Better Security and Network Analytics with EndaceProbe and Scrutinizer

plixer

Powerful flow and packet analytics combine for faster identification, investigation and resolution of network problems and security threats.

Plixer's Scrutinizer™ is a highly scalable, enterprise-wide network traffic analysis and incident response system. It turns an existing multi-vendor network into a distributed sensor by centrally collecting all types of flows and metadata. Leveraging this data, it provides insight into 100% of all wired and wireless communications across the network. Scrutinizer can quickly and accurately identify network and security events such as malware, botnet communication, DNS abuse, low and slow data theft, and poor application performance.

Complementing the powerful monitoring, reporting and alerting capabilities of Scrutinizer, EndaceProbe™ Network Recorders provide 100% accurate recording of network traffic regardless of network speeds or loads. Recorded network packets are time-stamped with nanosecond accuracy, allowing network events to be reconstructed with complete accuracy.

The high-fidelity network history recorded by EndaceProbes offers an unparalled source of evidence for analysts investigating the security or performance issues that Scrutinizer detects. Analysts can quickly and conclusively establish the root cause of issues and respond appropriately, dramatically reducing the time to investigate and resolve critical issues. False positives can be quickly identified and flagged so detection rules can be tuned.

PRODUCTS

- EndaceProbe Network Recorders
- Plixer Scrutinizer

BENEFITS

- Spot threats and issues sooner with powerful monitoring, reporting and alerting capabilities of Scrutinizer.
- Total accuracy, deliver conclusive and actionable investigations with drill down to the packet on EndaceProbe.
- Fast and efficient incident response and recovery with integrated workflow.
- Reduced threat exposure through greater analyst productivity, investigate more incidents each day.
- Definitive evidence trail with an accurate record of all relevant packets.
- Reduced false positives through better detection tuning.

FURTHER INFORMATION

https://www.endace.com/plixer.html

Solution Details

Leveraging RESTful APIs, Scrutinizer integrates with EndaceProbes, allowing analysts to seamlessly pivot from Scrutinizer into EndaceVision. Based on the IP address and time range information from a trigger incident in Scrutinizer, Pivot to Vision focuses the analyst directly on visualizations that are pre-filtered based on that incident data. This deep integration enables a streamlined investigation workflow for Network Operations (NetOps) and Security Operations (SecOps) teams that dramatically reduces investigation times and accelerates TTR (Time to Resolution).

Conclusion

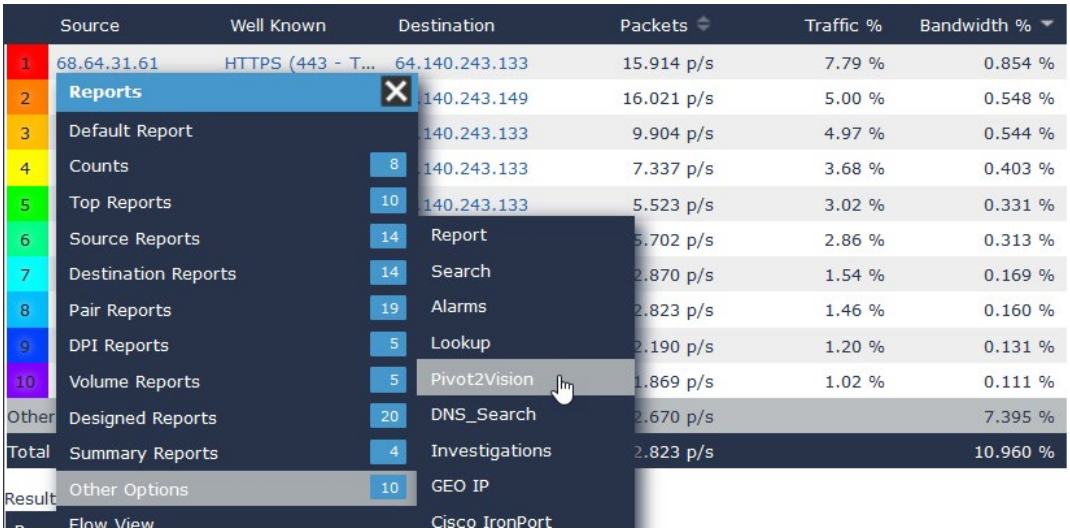
Scrutinizer's flow and metadata monitoring combined with network history recorded by EndaceProbes delivers deep, contextual insight for powerful end-to-end monitoring and investigation.

