kuppingercole ANALYSTS

SailPoint Non-Employee Risk Management

Paul Fisher

August 16, 2023

EXECUTIVE VIEW

This KuppingerCole Executive View looks at some of the options available to IT leaders and senior security strategists to manage non-employee and other third-party identities. A technical review of SailPoint's Non-Employee Risk Management solution is included.

Content

Introduction 2
SailPoint Non-Employee Risk Management 4
Strengths and Challenges 6

Figures

Figure 1: A survey of identity practitioners shows that organizations are not utilizing IAM for newer identity types. (Source: Kuppinger Cole Analysts)..3
Figure 2: SailPoint Non-Employee Risk Managemnent solution sits between third parties and the SailPoint Identity Security Cloud. (Source: SailPoint) 5

Introduction

Contemporary business operations encompass a multitude of interconnected networks, devices, assets, and individuals. At the same time, a substantial portion of a company's workforce comprises contractors, partners, seasonal workers and vendors. Effectively managing these identities and regulating access presents a complex challenge, necessitating an all-encompassing solution to bring these crucial non-employee identities under control.

> Many organizations have strategic shortfalls in third-party risk management governance. Specifically, only 42% of respondents say managing outsourced relationship risk is a priority and only 40% of respondents say there are enough resources to manage these relationships.
>
> (RiskRecon/Ponemon Institute September 2022)

For some time, Identity and Access Management (IAM) platforms have empowered IT security and compliance managers to govern internal system access. Without IAM, administrators had limited visibility regarding the identities accessing resources either on premises or within private clouds. Privileged Access Management (PAM) extended this control by regulating access to sensitive administrative tasks and high-value data assets.

However, modern organizations also need to accommodate external identities. This is particularly relevant for companies operating in the B2B, B2G, and B2B2C sectors with intricate supply chains and supplier/customer/partner relationships. The mix includes important actors within the supply chain, such as contractors, freelancers, and external auditors. It is crucial for the hosting or sponsor organization to have the means to regulate secure access centrally. The complexity increases when considering that suppliers have their own connections to partners and supply chains (known as “fourth parties”), which can further impact the sponsor organization.

According to the Ponemon Institute, 54% of respondents indicate that their organizations lack a comprehensive inventory of all third parties with network access, while 65% have not identified the third parties with access to the organization's most sensitive data. Furthermore, the same report reveals that 51% of organizations experienced a data breach caused by a third party in 2021.

There are several business problems that the unmanaged growth of non-employee identity presents. One is that managers and auditors do not have an accurate count of non-employee users or a clear understanding of the information they can access. It is also hard to determine whether a user is an employee, a contractor, or third-party supplier. There can be issues when a former employee returns to the organization as freelancer or when a contractor becomes a full-time employee.

Duplicate user accounts and multiple credentials are a big problem which can also result in multiple software licenses being created for the same user. Some organizations try to solve these issues by improving or modifying HR software tools – often with limited success, as these are very much focused on HR issues and HR workflows. Others may try developing a proprietary platform which often proves to be costly and time-consuming and tends to tie up valuable resources. All too often organizations simply do not have the correct IAM processes, policies, and software in place to cover all types of identities that require access to complete business workflows and tasks.

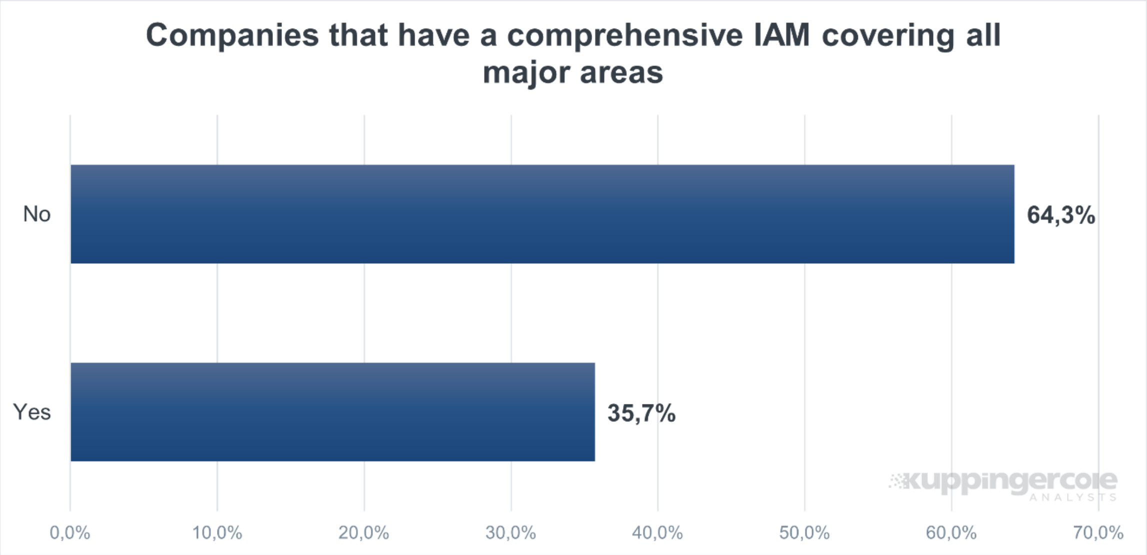

Figure 1: A survey of identity practitioners shows that organizations are not utilizing IAM for newer identity types. (Source: Kuppinger Cole Analysts)

