ISSUE 2

PAM Solutions Center

Privileged Access Management Research & Solutions

Magic Quadrant for Privileged Access Management

Privileged access management is one of the most critical security controls, particularly in today's increasingly complex IT environment. Security and risk management leaders must use PAM tools in a long-term strategy for comprehensive risk mitigation.

Strategic Planning Assumptions

By 2022, more than half of enterprises using privileged access management (PAM) tools will emphasize just-in-time privileged access over long-term privileged access, up from less than 25% today.

By 2021, 40% of organizations (up from less than 10% in 2018) that use formal change management practices will have embedded and integrated PAM tools within them, significantly reducing the overall risk surface.

By 2021, over 50% of organizations using DevOps will adopt PAM-based secrets management products, rising rapidly from less than 10% today.

Market Definition/Description

PAM tools help organizations provide secure privileged access to critical assets and meet compliance requirements by managing and monitoring privileged accounts and access. PAM tools offer features that enable security and risk leaders to:

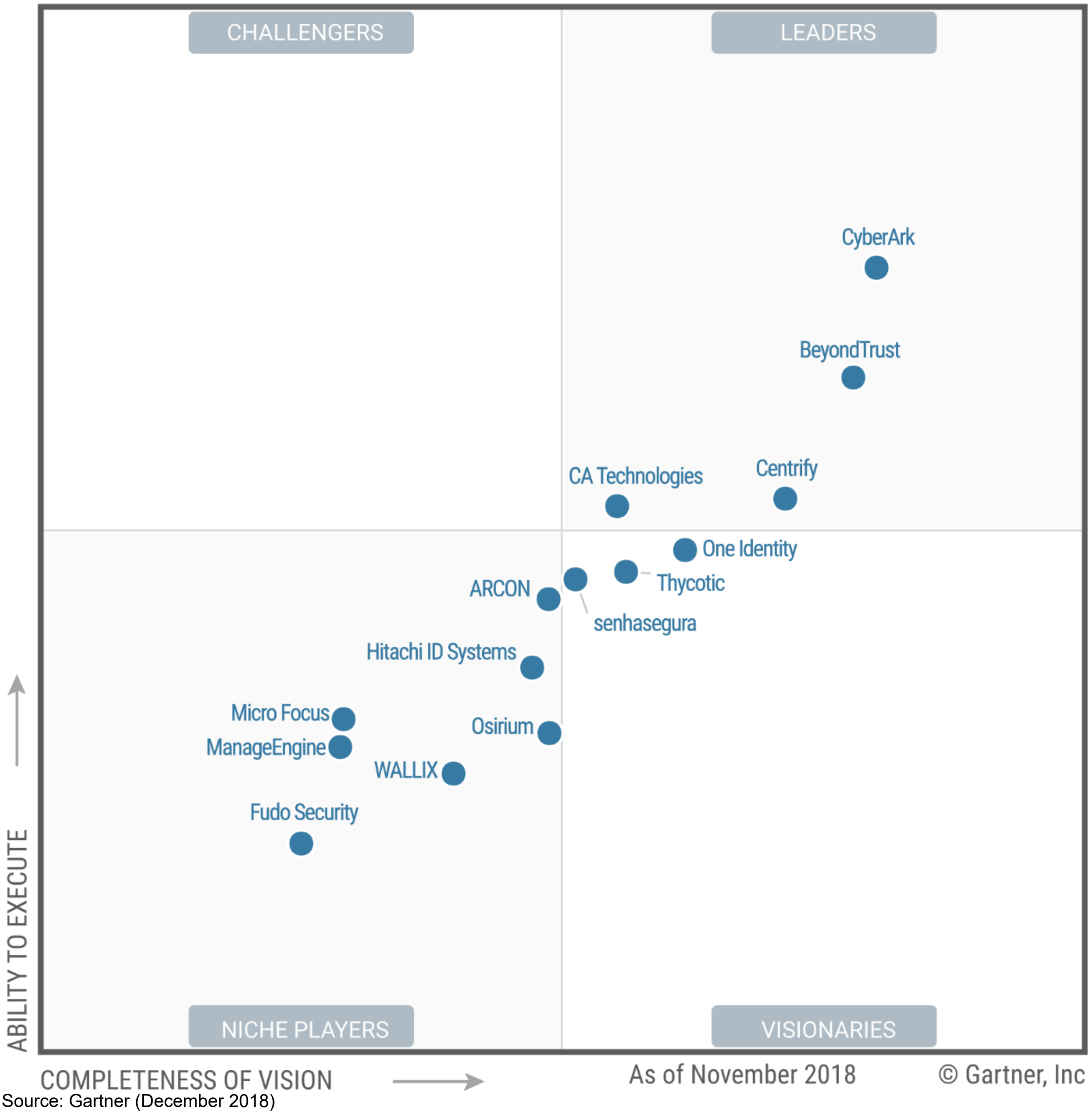
- For all use cases:
  - Discover privileged accounts on systems, devices and applications for subsequent management.
  - Automatically randomize, manage and vault passwords and other credentials for administrative, service and application accounts.
  - Control access to privileged accounts, including shared and "firecall" (emergency access) accounts.
  - Isolate, monitor, record and audit privileged access sessions, commands and actions.
- For human users:
  - Provide single sign-on (SSO) for privileged sessions, commands and actions securely to not reveal account credentials (passwords, cryptographic keys, etc.).
  - Delegate, control and filter privileged operations that an administrator can execute.
  - Ensure required levels of trust and accountability for privileged access by providing robust authentication capabilities or integrating with external authentication products or services.
- For services and applications:
  - Eliminate hardcoded passwords by making them available on-demand to applications. Two distinct tool categories have evolved as the predominant focus for security and risk management 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 also provide application-to-application password management (AAPM).

- **Privilege elevation and delegation management (PEDM).** Specific privileges are granted on the managed system by host-based agents to logged in users. This includes host-based command control (filtering) and privilege elevation, the latter in the form of allowing particular commands to be run with a higher level of privileges. Vendors covered in this Magic Quadrant must at least provide a fully functional PASM product and, optionally, PEDM tools as well. In the write-ups 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 (December 2018)

Vendor Strengths and Cautions

ARCON

ARCON offers a suite that spans both PASM and PEDM. Service account management is above average compared to competitors' offerings (see the entry for "service account management" under "Product or Service" in the Evaluation Criteria section to see what was evaluated). It can manually configure dependencies, multithreaded credential checking and rotation with pre-/postactions. Discovery capabilities include system discovery and privileged user discovery on systems and several databases. ARCON also supports indirect discovery on remote segments via gateways. The product features Secure Shell (SSH) management and discovery of keys in SSH authorized_keys files. The solution can change credentials in configuration files. There is also a REST interface that allows applications to pull passwords from the vault, but it relies on applications to keep a username and password for authentication to the vault.

PSM functionality is based on a secure gateway approach. The solution requires the use of special provided client access tools, which are essentially customized versions of SSH, RDP and SQL clients.

