EBOOK

JIT PAM: Time to Turn Off 'Always On'

Quick tips to give the right users the right access for the right time.

Saviynt

Table of contents

Saviynt

The era of “always-on” privileged account access is over.

Expanded risk surfaces, including clouds, DevOps, and SaaS, make managing privileged access more challenging than ever. At the same time, the volume and types of identities have exploded with remote work, third party workers, IoT devices, application IDs, and more.

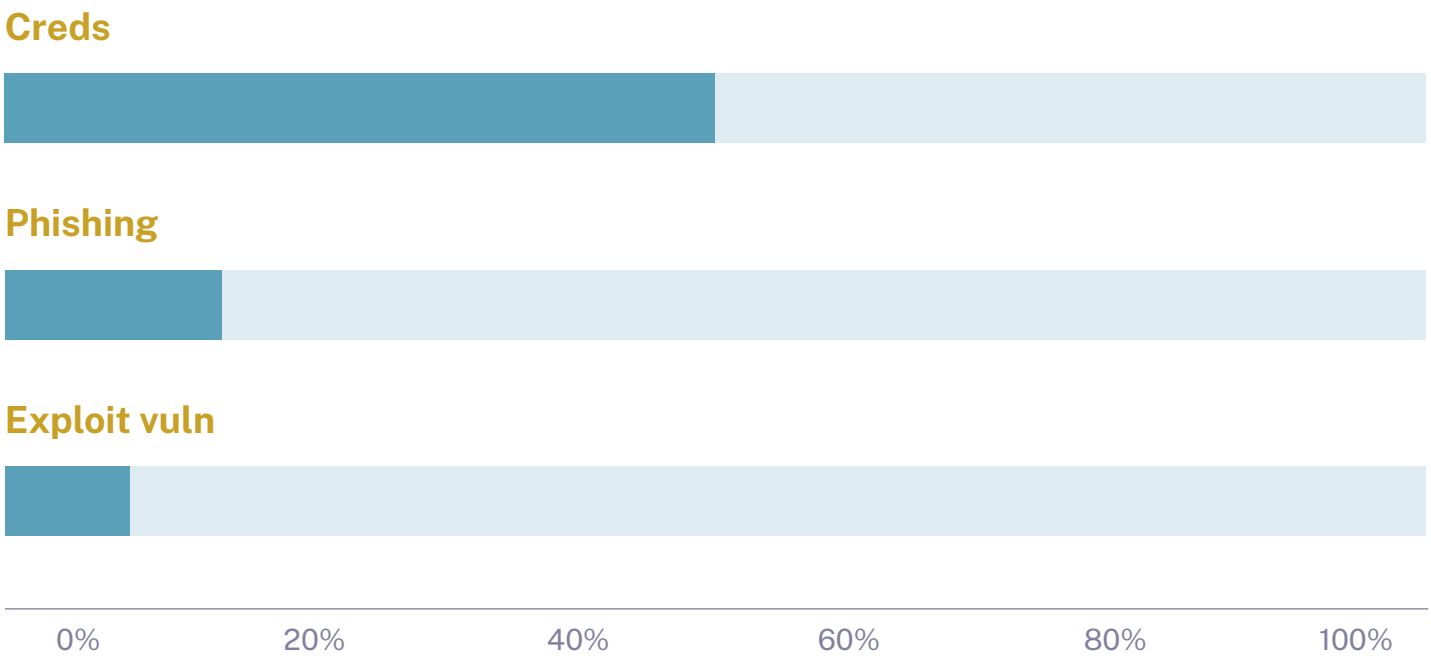
Today, organizations are assessing privileged access management (PAM) in a new light. Instead of simply locking and rotating credentials in a password vault, IT leaders are looking for ways to reduce risk by reducing privileged accounts.

Privilege abuse or misuse is a factor in nearly every cyber breach. In story after story, malicious actors show that they can bypass an organization’s security perimeter with something as low-tech as a phishing email.

Once inside a network, attackers can lurk undetected, looking for elevated privileges to open up more attack vectors. Depending on their goal, elevated access can help them gain access to sensitive data, deliver malware payloads, or even take full admin or root control over the entire environment.

These realities prove why the old model of privileged credential vaulting and session recording falls short. As long as standing accounts still exist, retain a high level of privilege, and stay centrally stored in a vault, organizations stay unnecessarily exposed.

