TRISUL

SOLUTION BRIEF

TRISUL NETWORK ANALYTICS

FOR

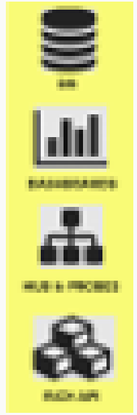
MANAGED NETWORK SECURITY SERVICE PROVIDERS

How Trisul can help you scale your business in all stages

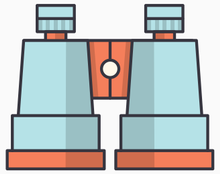
https://trisul.org

What is Trisul ?

Trisul is a network security monitoring and traffic analytics platform



Trisul Enables ..



VISIBILITY

100% multi-layer traffic visibility

Netflow and PCAP ingestion

Over 200 traffic KPIs

Real time views of hosts, apps

Top-K,Bottom-K, Trends

DETECTION

Spot malware and suspect activity

Built in integration with IDS

Keep record of all large flows

Alert on exfil, data leaks, scans

Unusual traffic patterns

RESPONSE

Quickly identify impact

Intuitive UI for Incident response

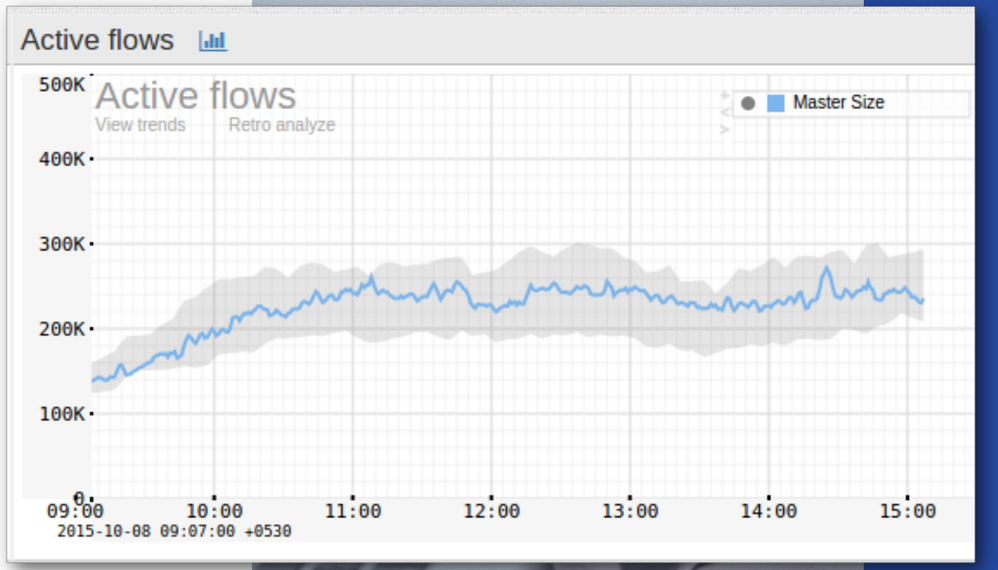
Drilldown all the way to packets

Automate using scripting API

Streaming DB for fast analytics

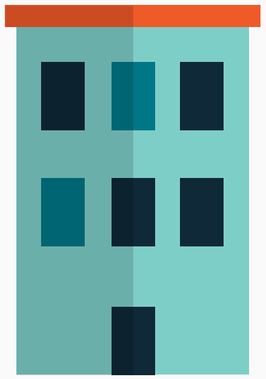
Trisul Advantages

Combines network traffic visibility with cutting edge security analytics



- **Single pane of glass view of Traffic and Security dashboards**
- **EASIER to setup and operate deep traffic monitoring**
- Full NSM stack reconstructs artifacts, flows, potential malware, IDS based alerts, threats and metrics.
- Go-to source of truth for incident response. Lossless threat analysis tools with no roll ups.
- Distributed probe-hub architecture for large networks
- Includes the backend storage and WebUI. Needs only 20-25% of the server resources as Elastic (ELK) based systems
- Top R&D product team responsive to your demands

how we can help MSPs as tech partner

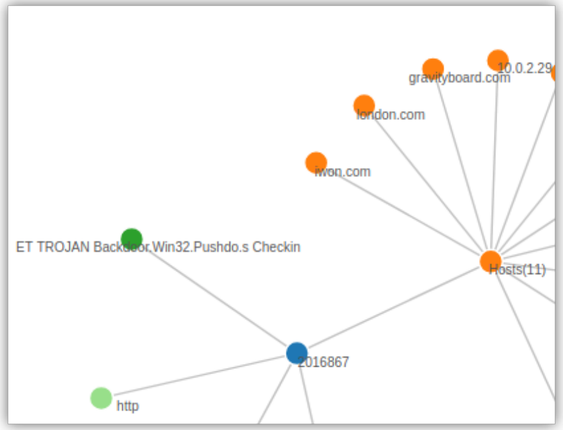


FOR ONE-PERSON, SMALL , AND MEDIUM SERVICE PROVIDERS

- Use Trisul during initial consulting or PoC/Trial stage to prove value to the customer **Audit/Review**
- Offer a professional service including **Traffic Monitoring,threat detection, forensics, and compliance**.
- Offer 24x7 **Network Security Operations** with immediate alerting and remediation.
- On-Prem or cloud based distributed deployment.
- Shared Multi-Tenant service on cloud
- Offer customer portal with your branding
- Simple pay as you go model.

Comparison with OSS

tool set based service solution



Trisul provides the replacement functionality of the following OSS tools in one integrated solution.

NTOP : Trisul provides much deeper long term visibility of traffic metrics from both packet capture and Netflow/SFlow

BRO/ZEEK : All the logs like DNS, TLS, Conn, HTTP, are also available from Trisul.

IDS: Trisul integrates with Snort/Suricata via Unix Sockets

Argus/SiLK: Full Netflow support including Device views

NAGIOS: For small networks Trisul can monitor using SNMP

Elastic/Kibana: Trisul includes a streaming database and UI Requires only a fraction of hardware resources as ELK/Splunk.

netsniff-ng/stenographer : PCAPs encryption and super fast querying.

Interested? Next steps

DOWNLOAD TRISUL FROM
https://trisul.com

Try it out in your lab or in a friendly customer network and discover value

Contact info@unleashnetworks.com for a one-on-one web demo

Thanks !