QUANTEA QP CASE STUDY: CYBERSECURITY, TOP TALKERS

OVERVIEW

The solution described in this case study is an example of how the Quantea QP Series® plus the PureInsight® traffic analysis solution was able to quickly identify crucial network information such as the top talkers and the applications being used by the top talkers. Newly analyzed data from this solution was also easily integrated into existing traffic monitoring dashboards and alerting through the API built into the QP.

For many large enterprise, where there can be easily thousands of devices connected concurrently, most of the security issues happen from the internal device rather than an external device connecting remotely. Being able to correlate and visualize large amounts of network traffic is difficult since essential information such as top talkers and their applications can change dramatically within 5 minutes especially during a potential cyberattack.

Not only the QP and PureInsight quickly provided top talker and application information, it is able to retain 100% of the packet data that it observed during its session. Due to the retroactive nature of the solution, a deeper investigation on what really happened can be performed easily with the QP.

THE PROBLEM

A large Fortune 1000 enterprise company had an issue with BYOD (bring your own device) since they we're not able to assure that these devices have Splunk® logging software installed on them. Therefore, the possibility of a compromised device going 'rogue' is certain if these devices are not monitored internally. In order to maintain order they will need a way to monitor all the devices connected to their network; however it presents a couple of issues in terms of effective implementation:

- The solution has be able to store large amounts of raw traffic data
- Be able to record traffic data at a high rate without packet loss
- Determine the top talkers without having to import and analyze the packet data to an external system
- Extract application information from top talkers to determine activity/behavior
- Be interoperable with existing analytics platform such as Splunk and Cascade®

By introducing a separate traffic analysis platform for the BYOD devices meant that all internal traffic data will be fragmented into two. In addition, raw packet data (binary) still needs to be converted to a text format for a log analyzer, like Splunk, to be able to correlate build statistics on. This introduces complexity that might bring about more technical problems in the long term. By having a fragmented network traffic data set means that finding network top talkers and their applications has to be done for each data set. It proved to be time consuming and ineffective.

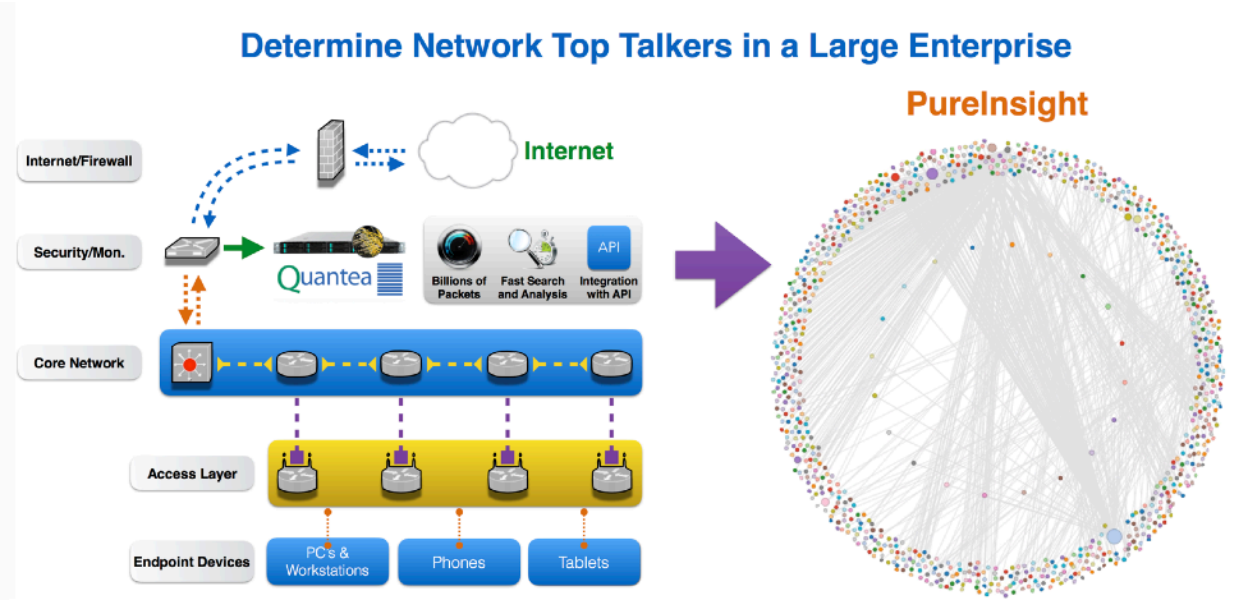
QUANTEA QP CASE STUDY: CYBERSECURITY, TOP TALKERS

THE GOALS

1. Be able to easily visualize the network and their top talkers
2. Ability to quickly “zoom” in and isolate packet data belonging to the top percentile
3. Sustain a 10Gbps traffic write rate
4. Be able to periodically query data and insert to existing Splunk data and monitoring dashboard
5. Maintain a 24/7 operation

