Saviynt

SOLUTION GUIDE

External Identity & Risk Management

Secure your extended enterprise without slowing business down

Despite the widespread use of third-party contractors, vendors, seasonal workers, and agencies, most organizations don't understand the scope of the external security risks in their supply chain and/or extended external workforce.

Saviynt is built to protect everywhere people work. External access control makes it easy for employees, contractors, and partners to access the applications, systems, and data they need from day one with the #1 converged identity platform.

Better Collaboration. More Control.

Simplify identity security for your complete business ecosystem and enable the internal and external relationships your business needs to thrive. Saviynt's #1 Identity Cloud enables you to power and protect the entire business relationship lifecycle from relationship kickoff to the final sign-off.

Despite the widespread use of third-party contractors, vendors, seasonal workers, and agencies, most organizations don't understand the scope of the external security risks across their identity access landscape. A lack of purpose-built non-employee identity tools and decentralized management processes contribute to this lack of visibility.

Third party individuals often require access to organizational resources such as shared tools, applications, and to provide critical services. Managing these non-employees through the HR system, the authoritative identity source for their IT ecosystem, is burdensome for HR and IT teams. Third parties bring additional risks, so ensuring that access is properly managed is critically important.

Build More Trust in Your Business Relationships

Saviynt External Identity & Risk Management offers industry leading identity management and governance throughout the engagement lifecycle. The Saviynt Identity Cloud is a central, trusted repository for all internal and external users. Eliminate disparate, non-purpose built tools and onboard vendors with a consistent, reliable process and develop a secure identity framework to create risk-based access for each external entity.

- Protect everywhere people work
- Secure third party access at scale
- Enforce least privileged access
- Simplify identity lifecycle management and enable continuous compliance
- Protect all human and machine identities with a single platform

Take the Burden off HR with Delegated Administration

Assign delegated administrators to manage access within their organization, allowing the vendor or partner organization to manage their users. Offload manual tasks from your HR and IAM teams and manage the relationships through access reviews, certifications and risk-based reporting.

Enable Right-Time, Right-Level External Access

Ensure a seamless day one experience by providing external workers and contractors with the access they need to get off to a great start. Say goodbye to management-by-spreadsheet and inefficient email-based workflows. Securely collect third-party non-employee data collaboratively with internal and external sources throughout the relationship, while meaningfully reducing the burden on your IAM team. Maintain access and ensure the access is appropriate for the person for the time it's needed.

Automate External Identity Lifecycle Management

Saviynt makes it easy for business managers, application owners, role owners and others to make informed decisions about access certifications.

Maintain continuous collaboration with internal and external stakeholders to ensure access is appropriate throughout engagement. Kickoff recertification campaigns through Saviynt's Identity Cloud for maximum control and trust. Ensure continuous compliance with complete audit trails and dashboards.

Close Out Projects With Confidence

Orphaned identities – access that persists when it's no longer needed – poses a large risk for organizations. It can lead to failed audits, wasted licenses and can leave the door open to a cyber breach. Saviynt Identity Cloud supports the ability for the appropriate internal or external stakeholder to update the identity directly, which automatically deprovisions access in a timely, efficient manner. By ensuring timely removal of this access, the risk of a third party breach is mitigated and critical data and systems are more secure.

Frictionless Access

- Just Enough Access (JEA)
- Access from Anywhere (mobile, browser, Teams, etc.)
- Automated Request Recommendations
- Policy Violation and SoD Conflict Detection
- API-based integration

Streamlined Approvals

- Automatic Non-Critical Access Approvals
- Risk insights
- In-Line Collaboration
- Escalation and Delegation for internal and external identities

Governance Automation and Management

- Ownership and Succession
- SoD Management
- AD and Service Account Management
- Third-Party Access Governance
- External Delegated Sponsorship
- Continuous Monitoring

Certification & Compliance

- Business Process Workflows
- Intelligent Certification Campaigns
- Continuous Micro-Certifications
- Application, Entitlement Owner, Service Account, and Role Owner Certification
- Consolidated Reporting for Streamlined Audits

Next Steps

Visit our website

Request a demo of Saviynt External Identity & Risk Management

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