While certain IAM and PAM platforms allow limited access for third parties, many do not, requiring specialized software to govern supply-chain access. Therefore, software has been designed to facilitate secure access and collaboration throughout the multiple tiers of an organization's supply chain and partners.

SailPoint Non-Employee Risk Management

SailPoint is a software company providing identity management solutions. It was founded in 2005 and is based in Austin, Texas. SailPoint’s Non-Employee Risk Management solution extends its identity expertise into controlling non-employee access.

True to the design ethos that runs through its product line, SailPoint’s Non-Employee Risk Management module puts superior identity management at the forefront of data and network security. This addition to the SailPoint Identity platform, based on the technologies acquired from SecZetta, is designed to manage non-employee and other third-party identities. SailPoint lists these to include contractors, vendors, suppliers, and partners, but the list potentially includes any identities that typically sit outside the traditional boundaries of the organization.

Importantly, the SailPoint Non-Employee Risk Management solution enables administrators to manage full identity lifecycles rather than simply manage authentication. For non-employee identities, this lifecycle will start with the creation of a new profile for the non-employee. The software supports delegated administration so that a third-party organization (e.g., a supplier of contractors or a partner organization) can build the profile in a format that is compatible with SailPoint technology. This way, both parties can save time by completing basic data about the non-employee and get agreement on Acceptable Use Policies and other key policies from the sponsor organization.

This is achieved using standard SailPoint Forms where third-party tasks can be delegated to a third-party HR administrator, or any approved title holder in a child organization, including authorization for other third-party admins to create new contractors. This is efficient, and by using the same SailPoint processes and design in the child organization, sponsor organizations retain full visibility over identities created and seeking access, and who has admin access in the third-party organizations.

Once a form is created for a third-party identity, it is submitted to the analysis engine. Using some AI techniques, it determines if this is a new person or a duplicate (for example). If a duplicate is found, all previous data and activity for the identity can surface in the dashboard.

The software allows for flexibility in the creation of forms. These can be set as “read-only”, “just approve or edit details” or “add additional data from the sponsor organization”.

Once an identity has been approved, it will be added to the SailPoint Identity Security Cloud as an authorized identity ready to be allowed access according to its attributes and policies built into SailPoint.

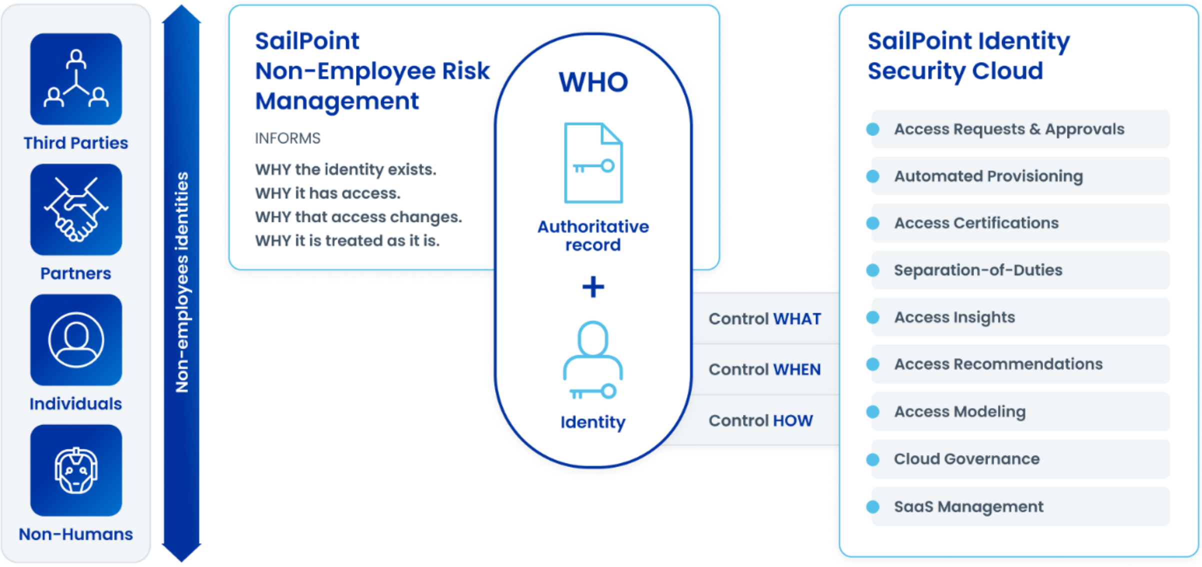

Figure 2: SailPoint Non-Employee Risk Management solution sits between third parties and the SailPoint Identity Security Cloud. (Source: SailPoint)

Customers need to be on the SailPoint Identity Security Cloud to get the specific benefits of the SailPoint Non-Employee Risk Management module.