ARCON PEDM consists of agents installed on Windows or UNIX/Linux systems to provide granular control for command execution. ARCON UBA is a reporting tool with some user and entity behavior analytics (UEBA) capabilities that can leverage machine learning to baseline privileged account access (but not commands or operations) to pinpoint anomalies. When ARCON PEDM and ARCON UBA are used in combination, they can send alerts when attempts are made to execute critical or dangerous commands.

The ARCON suite is available as software. It requires Microsoft Windows Server 2012 R2 and above, as well as a Microsoft SQL server 2012 R2 Standard Edition and above. ARCON's PAM solution natively supports multitenant configurations and is offered as a managed service by selected ARCON partners.

Strengths

- ARCON is able to filter SQL commands and can log SQL for database administrator access.
- 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.
- ARCON enjoys high penetration in the Middle East, Southeast Asia and Asia/Pacific regions, offering a mix of direct and indirect sales and support teams in the regions.
- 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

- ARCON's PAM solution requires the use of specialized client access tools, which can cause push-back from long-term administrators who will want to continue utilizing familiar access tools, such as SSH and RDP clients.
- ARCON still supports the use of an unsecure Java plug-in for its Client Manager. However, clients can use an ActiveX component instead for the same purpose.
- 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.

BeyondTrust

BeyondTrust offers a comprehensive suite of PAM products under the PowerBroker brand. BeyondTrust PowerBroker Password Safe (PBPS) is a PASM solution that uses a jump server approach for session management. Service account management and discovery functionality are well above average, and BeyondTrust offers some of it as a free stand-alone tool called PowerBroker Privilege Discovery and Reporting Tool (DART). Basic SSH key management is available. AAPM functionality is included, but relies on applications to keep a static key for authentication from the vault.

BeyondTrust also offers a PEDM solution for multiple systems. PowerBroker for UNIX & Linux (PBUL) includes Active Directory bridging for UNIX/Linux systems, which can also be acquired stand-alone as PowerBroker Identity Services (a free, but feature-limited version is also available). PowerBroker for Sudo is an alternative solution that extends native sudo for centralized policy management. PowerBroker for Windows (PBW) and PowerBroker for Mac implement command filtering for the respective operating systems. PowerBroker for Networks provides command filtering on a protocol basis for network devices and industrial control systems.

All products are built around a component called BeyondInsight, which is bundled with every PowerBroker product. BeyondInsight provides comprehensive discovery functions, and a unified management, reporting and threat analytics environment for several BeyondTrust solutions. Vulnerability management features can be added as an option.

PBPS is delivered as software, or as a virtual or hardware appliance. It is also available on several IaaS marketplaces (Amazon Web Services [AWS], Microsoft Azure and Google Cloud Platform) using a bring-your-own-license mechanism. BeyondTrust prefers to license PBPS on a per-target basis, but will allow customers to license on a per-user basis upon request. All other products are licensed exclusively on a per-target basis.

In October 2018, Bomgar acquired and merged with BeyondTrust. The new entity will retain the BeyondTrust name. This Magic Quadrant evaluation reflects BeyondTrust's capabilities before the merger was announced. The combined entity has many components and solutions that, if well-integrated, could create one of the most powerful and compelling solutions in terms of breadth and depth within the PAM market.

Strengths

- BeyondInsight, which is bundled with every PowerBroker product, can integrate PAM functions such as discovery with asset and vulnerability management. The synergy of this integration can help organizations reduce the risk surface more rapidly and accurately.
- PBPS's integration with ServiceNow stands out in functionality and advanced features, such as a threat intelligence connector for ServiceNow asset management and integration with PBUL. This allows authorized users to perform specific administrative actions from within ServiceNow without logging in as admins.
- BeyondTrust features file integrity monitoring as part of PBUL and PBW.
- The vendor offers both user- and target-based pricing mechanisms, and the costs for a series of pricing scenarios were below, and frequently well below, industry averages. In contrast, Bomgar, which acquired BeyondTrust, tended to have costs somewhat above industry averages. Prospective customers should monitor for pricing changes postacquisition.

Cautions

- Clients remark that configuration and customization can be complex, and are missing wizard-type flows for common configuration tasks.
- PBPS 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.
- The new merged BeyondTrust entity may undergo significant upheaval as product lines, channels and departments are consolidated. Gartner does not expect BeyondTrust to announce the end of life for any of its core products soon, but some of its PAM products will only be maintained, rather than actively sold and innovated. Clients are advised to seek clarity on the vendor's product strategy and roadmap before any major purchase.

CA Technologies

CA Technologies offers a comprehensive suite of PAM products, consisting of PASM, PEDM and analytics. CA Privileged Access Manager is a PASM product that supports session management flexibly through jump server and proxy mechanisms. Discovery and service account management capabilities are average.

SSH key management is good and can discover other user keys as well. The vendor provides excellent AAPM functionality with an add-on module, CA App to App Manager. The solution includes a module that provides standardized workflow integration with multiple IT service management (ITSM) products, including ServiceNow.

PEDM functionality for UNIX/Linux and Windows systems is provided by a software-based solution called CA Privileged Access Manager Server Control. In addition, the vendor provides some UEBA features through a separate product called CA Threat Analytics for PAM. The product uses machine learning for baselining location of a privileged user, time and duration of activity, system connections, and user history for risk scoring. Alerts can be sent, and privileged users can be locked out or forced to reauthenticate when risk threshold levels are surpassed.

CA Privileged Access Manager is delivered as a self-contained hardware or virtual appliance, the latter supporting a variety of formats, including VHD for VMware, and AMI or VHD for AWS and Azure, respectively. CA Privileged Access Manager Server Control is delivered as software, and requires a relational database (Microsoft SQL Server 2012 or later, or Oracle Database 12c). PASM is licensed on a per-user basis, and PEDM is licensed on a per-target basis.

CA Technologies was recently acquired by Broadcom.

Strengths

- According to the sizing guidelines evaluated, CA Privileged Access Manager has among the most efficient and scalable PSM capabilities that can handle more simultaneous connections than any other product evaluated.
- 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 AWS just-in-time privilege filtering and WAN-based clustering.
- CA's global presence and channel partners allow clients to find support and local skills for PAM worldwide.
- Pricing is very competitive, with quotes for pricing scenarios below, and sometimes well below, the average for the market as a whole.

Cautions

- CA still supports the use of an unsecure Java plug-in for its Client Manager tunneling solution.
- While customer reviews for the CA Privileged Access Manager PASM solution are overwhelmingly positive, reviews for CA Privileged Access Manager Server Control are less so, and contain frequent complaints about policy configuration and deployment complexity.
- The acquisition of CA Technologies by Broadcom is likely to introduce some level of uncertainty into operations as the organizations are integrated. Buyers should ensure that they understand planned product roadmaps and support capabilities postacquisition.

