Visibility for Encrypted Session Traffic

Identify, access and extract encrypted session metadata

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

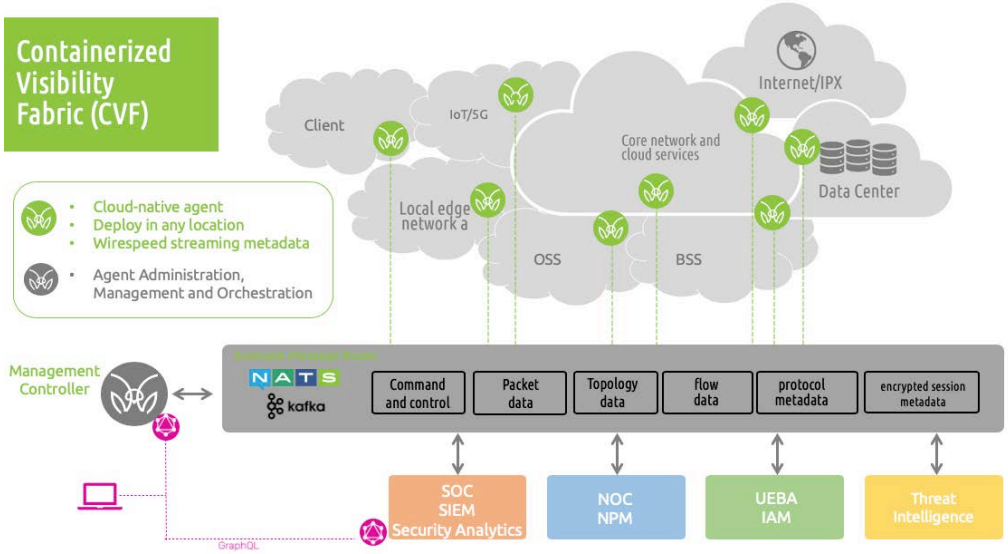
The MantisNet CVF architecture is an innovative combination of network sensor agents, and cloud-native technologies that efficiently produces all the information necessary to monitor the cryptographic status and health of your infrastructure as well as feed follow-on analytics solutions for decryption management and forensic analysis.

DETERMINISTIC

The CVF processing engines are lightweight and fast. They provide deep machine-level visibility into the underlying functions to enable the identification and extraction of specific cryptographic controls and other related information so as to be extremely efficient, scalable and performant.

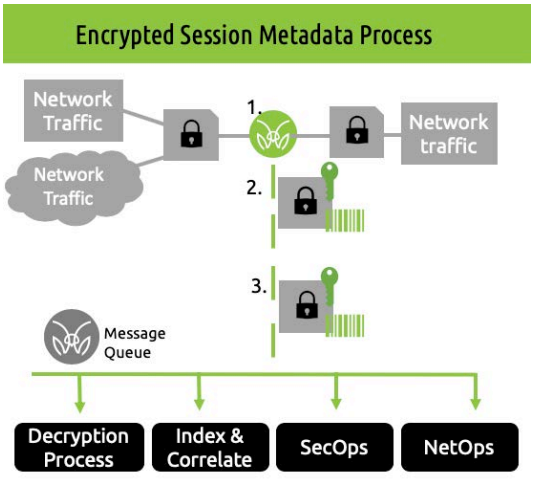
Containerized Visibility Fabric (CVF) - Encrypted Session Visibility

The MantisNet CVF performs a variety of complex functions for monitoring cryptographic controls, anywhere in the infrastructure. This cloud-native, composable solution goes beyond capturing packets to publishing new forms of encrypted session metadata to enable cryptographic monitoring and follow-on processing. Learn more about the CVF at MantisNet.com



Encryption Session Visibility

CVF agents provide the ability to identify, extract and publish all the encrypted session parameters and data that providers need to support all their cryptographic visibility, management and security demands. Regardless if it is to identify, monitor or quantify encrypted exchanges or to ensure the reliability and stability of systems, to differentiate legitimate cryptographic exchanges from potentially malicious unknown, unreliable or questionable traffic. The CVF architecture publishes all the metadata and traffic of interest needed to support analytics, decryption, storage and forensic analysis services.



Encrypted Session Processing

1. Agents monitor, identify, and access encrypted session controls and associated traffic

2. Agents selectively extract and publish any or all of the following:
   - Encrypted session metadata
   - Encrypted session key metadata
   - Encrypted session plain text

3. Follow on processing
The specific encrypted session controls and/or associated traffic of interest are used by subscriber programs to support and/or enrich a broad range of event correlation, decryption management, topology mapping, storage, or forensic analytics applications.

Benefits of CVF Encrypted Session Metadata Processing

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, NSS)
- 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