Saviynt

The Hidden Risks of Third-Party Access

How many vendors have the key to your kingdom? Use this guide to inventory, onboard, and provision with confidence, from procurement to termination.

Contents

Introduction

How many people can unlock your front door and walk right in? Nobody but you, of course.

Then again, there was that time you gave a key to your neighbor. And that petsitter. Did you change your keycode after you gave it to the repairman? Years pass, memory fades, and the number of people with access slowly grows.

Third-party access risk works the same way. Companies rely on a constellation of vendors (and bots, IoT devices, and non-humans) for everything from equipment maintenance to cloud storage. While this on-demand workforce has allowed us to scale up operations and double our reach, it has also generated hundreds or even thousands of "keys."

The sheer volume of access requests has pushed overwhelmed Identity and Access Management (IAM) teams and made third-party access a prime attack vector. After all, why would hackers pick your lock when they can simply slip past your gate with the smaller, more vulnerable vendors that share your key.

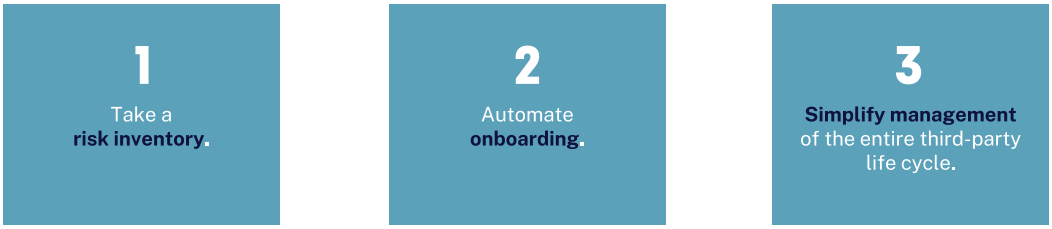
Last year, it happened to Toyota, Morgan Stanley, Upstox, and **a long list** of well-known companies. But it isn't just the big fish who need to worry. For the vast majority, it's not a matter of if, but when a breach will occur. Third-party software vulnerabilities accounted for **13% of breaches** in 2022, and **one-fifth** became full-on attacks.

These incidents are particularly insidious because they take an average of 26 days longer to identify and contain — and if you're operating in the United States, they cost about 5 million dollars more to remedy. Bad actors can lock down your system, steal company data, and exact double extortion: pay once to get your systems back, pay again to get your data back — but never fully recover your reputation.

How Vulnerable Do Your Third-Party Relationships Make You?

> **Traditional legacy IGA solutions weren't designed to manage the sophistication of today's third-party identities. Determining your exact level of exposure is difficult, and stitching together multiple point solutions is counter-productive.**

In this white paper, we'll look at the hidden risks companies are grappling with, and how Saviynt's converged IGA with **Third Party Access Governance (TPAG)** can help you:



Inventory Your Third-Party Risks in 6 Steps

Can you name all the external parties you rely on? Often, companies that think they have a handful end up discovering hundreds of third-party relationships.

Catching up with the depth and breadth of your exposure can be the hardest step. But since you can't manage what you can't see, an accurate inventory of all your third-party relationships is foundational to your IAM program's success.

1 Make The List: Third-Party Due Diligence

Gathering a **comprehensive system of record** of all your current third-party relationships. This includes suppliers, contractors, and other organizations that have access to your systems and data — along with all their contract details and contact information. If you just heard a record scratch, you're not wrong. This step takes considerable time and effort, so it's critical to begin the process by selecting a sponsor inside your company who will play point on communications with each third party.

Sponsors can identify internal and external administrators from different departments who can work together to:

- Evaluate The Third Party's Security Controls
- Define Roles
- Assign Levels Of Access
- Prevent Orphaned Accounts

Roles and responsibilities should be clearly defined and tailored to the tasks rather than being overly broad or duplicated for similar functions.

Sponsors can also ensure that these baseline expectations get communicated and written into your third-party contracts and SLAs (Service Level Agreements). Defining third-party accountability, ensuring a company's sensitive information remains secure, and requiring any breaches to be immediately disclosed should be standard contract terms. Of course, it takes some teamwork and patience to track down all of the organizations you're doing business with and hammer out the terms, but a risk inventory is the backbone of a strong security posture.

Of course, it takes some teamwork and patience to track down all of the organizations you're doing business with and hammer out the terms, but a risk inventory is the backbone of a strong security posture.

2 Hold Third Parties To The Same Compliance Standards As Employees

Third-party access is rapidly moving to the top of the audit checklist. How well are your vendors complying with data privacy laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)? If they're handling credit card transactions, are they adhering to the Payment Card Industry Data Security Standards (PCI DSS)?

Before granting access, work closely with your third parties to set expectations and ensure that security policies and standards are written into all your third-party contracts. If you're required to adhere to certain laws, then so should your third parties, then so should your third parties. In some cases, you may be held liable for their non-compliance.