Centrify

Centrify's PAM offering is branded Zero Trust Privilege and offers distinct modules that are available separately. Privileged Access Service is a PASM solution that includes good AAPM features, but below-average discovery and service account management features. Session recording is sold separately as Gateway Session Monitoring. There is no typical SSH management as found in other products; however, Centrify can use file integrity monitoring to watch for modifications to authorized_keys files.

An optional HTML5 access interface allows full privileged access from a web browser without any client tools. Privilege Elevation Service implements PEDM capabilities for UNIX/Linux and Windows. Centrify Authentication Service provides Active Directory bridging for UNIX/Linux systems — this solution is very popular and the Centrify brand is often identified with exactly this feature. The PASM solution is available on-premises or as SaaS, and is licensed on a per-target basis either as a subscription or perpetually.

Centrify also offers analytics services that leverage machine learning to baseline privileged account access and privilege elevation to pinpoint anomalies, and also integrates with multifactor authentication (MFA) as a service, priced separately and licensed per user.

Centrify was recently acquired by private equity company Thoma Bravo, and subsequently underwent corporate restructuring. It spun off its identity as a service (IDaaS) solution as a separate entity called Idaptive. The entity that offers its PAM solutions retains the Centrify name.

Strengths

- Centrify is one of the few vendors that feature a full remote privileged access solution for third-party technicians, making client-installed software such as VPN solutions unnecessary. In Centrify's case, this is delivered as SaaS.
- The vendor features file integrity monitoring as part of its Privilege Elevation Service.
- Centrify integrates with common DevOps tools, including continuous integration/continuous deployment (CI/CD) tools for secrets vaulting as well as privileged command controls.
- Deployment and licensing options are diverse and flexible, and include cloud, on-premises and SaaS-based arrangements, along with metered, perpetual and subscription-based pricing.

Cautions

- Pricing for Centrify products tends to be uneven, with smaller, less complex scenarios tending to cost less than industry averages. In contrast, larger, more complex scenarios tend to exceed those averages. Buyers that plan to grow their deployments over time (both in size and added functionality) should carefully examine projected future costs to avoid “sticker shock.”
- Service account management capabilities are below average among the solutions evaluated. The PASM solution lacks depth in support for complex service account management, such as pre-/postactions or checking whether account credentials have changed. System discovery is mostly limited to Active Directory and network scanning.
- The recent acquisition by Thoma Bravo and the subsequent spinoff of Idaptive have been disruptive, with departures of staff, including those holding senior positions. The partition of the companies has been defined along product lines, causing some features that were not essential, but previously considered to be synergetic, to no longer be under the control of Centrify. Clients are advised to ask for clarity on product roadmaps for the next two years.
- Although the solution is technically well-positioned for global distribution, the bulk of customers and direct support resources are currently located in North America. Customers with significant operations outside of North America should evaluate local support options.

CyberArk

CyberArk sells a comprehensive suite of PAM products. The Core Privileged Access Security Solution (PAS) is licensed on a per-user basis and offers PASM capabilities, including vaulting and session management, and recording that works using a proxy or jump server mechanism. Discovery and service account capabilities are well above average. An optional HTML5 access interface is included to allow full privileged access from a web browser without any client tools. SSH key management is also included. AAPM functionality is excellent, but sold separately as Application Identity Manager (AIM) on a per-target basis, with several editions available and priced differently, depending on the type of integration mechanism.

CyberArk also bundles its Privileged Threat Analytics (PTA) module, a basic UEBA solution. This can also detect suspicious activity and common threat scenarios, such as privileged credential abuse that bypasses PAM controls. A more capable agent-based component called Advanced Domain Controller Protection is priced separately. That component can also detect known attacks on Windows domain controllers, such as “golden ticket” or “pass the hash.”

PAS is sold as a fully self-contained virtual or hardware appliance. Images for Azure, AWS or Google Cloud Platform are also available. CyberArk also offers a free system and privileged account discovery tool called Discovery & Audit (DNA).

PEDM for UNIX/Linux is sold as On-Demand Privileges Manager (OPM) and includes some Active Directory bridging capabilities.

PEDM for Windows is sold as Endpoint Privilege Manager (EPM) on a per-target basis. The solution can either be bought as software or as a service that combines a software agent with a SaaS-based policy control and distribution mechanism.

CyberArk was the first PAM vendor to add a DevOps-focused solution to its portfolio with its acquisition of Conjur in 2017. This resulted in an additional API-enabled vault that easily integrates with CI/CD pipelines, containers and container management solutions.

Strengths

- 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 in their list of vendors to evaluate.
- CyberArk has a history of trendsetting innovations and aggressive expansion of the product line to improve functionality and expand capabilities, often through acquisitions.
- SQL logging and filtering for database administrators is supported as a Privileged Session Manager extension for Toad and Oracle SQL*Plus.
- A revised approach to pricing and product packaging has significantly simplified the acquisition process, making it easier for buyers to understand current and expected costs. While the updated pricing is generally competitive when compared to peers, larger-scale or more complex scenarios can generate costs above market averages.

Cautions

- 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.
- Password rotation and verification does not perform well at scale, which limits flexibility for scheduling credential rotation in large environments, or rotating credentials rapidly to respond to a large cyberattack scenario.
- While CyberArk has invested effort to make its end-user interface more user-friendly, clients remark that its configuration and customization are complex, unwieldy and not well-documented.
- Unlike other vendors that offer Active Directory bridging, OPM does not feature full Kerberos integration or group policy support for UNIX/Linux.

Fudo Security

Fudo Security, part of Wheel Systems, sells a PASM solution called Secret Manager that is sold in conjunction with a privileged session management and monitoring product called Privileged Session Manager. Secret Manager is a relatively new offering that meets the minimum requirements for PASM, but has only very basic functionality for password vaulting, service account management and discovery. Workflow integration with ServiceNow exists.

Privileged Session Manager is highly capable, and this is where the product truly shines. It supports many protocols in gateway, proxy and transparent gateway mode, including Modbus, ICA, HTTPS, RDP, SSH Telnet, VNC and X11. Several database protocols for SQL monitoring are also supported, such as those used with Microsoft SQL Server, MySQL and Oracle.

AAPM functionality is provided through another add-on product of the same name (AAPM module), but relies on applications to keep a static key for authentication from the vault. An optional HA cluster module is also priced separately. Wheel Systems also sells an add-on module called Efficiency Analyzer that can be used to report on productivity for administrators. The vendor claims that it delivers value especially for monitoring productivity of external collaborators.

All Fudo Security solutions are either sold as a hardware appliance or as a virtual appliance. Privileged Session Manager and the HA cluster module are sold on a per-target-based licensing model. AAPM and Efficiency Analyzer are priced as a percentage of Privileged Session Manager. Secret Manager is licensed on a per-user basis.

Strengths

- Fudo Security’s Privileged Session Manager stands out through extensive protocol support and its ability to be deployed as a transparent gateway, allowing it to record activity using different protocols in a transparent way, even without a password vault.
- Privileged Session Manager can provide 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.
- Privileged Session Manager supports SQL logging for databases using the TNS protocol, such as Microsoft SQL Server.