Once installed, a new *Manage Non-Employees* widget will appear in the main SailPoint administrator dashboard. The software allows for a hierarchical administrator structure so Chief Administrators can onboard non-employee identities directly or delegate the task to specific administrators. Administrator Accounts can be automatically created for external users the next time they log in and authenticate.

Identity Cubes

Central to identity management in the platform, are the user (or identity) role-based Cubes (profiles) that sit as internal datasets (within a SailPoint Tenant) for regulating access for non-employees, and for Administrators to have a complete map of all the non-employee data they need to track. Each identity is given its own unique Cube, which can be modified or deleted, depending on the working lifecycle of the identity – but the assigned identity will not change, it only can be deleted. Each identity will have one Cube throughout its lifecycle with the sponsor organization.

Administrators can create Cubes for individual non-employee identities. Again, this is designed to be business friendly with natural language processing used. For example, Cube types for non-employees’ identities can contain a list of organizations they come from, or the projects they are working on.

Detail on actual workflows and granular access by non-employees can be added to Cubes, making them very flexible and incredibly useful for audit and security purposes - those seeking access to sensitive areas can be given a more granular Cube to ensure that the right level of access is given.

The delegated administration allows both internal and external users to collect identity data while onboarding a new non-employee. Administrators can authenticate a non-Employee using a wide number of SSO solutions.

Overall, SailPoint Non-Employee Risk Management provides those organizations already invested in the SailPoint identity governance ecosystem with a useful solution that extends advanced governance controls to large and complex populations of non-employee users, while keeping overall management and control centrally.

Strengths and Challenges

SailPoint has successfully integrated parts of the technology it acquired from SecZetta and closed a gap in its overall identity governance platform with the release of SailPoint Non-Employee Risk Management. It is a simple package that does a good job of managing non-employee identities. Its delegation tools increase efficiency and take away some of the onboarding chores associated with third party identities. At the same time, it uses tried-and-tested SailPoint technology to keep ultimate control of non-employee access with sponsor organizations.

Because it works with the SailPoint Identity Security Cloud, existing SailPoint customers of that platform will find it easy to deploy and manage SailPoint Non-Employee Risk Management through familiar protocols and identity workflows. For those trusted delegated administrators sitting outside the sponsor organization, the use of SailPoint forms and dashboard makes it easy for them to create SailPoint compatible data without needing to know backend components or structures. This is wisely reserved for SailPoint-savvy administrators in the sponsor organization.

SailPoint needs to improve support for non-human identities. It is known these already outstrip human-based identities, and in the age of AI and bots, these are already part of the supply-chain identity landscape. While they can be managed differently to human-based identities, the fact that they can be spun up so readily by end users and hosted in multiple clouds, presents a growing security risk and a much greater identity management challenge. The good news is that this is firmly in SailPoint’s pipeline for the product and expected in early 2024. This will round out the product, and we look forward to seeing this.

We highly recommend existing SailPoint users to consider adding SailPoint Non-Employee Risk Management to their identity arsenal if they have any number of non-employee identities to manage. There are only likely to be more of them in the future.

Strengths

- Easy to configure dashboard controls accessible to both internal and external parties.
- Flexible workflows assist onboarding, offboarding, and identity lifecycle management.
- Form creation uses natural language processing and can be matched to business policies.
- Brings the governance power of SailPoint Identity Security to non-employee identities including the Identity Outlier capability.
- Ability to collect additional identity access-related information if needed.
- Enhanced onboarding with acceptance of NDAs and Acceptable Use Policies enabled by delegated administrator functionality.
- Automated provisioning of existing identities already held in SailPoint.
- Automatic disablement and termination of identity access if required.
- Lifecycle and policy-based controls extend control over non-employee identities.

Challenges

- Nonproprietary support for non-human third-party identities; we look forward to the promised full support in the next version.
- We would like to see more integrations with wider PAM and CIEM solutions or capabilities – but both are on the SailPoint roadmap.
- Primarily supports and integrates with SailPoint Identity Security Cloud.

Related Research

Executive View: SailPoint Identity Security Cloud

Leadership Compass: Identity as a Service (IDaaS) - IGA

Leadership Compass: Access Governance

Leadership Compass: Secrets Management

Executive View: SailPoint Identity IQ

About KuppingerCole

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and in making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.