Defend Your Endpoints With Red Canary + CrowdStrike

red canary + CROWDSTRIKE

BENEFITS

Red Canary now provides our industry-leading detection and response operations using Falcon's EDR data. Together, these solutions enable organizations to take advantage of the broadest possible threat detection coverage, without the burden of investigation and analysis.

1. Detect the broadest array of attacks
2. Eliminate the burden of investigation
3. Extend your security team's capacity and expertise
4. Gain immediate value on Day 1

What's Included	Description	Value
BROADER DETECTION	Combining Falcon's detection with Red Canary's detection engine makes it possible to detect attacker tactics, techniques, and procedures in near real-time	Identify the broadest spectrum of attacker behaviors, techniques, and tools
WORLD-CLASS SECURITY OPERATIONS CENTER	Red Canary's expert analysts accurately and efficiently investigate an average of four thousand potentially threatening events per day	Save time and eliminate the burden of analyzing mountains of data
REPORTING	Red Canary detection reporting provides customers with the necessary context to simplify remediation	Quickly understand the threat and its scope
CLOUD-BASED	Falcon and Red Canary are delivered through SaaS models	Easily deploy across your environment with no additional infrastructure and start seeing value from Day 1
TECHNICAL EXPERTISE	Red Canary's high-touch Technical Account Management (TAM) team provides everything from daily operational support to strategic recommendations	Extend your team's capacity and gain valuable expertise to help improve your security program

red canary + CROWDSTRIKE

HOW IT WORKS

COLLECT

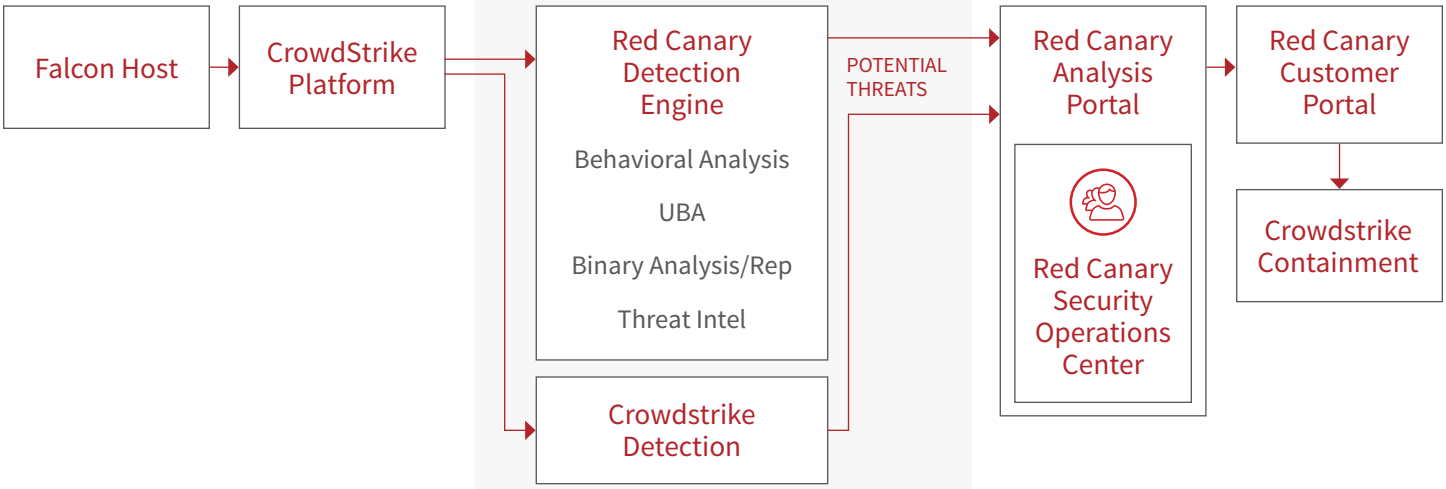
- CrowdStrike Falcon is an endpoint agent that collects low-level endpoint activity.
- The telemetry is sent to the cloud, where it is stored and made available to search.
- Raw telemetry is then forwarded to both CrowdStrike and Red Canary's detection subsystems.

DETECT

- The Red Canary Detection Engine analyzes the raw telemetry to surface potential threats, using broad behavioral analysis, UBA, binary analysis, and threat intelligence.
- Red Canary ingests CrowdStrike detections and treats them as potential threats.
- Together, these technologies provide the broadest possible detection in the industry.

RESPOND

- All potential threats are sent to Red Canary's world-class Security Operations Center for investigation.
- From the web-based UI, customers can drill into process information to do further root cause analysis as required.
- Red Canary TAM provides expert support to guide remediation.



Schedule a demo today

www.redcanary.com/demo-cs