Saviynt

Privileged Access Management Maturity in the Cloud Era

A Framework to Help Organizations Achieve and Sustain PAM Success

Contents

Introduction

Privileged access has emerged as the primary attack vector. Cyber attackers have been wildly successful in their efforts to exploit privilege to carry out their attacks.

Consider these statistics:

- **80% of data breaches** involve privilege misuse or compromise.
- The average cost of a data breach is **$4.35M**.
- Cybercrime increased **70% from 2019 to 2021** in the US. Damages from all types of cyberattacks total $6 trillion.
- Gartner predicts that mismanagement of identities, access, and privilege will account for **50% of cloud security failures** by 2023.
- On average, companies have 100 SaaS apps, and **43% are sitting abandoned** or unused, exposed to risks.
- By the year 2025, **75%** of cyber insurance providers will mandate the use of just-in-time Privileged Access Management (PAM) principles.

The analyst firm Gartner lists PAM as a **critical infrastructure** service and a **high-priority cyber defense capability**. However, the pace of cloud and SaaS adoption has exposed gaps in traditional privileged access management. IT is undergoing rapid digital transformation, bringing more cloud infrastructure and apps online every day. Combine that with the shift to remote work, the rise of machine identities, and the popularity of DevOps pipelines to stay competitive, IT teams have a significant security challenge to protect their rapidly changing environments:

- Lack of visibility across complex multi-cloud environments
- Privileged access sprawl with “always-on” privilege
- Limited or manual activity governance

Traditional PAM solutions are built on on-prem infrastructure and generally work by locking privileged credentials into a vault and rotating passwords to these accounts. The problem with this approach when it comes to cloud workloads include:

- Workloads created at cloud scale outpace agent-based PAM tools' ability to monitor access
- Local privileged credentials may remain undiscovered and therefore remain unmanaged by the PAM tool
- Certifiers can't get a unified view of the environment to attest to least privilege

Simply put, you can't fix today's cloud access challenges with yesterday's tools and approaches. Today's complex infrastructures require a comprehensive PAM approach that combines PAM, Identity Governance Administration (IGA), and Cloud Infrastructure Entitlement Management (CIEM) solutions to simplify management and continuously improve cloud security and compliance.

> **Most organizations have implemented some form of Privileged Access Management, but often these initiatives fail to live up to expectations or were never aligned with the business needs in the first place.**

As a leading innovator in cloud-native PAM, we work with customers every day to reduce cloud risks and improve their security posture. We have recognized a need to rethink what it means to have a mature PAM program in today's multi-cloud world. Most organizations have implemented some form of Privileged Access Management, but often these initiatives fail to live up to expectations or were never aligned with the business needs in the first place.

What's needed is a new definition of PAM success in the cloud world. This whitepaper will lay out five levels of PAM maturity, define the business challenges they solve, and what risks remain. We'll also explain why organizations typically struggle to meet PAM goals with traditional tools. Finally, you'll learn how identity-based PAM delivered in the cloud can help organizations meet their objectives and reduce risk more quickly and cost-effectively.

LEVEL 0: No Modern PAM Solution

But before we dive into the PAM Maturity Model, there are organizations at – let's call it – Level 0 that still rely on manual processes and tools.

In this risky category, organizations do not have a modern enterprise PAM solution. Security teams may be managing administration for Windows servers using Domain Admin Group membership or relying on manual methods, such as spreadsheets to track passwords, service accounts, and applications.

Characteristics:

Organizations in Level 0 of PAM maturity may share many of the following characteristics:

- Admins leverage local administrative credentials to perform privileged tasks on Unix/Linux systems, databases, etc.
- No PAM vault or visibility of the privileged credentials in the environment.
- Because of the reliance on manual methods, it's hard to tell who has access and what privileges they have, but:
  - it's probably safe to assume that users have more privileges than they need to do their jobs;
  - it's therefore not much of a stretch to imagine that privileges aren't revoked when the person leaves or goes to a different role.

Risks:

Because of rampant overprovisioning and lack of oversight, organizations at Level 0 are at a high risk of a severe data breach with loss of sensitive data, insider threats, ransomware, failed audits, and possible fines and litigation for being unable to certify appropriate access.

