ONELAYER

SECURING AND MANAGING IOT AND PRIVATE 5G/LTE MINING INFRASTRUCTURE

As the mining sector modernizes, companies increasingly adopt private 5G/LTE cellular networks and rely on IoT devices, connected assets and secure, highly reliable connectivity to run smart mining operations. Data, such as location and performance tracking of drills, conveyor belt systems, autonomous guided vehicles, sensors and other devices, is gathered and leveraged to increase business productivity, produce valuable insights and save on costs. But along with this modernization come new security and operation risks, such as avoiding or minimizing downtime caused by technology issues and ensuring the safety of your connected workers and equipment.

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

1.

A New Enterprise Network

Private 5G/LTE 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 5G/LTE networks have unique characteristics because they are based on cellular technologies, which are a new domain of knowledge for enterprises. They introduce different network architecture, data flow, device identifiers and more which disrupt extension of your standard IT/OT security and operations models.

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

3.

The Need to Coordinate Multiple Cellular Networks

In mining operations, often each mine or location has its own private cellular network: an “island network.” All these island networks need to be managed, preferably from a centralized location, with the same security requirements for all. This “network of networks” structure drastically increases the amount of cellular expertise and overhead required to successfully manage and secure it.

Key IoT and 5G/LTE Security and Operations Considerations

Most mining companies already have a variety of enterprise networks and legacy operational technology (OT) networks in use. The industry has well-established methods for securing and managing these networks, like segmentation and Zero Trust architecture principles, along with best practices for visibility, security monitoring, breach detection and asset management. But these methods and practices cannot be extended to 5G/LTE networks due to significant architectural differences that create security blind spots, operational management challenges 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 and asset management workflows ineffective. In addition, in many scenarios, cellular routers are used to support the connection of non-cellular-ready devices to the cellular network, with no visibility of the individual 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 were 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 mining security, operations 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 and asset management practices comply with highly prescriptive mining industry regulatory requirements, standards and other security and operations guidelines.

OneLayer Extends Mining Security, Asset Management and Compliance Practices to Private 5G/LTE Networks

The OneLayer Bridge Platform enables mining firms to harness the power of IoT, 5G and LTE technologies securely by extending security visibility and segmentation approaches like Zero Trust to private 5G/LTE infrastructure. OneLayer's systematic approach provides the critical missing link between the 5G/LTE packet core and the security and operations tools and practices used to protect and manage IT and OT networks.

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

- Implement geofencing to lock devices with location-based connectivity policies, track assets' geographic location and define responses to policy deviations
- Enhance the visibility of existing security and asset management tools to include even visibility of devices behind cellular routers or hotspots
- Deploy granular Zero Trust segmentation policies on private 5G/LTE networks, including setting policies for devices behind a router
- Provide continuous visibility of devices even if they failover to a public network
- Ensure regulatory compliance with industry requirements, standards and other security guidelines such as NIST, ISO, OSHA, MSHA, EPA and EIA

ERICSSON · NOKIA · verizon · athonet · celona · Druid · MAVENIR · Pente Networks · monogoto

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 and operations 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, enable geofencing 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 and operations monitoring tools to enable immediate response and avoid or minimize operational downtime.

Interested in learning more?

Visit onelayer.com to schedule a personalized demo or email us at contact@onelayer.com.