Cautions

- Secret Manager has not yet reached parity with the average product maturity of other vendors covered in this Magic Quadrant. In our evaluation, we consider capabilities for service account management, automation and DevOps integration to be well below average.
- The vendor’s pricing is consistently among the highest on offer from vendors examined for a series of pricing scenarios.
- Fudo Security is a small vendor that heavily relies on its partner network to deliver customer relationship management, including first-line support and, in some cases, even second-level support.

Hitachi ID Systems

Hitachi ID Systems’ Privileged Access Manager is a full-featured PASM product that also has some aspects of PEDM, without direct command control features. Its PASM solution comes with well-above-average discovery and service management features, including a wide selection of templates for discovery and credential rotation. AAPM capabilities and automated high-availability features are very good and are included in the base package. Integration with ITSM systems and other security products is another area where the vendor stands out by shipping with an extensive library of predefined integration packs.

The solution offers session management, including credential injection, session recording and remotely initiated session termination using three distinct, complementary mechanisms. The first is via a browser extension for any modern browser on Windows. A selected admin tool is launched and fed target address and credential information from the vault. The second is via an HTML5/HTTPS web proxy, where an SSH or RDP session is initiated from the proxy to the managed endpoint and its display is rendered into the user’s browser in a new tab. The third is like the first, but after first establishing a virtual desktop infrastructure (VDI) session to a proxy.

Session recording also happens locally, with the capture data streamed to a log server. VDI servers can be used in combination with the aforementioned session initiation options.

A special offering called Identity Express: Privileged Access Edition is a preconfigured and integrated build that delivers a number of scenarios and components with minimal configuration options. These quickly delegate control over how credentials are managed while enforcing corporatewide policies.

Privileged Access Manager is sold as software that is installable on Windows and requires Microsoft SQL Server (any edition). Alternatively, the vendor will provide a virtual instance on IaaS platforms. Managed services are also available as SaaS or on-premises as per customer preference. The solution is licensed on a per-target basis either as perpetual or subscription licensing.

Strengths

- The solution has excellent connectivity, discovery 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, and the ability to place privileged users temporarily into a security group during a session.

- 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.
- 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 rotated one-time keys. This method can effectively eliminate any static credentials from applications or scripts.

Cautions

- Hitachi ID Systems is limited by its lack of marketing investment and subsequent recognition, which causes potential buyers to overlook it.
- 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).
- Pricing is based on the number of target devices under management, and runs above the industry average for a series of pricing scenarios. Hitachi ID Systems also charges a base activation charge, or "vault fee," to all customers. That enables customers to run as many replicas of a single database as required for operational, development and testing purposes.

ManageEngine

ManageEngine's PASM solution is called Password Manager Pro (PMP) and is available in three editions: Standard, Premium and Enterprise. Only the Enterprise version fulfills all of the technical inclusion requirements for this Magic Quadrant and is used as the basis for its evaluation. Discovery capabilities are average, but service account management is below average, and there are no out-of-the-box connectors or integrations for ERP systems or application servers. Unlike most other vendors, however, ManageEngine's service account management leverages a provided agent for enhanced control, supporting Windows and Linux servers, and Windows domain controllers. A less capable agentless mechanism is also available as an alternative. Workflow integrations with ServiceNow, Jira and ManageEngine's ServiceDesk Plus are available.

PSM functions rely on a proxy-based approach, with a browser-based tool for SSH and RDP access. SQL logging is also supported. The solution features full SSH key management. AAPM functionality is included, but relies on applications to keep a static key for authentication from the vault.

PMP requires an external database: either Microsoft SQL Server, MySQL or PostgresSQL. It is delivered as installable software for either Windows or Linux, and is licensed per-administrator either as perpetual software or a subscription. IaaS instances for Azure and AWS are also available.

Strengths

- Clients are very positive about the user-friendly UI and ease of installation and maintenance.
- ManageEngine's pricing for the scenarios it supports consistently undercuts competitors. However, the vendor makes a separate charge for SSH keys being managed by the system, which may inflate costs for some organizations
- PMP features SQL logging for database administrators, as long as they use the interactive web-based SQL client interface through PMP's web gateway.
- ManageEngine's standard support is 24/5 (on workdays), and weekend support can be added for a flat fee of $10,000.

Cautions

- System discovery capabilities are not mature and rely on inadequate mechanisms such as requiring the same SNMP community credential, or only discovering Linux systems using the Telnet protocol. However, database accounts can be discovered on systems that have already been onboarded.
- PSM works exclusively through a web-based client access interface, which is prone to create bottlenecks due to scalability and throughput limitations.

- The solution does not integrate with local access tools, which can cause pushback from long-term administrators who will want to continue utilizing the access tools that they are used to.
- Apart from a general UI rewrite, the vendor has not delivered any innovations over the past 12 months.

Micro Focus

Micro Focus' Privileged Account Manager provides PASM and PEDM functionality. For connectivity to other systems and applications, the solution uses the same connectors as Micro Focus' Identity Manager product. Account discovery features are average, but service account management is well below average. Workflow integrations with ITSM are not available.

The solution has functionality to store and manage disclosure of SSH keys, but does not contain any other SSH management features. AAPM functionality is included, but relies on applications to keep a static key to authenticate to the vault.

Privileged Account Manager uses optional agents for Windows and UNIX/Linux platforms for fine-grained command control PEDM. Proxy servers are provided for RDP, SSH and database monitoring. Session replay and auditing features are excellent. Protocol-based command filtering is available, and can be used for risk scoring.

The solution is delivered as software for UNIX/Linux or Windows and has its own internal data store. It is priced on a per-target basis.

Strengths

- Micro Focus' extensive support for managing privileged access to databases is excellent and goes beyond simple SQL logging and filtering.
- Privileged Account Manager's session management, recording and auditing capabilities are very good, and the solution has excellent search capabilities for specific activity.
- Because of the possibility to use connectors from Micro Focus' Identity Manager, account discovery is supported for an extensive list of systems and applications.

Cautions

- Service account management is rudimentary, and Windows service account credential rotation is not supported in the current version. Privileged Account Manager lacks integration with ITSM systems.
- Pricing is mixed, ranging from below to well above market averages. Buyers should examine competitive bids and assess the value received to ensure they are receiving the best deal.
- For a vendor that is heavily invested in DevOps technology, Micro Focus' lack of credible DevOps integration is surprising.
- Product support is focused on North America, Europe and, to a lesser extent, the Asia/Pacific region, and is provided by a mix of the vendor and its partners. In other regions, support is managed remotely.

One Identity

One Identity offers a suite of PAM products. PASM functionality is provided by its One Identity Safeguard suite, which debuted in 2017 to replace its aging TPAM solution. Its core product is One Identity Safeguard for Privileged Passwords, which is sold as a hardware appliance. One Identity acquired Balabit in early 2018, and technology from that acquisition comprises the other two parts of the Safeguard suite. One Identity Safeguard for Privileged Sessions provides full PSM capabilities, and One Identity Safeguard for Privileged Analytics features full session and activity analytics. Both are sold either as a virtual or hardware appliance.

