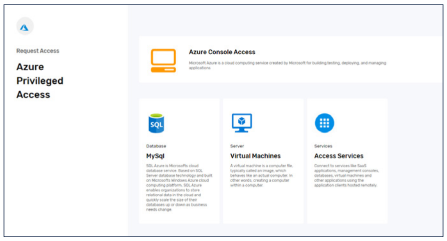
## COMPREHENSIVE SOLUTION FOR PRIVILEGED ACCESS AND CLOUD SECURITY

# Saviynt Cloud PAM for Azure, Azure AD and Microsoft 365 Applications



Request Access

Azure Privileged Access

Azure Console Access

Microsoft Azure is a cloud computing service created by Microsoft for building,testing, deploying, and managing applications

Database

MySql

SQL Azure is Microsofts cloud database service. Based on SQL Server database technology and built on Microsofts Windows Azure cloud computing platform, SQL Azure enables organizations to store relational data in the cloud and quickly scale the size of their databases up or down as business needs change.

Server

Virtual Machines

A virtual machine is a computer file, typically called an image, which behaves like an actual computer. In other words, creating a computer within a computer.

Services

Access Services

Connect to services like SaaS applications, management consoles, databases, virtual machines and other applications using the application clients hosted remotely.

### Total Visibility and Privileged Permissions Management

Saviynt's streamlined integration with Azure Active Directory provides visibility into access permissions and activities of all users, including highly privileged users and users that gain access via federated groups. It enables easy management of access permissions for various cloud and enterprise applications, with identity lifecycle automation and management. Saviynt's Cloud PAM auto-discovery of dynamic workloads provides JIT access to privileged access for consoles, workloads, and services across Azure. Sessions can be monitored in real-time and recorded. If risky access is detected these sessions can be terminated and access revoked. Risk-based access certification is enabled for Azure AD roles or groups, with Role/Rule engineering and governance for automatic discovery of hierarchical roles and rules. Organizations gain a 360° view into their cloud deployments with a single pane of glass dashboard that can graphically display all identity and access information.

### Real-Time Risk Identification and Monitoring

Saviynt's intuitive workbench enables security teams and auditors to instantly identify SoD violations and rapidly resolve them. The best-in-class mitigating controls library helps IT professionals accept or remediate risks as they are

## Overview

The rapid adoption of Microsoft Azure for Infrastructure & Application development is quickly shifting workloads and services to the cloud. And with more organizations adopting a hybrid solution, enterprises need to stay ahead of new risks. Critical assets are now more widely distributed. Sensitive data and critical infrastructure are on the cloud and outside the enterprise's traditional security perimeter. This can weaken IT administrators' ability to monitor access to key assets and detect and respond to security threats. Additionally, privileged access happens at a different scale and velocity in cloud infrastructure, creating exposure to risk never seen in premise datacenters.

Saviynt's Cloud Privileged Access Management (Cloud PAM) solution provides just-in-time access to managed privileged sessions of the Azure console, Azure workloads, tenant administration of Microsoft 365 applications, and other Azure services. Saviynt's Cloud Security Analyzer solution protects data security and privacy by using automated tools to enforce the principle of least privilege access controls for users within Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) cloud ecosystems. The Identity Governance and Administration-as-a-Service (IGAaaS) platform enables organizations using Microsoft Azure to adopt a holistic approach to identity governance and administration (IGA) when managing access to hybrid IT and ensuring control over data and activities within Azure. Saviynt features advanced analytics, data access governance, SOD management, real-time threat detection, and compliance controls to secure critical Microsoft Azure assets.

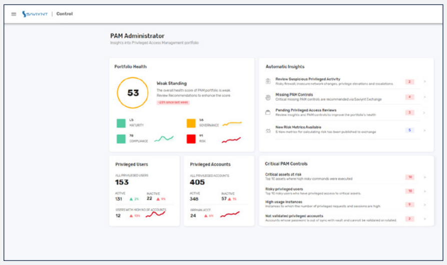
## The Business Challenge

Organizations using cloud-based services, like Microsoft Azure, face some unique challenges that did not exist when all their applications were on-premise. The expanding security perimeter is just one of these challenges.

Fragmented IT processes and siloed solutions can make it difficult to have complete visibility into complex granting or revoking of user permissions and the activities of users. Privileged access to dynamic cloud workloads is tricky because one must understand the status of workloads prior to authorizing sessions. Privileged users, like DevOps teams, require particularly stringent oversight, otherwise, they can open the organization to the greatest risk.

For example, a DevOps user with privileged access to Azure and CI/CD tools can incorrectly tag workloads, misconfigure instances, or open the wrong firewall ports or access points, leaving organizations vulnerable to security incidents and breaches. A strong cloud security posture needs to include continuous risk monitoring. But extending governance to complex cloud services and entities such as virtual networks, machines, and/or consoles can be time-consuming and burdensome to IT.

Organizations across all industries face the growing risk of data breaches. Without advanced protection within a unified framework, sensitive assets can be vulnerable and security policies difficult to enforce.



