INDUSTRY BRIEF

Securing the Rail Industry

Fortinet Cybersecurity Enables and Protects Rail 4.0

Challenges

Digital transformation initiatives are driving Rail 4.0 companies to update aging rolling stock and railway infrastructure to revolutionize the industry. This digital revolution is compelling manufacturers and rail operators to adopt new technologies that improve energy efficiency, reduce maintenance times, track inventory, optimize work scheduling, and transform the customer experience.

The vulnerability of older train systems

The average age of a locomotive is 28 years in North America and 14 years[1] in Europe. These older train systems make them particularly vulnerable to cyberattacks because their networks tend to share the same physical network with minimal security controls.

What does digital transformation mean for rail companies and terminal operators?

- Increased onboard networking and connectivity to enhance the customer experience with, for example: Wi-Fi, touchless payments, passenger entertainment system, comfort, lighting, and auxiliary systems
- Updated train station control systems for automatic train control (ATC) systems, rail monitoring, perimeter access, signaling, and communications
- Adoption of advanced driver-assistance systems (ADAS) and full self-driving (FSD) systems for light rail
- Intelligent systems to optimize railway and train operations like switch gear, traction systems, communications and signaling, power, and wayside communications
- High-speed rail and autonomous train projects to improve energy efficiency, speed, and the cost of operations
- Artificial intelligence (AI) for asset management, predictive maintenance, and emergency notification

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 rail companies execute their digital transformation strategy, their onboard and rail operations systems naturally become more connected. 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 all onboard control systems, such as HVAC, brakes, traction, diagnostics, lights, doors, HMI, and train-to-wayside communications. If a train system is compromised, passengers and the environment will be at risk.

Fortifying the Rail Industry's Cybersecurity

In order to accelerate digital transformation, the rail industry needs to rethink its security posture and move toward a seamless, comprehensive, and zero-trust cybersecurity strategy.

As rolling stock and operators 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 rail industry with a proactive and transformative approach to cybersecurity. It is called the Fortinet Security Fabric (Figure 1) and provides protection that is broad, integrated, and automated.

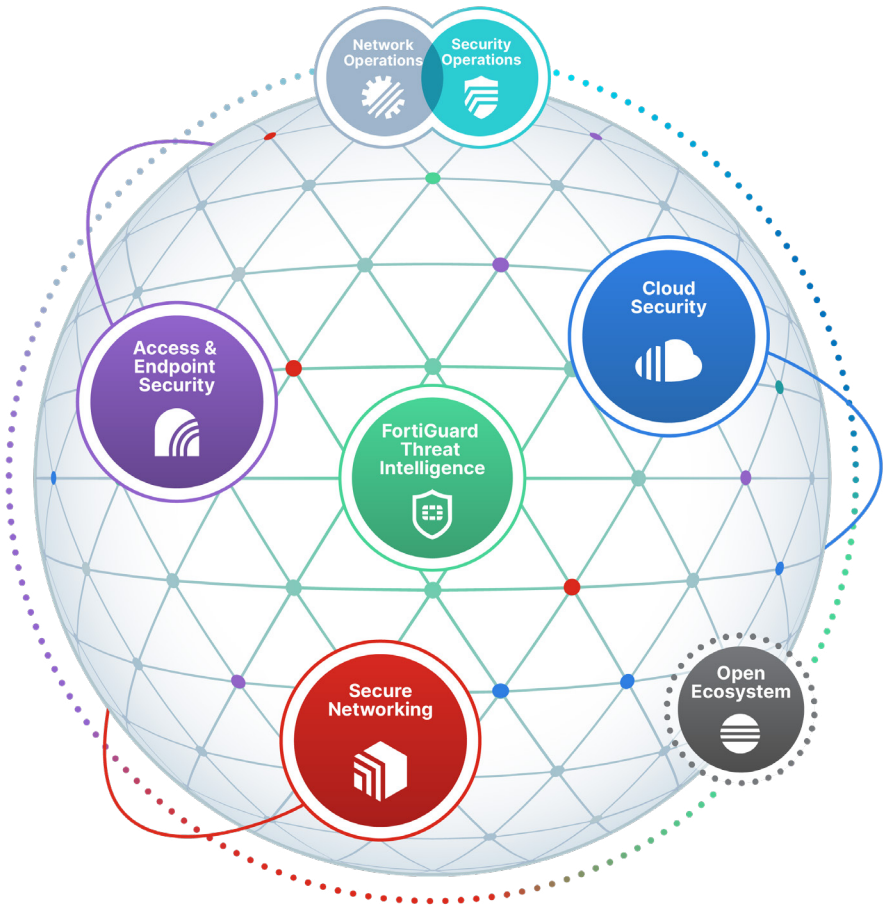

Figure 1: Fortinet Security Fabric.

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 Rail 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 rail industry addresses one of the major issues in a shipping company's environment—easily deploying technology to multiple locations with no on-site expertise. Through the use of FortiDeploy, Fortinet's cloud-based deployment and management solution, remote systems can be easily and centrally configured. 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, 3G/4G/5G, or SATCOM links, making it a truly borderless infrastructure. 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 rail 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 Rail Industry

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

Summary

Fortinet's solutions allow rail companies to accelerate their digital transformation by securing rolling stock and terminal operations. Once in place, these solutions provide a platform for future growth with minimum disruption. Securing Rail 4.0 is more than just securing a train against cyberattacks; it is essential to the safety of passengers, the crew, and the environment.

[1] "Average Age of North American Fleet," Statista, July 21, 2021.

February 23, 2022 6:42 AM
1470201-0-0-EN