MantisNet

Real-time, network visibility and intelligence solutions

5G & CLOUD-NATIVE SECURITY

WHITEPAPER

MantisNet

Real-time, network visibility and intelligence solutions

If the cloud-native future is on the not-so-distant horizon, what are the inherent security challenges to these new container-based environments? Do network professionals need to take a new approach given that these environments are built to be software-driven, dynamic, ephemeral, and highly scalable?

The push towards cloud-native, 5G networks is beginning to gain even more attention in the greater networking community. The amount of 5G-related commercials and marketing content alone helps support this statement, however, a recent study done by the Business Performance Innovation Network titled "Toward a More Secure 5G World" brings a bit more clarity to where things are today. Through the global polling of communications service providers, as well as supporting mobile networking technology companies, the study helps highlight where service providers are on their push towards establishing 5G environments. 45% of respondents indicated that they are "moving rapidly towards commercial deployment" of 5G networks, a significant increase from the previous year's tally of 26%. On top of this, 71% say they will begin commercial deployments in the next 18 months.

According to Business Performance Innovation Network Research: '45% of respondents indicated that they are "moving rapidly towards commercial deployment" of 5G networks, a significant increase from the previous year's tally of 26%.

On top of this, 71% say they will begin commercial deployments in the next 18 months.'

Now these numbers do apply to both non-standalone (NSA) deployments, as well as stand alone (SA) deployments…the largest difference between the two being which core is used- the already tried and true 4G core used in NSA deployments, or the next generation 5G core where SA architectures leverage a service-based architecture (SBA) standardized on container technology. However, one can also see that there is a significant push towards these true cloud-native/SA environments with the recent news Dish has made in their public commitment to SA, as well as what Rakuten has already accomplished in Japan. T-Mobile, AT&T, and Verizon have also all publicly stated that they will be standing up full SA environments in roughly the next year.

This push towards cloud-native environments highlights the desire for companies to leverage the full benefit and promise of cloud technology- distributed computing, virtualization of resources, on-demand horizontal scaling- the list goes on. For example, 95% of respondents from the BPI survey indicate that virtualizing network functions is either very important or important to their plans for 5G. This would be impossible to achieve without embracing cloud-native methodologies that allow for virtualization of core network functions- an inherently different approach than "pre-cloud" environments found in predecessor communication networks. The importance of container technology to 5G environments is also clearly stated by these communications companies, with 93% of respondents saying that containers "will be important to building out 5G"…52% say containers will be very important, and 41% say that they will be important.

5G Network Security

So if the cloud-native future is on the not-so-distant horizon, what are the inherent security challenges to these new container-based environments? Do network professionals need to take a new approach given that these environments are built to be software-driven, dynamic, ephemeral, and highly scalable? A recent Brookings report does a fine job of breaking the challenges down into a list of "five ways in which 5G networks are more vulnerable to cyberattacks than their predecessors":

Why 5G Requires New Approaches to Cybersecurity

1. The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing. Previous networks were hub-and-spoke designs in which everything came to hardware choke points where cyber hygiene could be practiced. In the 5G software defined network, however, that activity is pushed outward to a web of digital routers throughout the network, thus denying the potential for chokepoint inspection and control.

2. 5G further complicates its cyber vulnerability by virtualizing in software higher-level network functions formerly performed by physical appliances. These activities are based on the common language of Internet Protocol and well-known operating systems. Whether used by nation-states or criminal actors, these standardized building block protocols and systems have proven to be valuable tools for those seeking to do ill.

3. Even if it were possible to lock down the software vulnerabilities within the network, the network is also being managed by software—often early generation artificial intelligence—that itself can be vulnerable. An attacker that gains control of the software managing the networks can also control the network.

4. The dramatic expansion of bandwidth that makes 5G possible creates additional avenues of attack. Physically, low-cost, short range, small-cell antennas deployed throughout urban areas become new hard targets. Functionally, these cell sites will use 5G's Dynamic Spectrum Sharing capability in which multiple streams of information share the bandwidth in so-called "slices"-each slice with its own varying degree of cyber risk. When software allows the functions of the network to shift dynamically, cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution.

5. Finally, of course, is the vulnerability created by attaching tens of billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT. Plans are underway for a diverse and seemingly inexhaustible list of IoT-enabled activities, ranging from public safety things, to battlefield things, to medical things, to transportation things—all of which are both wonderful and uniquely vulnerable. In July, for instance, Microsoft reported that Russian hackers had penetrated run-of-the-mill IoT devices to gain access to networks. From there, hackers discovered further insecure IoT devices into which they could plant exploitation software.

