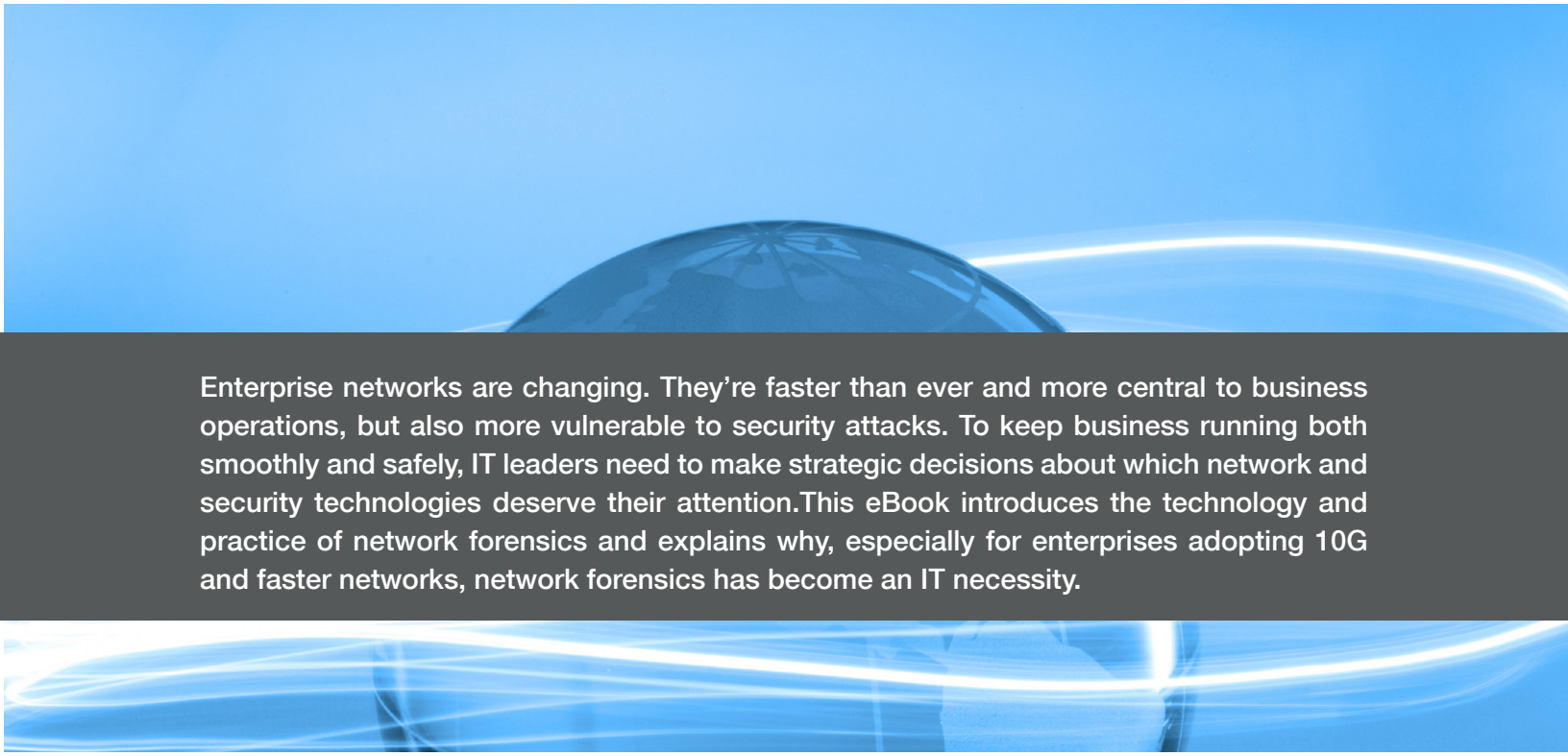
Business Benefits of Network Forensics

AN EBOOK FOR IT LEADERS
AND EXECUTIVES



Enterprise networks are changing. They're faster than ever and more central to business operations, but also more vulnerable to security attacks. To keep business running both smoothly and safely, IT leaders need to make strategic decisions about which network and security technologies deserve their attention.This eBook introduces the technology and practice of network forensics and explains why, especially for enterprises adopting 10G and faster networks, network forensics has become an IT necessity.