System and account discovery are supported for UNIX/Linux and Windows, and are average; service account management is below average among the solutions evaluated. SSH key management is limited to rotation of existing keys. AAPM functionality is included, but relies on applications to keep a static key to authenticate to the vault. Workflow integration with Remedy and ServiceNow is available.

One Identity also offers extensive PEDM capabilities: Privileged Access Suite for UNIX features UNIX/Linux and Active Directory bridging and full UNIX/Linux command control. A lower-priced alternative called Privilege Manager for Sudo provides similar capabilities and integrates with the stock sudo command. Active Directory bridging can also be bought separately as Authentication Services. PEDM for Windows is available as Privilege Manager for Windows.

One Identity Safeguard is sold at the customer's option on a per-user or per-system basis, plus a fee per appliance. PEDM capabilities are sold on a per-target basis.

Strengths

- 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.
- 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 biometrics analysis can be used for continuous authentication to detect unauthorized use through keystroke dynamics.
- One Identity shows strong penetration across a variety of verticals, and displays a good grasp of the needs and requirements of different industries.
- The vendor's PAM products possess above-average support for language localization.

Cautions

- Service account management is below average, with advanced features for service account rotation, such as account pools and custom actions, absent.
- One Identity Safeguard's capabilities for automation and DevOps integration are also below average, with features for privileged task automation and secrets management for DevOps tools and containers mostly not present.
- The pricing scenarios evaluated by Gartner tend to be somewhat above average.

Osirium

Osirium's PxM Platform consists of four components. Privileged Access Management and Privileged Session Management are required to fulfill PASM capabilities. Privileged Task Management provides extensive automation and delegation of complex, multistep tasks, allowing organizations to automate and delegate frequently repeated, routine tasks. The effect of this is to minimize the need for human action and decrease the risk for errors and other security breaches, while saving time and costs. Privileged Behaviour Management is an optional analytics component to analyze and automate responses to unusual behavior.

While Osirium does not support system discovery, account discovery is one of the best in class. Service account management is average. AAPM functionality is included, but relies on applications to keep a static key to authenticate to the vault. Workflow integration with ServiceNow is available. SSH management, including SSH key provisioning, is supported.

PSM functions are implemented as a proxy and support HTTPS, RDP, SSH TDS (for Microsoft SQL Server), Telnet and vSphere. A special client is required for privileged access. A Management Application Proxy (MAP) server can support jump server configurations to run remote applications in a terminal service environment. A large library of connectors, predefined tasks and templates is provided for discovery and automation.

Osirium's PxM Platform is sold as a self-contained virtual appliance. It is licensed on a per-target basis and sold as a subscription. Images are also available on the AWS and Azure marketplaces.

Strengths

- Osirium's privileged task management capabilities are best in class of all vendors evaluated.

- Account discovery functions are the most capable of all products covered in this research. However, the solution does not support discovery of new systems that have not been onboarded yet.
- The PxM Platform has ready-made connectors for an extensive number of systems and devices.

Cautions

- Osirium's philosophy for PAM promotes a cultural change from traditional practices that many potential clients are not yet ready to consider. However, clients looking to step up to a higher level of maturity will find that privileged task automation is an evolutionary step from existing accepted practices. This represents a next generation of PAM with clear benefits.
- Osirium's PAM solution requires the use of specialized client access tools on Windows administrator endpoints (although not on macOS administrator endpoints, where alternative access tools can be used). This could cause pushback from long-term administrators on Windows endpoints who will want to continue utilizing the access tools that they are used to.
- Compared to most other products evaluated in this research, the provided documentation touches on all capabilities, but is lacking in detail. Much functionality is moved into templates that are only sparsely documented.
- Osirium products are priced above average, sometimes well above average, for a series of pricing scenarios.

senhasegura

The PAM solution from senhasegura is split up into 17 different modules, including MFA and certificate management. The product is very popular in Brazil and is currently expanding into other international markets. Its PASM solution comes with well-above-average discovery features, including a wide selection of templates for discovery and credential rotation. Assets can also be discovered in virtualized and IaaS environments, such as AWS, VMware ESXi and Microsoft Hyper-V. However, overall service account management is below average. SSH management is also supported, as well as detection of where public keys are stored on individual SSH authorized_keys files. AAPM functionality is available, but relies on applications to keep a static key for authentication from the vault.

PSM supports HTTPS, RDP, SSH, Telnet, VNC and multiple database protocols through a remote connect proxy-based function. Templates for credential injection on web-based applications such as SaaS control panels can be configured. Commands can be filtered, and the solution can send alerts when attempts are made to execute critical or dangerous commands.

PEDM is provided as senhasegura.Go for Linux and Windows. For Windows PEDM, a special launcher is used to run elevated commands, rather than integrating the control into the native user experience.

The senhasegura solution is sold on an a la carte basis using different licensing metrics depending on the modules acquired. The PASM solution is available as a virtual or hardware appliance. PEDM functionality is available as software for UNIX/Linux and Windows.

Strengths

- The vendor's discovery and account mapping capabilities stand out from most other vendors evaluated in this research by the sheer number of predefined connectors and advanced features such as scanning authorized_keys and sudoers files.
- Sizing guidelines indicate that the RDP proxy function is very efficient, supporting more than a thousand simultaneous connections on a high-end hardware appliance.
- The vendor has built functionality to integrate with Docker and Kubernetes, including running discovery tasks in containers and controlling access to the Kubernetes management API.
- 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

- 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 about average compared to market norms, this requires frequent true-ups of license alignments.
- Compared to most other products, the provided solution documentation touches on all capabilities, but is lacking in detail.
- The vendor has few clients outside of Brazil. While senhasegura claims that the product and manual are available in multiple languages, many examples and screenshots are still only in Portuguese.

Thycotic

Thycotic provides an on-premises PASM solution called Secret Server. A separate offering, Secret Server Cloud, is available as a service but does not have the same functional depth as the on-premises version. Secret Server’s discovery features are average: Assets are discovered through network and Active Directory scanning. Accounts can be detected in UNIX/Linux and Windows systems, Microsoft SQL Server, Oracle, and Sybase. VMware ESXi instances can also be discovered and enumerated. It is possible to create custom scripts for discovery and onboarding. A free privileged account discovery tool for Windows is also available.

Service account management capabilities are above average. SSH key management is limited to SSH key rotation and updating of SSH authorized_keys files. AAPM functionality is included, but relies on applications to keep a static key to authenticate to the vault, or using source IP address verification, which offers little protection.

PSM functionality is provided through launchers that run on Windows and macOS administrator endpoints. A proxy is available for SSH. The SSH proxy allows commands to be filtered, and can react when attempts are made to execute critical or dangerous commands. Thycotic provides integration with Remedy and ServiceNow.

