ONELAYER

SECURING IOT AND PRIVATE 5G & LTE MANUFACTURING INFRASTRUCTURE

As the manufacturing sector modernizes, facilities increasingly adopt public and private 5G & LTE cellular networks and rely on IoT devices, connected assets, and secure, highly reliable connectivity, enabling Industry 4.0. Data, such as location & performance tracking of autonomous guided vehicles, sensors and other devices is gathered, increasing business productivity, producing valuable insights, and saving on costs. Alongside this modernization, new security risks disrupt the Purdue model, especially as more manufacturing companies turn to private cellular networks to effectively run smart and connected factories.

5G/LTE cellular technologies are changing connectivity infrastructure security requirements in two critical ways:

1. A New Enterprise Network – Private LTE/5G networks are a new separated LAN for enterprises. They create a new perimeter to protect, while co-existing with the IT and OT networks. Moreover, Private LTE/5G networks have unique characteristics, leveraging cellular technologies which are a new domain of knowledge for enterprises. They introduce a different network architecture, data flow, device identifiers and more which disrupt the immediate extension of the Purdue model.

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. Instead of dealing with a few devices behind Wi-Fi routers, organizations now need the ability to identify and secure hundreds or sometimes thousands of devices on the private cellular network, including those behind routers and devices moving between routers.

Key IoT and 5G Security Considerations

Most manufacturers already have a variety of enterprise networks and legacy operational technology (OT) networks in use. The industry has well-established practices for securing these networks, including the Purdue segmentation model, Zero Trust Architecture principles, and best practices like visibility, security monitoring, and breach detection. But these practices cannot be extended to 5G & LTE networks due to significant architectural differences that create security blind spots and other new risks to critical infrastructure.

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 workflows ineffective. In addition, in many scenarios, cellular routers are used to support non-cellular ready device's connectivity to the cellular network, with no visibility of the 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 we're 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 manufacturing security 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 practices comply with highly prescriptive industry regulatory requirements, standards, and other security guidelines such as NIST, and practices such as the Purdue Model.

OneLayer Solution Reconciles the Purdue Model Disruption

OneLayer Extends Manufacturing Security and Compliance Practices to Private 5G & LTE Networks

The OneLayer Security Platform enables manufacturing firms to harness the power of IoT,5G and LTE technologies securely by extending security visibility and segmentation frameworks like the Purdue model and Zero Trust Architecture to Private 5G & LTE infrastructure. OneLayer's systematic approach provides the critical missing link between the 5G & LTE packet core and the security tools and practices used to protect IT and OT networks.

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

- Extend Purdue model network architecture to 5G & LTE networks
- Enhance the visibility of existing security tools, including the visibility of devices behind cellular routers or CPEs
- Deploy granular Zero Trust segmentation policies on Private 5G & LTE networks, including setting policies for devices behind a router
- Ensure manufacturing compliance with industry regulatory requirements, standards, and other security guidelines such as NIST

ERICSSON NOKIA MAVENIR athonet celona Druid monogoto Pente Networks

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 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, Geo-fencing 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 monitoring tools to enable immediate response.

INTERESTED IN LEARNING MORE?

Visit one-layer.com to schedule a personalized demo, or write to us at contact@one-layer.com