Five Steps to **Effective Third-Party Access Governance**

Know Your Exposure and Secure Your Enterprise with Saviynt

Introduction

Attracting and retaining employees has become more complicated in recent years. In response, executives have been outsourcing functions to third parties (contractors, agencies, consultants, vendors, etc.) to accelerate growth or reduce costs. But the rush to bring a third-party workforce onboard has illuminated several significant security risks from third-party users themselves or the third parties' access being compromised and used as a conduit into a company's sensitive data.

And the problem isn't just limited to human users. Internet of Things (IoT) devices, bots, and service accounts have been growing. These non-human entities require access to applications and data, just like human users.

"66% of companies surveyed had no idea how many third-party relationships they had or how they were managed, even though 61% of the surveyed companies reported having a breach attributable to a third party."

- Data Risk in the Third-Party Ecosystem: Third Annual Study, Ponemon Institute

Yet, despite the widespread use of third-party companies in many industries – healthcare, manufacturing, energy, and more – most organizations don't actually know how many third-party relationships they have. A **survey** from the Ponemon Institute noted that 66% of companies surveyed had no idea how many third-party relationships they had or how they were managed, even though 61% of the surveyed companies reported having a breach attributable to a third party.

TABLE OF CONTENTS

Industry	Use Case			
HEALTHCARE	Contract Doctors and Nurses	Medical Billing	Suppliers	Clinics, Outpatient Services
MANUFACTURING	Contract Manufacturers	Suppliers	Distribution	Customers
RETAIL	Seasonal Workers	Franchisees	Suppliers	eCommerce
GOVERNMENT	Healthcare Contractors	Postal Contractors	IT Services	Suppliers

The use of third-party resources is widespread throughout many industries, yet many organizations don't know how many of these relationships they have.

There's a lot at stake. A **vivid example** of a third-party breach, 2021's Accellion FTA event was the most destructive breach of the year, impacting 31 companies and over 5.6M users. Using a zero-day vulnerability, malicious actors stole files stored on a decades-old server. For FTA users, the attack mimicked the **2020 SolarWinds breach**. Hackers used advanced techniques to gain access into larger organizations through their weaker third parties. The attack was only one of 81 incidents and 200 publicly disclosed third-party **breaches in 2021**.

And the number of third-party attacks is growing. Between 2019 and 2020 there was only a steady increase in the number of third-party data breaches, but the number jumped by **17% in 2021**.

The Top Issues Affecting Secure Third-Party Access

Third-party access security efforts have lagged behind those for employees. Many companies are now working on their second or third generation of Identity and Access Management (IAM) solutions for employees, while the issues involved in third-party access management are just starting to gain widespread attention. But securing third-party access is now being recognized as crucial. Both auditors and regulators agree that third-party access is a significant vulnerability.

OWNERSHIP CONFUSION

The complications start with determining who is responsible for third-party access within the organization. Line-of-business executives will often sponsor third-party organizations to solve a business problem. The CISO is concerned with the overall cybersecurity of the company. The procurement team ensures the company meets its contractual obligations, and the risk and compliance team enforces internal controls. Ultimately the problem lands in the lap of the IAM or IT security teams by default.

LACK OF TOOLS FOR THIRD-PARTY GOVERNANCE

Traditionally, these teams have deployed homegrown applications and processes that are limited in scope. Or they have attempted to use a vendor module of an HR system that wasn't built for vetting, onboarding, risk assessing, monitoring, and certifying third-party access. But they usually lack a solution fit to solve the challenge.

THE HIGH NUMBER OF THIRD-PARTY WORKERS

The lack of tools isn't the only issue. The workload generated by managing third parties also adds to the problem. In some industries, the number of third-party users is greater than employees. So, the joiners, movers, and leavers in a third-party organization will also outpace a company's employees. The workload associated with securely adding and managing third-party employees requires a shared responsibility arrangement with the third party. But there's a lack of visibility when a worker's status changes within a third-party company.

RUBBER STAMPING AND ROLE COPYING

A major complaint from line-of-business executives is that it takes too long to onboard a third-party organization and add their users so they can become productive as quickly as possible. To appease the business, rubber stamping or copying roles may occur, defeating the purpose of having a third-party IAM solution.

