EBOOK

PAM Buyer's Guide

A no-fuss, non-salesly tour of what matters most

Saviynt

Table of contents

Saviynt

Security Leaders, we wrote this guide with you in mind.

If reducing risk is on your agenda, the last thing you need is a complex deep dive into privileged access management.

In light of modern security challenges and demands for reduced time-tovalue, we're here to help you evaluate a new generation of PAM solutions.

Well run PAM programs add enterprise-wide visibility and leverage identity intelligence and analytics to help leaders make better access decisions. You're likely hunting for the right list of questions to ask and concerns to raise en route to this more secure reality.

We believe you'll discover this here.

New Problems with Old-School PAM

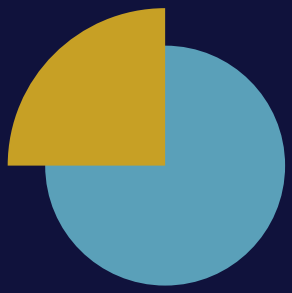
The frenzied pace of cloud adoption introduces breach risks that legacy privileged access management systems (PAM) fail to guard against.

VentureBeat **mocks the notion** of relying on out-dated PAM to protect cloud infrastructure, suggesting it's like "buying a new car and insisting on traditional key locks instead of Bluetooth-enabled key fobs."

While Zero Trust tops security leaders' priority list, insider privilege misuse continues to plague security efforts. Today, insecure or misconfigured credentials account **for almost** 50% of cyberattacks.

While fundamental controls are slowly entering the enterprise, concerningly, more advanced security lags:

Only 35% of enterprises **express confidence** in their ability to identify and manage privileged access.



32% of organizations are confident that privileged users cannot work around existing security controls.

- 2022 State of Enterprise Identity Security Ponemon Institute

Security risks are too pronounced to delay modernizing PAM. While Gartner suggests that the discipline is core to every security program, finding, evaluating, and understanding solutions offering differences is a challenge.

To simplify the work, our team offers expert insights into the PAM evaluation process. In this guide, we highlight:

- Defining Characteristics of PAM (Hint: not all “modern” PAM solutions are created equal!)
- The 4 Must-Ask Questions When Choosing PAM
- Truth vs. Hype: Functionality That Matters for Better Security

What are the Characteristics of a Modern PAM Solution?

For workloads in the cloud, traditional PAM underperforms with inflexible architecture, persistent over-privileging, and weak visibility and context for user access.

In contrast, modern PAM is cloud-built and cloud-native, not just for the cloud.

This is a critical distinction – and essential to understand if organizations expect to embrace multi-cloud security and the agility, availability, and scalability that cloud promises.

We define modern PAM through four common characteristics. Successful enterprises use these as baseline evaluation criteria, and each are discussed below.

Modern PAM:

- Is built on cloud-native architecture (“Cloud-born”)
- Delivers awareness around cloud risks
- Builds in governance
- Enables zero trust/zero standing privilege

CHARACTERISTIC #1

Born in the Cloud

Most IT security professionals know of a failed PAM project. Industry stories abound, and add unease for leaders ready to embark on a transformation effort.

This doesn’t have to be your story.

In general, the primary culprit is the practice of attacking sprawling privileges with decades old tools. Traditional PAM solutions are built on on-premises infrastructure and utilize outdated practices. Often this means locking privileged credentials into a vault and rotating passwords to these accounts. But when deploying this approach for cloud workloads, security lags. Among the key reasons:

- DevOps processes outpace accessing monitoring capabilities
- Local privileged credentials remain undiscovered (and unmanaged)
- Certifiers can’t grasp a full view of environment access to attest to least privilege

In their natural form, cloud environments are both scalable and elastic. This introduces a few problematic dynamics for on-premises IT infrastructure.

A particularly threatening one involves traditional PAM’s inability to support dynamic processes, including growing use of ephemeral resources. This is true even of solutions that market themselves as “for the cloud.”

PERSPECTIVE FROM THE PROS

“Building solutions in the cloud adds an understanding of how the cloud actually works: its scalability, elasticity, and velocity. If you’re just moving on-prem apps and methodologies the cloud, you’ll slow down.”