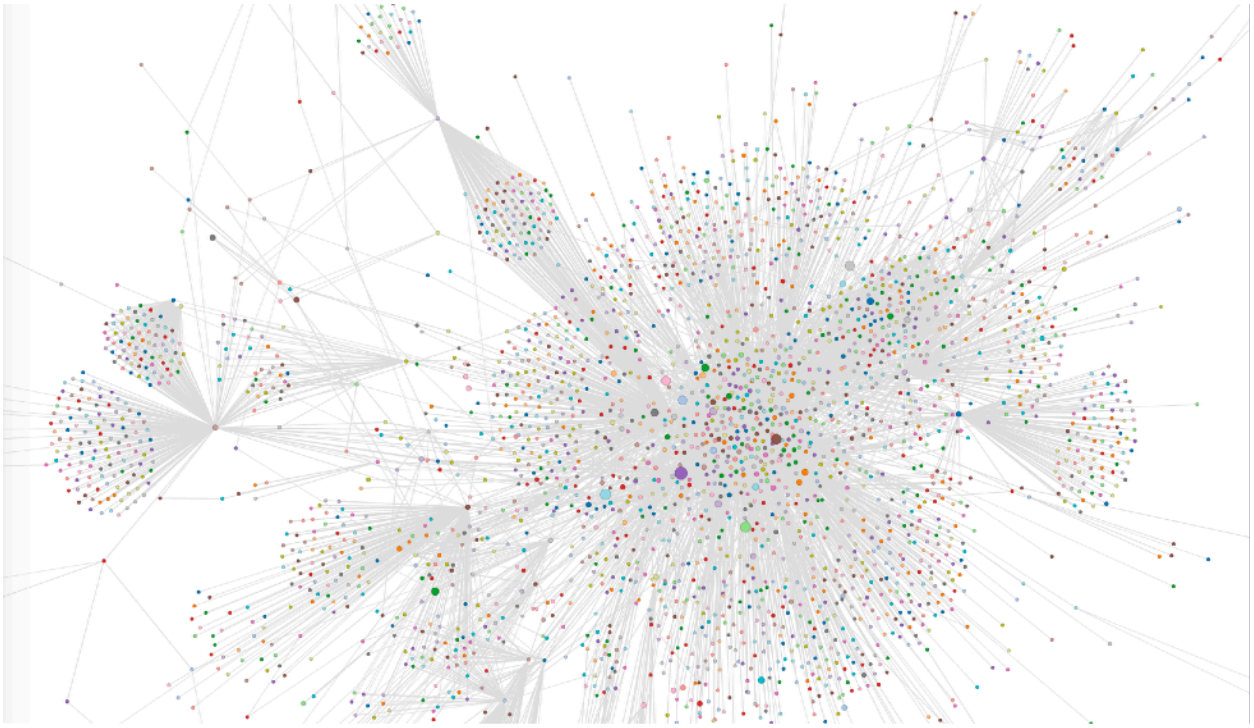
THE PROCESS AND SOLUTION

In conjunction with the QP and PureInsight, they were able to collect large amounts of network traffic and determine the top talkers in the network and determine the application being used. Using the QP’s API, they were able to integrate it to Splunk and into their existing traffic monitoring dashboards.

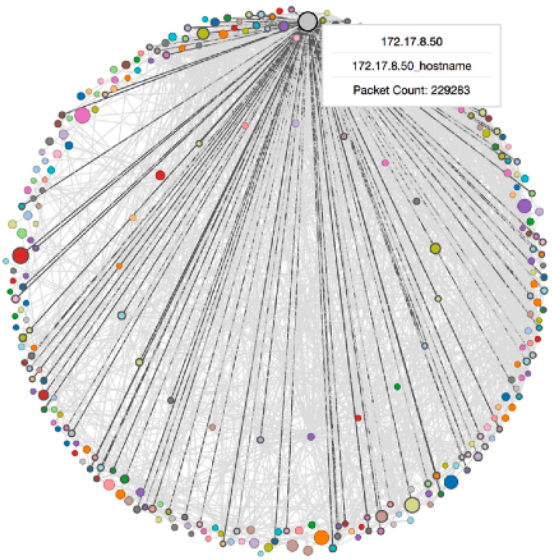


QUANTEA QP CASE STUDY: CYBERSECURITY, TOP TALKERS

VISUALIZATION WITH PUREINSIGHT



Visual Network Representation with PureInsight



"Noise" Reduction by Showing Top Talkers in the Tenth Percentile but responsible for 80% of the communication.

QUANTEA QP CASE STUDY: CYBERSECURITY, TOP TALKERS

KEY POINTS

- Fast ingestion of traffic and analysis with the plug and play functionality of the QP
- Obtain network top talkers in a complex network in a matter of seconds
- Obtain application information with the top talkers to determine any security impact
- Sustained 10Gbps record-to-disk performance in a small 1U form factor
- Integrate with existing security monitoring and logging dashboard using the QP's RESTful API
- Built in traffic search engine can go through TB's on traffic data quickly to zoom in.
- Ease-of-use: No command line interface necessary with GUI

INTEROPERABILITY

Because of how the Quantea solution is designed, it works on any network and the end user can use any packet analysis tool they choose to read and analyze the captured and stored data. Plus, the system can integrate with any TAP, network brokers, IDS/IPS, or security solution and network monitoring system via simple API's.