Cloud Native Traffic / Packet Capture

Capture full packets and cloud traffic when and where they are needed

WHY THIS MATTERS

The challenges with cloud-native network monitoring:

- Topology (virtual and physical) is hidden
- Interfaces (network namespace) are hidden
- Data flows (packets, octets and protocols) are hidden

The MantisNet CVF architecture is an innovative combination of network sensor agents, and cloud-native technologies that efficiently processes and produces all the information necessary for real-time monitoring needs:

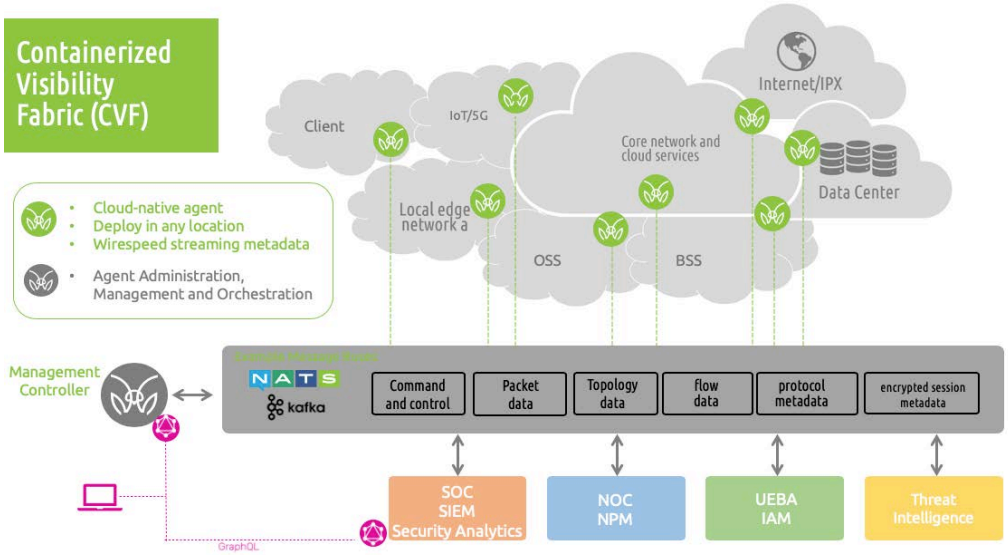
- Application Performance Monitoring (APM)
- Network Performance Monitoring (NPM)
- Continuous Discovery/ Inventory
- Security Assurance

DETERMINISTIC

The CVF processing engines (sensor agents) are lightweight and fast. Deployed as a daemon-set or container, they provide deep visibility into all the interfaces and functions at the machine level enabling the filtering and publication of specific traffic so as to be extremely efficient, scalable and performant.

Containerized Visibility Fabric (CVF) - Cloud Native Traffic / Packet Capture

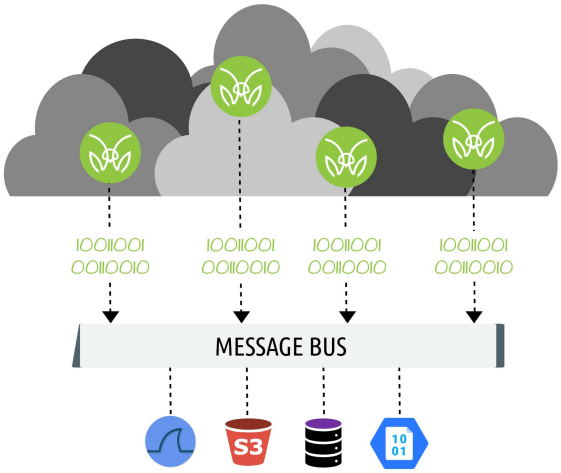
The MantisNet CVF performs a variety of complex observability and processing functions, anywhere in the infrastructure. This cloud-native, composable solution goes beyond simply capturing network traffic to publishing new forms of enhanced metadata that enables far more detailed observability than has been previously possible. Additionally, CVF metadata is published continuously and in real-time, supporting critical correlation, attribution and follow-on processing operations. Learn more about the CVF at MantisNet.com



Traffic / Packet Capture

CVF agents generate granular metadata for observability at speed and scale- providing detailed monitoring of cloud-native, serverless, resources, topology, flow, encrypted session communications, and specific protocols. In addition to metadata, CVF agents also have the ability to capture network traffic anywhere they are deployed, regardless of namespace. Full traffic capture is a CVF plug-in that is extremely useful for forensic purposes, or for troubleshooting complex network issues.

Packet Capture CVF Plug-in



Programmatic, on demand

The key to CVF packet capture is that it is done programmatically - simply publish a directive to turn on packet capture, and instantly start capturing packets from any CVF sensor agent in the environment. The agent will capture all traffic- regardless of namespace - if the information is traversing physical links or moving between microservices. The capture function can easily be toggled on/off, and can be captured at a 1:1 rate, or via a configurable sampling ratio.

Benefits of CVF Packet Capture

Cloud-native

- Flexible architecture that can be deployed anywhere and scale, on-demand, with cloud-native infrastructure

Flexible, Intelligent and Extensible

- Sensor agents publish telemetry, PCAP and metadata formats (JSON, Avro, Protobuf) into distributed message buses (NATS, Kafka) optimized for streaming analytic workflows or data-at-rest (block, file, or object) storage
- Capable of identifying common crypto libraries (OpenSSL, TLS, GNU)
- 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 providing deeper contextual and situational awareness.

High-resolution, precise and accurate

- 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 machine-level visibility and the ability to dynamically extract and generate telemetry

Efficient, highly scalable and performant

- Real-time and continuous
- Extremely lightweight, in-memory, microservices-based architecture- designed for minimal resource utilization
- Scalable, fast and efficient - delivering predictable, deterministic performance

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