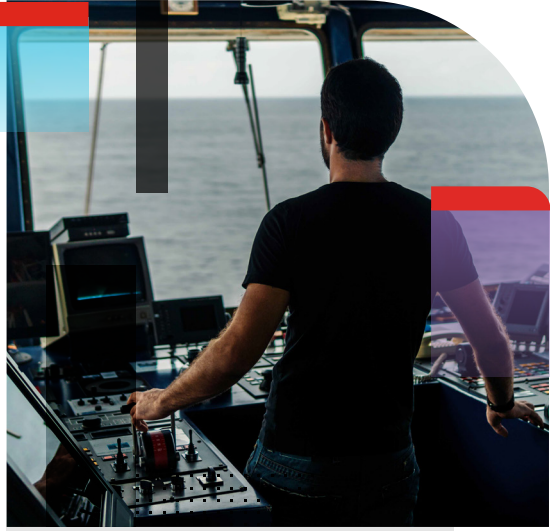
CASE STUDY

# Dutch Maritime Systems Integrator Fortifies Operations With New Integrated Security Architecture



With a proud heritage dating back to 1860, RH Marine is today recognized as a leading systems integrator and innovator of electrical and automation systems for the maritime industry.

Serving both defense and private sectors, the company provides a full range of solutions and services, including project management, consultancy, system design, engineering, commissioning, installation, site management, training, and support.

Through expert end-to-end support and advice across the entire life cycle of the ship, whether a naval frigate or a private super-yacht, RH Marine is able to ensure safe, sustainable, and cost-efficient continuity of operations for all its customers.

Cognizant of its responsibility not only to shareholders but to the environment and local communities, RH Marine continually explores the potential of innovative new technologies that will lead the industry toward a more efficient, greener, and safer future.

## The Cybersecurity Compliance Challenges of a Maritime Systems Integrator

For the maritime industry, classification and compliance mandates are defined and verified by organizations such as the International Maritime Organization (IMO), Lloyds Register, and DNV, 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 requirement for coverage.

For RH Marine, there are further, even stricter and more numerous cybersecurity requirements to be met.

## Integration of Operational Technology

For the factory (as for much of the equipment deployed to ships) there are also the unique security considerations of operational technology (OT) and its control systems.

Previous strategies of maintaining physical isolation between OT and information technology (IT) environments, the so-called “air gap” or “sea gap” as it is known in the maritime industry, are no longer viable given the prevalence of Ethernet connectivity, the need for regular software updates, and the potential business advantages of digital integration.

*“The number of vendors that met all our requirements as maritime system integrator in the naval and yachting industry was already limited, but Fortinet had clear advantages in terms of licensing, feature breadth, and above all, integration, through the Fortinet Security Fabric.”*

– Ramon Mastenbroek, Security Architect, RH Marine

## Details

**Customer:** RH Marine

**Industry:** Manufacturing

**Location:** Netherlands

## Business Impact

- Enhanced security, performance, and reliability of operations
- Enabled the integration of IT and OT
- Improved operational efficiency through integration of NOC and SOC

## A New Architecture for Performance, Efficiency, and Security Compliance

As part of RH Marine's ongoing efforts to improve the performance, efficiency, and security of its operations while maintaining the strict compliance required, the company recently decided to upgrade the network security architecture for its workshop, data centers, and branch offices.

After a thorough evaluation of competing solutions, RH Marine selected Fortinet.

"The number of vendors that met all our requirements as a maritime system integrator in the naval and yachting industry was already limited," admits Ramon Mastenbroek, security architect for RH Marine, "but Fortinet had clear advantages in terms of licensing, feature breadth, and above all, integration through the Fortinet Security Fabric."

The Fortinet Security Fabric brings an advanced range of capabilities that emerge from the tight integration among Fortinet products. It addresses the security challenges of organizations such as RH Marine by providing broad visibility and control of the digital attack surface to minimize risk, reduce the complexity of supporting multiple point products, and increase the speed of operation through automated workflows.