Thycotic also sells Privilege Manager, an agent-based PEDM solution for Windows and Mac systems. Thycotic Privileged Behavior Analytics is a UEBA solution that leverages machine learning to baseline privileged account access (but not commands or operations) to pinpoint anomalies. Remedial actions can be taken when thresholds are exceeded, such as logging or locking a user out, forcing two-factor authentication or running a custom script.

Secret Server is available as software for Windows and requires Microsoft SQL Server. The solution is priced per user and comes in three different editions: Vault, Professional and Platinum. Only the Platinum version fulfills all the technical inclusion requirements for this Magic Quadrant, and is used as the basis for its evaluation. Clients that buy a lower-priced edition may add additional functions (that would otherwise only be available in a higher-priced edition) in a modular fashion. Privilege Manager is sold on a per-target basis with a different price depending on whether the target is a server or a user endpoint.

Strengths

- Clients are very positive about the vendor’s technical support, the user-friendly UI, and the ease of installation and configuration.
- Thycotic has a strong standing in the small and midsize business (SMB) market.
- The vendor’s marketing strategy and execution are well-conceived and succeed in consistently reaching potential clients.
- OEM distribution with IBM Security will expand sales and support capabilities throughout the world, making it a more interesting option for geographically distributed organizations.

Cautions

- Pricing is uneven, with different pricing scenarios set at either above or below market averages. Consideration of competitive bids and the functionality provided is necessary to ensure receiving the best price.
- Session recording for RDP does not provide keystroke data or names of executed applications unless special agents are installed on target systems.

- Much of Thycotic's success comes from a strategy that is focused on addressing only initial steps of PAM maturity. The vendor offers several entry-level editions that are inexpensive but do not cover Gartner's minimum requirements for PAM basics, such as session recording and complex service account management.
- Thycotic's standardized professional services bundles are simpler in scope and less effective in terms of the desired end state than those of leading enterprise PAM vendors. Enterprise clients looking to go beyond the bare minimum in terms of PAM maturity are advised to negotiate a customized, more robust professional services deal as part of the purchase.

WALLIX

WALLIX provides a PASM solution, WALLIX Bastion, consisting of several modules. WALLIX Bastion Password Manager implements vaulting and credential management. WALLIX Access Manager provides the administrative portal and workflow capabilities. The freely available WALLIX Discovery can discover certain types of systems and accounts on Windows. However, discovery and service account management capabilities are below average.

SSH key management is available, as well as excellent AAPM capabilities. WALLIX includes workflow integration with Remedy.

WALLIX Bastion Session Manager is the PSM component with one of the most capable session management and recording features. It can work in either proxy or jump server mode. RDP, rlogin, Telnet, and SSH protocols are supported. Proprietary RDP extensions can provide extra metadata for graphical session recording, such as window titles and other UI data. These extensions are compatible with standard RDP clients. Command filtering for SSH is also available. OCR can be applied to graphical session recordings to screen scrape text from UIs into searchable text.

WALLIX Bastion is sold as a hardware appliance, or optionally virtual appliances are available for many hypervisors and IaaS solutions: VMware, Hyper-V, AWS, Azure and OpenStack. Licensing is available on a per-user, per-target or per-simultaneous-connection basis.

Strengths

- 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.
- 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.
- WALLIX offers connectors for certain cyberphysical systems, and has a partnership with Schneider Electric.
- The vendor has expanded senior staff over the last year, in an effort to expand its strength in the European market and to grow in additional geographies, including North America.

Cautions

- Service account management features are below average compared with other PAM solutions, and only a few connectors for databases and business applications are available.
- Automation is also 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 scenarios tend to be above average, although, in contrast with most competitors, a few larger and more complex scenarios tend to be priced below average.

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

This is a new Magic Quadrant; no vendors were added.

Dropped

During the data collection period for this new Magic Quadrant, it was determined that Bomgar would not be included, as it acquired BeyondTrust and merged with that company.

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:

- A secured, hardened and highly available vault for storing credentials and secrets.
- Tools to discover, map and visualize privileged accounts in 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 UIs by privileged users with approval workflows.
- UIs to check out privileged credentials.
- Tools to allow a privileged session to be automatically established using a protocol 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 applications, 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 on privileged accounts and their use.
- Underlying architecture for the above, including connector architecture.
- Products deployed for use with customer production environments for purposes consistent with the objectives of PAM.

To further qualify for inclusion in the 2018 PAM Magic Quadrant, the respective vendors must:

- Have booked total revenue of at least $2.5 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 January 2017 and 1 June 2018. Or they must have at least 50 clients across multiple regions (North America; Latin America, including Mexico; EMEA; Asia/Pacific) as of June 2018 that have paid more than $10,000 each in product or subscription costs.
- Sell and support their own PAM product or service developed in-house, rather than offer it as a reseller or third-party provider.
- Compete in at least two of the major regional markets (Americas; Asia/Pacific; and Europe, the Middle East and Africa).
- Have sold their PAM product or service to customers in different verticals or industries (i.e., vendors that only sell their product within a particular industry or vertical are excluded).

Honorable Mentions

The PAM market contains more vendors than those evaluated in this Magic Quadrant. Several vendors were not evaluated because they do not currently meet one or more of our inclusion criteria. They are:

- Devolutions
- Iraje Software
- Krontech
- MasterSAM
- Novasys
- NRI SecureTechnologies
- Onion ID
- Venustech

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:

Service account management was a heavily weighted subcategory, because this is an area where much risk is concentrated; yet clients often struggle to manage and rotate credentials for nonhuman users. We saw major distinctions between vendors in this area. We evaluated:

- Discovery for systems and devices
- Discovery of accounts on different systems, applications, devices and databases
- The availability of predefined connectors available, and special support for applications or services to rotate credentials while minimizing downtime
- Features and quality of SSH key management
- Special functionality to support IaaS/PaaS
- Features for application-to-application password management, and whether (or how) vendors would be able to eliminate any sort of hardcoded secret (password or application key)

Session management, auditing and analytics was also heavily weighted. Vendors offer different, and sometimes multiple, approaches (or combinations of them) to manage sessions: proxy servers, gateways, agents or jump servers. We evaluated:

- Whether administrators would be able to use their own tools, since lack of this ability will often complicate the acceptance of PAM tools by administrators.
- Support for protocols such as SSH and RDP, as well as additional protocols such as HTTPS, ICA, TDS, Telnet, VNC, X11, etc.
- The ability to filter commands or operations on a protocol basis.
- Session recording and replay capabilities — what could be recorded, and how easy it would be to quickly review sessions, search for particular events or quickly visualize what has been done.
- How a vendor’s offering approaches the use case of remote third-party privileged access. Vendors got points if they offered zero-install options that would provide a secure mechanism to allow remote parties to access systems through a web browser without requiring any additional tools, such as VPNs.
- How logs and recordings were protected, and what measures were taken to avoid logging passwords or credentials.
- The ability for solutions to identify risky or sensitive operations and react to them.