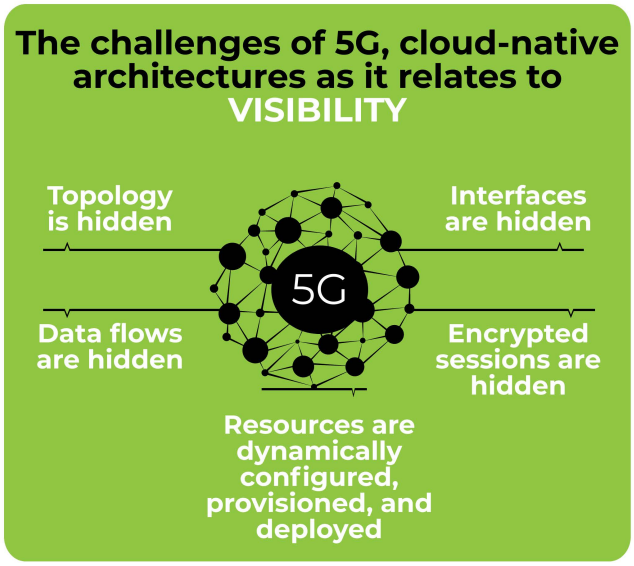
Brookings, Why 5G Requires New Approaches to Cybersecurity, T. Wheeler & D. Simpson, 2019
https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

Exploring 5G Network Security

The Brookings report has hit the nail on the head- many of the challenges facing cloud-native, 5G architectures are routed in the new architecture design and principles of the network. Arguably one of the most challenging security problems pointed out within the report is the shift from hub and spoke, infrastructure-heavy networks to distributed and dynamic virtual computing environments. As the report duly notes, the advantage of having central hubs, or chokepoints, within the network for security monitoring purposes is no longer a reality. Legacy solutions that leverage a mentality of "get the traffic to where it is needed" via network TAPs and packet brokers are now facing a very tough problem. Where are the correct points to tap to get the data if everything is distributed? How many packet brokers are needed across the infrastructure to get at the right data? Is it even possible to use these methods to gain visibility into container traffic.

Among other shortcomings, these legacy approaches focus on a "pull" mentality- of pulling data from where it is being generated, to where it is needed for analysis. This becomes troublesome and extremely cost-prohibitive in cloud environments. "Pulling" large amounts of data turns into an exercise of extracting copies of all network data and sending that replicated data over the cloud to a central processing point, which in turn sends the data to where it is needed. All of this wholesale data movement results in cloud transport expenses incurred and contributes to an unmanageable amount of data to be sifted through and forwarded to appropriate tools- introducing latency and increasing overall time to threat detection. It is also important to note that this flawed strategy is not limited to hardware centric visibility and security solutions. Many "cloud" offerings from visibility companies still rely on a "pull" mentality. The only difference is at the access point- perhaps a vTAP is being used to grab the data, or a container agent, but regardless of the method used, they still largely rely on backhauling that data to a central processing location in order to route information to security tools. The same latency, cost, and threat response time concerns remain.

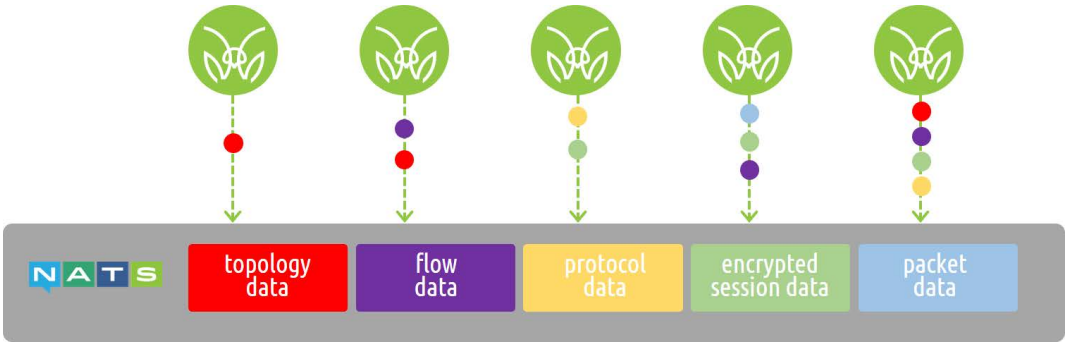
Another major consideration in terms of 5G network security is whether or not the security/visibility solution chosen is in fact cloud-native. Cloud-native is a term that is being thrown around quite a bit, but in most circles it can be broken down to be a label for any solution that is architected from the ground up with container technology at its core. Why does this matter for 5G network security? Any solution that does not leverage container-based agents (including solutions using vTAPs) simply does not have insight into either intra-container traffic or inter-container traffic. This is extremely important to take note of when looking at the mobile network communications world as it continues to push towards environments that are ultimately container based. Visibility at the container level is going to be a requirement.



