Critical Capabilities for Privileged Access Management

Published 25 July 2022 - ID G00756215 - 33 min read

By Analyst(s): James Hoover, Michael Kelley, Felix Gaehtgens, Abhyuday Data

Initiatives: Identity and Access Management and Fraud Detection

Exploitation of privileged accounts is a prime vector for breaches. Cyberinsurance companies are demanding the use of PAM tools. Effective PAM is more important than ever. Security and risk management leaders can use this research to compare the effectiveness of PAM tools.

This Critical Capabilities is related to other research:

Magic Quadrant for Privileged Access Management

View All Magic Quadrants and Critical Capabilities

Overview

Key Findings

- As last year, many vendors are offering SaaS-delivered privileged access management (PAM), with some moving toward a model that emphasizes their cloud offerings over software-delivered PAM.
- Several vendors are beginning to position themselves as providers of converged identity platforms, but the effectiveness of this approach is generally contingent on embracing a single-provider approach.
- Interest in secrets management has continued to grow as more vendors add this functionality to their PAM products, albeit with varying degrees of success.
- Cloud infrastructure entitlement management (CIEM) remains a growth area, with almost half the vendors surveyed offering at least some notable capabilities in this area.

Recommendations

Security and risk management (SRM) leaders responsible for identity and access management (IAM) should:

- Create or expand the control plane for privileged access by implementing, and extending the use of, appropriate PAM tools.
- Reduce PAM risk by prioritizing and expanding just in time (JIT) PAM approaches to pursue zero standing privileges (ZSP) as a goal.
- Investigate the potential for accelerated access to new features, simplified cost structure and more dynamic scalability by evaluating SaaS-delivered PAM services, especially given their maturity.
- Expand the scope and benefit of PAM programs by making full use of the features of PAM tools, especially secrets management features for DevOps use cases, and CIEM for infrastructure as a service (IaaS) visibility and remediation.

Strategic Planning Assumption

By the year 2025, 75% of cyberinsurance providers will mandate the use of just-in-time privileged access management principles.

What You Need to Know

PAM remains a top 10 security control, and recent highly visible cybersecurity incidents have demonstrated that the impact of breaches is felt not just online but also in the physical world. Regulatory frameworks and cyberinsurance providers are increasingly demanding implementation of PAM tools as a condition of compliance or coverage. Consequently, we are seeing increased adoption of PAM tools by organizations of all sizes, from global enterprises to small and midsize enterprises.

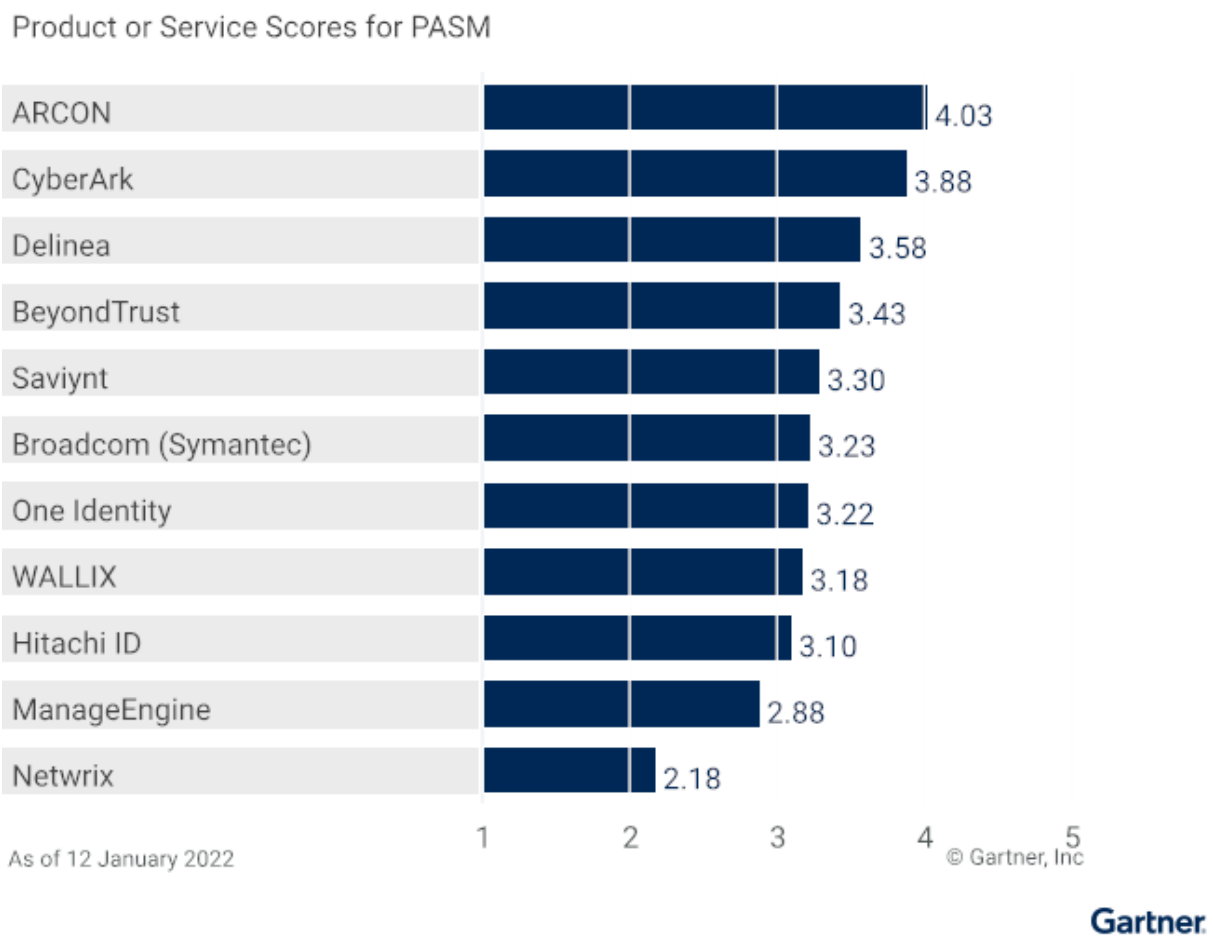
Although most PAM tools are available through software installed on servers, many PAM vendors still offer the ability to deploy an appliance or virtual image. The trend toward SaaS-delivered PAM offerings continues to grow, providing SRM leaders in organizations that take a “cloud-first” approach with viable alternatives to more traditional implementation options.

This Critical Capabilities is a companion to Gartner's Magic Quadrant for Privileged Access Management. Whereas the Magic Quadrant focuses on understanding the PAM market and vendors' relative positions therein, this Critical Capabilities concentrates on those vendors' PAM technologies and ability to provide needed functionality. SRM leaders who want a more technical understanding of the vendors evaluated in the Magic Quadrant should review this Critical Capabilities to gather additional technical data that will inform their evaluation process.