The secure interconnection of RH Marine's nine sites and two data centers was accomplished through FortiGate Next-Generation Firewalls (NGFWs), with FortiAP wireless access points complementing the FortiGate's integrated Ethernet ports to provide seamless endpoint connectivity across each local area network (LAN).

With its purpose-built security processors, the FortiGate NGFW has the power needed to identify thousands of applications inside network traffic and apply deep inspection and granular policy enforcement. This ensures that all of the traffic from RH Marine's OT manufacturing and test systems, as well as from all its other applications, are easily processed, optimized, inspected, and protected against potential threats without introducing latency into the network.

### Solutions

- FortiGate
- FortiClient
- FortiToken
- FortiNAC
- FortiAP
- FortiSandbox
- FortiManager
- FortiAnalyzer
- FortiSIEM

*"Although we've enabled pretty much all the advanced protection functionality available, the FortiGate NGFW just seems to take it all in its stride. In fact, application performance has actually increased in spite of all the extra security processing going on."*

– Ramon Mastenbroek, Security Architect, RH Marine

"Although we've enabled pretty much all the advanced protection functionality available, the FortiGate NGFW just seems to take it all in its stride," adds Mastenbroek. "In fact, application performance has actually increased in spite of the extra security processing going on."

For increased endpoint security as well as VPN client access for remote workers, FortiClient endpoint software was deployed in conjunction with FortiNAC and FortiToken.

FortiNAC, which is Fortinet's network access control solution, enhances the Fortinet Security Fabric with improved visibility, control, and automated response for everything that connects to the network, including Internet-of-Things (IoT) and third-party devices.

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

Although the FortiGate NGFW includes integrated authentication server functionality, RH Marine opted for the extended capabilities of FortiAuthenticator, with its greater range of user identification methods and increased scalability.

To increase protection from zero-day vulnerability exploits and other previously unencountered threats, RH Marine also deployed FortiSandbox. With artificial intelligence (AI)-powered malware analysis, advanced reporting, and investigative tools, as well as automated breach protection, FortiSandbox provides an essential added layer of defense, further enhancing the security, safety, and reliability of RH Marine's network infrastructure.

The solution leverages external threat intelligence provided by FortiGuard Labs, which collates and processes the data from myriad anonymized sensors and over 200 global partners around the world using AI and machine learning (ML) to identify unique features for both known and unknown threats.

*"The Fabric Management Center is incredibly powerful. Not only can I see at a glance the overall health, status, and security of the network, but it significantly reduces the time spent responding to security threats and other network disruptions."*

– Ramon Mastenbroek, Security Architect, RH Marine

## Integration of NOC and SOC

To provide centralized management, network automation, orchestration, and analytics across the entire Fortinet Security Fabric, RH Marine added FortiManager, FortiAnalyzer, and FortiSIEM, which combine to form the Fortinet Fabric Management Center.

With its single-pane view, FortiManager helps simplify oversight of the security infrastructure and automate responses to potential problems. FortiAnalyzer enables the application of FortiGuard Labs threat intelligence to identify problems in real time and correlate threat intelligence across the Security Fabric, leveraging its built-in analytics engine.

FortiSIEM adds powerful security information and event management (SIEM) capabilities, bringing together visibility, correlation, automated response, and remediation into a single, scalable solution. This reduces the complexity of managing network and security operations to effectively free resources and improve breach detection and prevention.

The resulting architecture combines the analytics traditionally monitored in separate silos of the security operations center (SOC) and network operations center (NOC) to provide a more holistic view of the security and availability of the entire business.

"The Fabric Management Center is incredibly powerful," concludes Mastenbroek. "Not only can I see at a glance the overall health, status, and security of the network, but it significantly reduces the time spent responding to security threats and other network disruptions."

FORTINET

www.fortinet.com



October 20, 2021 1:00 AM
1279751-0-0-EN