eSENTIRE

CUSTOMER CASE STUDY

Wetherby Asset Management

A top investment management firm seeks to continuously improve its security posture after being the target of a lengthy brute force attack on New Year's Eve.

WETHERBY
ASSET MANAGEMENT

- Independent Registered Investment Advisor
- Based in San Francisco and New York
- Over $5bn assets under management

THE ORGANIZATION

Wetherby Asset Management is a boutique portfolio management and wealth planning company with offices in San Francisco and New York. Founded in 1990, it pioneered independent investment advice, separating fees from investment recommendations to focus on its clients' best interests and carrying no internal products of its own.

Today, the 100 percent privately owned company has over 60 employees that focus on impact investing to align clients' portfolios with their values. This has earned Wetherby a sought-after B Corp certification, proving that it meets the highest standards of verified social and environmental performance, public transparency, and legal accountability.

Wetherby has over $5bn in assets under management (up from $2.3bn in 2011) and a 97 percent client retention rate. It has won several accolades, including B Corp's Best for the World Changemakers, Best for the World for Customers, and Best for the World for Workers awards (2018). It also featured on the Financial Times 2018 list of 300 Top Registered Investment Advisors (RIAs).

CUSTOMER CASE STUDY

Wetherby Asset Management

THE CHALLENGE

When Wetherby's Principal and CTO Trevor Hicks joined the company in 2013, he found a company with little structure applied to its information security program.

The problem was twofold. First, Wetherby had struggled to keep up with the fast pace changes within the information security space. "The technology was the scaffolding, and it only got attention when it fell apart," said Hicks.

The lack of technical staff led Wetherby to outsource most of its technology services, but without the internal resources to highlight issues that needed attention, the service providers were mostly reactive. The technology worked, but it was out of date and support was hard to find. Hicks knew hackers were targeting Wetherby, but the outdated infrastructure offered no network visibility, limiting threat intelligence.

The second problem was the lack of formalized security policies, procedures, and best practices for employees. Wetherby's focus on business growth meant the team was stretched and it hadn't invested in employee security policies and procedures.

Wetherby needed to overhaul its approach to security, otherwise a successful cyber attack was inevitable. Implementing a solution to reduce risk for this mid-sized organization with limited resources was going to take a clear understanding of the existing security threat landscape, and buy-in from senior management.

> **"It's a pleasure working with a group of people that know what they're doing. They are an extension of the the Wetherby technical security team."**
>
> **Trevor Hicks**
>
> *Principal, and CTO*
> Wetherby Asset Management

Wetherby Asset Management

The eSentire Solution

eSentire Managed Detection and Response™

esNETWORK™ provides 24x7x365:

- Rapid intrusion detection and response that auto-detects and responds to known and unknown threats with:
  - Real-time blocking of IOCs, signatures, and previously unseen attacks, including phishing, malware, ransomware, and botnets
  - An extensive, proprietary rules library covering 40+ threat categories
  - Highly-customizable rules and policies, including executable white lists, geo-IP, and blocking access to specific sites

THE SOLUTION

eSentire used its Managed Detection and Response (MDR) service to provide threat protection capabilities that go beyond alerting to disrupt threats to protect Wetherby's systems. The principal component of this service deployed was esNETWORK™, a zero-latency IPS/IDS designed to provide full network visibility eliminating attack blind-spots that traditional technologies miss. MDR and esNETWORK™ have identified and blocked thousands of cybersecurity events while giving Wetherby the network visibility it needed. "I call it the cornerstone of Wetherby security controls," said Hicks.

Alerts are now configured for events such as remote desktop connections and SSH sessions, which provides Wetherby with the data needed to understand what is happening in our environment, as well as to support new security policies. "Sometimes, I just want to know who's using FTP so I have better visibility into the tools that are being used in our environment. This information is incredibly valuable when thinking about our tehcnology and security roadmap," he said.

MDR provides Wetherby with a much-needed layer of technical defense as a backstop for the company's cybersecurity awareness initiative. If an employee forgets their training and clicks on a malicious link in an email or

Wetherby Asset Management

tries to open an infected file, MDR can find out what page the malicious code contacted and what payload it tried to download.

Wetherby also replaced an entire cybersecurity program with eSentire's Managed Vulnerability Service* which provides comprehensive risk identification and prioritization with unmatched accuracy across traditional enterprise IT assets. Hicks had previously commissioned annual penetration tests from a consultancy.

The pen tester had accessed its environment twice, but the remediation and testing cycle was too long. "You make fixes and then wait a year for the next testing cycle to find out if you scored any better," Hicks said. "With Managed Vulnerability Service, we're able to act on a contstant cycle of improvement," he added. Now, Wetherby can run a scan after every significant technical change it makes, leading to a cycle of continuous improvement.

*formerly known as esRECON

> **"Daily, there are thousands of instances where somebody is trying to do something malicious or trying to gain access to our environment. We had no visibility."**
>
> **Trevor Hicks**
>
> *Principal, and CTO*
> Wetherby Asset Management

Wetherby Asset Management

THE RESULT

The peace of mind that eSentire brings to Wetherby through automatic blocking and immediate alerting is of huge value. Besides the technology tools, eSentire's analysts in the Security Operations Center (SOC) provide expert help with emerging security issues the organization needs to be aware of.

