Saviynt

Modern IGA for Mid-Sized Organizations

Saviynt IGA delivers enterprise functionality with lower costs, reduced risks, and happier users.

Contents

Introduction

When big companies suffer a data breach, they make big headlines. So it might seem logical that mid-sized companies aren't attractive prey to cybercriminals. But in fact, ransomware targeted mid-sized companies with a vengeance in 2021, with **79% of IT teams** seeing an increase in rebuild rates, indicating that hackers are becoming more successful at infiltrating the endpoint.

Today, smaller companies are fending off bad actors as frequently as their enterprise counterparts. Last year, **46% of all cyber breaches** impacted businesses with fewer than 1,000 employees, and 61% of SMBs were the direct target of malicious activity.

To keep their systems secure from unauthorized access (or to limit the damage done if a user becomes compromised, negligent, or malicious), mid-sized companies need to double down on access reviews and **least privilege** protocols. But with the demands of onboarding and offboarding, constantly evolving regulations, and the emerging quagmire of third-party governance, IT teams are working harder than ever to scale — and nearly **half** believe their processes are ineffective.

Identity Governance and Administration (IGA) solutions and strategies differ greatly based on budget, size of your IT team, and overall risk profile. It can be overwhelming to wade through the pros and cons while trying to assess the cost of replacement, the unknowns of data migration, and the costs of retraining staff.

In this white paper, we'll explore common pain points and barriers to IGA modernization for mid-sized businesses, how a modern cloud-based IGA solution closes the gaps other solutions leave open, and the keys to maintaining a secure, compliant, and scalable identity management process.

Identity Governance:
Mid-sized Business, Supersized Pain

With smaller budgets and staff employed to tackle **rising threats**, mid-sized organizations take on a lot of headwind trying to manage and maintain an effective IAM program, especially when dealing with multiple platforms and systems. Do any of these sound familiar?

1. On-or Off-Boarding Employees Manually
2. Chasing Down User Access Reviews
3. Third-Party Sprawl
4. Audit Findings or Compliance Challenges
5. Human Error
6. Lack of Integration
7. Lack of Resources

1 On-or Off-Boarding Employees Manually

Whether your company is preparing to lay off 30% of its workforce — or grow by 300% — manual processes, broken tools, and spreadsheets can't successfully navigate these huge transitions. You need a solution that can automate and scale with your joiners, movers, and leavers (JMLs) and prevent orphaned accounts that might retain access to payroll systems and Concur. Even if just one employee leaves the company, that system should automatically revoke access and prevent unauthorized access to sensitive data.

2 Chasing Down User Access Reviews

If you're a financial services company, government and industry regulators demand stringent access control systems — and will enforce steep penalties if you fail to provide them. And of course, it only takes one breach or bad audit to permanently damage your reputation.

Whether your company is preparing to lay off 30% of its workforce — or grow by 300% — manual processes, broken tools, and spreadsheets can't successfully navigate these huge transitions.

User access reviews are a critical line of defense for financial institutions. They help you ensure compliance, reveal unauthorized access attempts or unusual user behavior, and identify potential weaknesses in your access control system. But if all this critical data lives on spreadsheets, then you probably have full-time employees working after hours and on weekends just trying to collect user access reviews.

3 Third-Party Sprawl

Let's say you're a manufacturing company with a large team of warehouse employees who only log into one or two applications. But you also rely on hundreds of knowledge workers, distributors, and suppliers (both vertical and horizontal) who need access to sensitive systems to do their job.

These third-party relationships are increasingly on auditors' radar, requiring companies to not only enforce their internal policies and procedures, but to also ensure that every vendor in their complex supply chain is compliant and up to date on any required certifications and training — not to mention environmental, ethical, health, and safety regulations.

This necessitates careful, time-consuming management of contracts and Service-Level Agreements, negotiating and agreeing on terms and conditions, as well as monitoring compliance with contractual obligations, such as delivery times and quality standards. All this while still ensuring that only authorized individuals have access to sensitive data.

