451 Research | Business Impact Brief

Securing Private 4G/5G Mobile Networks

The 451 Take

A private mobile network brings a range of benefits that are attractive for enterprises supporting workloads with latency intolerance that are mission-critical with the need to support a high degree of mobility. For these reasons, uptake of private mobile networks will be especially strong in industrial and 'mission critical' verticals such as manufacturing (Industry 4.0), mining, energy & utilities, water, oil & gas and public health. The emerging architectures of private mobile networks introduce new security challenges to enterprises that, until now, were only known to mobile operators. Will they hold up? We believe so, but an acceptable security posture will require a strong foundational security architecture to ward off cyberattacks and infiltration. A high level of cybersecurity readiness will ultimately de-risk private network investments.

The threat landscape is particularly challenging in industries where private mobile networks are most desirable. Adoption of next-gen connectivity is clearly on the upswing, as seen in the figure below. When it comes down to adopting and deploying private mobile networks, a robust cybersecurity strategy is needed that enables full visibility into all layers of the network, including the application layer (Layer 7) mobile tunnels. Attack techniques and targets are dynamically evolving as 'black hats' and are in constant competition with 'white hats' to locate, expose and attack security gaps for financial gain, terrorism or political motivations.

Current Deployment of Next-Generation Connectivity as Part of IoT Initiatives

Source: 451 Research's Voice of the Enterprise: Internet of Things, Voice of the OT Stakeholder, 2H 2018

Q: Has your organization deployed next-gen connectivity (e.g., 5G, Private LTE, LP-WAN) as part of a current IoT initiative(s)?

The Mirai botnet attack in 2016 demonstrated how IoT devices could be weaponized to carry out a distributed denial of service (DDoS) attack that reached 620Gbps using over 600,000 connected devices like routers and cameras. Other common threats to private mobile networks in mission-critical industries are cyber espionage to gain access to critical control systems and spear phishing campaigns run by nation-state actors to exfiltrate sensitive intelligence, trade secrets and intellectual property. In 2019, a cyber-espionage group targeted government and industry digital infrastructure in Saudi Arabia and the US. That same year, US grid regulator NERC issued a warning that a major hacking group with suspected foreign ties was conducting reconnaissance into the networks of electrical utilities. New malware families are constantly emerging and launching new attacks. In mission-critical industries, security breaches cost more than just downtime, lost revenue and tarnished brands; they can put human lives in jeopardy.

These verticals rely on their private mobile networks to interconnect and secure their complex, multi-vendor supply chains and industrial machinery. These systems are particularly difficult to secure from end to end because if only one participating vendor falls short on security, it jeopardizes the entire supply chain. Deploying or relying on a private mobile network requires vigilance when it comes to instituting security postures. IT leaders lack visibility into the mobile traffic because proprietary mobility protocols such as mobile encapsulation (GPRS Tunneling Protocol) are used on the data and signaling planes for carrying traffic. This results in difficulty in enforcing consistent security policies and threat prevention within the private mobile network.

451 Research® | Business Impact Brief

The 451 Take (continued)

Private mobile networks using LTE and 5G will require a dedicated network controller called an evolved packet core or 5G core. The network controller brings critical functionality such as mobility session authentication and management, data routing, quality of service and packet inspection. Network controllers can be attacked by in-network IoT devices infiltrated and weaponized with malware to launch a DDoS attack on the network. Unlike mobile network operators that have high-capacity network controllers, we expect the network controllers of private mobile networks to suit enterprise needs and have a relatively low capacity, so even a small-scale DDoS attack from internal devices and users could impact the network performance or completely stop it.

Traditional approaches to network security such as using IPSec encryption and firewalls on the internet gateway do not do an adequate job of protecting the most important part of a mobile network: the network controller. While encrypting IP traffic provides privacy of mission-critical or sensitive information, it makes it easier for hackers to hide and deliver malware and exfiltrate data. While deploying a perimeter firewall can help thwart external attacks, it is woefully inadequate in detecting attacks from inside the network. When an inside attack is detected, it's already too late to avoid damage.

Business Impact

PRIVATE MOBILE NETWORK SECURITY POSTURES MUST PROVIDE THREAT PROTECTION IN REAL TIME FROM AN EVER-WIDENING THREAT LANDSCAPE. In private mobile networks for mission- and business-critical industries, these threat actors are sophisticated and use a dynamic array of internal and external attack vectors.

PRIVATE NETWORK INVESTMENTS MUST INCLUDE A STRONG SECURITY POSTURE. At stake is business continuity, adherence with security and privacy regulation and client expectations, and overall customer confidence. One significant breach is all it takes to destroy reputation, cause financial ruin and, worst of all, loss of life.

Looking Ahead

When considering a private mobile network, security is job #1. Your security posture should enable you to detect and stop malware, command and control, and other vulnerabilities within the private mobile network; block multi-stage attacks across user, control and signaling planes; and excel at correlating, isolating and blocking compromised devices from the network. Best practices for securing a private mobile network include deploying a next-generation firewall within the mobile network between the radio access network and network controller, which will protect the network controller from IoT malware and DDoS attacks and unauthorized communications and provide full visibility into the network; cloud-based threat intelligence bolstered by AI/ML to respond to threats in real time; and real-time correlation of threat logs including mobile-specific identifiers IMSI/IMEI (SIM card ID/hardware ID) to ensure threats are isolated and infected devices removed.

Strong security portends digital success. The winners of the digital transformation efforts in the markets considering private mobile networks will be those that can efficiently transform while maintaining the same or improved security posture to what they have in place today. Choosing partners with the right solutions and skills to address the unique security challenges posed by private mobile networks will be germane to success.