Analysis

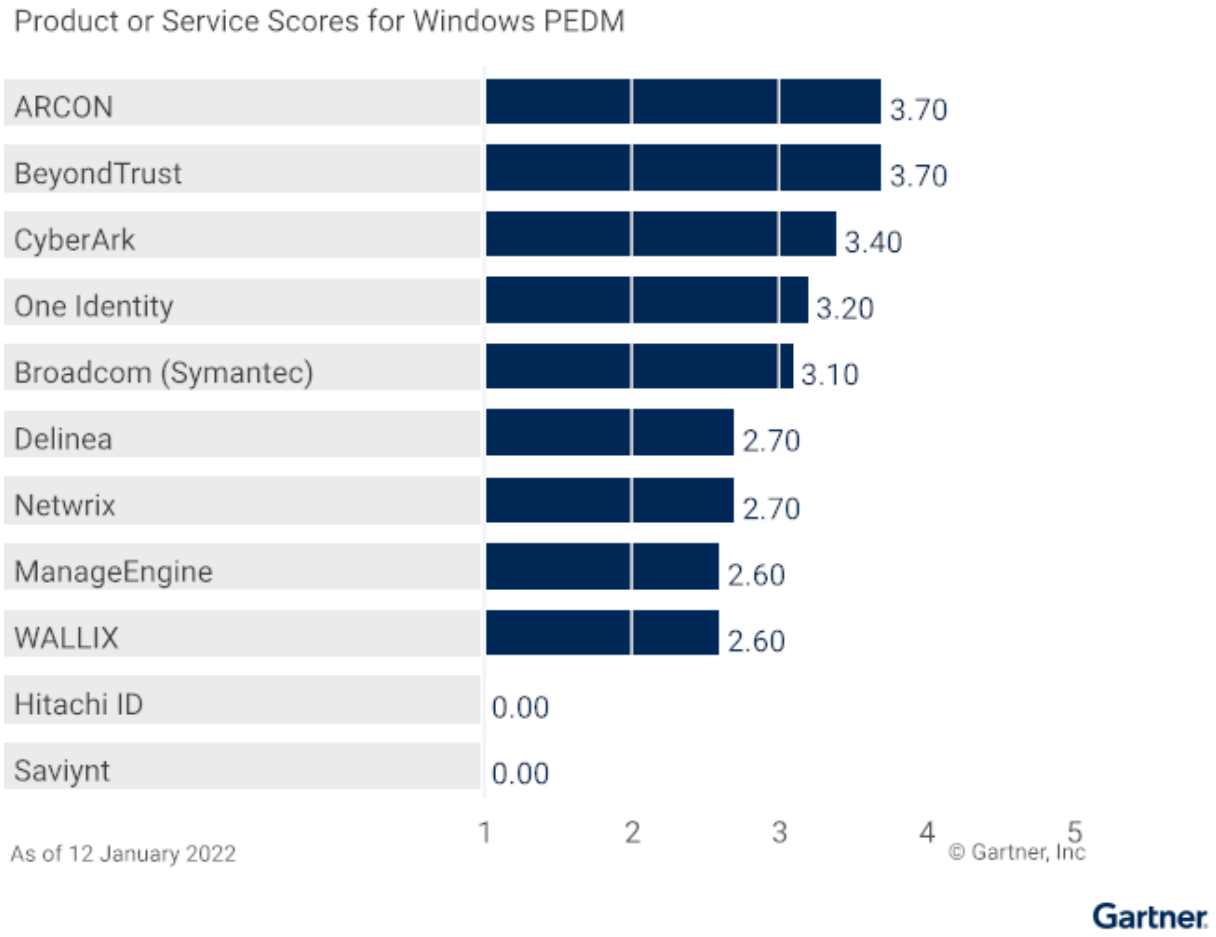
Critical Capabilities Use-Case Graphics

Vendors' Product Scores for PASM Use Case



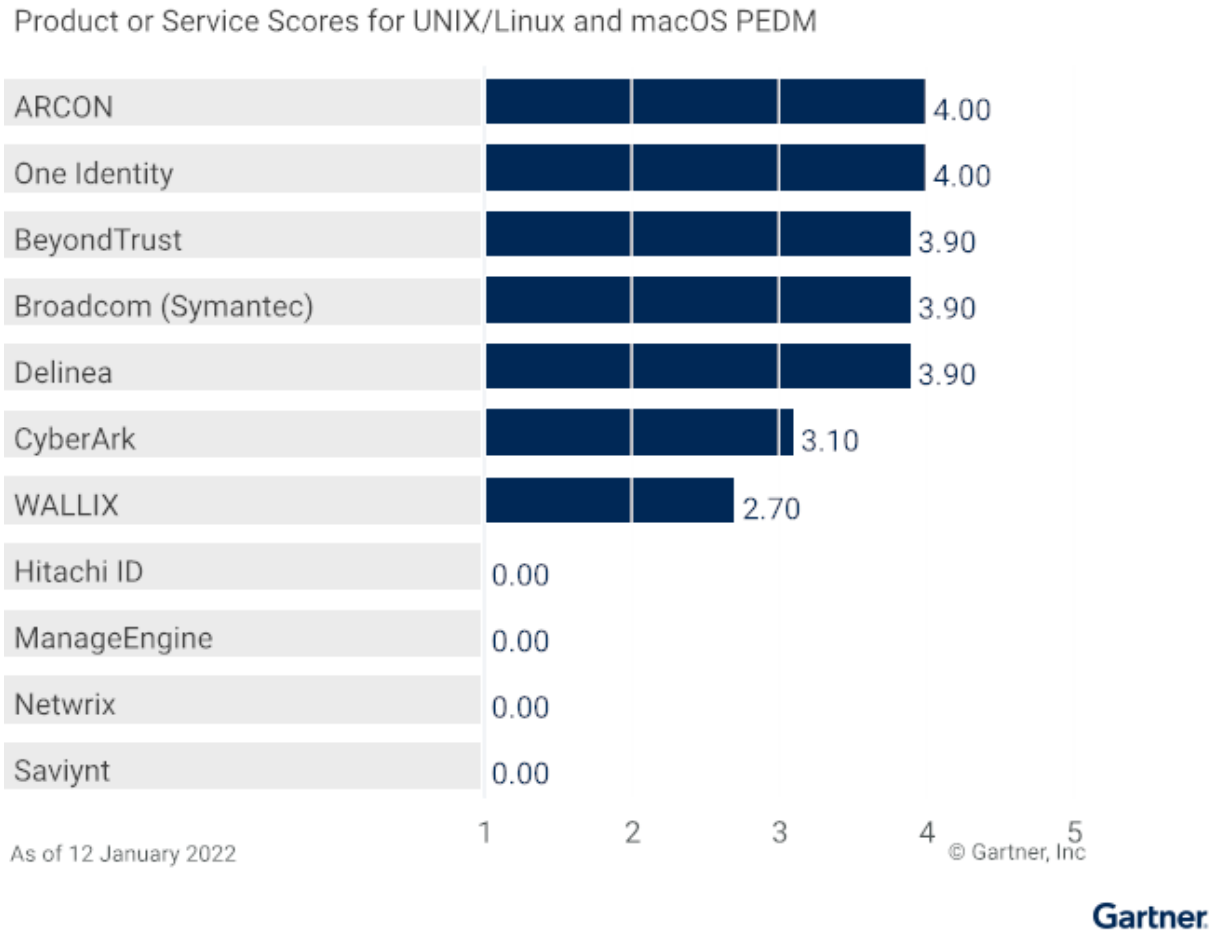
Source: Gartner (July 2022)

