Secure Your Endpoints

YOUR FASTEST PATH TO STOPPING CYBER THREATS

MANAGED ENDPOINT DETECTION AND RESPONSE

Endpoint Detection and Response (EDR) sensors vastly improve an organization's endpoint visibility, detection, and response capabilities. They are essential for detecting the threats your prevention tools miss.

Yet EDR requires so much more than just the sensor and few organizations can assemble the resources and expertise required for a mature EDR capability.

Red Canary was built to bring endpoint detection and response to every business.

QUICKLY DETECT AND RESPOND TO CYBER ATTACKS:

- Know what's happening on your endpoints
- Eliminate alert fatigue
- Respond to threats within 90 seconds

WHY RED CANARY?

Threat Detection

Red Canary continuously monitors and analyzes your endpoints, users, and network activity in search of threatening behaviors, patterns, and signatures.

Expert Investigation

Red Canary Security Operations Center analysts triage and investigate every potential threat to identify the true threats and eliminate the burden of false positives.

Empowered Response

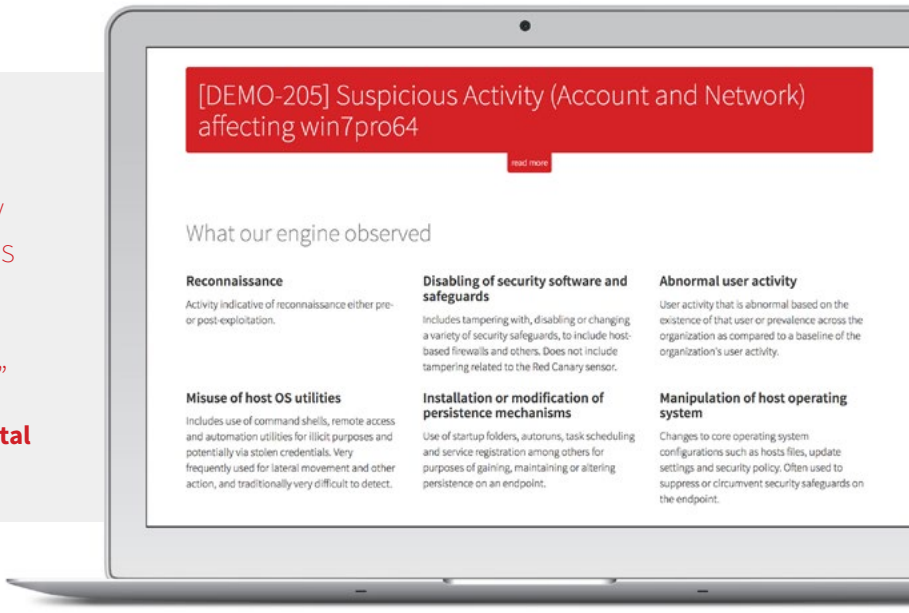
Confirmed detections alert your team and provide detailed and actionable context. Quarantine and rapidly respond regardless of where affected systems are located.

Extend Your IT Security Team

Our team of experts helps you protect your endpoints: threat investigation, false positive removal, early stage incident response, threat research, and infrastructure operations.

"The breadth of Red Canary's detection technology combined with the accuracy of their security operations center means they are a layer of security I can depend on while focusing my security team on securing other parts of my organization."

—Chief Information Officer at a 200+ bed hospital



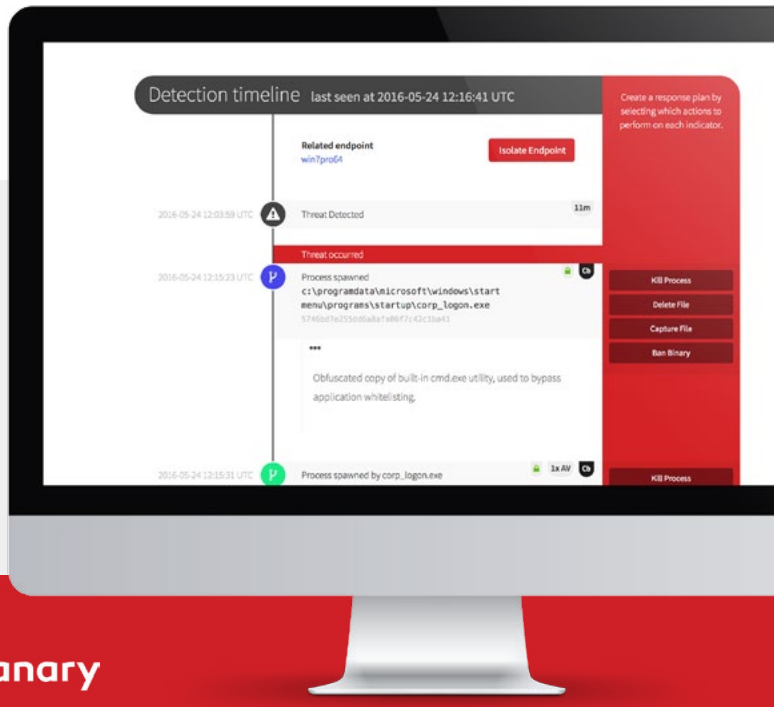
HOW IT WORKS

- **We start by recording all endpoint activity.**
  Our sensor continuously collects file modifications, network connections, registry modifications, process injections, and binary executions.
- **Our detection engine hunts through the activity.**
  Behavioral analysis, user behavior analytics and anomaly detection, and threat intelligence examine all endpoint activity in search of malicious or suspicious behavior.
- **Red Canary analysts triage and confirm threats.**
  Our expert analysts triage every potential threat to confirm actual threats and eliminate false positives.
- **You are immediately notified of the threat.**
  Detections present the intelligence needed to respond: what happened, affected endpoints, involved users, and associated IOCs.
- **You respond to the threat.**
  Remotely quarantine and respond to the threat using our point-and-click automated response tooling.

ACCURATELY DETECTS ATTACKS ACROSS THE KILL CHAIN

- **Attack deployment**
- **Initial intrusion and persistence**
- **Command & control connections**
- **Actions on objectives**
  - Credential access
  - Compromise, reuse, and abuse
  - Expansion and lateral movement
  - Foothold strengthening
  - Data exfiltration
  - Attempts to cover tracks and remain undetected

Defend your Windows, OS X, and Linux workstations, servers, and laptops, whether physical, virtualized, or in the cloud.



red canary

Start securing your endpoints today.

855.977.0686 | sales@redcanary.com | www.redcanary.com

Request Demo

30-Day Assessment