aeris

# Cellular IoT Security:

## Why Visibility is the Missing Link

Kaleido Intelligence

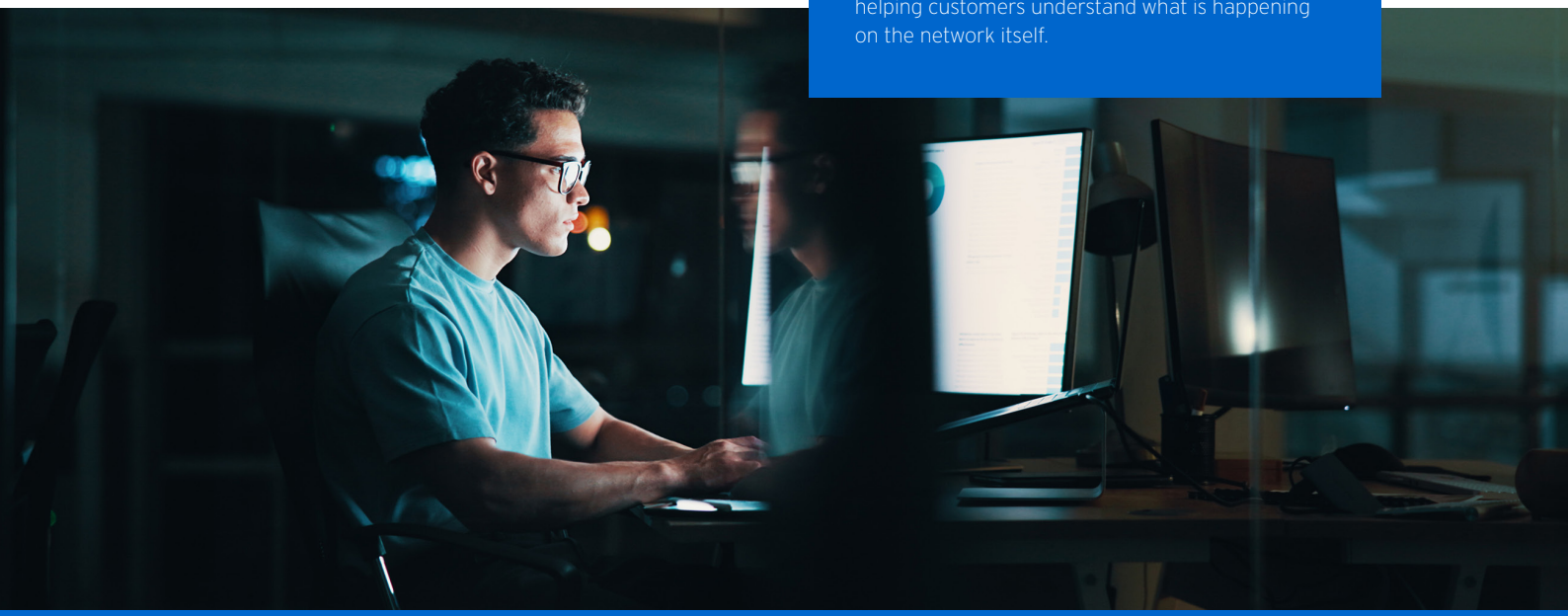
Mobilesquared
Decision-ready data

# Security is only as good as its weakest point

During September 2025, automotive OEM Jaguar Land Rover announced that it had fallen victim to a cyberattack that led to it shutting down IT and OT systems, rendering it unable to produce any vehicles. Losses as a result of the attack are substantial, with the company losing at least £50 million per week as a result of the inability to produce or sell vehicles. Meanwhile, many of its suppliers have been impacted by the incident. While details of the attack have not yet been released, it is evident that the near-total shutdown of its production systems highlights automotive as both a highly connected industry, as well as one that can be highly fragile where systems are compromised.

