Vendors must actively engage with CSPs to overcome challenges in implementing observability platforms

September 2022

Bence Szeidl

Communications service providers (CSPs) face a number of challenges when implementing observability[1] across their cloud-native environments. However, vendors can help by providing observability platforms with key features such as open APIs, the ability to contextualise telemetry data and the ability to expose that data for further analysis. Vendors should also help CSPs to overcome issues affecting their individual environments in order to maximise CSPs' returns on investment.

This article is based on research carried out for Analysys Mason's report, *The role of observability in a telecoms environment and how vendors can facilitate its implementation*.

Observability platforms can unlock key data about the cloud-native stack, but this data must be accessible and usable

The cloud-native stack is made up of software-based microservices that are designed to generate and expose data about their performance; the concepts of telemetry and manageability are built in. An observability platform is required to collect and aggregate this data for analysis so that management tools can understand what is happening in the environment and make the appropriate adjustments. Cloud-native stacks also can consist of many different tools provided by multiple vendors. As such, vendors need to design observability platforms that have certain key features built into them to ensure that they can effectively collect, store, analyse and expose data generated from CSPs' cloud-native software stacks. These observability platforms need to have open interfaces to enable the collection and exposure of telemetry data (logs, metrics and traces) from the entire cloud-native environment, and should be able to collect this data regardless of which vendor has supplied the cloud-native component. Open and standardised APIs are crucial for collecting telemetry data.

Contextualisation is another key feature of an observability platform; correlating telemetry data and performing basic analytics helps to uncover what is happening within the cloud-native stack. This capability is also responsible for filtering out noise from telemetry data.

Finally, an observability platform needs to expose the collected, correlated and contextualised data, as well as the insights it has generated, to external applications. These external applications include service assurance, security and application management systems, which can make use of observability data to perform further analytics and act on insights to address issues or optimise the cloud-native software stack.

---

1 Observability is defined as the ability to measure the state of a system based on the data it produces. For more information, see Analysys Mason's *CSPs must adopt an observability platform to unlock the key benefits of cloud-native environments*.

Challenges related to data availability can worsen the performance of observability platforms

Vendors and CSPs should expect to face challenges when implementing observability platforms due to data management issues, organisational changes and a lack of industry alignment. The top three issues related to data management are improper instrumentation, a lack of access to certain data sets due to encryption and a reliance on proprietary vendor solutions. The negative implications of not addressing these issues range from sub-par observability platform performance to an increased financial burden on CSPs.

- **Improper instrumentation.** Instrumentation is defined as the configuration of system components to measure/record what they are doing. Observability platforms need to have access to the data obtained by collection agents across the cloud-native stack, and this data must be stored within a centralised data platform. Failing to instrument components will result in incomplete data sets, thereby making the cloud-native environment less observable.

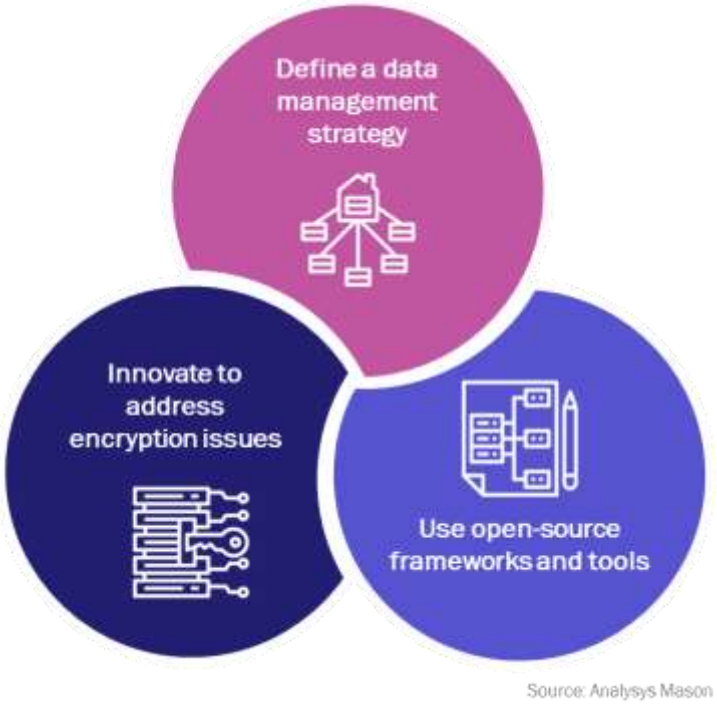
- **Lack of access due to encryption.** Data access challenges can stem from factors such as the encryption of communications between network functions within the 5G core. This means that observability platforms cannot perform effectively because they are unable to create a complete view of the cloud-native system.

- **Proprietary vendor solutions.** Proprietary monitoring tools that are embedded in cloud-native applications add to the challenges related to data management. It is important to consider the integration of these data collector agents during the implementation of observability platforms. The platform will not be able to provide full visibility of the cloud-native environment if these agents do not integrate with the data infrastructure that is established within the observability platform.

Vendors can play a pivotal role in helping CSPs to extract the most value from observability

Vendors should work closely with CSPs to help them to introduce observability platforms into their organisations. Vendors can help CSPs to define a data strategy, build on an open-source framework while delivering on that strategy and address issues related to encrypted data sets (Figure 1).

Figure 1: Key ways in which vendors can help CSPs to address data management challenges



A clear data strategy is crucial for CSPs; defining expectations and aligning existing capabilities/resources with systems' requirements for observability are essential to ensure a return on observability investments. Vendors can help CSPs to work out which tools they should use to collect various data sets and how frequently they should collect data. Additional considerations include the length of time that data can be stored for and which type of storage solution to use. Addressing these will lead to a clear and well-defined data strategy that helps CSPs to achieve specific outcomes while minimising costs.

Observability solution providers should adopt open-source frameworks and toolsets that enable observability. This will help to accelerate CSPs' implementation of observability. Projects such as OpenTelemetry (OTel), an open-source observability framework, can serve as the blueprint for the standardisation of instrumentation and data collection using tools developed by the Cloud-Native Computing Foundation (CNCF). OTel ensures that the relevant data sets are produced by the cloud-native components. It also makes data available in order to reduce the risk of data silos. OTel is not defined specifically for the telecoms environment, but observability vendors can adapt this framework and contribute their efforts to the OTel open-source community.

Challenges around producing or accessing data that is encrypted within the 5G core remain, but vendors are already exploring cutting-edge technologies to get around them.