SOLUTION GUIDE

Saviynt

Privileged Access Management

Right-Time, Right-Level Privileged Access for Users, Machines & Applications

Privileged access is the number one method threat actors use to compromise critical systems and data. With the explosion of cloud ecosystems and SaaS apps, the attack surface has never been larger or more complex. Monitoring of privileged access risks across a broad network of applications can be a nightmare.

The old-school way of vaulting privileged accounts just moves the risk around and doesn't provide the granular visibility and control over application, cloud and on-premises identities necessary for best security practices.

With high costs and complexity for on-prem infrastructure and poor visibility across hybrid multi-cloud environments and SaaS apps, it's clear we need a more agile, risk-based approach to PAM.

Leading the Charge — PAM for Modern Digital Ecosystems

The Identity Cloud from Saviynt is revolutionizing PAM, blending identity governance with Just-In-Time privilege to deliver true least-privilege role elevation. Unlike outdated PAM solutions that can't handle granular app privileges, Saviynt PAM discovers changes within elastic workloads, new privileged accounts, and access points in real-time. This provides real-time, granular visibility, enabling admins to take immediate actions like terminating risky sessions and revoking unauthorized access using Real-Time Intelligence.

Secure multi-cloud environments with continuous, live monitoring for misconfigurations and built-in cloud infrastructure entitlements and posture management.

Cloud-Native PAM Fueled by Identity Intelligence

Saviynt's unified platform brings together privileged access and identity governance, so organizations can streamline privileged access management for user and service identities across any platform and application.

Wrap Saviynt Identity Intelligence – which actively analyzes dozens of identity attributes, user activity and risk indicators – into PAM to enable administrators to make more complex decisions quickly. Enable administrators to handle complex decisions such as privilege requests at scale with Real-Time Intelligence. Tackle cloud risks head-on by continuously certifying appropriate access continuously and providing continuous PAM governance.

Today's enterprise ecosystems are too complex and non-static to rely on incomplete or standalone privilege and identity tools at scale.

- Single control plane for identities, infrastructure, and applications
- PAM for Applications, Infrastructure, and Machine Identities
- Secure third-party access with identity governance and privilege access management in a single solution
- Reduce risk exposure by implementing least privileged access
- Provision time-bound privileged access
- Accelerate Zero Trust adoption
- Simplify privileged access and governance with PAM and IGA in one cloud platform

Just-in-Time PAM and Zero Standing Access

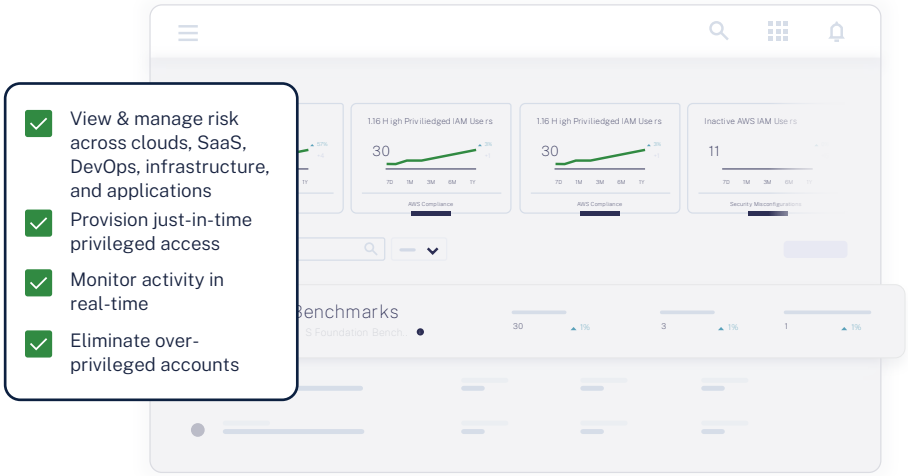
Push your Zero Trust goals forward with Saviynt's comprehensive identity and privilege platform. Use identity "roles" to manage time-bound, role-based privileged sessions. Enable just-in-time (JIT) access that provides users with elevated permissions exactly when needed, whether role-based, or account-based. Create true just-in-time accounts, preventing misuse and maintaining zero standing privileges (ZSP). Administrators can monitor those sessions live, preventing misuse or malicious activity. Enable administrators to limit the number of standing privileged accounts, preventing misuse and enabling management at scale.

Control Access and Secure Collaboration With External Parties

Use just-in-time access provisioning to cut risks and audit third-party activities. External partners, suppliers, and contractors often need elevated access to critical systems and data. Saviynt provides unmatched trust and control with seamless, secure self-onboarding, clearly defined roles and entitlements, time-bound role elevation, and smart session monitoring with notifications. Saviynt can offboard user privileges programmatically, require the user request JIT access, or can require a re-establishment of trust prior to further access to prevent offboarding.

Establish more trust and control with:

- Secure, seamless onboarding
- Defined roles and entitlements
- Time-bound role elevation
- Session monitoring with intelligent notification



Next Steps

Discover why analysts like Enterprise Management Associates (EMA) rate Saviynt as a privilege access governance leader

Get a demo of Saviynt PAM

Key Benefits

Unified Control Plane: Manage privileges within identities, infrastructure, and applications from a single control plane, simplifying privilege management and governance, providing a holistic view of all privileged activities.

PAM for Applications: Manage SaaS and thick-application access and identities, providing comprehensive risk visibility and access control to sensitive SaaS applications

Remote Privileged Access: Prevent third party misuse and lock down the most exposed area of your ecosystem –onboard trusted third-party identities properly, and offboard them when they no longer require access. Provision just-in-time access so third parties only have access when they need it.

Minimize Risk Exposure: Enforce least privilege access policies to minimize risk exposure. Implement time-bound access and ensure elevated permissions are only granted when necessary and are revoked once the session ends.

Push Zero Trust Forward: Support your Zero Trust initiatives by combining IGA and PAM, ensuring access is granted based on the principle of least privilege and continuously monitored for anomalies.

Continuous Compliance: Establish continuous compliance with built-in identity lifecycle management. Meet regulatory requirements with detailed audit-trails and automated certification campaigns.

Enhanced Productivity: Simplify identity security complexity, reduce legacy costs, and boost workforce productivity with the power of identity convergence. Intelligent automation delivers immediate value and transforms ROI. Enable all users across siloed personas to leverage a single, comprehensive platform –providing simpler user onboarding and enablement.

ABOUT SAVIYNT

Saviynt empowers enterprises to secure their digital transformation, safeguard critical assets, and meet regulatory compliance. With a vision to provide a secure and compliant future for all enterprises, Saviynt's cutting-edge solutions have been recognized as industry leaders. For more information, please visit www.saviynt.com.

Saviynt

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

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