ONELAYER

SECURING AND MANAGING IOT AND PRIVATE 5G/LTE INFRASTRUCTURE FOR SEAPORTS AND AIRPORTS

With the modernization of transportation and logistics, seaports and airports are increasingly adopting private 5G/LTE cellular networks and IoT devices to power smart facilities using technology such as Smart Port apps and Industrial IoT (IIoT) to help boost operations. Automated container and baggage management, real-time equipment condition monitoring, and streamlined PTT communication across teams allow for shorter turnaround times, higher productivity, and lower costs. Private 5G and LTE networks support these advancements, making it easy to track goods, vehicles, and workers.

This modernization comes with new risks and security, such as securing cellular network assets like IT/OT/IoT assets, finding the root of a security incident or operational issue, automating manual device management processes, and overcoming APN segmentation limitations. Challenges include identifying and tracking non-cellular devices connected to cellular routers.

Two key ways private 5G/LTE cellular technologies are changing connectivity infrastructure security and operations:

1. A New Enterprise Network

Private 5G/LTE networks are a new separated LAN for ports. They create a new perimeter to protect, while co-existing with the IT and OT networks. Moreover, 5G/LTE private networks are unique because they are based on cellular technologies, which is a new domain for port facility security and operations teams.

2. The New Cellular Network is Different from Existing Networks

Cellular networks use different network elements and communication protocols and are required to connect to new devices. The scale is also very different. Instead of dealing with a few devices behind Wi-Fi routers, facilities now need the ability to identify, secure and manage hundreds or sometimes thousands of devices on their private cellular network, including those behind routers and devices moving between routers.

Key IoT and 5G/LTE Security and Operations Considerations

The vast majority of airports and seaports already have a variety of networks and legacy operational technology (OT) networks. For securing and managing these networks, the industry has well-established principles like segmentation, zero trust, visibility, security monitoring, breach detection, and asset management. These methods and practices won't work for 5G/LTE networks, however, because there are so many architectural differences that create security blind spots, operational management challenges, and other new risks.

Device Identity and Monitoring Blind Spots

Cellular networks use a separate set of device identifiers. All cellular traffic flows through a centralized packet core that hides the identity of individual devices from security tools by making it appear that all activity originates from a single IP address. This renders existing security monitoring and asset management workflows ineffective. In addition, in many scenarios, cellular routers are used to support the connection of non-cellular-ready devices to the cellular network, with no visibility of the individual devices behind them.

Lack of Network Access Control Policies

Cellular networks use a star topology that is significantly different from the mesh-style IP networks or legacy OT networks that traditional security tools were designed for. This leaves security teams unable to implement segmentation policies to limit the impact of IoT device vulnerabilities, lateral movement within the cellular network and security breaches.

New Industry Compliance Complexities

Most port and airport security, operations and compliance teams have limited exposure to cellular networking technologies. This, combined with the technical complexities described above, makes it challenging to ensure that 5G/LTE security and asset management practices comply with highly prescriptive transportation industry regulatory requirements, standards and other security and operations guidelines.

OneLayer Extends Seaport and Airport Security, Asset Management and Compliance Practices to Private 5G/LTE Networks

The OneLayer Bridge Platform enables seaports and airports to harness the power of IoT, 5G and LTE technologies securely by extending security visibility and segmentation approaches like Zero Trust to private 5G/LTE infrastructure. OneLayer's systematic approach provides the critical missing link between the 5G/LTE packet core and the security and operations tools and practices used to protect and manage IT and OT networks.

The OneLayer platform integrates directly with leading cellular packet core technologies, including Ericsson, Nokia, Verizon, Athonet, Celona, Druid, Mavenir, Pente and Monogoto, to:

- Enhance the visibility of existing security and asset management tools to include even visibility of devices behind cellular routers or hotspots
- Deploy granular Zero Trust segmentation policies on private 5G/LTE networks, including setting policies for devices behind a router
- Maximize the operational efficiency of your network with automatic application of policy rules which prioritize QoS based on category of use, user and device
- Easily govern a large scale of assets with manual device management process automation and view of the full picture from a single pane of glass
- Ensure regulatory compliance with industry requirements, standards and other security guidelines such as TSA's Cybersecurity Requirements, ISO, ISA, IEC, NIST, ICAO Annex 17 and IMO Guidelines on Maritime Cyber Risk Management

ERICSSON · NOKIA · verizon · athonet · celona · Druid · MAVENIR · Pente Networks · monogoto

5G/LTE Device Discovery, Categorization and Assessment

All 5G/LTE connected devices are automatically discovered, fingerprinted, categorized and enriched with contextual details that make them more relevant to existing security and operations tools. This includes the identification of known device vulnerabilities for rapid remediation. In addition, an automatically generated and continuously updated topology map simplifies security incident response and non-security troubleshooting.

Zero Trust Segmentation of Private 5G/LTE Networks

Granular network segmentation is a well-established industry best practice. OneLayer extends this capability to the private 5G/LTE domain by empowering security teams to create Zero Trust segmentation policies that limit the blast radius of breaches and ransomware, enable geofencing devices using location-based policies and govern traffic flow between IT, OT and private 5G/LTE networks.

In addition, OneLayer sends alerts to existing security and operations monitoring tools to enable immediate response and avoid or minimize operational downtime.

Interested in learning more?

Visit https://onelayer.com/airports-ports/ to schedule a personalized demo or email us at contact@onelayer.com.