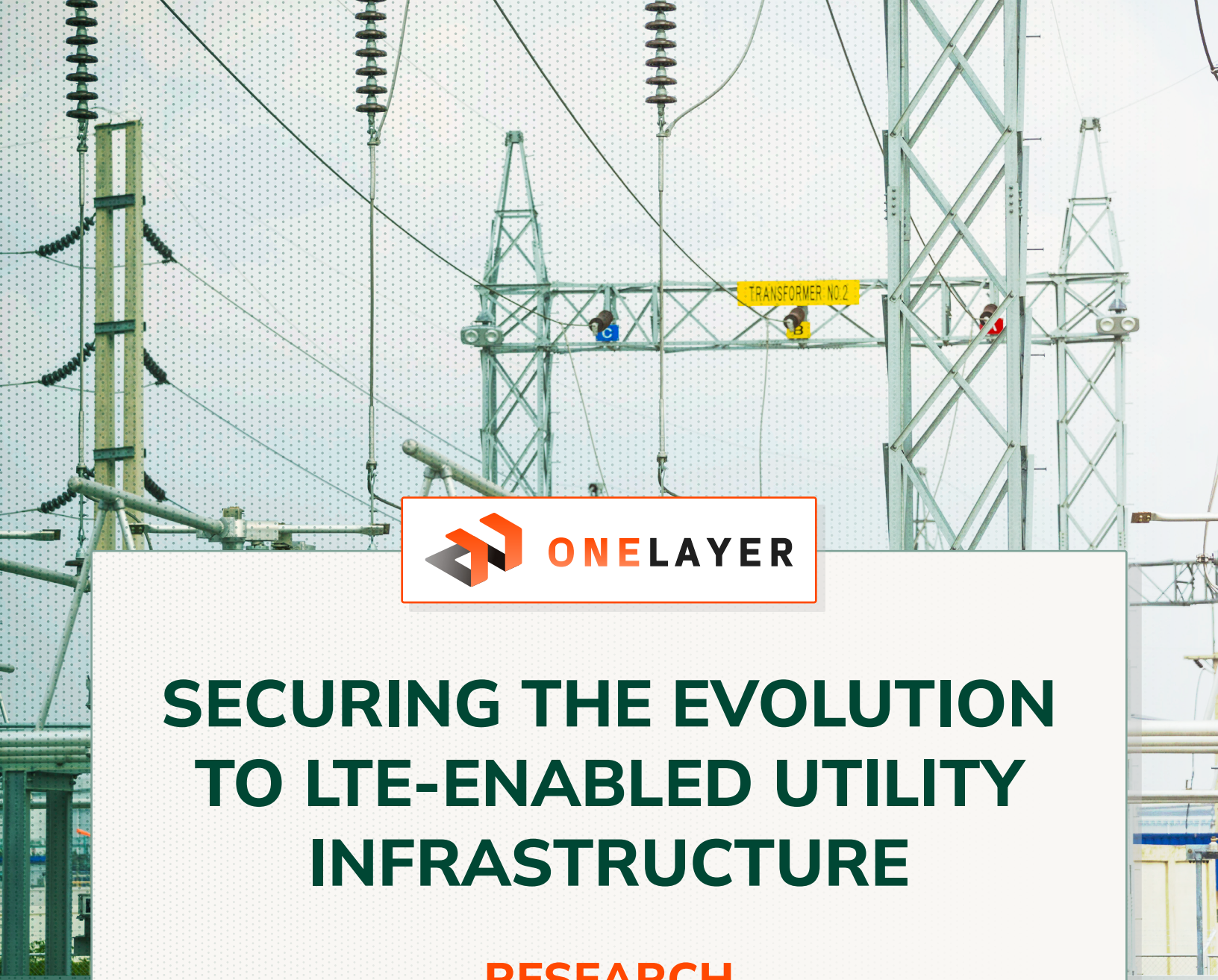
