SAVIYNT FOR MICROSOFT AZURE

CONSOLIDATED VISIBILITY WITH CONTINUOUS MONITORING AND ACTIONABLE CONTROLS

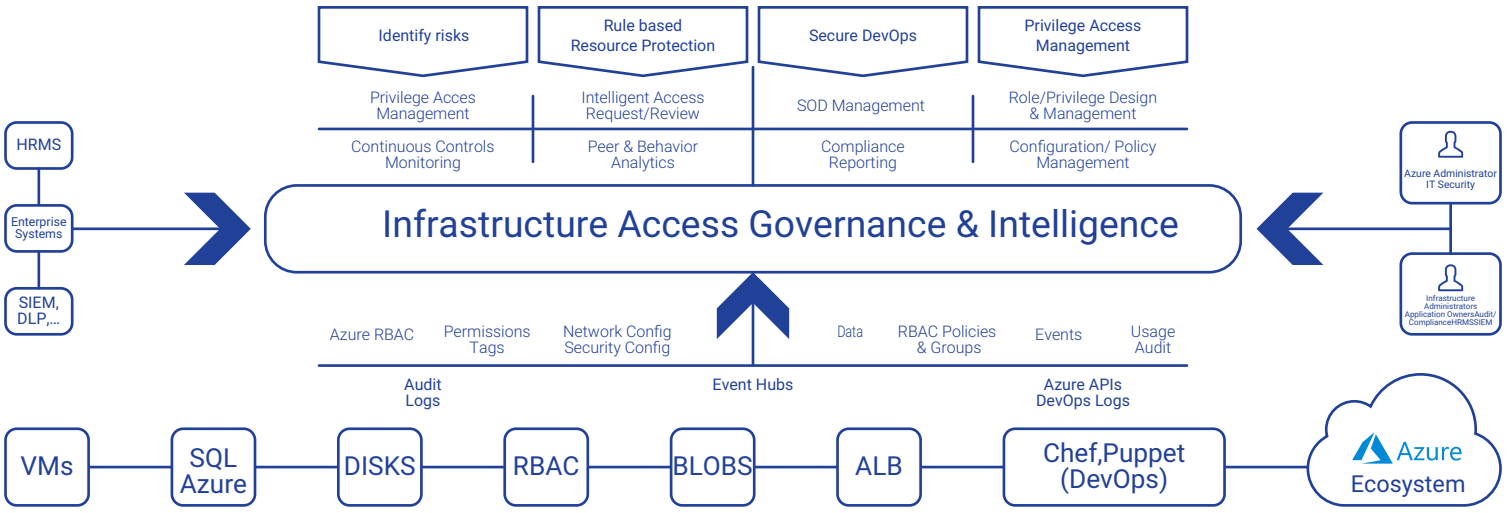
As organizations modernize and migrate their critical workloads from internal data centers to IaaS providers, such as Microsoft Azure, security and compliance concerns are taking center stage. One of the often overlooked areas is governance of both Azure subscriptions and DevOps processes. The sheer volume of audit, policy and configuration data that renders manual verification of vulnerable workloads is extremely difficult.

- Compromise of one privileged Azure subscription is enough to bring down the entire cloud infrastructure. Managing these **"keys to the kingdom"** is paramount.
- **Managing various objects/entities** is complex and involves entities such as virtual machines, storage objects, load balancers, VNETs, SQLAzure etc.
- **Simplifying IAM processes** that links these entities to enterprise systems (HRMS, DLP etc.) is key for a successful hybrid IT.
- Security controls and automated remediation are critical to **"Get Compliant" and "Stay Compliant."**
- **Continuous monitoring** is essential to protect cloud infrastructure from cyberattacks.

GET SECURE WITH SAVIYNT FOR AZURE:

Saviynt enables organizations with real-time identification of risks in their Azure implementation, automation of access lifecycle management processes, management of privileged access and enforcement of security policies. The comprehensive offering also extends to DevOps platforms such as Chef, Puppet and GitHub to secure Azure and DevOps resources.

SAVIYNT



Risk Discovery

- Identify over 150 risks across Azure and DevOps resources such as VMs, SQLAzure, VNETs, storage objects etc.
- Integrated data classification, access analysis and remediation recommendations
- Support for multiple Azure subscriptions

SOD and Compliance Controls

- Define cross platform SOD rules
- Out-of-box mapping of controls to compliance regulations such as SOX, HIPAA, FedRAMP, PCI, 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

Designed for Scale and Security

- Available as VMI to be deployed in organization's Azure subscription, eliminates 3rd party data compromise risk
- VMI allows auto-scaling security infrastructure
- Easily extend to secure other Cloud apps – Office 365, Azure AD, Salesforce, Workday, SAP, Oracle, etc.

Privilege Access Management

- Access request for limited duration privileged access grants (Azure RBAC roles)
- Automatic provisioning of access based on authoritative HRMS feeds
- Conduct session recording and activity review/ certification
- Perform user behavior analytics to identify suspicious activities, early Indicators of Compromise (IOC)

Saviynt El Segundo (Headquarters), 1301 E. El Segundo Bl Suite D, El Segundo, CA 90245, United States

info@saviynt.com
sales@saviynt.com

310-641-1664

Saviynt is a Cloud Access Governance and Intelligence company that focuses on providing simple, fast and cost effective solutions for organizations to manage security of their critical assets in the Cloud and Enterprise.