No matter what security systems are in place to protect assets, there will always be a weak point, which cybercriminals will attempt to exploit. **This underlines why continuous monitoring is a crucial part of cybersecurity defence: it can help mitigate against unknown threats.**

There can be no doubt that today's market for cellular IoT is maturing. Adoption rates among enterprises and OEMs are higher than ever, while the growing understanding of long-term risk associated with cellular IoT in the context of regulations, commercial relationships and security indicates that those embedded in the ecosystem value IoT as an integral part of their business operations. Security-conscious enterprises will undoubtedly have tools in place in their corporate and cloud environments to monitor for and mitigate against cybersecurity risk, but the reality is that many cellular IoT connectivity solutions on the market do not place a high enough emphasis on helping customers understand what is happening on the network itself.



# Security a top enterprise concern, and a barrier to IoT scale

Cellular technology is generally viewed as secure, particularly in comparison with many other communications technologies. It is supported by strong secure-by-design principles where manufacture of the SIM and network access credentials are concerned, but the network layer is not infallible and the backwards-compatible nature of mobile networks carries with it many risks. Even as the industry enters the 5G IoT era, the reliance on roaming connectivity for many devices may prove to be a weak point, given the differing approaches and schools of thought among providers where 'end-to-end' security principles for 5G Standalone roaming are concerned.

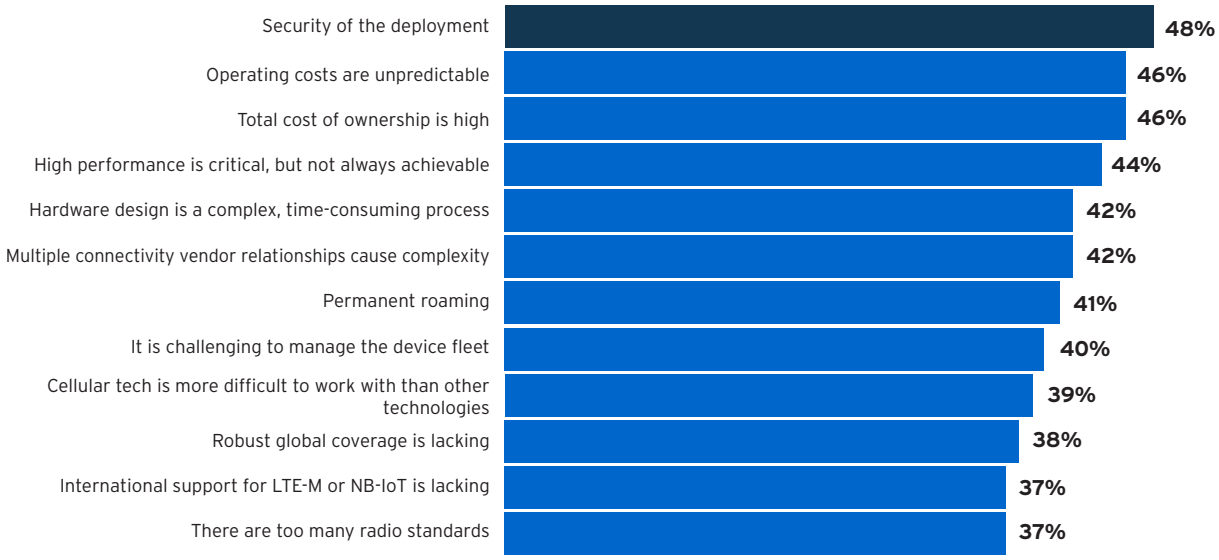
**Kaleido has heard of EV chargers being coerced into acting as part of a botnet, while SIM cards meant to be used for Point-of-Sale devices accessing Netflix content has also been uncovered**

In addition to this, one must consider the fact that IoT is, to a great extent, powered by devices that are deployed in remote locations or in environments where physical oversight of devices is rarely maintained on a consistent basis. Physical tampering of devices thus becomes a real risk, and the types of devices this potentially impacts is wide-ranging: Kaleido has heard of EV chargers being coerced into acting as part of a botnet, while SIM cards meant to be used for Point-of-Sale devices accessing Netflix content has also been uncovered. Most importantly, the fact that secure-by-design principles applied in terms of device design - traffic encryption, software or firmware updates applied during the device lifecycle and adherence to industry guidelines regarding secure product design and deployment - do not account for the fact that the 'hands off' nature of IoT devices make them inherently vulnerable to attack. All too frequently, the misuse of the connectivity capabilities present in IoT devices is discovered too late, due to the lack of visibility into the network that is required for continuous monitoring purposes.