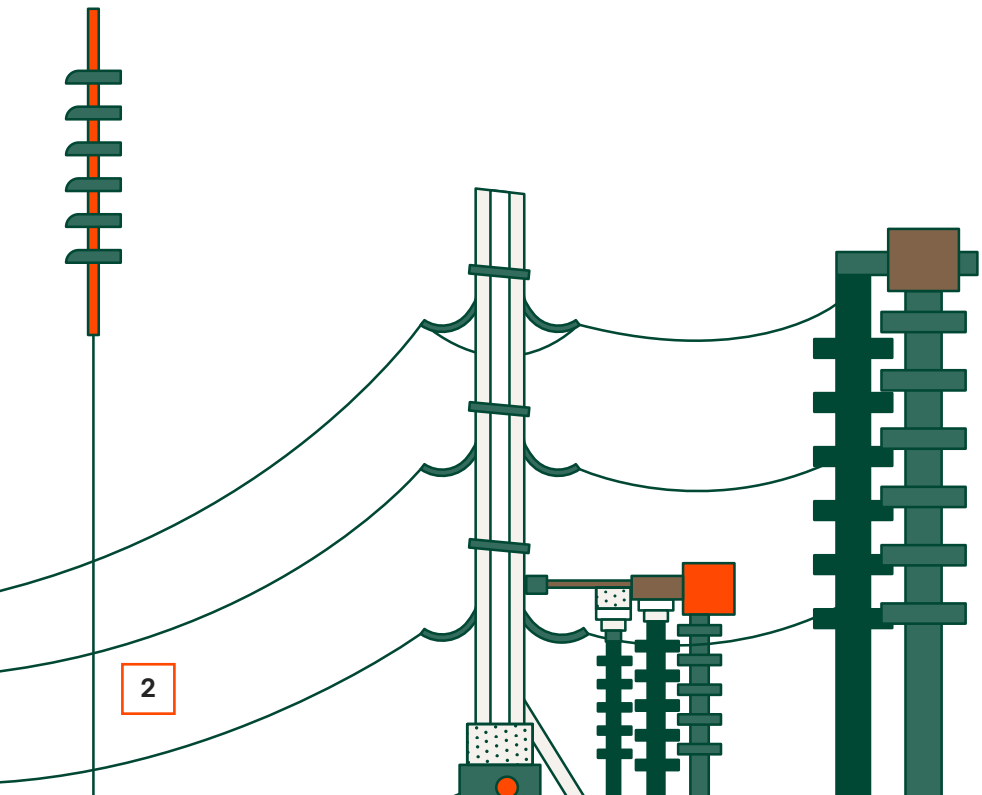


