Buyer's Guide for Privileged Access Management

21 August 2024 - ID G00809858 - 56 min read

By Jonathan Care, Felix Gaehtgens

Unlock more AI value

With unrestricted access to Gartner AI Insights from Gartner.

Explore the AI Plus ›

Learn how Gartner can help you succeed.

Talk to Us

Buying PAM tools without a strategy invites data breaches, ransomware lockouts and compromised systems. Cybersecurity leaders must define their specific requirements, maturity curve, and resource needs prior to selection of PAM vendors.

Insights at a Glance

Privileged access management (PAM) is essential for organizations confronting accelerating cyberattackers, stricter compliance requirements, and rapid digital transformation. The most significant risk is unmanaged privileged accounts and entitlements in attack surfaces of hybrid and cloud environments that are the focus of data quality, compliance gaps, and regulatory penalties. Only a strategic, phased PAM approach delivers lasting protection and incremental agility.

Gartner's five-step framework guides organizations to:

- **Define drivers and objectives** Identify business risks, compliance mandates, and digital transformation goals to shape your PAM vision.
- **Discover and inventory privileged accounts** Identify all privileged identities (human, machine, application, and service) and map them to systems and assets to expose hidden risks and enforce least privilege.
- **Establish a business case and build a roadmap** Align PAM investments with executive support via scoring, session recording, and a time-to-value timeline, and then prioritize with quick wins and long-term phases.
- **Select a tool and vendor** Evaluate and test solutions against your prioritized use cases, ensuring alignment with IT capability, and support for emerging trends such as cloud and machine identities.
- **Negotiate contracts and assess staffing** Leverage your business case and roadmap assurances for ongoing investments, and ensure you have the required skills to keep the program running.

Effective PAM programs are measured by reductions in privileged-account exposure and audit findings, increased automation, and enhanced visibility. Common pitfalls starting with fundamental controls, ignoring non-human accounts, adopting rigid rollout phases, and constructing regular reviews to adapt to evolving threats and technologies.

A well-executed PAM strategy, guided by the Gartner's five steps, delivers measurable security, compliance, and efficiency, empowering your organization to stay ahead of threats and business change.

Impact

When organizations lack a clear strategy for selecting and implementing a PAM solution, fragmentation takes hold. Security teams struggle with overlapping tools, duplicating disconnected tools, leaving critical privileges and credentials unmanaged and vulnerable to attackers.

The absence of strategy boosts IT and security teams into a constant state of reaction. Valuable time is lost training staff on multiple tools and patching system-level incompatibilities that could have been avoided with a unified framework. Routine audits and compliance checks turn into manual, error-prone efforts that drain focus from higher-priority initiatives.

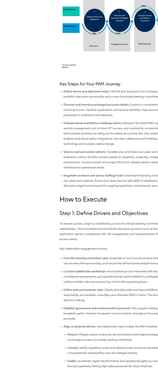
The business impact is significant. Without a coordinated PAM approach, security efforts lag behind emerging threats, and the results include an increased likelihood of breaches due to undetected credential harvesting, lateral movement, and the loss of customer confidence. Every incident becomes a scramble, not a lesson learned response. Ultimately, without a thoughtful PAM strategy, your security posture and time will never building lasting protection defense.

Actions

Simply purchasing a PAM platform does not solve the problem of privileged access. Before evaluating vendors, cybersecurity leaders must first determine how to understand their specific requirements. The five-step process guides cybersecurity leaders from discovering their exact operational requirements to selecting the right PAM tool.

The technology might introduce a five-step process to help you define your vision and requirements and select the appropriate PAM solution for your organization (see Figure 1).

