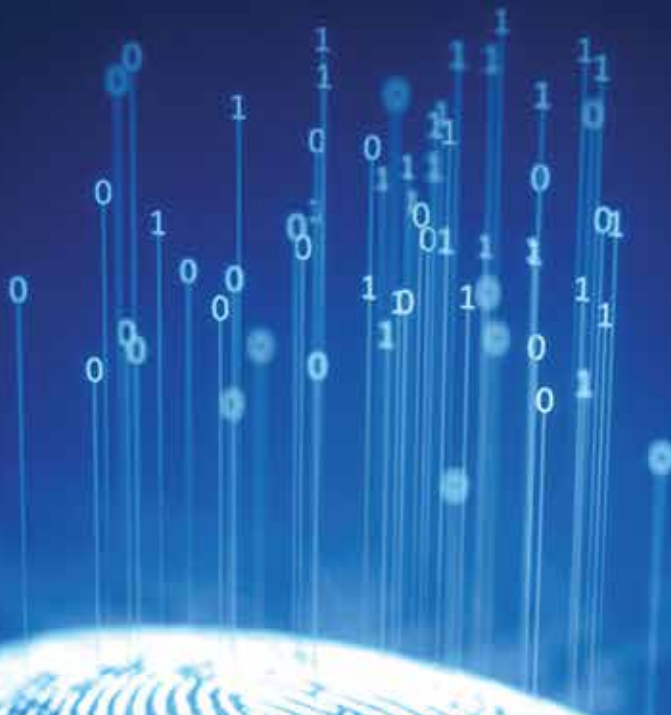


WHITE PAPER

IDENTITY GOVERNANCE AND ADMINISTRATION

Enabling Digital Transformation with Identity 3.0



CONTENTS

page 03 **WHY MODERNIZE YOUR IGA SOLUTION?**

page 04 **DIGITALIZATION & SECURITY**

- Legacy Systems Fail at IAM in the Cloud
- DevOp Security and Access Management in the Cloud
- Internet of Things (IoT) Increases Access Risk
- Increased Compliance Mandates Double Down Burdens
 - ◆ General Data Protection Regulation (GDPR): Data Protection by Design and Default
 - ◆ New York Department of Financial Services (NY DFS) Cybersecurity Rule
 - ◆ California Consumer Privacy Act (CCPA)

page 08 **BEST PRACTICES FOR CLOUD MIGRATION IN AN EVOLVING THREAT LANDSCAPE**

- Ensure Least Privilege Necessary
- Implement Role-Based or Attribute-Based Access Controls
- Maintain Segregation of Duties (SOD) Across the Ecosystem
- Comply with Vendor Risk Management Programs
- Continuously Monitor User Access
- Continuously Document Remediation and Response

page 09 **DEPLOY AUTOMATION TO EASE BURDENS**

- Understand the Capabilities
- Understand the Alerts
- Understand the Control Alignments
- Understand the Technology
- Understand the Security Controls

page 10 **IDENTITY 3.0 FOCUSED ON SECURITY BY DESIGN**

- Intelligent Risk Analysis
- Intelligent Compliance
- Intelligent and Intuitive Dashboards
- Intelligent Elasticity
- Intelligent Configuration and Deployment
- Intelligent Identity. Smarter Security

WHY MODERNIZE YOUR IGA SOLUTION?

Embracing digitalization positions enterprises for future growth, customer retention and improved operations. **However, modernizing the organization's business processes creates data security issues as new cloud enablements increase data access points, users, and privileged accounts.** Meeting modern needs requires modern Identity Governance and Administration solutions which not only enable cloud, hybrid, and on premises security but provide a secure solution.

Moreover, with data breaches increasing in severity and number, governments and industry organizations continue to change compliance requirements to force companies to provide documentation over their cybersecurity program governance. Continuous monitoring over internal information security controls as well as third-party business partners, including applications and cloud ERP solutions, also acts as a barrier to IT modernization.

A comprehensive Identity Governance and Administration (IGA) solution that can accelerate and enable cloud migration should:

- Meet customer expectations with a secure, cloud-based solution
- Effectively monitor the digital threat landscape to mitigate cybersecurity risk
- Ensure financial, reputation, and operations risk mitigation
- Meet regulatory and industry compliance requirements governing data privacy and security
- Evaluate & protect:
 - ◆ Access to sensitive customer data
 - ◆ Financial data & transactional processes

Digital transformation relies on the elasticity, power and convenience of cloud computing. **Companies need an IGA solution that enables cloud and on premises operations.** Although Cloud Services Providers (CSPs) work to protect their networks, systems, and software from cybercriminals by securing their perimeters, organizations also need to take control of the data they collect, store and transmit. Focusing on external monitoring such as IP address and network security only addresses one part of the problem with cloud and hybrid IT environments.

