CASE STUDY

The Riverside Company

The Business

Mid-Market Private Equity Firm
Domiciled in the United States

More than 30 locations worldwide

Two global data centers

200+ employees

The eSentire Solution

eSentire Network Interceptor™
for continuous network monitoring, threat hunting and remediation

eSentire Endpoint Managed Detection and Response™
for endpoint protection

US-Based Private Equity Firm Applies Managed Detection and Response Services to Protect its Network and Meet Compliance Requirements

Background

Financial institutions have faced a growing and ever-changing list of compliance requirements in response to heightened cybersecurity risk and widening governance measures. In addition to government controls, regulatory agencies like the U.S. Securities and Exchange Commission (SEC), hold financial firms to routine questionnaires and security audits to validate a firm's security posture and overall compliance.

The challenge

The Riverside Company is a US-domiciled, mid-market global private equity (PE) firm. Since founding in 1988, Riverside has invested in more than 430 transactions and has grown its international portfolio to more than 80 companies. When protecting its more than $5B USD in assets under management, the firm adopted a thoughtful and proactive approach, partnering with respected and trusted third-party service providers to enrich programs and measures supported through its in-house IT team.

Within its market, Riverside is unique. Unlike traditional firms operating in the space, the firm has a large global footprint with most offices located internationally. The firm operates with a sense of enterprise from a network architecture perspective with more than 17 global locations and a number of home offices. The vastness of of the network environment meant that the IT team often found themselves lacking a good sense of the types of data moving in and out of the organization's network.

"Being in the dark means you just don't know..."

The complexity of the firm's environment, coupled with an increasing number of SEC-based compliance requirements, led Eric Feldman, Riverside's Chief Information Officer, to source support to help drive a more mature security program. The firm already had a number of strong security layers in place (such as next-generation firewalls with SSL decryption functionality, web content and email security technology), however even with those technologies in place Mr. Feldman recognized that he still lacked visibility to the security events that hit the firm's network.

"Being in the dark means that you just don't know," said Feldman. "As an organization, we've always taken a progressive approach to cybersecurity. We realized that by partnering with trusted third-party providers, we could get a better sense of the data flowing in and out of our network and meet an importance compliance requirement at the same time."

The Solution

The firm had long recognized the value-add that managed services could provide to lean, in-house IT teams. However the benefits of eSentire Managed Detecion and Response™ service and its eyes-on-glass continuous monitoring model steered the firm's list of service needs, which required that the successful vendor must :

- Provide a simple service that would require little upfront configuration;
- Deliver network alerting capabilities that would help the team easily decipher actionable events and;
- Meet and exceed many requirments commonly listed on due diligence questionnaires and audit forms.

It was through multiple due diligence meetings that the firm learned about eSentire. "Many times I had sat in due diligence meetings with partners who would commonly raise eSentire as a trusted third-party managed detection and response security services provider," said Feldman.

"eSentire had developed brand recognition and a trusted reputation within the market that supported investor due diligence."

Eric Feldman, Chief Information Officer, Riverside

Riverside installed eSentire Network Interceptor at all of its global locations and at its two global data centers. "The combination of tools, technology, and eSentire's Security Operations Center (SOC) means that we have eyes and ears on our network at all times. This helps our own IT team to understand what's normal or abnormal, in terms of traffic flow," said Feldman. "Before, our team simply had limited visibility. The service and support provided through the SOC analyst team means that now we can make informed decisions, rather than arbitrarily making decisions without the data necessary to back them up."
Customized entirely to the firm's unique needs and network makeup, the firm's individual service level agreement pre-defines alerting cadence and event escalation paths.

"We consider the SOC an extension of our team," said Feldman. "From day one, we've had the ability to tweak escalation path definitions as we became more familiar with the types of data we wanted and needed to see. When we have questions around any alerts we receive, we feel confident that within minutes of reaching out to the SOC we'll get a lengthy response explaining the tools and actions we need to take to remediate a threat. When speaking to SOC analysts we feel like we're dealing with onsite team members; the SOC is an incredible resource, one that we use often enough that it's become our default."

The firm's success with eSentire has led to additional service rollouts, including Endpoint Managed Detection and ResponseTM, which provides the firm with next-gen 24/7 endpoint protection against advanced persistent threats

The firm's success with eSentire has led to additional service rollouts, including Endpoint Managed Detection and Response™, which provides the firm with next-gen 24x7 endpoint protection against advanced persistent threats targeting the endpoint.

The results

eSentire's unique blend of people, process and proprietary technology protects clients through several security checkpoints. The first line of defense is Network Interceptor, which is sensor-based technology that automatically blocks known threats. Unknown or suspicious threats are escalated to SOC analysts for further investigation. It's there that analysts determine how to handle and mitigate unusual threats.

Of the numerous unique, sophisticated threats that targeted Riverside's network in 2016, the SOC blocked nearly a dozen malware-based attacks and two phishing attempts. Any one of these attacks could've caused significant damage had they entered Riverside's network.

eSentire has become a mainstay in Riverside's defense posture since initiating in 2014. "eSentire and its services have become a critical component of our firm's security toolbox," said Feldman. "The fact that eSentire thoroughly understands regulatory expectations and impacts is a massive advantage as on an ongoing basis, we remain confident that our firm is protected and compliant."