Silverfort & CrowdStrike Falcon EDR

As the threat landscape evolves and cyberattacks become more complex, security teams are facing an urgent need to adopt more integrated and proactive approaches to threat detection and response. With identity now the front door to most attacks, adversaries routinely exploit credential-based access to infiltrate environments, avoid detection, and move laterally without being noticed.

To counter these threats, Silverfort and CrowdStrike Falcon Insight deliver a powerful bi-directional integration that unifies identity and endpoint security. Silverfort adds deep authentication visibility across users, devices, and access protocols, while Falcon Insight provides rich endpoint telemetry and behavioral analytics. Together, they offer a unified view of risk for earlier detection, smarter investigations, and faster, coordinated response to identity-driven and post-exploitation threats.

Bi-directional integration for shared risk intelligence

The integration between CrowdStrike Falcon Insight and Silverfort extends threat detection and response into the identity layer while leveraging Falcon's endpoint visibility. Silverfort's Identity Threat Detection and Response (ITDR) monitors and enforces security controls across hybrid environments. Meanwhile, CrowdStrike delivers real-time endpoint analytics and behavioral detection across devices.

Risk and alert sharing occur in both directions:

RISK SHARING

Silverfort to Falcon

Silverfort assigns risk scores to identities and devices, which are reflected onto corresponding endpoints in the Falcon platform.

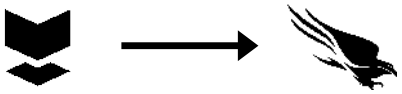
ALERT SHARING

Falcon to Silverfort

Endpoint alerts from Falcon, including detected malware or suspicious process activity, help to inform Silverfort's risk models, enabling dynamic policy enforcement for identity protection.

How it works

The Silverfort and CrowdStrike Falcon Insights integration creates a real-time feedback loop between identity and endpoint layers, so security teams can act faster and more effectively.



From Silverfort to CrowdStrike Falcon

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 Falcon, allowing endpoint analysts to immediately see which hosts are linked to high-risk identities. This additional context helps teams prioritize threats and take swift action.

From CrowdStrike Falcon to Silverfort

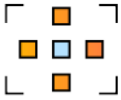
If Falcon detects malicious activity on an endpoint, like unusual process execution or malware activity, it sends that information to Silverfort and Silverfort then evaluates whether the identity involved should be considered higher risk and can take proactive steps, such as requiring MFA or temporarily blocking access.

By combining Silverfort's deep identity intelligence and policy enforcement with CrowdStrike's powerful endpoint telemetry and detection, security teams gain complete, unified visibility into identity and endpoint risks across their environments. This integrated approach empowers organizations to detect and stop attackers earlier in the kill chain, significantly reducing exposure to both identity-based and endpoint threats.

Key benefits

Investigate with full context
Correlate user authentication activity with endpoint and network telemetry for deeper, faster investigations.

Enhanced threat hunting
Link anomalous login behavior to suspicious activity on endpoints for deeper, more accurate threat hunts.



Lateral movement prevention
Detect and contain identity-based threats before attackers can pivot across environments.

Minimal disruption
Apply access policies on risky users by enforcing MFA or blocking users, without interrupting workflows.

User-centric risk propagation
Risk tied to a user is automatically applied to all devices they're logged into, not just the one where the activity occurred.

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.