Silverfort | servicenow

Ticket-based remediation for identity threats and exposures

Available for: *Cloud NHI, Cloud ISPM, Identity Graph & Inventory*

As organizations expand their identity security programs across human and non-human identities (NHIs), detection alone is not enough. Every finding needs to reach the right owner, in the right system, with the context required to act. IT Service Management (ITSM) platforms like ServiceNow are where IT and identity owners already manage remediation work across the organization.

Silverfort extends these workflows by connecting identity security findings directly into ServiceNow ticketing, ensuring that identity risks—including posture misconfigurations and NHI exposures—are not just detected, but routed, owned, and remediated through the systems your teams already use.

Turning identity findings into ITSM-ready action

The Silverfort and ServiceNow integration enables organizations to embed identity threat and exposure context into ServiceNow ticketing workflows. Instead of relying on manual processes to hand off security findings between security teams and IT owners, Silverfort ensures that every identity security finding is:

- Routed to the correct owner through ServiceNow
- Enriched with the identity risk context required to investigate and act
- Tracked end-to-end, with exposure status reflecting ticket progress

By tying identity security findings to ServiceNow tickets, organizations close the gap between detection and remediation, accelerating response and strengthening accountability across security and IT teams.

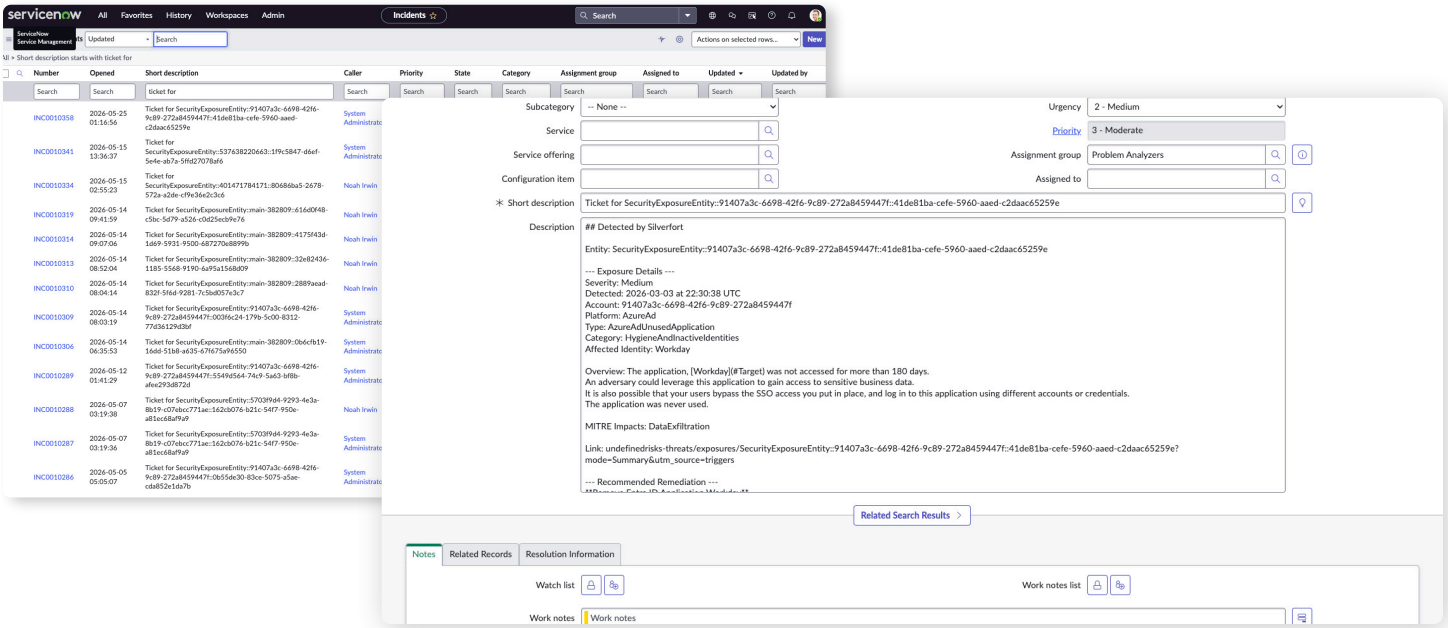
How it works

When Silverfort detects threats and exposures across Cloud NHI, Cloud ISPM, or Identity Graph & Inventory modules, a ServiceNow ticket can be opened directly from the Silverfort platform—manually, through predefined templates, or automatically based on pre-defined rules.

How it works (continued)

Silverfort sends full exposure context to ServiceNow, including the exposed identity, severity, MITRE mapping, affected account, and recommended remediation. The ticket is routed to the designated assignee or assignment group, and the exposure is marked In Progress with a direct link to the ServiceNow ticket.

This ensures every identity security finding is treated as a tracked, owned remediation task—investigated and resolved through ServiceNow without forcing teams to switch tools or duplicate work.



Key benefits

Unified response

Link Silverfort identity risk context directly to ServiceNow tickets, enabling security and IT teams to investigate and act without switching tools.

Predefined ticket templates

Configure default assignees, caller IDs, and assignment groups to enable one-click ticket creation for known exposure types and faster, consistent reporting.

Automated ticketing

Automatically open ServiceNow tickets the moment Silverfort detects identity threats or exposures—no manual steps required.

Operational efficiency

Reduce mean time to respond (MTTR) by embedding identity threat and exposure context into your existing ITSM workflows.

Align identity security with ITSM workflows

Leverage existing ServiceNow processes and ownership models without changing how IT teams receive or work tickets.

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.