INDUSTRY BRIEF

Securing the Maritime Industry

Fortinet Cybersecurity Enables and Protects Maritime 4.0

Challenges

The digital transformation initiative propelling Maritime 4.0 is revolutionizing the shipping industry by modernizing fleets and terminal operations. This digital revolution is helping shipping companies compete by optimizing ship operations and voyages, improving ship system efficiency, lowering their environmental footprint, and reducing fuel consumption and costs.

Maritime 4.0 enables terminal operators to aggressively invest in automation to modernize port infrastructure, increase cargo throughput, and meet environmental clean air restrictions.

What does digital transformation actually entail for the maritime industry?

- Increased networking and connectivity like ship-to-shore communications, IT-OT connectivity, remote control of offshore and onboard operations, cloud applications, and more
- Ship bridges as automation control centers with navigation, cargo information or declaration, administrative data, and more
- Smart ships and intelligent fleets with route planning, unmanned shipping, the EU Sea Traffic Management initiative seeking to synchronize shipping operations using communications, networking, and “Big Data” capabilities
- Intelligent and linked subsystems using industrial automation with a ballast water system, alarm and monitoring systems, and more
- Unifying network technology for advanced ship systems; for example, in the case of reefers, allocating ship costs according to the source rather than uniformly distributed
- Increase in connected IoT to support terminal modernization like cargo handling, cranes, semi-autonomous vehicles, robotics, and cargo tracking

Highlights

- Comprehensive and unified security solution
- Robust visibility and protection
- Unified management
- Simplified deployment
- AI-driven threat intelligence
- Intelligent network segmentation
- Secure SD-WAN
- Safeguard critical infrastructure and OT/IT

As shipping companies execute their digital transformation strategy, their business and systems naturally become more open and connected. As a result, the attack surface expands and increases their vulnerability to cyber threats. Furthermore, the complex and distributed nature of a shipping company’s network environment, with each area having its own unique set of IT requirements, introduces security gaps favoring the proliferation of cyberattacks.

Moreover, the critical control systems that ensure the safety and smooth running of onboard and terminal operations are increasingly under attack. Because of their connectivity to IT environments, OT systems have become visible to hackers, allowing them to exploit the security vulnerabilities within their environment.

Transforming Cybersecurity

In order to support and securely adopt these new technologies, the maritime industry needs to rethink its cybersecurity posture and move toward a seamless, comprehensive, and zero-trust strategy.

As shipping companies adapt their IT and OT infrastructure to account for digital transformation, they must also undergo a security transformation to protect against the evolving cyber threat landscape–the biggest risk to digital transformation.

Fortinet provides companies in the maritime industry with a proactive and transformative approach to cybersecurity. It is called the Fortinet Security Fabric (Figure 1). It provides protection that is broad, integrated, and automated.

