MantisNet Containerized Visibility Fabric (CVF)
Redefining network observability

CLOUD-NATIVE

◦ Flexible microservices architecture that can scale on-demand...
◦ Deploy in cloud-native environments or as an on-prem, appliance-based solution

SCALABLE, PERFORMANT

◦ Real-time and continuous
◦ Extremely lightweight- designed for minimum resource utilization
◦ Scalable, fast and efficient - delivering predictable, deterministic performance

HIGH-RESOLUTION

◦ Lossless, reliable and continuous inspection of data flows and infrastructure. Capture, filter, and analyze traffic of interest, resulting in situational awareness, simplified operations and fewer false positives
◦ Deep kernel-level visibility and the ability to dynamically extract and generate telemetry
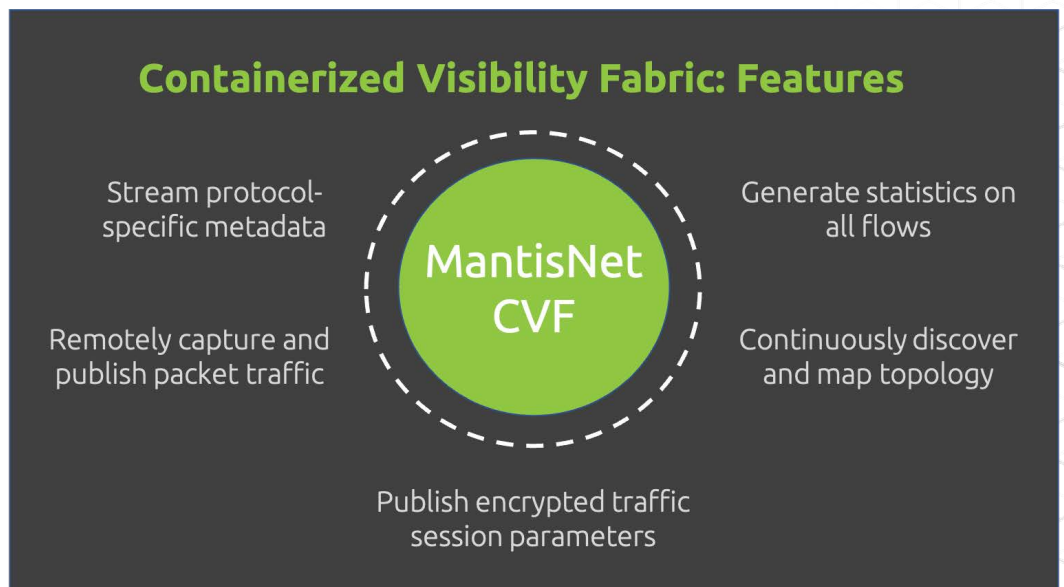
FLEXIBLE, EXTENSIBLE

◦ Sensor agents publish telemetry, PCAP and metadata formats (JSON, Avro, Protobuf) into distributed message buses (NATS, Kafka, etc.) optimized for streaming analytic workflows or data-at-rest (block, file, or object) storage.
◦ Additional plug-ins and worker applications can be used to provide a wide-variety of functions; indexing and correlation for enrichment and time-series analysis

PRODUCT OVERVIEW

The MantisNet Containerized Visibility Fabric (CVF) is a cloud-native visibility platform that handles the challenges of gaining insight into virtual/cloud resources. Leveraging a lightweight microservices architecture, the CVF can be deployed quickly (and at-scale) to capture packets, generate metadata and more.

With the MantisNet CVF, network professionals can gain unprecedented insight into virtual resources- to include continuous topology discovery, protocol specific metadata generation, flow metric reporting, and more.

