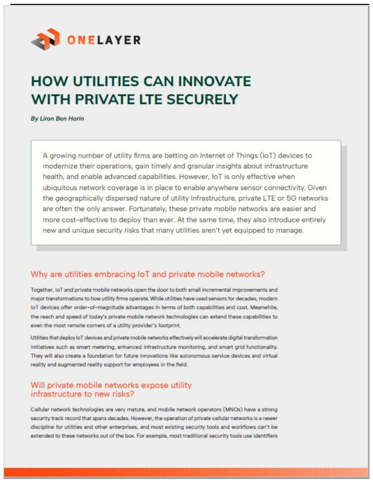

ONELAYER

HOW UTILITIES CAN INNOVATE WITH PRIVATE LTE SECURELY

By Liron Ben Horin

A growing number of utility firms are betting on Internet of Things (IoT) devices to modernize their operations, gain timely and granular insights about infrastructure health, and enable advanced capabilities. However, IoT is only effective when ubiquitous network coverage is in place to enable anywhere sensor connectivity. Given the geographically dispersed nature of utility infrastructure, private LTE or 5G networks are often the only answer. Fortunately, these private mobile networks are easier and more cost-effective to deploy than ever. At the same time, they also introduce entirely new and unique security risks that many utilities aren't yet equipped to manage.

Why are utilities embracing IoT and private mobile networks?

Together, IoT and private mobile networks open the door to both small incremental improvements and major transformations to how utility firms operate. While utilities have used sensors for decades, modern IoT devices offer order-of-magnitude advantages in terms of both capabilities and cost. Meanwhile, the reach and speed of today's private mobile network technologies can extend these capabilities to even the most remote corners of a utility provider's footprint.

Utilities that deploy IoT devices and private mobile networks effectively will accelerate digital transformation initiatives such as smart metering, enhanced infrastructure monitoring, and smart grid functionality. They will also create a foundation for future innovations like autonomous service devices and virtual reality and augmented reality support for employees in the field.

Will private mobile networks expose utility infrastructure to new risks?

Cellular network technologies are very mature, and mobile network operators (MNOs) have a strong security track record that spans decades. However, the operation of private cellular networks is a newer discipline for utilities and other enterprises, and most existing security tools and workflows can't be extended to these networks out of the box. For example, most traditional security tools use identifiers

HOW UTILITIES CAN INNOVATE WITH PRIVATE LTE SECURELY

Thank you for downloading this OneLayer resource. Carahsoft is the federal distributor for OneLayer solutions available via SWEP, GSA, ITES-SW2 and other contract vehicles.

To learn how to take the next step toward acquiring OneLayer solutions, please check out the following resources and information:

For additional resources:
carah.io/OneLayerResources

For upcoming events:
carah.io/OneLayerEvents

For additional OneLayers solutions:
carah.io/OneLayerSolutions

For additional Big Data solutions:
carah.io/bigdata

To set up a meeting:
(703) 230-7596
OneLayer@carahsoft.com

To purchase, check out the contract vehicles available for procurement:
carah.io/OneLayerContracts

For more information, contact Carahsoft or our reseller partners:
OneLayer@carahsoft.com | (703) 230-7596

ONELAYER

HOW UTILITIES CAN INNOVATE WITH PRIVATE LTE SECURELY

By Liron Ben Horin

A growing number of utility firms are betting on Internet of Things (IoT) devices to modernize their operations, gain timely and granular insights about infrastructure health, and enable advanced capabilities. However, IoT is only effective when ubiquitous network coverage is in place to enable anywhere sensor connectivity. Given the geographically dispersed nature of utility infrastructure, private LTE or 5G networks are often the only answer. Fortunately, these private mobile networks are easier and more cost-effective to deploy than ever. At the same time, they also introduce entirely new and unique security risks that many utilities aren't yet equipped to manage.

Why are utilities embracing IoT and private mobile networks?

Together, IoT and private mobile networks open the door to both small incremental improvements and major transformations to how utility firms operate. While utilities have used sensors for decades, modern IoT devices offer order-of-magnitude advantages in terms of both capabilities and cost. Meanwhile, the reach and speed of today's private mobile network technologies can extend these capabilities to even the most remote corners of a utility provider's footprint.

Utilities that deploy IoT devices and private mobile networks effectively will accelerate digital transformation initiatives such as smart metering, enhanced infrastructure monitoring, and smart grid functionality. They will also create a foundation for future innovations like autonomous service devices and virtual reality and augmented reality support for employees in the field.

Will private mobile networks expose utility infrastructure to new risks?

Cellular network technologies are very mature, and mobile network operators (MNOs) have a strong security track record that spans decades. However, the operation of private cellular networks is a newer discipline for utilities and other enterprises, and most existing security tools and workflows can't be extended to these networks out of the box. For example, most traditional security tools use identifiers such as IP addresses and MAC addresses to identify, fingerprint, and monitor devices. Performing a similar function for cellular devices requires awareness of international mobile equipment identity (IMEI) and other cellular-specific identifiers that today's enterprise security tools don't understand.

This reduced security visibility is exacerbated by the fact that other established best practices like network segmentation can't be performed in the same way on private mobile networks. Unlike the IP networks that utilities use widely today, which have a mesh topology and mechanisms like control lists for compartmentalizing network-based communication, cellular networks use a star topology that requires all traffic to flow through a centralized packet core.

The ramifications of this are substantial. In the case of a network breach, there is less of a safety net to prevent attacks from advancing to other areas of the utility infrastructure, including the cellular core. This risk is amplified by the fact that low-cost IoT devices are often more prone to unaddressed software and hardware vulnerabilities. In addition, network segmentation is explicitly mandated by key utility industry regulations, including the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.

How can utilities prevent private mobile networks from becoming a weak link in their security posture?

While the unique security risks posed by private mobile networks will put critical utility infrastructure at risk if left unaddressed, best practices for using using private mobile networks securely are taking shape. Three specific best practices that utilities implementing private mobile networks should consider are:

1. Eliminate blind spots in monitoring visibility so effective device discovery and asset management can be performed in the cellular domain.

At a minimum, utilities should develop approaches for providing enriched data about cellular device identity to security tools, so they have the necessary context to detect device-level risks and engage security response workflows. Ideally, this will also include intelligent grouping of devices, geolocation capabilities, and cellular network topology map generation to streamline troubleshooting and security response activities.

2. Extend vulnerability management efforts to include cellular devices.

Most utilities have well-established practices for finding and remediating vulnerabilities in traditional IT systems, but these practices will not extend automatically to cellular-connected devices. In addition to fingerprinting cellular devices, it's also critical to add the capability to cross-reference device software and hardware versions with known vulnerability information and take proactive measures to isolate and remediate vulnerable devices.

3. Implement network segmentation capabilities on private mobile networks.

Given network segmentation's importance to both risk mitigation and compliance in the utility industry, it's critical to augment existing approaches used on traditional IT networks with cellular-specific network segmentation techniques. This will contain any breaches to a micro-segment of the overall network, prevent ransomware from propagating, and simplify regulatory compliance activities.

Liron Ben Horin is Vice President of System Engineering at OneLayer, a provider of security technologies for private LTE and 5G networks.