FLOWTRAQ

THE “NEW” NETWORK FLOWS

How Today’s Network Flow Data Provides More Value Than Ever for Security Threat Incident Detection

Because technology continues to evolve and gets smarter and faster every day, old labels don’t necessarily equate to old technology. For instance, today’s cars are equipped with Bluetooth and blind spot detectors and automatic starters, yet they are still cars — just like your father’s Oldsmobile (or more likely your grandfather’s).

Along those same lines, significant innovations in server hardware and software allow network flow data (e.g., NetFlow, jFlow, sFlow and cFlow) to provide so much more information and value than they did 15 years ago — far beyond network analysis. That level of detail can be the difference in detecting network threats more quickly and keeping your network safe.

MORE THAN A NETWORK PERFORMANCE TOOL

Network flow data today can provide so much more value than simply frame packet transfers or information on network bottlenecks. Significant technological advances in flow analysis allow companies to analyze data in a way that makes it much more effective for security threat incident detection than it was even just a few years ago. For instance:

- Today’s flow tools are faster and less expensive
- The cloud provides storage availability for scalability
- Algorithms have been refined to handle the much larger volumes of data on the network, while providing more valuable insights
- Multi-processing CPU systems allow parallel processing of high volumes of network data that would have been impossible years ago, enabling more complex security analysis algorithms

NETWORK FLOW DATA FOR PREMIER SECURITY THREAT INCIDENT DETECTION

Because of the technological advances mentioned above, today’s network flows are some of the best sources for security incident threat detection. For example, they:

- Provide important information about what’s happening on your network
- Identify traffic anomalies and potential threats, such as scans, new and unwanted services, data exfiltrations, or botnet behaviors
- Replay incidents of security breaches, even if they happened months ago

- Find threats, such as malware downloads or hacker reconnaissance behavior in real time before they become an issue
- Provide on-demand ability to drill down on network incidents
- Do all of the above at an affordable price

THE POWER OF FLOWTRAQ

FlowTraq is unique in the way it uses network flow data to address many of your network security-related business problems with one powerful tool.

ROBUST RESOURCE

Whether you have limited resources in terms of network security talent or you have **a dedicated 24/7 cyber hunt team**, FlowTraq can help by being supplemental eyes and ears, alerting you to network anomalies and unusual or suspicious network activity. With FlowTraq you get security incident detection in real time, at a surprisingly affordable price, so you can respond accordingly.

PROPRIETARY TECHNOLOGY

Our unique technology approaches network security incident detection in a completely different way from other solutions. FlowTraq minimizes the time required for auditable recourse after a security breach, expands the capacity of security analysts to monitor ever-increasing network traffic volumes by focusing them on what needs attention right now, and boosts anomaly detection performance when deployed across multiple processors. We're able to do this because of three essential ingredients.

Specifically our:

1. **High-speed proprietary database** that allows FlowTraq to process massive volumes of real-time network traffic faster than other flow-based network security tools, and tracks months' or years' worth of stored network traffic flows to be used for forensics.
2. **Unique proprietary algorithms** that can learn a range of network behaviors and will instantly alert when anomalies are detected.
3. **Scalable architecture** distributed over multiple servers that work together to form an intelligent FlowTraq Cluster for unmatched performance regardless of traffic volume.

FULL-FIDELITY FLOW RECALL

FlowTraq's full-fidelity feature allows for more powerful analysis and forensic capabilities than traditional network flow collectors. High flow traffic volumes can be more demanding on the hardware; fortunately, server hardware is more powerful and affordable than ever and FlowTraq is designed to take advantage of multi-core processors and virtual environments.

A FlowTraq server handling a 24/7 **sustained flow rate of 25,000 updates per second can be configured**, for instance, on an 8-core CPU and with 8GB of RAM per core, for a total of 64GB. Disk space configuration can be matched to your required retention period. Full-fidelity retention of 25,000 flow updates per second will consume about 1TB per week; therefore, keeping three months of flow data at a saturated 10Gbit network will take about 12TB.

In demanding environments, such as those with a flow load higher than 25,000 updates per second, many FlowTraq users run more than one FlowTraq server in a cluster configuration. This automatically balances the processing load over multiple systems and is completely transparent to the user. For example, a cluster of eight FlowTraq nodes will handle 200,000 flow updates per second of full-fidelity flow data.

BEYOND TRAFFIC MONITORING

While 80 percent of users rely on flow data just for network traffic volume monitoring, FlowTraq uses that same data for security incident detection including data loss, DDoS attacks, network scans, worms, insider threats and more by using a unique and fast software architecture that **takes advantage of the resources you already have**. The scalable architecture, use of algorithms and a proprietary database all add up to make FlowTraq an unparalleled tool for security incident detection.

ABOUT FLOWTRAQ

FlowTraq® provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, botnets, worms, network scans and other network traffic anomalies. To request a free trial of FlowTraq, visit **www.flowtraq.com/trial**.

FlowTraq

16 Cavendish Court, Lebanon, New Hampshire 03766 USA
Phone +1 (603) 727-4477 | Email info@flowtraq.com | www.flowtraq.com