Figure 1: Five Steps to a Strategic PAM Journey



Gartner

Key Steps for Your PAM Journey

- **Define drivers and objectives** Identify security and document your business risks and compliance requirements, and establish executive sponsorship across functional steering committee to drive alignment and support.
- **Discover and inventory privileged accounts (what)** Conduct a comprehensive discovery of all privileged accounts, including human, machine, application, and service identities. This uncovers hidden risks and establishes procedures to understand and govern.
- **Evaluate trends and define a roadmap (when)** Research the latest PAM capabilities such as PEDM, PEDV, MFAs, or passwordless access to identify your IT scenarios, and estimate the cost of ownership. Use your findings to create a phased plan with business priorities by rolling out foundational controls first, then phasing in advanced features such as AI anomaly detection. Set clear milestones and timelines, and ensure your plan can adapt as technology and business needs change.
- **Select and test vendors (which)** Translate your prioritized use cases and requirements into a detailed RFP or evaluation criteria. Shortlist and test vendors in a proof of concept (POC) to validate their capabilities in your environment. Conduct proofs of concept (POCs) to validate vendor claims and ensure the chosen solution fits your technical and operational needs.
- **Negotiate contracts and assess staffing (how)** Understand licensing models and negotiate terms that align with your business case and roadmap. Assess your team's skills and plan for training or hiring to support the new platform. Allocate budget and resources for ongoing operations, maintenance, and continuous improvement.

How to Execute

Step 1: Define Drivers and Objectives

To ensure success, begin by establishing a cross-functional steering committee that actively engages all relevant stakeholders. This could then include executive sponsors from each of the CISO, CIO, or CTO, IT operations, application owners, compliance, HR, risk management, and representatives from any business units with privileged access needs.

Key stakeholder engagement actions:

- Form the steering committee early. Assemble a cross-functional team before project execution to build consensus, ensure accountability, and ensure that all technical perspectives and risks are covered.
- Conduct stakeholder workshops. Host sessions and interviews with key stakeholders to identify business risks, compliance mandates, and digital transformation goals that will shape the PAM process. The collaborative approach surfaces hidden risks and ensures buy-in from all impacted groups.
- Define and communicate roles. Clearly articulate roles and responsibilities for each stakeholder group using a responsible, accountable, consulted, and informed (RACI) matrix. This ensures accountability and streamlines decision making.
- Establish governance and communication protocols. Set a regular meeting cadence and define decision-making and escalation paths. Maintain transparent communications throughout the project to foster trust and address concerns promptly.
- Align on business drivers. Use stakeholder input to align the PAM initiative with business objectives:
  - Prioritize mitigate severe enterprise risk and enhance end-to-end privilege controls to prevent the exploitation of unmanaged accounts by actively auditing credentials.
  - Comply. Satisfy regulatory, audit, and cybersecurity insurance mandates by establishing continuous discovery and comprehensive observability over all privileged activity.
  - Enable. Accelerate digital transformation and operational agility by automating administrative workflows and DevOps pipelines, ensuring it keeps pace powered for other initiatives.

Table 1 illustrates the main objectives for managing privileged access and how they align with business drivers and stakeholder committees.

- Maintain a risk register. As you define drivers and objectives, create a risk register to track key risks and mitigation actions. Update it throughout each phase of your PAM journey, and have the steering committee review it regularly as part of program governance.

Table 1: Objectives for Managing Privileged Access

Objective	Protect	Comply	Enable
Discover where privilege exists (accounts or entitlements)	✓	✓	
Secure and vault privileged accounts	✓	✓	
Remove unnecessary privileges	✓		
Eliminate static or cloaked credentials used by applications	✓		
Implement multifactor authentication for all administrative access	✓		
Gain observability of privileged access		✓	✓
Implement just-in-time and just-enough privilege	✓		✓
Enable automation for DevOps and cloud-use cases	✓		✓

Source: Gartner (August 2024)

Purchasing a PAM product without first defining enterprise requirements and engaging stakeholders guarantees a misaligned investment. By anchoring a potential engagement on the definition of drivers and objectives, you ensure that your PAM strategy is comprehensive, business-aligned, and supported throughout the organization.

Step 2: Discover and Inventory Privileged Accounts

A successful PAM program is built on the foundation of knowledge. It is impossible to secure what you don't know you control. Attackers actively seek out these hidden, orphaned, or excessive privileged accounts and entitle targets for attackers to exploit. Therefore, the first technical step in your PAM journey is a comprehensive discovery initiative. This process identifies and catalogs every privileged account, including human, machine, application, and service identities. By creating a centralized inventory, you can establish a clear baseline for risk assessment, prioritize remediation efforts, and implement the controls that are the cornerstone of your PAM initiative.

