Silverfort and SentinelOne: Risk-based policy escalation

As the threat landscape evolves and cyberattacks become more complex, security teams need more integrated and proactive approacAs identity threats evolve, risk can shift faster than static policies can be manually updated to match it. Security teams can see the risk change in real time, but still have to act on it manually, mid-incident.

To close this gap, Silverfort brings live identity and device risk into SentinelOne's policy engine, automatically escalating endpoints into stricter policy groups when risk crosses a configured threshold, and reverting them once it resolves. hes to threat detection and response. With identity now as the entry point to most attacks, adversaries routinely exploit credential-based access to infiltrate environments, evade detection, and move laterally without being noticed.

Automatic endpoint policy escalation, driven by identity and device risk

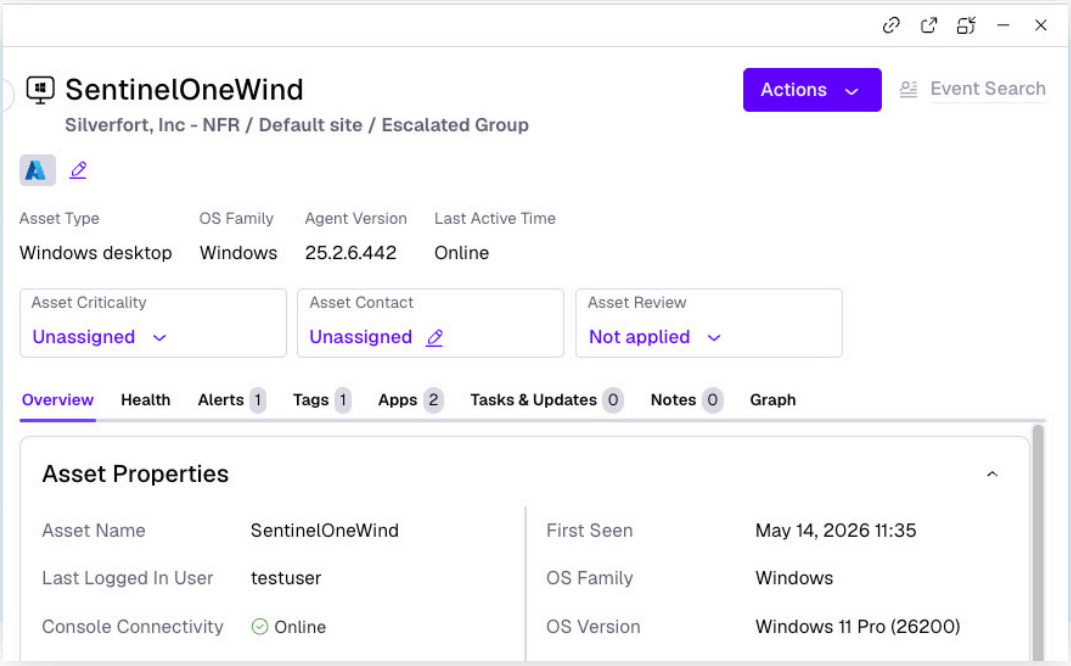
Silverfort integration with SentinelOne enables security teams to keep endpoint policy in step with identity and device risk change, automatically. Instead of pausing to reassign a host's policy as the incident unfolds, SentinelOne policy escalation shifts with risk on its own:

- Escalating a host into a stricter, pre-configured SentinelOne policy group the moment its identity or device risk crosses a configured threshold
- Applying every security control configured for that group as soon as escalation triggers, rather than a single fixed action
- Returning the host to its original policy group automatically once risk resolves, with no cleanup step required

By tying SentinelOne policy enforcement to Silverfort's identity and device risk signals, security teams get endpoint controls that tighten and loosen automatically, without manual policy changes slowing down the response.

How it works

When Silverfort identifies risky behavior, such as lateral movement, credential misuse, or abnormal login patterns, it raises the risk level of the associated host or user. If that risk crosses the configured escalation threshold, the corresponding SentinelOne endpoint moves into a stricter, pre-configured policy group, extending protection beyond the identity itself to every control enforced on the endpoint. Escalation can be driven by identity risk, device risk, or both; if both contributed, the endpoint stays escalated until both have resolved. Once risk falls below the de-escalation threshold, the endpoint returns automatically to its original policy group, so protection scales with the actual threat instead of staying elevated indefinitely.



Key benefits

Automatic policy escalation
Move endpoints into a stricter SentinelOne policy group the moment Silverfort detects identity or device risk crossing a configured threshold, and back once it resolves.

Full policy enforcement, not one action
Apply every control configured for the escalated SentinelOne group at once, for broader containment than a single fixed response.

Continuous policy alignment
Endpoints move between policy states automatically as Silverfort's risk assessment changes, keeping SOC teams focused on investigation instead of manually reconfiguring SentinelOne.

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.