MantisNet

Real-time, network visibility and intelligence solutions

VENDOR AGNOSTIC 5G VISIBILITY

WHITEPAPER

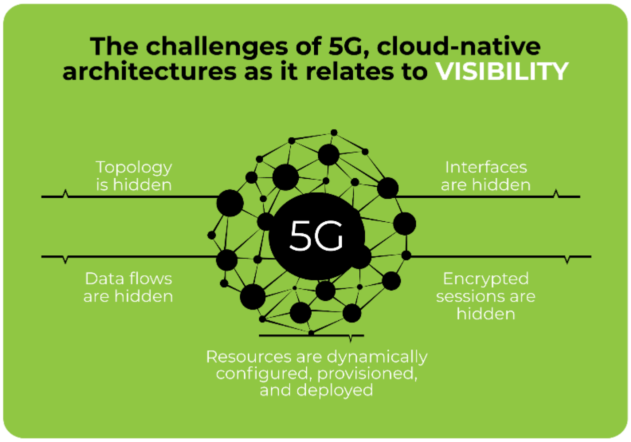
Table of Contents

Introspecting 5G SA Environments:

Containers are essential to the success of 5G networks, as they are leveraged heavily throughout the entire network deployment (Core, MEC, and RAN/O-RAN) and are needed to establish highly scalable infrastructure that can deliver on the latency and speed promises of 5G networks. Additionally, the 3GPP has dictated that any 5G Stand Alone (SA) environment needs to leverage a Service Based Architecture (SBA) core. The SBA is standardized on container technology, thus further highlighting the fact that container environments are "here to stay" in 5G networks.

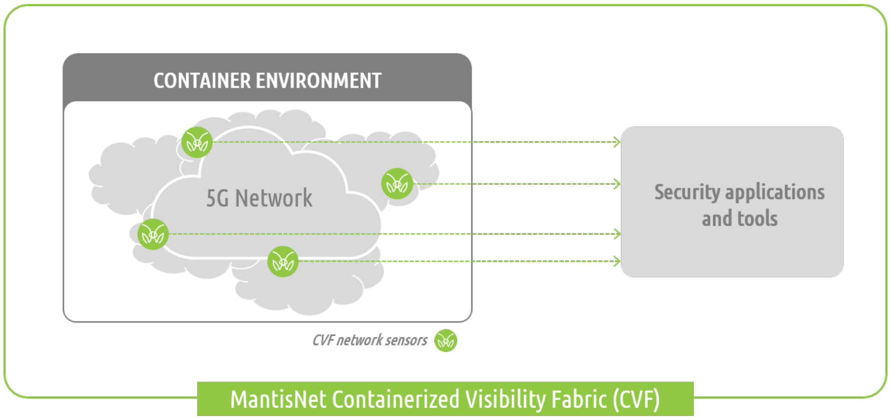
When discussing the importance of containers to 5G environments, it is also important to note the challenges that come along with the many benefits of deploying container technology within a network. The main challenge containers introduce is that of data visibility, or more specifically, a lack thereof. Organizations of all sizes have long seen the value of monitoring the networks through which their data moves (AKA establishing network/data "visibility"). By establishing a data visibility strategy, organizations can ensure that a) the network is operating as designed from an availability and performance standpoint and that b) the network is not exposed to cybersecurity threats and is positioned to identify and mitigate any threats that breach the network.

However, 5G visibility has been a challenging problem to solve because container environments do not lend themselves well to traditional "data access" tools and techniques. The use of physical network TAPs, SPAN/Mirror ports, network packet brokers, and vTAPs is no longer a viable option to gain visibility into containerized 5G networks. Simply put, these solutions provide zero visibility into container environments. Additionally, options offered by Amazon, Microsoft, and Google for visibility into data residing within their "hyperscaler" cloud environments (AWS, Azure, GCP) completely lack container-level visibility. These shortcomings are why a new approach must be taken to ensure that organizations can still monitor and secure networks that leverage container technology (such as 5G environments), and to do so wherever the environment is deployed.


