eSENTIRE

CASE STUDY

Venerable

How a leading organization in the insurance annuity sector is leveraging eSentire's 24/7 Managed Detection and Response (MDR) to move ahead of the threat curve

Business and Security Outcomes

- Having the right security expertise to monitor and enforce standardized configurations across multiple cloud platforms to protect against misconfigurations and vulnerabilities
- Achieving a "single pane of glass" for a multi-cloud security environment
- Keeping pace with the evolution of various cloud technologies
- Outpacing the business technology requirements by maintaining a cohesive cybersecurity strategy that combines the necessary toolsets, resources, and cyber expertise regional hubs in other major markets

Solution and Results

The eSentire Managed Detection and Response (MDR) solution included:

- **24/7 Threat Detection and Investigation** with eSentire's MDR for Log to identify and investigate cyber threats within Venerable's AWS environment
- **Cloud Security Posture Management** to reduce their risk by improving cloud visibility, tracking critical assets, and monitoring for misconfigurations, policy notifications and security vulnerabilities
- **MDR for Microsoft** to ensure complete detection, response, and remediation across endpoints.

The Business

Venerable is a leading US-based organization within the insurance annuity sector that focuses on building and growing insurance businesses with long-term capital. Since 2018, Venerable has owned and managed legacy variable annuity businesses acquired from other entities.

- Dynamic multi-cloud network with 1,000+ endpoints
- 100% cloud-native infrastructure
- Security program overseen by the CISO and a small team responsible for monitoring, security operations, incident response, vulnerability management, application security testing, penetration testing, and compliance scanning.

Background

Venerable was initially established in 2018, after being divested from Voya Financial. Once Venerable began its operations, they knew they needed to move fast and couldn't take a risk with an unproven MDR provider given the increasing number of high-profile insurance organizations falling victim to crippling cyber attacks.

As an organization that focuses on the long-term growth of insurance businesses, Venerable's existing security team is small, albeit with a broad scope – it is responsible for maintaining its security posture in a way that outpaces the business itself so they can drive the most value for their customers.

To ensure Venerable has a leading, world-class cybersecurity program, the security team had three main principles:

i) They did not want to rely on old legacy systems to store their critical data assets,
ii) They understood that security functions don't operate in silos, and
iii) They proactively managed their cyber risk to protect their sensitive client data (e.g., PII and business intellectual property) from cyber threats.

As a result, Venerable needed a trusted security partner with deep expertise and a strong reputation within the financial and insurance annuity space that would allow their team to zoom out and take an integrated approach toward building a complete security posture.

> *"A big part of why eSentire has shown value to us, in addition to the people, is how far ahead they are from a technology standpoint. eSentire gets ahead of the direction that we're moving in before we know we're heading in that direction."*
>
> *Simon Scully, Assistant Vice President, IT Security - Security Operations at Venerable*

The Challenge

Since Venerable was a spin-off from an existing organization, it was able to adopt a 100% cloud-native approach to running all internal applications and build its architecture. Initially, Venerable relied heavily on Amazon Web Services (AWS), but began to adopt Microsoft Azure and Microsoft 365 to decrease their reliance on a single cloud platform. This transition to Microsoft compliments the firm's disaster recovery efforts, and enables the Venerable team to leverage the technologies and platforms also used by their customers.

Adopting a multi-cloud strategy added a layer of complexity for the Venerable team as it's harder to monitor and enforce standardized configurations across multiple platforms. Native security features vary across each cloud platform and achieving a "single pane of glass" operational state across cloud environments is challenging. For example, AWS's native services for checking cloud compliance configurations do not work for a non-AWS cloud application like JIRA.

In addition, cloud technologies are constantly evolving, so security teams must not only be able to keep up with that evolution, but also have the resources necessary to secure the technologies. This is especially critical from a configuration management standpoint since cloud environments move faster than most security teams can manage, making it that much more difficult to keep track of any new vulnerabilities that could be exploited.

As a result, Venerable's small but mighty security team needed a partner that could mitigate cyber risks and address multi-cloud security by:

- Evolving at the same speed with which cloud technologies are evolving,
- Prioritizing a security strategy that encapsulates the necessary toolsets, resources, and cyber expertise that can support their security roadmap and outpace their business technology requirements, and
- Having the security expertise to ensure that their multi-cloud environment was protected against misconfigurations and vulnerabilities.

