

Accelerate threat detections with Cohesity and CrowdStrike

Consolidate data security insights on anomalies, sensitive data, and threats within your Cohesity data estate into CrowdStrike® Falcon LogScale™.

Key Benefits

- Enhance visibility into sensitive data and threats in your secondary data within the CrowdStrike Falcon platform.
- Consolidate and automate the alert process for data security insights for faster threat detection.

Organizations today generate and distribute data at an unprecedented rate, spreading it across data centers, cloud environments, and edge locations to power application development, analytics, and business operations. However, this widespread data proliferation increases exposure to cyberattacks, as malicious actors look to exploit vulnerabilities or steal valuable information. Backups—often containing critical and sensitive data—have become a prime target for ransomware groups, who seek to impede recovery efforts and extort organizations through ransom payments.

To mitigate these risks, it's essential to gain full visibility into your entire data estate, including secondary data such as backups, files, objects, and analytics environments. A modern data security and management platform with advanced threat detection capabilities enables organizations to identify threat exposure across all secondary data. Automation is critical in transferring detected sensitive data and threats in your secondary data into log management systems, streamlining incident response.

Enrich signals, better correlate events, and spot threats faster

The integration of Cohesity's advanced data security and management capabilities for secondary data with CrowdStrike Falcon LogScale's powerful security logging and rapid detection is designed to tackle modern security challenges. This solution allows Cohesity to push critical security detections for:

- Sensitive data, using AI/ML-powered data classification
- Indicators of compromise (IOCs), file corruption, and other vulnerabilities
- Anomalous changes in data ingestion that could indicate a potential ransomware attack on your primary environment

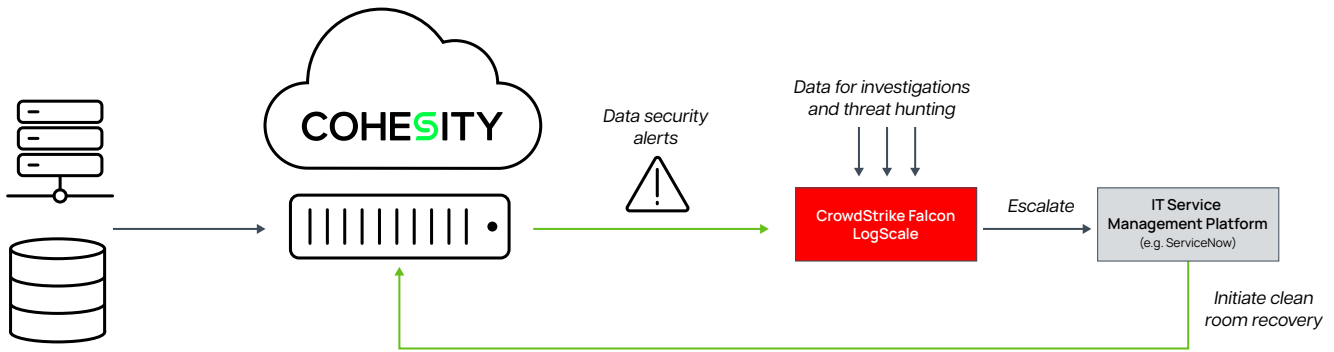


Figure 1: High-level workflow of Cohesity Data Cloud and CrowdStrike Falcon LogScale integration.

Falcon LogScale instantly ingests and aggregates Cohesity telemetry with large log data volumes from other sources, achieving an aggregated view of all relevant security data sources and analyzing and correlating across all of that data within all types of infrastructure. Security teams can investigate and take necessary actions from the CrowdStrike Falcon® platform, including initiating workflows to restore compromised data or workloads to a clean room environment for incident investigation.

Get the integration

Dive deeper into integration and get the technical documentation from the [Cohesity Marketplace](#) and [CrowdStrike Marketplace](#). Use this feature alongside the [latest integration with CrowdStrike Falcon® Adversary Intelligence](#) to enhance threat hunting and response using your secondary data on Cohesity Data Cloud.

To learn more about Cohesity and CrowdStrike security collaborations, visit cohesity.com/crowdstrike.

Operational Benefits

Faster threat detection - With this integration, security teams can quickly store, correlate, and search Cohesity telemetry in Falcon LogScale to identify security issues before they impact your business.

Streamlined IT and security collaboration - The rapid transfer of data from Cohesity to Falcon LogScale accelerates handoffs between your IT backup team and Security Operation Center (SOC) while giving both teams simultaneous access to alerts for faster threat detection.

To learn more about Cohesity and CrowdStrike security collaborations, visit cohesity.com/crowdstrike.

© 2024 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and © is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.