Containerized Visibility Fabric: Features

Stream protocol-specific metadata

Remotely capture and publish packet traffic

MantisNet CVF

Generate statistics on all flows

Continuously discover and map topology

Publish encrypted traffic session parameters
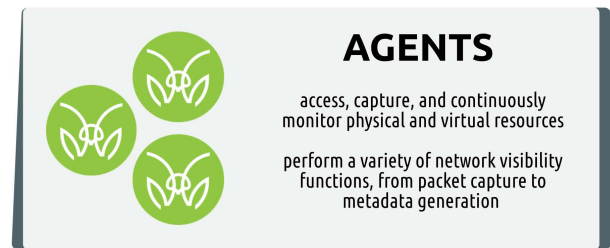
PRODUCT DESCRIPTION

The MantisNet CVF consists of a cloud-native microservices-based compute engine that is able to perform a variety of complex functions anywhere in the infrastructure. The CVF application is a lightweight piece of code that communicates safely with the bare-metal operating system, deployed as a container in cloud-native environments. The CVF application is typically managed as a Daemonset with a helm chart within the Kubernetes ecosystem to ensure scalability, consistency, and maintainability.

The power of CVF lies in the fact that it allows for deep observability and control: from individual machines (bare-metal OS) to across an entire cloud infrastructure; core-to-edge. Furthermore, the CVF architecture is flexible, extensible, and open: CVF compute engines can be updated on-the-fly, new functional capabilities can be added with plug-ins, and communications are provided via an open standards distributed messaging queue / publish-subscribe architecture.

HOW IT WORKS

The CVF is comprised of two main components, "agent(s)" and the "controller":

Agents are lightweight network sensors that can accomplish a variety of network visibility functions- these functions are referred to as "tasks". Agents also include native tapping capabilities for auto-discovery of all containers, infrastructure, and interfaces.

AGENTS

access, capture, and continuously monitor physical and virtual resources

perform a variety of network visibility functions, from packet capture to metadata generation

The **controller** is a container that manages multiple agents within an environment- providing configuration and provisioning control, as well as instructing the agents what their current "directive" is. A directive is a combination of one or more tasks that are to be performed by the agent.
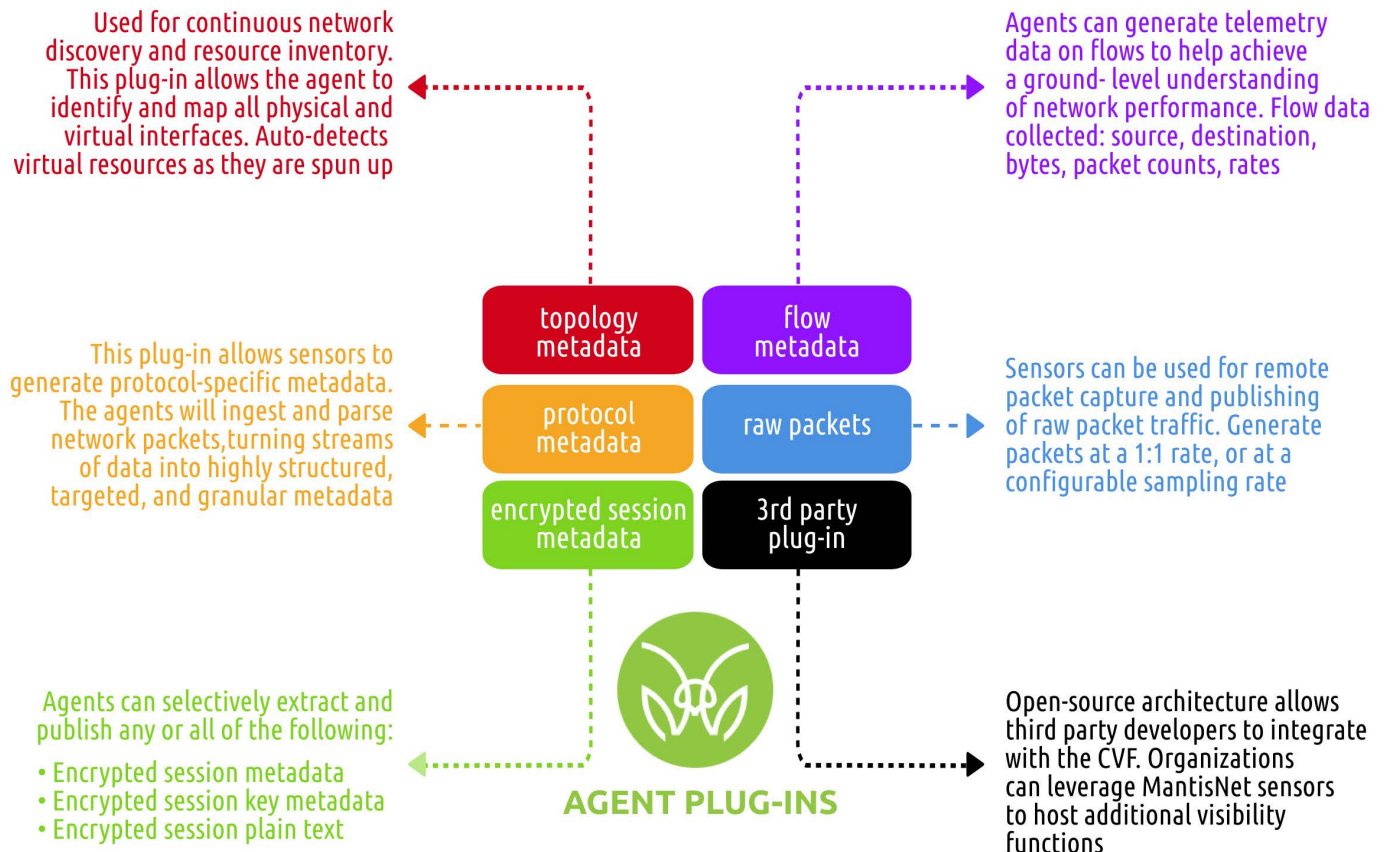
CONTROLLER