The concept of visibility and continuous monitoring in mobile networks is, for the most part, a key challenge. In networks owned by the enterprise, it is a matter of policy and investment to deploy the necessary security solutions to mitigate the risk of cyberattacks. Cellular networks are not owned by the customers deploying connected devices in them and as such, it is a point of policy on the network owner's part as to whether relevant and timely network traffic information will be exposed to the end customer as part of a continuous monitoring initiative. Today, relatively few operators offer self-service security tooling to end customers, which effectively means that operational visibility is obscured within the mobile network.

There is evidence to suggest that this paradigm has lowered the appeal of cellular as a technology to support IoT operations. I**n an H2 2024 survey of 1,000 enterprises and OEMs conducted by Kaleido, security was cited as the number one reason as to why scaling IoT operations up is perceived as challenging, with 48% of the audience reporting this as a top 5 concern for their organisation.**

**What do you perceive to be the top 5 challenges where scaling up cellular IoT connectivity deployments is concerned? (proportion selected within top 5)**

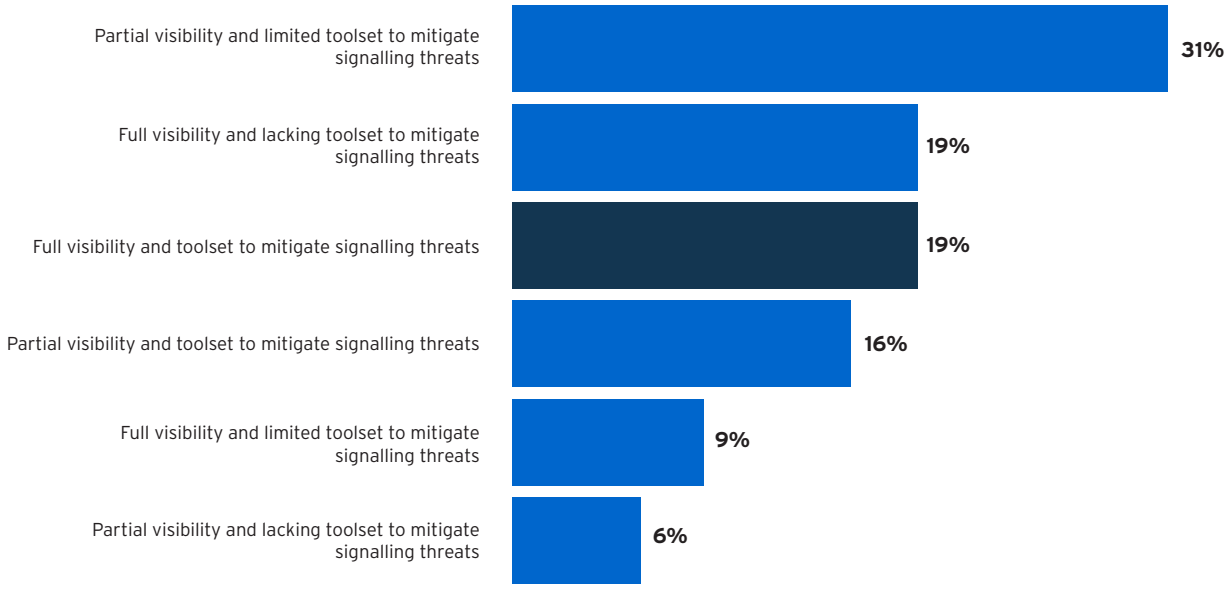



*Enterprise & OEM IoT Connectivity Survey, H2 2024 (n = 1,000)*

# Asset visibility builds trust and scale

Mobile operators will naturally deploy their own tooling to protect their networks in the form of monitoring capabilities and firewalls. However, solutions are rarely complete: in a 2023 security survey targeting 64 MNO and full MVNO respondents conducted by Kaleido, only 19% of respondents reported having a complete toolset to mitigate against signalling security threats. Tools offered to IoT connectivity customers often involve private APNs or VPNs, essentially segregating IoT traffic away from the public Internet and significantly reducing the risk of interception and compromise. However, none of these solutions solve the issue of visibility and continuous monitoring for the end customer, which is an evident requirement given the remote nature of IoT device estates. This means that, if a device inside the cellular network were to be compromised, the end customer would find it difficult, if not impossible, to understand that a breach had occurred. Consider this: if compromised devices are instructed to communicate with rogue servers rather than normally defined endpoints, without the capability to observe the traffic metadata of that device, how will the device owners be able to understand that this traffic is malicious and impacting the business? A savvy user monitoring traffic consumption levels closely may be able to identify an issue, but how timely will this conclusion be formed, and what does it tell the user about the device? Without visibility, it will not be possible to determine whether the device is suffering from a software misconfiguration, or whether it has been compromised in a security incident.