5G Network Security - Emerging Technologies

With these challenges in mind, it is important to note that there are new technologies emerging which address the unique challenges of 5G network security. Cloud-native, container-based network sensors are one solution to the challenge. Starting with the most important feature- they provide disaggregated visibility into all container level traffic. Cloud-native sensors exist as container agents, which are deployed dynamically with infrastructure as it is being stood up and torn down. Often through Kubernetes (operating as a daemonset), they are able to scale up and down with environments to ensure all necessary visibility points are covered at all times. Distributed across the entire environment, and with built-in "tapping" capabilities, these agent sensors are able to access all necessary traffic- whether it is traditional packet traffic, or internal container "API-like" exchanges. Anything short of a cloud-native sensor can not gain this level of visibility.

Another promising feature of these container-based sensors is that they can tackle one of the largest problems within 5G security solutions- the movement of traffic, and associated cloud costs. As opposed to previously discussed solutions, these agents can be designed in a way to do more than "just capture packets, and send them to a location". As a leader in the cloud-native network visibility space, MantisNet has taken an approach that flips the "pull" mentality of predecessor technologies on its head. MantisNet's sensors are designed to "push" data as a composable system- composable meaning a system made up of multiple components that can be mixed and matched in a variety of ways to achieve an end result. In this particular case, the "components" making up the solutions are Visibility Functions (VFs)- for example, "generate topology metadata" or "generate DNS metadata". Essentially, each container agent has the ability to perform one or more of these VFs at any given point in time (see below diagram for example of the VFs that can be performed). The approach here is to provide each agent with the ability to "push" or "publish" particular types of data from the location they are deployed at, directly to a message bus where any security tool or analytic application can immediately ingest the information.



These agents can be queried by any individual, or analytic system, to send out very specific data…data that is often representative of the larger data being moved, or, if needed, a full copy of the data. The agents are "queried" or "instructed" to perform a particular set of VFs to generate the exact data that is needed. Many of these functions are based on generating metadata- a summation or representation of the larger data flows. It is due to this that cloud data movement costs can be greatly reduced- you are no longer moving all the data, as a complete replicate. You are only moving the data that you directly request, in a consolidated form.

This usage of targeted data "pushing" as opposed to full scale packet capture, or pulling, also helps with the explosion of data 5G systems are bringing. Organizations need to effectively monitor and identify network threats in real-time, however, the amount of information is overwhelming and widely distributed. Leveraging a solution that allows you to selectively target areas of the network to pull out very targeted data sets can lead to an advantage in security posturing. Data is a bit less overwhelming, and traditional tools can now engage with meaningful information in real time.

Turning 5G Networks Into A Data Science Problem - Closed Loop Automation

While targeted metadata can better serve legacy analytic solutions, it is also a prime form of data to fuel the next generation of analytics- mainly streaming analytic engines or event processing engines. These engines/applications are built to operate at blazing fast speeds and interact with data in a very different way than "store, then analyze". Streaming analytic solutions rely heavily on the world of data science, as well as artificial intelligence, to effectively model data sets and set parameters in place to provide real-time analytics on data as it is ingested into the system. Streaming analytic systems are positioned to handle massive amounts of data and provide quick decisioning when it comes to network threats.

However, the only draw back with streaming analytic systems is that of data access. Particularly in cloud environments, data access can often be burdensome, incomplete, cost preventive, or simply hard to manage at scale if using legacy solutions. Newer, cloud-native container-based sensors like MantisNet's Containerized Visibility Fabric (CVF) help address this challenge. Although these sensors are performing many VFs at any given time, one thing holds true across all the data that is being generated (except for raw packet capture)- the data coming out from these sensors is highly structured JSON (or other serialization if desired) key value pairs… AKA metadata. The sensors generate this data continuously and in real time- publishing it immediately into a message queue for streaming analytic consumption. In essence, the sensors are turning the network- a world of highly unstructured and varied data- into a structured data science problem that is primed to be solved by bleeding edge streaming analytic applications.

So why does this matter? Considering that 5G environments are promising an extreme increase in amount of data served, as well as the speed it is transported, traditional "people centric" approaches will no longer suffice. Cyber criminals are leveraging modern machine-driven attacks to target 5G infrastructure in the most effective means possible. In the Brookings report, one of the respondents stated that "we are fighting a software fight with people" whereas the attackers are machines. This very apt statement helps identify the true problem at hand- and the changes in security strategies that need to be taken.