Vendors' Product Scores for Windows PEDM Use Case



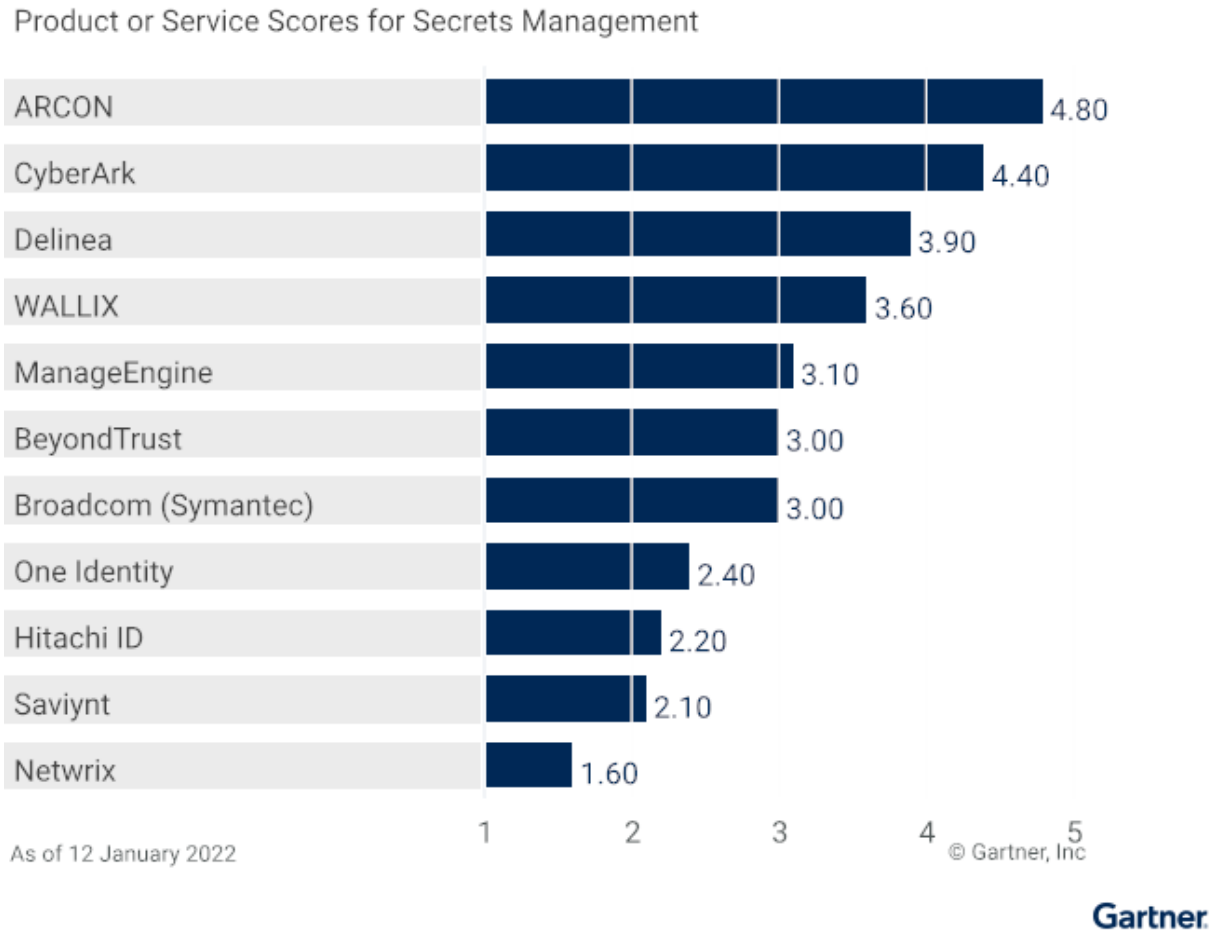
Source: Gartner (July 2022)

Vendors' Product Scores for UNIX/Linux and macOS PEDM Use Case



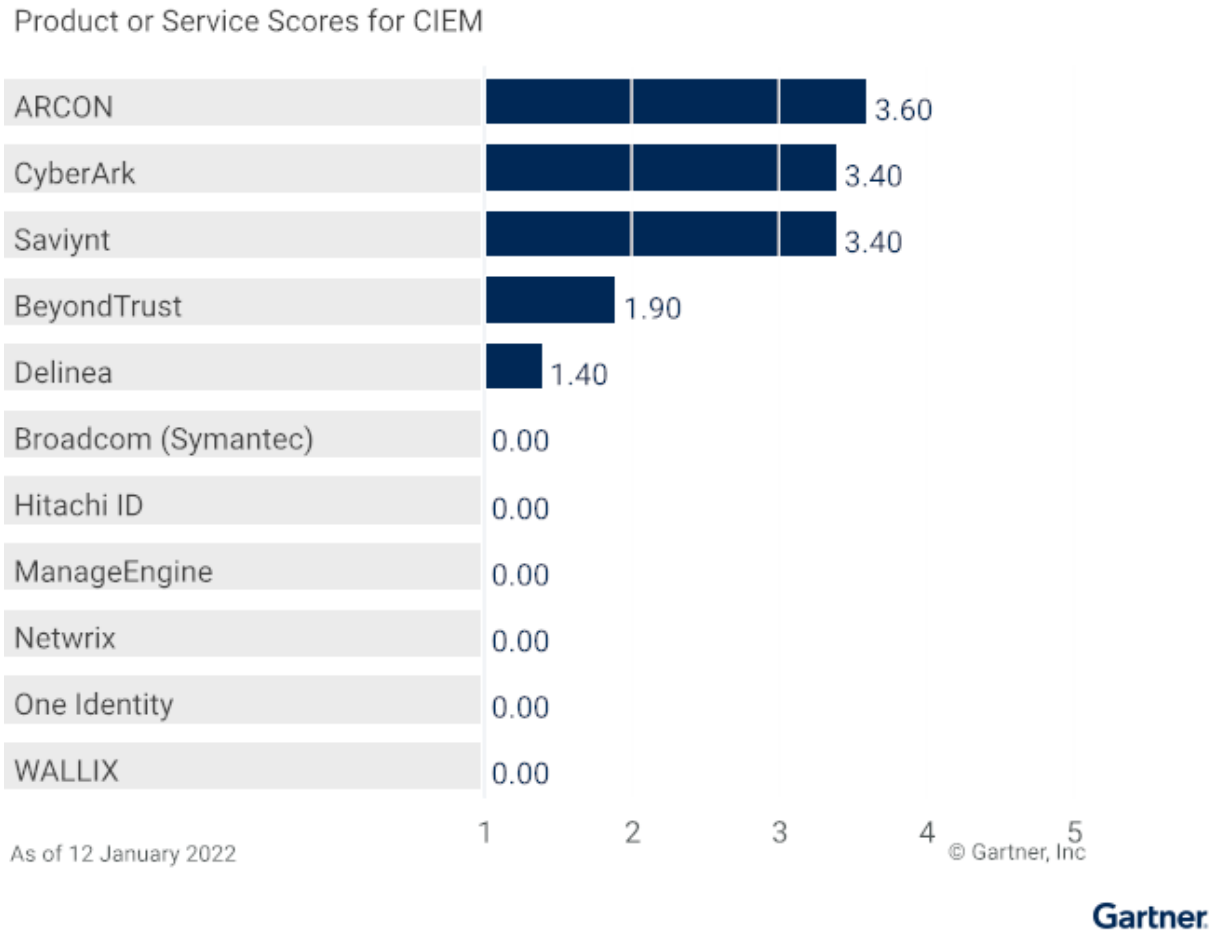
Source: Gartner (July 2022)

Vendors' Product Scores for Secrets Management Use Case



Source: Gartner (July 2022)

Vendors' Product Scores for CIEM Use Case



Source: Gartner (July 2022)

Vendors

ARCON

ARCON scores above average for most of the critical capabilities assessed. Its onboarding, governance and just-in-time (JIT) capabilities are exceptional — they make its solution a strong one for privileged account and session management (PASM). This solution is offered both as software for on-premises deployment and as SaaS.

