ONELAYER

SECURING IOT AND PRIVATE LTE UTILITY INFRASTRUCTURE

Internet of Things (IoT) technologies are transforming how utility services are delivered and opening the door to new and exciting industry innovations. But the expansive geographic footprint of utility infrastructure makes unlocking the full potential of IoT challenging.

LTE cellular technologies are changing this in two critical ways:

1. The high-speed and low latency characteristics of LTE make it uniquely capable of supporting large numbers of IoT devices and ensuring the timely delivery of high-quality operational data.

2. Cloud-enabled LTE packet core technologies make it much more practical and cost-effective for utilities to deploy private cellular networks that suit their unique needs.

IoT and LTE are poised to reinvent metering and accelerate innovations such as smart grids, drone-enabled infrastructure support services, and VR/AR-assisted employee enablement. At the same time, utilities must also balance the business benefits unlocked by IoT and LTE with the need to ensure that the industry's stringent security and compliance standards are met.

Key IoT and LTE Security Considerations

Most utilities already have a variety of enterprise networks and legacy operational technology (OT) networks in use. The utility industry has well-established practices for securing these networks, including the Purdue Model, Zero Trust Architecture principles, and best practices like visibility, security monitoring, and breach detection. But unfortunately, these practices cannot be extended to 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, and all 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.

- **Geo-Fencing Devices Challenge** – As IoT devices multiply and physical control over enterprise devices can't be assured, approaches like Zero Trust Architecture become a necessity. Geo-Fencing enables specific location-based device policy settings, e.g., blocking the device from accessing the network when not where it's physically supposed to be.

- **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 existing security tools protect. This leaves security teams unable to implement segmentation policies to limit the impact of IoT device vulnerabilities and security breaches.

New Industry Compliance Complexities – Most utility 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 LTE security practices comply with highly prescriptive industry regulations like NIST Smart Grid Framework and SP-1800-23.

OneLayer Extends Utility Security and Compliance Practices to Private LTE Networks

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

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

- Enhance the visibility of your existing security tools
- Deploy granular Zero Trust segmentation policies on your Private LTE networks, including Geo-Fencing devices
- Extend Purdue model network architecture to LTE networks
- Ensure compliance with utility regulations such as NIST Smart Grid Framework and SP-1800-23
- Enable the evolution to private 5G networks

LTE Device Discovery, Categorization, and Assessment

All 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 LTE Networks

Granular network segmentation is a well-established utility industry best practice and is mandated explicitly by regulations like NIST Smart Grid Framework and SP-1800-23. OneLayer extends this capability to the Private 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 LTE networks. In addition, we send alerts to your 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