The overall health score of PAM portfolio is weak. Review Recommendations to enhance the score.

Review Suspicious Privileged Activity — Risky firewall, insecure network changes, privilege elevations and escalations — 2

Missing PAM Controls — Critical missing PAM controls are recommended via Saviynt Exchange — 4

Pending Privileged Access Reviews — Review insights and PAM controls to improve the portfolio's health — 3

New Risk Metrics Available — 5 New metrics for calculating risk has been published to exchange — 5

Critical assets at risk — Top 10 assets where high risky commands were executed — 10

Risky privileged users — Top 10 risky users who have privileged access to critical assets. — 10

High usage instances — Instances to which the number of privileged requests and sessions are high. — 9

Not validated privileged accounts — Accounts whose password is out of sync with vault and cannot be validated or rotated. — 2

identified. The solution's fine-grained SoD management controls can be automated to ensure security policies are applied continuously. Saviynt's end-to-end risk assessment supports organizations in the deployment of DevSecOps across network assets.

### Complete Cloud Security

Saviynt Cloud Security for Azure Infrastructure Services integrates with Azure AD and leading DevOps tools to help secure DevOps and cloud deployments. This prevents risky actions, such as launching workloads that violate security policies and unauthorized access escalations or role modifications. Near real-time remediation capabilities shut down risks before they cause major issues. Saviynt's Cloud Access Governance and Intelligence platform, delivered either from the Cloud or on-premises, combines intelligent IGA processes with usage and risk analytics. Enterprises can secure their DevOps CI/CD with Saviynt's near-real-time detection, prevention, and remediation capabilities.

## Learn More

Find out about Saviynt Cloud PAM – the latest addition to Saviynt's core IGA Platform

## Try a Demo

**SAVIYNT, INC.**

Headquarters
1301 E. El Segundo Bl, Suite D,
El Segundo, CA 90245
United States
+1. 310. 641. 1664
microsoftsales@saviynt.com

# The Saviynt for Microsoft Solution

Saviynt Cloud PAM for Microsoft Azure provides complete privileged access management capabilities. Included are risk-aware intelligent access request, credential and key management and vaulting, session management, session monitoring, session recording, keystroke invocation policy and keystroke logging of privileged users. This is done across the Azure console, Virtual Machines, Databases, Storage, Serverless Functions, as well as providing tenant administration over the Microsoft 365 applications and Azure AD.

Saviynt Cloud Security for the Microsoft eco-system applies continuous controls to automatically detect risks and policy violations across cloud activity, including key management, data security and DevOps policies, and network and security configurations. We use a comprehensive library of risk signatures to continuously scan Azure objects for misconfigurations, unauthorized user access and other high-risk events. Azure objects include virtual machines, roles, blobs, and resource templates. The risk signatures are mapped to industry standards including CIS Controls, SOX, FISMA, PCI, and HIPPA/HITRUST. Saviynt's platform integrates with Azure AD and leading DevOps tools like GitHub, Chef, Jenkins, and Puppet to help organizations secure all their development activities and cloud deployments.

The joint solution helps prevent risky actions, such as launching workloads that violate security policies, and unauthorized access escalation and role modifications. IT teams and executives can track and identify these threats using Saviynt's risk analytics and intelligence, empowered by the development and enforcement of security policies. Near-real time risk monitoring and identification makes it easier to remediate any violations.

## Key Solutions Benefits

### Risk Management

- 250+ risk controls to improve visibility and speed up remediation
- Integration with DevOps tools including GitHub, Chef, Jenkins, and Puppet for secure CI/CD
- Risk-based access certification for Azure AD roles and groups
- Identity lifecycle automation and management
- Full featured privileged access management including credential vaulting, session management, session monitoring and session recording.
- Integration with Microsoft Sentinel for enhanced Threat and Behavior intelligence

### Continuous Compliance

- Enforcement and management of security policies and compliance controls
- Controls for reporting mapping including CIS & NIST Controls, SOX, FISMA, PCI, and HIPAA/HITRUST
- Actionable controls with real-time prevention and remediation
- Support for multi-cloud providers and applications

### Rapid Remediation

- Near real-time workload security policy enforcement
- Powerful analytics to quickly derive risk from audit trails
- Continuous scanning of Azure objects, so risks are identified before they have a major impact
- Prioritized, real-time risk dashboards for actionable investigations

### Frictionless Experience

- Built-in IGA functionality & Federated group management to streamline access requests and reviews
- Seamless integration with Azure Security Center
- Lower-TCO cloud deployment with no compromises
- Drill-down dashboard level view of cloud security controls
- Business-ready interface accelerates implementation
- Increased ROI for cloud initiatives

### About Saviynt

Our vision is to redefine IGA by converging traditional Identity Management with Cloud Security, PAM and Application GRC capabilities. In doing this, Saviynt enables enterprises to secure applications, data and infrastructure in a single platform for cloud and enterprise.

**saviynt.com**

22May20_SaviyntCPAM_AzureInfrastructureServices_SG-v02