Anterix®

Successfully Managing Utility Grid Security

Enhancing Cyber and Physical Security with Private Wireless Broadband

Every utility is diligently striving to safeguard the grid against continuously evolving cyber and physical security threats. Utilities face the challenge of integrating more devices, including existing devices with limited security features, as well as new connected devices—sensors, control systems, smart devices, electric vehicles, and distributed energy resources. The growing device landscape increases utilities' need for a secure, reliable, resilient, utility-grade communication network.

A 900 MHz private wireless broadband network provides utilities with enhanced control, helping to mitigate potential threats. Utilities have more control over the network design, build, and operation, as well as end-to-end system security, access, and data visibility. A private network offers a smaller and more visible threat landscape.

By owning and managing a private wireless network, utilities benefit from the ability to customize their network to their specific needs. They can integrate cyber tools and capabilities directly from their existing utility data or operations center while selectively enhancing security measures at the network's edge for optimal protection.

Built-In Security

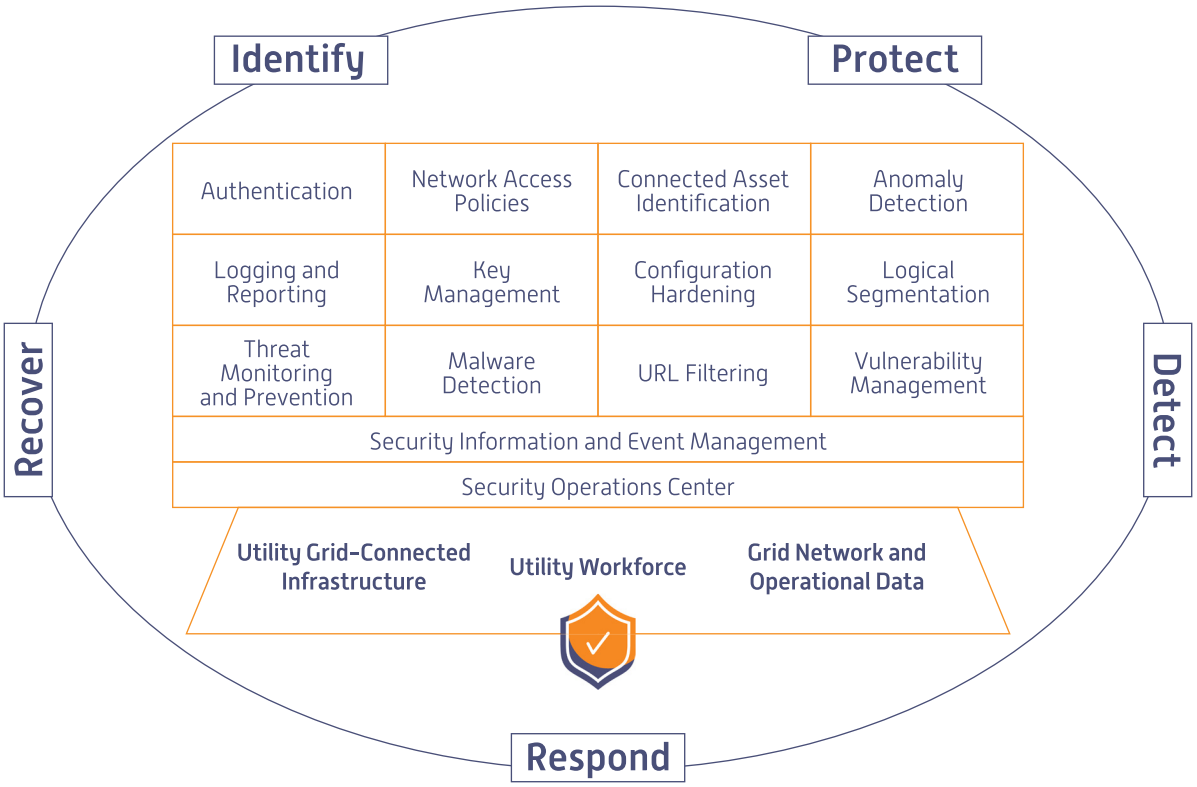
LTE comes with a broad set of security capabilities and features defined by the global wireless standards body, 3rd Generation Partnership Project (3GPP), to enable delivery of advanced cybersecurity protections not typically deployed in commercial carriers' networks today. Many of these built-in security capabilities are fundamental to private LTE-like network authentication to ensure devices belong on a network, subscriber identity protection to protect network information from being compromised, and strong authentication management and encryption capabilities.