The challenges of 5G, cloud-native architectures as it relates to VISIBILITY
Topology is hidden
Interfaces are hidden
5G
Data flows are hidden
Encrypted sessions are hidden
Resources are dynamically configured, provisioned, and deployed

Container Visibility and Data Access Solution

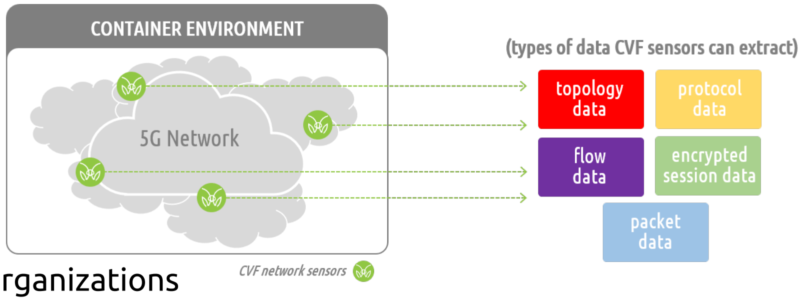
To solve this problem, MantisNet has developed a solution called the Containerized Visibility Fabric (CVF). The MantisNet CVF© is a cloud-native, 100% containerized solution that provides **data access/visibility** into container environments, anywhere from the core to the edge.


CONTAINER ENVIRONMENT
5G Network
Security applications and tools
CVF network sensors
MantisNet Containerized Visibility Fabric (CVF)

The CVF leverages container-based network sensors to achieve data access into any cloud-native/container environment. These containerized sensors provide comprehensive visibility into all container level traffic and are deployed dynamically with infrastructure as it is being stood up and torn down. Often through Kubernetes (operating as a daemonset), the sensors automatically scale up and down with 5G network resources to ensure continuous, real-time access to the functions being monitored. Distributed across the entire environment, and with built-in "tapping" capabilities, these sensors are able to access all 5G traffic- whether it is traditional packet traffic, or internal container-to-container "API-like" exchanges.

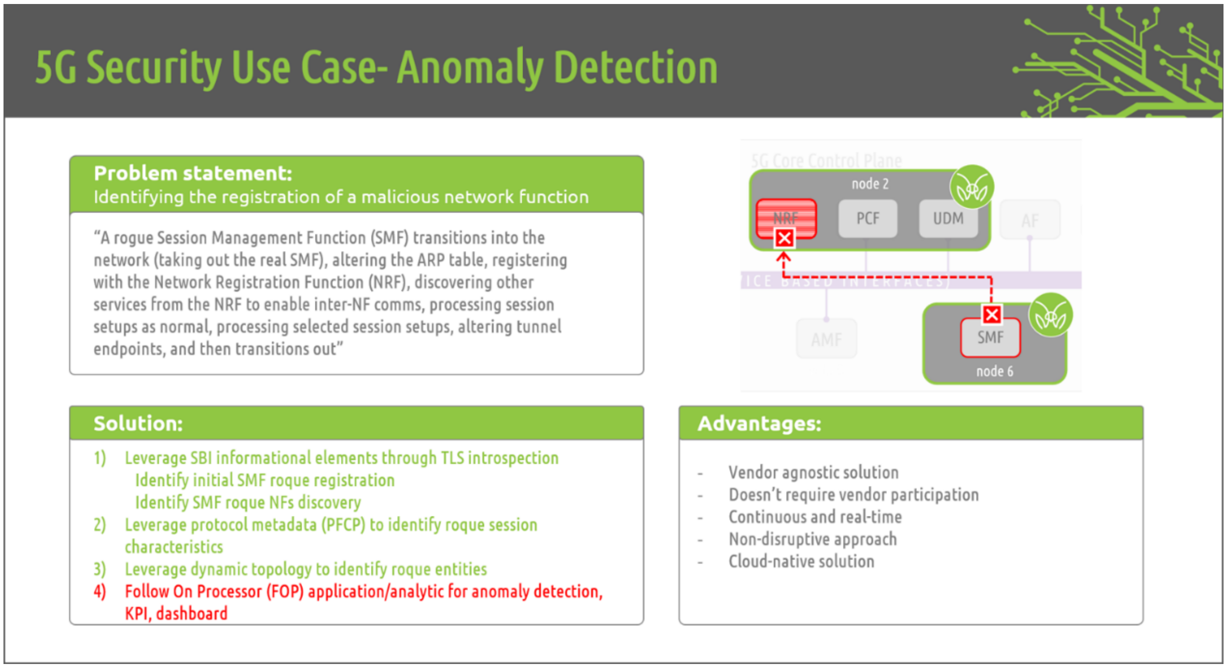
Benefits of the solution:

First and foremost, the CVF allows organizations to **overcome the visibility gap** that exists today for gaining insight into container environments (as outlined above). In addition to this, the CVF is also **highly customizable**- organizations can target different areas of any 5G network and extract a variety of datasets. Whether it is gathering and storing full packet captures, or inspecting metadata and cloud-native flow records, the CVF provides a unique ability to gather targeted data from any location and immediately send this data into a wide range of security applications and tools.