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

Executive Summary

In recent years, business networks have changed in three important ways. They're faster than ever. They connect to more devices, in part because so many workers are carrying multiple mobile devices. And a growing share of network traffic consists of rich media such as VoIP and video that is highly sensitive to network delays.

In addition to being faster, more connected, and voice- and video-centric, networks have also become more difficult to troubleshoot and secure. In part, this is because today's networks, which run at 10G[1] or faster, simply transport too much data for traditional network monitoring and troubleshooting tools to collect and analyze reliably. To get by, analysis tools end up relying on sampled traffic and high-level statistics. Unfortunately, samples and statistics lack the details and hard evidence that IT engineers need for quickly troubleshooting problems and characterizing security attacks.

Network downtime is costly. About half of organizations spend an hour on average troubleshooting each performance problem and, once all expenses are tallied, that hour of investigation ends up costing the organization nearly $4,320,000.[2]

Costly downtime isn't the only problem. Operating with reduced network visibility weakens an organization's defenses against IT security attacks, especially those designed to lurk on internal networks and steal confidential data. Data breaches can abet fraud, ruin reputations, and cost millions of dollars in regulatory penalties and lost competitive advantage.

How can enterprises regain visibility into their fast, vulnerable networks? Through network forensics. Network forensics is the recording, storage, and analysis of network traffic. It provides a complete record of network communications, along with powerful search and analysis tools for combing stored traffic to find critical information.

Network forensics provides these important benefits to enterprises:

- Faster troubleshooting, which reduces downtime and increases employee productivity
- Faster characterization and remediation of security attacks
- Better utilization of network resources through better reporting and planning
- Reduced exposure to regulatory penalties and fines

Enterprise leaders should recognize that network forensics has become an essential IT capability to be deployed at every network location, providing ubiquitous 2/47 visibility into business operations, network performance, and IT risks.

1 10G is 10 Gigabits per second, which is roughly 1.25 GB/sec or 10 times more data than "fast" networks carried a decade ago.
2 TRAC Research, 2013.

Introduction

We wrote this ebook to give IT and business decision-makers a clear, concise look at some important aspects of enterprise networks today, and to help them understand the role that network forensics can play in addressing issues like network security and network uptime.

If you would like to learn more about network forensics, please explore our Network Forensics resources at:

www.savvius.com/learn

This portal offers white papers, recorded Web seminars, industry reports, and a buyer's guide.

If you have questions about forensics or comments on this ebook please drop us a line at **forensics@Savvius.com**.

Now let's get started with a look at enterprise networks.

Enterprise Networks Today

How are today's networks different from those of just a few years ago?

Here are three important differences. Today's networks are:

- **Faster than ever.**

  For several years now, enterprises have been upgrading their networks, buying network ports, routers, and other gear that supports exponentially greater bandwidth. A few years ago, 1G networks were the norm. Now most enterprises are investing in 10G networks: 10G network ports make up 75% of high-speed (10G+) port purchases, the remainder consisting of 40G and 100G ports.

- **Connecting to more devices and more types of devices.**

  A decade ago, enterprise networks mostly connected desktop PCs to servers. In today's Bring Your Own Device (BYOD) world, nearly all employees are carrying mobile devices, and not just one or two: the average in 2012 was 2.9 devices per user.[3] Traffic to and from a desktop PC has now become traffic to and from a smartphone, a tablet, and a laptop, all of which are likely running different operating systems (usually a mix of Windows, OS X, iOS, and Android). All these devices may also be regularly exposed to public networks such as Wi-Fi hotspots. According to Cisco, about a quarter of consumer IP traffic originated with non-PC devices in 2012. By 2017, the non-PC share of consumer IP traffic will grow to about half.[4]

- **Carrying richer media.**

  Visit just about any enterprise Web site, and you'll be reminded of the prominence of video content in business today. Here's another reminder: the second most popular search engine isn't Bing; it's YouTube.[5] Of course, video isn't the only rich media traversing enterprise networks. By now, nearly all business phone systems run on VoIP. Cisco predicts that by 2015, 62% of consumer Web traffic will be voice and video.[6]

