Simplify IAM with Convergence and Automation

The plethora of Personas, Identities, corresponding accounts, and their unique sensitivity profiles demands the need for a converged and simplified IAM approach. Disparate IAM solutions are a hindrance to security posture enhancement and obstruct an organization’s ability to maximize the “signals” and “states” of Identities and accounts to drive effective security actions.

Inspira’s vision with its “I-AM Digital” solution is to empower organizations with a simplified IAM approach through “Convergence and Automation” while being a catalyst for digitalization in alignment with your organization’s security and business imperatives. This solution provides a comprehensive and seamless approach to managing identity and its access across an organization’s landscape of systems and applications. Inspira can facilitate the organization to achieve high-fidelity interoperability between the two systems, Saviynt and Microsoft Entra.

Inspira’s “iSMART2 (Intelligent | Simplified | Measurable | Adaptive | Risk | Threat Centric | Tailored) I-AM Digital” platform is powered by leading solution providers Saviynt and Microsoft which enables organizations to benefit from the true power of the converged IAM solution bringing in enhanced efficiency, improved security, maximized return on investments, enhanced user experience and elevated cybersecurity posture.

Achieve IAM Convergence with Inspira’s I-AM Digital

Converged IAM solutions provide organizations with a comprehensive and integrated approach to managing identities and access, which helps improve security, increase efficiency, and enhance the user experience. Inspira’s converged platform provides a structured approach to deliver the desired outcome for the seamless integration of disparate IAM technologies. Inspira’s I-AM Digital framework and accelerators can be leveraged to help you achieve your Organization’s IAM convergence goals.

The solution converges Saviynt and Microsoft Entra suite. The individual features leveraged from each solution are below:

- **Enhanced User Experience**
- **Reduced TCO with Increased Operational Efficiency and ROI**
- **Visibility across the Identity platforms**
- **Elevate security posture**
- **Enhanced Threat protection with reduced mean time to respond**
• Azure Identity Protection (AIP) generates the signals based on the user's activity in the organization.
• Saviynt EIC consumes the signals triggered from AIP and takes preventive action to protect the organization by managing user access to applications, data, and other IT resources. It further sends the logs and user information to the SIEM solution for advanced investigation and monitoring.
• Microsoft Sentinel, a cloud-native security information and event management (SIEM) system, helps analyze and respond to security threats in real-time and coordinates with the respective source for closed-loop remediation.

This package solution will provide a single pane of glass that brings all IAM technologies deployed in the enterprise under one interface using advanced API and integration methods. The customer can access this solution via Azure Marketplace, Saviynt Exchange, and Inspira's website.