Another area where the CVF provides clear value is that of **introspecting and gaining visibility into 5G cores (SBA)**. Within the SBA, all Network Functions (NFs) communicate through a Service Based Interface (SBI). This interface/communication path provides two unique challenges to any organization attempting to monitor the information moving within the 5G core. The first challenge is that all information is TLS1.3 encrypted…the encrypted traffic must be presented in a form (plaintext) that is readable by security tools. The second is that these NFs do not communicate via typical packet exchanges- the SBI interface utilizes HTTP/2, leading to information exchanges that are more “API-like” in nature. Any solution attempting to provide visibility into the SBA core needs to handle both challenges simultaneously.

While other network visibility companies are beginning to develop container-based network sensor solutions, MantisNet already holds a unique position in the marketplace in being able to provide 100% visibility into the SBA. The MantisNet CVF provides the payload (in plaintext format) for all 5G core encrypted data exchanges, as well as handles the API-like nature of these NF communication exchanges. In short, when CVF sensors are deployed within a 5G core they serve as a data source for security applications to introspect all the traffic and access unencrypted SBA traffic, packaged in an easy to ingest format. Establishing visibility into the SBA (and ensuring security of all 5G core network functions) is critical for any 5G network to be successful. The following use case will help better explain the importance of securing these container-based 5G environments, and how MantisNet aids in accomplishing this.



5G Security Use Case- Anomaly Detection

Problem statement:
Identifying the registration of a malicious network function

“A rogue Session Management Function (SMF) transitions into the network (taking out the real SMF), altering the ARP table, registering with the Network Registration Function (NRF), discovering other services from the NRF to enable inter-NF comms, processing session setups as normal, processing selected session setups, altering tunnel endpoints, and then transitions out”

Solution:

1) Leverage SBI informational elements through TLS introspection
   Identify initial SMF roque registration
   Identify SMF roque NFs discovery
2) Leverage protocol metadata (PFCP) to identify roque session characteristics
3) Leverage dynamic topology to identify roque entities
4) Follow On Processor (FOP) application/analytic for anomaly detection, KPI, dashboard

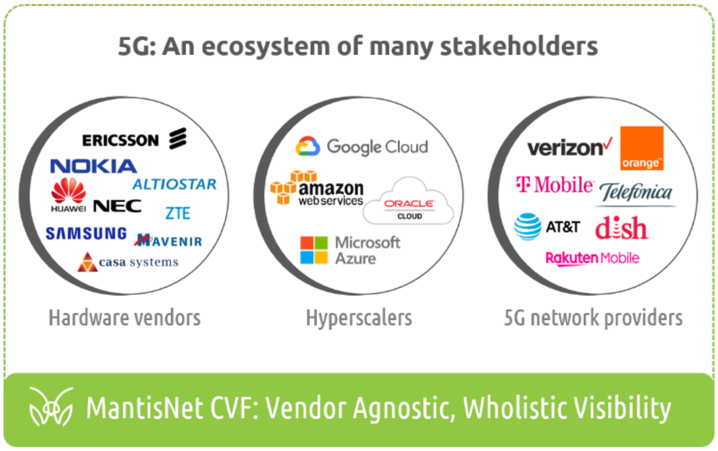
Advantages:

- Vendor agnostic solution
- Doesn’t require vendor participation
- Continuous and real-time
- Non-disruptive approach
- Cloud-native solution

