SOLUTION BRIEF

Protecting Transportation Smart Infrastructure with the Fortinet OT Security Platform

EXECUTIVE SUMMARY

From 2020 to 2022, the number of cyberattacks on transit systems increased by 186%, according to the Mineta Transportation Institute.[1] A growing number of organizations in the transportation sector, from public transit authorities and vehicle manufacturers to air, rail, and maritime service operators, are implementing digital and smart technologies. This transformation offers significant benefits to both service providers and users, such as time and fuel efficiencies, reduced environmental impact, improved customer experience, and cost-savings opportunities. However, digital and smart infrastructure relies on digital interconnections to various systems including external networks, giving bad actors a larger attack surface. Safeguarding this infrastructure from bad actors often requires a team of cybersecurity professionals. However, the cybersecurity skills gap has made recruiting and retaining cybersecurity personnel a critical challenge.

The Fortinet OT Security Platform offers smart transportation operators the industry's highest-performing cybersecurity platform. It offers transportation service providers and operators full visibility, controlled access, and robust threat detection and response, while still achieving all the benefits that smart transit technology delivers. Fortinet's combination of proven and scalable security solutions, deep knowledge, and skilled personnel creates a comprehensive, manageable security environment from proposal, design, and deployment through the entire life cycle.

Vulnerabilities in Smart Transportation

A smart transportation system is a network of technologies and infrastructure designed to improve the efficiency, safety, and sustainability of transportation systems. These systems leverage data, communications networks, industrial protocols, physical equipment, and automation to enhance various aspects of transportation, from scheduling and vehicle operation to traffic management and infrastructure maintenance. However, smart infrastructure in the transportation sector also presents a unique, expanded set of security challenges that must be solved. This is especially true because the growth of smart cities increases the likelihood of more municipal services being connected, potentially increasing the damage that could be caused by attacks on transportation systems.

IBM found that the average cost of a data breach in the transportation industry was $3.59 million.[2]

When physical meets cyber

Transforming typical transit infrastructure into smart infrastructure requires removing the barrier between the physical and cyber. There is no longer protection via "air gap" or "security by obscurity." OT and IT systems have an interdependence that improves the service, but the ability for cybercriminals to control physical components such as rail crossing gates, stoplights, or subway signals creates new risks with serious consequences.

Expanding attack surface

With the digital transformation that drives smart transit, the intersection between the physical and cyber increases the size of the attack surface. Connected components on a network, such as smart stop lights, traffic cameras, road sensors, and even vehicles themselves, become new potential entry points for bad actors. Because much of smart transit is provided by government entities on limited budgets, contamination of the supply chain with temptingly underpriced components—already embedded with backdoors—is also a real threat.

Threats to public safety

Because smart infrastructure like transportation systems is required for the normal functioning of a society, and can wreak havoc in terms of both physical safety and economic impact, it is a particularly attractive target. Nation-states and hacktivists want to cause socio-political disruption, while other cybercriminals are looking to profit by disrupting an essential service or holding data for ransom.

With infrastructure such as transportation continuing to evolve through digital transformation and become smart infrastructure, Fortinet can help municipal and private service providers overcome these unique security challenges by delivering cybersecurity at scale, legacy-system protection, enhanced compliance, and security as a service. The Fortinet OT Security Platform also offers futureproofing for organizations that intend to continue modernizing and innovating.

"In a time when technology plays an increasingly important role in public transit, prioritizing cybersecurity is critical. Through adopting proactive measures and prioritizing cybersecurity efforts, transit agencies can lower the risk of a cyberattack, improve their resilience, and ultimately protect their riders."

— **David Avery,** Director of IT for South Central Transit Authority, in Mass Transit Magazine

Cybersecurity for Smart Transportation

To thrive throughout digital transformation, the transportation industry relying on smart and intelligent transport infrastructure needs to rethink its security posture and move toward a seamless, comprehensive, and zero-trust cybersecurity strategy for its smart infrastructure. The Fortinet OT Security Platform unifies the best of current IT network security capabilities with an in-depth understanding of the OT security requirements including applications and protocols and offers:

- **Visibility:** FortiNAC network access control (NAC) and FortiGate next-generation firewall (NGFW) provide comprehensive visibility into the network by continuously monitoring and analyzing traffic, user behavior, and device activities. This visibility helps identify potential security threats and vulnerabilities in real-time, ensuring proactive threat mitigation. FortiNDR network detection and response (NDR) offers deep visibility into network vulnerabilities, threats, and malicious network behavior through its patented artificial intelligence and machine learning (AI/ML) techniques. FortiNDR can integrate with Fortinet or third-party security solutions to support response and remediation actions for any detected network anomalies.
- **Secure Networking:** FortiGate serves as the cornerstone of the network infrastructure, offering advanced firewall, intrusion prevention system (IPS), virtual private network (VPN), and secure software-defined wide area network (SD-WAN) capabilities. FortiAP access point and FortiSwitch secure network switch provide secure wired and wireless connectivity while FortiManager, a central management and policy orchestration platform, centralizes network management—making it easier to configure, monitor, and maintain the network infrastructure. FortiAnalyzer, a centralized network analysis and troubleshooting solution, offers centralized logging, monitoring, and reporting capabilities and includes tailored compliance reports mapped to well-known cybersecurity frameworks.