"The SOC analysts are incredibly knowledgeable, and if I need more information, they will find it for me," he noted.

Hicks has proof that eSentire's protection has stopped significant cyberattacks on the organization. On December 31, 2018, attackers began a sustained 12-hour brute force attack on the company.

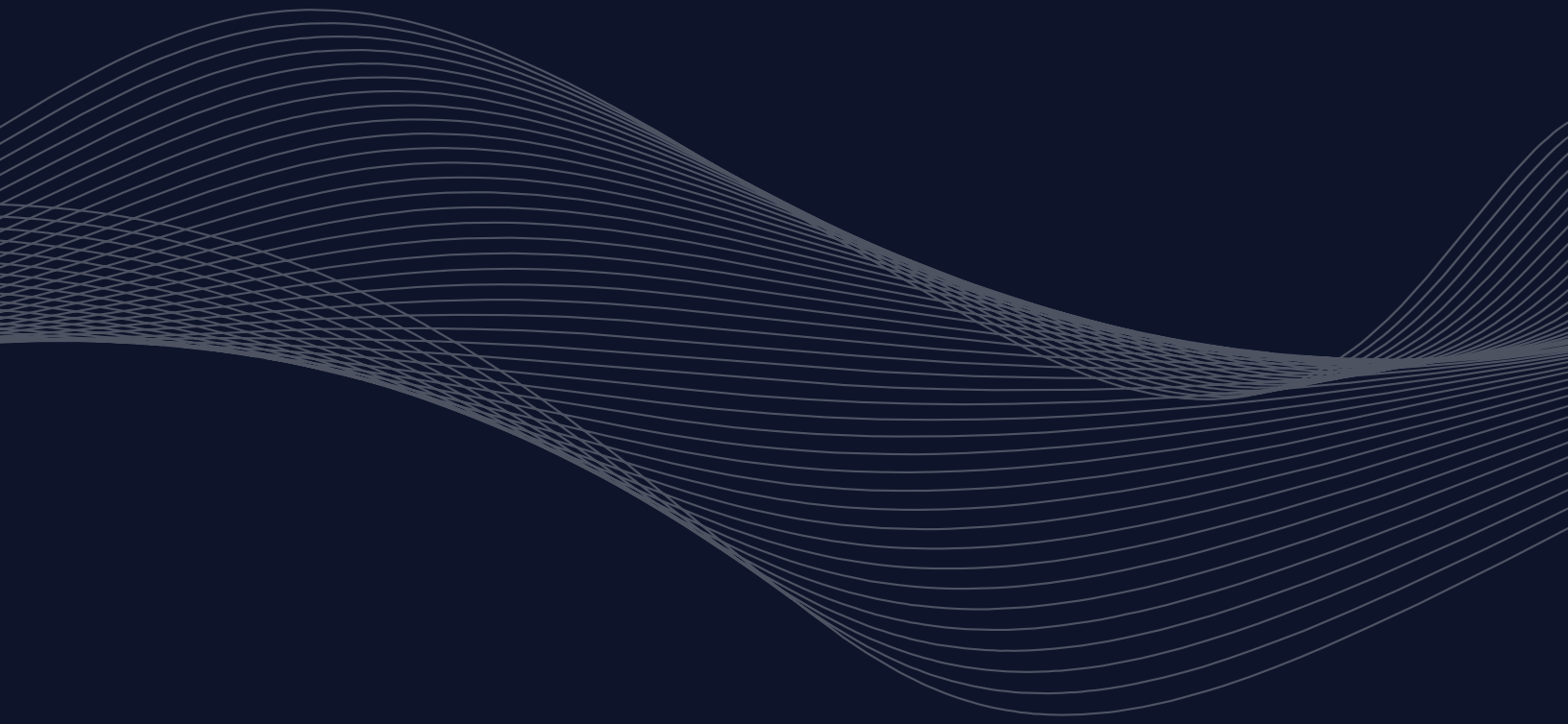
"I think they chose New Year's Eve because they thought we wouldn't be watching," he explained. But eSentire was watching. The SOC alerted Hicks via email that a sustained attack was coming from several European countries including Poland and the Netherlands.

"We blocked traffic from those countries for the duration of the attack so we could revisit it later," he said. This enabled employees to enjoy their evening knowing that their systems were not in danger.

That incident showed up as a spike in brute force attack data in Wetherby's next quarterly phone review with eSentire. These 15-minute sessions are valuable because they bring the team up to speed, explaining any issues that have arisen in the last three months.

eSentire's regular reports also surface useful statistics that Hicks can use to prove the need for focused security investments to management. "Now I have reports and metrics that I can show to the rest of the firm and say, 'it is an issue. People are targeting us, and we need to continue on our path to improve our security posture.'"

For a company dealing with so many high-value clients' sensitive data, the online attacks are unlikely to stop. At least now, with an expert security team monitoring every network packet, Hicks and Wetherby know that someone has their back.



eSentire

eSentire, the global leader in Managed Detection and Response (MDR), keeps organizations safe from constantly evolving cyber attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire**.