napatech

Case study: #1 social network provider steps up security and sees million-scale savings

Industry pain points

Identifying malicious activity on the network requires complete visibility at all times. Overlooking even the slightest bit of evidence can deem an entire investigation worthless and provide hackers the needed loopholes to continue to exploit and drain the network of business-critical information.

To gain the required visibility, Incident Response Teams therefore need the ability to capture all data packets and retrieve selected packets for further investigation after the fact. But scaling packet capture infrastructure to meet corporate demands offers its own set of challenges, e.g.:

- Physical space limitations at datacenter level
- Insufficient retention capabilities
- Need for multiple hosts to load balance the captured traffic
- Prohibitive cost and complexity of proprietary solutions

Client challenges

A leading social network provider was facing these challenges, as they needed to capture all data at 20G in real time and retain the data for up to 90 days for in-depth security forensics – a task which their existing capture appliances had failed to deliver.

Alternative market solutions were pricey, proprietary and excessively analytics heavy – causing undesired burdens and restraints. The company was already deploying Bro and Suricata for security forensics and wanted to avoid the cost and hassle of adding proprietary analytics. What they needed was a stand-alone high-performance PCAP solution focusing only on capture and recording.

A decisive factor for the company was that they could continue to write data to their existing large-scale cloud-distributed storage solution, based on GlusterFS – rather than invest in new and costly storage.

Solution

The company's in-house security team therefore decided to develop their own scalable, cost-effective and multi-petabyte solution based on open configurable computing.

Challenge

A leading social network provider needed to capture and retain 20G data for up to 90 days for security forensics. But proprietary capture solutions were cost-prohibitive and excessively analytics heavy.

Solution

The company built their own 7.5 PB storage solution based on open configurable computing. To ensure 100% packet capture and 90-day retention at 20G, they entered a co-creation alliance with Napatech – and the Pandion capture-to-disk technology was customized and integrated.

Benefits

Working with Napatech, the company gained:

- Million-scale savings in proprietary storage costs
- A tailored PCAP solution focusing only on packet capture and recording
- Seamless compatibility with existing cloud storage

Key objectives were:

- Flexible storage size
- Network accessible storage
- High throughput
- PCAP as a service

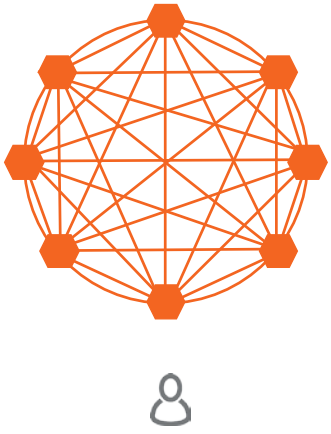
Dedicated co-creation

The company needed a partner to deliver a high-performance, stand-alone PCAP solution. And with over a decade of industry-proven experience in accelerating PCAP applications, Napatech was the preferred partner. The company entered a co-creation program with Napatech to customize the Pandion capture-to-disk technology to their specific needs. The solution was then integrated at the back-end of their existing cloud storage, ensuring 100% capture of all packets at 20G and 90-day retention guaranteed.

Benefits

With the Pandion packet capture technology, the company would now be able to investigate any incidents flagged by Bro or Suricata; just a simple query in Pandion and they could promptly pull the relevant packets – even packets dating back months.

Pandion's powerful federated search capabilities made it possible to access all traffic from any tap point in the network and monitor and query the cloud from any single node.



Federated search across multiple tap points with just a single query.

Added benefits included:

Massive savings

By using Napatech, the company built a 7.5 PB storage solution, saving millions in proprietary storage costs. The cost of the entire solution equaled just the support cost from a competitive capture vendor.

Stand-alone network recording

By focusing only on capturing and storing the data, Napatech afforded the company a high-performance building block and the freedom to pick and choose their analytics.

Seamless integration

Napatech developed a number of bespoke features to ensure that Pandion could be seamlessly integrated with the existing cloud storage solution.

Napatech Pandion

In a time of data overload, relevance is everything. The Pandion network recorder enables you to seize all traffic in real time and retrieve only the relevant data on demand.

Napatech Pandion is based on Napatech SmartNICs available in a range of Ethernet interface options, with configurable storage and Napatech Pandion software.

Pandion builds on more than a decade of industry-proven Napatech FPGA technology and delivers 100% capture and write to disk for leading security analytics and compliance applications.

Find out more at:
www.napatech.com/products/napatech-pandion

For additional details about the case study, visit:
www.napatech.com/fb-flocon2017

NORTH AMERICA
Napatech inc.
Boston, Massachusetts
Los Altos, California
Washington D.C.

Tel. +1 888 318 8288

info@napatech.com
www.napatech.com

EUROPE, MIDDLE EAST AND AFRICA
Napatech A/S
Copenhagen, Denmark

Tel. +45 4596 1500

info@napatech.com
www.napatech.com

APAC
Napatech China/South Asia
Taipei City, Taiwan
Tel. +886 2 28164533 Ext. 319

Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374

ntapacsales@napatech.com
www.napatech.com