Three Challenges That Undermine Traditional Security Tools in the Private Cellular Domain

ONELAYER

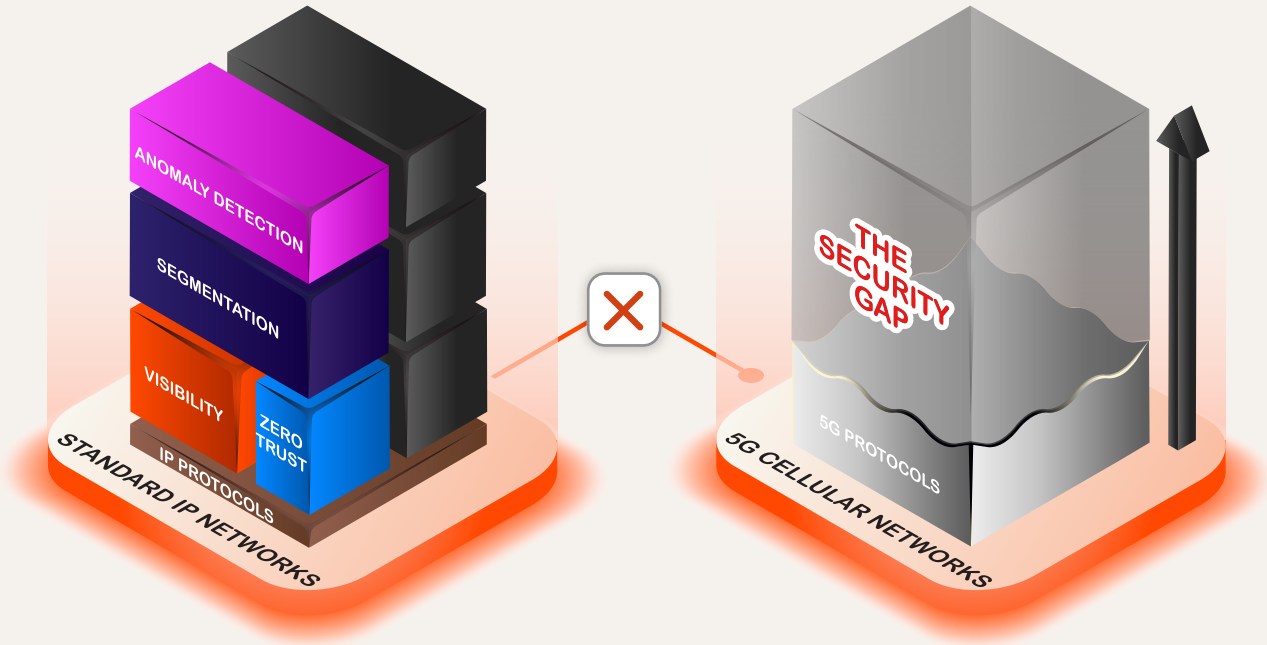
The growing use of Internet of Things (IoT) devices and the evolution of LTE and 5G cellular technologies are leading many enterprises to deploy private cellular networks alongside their existing network infrastructure. Private LTE and 5G networks overcome many of the limitations of traditional enterprise WiFi technologies while also enabling new and innovative uses of connected devices.

But they also introduce an entirely new set of network technologies, most of which are unfamiliar to enterprise security teams and incompatible with existing security techniques and tools.

Like all other IT, OT, or cloud networks that support IoT devices, private cellular networks are extensions of the enterprise domain.

Therefore, enterprise security teams must take security ownership of private cellular networks and apply the same types of IoT security measures used on their existing enterprise networks. However, numerous unique attributes of cellular networks make this impossible using traditional security tools alone.

The following are three specific challenges that enterprise security teams will face as they attempt to extend their traditional security tools to private cellular networks.



