APRIL 2016

WHITE PAPER
THE LAST SECURITY TOOL

THE REAL SECURITY CHALLENGE

There is a new area of challenge to the security teams in the enterprise, government and education sectors – the constant attack by hackers or other adversaries that are sponsored by a government entity or are part of organized crime.

The attackers are finding new and advanced techniques to break the security measures in place, and security staff now have to concede that when the attackers are determined and well-funded, they will ultimately breach the defenses systems of any organization on the Internet.

Growing network speeds, now routinely hitting 100 gigabits-per-second, or roughly 70 million times faster than the typical network connection when firewalls were introduced, pose a number of challenges, particularly in the area of security. Network growth along with the data deluge puts a great amount of pressure on organizations to combat cyber threats and analyze cyber-attacks in real-time so that necessary actions can be taken with minimum delay.

Post analysis of the data, after a threat or security breach, is critical for all organizations. The analysis allows management to make decisions and take actions in response to an attack. More importantly, it is needed to ensure that a cyber event has been truly resolved so that all public disclosure, notification of impacted parties and internal remediation can be completed.

THE PAIN

We live in an age where cyber-attacks on high-speed networks are at an all-time high and increasing. However, in most cases the attacks are only discovered weeks later. “Network security solutions are facing a two-fold growth challenge,” says Peter Ekner, Chief Technology Officer at Napatech. “Data traffic is increasing exponentially, so there is more to analyze at faster speeds. At the same time, cyber-attacks are also growing in number and complexity.”

In the never-ending race to combat security breaches, there is no shortage of security alerts or events in a given firm’s environment, in fact just the opposite. Entire industries have been created to fulfill the need to process the tens of billions of events generated every day in a typical large enterprise. The security team faces the huge task of collecting this data from all the tools and then need to prioritize them by severity.

However even with this enormous number of events reported, organized and prioritized, the tools often give either incomplete or contradictory information about a given event. Add to this that once an attacker is inside, he will often compromise the credentials of a legitimate user and might disguise himself as an employee to do searches and extract sensitive data.

THE DAMAGE

In 2014, average costs for data breaches rose (USD 5.9 million, up from to USD 5.4 million), lost business (USD 3.2 million, up from USD 3.03), and lost or stolen records (USD 246 per). Malicious or criminal attacks are the main cause (44%)[1]. Worse, these direct expenses often are just the first of many legal, shareholder, employee, regulatory, customer and reputational ripples (See figure 1).

While, detection and escalation costs rose to USD 417,700, up from USD 395,262 over the past year.[2] Post-data breach response and detection costs rose to USD 1.6 million, up from approximately USD 1.41 million [3] (See figure 2).

[1] Ibid.
[2] Ponemon Institute, The Data Breach Boom, 2013.
[3] Ibid.

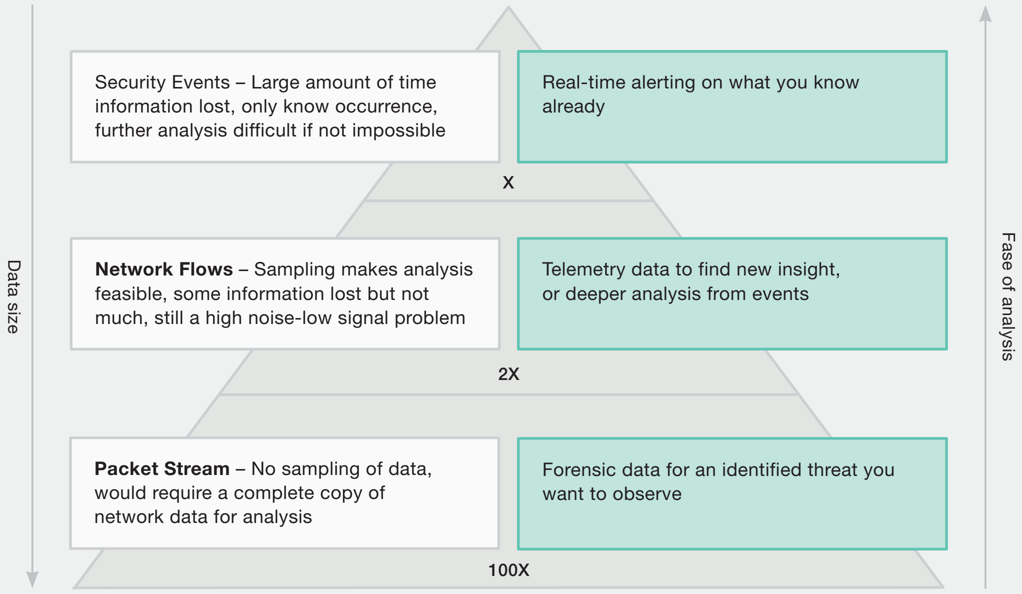

Data size
Security Events – Large amount of time information lost, only know occurrence, further analysis difficult if not impossible
Real-time alerting on what you know already
X
Network Flows – Sampling makes analysis feasible, some information lost but not much, still a high noise-low signal problem
Telemetry data to find new insight, or deeper analysis from events
2X
Packet Stream – No sampling of data, would require a complete copy of network data for analysis
Forensic data for an identified threat you want to observe
100X
Fase of analysis