To create a holistic, risk-based approach to data security in the cloud, organizations need to incorporate data access and user privilege. Information security controls need to also address:



1. *However, modernizing the organization's business processes creates data security issues as new cloud enablements increase data access points, users, and privileged accounts.*
2. *Companies need an IGA solution that enables cloud and on premises operations.*

DIGITALIZATION & SECURITY

Digitalization requires organizations to adopt a new business model. Instead of only adding new people to the organization, they add new applications to their IT environment and new channels to their communication models, all aggregated in a single location. This results in a dramatic increase in internal and external identities. As such, traditional methods of storing all identities in an on-premises directory, no longer provide appropriate flexibility for or security over the cloud or hybrid environment. Organizations need to review the risks inherent in cloud migration and access control over these environments, particularly in terms of employees, contractors, vendors, affiliates and customers/constituents. Thus, to create effective risk-based access and identity management programs they need review the risks each identity poses by asking:

- Who has access to critical company applications (legacy & cloud)?
- What risk does that access present to the organization?
- Why did they receive the access & is it appropriate?
- Is there an audit trail of the request & review process?
- How is the access being used, in terms of business risk?

Single-sign-on (SSO) solutions focus on the who and what of identity. Using SSO, organizations can authenticate one identity across a variety of domains. However, SSO does not respond to the important questions of why and how users gained access to information. More critically, they don't focus on why or how privileged access accounts were approved. And most implementations are tied back to an authorization model within Active Directory groups. We all know how that story goes.

Thus, many organizations struggle with the need to manage a multiplicity of applications that control identity, manage identity, and authorize users. Often, these solutions and applications do not integrate with one another, and the identity and access management program fails to secure information because the lack of overlap and visibility lead to gaps.

For example, most CSPs offer a built-in IAM solution. Most Cloud ERP vendors (SAP, Oracle, Salesforce) offer a proprietary IAM, as does Microsoft with AzureAD. Some desktop applications use Lightweight Directory Access Protocols while web-based applications often use Security Assertion Markup Language (SAML) or Open Authentication (OAuth). Research by Ping noted that 90% of survey respondents agree that IAM matters to modernizing their IT environments and that 89% see IAM as a value-add to their customer experience and engagement. Moreover, the research also noted that SSO, multi-factor authentication and secure access in customer identity remains low, with 43% adopting SSO, 40% adopting MFA, and 48% adopting secure access. Finally, 85% of respondents believed IAM solutions are critical to managing supply chain partnerships. In short, organizations recognize the importance of IAM, but by not adopting these strategies they reduce customer engagement and drive down customer retention.

Legacy Systems Fail at IAM in the Cloud

Even more challenging, many organizations seek to incorporate their legacy systems into their modernization projects. Unfortunately, data security for these systems traditionally focuses on perimeter defenses that no longer fully secure data as companies add more applications and access.

For example, the 2018 Verizon Data Breach Investigations Report (DBIR) noted that stolen credential accounted for 399 data breaches, making it the top data breach variety. Additionally, the DBIR also noted that the top data breach internal actors were system administrators, account for over 20% of the internal data breach activities. Finally, databases (servers), POS terminals (user devices), POS controllers (servers), and web applications were the top four assets implicated.

Since legacy systems focus defending against external infiltration via insecure networks, they fail to protect against internal actors or stolen credentials. To expand beyond the basic user provisioning of legacy IGA and IdM systems, enterprises need to secure data, infrastructure, supply chain management, cloud-based Privileged Access Management (Cloud PAM), and server/container-based solutions.

The inherent ability to assess these dynamic controls is a baseline: as each compliance frameworks evolves, the rigid, one-to-one mapping of legacy systems fail. Thus, as organizations modernize their IT environments, they need to better control identity and access to secure the personally identifiable, nonpublic information that they store, transmit, and collect.

DevOp Security and Access Management in the Cloud

Many organizations migrate their DevOps processes to the cloud to ensure **Continuous Integration (CI) and Continuous Deployment (CD) required to meet Agile development methods**. DevOps teams that seek to support SDLC at the speed and quality of customer demand turn to automation.

Traditional workflows and processes no longer protect data, so organizations seeking to use agile development strategies need to focus more on access policy management, SOD and privilege changes. Enforcing SOD focuses on ensuring that developers only write code, operators maintain application availability, and security staff grants permissions at developers' request.