controls agents in the environment- provisioning, configuration, hit-less upgrades, etc.

dynamically controls which tasks/functions each agent is performing

LEVERAGING MESSAGING QUEUES
(agent and controller interaction)

The controller communicates to the agents in the environment via an open-source messaging queue, such as NATS or Kafka. A "command and control" topic is used within the queue to be the touch point between the controller and the agents- the controller acting as the publisher to the C2 topic, while the agents act as subscribers to that same C2 topic. This design allows for instant updating of the agents, when desired changes need to be implemented (for example: switching a particular agent from executing the task "capture packets" to now "capture packets" and "generate DNS metadata"). The design also allows for a smooth interface for updating agents in the field, and also enables the controller to issue constant "health checks" to the agents to ensure everything is online and operating smoothly. Finally, leveraging the messaging queue allows for an upgrade strategy that does not require any maintenance windows that end users need to coordinate.

While the messaging queue is used for command and control of the CVF, it is also used as the egress point for all data coming out of the CVF agents. This strategy ensures that there is a clean interface between the MantisNet CVF and analytic/monitoring tools- while also leveraging an interface that enables true streaming or event driven analytics and platforms, as well as integration with batch-mode focused data ingestion applications.
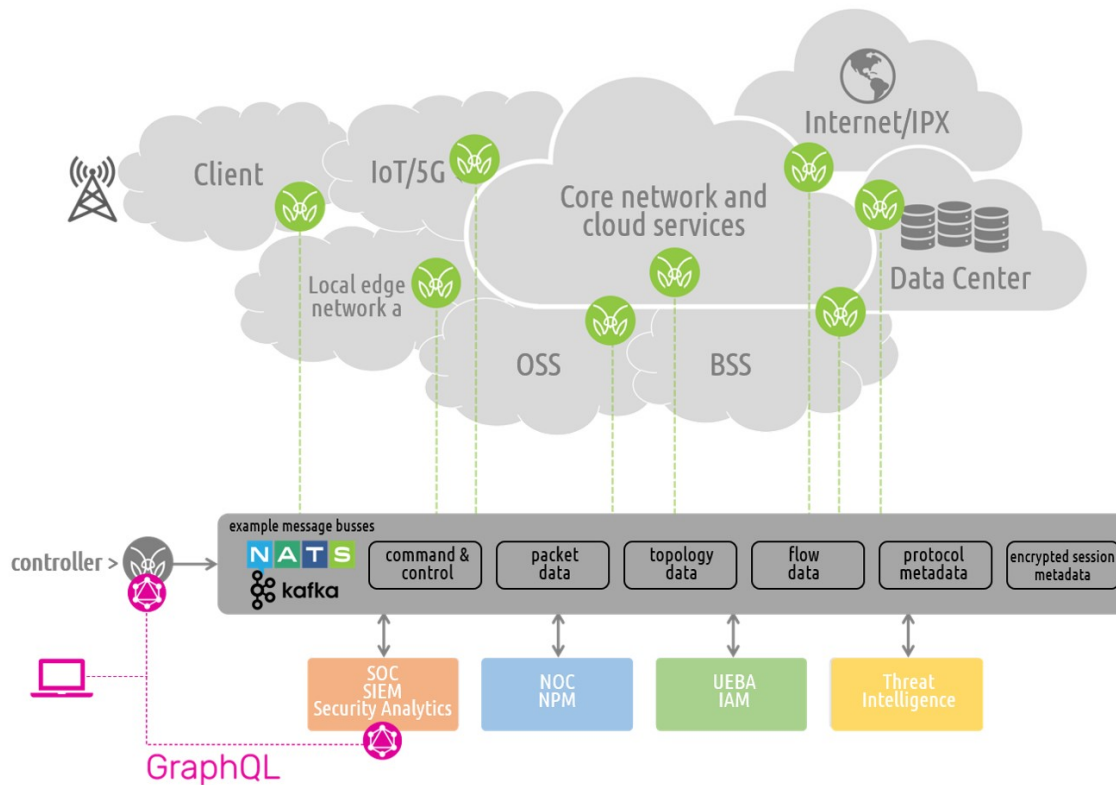
MantisNet

