FlowTraq

Security Visibility at Scale

High-performing network security and forensics solution that accelerates incident triage and detect anomalies typical of hacker behavior.

Business Challenge

The cyber threat community stepped up their game to take advantage of the expanded threat surface caused by the pandemic and work from home. Security operations (SecOps) was similarly challenged to protect the enterprise from increasingly active and more aggressive and sophisticated attackers. Cyber security threats rose by nearly 50% in email spam, phishing, malware, ransomware, and malicious domains. Without the right visibility into your network, you could become another Colonial Pipeline or SolarWinds.

About FlowTraq

FlowTraq is a high-performing network security and forensics tool that accelerates incident triage and detects anomalies that are typical of hacker behavior. FlowTraq provides powerful, scalable, and easy-to-use network security analytics based on the ubiquity of NetFlow. Security analysts can detect a complete range of network anomalies, including simple traffic threshold alerts, deviations from baselines, and DDoS events.

FlowTraq helps customers:

- Recognize DDoS and brute force password attacks in real time.
- Defend the network from malicious botnets.
- Protect sensitive information from outside intruders.
- Improve forensics recall with full-fidelity NetFlow data.

Capabilities

Network performance management, DDoS mitigation management, peering analysis, and ultimately security — they all flow from one common root: Visibility at Scale.

Unrestricted Visibility

Data sources are only half of the security visibility story. The ability to arbitrarily filter, view, and manipulate the data is what turns the data into valuable security intelligence. FlowTraq gives the operator infinite control over how to filter the data, and how to view the data. Boolean filtering control allows you to zero in on the needle in the haystack, which includes botnet command & control channels, rootkit and backdoor communications, and data leaks. It also gives you unprecedented control over performance-sensitive data by creating arbitrary top-N lists of any aspect of your network traffic.

Big Data Database

Doing meaningful analysis with flow data requires a big data approach to data management. FlowTraq uses a patented database technology designed for handling infinite amounts of flow data, without needing to aggregate. Flow aggregation is a common technique to cope with scalability problems, but it greatly impairs the accuracy of the data and makes it useless for security visibility purposes. Built for modern parallel architectures, FlowTraq makes optimal use of all the computer and IO resources available, so you do NOT need to aggregate your valuable flow data.

Triple-Split Storage Architecture

The FlowTraq database features a “triple-split” design, where flow data can be stored in progressively slower, but larger storage layers. The most recent flow data is quickly and directly available from the RAM database. Longer queries are serviced from a local SSD database, while the furthest history is stored on archive that can be provisioned on spinning RAID, or remote SAN/NAS solutions. This ensures the operator has fine-grained control over retention history of forensically accurate flow data, without breaking the hardware budget.

Long-Term Trends and Baselines

Network Performance Management is all about understanding how traffic volumes and patterns are changing in your environment. FlowTraq builds baselines of normal traffic, and stores long-term trends for all your interfaces, and network traffic groups. These include top-N lists of top talkers, top endpoints, as well as source and destination country, an autonomous system. These let you quickly evaluate peering relationships and link utilization over years of collected data.

Traffic And Security Alerts

FlowTraq detects a complete range of network anomalies. Including simple traffic threshold alerts, deviations from baselines, as well as Distributed Denial of Service events, and security violations. Use FlowTraq to detect:

- data leaks from your network
- zombie botnet control channels
- malicious services popping up in your network
- scanning
- brute-force password behavior.

Alerts are delivered by email, or to the SIEM of your choice. Thanks to a flexible plugin architecture, FlowTraq can even take mitigating actions when bad behaviors are detected.

Distributed Load Balanced Clusters

Have a lot of flow? No problem. Our patented flow analysis clustering technology allows you to run FlowTraq over multiple servers at once, combining their storage and processing power to handle unlimited quantities of flow data. As your flow volumes grow, you can simply add additional hardware or virtual containers, and they will transparently add to the collective power of the FlowTraq cluster. Our own distributed cloud service is handling 22 million flow records per second at peak!

API and CLI

Security visibility is all about control and data integration. FlowTraq ships with a full suite of command-line tools (available on all our supported platforms) plus a complete REST-API, that enables you and your scripts to interact directly with the distributed FlowTraq database. Supporting all common data formats, from CSV to JSON, the CLI and API interface brings all the power of FlowTraq into an easily scriptable package.

Cloud or On-Prem

FlowTraq offers two deployment models: our servers, or your own. The FlowTraq managed cloud is built upon the dependable resources from AWS, Azure, and Google. Simply create your account and start sending flow. If you instead prefer to keep the flow local to your environment, simply download the Virtual Appliance Container, and run FlowTraq from ESXi, KVM, or Hyper-V. Learn more about Flowtraq's server hardware requirements.

Multi-Tenancy at Core

Built with a multi-tenant database core, you can create as many partitions as needed to support a diverse range of end-customers. Each partition is fully independent yet receives access to the full storage and compute resources of the entire FlowTraq cluster. Partitions support both regular and administrative users and have their own monitoring and security policies. A single FlowTraq cluster supports thousands of partitions.

MSP Remote Site Support

Use our lightweight flow proxy daemon to collect flow at remote sites, encrypt it, and bring it back to your central multi-tenant FlowTraq installation. Our proxy daemon is free of charge, and can easily be deployed in local CPE devices, or run on a small server in the remote environment. Original exporter addresses are maintained, so no visibility is lost. Combined with FlowTraq multi-tenant partitioning, there are no collisions when there is IP address range overlap between multiple remote sites. Each partition is completely independent of the others.

Detect DDoS Fast and Manage Mitigation Automatically

When a DDoS attack is detected, FlowTraq will automatically select and invoke the appropriate response. Thanks to integration with dozens of scrubbing and mitigation vendors, FlowTraq is able to automatically pick the best mitigation approach for each attack, maximizing mitigation effectiveness, and minimizing your cost-to-mitigation. Support scrubbers include A10 TPS, RadWare DefensePro, ForiDDoS, Verisign OpenHybrid, and Voxility.

All Flow: NetFlow, SFlow, IPFIX, cFlow, Jflow

FlowTraq supports all flow formats, and "normalizes" their content. This means you can mix and match flow sources, and filter, view and compare traffic from any data source in your network. Even when some are sampled, and others are not. We encourage the operator to improve security visibility by collecting data from as many flow-capable devices as possible in the network. Visibility starts with data sources.

About Riverbed

Riverbed enables organizations to maximize visibility and performance across networks, applications and end-user devices, so they can fully capitalize on their cloud and digital investments. Riverbed solutions enable organizations to visualize, optimize, remediate and accelerate the performance of any network for any application, while supporting business objectives to mitigate cyber security risk and enhance the digital experience for all end-users. Riverbed offers two best-in-class product lines: end-to-end visibility – including NPM, APM and EUEM – that delivers actionable insights; and network and acceleration solutions, including application acceleration (SaaS, client and cloud acceleration), WAN optimization, and enterprise-grade SD-WAN.
Riverbed's 30,000+ customers include 95% of the *Fortune* 100. Learn more at riverbed.com.

riverbed®