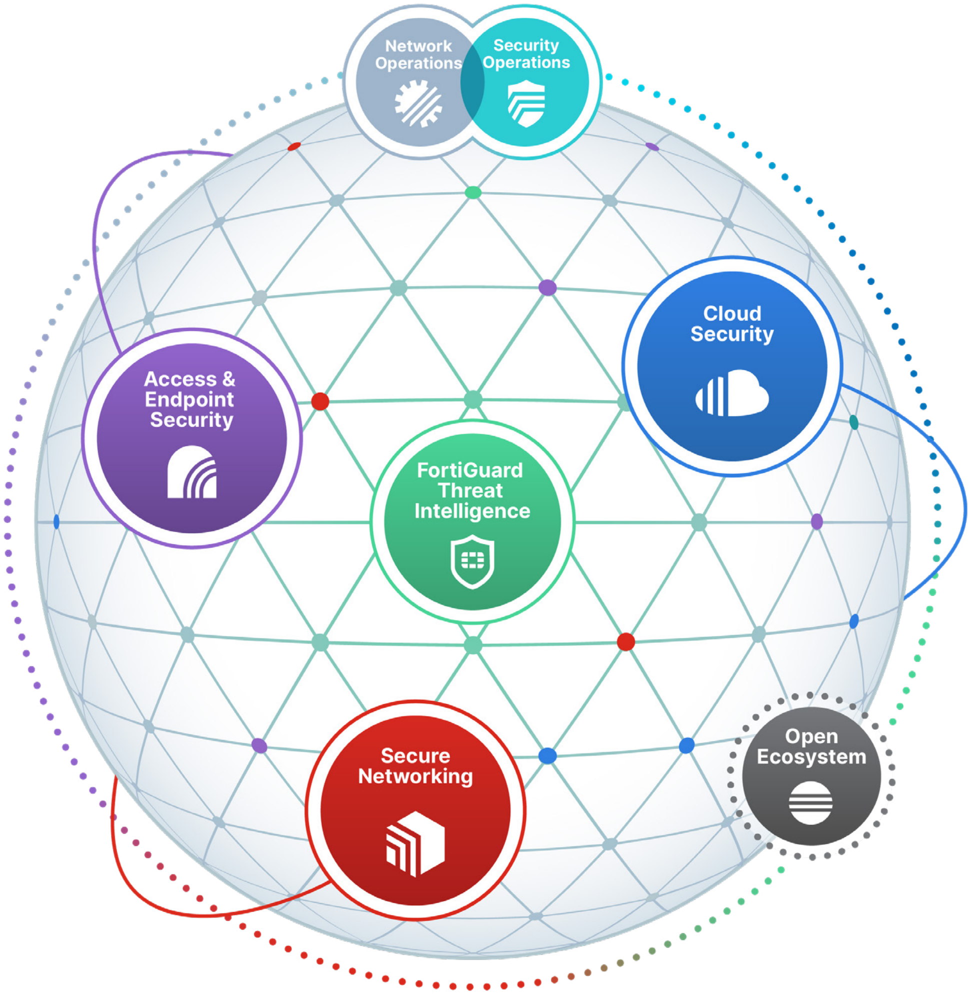

Figure 1: Fortinet Security Fabric.

Broad

Visibility and protection of the entire digital attack surface to better manage risk.

Integrated

Solution that reduces management complexity and shares threat intelligence.

Automated

Self-healing networks with AI-driven security for fast and efficient operations.

The Fortinet Security Fabric in Action for the Maritime Industry

From secure software-defined wide-area network (SD-WAN) access to intelligent network segmentation, the Fortinet Security Fabric ensures that critical resources and data are protected, business activities are uninterrupted, and operational costs optimized.

Single Box Solution

FortiGate firewall solutions are compact, cost-effective, all-in-one security appliances that reduce the complexity and risks of multivendor solutions. They include high-performance firewall, virtual private network (VPN) functionality, intrusion protection system (IPS), application control, URL filtering, antivirus, antispam, and integrated wired and wireless capabilities—and are easily managed via a single console.

Ease of Deployment

Fortinet's solution for the maritime industry addresses one of the major issues in a shipping company's environment—easily deploying technology to multiple remote locations, including ships, within a fleet with no on-site expertise. Through the use of FortiDeploy, Fortinet's cloud-based deployment and management solution, remote ships within a fleet can be easily configured centrally. Once shipped to the remote location, all that is required is to plug in the cables and power it on.

Intelligent Network Segmentation

With Fortinet's solution, segmenting the network and devices is about assigning policies and managing risk:

Identify Risk: With Fortinet's intelligent segmentation, users, data, devices, locations, and a host of other criteria can be used to identify categories and assess risk.

Manage Policies and Devices: The Fortinet solution can provide the granularity to see all device activity and set policies appropriately. It also has the flexibility to set policies by type of device or by users and traffic type.

Exert Control: The Fortinet solution can secure critical network zones and grant device privileges, based on the risk profile, without compromising other segments of the network.

Unified Management

Day-to-day management of the Fortinet solution is simplified by a single-pane-of-glass management capability. Regardless of the mix of products or configuration at an individual site, all aspects of control and configuration are handled centrally to reduce complexity and improve day-to-day operations.

Secure SD-WAN

Fortinet makes it easy to deploy and manage the right security in the right place with our Secure SD-WAN solution. The solution links network and security paths across the world through the internet, Wi-Fi, 3G/4G/5G, or SATCOM links, making it easy to switch between satellite connections at sea and Wi-Fi or cellular at the port. It provides application visibility for encrypted traffic and smart load balancing that helps to reduce WAN cost without impacting the service-level agreement for business applications.

Real-time Actionable AI-driven Threat Intelligence

Powered by FortiGuard, Fortinet's solution for the maritime industry receives tailored threat intelligence data to mitigate malicious activities. The consolidated architecture enables fast reaction times to security incidents. With each Fortinet appliance receiving security updates from FortiGuard, elements can rapidly exchange threat intelligence, ensuring that end-to-end, seamless security and coordinated actions are maintained for an automated response to threats. The power of FortiGuard is the culmination of people, in-house and patented technology, and experience.

Safeguarding Critical Infrastructure

The Fortinet solution unifies the best of current IT network security capabilities with an extensive understanding of the OT world and its processes and protocols by providing:

- Zero-trust network access
- Secure physical to digital transformation
- Top-rated, industrial-control-specific protection from advanced threats
- Broad visibility
- Integrated detection
- Automated response

Fortinet for the Maritime Industry

Fortinet solutions are designed for zero-touch deployments and seamless integration of multiple technologies with the operational efficiency that is critical for day-to-day shipping operations. Connectivity is at the heart of the shipping environment—wireless and wired networks must be secure, reliable, and easy to deploy and manage. Extending onshore security policies to the vessel is a critical part of protecting against advanced threats and must be an inherent part of a shipping company's network architecture.

Summary

Fortinet's solutions allow shipping companies and terminal operators to ensure vessel safety and reliability while improving terminal efficiency. Once in place, these solutions provide a platform for future growth with minimum disruption. Securing Maritime 4.0 is more than just securing a ship or terminal against cyberattacks; it also entails crew safety and operational safety.

www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 24, 2022 5:59 AM
954576-A-0-EN