> *"While 1G port revenue is actually declining due to commoditization and becoming a standard feature on network equipment, we expect high-speed (10G+) port revenue to double by 2017, to over $42 billion."*
>
> *–Mattias Machowinski*
> *Directing Analyst, Enterprise Networks and Video*
> *Infonetics Research*

3 http://nakedsecurity.sophos.com/2013/03/14/devices-wozniak-infographic/
4 http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf
5 http://socialmouths.com/blog/2013/02/12/youtube-in-2013/
6 http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf

Three Big Problems

Enterprise computing is more convenient and powerful than ever before. 1G, 10G, and faster networks carry rich media, Web services, and more, enabling us to connect easily to business data and colleagues via smartphones, tablets, and laptops.

But IT managers and other executives need to consider three important problems with these fast, hyperconnected networks.

The High Cost of Downtime

When business runs on the network, network degradations and outages can be expensive. Speeding up networks makes them more difficult to monitor and increases the volume of traffic affected by every minute of downtime.

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.

Organizations lose $72,000 on average for every minute of network downtime, according to TRAC Research.

Increased Security Threats

A decade ago, the most common network security threats were deluges of spam or malware such as worms that might congest a network or interrupt IT operations.

Today's security threats are more subtle, more sophisticated, and more pernicious. Instead of blatantly interrupting services or peddling foreign pharmaceuticals, today's security attacks are designed to slip unnoticed onto a network and spend days or weeks prowling for data, such as product plans or customer records. This data is then "exfiltrated" at a low-volume trickle to remote command-and-control centers, which might be located in a foreign country. No longer content with cybervandalism, today's attackers are seeking to steal intellectual property, which can be sold on the black market, and confidential data that can be used for identity theft and financial fraud.

Recent security surveys paint a bleak picture of IT security:

- The vast majority—92%—of data breaches are perpetrated by outsiders.
- The motivation for 75% of these breaches is financial gain.[7]
- About 85% of organizations have 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.[8]

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.

Verizon's *2013 Data Breach Investigations Report* found that 66% of breaches took months or longer to discover.[9] **IT organizations seem to lack the tools necessary to adequately investigate and stop data breaches that threaten to cost organization's hard cash, competitive advantage, or both.**

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

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

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

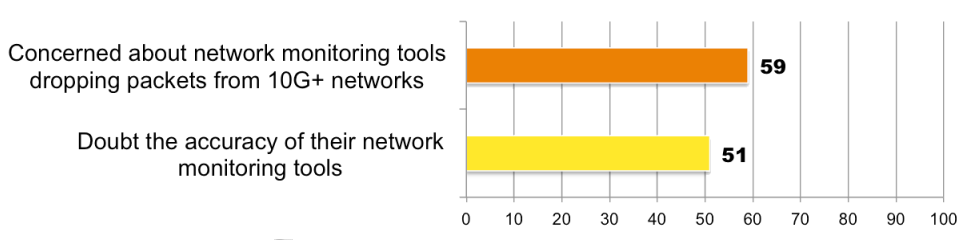
Reduced Visibility

Ironically, just when enterprises are doing more with their networks than ever before, most enterprise IT organizations are finding they have reduced visibility into network activity. They can still see high-level statistics based on general trends and application flows, but they can no longer dive into the details that can be crucial for troubleshooting problems or tracking down security breaches.

The problem comes down to throughput. Most traditional IP packet-level monitoring tools that IT engineers used to look closely at network traffic simply can't keep up the high bandwidth traffic of 10G and faster networks, even if those networks are running only at half their theoretical capacity. Because they can't keep up, they drop packets, and they skew the results they report.

Many IT departments have noticed the problem. In a recent survey by TRAC Research, 59% of IT respondents expressed concern about their network monitoring tools dropping packets instead of reliably recording high-speed traffic for analysis. Similarly, 51% of respondents doubted the accuracy of the data being presented by their network monitoring tools.

The bottom line: networks are doing more, but IT is seeing less.



Reduced visibility can be costly to business. Degraded network performance can reduce employee productivity. IT may find it difficult to optimize application services without adequate visibility into network events.

Network Forensics: Visibility of Every Network Location at Every Moment and at Every Network Speed

Network Forensics Defined

To monitor and troubleshoot high-speed networks, to minimize network degradations and downtime, and to find proof of elusive security attacks.