RISK OF "NTH PARTIES"

In addition to the risk associated with third-party users, third-party organizations have multiple relationships with other third parties or what's often called "nth parties" — since business-to-business access continues throughout the whole value chain. These complicated relationships lead to security risks. Many third-party users still have system access months or even years after their access should have been revoked. These orphaned accounts are fertile ground for hackers to gain initial entry into a company.

Another technique is to inject malware into organizations' systems by exploiting the security updates for widely-used tools. These attacks can ripple through hundreds of organizations when hackers gain access through an nth party's weaker security posture. The **SolarWinds attack of 2020** was a prime example of this type of attack.

Five Key Steps for Securing Third-Party Access

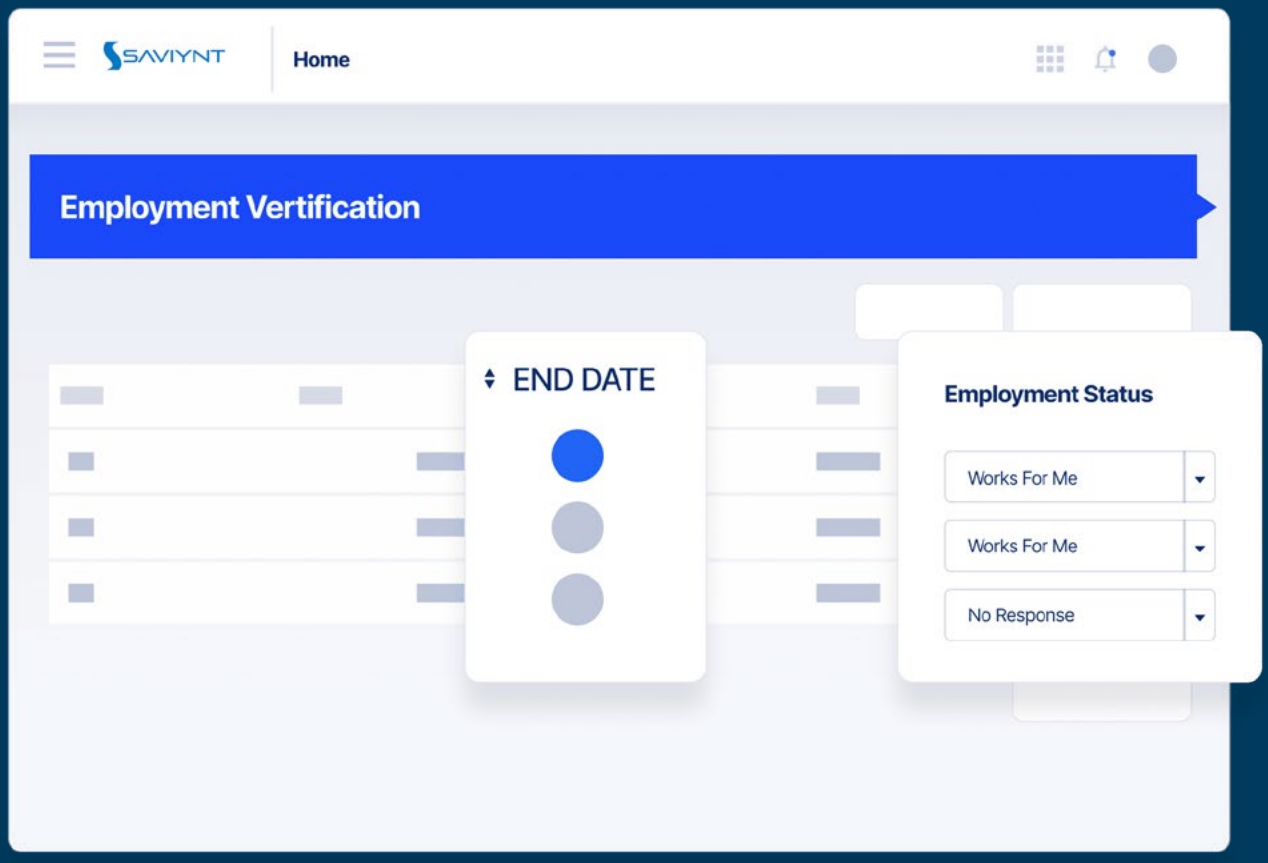
The good news? Companies and their third-party counterparts are actively working together to improve third-party security posture and provide better access control. We recommend implementing the following five key strategies to reduce third-party risk exposure if your organization is on the journey.

