The Wingman for CrowdStrike Falcon

Deterministic second-opinion intelligence that multiplies your Falcon investment

Falcon Sees the Endpoint. File-Borne Threats Don't Stay There.

CrowdStrike Falcon gives SOC teams unmatched behavioral detection and adversary intelligence at the endpoint. But Falcon watches processes, not the full file around them, and retains artifacts for only 30 to 90 days. A file that's unknown at first contact can be gone by the time it's reclassified.

File-borne threats are evolving faster than any single layer can cover alone:

- Malicious npm and PyPI packages slip past behavioral rulesets
- Ransomware variants iterate in days, not months
- Supply chain attacks hide in signed binaries and legitimate-looking installers
- Reclassifications surface weeks or months after Falcon drops the file

Falcon makes the fast call. It needs a second opinion that never forgets.

The Wingman for CrowdStrike Falcon

ReversingLabs Spectra Analyze is a wingman for CrowdStrike Falcon: a second-opinion layer that extends Falcon's reach and never replaces it. Every Falcon detection gets an authoritative verdict from the world's largest threat intelligence database in seconds, curated intel flows back into Falcon automatically, and every file is preserved permanently for retrospective hunting long after Falcon's window closes.

Key Benefits

- Trusted second-opinion verdicts against 450B+ validated samples in seconds
- Secondary IOCs and preemptive block recommendations at the endpoint, proxy, and firewall
- Curated threat intel delivered into Falcon via RL's custom IOC API or via MCP, with no TIP required
- YARA authoring + Retro Hunting pushed back into Falcon via the IOC management API or via MCP
- A permanent file vault for retrospective hunting beyond Falcon's 30–90 day window
- Pre-built integration with setup wizard for fast and easy deployment

How It Works

Spectra Analyze plugs into the CrowdStrike Falcon platform and runs continuously alongside Falcon:

- Spectra Analyze monitors Falcon alerts and automatically retrieves each detected file
- Every file gets a second-opinion verdict against 450B+ validated samples, plus secondary IOCs Falcon didn't capture
- Verdicts and IOCs push back into Falcon in seconds, with no manual lookup required
- Every file is stored permanently in the RL private vault for retrospective hunting and YARA authoring
- New YARA rules and IOCs flow back into Falcon continuously through a direct, agentic MCP connection between Spectra Analyze and CrowdStrike

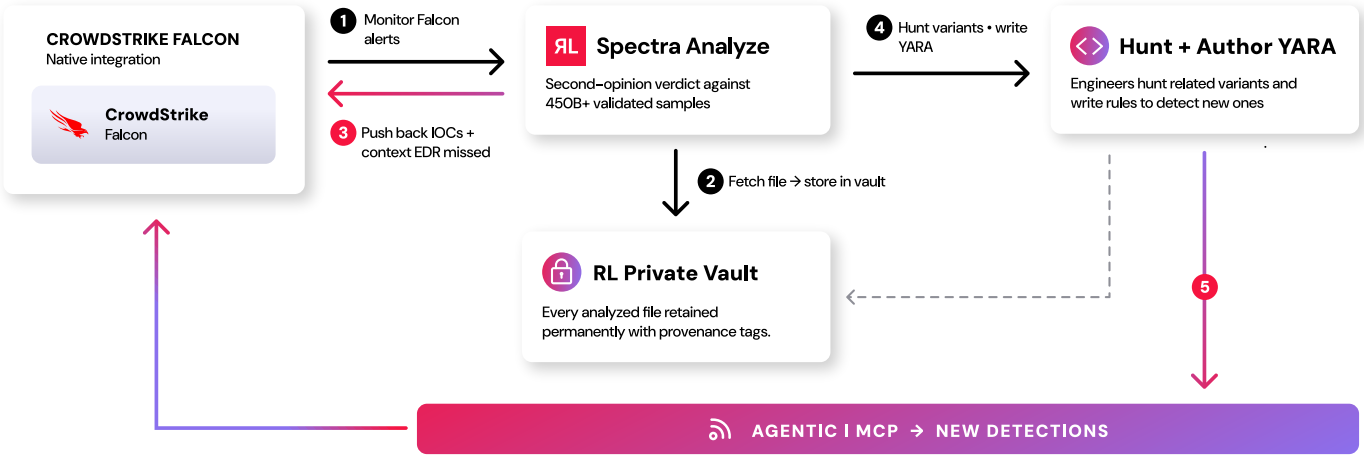

Figure 1. How Spectra Analyze Extends CrowdStrike Falcon

Verify Every Falcon Detection — USE CASE 1

CHALLENGE:
Falcon delivers fast, accurate behavioral verdicts at the endpoint, but a behavioral verdict alone can't confirm everything about the file behind it. SOC analysts triage detections without a second opinion, secondary IOCs, or a way to catch the next variant before it lands.

SOLUTION:
Spectra Analyze runs every Falcon detection through binary analysis, producing an authoritative second-opinion verdict against 450B+ validated samples in seconds. Analysts get secondary IOCs and preemptive block recommendations at the endpoint, proxy, and firewall, so the next variant of an active campaign gets caught before it lands.

