red canary + Carbon Black.

# 5 Reasons Organizations Choose Red Canary + Carbon Black Response

Not all Carbon Black partners are equal. Learn why organizations rely on Red Canary to extend their team's capacity, gain deep EDR expertise, and cut threat detection and response time.

**5 Reasons Organizations Choose Red Canary + CbR**

1. **Free up resources consumed with triage and investigation**
2. **Gain an immediate EDR capability**
3. **Enlist a team of specialized, highly focused experts**
4. **Cut threat detection and response time**
5. **Maximize return on investment**

> "Carbon Black Response collects thousands of events every hour. Analyzing that volume of data would take a huge level of effort and time from our internal team, even with automation. Red Canary is a hands-off strategy. I deploy the sensor to my endpoints and am provided assurance that Red Canary is taking care of the rest. I can log into the portal at anytime and see exactly what's happening."

**- Lead Infrastructure Security Engineer, Technology Company**

## 1 FREE UP RESOURCES CONSUMED WITH TRIAGE & INVESTIGATION

A mid-sized medical center implemented Carbon Black Response (CbR) and lacked the time to improve detection criteria, investigate every alert, and respond to confirmed threats.

| Industry: | Endpoints: | Employees in IT: | Information security team: |
|---|---|---|---|
| HEALTHCARE | 7,500 | 150 | 👤 = 5 |

**CHALLENGE**

The medical center had implemented CbR to get better visibility into its endpoints and defend against evolving threats. But the security team found that managing CbR 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 CbR, 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.

## 2 GAIN AN IMMEDIATE EDR CAPABILITY

A small team with solid security controls wanted to improve their security with CbR 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 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 CbR 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 ENLIST A TEAM OF SPECIALIZED, HIGHLY FOCUSED EXPERTS

The rapidly growing technology company wanted to implement CbR as part of its defense-in-depth strategy, but the internal team did not have the expertise to build an EDR capability.

| Industry: | Endpoints: | Employees in IT: | Information security team: |
|---|---|---|---|
| TECHNOLOGY | 650 | 10 | 👤 = 3 |

**CHALLENGE**

The organization regularly faced advanced and malwareless attacks and needed to safeguard valuable IP against threats that slipped past antivirus. The Infrastructure Security team knew that CbR would add a critical layer of protection—but it would also require a high level of technical expertise to analyze all the data, write rules and logic, and investigate alerts. The team leader realized they either needed heavy automation and additional staff or a very technical managed provider.

**SOLUTION**

With Red Canary, the company gained a high level of technical expertise across multiple disciplines: analysis, threat research, incident response, forensics, and engineering. They benefited from scalability and a high quality of detections without the burden of chasing false positives. Red Canary quickly detects and validates each threat, and the company's internal security team has the reporting and tooling they need to limit dwell time and eliminate threats.

## 4 CUT DETECTION & RESPONSE TIME

A private investment firm rolled out a managed Carbon Black solution through its existing MSSP but discovered that threats often lingered in the network for days or weeks at a time

| Industry: | Endpoints: | Employees in IT: | Information security team: |
|---|---|---|---|
| FINANCIAL | 300 | <5 | 👤 = 0 |

**CHALLENGE**

The Director was convinced that CbR was the best EDR sensor due to its depth of visibility into endpoint activity and robust forensics capabilities. However, the managed solution offered through the firm's MSSP was not effective. Threats often lingered in the network for days or weeks at a time, leaving endpoints vulnerable. The firm needed a partner that deeply understood endpoint data and would quickly and accurately detect threats.

**SOLUTION**

The Director knew that Red Canary had a strong partnership with Carbon Black and expertise managing the endpoint data it collected. After deploying Red Canary, the firm saw an immediate improvement in detection efficiency and response time. Whereas it previously took days or weeks to detect a threat, Red Canary enabled the team to control the situation within minutes to hours, regardless of the endpoint's global location.

## 5 MAXIMIZE THE RETURN ON INVESTMENT

A team with advanced security controls needed a partner to help them safeguard sensitive financial information and leverage the full power of its CbR investment.

| Industry: | Endpoints: | Employees in IT: | Information security team: |
|---|---|---|---|
| BANKING | 3,300 | 100 | 👤 = 10 |

**CHALLENGE**

The bank's security team had already invested in application whitelisting and CbR to secure its endpoints. The whitelisting solution succeeded in defending against the vast majority of attacks but CbR sat mostly idle. The team knew that to get the most value out of the product, 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**

"Red Canary has the ability to master Carbon Black data and detect threats as they happen. We haven't seen the same level of Cb expertise with any other vendor."

**- Director of Technology**

"Red Canary has proven time and time again they will detect the worst threats we face without ever burdening our organization with false positives. The detection and response service they built on top of Carbon Black is extremely effective, and Red Canary has become one of our closest partners."

**- Chief Information Officer**

red canary

## About Red Canary

As Carbon Black's first and most experienced partner, Red Canary delivers an unparalleled Endpoint Detection and Response (EDR) capability. The custom-built solution layers on top of CbR to quickly and accurately identify threats on customers' endpoints ranging from compromised credentials to lateral movement to crimeware. Every threat is investigated by a Red Canary Analyst to remove false positives and provide the context required for remediation.

Learn more at redcanary.com/cb-response

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