Optimize Your CrowdStrike Falcon Controls

Reach

Find and Fix Misconfigurations and Activated Unused Security Capabilities

CrowdStrike Falcon

CrowdStrike Falcon is a cloud-native endpoint protection platform that delivers endpoint detection and response (EDR), next-generation antivirus (NGAV), threat intelligence, and automated threat protection across endpoints, servers, and cloud workloads. It helps organizations detect malicious activity and stop threats before they spread.

Key Capabilities

Next-gen antivirus (NGAV) for preventing malware execution

EDR for detecting and investigating suspicious activity

Behavioral detection and threat intelligence for identifying sophisticated attacks

Device control and endpoint hardening capabilities to reduce attack surface

The Configuration Challenge

CrowdStrike Falcon's controls and detection capabilities must be carefully configured and monitored to provide strong protection. Over time, security controls will be changed and drift from security baselines. These misconfigurations can go unnoticed and leave organizations susceptible to attacks.

Common Misconfigurations

Incomplete sensor deployment across endpoints can leave portions of the environment unprotected.

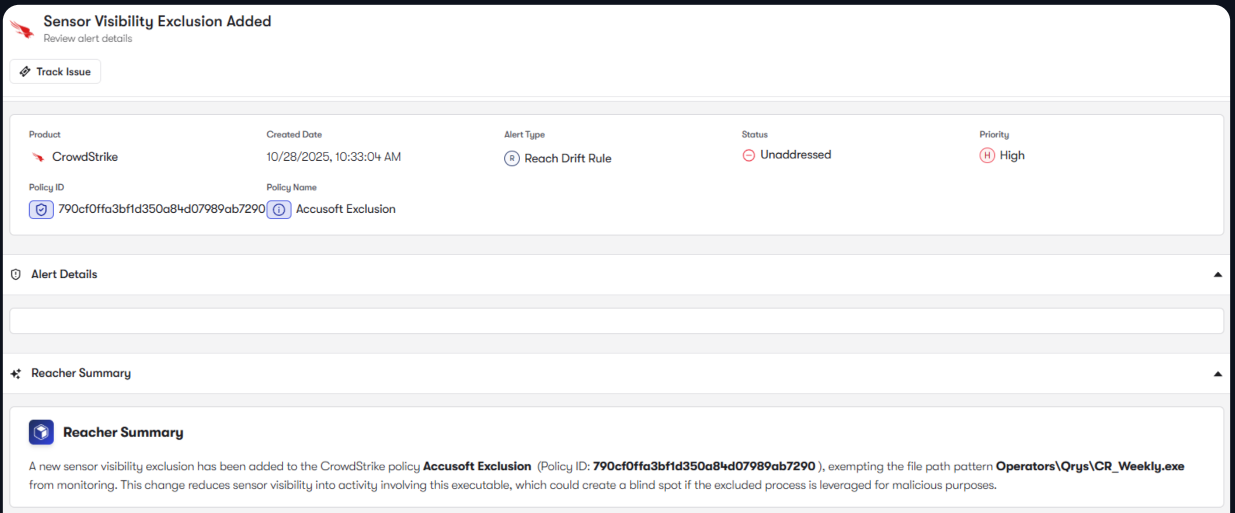
Overly permissive prevention policies or too many exceptions can fail to block malware or suspicious activity.

Disabled or weakened behavioral detections can fail to alert security teams of potentially harmful activity.

Underutilized attack surface reduction features, such as device control and exploit mitigation, can weaken defenses.

Reach Supercharges Your CrowdStrike Security Controls

Reach connects to CrowdStrike Falcon to analyze endpoint protection controls, detection configurations, and deployment coverage. Reach develops a genius-level understanding of how your Crowdstrike Falcon tool is being used (and misused), and then automatically identifies and remediates misconfigurations, activates unused capabilities, stops configuration drift, and validates over time that security posture remains strong.



Sensor Visibility Exclusion Added

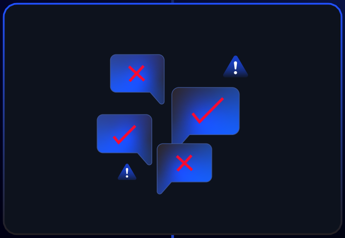
Review alert details

Product	Created Date	Alert Type	Status	Priority
CrowdStrike	10/28/2025, 10:33:04 AM	Ⓡ Reach Drift Rule	⊖ Unaddressed	Ⓗ High

Policy ID	Policy Name
790cf0ffa3bf1d350a84d07989ab7290	ⓘ Accusoft Exclusion

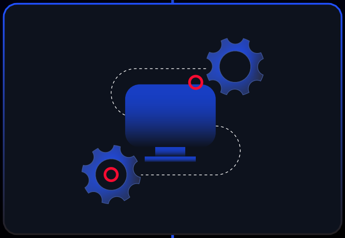
Reacher Summary

A new sensor visibility exclusion has been added to the CrowdStrike policy **Accusoft Exclusion** (Policy ID: **790cf0ffa3bf1d350a84d07989ab7290**), exempting the file path pattern **Operators\Qrys\CR_Weekly.exe** from monitoring. This change reduces sensor visibility into activity involving this executable, which could create a blind spot if the excluded process is leveraged for malicious purposes.



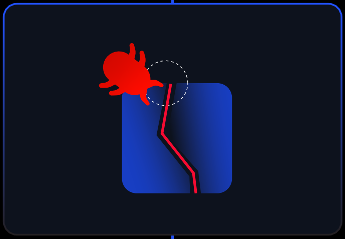
Falcon sensor deployment and version coverage

Reach analyzes endpoint coverage and sensor deployment status and identifies devices without the Falcon sensor – or where sensor tampering prevention has been disabled – so that organizations ensure consistent threat visibility across all devices.



Prevention policy configurations and protection levels

Reach analyzes prevention policies and configuration settings and identifies endpoints operating in detection-only mode, weakened malware blocking settings, or inconsistent prevention policies so that organizations can ensure threats are actively blocked instead of only detected.

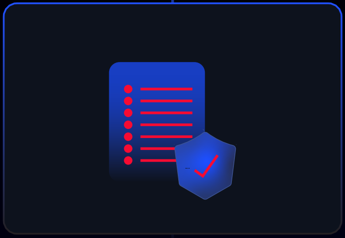


Behavioral detection and threat protection settings

Reach identifies and remediates disabled or weakened behavioral detection configurations (such as a behavioral IOA detection for privilege escalation) so that organizations can improve the platform's ability to detect sophisticated or fileless attacks.

Endpoint attack surface reduction capabilities

Reach alerts you to disabled device controls (such as a USB insertion-triggered scan) or controls that detect common exploitation techniques (to weaken or circumvent application security), and then activates them to stop common attacker techniques.



Policy consistency across device groups

Reach analyzes how Falcon policies are applied across host groups and identifies policy inconsistencies, configuration drift, or misaligned enforcement policies so that organizations can maintain consistent endpoint protection across their environment.

Reach + CROWDSTRIKE

Together, CrowdStrike Falcon and Reach help organizations ensure their endpoint protection platform remains fully deployed, correctly configured, and continuously aligned with security best practices. Organizations benefit from a reduced endpoint attack surface through strengthening endpoint protection policies and consistent enforcement across devices. Security teams can use behavioral protections to block malware and identify advanced attacks. Security teams also gain better visibility by ensuring endpoints are protected and monitored.

Learn More reach.security/connect | Webpage | Demo Video