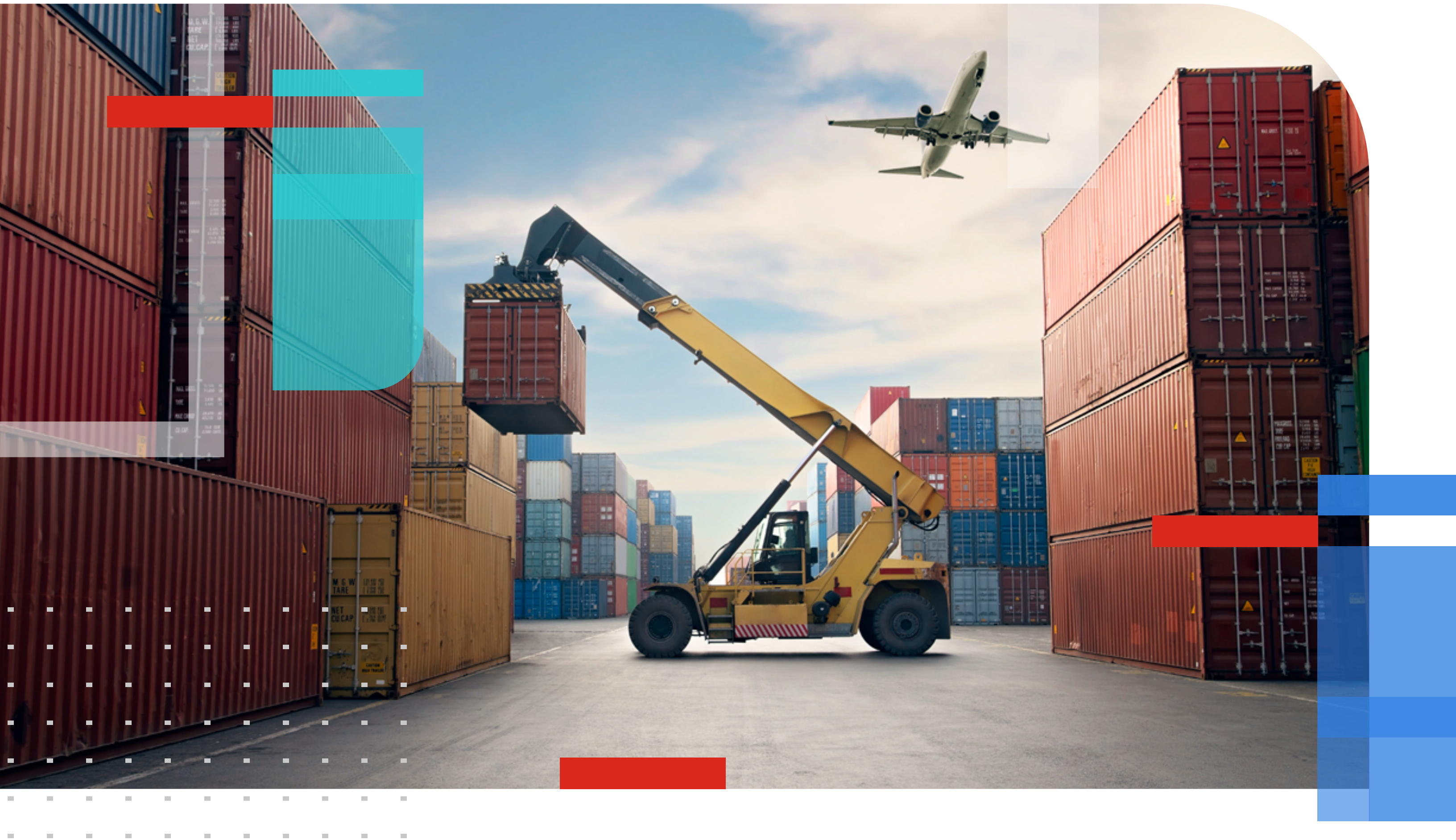
SOLUTIONS OVERVIEW

# Fortinet Transportation and Logistics Cybersecurity Solution

## Safeguarding Air, Rail, and Maritime Control Systems



## Executive Summary

The transportation and logistics (T&L) industry is in the midst of business transformation. This change is being driven by the need to improve delivery time, sustainability, and customer experience to avoid unexpected disruption and allow a simple flow to the final destination.[1] To address growing global freight demands, T&L companies are modernizing their infrastructures and systems by investing in the Internet of Things (IoT), operational technology (OT), big data, 5G, and artificial intelligence (AI).

These digitization efforts are connecting people and onboard systems with the cloud but also increasing cybersecurity risk. With the average cost of a breach being $4.35 million, organizations engaged in transportation must implement strong security controls that protect their systems, data, and all stakeholders.[2]

The size of the global T&L industry is projected to surpass $570.9 billion by 2030.[3]

## New Initiatives Can Introduce New Threats

To enhance the customer experience and ensure brand consistency, T&L companies are using omnichannel marketing approaches such as:

- Onboard internet access
- Customer portals
- Real-time status tracking
- Touchless payments

Modernization and digital transformation projects are designed to improve uptime, asset utilization, and employee productivity.