"PLUG-IN" DESIGN

Another key design approach of the MantisNet CVF is that the agents are multi-faceted- they have been developed to do more than just "capture packets". As mentioned previously, these agents are capable of performing a variety of network visibility "functions", or "tasks", to deliver unparalleled insights. At the most basic level, the CVF agent acts as a powerful network sensor that can accomplish a variety of functions, in any combination, to deliver the visibility that is needed where the agent resides. These functions are simply modular plug-ins that can be used by the sensor in the field. The plug-in construct is also based on a completely open-source framework- allowing for others to develop their own plug-ins to be used within the MantisNet CVF. There are additional plug-ins in various development stages at MantisNet.

Used for continuous network discovery and resource inventory. This plug-in allows the agent to identify and map all physical and virtual interfaces. Auto-detects virtual resources as they are spun up

Agents can generate telemetry data on flows to help achieve a ground- level understanding of network performance. Flow data collected: source, destination, bytes, packet counts, rates

This plug-in allows sensors to generate protocol-specific metadata. The agents will ingest and parse network packets,turning streams of data into highly structured, targeted, and granular metadata

Sensors can be used for remote packet capture and publishing of raw packet traffic. Generate packets at a 1:1 rate, or at a configurable sampling rate

topology metadata	flow metadata
protocol metadata	raw packets
encrypted session metadata	3rd party plug-in

Agents can selectively extract and publish any or all of the following:

• Encrypted session metadata
• Encrypted session key metadata
• Encrypted session plain text

Open-source architecture allows third party developers to integrate with the CVF. Organizations can leverage MantisNet sensors to host additional visibility functions

AGENT PLUG-INS

MantisNet

Containerized Visibility Fabric: redefining network visibility

The MantisNet Containerized Visibility Fabric is a dynamic, cloud-native approach to data visibility. Given the complex challenges of container and virtual environments, CVF agents have been designed to be performant, lightweight, and flexible. These sensors provide a framework to perform a multitude of functions/tasks (plug-ins) in order to provide continuous, real-time visibility directly to the various analytic workflows, management services, and orchestration services. The MantisNet CVF seamlessly integrates these capabilities into a holistic, cloud-native, network visibility strategy.

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.

MantisNet combines end-to-end visibility, monitoring and control (from L2 to L7) with the ability to perform real-time processing and remediation to detect and respond to potential operational issues, security threats, fraud, and malicious activities with advanced interfaces and machine-to-machine controls. Our solutions are deployed at leading telecom, service providers, NEM labs and government installations. We work to make network intelligence actionable for a broad range of DevOps, network and application performance testing, streaming analytics, and cyber security applications.

For more information, visit www.MantisNet.com

MantisNet

11160 C1 SOUTH LAKES DRIVE, SUITE 190 RESTON, VA 20191

571.306.1234
INFO@MANTISNET.COM