The primary areas of relative weakness in ARCON's offering are ease of deployment and integration with adjacent systems. Session management is functional, but less flexible than is the case with other vendors, as ARCON either prefers its own client tools or requires a browser plug-in.

Scalability is slightly above average — it requires the use of external load balancers, but there are unique mechanisms for distributing loads across multiple vault processors. ARCON's session gateway/proxy can support up to 5,000 sessions per server. Additionally, ARCON can provide a secure "break glass" approach for disaster recovery (DR) scenarios in which its PAM tool is unavailable.

Although no formal privileged threat analytics function is built into its product, ARCON offers an add-on, Knight Analytics, that can mitigate this shortcoming.

ARCON's privilege elevation and delegation management (PEDM) for UNIX/Linux and macOS is above average, offering centralized sudo management and an ability to extend group policy objects (GPOs) to UNIX/Linux environments (though this is discouraged as ARCON favors its own policy-based controls). Windows PEDM controls are also mature, but are missing comprehensive application control functionality.

ARCON has the strongest CIEM offering assessed. It can integrate with a number of SaaS applications, and with public clouds such as those of Amazon Web Services (AWS), Microsoft (Azure), and Google (Google Cloud Platform) to discover privileged entities for management.

ARCON has the highest rating in this research for secrets management.

BeyondTrust

BeyondTrust's PAM offering is notable for its account discovery, logging and reporting capabilities, and for its analytics, which includes an extensive number of preconfigured templates and dashboards. Privileged governance and administration is above average, but review and certification requires integration with an identity governance and administration (IGA) tool. BeyondTrust's PAM offering is available as software, an appliance or SaaS.

BeyondTrust's Password Safe offering is above average for credential management and has several connectors; there is also a software development kit (SDK) that clients could use to create custom connectors for password rotation. Session management in Password Safe, however, lacks capabilities commonly found in competitors' products, such as browser-based session management and native controls for database and SaaS control panel access. An additional product called Privileged Remote Access (not evaluated in this research) can be used to mitigate these shortcomings, but is priced even higher than Password Safe.

PEDM offerings for UNIX/Linux are strong. They include centralized sudo management and GPO extension and full feature parity for macOS.

Windows PEDM capabilities are robust, but the score for these suffers somewhat from the lack of support for some legacy OS versions and the absence of support for session recording.

BeyondTrust has above-average capabilities for scaling and recoverability. However, ease of deployment and maintenance is below average — despite being an appliance-based model, BeyondTrust's solution has limited prebuilt deployment automation and lacks capabilities for live updating and upgrading. The complexity of deployment might demand a professional services engagement.

Although BeyondTrust offers CIEM, its capabilities in this area lag behind those of other vendors, as it does not offer strong cloud entitlement discovery capabilities. There is only basic visualization, with no support for anomaly detection or JIT approaches for CIEM.

For overall secrets management functionality, BeyondTrust scores lowest of all the vendors that offer a separate product for this. It lags behind in support for machine authentication mechanisms and integration with common DevOps tools.

Broadcom (Symantec)

Broadcom (Symantec) scores highly for ease of deployment. Its solution is highly optimized for performance — a single server can support up to 3,000 concurrent sessions, and scales easily with native load balancing and automatic clustering. Disaster recovery (DR) is highly dependent on this scaling/clustering approach, but there is no formal break-glass procedure for recovery. The PAM solution is delivered as a physical or virtual appliance, but is not offered as SaaS.

Both Windows PEDM and UNIX/Linux PEDM are highly capable. They include file integrity monitoring for Windows, AD bridging and extension of Windows controls for UNIX/Linux, and good template support for elevation policy. Although the vendor does not offer sudo management directly, it does provide sudo enhancements via the sesudo utility.

The PASM offering depends on IGA integration for several key functions, including governance and administration, JIT, logging and reporting, as well as onboarding and discovery. Thus, the vendor has not received any points for scenarios that require the additional IGA product. It also suffers from limited extensibility via prebuilt integrations. For credential management, it does not offer many connectors, but rather requires clients to build their own using an SDK.

Secrets management capabilities are limited by a lack of support for session brokering and prebuilt integrations.

This vendor does not offer native CIEM capabilities, but connections to its IGA suite can be used for some limited cloud governance.

CyberArk

CyberArk is a high-scoring vendor, with above-average capabilities in most areas. In particular, its privileged credential management is highly rated, and has many connectors to different target applications and systems. The logging, auditing and reporting capability is noteworthy for its ability to flag sessions for review, based on risk scoring, which makes the PASM offering very strong. CyberArk's solutions are offered as software or SaaS.

CyberArk suffers in terms of ease of deployment and maintenance. The software version especially may not be suitable for resource-constrained teams. Although it does offer hybrid and cloud deployment models to alleviate some of these issues, those models may not be suitable for all organizations. Account discovery and onboarding offerings are merely average, which exacerbates potential issues with deployment and maintenance.

PEDM capabilities for both Windows and Linux are average. Windows PEDM is missing file integrity monitoring. There is very basic Active Directory (AD) bridging for UNIX/Linux, but no extension of GPO controls to those platforms. The solution can centrally manage sudo policies, but only for Red Hat Enterprise Linux (RHEL).

CyberArk offers strong CIEM capabilities — a reflection of its status as one of the first PAM vendors to provide this functionality.

CyberArk scores highly for secrets management because it offers SDKs in several common programming languages, as well as broad support for integration and authentication mechanisms.

Delinea

Delinea's offering has emerged from a combination of the PAM solutions of Thycotic and Centrify. It has largely been able to combine the strengths of both companies. Its solution offers above-average functionality for all capabilities. For PASM, we evaluated the Secret Server product. For Windows PEDM, we evaluated Delinea Server PAM. For UNIX/Linux PEDM, we evaluated Authentication Service, Server Suite and Cloud Suite. Delinea's solutions are offered as software or SaaS.

Delinea's PAM offering is one of the strongest for account onboarding and discovery, although there is a lack of native support for Azure. The solution scores well for both ease of deployment and scalability, though its deployment model is inconsistent, being on-premises-only, SaaS-only or hybrid, depending on the particular product or add-on. Delinea's PAM solution has extensive preconfigured templates for reports and dashboards.

Delinea's Linux PEDM offering provides a feature-rich AD bridging tool for authentication and extension of a comprehensive set of Windows controls to UNIX/Linux servers, and central management of sudo policies.

Delinea's Windows PEDM offering is average, being held back by limited application control and a lack of file integrity monitoring.

Although Delinea offers CIEM functionality via an account life cycle product, it is fairly basic.

Delinea's secrets management capabilities are above average, offering broad authentication mechanism support and extensive capabilities for connecting with DevOps tools.

Hitachi ID

Hitachi ID offers a PAM solution that we consider above average for scalability and recoverability. Although it requires external load balancing, its clustering and scaling mechanisms utilize container technology. It does not, however, support a break-glass process for recovery.