> **Organizations at Level 0 are at a high risk of a severe data breach with loss of sensitive data, insider threats, ransomware, failed audits, and possible fines and litigation.**

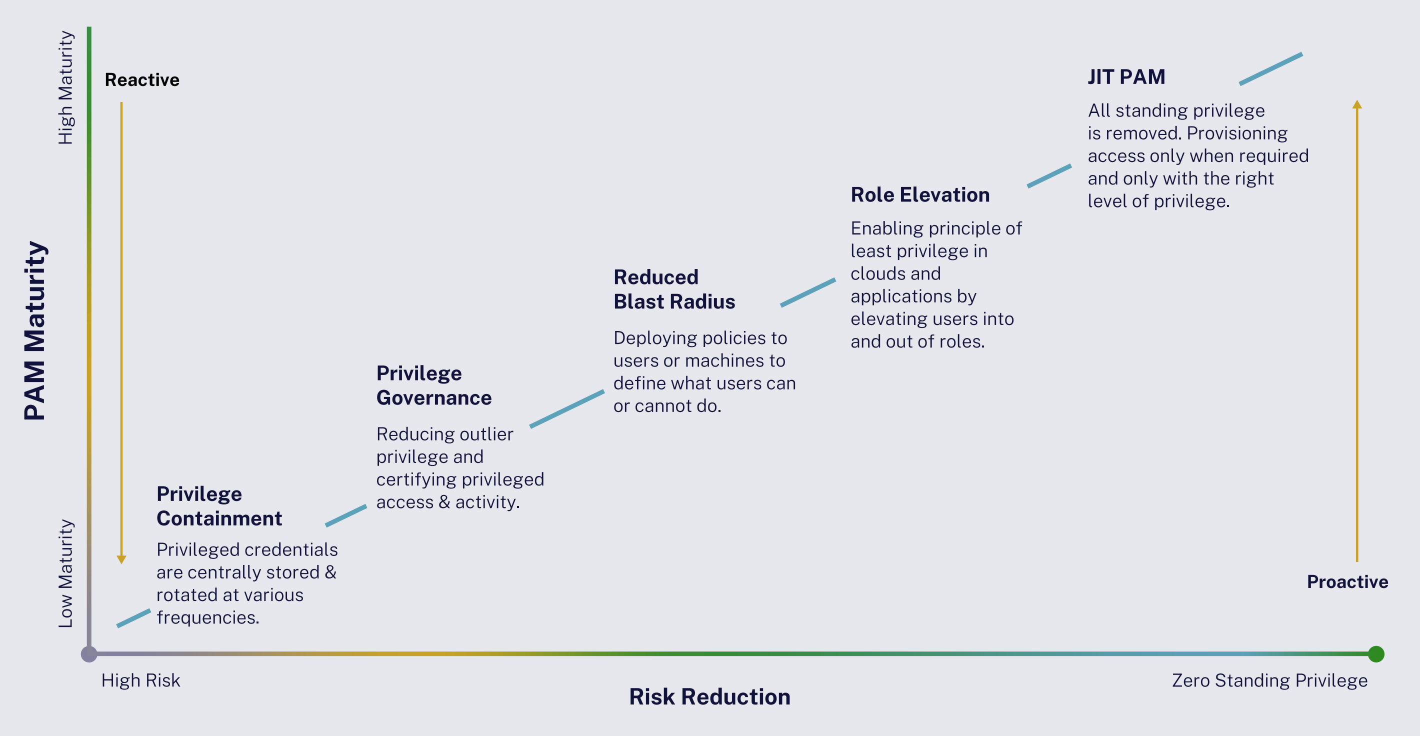
With the right planning — which includes identifying business objectives — and a cloud-delivered identity-based approach, achieving PAM maturity isn't as far away as it once was. With a PAM solution, organizations can reduce cyber risk without long implementation cycles and expensive infrastructure.

A fully mature PAM program will embrace the following controls:

- Privilege Containment
- Privilege Governance
- Reduced Blast Radius
- Role Elevation
- Just-in-Time PAM

Organizations can reduce cyber risk by working to programmatically implement least privilege in their entire ecosystem, including multi-cloud, SaaS, and IaaS. A PAM approach can help automate the underlying set of tasks for each area.

