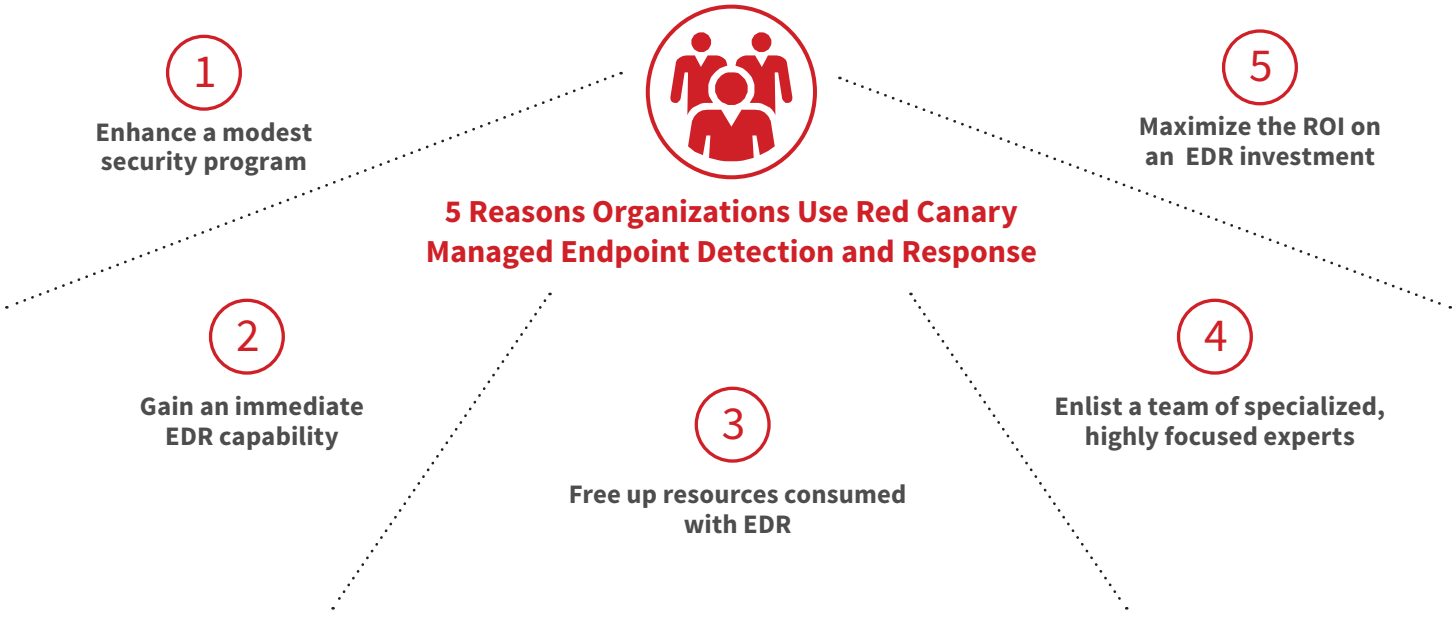
5 Reasons Organizations Outsource Security to Red Canary

Every organization needs to detect new threats and immediately respond. But few can assemble the resources and expertise. Red Canary was built to bring Fortune 100 threat detection and response to organizations of all sizes and security maturity levels.



"The CISO's problem is never finding enough tools to purchase. And it's not that they can't find the right tools. CISOs can't find the right people, and without the right people you can't build effective security operations."

- Keith McCammon, Red Canary Chief Security Officer

red canary

1 ENHANCE A MODEST SECURITY PROGRAM

A small defense contractor with a limited security program needed to make a strategic investment that would not require additional time or resources.

Industry:	Endpoints:	Employees in IT:	Information security team:
DEFENSE	200	< 5	= 0

CHALLENGE

An onsite government contractor with limited infrastructure and staff needed advanced information security that minimally increased overhead costs. The organization's small IT team managed a modest unclassified infrastructure environment and protected its endpoints with antivirus and a firewall. However, threats continually slipped past its preventative tools and the organization knew it needed an additional layer of defense.

SOLUTION

Red Canary helps the organization significantly improve its daily security operations, delivering a complete EDR capability with endpoint threat detection, investigation of potential threats and removal of false positives, and response support. The lean organization was able to tap into a full endpoint Security Operations Center with threat analysts, researchers, data scientists, forensics experts, and incident responders—all at approximately a quarter of the salary of an employee.

---

2 GAIN AN IMMEDIATE EDR CAPABILITY

A small team with solid security controls wanted to improve their security with EDR but knew they would not be able to manage it.