Enterprises need dramatically improved network visibility in order to:

- Monitor and troubleshoot networks, especially 10G, 40G, and 100G networks that outpace traditional monitoring tools
- Minimize costly network degradations and downtime
- Find proof of elusive security attacks so they can be understood and stopped.

To get that visibility, enterprises should invest in network forensics.

Network forensics is the recording, storage, and analysis of network traffic. A network forensics solution records network traffic, stores it in a searchable repository, and provides IT engineers with filters for mining stored data to discover and analyze network anomalies. Using network forensics, IT engineers can discover both the cause of an anomaly and its effects on IT services and IT assets such as servers and databases.

Think of network forensics as the 'network time machine' that enables you to replay, re-examine, or closely analyze traffic so you can identify the cause of performance problems and uncover the source of security attacks.

How far back will this time machine travel? It depends on how much storage you allocate and how much bandwidth your network traffic typically consumes. A best practice, though, is to record data for multiple days, so that a security attack that begins on Friday night can still be detected and analyzed in detail on a Monday morning.

> *"Packet monitoring really is the most definitive, most complete source of performance data you can get for managing networks and for troubleshooting in particular."*
>
> — *Jim Frey*
> *Managing Research Director*
> *Enterprise Management Associates, Inc.*

The Importance of Packet-level Analysis

Network forensics does more than simply give you high-level summaries of network events. It gives you the traffic itself: every packet that traversed the network. And it makes this traffic available to you through a variety of search tools and filters, so you can examine it in multiple ways and pinpoint the network packets that interest you.

Use Cases for Network Forensics

With Savvius Network Forensics solutions in place, you can conduct various types of forensic investigations:

- **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 occur 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.

Performance Analysis and Troubleshooting

- Capture and analyze intermittent network problems
- Troubleshoot problems that occurred hours or days ago
- Find patterns that ad hoc, reactive troubleshooting will miss

Transaction Analysis

- Create the ultimate audit trail for business transactions—not just server activity but the business transactions enacted by clients and servers
- Troubleshoot the transaction problems that server logs miss

Compliance

- Find evidence of network activities that violate relevant industry regulations, such as HIPAA for healthcare organizations and Gramm-Leach-Bliley for financial services firms.
- Find evidence of user activity that violates HR policies and other company guidelines.

Security Attack Analysis

- Find proof of attacks—whether they've just begun or occurred days ago–so that IT engineers and security teams can understand the attacks and stop them
- Apply filters to isolate malicious behavior
- Equip your network IT team with a powerful incident response tool

Case Study: Using Network Forensics to Pinpoint a Security Attack

Here's a true story about how network forensics helped an enterprise IT team discover the scope and modus operandi of a security attack.

A security tool installed on the network raised an alert about unusual activity on a server. When the IT team investigated, they discovered that the server had been compromised by a security attack. Unfortunately, the security tool provided no further information about the attack, such as who the culprit was and which other systems might also have been compromised. This vague nature of this alert is quite common. Security tools might detect an anomaly, but to thoroughly understand the nature and scope of an attack, IT engineers need to investigate matters themselves.

To start their investigation, the team turned to their network forensics system, which had recorded network traffic before, during, and after the attack. Using a dashboard (in this case, Savvius Compass), the team discovered that the compromised system had initiated a spike in Common Internet File System (CIFS) traffic shortly after the attack had begun. (CIFS is an network protocol used by Windows computers to manage access to files and printers.)

To learn more about the systems involved in the CIFS spike, the team opened a Peer Map, showing a visual record of all the network communications that took place during the period in question.

The Peer Map confirmed that the compromised server had communicated with several other systems.