ONELAYER

SECURING THE EVOLUTION TO LTE-ENABLED UTILITY INFRASTRUCTURE

RESEARCH

TABLE OF CONTENTS



ONELAYER

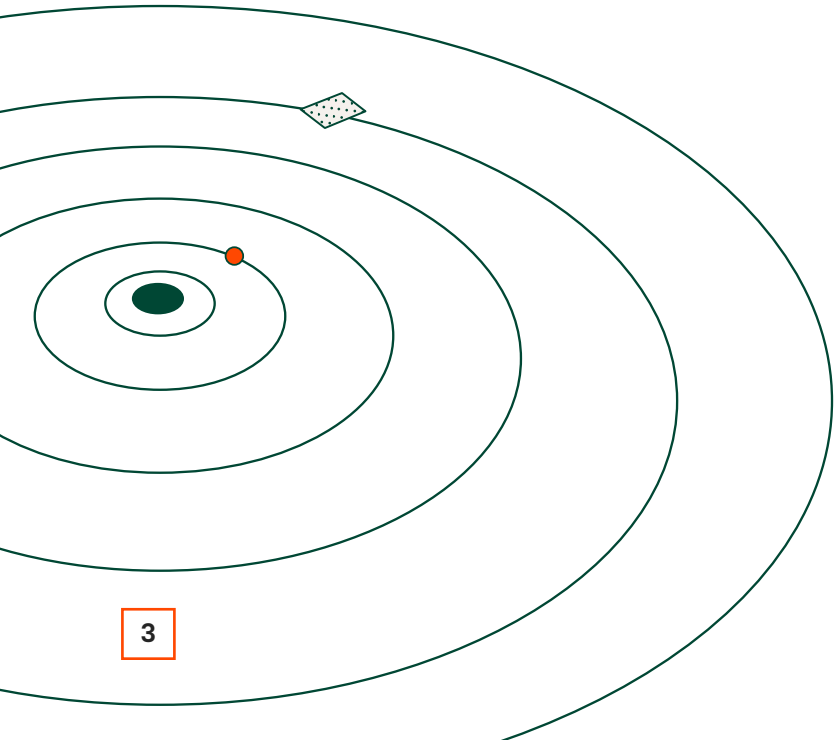
SECURING THE EVOLUTION TO LTE-ENABLED UTILITY INFRASTRUCTURE

The utilities industry faces unprecedented pressure to innovate and evolve to meet growing demands for capacity, reliability, and advanced capabilities. Forward-thinking utility firms are already applying early Internet of Things (IoT) capabilities to modernize their infrastructure and streamline operations. However, IoT's full potential to transform the utilities sector is far from fully realized.

A lack of reliable and ubiquitous network connectivity across the expansive geographic footprint of utility infrastructure is one of the primary obstacles to IoT innovation. Fortunately, the emergence of LTE public and private wireless technologies makes it much more practical and cost-effective for utility firms to deploy IoT devices at scale across an expansive and diverse set of operational environments. Private LTE networks are also providing more of the reliability utilities need in the case of a crisis, and additional cost savings.

The combined power of IoT and LTE technologies will empower utilities to accelerate existing digital transformation initiatives while also opening the door to innovation opportunities that were previously impossible. However, utilities must also balance the pressure to innovate quickly with their responsibility to ensure the security of critical infrastructure and meet the industry's highly demanding regulatory requirements.

In this paper, we will explore the transformational capabilities that are unlocked by IoT and LTE, the potential security and compliance obstacles that utility firms may encounter, and practical strategies for embracing IoT and LTE securely.



EMERGING IOT AND LTE USE CASES IN THE UTILITIES SECTOR

The scale and complexity of utility infrastructure make it one of the leading beneficiaries of sensor technologies. While sensors have been used by utilities for decades, modern IoT devices provide an order-of-magnitude advance over legacy sensors in terms of both capabilities and cost. Meanwhile, the reach and performance afforded by public and private LTE networks make it possible to extend sensor coverage into more locations than ever and enable new advanced capabilities.

The new use cases enabled by LTE, combined with increasing ability to implement private LTE infrastructure more cost-effectively using cloud-based packet core infrastructure, make it more practical for utilities to achieve a positive return on investment on their IoT and LTE technology initiatives. The following are specific examples of how utility firms can harness the combined power of IoT and LTE to improve operational efficiency and enable more dynamic and efficient energy usage.

Improving Smart Meter Coverage and Fidelity

Smart meters are an increasingly common way for utility providers to capture more accurate and timely energy usage information. Some smart meter implementations also provide information directly to energy consumers about their usage, so they can make more informed decisions about their consumption and spending. LTE network capabilities make it possible to extend the reach of utility provider smart meter telemetry to remote locations. The increased data speeds that LTE networks are capable of can also be leveraged to increase the volume and speed of data collection, providing higher fidelity data and richer insights.

Enabling Advanced Monitoring and Smart Grid Capabilities

Smart grid implementations use IoT devices in a two-way manner to optimize energy delivery across the power grid based on sensor signals. Utility firms that can collect low-latency, real-time data about energy consumption and the health and operation of power delivery infrastructure can use big data analytics to identify optimizations that can be applied in real-time. The coverage, sensor density, data speeds, and low latency enabled by LTE create new opportunities for high-performance sensor deployment, simplifying and accelerating smart grid initiatives.

