Defend Your Endpoints With Red Canary + Endgame

red canary + ENDGAME.

BENEFITS

Red Canary now provides our industry-leading detection and response operations using Endgame's EPP solution. Organizations can take advantage of the broadest possible threat detection coverage, without the burden of investigation and analysis.

1. Detection, investigation, and response within minutes of activation
2. Configurable behavior-based blocking
3. Stop targeted attacks

What's Included	Description	Value
BROADER DETECTION	Combining Endgame's advanced sensor capabilities 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 CYBER INCIDENT RESPONSE TEAM (CIRT)	Red Canary's expert detection engineers accurately and efficiently investigate thousands of potentially threatening events per day	Save time and eliminate the burden of analyzing mountains of data
REPORTING	Red Canary detection reporting provides the necessary context to simplify remediation	Quickly understand the threat and its scope
CLOUD-BASED	Endgame 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 incident handlers provide 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 + ENDGAME.

HOW IT WORKS

COLLECT

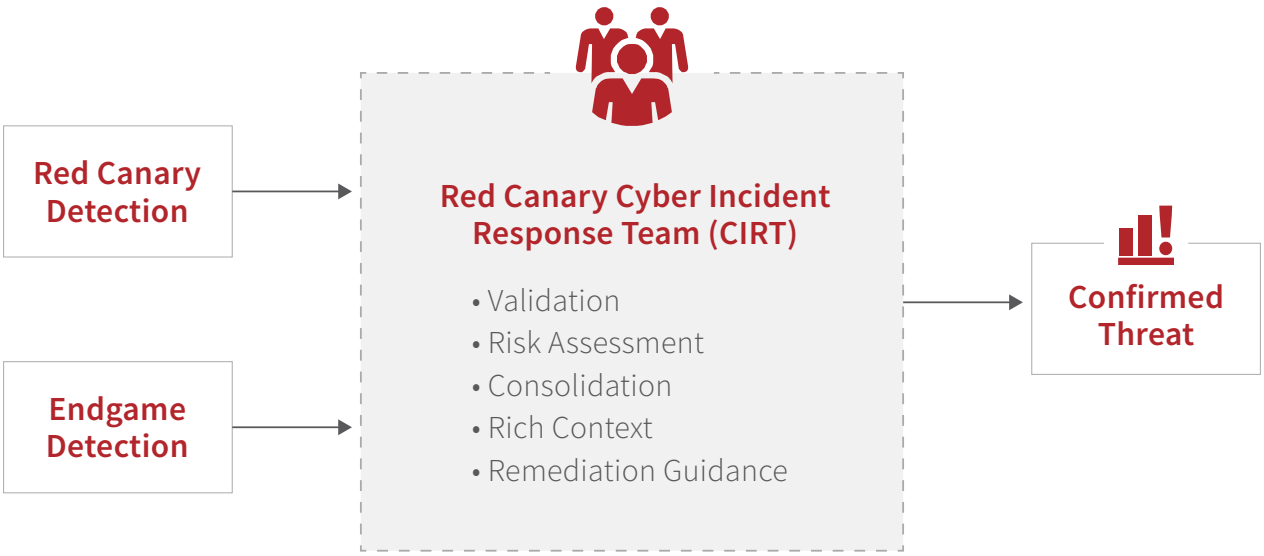
- The Endgame sensor collects low-level endpoint activity.
- Telemetry is sent to the cloud, where it is stored and made available to search.
- Telemetry is then forwarded to both Endgame and Red Canary's detection subsystems.

DETECT

- Red Canary standardizes all data into its internal format.
- The Red Canary Engine analyzes the telemetry to surface potential threats, using broad behavioral analysis, UBA, binary analysis, and threat intelligence.
- Red Canary ingests Endgame detections and treats them as potential threats.

RESPOND

- The Red Canary CIRT investigates and confirms all potential threats.
- Full-context detections are published to your incident response team.
- From the web-based UI, customers can drill into process information to do further root cause analysis as required.
- Red Canary incident handlers provide expert support to guide remediation.



Schedule a demo today

www.redcanary.com/endgame