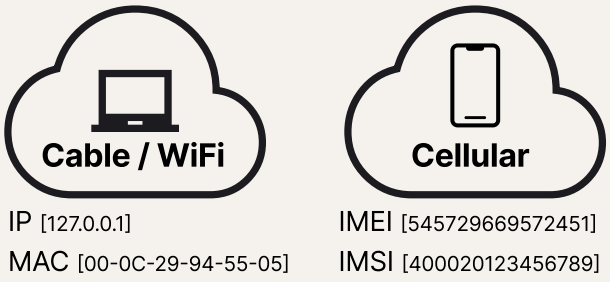
Challenge 1: Tracking of cellular device activity by traditional security tools is significantly complicated by the lack of IP and MAC addresses in cellular network traffic

Correlating network activity with specific device identifiers provides the necessary context to analyze patterns of behavior and detect anomalies that require a prevention or mitigation response. Therefore, device identity is a critical element of most security monitoring and policy enforcement workflows. Most enterprise security tools rely on identifiers such as IP and MAC address to track device identity for this purpose.

However, IP and MAC addresses can't be used as methods of device identification in cellular networks. Cellular networks use separate identifiers, such as international mobile equipment identity (IMEI) and international mobile subscriber identity (IMSI) numbers as identifiers instead.

Traditional enterprise security tools designed for IP networks are incapable of understanding and supporting these cellular-specific device identifiers.
In addition, similar device-level visibility challenges created by use of network address translation (NAT) in traditional IT and OT networks are often overcome using network taps or integration with DHCP servers. However, in cellular architectures, IP addresses are allocated to the devices at the cellular network gateway. As a result, tapping and DHCP integration are viable workaround on cellular networks.

SPECIALIZED DEVICE FINGERPRINTING CAPABILITIES MUST BE INTEGRATED WITH THE ENTERPRISE ARCHITECTURE TO EXTEND SECURITY MONITORING AND CONTROL TO PRIVATE CELLULAR NETWORKS.



Different "unique identifiers"

Challenge 2: Security tool efficiency and effectiveness is severely degraded by the need to correlate separate user data and cellular network metadata in real time.

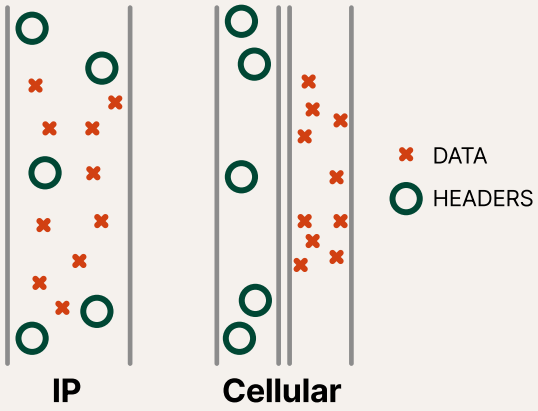
Firewalls and other traditional security tools use device identity as a key input when analyzing traffic on IT networks for security threats. This is simplified by the fact that on IP networks, device identification details appear alongside the user data payload being transmitted.

In contrast, cellular networks include two distinct types of network activity:

- Control-plane traffic related to the operation of the network.
- User-plane traffic related to the actions performed by individual users and devices.

The only way for firewalls and other traditional security tools to monitor and control cellular traffic effectively is by correlating the disparate control-plane and user-plane network activity in real time. The same device identification challenges noted above complicate this greatly, and early attempts to use traditional security tools to perform real-time correlation of device identifiers and activity through network taps have been unsuccessful due to data leakage, data loss, and unacceptable latency.

A CENTRALIZED METHOD OF CORRELATING CONTROL-PLANE AND USER-PLANE TRAFFIC IS NECESSARY TO ENABLE EFFECTIVE MONITORING AND CONTROL OF PRIVATE CELLULAR NETWORKS BY ENTERPRISE SECURITY TOOLS.



Separate route for signaling and data

Challenge 3: Critical segmentation techniques like access control lists and port-level rules are impossible on cellular networks.

Many enterprises now use Zero Trust Architecture principles to implement fine-grained policies that limit access to specific network segments to only those devices with an explicit business need. This greatly reduces exposure in the case of a network breach.
These efforts benefit greatly from the fact that IP networks have a mesh topology with support for access control lists and other methods of controlling the flow of traffic to different sub-segments of the network.
In contrast, cellular networks have a star topology. In this architecture, all traffic flows through a centralized packet core.
While access controls and other security policies can be implemented at the cellular packet core, the star topology of a cellular network is more difficult to segment beyond this level due to the lack of distributed access control lists and port-level rules that are possible on IP-based enterprise networks.