Vendor Agnostic Visibility

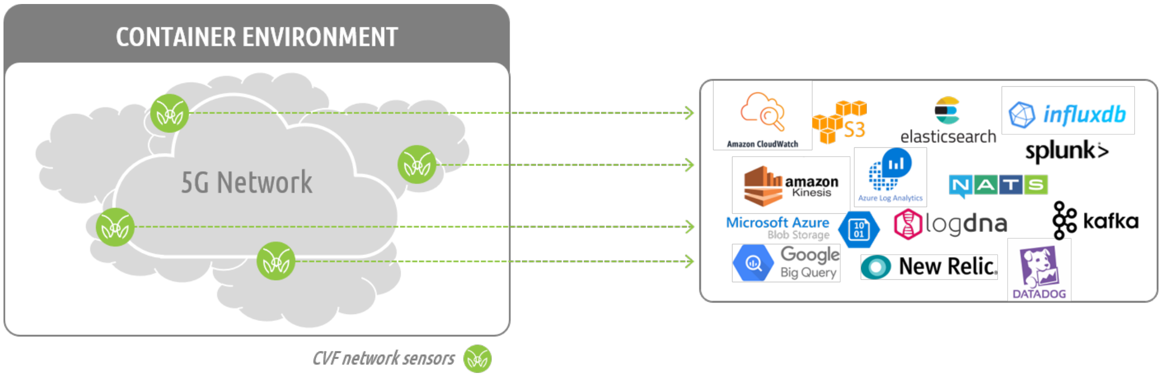
The MantisNet CVF is a **completely vendor agnostic solution**- the underlying infrastructure does not matter to the CVF solution. Whether the 5G components are deployed on-premise as part of a private network installation, within a carrier's network, or by a hyperscaler such as AWS, the MantisNet CVF provides granular visibility into what is occurring within and across the network.

To take a closer look at this, let's consider a 5G environment that has multiple vendors deployed at all levels- different vendors within the core, the MEC, and the O-RAN for instance. These network equipment manufacturers may provide some proprietary monitoring statistics/information on what is happening within their infrastructure; however, network operators are now challenged with implementing a monitoring system that can collect, correlate, interpret, and analyze all the formats of vendor specific data to determine what is happening across the entire 5G network as a whole. MantisNet provides a solution to this challenge: a wholistic (and customizable) source of data across the entire 5G network, regardless of vendors being used, that is immediately streamed to any security tool available.



Being vendor-agnostic, it does not matter to the CVF what underlying vendors are being used for the specific systems, subsystems, and components within a network. The CVF acts as a single touch point to gain access into the information within containerized environments and provide a rich variety of data to security applications- above and beyond what vendors provide. Furthermore, the CVF does not even *require* vendor participation- if you have access to the environment (and common tools such as Kubernetes), then you can deploy the MantisNet CVF.

As mentioned above, another fundamental CVF design principle is to provide **easy integration with a wide variety of security applications and tools**. As a reminder, the CVF provides targeted and wholistic visibility into all 5G/container-based environments, but it does not provide the security analysis component. Our approach is to take the information from our containerized visibility fabric and present it in a format that is easily ingested by **any** security tool or application.



From leveraging messaging busses such as NATs and Kafka, to integrating with open-source content conversion tools such as Fluentbit, our technical approach facilities the movement of data from our CVF into any security application or tool.

5G SA Deployment Considerations

Where can this solution be used?

The MantisNet CVF is designed to be used within true 5G Stand Alone (SA) environments- these environments heavily leverage containers by design, and the CVF provides the most value in this scenario. Here are three points to consider when evaluating whether or not MantisNet can add value in a specific 5G deployment:

1) Is it containerized? It does not matter if the container environment is deployed on bare metal or on virtual machines. What does matter is if containers can be supported within the system natively, or in a VM.
2) What version is the Linux kernel? The CVF leverages eBPF as a core component of its design. eBPF allows the CVF to have a very performant and lightweight footprint, however, the underlying Linux kernel needs to be able to support eBPF technology. A general rule of thumb is that the CVF will work with a Linux kernel that is version 4.19 (released in October 2018) or newer
3) Are resources available to be used? The CVF operates no differently than any microservice deployed in a cloud/container environment- it requires resources. Discussions must be had regarding these resources early on, to ensure that MantisNet sensors can operate effectively. This is normally not an issue, as MantisNet sensors are extremely lightweight (for example, a sensor collected topology data only utilizes .05% of compute resources), but it is important to note upfront.

ABOUT MANTISNET

MantisNet solutions provide organizations the real-time network monitoring and processing solutions they need. MantisNet's advanced technology enables organizations to better monitor and manage network traffic as compared to legacy hardware and software solutions.

FOR MORE INFORMATION VISIT WWW.MANTISNET.COM

MantisNet
11160 C1 SOUTH LAKES DRIVE,
SUITE 190
RESTON, VA 20191
571.306.1234
INFO@MANTISNET.COM