- **Zero Trust Network Access:** Zero trust network access (ZTNA) ensures secure access to applications or devices hosted anywhere, whether users are working remotely or in the offices. FortiNAC, FortiAuthenticator, and FortiPAM play vital roles in ZTNA implementation. FortiNAC enforces strict access policies based on user and device identities, ensuring that only authorized users and devices can access network resources. For enhanced security, FortiToken provides multi-factor authentication (MFA) and can integrate with FortiAuthenticator for single sign-on. FortiPAM combined with FortiClient provides role-based access control and privileged access management capabilities to roll out zero-trust across internal and external users and critical systems at scale so that the users are restricted based on their roles and can perform their activities securely and safely.
- **Endpoint Detection and Response:** A smart infrastructure has an increased number of endpoints and securing these endpoints is critical to ensure end-to-end security. FortiEDR, an endpoint detection and response solution, is an essential part of the Fortinet Security Fabric that can detect and respond to suspicious behavior or threats across a large number of endpoints, minimizing the risk of security breaches in the smart infrastructure.

The Fortinet OT Security Platform is tailored to meet the security requirements of the smart transportation industry. It encompasses a broad portfolio of security solutions, covering detection, prevention, containment, and recovery. Implementation of the Fortinet OT Security Platform assures both providers and users that the cybersecurity requirements for smart infrastructure are met. This includes addressing security audit requirements from regulators and demonstrating compliance. Likewise, the security architecture team can trust that the smart infrastructure adheres to industry-compliant security implementation. Ultimately, the Fortinet OT Security Platform offers an end-to-end security solution.

Enhancing Cyber Resilience Through the Fortinet OT Security Platform

With its breadth and depth, the implementation of the Fortinet OT Security Platform ensures that critical operational resources and data are protected from cyberthreats. As a result of this security implementation, business activities and services remain uninterrupted, and schedules and resources such as time and fuel are optimized. Fortinet supports the key outcomes that the smart transportation industry needs most, including:

- **Maintaining Reliability:** Cyberattacks can shut down vital equipment such as ticket machines, fare gates, and toll booths. Attacks can also expose operational data and lead to a loss of control over systems. All of this affects an operator's ability to deliver the experience customers depend upon. Fortinet's commitment to constantly updated threat identification and protection mitigates the risk of service disruptions due to cyberattacks like ransomware and infrastructure takeover.
- **Ensuring Compliance:** As the federal government invests in infrastructure, operators in the transportation sector will need to stay within operational rules to ensure funding. There are also increasingly tough mandates for ensuring the resilience of systems and services. Fortinet both simplifies regulatory reporting and supports security audit requirements.
- **Managing Reputational Risk:** Smart transportation providers who don't take security seriously risk severe institutional and personal damage to the reputations of those involved in theft of sensitive information or accidents due to cyber intrusions. Partnering with Fortinet, a respected industry leader in cybersecurity, helps mitigate the exposure to reputational risk due to cyber-driven data breaches or disruption of systems and services.

Through a comprehensive and scalable security technology platform, Fortinet can secure smart transportation infrastructure, catering to entities of all sizes—from the smallest independent organizations to the largest public operators. Regardless of the size or extent of smart infrastructure, Fortinet offers cybersecurity for every user, system, and network.

Fortinet for Smart Transportation

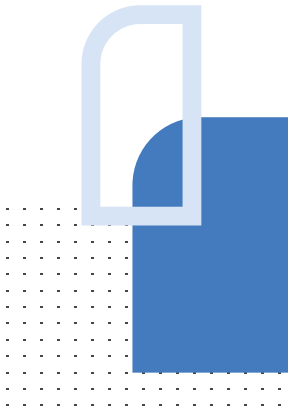
Providing safe, reliable transportation options is critical to maintaining society as we know it. Transit providers are under immense pressure to increase reliability, reduce carbon footprint, and ensure that the public and their employees are kept safe at all times. Smart infrastructure solutions for transportation are an exciting way to improve quality of life while reducing environmental impact, but digital transformation comes with increased security challenges.

The Fortinet OT Security Platform secures modern and legacy systems by scaling to meet all the requirements in a partnership that provides the technology, knowledge, and expertise to create a comprehensive security environment for smart transportation operators. The Fortinet OT Security Platform is the only cybersecurity platform rated by Westlands Advisory as a Leader in the 2023 IT/OT Network Protection Platforms Navigator[3]—and delivers broad, integrated, and automated digital security for all infrastructure innovations.

[1] Miroslav Katsarov, "The Intersection of Data Security and Smart Public Transit Systems," Forbes, March 31, 2023.

[2] Skip Wombolt, Stacy Shaw, Hannah Hoeflinger, "A Glitch on the Road: Cybersecurity Trends Facing the Trucking and Transportation Industry," Marsh McClennan Agency, May 4, 2023.

[3] "Fortinet Recognized as the Sole Leader in the Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator™," Fortinet, July 27, 2023



FORTINET

www.fortinet.com

February 2, 2024 7:54 PM

123456-0-0-EN