CASE STUDY: FINANCIAL

Securing the Endpoint: How a Multibillion-Dollar Investment Firm Defends Against Cyber Attacks

BUSINESS ENVIRONMENT

AUM: $40B
Employees: 100+
Highly Mobile Users: 50+

CHALLENGE

Threats lingered in the network for days and the security team lacked visibility on endpoints, especially the laptops of its mobile workforce.

SOLUTION

Red Canary Managed Endpoint Detection and Response (MEDR) improved visibility into what was happening on endpoints, quickly identified threats, and provided the firm with the necessary intelligence and tooling to respond to threats.

SNAPSHOT

As a private investment firm with close to $40 billion in assets under management, cybersecurity is critical to the business. The firm has invested in robust security posture with multiple overlapping layers of security solutions and personnel. However, the firm lacked visibility on devices inside and outside its core network—a significant risk for a firm whose research-driven investment process has analysts traveling around the globe.

BETTER VISIBILITY AND FASTER THREAT DETECTION

Red Canary now helps the firm secure its endpoints with Managed Endpoint Detection and Response (MEDR). The Director of Technology has seen an immediate improvement in detection efficiency and response time. Whereas it previously took days or weeks to be notified of a threat, Red Canary enables the team to control the situation within minutes to hours, regardless of the endpoint's global location.

TYPICAL 30-DAY PERFORMANCE

4	confirmed threats detected by Red Canary that the firm remediated
445	potentially threatening events investigated by the Red Canary Security Operations Center
6.42M	processes & executables analyzed across 195 endpoints

red canary

"Red Canary is set up specifically to be experts in endpoint monitoring, detection, and response. They are extremely efficient at handling all of the endpoint data and accurately detecting threats. We haven't seen the same level of expertise with any other vendor."

— Director of Technology

DIGGING DEEPER

Security Profile: Tools & Processes

The firm's internal team is focused on both IT and security. As a result, the firm outsources a number of its security functions to managed security providers. A boutique MSSP (MarLabs) manages the firm's SIEM, DLP, IPS, and day-to-day cybersecurity posture. SecureWorks manages the firm's IDS. The firm's team also has a leading endpoint protection suite deployed.

Lack of Visibility

Enhancing visibility and threat detection across laptops was a critical concern for the firm. Over thirty Research Analysts constantly travel around the world. It was not uncommon for their computers to not check into the corporate network for multiple months. Aside from the lack of visibility, these computers continually missed critical IT patches and updates.

Value of EDR for a Multi-National Investment Firm

The Director of Technology knew that EDR was the best way to continuously monitor all endpoint activity and detect potential threats. He selected Carbon Black Response due to its ability to provide deep, comprehensive endpoint data. However, he soon realized that managing the product required a deep level of expertise and time commitment. His existing team was already dedicated to other priorities and struggled to look through all of the information and pinpoint events that needed further investigation.

Red Canary Improves Detection and Response

The Director knew about Red Canary's strong partnership with Carbon Black and deep expertise managing the endpoint data it delivers. Red Canary's analysts quickly analyze activities and alerts, investigate potential threats, and notify the firm of events requiring attention.

The team saw an immediate improvement in detection efficiency and response time after deploying Red Canary's MEDR solution. Whereas it previously took days or weeks to be notified of a threat, Red Canary now enables the team to control the situation within minutes to hours, regardless of an endpoint's global location.

"Red Canary has been an excellent investment for us," the Director says. "It has improved our security program and we've seen positive benefits in terms of incidents identified and effectiveness of the platform."