SOLUTION GUIDE

SAVIYNT FOR AMAZON WEB SERVICE (AWS)

SECURE AND GOVERN IDENTITIES AND CLOUD PRIVILEGED ACCESS

Saviynt

aws PARTNER Security Software Competency

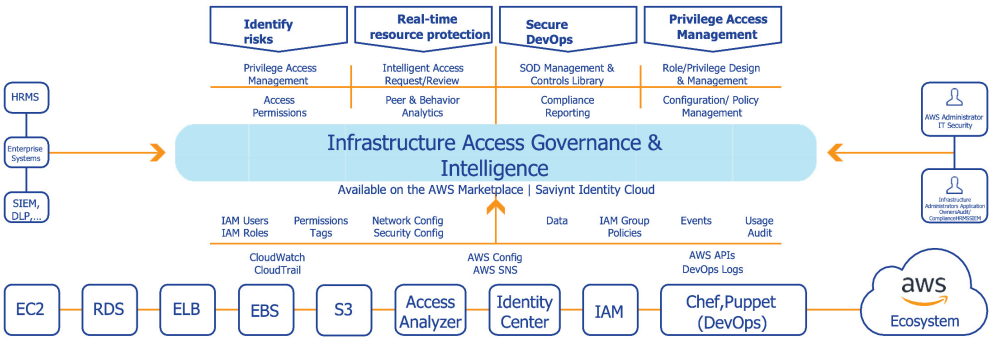
As organizations migrate workloads from internal data centers to cloud providers such as Amazon Web Services (AWS), security and compliance concerns need to take center stage. Security and Governance of AWS accounts, Identity Access Management (IAM), and DevOps users is often overlooked. The sheer volume of audit, policy and configuration data renders manual verification of vulnerable workloads extremely difficult. Privileged access--whether for applications running on AWS or for the infrastructure itself requires the same level of management and monitoring as it would on-premises. A number of drivers impact the security of AWS:

- Compromise of one privileged AWS account is enough to bring down the entire cloud infrastructure. Managing these "keys to the kingdom" is paramount.
- Managing IAM entities is complex and involves entitlements such as roles, cross-account roles, inline and managed policies, or access control lists (ACLs)
- Simplifying IAM processes that link these entitlements to enterprise systems (HRMS, ITSM, DLP, etc.) is key for a successful hybrid IT.
- Security controls and automated remediation are critical to "Get Compliant" and "Stay Compliant."
- Continuous monitoring and real-time prevention are essential to protect cloud infrastructure from cyber attacks. However, gaining sufficient visibility needs correlation of at least 5 different audit sources.

Get Secure with Saviynt

Saviynt enables organizations with real-time identification of risks in their AWS implementation, automation of access lifecycle management processes, management of privileged identities, access & sessions, enforcement of organizational security policies, and clipping of unused access.

The comprehensive integrations extend to many different AWS services including AWS IAM Identity Center and Access Analyzer. Additionally Saviynt Identity Cloud connects to DevOps platforms such as Chef, Puppet, and GitHub to secure AWS resources with Just-in-Time (JIT) privileges, aligning with a Zero-Trust model.



Get Secure with AWS

Cloud Privileged Access Management

- Real-time workload discovery and automated registration
- Keyless, browser-based containerized terminal sessions, no jump-host needed
- In-session role / access elevation and privileged ID-based assignment
- Session recording and activity review / certification

Risk Discovery

- Identify over 250 risks across AWS IAM Identity Center & Access Analyzer as well as DevOps resources such as EC2, S3, VPC, ELB, RDS, RedShift and CloudFormation Templates
- Integrated data classification, access analysis and remediation recommendations
- Support for multiple AWS accounts with local AWS IAM users and/or federated user

Designed for Scale and Security

- Available to purchase via AWS Marketplace & deployed in Saviynt Cloud hosted on AWS
- Enhanced data security and control with Bring Your Own Key (BYOK) and Bring Your Own Vault (BYOV)

Get Secure with AWS

Designed for Scale and Security

- Easily extend to secure other Cloud apps – Office 365, Azure, ServiceNow, Salesforce, Workday, SAP, Oracle, etc.

Real-Time Preventive Policies

- Identify policy violations in real-time with AWS Config and AWS Cloudwatch Events integration
- Define custom context-based access policies with flexible rules engine
- In-line collaboration
- Perform preventive actions such as stop launch of vulnerable workloads, seek multi-level approvals, perform access review/micro-certifications, prevent privileged access elevation

Sod and Compliance Controls

- Define cross-platform SOD rules for normal and privileged access
- Out-of-the-box mapping of controls to compliance regulations such as CIS, HIPAA, FedRAMP, PCI-DSS, SOC etc.
- Analyze SOD/controls violations using Usage and Access analytics
- Provide recommendations for clean up

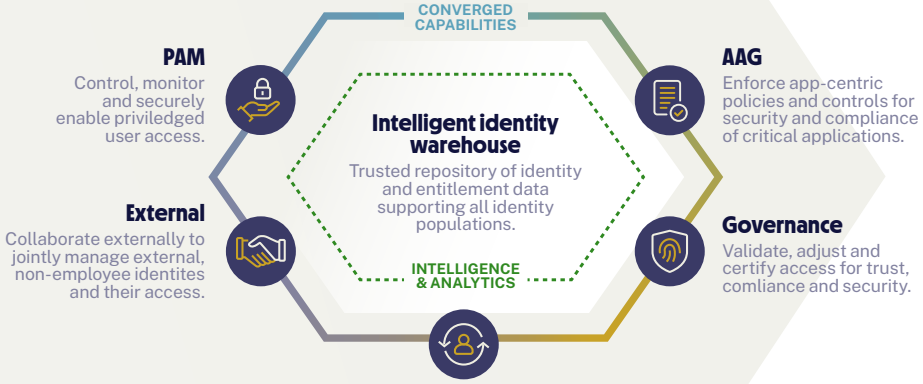
Security Intelligence

- Prioritized, real-time risk dashboards for actionable investigations
- Behavioral pattern analysis and peer comparison to detect outliers and unknown/insider threats
- Interactive drag-and-drop link analysis for rapid investigation on high risk events
- Perform user behavior analytics to identify suspicious activities, early Indicators of Compromise (IOC)

Cloud Platform Benefits

- Eases over-burdened IT resources
- Deploys rapidly
- Access to Saviynt Control Exchange to stay ahead of evolving compliance needs
- Availability tailored to meet every enterprise's needs

The Identity Cloud combines core identity security capabilities in a single platform that enhances security while reducing costs and management headaches.



Next Steps

- **AWS Partner Profile** to see Competencies & Certifications
- **Request a Demo** of Saviynt Identity Cloud

ABOUT SAVIYNT

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. The Identity Cloud 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