4 Audit Findings or Compliance Challenges

Perhaps your company has suffered a breach due to compromised credentials or unauthorized access. Or, maybe you're lucky enough to have caught **Separation of Duty (SOD)** violations in a compliance audit. Either way, undetected threats are slipping past your access controls and putting your reputation and financial stability at risk.

But with so many employees, third-party vendors, and customers accessing your systems, it's challenging to maintain effective access controls and to verify that only the right individuals have the right kind of access for the right amount of time. This complexity only increases when employees leave the company or change roles, resulting in access that's not revoked or entitlements that are no longer necessary.

5 Human Error

An employee accidentally clicked on a phishing email or downloaded malware onto their computer. Now, an attacker gained access to your sensitive information. Hopefully, this is just your worst-case scenario and not your reality.

To make sure it stays in the realm of What If, you need stronger access controls and IAM processes that can limit the scope and contain the radius of a breach — or prevent it altogether. Additionally, a **least privilege** approach to access controls, where employees only have access to the information they need to perform their job functions, can vastly reduce the impact of a breach.

Companies also need a comprehensive incident response plan with a step-by-step guide for detecting, containing, and resolving security incidents, as well as identifying key personnel responsible for each stage of the response.

6 Lack of Integration

Does your IGA solution manage user access and permissions with your on-prem applications — but not for applications hosted in the cloud? Or do you rely on applications developed in-house or by third-party vendors? If so, you may have run into roadblocks that require significant customizations before access controls can run seamlessly across all your applications.

7 Lack of Resources

What do all these IAM processes have in common? They require expert staff who can devote their time to redundant processes and complex problem-solving, and that requires more budget. If you don't have dedicated IAM professionals, effectively managing IAM systems stays perpetually out of reach.

Identity Governance, Evolved

Previously, IGA solutions were managed on-premises and required a lot of manual effort. As organizations grow, their IT environments become more sophisticated. They don't need siloed solutions that require specialized expertise to manage, or custom code that must be integrated with other systems and non-human identities. They need a user-friendly deployment that can automate and scale without springing leaks.

Companies don't need siloed solutions that require expert management, custom code, or complicated integration. They need a user-friendly deployment that can automate and scale without springing leaks.

There are 4 key features of a modern IGA system that speed implementation, streamline management, and keep complexity and costs down. Here's what companies should look for:

- "Cloud-architected" solutions allow your organization to access the solution from anywhere with an internet connection. **This eliminates the need for expensive physical hardware** and IT infrastructure, improving scalability, and facilitating access to the latest technology and features.
- Web-based cloud interfaces allow organizations to **automate manual tasks**, such as user provisioning and access reviews. This reduces the workload of IT staff, freeing them up to focus on more strategic initiatives.
- **Converged platforms** offer integrated **Identity and Access Management (IAM)** solutions, which saves companies from having to patch together multiple systems — reducing friction and driving **improved user experience** across all applications and services. Eliminating multiple point solutions helps you **lower staffing and licensing costs**.
- **No/low code design** reduces the Total Cost of Ownership (TCO) because your non-technical users can customize their IGA solution without requiring help from highly skilled developers or dedicated IT staff. Your teams can configure and manage IGA policies and workflows with **customizable pre-built modules and templates** that support your unique business processes, workflows, and compliance require-ments — and allow you to deploy on day one.

Enterprise-Grade Features

With a Low TCO

In 2015, Saviynt introduced the world to the first **SaaS-based IGA solution**. Our cloud-native, converged identity platform delivers no/low code design without the headache of multiple point products. The result: mid-sized organizations are empowered with enterprise functionality — without the enterprise price tag. Here's what we deliver:

Deeper integration into all your applications: Saviynt empowers fine-grained integration with hundreds of leading applications, including ERP systems, HR solutions, financial tools, and more. This allows organizations to automate many manual tasks, such as user provisioning and access reviews, reducing the workload of IT staff and improving user experience.

Rapid identity lifecycle management delivers rapid ROI: With automatic provisioning and deprovisioning of access (based on predefined roles and permissions), your company gains peace of mind that only authorized users retain access to systems and apps, no matter how roles might change. The best part: onboarding times can be reduced by 70% — minus the risk of human error.