To discover and inventory your privileged accounts, execute these steps:

- Establish scope and ownership.
  - Define which systems, environments (on-premises, cloud, hybrid), and account types (human, machine, service, application) are in scope.
  - Assign responsibility for the discovery process to a dedicated team or individual.
- Select discovery methods.
  - If automated discovery tools are available (e.g., features within an existing PAM platform, identity management), recently invest, use them to scan for privileged accounts across your environment.
  - If automated tools are not available, leverage manual and semiautomated methods:
    - Collaborate with system and application owners to identify privileged accounts in their critical systems.
    - Use scripts or built-in OS commands (e.g., Active Directory queries, Linux scripts, cloud IAM roles) to identify accounts with elevated permissions.
    - Review existing documentation, audit logs, and access controls (SOC) to uncover undocumented identities.
- Catalog and document accounts.
  - Record all discovered accounts in a centralized inventory, noting account types, associated systems, business owners, and risk levels.
  - Identify accounts that are active, dormant, orphaned, or have excessive permissions.
- Validate and analyze inventory.
  - Confirm inventory accuracy with system and business owners.
  - Analyze the inventory to understand risk exposure and highlight critical gaps needing remediation or further monitoring.
- Establish an ongoing process.
  - Schedule periodic reviews or scans to keep the inventory current.

Table 2 provides a catalog of privileged account inventory capturing key details.

Table 2: Privileged Account Inventory

Account name	Account type (human, machine, application, service)	Associated system or application	Business owner or technical owner	Privilege level or role	Purpose (why this account exists)	Last used date	Risks

Source: Gartner Analyst Research

A thorough discovery of privileged accounts is essential for exposing the true scope of privileged access risk and establishing a strong business justification for your PAM initiative. The foundational step also provides the clarity needed to design an effective deployment roadmap. Many discovery activities can be accomplished with existing resources or free tools. Learn more about this process in the Gartner Research Privileged Access Maturity Toolkit and Resources or Hype Cycle for Digital Identity, 2024.

Step 3: Evaluate Tends and Define a Roadmap

To ensure a precise vendor fit and future-proof your PAM investment, it is essential to develop a maturity-driven roadmap that not only offers your organization's current and emerging requirements but also aligns with broader security and IT initiatives. The process should be highly collaborative, involving key stakeholders from business units, IT operations, and cybersecurity teams to address priorities, ensure organizational alignment, and secure executive buy-in.

Key actions for this step:

- Leverage the steering committee to guide roadmap development. Use the newly established cross-functional steering committee to review discovery findings, prioritize risks, and validate the roadmap's alignment with business objectives. Regular committee engagement is critical to drive executive support to maintain momentum and address evolving risks and challenges.
- Map PAM requirements to market capabilities and trends. Analyze your organization's specific needs against current PAM market capabilities and technology trends (e.g., AI, cloud integration, remote access).
- Figure 2 illustrates the primary PAM tool categories that should be considered as part of your evaluation process. These categories are directly aligned with market trends and Critical Capabilities for Privileged Access Management.

Figure 2: Categories of PAM Tools



Gartner

Gartner covers these core tool categories for PAM: privileged account and session management (PASM), privileged elevation and delegation management (PEDM), and secrets PAM (SPAM), along with two adjacent tool categories: cloud infrastructure entitlement management (CIEM) and secrets management. Each category addresses a specific requirement for securing human and machine privileged access and other cybersecurity leaders considering an investment in PAM tools.

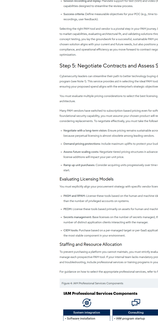
- PASM: Vaults and manages privileged credentials, isolates sessions, and records sessions for both human and machine users.
- PEDM: Grants specific privileges on endpoints, allowing users to run approved commands or applications with elevated rights.
- Remote PAM: Secures remote privileged access without a VPN, providing session monitoring, credential injection, and zero-trust enforcement.
- Secrets management: Programmatically manages and stores credentials and secrets for applications, services, and DevOps pipelines through APIs.
- CIEM: Governs and analyzes cloud entitlements, using analytics to enforce least privilege and detect risky permissions in cloud environments.