Saviynt PAM Maturity Model



Privilege Containment
Privileged credentials are centrally stored & rotated at various frequencies.

Privilege Governance
Reducing outlier privilege and certifying privileged access & activity.

Reduced Blast Radius
Deploying policies to users or machines to define what users can or cannot do.

Role Elevation
Enabling principle of least privilege in clouds and applications by elevating users into and out of roles.

JIT PAM
All standing privilege is removed. Provisioning access only when required and only with the right level of privilege.

LEVEL 1:

Privilege Containment

Traditionally, PAM programs start by discovering privileged accounts, putting them into a vault and onboarding. By centrally storing privileged credentials and rotating them at regular frequencies, access to these credentials are controlled by processes that can include workflows. By leveraging privileged session management and recording capabilities, organizations can track what actions were performed for auditing and compliance purposes.

Business Outcomes

- Known privileged accounts are centralized in a vault, providing increased visibility
- Improved audit results and compliance posture
- Some degree of automation for manual tasks

Security and identity teams can enhance their PAM programs with a dedicated tool that helps discover and establish an inventory of administrative privileged accounts and passwords — no more management by spreadsheet. Improved visibility enables teams to classify the types of credentials and secrets within the organization and establish privileged access workflows.

Risks and Challenges

Privilege containment — vaulting — doesn't reduce the overall risk posture and leaves organizations in a reactive security mode.

Vaults were first designed to manage default built-in credentials. Typically, the accounts that are vaulted first are those with the highest risk, such as administrator, root, and SA accounts. Sounds logical, but onboarding only high-risk accounts has limited business impact because very few people use them. From there, customers may move on to least privilege, possibly Active Directory (AD) bridging (a mechanism that allows users to log on to non-Windows systems using AD login credentials) to consolidate identities.

> **Saviynt’s simplifies onboarding of on-prem and SaaS applications via an intuitive wizard that includes real-time account, workload and entitlement discovery.**

Some organizations may move on to application and service accounts. But in reality, these are complex, lengthy deployments and many companies simply don’t get to this stage.

Saviynt PAM Difference

Vaulting is necessary for those critical standing accounts mentioned earlier — admin account on Windows, root account on UNIX, etc. These accounts need management and should be there for break glass purposes only. Once those basics are covered, removal of always-on privileged accounts can occur.

Saviynt’s approach is to simplify onboarding of on-prem and SaaS applications into our cloud platform via an intuitive wizard that includes real-time account, workload and entitlement discovery. Built-in automation and intelligence does the heavy lifting so that customers drastically shorten onboarding time and move to further levels of maturity.

LEVEL 2: Privilege Governance

Many organizations have a large footprint of privileged access in their environment. In the name of speed and convenience, administrators are given — or inherit — expansive, persistent privileged access. Over time, this access remains available even if no longer necessary, such as when the employee leaves or changes roles. The result is privilege sprawl, which can also extend to nonhuman accounts including:

- Service accounts (execute applications and run automated services)
- IoT devices (smart devices and sensors that can make changes to a network)
- DevOps tools (software coding that can make changes to DevOps environments)

To get privilege sprawl under control, organizations should leverage PAM tools to discover privileged accounts and work to define roles and access needed to rein in ubiquitous, always-on privilege. Activities like certification campaigns and their related cleanup processes should be programmatized to establish privileged access governance.

Business Outcomes

- **Reduced risk:** discovering and eliminating orphaned accounts and outlier privilege
- **Hardened access:** identifying environments and applications with default credentials
- **Automation:** improving the ability to certify privileged access and activity
- **Better insights:** understanding who has what privilege
- **Superior capabilities:** advanced attestation, audit, and compliance features

Risks and Challenges

Traditional PAM tools don't have governance. They can produce a report that says this 'user has access to these credentials,' but they can't lend any insight into whether the user *should* have this access. And it's up to humans to manually react to any findings in a timely and consistent way.

