CASE STUDY: FINANCIAL

A Multi-Layered Approach: How An Investment Firm Uses Multiple Managed Security Providers for a Robust Line of Defense

BUSINESS ENVIRONMENT

AUM: $40B

MSSPs: 3

Highly Mobile Users: 50+

CHALLENGE

The firm needed a market-leading Managed Endpoint Detection & Response solution that could integrate into its existing security program, which already included two managed providers.

SOLUTION

Integrating Red Canary Managed Endpoint Detection and Response (MEDR) alongside the firm's existing MSSPs enabled the firm to secure its endpoints without increasing operational complexity.

BENEFITS

- Ability to seamlessly integrate alongside other managed solutions
- Endpoint security experts and detection operations analyze endpoint activity and detect threats, complementing the work of MSSP security functions
- Intelligence and tooling to rapidly respond to threats

SNAPSHOT

Enhancing visibility and threat detection across laptops was a critical concern for a private investment firm with dozens of highly mobile users. The firm's Director of Technology knew that an endpoint detection and response (EDR) solution was the best way to continuously monitor all endpoint activity and detect potential threats. However, he needed to find EDR expertise that would integrate into the firm's existing security program and work alongside its MSSPs.

SEAMLESS INTEGRATION OF MULTIPLE MANAGED PROVIDERS

Red Canary Managed Endpoint Detection and Response (MEDR) seamlessly integrates alongside the firm's MSSPs. This enables the Director to rely on each managed vendor for their specialties, yet also have integrated data sources that he and his team can work with and manage. They're able to assess similarities and differences in the data each solution reports, gain independent validation of events, and prevent any single point of failure.

TYPICAL 30-DAY PERFORMANCE

3	managed security providers focused on a variety of expert capabilities including EDR (Red Canary); IDS (SecureWorks); and SIEM, DLP, and IPS (Regional MSSP)
6.42M	processes & executables analyzed across 200 endpoints by Red Canary Security Operations
445	potentially threatening events investigated by Red Canary security analysts and 4 confirmed threats detected

red canary

> “We work with several managed service providers. Cybersecurity is such an important aspect of our business, we really want to have multiple independent views into what’s happening. I enjoy having completely independent validation that our networks aren’t compromised and our workstations aren’t infected.”
>
> — Director of Technology

DIGGING DEEPER

Security Profile: Tools & Processes

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

Why Multiple Providers Are Needed: A Layered Approach to Security

The Director is a firm believer in using multiple independent solutions. He would rather use a market leader than an MSSP that does everything sub-par. That is why he uses multiple MSSPs as a part of his security program. One of the firm’s MSSPs performs a number of overall security functions, while Red Canary is specifically set up to monitor his endpoint data and detect threats.

“We’ve layered our security in a way that brings us domain expertise from multiple security providers,” the Director says. “Red Canary has mastered endpoint data and analysis and is a critical part of our overall security program.”

Red Canary Provides Deep EDR Expertise

The Director of Technology was convinced that Carbon Black Response was the best EDR technology due to its ability to provide comprehensive endpoint data. He knew that Red Canary had a strong partnership with Carbon Black and deep expertise managing the endpoint data it delivered.

After deploying Red Canary’s MEDR solution, 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. The Director says: “Many times, we get an alert from Red Canary and already have a man on the scene by the time our MSSP’s analysts can say that an incident has been validated. We haven’t seen the same level of EDR expertise with any other vendor.”

See how Red Canary can help you secure your endpoints.

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

red canary