The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.



Select enumerations in non-Error, non-Misuse breaches (n=4,291)

Assume Breach and Zero Trust IAM

Organizations must now adopt an "assume breach" mindset. This requires less reliance on a perimeter-only defense. Instead, they must shift to proactively limit an attacker's range and damage potential. The basis for this: Zero Trust.

Zero Trust identity means granting access only for the right reasons, to the right entities, for the right amount of time. Well-executed PAM programs need to enable *1) zero standing privilege (ZSP), and 2) principle of least privilege (PoLP)* to limit the time and scope of their privileged accounts.

SUMMARY BENEFITS

- **JIT PAM Enabler**
- **Quick Deployment Tips**
- **5 Approaches to JIT PAM**
- **Simplifying with the Saviynt Way**

Together, ZSP and PoLP reduce the time privileged access exists, and help provision privilege with precision.

Zero standing privilege is a target state of limiting access to critical information systems by applying Zero Trust principles to problems in privileged access management. ZSP represents the shift away from traditional privilege management where account access was "always on," – to granting access to privileged resources for a limited time on an as-needed basis.

The principle of least privilege focuses on access control and setting up minimal access privileges for every user and identity. Users are given the minimum level of permissions, resources, and data access needed to perform their job.

Adhering to least privilege principles reduces an attack surface by containing security compromises to a smaller area.

Just-in-Time PAM as an Enabler

Just-in-Time (JIT) PAM is a security practice that grants users, processes, applications, and systems an appropriate level of access for the necessary time to complete a task.

Implementing and automating JIT access provisioning reduces your attack surface and helps to prevent expensive and brand-damaging security breaches.

As organizations look to their PAM tool to help them with advanced capabilities like Just-in-Time privilege, they often stall out.

In general, we've found three primary causes for this:

- Traditional PAM solutions' JIT capabilities are limited to on-prem infrastructure.
- Security teams' awareness of where privileged accounts and entitlements exist is limited. The uncertainty adds confusion about where to start.
- Resistance to change: Stakeholder concerns weren't addressed in planning and deployment, and now these audiences are reluctant to change behavior.

To improve adoption and JIT privilege efforts, we share a few key ways to preempt (or eliminate altogether) the issues above.

Strategy Before Gadgetry: Quick Tips to Unleash High-Performing JIT PAM

Engage the Right Teams

Implementing PAM initiatives requires a cross-functional team paired with strong executive support.

The right team will include members from Security, IT Operations/DevOps, Audit and Compliance, Application Owners, and Executive Management. However, before you engage any teams, understand their *priorities, concerns, or drivers.*

SECURITY TEAMS

Expect to stave off potential cyber risks. Responsibilities may include:

- Minimizing attack surfaces
- Maturing security programs
- Aligning to best practice frameworks, cyber insurance, and other mandates

AUDIT & COMPLIANCE STAFF

Need to report on past or present-day risks. Concerned with:

- Documenting who has access to what – and what they are doing with that access
- Delivering reporting in an easily accessible and understood business language

IT USERS

Want to perform tasks in a risk-free way, but are hesitant to add steps that will slow them down, or tax existing resources. Considerations include:

- Likely end users of the PAM tool – need ongoing, consultative participation.
- May be resistant to change, fearful of being 'the bottleneck,' or adding access impediments
- May see 'access levels' as part of their status and identity. Withdrawing high levels of ongoing privilege may be seen as personal

EXECUTIVE MANAGEMENT

Care about overall business and IT initiative performance. Must balance risk/safety with achievement. Concerned with:

- Protecting the company's data and brand
- Eliminating risks, while empowering users toward high-performance productivity

Ensure that your executive sponsor grasps the business benefits behind PAM improvements. Then, they will clear obstacles or cut through internal bureaucracy where required.

Gather the Facts

First, companies need to understand the privileges landscape throughout the organization. This includes:

Inventorying what privilege currently exists and documenting dependencies.

Find out where credentials are used and if they are using services or are embedded in scripts. Some privileged accounts may have existed for years. These are likely interwoven in multiple apps and databases, and potentially hard coded and embedded in scripts. If you have a reliable asset inventory, this is a great place to start. If not, consider deploying an open source tool to generate this. A vulnerability management tool or ITSM system may also help catalog your IT assets.