Closed Loop Automation (CLA) is not a new concept, though it is one that is rising in popularity. Networks that are built with CLA in mind aim to be environments that are self-healing and immediately able to identify, characterize, and isolate security threats. Establishing these networks is a goal of many professionals facing the challenges of maintaining and operating 5G infrastructure. The amount of data and the speed of data requires a solution that can turn the network (and observation/security of that network) into something less high touch, and much more machine-driven. CLA hinges on the circular connection of Observing, Identifying, Adjusting, and Optimizing network resources. A combination of cloud-native sensors from companies like MantisNet, streaming analytic solutions, and an orchestration system provide the necessary pieces to establish CLA.

5G Network Security - Attribution

Cloud-native, container-based sensors have a very network centric view of the world. They operate as an event driven system, identifying and alerting to specific network events as they are uncovered. This is not much different from the days of the wired world, where TAPs and packet brokers were used to achieve the same level of visibility. The main difference is where the access is happening. It is no longer on the wire- these sensors are deployed as containers with kernel-level visibility. They are now resident on baremetal machines, or within virtual machines, with complete visibility into all data moving into and out of the machine (on physical wires or virtual paths) as well as all container-level traffic. It is a unique position to be in for network visibility solutions, because for the first time they now have access not only to the network data, but to the end point data as well.

This unique deployment scenario allows for cloud-native sensors to provide correlation between what it is seeing on the network (or within a machine) to what end point or application drove the network event. For the first time network professionals can now associate, or provide attribution to, endpoints based on what is being observed on the network. MantisNet's CVF includes this functionality- for every network event observed, users now have the ability to identify all associated containers, processes, links, flows, PID/UID/GIDs, applications, and command paths. Users can go as far as searching against a particular application, or process type, to find all associated network data. This provides a far more holistic view regarding any network threat, and helps drastically increase the speed to resolve any issues or threats.

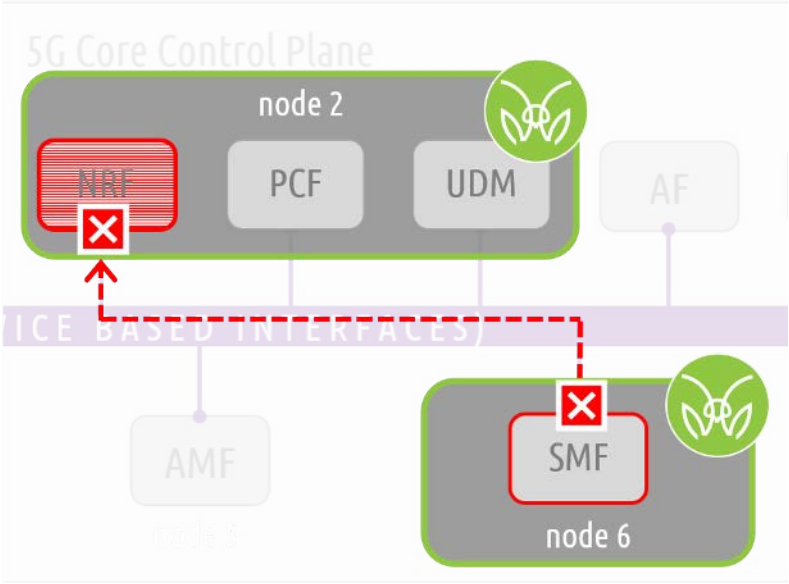
Given the significant changes within 5G, it is apparent that network security approaches need to change with the times. Cloud-native, container-based visibility sensors provide a way to achieve such a shift while maintaining visibility into dynamically changing and highly scalable resources. Solutions such as the MantisNet CVF allow network professionals to deploy a solution that is highly disaggregated and composable- visibility can now shift with resources as they are being leveraged in real time, and a means for dialing in the type of data to push out of the environment can be established. Click here to find out more about the MantisNet CVF offering.

Security Use Case - Anomaly Detection in the 5G SBI

With the potential for compromise elevated in the 5G core services based interfaces (SBI) due to various vendors providing unique network functions (NF), it becomes a priority to monitor for anamolous activities that could compromise the 5G core traffic.

How would you identify 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-NRF communications, processing session setups as normal, processing selected session setups, altering tunnel endpoints, and then transitions out."



With the MantisNet CVF deployed across the 5G environment this can be solved in the following way.

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

The MantisNet CVF provides a few advantages when deployed to observe 5G environments. The CVF is a vendor agnostic solution, that doesn't require vendor participation. Meaning, since we are deployed, and process in-node, we can stream the network data in any vendor format and produce it in an agnostic feed. The CVF is a cloud-native solution that is "always on" and provides continuous and real-time streaming network visibility, that is non-disruptive (deployed as k8s DaemonSet or ReplicaSet).

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