STEP ONE

Consolidate Third-Party Organizations

The consolidation of all third-party organizations can begin with finance and procurement. Anyone with a contract to provide services to any department in your company should be identified and cataloged in an authoritative System of Record (SoR) that includes any standing access privileges assigned to current users. Saviynt provides multiple gateways for onboarding, including delegated and federated onboarding.

For starters, your company should run an initial test to determine the last time third-party organizations used the credentials. This step allows you to locate and mitigate stale accounts. Credentials that have not been used in a specified time should be flagged for follow-up and de-provisioning if the user has left or is in a different role.



Saviynt employment verification and time-based access reduce orphaned accounts.

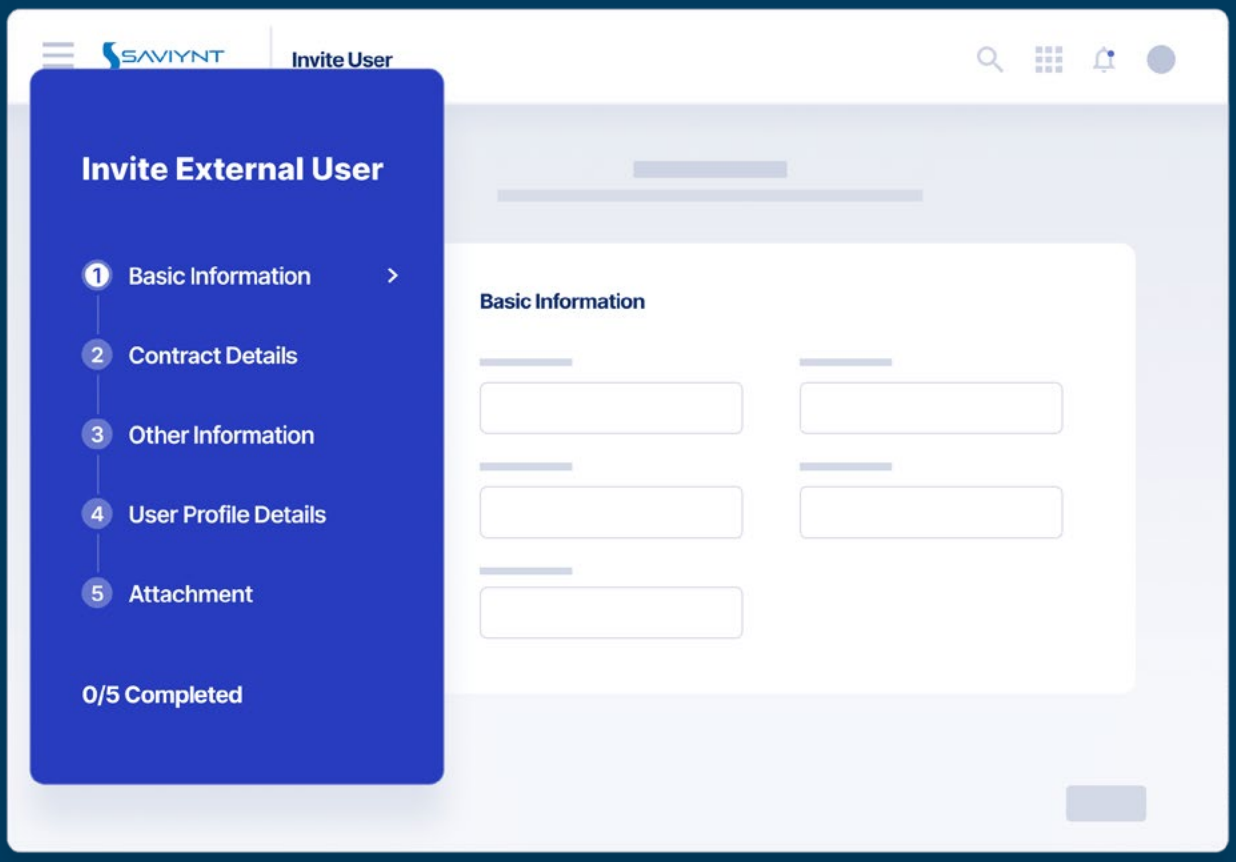
This step is a perfect time to assign sponsorship and joint accountability to third-party administrators. These administrators have better visibility to joiners, movers, and leavers from within their organizations and should be the focal point for recurring access reviews and certifications. Service-level agreements that stipulate the third-party organization's responsibilities and commitment to administrative support should be included as contract renewals occur.