Deploying Autonomous Service and Diagnostics Devices

One of the biggest operational challenges that utilities face is the ability to service infrastructure in distant or difficult-to-access locations. Autonomous devices such as aerial drones are unlocking new opportunities to service infrastructure in remote or otherwise operationally challenging locations with much less time delay, risk, and cost than traditional service fleet dispatch. LTE networks play a pivotal role in these types of operational innovations by providing the continuous high-speed connectivity that autonomous devices need to function effectively in the field.

Empowering Employees Through Virtual Reality and Augmented Reality

Utility personnel faces the difficult challenge of supporting, troubleshooting, and maintaining complex – and potentially dangerous – infrastructure. These efforts are frequently further complicated by factors such as natural disasters, equipment failures, and cyberattacks. Advances in virtual reality (VR) and augmented reality (AR) offer a transformational opportunity to provide immersive training. These technologies can also be used to provide real-time information and guidance that will improve service quality and increase the speed of troubleshooting and recovery when unplanned events occur.

HOW SECURITY COMPLEXITY CAN UNDERMINE IOT AND LTE INNOVATION

While the potential applications of IoT and LTE in the utility industry are compelling, these technologies also introduce new security challenges that utility firms must address to fully realize their potential. The following are common examples.

Device Identity and Monitoring Blind Spots

Given the critical importance of ensuring both the security and availability of utility services, most service providers invest heavily in security tools that can identify and assess connected devices and monitor continuously for potential security threats. However, the traditional tools used for network visibility and monitoring are based on a combination of IP network identifiers such as IP and MAC addresses and well-established legacy operational technology (OT) identifiers. Cellular networks introduce an entirely new set of device identifiers that are unfamiliar to both traditional enterprise security tools and more specialized tools that utilities use to monitor their OT networks. This creates a potential "perfect storm" of security risks.

For example, one of the trade-offs that come with the low cost of IoT devices is that they are more prone to security vulnerabilities than traditional IT and OT devices. Just as large numbers of these devices are connecting to the utility provider's infrastructure, existing enterprise security tools are rendered incapable of identifying and monitoring them effectively.

No Network Access Policy Controls

While utility providers go to great lengths to prevent security breaches, most now recognize that device security vulnerabilities and targeted security breaches are an unavoidable certainty. As a result, network segmentation has become a critical best practice in the utilities industry. In fact, many organizations are moving to Zero Trust Architecture models that assume that no devices can be implicitly trusted and govern network access and communication at a granular level.

Some of the same differences between IT, OT, and cellular networking technologies that make device discovery and network visibility challenging also severely limit utilities' ability to implement policies to govern network access and movement. Unlike traditional IP networks, which use a mesh topology with support for techniques like access control lists, cellular networks use a star topology that requires all traffic to flow through a centralized cellular core. Similarly, any specialized security tools that utilities may use to implement policies on OT networks will also be ineffective on cellular networks.

For private LTE networks, organizations are realizing that there is a better way to get to zero trust than to use traditional security tools and develop complex architectures based on Firewalls.

Geo-Fencing Devices

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.

For example, it's difficult for a threat actor to walk into a secure enterprise data center and access a traditional enterprise system. But climbing a utility pole in an isolated location to gain physical access to an IoT device can be achieved by an overzealous hacker.

