paloalto NETWORKS | CPSP

CASE STUDY

Knutsen OAS Shipping

DataEquipment

Norwegian Shipping Company Reinforces Entire Security Platform While Consolidating to One Supplier with Aid from Data Equipment Services

Industry
Transportation (Commercial Shipping)

Company
Knutsen OAS Shipping

Challenge
Move from a multi-vendor existing legacy system, to a consolidated state-of-the-art security solution

Answer
Engage Data Equipment to help overcome current security solution limitations and fragmentation

Results

- Migrated to a next-generation security platform forming an ecosystem for all cloud (and on-premise) end points and firewalls
- Replaced blacklisting with application and URL whitelisting together with dynamic address groups
- Achieved required scalability and full visibility of internal and external traffic for a complex company that has "floating branch offices"
- Achieved the IMO guidelines and compliance as defined by the "The Guidelines on Cyber Security Onboard Ships*" v3 regarding the network and security

Products and Services

Data Equipment, a PAN Certified Partner

- Consulting; project management; design; systems integration; testing, education
- Panorama deployment; all FW in HA deployment
- Transformation Services; BPA; Periodic Health Check

Palo Alto Products

- Cortex Data Lake, Premium Support, Threat Prevention, URL Filtering, WildFire (headquarters, branches,vessels); GlobalProtect Gateway and DNS Security (headquarters)
- (1000 Licenses) Cortex XDR Pro; (5 TB) Cortex XDR; (10 TB) Cortex Data Lake; (~100) PA-220 in 50 different location; (2) PA-3220; Panorama

Organization

Established over 120 years ago in Norway, Knutsen OAS Shipping has one of the largest commercial fleets in Europe.

The fleet consists of shuttle tankers, LNG carriers, and product tankers. Knutsen OAS Shipping, a division of the Knutsen Group, invests heavily in advanced technology and quality vessels to ensure the safety, security, and protection of its clients' transportation of goods- as well as Earth's wellbeing. The company's advanced technical investment strategy also applies to their security strategy.

Moving a Complex Organization to a Next-Generation System

Knutsen OAS Shipping needed a new supplier that could provide a complete, superior network security system.

Previously, the company had different suppliers, and the current security system lacked the ability to oversee, safeguard, and secure the entire VPN and communications platform.

"We are a relatively complex company to work with in terms of security and VPN solutions. Our company is headquartered in Norway with offices around the world, and we have more than 45 ships which are considered "branch offices". These ships, or branch offices, are in constant motion and can be anywhere in the world. This business model creates network complexity not seen in ordinary businesses," states Nils Johan Gabrielsen, Cyber Security Manager, Knutsen OAS Shipping.

The IT department set out to identify a professional services firm that could handle a customized deployment of its next security system, and to find a supplier that was at the forefront of development in cybersecurity.

Knutsen OAS Shipping Turns to Data Equipment and CIS Top 20 Guidelines

Knutsen OAS Shipping IT leaders engaged Data Equipment to build a customized superior security system.

"We learned how Data Equipment security engineers could bring their training and expertise to design, configure, and deploy a sophisticated solution to address our complex structure—including protecting our floating offices," says Nils Johan Gabrielsen.

Data Equipment, in turn, recommended the complete security portfolio from Palo Alto Networks together with necessary and value-added software subscriptions.

Data Equipment is a Certified Professional Services Partner, accredited by Palo Alto Networks.

Data Equipment and Knutsen OAS Shipping engineers got to work on designing and configuring a customized solution. The engineers strictly adhered to the Center for Internet Security (CIS) Top 20 Guidelines 7.1**.

These guidelines are designed to prioritize the myriad of security controls that are available for cybersecurity, and tested by CIS for "what really works".

The workstream goals included:
1. Shutting down all vulnerable points of entry
2. Reducing infrastructure costs by eliminating several suppliers
3. Obtaining centralized administration and visibility of the organization's firewalls
4. Future-proofing the network

Using Advanced Artificial Intelligence (AI) to Focus On Real Threats

The team compiled and integrated the Palo Alto Firewalls, Cortex XDR Pro, and Cortex Data Lake to fortify the network security.

