CASE STUDY DEFENSE

Closing Critical Gaps in the Defense Industrial Base

CHALLENGE

Targeted attackers successfully breached the organization.

REQUIREMENTS

The organization needed to address gaps in their security by finding comprehensive endpoint detection at an affordable price.

SOLUTION

Red Canary helps the organization quickly and effectively expel attackers from its endpoints – at less than a third the cost of a single security engineer.

SNAPSHOT

A leading midsize United States Defense Industrial Base (DIB) organization became the victim of a targeted attack. Its security team knew it needed a security solution that could accurately detect advanced attacks bypassing other security tools. Red Canary helped the organization continuously monitor endpoints, detect threats, and respond to advanced attackers.

BETTER SECURITY AT AN AFFORDABLE PRICE

The organization now benefits from Red Canary's extensive threat coverage that encompasses detection of attacks from initial installation all the way to data exfiltration. Red Canary helps the organization quickly and effectively expel attackers from its endpoints and network. 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 headcount.

12-MONTH RESULTS

80+	threats detected that bypassed existing security tools and processes
3,400	false positives eliminated per 100 endpoints
1/3	the cost of a single security engineer

red canary

"Red Canary helps quickly and effectively expel attackers. At a third the price of a single employee, Red Canary returns a positive ROI by allowing the organization to grow without having to increase security headcount."

— Chief Technology Officer

DIGGING DEEPER

Security Profile: Tools & Processes

The organization had a strong security posture prior to the incident, with a dedicated team managing:

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

Staffing & Resources

The organization employed a full-time incident responder 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.

A Costly Breach

After the defense contractor was breached, days were spent imaging endpoints, collecting and correlating log events, and obtaining binary samples that had not been thoroughly deleted. An incident post-mortem determined that targeted attacks were only going to continue and a comprehensive endpoint security solution was needed to complement existing security investments.

Red Canary Adds a Layer of Defense

The organization deployed Red Canary to its unclassified endpoints and addressed several security gaps. In one year of deployment, Red Canary helped the organization defend its endpoints against dozens of threats before they became breaches, including:

- Malicious software that 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