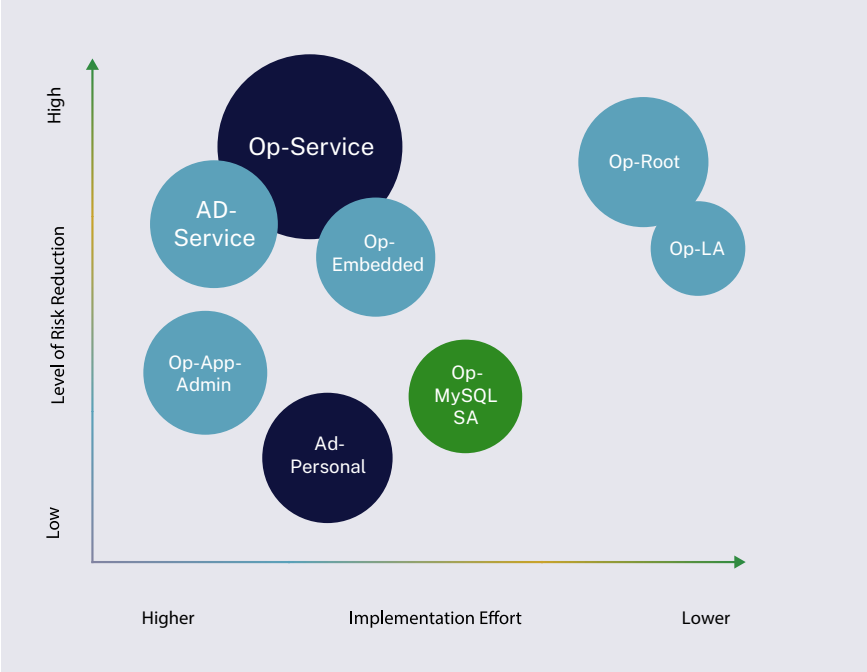
Determining systems, apps, and account owners. These 'owners' are your end users and stakeholders. This group must make decisions about what the PAM tool can and cannot do with the account.

Keep in mind: Finding accountable owners may be harder than finding the privileged accounts themselves. Often, privilege goes back years (pre-dating a current owner) and people may be hesitant to make disruptive decisions that can impact a system or process. This is where an executive champion can break through an impasse. In other instances, privilege may be hard coded into an application.

Map Your Risk Landscape

After you've inventoried assets and existing privileges, the next step is to build an implementation roadmap. Too often projects stall here. After all, it's common for enterprises to have four-times the number of privileged accounts as employees.

But, don't stress!



Expedite the process by organizing your accounts on a Risk vs. Impact matrix (See figure). Determine if the accounts represent high risk or low risk, and whether onboarding effort is straightforward or demanding. This mapping exercise can produce an easy-to-digest visual that displays where to start for maximum impact with minimal effort.

Find the Low-Hanging Fruit

Start a JIT PAM rollout with accounts that are relatively easy to address, but offer high returns in terms of reducing risk.

Examples include:

Administrator and Root Accounts. These are easy to onboard into a PAM tool, and are generally unused. Few users rely on these, however privileges are often extensive and unchecked.

Cloud Workloads. Attackers often target cloud workloads first, so these represent a major risk source. Workload access often comes via local accounts instead of through a shared network mapping system, so onboarding is particularly simple.

Third-Party Accounts. Contractor and vendor access is consistently a weak link. Varying access requirements and constant turnover make third-party access difficult to manage with precision. Fortunately, these accounts are not usually connected to Active Directory, so workforce impacts are minor.

As you assess starting points, guard against over-analyzing. Early on, the goal is traction. Once benefits become visible, eagerness among stakeholders to participate and grow security wins will expand. Keep in mind: Progress, not perfection while prioritizing momentum on simpler implementation path efforts.

The Various Approaches to JIT

If you envision Zero Standing Privilege as a destination, and JIT PAM as your vehicle, then the next metaphorical step is to *map your route.*

But which way makes sense? After all, just like on a road trip, there are multiple routes to consider. Here's a little travel guide to help you decide what path makes sense for you.

JIT: 5 Ways

1

APPROACH

Faster Deployment and Simpler Management

DESCRIPTION

A standard non-privileged account is temporarily added to a group which grants privileged access. Group membership is controlled by a tool.

