Datasheet

Virtual Programmable Packet Engine (vPPE)

Enable actionable network analytics

MantisNet

The Challenge

Understanding network behavior in real-time, between physical and virtual environments, is a challenge many organizations face. The move towards continuous monitoring and remediation can only be fully realized with a solution that can provide real-time, actionable, insights to your network traffic. Most tools available today use only asynchronous information such as data-at-rest (logs or file-based information) or data that has been previously captured to attempt to conduct actionable analytics on network traffic which only provides intelligence after an event has occurred, if it is detected at all. MantisNet's Programmable Packet Engine (PPE) takes the next step in continuously decoding, extracting and converting unstructured network data into actionable intelligence allowing you to better protect your information and network assets in real-time.

The Solution

MantisNet's virtual PPE (vPPE), for the cloud and virtualized or container-based use cases, builds on our in-memory and stream processing capabilities for physical environments and advances the evolution of network monitoring. vPPE enables the deployment of network sensors and processes elements in the virtual environment that DevOps and SecOps teams need to understand the characteristics and behavior of data to make decisions in real time.

The MantisNet vPPE sensor technology helps organizations keep pace with accelerating analytical demands and deliver timely results that facilitate Time-To-Value (TTV) decisions.

The vPPE:

- Provides real-time monitoring in the network when and where it is needed with intelligence to decode and parse any protocol and interrogate any payload type
- Utilizes protocol decoders to monitor, filter and generate specific metadata, that can be inserted anywhere in the cloud or physical networks
- Handles all network underlays, overlays and encapsulations
- Scales from lower bandwith at individual nodes to enterprise-wide, cloud infrastructure and hybrid architectures, up to the fastest +100G core transports
- Leverages containerization and orchestration tools (Docker, Kubernetes etc.) for rapid and flexible deployment
- Publishes streaming metadata, using well-known serializations, and leveraging existing data science tools
- Is simple to use, easily deployed, inter-operable with existing analytic toolsets and be provisioned and configured with a rich set of well understood and commonly used API's.

MantisNet vPPE can be deployed in today's business environments.

The vPPE Difference

In-memory compute engine

Provides programmable metadata publishing engine for streaming analytic workflows

The MantisNet vPPE sensor is an in-memory, programmable decoder and metadata publishing engine that is the foundation for enabling streaming analytic workflows; providing the ability to programmatically search for, and extract detailed information about network traffic patterns, payloads, protocols and behaviors and deliver information in the form of highly efficient serialized metadata at wire-speed to data analytics platforms. It is THE wire-speed data source for network situational awareness, visibility and control.

Cloud-Ready Containers

Enables real-time monitoring of cloud/ virtualized environment traffic

The vPPE provides cloud-based, or virtualized environments a containerized service that ingests native traffic and generates serialized metadata into streaming analytic pipelines. The vPPE platform is designed with the key enabling idea/

abstraction that network traffic and underlying protocol contents can be represented, in data stream processing terms, as canonical tuples; key:value pairs (metadata).

High-Resolution Network Insight

THE data source for network situational awareness, visibility, and control

The vPPE generates high-resolution detail of protocols, traffic types and payloads and is designed to be used with time tested, descriptive and predictive analytic workflows. The resulting serialized metadata can be used with existing data science 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.

Functionality

Inputs

- The vPPE supports a broad variety of common protocol decoders: some examples are GTP, DNS, DHCP, HTTP, TLS. Optionally, payload entropy, time series, and regex. decoders can convert packet traffic into protocol-specific metadata for continuous stream publishing
- Protocols are fully decoded, supporting programmatic parsing of any/all fields for extraction and follow-on processing
- Supports all manner of network underlays, overlays and encapsulations out-of-the-box
- Supports dynamic field reconfiguration; the parser can be updated to reverse engineer unknown, previously non-parseable headers/protocols allowing for changes as to how network packets are parsed and processed at runtime

Outputs

- Converts packet traffic into serialized streams (json, avro, msgpack, protobuf…)
- Schema driven; extracted metadata fields are configurable and can be programmed at runtime
- Supports native ingest into a wide variety of streaming analytic frameworks and easily interfaces with a wide variety of in-memory systems; both open source platforms such as NoSQL (MongoDB, Neo4J, RethinkDB, Elastic), SQL (PrestoDB, VoltDB, PipelineDB), Storm, and Flink, as well as to commercial analytics platforms such as Splunk, SAS (ESP), Software AG (APAMA) and SAP (HANA) and TIBCO
- Interfaces with a broad range of stream processing architectures/ pipelines and management applications such as kafka, websocket, http, mqtt, NATS, as well as kinesis firehose (aws) — future [pub/sub (google cloud), stream

Management

- Employ's a dynamic and open management architecture; YANG model driven supporting open APIs and RESTful, NETCONF, and CLI interfaces.

Security

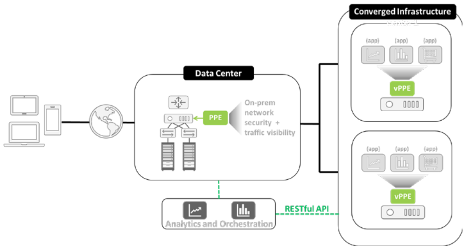
- Designed with security and compliance in mind: Compliance (HIPAA, PCI-DSS, FISMA, DFARS, GDPR, ISO 27001:2013 and GPG-13) is a non-issue as event messages are cryptographically hashed to retain data lineage and there is no data persistence or archival functions: PII/PHI data is never at rest.

Specifications

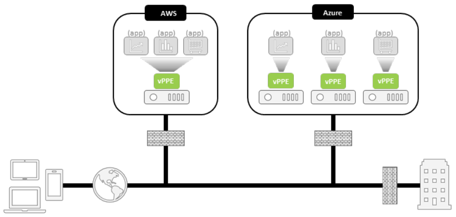
Available in a range of performance options; the vPPE can be sized and configured to suit the demands of the specific protocol decoders and required throughput. Maximum performance is based on throughput and capacity of available resources (network bandwidth, number of CPU cores/memory) allocated as well as the resource demands, of the specific licensed protocol decoders.

Deployment Options

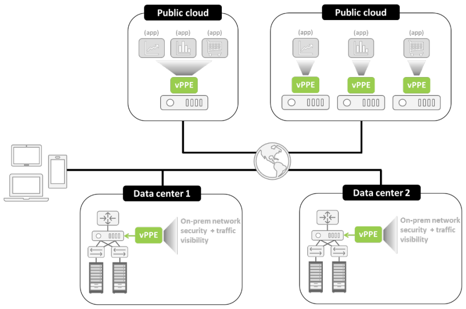
Private Cloud



Public Cloud



Hybrid Cloud



Simplified licensing

MantisNet licensing can scale with your network monitoring and protocol decoder use.

Select PPE or vPPE and then number of decoders.

MantisNet software licensing provide predictable lifecycle upgrades by offering support for up to two major software releases*

Try the vPPE with a free evaluation license