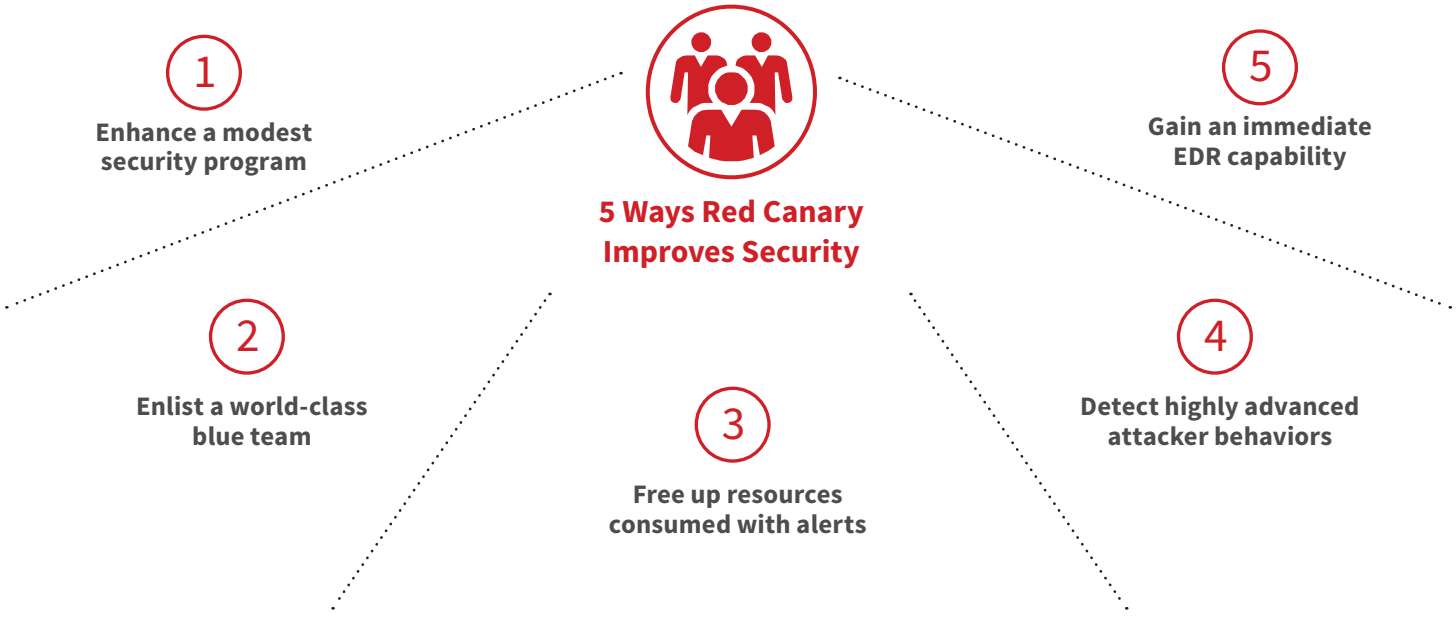
5 Reasons Organizations Rely on Red Canary to Improve Their Security

Every organization needs to prepare for, identify, and eradicate threats. But few can assemble the resources and expertise. Red Canary empowers security teams of all sizes and maturity levels to win against modern adversaries.



"Red Canary helps us defend against many different types of threats and gives us a level of visibility that we previously never had. They are a foundational part of my security program."

- Chief Technology Officer, Investment Firm

red canary

1 ENHANCE A MODEST SECURITY PROGRAM

A global law firm needed to improve its security program to protect high-profile client data against attacks.

Industry: LEGAL

Endpoints: 2,500

Employees in IT: 100+

Information security team: = < 5

CHALLENGE

The firm had basic security tools like antivirus and firewall in place, but the bulk of its controls were focused on meeting compliance regulations rather than improving security. When a new Director of Information Security joined the firm, he recognized the need to quickly improve the organization's security program. Sophisticated and commodity attacks could easily bypass the firm's existing tools without anyone knowing.

SOLUTION

The Director had previously partnered with Red Canary and was impressed with the team's deep security expertise. Deploying Red Canary enabled the firm to quickly level up its security program and get results on day one. Benefits included visibility across endpoints, continuous hunting and threat detection, investigation of every potential threat, and remote remediation tooling. The Director gained confidence that sensitive client data was secured against even the most advanced attacks.

---

2 ENLIST A WORLD-CLASS BLUE TEAM

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 continuous endpoint monitoring, but recognized that building a sophisticated blue team with 24/7 coverage would be costly and time-consuming.

SOLUTION

With Red Canary, the firm gained a team of experts without having to staff up internally. The Red Canary Cyber Incident Response Team 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 to tell them about the threats that every other security product has missed.

3 FREE UP RESOURCES CONSUMED WITH ALERTS

A mid-sized medical center lacked the time to investigate the flood of alerts raised by its endpoint security products 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 endpoint detection and response (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 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 DETECT HIGHLY ADVANCED ATTACKER BEHAVIORS

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 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.

5 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: MANUFACTURING

Endpoints: 3,000

Employees in IT: < 5

Information security team: = 0

CHALLENGE

An industrial manufacturer needed visibility into its 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. Red Canary's Cyber Incident Response Team 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.

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

"There is a level of impact you can make with automation, but you'll never get to the scale of a partner who sees across multiple environments. We would have had to hire more people or sacrifice quality. You can't have it all—unless you partner with Red Canary."

- Lead Infrastructure Security Engineer, Technology Company

About Red Canary

Red Canary defends hundreds of organizations around the world, with customers ranging from global Fortune 100s to 100-endpoint organizations. Our cloud-based service levels the playing field for businesses of all sizes by empowering every security team to win against rapidly evolving adversaries.

See how Red Canary can help you improve your security.

www.redcanary.com