Privilege elevation and delegation management had a medium weight and vendors that had offerings in this area were able to score points in this subcategory. Vendors would score better when they supported multiple different operating systems. We also evaluated:

- Logging features

- Flexible configuration mechanisms for policy-based command and execution control
- Active Directory bridging for UNIX/Linux systems

Features for controlling privileged access to databases had a medium-low weight. Most vendors supported running special database administration tools on jump servers on VDI servers. Other vendors had differentiated capabilities such as SQL logging and filtering. In some cases, vendors even offered capabilities to alert on specific database administration activity, and provide response mechanisms. Data breaches can occur when files are being moved in or out of controlled environments, so vendors could score additional points for being able to control file movements.

Automation and DevOps also had a medium-low weighting. We evaluated:

- Integration with other systems, such as ITSM and CMDB
- Out-of-the-box integrations with other security management and automation tools
- The availability and quality of APIs to support custom use cases
- Support and features for privileged task automation
- Integration with DevOps tools, containers and container management systems such as Docker, Swarm, Kubernetes, etc.

Deployment and integration was weighted low and evaluated by looking at several factors. The overall approach and capabilities of products were evaluated to see how they would make the products easier to deploy. We also evaluated:

- The availability of common extension points and APIs that could be used for customization or integration with other products
- Integration with MFA products and standards, and hardware security modules (HSMs)
- Facilities for troubleshooting and debugging
- Features to facilitate the delivery of upgrades, patches and hotfixes

Scalability and performance was weighted low. Vendors were asked to provide guidelines for product sizing, scaling, fault tolerance and recoverability. Vendors that offered the ability to spread workloads over multiple or specific instances scored extra points. Other factors evaluated include:

- Facilities for the archival of log, session recordings and history information
- Configuration and tuning options to enhance scalability and performance

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 strength of the organization, based on overall size, profitability and liquidity. A vendor's success in the PAM market was 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 company supports customers in the sales process, utilization of direct and indirect channels, a cogent understanding of competitive strengths and weaknesses, 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 10 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, 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 24 months to emerging needs of customers, evolving regulations and competitor activities. We also evaluate responsiveness to market developments of other adjacent technologies, including robotic process automation (RPA), industrial control systems and operational technology security, DevOps, IaaS, and SaaS.

Marketing Execution: Assesses the clarity, quality, creativity and efficacy of programs designed to deliver the organization's message. 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 with technical support, or account support, measured by evaluating customer relationships and services. We are 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 gathered from inquiry, customer interactions and other Gartner data sources.

Operations: Assesses the ability of the organization to meet goals and commitments. Factors include the overall size and quality of the organizational structure; and the presence of processes and programs, supported by relevant certifications where appropriate, supporting quality management, information security, defect resolution and other elements of customer satisfaction. Also included are the skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently. We also evaluated organizational changes, internal processes and the capability to support multiple versions of the product.

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 (December 2018)

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 how well vendors understand buyers' changing requirements, use cases and functional needs. We also evaluated 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. Consideration was also given to the geographical disbursement of marketing activities. 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 by reviewing several factors. First, we evaluated its understanding of its buyers and possibly the unique buyers it targets. Second, we looked at its use of multiple channels to drive sales through direct and indirect sales, marketing, service, and communication. Third, we assessed the vendor's ability to extend its reach through use of implementation partners that further the scope and depth of market reach, expertise, technologies, services and its customer base. Weight was given to those with geographically diverse implementation partners. 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 is weighted heavily. We also measure vendors' future plans to meet customers' selection criteria, and evaluate software development practices, participation in industry or standards organizations, and certifications.

Business Model: Emphasis is given to the design, logic and execution of the organization's business proposition to achieve continued success. Key justifications for continued investments were evaluated, along with stated technical and nontechnical differentiators. In addition, a vendor's ability to establish and maintain partnerships (technology, VAR, SI) is 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, skills and offerings to meet the specific needs of individual market segments, including SMBs, 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 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 year were heavily weighted. We also evaluated previous technical and nontechnical innovations, as well as foundational advancements 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, multilingual 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	Low

Source: Gartner (December 2018)

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

PAM 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 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, 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

As you consider investment in a PAM tool, remember that tool features and functionalities will never mask the lack of a PAM vision, practices and processes in your organization. There are some fundamental concepts that can inform your 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 appropriate 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. You can't manage or control what you 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. 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 success for discovery from PAM vendors. Success in discovering all privileged accounts, including service accounts, both inside and outside of Active Directory, is foundational to a PAM program.

Govern and control access. Develop or acquire an effective identity governance program for PAM access to ensure all changes in accounts, systems and access are accounted for. Decide which kind of control you can be successful in capturing now, and which you 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 access — things like automation, normal users running scripts with privileged access and workflow processes for requesting just in time (JIT) access.

JIT access is an emerging method for privileged access. It is based on the principle that access is granted only for a short period of time 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. It allows individual permissions to be attached to an account for a short period of time. For example, a privileged account receives additional permissions for the time of a particular session, and those permissions are then removed. Or, an ephemeral account, or token, is created just for that one-time event with just the right set of permissions; after the session, the account is then removed again (this mechanism is common for AWS access).

Each step down this path takes your organization closer to 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 ineffective exercises, and some vendors differentiate their products by providing users with tools to more easily find unusual activity in logs and recordings.

Don't limit your visibility to what is provided in the PAM tool, security infrastructure which is devoted to logging, monitoring and analytics must be a part of this effort. Mature SIEM tools will give you visibility for privilege access use. While several 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 like identity governance and administration (IGA), orchestration, and workflow platforms. Your goal will be to move beyond the legacy functions of PAM, password vaulting, session recording, etc., into the next-generation functions of no standing privileged access, and little to no human interaction for support of privileged task execution.

Considerations for PAM tool selection:

- *Best practices:*
  - Expect to support multiple approaches to PAM methodologies and technologies in your environment. For example, organizations may find that many legacy applications and systems only

support password vaulting approaches, while more modern applications, as well as IaaS, PaaS and SaaS platforms, offer opportunities to apply JIT access, and provide the added flexibility of API interaction.

