30-day Impact Report

Last updated at 2015-04-07 00:14:39 UTC

Red Canary analyzed **190 thousand executables** and **16 million processes** that executed on your endpoints over the last **30 days.** Our expert threat analysts reviewed **25 thousand potentially threatening events** and alerted you to **8 confirmed threats** that affect **6 of your 436 endpoints.**

The bottom line

Detections 8

"Detections" are threats or breaches Red Canary has detected in your organization and have been confirmed by our expert threat analysts. Every detection includes actionable information about the threat, indicators of compromise, and a "classification" so you know exactly what you're dealing with.

Red Canary detected **8 threats** to your organization that affect **6 of your endpoints.** We alerted your team to these detections through email.

We detected **5 instances of Malicious Software.** These represent significant threats to your organization.

We also detected **3 instances of Unwanted Software.**

63% of these detections represent known malicious software and thus a serious threat to your organization. The remaining Unwanted Software detections represent privacy risks and configuration control gaps that are very commonly exploited by malicious actors.

How we got here

Processes 15,602,859

Red Canary analyzes every process or program that runs across your monitored endpoints and uses our realtime threat detection engine to look for threats using behavioral analysis, advanced analytics, and threat intelligence.

We started by analyzing **15,602,859 processes** that executed across the **436 endpoints** in your enterprise.

Our threat detection engine inspects inbound and outbound network connections, file modifications, child processes, registry changes, and more. Endpoint activity is analyzed with:

- millions of malware signatures,
- our **124 advanced behaviour detectors** ,
- proprietary machine learning and anomaly detection algorithms,
- millions of indicators provided by our threat intelligence partners and
- checked against our own curated list of **1,092,534 currently active indicators of compromise**

Our threat detection engine is instantly updated with indicators whenever we detect a threat so your organization benefits from a threat detected to another Red Canary customer.

Binaries 190,408

Binary analysis is a key pillar of world class threat detection. We use a set of proprietary and third party binary analysis tools, reputation sources, and threat intelligence to look at executables from several perspectives.

We observed **190,408 unique executables or binaries** in your enterprise.

Our threat detection engine uses a variety of techniques including our indicators of compromise, threat intelligence from our partners, and third party reputation services to identify potentially threatening or suspicious applications.

47% of the binaries we observed were unsigned and cannot be attributed to a software publisher. Malicious software generally poses as an unsigned application.

Events 24,663

"Events" are created by when our threat detection engine sees potentially threatening activity and are reviewed by our expert threat analysts and confirmed as a threat or discarded as a false positive.

Our threat engine surfaced **24,663 potentially threatening events,** averaging **822 per day** and **57 per endpoint.** Our threat analysts reviewed **1,542 individual events.**

We expect to review at least **300,030 more events** in the next year, given your current event rate.

What your organization looks like

Endpoints 436

An "endpoint" is one of your workstations, laptops, or servers that has our sensor installed and is being monitored around the clock.

We monitored a total of **436 endpoints.**

99% of your endpoints did not produce any detections. [redacted] was the most affected endpoint with **3 detections.**

The most common operating systems in use are **Windows 7 Service Pack 1, 64-bit (507) and Windows Server 2008 R2 Standard Edition Service Pack 1, 64-bit (78).** The least common is **Mac OSX 10.9.5 (1).**

