SailPoint

Datasheet

Quick and secure access for state and local Non-Employees

State and Local organizations today manage a wide range of identities beyond employees and may struggle to centrally view, govern, and quickly grant their access. Contractors, supply agents, outside supply houses, business partners, vendors, and others make up a large percentage of their workforce. Manually reviewing and granting access can be error-prone and time-consuming. However, automating secure access and simplifying onboarding can bring all these critical identities under control.

SailPoint Non-Employee Risk Management provides government agencies with a powerful identity security solution that extends advanced identity governance controls to large and complex populations of non-employee users. Government agencies can reduce their cyber risk with increased visibility and the ability to efficiently eliminate over provisioned and orphaned account access. Together with SailPoint Identity Security Cloud, you can secure both your employee and third-party identities with automated provisioning and ensure productivity on Day 1.

Feature overview

SailPoint Non-Employee Risk Management provides operational efficiency and minimizes risk by dynamically informing you exactly which non-employees need access, why they require it, and when it's appropriate.

SailPoint Non-Employee Risk Management

Comprehensive identity security for non-employees

Identity solution
Centralized and scalable solution for all third-party non-employees

Non-employee record
System of record for identity access

Strengthens security
Full visibility into your non-employees and their access

Enables collaboration
Both internal and external users can easily contribute information for onboarding

Simplifies audits
Captures essential identity data and documents the entire non-employee lifecycle

Process orchestration
Flexible workflows for onboarding, offboarding, and daily lifecycle management

State and local use cases

Take control of your agency's non-employee identities:

- **Expedite non-employee onboarding with delegated administration.**
  Scenario: A state agency hires a third-party vendor to conduct an independent audit and the team needs to be onboarded quickly. Rather than relying on manual processes to collect information about these non-employees, both third-party administrators and non-employees can easily provide data to your team utilizing delegated administration to expedite the process.

- **Centralize and scale master identity data to accurately inform access decisions.**
  Scenario: A master identity prevents duplicate identities from being created when a government non-employee has multiple assignments over time. It also allows you to identify someone who was terminated for cause and later hired by another third-party vendor.

- **Accelerate non-employee onboarding.**
  Scenario: Some state and local agencies must rely upon other agencies for human resources functionality. This can often cause a delay in the onboarding of non-employee workers. Instead of waiting for the official human resources information, agencies desire to onboard the new employee ahead of time to ensure they are productive on Day 1.

- **Avoid expensive ERP costs to manage non-employees.**
  Scenario: The cost and responsibility for managing non-employees should reside with the contract managers. Contract managers are responsible for managing all aspects of the relationship including the people and the applications those workers should be entitled to access. Non-Employee Risk Management allows managers to truly manage the entire relationship without relying upon the ERP system.

- **Protect non-employee access to sensitive data.**
  Scenario: Before allowing a non-employee access to sensitive data, they must sign a usage agreement and meet your department's qualifications, such as training, compliance, and onboarding requirements. Non-Employee Risk Management will ensure the person meets the qualifications and present a usage agreement for them to sign as a part of the onboarding process.

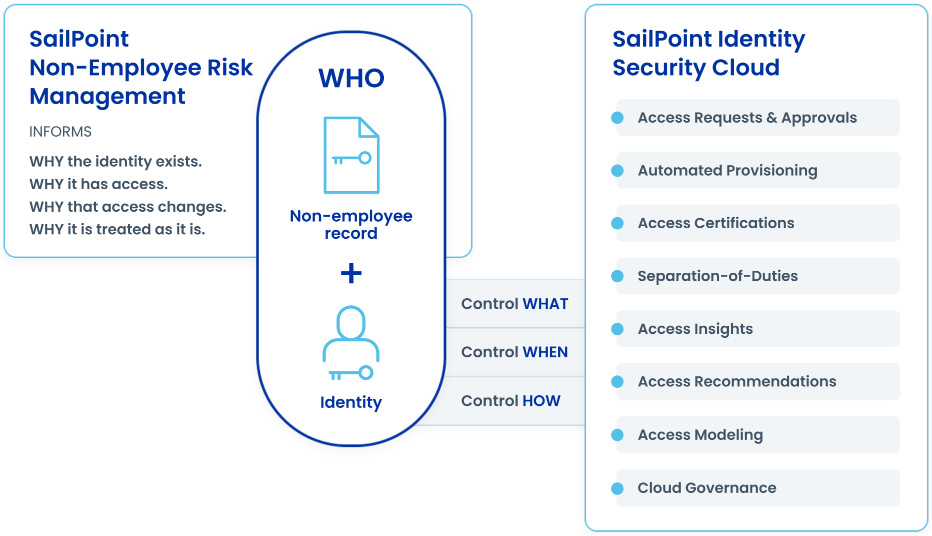
- **Manage non-employee staffing surges.**
  Scenario: Easily onboard public sector non-employees during high volume staffing needs such as during natural disasters. Removing access when it's no longer needed can be automated or removed immediately with a click of a button.

- **Document lifecycle management processes to simplify audits.**
  Scenario: With SailPoint reporting, organizations can see which non-employees have access to what systems, applications, and data. Organizations can also keep track of which vendors, contractors, and suppliers have direct access to project management systems. Organizations can also keep track of which affiliate agencies, municipalities, judicial branches, and the like have direct access to sensitive information.

- **Maintain a single identity for a non-employee, even when their relationship with your organization changes.**
  Scenario: Granting the right access for a supplier that may work in multiple departments that are short staffed and may travel to different facilities within a county. The supplier will maintain one identity, even as their relationship (and therefore, their required access) with your organization changes.

With **SailPoint Non-Employee Risk Management** and **SailPoint Identity Security Cloud**, your government agency can easily manage the simplest to the most complex scenarios when it comes to non-employee identities the same way it manages employee identities.

Learn how to solve your state or local agencies' non-employee identity security gap. Listen to our webinar, **Solving the non-employee identity gap in third party risk management** to learn more.



SailPoint Non-Employee Risk Management

INFORMS

WHY the identity exists.
WHY it has access.
WHY that access changes.
WHY it is treated as it is.

SailPoint Identity Security Cloud

- Access Requests & Approvals
- Automated Provisioning
- Access Certifications
- Separation-of-Duties
- Access Insights
- Access Recommendations
- Access Modeling
- Cloud Governance

About SailPoint

SailPoint equips the modern enterprise to effortlessly manage and secure access to applications and data through the lens of identity - at speed and scale. As the category creator, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

sailpoint.com