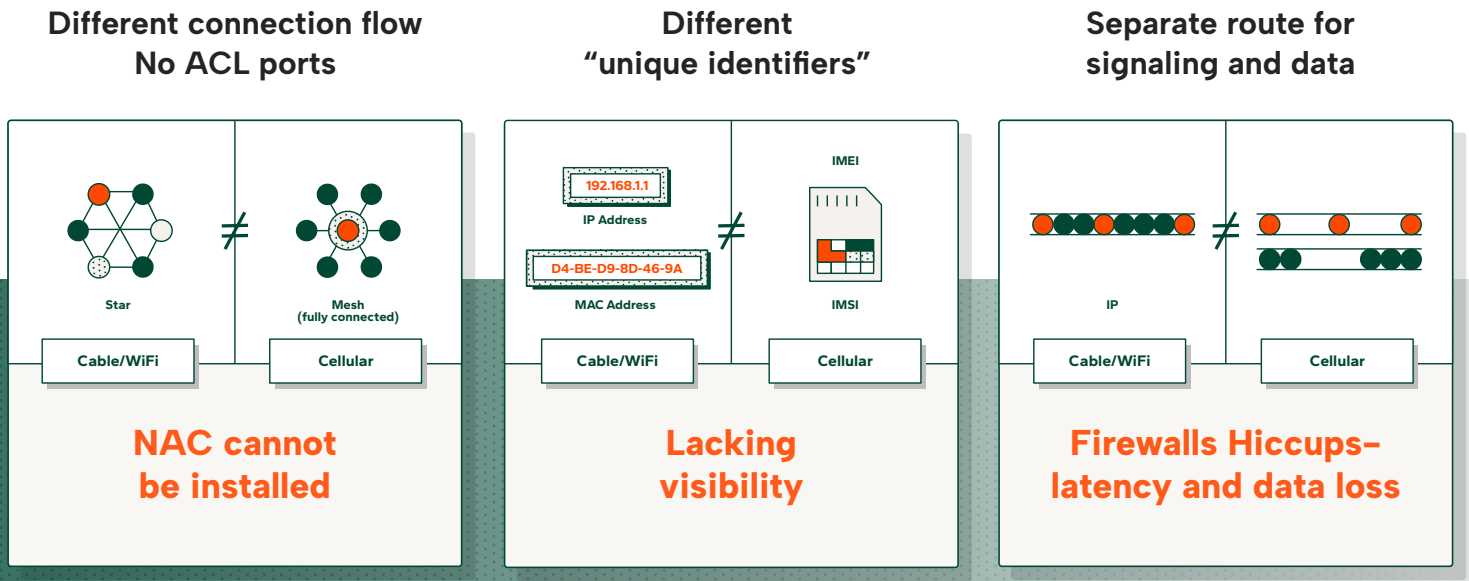
New Utility Industry Compliance Obstacles

Given the criticality of utility infrastructure, utility firms must comply with industry regulations that mandate specific security standards and practices. One of the best-known examples is the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards that bulk electric system operators in North America must adhere to. Another example is the ISA/IEC 62443 series of standards that define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).

NERC CIP includes numerous requirements that are complicated by the LTE security challenges described above. The following are some notable examples:

- NERC CIP-002-5.1a (BES Cyber System Categorization), which calls for discovery and classification of cyber assets, is complicated by the visibility and identity challenges described above.
- NERC CIP-005-6 (Electronic Security Perimeter(s)), which defines specific requirements for the creation of virtual boundaries and network segments, is complicated by the lack of traditional IP-based network controls on LTE networks
- Numerous requirements pertaining to system-level security, security monitoring, and vulnerability assessments, such as those described in NERC CIP-007-6 (System Security Management) and NERC CIP-010-2 (Configuration Change Management and Vulnerability Assessments) are complicated by the LTE network monitoring blind spots described above.

As IoT devices and LTE networks grow in popularity – and become a bigger target for threat actors – the regulatory demands on utilities will likely increase. Therefore, it is critical to ensure that existing audit and compliance practices can be extended to these new devices and network environments.



ONELAYER

Extending Security Tools and Best Practices to the LTE Domain

To extend existing security tools, practices, and regulatory compliance efforts to LTE networks, utilities must approach the security challenges described above strategically and systematically. Ideally, the approach should include critical capabilities such as:

- The ability to capture detailed device attributes and activity details for all LTE-connected devices.
- Device fingerprinting and classification techniques that enrich the data about LTE-connected devices that security tools are analyzing on an ongoing basis.
- Methods of creating segmentation policies that can govern the flow of LTE network traffic with granular precision, including geo-fencing devices.
- Simplifying the overall architecture and consolidating different wireless technologies, such as LoRa, under private LTE, with unified visibility, asset management, monitoring, and so on, eliminating potential mistakes and weak links. All devices can be managed under one system.