- Cris Owen, Product Director, Saviynt

Cracks emerge within access security efforts as enterprises push for speed and agility within cloud (in particular, multi-cloud) environments. Notably, outdated tools lack continuous monitoring capabilities to identify new instances and anomalous activities. Visibility is fundamental to governance and security – without it, particularly across multi-cloud environments, security postures weaken.

CHARACTERISTIC #2

Detects Cloud Entitlements & Misconfiguration

Granular awareness of identities, resources, and entitlements is a must-have to securely manage privileged access.

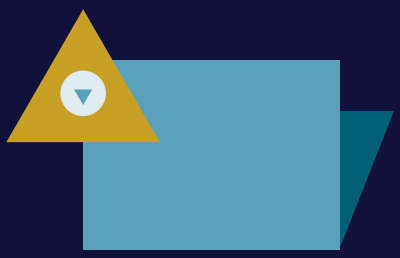
This type of awareness is achieved through visibility – and is essential for simplified onboarding, including for on-prem or SaaS applications. For this, functionality like real-time workload or entitlement discovery is useful.

Continuous discovery remains central to this – but so too is automated remediation of risks or misconfigured objects as they arise. High performing PAM tools introduce this advanced remediation capability and handle tasks like auto-terminating a session or removing a user’s access. Where you can put automation to work on behalf of your security team, do it!

We see this as a crucial characteristic because enterprises have a nasty habit of splicing disparate solutions when trying to reduce risks.

However, once varied cloud security services, access management, privileged user access, and governance tools are put in place, leaders are left with disjointed access management processes and inconsistent implementation of infosec policies. The inherent complexity and inconsistency that comes with this approach weaken an organization's overall security posture.

PERSPECTIVE FROM THE PROS



"Using disjointed tools leads to delays and inefficiant, manual, or incomplete discovery of anomalies. Reducing the risk of malice, misuse, and mistakes requires near-real-time detection and automation."

- Dennis Shea, Director PAM, Saviynt

CHARACTERISTIC #3

Offers 'Governance by Design'

'Governance' within traditional PAM tools is a misnomer.

Platforms may produce reports signifying what credentials a user has access to, but they can't affirm whether the user should have access to begin with.

Reconciling inconsistencies requires manual, human intervention. This isn't governance at all.

Gartner **calls effective governance** a pillar of PAM. For real governance, enterprises must understand appropriate access and possess the means to right-size as needed, including across infrastructure, apps, and cloud.

Built-in governance allows enterprises to clearly define roles and access, and then roll back their privileged access footprint. Many start by reigning in always-on privilege (like access residing with former IT Administrators, for example) with certification campaigns and ownership succession management.

Governance by design ultimately catalyzes the end goal of just-in-time (JIT) privileged access. By embedding this, enterprises have the necessary checks and balances before a user, session or asset is created within the privileged environment.

CHARACTERISTIC #4

Enables Zero Trust & Zero Standing Privilege

Zero Standing Privilege (ZSP) describes that utopian-state practice whereby security tools eradicate any 24 x 7 x 365, always-on, permanent permissions.

ZSP policies ensure that user access to systems, applications, or servers is retrieved as needed, where credentials are created every time an approved access request is generated.

Privileges get granted at the minimum-level required – versus over-provisioning for simplicity – and specifically for the required task.

This tactic reduces both attack surface and blast radius, making it more difficult for attackers to gain access and move unabated inside the IT ecosystem.

In a ZT or ZSP world, admins evaluate a user requesting access based on their identity profile and grant or deny access. Fine-grained entitlements allow them to grant precise access, too. Some PAM solutions also support dynamic risk scoring based on usage, behavioral analytics, peer group analysis, and risk information gathered from external applications.

PERSPECTIVE FROM THE PROS

“Removing as much static privilege as possible will be on of the biggest contributors to risk reduction you’re likely to see.”

- Chris Owen, Product Director, Saviynt

Your 4 Must-Ask Questions When Choosing PAM

1

How will the solution advance my risk reduction strategy?

The big reason this question matters.

Reducing privileged access sprawl is the first-step in proactive risk-reduction. Organizations must be able to execute this regardless of identity type – and in real-time.

The effort must extend to securing, managing, and monitoring elevated access of non-human identities too, like bots, IoT devices, serverless functions, containers, and APIs.

Holistic risk reduction strategies depend on IT doing more than just securing known privileged credentials and repurposing outdated vault-driven tactics.