Capabilities for credential management and onboarding and discovery are above average. The solution supports account discovery for a wide range of IaaS platforms and application servers, and has strong capabilities to onboard discovered accounts automatically. However, it lacks native threat analytics and offers fewer prebuilt integrations than other competitors. Many of the shortcomings of the stand-alone solution can, however, be mitigated by connections to Hitachi ID's IGA solution, which may make it an attractive offering for existing Hitachi ID customers. The solution is offered as both software and SaaS.

Hitachi ID does not offer PEDM for UNIX/Linux or Windows.

HItachi ID does not have an offering for CIEM.

Hitachi ID's offering for secrets management is rudimentary, and focuses on passing credentials to APIs. It may, however, be suitable for customers with simple requirements in this area.

ManageEngine

ManageEngine's PAM360 product offers both PASM and Windows PEDM. It scores highly for deployment and maintenance, and for account onboarding and discovery, making it an attractive offering for those seeking a straightforward and quick time-to-manage PAM solution. It is currently available only as software; there is no SaaS offering.

This vendor's offerings for governance and administration are limited, as they have no native access certification capabilities, nor do they manage the life cycles of privileged accounts. Access and reporting capability is also below average, as many of the offerings for detection and response require integration with non-PAM products.

ManageEngine does not offer UNIX/Linux PEDM, and only limited Windows PEDM. There are very few options for gathering contextual information about a privileged session (such as the network location of a device). Application controls and file integrity monitoring require the purchase of additional products.

Secrets management capabilities are slightly below average, as many common machine authentication methods are not yet supported. The solution cannot perform session brokering for workloads.

ManageEngine does not offer CIEM capabilities.

Netwrix

Netwrix's SbPAM product has average scores or below for all capabilities assessed, because Netwrix requires the purchase of additional tools to fulfill many of them. As a stand-alone solution, it provides few capabilities for discovery and onboarding; simple logging, reporting, analytics and response; and average scalability. There are no break-glass procedures for DR. Overall, it is a below-average PASM solution. Netwrix does not have a SaaS offering. Its product is deployed only as software.

Netwrix does not provide PEDM for UNIX/Linux. Its PEDM offering for Windows does not support session recording or file integrity monitoring, but does have some rudimentary application control functions.

Netwrix does not provide CIEM functionality.

Netwrix's secrets management capabilities are very basic, being limited largely to using custom PowerShell modules to inject credentials into configuration files and API-based integration with third-party secrets vaults.

Many of the limitations of SbPAM as a stand-alone product can be overcome by also using other software offered by Netwrix. This may make it a more attractive offering to existing Netwrix customers.

One Identity

One Identity, which is part of Quest, sells both PASM and PEDM functionality (One Identity Safeguard). One Identity's PASM tools are available as SaaS, or within a software or hardware appliance. PEDM tools (Privilege Manager for Windows, Safeguard for Sudo and Privilege Manager for Unix) are available as software.

One Identity's PASM scores are below average. This is due to weaknesses in terms of scalability arising from requirements for external load balancing between clusters, a lack of DR break-glass capability, a below-average onboarding and discovery capability, and a strong dependency on the purchase of an additional IGA solution for governance and administration capabilities. These weaknesses are somewhat offset by ease of deployment and a moderate number of prebuilt integrations with adjacent systems.

Windows PEDM functionality is strong, but requires the use of additionally licensed products for more granular functions and file integrity monitoring.

UNIX/Linux PEDM is also strong, supporting a comprehensive number of UNIX/Linux and macOS clients, a mature AD bridging tool, and the capability to extend Windows controls to UNIX/Linux platforms.

One Identity does not offer CIEM capabilities, but may be able to extend its IGA product for some governance options.

Secrets management capabilities are below average, due to a heavy dependence on third-party software to provide functionality.

Saviynt

Saviynt is an identity platform vendor with a PAM offering called Cloud Privileged Access Management (CPAM). As a SaaS solution, CPAM rates well for ease of deployment and maintenance, and has good scalability. Saviynt offers extensive integration capabilities within its own environment, but is somewhat limited in its ability to integrate beyond the Saviynt ecosystem. Its PASM solution has minimal capabilities for logging and auditing privileged account activities, though Saviynt's governance and administration and discovery and onboarding functions are some of the highest rated, partly owing to its history as an IGA vendor.

CPAM does not have PEDM functionality, and its logging and reporting capabilities are below average as they do not support added metadata or detection of out-of-band privileged access.

Saviynt scores above average for CIEM as it supports all major cloud service providers, as well as SaaS applications and identity providers.

Secrets management functions are below average, due to a dependency on third-party software.

Many of the limitations of CPAM as a stand-alone solution can be mitigated by also using Saviynt's IGA solution. This may make it a more attractive offering to existing Saviynt customers or those looking for a one-stop identity platform.

WALLIX

WALLIX is a PAM vendor well known for its session management. WALLIX sells PASM (WALLIX Bastion) and PEDM (WALLIX BestSafe) products, both of which can be delivered as software or SaaS.

WALLIX Bastion is notable for its ease of deployment, adjacent-system integration, and above-average JIT offering.

WALLIX has cost-effective PEDM capabilities, but these lack some expected functions. Windows PEDM application control and file integrity monitoring are very basic, though WALLIX does provide ransomware-specific rules to protect against malware propagation. Only Linux is supported for PEDM (there is no support for UNIX or macOS). The Linux offering lacks AD bridging capabilities.

WALLIX has above-average capabilities for secrets management, though it is limited by a lack of support for some common authentication mechanisms.

In general, WALLIX's PASM functionality scores below average. Its session management capability is strong, but its capabilities for governance, account discovery and credential management lack features expected in this market. Many of WALLIX's governance features require third-party IGA or IT service management (ITSM) tools to deliver full functionality.

WALLIX does not offer CIEM-specific capabilities, but it has them on its roadmap.

Context

Every device and virtually every piece of software installed in any environment comes with privileged accounts. These are necessary for everything from initially installing and configuring a resource, to providing services for network users. But the privileges associated with resources, and which are so valuable in managing them, are targets for bad actors. This is because of their elevated access, potential for wider access to additional information and resources, and potential to disrupt a network or business.

A privileged account can be loosely thought of as any account that has more powerful permissions than a regular user account. This includes permissions that allow changes to be made to settings (such as security configurations) and permissions that allow a user to bypass existing security controls (for example, by reading bits directly off a device and thus bypassing logical access controls for structured data). By nature, privileged accounts often have potential to both create and destroy from an IT perspective. They have the greatest potential for operational risk, reputational risk, loss of intellectual property, loss of regulated data or even, in the case of cyber-physical incidents, catastrophic loss (including of health and lives). Because the risk associated with these accounts is so high, Gartner has identified PAM as a top 10 security control.

PAM tools and PAM practices are designed to help mitigate poor practices when it comes to the principle of “least privilege.” Gartner strongly recommends that personal privileged accounts be eliminated or at least dramatically reduced, in favor of granular controls focused on specific segments of infrastructure.