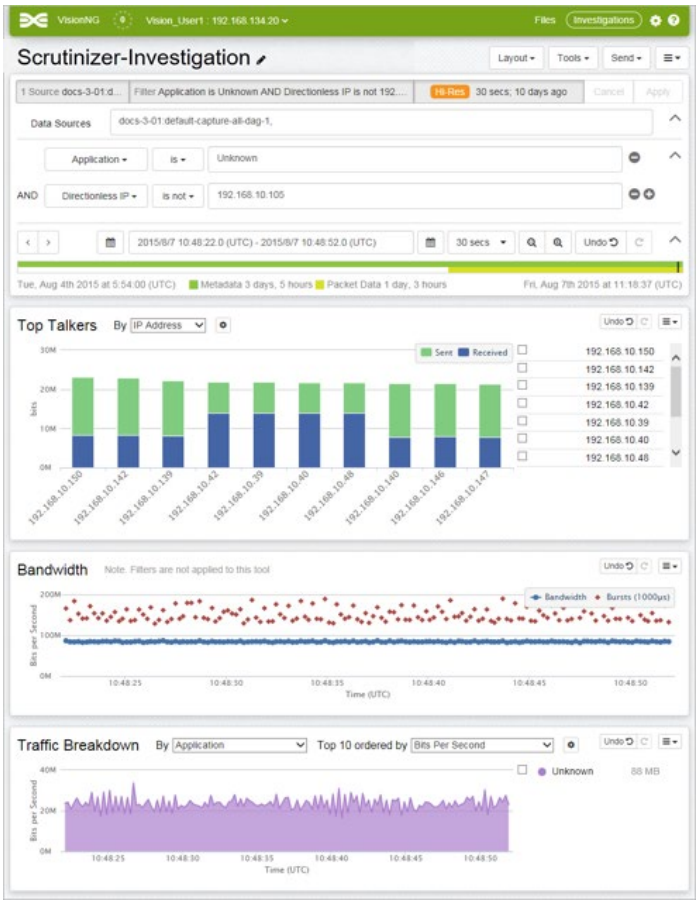
Integrating the two technologies gives SecOps and NetOps teams broader and deeper visibility into network activity and optimizes the detection, investigation and resolution of network security and performance issues

Streamlining Investigations with fast access to definitive evidence

Step 1.

From an event in Scrutinizer, choose Pivot2Vision to go directly to the related packet history stored on one or more EndaceProbes on your network.





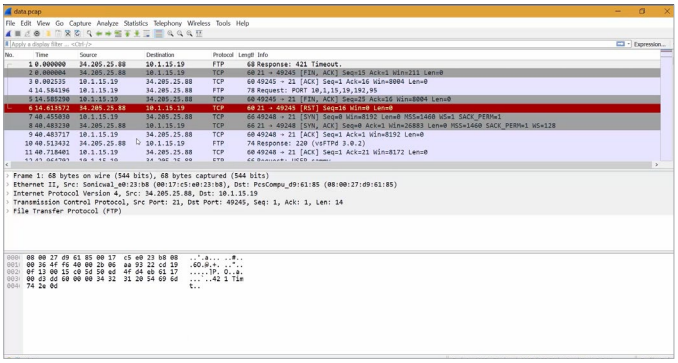
Step 2.

Search parameters are pre-filled. The related packets are shown in EndaceVision.

You can apply filters and use a range of built in views to quickly identify the specific packets of interest for analysis.

Step 3.

Decode packet data directly using EndacePackets or download a packet capture file to analyze in Wireshark



Contact sales@endace.com to arrange a demonstration of the power that integrating EndaceProbe Network Recorders and Plixer Scrutinizer provides.