As we've **explored** before, centralizing privileged accounts in a vault can't reduce the number of privileged accounts or reduce the risk of these privileges. Although the intent is genuine (and once offered reasonable perimeter-based security), the practice actually perpetuates a problematic "always-on" access principle.

To better understand a solution's risk-reduction potential, Dennis Shea, North American PAM Director at Saviynt, encourages organizations to ask use-case specific questions. These should relate to risk concerns you regularly navigate.

"Ask your provider: 'How can I be sure that when a vendor or contractor leaves, they can no longer use the account, and that the account can't be compromised from an external attack or through internal misuse?'"

According to Shea, "this forces vendors to systematically walk through a real-world example and connect standard identity processes to risk reduction capabilities."

2

What business & stakeholder needs should I consider during evaluation?

The big reason this question matters.

Before selecting a PAM solution, project sponsors should understand the goals, applications, and workflow impacts across a range of stakeholders. Prior to making a purchasing decision, make sure to outline a) key stakeholder personas, and b) their relationships with 'risk.'

Awareness here improves your odds of adoption and risk-reduction outcomes. Select stakeholders may include cybersecurity teams, IT users, audit staff, and executive leadership. These specific stakeholder groups prioritize varied elements of the risk reduction effort. Further, stakeholders may have distinct concerns ranging from reducing attack surfaces, to eliminating manual work, simplifying lifecycle management, or reducing expenses.

Figure 1: Risk Relations

Modern PAM platforms address these myriad priorities through functionality like:

- Drag-and-drop roles and policies to streamline PAM onboarding
- Discovery of hidden or unmanaged privileged accounts to eliminate or govern them (and reduce likelihood of breach)
- Unlocking easy elevated access request approvals to help users perform time-bound privileged tasks

Even under optimal conditions, implementing PAM can be challenging. As you **build support for PAM** initiatives, getting buy-in from every department is critical. PAM programs affect different teams in different ways. Start smart: map different roles to their relationship to risk, and coordinate an approach to build consensus. Then, evaluate PAM solutions with respect to the needs and corresponding capabilities that you find.

3

Will this solution fast-track identity tool consolidation/convergence?

The big reason this question matters.

The right PAM solution eliminates business and IT silos now, not later. It is positioned to integrate seamlessly no matter the direction of future security initiatives.

In the last few years, we've seen aggressive shifts toward providing approved, time-bound, leastprivilege access to critical assets that can be monitored and audited. Modern PAM meshes with this priority, using real-time discovery of assets continually spun up in the cloud, and utilizing cloud-native technologies to manage the velocity and scale of these changes.

This has helped businesses to reduce the **impact radius** of a security incident, and slash the time required to exfiltrate data from adversaries.

In many cases, **modern PAM eliminates the need for supplemental tools – like standalone CIEM** which may introduce complexity and new operational burdens.

Modern PAM platforms address these myriad priorities through functionality like:

- Drag-and-drop roles and policies to streamline PAM onboarding
- Discovery of hidden or unmanaged privileged accounts to eliminate or govern them (and reduce likelihood of breach)
- Unlocking easy elevated access request approvals to help users perform time-bound privileged tasks

Even under optimal conditions, implementing PAM can be challenging. As you **build support for PAM** initiatives, getting buy-in from every department is critical. PAM programs affect different teams in different ways. Start smart: map different roles to their relationship to risk, and coordinate an approach to build consensus. Then, evaluate PAM solutions with respect to the needs and corresponding capabilities that you find.

TRADITIONAL PAM

For on premises systems and servers, traditional PAM solutions do everything you'd expect around vaulting, admin credential rotation and secrets management. These solutions are not equipped to handle the velocity of dynamic cloud workloads.

To solve for this, many organizations incorporate CIEM tools into their already crowded security toolbox.

TRADITIONAL PAM + STANDALONE CIEM

CIEM tools manage what an identity can access in cloud environments, but they don't solve the governance problem and only offer limited privilaged access management within applications.

Plus adding tools means adding complexity and operational burdens.

SAVIYNT PAM

Saviynt PAM, powered by our converged Saviynt Identity Cloud platform, is a more complete solution. With it, you can address the vest majority of today's modern PAM use cases - including PAM for any app - and decrease your reliance on multiple point tools.