These key competencies are described in more detail in the sections that follow.

Visibility and Asset Management

One of the most important initial steps that utilities adopting LTE should take is to eliminate device discovery and security monitoring blind spots in their cellular networks. For example, if a new type of sensor appears on a LTE network that is unknown to existing management systems and does not appear in any manually created asset lists, the utility must be able to discover and fingerprint it, so security tools have the context they need to be effective.

It is equally important to find ways to enrich the level of visibility that security tools have for devices that are visible at the IP network level but cannot be identified. For example, some cellular traffic includes user plane functions that interoperate with the IP network through network address translation (NAT). As a result, these devices all appear to security tools as originating from the IP address of the packet core.

Similarly, implementation details such as a combination of 3GPP and non-3GPP devices may cause cellular devices to be hidden from security tools. This can be even further complicated when devices are connected to mixed environments that include both cellular and Wi-Fi connectivity.

These challenges can only be overcome by providing existing security tools in the IP network with enriched data about the device identity, so they can detect device-level security risks and take the necessary responses. Ideally, these capabilities will include:

- Grouping of devices based on context
- Automatic creation of cellular network topology maps
- Correlation of network identifiers and physical devices for accurate location tracking

A Day in the Life

A utility company experiences a failure of a sensor connected to a piece of customer-premises equipment (CPE) at a power plant. Unless they have proactively addressed LTE network visibility gaps, it will be impossible to pinpoint the location of the sensor and resolve the problem. In contrast, if instrumentation is in place to automatically discover, fingerprint, and map cellular devices, an operator can use this information to quickly identify the CPE device that the sensor is connected to and coordinate repair or replacement.

Vulnerability Management and Risk Mitigation

Utilities that develop their competency with LTE device discovery, fingerprinting, and categorization capabilities will also be better equipped to discover LTE-connected devices with security vulnerabilities and take the necessary steps to remediate them.

This requires specific types of device assessment and data enrichment capabilities, such as the ability to cross-reference device software and hardware versions with known vulnerability information. If this vulnerability state information is then combined with additional contextual information like network location, configuration details, and segmentation state, utility security teams will be in a better position to prioritize and execute vulnerability management activities, including those specified in NERC CIP-010-2.

