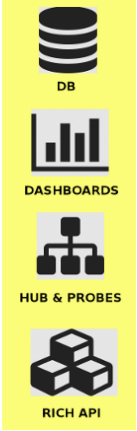
Trisul Network Analytics 6.5

Network Security Monitoring & Traffic Analytics Platform

DATA SHEET FOR NETFLOW MONITORING

Trisul Network Analytics helps organizations develop a comprehensive network visibility , security, audit and incident response capability. Trisul works with *FULL PACKET CAPTURE* or *NETFLOW* technologies to provide complete correlated real time visibility and historical analytics reports. The five major building blocks by Trisul are monitoring Traffic Metrics, Network Flows, Metadata, Alerting and Intelligence, and finally Packet Capture and Recall.



NETFLOW ANALYTICS FEATURES

SUPPORTED MODES : Netflow v5, v9, v10, SFLOW, IPFIX, Flexible Netflow (FNF),JFLOW

Autodiscovery of Netflow topology

No need to configure routers or interfaces. Just send Netflow from as many devices as you want. Trisul will automatically build a topology of routers and interfaces. Routers and interfaces no longer active are automatically removed from the live topology but they exist in the historical traffic analytics.

Traffic and Bandwidth Metrics

Monitor 200+ traffic metrics at 1 minute resolution without any roll ups or summarizations for long term analytics. Advanced statistical metrics like cardinality counters (eg unique applications per host) and top-N snapshots are all enabled out of the box. A few of the hundreds of metrics are Hosts, Applications,, Countries, AS Numbers, Routers, Ports, etc.

Flows and Device Views

Network flows are analyzed and stored in a custom built database engine designed for very fast storage and retrieval. Trisul stores every flow and does not summarize for maximum fidelity. The **Netflow Router and Interfaces Manager** tool lets you effortlessly drill down into interface level usage reports for long term analysis. **SNMP integration** resolves all ports and devices to their readable names. The **Netflow Interface Tracker** is a streaming analytics algorithm that lets you generate long term accurate drilldowns of interface usage.

Alerts based on flows, traffic, or anomalies

Rich automatic email alerting with context embedded within the email for anomalous flow based activity due to large Email attachment upload, data theft, exfiltration, or long remote desktop logins. Set **Threshold Crossing** alerts for all interfaces that alert you when they cross pre-set thresholds. **Threshold Band** alerts detect anomalous usage based on machine learning data.

SYSTEM REQUIREMENTS IN NETFLOW MODE

SMALL < 100 DEVICES	MEDIUM 100-2000 DEVICES	LARGE > 2000 MULTI SITE
Single Probe+Hub	Single Probe+Hub	One Hub + multiple probes
Core i5 & Above / 8GB RAM/ 1TB HDD/ 1 Gigabit NIC	Xeon 8 Core / 16 GB RAM / 2TB HDD / 1 Gigabit NIC	Hub: Xeon 8 Core /32 GB/ 8TB HDD Each Probe : Core i5/8GB/16GB RAM