# Silverfort + SailPoint: Integrating Identity Risk into Governance Decisions

Organizations are under increasing pressure to align identity security and governance around real-time user risk. Traditional governance systems rely on static data and periodic reviews, leaving gaps when user behavior or threat posture changes suddenly. To address this challenge, Silverfort and SailPoint have partnered to deliver a seamless integration that brings continuous, risk-based intelligence directly into SailPoint's governance workflows, enabling adaptive and risk-aware decisions across the identity lifecycle.

## Enforcing governance with shared real-time risk context

Through the integration between Silverfort and SailPoint, organizations enhance their ability to make risk-informed governance and access decisions that reflect users' real-time behavior and security posture.

Silverfort provides user-specific identity risk assessments via its API, which are ingested and normalized within SailPoint as account attributes. These risk insights enrich SailPoint's governance processes, allowing access reviews, certifications, and approvals to dynamically adjust based on each user's current risk level, helping organizations focus on high-risk identities and respond faster to emerging threats.

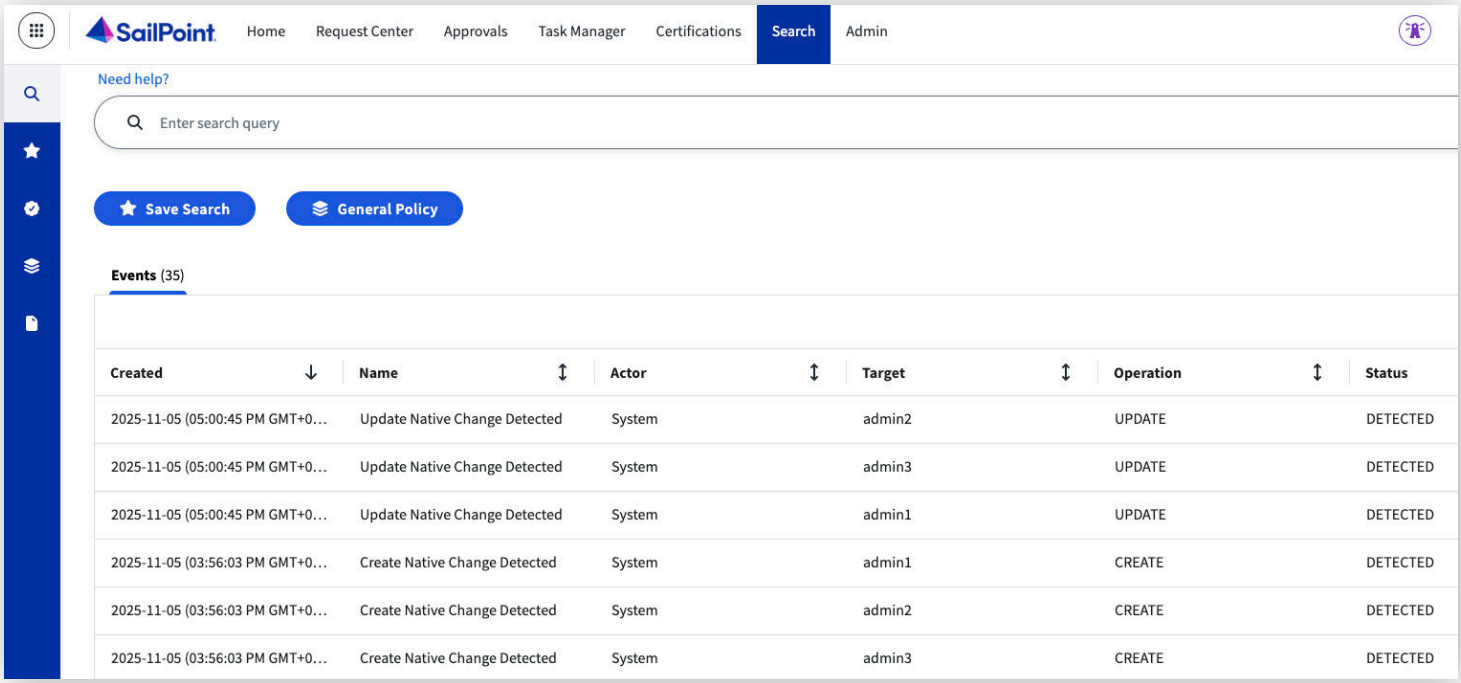
## How Silverfort and SailPoint's integration works

Silverfort evaluates user activity and assigns a dynamic risk level through its API. When risk levels change, the connector retrieves the update and translates it into SailPoint's account model. SailPoint ingests this data as a risk attribute, enabling workflows, approvals, and certifications that adapt in real time.

The integration follows a streamlined wiring pattern. Silverfort's risk attributes are ingested via the connector and mapped to identity attributes within SailPoint's Identity Profile. The scores are normalized into bands: Low, Medium, High, or Critical, to simplify policy logic. When the risk attribute changes, SailPoint triggers workflows using the Identity Attribute Changed event to act on higher-risk users. These workflows can automatically adjust approvals, revoke entitlements, launch certifications, or notify the SOC. SailPoint's Outliers and AI features further monitor risky identities and schedule recurring, risk-based certifications.

This unified approach keeps SailPoint's governance decisions continuously aligned with Silverfort's real-time identity risk intelligence.

## How does Silverfort and SailPoint integration work




Example of SailPoint identity change events ingested by Silverfort via API for real-time risk evaluation and automated response.

## Key benefits

**Risk-aware governance**
Align governance and access decisions with real-time user risk from Silverfort.

**Automated remediation**
Trigger SailPoint workflows to revoke access or alert security when risk increases.

**Context-driven approvals**
Give approvers instant visibility into user risk for smarter, faster decisions.

**Unified visibility**
Combine Silverfort's risk insights with SailPoint's governance data in one view.

## About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.