Industry:	Endpoints:	Employees in IT:	Information security team:
MANUFACTURING	3,000	< 5	= 0

CHALLENGE

The industrial manufacturer needed visibility into their endpoints to safeguard valuable IP. But with only two employees running security and IT for thousands of endpoints, the team knew they would not be able to effectively implement and manage the high volume of data and alerts an EDR product would deliver.

SOLUTION

Red Canary delivered the organization a fully operational EDR capability on day one. A team of Red Canary threat analysts continuously monitors endpoint activity, investigating potential threats and reporting confirmed malicious activity. The manufacturing organization only needs to focus on legitimate threats and can use the tools and intelligence included in Red Canary detection reports to quickly respond to every threat. They get a full EDR capability and dedicate almost no internal time and resources.

3 FREE UP RESOURCES CONSUMED WITH EDR

A mid-sized medical center implemented EDR and lacked the time to improve detection criteria, investigate every alert, and respond to confirmed threats.

Industry: HEALTHCARE

Endpoints: 7,500

Employees in IT: 150

Information security team: = 5

CHALLENGE

The medical center had implemented an EDR product to get better visibility into its endpoints and defend against evolving threats. But the security team found that managing EDR alongside all its other daily operational tasks was extremely difficult. Inundated with 100,000+ alerts and binaries that needed to be investigated, the in-house analyst was only able to devote time to a limited number of alerts, leaving uncertainty about what might have been missed.

SOLUTION

Red Canary saves the medical center 100+ hours of in-house security time per month and has enhanced security operations. With Red Canary taking over management of endpoint detection and response, the medical center's security team can focus on other parts of the security program. The organization trusts Red Canary to thoroughly analyze its environment and pinpoint the threats that require immediate action.

4 ENLIST A TEAM OF SPECIALIZED, HIGHLY FOCUSED EXPERTS

A global investment firm needed visibility across its endpoints but did not want to hire or train a specialized staff.

Industry: FINANCIAL

Endpoints: 3,600

Employees in IT: 250

Information security team: = 8

CHALLENGE

With over 3,000 endpoints across 30 countries, the financial investment firm's network was large, distributed, and vulnerable. Their endpoint security solution was burdensome to the business and IT department, and threats continued to slip through. The CISO wanted to implement EDR, but recognized his team's expertise sat in other security disciplines. He did not want to hire and train a new team and knew his existing team would not have the time to learn a new product.

SOLUTION

With Red Canary, the firm gained a team of endpoint experts without having to staff up internally. The Red Canary SOC quickly detects and validates each threat, and the firm's security team has the reporting and tooling they need to limit dwell time and eliminate threats. The firm relies on Red Canary's experts to tell them about the threats that every other security product has missed.

5 MAXIMIZE THE ROI ON AN EDR INVESTMENT

A team with advanced security controls needed a partner to help them safeguard sensitive financial information.

Industry: BANKING

Endpoints: 3,300

Employees in IT: 100

Information security team: = 10

CHALLENGE

The bank's security team had already invested in application whitelisting and EDR to secure its endpoints. The whitelisting solution succeeded in defending against the vast majority of attacks but the EDR product sat mostly idle. Penetration testing showed that gaps remained. The team knew that to get the most value out of EDR, they needed experts constantly watching endpoint activity and identifying threats slipping past other security controls. A team they did not have.

SOLUTION

Red Canary gives the bank the visibility and detection coverage they need to feel confident that advanced attacks are not being overlooked. The bank's internal red team tested Red Canary thoroughly and the solution detected each attack launched, the majority of which did not use malware and exploited native operating system tools like PowerShell. Red Canary helped fill a critical gap by offering the ideal combination of advanced detection technology coupled with a security team of experts in endpoint activity, forensic investigations, and threat hunting.

IN THEIR OWN WORDS

"Red Canary analysts effectively double or triple the staff available to triage our alerts, incidents, and concerns. This frees up a tremendous amount of time so we can do proactive rather than reactive work."

- IT Security Manager, Mid-Sized Medical Center

"At a quarter the price of a single employee, Red Canary returns a positive ROI by allowing our organization to grow without having to increase security headcount."

- Chief Technology Officer, Defense Organization

About Red Canary

Red Canary delivers effective security operations to organizations around the world, ranging from 100-person companies to Fortune 500 enterprises. The Managed Endpoint Detection and Response (MEDR) solution quickly and accurately identifies threats on customers' endpoints and helps stop attacks before they result in breaches. Every threat is investigated by a Red Canary Analyst to remove false positives and provide the context required for remediation.

See how Red Canary can help you secure your endpoints.

855.977.0686 | info@redcanary.com | www.redcanary.com