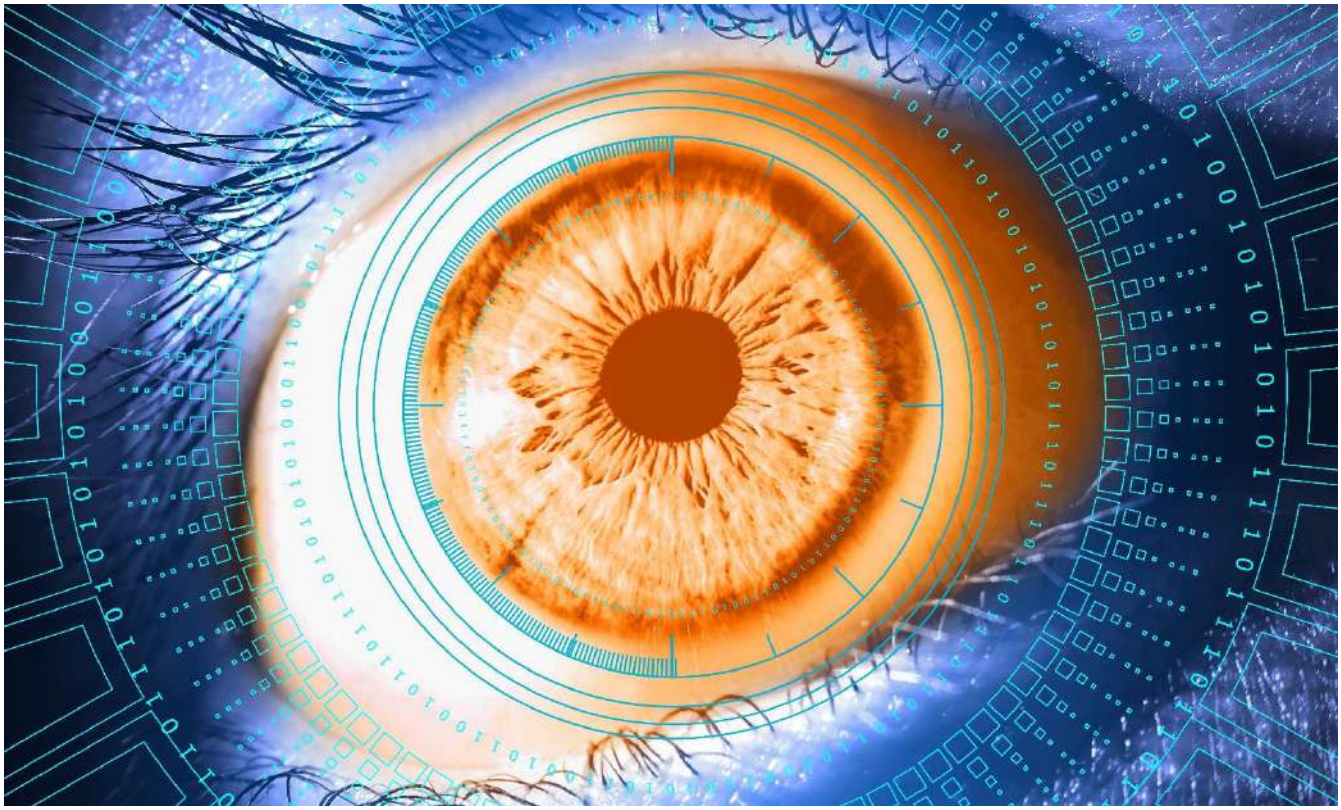

OVERVIEW

Industry points of Pain

- Most packet capturing solutions struggle to maintain both a heavy traffic load and DPI simultaneously, forcing customers to choose one or the other.
- Over 95% of network and cyber visibility tools retain as little as 2% to 5% of all information collected resulting in misleading analytics and risk.

Available solutions

- CySight's Dropless Collection results in substantially improved time to discover, detect, react and repair.
- Unsurpassed granularity of network traffic big data retained in the smallest footprint.

Customer Profile

This deep packet analysis organization has regularly relied on raw packet inspection (DPI) to provide insights to their customers. One of their largest customers drives Europe's main and busiest production and transportation lines, providing a consistent and reliable day to day routine.

After almost two centuries of leading the industry, they still require flawless monitoring of daily performance while keeping their eyes on their growing complex network environment. To remain flawless, they need to find ways to ensure they can have complete visibility of all the data traversing their network, network connected systems and transport equipment.