To ensure your PAM roadmap is both effective and sustainable, outline these steps:

- Integrate with broader security and IT initiatives. Ensure the PAM roadmap is aligned with related organizational projects, such as zero trust, cloud transformation, and digital workplace. This prevents duplicate efforts and maximizes investment value.
- Prioritize roadmap phases based on risk and business impact. Use risk assessments and business context to sequence implementation phases, addressing high-risk or critical-business areas first. Regularly review the roadmap to adapt to changing priorities.
- Define metrics, milestones, and success criteria. Establish clear KPIs and measurable milestones for each phase of the roadmap (e.g., percentage of accounts audited, reduction in audit findings, deployment timeframes). These metrics will track progress and demonstrate program success.
- Plan for change management and ongoing operations. Include communications and change management plans to drive adoption and engagement, provide training, and address resistance at the roadmap workflow.
- Evaluate vendor integrations and ecosystem fit. Ensure new workflows PAM solutions will integrate with your existing and future security stack (SIEM, SOC, ITSM, cloud platforms), prioritizing adaptability and seamless integration.
- Build flexibility into roadmap and address changes. Design the roadmap to accommodate evolving business requirements and emerging PAM technologies (e.g., AI, cloud integration, remote access).
- Adopt a maturity-driven, phased implementation approach. Purchasing a PAM tool based solely on current needs guarantees rapid obsolescence. You must evaluate vendors using a long-term roadmap designed to handle future challenges such as AI and remote access.

To plan for these advanced features, you must follow a strategic maturity curve as illustrated in Figure 3.

Figure 3: Example of PAM Maturity Roadmap



Gartner

By leveraging the steering committee for governance and validation, mapping requirements to market capabilities, and ensuring a tool-to-vision, risk-prioritized approach, organizations can develop a PAM roadmap that is actionable, measurable, and aligned with both business and regulatory needs. Treat PAM as an ongoing program rather than a one-time project. Regularly review and update the roadmap to address emerging threats, technologies, and business changes. Leverage the steering committee and executive sponsorship to drive success and demonstrate value.

Treat PAM as an ongoing program rather than a one-time deployment.

Step 4: Select a Tool and Vendor

To create a shortlist of vendors, collaborate with business leaders to explore the market and map your specific use cases against core capabilities. Review PAM platform deployment options to ensure they align with your organization's cloud policy. Your foundational requirements, and consider whether to host an RFP or schedule and review the RFQ, with at least four of your primary contenders, giving them your most difficult PAM use cases to solve.

For this step, use the categories from the Critical Capabilities for Privileged Access Management document to narrow down your vendor selection.

For further support might on RFP vendors, refer to Magic Quadrant for Privileged Access Management.

Architectural Considerations for PAM

PAM tools are delivered as software or provided as SaaS. SaaS offerings are gaining significant momentum, with most vendors now offering cloud-based options. Regardless of the delivery model, the tool must integrate with your existing IT environment to fully understanding both SaaS and software-delivered tool functionality. You must evaluate the following architectural considerations:

- Disaster recovery. Maintain access to critical infrastructure when the PAM tool or internet connection is completely unavailable.
- Break-glass procedures. Document, and periodically test procedures to retrieve credentials outside the PAM system.
- Customized credentials. Verify that SaaS-delivered services offer the same level of custom report generation as their software counterparts.

Conducting the and RFI Process

Use an RFI process to narrow the vendors by desired features. Use Gartner's Toolkit: RFI and RFP Questions and Vendor Selection Framework for Privileged Access Management to streamline your selection process. Use the tool to help you create a shortlist of vendors and a comparison matrix.

Running Proofs of Concept With Vendors

When executing a POC with vendors, focus on determining the user experience and overall solution effectiveness. Base your proof of concept (POC) on the following key areas, Gartner recommends you dedicate at least four weeks to:

- Session timeouts. Require similar management and session reconnection capabilities to improve the user experience.
- High availability. Clone and force-activate for SaaS solutions and verify resilience against internet outages or component failures.
- Service and machine account management. Confirm the presence of a built-in connectors to easily configure discovered.
- Session recording and replay. Mandate support for both SSH and video (RDP) recordings, and keystroke searchable AI capabilities designed to streamline the review process.
- Secrets vaulting criteria. Define measurable objectives for your POC (e.g., time to onboard accounts, success rate of session recordings, user feedback).

Selecting the right PAM tool and vendor is a pivotal step in your PAM journey. By rigorously mapping your requirements against market capabilities, conducting a thorough RFP process, and validating your choice through a proof of concept, you can make an informed decision that aligns with your technical and business needs. Remember, the goal is not just to find the chosen solution aligns with your current and future needs, but also positions your organization to maximize security, compliance, and operational efficiency as you move forward to combat cyberattacks, deployment, and ongoing program maintenance.