Levels of Defense

Multiple layers of customizable security can be incorporated to align with established cyber frameworks such as National Institute of Standards and Technology (NIST) or International Organization for Standardization (ISO). Security features can provide full visibility into connected assets and their behavior, including traffic monitoring and the establishment of device and traffic policies for effective segmentation. Private LTE supports additional security layers, including device threat monitoring and prevention, device URL filtering, traffic monitoring, identification and authentication, implementation of customized network access policies, and network segmentation to permit only authorized host network devices while monitoring device traffic.

Physical Security

Multi-layer cyber security capabilities enabled by 900 MHz private wireless broadband in support of utility communications networks.



The private LTE network also offers many benefits for physical security applications including low latency, quality of service, and analytics capabilities. Many utilities with substations and other network assets in remote areas are concerned about physical security attacks. Private LTE enables physical security applications like video monitoring with analytics, gunshot detection, and the ability to deliver alerts and dispatch field personnel.

Spotlight Anterix Active Ecosystem Members

Security has long been an area of vital importance for utilities and critical infrastructure entities. Increased digitization and proliferation of connected user equipment, devices, and sensors have broadened the attack surface that companies must defend. Meanwhile, the ever-increasing frequency and sophistication of cyberattacks compound the challenge.

Recognizing the complexity facing utilities in addressing their security challenges, Anterix has formed the Anterix Security Collective® within the Anterix Active Ecosystem. The Anterix Security Collective brings together a team of cyber -physical security solutions providers to help drive secure solutions in connection with the deployment of 900 MHz private wireless networks.

The Anterix Security Collective, a subgroup of the Anterix Active Ecosystem, provides a comprehensive array of security solutions to bolster the establishment of a robust and secure 900 MHz grid communications network.

Binary Armor: SNC's Binary Armor® cybersecurity provides inline, endpoint protection for critical infrastructure. Binary Armor's patented "functional whitelisting" stops internal and external threats from harming operational technology (OT), like malware and unsafe or erroneous instructions. With Binary Armor, only pre-approved, safe messages reach OT. This provides real-time cybersecurity against accidents and malicious commands while enforcing workflow to prevent disruption of operations, equipment damage, and personnel injury.

Mandiant: Mandiant is on a mission to make every organization secure from cyber threats and confident in their readiness. The Mandiant Advantage platform gives security teams an early knowledge advantage via the Mandiant Intel Grid, which provides platform modules with current and relevant threat data and analysis expertise.

Onclave: The Onclave TrustedPlatform™ is a network-based, enterprise security solution designed to protect all OT/internet of things (IoT) systems and devices based on Zero Trust principles. The Onclave TrustedPlatform™ creates cryptographically secure private networks (microsegments) that isolate, contain, and optimize management of OT/IoT assets. These microsegments are continuously monitored and become invisible, undetectable, and inaccessible – allowing enterprises to securely operate from edge to core.

OneLayer: OneLayer provides enterprise-grade security for private LTE/5G networks. Its platform and IoT security toolkit can be implemented in private cellular networks to provide better visibility and protect organizations from security attacks, creating one identity, one policy rule, and one security approach which covers every IoT device in an organization.

PacketViper: PacketViper provides transformative and trusted solutions for organizations seeking to modernize the cybersecurity of converging OT and IT networks without a costly 'rip and replace'. PacketViper's flagship Deception360 is a deception-based network detection, prevention, and response technology that automates attack prevention from both external and internal threats.

Q-Net Security: Q-Net Security produces dedicated, no-update hardware that creates a barrier between defined endpoints within a new or existing network. Q-Net uses a patented hardware barrier that leverages strong, quantum-resistant encryption and True Random Number Generated symmetric keys that can change every packet or transaction to move and authenticate data securely and is drop-in ready to implement in public or private networks, with no manual key management. By operating at line rates, Q-Net can also protect endpoints from such nefarious activities as DDoS attacks.

Quibtekk: Qubitekk commercializes quantum technology with a variety of products tailored to strengthen American leadership in quantum information science. As a world leader in the design and manufacture of entangled photon sources and state measurement systems, Qubitekk's physicists and engineers have many decades of experience developing, manufacturing, and characterizing the performance of quantum devices.

Anterix® ACTIVE ECOSYSTEM

Reach out to the Anterix Active Ecosystem team at AnterixActive@anterix.com for additional information on our metering solutions members.