red canary

CASE STUDY

Closing Critical Gaps in the Defense Industrial Base

Industry

Defense Industrial Base, *Washington D.C.*

Security Challenge

Customer had recently been the victim of a targeted attack and needed comprehensive endpoint detection at an affordable price.

Solution

Red Canary's Managed Endpoint Security Service

Key Benefits

- *Extensive threat detection*. Best-in-breed technologies and techniques detect threats throughout the entire lifecycle – from initial intrusion through exfiltration.
- *Empowered and expedited response.* Red Canary provides the tools and live response capabilities needed for complete and timely response.
- *Breakthrough economics*. At a third the cost of a single security engineer, Red Canary showed a positive ROI from day one.

Summary

A leading midsize United States Defense Industrial Base (DIB) organization deployed Red Canary to its unclassified endpoints following a successful targeted attack. Since deployment, Red Canary's threat detection and response service has helped protect the organization from a significant number of external and internal threats.

The Problem

A midsize United States DIB organization was the victim of a targeted attack. An incident post-mortem determined that targeted attacks would continue and a comprehensive endpoint security solution was needed to complement existing security investments.

The Solution

Red Canary's threat detection and response capabilities fill a critical gap in the organization's defenses. The organization deployed Red Canary to its unclassified endpoints and addressed several security gaps:

- Detection of malicious software that bypassed existing network and endpoint controls and safeguards
- Detection of suspicious system activity including insider threats

During the past 12 months, Red Canary detected an average of 20 threats per 100 endpoints, including:

- Malicious software that successfully bypassed mail gateways and web content filtering
- An insider threat event that would have seriously harmed the business's brand and ability to retain existing contracts
- Systems mistakenly placed into service without using approved baseline images

The Red Canary endpoint security operations center removed 3,400 false positive alerts per 100 endpoints in the past 12 months, allowing the organization to focus on legitimate threats. At a third the price of a single employee, Red Canary returns a positive ROI every year for the organization by allowing it to grow without having to increase security head count.

The Details

The organization in this case study had a strong security posture, with a dedicated team managing the following tools and processes:

- Firewalls
- Web content filtering
- Mail gateway services
- Access control to the internal network, brokered by a Network Admission Control (NAC) system
- Endpoint anti-virus
- Endpoint anti-exploitation software
- Endpoint imaging protocols
- Centralized endpoint and network monitoring

The organization employed full-time incident responders as a part of their well-staffed IT department, but they did not operate a formal security operations center. As a security-conscious organization, the IT and corporate security departments coordinated closely on threat identification, communication, and technical security safeguards.

Despite industry-standard staffing profiles, targeted attackers breached the organization, and as a result burdened it with the pace and cost of traditional incident response. Days were spent imaging endpoints, collecting and correlating log events, and obtaining binary samples that had not been thoroughly deleted.

Following the incident, the organization deployed Red Canary to protect its unclassified endpoints. In one year of deployment, Red Canary helped the organization defend its endpoints against over 80 cases of malware breaching network defenses on the perimeter, suspicious activity, and unwanted software.

The organization now benefits from Red Canary's extensive threat coverage including detection of costly advanced attacks and misuse of legitimate accounts. Red Canary helps the organization quickly and effectively expel attackers from its endpoints – at a cost of less than a third of a single security engineer.

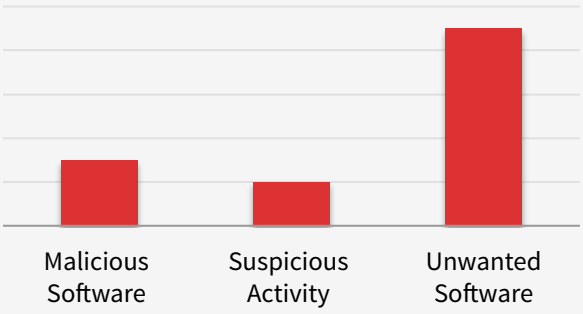
Interested in learning how Red Canary can help defend your endpoints? Contact us at info@redcanary.co to schedule a demo.

After 12 Months of Red Canary – A Snapshot

3,400 false positives eliminated by the Red Canary analysis team per 100 endpoints

20 threats detected per 100 endpoints

Detected Threats by Classification



Cumulative Threats Detected