By providing a deep packet inspection network management platform this company helps to empower the hundreds of thousands of employees of its customers to efficiently coordinate between all its applications and stay ahead of potential issues.

The Challenge

Given the fact that this organization's customers demanded as much network visibility data as possible, they were seeking the most complete solution available in the market. They began researching to find a tool that could deliver the vision trio, comprising of the highest level of scalability, flexibility, and granularity.

Many of these giant organizations are at constant risk of blind spots that are caused by inefficient monitoring solutions that can cause misdiagnosis with tools which lack retention capability. When analyzing an important resource such as traffic data movement there can be no room for error and naturally the deep packet analyzer must attempt to deliver as such.

A deterioration of performance in production, alerting, scheduling, or any high traffic environment, can have immense effects on businesses that depend on network performance and security metrics to run smoothly. Most packet capturing solutions struggle to maintain both a heavy traffic load and deep packet inspection together, forcing customers to choose one or the other. To overcome this, the need for a scalable NetFlow collector solution to partner up with had become evident.

> "For us, CySight was the best solution in the market, providing a bridge between NetFlow data and highspeed capture appliances - in a single GUI and workflow."

The Solution

The company needed a flow partner that could scale in both collection and granular retention and also be capable of pushing all new kinds of metadata into their API. Extended flow metadata is a growing field that enables customers to gain DPI insights in a distributed and cost-effective manner. Today, customers are all looking to leverage their existing Network investment and make use of new advances in metadata visibility technology. They were looking to bring additional fields and new metadata supported by flow vendors such as; SSL, Threat Intelligence information and many other Applications Intelligence metadata along with the flexibility to support the widest possible vendor extensions in NetFlow, IPFIX and sFlow records.

This packet analysis organization was interested in providing its customers with more than just the standard fields that are usually provided by vendors who support flow exports. As the packet analysis company was upgrading its data consumption methods, the initial packet broker solutions they tested were not sufficient in their flow metadata capabilities until they found a more advanced and capable packet broker that provides extended Applications Intelligence metadata.

This led them to CySight who specialize in the most granular NetFlow retention, supporting the broadest vendor flow fields at an unprecedented level using a unique method to ensure Dropless Retention.

CySight is both used as an OEM providing information to the deep packet analysis organization, enabling them to interface to

its customers and to display its own style and workflow practices and where needed, providing access to CySight's interface with its rich open and flexible analytics, machine learning, A.I. Diagnostics alerting and Report Automation. CySight was the exclusive solution that could provide the level of network visibility needed. This joint solution now enables both massive amounts of data to be analyzed with deep packet inspection features whilst losing none of its crucial context as it leverages the broader and in-depth CySight Dropless Collection data capabilities.

Results

This packet analysis company can now deliver the best and most complete network data analysis to their high-end customers. With customers that demand and require a premium level of visibility throughout their network to sustain an uninterrupted workflow, CySight's solution was a logical and easy choice with its ability to consume all types of metadata. Relying heavily on network performance monitoring and cyber security intelligence data analysis from a single flow source enables the customer to quickly mitigate network and cyber issues, increasing the stability and economic viability of any organization whilst also providing real usage analysis of infrastructure and business communications used by the entire organization such as; customer service, supply chain and security. This directly impacts the bottom leaving little to no room for oversight or misuse of the network or its valuable data.

Together with the rich packet broker metadata and CySight's correlation engine, CySight enables the customer to eliminate blind spots, reduce bottlenecks and identify threats and risky communications in production early on instead of waiting for issues to be presented and dealt with once the damage has been done. This partnership covers the fault in other solutions that miss either most contextual data or cannot scale to the needs of their customers. Ultimately, no other solution in the market today can provide the in-depth Dropless Collection that can only be made possible with CySight.

For Additional info about CySight's Dropless Collection, visit https://CySight.ai to see how you can optimize the use of your data

Feel free to send us questions or advise areas you would like us to expand on.
Please email us at support@CySight.ai

© 2021 IdeaData. All rights reserved. IdeaData and CySight and their respective logos are trademarks of IdeaData in Australia, Israel and/or other countries. All other trademarks are the trademarks of their respective owners. IdeaData reserves the right to change, modify, transfer, or otherwise revise this publication without notice.