Why Venerable Chose eSentire

Simon Scully, Assistant Vice President, IT Security - Security Operations, joined Venerable following his tenure at Voya Financial and had been impressed with eSentire's capabilities & expertise during his time there. So, when Venerable needed an MDR provider, eSentire was the obvious choice.

To mitigate Venerable's cyber risks and address their multi-cloud security strategy, eSentire delivered:

- **24/7 Threat Detection and Investigation** with eSentire's MDR for Log to identify and investigate cyber threats within Venerable's AWS environment
- **Cloud Security Posture Management** to reduce their risk by improving cloud visibility, tracking critical assets, and monitoring for misconfigurations, policy notifications and security vulnerabilities
- **MDR for Microsoft** to ensure complete detection, response, and remediation across endpoints.

The initial engagement began with multi-signal Managed Detection and Response (MDR) for Log and Endpoint to improve visibility into the cloud and get increased MITRE coverage.

Throughout the partnership, eSentire has demonstrated deep knowledge of AWS-specific threats and vulnerabilities, provided proprietary runbooks and detections to hunt and investigate threats across the AWS environment, and captured endpoint telemetry to prevent adversaries from moving laterally through Venerable's network by isolating and containing compromised endpoints quickly.

In addition, eSentire facilitated a seamless transition from Venerable's existing redundant endpoint licensing to Microsoft Defender for Endpoint to consolidate their security spending and to maximize their investment in Microsoft Office 365 E5 licensing. As part of the migration, eSentire provides 24/7 MDR services and leverages Venerable's own Defender for Endpoint licensing.

From the start, what differentiated eSentire was the market leadership and specialization demonstrated by the team in the Managed Detection and Response space in addition to the cyber expertise shown continually by eSentire's team of security experts who are committed to 24/7 threat detection, eyes on glass capabilities, and immediate support in case of an incident:

"Being able to have someone you can reach out to if something's gone sideways and know they're a trusted partner who understands your environment and the MDR space was essential for us," Scully said.

Since Venerable's security team is focused on moving ahead of the business roadmap based on their own end customers' needs, eSentire has shown the capability to outpace the market in terms of their innovative, and transparent roadmap of services.

"A big part of why eSentire has shown value to us, in addition to the people, is how far ahead they are from a technology standpoint. At Venerable, we are very committed to leveraging cloud technologies and we need a partner whose people and technology are there first. eSentire's team has a roadmap that outpaces ours, and starts looking at technologies and solutions before we've begun to think about them. eSentire gets ahead of the direction that we're moving in before we know we're heading in that direction," added Scully.

As eSentire continues to grow its services portfolio, by expanding its multi-cloud expertise with MDR for Microsoft & MDR for AWS and deepening its Cyber Investigations capabilities with Incident Response Retainer offerings and Security Incident Response Planning (SIRP) services, organizations similar to Venerable will see considerable benefits in working with a trusted partner like eSentire that can offer end-to-end risk management.

Conclusion

Organizations within the insurance and financial sectors have a bullseye on their backs. Adversaries are targeting them not only due to the client data they store, but also because they are able to use protected policy and premium coverage data to negotiate on ransom payments with the downstream victims.

As more organizations adopt a multi-cloud strategy, it's imperative that they can keep up with the rate at which cloud technologies are evolving, the increased incidence of cloud misconfigurations, and the necessary security expertise required to get ahead of the threat curve.

A trusted security advisor like eSentire can help simplify multi-cloud security by providing seamless monitoring, scanning and control over your multi-cloud environment while delivering unmatched visibility, correlation and protection from cloud-specific threats.

eSentire prioritizes the detection of misconfigurations and suspicious activity in the cloud, so your in-house security team can focus on scaling business operations securely. By leveraging eSentire MDR as Venerable has, organizations can benefit from 24/7 threat detection and response as well as cloud security posture management solutions to secure their multi-cloud environments across the AWS, Microsoft, and Google Cloud platforms.

If you're experiencing a security incident or breach contact us  **1-866-579-2200**

eSENTIRE