CASE STUDY

Large US Law Firm Augments Network Visibility with Keysight

KEYSIGHT

Organization

- Global, US-based law firm
- Top 10 law firm worldwide in terms of yearly revenues[1]

Challenges

- Security risks and challenges introduced by increasing adoption of IoT
- Lack of complete visibility into the IoT infrastructure

Solutions

A comprehensive visibility solution, consisting of:

- Optical TAPs (Flex TAP)
- Edge (Vision E10S) and core (Vision ONE) packet brokers
- NPB clustering (IFC Clustering)

Results

- Full network visibility into all physical and IoT infrastructure components
- Optimization of IoT security tooling
- Unified network visibility management

On a global scale, cybersecurity incidents continue increasing and are becoming more impactful, leaving no industry untouched. The Law Firms industry faces increasing cybersecurity risk and challenges, and the firms are pressured, more than ever, to upgrade or deploy threat visibility and detection technologies to support their business and reputation.

As part of case work, law firms can get access to sensitive client information, including trade secrets, intellectual property (IP), business plans and personal data. This makes law firms, regardless of size or practice area, an attractive target for cyber criminals. Legal clients, as well as cyber insurance companies, are increasingly requiring cybersecurity tools and controls be implemented by the law firms before engaging them.

[1] Law.com

Situation and key objectives

The customer is a top law firm headquartered in the US, with 20+ offices across the globe. As part of ongoing digital transformation efforts, the firm has increased the adoption and reliance on IoT devices and endpoints. This has introduced a number of security risks and challenges to the firm's SecOps team.

As part of a comprehensive network upgrade, the firm's SecOps launched a security initiative to properly secure and establish real-time visibility into their IoT infrastructure. After a rigorous evaluation of multiple security vendors, the team selected a sensor-based, IoT security solution that uses behavioral analytics to automate threat detection and response for the IoT infrastructure. At the same time, the SecOps team was seeking a visibility solution that would ensure the IoT security solution had the network access it required while also enabling a cost-effective deployment of sensors across all sites.

The law firm was already using Keysight visibility equipment to feed network monitoring tools, and the NetOps team was highly satisfied with the ease of use, stability, and performance of the Vision NPBs. As a result, the firm approached Keysight for the new visibility network solutions.

The Keysight team worked extensively with the firm's SecOps and the IoT security solution vendor on the design of a visibility architecture that mapped closely to the firm's and vendor's specific needs, to ensure flexibility for evolving visibility needs.

The Visibility solution

Keysight Flex TAPs were deployed in on-premises locations across all the law firm sites, providing complete access to network traffic. Flex TAPs provide an exact copy of network traffic without impacting equipment on the network, ensuring seamless and reliable capture of traffic.

Keysight's visibility solution did more than enable pervasive visibility. Vision network packet brokers (NPBs) were deployed across all law firm sites to aggregate and optimize data through intelligent filtering and packet manipulation techniques such as deduplication. The NPB eliminated the unnecessary packets, thus sending only relevant data to the security sensors This enabled the firm's SecOps team to cost-effectively scale the number of sensors thus increasing the efficiency of the overall security visibility solution.

In the law firm's smaller offices with <100 employees and medium offices with ~750 employees, the Vision E10S provided the port density and advanced processing capacity needed. In larger sites with ~1,400 employees, a bundle of Vision E10S and Vision ONE was deployed to meet port density and advanced processing capacity needs. Additionally, Keysight IFC Clustering solution was implemented to consolidate management and ease orchestration efforts across all 20+ sites.

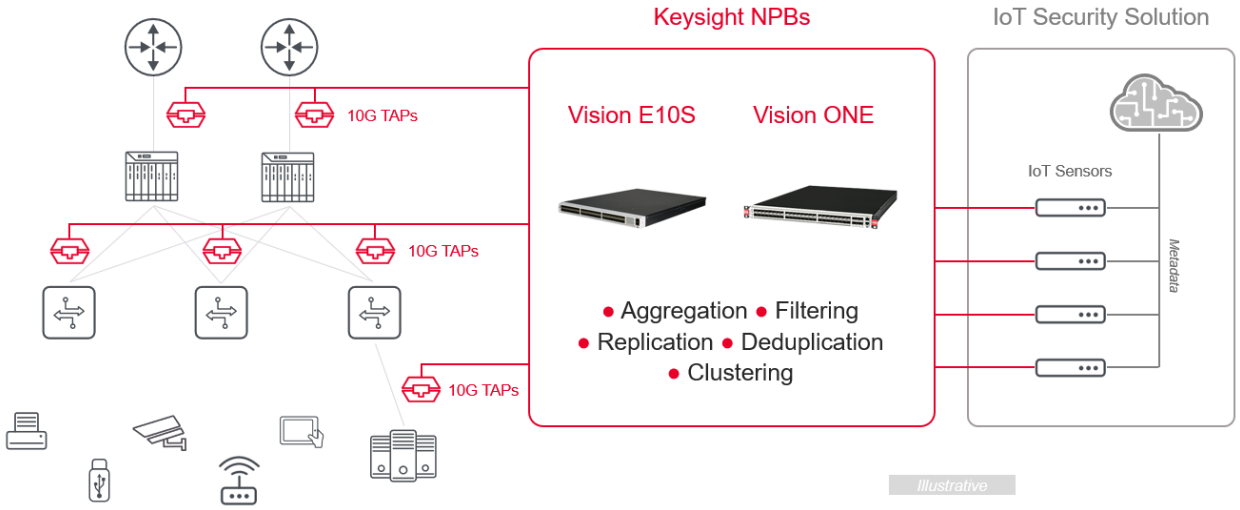

Figure 1. Large site configuration (illustrative)

Results

With Keysight Flex Taps, the firm's SecOps team now maintains full visibility into the network and IoT infrastructure. In addition to providing complete packet access, the Keysight visibility solution significantly reduced the traffic that required inspection by using a powerful processing inside its NPBs to strip away unnecessary data before sending it to the IoT security sensors. This ultimately allowed the SecOps team to optimize the deployment of sensors.

Given the distributed and global nature of the firm's infrastructure, reducing administrative complexity was of utmost importance. Keysight IFC Clustering solution provided the SecOps team with a single management console to centrally manage and monitor all the Vision NPBs deployed in the network.

Further, the Vision One packet broker supports 1G /10G/40G speeds and up to 160Gbps of FPGA-based advanced packet manipulation, allowing the law firm to upgrade speeds and implement additional advanced functions (in addition to deduplication) via software licenses.

Now both the firm's NetOps and SecOps are highly satisfied with the ease of use and performance of Keysight visibility solutions.