eSENTIRE

CASE STUDY

Global Investment Firm

Global Investment Firm Uses Managed Detection and Response (MDR) Services to Protect Proprietary information and Private Data

The Business:

Global investment firm that offers financial products and services throughout the world:

- One of the world's largest asset management firms
- 5,000+ employees
- History and reputation dating back 80+ years
- Business is built on knowledge and collaboration
- Major presence in North America and Europe with regional hubs in other major markets
- In-house security and incident response capabilities led by regional CISOs

Solution and Results:

- eSentire MDR for Network provides full network visibility, eliminating attack blind spots that traditional technologies miss
- eSentire MDR for Endpoint combines Endpoint Detection and Response (EDR) technology with proprietary machine learning and human expertise to rapidly detect and contain threats that bypass preventative controls
- eSentire MDR for Log aggregates meaningful and actionable intelligence across network assets, endpoints, applications and cloud services
- Incident Response consultation ensures IR plans are effective with clear division of responsibilities

Customer Pain Points and Drivers:

- The customer had a fairly good-sized security team, but struggled to handle alerts, do triaging and investigation on top of their day jobs
- The need for a Security Operations Center (SOC) that could provide 24/7 global coverage
- They looked at building their own SOC, but it was complex and costly
- They needed an MDR solution that could provide multi-signal coverage and be a partner to their existing security team
- They were shifting to remote work and migrating to cloud

The Business and Security Outcomes:

- Around-the-clock global network coverage with 24-hour support from eSentire threat hunters who respond to and contain threats
- Cost-effective solution compared to building an in-house 24/7 SOC
- "A much better state of prevention and protection"
- Significantly reduced workload for the IT and security teams
- eSentire has already detected and stopped multiple threats that the firm believes would have gone under the radar in the past
- eSentire has detected every single penetration test run since deployment

> *"Previously, we tried to build our own SOC, but it was simply too difficult. The cost-benefit of working with eSentire massively outweighed building up these capabilities ourselves. It's a real no-brainer."*

Background

The customer is one of the world's largest investment firms, with a global presence and more than 5,000 employees. Knowledge-based insights are the foundation of informed investment and business decisions and represent one of the firm's strongest differentiators. Protecting these assets and the private information of the firm's clients is an absolute necessity.

The Challenge

Through growth over the firm's history—extending more than 80 years—the customer has become a truly global and interconnected organization.

The company's information assets contain proprietary research and analysis, plus private and personal data belonging to the firm's customers. As is the case with many collaborative businesses who deal with end clients, much of this information needs to be shared securely and accessed remotely.

Keeping this global operation running smoothly and protecting the valuable information is a team of experienced information technology (IT) and security personnel. To enable this distributed architecture, the firm utilizes a hub model using MPLS and VPNs with endpoints protected by a leading endpoint protection platform.

Following an internal restructuring, the team took a high-level look at the organization's evolving IT and security needs. These needs were shaped by a keen awareness of multiple factors, including:

- An increased number of employees working from home; the firm had to ensure that this shift did not jeopardize the organization's security posture
- A growing cloud footprint; the firm has adopted more cloud services in recent years and expects this trend to continue; the cloud cannot become a blind spot or source of unmanaged risk
- A recognition that attacks against similar organizations are commonplace
- An understanding that third-party solution vendors introduce additional risk, whether from supply chain compromises, valid account credentials or other avenues

After careful consideration and having previously explored the option of building an internal SOC function, the decision was made to augment the in-house capabilities with specialized external expertise, particularly for MDR and security operations.

As the firm's Europe-based IT security lead put it, "We have a really solid IT security team in house, but we needed a specialist looking at events and triaging logs, deciding what warranted escalation. In the past, we had too many false positives and the volume overwhelmed our team."

The Solution

The firm's IT security lead prepared an RFP and invited seven vendors to respond. The questions were grouped into a handful of categories and a five-person technical team scored the seven responses. The top four vendors were asked to deliver specialized presentations and to introduce their technical teams for more detailed discussions.

Based on these initial rounds, the firm shortlisted two vendors. eSentire was joined in this final round by the security division of an enormous multinational technology enterprise.

Ultimately, the eSentire proposal—consisting of eSentire's multi-signal approach to MDR services leveraging eSentire MDR for Endpoint, eSentire MDR for Network and eSentire MDR for Log—was selected. The firm cited several specific areas, including:

- Expertise: The team liked that eSentire is a true MDR provider, not an MSSP focused on doing other things
- Global SOC capabilities: The evaluators believed that eSentire's keen focus on MDR and the stellar SOC that is a key component of this service would lead eSentire to outperform the other finalist, for whom security services were simply a small part of much less focused portfolio

- Service level and support: The team anticipated much more attentive ongoing service from eSentire and particularly valued that eSentire has much lower turnover rates than the industry norm
- Advanced multi-signal detection capabilities: The technical evaluators felt confident that eSentire's combination of endpoint, network and log-based visibility and AI-driven analysis and correlation would be able to detect the latest threats
- Price: The project sponsor's initially preferred a vendor that submitted a response at a cost three times higher than eSentire's, and was eliminated in the initial round. eSentire and the other finalist were similar on price, but eSentire's superior capabilities offered greater value

The Results

One of the biggest differences for the firm is that the workload on the security team is substantially lower, which allows them not only to keep pace with day-to-day demands but also to move forward with other initiatives.

In the customer's words, "The information we get back from eSentire is much more filtered, in a good way—there's considerably less noise than we're used to, because the investigation has been done before it comes over to us. Our experience with other companies is that they just send a stream of logs and make understanding it our problem."

True to expectations, the firm has been impressed with eSentire's people and level of service, sharing that, "The team is very responsive. We can always get someone on the phone or by email, and it's always a human response—not some automated thing about our request being important. eSentire's people are very skilled, very approachable and very knowledgeable."

Crucially, when it comes to security outcomes, the results are exactly what the firm hoped for.

For example, the customer has performed multiple penetration tests since introducing eSentire, and eSentire's defenses have always picked up these exercises.

That's fine for peace of mind, but what about legitimate attacks?

In this domain, eSentire has detected multiple real threats, leaving the firm convinced that they are in a much better state of prevention and protection than in years past. "eSentire has already picked up a number of malware and other threats that likely would have gone under the radar otherwise. And I think that comes down to the level of threat intelligence and proactive investigation that eSentire performs—it's terrific, it's what we had hoped for and it leads to real results."