Silverfort and SentinelOne Singularity XDR

As the threat landscape evolves and cyberattacks become more complex, security teams need more integrated and proactive approaches 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.

To counter these threats, Silverfort and SentinelOne Singularity XDR deliver a powerful bi-directional integration that unifies identity and endpoint security. Silverfort adds deep authentication visibility across users, devices, and access protocols, while SentinelOne Singularity XDR platform provides real-time AI-driven endpoint telemetry and behavioral detection. Together, they provide a unified view of identity and endpoint risk for earlier detection, smarter investigations, and faster, coordinated response to identity-driven and post-exploitation threats.

Bi-directional integration for unified risk intelligence

The integration between SentinelOne Singularity XDR platform and Silverfort extends threat detection and response into the identity layer while leveraging SentinelOne's real-time, AI-driven endpoint protection. Silverfort's Identity Threat Detection and Response (ITDR) monitors and enforces security controls across hybrid environments. Meanwhile, SentinelOne delivers real-time behavioral detection and autonomous response across endpoints.

Risk and alert sharing occur in both directions:

RISK SHARING

Silverfort to SentinelOne

Silverfort assigns risk scores to identities and devices, which are reflected on corresponding endpoints within the SentinelOne Singularity XDR platform. These risk indicators can be synced as tags on SentinelOne agents to enable filtering, policy enforcement, and automated response workflows.

ALERT SHARING

SentinelOne to Silverfort

Endpoint alerts from SentinelOne, including detected malware or suspicious process behavior, inform Silverfort's identity risk models, enabling MFA enforcement or temprorary access blocking to prevent lateral movement.

How it works

The Silverfort and SentinelOne Singularity integration connects identity risk with endpoint detection and response, enabling security teams to act faster and with greater precision.

From Silverfort to SentinelOne Singularity XDR

When Silverfort identifies risky behavior, such as abnormal login attempts, lateral movement, or use of compromised credentials, it flags the associated users or devices. These risk levels are shared with SentinelOne, allowing endpoint analysts to immediately see which hosts are linked to high-risk identities. This identity context helps prioritize investigations and trigger appropriate response actions.

From SentinelOne Singularity XDR to Silverfort

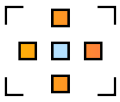
If SentinelOne detects malicious activity on an endpoint, like malware or unusual process execution, it can send that signal to Silverfort. Silverfort then evaluates whether the associated identity should be elevated to higher risk and can take proactive steps, such as triggering MFA or temporarily blocking access to protect resources.

By combining Silverfort's deep identity intelligence and adaptive policy enforcement with SentinelOne's AI-powered endpoint detection and response, security teams gain complete visibility into identity and endpoint risks across their environments. This integrated approach enables earlier detection and containment of attackers, significantly reducing exposure to identity-based threats and ransomware.

Key benefits

Investigate with full identity context
Correlate user authentication activity with endpoint detections for faster, more precise investigations.

Enhanced threat hunting
Link anomalous login behavior to suspicious endpoint activity to improve hunt accuracy.



Lateral movement prevention
Detect and contain identity-driven threats before attackers can pivot across systems or escalate privileges.

Adaptive access enforcement
Apply access policies on risky users by enforcing MFA or blocking users, without disrupting legitimate workflows.

User-centric risk propagation
Automatically apply identity risk across all active user sessions and devices – not just the initially compromised endpoint.

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.