**Do you have visibility to differentiate M2M/IoT from human connections on your network, and do you believe you have the tools to mitigate signalling security threats posed by these connections?**




*MNO & full MVNO Survey, H2 2023 (n = 64)*

It is therefore important to consider that the 'visibility' being talked about in this report has many different qualities. Typical CMPs (Connectivity Management Platforms) will universally expose data consumption per device, but how quickly this information is able to be presented by the CMP varies widely, with some MNOs and connectivity service providers only receiving CDRs (Call Data Records) with data consumption information from their partners up to a day after-the-fact. In addition to this, the session information linked to devices is often high-level, providing only insight into when the device was active on the mobile network and how much data was downloaded or uploaded.

Under an optimal scenario, visibility should be real-time insofar as is possible. As was observed in the Marks & Spencer incident, a lack of continuous monitoring allowed cybercriminals to do far more damage than if systems had been in place to monitor assets in real-time and relay possible indicators of compromise to security staff. The same principle applies to IoT connectivity, in that real-time information simply lowers the risk of threats that persist on the network. In the instance of the Point-of-Sale device being able to access Netflix for instance, the ability to detect this anomalous behaviour on a real-time basis has an immediate impact in terms of cost controls.

**Typical CMPs (Connectivity Management Platforms) will universally expose data consumption per device, but how quickly this information is able to be presented by the CMP varies widely, with some MNOs and connectivity service providers only receiving CDRs (Call Data Records) with data consumption information from their partners up to a day after-the-fact**

# Do you know what your IoT devices are doing?

aeris

Most enterprises don't, but with Aeris IoT Watchtower™ they do! In just four weeks, it detected 17 million dark web events and 50,000 malware incidents across 600,000 IoT devices - all threats traditional security solutions missed.

Learn more


In addition to this, the ability to access detailed information regarding devices' activity is not only desirable, but essential in a security context. Understanding device behaviour in terms of which destination IP targets it is communicating with, how ports or protocols are being utilised in the device, all serve as key indicators as to whether a device is functioning as expected, or if there is something potentially malicious impacting it. In many cases, the traffic flows from compromised devices may look similar to expected traffic, and finding indicators of compromise may prove challenging without the ability to understand how the device is communicating at a deeper level. In addition to this, **regulations such as the EU's Cyber Resilience Act and NIST's IR 8563 increasingly demand that IoT device estates a subject to continuous assessment in terms of their behaviour and risk level in a security context, while the UNECE's R155 regulation means that vehicle OEMs must assume responsibility for the security of assets across the value chain, meaning that compliance must be demonstrated across that value chain**, which the mobile network is a part of. In practice these regulations mean that any company audited or impacted by a security incident and requiring a means to demonstrate compliance is likely to benefit from key points of proof.

There can be no doubt that asset visibility forms the bedrock of any robust cybersecurity risk mitigation strategy, with such tools being applied across many enterprise environments. However, without visibility into the behaviour of devices on the mobile network, IoT deployments over cellular networks essentially prevent end customers from having a holistic view into the security of their device estates. This erodes trust in the technology - those operating in regulated industries or where security of operations is paramount are likely to be deterred from using cellular as an IoT technology, unless this gap is bridged. The duality of increasing reliance on IoT to achieve positive business outcomes, as well as an increasingly strict regulatory environment with financial liabilities associated with non-compliance, therefore provides those who are able to offer appropriate tooling a differentiator, and help build scale in cellular IoT. As observed in the Marks & Spencer incident, blind trust can lead to serious consequences where cybersecurity is concerned.


Kaleido Intelligence

Mobilesquared
Decision-ready data