CASE STUDY

Leading Dutch Maritime Communications Provider Fortifies Managed Network Service Solutions with Cybersecurity Platform Approach

Castor Marine is a leading satellite service provider and teleport operator, providing a suite of Global Connectivity Services, which are seamlessly integrated and managed through Fortinet's online portal. These include Global VSAT Ku-band services based on a fully owned and operated global Ku-band network Starlink OneWeb, in addition to L-band and 4G LTE services. Castor Marine's IT services include the design, implementation, and support of IT systems on board and SD-WAN solutions to connect fleets to the internet.

Castor Marine operates worldwide and offers installation, integration, and real-time monitoring of internet traffic, reliable connectivity solutions, and all related IT systems. To guarantee global coverage, Castor owns and operates several teleports.

For all systems and equipment, Castor offers a broad range of services, including 24×7 support, maintenance, spare parts, and training. Services include the design, implementation, and support of IT systems onboard and SD-WAN fleet connectivity solutions. The company's professionals are fully certified to work onboard worldwide.

The Cybersecurity Challenges of the Maritime Industry

With around 90% of the world's traded goods carried by shipping, the collective reliance on the maritime industry is hard to overstate, even though this dependence is only noticed when things go wrong—for example, when an oil tanker runs aground or when the Suez Canal is blocked by a 220,000-ton container ship.

Given the accelerating digitalization of the sector and with trials of the first Maritime Autonomous Surface Ships (MASS) already underway, it is no surprise that cybersecurity is becoming a top priority for all shipping operators and is subject to increasing regulations.

Maritime compliance mandates are defined and verified by the International Maritime Organization (IMO), Lloyd's Register, and DNV GL, which publish and maintain rules and guidance concerning the safety and security of shipping and its supply chain.

At a global level, since January 2021, IMO resolution MSC.428(98) now requires cybersecurity in all shipping company management systems. In addition to this, many insurers stipulate minimum cybersecurity standards as a prerequisite for coverage.

"To be able to deliver secure and reliable, global internet with hybrid, future-ready, managed network and IT services to our customers, it was essential for security to be integrated at the network level. We needed a solution in which any new addition or extension to the network would be intrinsically secure and immediately manageable from our central operations center."

Mark Olthuis
Managing Director
Castor Marine

Details

Customer: Castor Marine

Industry: Technology provider

Location: The Netherlands

Business Impact

- Increased reliability and security of customers' managed IT, network, and communications services
- Increased operational efficiency through centralized visibility and control

Consequently, for Castor Marine's customers, the security of all managed network services is expected to be as multi-layered and as impenetrable as the ship's hull.

Integrated Cybersecurity by Design

With mobile and cloud computing reducing the effectiveness of traditional perimeter-based approaches to cybersecurity, Castor Marine was looking for a new security architecture in which the expanded digital attack surface of a modern shipping fleet would always be fully protected against the latest threats.

"To be able to deliver secure and reliable global internet with hybrid, future-ready managed network and IT services to our customers, it was essential for security to be integrated at the network level," explains Mark Olthuis, Managing Director for Castor Marine. "We needed a solution in which any new addition or extension to the network would be intrinsically secure and immediately manageable from our central operations center."

A Cybersecurity Platform Approach

Having evaluated all the available options and consulted the reports and recommendations from leading analyst firms, Olthuis chose Fortinet as the basis not only for all the below-deck IT managed services delivered to customers but also for the backbone infrastructure linking Castor Marine's four corporate office and teleport locations.

Fortinet's solutions are delivered through the Fortinet Security Fabric cybersecurity platform, intelligently combining the capabilities and threat data from multiple security elements to deliver broad, integrated, and automated protection across the entire digital attack surface.

This reduces the complexity of supporting multiple point products, increases operational efficiency through automated workflows, and enables broad visibility across all of Castor Marine's deployments, from its corporate infrastructure to myriad managed onboard networks of shipping clients around the world.

The Fortinet Security Fabric leverages external threat intelligence from FortiGuard Labs, which collates and processes the data from a huge number of anonymized sensors and partners from around the world using artificial intelligence and machine learning to identify unique features for both known and unknown threats.

Onboard wide area network (WAN) requirements for Castor Marine's customers are fulfilled through FortiGate Next-Generation Firewalls (NGFWs) interconnected via a combination of satellite and 4G/5G communications links, thanks to FortiExtender. For customers operating fleets of ships, FortiGate integrated software-defined wide area network (SD-WAN) functionality provides a secure, highly reliable, and cost-effective connectivity solution with simultaneous access to cloud-based applications and the internet.

To further maximize performance, its dedicated custom security processing unit (SPU) allows FortiGate NGFWs to identify thousands of different applications quickly and accurately, enabling fast, intelligent traffic steering, enhanced quality of service, and rapid application-aware security processing.

"The performance and granular traffic control of the FortiGate Next-Generation Firewalls was a key factor for us," adds Olthuis. "Since the throughput of satellite communications is so much lower than terrestrial alternatives, it's doubly important to make optimal use of all available bandwidth."

Business Impact (cont.)

- Reduced corporate exposure to risk through enhanced security and performance of backbone infrastructure

Solutions and Services

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiAP
- FortiClient
- FortiAuthenticator
- FortiToken
- FortiManager
- FortiAnalyzer
- FortiExtender

"The performance and granular traffic control of the FortiGate Next-Generation Firewalls was a key factor for us."

Mark Olthuis
Managing Director
Castor Marine

For consistent policy enforcement of both wired and wireless access onboard, Castor Marine's managed services also include FortiSwitch and FortiAP wireless access points. As well as adding ultra-reliable, switched and Wi-Fi coverage to any environment, both devices are managed through FortiManager (which includes an integrated wireless LAN controller), consolidating access management under a single console and thereby greatly reducing administration complexity.

For increased endpoint security as well as VPN client access for Castor Marine's internal staff, FortiClient endpoint software was deployed in conjunction with FortiAuthenticator and FortiToken.

Although FortiGate NGFW already includes integrated authentication server functionality, the addition of FortiAuthenticator extends the range of user identification methods and increases scalability.

FortiToken, available both as an OAuth-compliant one-time password (OTP) generator application for mobile devices and as a key fob physical device, provides a convenient solution for ultra-secure token provisioning using dynamically generated token seeds.

To further simplify the overall management of Castor Marine's internal infrastructure as well as that of its customers, FortiManager was deployed at headquarters to provide single-pane-of-glass visibility and control and minimize the time taken to add or replace network components.

"One of the challenges for us which you don't have with land-based installations is that physical access to our customers' networks is usually limited to their time spent in port," says Olthuis. "Through FortiManager, we can now prebuild device configuration templates so that once the ship docks, any new equipment additions or replacements can just be plugged in, and, after a minute or so, they're all configured and ready to go."

For enhanced analytics and reporting and to help ensure IMO compliance, FortiAnalyzer was also deployed. Using threat intelligence from FortiGuard Labs to identify problems in real time and leveraging its built-in analytics engine to correlate that with data collected from across the Fortinet Security Fabric, FortiAnalyzer also gives Castor Marine the power to automate responses to many potential problems.

August 31, 2023 12:35 AM

2259604-0-0-EN