An often overlooked challenge for DevOps Security teams during the cloud migration process is storage of application code. When teams store their application security code to their cloud, cybercriminals can more easily access the data, ultimately undermining the security model.

continues

Finally, as DevOps teams test their code in runtime environments, they often need to escalate privileged access. Unfortunately, as part of this process, they may neglect to create timebound access rules. Thus, data exported during testing, which may incorporate personally identifiable information or other sensitive data, may be at risk for unauthorized access.

Maintaining Secure Development Life Cycle (SDLC) throughout the CI/CD process requires organizations to maintain compliance with internal controls as well as external industry standard and regulatory requirements governing access identity and management.

Application code storage and runtime environments require new strategies for managing access to secure DevOps for cloud migration.

Internet of Things (IoT) Increases Access Risk

Workforce members and customers increasingly access organizations using mobile devices. Whether on smartphones or tablets, these remote access vectors also lead to data security issues. SSO solutions fail at securing IoT devices since many do not require passwords, choosing to instead employ biometrics or behavioral authentications via APIs.

Thus, while SSO provides password and authentication solutions, it does not control for identities as they move across IoT and cloud environments. Integrating IoT requires visibility into identities, the APIs and relationships because devices must be identified in multiple domains. In 2015, the Cloud Security Alliance IoT Working Group suggested an initial series of best practices for managing IoT Identity and Access Management. Despite the paper's age, it remains relevant even in a continuously evolving threat environment.

- Implement restrictive logic in their identity management workflows to proactively restrict access
- Implement a privileged user management system that enables session monitoring
- Establish relationship mapping between people and devices to enforce individuals' authorized behaviors on specific data sets

Increased Compliance Mandates Double Down Burdens

In response to the increased number and complexity of data breaches, regulatory and industry standard requirements continue to evolve. These requirements place an even greater burden on organizations since cloud migration and IoT enablements make documenting security controls difficult. Organizations need to incorporate Governance, Risk and Compliance (GRC) in a way that integrates critical business operations and identity access management.

However, support for GRC within these critical applications are often also siloed. Internal audit teams continue to struggle with the reconciliation of account access in SAP, Oracle, Info, Peoplesoft, Epic and other ERP & EMR solutions with the identity of the employee, contractor, vendor or customer. Legacy IGA solutions provisioning just enough access to these critical applications and leave the heavy lifting to GRC solutions, resulting in manual process to check for SOD violation and fulfill the access needs.

General Data Protection Regulation (GDPR): Data Protection by Design and Default

The GDPR's strict controls require organizations to enforce user access. Specifically, Article 25 states:

“...such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons ”

Thus, to meet GDPR objectives under article 24, data controllers need to ensure that they not only limit access from external actors but also internal actors. Data access is paramount to maintaining GDPR compliance.

New York Department of Financial Services (NY DFS) Cybersecurity Rule

Enforcement of NY DFS Cybersecurity Rule begins in 2019. As covered entities seek to meet the stringent cybersecurity program requirements, they need to focus on access controls and identity management. Under Section 500.07, the Rule specifies:

“ As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges. ”

Unfortunately, for organizations migrating to the cloud, the NY DFS requirement of multifactor authentication under Section 500.12 only meets part of the user access requirements in Section 500.07.

California Consumer Privacy Act (CCPA)

Similar to the GDPR, the CCPA focuses on privacy as paramount, although it embeds security concepts within it. In the preamble, the CCPA states,

“ The bill would provide for its enforcement by the Attorney General, as specified, and would provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's non-encrypted or non-redacted personal information, as defined. The bill would prescribe a method for distribution of proceeds of Attorney General actions. ”

In addition, the CCPA also requires companies that collect information to verify customer identity in response to customer requests protected under the act.

This list of regulations is not exhaustive, but all have similar provisions which make it obvious that organizations need identity access and governance solutions that manage internally and externally facing cloud applications to meet privacy compliance requirements.

BEST PRACTICES FOR CLOUD MIGRATION IN AN EVOLVING THREAT LANDSCAPE

IT modernization requires organizations to create a dual-focused cybersecurity program -one incorporating external infiltration and internal access risks. Organizations seeking to create a proactive rather than reactive approach to cybersecurity need to look not only at the network security issues such as Distributed Denial of Service (DDoS) and common vulnerability exploits, but they also need solutions that support access and identity.