"To meet the project goals, Cortex XDR was a key component. The Palo Alto Networks application uses artificial intelligence to detect the root cause of sophisticated attacks, helping to speed up the investigation. Based on machine learning, the application also eliminates most non-real threats so that Knutsen OAS Shipping engineers can focus their time on true potential attacks," explains Thomas Brodersen, Sales Manager Large Enterprise, Data Equipment.

The team then added Proofpoint (a secure email gateway product) and Duo MFA (a multi-factor authentication service) to provide an additional layer of security before employees log into various applications and websites.

"We've been working on this project for almost two years. It has been an incredibly exciting project. It has given us insight into security solutions that support a slightly unusual, but advanced organization, with high technical requirements," summarizes Brodersen.

A Deployment Complication and an Innovative Fix

Cortex XDR:
During the deployment, Knutsen OAS Shipping experienced a few false positives that were verified, and exceptions were then constructed.

"On the flip side, the visibility with Cortex XDR is amazing! For example, Knutsen OAS Shipping has implemented BIOC rules that examine PST files and identify those that are not part of the domain (a business policy violation) enabling them to act," says Kim Hansen, Solutions Specialist Security, Data Equipment.

Device Security: Knutsen OAS Shipping previously had a Cisco firewall which was port-based and blacklisted IP addresses without providing visibility.

To solve this problem, Data Equipment engineers:

- Replaced outdated firewall rules with app-id based whitelisting rules and URL-filters together with dynamic address groups and outgoing decryption of traffic
- Established region blocks to-and-from specific countries identified as high threats

Vessel Application Performance: When out to sea, a ship's bandwidth is generally limited to between 380kbit to 5mbit for up to 30 employees on any given vessel.

To address this issue, the team:

- Applied PAN Best Practice Assessments several times during the project to visualize and optimize the configuration for performance
- Implemented dynamic address groups for public Wi-Fi to blocks all outgoing traffic up to 24 hours if the device/guest is trying to bypass the security policies
- Implemented dynamic address groups to block inbound IP for 5000 minutes if an attacker is attacking with known vulnerabilities or tries to connect on any unauthorized ports or application e.g. ssh, rdp, sql or vnc

Results that Exceed Expectations

Data Equipment delivered a total security package, with forward-looking functionality. With its new system, Knutsen OAS Shipping protects clients and servers. The security tools also provide the IT team with data analytics and complete control and visibility of its network traffic, all from one supplier—Palo Alto Networks.

"The biggest gain is that we now have a highly effective solution that gives us full visibility, something we lacked with our previous solution. And more importantly, we have a stable and secure solution that we can trust and which in the literal sense of the word, "holds water", no matter where our ships are located across the oceans."

— Nils Johan Gabrielsen, Cyber Security Manager Knutsen OAS Shipping

Corporate Social Responsibility

Knutsen OAS Shipping
Knutsen OAS Shipping (along with its parent company Knutsen Group) is committed to the environment.

Knutsen maintains a "zero commitment" including zero environmental spills, zero material damages, and zero work-related illnesses or injuries.

To achieve their commitment, the Knutsen Group continuously works on its Health, Safety, Security, Environment, and Quality Assurance practices.

Data Equipment
Data Equipment leverages technology to minimize the waste of resources and protect the environment, relying on digital processes as much as possible.

Notes
* URL reference for the Guidelines on Cyber Security Onboard Ships:

https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-on-board-ships

**URL reference for the CIS Controls:

https://www.cisecurity.org/cybersecurity-best-practices/

Learn more about Knutsen OAS Shipping and Data Equipment:

Knutsen OAS Shipping- https://knutsenoas.com/

Data Equipment- https://www.dataequipment.no/

paloalto NETWORKS | CPSP