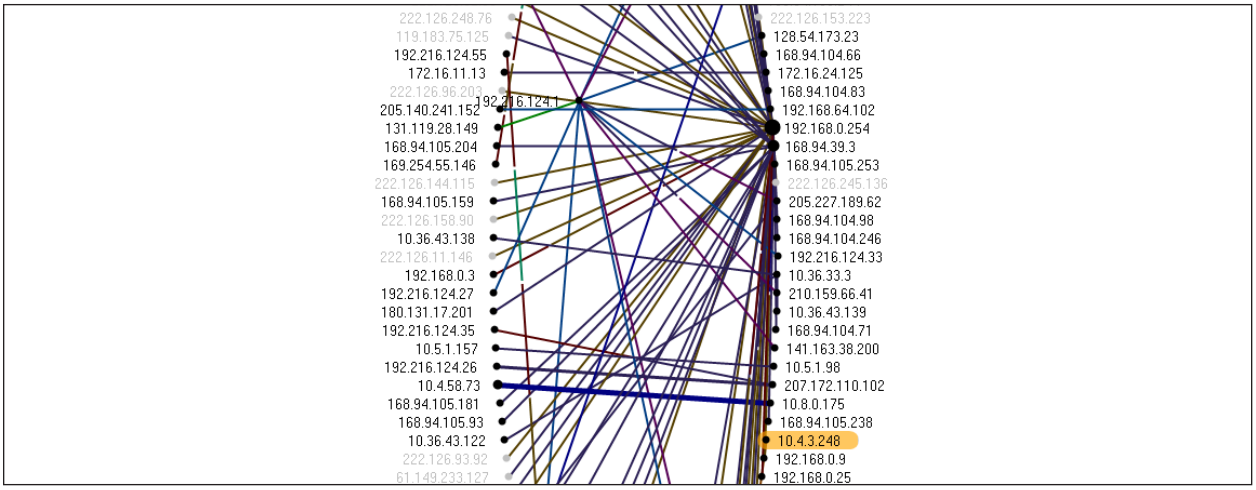


Figure 1. A Peer Map illustrates all network conversations during a selected period of time.

Next the team filtered traffic to show communications only from the compromised server. This made it easy to identify the three other systems that the compromised server had communicated with after the attack.

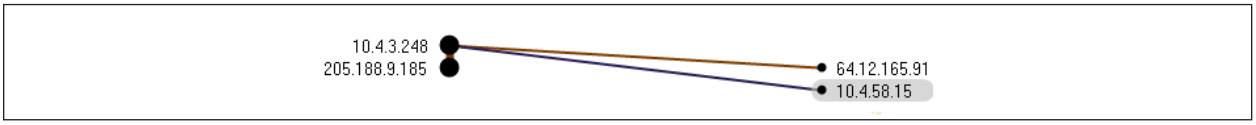


Figure 2. Filtering on the Peer Map made it easy to identify the addresses of the systems with which the compromised server had been communicating. Network forensics provided critical information that security tools overlooked.

Now the IT team knew which servers to focus their attention on in their efforts to contain the attack and reverse its effects. In addition to quarantining and repairing the server that was initially attacked, the IT team quarantined the three other infected servers, as well.

Working from a vague security alert, the team was able to use network forensics to identify specific systems to quarantine and where to focus attention on cleaning up the attack. Network forensics enabled the team to find proof of the attack and trace its effects.

☛ To read other network forensics case studies, see the Savvius white paper *Real-World Security Investigations with Network Forensics*, which is available on www.savvius.com.

A Network Forensics Solutions Checklist

Solution Components

A network forensics solution typically includes:

- **A network recorder**, an appliance configured with disk storage and Network Interface Cards (NIC) 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.

Solution Capabilities

A network forensics solution needs to provide powerful, precise, and cost-effective capabilities for each aspect of network forensics:

- **Data Recording**
  The solution should be able to capture traffic—all packets of all flows for all network protocols, not just high-level flow statistics—reliably at rates up to 20G, the equivalent of a full-duplex 10G link. It should never drop packets. Statistics must always be accurate, even when network segments are experiencing high utilization. The solution should support multiple independent data captures, and it should enable captures to be initiated by policy triggers, so that when certain conditions occur, relevant traffic is automatically recorded.
- **Data Storage**
  The solution should be able to record and store traffic at rates up to 20G, the equivalent of a full-duplex 10G link, with zero data loss. No packets should be dropped when writing data to storage, even when network segments are experiencing high utilization. The system should scale easily to support tens or hundreds of terabytes of stored traffic. It should also support the on-the-fly addition of external storage systems such as SANs or JBODs (external storage systems).

- **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.