The principle of least privilege should guide the vision of every PAM practice, and multiple strategies for PAM, JIT and ZSP should play a key role. The risk of privileged accounts, stemming from the permissions they carry, can be mitigated by taking a JIT approach. JIT means that privileges are available only when they are required to fulfill legitimate operational needs and at the appropriate level. The purest form of JIT is ZSP, which means that no standing privileges exist and all administrative access is defined and allocated on a JIT basis. In addition, any type of administrative access that cannot be delivered through a JIT model (such as root or local administrative access) is managed by a PAM tool to ensure the principle of least privilege is applied across all administrative access.

Before purchasing a PAM tool, review the “four pillars” of PAM:

1. **Track and secure** to discover all PAM use cases used by both humans and software.

2. **Govern and control** to examine the PAM access happening in your environment right now through the lens of the principle of least privilege (only the right user getting the right access to the right resource for the right reason at the right time).

3. **Record and audit** to give you the visibility required for privileged access.

4. **Operationalize** to couple the PAM tool with other tools, such as those used for change control and ITSM, to gain additional value, such as JIT access.

This will help you understand your PAM risk and define your requirements.

Once this review is complete, it is time to choose a PAM tool. Use this Critical Capabilities document to relate the functionality of available PAM tools to your requirements. Also consult Buyer's Guide for Privileged Access Management, which provides a simple five-step approach to buying the right PAM tool.

Finally, start moving the PAM use cases in your environment to a JIT/ZSP approach, which reduces the risk associated with the existence of privileged accounts. Reduce Risk Through a Just-in-Time Approach to Privileged Access Management will guide you through the process of finding use cases, and give you guidance on how to achieve JIT PAM access.

Product/Service Class Definition

Gartner covers three distinct tool categories that have evolved as the predominant focus for SRM and other IT leaders considering investment in PAM tools:

- **Privileged account and session management (PASM):** Privileged accounts are protected by vaulting their credentials. Access to those accounts is then brokered for human users, services and applications. Privileged session management (PSM) functions establish sessions with possible credential injection and full session recording. Passwords and other credentials for privileged accounts are actively managed by, for example, being changed at definable intervals or upon the occurrence of specific events. PASM solutions can also manage (rotate) credentials for service accounts.
- **Privilege elevation and delegation management (PEDM):** Specific privileges are granted on the managed system by host-based agents to logged-in users. PEDM tools provide host-based command control (filtering) and privilege elevation for servers, the latter by allowing particular commands to be run with a higher level of privilege. PEDM tools must execute on the actual operating system (kernel or process level). For UNIX/Linux PEDM tools, directory bridging functionality is often included to enable users to log into UNIX/Linux systems with their Active Directory (AD) credentials. *Command control through session monitoring — command filtering on Secure Shell (SSH) sessions, for example — is explicitly excluded from this definition, because the point of control is less reliable.*

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

Critical Capabilities Definition

Privileged Access Governance

This capability provides features and functions to manage privilege assignment, manage the identity life cycle for privileged accounts, review and certify privileged access, and ensure segregation of duties.

Some vendors provide the ability to manage the full life cycle of privileged accounts.

Account Discovery and Onboarding

This capability provides features that discover, identify and onboard privileged accounts, including the ability to support periodic, ad hoc or continuous discovery scans. Included is the ability to automatically discover target services and systems for further discovery of privileged accounts.

Privileged Credential Management

This capability provides core features and functions that manage and protect system- and enterprise-defined privileged account credentials or secrets (including SSH keys). It includes generation, vaulting, rotation and retrieval for interactive access to these credentials by humans or machines.

Included is the rotation of service and software accounts (that is, embedded accounts) on target systems.

These functions require the ability to access the PAM tool through a web console or API, at minimum.

Privileged Session Management

This capability provides session establishment, management, recording and playback, real-time monitoring, protocol-based command filtering, and session separation for privileged access sessions.

Included are functions to manage an interactive session with the PAM tool, from check-out of a credential to check-in of that credential, although in normal cases the credential is not disclosed to the user.

This capability may also involve restrictions (allow/deny) of certain types of commands and functions while logged into the target system.

Secrets Management

This capability enables management of access to credentials (such as passwords, OAuth tokens and SSH keys) for nonhuman use cases, such as machines, applications, services, scripts, processes and DevOps pipelines.

It includes the ability to generate, vault, rotate and provide a credential to nonhuman entities (for example, via an API). It also includes the ability to broker trust between different nonhuman entities for the purpose of exchanging secrets, and to manage authorizations and related functions.

Additionally, it includes the optional ability to establish trust with a nonhuman entity without requiring a credential by using other mechanisms of recognition (including zero-factor authentication). IaaS/PaaS identities can also be used to establish trust with the vault. In combination, these functions support secrets management for dynamic environments and support robotic process automation platforms.

Logging and Reporting

This capability provides the ability to record all single events, including changes and operations, as part of a PAM operation. A single event is based on user, time, date and location, and is processed with other events via correlation in a logical order.

This capability is valuable for determining and monitoring the root causes of risk events and for identifying unauthorized access. It also provides the features required for auditing and reporting of the events database, including prebuilt reports and support for ad hoc reports. Events data must also include information from privileged sessions.

Additionally, this capability provides analytics (which can include machine learning) for privileged account activities to detect and flag anomalies, including baselining, risk scoring and alerting. The objective is to better identify lagging and leading indicators that identify privileged access anomalies with a view to triggering automated countermeasures in response to alerts.

PEDM — UNIX/Linux

This capability covers agent-based privilege elevation and delegation for UNIX/Linux servers and for macOS. Functionalities include the ability to elevate the access of a logged-in user to permit authorized commands or applications to run under elevated privileges.

This capability can also provide Active Directory (AD) bridging, which applies AD controls to Linux/UNIX systems, including the ability to authenticate to these systems with AD credentials, and pass through GPO policies. This also covers file integrity monitoring and sudo controls.

PEDM — Windows

This capability covers agent-based privilege elevation and delegation for Windows systems. Functionality includes the ability to elevate the access of a logged-in user to permit authorized commands or applications to run under elevated privileges.

This capability provides the ability to control privileges for applications and subprocesses for applications on the server, including the ability to allow, deny and isolate applications. It also provides file integrity monitoring.

Automation and Adjacent Integration

This capability provides functions and features that automate multistep, repetitive tasks related to privileged operations that are orchestrated and/or executed over a range of systems. It also uses extensible libraries of preconfigured privileged operations for common IT systems and devices.

This capability can orchestrate back and forth between different activities and ask for more information as needed, while providing guardrails by checking inputs against policies and settings.

This capability requires the ability to provide functions and features to integrate and interact with adjacent security and service management systems. These systems include identity governance and administration (IGA), standards-based single sign-on (SAML, OAuth, OIDC), multifactor authentication (MFA), enterprise directories, flexible connector and integration frameworks, APIs, hardware security modules (HSMs), IT service management (ITSM) systems, security information and event management (SIEM) systems, and vulnerability management systems.

Ease of Deployment and Maintenance

This capability provides functions and features that simplify the deployment and ongoing maintenance of the PAM solution, including automation capabilities, upgrade processes, and requirements for outside assistance during the life cycle of the solution.

This capability generally focuses on the features of a vendor's software-delivered tools.

Many vendors have introduced SaaS-delivered PAM services as well, which provide many of the benefits native to a SaaS-delivered service, including simplified deployment and maintenance processes.

Performance and Availability

This capability provides functions and features that improve system performance under load, increase system availability, and enable the solution to scale effectively to meet demand.