> **Traditional PAM tools don't have governance. They can produce a report that says this 'user has access to these credentials,' but they can't lend any insight into whether the user *should* have this access.**

For example, let's look at Rob, a sample user who has accounts on infrastructure workloads and various applications that allow him to perform certain activities. Rob has the ability to check in and check out privileged accounts. He may decide to take shared accounts under his wing. All of his accounts might have different naming protocols, which creates complexity when someone wants to see Rob's privileges across infrastructure, apps and clouds. This requires a whole new solution to see across these systems and tie together Rob's identity from the IGA tool and his privileged accounts in the PAM tool.

The entire process demands a lot of effort to correlate data, optimize policies and operationalize.

Saviynt PAM Difference

An integrated IGA and PAM solution can govern and manage all identities from one cloud platform. Saviynt's Identity Cloud platform allows organizations to onboard once and turn on additional capabilities like service account management anytime. With built-in compliance and control frameworks, organizations can make smarter decisions about access risks and ownership succession management.

LEVEL 3:

Reduced Blast Radius

This phase marks a shift to proactive controls and processes aimed at removing administrative rights from users and machines to reduce the impact of a security breach. According to the **2022 Verizon Data Breach Investigations Report**, 61% of all breaches involve credentials, whether stolen via social engineering or hacked using brute force. Organizations can harden their attack surface and reduce the blast radius of a breach by defining what permissions are granted, to what systems, and the duration of those permissions.

Business Outcomes

- Removed standing administrative rights from end users
- Fine-grained definitions of what users can and can't do
- Freed up IT teams by enabling more self-service access management
- Reduced attack surface by reducing the number of privileged accounts

Risks and Challenges

In a traditional tool world, getting to this stage is ultimately about deploying agents and capturing events on desktop, servers, and other systems. After months of observing user behavior, rules around role elevation can be created. Then constant human management of these rules is required.

> **Agents aren’t designed for cloud or ephemeral workloads, and many organizations only cover a few critical apps — no widespread deployment.**

At the end of the day, agents aren’t really designed for cloud or ephemeral workloads, and many organizations only cover a few critical apps — no widespread deployment. As organizations migrate to digital and cloud-first infrastructure, they may look to CIEM solutions to fill the cloud security gap and to enforce least privilege to cloud entitlements.

Saviynt PAM Difference

With Saviynt’s converged identity platform, Saviynt PAM tool leverages our IGA connectors to understand users and the access they have to applications and systems. This allows our customers to skip the agents and bypass this stage altogether.

Continuous monitoring and AI/ML-driven insights enable customers to detect and remove excessive access.

LEVEL 4:

Role Elevation

In this phase of PAM maturity, organizations apply the principle of least privilege to applications and cloud services. Users can be provisioned into and out of elevated roles to perform tasks with the least possible privilege. Organizations are able to discover and provision service accounts across identity and cloud service providers.

PAM is integrated with Identity Governance and Administration (IGA) tools for attestation and risk-based approvals. This enables identity teams to establish more granular policies for privilege elevation, manage the lifecycle of privileged credentials in the environment.

Business Outcomes

At this level of PAM maturity, organizations are employing preventative controls to harden their privileged attack surface. Gains include:

- Real reduction in privileged accounts across the enterprise, leading to a significant reduction in cyber risk
- Privilege Access Management extended to endpoints, clouds and applications
- Integration of privileged and standard user identity lifecycle management to prevent over-provisioning

Risks and Challenges

PAM tools were designed to grant access to accounts and manage them. Later, when organizations needed to conform to least privilege requirements, PAM solutions addressed this by granting permission to run a command. However, as stated earlier, these tools weren't built to understand roles or the complex, granular entitlements commonplace in cloud infrastructure and SaaS application entitlements. Roles and role management come from the IGA world and this is why many traditional PAM vendors are trying to move into identity governance.

PAM Difference

As a leading IGA vendor, Saviynt has more than a decade of experience developing the industry's most versatile Identity Warehouse, which houses every identity – human or machine and provides granular insights on all identities, access and usage from a single repository. Saviynt's combined IGA and PAM offering allows organizations to add the governance most PAM solutions are currently missing.

