Tools: Network Traffic Analysis

Return to Tools Area

Network Traffic Analyzers are generally deployed within Enterprises. Although having many of the characteristics of a single, united Enterprise, DIDOs are naturally more of a federation or coalition of the willing spread across the internet. This is why virtualized testing is so important.

Source: The 14 Best Network Traffic Analysis Solutions for 2019 and Beyond, September 17, 2019, https://solutionsreview.com/network-monitoring/the-14-best-network-traffic-analysis-solutions-for-2019-and-beyond/

- ***Awake Security Platform*** *is a network traffic analysis solution that focuses on discovering, assessing, and processing security threats. The tool is broken down into three parts: Awake Sensors, which continuously monitor and collect data from devices, apps, and users; Awake Nucleus, which analyzes that data to understand behaviors and attributes of entities and applying deep forensics; and Ava, a privacy-aware security expert system that applies machine learning to collected data.*
- ***Corelight*** *is a security-focused network traffic analysis provider that uses the open source network security monitor Zeek as its basis. Corelight Sensors convert network traffic data into logs and extracted files which can all be managed through the Corelight Fleet Manager. Through the Fleet Manager, admins can define custom groups, assign individual roles, and set access levels. Corelight Sensors come either as hardware for networks, as a virtual sensor, or as a cloud traffic monitor for AWS.*
- ***Flowmon*** *is a network performance and security solution provider that offers network traffic monitoring and analysis capabilities. The solution offers real-time NetFlow and IPFIX monitoring and analyzes network traffic data from a physical, virtual, or cloud infrastructure. It also gathers flow data statistics generated by routers, switches, or standalone hardware probes. Users can add self-defined filters that set parameters for data collection based on what data the user wants to look at.*
- ***Kentik Platform*** *is an AIOps platform that applies artificial intelligence and machine learning capabilities to network traffic analysis. The solution analyzes downstream and transit traffic flows and helps enterprises identify peering opportunities, optimize their network routing, and gain more control over their service performance. They also offer network traffic engineering capabilities to maximize resource utilization and traffic delivery, and insights into network capacity to help drive cost-efficient traffic flow.*
- ***LogRhythm NetworkXDR*** *is a security-focused network traffic analysis solution that focuses on threat detection and analytics. It offers real-time network traffic analysis via network sensors that allow for distributed traffic data collection and reporting. The solution is designed to increase network traffic visibility with application identification, app-aware metadata, and full packet capture. NetworkXDR also integrates with LogRhythm's NextGen SIEM Platform to help identify security threats.*
- ***ManageEngine Netflow Analyzer*** *is a bandwidth monitoring tool that is built on network traffic monitoring and analysis functions. The program implements network flow analysis to examine bandwidth usage, network data, and traffic patterns. It condenses information about which users*

and devices are using available bandwidth on your network – as well as what they're using it for. The solution also feature network forensics and security features, application monitoring, and data capacity planning and billing capabilities.

- ***Netfort LANGuardian** is a network traffic analysis and packet inspection software that monitors network and user activity. LANGuardian uses packet inspection tools to troubleshooting bandwidth problems, create audit trails of file and folder activity, and examine Internet gateways. The solution uses wire data analytics to capture metadata from network packets, provides continuous health checks on network and user activity, and alerts admins to any suspicious data.*
- ***NETSCOUT** is a service assurance and network monitoring vendor that provides network traffic data inspection and analysis. The solution continuously inspects traffic data and analyzes large volumes of data through Layer 7/8 deep packet inspection, load balancing and acceleration, aggregation and desegregation, and packet decoding. NETSCOUT also utilizes their Adaptive Service Intelligence (ASI) technology that uses traffic data to gain visibility into user communities, services, and IT assets.*
- ***ntopng** is an open source network traffic probe and analysis tool. The traffic probe sorts network traffic into different criteria, including IP addresses and throughput. By characterizing network traffic, your enterprise can easily determine different network statistics that are affecting your network; the solution can reference real-time and historical traffic data in this analysis. While ntopng's Community version is open source, Professional and Enterprise versions are also available.*
- ***Paessler PRTG** is an IT monitoring tool that includes network traffic analysis functionality. PRTG's network traffic analysis system helps administrators track network capacity and seeing how much of their data analysis is actually being used. The solution combines SNMP monitoring, packet sniffing, and data flow technologies like NetFlow, IPFIX, jFlow, and sFlow for their traffic analysis capabilities; it displays traffic data alongside the other performance and security insights it uncovers.*
- ***Plixer Scrutinizer** is a network traffic analysis system that gathers network traffic flow and metadata across an entire network infrastructure. The solution collects data from SD-WAN, cloud, firewalls, routers, data centers, probes, data collectors, and wired/wireless edges. Scrutinizer then takes this data and provides valuable security and performance insights. This tool can help IT teams optimize network and application performance by providing end-to-end network visibility.*
- ***SolarWinds NetFlow Traffic Analyzer** is a NetFlow traffic analysis and bandwidth monitoring solution. The tool is designed specifically to analyze NetFlow traffic data as well as IPv4 and IPv6 flow records and application traffic. Users can also visually correlate performance and traffic data discrepancies by displaying metrics right next to each other. It also can integrate with SolarWinds' other Orion Platform products, such as their Network Performance Monitor and Network Configuration Manager.*
- ***Ipswitch WhatsUp Gold** is an all-in-one infrastructure monitoring tool that features network traffic analysis capabilities. WhatsUp Gold provides insight into application bandwidth usage and helps administrators to manage the performance of your infrastructure, applications, and services. It also leverages real-time and historical bandwidth usage data to help enterprises keep track of capacity, as well as determine what traffic was consuming bandwidth during a period of slow*

network performance.