FLOWTRAQ®

THE NETWORK VISIBILITY EXECUTIVE CHECKLIST

When you are responsible for the performance and security of the enterprise network, you need visibility into what's happening. There are a lot of technologies available on the market that claim to provide network visibility — and most of them do. But what exactly does "visibility" mean? And, more importantly, what characteristics of a visibility technology are critical to ensure your team has the right kind of visibility needed to do their jobs as effectively and efficiently as possible?

✓ VISIBILITY INTO DATA IN MOTION

Many organizations have good visibility into their data at rest via the logs collected by a security information and event management (SIEM) system. But organizations also need visibility into data in motion — to understand when data travels, where it travels to, and from where and how often it travels. Network traffic flow records are ideal for providing this level of visibility. Here are key requirements for a network flow monitoring tool:

— Full-fidelity data capture

Some systems sample incoming network traffic records which can provide faster processing, but this comes at a cost: gaps in the data that could reveal other threats to the integrity of the network. Instead, ensure that your network flow monitoring solution offers high-performance network traffic records processing without sampling.

— Support for all common flow formats

There are a variety of flow export formats, including NetFlow, sFlow®, IPFIX, CFlow, JFlow, and PCAP. Ensure that your network flow monitoring solution is compatible with all common flow formats, sampled or not.

— Support for IPv6

Ensure that your flow monitoring solution is fully IPv6-compliant and works seamlessly in IPv4/IPv6 networks.

✓ VISIBILITY INTO INSIDE THREATS

Many organizations focus on keeping bad guys out. But, as the breaches that continue to dominate the headlines demonstrate, there is unintentional and intentional bad behavior happening inside the network as well. You need to be able to identify compromises from within. Data loss prevention (DLP) systems are good at identifying structured sensitive data — such as social security numbers or credit card numbers — leaving the organization, but they can't recognize many other types of data exfiltration — such as encrypted data, confidential intellectual property, or insider information — that can have serious business, ethical, regulatory, and legal repercussions.

— Behavior-based intelligence

Identifying unexpected network behavior patterns — such as hosts receiving data outside of normal thresholds — enables you to detect a broad range of insider threats so you can quickly shut them down.

✓ VISIBILITY INTO WHAT HAPPENED IN THE PAST

Real-time visibility is important, but so is the ability to go back in time to determine what happened. The challenge is that you never know in advance how far back you may need to go, or what exact information you need to go back to.

— Full data recall

Ensure that your network flow monitoring system stores flow records instead of packets or aggregations — and that it retains full-fidelity data that goes back far enough to stage a meaningful incident response and forensic investigation.

✓ SUPPORT FOR TODAY-SIZED NETWORKS

There's no question that enterprise networks are larger and more complex than they've ever been. In today's era of big data, traffic volumes have exploded. And trends such as BYOD and networked-everything are changing the nature — velocity and variety — of the traffic traversing the network. These factors make visibility into what's happening on the network more important — and more challenging — than ever.

— Support for high traffic volumes

Ensure that your network flow monitoring system supports big, high-performance networks — networks with traffic flow rates of one million flows per second or more.

— Scalability

You also need to ensure your network flow monitoring system can support your network as it grows over time. Look for a solution that will seamlessly spread over multiple physical servers to give you unlimited processing power in a cluster.

✓ INTEGRATION WITH OTHER TOOLS

A good enterprise security strategy leverages a variety of tools and technologies — and this means that your visibility tools need to be able to integrate with those systems to create a seamless security infrastructure.

— Integration with SIEM systems

Ensure that your network flow monitoring tool can correlate anomalous traffic with system logs in your choice of SIEM.

— Integration with mitigation tools

Ensure that your network flow monitoring system integrates with DDoS and other mitigation tools, so that you can begin remediation immediately.

— Command-line tools and APIs

Ensure that your network flow monitoring system offers a complete set of command-line tools and APIs to provide you additional integration flexibility.

ABOUT FLOWTRAQ

FlowTraq® provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, botnets, worms, network scans and other network traffic anomalies. To request a free trial of FlowTraq, visit **www.flowtraq.com/trial**.

FLOWTRAQ®

16 Cavendish Court, Lebanon, New Hampshire 03766 USA
Phone +1 (603) 727-4477 | Email info@flowtraq.com | www.flowtraq.com