Just-in-Time PAM Methods

This capability provides on-demand privileged access without the requirement for shared accounts that carry standing privileges. Typically, this involves nonprivileged accounts being granted appropriate privileges on a time-bound basis.

Common methods for achieving this include the use of PEDM approaches, temporary and on-demand group membership, and ephemeral accounts or security tokens. This capability focuses on compliance with the principle of least privilege and, subsequently, achievement of ZSP for PAM access.

Basic JIT use cases include dynamically adding and removing users from AD groups, agent-based privilege elevation, and dynamic provisioning of limited access to privileged accounts.

Advanced JIT/ZSP use cases include on-demand creation and deletion, use of ephemeral tokens, and ephemeral access to SaaS control panels.

CIEM

This capability provides management of cloud entitlements for cloud infrastructure via administration time controls for the governance of entitlements in hybrid and multicloud IaaS.

This capability typically uses analytics, machine learning and other methods to detect anomalies in account entitlements, such as accumulation of privileges and dormant and unnecessary entitlements. CIEM ideally provides remediation and enforcement of least-privilege approaches in cloud infrastructures.

Use Cases

PASM

This use case reflects core PAM functionality, account vaulting, check-out/check-in, session recording, privilege task automation, credential rotation and JIT PAM approaches.

Windows PEDM

This use case reflects PEDM functionality, agent-based privilege elevation and delegation for Microsoft Windows.

Vendors were scored on functionalities such as privilege elevation, application controls, allow/deny/isolate and sandboxing.

UNIX/Linux and macOS PEDM

This use case reflects PEDM functionality, agent-based privilege elevation and delegation for UNIX/Linux and macOS.

Vendors were scored on functionalities such as privilege elevation, AD bridging, application controls, allow/deny/isolate and sandboxing.

Secrets Management

This is a specialized use case for privileged access. It reflects the need to programmatically manage, store, and retrieve credentials and secrets for software and machines.

Secrets management scenarios are typically dynamic — as, for example, with brokerage of trust between individual applications, services or devices, containers and DevOps pipelines.

CIEM

This use case reflects the growing market for management of cloud entitlements for cloud infrastructure using PAM tools.

Vendors were scored on their functionality for managing cloud access risks via administration time controls for the governance of entitlements in hybrid and multicloud IaaS.

Vendors Added and Dropped

Added

- Delinea (a merger of Thycotic and Centrify, both of which were participants in last year's Critical Capabilities)
- Hitachi ID
- ManageEngine
- Netwrix
- Saviynt

Dropped

- Krontech was dropped after not meeting the inclusion criteria for $15 million in annual revenue
- senhasegura was dropped after not meeting the inclusion criteria for $15 million in annual revenue

Inclusion Criteria

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

- **Mandatory:** Privileged account and session management (PASM), core PAM functionality, account vaulting, check-out/check-in, session recording, privilege task automation, credential rotations, deployment and scalability, logging and reporting, and JIT PAM approaches. Vendors that do not provide these functions will not be included in the Critical Capabilities for Privileged Access Management.
- **Optional:** A vendor may also offer secrets management, cloud infrastructure entitlement management (CIEM), and privilege elevation and delegation management (PEDM) by host-based agents for UNIX/Linux, macOS or Windows operating systems.

The vendor's solution must meet the following **minimum capabilities** as of 21 February 2022:

- A secured, hardened and highly available vault for storing credentials and secrets.
- Tools to discover, map and report privileged accounts on multiple systems, applications and devices.
- Tools to automatically randomize, rotate and manage credentials for system, administrative, service, database, device and application accounts.
- Tools to manage the end-to-end process of requesting access through user interfaces by privileged users with approval workflows.
- User interfaces to check out privileged credentials.
- Tools to allow a privileged session to be automatically established using protocols such as SSH, RDP or HTTPS without revealing credentials to the user.
- Features must exist to fully record and review sessions, as well as manage live sessions by allowing them to be accompanied or terminated.
- Tools that broker credentials to software, thereby allowing the elimination of clear-text credentials in configuration files or scripts.
- Support for role-based administration, including centralized policy management for controlling access to credentials and privileged actions.
- Analytics and reporting of privileged accounts and their use (for example, discovering unauthorized use of privileged credentials or reporting on unusual activities).

- Underlying architecture for the above, including connector architecture.
- Products must be marketed, sold and deployed for use with customer production environments for purposes consistent with objectives of PAM.
- All tools and features must be fully documented, including the documentation of the configuration (if applicable), as well as the use of the feature. Features that are not documented, or that are merely listed, or referenced in passing but not documented, cannot be considered.

To further qualify for inclusion in the 2021 Critical Capabilities for Privileged Access Management, the respective vendors must meet the following criteria:

- **Revenue:**
  - Have booked a total revenue of at least $15 million for PAM products and subscriptions (inclusive of maintenance revenue, but excluding professional services revenue) for any period of 12 consecutive months (fiscal year) between 1 March 2020 and 31 December 2021, or
  - Have 500 distinct paying customers using its PAM tools
- **Geography:** Vendors must compete in at least two of the five major regional markets (North America; Latin America [including Mexico]; Europe, the Middle East and Africa; Asia/Pacific, including ANZ). This condition would be met if a vendor has no more than 90% of its client base in one particular region.
- **Intellectual property:** Sell and support its own PAM product or service developed in-house, rather than offer as a reseller or third-party provider.
- **Verticals:** Have sold PAM products or services to customers in different verticals or industries.
- **Positioning:** Market products for use consistent with PAM.

With respect to the previous year's Critical Capabilities, the minimum revenue and customer counts for inclusion were increased in line with market forecasts.

Table 1: Weighting for Critical Capabilities in Use Cases

(Enlarged table in Appendix)

Critical Capabilities	PASM	Windows PEDM	UNIX/Linux and macOS PEDM	Secrets Management	CIEM
Privileged Access Governance	8%	0%	0%	0%	0%
Account Discovery and Onboarding	14%	0%	0%	0%	0%
Privileged Credential Management	14%	0%	0%	0%	0%
Privileged Session Management	15%	0%	0%	0%	0%
Secrets Management	0%	0%	0%	100%	0%
Logging and Reporting	8%	0%	0%	0%	0%
PEDM — UNIX/Linux	0%	0%	100%	0%	0%
PEDM — Windows	0%	100%	0%	0%	0%
Automation and Adjacent Integration	10%	0%	0%	0%	0%
Ease of Deployment and Maintenance	11%	0%	0%	0%	0%
Performance and Availability	8%	0%	0%	0%	0%
Just-in-Time PAM Methods	12%	0%	0%	0%	0%
CIEM	0%	0%	0%	0%	100%
As of 12 January 2022					

Source: Gartner (July 2022)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Each of the products/services that meet our inclusion criteria has been evaluated on the critical capabilities on a scale from 1.0 to 5.0.

