Silverfort | SOLARWINDS

# Silverfort and SolarWinds: Identity incidents, routed to your service desk

Available for: *On-prem ITDR*

As organizations build their Identity Threat Detection and Response (ITDR) programs, detection alone is not enough. Every incident needs to reach the right owner, in the system they already work in, with the context required to act. IT service management (ITSM) platforms like SolarWinds Service Desk are where IT and security teams already assign, track, and resolve the work that keeps operations running.

Silverfort extends these workflows by sending its incidents directly into SolarWinds, ensuring that identity threats—like kerberoasting, lateral movement, and brute-force attacks—are not just detected, but raised as tickets, routed to the right owner, and tracked through the service desk your teams already run.

## Turning identity incidents into service desk action

The Silverfort and SolarWinds integration brings identity incidents into the ticketing workflows your teams already run. **Every incident is:**

- Raised as a SolarWinds ticket the moment it's detected, routed to the assignee and queue you've configured
- Enriched with the context needed to triage and act —incident type, priority, and the affected identity
- Synced end-to-end, with the SolarWinds ticket reflecting Silverfort's status as it moves from **open** to **acknowledged** and **resolved**

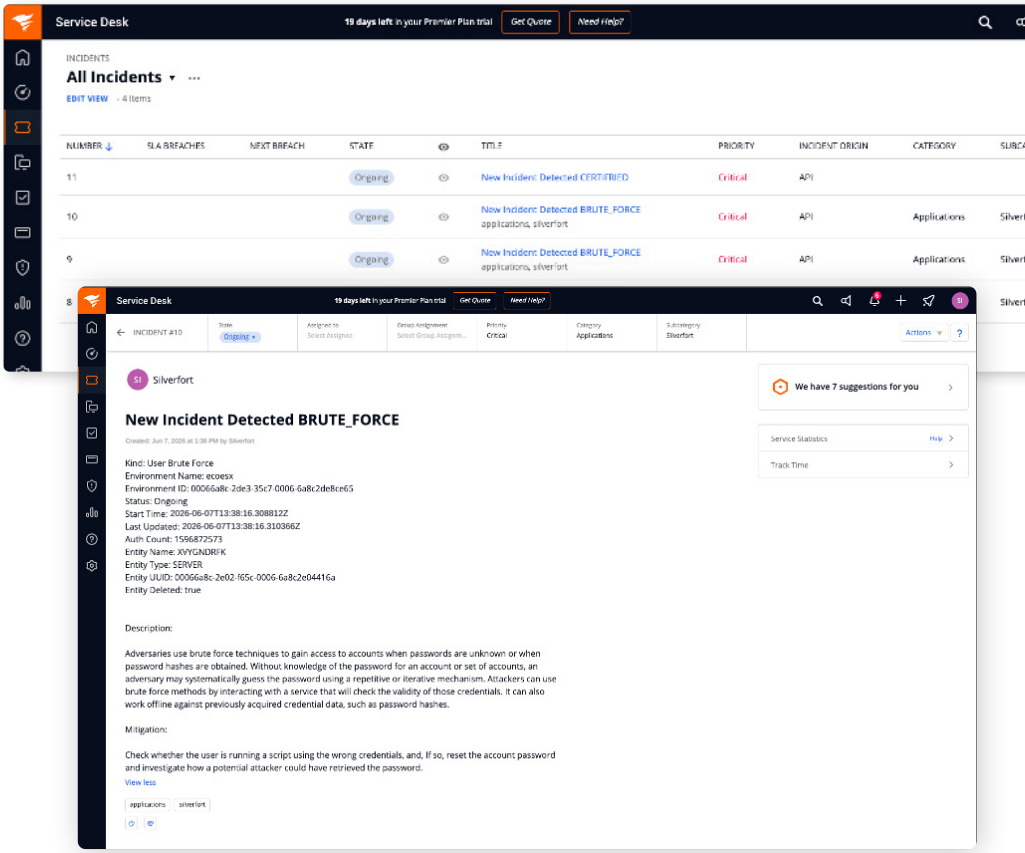
By connecting identity incidents to SolarWinds, you close the gap between detection and response, cutting the time between when an incident is raised and when the right owner acts on it.

## How it works

When Silverfort detects an identity incident, it's raised in SolarWinds automatically—created the moment Silverfort detects it, with no manual steps. Each ticket is assigned to the category, subcategory, and assignee you've configured, so it lands in the right place in the service desk your team already runs.

Silverfort sets each ticket's priority from a mapping you define, matching incident types to SolarWinds priorities like Critical or High so teams can act on the most serious identity threats first.

As the incident progresses, the integration keeps SolarWinds in sync: when Silverfort marks an incident acknowledged or resolved, the SolarWinds ticket reflects the same state—so you keep a single source of truth.




## Key benefits

### Get identity threats into the service desk in real time

Surface identity incidents as SolarWinds tickets the moment Silverfort detects them, so threats reach the right owner as fast as any other ticket your team works.

### Prioritize identity threats by what matters most

Update virtual fencing policies (risk thresholds, protocol scope, allowed sources and destinations) to contain compromised service accounts directly from the response workflow.

### Route identity threats through the processes your team already trusts

Run identity incidents through the categories, assignees, and ownership models already set up in SolarWinds, so identity gets the same accountable response as the rest of your operations.

### Keep identity incident status aligned across tools

Reflect Silverfort's acknowledged and resolved states in SolarWinds automatically, so your team tracks one consistent view.

## 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.