> **Roles and role management come from the IGA world. This is why many traditional PAM vendors are trying to move into identity governance.**

Additionally, if an organization wants to add third-party access governance, application access governance, or data access governance, they can easily add those capabilities in the future without having to add numerous point solutions to their ecosystem.

LEVEL 5: Zero Standing Privilege

Zero Standing Privileges (ZSP) is a term coined by Gartner, to describe the target state for privileged access in an organization to minimize risk of stolen credentials, privilege abuse, breaches, data loss and non-compliance. To enable ZSP, organizations restrict access to administrative identities by leveraging **Just-in-Time** (JIT) provisioning. Privileged access is explicitly granted and usage is monitored, allowing machine learning algorithms to identify anomalous behavior. Access is also granted at the minimum level of privilege required and only for the time needed to perform the task. This enables organizations to detect breaches early before attackers move laterally across organizational IT ecosystems.

Business Outcomes

- Ability to apply Zero Trust principles to privileged access management
- Reduce risk exposure by reducing the privileged attack surface
- Continuously discover cloud risks

Risks and Challenges

Traditional PAM solutions were purpose-built to discover and vault everything — and that capability is still widely promoted by the industry. So unless organizations are actually removing privileges as soon as accounts are onboarded, they will not be able to achieve zero-standing privilege.

Moreover, traditional PAM solutions scan environments at fixed intervals, but cloud resources are constantly scaling up and down. To make up for this deficiency, many organizations seek out cloud infrastructure entitlement management (CIEM) solutions.

> **Most cloud environments can benefit from a unified platform that combines IGA, PAM, and CIEM capabilities to provide an in-depth understanding of entitlements.**

According to Gartner, which coined this phrase in its 2020 Hype Cycle for Cloud report, “CIEM offerings are specialized identity-centric SaaS solutions focused on managing cloud risk via administration-time controls for the governance of entitlements in hybrid and multi-cloud IaaS.”

Limitations of Standalone CIEM

Adding another point solution into the identity stack can introduce more operational complexity. CIEM solutions rely on logs, which make them reactive. Organizations have many different use cases when it comes to cloud security. You should ask yourself, is CIEM enough? A stand-alone CIEM solution lacks IGA capabilities and is mostly limited to IaaS.

PAM Difference

Most cloud environments can benefit from a unified platform that combines IGA, PAM, and CIEM capabilities to provide an in-depth understanding of entitlements. This includes:

- Entitlement discovery
- Policy management
- Access provisioning
- Privileged access management
- Ongoing monitoring

Saviynt’s converged cloud identity platform has built-in CIEM capabilities to identify excessive access and unused entitlements and improve cloud security.

Saviynt Recommendations

✓ Take a risk-based approach to PAM adoption

Leverage a solution that can help you pinpoint risks and implement controls that will make the greatest impact in your environment.

✓ Go fully SaaS

A SaaS-based solution will improve adoption of advanced features.

✓ It's all about the platform

A tightly integrated PAM, IGA and CIEM solution that can be managed from a single control plane can increase visibility and staff productivity.

✓ Use built-in cloud IAM roles

Don't waste time, money and effort building your own.

✓ Extract fine-grained entitlements from other roles

Provisioning multiple roles to a user can lead to access creep and separation of duties violations.

✓ Don't settle for lengthy services engagements or rule-building cycles

Look for adaptive tools and solutions that provide near real-time detections out-of-the box.

Achieving zero standing privilege is not an easy task, and many times legacy PAM tools aren't up for the task in today's multi-cloud, pervasive SaaS world. But with an identity-based, SaaS-delivered approach, reaching PAM maturity does not need to be an arduous journey.

Where Are You?

How mature is your PAM program? Is it stuck in yesterday's approach or agile and future-forward? Take our three-minute self-assessment and get some insights on what is enabling or impeding your journey to PAM maturity.

ABOUT SAVIYNT

The Saviynt Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution.

Saviynt PAM solution is delivered via an agentless, zero-touch cloud-architecture so you can quickly deploy privileged access capabilities. Achieve zero-standing privileges with just-in-time (JIT) access and intelligent risk insights to power your PAM program.

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

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