ENEA

Customer Case Study

MSSP Uses Qosmos Probe to Improve Service Levels

Stronger, cost-effective managed security with DPI-based Network Traffic Analysis (NTA)

Overview

- A European MSSP required a high-performance DPI sensor to provide traffic visibility inside a custom-built NTA solution that would go beyond signature-based threat detection
- The DPI sensor must integrate with open source components and other ecosystem applications
- The DPI sensor must be able to passively capture packets at high throughput, detect applications, parse protocols, and extract traffic metadata, used to contextualize alerts.

Benefits of Qosmos Probe

- Enables MSSPs to increase differentiation and raise the quality of security services provided to their customers:
  - Enrich existing detection methods to enable discovery of attacks missed by other tools (unknown signatures)
  - Improve accuracy of detection and speed investigation of alerts through full visibility of network traffic on critical parts of the internal network
  - Increase traffic data retention period to months instead of days
  - Enrich alerts with metadata to make forensics easier and more efficient
  - Technology already operational in the most advanced cyber defense systems
- Lower SOC total cost of ownership through improved traffic visibility, enriched alert information, fewer false positives and faster investigations.

The Customer

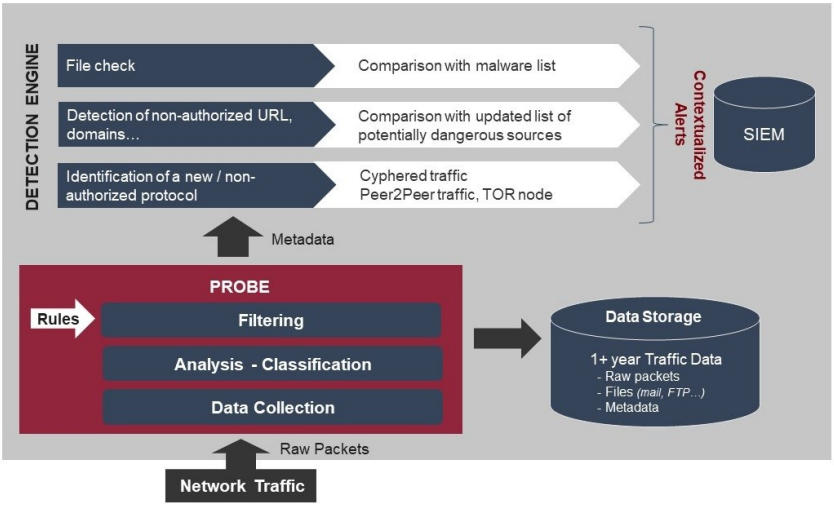
The customer is a European MSSP who delivers managed security services (firewall, IDS, etc.) to large enterprises with critical infrastructures, (utilities, banks,…) and to small and medium businesses (SMBs). The services are delivered remotely from a central Security Operations Center (SOC).

The Challenge

The MSSP customer wanted to increase accuracy and speed of its threat detection to improve service quality and differentiation vs. competitors. To do this, the MSSP decided to assemble a network traffic analysis (NTA) solution that would enable its security operations to go beyond signature-based detection and identify suspicious network traffic that other tools had missed. It would also enable the customer to offer a top-of-the-line service to SMB clients without jeopardizing profitability.

The effectiveness of an NTA solution is totally dependent on the traffic information that is fed into it. The customer combined open source applications with a commercial DPI sensor providing detailed traffic visibility. The customer was looking for a proven, advanced DPI sensor that would be easy to integrate into client infrastructures and could deliver granular traffic visibility up to layer 7. Extraction of traffic metadata was a key requirement to improve alerting, reduce false positives and speed problem resolution.

Full maintenance and support with regular software updates was also important to ensure service quality at all times.



The Solution

The MSSP chose the Qosmos Probe, an advanced DPI sensor with proven traffic recognition technologies, including encrypted traffic. The sensor provides traffic visibility up to layer 7 and can extract metadata for a more detailed analysis.

Provided as a software component, the Qosmos Probe was delivered with native interfaces to open source, companion cybersecurity solutions. The customer chose, for example, to activate the API to Fingerbank to enable device identification.

The approach combining open source applications with the Qosmos Probe provided a flexible NTA solution, optimized deployment and low operational costs.

Ensuring the Highest Level of Traffic Visibility

The value of Qosmos technology resides in the quality of the information extracted from the traffic. The Qosmos Probe is an advanced DPI sensor that passively captures packets at high throughput (up to 20 Gbps per sensor), detecting applications, parsing protocols, and extracting traffic metadata. Traffic metadata is used to contextualize alerts, reducing the number of false positives, and allowing analysts to carry out more efficient investigations, resulting in faster remediation.

The Qosmos Probe is deployed as a virtual agent on every node requiring security monitoring. A centralized management tool enables flexible administration and clustering.