  ☛ For a detailed list of solution requirements, see Savvius *Network Forensics Buyer's Guide*, which is available on www.savvius.com.

Best Practices

Network forensics gives your IT team, your security team, your HR department, and your legal and compliance teams comprehensive evidence for investigating anomalies and resolving crises. By following the best practices below, you can ensure that your organization realized the full potential of network forensics.

Best Practice #1: Deploy Network Recorders that Can Reliably Capture Your Network's Traffic for Multiple Days

It's a good idea to benchmark network recorders before deploying them. Some vendors promise high-speed performance, but fail to capture traffic reliably when bandwidth utilization reaches 10G or higher.

☛ For Miercom's third-party lab test and benchmark analysis of Savvius Omnipliance TL network forensics appliance, visit www.savvius.com.

Best Practice #2: Capture Traffic at Every Location

To facilitate network troubleshooting, strengthen network security, and support compliance, IT organizations should capture traffic at every location, not just as the network core.

Consider the case of a large enterprise that suffered a security attack at a branch office. The breach spread from the branch office to headquarters. Without a detailed analysis of the traffic in the branch, the IT organization would have been unable to identify the source of the attack and apply the appropriate controls to prevent its spread.

Best Practice #3: Capture Traffic 24/7

In addition to capturing traffic at every location, IT organizations should ensure that they capture traffic around the clock, so that even anomalies that occur outside of business hours can be investigated.

Best Practice #4: Take Baseline Measurements of Network Performance

To get a sense of "normal" conditions before trouble arises, IT engineers should take baseline measurements across specific network traffic such as HTTP, VoIP, and key business applications over typical cycles, such as an hour, a day, and a week, for the network as a whole.

Best Practice #5: Set Filters to Detect Anomalous Behavior

In addition to maintaining a continuous, days or week-long capture of all network traffic, it's often helpful to define a secondary capture consisting only of network anomalies that may signal a security violation. If no anomalies occur, then no secondary capture is initiated and no alerts are raised. But if anomalies occur, IT engineers and security experts can take advantage of the evidence in a small capture file containing just the relevant data.

☛ For a longer, more detailed list of network forensics best practices, read the Savvius white paper, *Best Practices for 10G and 40G Network Forensics*, which is available on www.savvius.com.

Summing Up and Looking Ahead

By continuously capturing network traffic for analysis, network forensics solutions ensure that enterprises are always ready to analyze and investigate performance problems, security threats, and other network anomalies–even on today's cutting-edge high-speed networks.

With faster troubleshooting and faster remediation of security attacks, your organization can:

- Reduce network downtime and increase employee productivity
- Reduce exposure to security attacks and regulatory penalties from data breaches
- Make better use network resources based on a better understanding of network utilization

Asking Critical Questions

How can network forensics help your own organization?

When evaluating your organization's IT strengths, weaknesses, strategies, and potential investments, you may find it useful to consider these critical questions:

- What capabilities are in place today for investigating network performance problems, HR violations involving network communications such as email and chat, and security attacks?
- Are we capturing traffic at every location to ensure that we can troubleshoot problems and characterize security attacks quickly?
- If one of our servers was attacked, would we be able to quickly identify all the devices with which that server subsequently communicated? If so, how, and how long would the investigation likely take?
- If the organization's most confidential data were leaked, what consequences would result? Are we satisfied with our current security defenses and investigative capabilities for mitigating such a leak?
- If we are planning to increase the speed and bandwidth of our networks, are we also planning to increase IT's ability to monitor and analyze those networks? Have we audited our current network monitoring and network analysis tools to determine which, if any, might become obsolete in light of trends such as high-speed networks, the growth of rich media such as VoIP and video, and increased endpoint communications and security exposure through the use of personal mobile devices in the office?

By answering these questions, you and your organization can make critical decisions about network forensics, security, application delivery, and employee productivity.

About Savvius

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 25Gbps and rapid analysis through highly flexible filtering and powerful search tools.

Savvius Vigil™ is he industry's first appliance capable of intelligently storing months of packet-level information to enhance security investigations. With Savvius Vigil, packets related to a breach can be examined weeks or months after the incident occurs. This detailed network information is often vital to a full understanding of the threat.

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

More Resources

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

http://www.savvius.com/learn