CASE STUDY

Real-time detection and response across 280 sites

The Challenge

- Limited visibility into OT Networks
- Disjointed Detection or Response capability across AWS & OT
- Poor network segmentation allowing large impact zones

The Solution

- AWS Cloud Trail, Guard Duty, & Security Lake in One tool with existing OT
- AWS hosted SaaS, whole network detection & response
- Automated Threat Detection and Response globally across AWS & private environments

The Results

- Auditable, accurate inventory of all connected assets in AWS and plants with network traffic profiles
- Single NDR tool integrated with existing security stack covering IT & OT across 280 locations in 70 countries
- Real-time anomalous activity alerts across AWS and physical

Industry Consumer & Packaged Goods Manufacturing

Location New York City HQ

Size 34,000 employees; $20B+ annual revenue

"Now there's no need to look at each point solution and aggregate that information manually. When we look at the OT environment, we don't have to pivot to those tools. The Armis dashboard brings in the data from and enables us to view it through a single pane of glass, which minimizes our need to look at different interfaces. It's a great feature, and something Armis does really well."

Rafia Noor
Sr. Security Engineer

Executive Summary

Colgate leveraged Armis Centrix to See, Protect, and Manage their IT assets in AWS and on premises but struggled to do the same for their OT Network. Their networks did not share event information or correlate risk across environments. This caused delays to remediation tasks from lack of context and potential impact. Central IT's hybrid environment had many strong security tools including AWS GuardDuty, AWS Cloud Trail, and plans for Security Lake but lacked full cloud to ground detection and remediation capabilities. Many OT networks operated with low visibility across diverse, unique assets and little/no secure cloud connections.

Armis demonstrated how Colgate could gain full visibility to all network devices and traffic in both their AWS and distributed OT environments through a single SaaS platform running in AWS. This implementation reduced IT incident response mean time averages from over an hour to under 5 minutes. Real-time alerts now trigger for any unauthorized changes in the distributed OT environment or AWS environments. Alerts from AWS native services are correlated and deduplicated with OT alerts finding anomalous behavior across the consolidated environment in a single pane of glass where any instance of unauthorized access or network volume change is alerted instantly.

Background

Colgate-Palmolive has been supplying hundreds of millions of consumers all over the world with personal care, household, healthcare, and veterinary products. The company has over 60 locations in the U.S. and 280 locations in more than 70 countries overseas.

While Colgate-Palmolive has a large, seasoned security team overseeing IT in AWS and on-premise, the operational technology (OT) security team is newer, focused on evolving and growing. AWS & Colgate saw the value received through their native security services within AWS and wanted similar value across their on-premise OT environments. Security Engineers Rafia Noor and Shem Stephens

© Copyright Armis 2024

280 sites across 70 countries

AWS, Data Centers, & OT networks protected with 1 platform

10's

of thousands of employees and over 500k employees globally

Security audits of any site in the world compared to established standards

Automated remediation anywhere in the world enabled with MTTR under 10 minutes

led the OT efforts with IT and AWS. They successfully brought a centralized NDR solution to all of the organization's more than 40 manufacturing plants and ever growing list of Availability Zones.

Discovering the Unknown

Immediately, Armis encountered several on-premise devices the team was not aware of. Noor and Stephens noted the manufacturing plants are always adding new technologies leading them to spot check the OT network and supporting AWS environments with Armis for security vulnerabilities. This increased visibility enabled even faster remediation when incidents were detected.

"*From an overall security perspective, visibility into the manufacturing area was a big thing for us. We needed a tool to see what our plants are doing in order to better support them and Armis fit the bill perfectly,*" explains Stephens.

Colgate is now evaluating VPC mirroring within AWS. AWS will enable discovery of traffic anomalies and attacks between and within VPCs. Armis' will ingest this traffic pattern information from AWS and compare it to Armis' global asset intelligence database. By comparing ingested information to the database, Armis can identify anomalous traffic patterns & behaviors of cloud assets to manage vulnerabilities & risks even more effectively.

Armis differentiates from the Competition

Colgate-Palmolive chose Armis because they saw something unique in the market, a single tool that provides visibility into AWS native security services, on-premise IT, and OT in physical plants around the world.

"*In my experience, this is where these [Armis] tools really stand out,*" says Noor. "*It provides the complete picture. The cloud infrastructure and ease of management is huge*"

Armis' ability to integrate with existing AWS & on-premise security tools, including AWS GuardDuty and Cloud Trail, made it a wise investment for Colgate-Palmolive. Once IT adopts AWS Security Lake, OT will be ready with Armis' native OCSF integration. AWS was able to address security concerns in the cloud. Now all security concerns can be addressed within Colgate's AWS cloud.

Results

After a successful proof-of-value (PoV), the OT security team deployed Armis to monitor and protect close to 1 million devices across its manufacturing locations, data centers, and AWS.

"*Armis provides a broad-sweep view of the devices and traffic, enabling us to visually comprehend what devices we have and effectively respond to detected incidents anywhere.*"

– Rafia Noor, Sr. Security Engineer

Colgate-Palmolive's security team uses many built-in policies and creates their own custom network policies leveraging AWS native services in cloud and throughout each of their plants to enhance their global security practice and better detect adversaries, everywhere.

ARMIS®

1.888.452.4011
www.armis.com

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.