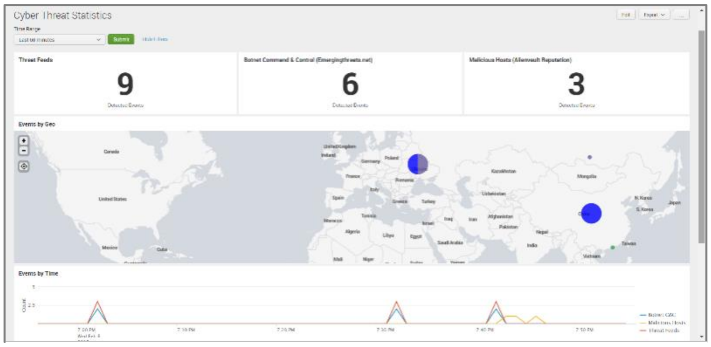
Solution Brief

NetFlow Optimizer for Network Security



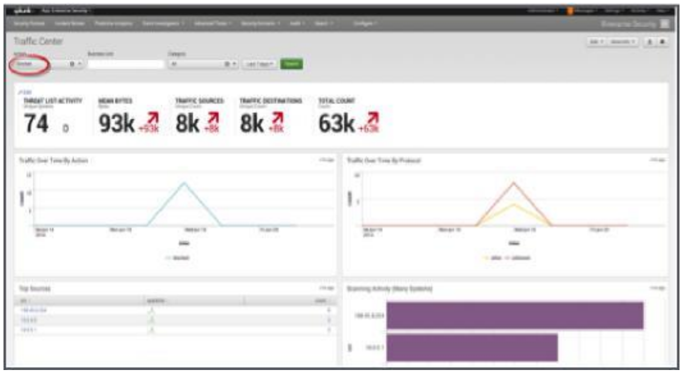
(Cyber Threat Statistics within NetFlow Analytics for Splunk App)

Virtualization and other technologies have changed the way companies do business today. The volume of network data coming from today's networks is massive and can be overwhelming to security teams. Everyday cybercriminals are becoming more ruthless and their attacks significantly more advanced and sophisticated. At the same time, most companies rely on legacy IT systems consisting of perimeter security and endpoint protection. But these systems cannot protect from unknown threats. To address new challenges network operators need in-depth understanding of network traffic, and **NetFlow Optimizer™ (NFO) offers exactly that,** providing an additional security solution for early warning threat detection.

NFO is designed to leverage existing IT infrastructure and provides a processing engine for various formats of flow data: NetFlow, IPFIX, sFlow, j-Flow, etc. Like its predecessor - NetFlow Integrator™ - NFO **optimizes and enriches flow data** in **real-time.** By identifying and highlighting meaningful information in flow data, NFO transforms it into actionable intelligence.

NetFlow Optimizer provides an easy and scalable way to analyze the massive volumes of network data generated by routers, switches, next generation firewalls, and load balancers - whether it is from a physical or virtual network, or both. By bringing syslog created by NetFlow Optimizer into Splunk Enterprise, VMware vRealize Log Insight, or other SIEM platform, security analysts can visualize real-time data from network devices, and correlate it with other machine data. Monitor your end-to-end infrastructure to gain security intelligence with real-time visibility and critical security insights.

Delivering Virtual and Physical Network Security Intelligence



(NetFlow Logic Technology Add-On for Splunk Enterprise Security)

Enhance perimeter security awareness by including "blocked" and "suspicious" traffic from your next generation firewall, consolidating NetFlow volumes by more than 4x. Enables the investigation of detailed network conversations directly within Splunk Enterprise Security.

Solution Benefits

- **Threat Intelligence and IP Reputation ready** – Pre-process all flow data from the entire virtual and physical network and send flows matched with threat lists as high priority events to Splunk Enterprise, VMwarev Realize Log Insight, or any other SIEM system for further investigation and correlation with other machine data.

- **Data enrichment** – Resolves and adds host names, VM names, GeoIP information, and Reputation information to syslog messages.

- **Compliance and forensics** – Capable of simultaneously sending all flow records in syslog format to Hadoop for full fidelity long term storage and forensic investigations.

- **Powerful processing engine**–Employs sophisticated proprietary algorithms to consolidate, correlate and pinpoint critical events.

- **Low deployment costs** – Save on customer training by using one unified platform.

Get up and Running in minutes

NetFlow Optimizer software or VM Ready Virtual Appliance installs in minutes. It enables security teams to discover relevant security events, no matter the architecture - traditional, server, and virtualized, or fully virtualized data centers. Download it for deployment in your existing environment today.

For more information or to register for a demo or evaluation, please visit: www.netflowlogic.com

System Requirements

Hardware/Virtual Appliance
16GB RAM, 8 Cores CPU, 20 GB disk space.
Virtual Appliance
VMware ESXi 5.x and above
Operating System
Linux CentOS 5.5, 6.5, 7 – Debian 6 – RHEL 5.5, 6.5, 7 – SUSE ES 11 (kernel 2.6+ 64-bit)
Windows Server 2008 R2, 2012, and 2012 R2 (64-bit)

Contact NetFlow Logic
Website: www.netflowlogic.com
Email: info@NetFlowlogic.com
Phone: +1 (650) 308-8887