- *Innovation:*
    - Target vendors that are working to innovate PAM approaches, providing competent core PAM capabilities today, while working toward new capabilities needed in the future. Examples of innovation in PAM markets include:
    - Discovery, provisioning and workflow integrations with other enterprise systems like CMDBs, ITSM, IGA, and SIEM.
    - Expanding 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.
    - Leveraging strategies like privileged task automation, JIT access, and no standing (i.e., long-term) privileged access.
    - Some PAM vendors are providing web-based mechanisms for remote access, offering an innovative approach for giving business partners and support teams access to systems without leveraging VPN or other remote access technologies.
    - Migrating manual execution of privileged tasks into automated execution of privileged tasks.
    - Leveraging advanced identity corroboration techniques like mobile push, public key tokens and other methods, like biometrics.
- *Reliability and availability:*
    - As you expand your PAM capability to all privileged access in your enterprise, reliability and uptime of your systems will now depend on availability of PAM access. Key considerations you should discuss with PAM vendors include redundancy, high availability, time to recovery and a “break the glass” capability, which gives you emergency access to your privileged accounts and passwords when the PAM system is unavailable.
- *Authentication:*
    - Since PAM access provides access to your most critical assets and data, single-factor authentication is no longer appropriate for accessing PAM credentials, MFA must be required for PAM access. Organizations looking for a PAM tool must ensure that the tool they select will accommodate an existing, or include a built-in, MFA capability that provides an advanced level of security. See “Market Guide for User Authentication” for additional guidance.
- *Organizational change management:*
    - Organizations should not underestimate the organizational change management impact of a PAM program. Leaders will encounter resistance among user communities, particularly if adopting PAM products, which significantly impact the daily tasks and responsibilities of administrative employees. This impact can be somewhat mitigated with mature organizational management practices like executive sponsorship, clear communication regarding coming changes and training on the new platform before it is rolled out. In addition, user friction can be avoided by adopting technologies that are less impactful for administrators (for example, allowing them to leverage tools that they are familiar with and that allow them to be most productive). In addition, PAM products that leverage automation and scripting to execute privileged tasks, rather than granting full operating system or application access, will also help minimize disruption for users by reducing the amount of tasks for which they are responsible.
- *Program maturity:*
    - Remember that success in a PAM program is dependent on program maturity. This is one crucial piece of advice that should not be ignored. Gartner finds that many organizations stop at a point where only minimal functionality is deployed and never go beyond that point —

thus leading to a large residual risk surface not being properly addressed. While some vendors ship easy-to-install and easy-to-use tools, PAM will always get complicated as soon as you move beyond the most common features (vaulting for human users). Service account management is, by nature, a complex topic and requires special skills and deep knowledge of the product. Security and risk management leaders must be realistic about the skill sets in their organization and, as appropriate, plan to leverage professional services from the vendor or its partner system integrators that can take their PAM program beyond the simplest steps.

Market Overview

Market Size and Drivers

The PAM market exceeded $1.1 billion in 2017, representing growth of 16.9% over 2016. The market is expected to continue to grow at a rapid pace, with a CAGR of almost 19% for the period of 2016 to 2022 (see “Forecast: Information Security, Worldwide, 2016-2022, 2Q18 Update”).

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.

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

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
- 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 bulk of consolidation activity can be traced to a relative handful of companies. In a series of transactions, beginning in February 2018 with the acquisition of Lieberman Software, Bomgar initiated an aggressive expansion of its product portfolio. Lieberman Software had long competed in the PAM market with solutions primarily focused on Windows-based systems. Shortly afterward, in April 2018, Bomgar itself was acquired by Francisco Partners from Thoma Bravo, both private equity firms. In July, Bomgar announced it was acquiring Avecto, a U.K.-based PAM vendor focused on PEDM solutions. That announcement was followed in September with the revelation that Bomgar would acquire BeyondTrust, and take on the (better known) name of the acquired company.

This flurry of acquisitions has created a vendor rivaling longtime leader CyberArk in overall size, with a well-known brand, but possessed of an overlapping and potentially problematic portfolio of products. As of the publication of this Magic Quadrant, the precise roadmap for this combined portfolio is unclear. Clients — prospective and current — are advised to exercise caution in purchases, follow roadmap announcements carefully, and evaluate planned portfolio, service and support changes in the context of their unique requirements.

Four other acquisitions are noteworthy:

- Broadcom, known mostly as a semiconductor device provider, completed the acquisition of CA Technologies in an $18.9 billion transaction on 5 November 2018. At the time of publication of this Magic Quadrant, the transaction is not expected to directly impact CA's PAM offering. However, some level of disruption of sales, service and support — not uncommon in any acquisition — may result.
- In January 2018, Balabit, a European-based PAM vendor, was acquired by One Identity, which had previously integrated Balabit technology in its offerings via an OEM relationship. Balabit's products have been incorporated into One Identity's PAM portfolio to bolster its privileged user and password advanced analytics capabilities. Terms were not disclosed.
- CyberArk acquired Vaultive in March 2018, and is incorporating that company's technology to expand capabilities for controlling privileged access to SaaS, IaaS and PaaS systems.
- In July 2018, private equity firm Thoma Bravo revealed that it had made a majority investment in Centrify, acquiring control of the firm. That was followed by an additional investment in the company via a secondary market offering in August. Terms or amounts for the transactions were not revealed, although the investments followed a previous seven venture rounds totaling $94 million invested in the firm. In October, it was announced that Centrify would spin out its IDaaS capabilities into a separate company, Idaptive. The original Centrify will remain as a stand-alone company, focusing specifically on PAM solutions. This change, in addition to the structural and product changes, included changes in senior management. As is the case with any significant change or restructuring, some staff were lost and customers should anticipate some disruption as the transaction is consummated.

In May 2018, Thycotic announced that it had entered into an OEM relationship with IBM Security. IBM Security's existing PAM solutions will be withdrawn from the market, in favor of a new product based on Thycotic technology. To date, Thycotic has focused most of its attention on the North American market, garnering additional sales through indirect channels, mostly in Europe. The relationship with IBM Security, at least indirectly, significantly expands Thycotic's reach in the worldwide marketplace, with distribution and support channels that rival other PAM vendors, most notably CA Technologies and CyberArk.

Geographic and Vertical Trends

Across the world, North America and Europe remain the primary markets for PAM products. However, other regions — particularly the Middle East, the broader Asia/Pacific region and, to a lesser extent, Latin America — continue to exhibit increased interest and sales. Vendors have continued to split into two groups. Large, enterprise vendors — such a CA Technologies, CyberArk, Micro Focus, and, somewhat aspirationally at the moment, BeyondTrust 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 Middle East and Asia/Pacific region, senhaseguara in Latin America, and Osirium, WALLIX and One Identity (which also has a substantial presence in North America) 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 government and, increasingly, healthcare — 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 vertical solution, with increasing demand from communications, media and services; manufacturing and natural resources; utilities; and technology firms. And while PAM has long been a focus of larger enterprises, increased demand among midsize enterprises, and even some small businesses, has emerged.

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.

Source: Gartner Research Note G00356017, Felix Gaehtgens, Abhyuday Data, Dale Gardner, Michael Kelley, Justin Taylor, 3 December 2018

Return to Home (index.html)

(http://www.gartner.com)

PAM Solutions Center is published by Beyondtrust. Editorial content supplied by Beyondtrust is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2018 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of Beyondtrust's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" (/technology/about/ombudsman/omb_guide2.jsp), on its website.

About Gartner (/technology/about.jsp) | Careers (/technology/careers/) | Newsroom (/it/products/newsroom/) | Policies (/technology/about/policies/guidelines_ov.jsp) | Site Index (/technology/site-index.jsp) | IT Glossary (/technology/it-glossary) | Contact Gartner (/technology/contact/contact_gartner.jsp)