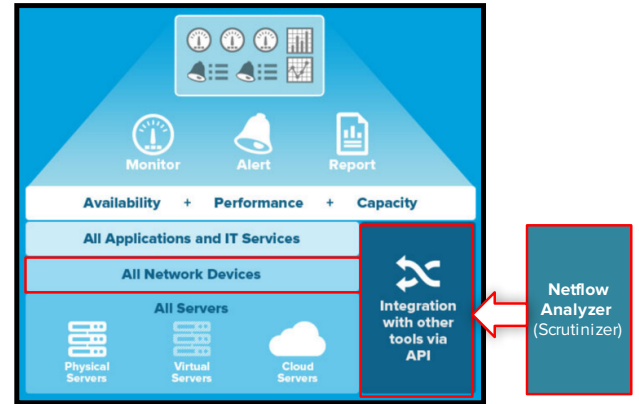


Uptime Infrastructure Monitor with Netflow Analyzer Integration

COMPREHENSIVE VIEW OF THE NETWORK TRAFFIC ON A SINGLE PANE OF GLASS

Uptime Infrastructure Monitor provides a comprehensive yet simple to use network management solution with a broad set of monitoring and analysis capabilities. Uptime Infrastructure Monitor provides collection and alerting for latency, packet loss, and throughput, errors and discards, as well as custom monitors for any published SNMP metric, accessible direct via the OID, or through manufacturer MIBs. It ensures that service levels are being met for enterprise and service provider networks.

Uptime Infrastructure Monitor's optional Netflow analyzer, Scrutinizer by Plixer, provides in-depth network analysis by collecting NetFlow, IPFIX, JFlow, NetStream, sFlow and others. The data is then compiled to build profiles of the end systems hosted on the network. This add-on provides the ability to observe your network traffic by switch port number, protocol, port, MAC address, subnet, VLAN, DSCP value and much more. Just click on a specific application or device and display the data usage details.

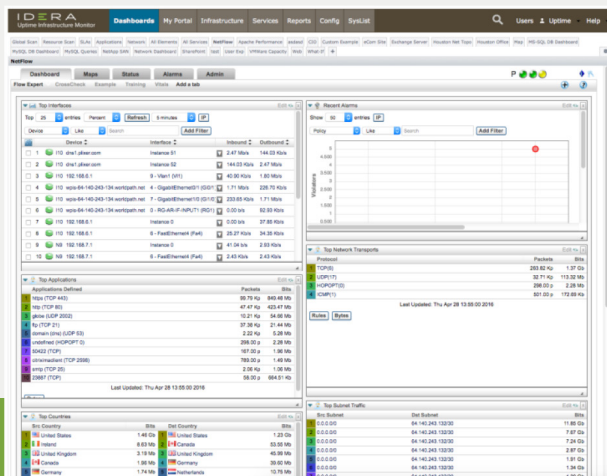


NETWORK FORENSIC ANALYSIS

Quickly and easily investigate and isolate network bandwidth hogs by finding out who, what, where, when, and how much. These details allow administrators to shut down problems - fast. Dive into any performance issue by user, application, protocol, or group and gain broader more comprehensive traffic insight.

PROACTIVE ALERTS & CUSTOMIZABLE REPORTS

Scrutinizer offers IT administrators automatic real-time alert notification of potential problems and threats detected across network devices. Scrutinizer also provides historical and advanced reporting. Create customizable reports per interface on top hosts, protocols, applications, top countries, domains, subnets or many more. Save all flow reports and configure any of those with a threshold to trigger an alarm.



NETWORK-LAYER THREAT DETECTION

Detects DDoS attacks, DNS tunnels, C&C communications, and low and slow data leaks. Builds behavior baselines and triggers for changes in traffic patterns. Provides the ability to create custom monitors that watch for specific unwanted communications. Correlates usernames with IP addresses by integrating with Microsoft Active Director, Cisco ISE and other authentication platforms. Maintains a Threat Index on end systems and triggers corrective action for threshold breaches.

VISIBILITY ACROSS THE ENTIRE NETWORK

Scrutinizer is a comprehensive Netflow, sFlow and IPFIX solution that provides a complete view of data flow. It helps administrators watch over the performance and availability of all routers, switches, servers, firewalls, and SNMP-enabled devices and to see where threats are originating and how the network is being used. Devices can be mapped visually using google maps integration around the globe. Device to device communication can also be visualized on these maps real-time.

EASE OF USE

Scrutinizer's ease of deployment and administration, coupled with its easy to use and customizable dashboards, make it a powerful tool for network administrators to help identify issues with their network infrastructure.