Modern PAM **also converges with identity governance and administration (IGA)** tools to tie identity to privileged access and preserve future investment.

Converged solutions offer consistent visibility and security across hybrid and multi-cloud environments, without needing multiple products. Unlocking converged IAM capabilities including, IGA, PAM, third-party, application access, and data access governance also helps organizations reduce costs (TCO) and increase productivity (ROI).

Of particular note, unifying IGA with PAM **allows organizations** to administer standard and privileged access – and add essential visibility into changes and activity for critical access.

The outcome: For the first time, enterprises understand the risks associated with a person's, group's, or asset's access across the enterprise. To sustain this, your PAM must not present an onerous, expensive, or manual requirement for maintaining integration.

4

How can my time to value shrink?

The big reason this question matters.

The outsized success factor for identity security campaigns is quick, obvious, value. Projects flop when issues like cumbersome management, security operations complexity, and unintuitive user experiences persist.

For enterprises to generate the immediate value they want, they must start with minimally disruptive solutions. This means both unity in otherwise fragmented tools (see above) and reducing complexity. As we always ask: Do you want to run your identity program or have it run for you?

To evaluate ways to compress time to value, probe where complexity and waste are most pronounced. Does your solution display:

- Modern user interface
- Low code/no code architecture for workflows and connectors
- Simple, wizard-based application onboarding
- Cloud-native architecture for scalability
- Auto-discovery of varied workloads and identities
- A “light,” modular that supports adding capabilities if/when needed
- Real-time risk insights and intuitive dashboarding
- Seamless, no-touch updates

The job of identity security is to verify that the right users (both human and machines) take the right actions in the right apps at the right time. Friction equals value loss: So weigh features, capabilities, and interactions accordingly.

Truth vs. Hype: Functionality That Actually Matters for Better Security

Modern risk plans tend to boil down to three priorities: **Security, efficiency, and cost effectiveness.**

In pursuit of these, we highlighted platform capabilities that are most worthwhile when evaluating new PAM solutions.

Simplified Management & Monitoring

Solutions must offer critical access management capabilities including risk-aware intelligent access requests, credential and key management and vaulting, session management, session monitoring, session recording, keystroke invocation policy, and keystroke logging of privileged users.

True JIT Support

Verify the ability to limit potential for users to bypass admin controls or experience standing privilege regardless of location or device. Your PAM platform should support credential-less access, time-bound access, dynamic risk assessment, and progress toward zero standing access.

Out-Of-The-Box Automation

Automation capabilities increase reliability and security. “Removing the human element,” particularly in new DevOps or robotic process automation (RPA) initiatives, and when delegating privileged access for third-parties adds value, **suggests** Gartner.

Rapid Asset Recognition

To close common entry points for data breaches and attacks, companies must be able to real- time discover assets spun up in the cloud (including those in cloud infrastructure and apps across DevOps tools, CI/CD solutions, cloud workloads, and data stores.)

Continuous Compliance

Confirm robust enforcement and management of security policies and compliance controls. Enterprises benefit when PAM solutions have comprehensive control libraries mapped to industry standards including CIS & NIST, SOC 2, SOX, FISMA, PCI, and HIPAA/HITRUST. Verify support for multi-cloud providers and applications, too.

Built-in IGA Functionality

Combining identity security functions in a single, cohesive platform lowers costs, increases efficiencies, and supports ongoing compliance. PAM vendors must be able to detail IGA, PAM, and other capability cohesion. Verify the existence of unifying controls and risk management for every identity and application, including administration of standard and privileged access for all human and machine identities.

Third-Party Privileged Access

Modern solutions must provide automated means for access provisioning, verification, and de-provisioning for all human and machine identities. Ensure that **third-party management** capabilities include basic lifecycle management (including onboarding and low-risk self-service registration) as well as risk and context-aware analytics for access review and policy management.

WANT TO LEARN MORE?

On a journey toward least privilege? We'd love to hear from you.

Our modern PAM solution is delivered via an agentless, zero-touch cloud-architecture so you can quickly deploy privileged access capabilities. We'll power your progress toward zero-standing privileges with just-in-time access and intelligent risk insights.

Comprehensive, yet simple. | We call it **PAM the way it should be.**

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com