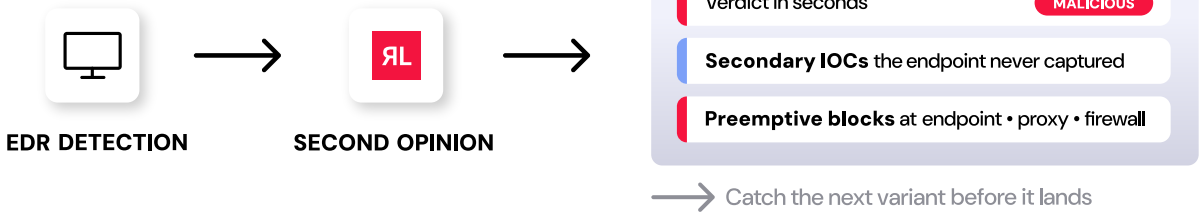

Figure 2. Verify Every Falcon Detection with a Trusted Second-Opinion Verdict in Seconds

Push Proactive Threat Intel into Falcon

USE CASE 2

CHALLENGE:
Curated threat intelligence on ransomware, open-source threats, supply chain attacks, and the latest CVE exploits often lives in a separate TIP, disconnected from Falcon. That gap costs precious time during a fast-moving campaign.

SOLUTION:
ReversingLabs delivers curated IOC feeds directly into CrowdStrike Falcon via the Custom IOC API or via MCP, with no TIP required. Workflow-ready expirations keep Falcon's blocklist current automatically, so protection against breaking threats never lags behind the intelligence.

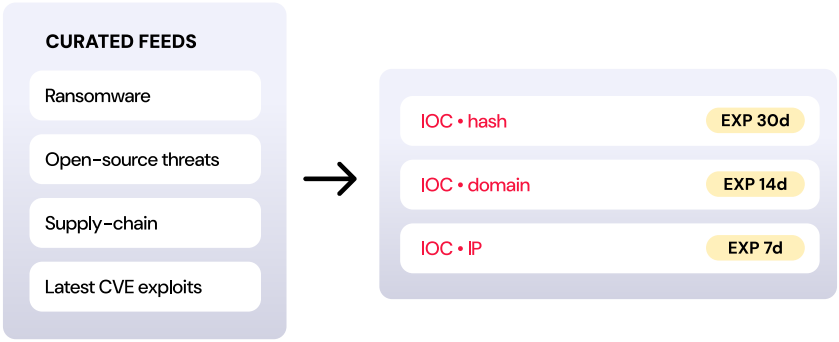

Figure 3. Push Proactive Threat Intel into Falcon via the Custom IOC API

Retain and Monitor Every File

USE CASE 3

CHALLENGE:
Files don't stick around. Most endpoint security platforms, including CrowdStrike Falcon, only retain artifacts for 30–90 days and quarantine the file for even less, so the original sample is gone and secondary IOCs were never captured. If new intelligence emerges beyond Falcon's limited retention window that identifies the file as part of an active campaign, teams won't have a record of the file to hunt backwards.

SOLUTION:
ReversingLabs permanently retains every analyzed file in a private Spectra Analyze instance at no extra cost for storage, enabling teams to quickly re-examine the file and rerun YARA the moment new intelligence emerges, surfacing zero-day reclassifications months later. Organizations get a crucial permanent and complete file record for retroactive hunting that Falcon's endpoint telemetry alone cannot provide.

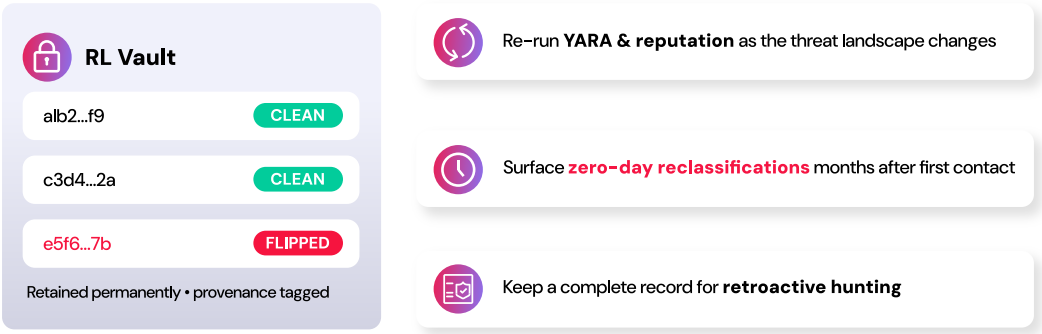

Figure 4. Permanently Retain Every File in a Private Vault

Conclusion

Falcon makes the fast call at the endpoint. ReversingLabs makes sure that call has the full file behind it, with a deterministic second opinion in seconds, proactive intel flowing in continuously, and a permanent vault for the hunts that come later.

It's not another agent competing for the same alert. It's a wingman, built to make Falcon better.

Better Together: Founding Members of the Agentic SOC Alliance

ReversingLabs and CrowdStrike are both founding members of the Agentic SOC Alliance, a coalition of security and AI leaders, including ExtraHop, and over a dozen other innovators, defining the open operating model for autonomous security operations.

It's the same principle behind this integration: outpacing machine-speed threats takes an open ecosystem, not a single vendor. Learn more at extrahop.com/agentic-soc-alliance.

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, RL Spectra Core powers the software supply chain and file security insights, tracking over 450 billion searchable files with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

Get Started!

Experience the ReversingLabs Difference

REQUEST A DEMO

reversinglabs.com

PB-Rev-08.28.26

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com