This makes extending a Zero Trust Architecture to cellular networks challenging and makes it easier for an attacker who compromises a cellular-connected device to move laterally to higher-value assets in other parts of the network. This makes extending a Zero Trust Architecture to cellular networks challenging and makes it easier for an attacker who compromises a cellular-connected device to move laterally to higher-value assets in other parts of the network.

» ***SPECIALIZED DEVICE FINGERPRINTING CAPABILITIES MUST BE INTEGRATED WITH THE ENTERPRISE ARCHITECTURE TO EXTEND SECURITY MONITORING AND CONTROL OF PRIVATE CELLULAR NETWORKS.***

Star

Cellular

Mesh

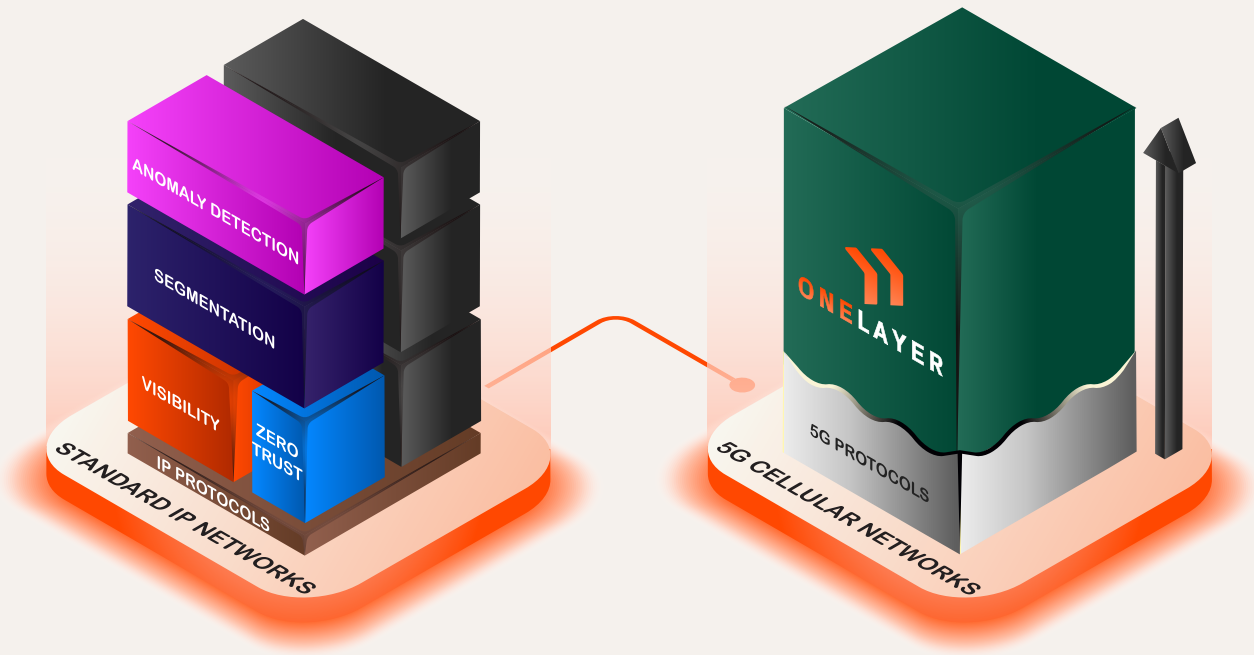
Cable / WiFi

Different connection flow
No ACL ports

Start your journey to secure IoT and private cellular network

The business potential – and the security requirements – for IoT are now well-understood by most enterprises. Now that private cellular networks have emerged as a fundamental architectural building block for IoT, it's more important than ever for networking and security teams to find ways to overcome the limitations described above.

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

ONELAYER