FIGURE 1
Bridging the Gap
Source: Increasing the Insight from Network Flows – Connecting Science to Operational. Intel Data Center Group

DEFENSE IN DEPTH

With so much at stake, organizations need to implement a diverse solution that 1) prevents intrusion, 2) alerts on suspicious activity, 3) continuously collects forensics data so that the inevitable breach is fully captured and 4) offers post analysis possibilities "It is no longer possible to rely on one single security solution. Traditional point defenses cannot adequately address the new, faster-moving, multi-layer threats and more sophisticated attackers," says Daniel Joseph Barry, Vice President of Positioning and Chief Evangelist of Napatech. "What's required is a layered approach with defense-in-depth, where we not only rely on network security appliances for indications of data breaches, but also network behavior analysis."

Continuously recorded network data is the "last security tool". A network forensics solution should continuously capture all data 24x7 regardless of whether anything interesting is happening in a particular moment or not. Then in conjunction with alerts from the other tools, the security team can investigate whether the event was a false alarm or something that needs to be actioned. Moreover, they can see what happened after the breach and achieve the ultimate goal: determining all the assets the attacker may have accessed and whether he has truly been eliminated from their environment.

A PURPOSE BUILT FORENSICS TOOL

Although many tools can provide a partial network recording based on an event, that data is inevitably incomplete if the recording tool did not see anything it considered interesting. For effective network forensics, we need a tool that can record everything continuously at high speed. It must be purpose-built for this since the demands for storage and indexing of this volume of data are much different than the architecture of the other security tools.

DATA ON-DEMAND

Real-time data capture can be taken a step further by introducing the concept of data capture and retrieval on-demand. The network forensics solution must provide an immediate and indexed answer to an investigator pursuing an event. It is crucial that security officers can quickly go to the time and place of the event to start our analysis, and waiting several hours for this initial answer can cause serious delays while our attacker may still be inside. One of the challenges faced by CTOs and IT managers is the exponential growth in the volume of data. Storing and analyzing every single data packet can be a tedious task and often very expensive. Hence the need for retrieving data on-demand with a few simple commands, where users can access the packets from a certain server or time-period, in order to get to the root of the problem. So retrieval speed and the need for data on-demand is just as important as capturing it.

NAPATECH PANDION

The Napatech Pandion Flex is the latest offering from Napatech and is a cost-effective, highly reliable network recorder that guarantees 100% data capture and retrieval on demand in

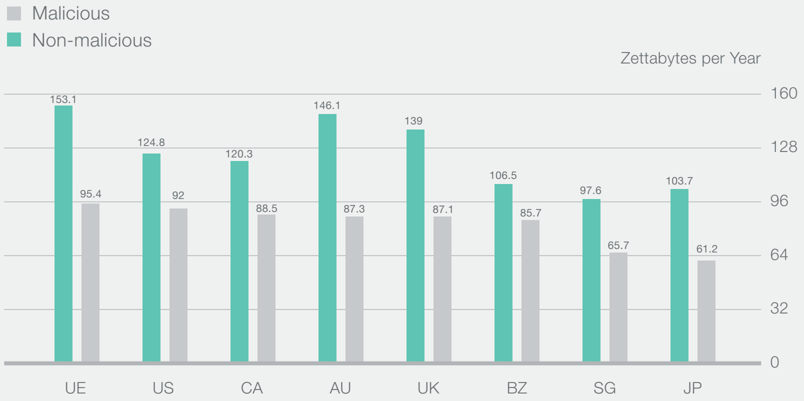


FIGURE 2
Time To Recover From a Breach (in days)
Source: Cisco Global Cloud Index. 2013-2018

real-time. Join the journey towards Smarter Data Delivery, by combining full packet capture, zero latency and data on-demand into one simple solution. With the Pandion Flex, users get accurate data that comes with nanosecond precision timestamping and get zero packet loss. With an easy to use REST API, this device can easily sit with any existing infrastructure, a smart way to bring down additional investment costs and leverage the scope of existing applications.