A standard account, for instance, a non-privileged contractor, gets temporarily added into a privileged group to perform a specific set of tasks for a defined amount of time. Groups can be used to govern access to local privileged groups, Active Directory, and cloud services.

Although access is time bound and task specific, the model works only when privileged groups are well-defined. Over time, even well-defined groups start to morph as exemptions get granted. Before long, groups deviate from their original purpose.

Principle of Least Privilege

Yes, least privilege access is granted and enforced based on the defined policies and roles.

Zero Standing Privilege

No. Elevation policies are typically static policy files which always apply to the user. If that user or their machine is compromised, the attacker gains those privileges.

Operationally Friendly?

No. Keeping static rules up-to-date within a dynamic environment is time-consuming and error prone. For ease of management, users often end up over permissioned.

2

APPROACH

JIT Group Membership

DESCRIPTION

A standard non-privileged account is temporarily added to a group which grants privileged access. Group membership is controlled by a tool.

A standard account, for instance, a non-privileged contractor, gets temporarily added into a privileged group to perform a specific set of tasks for a defined amount of time. Groups can be used to govern access to local privileged groups, Active Directory, and cloud services.

Although access is time bound and task specific, the model works only when privileged groups are well-defined. Over time, even well-defined groups start to morph as exemptions get granted. Before long, groups deviate from their original purpose.

Principle of Least Privilege

Yes, as long as the privileged group features well-defined policies.

Zero Standing Privilege

Yes. Group membership is temporary and is removed automatically.

Operationally Friendly?

No. Operationally demanding because group management and account addition and removal are manual. In addition, movement is project dependent, and project start/end dates often blur.

3

APPROACH

Enabled/Disabled Administrative Accounts

DESCRIPTION

Administrative shared accounts on networks or devices enabled or disabled to provide needed access.

In this model, shared administrative accounts that exist on devices or in the network get 'enabled' to allow users to perform specific tasks. When the task is complete, these accounts get disabled.

Encouragingly, privilege is not persistent. However, once enabled, full privilege is unleashed. Shared accounts usually contain excessive privileges, and can be difficult to manage.

Principle of Least Privilege

No. Accounts usually contain excessive privileges. Ideally, remove shared accounts and opt for an individual account approach.

Zero Standing Privilege

Yes, although the account is always fully privileged when enabled.

Operationally Friendly?

No. Configuring roles is manual and time-consuming. Dynamic cloud ecosystems can compound difficulties.

4

APPROACH

JIT Security Tokens

DESCRIPTION

An ephemeral, one-time access token is created for a specific task, device, and person.

JIT security tokens provide ephemeral certificate-based access to critical IT resources. Instead of using username/password credentials to obtain access, the user obtains a one-time security token to access the target system. Tokens are typically used with SSH-based workloads and provide granular, task-specific access.

Principle of Least Privilege

Yes, as long as the token is configured with precise, task-specific access.

Zero Standing Privilege

Yes, and reduces the number of standing privileged accounts.

Operationally Friendly?

No. Configuring roles is manual and time-consuming. Dynamic cloud ecosystems can compound difficulties.

5

APPROACH

JIT Account Creation/Removal

DESCRIPTION

An ephemeral privileged account is created for a defined task and is removed upon task completion.

This methodology helps eliminate standing privileged accounts that may be exploited in a cyber-incident. In this model, organizations keep a few admin/root accounts that are vaulted for break-glass purposes. All other privileged accounts exist for a finite period, with limited permissioning. JIT Account Creation/ Removal meshes with the core tenets of Zero Trust.

Principle of Least Privilege

Yes, as long as granular privilege is defined for the account.

Zero Standing Privilege

Yes. An account only exists for a specific period of time for a relevant task.

Operationally Friendly?

It depends. With traditional PAM tools, this approach is difficult to achieve.

To extend JIT PAM for cloud-based workloads, organizations can simplify operations with a SaaS-delivered cloud PAM layer. By integrating into existing identity and security environments, security leaders can easily monitor excessive cloud entitlements.

The ‘Saviynt Way’ to Simplify JIT PAM

Saviynt’s Enterprise Identity Cloud (EIC) platform unifies privileged access management and identity governance with built-in cloud infrastructure entitlement management (CIEM).