Although these new marketing strategies benefit customers, they introduce new threat vectors that attackers can use to compromise systems. Organizations need to implement cutting-edge cybersecurity solutions to protect their networks and reduce the risk of data breaches.

## Key Transportation and Logistics Cybersecurity Challenges

On average, it takes 287 days between the time a victim's network is breached and the containment of that breach.[4]

Addressing transportation and logistics security requires understanding the challenges and effective solutions to address them. These are a few key cybersecurity challenges and methods of remediation:

- **Passenger, employee, and environmental safety**

  Ensuring the safety of passengers, employees, and the environment is critical. Breaches of onboard systems, communications, and control systems can be used to launch attacks such as a man-in-the-middle (MITM) or those that compromise safety. Preventing breaches such as unauthorized initial access to or lateral movement within critical systems is essential to ensuring safety and reliability.

- **Visibility across IT and OT systems**

  Maintaining control of operations and onboard systems requires visibility into both OT and information technology (IT) systems. The challenge is that many of these systems reside on different, siloed networks. Without a holistic view, troubleshooting and identifying the root cause of a problem can be difficult and time-consuming. Presenting a common view across IT and OT devices and systems requires asset visualization and discovery through simple searches and correlation rules, monitoring, analysis, prioritization, and a security information and event management (SIEM) system.

- **Control and response**

  When notified of an anomalous security event or breach, the security operations center (SOC) must be able to control and respond. Having the right incident response plan within an orchestrated security platform will enable proper containment, eradication, and recovery from the incident.

- **Protecting legacy equipment**

  Some industrial control system (ICS) devices in the field operate for decades after deployment. Legacy equipment that depends on older and potentially unsupported operating systems must be protected with strong access controls, network segmentation, and monitoring and response.

- **Protecting operations centers**

  Transportation operations centers are critical to the overall safety and reliability of the services delivered. The centers serve as the hub for coordinating traffic, work scheduling, communications, and supply chain logistics. To ensure that communications are secure and systems maintain their integrity, centers should be protected with zero-trust architecture design principles, including ubiquitous authentication, encryption, and “least privilege” access.

To ensure that communications are secure and systems maintain their integrity, ops centers should be protected using solutions that support the zero-trust networking model, strong authentication, and confidentiality.

## Transportation and Logistics Cybersecurity Use Cases

### Aircraft, ground systems, and operations

The aviation industry is critical to the global economy. In 2022, U.S. airlines had 194 million more passengers than in 2021, which is a 30% increase. Throughout the entire year of 2022, from January to December, they carried 853 million passengers, compared to 658 million in 2021 and 388 million in 2020.[5] Aircraft components and systems such as full authority digital engine control systems (FADECS), navigation, radar, and flight control systems are governed by the most stringent security requirements under standard practices enforced by agencies such as ICAO. Extending that high bar of security to connecting onboard systems, airport operations centers, and airport terminal infrastructure is critical to ensuring critical systems’ safety, reliability, and resilience.

Airport operations typically require separate networks for their various management systems. These networks must be protected against physical, inbound, and lateral attacks should any system or endpoint be compromised.

### Rail travel and transportation

Rail operators must protect against various threat vectors, such as physical access, compromised remote access, and client-side attacks on endpoints. Cyberattacks on control and communications systems can compromise the safety of passengers and turn trains into attack vectors.

Onboard rail systems are particularly vulnerable to attacks due to relatively weak physical security and flat network topology on trains. Breaching a single computer on a train via a USB port may allow access to onboard control systems, such as brakes, traction, lights, doors, human-machine interface, and train-to-wayside communications.

Trains are part of an interconnected network of onboard systems and connected networks. These networks must be segmented so that a breach of one network will not lead to the compromise of another.

### Maritime transportation

Maritime trade recovered in 2021, but in 2022 faced a complex operating environment fraught with risk and uncertainty. Following a 3.8% decline in 2020, international maritime trade bounced back in 2021 with an estimated growth of 3.2% and overall shipments of 11 billion tons.[6] Modern maritime operations systems utilize more automation to improve throughput and efficiency at ports and terminals. Additionally, ports serve as intermodal trucking, rail, and logistics touchpoints. A breach of a terminal operator’s systems can compromise other parts of the supply chain, resulting in lost cargo, port disruptions, physical damage, and environmental disasters.

Cybersecurity is crucial to protect connected systems in the maritime supply chain for safety and integrity. The International Maritime Organization (IMO) adopted resolution MSC.428(98) on maritime cyber-risk management in safety management systems (SMS). The resolution encourages administrations to ensure that cyber risks are appropriately addressed in the SMS.