In addition to fines from regulatory agencies, and legal action from affected parties, you'll likely be required to enact costly security protocols around identity and access, monitoring, and incident response.

> **Compliance is complicated, so the name of the game is consistency. Bringing all third-party access under the same compliance process as your entire workforce can go a long way toward reducing risk.**

Applying uniform standards across the board fosters a more cohesive and consistent organizational culture that can encourage the trust and confidence of employees, customers, and other stakeholders.

3 Insure To Prevent Financial Losses

Whether it's vendor fraud, mismanagement of funds, or lax security, the blast radius from third-party breaches is harmful and far-reaching. The process of hiring cybersecurity experts and future-proofing your environment can outpace the time and money required for customer payouts. The widely-covered **T-mobile data breach** that occurred last year cost a record-breaking **$350 million**.

Needless to say, organizations should carefully review the financial stability of their third parties and put in place financial safeguards to protect against losses that may arise as a result of a third party's failure to perform as required or specified.

4 Have The Talk: What To Ask Your Third Party

Ideally, prevention starts before entering into any agreements. But it's never too late to begin understanding the cyber posture of your existing external partners. Get familiar with a vendor's security practices, policies — and potential vulnerabilities — by asking these key questions:

- Do they have policies in place to protect the confidentiality, integrity, and availability of any data they handle on your behalf, such as **encryption**, **access controls**, and **incident response plans**?
- Can they provide evidence of appropriate security measures **(firewalls, antivirus software, vulnerability management processes, etc.)** that protect their networks and systems from cyber threats?
- How secure are their physical facilities? Do they have access controls, surveillance, and **disaster recovery plans** in place?

- Does the vendor conduct **employee training and awareness** on security best practices, such as password management, secure communication, and identifying and reporting potential threats?
- Do they have cybersecurity **policies for "nth" parties**? A growing concern is that attackers are often gaining access to your data by attacking the third parties of your third parties.

5 The 3 Rs: Review, Reevaluate, Renegotiate

What's in your contracts? Regularly reviewing and updating contracts and agreements with third parties can ensure you're not overlooking changes in your risk profile. Will your vendor be responsible for promptly administering identity access for their Joiners, Movers, and Leavers (JMLs)? Will they regularly complete access reviews and certifications? Will they promptly disclose breaches so you can take action to reduce the potential fallout? These are critical features you need.

Establishing clear lines of communication with third parties can help you stay ahead of emerging threats and protect your systems and data from potential vulnerabilities.

6 Don't Forget the Machines

Machine identities and **Internet of Things (IoT)** devices provide access to critical systems and resources. Service identities are used to identify and authenticate services (such as APIs) to each other and to the systems they rely on. If they aren't properly secured, unauthorized devices can gain access to your network and sensitive resources, potentially leading to data breaches and security incidents.

Considerations Before You Go Live

Onboarding a third party often involves integrating their systems with yours — and that can be tricky. If their system uses different software or tools, or different reporting or testing protocols, misintegration can lead to potential system downtime or data loss.

If your company's survival is dependent on a vendor, it's all the more imperative to plan, test, and validate the integration to ensure that it meets your company's requirements and is fully compatible. To avoid major business continuity problems, and to identify and resolve issues as soon as they arise, your company should also continuously monitor performance.

It's also critical to develop an incident response that would inform all relevant stakeholders, provide next steps, and minimize the impact of a disruption. Set a contractual service-level agreement regarding notification of any breaches occurring in a third party's system.

Onboarding third parties to your IAM system may also involve manual processes, such as creating and assigning user accounts and permissions. When individuals aren't trained well, if communication or monitoring is poor, or if someone misses a key requirement in the third party's contract (or simply makes an access mistake), this could result in data entry errors, breaches, and compliance violations.

The 4 Key Advantages of Delegating Administration

If you're trying to manage a complex IT ecosystem with point solutions and a legacy IGA tool, you're increasing obstacles to security — and you're losing your line of sight.

Saviynt's cloud-native Identity Cloud platform converges IGA and **Third-Party Access Governance (TPAG)** into a single centralized platform that streamlines onboarding, automates compliance activities, and documents governance. The Identity Cloud also provides integration with many of the leading system of record (SOR) solutions for non-employee user identities and many of the leading IDaaS solutions used for federation.

Saviynt TPAG delegated administration model automates access provisioning and verification for human and non-human identities, takes the guesswork out of vendor evaluation, and reduces the burden of constantly monitoring all your vendors. Here's how.

Onboarding, Simplified

You've heard the expression, "location location location." With Saviynt TPAG, it's delegation, delegation, delegation. As you begin your inventory process, Saviynt provides multiple ways to facilitate collaboration between internal and external departments, delegate the process of collecting third-party non-employee data, and facilitate the completion of your third-party inventory.

