CASE STUDY

ONESA - Scaling SOC Operations with AWS-Powered Trellix® Architecture

Company Overview

ONESA is a cybersecurity consultancy serving clients across multiple industries. As a consultancy, ONESA faces unique challenges in that they must be capable of implementing and managing diverse security solutions across varying client environments and requirements. The company has built its reputation on delivering sophisticated security postures, advanced email protection, server security solutions, and comprehensive SOC (Security Operations Center) assistance. Their business model requires deep expertise across multiple security platforms and the ability to rapidly adapt solutions to meet specific client needs and compliance requirements.

The Challenge

As a cybersecurity consultant, ONESA encountered numerous complex business challenges that required sophisticated, scalable solutions. These challenges were particularly acute due to the diverse nature of their client base and the varying security requirements across different industries and organizational structures.

Multi-Client Complexity:

- **Diverse Compliance Requirements:** Each client operated under different regulatory frameworks, requiring tailored security implementations that could meet various compliance standards including GDPR, HIPAA, PCI DSS, and industry-specific regulations
- **Varying Infrastructure Environments:** Clients maintained different technology stacks, cloud platforms, and hybrid architectures, necessitating flexible security solutions that could integrate seamlessly across diverse environments
- **Scalability Demands:** The need to provide consistent, high-quality security services across organizations of vastly different sizes and complexity levels

Technical Implementation Challenges:

- **Email Protection Complexity:** Implementing advanced email security solutions that could adapt to different email platforms and organizational communication patterns
- **Advanced Server Security:** Providing comprehensive server protection across on-premise, cloud, and hybrid environments while maintaining performance and accessibility
- **SOC Integration Requirements:** Delivering effective SOC assistance that could integrate with existing client security tools and processes

Operational Efficiency Needs:

- **Response Time Optimization:** Clients demanded faster incident response and threat analysis capabilities
- **Threat Intelligence Integration:** The need for real-time, actionable threat intelligence that could inform proactive security measures
- **Centralized Management:** Requirements for unified visibility and control across multiple client environments

The Solution

ONESA designed and implemented a sophisticated, multi-environment Trellix solution that leveraged AWS infrastructure to deliver scalable, high-performance security services across their diverse client base.

Comprehensive Trellix Security Stack:

- **Trellix Email Security:** Advanced email threat protection with machine learning-based detection and response capabilities
- **Trellix Helix Connect:** Central security operations platform providing unified visibility and orchestration across all security tools
- **Trellix Threat Intelligence:** Real-time threat intelligence feeds providing context and attribution for security events
- **Trellix Wise™:** Intelligent automation platform enabling advanced analytics and automated response capabilities
- **Trellix Data Security:** Comprehensive data protection across all data states and locations
- **Trellix Endpoint Security:** Advanced endpoint detection and response capabilities with behavioral analysis

Advanced Multi-Cloud Architecture: The deployment utilized a sophisticated hybrid architecture designed to maximize flexibility and performance:

Hybrid Infrastructure Components:

- **On-Premise Deployments:** Critical security functions maintained within client-controlled environments for sensitive operations
- **AWS Cloud Integration:** Leveraging Amazon Web Services for scalable, high-performance security operations
- **Multi-Cloud Flexibility:** Integration with other cloud platforms to accommodate existing client infrastructure investments

AWS Integration Details:

- **Amazon EC2 Implementation:** Utilized Amazon Elastic Compute Cloud instances to provide scalable compute resources for security operations, enabling dynamic scaling based on threat levels and client demands
- **Performance Optimization:** EC2 instances were optimized for security workloads, providing the computational power necessary for advanced threat analysis and machine learning operations
- **Geographic Distribution:** AWS regions were strategically selected to minimize latency and ensure optimal performance for clients across different geographic locations

Implementation Strategy

The deployment was executed in phases to minimize disruption while maximizing the speed of value realization:

Phase 1: Core Infrastructure

- Establishment of AWS-based security infrastructure using Amazon EC2
- Implementation of Trellix Helix Connect as the central orchestration platform
- Integration with existing client security tools and processes

Phase 2: Advanced Capabilities

- Deployment of specialized security solutions including Email Security and Endpoint Security
- Implementation of Trellix Wise for automated threat analysis and response
- Integration of comprehensive threat intelligence feeds

Phase 3: Optimization and Expansion

- Fine-tuning of automated response capabilities
- Optimization of AWS resource utilization for cost-effectiveness
- Expansion of capabilities based on client feedback and emerging threat landscapes

Results and Business Impact

The AWS-powered Trellix deployment delivered transformative results across ONESA's entire client portfolio:

SOC Operations Excellence:

- **Revolutionary Response Time Improvement:** SOC teams across client organizations experienced dramatic improvements in incident response times, with many achieving sub-minute initial response capabilities for high-priority threats
- **Enhanced Threat Analysis Capabilities:** By pairing Trellix Wise with AWS compute power, ONESA unlocked advanced threat analysis capabilities once out of reach, including advanced behavioral analysis and machine learning-based threat detection
- **Improved Accuracy:** False positive rates decreased significantly while true threat detection improved, allowing SOC analysts to focus on genuine security events

Operational Efficiency and Scalability:

- **Centralized Alert Management:** The implementation of centralized alerting through Helix Connect reduced alert fatigue and improved analyst productivity
- **AWS Scalability Benefits:** The ability to dynamically scale security operations based on threat levels and client demands provided significant cost optimization while maintaining performance
- **Multi-Tenant Efficiency:** The architecture enabled ONESA to efficiently serve multiple clients from shared infrastructure while maintaining security isolation

Financial and Business Benefits:

- **Cost Optimization:** AWS-based deployment reduced overall infrastructure costs while improving performance
- **Service Expansion:** Enhanced capabilities enabled ONESA to offer new, higher-value services to existing clients
- **Client Retention:** Improved security outcomes led to higher client satisfaction and retention rates

Strategic Expansion and Future Vision

The success of the initial deployment has catalyzed significant expansion opportunities:

Network Detection and Response (NDR) Expansion: Multiple clients are actively pursuing NDR solutions as the next phase of their security evolution. This expansion is driven by several factors:

- **Enhanced Threat Visibility:** Clients recognize the value of comprehensive network visibility to complement their existing security investments
- **Integration Benefits:** The proven success of native Trellix product integration through Helix Connect has demonstrated the value of a unified security ecosystem
- **Centralized Operations:** The effectiveness of centralized alert management has created demand for extending this approach to network security

Technology Integration Strategy:

- **Native Product Preference:** Clients are specifically requesting native Trellix products for new security capabilities, recognizing the integration benefits and operational efficiencies
- **Ecosystem Expansion:** Plans for comprehensive security ecosystem expansion that leverages existing Trellix investments
- **Advanced Analytics:** Interest in extending machine learning and advanced analytics capabilities to new security domains

AWS Infrastructure Evolution:

- **Enhanced AWS Services Integration:** Plans to leverage additional AWS services for improved security operations
- **Global Expansion:** Utilization of AWS global infrastructure to support international client expansion
- **Advanced Automation:** Implementation of AWS-native automation capabilities to further enhance security operations efficiency

This case study demonstrates how a strategic approach to security platform selection, combined with cloud infrastructure optimization, can create scalable, high-performance security operations that deliver exceptional value across diverse client environments.

aws PARTNER

Trellix is available in the AWS Marketplace.

Contact us today.