# Deploying EndaceProbe Network Recorders and Splunk

## Together, Endace and Splunk deliver an elegant and seamless workflow solution for detecting, investigating and resolving network security and performance issues

Splunk® is an industry-leading software platform for collecting and correlating machine data generated by a variety of different IT systems and infrastructure components. Customers use Splunk to provide real-time visibility into network security and performance issues, detect threats and analyze user behavior for evidence of malicious activity.

Combining Splunk's detection and alerting capability with a complete and granular history of network traffic gives analysts deep context around events and provides the definitive evidence they need to investigate events conclusively and respond appropriately.

EndaceProbes™ capture and record 100% of network traffic, regardless of network speeds or loads, providing an unparalleled level of detail and accuracy. Recorded network packets are time-stamped to nanosecond-level accuracy allowing analysts to zoom in to investigate short-lived events – such as microbursts or pre-attack intrusions - that are often invisible to other monitoring solutions. Access to detailed packet-level history lets analysts accurately reconstruct events to identify conclusively what happened, why and how it happened and how to respond. Critical issues can be prioritized, and false positives quickly identified and flagged so detection can be tuned.

Leveraging the EndaceProbe's open architecture, Endace's Fusion Connector for Splunk integrates with and extends Splunk. Security Operations (SecOps) or Network Operations (NetOps) analysts can select an event in the Splunk dashboard and quickly pivot straight to the related packet-level history recorded on EndaceProbes, dramatically reducing the time needed to investigate and resolve issues.

### PRODUCTS

- EndaceProbe Network Recorders
- Splunk
- Endace Fusion Splunk Connector

### BENEFITS

- Accurate, complete and granular network history provides definitive evidence for network security and performance issue investigation and response
- Streamlined investigation workflow improves SecOps and NetOps efficiency and ensures fast investigation and response
- Faster resolution times increase network security, improve uptime and reliability and reduce OPEX costs
- More effective detection tuning reduces the overhead of false-positives
- Recorded network history provides a reliable. irrefutable evidence trail

### FURTHER INFORMATION

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

## Solution Details

Endace's Fusion Connector for Splunk is a free, easily-installable plugin available through SplunkBase. It directly connects analysts, via an elegant and seamless workflow, to the precise network packets they need to investigate the root cause of problems and respond. Analysts can click on a Splunk event to pivot straight to the packets of interest. These are delivered as a .PCAP or .ERF packet capture file which can be analyzed using Wireshark® or other packet decode tools, or archived for evidentiary purposes.

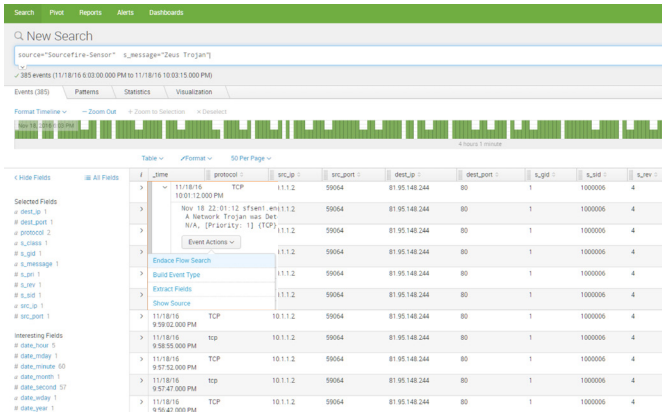


*Figure 1. Drilling down from an event in Splunk*

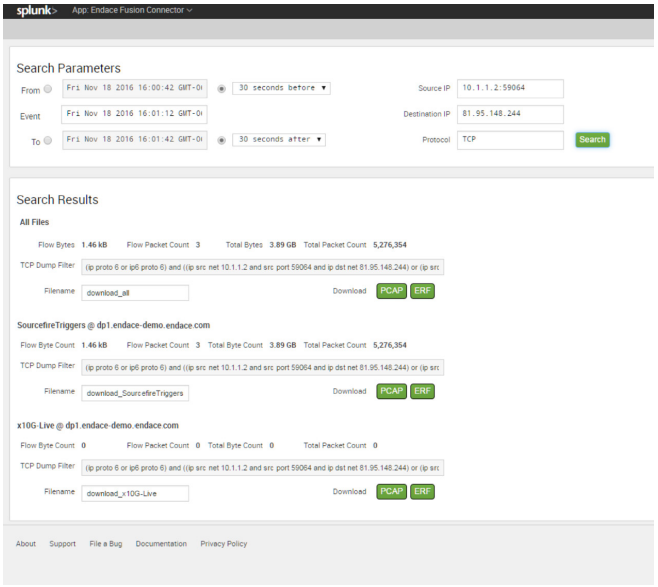


*Figure 2. Packet search parameters are pre-populated*

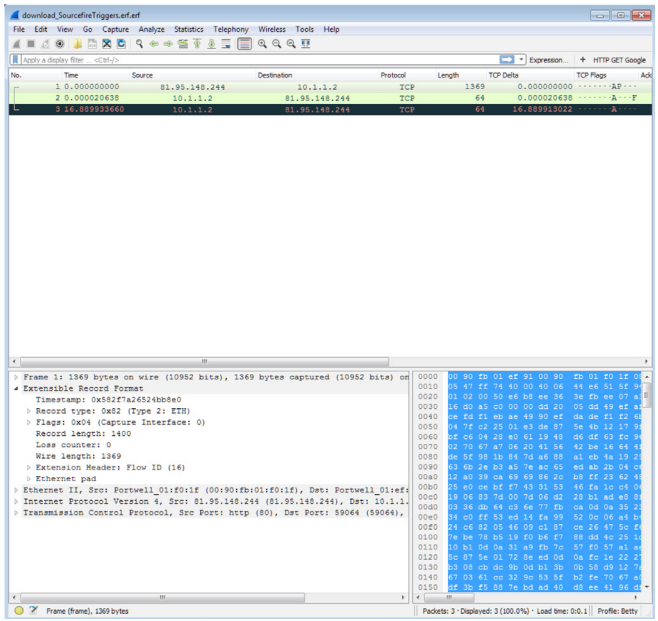


*Figure 3. Packets of interest retrieved as a PCAP file for analysis in Wireshark*

## Conclusion

Integrating EndaceProbes with Splunk combines broad network visibility with comprehensive search and drill down investigative capability. It gives SecOps and NetOps teams the fastest, most conclusive way to investigate and respond to the security and network performance issues Splunk detects.



Contact sales@endace.com to arrange a demonstration of the power that integrating EndaceProbe Network Recorders and Splunk can offer.