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*

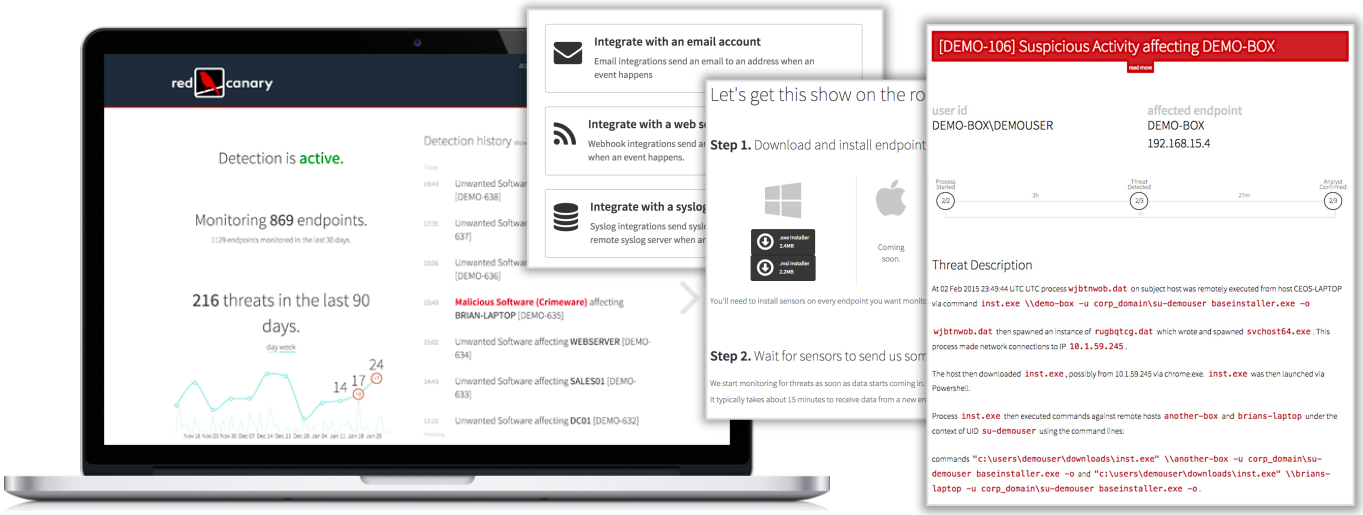
- Accuracy balanced with extensive detection. Analysts review every potential threat flagged by the detection engine so customers get unparalleled detection without the false positives.
- Faster and more effective response with Red Canary's detailed detections and live response capabilities.
- Budget 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.

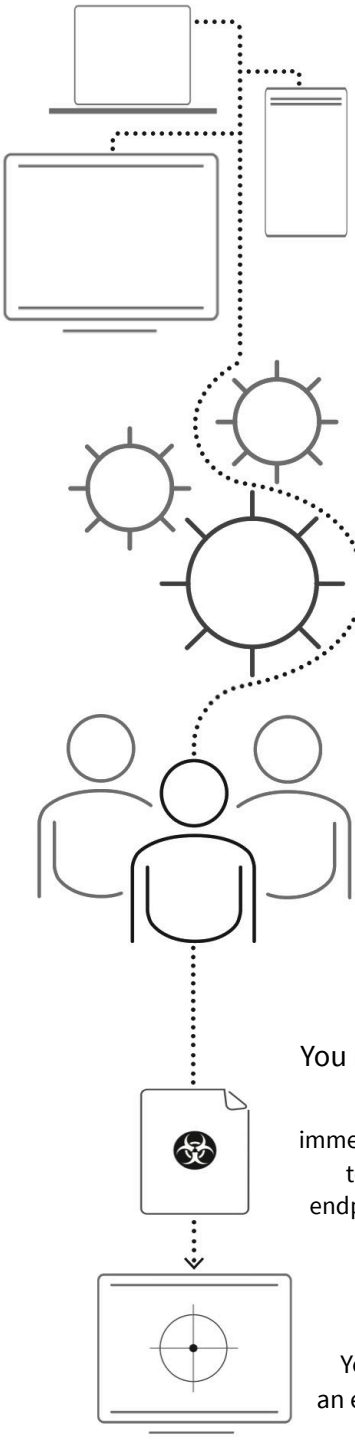
Deploy in minutes.

Easily integrate into your workflow.

Understand everything.



How it works:



The endpoint sensors monitor activity.

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

Our Threat Detection Engine identifies potential threats.

Behavioral and binary analysis, analytics and threat intelligence are used to 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.

You respond to threats.

Your team can 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

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 malware researchers and analysts
- Aggregating and analyzing huge amounts of endpoint data
- Detecting attackers on your endpoints
- Removing false positive alerts
- Providing response intelligence and IOCs

"*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.*"

- CIO, Defense & Intelligence Contractor

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

red canary