5G MNO IoT security roles across the IoT stack

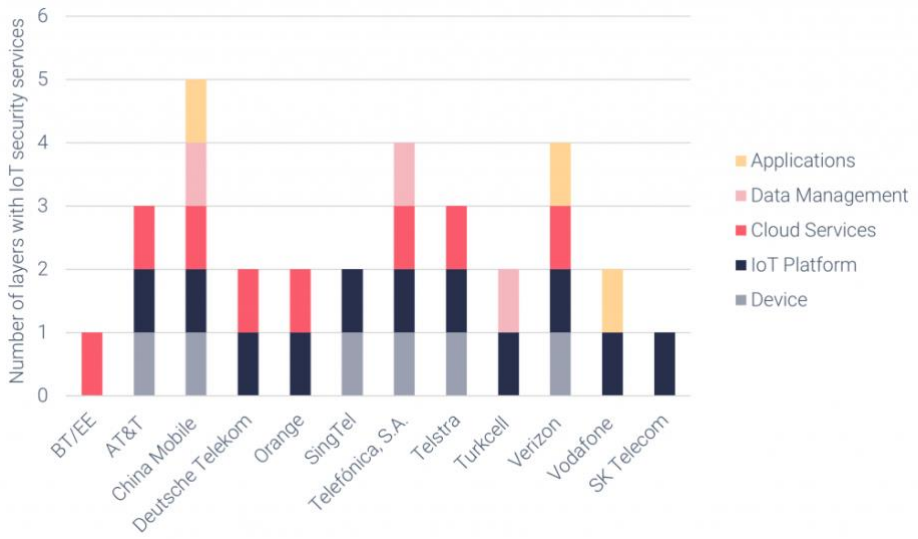
As part of our study IoT security: The foundation for growth beyond connectivity, we looked at the IoT security services of 12 MNOs to see what they are doing to address enterprise IoT security needs beyond that of secure connectivity.

STL Partners

The architecture stack for an IoT solution can be simplified into four layers: Data collection (sensors, devices for data gathering), data exchange (connectivity to enable transmission), data management (organising, analysing and acting on data) and data utilisation (applications). Each layer represents a surface area for a potential security breach. For this reason, enterprise customers require visibility at every stage in the deployment of an IoT solution, in order to monitor and respond to IoT security threats.

We analysed the services of the 12 MNOs based on the architecture layer that the services provide insight into to assess their current areas of focus (beyond connectivity) from an IoT security perspective. For the purposes of the analysis, the data management layer is broken down into three sub-layers (IoT platform, cloud services and data management) to reflect the different revenue streams operators are targeting in IoT security.

MNO's IoT security offerings by architecture layer



Source: STL Partners

IoT security beyond connectivity

China Mobile offers the richest portfolio of IoT services, with offerings that provide visibility all the non-connectivity layers of the IoT stack. It offers the most insights to its enterprise customers; whether this is translated as billable insights, as part of a security offering, is not clear. Other operators such as Verizon and Telefónica S.A. offer services in four categories.

IoT platform analytics is the most readily available asset that IoT-oriented MNOs can leverage to address enterprises' need to continuously monitor and respond to security events in their deployments, as well as to contextualise security incidents and events. Using

cloud-based platforms, MNOs can to pull together data from their connectivity services (e.g. SIM and device statuses) and apply analytics to offer their IoT customers information about their deployments, such as cloud access and authorisation, privacy management, security updates and remediation. As IoT platform capabilities expand to enable easy integration of IoT status and data directly into enterprise systems through APIs, IoT operators that have their own platforms or have influence on the development roadmaps of the platform they are licensing will be better at supporting their enterprise customers.

As operators' IoT portfolios progress from providing connectivity for a small number of M2M SIMs to larger scale deployments with thousands of IoT connections, the requirement for more sophisticated deployment, device management and monitoring services will grow to enable more intelligent applications. Similarly, security offerings will be required to evolve from point solutions, to more coordinated, integrated, and scaled propositions that address security requirements across the stack.

For more detail on this, please go to IoT security: The foundation for growth beyond connectivity

Other reports addressing the IoT include:

- Why the consumer IoT is stuck in the slow lane
- eSIM: How to break through the barriers?
- Reliance Unlimit: How to build a successful IoT ecosystem

How STL Partners Growing Enterprise Revenues can support you

Our research provides insights into how enterprises in different verticals are leveraging new technologies such as 5G, AI, IoT and cloud to solve critical operational needs, as well as key strategies and partnership models telecom operators are leveraging to address these needs.

Get in touch to understand how STL Partners can support you:

amy.cameron@stlpartners.com

Or visit our website to discover more:

https://stlpartners.com/growing-enterprise-revenues