COHESITY | CROWDSTRIKE

Strengthen threat hunting and response with Cohesity and CrowdStrike

Uncover the latest threats and extract intelligence from your secondary data to help level the playing field with adversaries.

Key Benefits

- Improve detection accuracy
- Increase the effectiveness and efficiency of your response
- Manage risk during recovery

Detecting and stopping cyber threats is becoming harder as attackers use more effective methods and quickly adapt their techniques with AI and other advanced technologies. Despite efforts to strengthen their security measures, organizations are often forced into a reactive position when attackers strike, leading to a race against time to confirm the attack, determine the scope of impact, and contain the threat.

To outmaneuver adversaries, organizations need to continuously harden systems while bolstering their early detection, response, and recovery capabilities and tools. This includes using the latest threat intelligence and understanding the adversaries' methods throughout the entire attack lifecycle, enhancing response effectiveness and efficiency and reducing the impact of cyber attacks.

Detect the latest threats in your Cohesity backups

Cohesity's integration with CrowdStrike delivers industry-leading threat intelligence from CrowdStrike Falcon® Adversary Intelligence directly into the Cohesity Data Cloud, allowing you to detect threats with higher fidelity and accuracy. CrowdStrike's world-class threat intelligence telemetry tracks over 250 adversaries—exposing their activity, tools, and tradecraft—while incorporating indicators of compromise (IOCs). With the enhanced threat protection in the Data Cloud, you can scan your secondary data for threats more effectively by integrating default threat intelligence feeds, custom Yet Another Recursive Acronym (YARA) rules, and telemetry from Falcon Adversary Intelligence—all in a single scan.

Configure Falcon Intelligence in the Data Cloud's threat library effortlessly. Use it alone or alongside built-in threat feeds and your YARA rules to detect the latest threats in your Cohesity backups. Review the affected data assets and IOCs detected, and share this information with other security tools to gain a complete picture of the attack and help your organization navigate the response more confidently and with less risk.

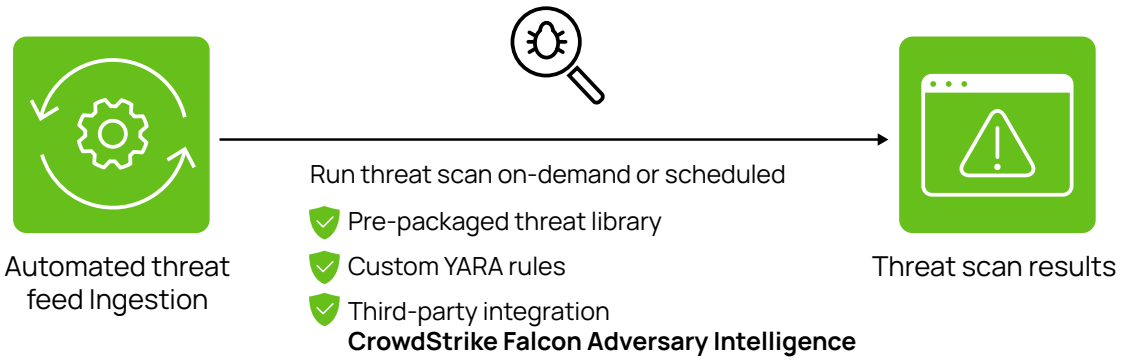

Fig. 1: High-level workflow: First bring-your-own (BYO) threat feed implementation to enhance the Cohesity Data Cloud's threat protection with CrowdStrike Falcon Adversary Intelligence..

Use cases

Ways to leverage Cohesity's enhanced threat protection in your security operations:

Threat hunting - Augment your threat intelligence with industry-leading insights from Falcon Adversary Intelligence to proactively hunt for undetected threats lurking in your Cohesity backups, enhancing your defense strategy. Run threat scans on-demand or on a schedule.

Forensic analysis and response - Detect threats on your secondary data estate across data centers and edge locations using the latest threat intel feeds from CrowdStrike—without being impacted by incident containment activities that may isolate hosts and networks. With Cohesity, you can conduct your investigation passively, ensuring that adversaries cannot detect or disrupt it.

Data recovery - Use the latest threat intel feeds to identify IOCs before restoration, minimizing the risk of re-attack while streamlining the response and recovery process.

Get the integration - Dive deeper into integration and get the technical documentation from the Cohesity Marketplace. Use this feature alongside the existing integration with CrowdStrike® Falcon LogScale™ that helps security teams detect more threats faster and investigate with greater intelligence.

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

COHESITY.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

3000158-001-EN 9-2024