Legacy Systems Fail at IAM in the Cloud

The first step to securing data is limiting access. Unfortunately, cloud migration creates least privilege access challenges. As companies adopt new applications in their cloud environments, they add new users. Those new users often need greater access than traditional roles if they manage activities such as security software updates. Therefore, organizations struggle to maintain least privilege necessary throughout their cloud ecosystem which leaves privileged access accounts at risk.

To compound the problem, many times a system administrator will need to appoint several business administrators to manage particular populations. These “tenant administrators” are privileged accounts in and of themselves, and need to be parceled out in a governed fashion.

Implement Role-Based or Attribute-Based Access Controls

Role-Based Access Controls (RBAC) and Attribute-Based Access Controls (ABAC) focus on users, their relationship to the organization and their need for data. RBAC starts by associating employee roles to a set of privileges. ABAC focuses on a set of values including role, project, and data sensitivity. ABAC also focuses on relationships between and among users, data access locations, and context. RBAC and ABAC create challenges as part of cloud migrations because of the disconnect between legacy and cloud environments.

Maintain Segregation of Duties (SOD) Across the Ecosystem

Increased Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) use to enable business operations can decrease visibility into data access. Maintaining compliance with internal controls to prevent fraud requires ensuring “cross-application” SOD across the connected ecosystem, whether in the cloud or on-premises as organizations run hybrid environments.

Comply with Vendor Risk Management Programs

SaaS, IaaS, and PaaS not only create internal control risks, but they can also lead to external access control risks. To maintain compliance with vendor risk mitigation strategies, organizations that migrate to the cloud need to consider several aspects of Vendor Management: the complexity of contractors supplied by partner organizations, data sovereignty, data retention and vendor access and activity.

Continuously Monitor User Access

Whether arising from external or internal malicious actors, data access governance requires continuous monitoring to protect data integrity, accessibility, and confidentiality. Stolen credentials arising from a malware or ransomware attack can lead to unauthorized access. Meanwhile, employees can either accidentally or maliciously use their access to undermine data security and privacy protections. Traditional access reviews act as a point-in-time assurance over access controls. However, as cybercriminals evolve their methodologies, organizations need to evolve their monitoring controls. Continuous monitoring automations that enable real-time, or near-real-time, insight into user behavior give organizations stronger visibility into how and when users access data.

Continuously Document Remediation and Response

Traditional point-in-time documentation no longer protect organizations from fines and penalties. Organizations need to react rapidly to mitigate the effects that data events can have on their financial, reputational, and operational bottom lines. Moreover, as organizations migrate to the cloud, they need to provide documentation proving governance over their data security programs.

DEPLOY AUTOMATION TO EASE BURDENS

The 2018 Ponemon Data Breach Investigations Report noted that deploying an automated security solution saved \$8 per compromised record. Automated solutions enabled organizations to increase visibility into their environments and ecosystems. The report defined automation as “technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches.”

However, only 15% of the 477 companies surveyed reported full deployment. Meanwhile, 34% of the companies reported partial deployment. 38% of companies reported that although they had not deployed automation at the time, they planned to do so within the next 24 months.

For organizations seeking to reap the benefits of modernization while attempting to mitigate the risks, automation needs to be incorporated as part of their cloud strategy. However, not all automation is equal, which means that companies need to purposefully and thoughtfully seek out solutions that meet their individualized needs or they will end up as another incomplete deployment..

Understand the Capabilities

Identity and access management in the cloud often becomes obfuscated by “shadow IT.” Cloud migration increases the number of applications connected to an organization’s IT infrastructure. These applications request access to systems, software, networks and devices, yet the company’s IT department does not control the approvals. Employees using SaaS based enablements such as Dropbox or Office 365 can approve the access without the IT department realizing it. Organizations seeking to deploy automated systems need to ensure that the solution chosen can secure and monitor this access risk.

Understand the Alerts

Every automated solution provides alerts. However, some solutions tout themselves as real-time monitoring when, in fact, they simply act as a database. To enable stronger data privacy and security, organizations need to understand the types of alerts the platform sends, how it determines an alert should be sent, and the data it uses to send the alerts.

Understand the Control Alignments

Different industry sectors need to meet different compliance requirements. An automated solution may offer a “controls library,” but if it does not incorporate a cybersecurity framework that the company’s industry requires, the solution may be useless.

Understand the Technology

Automation comes in a variety of forms. Some automated solutions act as single-source-of-information databases. Some solutions provide analytics that aggregate information available from public sources. Some solutions incorporate internal facing analytics to help the organization focus on its own specific risks.

Understand the Security Controls

Every automated solution is another SaaS, IaaS, or PaaS provider. They inherently come with the same information security risks. Therefore, organizations need to be aware that their security enablement can be a security risk. As such, before deploying the automated solutions, organizations need to engage in third-party risk mitigation reviews to ensure their automated solution is not a data breach risks.