Saviynt TPAG helps you assess vendor risk prior to onboarding by aligning human owners and risk-based access policies to machine identities, providing admins from all organizations with real-time visibility into who has access to systems and data — and what they're doing with that access.

Throughout the relationship, Saviynt's self-service portal enables third parties to complete many of the onboarding tasks on their own via Access Request System, bulk upload, or federated identity systems. Our intelligent, out-of-the-box, customizable controls can help identify common vulnerabilities or address specific risks unique to a third party, as well as set **just-in-time** access privileges that can be deactivated when not in use.

Together with an extensive set of pre-built templates and control libraries, Saviynt TPAG can reduce onboarding times by **up to 90%**, allowing users to become productive quickly.

Free Up Your Teams With Automated, Intelligent Access Reviews

Regular access reviews are a best practice that ensures third-party users are not completing activities outside granted access — and that stale access to systems or data gets detected and tossed out. But manually managing this can be time-consuming, resource-intensive, and rife with delays and errors.

As your number of users grows, so do our automation capabilities. Saviynt TPAG can streamline the creation of user accounts, assignment of roles, and other access-related tasks, ensuring that access is granted consistently and in accordance with your established policies and procedures.

For example, **built-in workflows** can delegate access reviews to the third-party administrator and can automatically send reminders when it's time for an update. Or, when third-party access changes, Saviynt can automate the approval process and the JML processes you have to manage throughout the identity lifecycle.

Artificial intelligence capabilities continuously learn about your environment to provide access and provisioning recommendations and identify SoD violations. Having 360-degree visibility into all the controls you have in place, the weakness/effectiveness of those controls, and the frequency of attack or compromise keeps you and the third-party organization in sync. This slashes the likelihood of orphaned accounts, and identifies potential security incidents before they become a problem — all while reducing the drag on your time and resources.

Make Smarter Decisions With Expedited Certifications

Saviynt makes it easy for business managers, application owners, role owners, and others to make informed decisions about access certifications, whether for internal users or across a large number of third parties. Our **peer and access-based analytics** flag high-risk requests for additional review, reducing rubber stamping and **decreasing decision times by up to 70%**.

Saviynt TPAG lets you prioritize critical reviews, understand certification decisions, and **trigger micro-certifications for continuous compliance**. Automating these processes significantly increases engagement and reduces your enterprise risk.

Take The Headaches Out Of Audit Prep

To proactively manage cyber risk, you need access to real-time, actionable information and insights 24/7. Waiting for an incident to occur or relying on inherent risks to predict impact is not an effective approach. Any delay in response can mean a higher impact if an attack occurs. But for many organizations, it isn't feasible to hire staff with the skills and experience to identify, assess, and respond — let alone keep up with the latest threats and regulatory standards. Adding to the complexity, regulators are cracking down on third-party access as this threat vector continues to make headlines.

Saviynt's risk and context-aware analytics and reporting can help you identify areas for improvement and get real-time visibility into third-party compliance with industry regulations and standards. **Out-of-the-box controls** are cross-mapped across regulations, industry standards, platforms, and control types, **accelerating audit prep** and providing fully documented compliance reports and dashboards for regulations like SOX, HIPAA, PCI DSS, GLBA, ISO 27002, FISMA, and CMMC.

Lose The Risk. Keep The Relationships

Taking stock of your third-party risk might feel like an overwhelming task, but you've taken the first steps to protect your assets, reputation, and bottom line. You don't have to do it alone. Saviynt has your back for the entire third-party journey, from introduction to relationship completion.

You've taken the snapshot. Now improve your cybersecurity posture with a combination of **Saviynt's IGA, Privileged Access Governance, and Third-Party Access Governance**.

Our identity-centric approach allows for centralized onboarding, better control over the access that third parties can request, and quick removal after the relationship ends. Together with proper third-party risk inventory and onboarding, delegation can help you simplify communication between departments, reduce administrative burden, and provide identity oversight throughout the third party's entire lifecycle.

Saviynt's **Identity Cloud** platform delivers intelligent out-of-the-box and custom controls that automate the approval of low-risk access and flag high-risk requests for additional review using peer and access-based analytics. Not only do we ensure third parties have only the minimum access necessary to perform specific tasks, we also allow for one-click certification, revocation, and decommissioning — moving you closer to the ideal of **Zero Standing Privilege**.

Saviynt can also help you manage evolving IoT, OT, and **DevOps** complexities by governing machine identities (APIs, RPAs, and containers) with zero trust principles.

Companies need a way to maintain visibility, monitor access, and remediate third-party risk on a day-to-day basis. With Saviynt, you can streamline management for the entire lifecycle of your business relationships, complete with a great user experience, attractive return on investment, and a low total cost of ownership.

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