[Joint Solution Brief]

Dynamic Duo Cracks the Code on Third-Party Risk

SDG and Saviynt Joint Solution Solves Third-Party Identity, Access, and Risk Challenges

OVERVIEW

Enterprise-level third-party risk management is a critical security priority for organizations that rely on third-party suppliers, vendors, contractors, and even nonhumans to succeed. This reliance, combined with the growing number of bad actors and cyber-attacks, means organizations must be diligent when provisioning access to their systems and data to hundreds—sometimes even tens of thousands—of external users.

To mitigate the risk of compromised sensitive and valuable data, organizations are working swiftly to deploy third-party identity and risk management solutions and data security best practices, including restricting access to the right people at the right time for the right reason as a safeguard.

CHALLENGES

The access requirements for external users are often similar to those of internal employees, but the processes to secure this access can be exponentially more difficult. Access decisions and processes can be decentralized across multiple applications with multiple internal stakeholders, making it difficult to monitor this access securely and consistently. The potential gaps can open the door to risks, such as:

- **Unauthorized Access:** Without proper access controls, the third party could gain unauthorized access to sensitive data.
- **Data Breaches:** Granting third-party access to internal systems and data increases the potential for a data breach.
- **Insider Threats:** Access to sensitive data may inadvertently or intentionally be misused by a third party.
- **Compliance and Regulatory Violations**: Failure by the third party to meet compliance and regulatory requirements could subject the organization to legal and financial repercussions.

Other issues that can threaten the security of an organization's data include overprovisioning access to third parties and the risk of unauthorized access by former employees whose access was never revoked. Effectively mitigating risks associated with third-party data access requires robust identity authentication processes and authorization mechanisms, ongoing monitoring, and strict adherence to data privacy laws.

SOLUTIONS

Controlling Identity Risk Without Compromising Productivity

The Identity Cloud, Saviynt's enterprise-ready converged identity platform is built to protect organizations wherever its employees or partners work, including third-party contractors, vendors, seasonal workers, and agencies. External access control makes it easy and secure for an organization's employees, contractors, and partners to access the applications, systems, and data they need from day one.

With Saviynt, organizations can set the stage for success with:

- Tailored third-party access invitation processes establish risk-based policies and end dates.
- A seamless external user experience that ensures access to what they need to do the job from day one.
- Policy-based, third-party access lifecycle management workflows for improved productivity and enhanced security.
- Certification campaigns that effectively remove personal data from less secure inboxes.
- An intuitive, user-friendly identity platform that empowers internal sponsors to act and provides relief to internal IAM teams.
- A reliable access review process with policy-based access revocation.

Saviynt's External Identity & Risk Management solution provides industry-leading identity management and governance throughout the identity engagement lifecycle. Collect third-party non-employee data collaboratively with internal and external sources and onboard third-party vendors quicker with a consistent, reliable process in a secure identity framework. Assess a vendor's risk before onboarding. **Additional key benefits include:**

- **Identity Verification and Authentication:** The software offers advanced identity verification and authentication mechanisms to ensure that only authorized individuals gain access to sensitive data.
- **Access Control Policies:** Enable organizations to define granular access control policies based on roles, responsibilities, and contextual factors. This ensures access to sensitive information is restricted to individuals with the appropriate clearance and authorization.
- **Monitoring and Alerts:** Triggers immediate alerts, allowing administrators to take proactive measures to mitigate potential risks and security threats when suspicious or anomalous behavior is detected.
- **Privileged Access Management (PAM):** Prevents unauthorized access and credential misuse utilizing just-in-time access provisioning, session monitoring, and automated password rotation.
- **Risk Score Dashboard:** This dashboard provides visibility into third-party identity and automates risk management scoring to determine appropriate levels of access.
- **Integration with IoT Devices:** Integrates with IoT devices to extend identity and access management policies to IoT endpoints.

SDG's Unparalleled Approach to Third-Party Risk

SDG has over 30 years of experience supporting some of the world's largest brands through a mix of actionable strategic advice, expert systems integration, and smart managed services. Our comprehensive understanding of identity and access management, including extensive knowledge of third-party risk management and technologies, brings thought leadership, a passion for customer success, and a keen eye on risk management to the table every time.

The SDG team is composed of highly qualified cybersecurity, IGA, and Saviynt-certified professionals who are committed to securing data, streamlining identity and access management controls for internal, external, and third parties, and reducing an organizations risk of a breach.

SDG's Delivery Maximizes Business Value Through:

ANALYSIS: SDG starts by thoroughly analyzing an organization's current environment and works to fully grasp the business value expected from Saviynt's solution. With this detailed understanding, SDG creates a clear business case and collaborates with Saviynt and the organization to establish priorities, define scope, and set timelines.

INTEGRATION: This stage involves implementation. SDG adheres to a disciplined DevOps process. Playbooks are written, staff are trained, systems are tested, and end users are informed of the changes to come. This stage is agile, and priority follows a line that delivers the target business value quickly and repeatedly.

DEPLOYMENT: As components of the integration progress, SDG conducts user acceptance testing (UAT), exercises migration plans, and invokes organizational change management tasks. Having defined metrics for success that align with Saviynt and the organization's objectives, those metrics are now tracked to ensure the value is being realized.

CONTINUOUS MONITORING AND RESPONSE: SDG offers continuous monitoring of third-party activities and can promptly address potential threats and vulnerabilities. This proactive approach ensures that risks are identified and mitigated before they can impact an organization.

REGULATORY COMPLIANCE: Always up-to-date on the latest regulations and standards, SDG is able to provide comprehensive support to organizations needing to remain compliant with industry-specific requirements to avoid potential legal and financial repercussions.

SDG's vast knowledge of Saviynt's Identity Cloud platform, superior approach to integration, and decades of expertise in real-time monitoring and response significantly reduce an organization's risk of unauthorized access and data breaches.

CONCLUSION

Saviynt's robust third-party access management solution, designed to power and protect your extended enterprise, combined with SDG's unwavering commitment to process excellence, seamless integration, and measurable results, forms a powerful partnership. This dynamic duo is uniquely equipped to tackle any organization's most complex third-party identity, access, and risk management challenges, ensuring enhanced security and peace of mind.

ABOUT SDG: With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

Contact Us: solutions@sdgc.com

SDG
75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com