How a Fast-Growing Technology Company Secures Its Endpoints and Valuable IP With Red Canary

BUSINESS ENVIRONMENT
Annual Recurring Revenue: $100M+
Endpoints: 650

CHALLENGE
A tech company’s security team wanted to implement Endpoint Detection and Response (EDR) as part of its defense-in-depth strategy. But the lean team recognized they did not have the resources required to build an internal EDR capability.

SOLUTION
Red Canary Managed Endpoint Detection and Response (MEDR) gave the organization a full EDR capability without requiring additional investments in staffing and technology.

BENEFITS
- Expert endpoint security analysts to detect threats and remove false positives
- Visibility into endpoint activity without the burden of sifting through data
- Confidence that endpoints and intellectual property are protected against advanced threats

SNAPSHOT
A rapidly growing technology company that worked with much of the Fortune 500 appointed a Chief Information Security Officer to build out its security program. 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 Endpoint Detection & Response (EDR) would add a critical layer of protection to their defense-in-depth strategy. However, the team of three did not have capacity to manage the massive volume of endpoint data, define and tune detection criteria, investigate potential threats, and quickly respond.

EXTENDING THE SECURITY TEAM WITH RED CANARY’S MANAGED SOLUTION
The team realized that Red Canary Managed Endpoint Detection & Response (MEDR) would provide multiple benefits: a team of experts, resources, scalability, and a high quality of detections without the burden of chasing false positives.

The Lead Infrastructure Security Engineer said: “With Red Canary, we get a team of analysts to make sure nothing is missed, and we still get access to the endpoint data so we can look at everything we need or want to review. It’s a win-win.”

TYPICAL 30-DAY PERFORMANCE

| 330M | processes and executables analyzed across 667 endpoints |
| 2,355 | potentially threatening events investigated |
| 2 | confirmed threats detected |
| 0 | false positives delivered to the organization |
“Without Red Canary, we’d be losing an entire layer of our defense-in-depth strategy. Now, we have assurance that we can detect and stop threats on our endpoints.

Red Canary catches the threats our antivirus misses and we’ve had zero false positives. Red Canary MEDR is critical to our security program.”
— Chief Information Security Officer

**DIGGING DEEPER**

**Security Profile: Staffing, Tools & Processes**

The security team is comprised of several different teams that report to the CISO. The Infrastructure Security team is responsible for securing all endpoints, cloud, and on-premise systems.

The organization primarily runs OS X and in AWS, with a subset of Windows devices and virtual machines. The security team had a legacy antivirus solution in place and used a jamf configuration tool to gain insight into applications running in its environment. The team also had a solid developer background and extensively used automation and scripting to streamline workload.

**EDR: A Critical Layer of Defense**

As a technology company working with critical data from many of the world’s largest companies, the organization needed to protect against all types of malicious activity. This included coverage against external attackers and insider threats who might have access to sensitive customer information or source code. Having the ability to detect suspicious activity based on behavioral analysis rather than signature-based detection was critical.

To improve endpoint security, the Infrastructure Security team evaluated EDR and next-generation antivirus solutions, comparing critical functionalities and technology components. They determined that EDR would provide the layer of defense the organization needed. Not only would the solution stop advanced threats that antivirus didn’t catch, but it would also record all endpoint activity.

“EDR has become the most critical security tool for endpoints because you are capturing everything that is happening,” the Engineer explained. “Anything that executes, you’re tracing it, tracking it, and doing analytics on it. If someone manages to do something bad on an endpoint, EDR will see it. Without it, you’re missing a critical component of defense.”

**Saving Valuable Resources with a Managed Solution**

The Engineer chose Carbon Black Response based on the sensor’s depth of visibility and data, but he knew it would be a full-time job to look at all the data, write rules and logic, and investigate alerts. He realized they either needed heavy automation and additional staff or a very technical managed provider.

“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.”
IN THEIR OWN WORDS

Building an EDR Capability
“My best advice for other security teams is to make sure you understand the value EDR provides. Once you see why it’s important, you can decide whether to bring in people and have analysts hunting through those events, or partner with a managed provider. For us, the choice to use Red Canary was obvious. It provides better benefits and is sustainable over the long term.”

Automation vs Expertise
“It is my firm belief that in any security program, you cannot solve it with automation alone. It’s just not possible. You still need to have human eyes, reasoning, and logic to answer and get assurance around your program itself. Without it, you might catch 95% of things—but what about the other 5%? Ask any company that’s been breached; that’s not good enough. A solid security program requires automation and human logic to get assurance. It’s a two-pronged approach.”

Seamless Deployment & Integrations
“The deployment was completely flawless. Red Canary developed a deployment script with one of our engineers, and we had it deployed through Casper in one day. It literally took no effort. The solution integrated into our existing systems and processes to make workflow easy. For example, Slack notifies the right team when something is going on and we can respond quickly.”

Benefits of Red Canary’s Managed Solution
“There is a level of impact you can make with automation, but you’ll never get to the scale of a vendor who is seeing all different things in different customers’ environments. We would have had to hire more people or sacrifice quality; that layer of our defense-in-depth strategy would have been far weaker. You can’t have it all—unless you partner with a solution like Red Canary.”

About Red Canary
Red Canary helps customers secure their endpoints and stop attacks before they result in breaches. The Managed Endpoint Detection and Response solution quickly and accurately identifies 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.

See how Red Canary can help you secure your endpoints.

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