- **Marine approval DNV GL:** To earn this approval, a vendor must pass testing certifications/ratings in the following areas: vibration, IP protection, temperature, humidity, and electromagnetic compatibility (EMC). This is to ensure safe operations onboard and offboard shoreside.

- **EN50155:** Refers to requirements for electrical components installed onboard rail. Categories for testing are similar to DNV GL. Electromagnetic compatibility, vibration, temperature, and humidity requirements must be met. Another factor taken into account for EN50155 is the power supply. The electrical components must be able to support a wider range of voltage requirements because of the nature of what is available onboard rail.

### Logistics and delivery

Sixty-seven percent of organizations consider meeting customer expectations for speed of delivery as a critical force impacting the structure and flow of their supply chains over the next 12–18 months.[7] Securing the distribution facilities, sorting centers, depots, and operations control rooms is essential to smooth operations and efficiency. Ransomware and advanced persistent threats (APTs) have disrupted logistics operations, especially in facilities that have older, flat networks. For example, a breach of an auto-sort system could result in disruption, delays, or packages being diverted to a bad actor.

Ransomware and advanced persistent threats have disrupted logistics operations, especially in facilities that have older, flat networks.

Logistics systems must be securely integrated with IT service management (ITSM) back-end platforms. Ensuring the integrity of these systems is essential to building a trustworthy system end to end.

## The Fortinet OT-Aware Security Fabric: A Solution for Transportation and Logistics

The Fortinet OT-Aware Security Fabric is a high-performing cybersecurity platform that standardizes security across terminals, operations centers, and a variety of air, maritime, rail, and transportation systems. Powered by the FortiOS operating system, the Fortinet Security Fabric blends critical infrastructure-grade security, self-healing connectivity, application acceleration, and advanced networking functionality into a seamless solution that spans all edges, endpoints, and clouds. This solution enables a comprehensive and automated approach to security to protect critical operations and onboard systems.

FortiGate Rugged series Next-Generation Firewalls (NGFWs) and FortiAP Outdoor series wireless access points provide robust security protection and segmentation while withstanding the extremes of travel and industrial environments. The NGFWs receive a FortiGuard Labs threat feed, customized for ICS and SCADA systems.