STEP TWO

Institute Vetting and Risk-Aware Onboarding Processes

Your company and the third-party organization need to determine a workflow for vetting and onboarding third-party users to ensure they are who they say they are and that their onboarding process follows the concept of least privilege. They should be given only the appropriate access to complete their assigned roles. The role definitions should be specific to the actual tasks and not simply duplicated because the roles are similar.

To aid in collecting information for vetting and ID-proofing, third-party users could use a self-service portal to request access and provide required documentation. Self-service portals speed up vetting and provisioning, so users can quickly become productive. Having a clear workflow between your company sponsor and the third-party administrator will reduce the phone calls and emails that typically slow down the process.



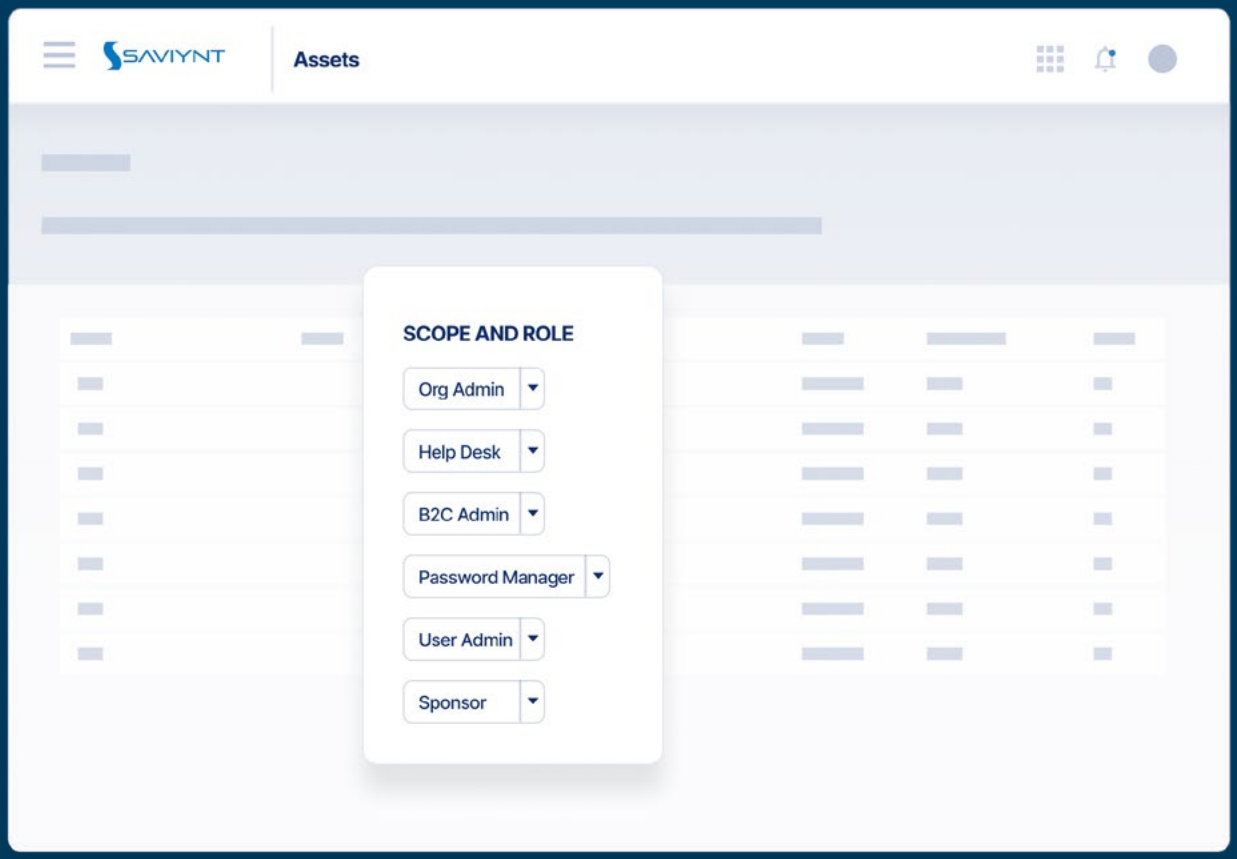
Saviynt makes onboarding third-party users easy and consistent.

