Network Forensics Buyer's Guide

Network forensics–the recording and analysis of network traffic–is a powerful tool for finding proof of security attacks, and it has become an essential capability for any organization interested in monitoring and troubleshooting 10G and 40G networks.

What should you look for in a Network Forensics solution? From data recording to in-depth analysis, this Buyer's Guide lists the features you need and the ramifications you should consider.

Savvius, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
925.937.3200
www.savvius.com

Why SMBs and Enterprises Need Network Forensics 3
Why Has Network Visibility Decreased? 3
Limitations of Flow-based Solutions...3
The High Cost of Downtime..4
Why Network Forensics Has Become a “Must-Have” Security Tool...4

Network Forensics Defined...5
Use Cases...5
Solution Components 5

Network Forensics Checklist 6
Data Recording 6
Data Storage 8
Data Analysis...9

Savvius Network Forensics Solutions 11
Learn More...11

Why SMBs and Enterprises Need Network Forensics

It's ironic: Enterprises are doing more with networks than ever before, but most IT organizations have decreasing visibility into network traffic.

Today's networks support everything from database transactions to video conferences to Web traffic to interactive maps. Media is richer and more interactive.[1] The popularity of mobile devices has led to new types of business applications, as well as more devices and a greater diversity of devices accessing the network. Enterprise networks have never carried such high volumes of diverse traffic to so many different types of devices before.

Why Has Network Visibility Decreased?

So why has IT organizations' visibility into this rich mix of application traffic diminished? The primary reason is speed. At the same time that applications have become richer, networks have become faster. 10G network ports have become the de facto standard for new network investments, and some enterprises are even beginning to deploy 40G and 100G ports.[2] Unfortunately, the volume of traffic on these faster networks outstrips the data collection and analysis capabilities of traditional network monitoring tools. Network analyzers that were originally developed for 1G or slower networks end up dropping packets or reporting erroneous results when tasked with monitoring today's high-speed networks.

This analytical shortfall has not gone unnoticed by IT organizations. In a recent survey by TRAC Research, 59% of IT decision-makers expressed concern about their network analyzers dropping packets, and 51% questioned the reliability of the traffic that their network analyzers were capturing.

> 59% of IT decision-makers are concerned about network analyzers dropping packets, and 51% question the reliability of the traffic being captured.

Limitations of Flow-based Solutions

Many organizations have chosen to skirt the problem of capturing high-speed traffic by dispensing with detailed analysis of traffic altogether, and making do instead with high-level flow statistics and traffic sampling. Flow-based systems, such as those based on NetFlow and sFlow, can usually keep up with high-level traffic. They provide a general picture of traffic activity that's good enough for monitoring bandwidth utilization and application performance.

However, the imprecision of flow-based analysis can be a real obstacle when IT engineers have to troubleshoot network outages or find proof of a security attack so that the attack can be quickly characterized and stopped, and the damage assessed. For investigations like these, access to complete traffic down to the packet level is invaluable. Without complete access to the traffic itself, IT organizations too often end up hunting in the dark.

[1] Cisco predicts that by 2015, 62% of consumer Web traffic will be voice and video. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf

[2] Shipments of 10G, 40G, and 100G grew 62% in 2013, according to Infonetics. 10G ports comprised the majority of these shipments. http://www.infonetics.com/pr/2013/2H12-Networking-Ports-Market-Highlights.asp

The High Cost of Downtime

To judge whether this high-level hunting is operationally sufficient or financially prudent, consider the duration and cost of the Mean Time to Resolution (MTTR) reported by most IT organizations in the TRAC Research survey:

- 48% of organizations typically spend over 60 minutes per incident diagnosing network problems.
- Organizations lose $72,000 on average for every minute of network downtime.

If a network incident results in network downtime and requires an hour of troubleshooting, the affected organization loses $4,320,000 on average. Even if taking into account lost productivity and other results, the downtime ends up costing only half this much, the cost is still high enough to compel many IT organizations to find a better way to troubleshoot networks.

Why Network Forensics Has Become a "Must-Have" Security Tool

Besides network performance and productivity costs, there's another reason for IT organizations to ensure they can analyze traffic in detail: security.

The increasing sophistication, stealth, and financial cost of security attacks should compel any reasonable IT organization to seek greater visibility into network traffic. Unlike the spam deluges and obvious worm attacks of the past, today's security attacks are subtle, highly targeted, and difficult to detect. High-level flow data will not help IT engineers find a small rootkit that is quietly "exfiltrating" confidential data at a trickle to a remote server. IT organizations must now defend against determined, crafty, and patient criminal syndicates and hackers who are intent on stealing intellectual property, personal information of customers and employees, and gaining access to financial controls.

> About 85% of organizations have experienced data breaches.