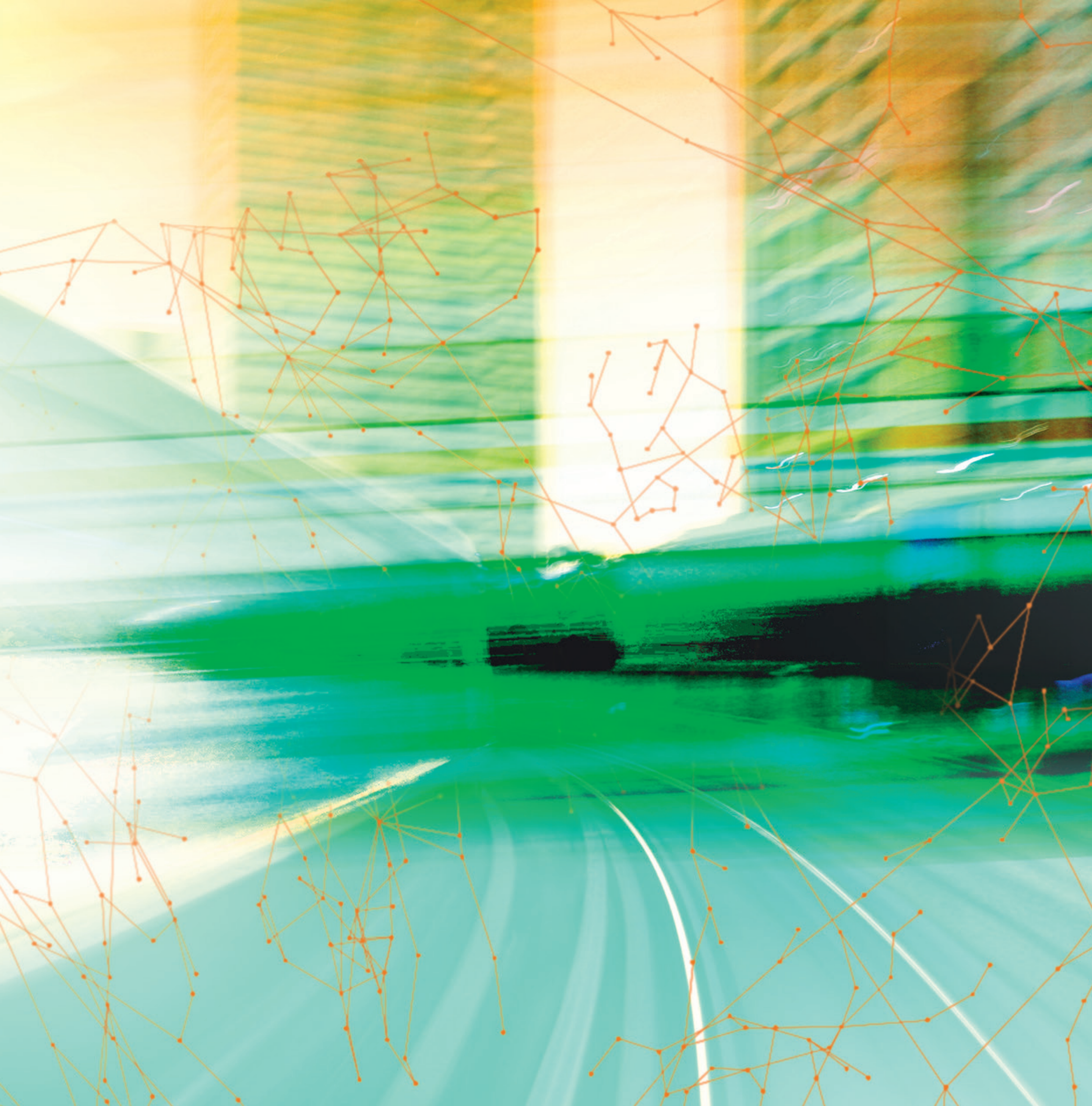
Businesses can reduce their time-to-market with the Pandion Flex with features that offer data on-demand. The device is capable of capturing all PCAP and PCAP NG and with further analytical tools, guarantee smarter data delivery with a solution that can scale with network needs. Access the exact data that is relevant, when and where you want it, with the highly intuitive features in the Pandion Flex. With the Pandion Flex, users can address multiple challenges with one some simple solution.

COMPANY PROFILE

Napatech is the world leader in data delivery solutions for network management and security applications. As data volume and complexity grow, organizations must monitor, compile and analyze all the information flowing through their networks. Our products use patented technology to capture and process data at high speed and high volume with guaranteed performance, enabling real-time visibility.

We deliver data faster, more efficiently and on demand for the most advanced enterprise, cloud and government networks. Now and in the future, we enable our customers' applications to be smarter than the networks they need to manage and protect.

Napatech. FASTER THAN THE FUTURE



EUROPE, MIDDLE EAST AND AFRICA
Napatech A/S
Copenhagen, Denmark

Tel. +45 4596 1500
Info@napatech.com
www.napatech.com

NORTH AMERICA
Napatech Inc.
Boston, Massachusetts
Los Altos, California
Washington D.C.
USA

Tel. +1 888 318 8288
Info@napatech.com
www.napatech.com

APAC
Napatech China/South Asia
Taipei City, Taiwan
Tel. +886 2 28164533 Ext. 319

Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374

Napatech Korea
Seoul, South Korea
Tel. +82 2 6001 3545

ntapacsales@napatech.com
www.napatech.com

Disclaimer: This document is intended for informational purposes only. Any information herein is believed to be reliable. However, Napatech assumes no responsibility for the accuracy of the information. Napatech reserves the right to change the document and the products described without notice. Napatech and the authors disclaim any and all liabilities. Napatech is a trademark used under license by Napatech A/S. All other logos, trademarks and service marks are the property of the respective third parties.