CASE STUDY

RIA Takes Necessary Precautions to Comply with Increasing Regulatory Requirements and Defend Against Cyber Threats

THE BUSINESS

- Registered Investment Advisor
- Based in New York City
- 50+ employees
- Faced with intensifying regulatory pressures and cyber threats

THE eSENTIRE SOLUTION

eSentire Advisory Services

eSentire Managed Detection and Response™

Employing esRECON™, esENDPOINT™ and esNETWORK™

Background

One of the biggest business risks to the financial services industry is cybercrime. Whether it's account data or investor information, financial firms hold a wealth of information that can be quickly turned into monetary gain, making them an attractive target for cybercriminals.

For a Registered Investment Advisor (RIA), being the victim of a data breach can have a number of negative repercussions. First, it creates problems with investors. Under the new SEC guidance, public firms need to disclose incidents to investors. This means investors will be immediately notified of a security incident, potentially creating mistrust in their advisor.

Second, a breach would demonstrate non-compliance with regulators. While it is clear firms are mandated to comply with regulations, the requirements can sometimes be complex and difficult to navigate, making this process challenging for the firm.

The increased likelihood of a cyber-attack and data breach has prompted regulators, like the SEC and NYRCC 500, to put a stronger focus on cybersecurity in 2018. As a result, firms need a cybersecurity professional that can keep up to date ever-changing cyber-threats as well as growing regulatory requirements.

The Challenge

RIAs have a fiduciary duty to their clients, which means they are fundamentally obligated to provide suitable investment advice and act in their clients' best interests. As a result, the staff at this firm manage their clients' confidential financial information on a daily basis, which makes identity and information security a top priority.

The firm knew that with the current threat landscape, in addition to the ever-increasing number of regulations, it would be difficult to acquire the expertise and knowledge that a cybersecurity provider has. Ultimately, they didn't want to invest the time or resources into building a program internally because they knew a partner would have a more fulsome and in-depth knowledge base and offering.

The RIA's Chief Technology Officer met Eldon Sprickerhoff—Founder and Chief Security Strategist at eSentire—several years ago through another company. When he heard about Managed Detection and Response he signed his current company up with eSentire, knowing they would be safe in the hands of these cybersecurity experts.

As the CTO changed jobs in the years that followed, he brought eSentire's expertise to each new company he joined. This RIA has now been a customer for over 10 years, making them one of the longest-standing customers of eSentire.

The Solution

eSentire introduced the firm to Managed Detection and Response (MDR), a solution designed to detect and respond to threats that bypass traditional security technologies. The solution included esRECON, esENDPOINT and esNETWORK.

esRECON scans servers, databases, endpoints and web applications for known vulnerabilities, while esNETWORK uses advanced behavior-based anomaly detection and attack pattern analysis to detect threats that have bypassed all other security controls. Finally, esENDPOINT eliminates any endpoint blind spots. Now, with these solutions, the firm knew they'd be protected by the best technology in the business.

"eSentire is set apart by their Security Operations Center (SOC). I know that if something bad happens at 3am, they're going to call me, and if they don't get me, they're going to take action on my behalf. That's the best part about the service they provide." – CTO

The firm also employs Advisory Services, which includes services like Virtual CISO, Phishing Campaigns and TRAP/DNS. eSentire's Advisory Services performs an annual review of their policies to ensure they're meeting the latest regulatory requirements. Not only does the firm know they're protected from attacks, but they can also be confident they're meeting the latest regulatory requirements.

Occasionally, investors will question their "over-reliance" on eSentire. To address this, the firm hired a third party do a penetration test, a gap analysis and other tests on their network, and didn't tell eSentire. Immediately after the tests began, eSentire notified the firm of the third-party actions and alerted them to the situation.

> "We're confident that we have a cybersecurity program better than our peers."

The Results

In the CTO's early days as an eSentire customer, the firm he was working for at the time was hit with an attack. Cybercriminals installed remote control software on one of the firm's trader's work stations. Using the software, they were able to infiltrate the system through a market data vendor. Immediately, the eSentire SOC called and alerted them to the installation. The firm was instructed to pull the plug on the affected system and let their vendor know their network had been compromised.

At his current firm, a zero-day crypto malware recently breached their network via email. The malware bypassed the anti-virus software the firm had installed and began encrypting. That's when eSentire stepped in. The eSentire SOC quickly detected the malware and remotely quarantined the computer. As it turns out, the malware had evaded four other security technologies as it moved throughout the network. eSentire was the only one that detected it. Since then, the firm has added esENDPOINT™, which prevents the attack from spreading.

"The daily alerts give me insight into what is happening on my network that I wouldn't otherwise have," said Chief Technology Officer. "I sleep better at night knowing eSentire is on the job."

After 10 years with eSentire, the firm feels confident that they're in safe hands. No matter what they're faced with, they've been able to count on eSentire to protect their network from a cyber-incident that could damage their business or reputation.

About eSentire

eSentire Managed Detection and Response™ protects financial firms against cyber-attacks that traditional security technologies can miss. Our Security Operations Centers are equipped with elite security analysts who hunt, detect, investigate and respond to known and unknown threats in real time. Beyond MDR, our dedicated security experts will help you assess risks, address known gaps and build a comprehensive program that meets stringent regulatory requirements.

Learn more at www.eSentire.com

esentire®