IDENTITY 3.0 FOCUSED ON SECURITY BY DESIGN

We are entering the next generation of IGA maturity and capabilities, the advent of Identity 3.0. Innovation and modernization in the identity space can now enable organizations to secure critical applications, data and infrastructure across cloud, hybrid, and on premises, creating a streamlined, cost-effective solution. Companies need next-generation, innovative solutions that use intelligence to ease continuous monitoring and documentation burdens so that organizations can modernize their architecture and meet cloud migration Best Practices.

With the capabilities provided by modern elasticity, compute power and analytics, Identity 3.0 goes beyond legacy identity management solutions and applies intelligence to every aspect of identity governance and administration.

continues

Intelligent Risk Analysis

Intelligent risk analysis means using access and usage analytics with individual user activity and inherent risk to develop a full portrait of a user's risk profile. Companies need to be able to leverage risk profiles to align data and user access with their cybersecurity program risk tolerance levels.

By analyzing user activity with filters such as type, role, permissions, data accessed and functionality performed, IT departments gain visibility into interactions with customer data, i.e., who's accessing which systems at what time, and why.

Identity 3.0's capabilities must extend even further, though. Integrating user and entity behavior analytics (UEBA) to enhance understanding creates a mature, enriched dynamic risk model. Companies can have deep visibility into not only what access does a user have, but are they using it correctly. This active risk intelligence helps organizations see threats as they are evolving, in real-time rather than in forensic logs after the fact

With a solution that uses intelligent access analytics, companies can surface suspicious user activities requiring immediate response and mitigation. Automated risk calculations help comply with internal controls, mitigate SOD violation risk, and meet industry standards and regulatory compliance continuous monitoring requirements.

Intelligent Compliance

Identity 3.0 defines and implements controls to maintain continuous compliance for organizations. To move from compliance to intelligent compliance, companies need solutions that provide out-of-box controls aligned with compliance requirements, including but not limited to SOX, PCI, NIST and HIPAA/HITRUST.

However, companies also need to find solutions that map across industry domains and applications, so the identity platform has to be able to incorporate the vast number of published security controls, including SAP, to accelerate control mapping to specific platforms and regulatory frameworks. Additionally, organizations need the ability to create custom configurations which allow them to retain control over critical applications, as per individual organizational requirements. Identity 3.0 must deliver this architecture and framework.

Intelligent and Intuitive Dashboards

Effective governance requires ease-of-use for IT administrators and business managers. Identity 3.0 must include holistic dashboards that incorporate business-related metrics and rich visibility to enable stakeholder collaboration and governance. Actionable dashboards provide simple drill-down into the presented information to deliver user-friendly interactions for IT and business administrators.

Intelligent Elasticity

Identity 3.0 solutions must adapt to changes in the organization, reducing the administrative burden on managers who control requests, approvals and maintenance of all types of accounts. Thus, as the organization scales, the chosen automation should enable the organization to maintain enforcement over policies and procedures as required by industry standards and regulatory compliance requirements.

Intelligent Configuration and Deployment

An intelligent IGA must quickly capture and model requirements, providing a rapid deployment with minimal workflow impact. Rather than months, a streamlined implementation of an Identity 3.0 solution should only take weeks and should include prebuilt enterprise application integrations for rapidly on-boarding identities at cloud scale.

Intelligent Identity. Smarter Security.

Despite a market flooded with identity governance vendors, Saviynt's cloud-born Identity Governance and Administration platform is driving innovation in the industry as we deliver new, visionary capabilities with Identity 3.0. For organizations looking to ease the transition and mitigate risk when moving from on-premises to the cloud, our intelligent identity capabilities make your security smarter and enable you to achieve modernization and digitalization.

LEARN MORE

FIND OUT!

Why Saviynt received the highest product score for Midsize or Large Enterprise and Governance-Focused use cases in Gartner's 2018 Critical Capabilities for Identity Governance and Administration.

CONTACT US

info@saviynt.com

START A FREE TRIAL

Saviynt's Enterprise Solution

TRY A DEMO

Saviynt IGA Platform

About SAVIYNT

Saviynt is a leading provider of next generation **Identity Governance and Administration solution for Data, Infrastructure and Critical Applications in the Cloud and Enterprise**. Saviynt combines traditional IGA features with advanced usage analytics, data or infrastructure access governance, behavior analytics, real-time threat detection and compliance controls to secure organization's critical assets.