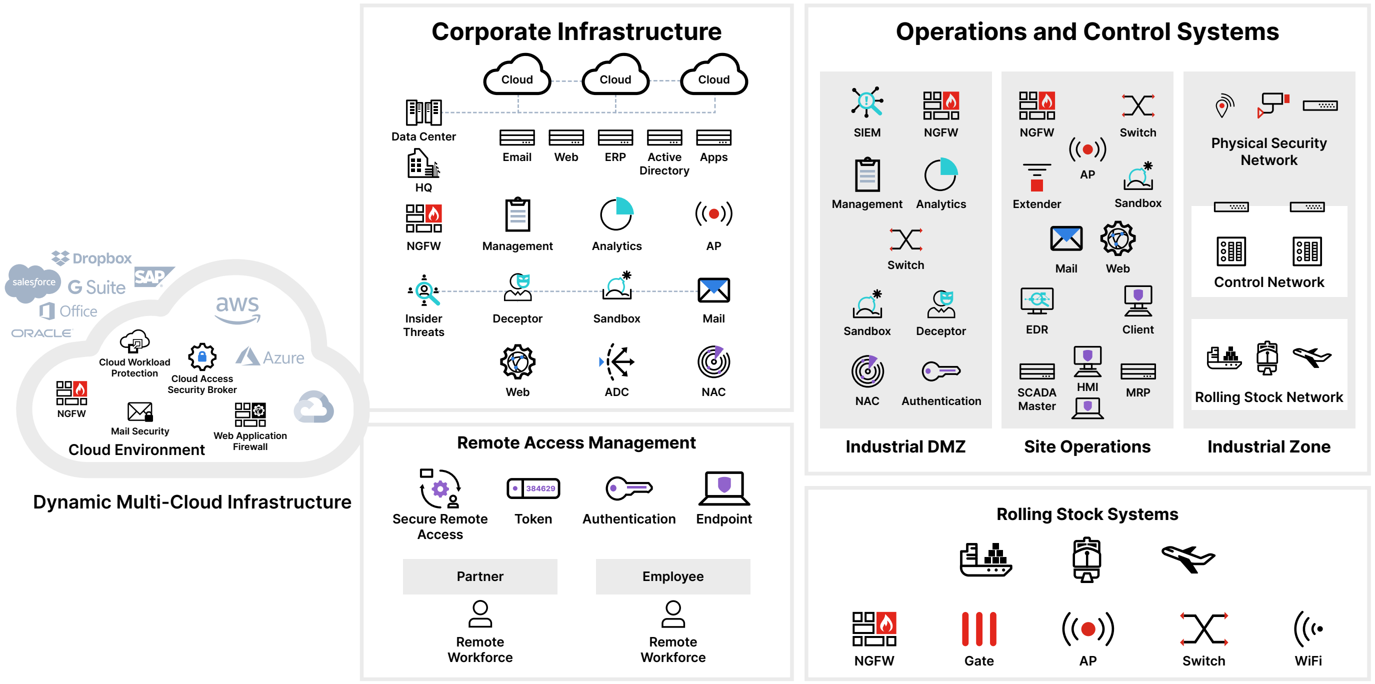


Figure 1: Fortinet cybersecurity solutions for end-to-end, integrated security

The Fortinet Security Fabric also includes FortiManager, FortiAnalyzer, FortiSIEM, FortiEDR, and FortiNAC. These tools enable transportation and logistics companies to monitor, protect, and rapidly respond to security events. FortiCamera and FortiRecorder provide the visibility required to protect against physical intrusions.

## Fortinet Differentiators for T&L Companies

### IT and OT network visibility

The Fortinet Security Fabric provides an orchestrated security platform for IT and OT converged networks. An Industrial Security Service (ISS) service on the FortiGate NGFW monitors and policies OT protocols and blocks known vulnerabilities from exploitation. The NGFW provides contextual awareness while monitoring east-west and north-south traffic.

The Fortinet Security Fabric provides end-to-end visibility across IT and OT environments.

### Compliance with OT standards and regulations

Fortinet products and solutions are designed to support T&L asset owners and systems integrators along their specific compliance journey. From IEC 62443 standards to the NIST Cyber Security Framework through more sub-industry-specific regulations like the IMO 2021 resolution for the maritime industry, Fortinet products are designed to meet industry standards.

### Proactive threat intelligence

The Fortinet FortiGuard Labs team collects and processes millions of security events per day using an advanced AI system to identify and track down breaking threats. The resulting actionable threat intelligence is then disseminated throughout the Fortinet Security Fabric to detect and defend against the latest threats. FortiGuard Labs offers several advanced threat-intelligence feed subscriptions that enable organizations to further customize their security deployments. The FortiGuard Labs Industrial Security Services specifically targets vulnerabilities found in ICS.

### Next-gen firewall

The Fortinet FortiGate NGFW moves beyond traditional firewall port/protocol inspection, network segmentation, and blocking techniques by adding application-level inspection, intrusion prevention, and intelligence from sources outside the firewall. The FortiGate NGFW provides a contextual approach to network security.

### Fortinet Security Fabric ecosystem

The Fortinet Open Ecosystem is composed of a broad set of Fabric-ready technology alliance partners, collaborations with threat-sharing organizations, and technology vendor integrations. The Fortinet ecosystem approach extends the benefits of the Fortinet Security Fabric to other assets, ensuring customers can leverage their existing investments while deploying protection across every point of their IT infrastructure.

### Ruggedized security appliances

Fortinet security solutions can run in the harshest industrial environments, including extreme temperature, air quality, vibrational, and electrical conditions. Ruggedized FortiGate NGFWs, FortiAP Outdoor series access points, and FortiSwitches can protect critical infrastructure in areas that are difficult to physically secure.

## Why Fortinet for OT Security

Air, rail, and maritime companies are modernizing their infrastructures to support strategic digital transformation projects that will improve speed, efficiency, visibility, and customer experience. Realizing the value of investing in IoT, 5G, analytics, and the cloud requires proactively addressing the security risks across IT and OT environments.

Transportation and logistics companies are also implementing omnichannel marketing and engagement techniques to offer innovative services and improve customer experiences. Reducing the risk of these strategically important initiatives is essential to justify the large capital and resource allocations that these projects require.

Fortinet is committed to providing cybersecurity solutions for the T&L industry. The Fortinet Security Fabric provides a single security platform that addresses the unique risks and vulnerabilities of air, rail, maritime, and logistics networks and systems. Learn more about Fortinet OT security solutions at fortinet.com/OT.

[1] "The Supply Chain Trends Shaking Up 2023," KPMG, 2023.

[2] "Cost of a Data Breach Report," IBM, October 2022.

[3] "Global Logistics Market Size & Share to Surpass $570.9 Billion by 2030," Vantage Market Research, May 16, 2023.

[4] "Report: Average Time to Detect and Contain a Breach is 287 Days," VentureBeat, May 25, 2022

[5] "Full Year 2022 U.S. Airline Traffic Data," Bureau of Transportation Statistics, March 16, 2023.

[6] "Review of Maritime Transport 2022," United Nations Conference on Trade and Development, November 29, 2022.

[7] "The Supply Chain Trends Shaking Up 2023," KPMG, 2023.

www.fortinet.com

November 30, 2023 10:07 AM

1301570-A-0-EN