Step 5: Negotiate Contracts and Assess Staffing

Cybersecurity leaders are streamline their path to better technology buying decisions using the Gartner Buyertm program (see Note 1). The service provides you a roadmap to the best PAM tool, optimizing financial contracts, and ensuring your proposed spend aligns with the extracted strategic objectives.

You must evaluate scaling and pay considerations to select the best licensing approach for your foundational architecture.

Many PAM vendors have switched to subscription-based pricing over the traditional perpetual licenses. Given that PAM is a foundational security capability, you must assess your chosen provider's IP model to use for five to seven-year-before considering cybersecurity. To negotiate effectively, you must take the following actions:

- Negotiate with a long-term vision. Ensure pricing remains available across the expected platform life cycle. Increase personal licensing to avoid unfavorable renewing flexibility models.
- Demand pricing protections. Include maximum uplifts to protect your budget when your subscription deal expires.
- Assess future scaling needs. Negotiate tiered pricing structures to advance to a predictable model for long-term IT license additions will impact your per unit cost.
- Review up-all purchases. Consider acquiring only permanently over time rather than deploying all of them at the start.

Evaluating Licensing Models

You must explicitly align your procurement strategy with specific scaling models and licensing:

- PASM and SPAM. License these tools based on the human and machine identities getting privileged access when and the number of privileged accounts you manage.
- PEDM. Purchase licenses per endpoint, server, or device. Consider a hybrid model for environments.
- Remote management. Base licenses on the number of concurrent sessions managed, the total management transactions, or the number of remote applications. Avoid licensing each VM, for example.
- CIEM models. Purchase based on a per-managed target or per-feed application model. If both options exist, license the most stable component in your environment.

Staffing and Resource Allocation

To prevent purchasing a platform you cannot maintain, you must critically evaluate the operational skills required for ongoing administration. Assess your team's capabilities against the demands of the solution to identify training requirements, and recommend hiring, and professional services or training programs to close your implementation budget.

For guidance on how to select the appropriate professional services, refer to Figure 4.

Figure 4: IAM Professional Services Components

IAM Professional Services Components



Gartner

A diversified approach to contract negotiation and staffing ensures your PAM investment delivers sustainable and operational resilience. By aligning licensing models with your business case, prioritizing price protection, and building a skilled team, you can maximize the value of your PAM solution and mitigate long-term risks. Remember, continuously monitor your contract and staffing needs to adapt to evolving threats and business changes, ensuring your PAM program remains effective and aligned with your business and technology needs evolve.

Success Measures

As established in Step 3, defining clear metrics, milestones, and success criteria is essential for tracking progress and demonstrating the value of your PAM program. Therefore, to measure the success of a PAM implementation and ongoing operations, cybersecurity leaders must adopt ODMs that demonstrate direct business value. Rather than merely tracking operational activities, leaders should use the following examples to link technical achievements directly to risk reduction and operational efficiency.

Table 3 illustrates example ODMs and how they relate to business outcomes.

Outcome-Driven Metrics Enlarge Table

Metric category	Technology metric	Business outcome
Discovery, inventory, implementation	Percentage of total privileged accounts successfully discovered, vaulted, and stripped of poor hygiene markers	A measurable reduction in the unmanaged attack surface and decreased likelihood of credential-based breaches
Enforcement of least privilege (protect)	Percentage of privileged access transactions executed through just-in-time and just-enough privilege controls versus standing access	A significant reduction in uncontrolled, always-on privileged transactions, and fewer related audit findings
Session visibility and control (comply)	Percentage of privileged interactive sessions successfully recorded, indexed, and actively reviewed by audit teams or AI analytics	A measurable reduction in the time and financial cost required to conduct forensic security investigations
Integrations and automation (enable)	Percentage of privileged access provisioned and managed automatically by the PAM tool (eliminating manual	A reduction in manual IT administrative overhead and operational risks caused by manual

Source: Gartner Analyst Research

For further insight, please review Drive IAM Value With Outcome-Driven Metrics.

Note 1: Gartner BuySmart™

The Gartner BuySmart™ tool helps guide you through technology evaluations with templates containing requirements and scorecards to help you select the best providers for your needs. Using a connected workflow, BuySmart enables you to conduct thorough evaluations to invest confidently. See the BuySmart template designed for privileged access management.

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.