Silverfort | torq

Silverfort and Torq Integration

Identity is the fastest-moving layer in any attack, and the hardest one to contain once a threat is underway. Security teams see incidents and risk signals as they happen—but responding to them means leaving the tools they already work in.

To respond to identity threats at runtime, security teams need identity incident and risk data automatically routed into their SOAR environment. Silverfort sends live identity threat signals—incidents and risk events—directly into Torq, enabling security teams to move from identity detection to structured, automated response without leaving their existing workflows.

Faster response of identity threats

The Silverfort integration with Torq automatically translates identity threat events into structured Cases and correlated Observables within the Torq platform. Instead of manually monitoring Silverfort for new incidents or risk changes and routing them into response tools, analysts receive structured Torq Cases the moment a Silverfort incident fires — with risk observables automatically linked when they share the same entity.

This enables security teams to automate identity threat response actions such as:

- Receiving a structured Torq Case automatically when Silverfort detects an identity-based incident
- Correlating identity risk events as Observables within Torq, tied to the entities that triggered them
- Linking risk Observables to open Torq Cases automatically when the risk event and incident share a common entity
- Triggering Torq response workflows based on Silverfort incident and risk signals, without manual handoff

By bringing Silverfort's identity threat signals into Torq's case management and automation engine, security teams can respond to identity incidents faster, reduce manual triage, and run consistent response workflows across their environment.

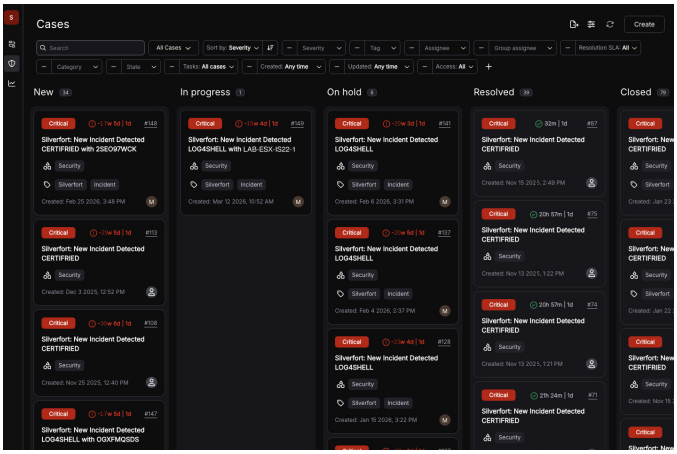
How it works

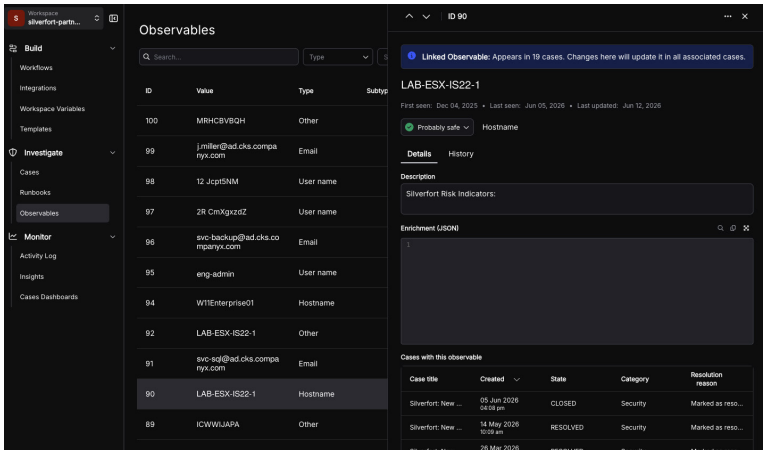
Silverfort sends identity threat events to Torq via real-time integration. When Silverfort detects an incident—such as a brute force attack, lateral movement attempt, or suspicious authentication—it automatically creates a Case in Torq. Silverfort generates a corresponding Observable in Torq, tied to the affected entity. If a risk event's entity matches an open incident's entity, Silverfort correlates the Observable to the Case automatically, connecting risk context to the active investigation.

The integration covers two Silverfort event types—Incidents and Risk—giving security teams continuous visibility into identity-based threats within their Torq environment:

- Receive structured Cases for every Silverfort incident automatically
- Correlate risk Observables to open Cases without manual linking
- Trigger Torq response workflows from identity threat signals
- Cover incidents and risk events across users and service accounts

By routing Silverfort's identity threat signals directly into Torq, security teams gain real-time incident structure, correlated risk context, and automated response—all without leaving Torq.





Key benefits

Structured response from the first signal

Every Silverfort incident automatically opens a Case in Torq, giving responders a structured record to investigate and act on from the moment a threat is detected.

Identity-aware automation

Torq response workflows trigger on Silverfort incident and risk signals, enabling consistent, repeatable response to identity threats without waiting for analyst intervention.

Automatic risk correlation

When a risk event and an incident share a common entity, Silverfort links the Observable to the Case automatically—so analysts see the full identity risk picture without manual cross-referencing.

Unified identity threat visibility

Centralizing Silverfort's incident and risk signals within Torq eliminates manual handoffs between tools, streamlines triage, and keeps response contained within a single workflow.

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across on-prem, cloud, and hybrid environments. We are the first to deliver an end-to-end Identity Security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline and at runtime to stop lateral movement, ransomware, and other identity threats.