Recent security surveys paint a bleak picture:

- The vast majority—92%—of data breaches are perpetrated by outsiders.
- The motivation for 75% of these breaches is financial gain.[3]
- About 85% of organizations have been experienced data breaches.
- A study of 56 large companies in 2012 discovered 1.8 successful cyberattacks per week per company.
- Average annualized cost of cybercrime per company in 2012 was $8.9 million, ranging from $1.4 million to $46 million.[4]

How can IT organizations get access to the details that make network analysis and network troubleshooting more fruitful, so they can quickly troubleshoot problems and find and stop security breaches? If high-level flow statistics won't provide the necessary detail analysis, what type of solution will? The answer is network forensics.

[3] *Verizon 2013 Data Breach Investigations Report*, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

[4] https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Network Forensics Defined

Network forensics is the collection, storage, and analysis of network traffic. It’s an analytical practice that uses network recorders to capture live network traffic and copy it to high-performance disk arrays, so that recorded traffic can be searched, investigated, and if necessary benchmarked and logged.

Use Cases

IT organizations can use network forensics for:

- **Network performance benchmarking** for detailed reporting on network performance, business activities, resource allocation, and other purposes.
- **Network troubleshooting** for resolving any type of network problem, especially those that happen intermittently.
- **Transactional analysis** for providing the “ultimate audit trail” for all kinds of transactions, including ecommerce and banking transactions. When server logs and other server-based evidence does not provide sufficient data for characterizing a transaction, network forensics enables IT organizations to locate and examine the exact content and execution of an online transaction.
- **Security attack analysis** for enabling security officers and IT staff to characterize and mitigate an attack that slipped past network defenses. Network forensics enables investigators to find proof of an attack and to trace its effects on IT resources.

Solution Components

A network forensics solution typically includes:

- **A network recorder**, an appliance configured with disk storage and Network Interface Cards that connect to network ports and record their traffic.
- **A network analyzer**, a powerful software application that provides tools for searching through and analyzing recorded traffic. Ideally, the network analyzer should be able to export data for reporting and make it easy for various IT experts to collaborate on resolving problems with network performance or security.

Many solutions combine a network recorder and a network analyzer in a single hardware appliance.

Network Forensics Checklist

The remainder of this document presents a checklist of features that SMBs and large enterprises should look for in a network forensics solution.

Features are organized in the following categories:

- Data Recording
- Data Storage
- Data Analysis

Data Recording

Data recording involves capturing network traffic from live network segments and copying it reliably to disk. Data recording must be fast and accurate. It must never interfere with the transmission of the traffic being recorded.

❑ **Loss-less packet capture up to 25G**

The solution should be able to capture traffic—all packets of all flows, not just high-level flow statistics—reliably at rates up to 25G, the equivalent of a full-duplex 10G link in both directions. It should never drop packets. Statistics must always be accurate, even when network segments are experiencing high utilization.

❑ **Comprehensive collection of data types**

The solution should be able to collect all types of network traffic, including HTML, CIFS, VoIP, and video. IT engineers must never find themselves unable to diagnose a problem because a network forensics solution could not record a particular protocol or traffic flow.

❑ **Complete data collection**

The solution should be able to record complete network traffic, including packet headers and packet payloads.

❑ **Flexible data collection**

IT engineers should be able to customize data collection to focus on specific attributes, such as traffic on a specific segment, to or from a specific group of users, using a specific protocol, and so on.

❑ **Multiple simultaneous collections**

IT engineers should be able to run multiple, independent traffic captures simultaneously. For example, engineers should be able to run a continuous capture of all network traffic, a custom capture of just traffic involving an email server, and a custom capture that is triggered only when specific conditions are met. Data from each capture should be stored in separate files for ease of analysis.

❑ Data collection initiated by alerts and triggers

IT engineers should be able to define conditions that would automatically trigger the collection of traffic. Collection parameters should be customizable. For example, IT engineers should be able to trigger the collection of SMTP traffic if an email server suddenly starts sending out email whose volumes rises above a specified threshold.

❑ Ability to capture from multiple NICs simultaneously in a single appliance

To spare IT organizations the expense of provisioning a separate appliance for each type of network port being monitored, a single network forensics appliance should be able to be configured with different speed NICs. For example, an IT organization should be able to deploy a single appliance to monitor a 1G network and a 10G network.

❑ Support for on-the-fly capture filters

IT engineers should be able to create and apply custom filters to capture and analyze specific types of traffic on the fly. For example, if VoIP services suddenly need extra attention, they should be able to dynamically define and apply filters to select VoIP traffic for special analysis without having to start a new capture.

❑ Support for filtering and packet slicing in hardware

To eliminate the computational overhead of capturing traffic not required for the requested forensic analysis, the solution should support hardware-based filtering and packet slicing. After filtering data, the solution should be able to slice packets to further reduce the amount of data uploaded to the CPU. Slicing parameters should be configurable, so that packets of varying encapsulations and header lengths can be sliced at the appropriate points.

❑ Support for hardware timestamping

The solution should timestamp traffic to a high precision (~10ns) in hardware so that forensics analysis can accurately measure traffic latency. Latency measurements are especially important for analyzing VoIP and video traffic.

Data Storage

A network forensics solution must be able to store enough traffic to meet the post-capture analysis needs of the IT organization. For some organizations, this might entail preserving one day of traffic; for others, it might entail preserving multiple days of traffic.

