavioral analytics. Fudo Security is not included in this Magic Quadrant because it did not meet the technical inclusion criteria for agent-based PEDM.

HashiCorp offers a stand-alone secrets management solution called Vault, and has recently introduced another product called Boundary that supports session management and basic PASM use cases for interactive access. HashiCorp did not meet this Magic Quadrant's technical inclusion criteria for agent-based PEDM, or for discovery and service account management.

Microsoft offers several PAM features in its offerings. Azure Active Directory Premium P2 contains a privileged identity management (PIM) capability focused on JIT elevation of privileged sessions upon approval for roles in Azure AD and Azure infrastructure. A similar mechanism is available for Microsoft 365. In addition, Microsoft offers a freely downloadable Local Administrator Password Solution (LAPS) that stores passwords for local administrator accounts in Active Directory and makes them available to administrators upon approval. Although it supports some aspects of PAM, Microsoft did not meet this Magic Quadrant's technical inclusion criteria for agent-based PEDM. It also lacked discovery and service account management features.

Remediant offers a PAM product that uses an innovative approach to JIT PAM, one that removes standing access whenever possible. Remediant did not meet this Magic Quadrant's technical inclusion criteria for agent-based PEDM or service account management.

Saviynt sells a product called Cloud Privileged Access Management that offers PASM capabilities and comes with built-in CIEM capabilities. Saviynt did not meet this Magic Quadrant's technical inclusion criteria for agent-based PEDM.

Teleport takes a different approach to PAM in multicloud scenarios by creating a virtual privileged access mesh and targeting four main access use cases: SSH, Kubernetes, web applications and databases. Teleport did not meet this Magic Quadrant's technical inclusion criteria for agent-based PEDM, or for discovery and service account management.

Xton Technologies sells Xton Access Manager, 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. Xton did not meet this Magic Quadrant's technical inclusion criteria for agent-based PEDM.

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 credentials for 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. 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. 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 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 (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 capability 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. PTA 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 guardrails by checking input against policies and settings.***
- ***Privilege elevation and delegation for UNIX/Linux: This capability provides host-based functions and features for enforcing policies on UNIX/Linux systems and macOS 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).***
- ***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, in effect 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.***
- ***Adjacent system integration: This capability requires the ability to provide functions and features to integrate and interact with adjacent security and service management capabilities. Systems include IGA, SSO, MFA, enterprise directories, support for flexible connector and integration frameworks, general API access, integration with ITSM systems, SIEM systems and vulnerability management systems.***
- ***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, 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 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 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. 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, 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). 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

Enlarge Table

-

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

Source: Gartner (July 2021)

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 with 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 in terms of use of appropriate networks. These include direct and indirect sales, marketing, service and communication and partners that extend the scope and depth of market reach, expertise, technologies, services and the vendor's 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 evaluated 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, value-added resellers, system integrators) 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

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 (July 2021)

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 as Leaders do. Due to smaller size, there may be initial concerns among some potential buyers regarding long-term viability.

Challengers have not yet demonstrated the feature completeness or maturity, 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.

Visionaries

Visionaries provide products that meet many PAM client requirements. Visionaries are noted for their innovative approach to PAM technology, methodology and/or means of delivery. They may have unique features, and may be focused on a specific industry or specific 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 methodology. They may focus on specific industries, or customer segments, and can actually outperform many competitors. They may focus their PAM features primarily on specific use cases, 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, a geographically limited footprint or other factors that inhibit them providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. 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

Before making any selection of a PAM tool, buyers should pause and consider the following hard questions:

1. *What changes to the current operational model (process and practice) for privileged access are you willing to consider?*
2. *Is there a clear roadmap to include machine identities, and not just people, when managing account credentials and privileged access?*

One of the top drivers for PAM is to protect the business by reducing the attack surface. Another important driver is to enable the business for change and thus promote agility. Just buying a PAM tool without changing how privileged access is

granted and used leaves organizations exposed. There are many stories of organizations being breached or hacked despite using PAM tools. Usually, such incidents can be avoided if the tools are used correctly.

Deploying a PAM tool properly requires two major things: A clear understanding of where the privileged accounts are (with a roadmap to secure them) and organizational process change to maximize the effectiveness of privileged access controls. To do this, organizations should put in place comprehensive privileged account discovery practices to understand what privileged access exists in their environment, and then define how privileged access will happen.

