FLOWTRAQ®

WHITE PAPER

# YOU GOTTA KEEP UP:

## THE NECESSARY EVOLUTION OF NETWORK SECURITY TOOLS

Security breaches and hacks don't happen in a vacuum. But it's important to remember that behind every attack, there's a human adversary. Whether it's an insider, a script kiddie, a hacktivist, a foreign government, or a cyber criminal — there is intent. Computer security tools need to properly equip information security professionals to defend their networks.

Today's networks are complex and handle ever-increasing volumes and sources of data, which creates a lot of noise and makes it very difficult to identify real threats. When you factor in the continuous innovation and increasing sophistication of attackers, yesterday's security tools just don't cut it — not even close. Even today's state-of-the-art security technologies need to evolve to address changes and shifting requirements when it comes to data volumes, awareness, and insight.

## DATA VOLUMES: FROM CHALLENGE TO ASSET

According to a recent report by Cisco, "By 2016, global IP traffic will reach 1.1 zettabytes per year, or 88.4 exabytes (nearly one billion gigabytes) per month, and by 2019, global IP traffic will reach 2.0 zettabytes per year, or 168 exabytes per month."[1]

Any security tool — any network tool, in fact — must be able to handle today's data volumes. And tools that were developed in "the good old days" weren't architected from the ground up to handle today-sized networks. This isn't due to a mis-step on their part — the big data technologies simply weren't yet available. Unlike modern-day systems with multiple processors that allow you to scale based on increasing bandwidth needs, many older systems just can't keep up — even if you buy more and more of them — and you have to make tradeoffs, such as **sampling data**. But you shouldn't have to choose between speed and scalability.

The good news is that data isn't just a challenge to be addressed; it has the potential to be an asset to be leveraged. With today's volumes, it's impossible to correlate and analyze all of the available data in any meaningful way using traditional reports. Machine learning, which can take vast quantities of data and use it to provide actionable insight, is being used today in industries like e-commerce, financial services, and technology to build business value. When applied to network security, this approach gives data the power to transform the way network security is managed.

## AWARENESS: FROM MONITORING TO VISIBILITY

Security tools are designed to deliver awareness about the security of the network. But there are varying types of awareness, and it's important to understand the difference. Some security tools provide monitoring, which is the

[1] Cisco, The Zettabyte Era — Trends and Analysis, May 2015

process of watching for specific conditions and fixing them when they occur. Monitoring is useful, but only if you know exactly what you should be looking for. Visibility, on the other hand, is about understanding what is happening on your network — having multiple vantage points from which you can observe what is happening now and learn from what has happened in the past. Visibility helps prepare you for dealing with the unknown.

Visibility is required to quickly identify "events," which are anomalies in the data such as a failed login attempt or an IDS alert. But an individual event is only a signal, and it needs to be collected together with other related events that represent an incident, such as a series of failed login attempts from one source that could represent an attempted breach.

The nature of today's threats demand real-time visibility into what's happening on the network. **And because time is of the essence when there's a breach**, you need to be able to identify incidents and drill down as far into the details as necessary so you can quickly assess the nature and scope of the problem and immediately begin to formulate a mitigation strategy.

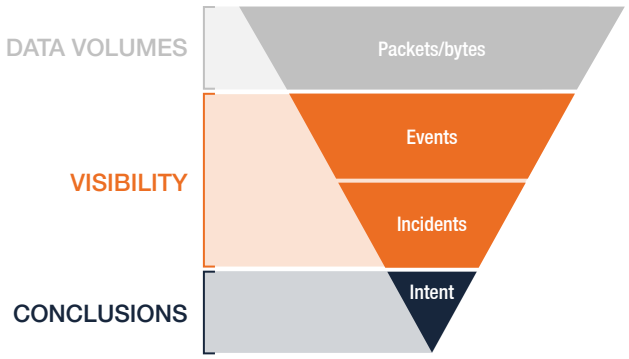
Sometimes you need to go back in time to determine what happened, so forensic visibility is also important. Because you don't know in advance how far back you may need to go, or what exact information you need to go back to, you need full historical data recall that goes back far enough to stage a meaningful incident response and forensic investigation.

## INSIGHT: FROM DATA-BASED TO CONCLUSION-BASED

Today, the process of turning individual events into an incident is often manual. As data volumes continue to grow, the number of events will also increase, and the manual effort of identifying incidents that require attention becomes unmanageable. The next phase of evolution is going to shift to a model where tools don't just identify anomalies and patterns or behaviors of interest, but go a step further to draw conclusions about what they mean and what next steps are required.

**This isn't about adding more data feeds, but about doing more with the data we already have.**

It's not about creating a better dashboard, but about gaining a better understanding of what's happening on the network. It's not about providing more reports, but about making the security professional's job easier. To do this, the security tool will tell you what's going on that you need to be aware of, why it's important, and what steps to take next.




The evolution of security tools reflects the growing data volumes, which in turn increase the number of events that need to be parsed into incidents — and will eventually provide actionable insight about intent.

For example, the system could send you a daily email that provides analysis — such as network traffic to China was up 48% yesterday, or there are 500 new clients connected to your network which is down 30% from last week — so you have insights that help you prioritize how to focus your time. And the system would not only alert you on issues, but also provide details about what it means, links to resources to help you understand the situation, and suggested actions that need to happen next.

This level of conclusion-based insights will transform security operations and deliver benefits to a number of different groups.

## Enterprise InfoSec Teams

Many large enterprises have teams of high-caliber — and expensive — security experts that today spend a lot of time gathering and weeding through "data." When supported by a tool that delivers actionable insight, these skilled professionals can focus instead on applying their expertise to solving problems and executing on higher-value activities.

## Mid-sized Organizations

Many mid-sized organizations don't have the budget to hire dedicated security pros, but still face the same security risks. Tools that deliver conclusion-based insights provide these organizations with an additional level of "expertise" to help them improve their security posture and empower their IT generalists.

## Service Providers

Service providers are responsible for the security of the data and systems of hundreds — and even thousands — of end customers. A conclusion-based approach facilitates their ability to secure and manage all of their users and still provide individual customer-level visibility and customized configurations.

## THE FUTURE STARTS NOW

This evolution of network security capabilities isn't a matter of if, but when. Vendors have a responsibility to advance their solutions to enable organizations to continuously defend their current-state networks against current-state threats. And those organizations have a responsibility to their own customers, employees, shareholders, and other parties to invest in tools that will protect them today and over time. Some of the capabilities described above are available today — organizations that aren't using them are ripe for being compromised (**and it's happening much too frequently**) — while others are still in the "vision" stage. It's important to ensure that you invest in security providers that have a roadmap designed to turn that vision into your security reality.

## 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
Phone +1 (603) 727-4477 | Email info@flowtraq.com