Behind Saviynt’s agile, risk-based approach to PAM is a fundamental goal: ***Eradicate persistent accounts, standing privilege, and establish governance from Day 1.***

With our converged identity platform, enterprises can leverage a vast library of out-of-the-box integrations to provision privileged access management in days, while reducing operational complexity.

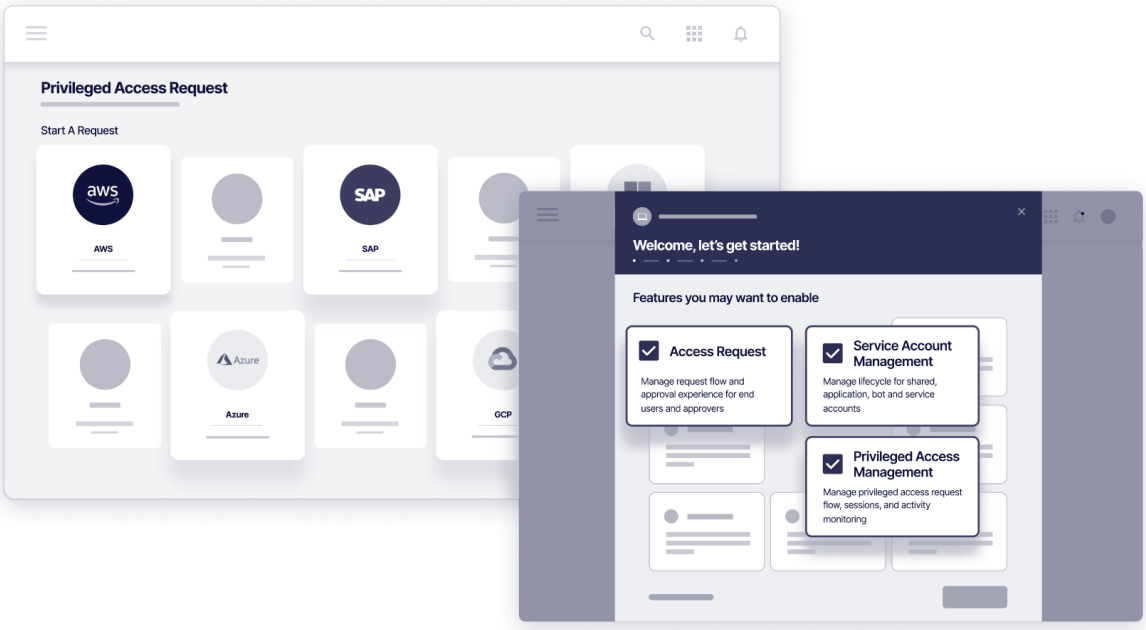
Saviynt Cloud PAM can help you:

- Manage privileged access for all applications and infrastructure from a single control pane.
- Use our vault to store credentials, keys, and tokens, or bring your own vault and add Saviynt Cloud PAM to reinforce modern use cases, such as cloud infrastructure, SaaS, and Just-In-Time capabilities.
- Achieve a zero standing privilege (ZSP) posture by enabling Just-in-Time and Just-Enough privilege.
- Discover cloud risks, continuously. Avoid piecemealing multiple point products with built-in CIEM.
- Make smarter decisions with governance-driven risk data and AI-informed privileged access data.
- Onboard privileged accounts and provision privileged workflow rules with a simple drag-and-drop.
- Declutter IT inboxes and improve visibility by supporting privileged access requests through our intuitive, visual platform.

Importantly, our EIC platform supports rapid, sustained progress.

Like you, we cringe at the horror stories of bogged down implementation projects stymied by brittle tools – and made worse by multi-faceted process steps, stakeholder inputs, and hard-coded privilege accounts. Instead, we architected an approach built around simplicity.

Deployment is a breeze, accentuated by smart touches like drag-and-drop, wizard-based approach to role provisioning. Sure, every organization has people and processes that may be sticking points to navigate – but with the right tools, these can be simply, securely, overcome.



Saviynt's drag-and-drop, wizard-based approach to role provisioning.

PAM the Way It Should Be

Saviynt's 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 powering your PAM solution.

ABOUT SAVIYNT

Saviynt is the leading identity governance platform built for the cloud. We help enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time.

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

REQUEST A DEMO

Saviynt

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

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