❑ **High performance storage**

The solution should be able to record and store traffic at rates of at least 20G–the equivalent of a full-duplex 10G link in both directions–with zero data loss. For 40G networks, even higher data rates should be supported. No packets should be dropped when writing data to storage, even when network segments are experiencing high utilization.

❑ **Scalable storage**

The system should scale easily to support tens or hundreds of terabytes of traffic. It should also support the on-the-fly addition of external storage systems such as SANs or JBODs (external storage systems).

❑ **Cost-effective Storage**

Storage should be cost-effective and affordable. Inefficient storage not only raises hardware costs; it also consumes more rack space and raises cooling and electrical costs.

❑ **Exportable storage formats**

However the data is stored, it should be able to be exported easily to other systems for reporting and further analysis.

Data Analysis

Fast, easy-to-use, and intuitive search and filtering tools are essential. Capturing and storing data is meaningless if IT engineers cannot search through that data (potentially tens of terabytes of data) quickly and efficiently to identify the root cause of problems, discover proof of security attacks, and perform other types of forensics investigations.

❑ **Real-time statistics that help IT engineers quickly identify and zero in on network problems**

In a recent survey of network engineers and IT directors about the challenges of analyzing 10G and faster networks, 65% of respondents identified the need for real-time statistics as a top concern.[5] Real-time statistics should include Top Talkers, Top Protocols, Most Delays, and related metrics.

❑ **Ability to quickly search through and filter data**

The solution should enable IT engineers and security experts to quickly sort through vast amounts of recorded data to pinpoint the root cause of problems and to find proof of attacks. In a recent survey of enterprise IT organizations about the challenges of monitoring 10G networks, 40% of respondents cited the length of time required to perform detailed analysis as a major challenge.[6] The solution should address this challenge with powerful, easy-to-use search tools and filters.

❑ **Support for frame decodes**

The solution should be able to pre-parse and recognize common Ethernet-based protocols, extracting information for use in filters, slicing, and packet descriptors. Frame decodes are important when analyzing traffic using VLANs and MPLS encapsulation.

❑ **Support for Expert analysis that explains the context of network activity, accelerating IT engineers' interpretation of data**

The solution should provide Expert analysis that explains the context of network activities, alerting IT engineers to problematic network conditions and explaining away common network activities.

❑ **Ability to drill down to individual packets**

IT engineers should be able to examine the individual packets of any captured traffic.

❑ **Ability to reconstruct media such as Web pages and Word files**

To investigate HR issues, security issues, and other types of issues involving content, IT engineers should be able reconstruct media such as Web page and Word files and view them as end users did.

❑ **Ability to organize flows by application type**

IT engineers should be able to organize flows by application type. The solution should also support application tagging, so that it's easy to identify and track traffic associated with critical applications such as Oracle Financials, NetSuite, and SAP.

❑ **Ability to organize flows by client/server pair**

IT engineers should be able to organize flows by client/server pairs in order to more easily analyze traffic patterns, application latency, and other issues related to client/server communications.

[5] *The State of Faster Networks*, Savvius, October 2013.

[6] *Ibid*.

❑ **Ability to quickly isolate flows for a specific user, application, or protocol**

IT engineers should be able to quickly isolate traffic when a specific user, application, or protocol is suspect.

❑ **Support for filtering flows by relationships (through a “Select Related”-style functionality)**

To explore patterns, IT engineers should be able to filter data by relationships. For example, if a specific server is suffering performance problems, IT engineers should be able to quickly filter traffic and isolate flows going to and from that server.

❑ **Support for full VoIP analysis**

VoIP analysis should include complete signaling and media analyses, as well as a Call Detail Record (CDR), providing full visibility into calls and video streams as well as comprehensive, real-time statistical and quality-of-service reports for baselining.

❑ **Peer maps**

The solution should provide peer maps that provide a graphical representation of all active network conversations. peer maps should be configurable, so that IT engineers can zero in on communications between specific devices over specific periods of time.

❑ **Reporting**

The solution should support reporting and information sharing. IT engineers should be able share data and collaborate on analysis. They should also be able to generate reports for line-of-business managers, compliance officers, and auditors.

Savvius Network Forensics Solutions

Savvius provides network forensics solutions that enable SMBs and enterprises to monitor, analyze, and troubleshoot 1G, 10G, and 40G networks. Savvius network forensics solutions feature award-winning OmniPeek® network analysis software and the Omnipliance family of network analysis and recorder appliances.

Each Omnipliance continuously captures, stores, and analyzes data at a remote location, and gives IT engineers real-time and post-event visibility into every aspect of network activity, including Ethernet, 1/10/40 Gigabit, and voice and video over IP. Omnipliances are engineered to meet the technical demands of monitoring and analyzing high-speed networks. They provide loss-less data capture at speeds up to 25 Gbps and rapid analysis through highly flexible filtering and powerful search tools.

For more information, please visit www.savvius.com or call +1 (925) 937-3200.

Learn More

You'll find white papers and other resources about network forensics here:

http://www.savvius.com/learn