Strengthening Internal Resources

Now operating inside the customer's NTA solution, the Qosmos Probe:

- Provides granular visibility of key protocols that the MSSP wanted to focus on, including SSL, HTTP, DNS, SMTP, SMB, LDAP
- Enriches protocol information with metadata (server_name, common_name, version, header name, header value, method…)
- Reduces size of forensic data by up to 150x compared to full packet capture (FPC)
- Enriches the IDS/IPS solution with metadata, enabling detection of suspicious network traffic that other security tools might have missed

Cost-effective Ecosystem Approach

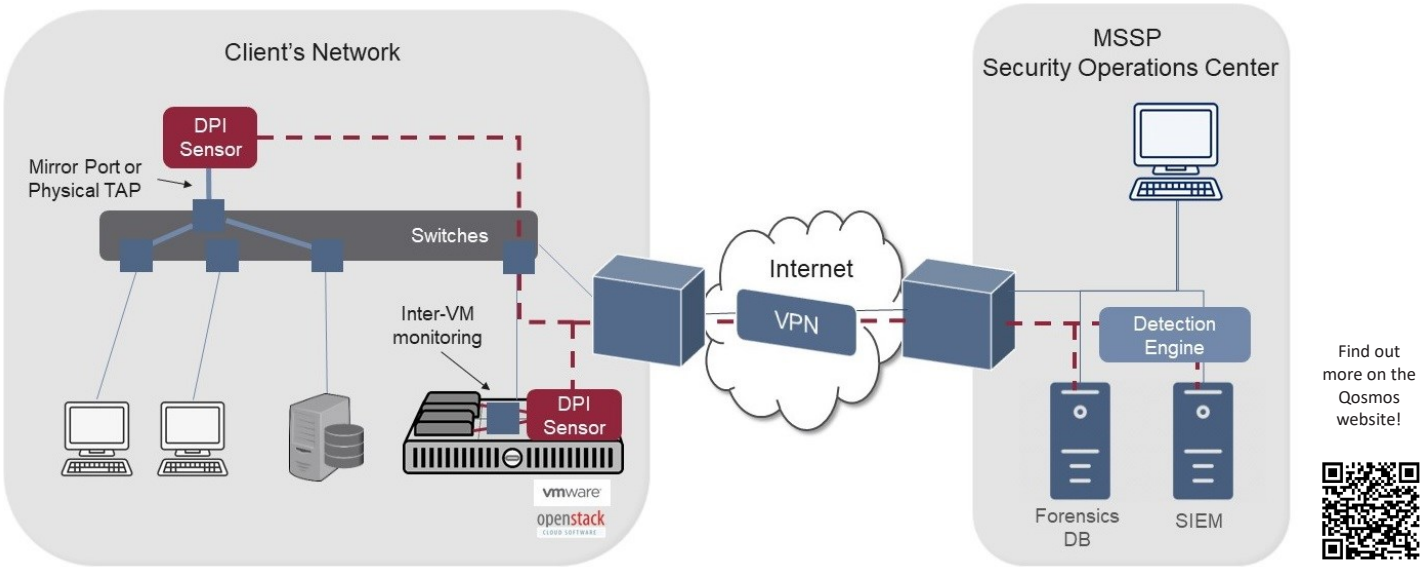
- The Qosmos Probe was fully customized to the customer's specific needs, connecting with the other NTA components, including community-based and open source cybersecurity software
- The Qosmos Probe integrated easily into the existing ecosystem that included device fingerprinting, URL reputation, phishing detection, malware detection, IDS engine…
- The customer also added a selection of optional Qosmos modules

The MSSP customer was able to benefit from cost-effective open source applications while ensuring the quality and reliability of the traffic information used for its threat detection services, whether for critical infrastructures or SMB top-of-the-line services.

The Benefits

The quality of traffic analysis provided by the Qosmos Probe enables you to create a superior NTA solution without compromising the profitability of your services. Used in addition to existing detection tools, you can significantly improve the protection of your enterprise client networks through faster and more accurate threat detection, with fewer false positives and better remediation.

As a fully flexible and customizable software component, the Qosmos Probe allows you to build your own custom detection engine according to your specific operational and system requirements. Standard interfaces facilitate integration into the NTA solution and the existing ecosystem. Installation is transparent - no access rights are required and the probe operates independently from existing applications.



Find out more on the Qosmos website!

Enea develops network software for the connected society. We provide solutions for mobile traffic optimization, subscriber data management, network virtualization, traffic classification, embedded operating systems, and professional services. Solution vendors, systems integrators, and service providers use Enea to create new world-leading networking products and services. More than 3 billion people around the globe already rely on Enea technologies in their daily lives. For more information: www.enea.com