Critical Capabilities Rating

Table 2: Product/Service Rating on Critical Capabilities

(Enlarged table in Appendix)

Critical Capabilities	ARCON	BeyondTrust	Broadcom (Symantec)	CyberArk	Delinea	Hitachi ID	ManageEngine	Netwrix	One Identity	Saviynt	WALLIX
Privileged Access Governance	4.5	3.7	3.1	4.3	3.6	2.1	2.5	3.6	2.0	4.7	1.4
Account Discovery and Onboarding	4.5	3.5	3.3	3.8	4.2	3.9	4.1	0.0	3.3	4.3	2.3
Privileged Credential Management	4.1	4.0	2.8	4.8	3.1	3.8	2.5	1.4	3.3	1.8	2.3
Privileged Session Management	4.1	2.4	3.4	3.5	2.8	2.5	2.4	2.3	4.0	2.3	4.3
Secrets Management	4.8	3.0	3.0	4.4	3.9	2.2	3.1	1.6	2.4	2.1	3.6
Logging and Reporting	3.6	4.1	3.0	4.0	3.8	2.6	2.6	2.2	3.4	2.9	3.2
PEDM — UNIX/Linux	4.0	3.9	3.9	3.1	3.9	0.0	0.0	0.0	4.0	0.0	2.7
PEDM — Windows	3.7	3.7	3.1	3.4	2.7	0.0	2.6	2.7	3.2	0.0	2.6
Automation and Adjacent Integration	3.8	3.7	3.9	4.6	3.8	3.4	3.6	3.0	4.0	3.4	4.5
Ease of Deployment and Maintenance	3.3	3.0	3.6	2.8	3.4	3.3	3.6	3.1	3.3	4.2	3.6
Performance and Availability	3.3	3.6	3.6	3.6	3.5	3.6	1.7	2.8	3.0	3.5	3.2
Just-in-Time PAM Methods	4.6	3.4	2.5	3.6	4.3	2.3	2.5	2.6	2.2	3.4	3.5
CIEM	3.6	1.9	0.0	3.4	1.4	0.0	0.0	0.0	0.0	3.4	0.0

As of 12 January 2022

Source: Gartner (July 2022)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

(Enlarged table in Appendix)

Use Cases	ARCON	BeyondTrust	Broadcom (Symantec)	CyberArk	Delinea	Hitachi ID	ManageEngine	Netwrix	One Identity	Saviynt	WALLIX
PASM	4.03	3.43	3.23	3.88	3.58	3.10	2.88	2.18	3.22	3.30	3.18
Windows PEDM	3.70	3.70	3.10	3.40	2.70	0.00	2.60	2.70	3.20	0.00	2.60
UNIX/Linux and macOS PEDM	4.00	3.90	3.90	3.10	3.90	0.00	0.00	0.00	4.00	0.00	2.70
Secrets Management	4.80	3.00	3.00	4.40	3.90	2.20	3.10	1.60	2.40	2.10	3.60
CIEM	3.60	1.90	0.00	3.40	1.40	0.00	0.00	0.00	0.00	3.40	0.00
As of 12 January 2022											

Source: Gartner (July 2022)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

Document Revision History

Critical Capabilities for Privileged Access Management - 16 July 2021

Critical Capabilities for Privileged Access Management - 4 August 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

How Products and Services Are Evaluated in Gartner Critical Capabilities

IAM Leaders' Guide to Privileged Access Management

Magic Quadrant for Privileged Access Management

Buyers' Guide for Privileged Access Management

Best Practices for Privileged Access Management Through the Four Pillars of PAM

Securing Remote Privileged Access Through PAM

Reduce Risk Through a Just-in-Time Approach to Privileged Access Management

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	*PASM*	*Windows PEDM*	*UNIX/Linux and macOS PEDM*	*Secrets Management*	*CIEM*
Privileged Access Governance	8%	0%	0%	0%	0%
Account Discovery and Onboarding	14%	0%	0%	0%	0%
Privileged Credential Management	14%	0%	0%	0%	0%
Privileged Session Management	15%	0%	0%	0%	0%
Secrets Management	0%	0%	0%	100%	0%
Logging and Reporting	8%	0%	0%	0%	0%
PEDM — UNIX/Linux	0%	0%	100%	0%	0%
PEDM — Windows	0%	100%	0%	0%	0%
Automation and Adjacent Integration	10%	0%	0%	0%	0%
Ease of Deployment and Maintenance	11%	0%	0%	0%	0%

Critical Capabilities	*PASM*	*Windows PEDM*	*UNIX/Linux and macOS PEDM*	*Secrets Management*	*CIEM*
Performance and Availability	8%	0%	0%	0%	0%
Just-in-Time PAM Methods	12%	0%	0%	0%	0%
CIEM	0%	0%	0%	0%	100%
As of 12 January 2022					

Source: Gartner (July 2022)

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	*ARCON*	*BeyondTrust*	*Broadcom (Symantec)*	*CyberArk*	*Delinea*	*Hitachi ID*	*ManageEngine*	*Netwrix*	*One Identity*	*Saviynt*	*WALLIX*
Privileged Access Governance	4.5	3.7	3.1	4.3	3.6	2.1	2.5	3.6	2.0	4.7	1.4
Account Discovery and Onboarding	4.5	3.5	3.3	3.8	4.2	3.9	4.1	0.0	3.3	4.3	2.3
Privileged Credential Management	4.1	4.0	2.8	4.8	3.1	3.8	2.5	1.4	3.3	1.8	2.3
Privileged Session Management	4.1	2.4	3.4	3.5	2.8	2.5	2.4	2.3	4.0	2.3	4.3
Secrets Management	4.8	3.0	3.0	4.4	3.9	2.2	3.1	1.6	2.4	2.1	3.6

Logging and Reporting	3.6	4.1	3.0	4.0	3.8	2.6	2.6	2.2	3.4	2.9	3.2
PEDM — UNIX/Linux	4.0	3.9	3.9	3.1	3.9	0.0	0.0	0.0	4.0	0.0	2.7
PEDM — Windows	3.7	3.7	3.1	3.4	2.7	0.0	2.6	2.7	3.2	0.0	2.6
Automation and Adjacent Integration	3.8	3.7	3.9	4.6	3.8	3.4	3.6	3.0	4.0	3.4	4.5
Ease of Deployment and Maintenance	3.3	3.0	3.6	2.8	3.4	3.3	3.6	3.1	3.3	4.2	3.6
Performance and Availability	3.3	3.6	3.6	3.6	3.5	3.6	1.7	2.8	3.0	3.5	3.2
Just-in-Time PAM Methods	4.6	3.4	2.5	3.6	4.3	2.3	2.5	2.6	2.2	3.4	3.5
CIEM	3.6	1.9	0.0	3.4	1.4	0.0	0.0	0.0	0.0	3.4	0.0
As of 12 January 2022											

Source: Gartner (July 2022)

Table 3: Product Score in Use Cases

Use Cases	*ARCON*	*BeyondTrust*	*Broadcom (Symantec)*	*CyberArk*	*Delinea*	*Hitachi ID*	*ManageEngine*	*Netwrix*	*One Identity*	*Saviynt*	*WALLIX*
PASM	4.03	3.43	3.23	3.88	3.58	3.10	2.88	2.18	3.22	3.30	3.18
Windows PEDM	3.70	3.70	3.10	3.40	2.70	0.00	2.60	2.70	3.20	0.00	2.60
UNIX/Linux and macOS PEDM	4.00	3.90	3.90	3.10	3.90	0.00	0.00	0.00	4.00	0.00	2.70
Secrets Management	4.80	3.00	3.00	4.40	3.90	2.20	3.10	1.60	2.40	2.10	3.60
CIEM	3.60	1.90	0.00	3.40	1.40	0.00	0.00	0.00	0.00	3.40	0.00
As of 12 January 2022											

Source: Gartner (July 2022)