Role and attribute-based access controls: To ensure that users have the right amount of access necessary to perform their job functions, Saviynt helps organizations create granular access policies that align with the business roles and responsibilities of their users. These controls restrict access based on attributes such as job title, location, or other criteria, and are critical to demonstrating compliance with regulations such as GDPR, HIPAA, and others.

Centralized Identity Warehouse with machine learning: Intelligent at its core, Saviynt's versatile cloud identity warehouse allows organizations to store and manage all identities in one place so teams have 360-degree visibility across identities and access. Our AI/ML-driven capabilities automatically identify security risks and potential breaches and recommend remediation so that your organization can respond to security threats quickly.

Continuous Compliance: To comply with various regulations and standards, such as GDPR, HIPAA, and PCI DSS, companies need strict access controls and audit trails. Saviynt's automated compliance checks save time and help ensure that only authorized individuals have access to sensitive data — and that all access requests and changes are tracked.

Automated monitoring and user access reviews: Saviynt IGA grants users only the minimum access required to perform their jobs, moving your company one step closer to zero standing privilege. If a user attempts to access systems or data they don't typically need for their job — or if they leave the company or change roles, Saviynt IGA can automatically review and revoke access. This automatic oversight protects your sensitive data from breaches, and your IT staff from burnout.

Enterprise functionality with a light deployment: Saviynt can offer mid-sized organizations the ability to deploy only the features they need (aka – lightly) without getting bogged down in ones they don't. If researched properly, **light deployments** can be a good fit for a single-cloud environment, reducing your financial outlay and time to value, all with a simplified deployment.

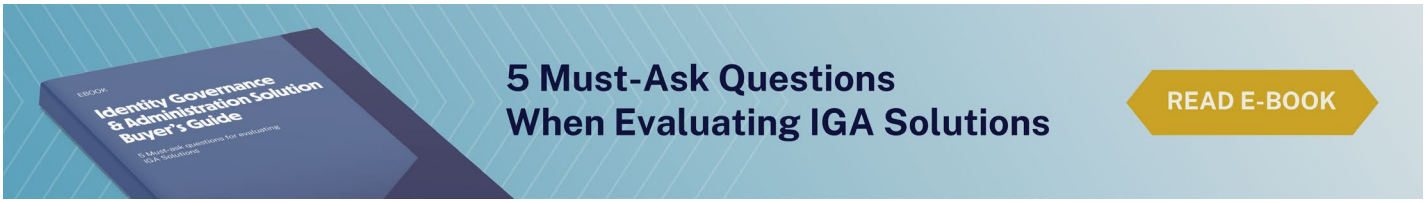
Saviynt IGA: Maximum Return Without Maximum Investment

Every day, more cloud infrastructure and applications come online, and new security breaches follow. Data protection is paramount for mid-sized organizations — but so is cost. Any new tool will significantly impact your users, so the right IGA needs to deliver a top-level experience from day one.

Intelligent at its core, Saviynt's versatile cloud identity warehouse allows organizations to store and manage all identities in one place so teams have 360-degree visibility across identities and access.

The beauty of Saviynt IGA is its power to clear the chaos, lower costs, and delight users. Your organization gains a cloud-focused solution to manage access, safeguard critical assets, and reduce risk. Your teams gain real-time visibility into all identities, applications, and data through a single control plane. They can say goodbye to toggling between point products and endless spreadsheets, and hello to quick deployment, simplified workflows, and fast-tracked decision-making. Together with Saviynt, your organization can see a payback in less than three months, with a potential 240% return on your investment over three years.

Modern IGA isn't just for large organizations. Find out why **Forrester**, **KuppingerCole**, and mid-sized **customers** just like yours recognize Saviynt as a leader.



ABOUT SAVIYNT

The Saviynt Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution.

Saviynt PAM solution is delivered via an agentless, zero-touch cloud-architecture so you can quickly deploy privileged access capabilities. Achieve zero-standing privileges with just-in-time (JIT) access and intelligent risk insights to power your PAM program.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suit e D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com