Network and IT Protocols Support

MantisNet Protocol Decoders enable real-time visibility and management for cybersecurity and network operations

INSIGHTFUL

- Complete access to, and management of, network traffic for engineering and cybersecurity needs
- Real-time, network monitoring and visibility for virtual and cloud environments
- Protocol decoding and parsing for network layers 2 – 7
- Convert unstructured network data into high-resolution metadata formatted to open-standard key value pairs

EFFICIENT

- Programmable, in-memory, processing technology
- Supports RegEx and entropy transcoders
- Inter-operable, easily deployed and manageable via existing analytic toolsets via a rich set of RESTful APIs

The increasing complexity of infrastructure (Hybrid IT & Cloud) and operating modalities (micro-services, SDN, serverless, and perimeter-less networks) means that ubiquitous, continuous, real-time visibility of network communications is more important than ever.

MantisNet protocol decoders provide visibility, data classification, inspection, and application-aware processing power across the enterprise: from the core to the edge, from the cloud to the network end-point. MantisNet decoders enable pay-as-you go, protocol services, and are flexible with the Programmable Packet Engine (PPE) cloud-native and micro-services-based metadata publishing engines.

Why MantisNet Protocol Decoders

The decoders provide modular support for any protocol, traffic type or network payload, continuously, in real-time. They can produce unsampled, lossless streaming metadata as well as NetFlow and IPFIX telemetry for follow-on applications and/or streaming analytic workflows.

The resulting metadata telemetry can be used with most existing tools or as a source to enhance, transform, and augment data streams or batch processing, facilitating deep analytics, wire-speed traffic shaping and effecting network behavioral changes.

CORE PROTOCOLS SUPPORTED

CPRI/eCPRI Common Public Radio Interface
DHCP Dynamic Host Configuration Protocol
DNP3 Distributed Network Protocol
DNS Domain Name System
FTP File Transfer Protocol
GTP GPRS Tunneling Protocol
HTTP Hypertext Transfer Protocol
HTTPS Hypertext Transfer Protocol Secure
ICMP Internet Control Message Protocol
IPFIX Internet Protocol Flow Information Export
LDAP Lightweight Director Access Protocol
LLDP Link Layer Discovery Protocol
MODBUS
MPLS Multiprotocol Label Switching
NetFlow
NGAP Next Generation Application Protocol
PFCP Packet Forwarding Control Protocol
SCTP Stream Control Transmission Protocol
SSL Secure Sockets Layer
TCP Transmission Control Protocol
TLS Transport Layer Security
UDP User Datagram Protocol

SUPPORT FOR LEGACY AND EMERGING PROTOCOLS

ActiveMQ Apache Active Message Queuing
ARP/RARP Address Resolution Protocol
BGP Boarder Gateway Protocol
CIFS Common Internet File System
Diameter
ESP Encapsulating Security Payload
HL7 Health Level 7
IMAP Internet Message Access Protocol
Kerberos
MSRPC Microsoft Remote Procedure Call
NFS Network File System
NTP Network Time Protocol
RADIUS Remote Authentication Dial-In User Service
RIP Routing Information Protocol
RTCP XP Real-time Control Protocol Extended Reports
RTP Real-time Transport Protocol
SIP Session Initiation Protocol
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
Telnet Teletype Network Protocol

WHAT IS A PROTOCOL DECODER?

A protocol decoder is a plug-in at the heart of the Programmable Packet Engine (PPE). It consists of a set of containerized P4 driven software applications that extracts, filters and transcodes unstructured network traffic and communication protocols into structured metadata, for the ultimate situational awareness and optimal operational visibility at speed and scale.

The key enabling action is that network traffic is continuously filtered and transcoded into canonical tuples, that is, key:value pairs (in stream processing terms). By converting specific traffic types into a stream of tuples, a multitude of existing monitoring and analytics frameworks can be applied to complex networks converting network traffic into actionable insight. Protocol decoder delivers the streaming metadata for consumption as JSON, Kafka (other formats available upon request).

APPLY THE VALUE OF THE EXTRACTED NETWORK PROTOCOL DATA FOR:

- Application and Network Performance Monitoring (APM and NPM)
- Continuous monitoring, traffic analysis, classification and event correlation
- Data Plane Engineering
- De-encapsulation / Re-encapsulation
- Detect command & control servers, rogue /hijacked servers / DDoS and MITM attacks
- Detect unauthorized access (ATO), and surreptitious file transfers (DLP)
- GRC Compliance Monitoring
- Next Generation Firewalls (NGF)
- Network Detection and Response (NDR)
- Network Monitoring & Lawful Intercept
- Network Telemetry Generation
- Network Traffic Analysis (NTA)
- Policy Control & Charging (PCC)
- Quality of Experience (QoE)
- Security and Anomaly Detection
- Security Incident and Event Monitoring (SIEM) analytics
- Threat Hunting
- Understand the cryptographic health of systems
- User and Entity Behavioral Analytics (UEBA)

BENEFITS:

- High-fidelity, deep resolution into any virtual/physical network traffic without needing dedicated monitoring infrastructure
- Supports a variety of legacy and emerging protocols and metadata formats for continuous, rapid ingest into analytic tools
- Can be deployed anywhere; on-premises, or cloud infrastructure
- Interfaces with a broad range of stream processing architectures/ pipelines and management applications such as kafka, websocket, http, mqtt, s3

ABOUT MANTISNET

MantisNet develops Software Defined Network (SDN) and Network Function Virtualization (NFV) network intelligence solutions that provide businesses and governments real-time network monitoring solutions, for 100G speeds and beyond. MantisNet's solutions better enable network teams to monitor, manage and engineer the increase in network traffic flows they're experiencing compared to the preceding generation of packet brokers, firewalls, load balancers and event management solutions.

MantisNet combines end-to-end visibility, wire-speed network monitoring and protocol analysis (from L2 to L7) with the ability to perform real-time traffic engineering and remediation against operational issues, security threats, fraud, and malicious activities, either manually or autonomously. Our solutions are deployed at leading telecom, service providers, NEM labs and government sites. 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