red canary

Endpoint Threat Detection and Response

Red Canary continuously monitors your endpoints, reviews suspicious activity, eliminates false positives and provides actionable detections so you can respond faster.

It's time for a new approach.

Network and signature-based defenses are no longer enough to protect your organization. Malicious actors are constantly bypassing the perimeter, disrupting companies' infrastructure and stealing intellectual property, financial records, and customer information.

Rather than trying to build smarter and more complex defenses, it is time you consider enlisting a new strategy – intelligence driven endpoint monitoring and threat detection.

Why the endpoint?

The most effective way to detect attackers is by watching everything that happens across an organization. Red Canary detects attacks as they are happening, before valuable information can be stolen.

The Red Canary advantage.

- Extensive detection with Red Canary's Threat Detection Engine, which layers best-in-breed detection technologies and techniques.

  Behavioral analysis *Analytics*

  Binary analysis *Threat intelligence*

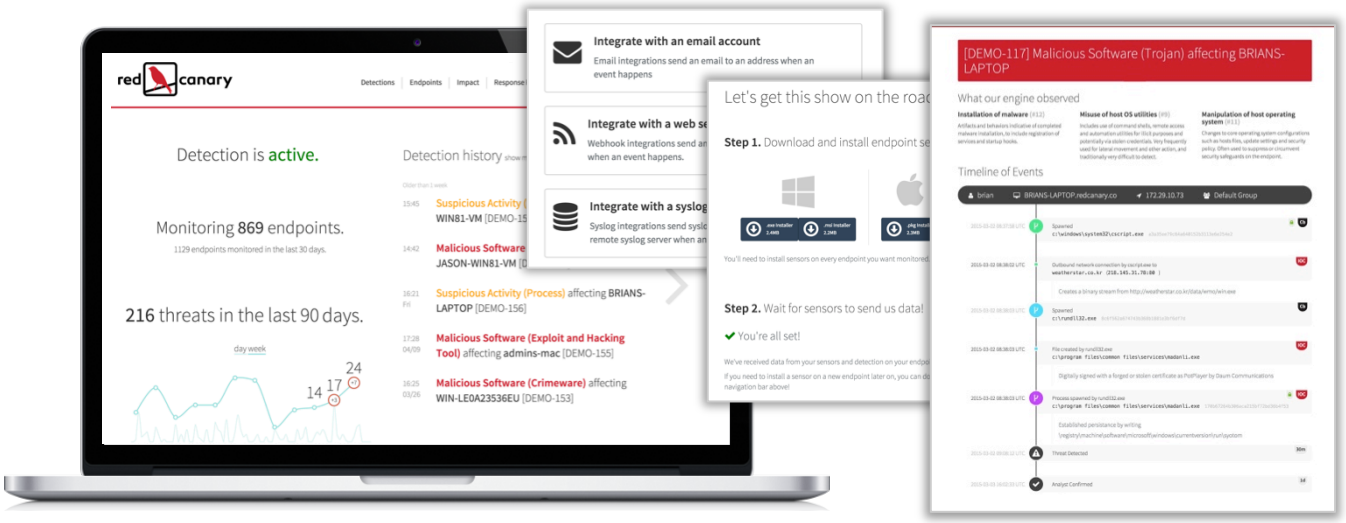
- Accuracy balanced with extensive detection. Analysts review every potential threat flagged by the detection engine so customers get unparalleled detection without the false positives.
- Faster and more effective response with Red Canary's detailed detections and live response capabilities.
- Budget relief by letting companies leverage Red Canary's efficiencies, advanced technology, malware research and expert analysts – for significantly less than building a similar internal service themselves.

We're obsessed with simplifying security.

Deploy in minutes.

No Alert Fatigue.

Respond with power.



Start Your 14-Day Evaluation.

+1 (855) 977 0686

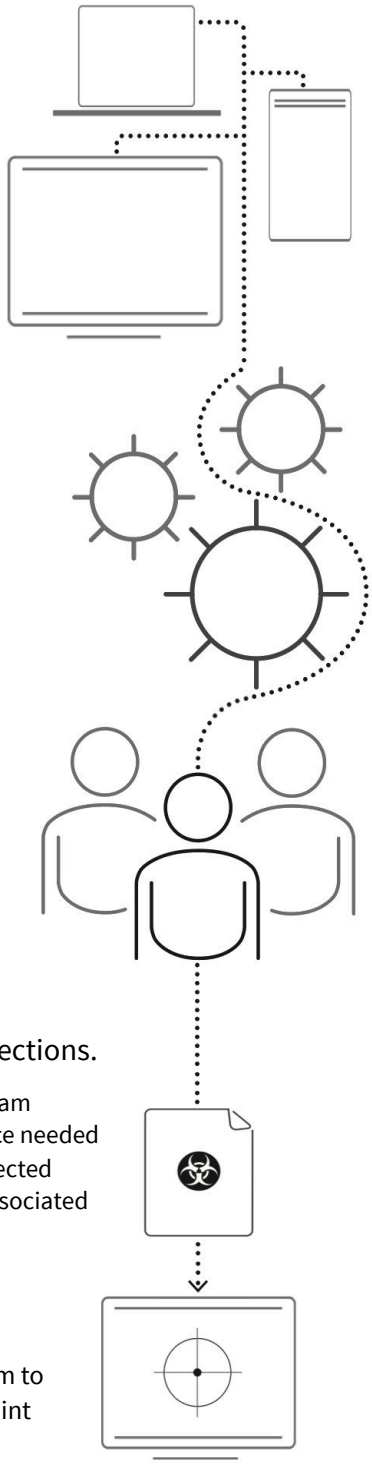
sales@redcanary.co

> *Red Canary addresses a critical gap in enterprise security by providing actionable alerts and valuable security expertise at far less that it would cost to hire a single employee on our own.*
>
> *- Chief Information Officer, Defense & Intelligence Contractor*

How it works

Endpoint sensors monitor activity.

Our sensor continuously streams file modifications, network connections, registry modifications, process injections and binary executions.



Our Threat Detection Engine identifies potential threats.

Behavioral and binary analysis, analytics and threat intelligence examine all endpoint activity in search of malicious or suspicious behavior.

Red Canary analysts confirm threats.

Our expert analysts review every potential threat to confirm actual threats and eliminate false positives.

You receive actionable detections.

Detections alert your security team immediately with the intelligence needed to respond: what happened, affected endpoints, involved uses and associated IOCs.

Respond with power.

Response tools allow your team to remotely quarantine an endpoint and terminate an attack.

Red Canary detects attacks across the attacker's kill chain.

- Attack deployment
- Initial intrusion and persistence
- Command & control connections
- 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 acts as an extension of your IT security team.

- Continually evaluating and deploying new detection technologies and techniques
- Researching and integrating the best threat intelligence feeds
- Hiring top researchers and analysts
- Aggregating and analyzing huge amounts of endpoint data
- Detecting attackers on your endpoints
- Removing false positive alerts
- Providing response intelligence, IOCs, and live response tooling

Red Canary, Inc. | 2531 West 62nd Court, Suite A, Denver, CO 80221, USA | www.redcanary.co