Bylined Article

Actionable insights to address Enterprise 5G cybersecurity threats

Carlos Cordero, CTO at Fujitsu Spain

Is your organization considering Enterprise 5G (E5G) as part of a digital transformation program? Because more and more organizations are. And there are several good reasons why it might be on your agenda.

- E5G is an agile and powerful infrastructure model. Its high-speed, high-capacity, and low-latency capabilities enable real-time data utilization and greater scope to respond promptly to market dynamics and innovate faster.
- E5G supports massive Machine Type Communications (mMTC) for deploying sensors, cameras, and IoT devices. This connectivity revolutionizes operations across various industries, from manufacturing to logistics, by creating new sustainability options, boosting worker safety, enabling automation and autonomous vehicles, and delivering data-driven decision-making.
- Beyond being a network technology, E5G serves as an innovation platform. Combined with edge computing services, AI, machine learning, and data analytics, it unlocks new possibilities to transform processes, enhance services, and secure assets.

New attack surfaces

You can't assume that all E5G networks are secure by design, though. When you create one, you connect thousands of things to the network, an order of magnitude greater than Wi-Fi. That's why you're doing it, but it also increases the potential attack surface. Nokia published a report in June 2023 that showed distributed denial of service (DDoS) on IoT networks, originating from insecure IoT devices, increased five-fold over the previous 12 months. That's just the tip of the new threat iceberg you could face.

Specific vulnerabilities that arise with increased devices and IoT include malware propagation, denial-of-service attacks, and compromised sensors impacting critical operations.

There are threats beyond the network too, such as compromised software updates or ecosystem or supply chain vulnerabilities affecting hardware used in the network. If you want to get deeper into this, also taking compliance into consideration, the European Union Agency for Cybersecurity (ENISA) has performed a deep threat analysis. Based on that, it has also published a wide range of documents that define 5G Security and outline proper protection of 5G and network function virtualization infrastructure.

Actionable insight 1: Enforce zero-trust media access controls.

You must take care of this from the beginning by integrating a solid layer of cybersecurity technology. For example, we integrate a hard layer of protection on the media access control. This means the bad guys can never connect to the RF equipment or endpoints without your approval. This is an enforced zero-trust policy. The technology even analyzes device "behavior". After only a few days of operation, we can detect if a firmware device has

been tampered with or updated and, if yes, it is automatically disconnected. We are so confident of our approach that we guarantee 100% access point control.

While this protects your private 5G infrastructure, in addition to media access control, customers still need to protect their apps, servers, and protocols — just as they would with any other network technology, such as Wi-Fi or 4G.

Actionable insight 2: Start to leverage the data from your E5G network.

In addition, you need some kind of observability platform for threat detection – a bit like you might already have for managing cloud activity. This is new, and there will be significant changes in 2024 regarding private 5G and observability. These changes will profoundly impact real-time monitoring, anomaly detection, incident response, overall network health, power consumption and CO2 reduction.

Given the huge number of features included in the 5GSA 3GPP standard, many more metrics are available from the network core and the user plane than in previous releases. These will allow businesses to develop their own observability platform metrics and enable real-time monitoring of every network slice, as well as detection and even prediction of anomalies on the network. In addition to those metrics, users will also be able to manage the power consumption of the network in real-time using, for example, Fujitsu AI network technology.

What has been happening in E5G so far has chiefly involved pilots testing the edge of the technology. 2024 will be different — with increased deployments and huge numbers of sensors attached to networks — observability is now a must-have. It's a fascinating time in E5G, with new use cases and business value propositions emerging rapidly.

Carlos Cordero
CTO at Fujitsu Spain

Carlos Cordero has been CTO of Fujitsu Spain since 2016. Since joining the company, he has promoted, with his strategy, projects aimed at building an integrated value proposition that enhances the digital transformation of companies.

Carlos Cordero has studies in Medicine and Surgery from the San Pablo CEU University and has extensive experience of more than 30 years as a manager in the Information Technology sector. His professional career includes highly responsible positions in different companies, such as vice president and CTO of Iberia at Capgemini or Corporate Director of Alliances at Indra.

