Silverfort | paloalto NETWORKS

Silverfort & Cortex XDR

To combat the growing threat landscape, Silverfort and Cortex XDR have combined their strengths to deliver a powerful integration that enhances incident monitoring across identity and endpoint layers. Silverfort provides authentication-level visibility and context on top of Cortex XDR's endpoint telemetry to empower organizations with broader visibility, faster detection, and a coordinated response to identity-based threats and post-exploitation activity.

Silverfort and Cortex XDR: Enhancing identity threat investigation

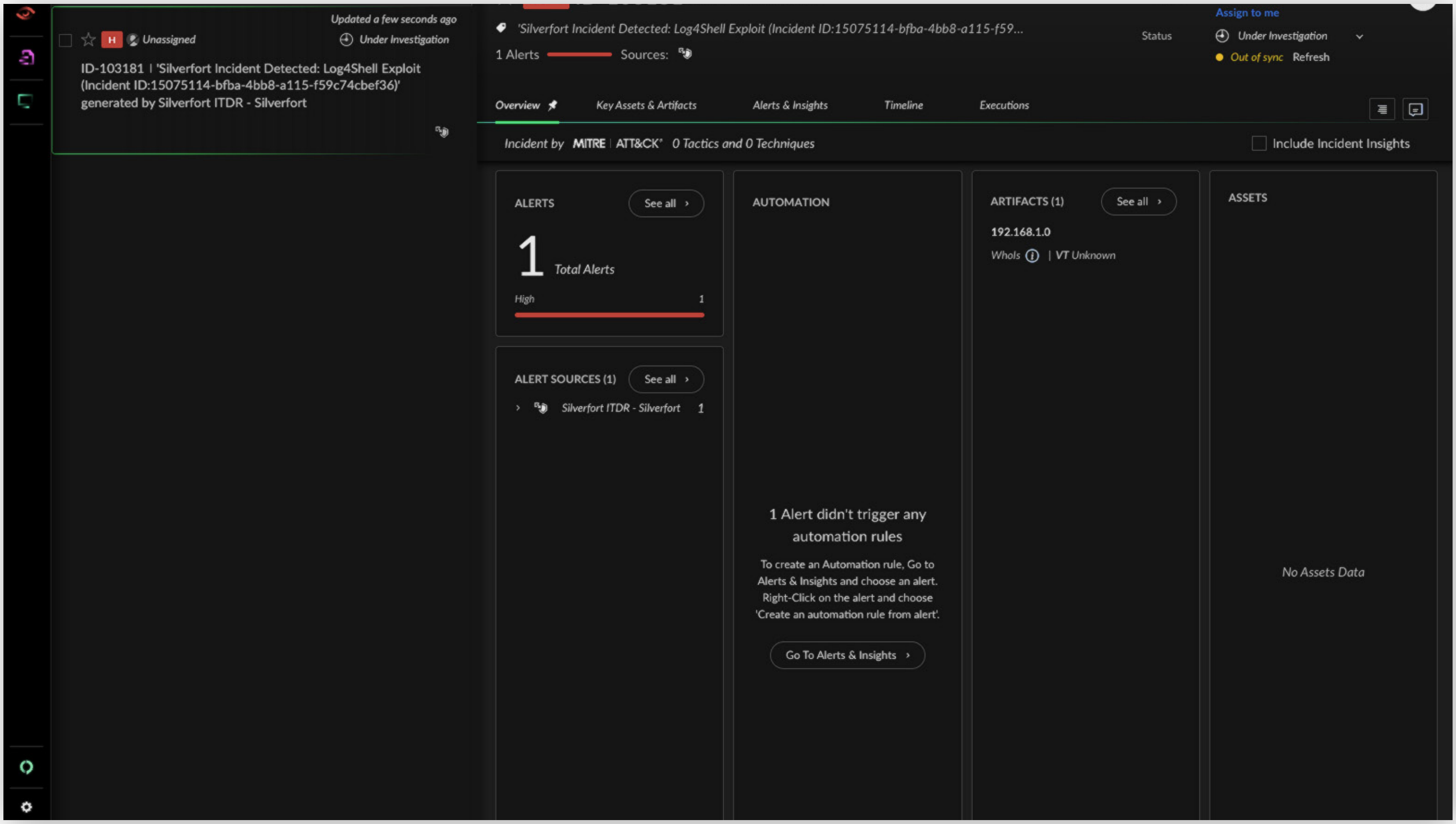
With Silverfort and Cortex XDR's integration, organizations can extend threat detection and response into the identity layer for unified protection across endpoints and authentication systems. Cortex XDR provides real-time analytics and behavioral detection across the environment on the endpoint layer, while Silverfort monitors and enforces access policies across on-prem and cloud identities.

Together, they enhance incident monitoring by ingesting Silverfort's high-fidelity alerts into Cortex XDR, where they trigger incident creation and support end-to-end investigations. When identity-based threats are detected, such as unauthorized Kerberos ticket use, Pass-the-Hash attacks, or excessive authentication failures that may indicate brute force, Silverfort can block access attempts in real time, enabling security teams to contain attacks more efficiently, respond faster, and reduce their overall attack surface.

How Cortex XDR and Silverfort prevent incoming attacks

When Silverfort identifies suspicious authentication activity, such as brute force attacks, lateral movement, or use of compromised credentials, it generates alerts with severity levels and unique identifiers. These alerts are sent to Cortex XDR via API; those marked medium or higher automatically trigger new incidents. As related events unfold, Silverfort continues to update Cortex XDR incidents with relevant context to give analysts a real-time, complete view of identity threats.

This provides organizations with enriched visibility across identity and endpoint data, helping them correlate events, prioritize threats, and accelerate response. By combining Cortex XDR's detection and investigation capabilities with Silverfort's identity intelligence and enforcement, organizations can more effectively contain identity-driven attacks and reduce risk.



Updated a few seconds ago

H Unassigned — Under Investigation

ID-103181 | 'Silverfort Incident Detected: Log4Shell Exploit (Incident ID:15075114-bfba-4bb8-a115-f59c74cbef36)' generated by Silverfort ITDR - Silverfort

'Silverfort Incident Detected: Log4Shell Exploit (Incident ID:15075114-bfba-4bb8-a115-f59...

1 Alerts — Sources:

Status: Under Investigation

● Out of sync Refresh

Incident by MITRE | ATT&CK® 0 Tactics and 0 Techniques

□ Include Incident Insights

ALERTS: 1 Total Alerts — High 1

ALERT SOURCES (1): Silverfort ITDR - Silverfort 1

AUTOMATION: 1 Alert didn't trigger any automation rules

To create an Automation rule, Go to Alerts & Insights and choose an alert. Right-Click on the alert and choose 'Create an automation rule from alert'.

ARTIFACTS (1): 192.168.1.0 — WhoIs | VT Unknown

ASSETS: No Assets Data

Example of a security alert generated by Silverfort with severity and unique ID, sent to Cortex XDR via API for investigation and response.

Key benefits

Prevent lateral movement

Detect and block identity threats that enable lateral movement and ransomware propagation before they escalate.

Enable identity-first response

Surface identity-based threats earlier in the incident lifecycle to drive quicker, more informed response decisions.

Investigate with full context

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

Respond without disruption

Enforce MFA or block access for compromised users without interrupting incident response workflows.

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.