Here are some very common mistakes:

- *A focus on privileged access by people only or on a narrow use case (for example, only for Windows administrators). Where's the problem? This approach leaves a considerable amount of privileged accounts unaddressed.*
- *A tendency to use personal, highly privileged accounts (for example, domain admin). Where's the problem? Personal privileged accounts violate the principle of least privilege because they are "always on" and usually carry too many privileges. With modern PAM tools, accounts can be shared among multiple people using a JIT approach, with full accountability.*
- *A failure to take modern cloud and development use cases into consideration. Where's the problem? New use cases like DevOps, continuous integration/continuous delivery (CI/CD) can introduce new attack vectors and vulnerabilities that PAM can help mitigate.*

In terms of process and practices, when deploying a PAM tool, SRM leaders should follow Gartner's Best Practices for Privileged Access Management Through the Four Pillars of PAM:

- *Track and secure every privileged account.*
- *Govern and control access.*
- *Record and audit privileged activity.*
- *Operationalize privileged tasks.*

Market Overview

Market Size and Drivers

Gartner estimates that the PAM market revenue for the vendors covered in this Magic Quadrant was $1.5 billion at the end of 2020, representing a growth of 12% over 2019. Readers, particularly investment 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. The market will continue to witness increased interest for the coming two to three years and the worldwide market, measuring buyer spending, is expected to reach $2.7 billion by 2025 (see Forecast: Information Security and Risk Management, Worldwide, 2019-2025, 2Q21 Update).

The growth is mainly driven by the increasing awareness among security staff regarding criticality of PAM solutions. Several high-profile breaches have been

linked to compromised privileged account credentials. Coupled with this, the accelerated migration to cloud, blurring enterprise security perimeters and the overall increase in the number of cyberattacks all contribute to the growth of PAM adoption.

The PAM market has also witnessed heightened interest due to the pandemic-driven sudden shift to remote work of privileged users (both employees and contractors/consultants). Use of PAM tools to enable privileged remote access is the recommended best practice to meet remote privileged access compliance requirements and mitigate remote-access-associated security risks. This has resulted in increased sales of remote-access-focused products, as compared with other PAM capabilities. Vendors, accordingly, prioritized development of remote access capabilities over others.

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 also seeing a shift toward the adoption of SaaS-based solutions, albeit with regional variations and, in some cases, managed service offerings.

Also, a significant majority of the early adopters of PAM — the large enterprises — are looking to increase their PAM maturity to extend beyond basic use cases. In order to address these advanced needs, vendors have doubled down on capabilities such as secrets management, JIT PAM, privileged task automation 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 vendors that offer stand-alone secrets management or CIEM products.

Market Dynamics

Competition in the PAM market remains intense owing to the presence of a large number of players. In the past few years, the market has been moving continuously toward consolidation. The recently announced Thycotic and Centrify merger to form ThycoticCentrify is also another sign of this trend.

The market will also likely be impacted by convergence within the overall identity and access management (IAM) market. Access management vendors are adding some lightweight PAM capabilities to their platforms to help address certain PAM needs of organizations that do not yet require a full-blown PAM solution (similar to what those vendors are already doing with IGA capabilities). At Oktane21, Okta announced a formal venture into both the PAM and IGA markets with, respectively, Okta Privileged Access and Okta Identity Governance. Both products are slated to be launched in 1Q22. Microsoft has also introduced elements of light PAM and identity governance with a privileged identity management (PIM) capability and Azure Active Directory (Azure AD) Identity Governance, available with an Azure AD Premium P2 license.

PAM vendors have also reacted to this shift with product launches and acquisitions of their own. CyberArk acquired Idaptive, an AM vendor. To bridge the gap between legacy IGA and PAM solutions, Thycotic launched an Account Lifecycle Manager product to enable governance and life cycle management for service accounts.

Geographic and Vertical Trends

North America and Europe still remain the primary markets for PAM products. However, the broader Asia/Pacific region has also exhibited increased interest and sales. Global enterprise vendors — such as Broadcom (Symantec), CyberArk and, somewhat aspirationally at the moment, BeyondTrust and Thycotic/Centrify — are increasingly attempting to diversify their geographic reach to extend to all regions. Once there, they'll be met by strong regional vendors: ARCON in the Middle East and the Asia/Pacific region, 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.

Diversified financial services (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 both risk and the heavy compliance load faced by these industries, as well as auditor requirements. Although PAM is typically a horizontal solution, with increasing demand from healthcare, manufacturing and natural resources, an emerging need from a vertical standpoint is for specific features for organizations using the 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.

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.