



SOLUTION GUIDE

Saviynt for AWS

Simplify and secure AWS access –every workload, every instance, every time

AWS has become a cornerstone for organizations seeking rapid innovation, scalability and operational agility in the cloud. Its flexibility, cost-efficiency, and proven reliability have made it the platform of choice for both startups and global enterprises. But as businesses accelerate cloud adoption and migrate more critical workloads, the challenge of securing who – and what – has access to those assets has never been greater.

While AWS offers foundational access management tools, these are largely confined to AWS. They narrowly focus on access management, often require heavy manual processes and lack least-privilege enforcement. The result is limited governance and blind spots in understanding and managing identity risk across cloud infrastructures.

Saviynt Identity Cloud empowers organizations with deep visibility and control over access to critical AWS resources. Enforce least-privilege access through just-in-time and just-enough access, eliminating standing permissions and shrinking your attack surface. Continuously monitor access behavior and governance controls to detect risks early, maintain compliance and stay audit-ready.

Saviynt Identity Cloud delivers a unified solution that manages all identities -workforce, external, human and non-human -across on-prem, hybrid, and multi-cloud environments. Strengthen your identity security, improve compliance, and limit risks caused by policy misconfigurations, compliance drift and standing privileges.

Achieve Zero Standing Privilege with Continuous Governance

With a 360-degree of visibility of all identities and management from a single pane of glass, Saviynt Identity Cloud helps organizations gain control over AWS cloud access and user activity. By integrating with AWS Identity Center and HR systems, organizations can automate the entire identity lifecycle, mitigate Separation of Duties (SoD) conflicts, and correct misconfigurations to enforce granular access controls.

Benefits

- Enforce least privileged access with time-bound and just-in-time access to permission sets
- Automate the entire identity lifecycle
- Proactively identify and remediate risks before they become incidents
- Maintain and prove continuous compliance

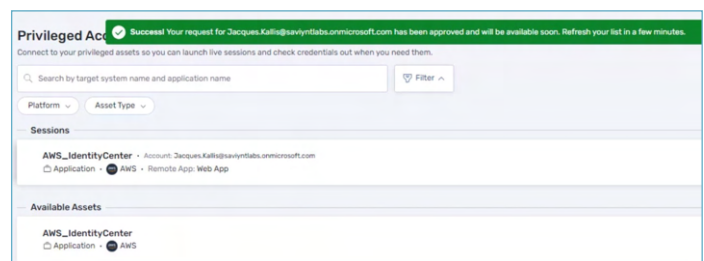
Industry Leading Identity Security

KuppingerCole Compass Leader

- Identity and Access Governance
- Privileged Access Management
- Multi-Vendor Access Control

Gartner

- Peer Insights Customers' Choice -'21, '22, '23, '24



Saviynt Identity Cloud streamlines processes and reduces human errors by automating the entire lifecycle.

Enforce Least Privileged Access Across all AWS Environments while Supporting Audits

Being able to define and manage access down to the resource level lets you minimize overprivileged access and align with zero-trust principles. Just-in-time and just-enough-access to AWS and non-AWS systems helps minimize fraud and eliminate orphaned accounts. Ensure audit readiness with end-to-end session recording and keystroke logging.

Account Detail	Owner	Entitlement Hierarchy	Associated Entitlement
Entitlements Hierarchy			

Fine-grained integration allows for greater analysis and control over data, access and governance posture.

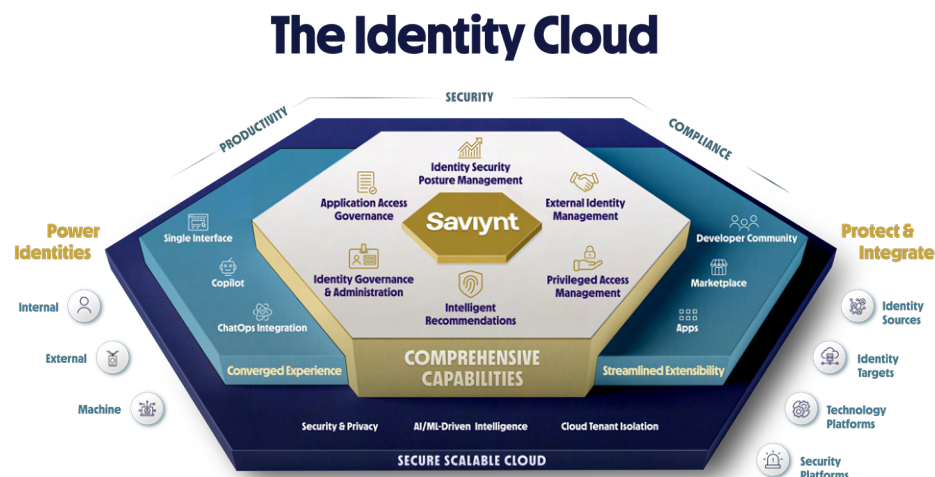
Recommendations Show All (20) →	
2 target systems have outdated credentials over 90 days	Review
9 sessions with suspicious command patterns detected	Review
8 privileged accounts have been inactive for over 90 days	Review
12 terminated users with active system access detected	Review

Dynamic recommendations prioritize risks that would have the greatest impact on the organization if exploited.

Elevate Your Identity Posture

Proactively identify and remediate identity risks before they become incidents. Continuous monitoring of identity access, data, and governance postures identifies anomalous behavior and problematic access patterns before they can be exploited by bad actors. Remediation recommendations are prioritized based on the biggest potential impact to the organization and allows administrators to promptly clip unused access across roles, passwords/secrets, access keys and permissions.

Identity Security Posture Management is a core component of the Saviynt Identity Cloud



Saviynt Identity Cloud Delivers:

- Identity Governance and Administration
- Privileged Access Management
- Application Access Governance
- Identity Security Posture Management

Identity Security for Any Application and Identity

- Multi-cloud, on-premises and hybrid environments
- Human or non-human
- Workforce or external

Next Steps

- Visit www.saviynt.com to learn more about The Identity Cloud from Saviynt
- Schedule a [demo](#)
- [Contact us](#) to learn more

ABOUT SAVIYNT

Saviynt's Identity Cloud is the leading identity governance platform. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. Saviynt converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution.

Saviynt

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

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