eSentire MDR for AWS
Top APAC Investment Company

aws partner network

Executive Summary

Expanding applications, data and users continue to push the boundaries of security personnel and preventative controls. As attackers arm themselves with the latest malware and evasive tactics, under-resourced security teams face a nearly impossible task protecting business operations. Operating with increasing speed and precision, attackers are forcing all organizations to compliment preventative controls with advanced detection and response capabilities. While enterprise organizations have the budget and personnel to monitor environments and hunt attackers, most small and medium sized organizations are severely restricted with the resources available.

For over 20 years, eSentire has put small and medium businesses (SMBs)on the cutting-edge of protection against attackers that bypass traditional security controls. eSentire is the Authority in Managed Detection and Response (MDR) and we have absorbed the complexity of delivering enterprise-level cybersecurity to customers across the globe. Our MDR services deliver 24/7 protection powered by our proprietary XDR platform and expert threat hunters that investigate security events and shut down attackers on our customer's behalf.

Customer Challenge

A top investment organization based in the APAC region operates a large footprint within AWS. They were looking for a Managed Detection & Response partner, who could provide visibility into resources across their multiple AWS accounts and on-premise network infrastructure. In additional to resource visibility and misconfiguration assessment, threat hunting leveraging network, endpoint and vulnerability data was a key desired outcome. As this customer does not have a large security team or SOC, eSentire was uniquely positioned to provide our entire MDR portfolio, complimented by Managed Risk Advisory services, becoming an extension of the customer's security team.

eSentire MDR

eSentire's multi-signal MDR service provides the most in-depth detection, investigation and response capabilities for AWS. Signals from Cloud, Network, Log and Endpoint are ingested to the Atlas XDR pipeline, where cutting-edge machine learning enables distillation of threats at scale. SOC Analysts leverage a custom, purpose-built dashboard, which enables investigation and response across all signal types deployed within a customer's cloud and on-premise infrastructure.

MDR for Cloud

A Cloud Security and Posture Management solution is essential to understand the inventory of resources within AWS accounts, identify misconfigurations which can lead to breaches, evaluate adherence to regulatory frameworks and identifying unusual/suspicious user or endpoint behavior. eSentire's MDR for Cloud enables visibility across multiple AWS accounts, ensuring that customers have a consolidated view of AWS resources across all AWS accounts. SOC Analysts investigate potential threats and where appropriate, initiate a remediation action to mitigate the identified threat.

MDR for Network

eSentire MDR for Network is a zero latency Managed Network Detection and Response service that neutralizes attacks missed by traditional network security controls. Operating on a zero-trust philosophy, Network combines always-on full packet capture (PCAP) with proprietary attack pattern analysis and behavioral analytics to rapidly identify known threats and suspicious activity. Suspicious activity is investigated by eSentire's SOC Analysts, who confirm attacker presence and determine root cause.

About the customer:

- **AWS infrastructure spread across 12 AWS accounts & on-premise network**
- **eSentire services include MDR for Network, Log, Endpoint, Cloud, Vulnerability Management**
- **Initially found over 11K misconfiguration & alert conditions across AWS**
- **Worked with customer over 2 months to identify false positives and correct misconfigurations**
- **Customer averages 30 misconfiguration alerts a month, which eSentire remediates in most cases**
- **MDR for Log enables visibility into signals from AWS services such as GuardDuty, WAF & Shield**
- **eSentire 24/7 SOCs in Waterloo, Ontario and Cork, Ireland support customer**
- **eSentire's scalable MDR services enable the customer to grow their AWS footprint with confidence that new resources will automatically be included in monitoring**

MDR for Endpoint

Endpoint combines the power of elite threat hunting with Next-Gen Antivirus and Endpoint Detection and Response under a single agent to eliminate blind spots traditional technologies miss. Applying predictive threat modeling, eSentire experts continuously manage and tune preventative measures ensuring automated blocking of known, unknown and file-less attacks. Proprietary machine learning layered with an attack pattern and behavioral analytics engine, watches and records every activity, identifying suspicious actions and zero-day attacks. eSentire's threat hunters support the incident lifecycle including isolation of compromised endpoints, minimizing threat actor dwell time. As a result, your organization's endpoints are hardened against the latest known and unknown attacks protecting sensitive data while satisfying regulatory requirements.

MDR for Log

Powered by one of the industry's most powerful AWS hosted data analytics platforms, eSentire's MDR for Log aggregates and enriches logs from assets across your environment, providing the critical visibility required to detect advanced threats. A dedicated team manages the entire counterthreat content creation process, from the creation of detectors to the deployment of runbooks, ensuring your defenses evolve with the threat landscape. This empowers analysts from eSentire's 24/7 SOC to swiftly investigate and respond to events on your behalf, shrinking the dwell time of threat actors targeting your hybrid environment.

Managed Vulnerability Service

Managed Vulnerability Service identifies vulnerabilities with precision across traditional and dynamic IT assets such as mobile devices, OT, IoT, virtual machines and Cloud for full visibility across your business environment. eSentire experts are an extension of your team, providing analysis and guidance that facilitates accuracy of asset classification and lifecycle tracking with prioritization of risk contextual to your business objectives. Delivered as a flexible co-managed model, Managed Vulnerability Service alleviates the managerial burden for your team and provides continuous platform refinement and progress measurement. Your team receives full system access to run customized scans and reports for greater operational efficiency and satisfaction of regulatory requirements.

Results and Benefits

Having infrastructure spread across 12 AWS accounts, in addition to on-premise components, eSentire's MDR service provides a consolidated view of threats across networks. Leveraging eSentire's MDR for Network, Log, Endpoint, Cloud and Managed Vulnerability Service, SOC Analysts are able to investigate detected threats and provide remote remediation support 24/7. Upon initial deployment, eSentire discovered approximately 11,000 alert conditions within the AWS environment. Working with the customer, services were tuned to filter false positives and critical misconfigurations were remediated. The customer now averages 30 misconfiguration alerts a month, which eSentire remediates on their behalf in most cases. The customer is now growing their AWS footprint with confidence that any new resources are automatically discovered and included in eSentire's MDR service visibility.