STEP THREE

Define and Refine Policies and Controls

Your company and third-party organizations should define and continually optimize policies and controls to identify potential violations and reduce false positives, which helps reduce administrative workload. Over time, you can also embrace auto-remediation to improve efficiency further.

Test policies and controls regularly – monthly or quarterly – with the administrators from your company and third party. Running periodic access reviews and ongoing certifications will help ensure no user is over-provisioned and that orphaned accounts won't provide a conduit into sensitive data.



Saviynt provides a complete System of Record that includes any standing privileges assigned to third-party users.

STEP FOUR

Institute Compliance Controls for the Entire Workforce

Third-party access is rising in importance with several regulatory frameworks and is becoming a focal point for auditors. For example, Sarbanes-Oxley (SOX) includes several controls for managing third-party risk:

- APO10.01/APO10.02: Vendors must be selected per the organization's third-party vendor risk management policy and processes
- APO10.03: A designated individual must regularly monitor and report on whether third parties are meeting the organization's service level performance criteria
- APO10.04: Third-party service contracts must address the various risks, security controls, and procedures to protect information systems and networks.

Ultimately, the goal is to bring all third-party access under the same compliance required of employee users, so there is consistency across the entire workforce, and any violations get mitigated quickly. You can tie compliance controls to user type and enact auto-remediation policies to take swift action on non-compliant identities.

Having out-of-the-box regulatory compliance reports for Sarbanes-Oxley, HIPAA, GDPR, PCI-DSS, and others makes it easier to enforce compliance controls and more efficient to provide audit documentation.

STEP FIVE

Implement Converged Governance

Once you complete the first four steps, you can raise your cybersecurity maturity through converged governance of your entire workforce using a combination of IGA, Privileged Access Governance, and Third-Party Access Governance.