Network Segmentation and Protection

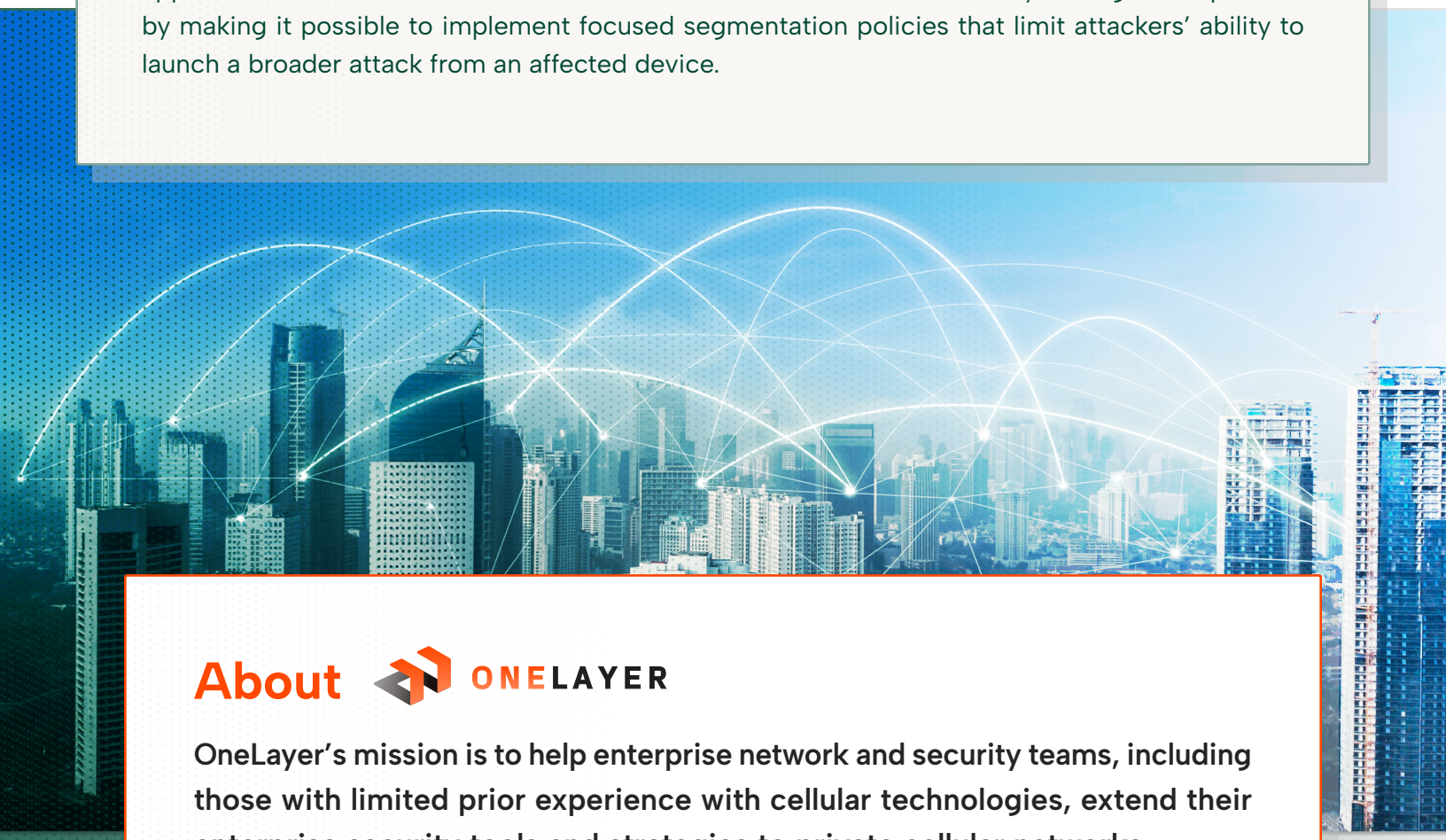
Granular network segmentation is one of the most effective ways to reduce the risks presented by an isolated infrastructure breach or device compromise. As noted above, many utilities, particularly those that are governed by NERC CIP, already have segmentation capabilities in place on their primary networks, for example, using VPN, DMZ, and complex architectures to group devices and control access. However, because these existing technologies will not extend to LTE networks, utilities must take proactive steps to add equivalent capabilities, such as zero trust segmentation policies, geo-fencing devices, governing traffic flow between IT, OT, and private LTE networks, and alerting on anomalous activity in the cellular domain. Doing so will provide many security benefits, including:

- Containing breaches to a micro-segment of the overall cellular network
- Preventing ransomware from propagating
- Reducing the impact of distributed denial of service attacks

In addition to restricting lateral movement within the cellular network, utilities should also develop a strategy for controlling communication between the cellular network and other IT and OT networks.

A Day in the Life

A new vulnerability is discovered in a specific vendor's programmable logic controllers (PLC), which is deployed in many locations across a utility provider's operational network. A utility that has extended their vulnerability management to the cellular domain proactively will be able to identify and group all cellular-connected devices from the affected vendor. This will accelerate the speed with which firmware updates can be applied to eliminate the vulnerability. An effective segmentation approach for the cellular network will work in concert with the vulnerability management process by making it possible to implement focused segmentation policies that limit attackers' ability to launch a broader attack from an affected device.



About ONELAYER

OneLayer's mission is to help enterprise network and security teams, including those with limited prior experience with cellular technologies, extend their enterprise security tools and strategies to private cellular networks.

INTERESTED IN LEARNING MORE?

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