Saviynt

MICROSOFT + SAVIYNT JOINT SOLUTION GUIDE

Saviynt for Microsoft Teams

Comprehensive solution for identity governance

Overview

Microsoft Teams is the new standard for communication and collaboration, enabling the dynamic creation of collaborative groups. It places more power in the hands of the business user, with persistent chat, video conferencing, file storage, and integration across a wide number of applications. Such a powerful tool needs a powerful, intelligent governance solution to help ensure that the tools that allow ad-hoc teaming capabilities don't let business users expose the organization to additional risk.

Saviynt wraps automation, access request, risk visibility, and certification around the collaboration environment, enhancing security without impeding business agility or adding friction to collaboration. Saviynt's solution provides automated access based upon lifecycle management, request and approval workflows, and succession management in Microsoft Teams. The platform enables organizations using Microsoft Teams to adopt an identity-based approach to Teams governance, enabling them to control access configuration, data, and identities within Teams. Saviynt combines traditional IGA features with advanced usage analytics, data access governance, user behavior analytics, Segregation of Duties (SoD) management, real-time threat detection, and compliance controls to secure critical Microsoft Teams assets.

The Business Challenge

Managing access, configuration, and ownership of your organization's Microsoft Teams ecosystem can be challenging. User can create Teams and Channels, add members and change roles, and invite collaborators external to the organization to join a Team. This highly dynamic user population allows new flexibility in approaching business challenges, but means that a Team or a Channel may at times have members with access they no longer need, overpermissioned external users accessing private business discussions, or a Team or Channel configuration otherwise operating without appropriate security controls.

Additionally, data shared on Teams Channels or in Teams Site Collections can easily escape scrutiny. Once a Team Site Collection is created, access to uploaded data can be granted outside of the Team as well as through it. This can result in Personally Identifiable Information (PII), Payment Card Information (PCI), Personal Health Information (PHI), or Intellectual Property being inappropriately exposed, leading to reporting and compliance issues.

To combat these new risks, organizations must upgrade their control around who can create teams, how teams are configured, what rights different roles within teams have, who can upload documents, what data should be exposed to whom, and so on. Security around Microsoft Teams can be enhanced with lifecycle management, approval workflows, and succession management, and you get all that — and more — with Saviynt for Microsoft Teams.

The Saviynt Microsoft Solution

Saviynt for Microsoft Teams offers industry-leading governance across Teams, Channels, members, external users, and data in a unified, seamless solution, including:

- A single pane of glass to understand the risk posture of your Teams ecosystem, with real-time dashboards providing insight into misconfigured roles and channels, excess permissions, or anomalous external access
- Data access visibility and governance within your Teams Channels and Teams Site Collections, ensuring you know who has access to what at all times, as well as visibility into high-value and high-risk data being shared through Teams
- Automated membership provisioning based on user identity data, such as job or role, as well as access request for membership
- Deep visibility to set up segregation of duties or other controls for Teams with sensitive information

Complete Visibility Into Team Risk

Saviynt's converged identity, application access, infrastructure and privileged access solution is designed to give organizations a real-time view into risk across the ecosystem. For Microsoft Teams, this means alerting administrators to Teams configured to allow Guest users to create Channels, Teams with only Guest users, Teams with disabled owners, and other potential security risks. Saviynt surfaces these risks for administrators so they can make informed decisions to remediate each situation.

Team Member Lifecycle Management

Saviynt's real-time automation capabilities provision team members directly into teams based upon their identity, or remove them when they no longer need access, while also providing an intelligent access-request capability for users. Access certification reviews let Team owners periodically inspect of the validity of Team members. And when a Team owner departs or changes roles, Saviynt provides automated succession management to assign a new owner so no Team is ever unmanaged.

Data Discovery, Analysis and Governance

The flexibility of data sharing among Teams means that collaborators upload large numbers of documents, either to Channels or to Site Collections, with permissions to data in Site Collections assigned in many ways. Saviynt lets organizations scan Teams data stores and locate PII, PCI, intellectual property or other high value data to see who has access to it. Organizations can restrict what users can do — such as not allowing a Guest to edit files — and can restrict access to sensitive data.

Continuous Compliance for Teams

Saviynt provides out-of-the-box controls for common platforms to meet compliance mandates such as SOX, HIPAA, GDPR, and more, as well as allowing Organizations to design their own controls based on corporate security policy. Microsoft Teams becomes compliance-enabled with the Saviynt solution, ensuring Segregation of Duties (SoD) and other controls are monitored and enforced.

Key Solution Benefits

Continuous Compliance

- Holistic approach to compliance across Teams, the Microsoft ecosystem, and beyond
- Prioritized, real-time risk dashboards for actionable investigations into violations
- Compliance controls for meeting requirements such as SOX, PCI, HIPAA, GDPR, industry-specific, and more
- Fine-grained SoD management for sanctioned IaaS and SaaS providers

Data Governance

- Data discovery to locate all Teams data, wherever it resides
- Content inspection to understand data sensitivity and implement classification for access and governance
- Context-aware policies to control who can access which Teams Channels and Teams Site Collection data at what time

Risk Management

- 250+ risk controls to improve visibility and speed up remediation
- Dashboards providing visibility into risk posture of Team and Channel permissions, and an overview of anomalous Team membership, such as Teams with only guests, or inactive Team owners

Lower TCO

- Full-featured, no-compromise, lower-cost cloud deployment
- 60% quicker deployment time than traditional IGA solutions
- Painless integration with Azure AD and Azure infrastructure deployments
- Business-ready interface and intuitive end-user experience that reduces adoption friction

Next Steps

Find out why Saviynt was named a Leader in the Gartner 2019 Magic Quadrant for Identity Governance and Administration (IGA)

Try a Demo of the Saviynt IGA Program

Start a free trial of Saviynt's Enterprise Solution

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