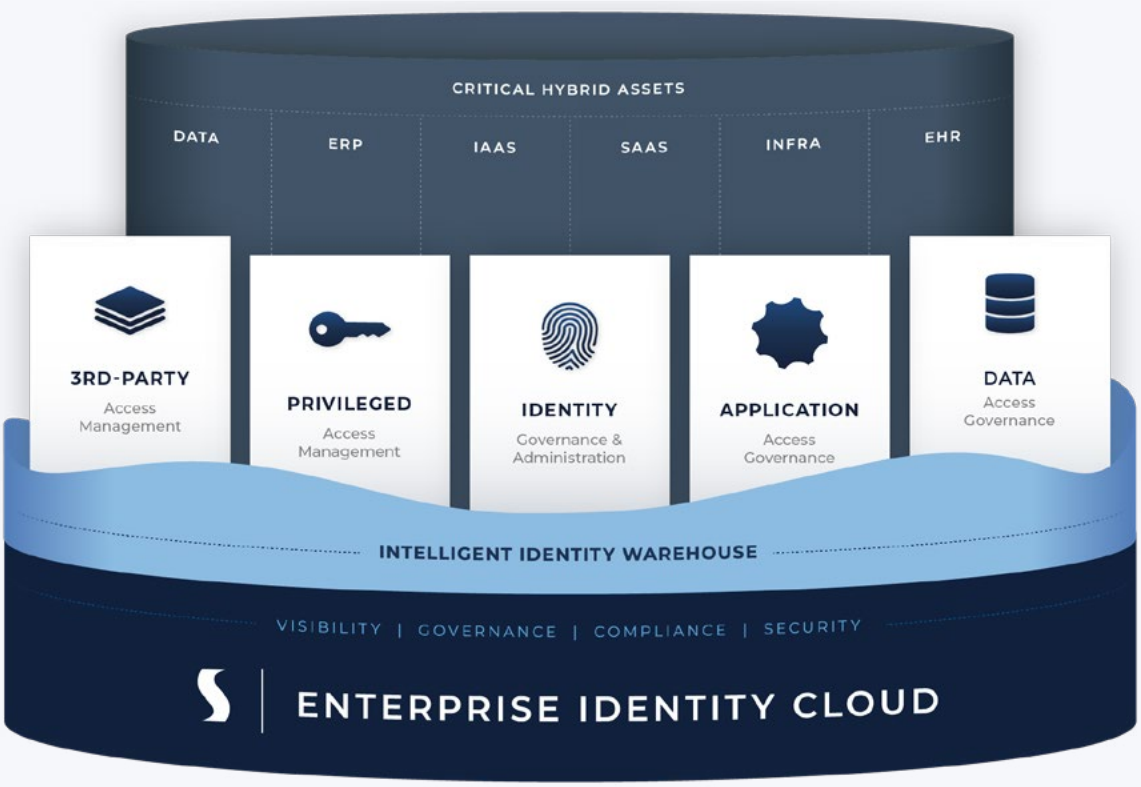
This converged view provides a single-pane-of-glass for complete visibility of your entire workforce. It also provides another level of safety by immediately revoking access to downstream systems if warranted and providing time-based access so that access gets revoked when a contract ends. Adding Application Access Governance can allow you to identify potential and actual cross-application Separation of Duty violations across SaaS and on-premises applications.

Secure Your Enterprise With a Cloud-Native, End-to-End Identity Solution

Rather than managing multiple relationships and integrations to provide an end-to-end identity platform, you can leverage Saviynt's **Enterprise Identity Cloud (EIC)** to quickly gain the business benefits of a world-class identity solution.

Enterprise Identity Cloud

The leading cloud identity & governance platform built for simplicity and scale.



EIC combines multiple identity management capabilities into a single cohesive platform to unify controls and risk management for every identity, app, and cloud across your business. EIC allows you to onboard people, apps, and machines in minutes and selectively turn on access & governance functionality.

As part of EIC, Saviynt Third-Party Access Governance plays a key role in helping many organizations simplify the third-party access process and reduce non-employee risks. It helps reduce risks by utilizing a sponsor-based approach to third-party access. Saviynt provides automation, access request, risk visibility, and access review throughout the third-party onboarding process and manages these identities throughout their lifecycle.

Our Third-Party Access Governance product enables you to:

- Collaborate with third parties confidently
- Reduce risk across remote workforces
- Manage the lifecycle of third-party organizations, people, and identities
- Consolidate access visibility and controls onto a single platform

Internal and external sponsors shepherd the account from inception through access management, periodic reviews, and eventual decommissioning. With Saviynt, you get:

- Accelerated onboarding and reduced costs
- Complete visibility into vendor risk
- Vendor account lifecycle management
- Configurable policies for access requests
- Auto-remediation for non-compliant accounts

The need for better third-party access governance is only going to grow. By addressing it now, with Saviynt's proven end-to-end, cloud-native solution, you can close the third-party security gap and gain complete security for your enterprise — now and into the future.

Saviynt is the leading identity governance platform built for the cloud. It helps enterprise customers accelerate modern cloud initiatives and solve the toughest security and compliance challenges in record time. The Saviynt Enterprise Identity Cloud converges IGA, granular application access, cloud security, and privileged access into the industry's only enterprise-grade SaaS solution. Learn more at **saviynt.com**.

Want to talk to an identity and security expert?

Reach out to us today at
saviynt.com/contact-us