WHITE PAPER

# Enabling adaptive security with advanced threat detection solutions

Contents

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.

## NETWORKS UNDER CYBER-SIEGE

According to the Symantec Internet Security Threat Report of April 2016, 431 million new malware variants were discovered in 2015, representing a 36% increase since 2014. On average, a new zero-day-threat was discovered each week representing a 125% increase compared to 2014.

From these figures it is clear that a veritable cyber-siege is underway that affects us all. It is not just large corporations and governments that are experiencing attacks either. In the same report, Symantec indicated that spear-phishing attacks targeting employees increased 55% in 2015 and that 43% of those attacks were directed against small businesses!

Such figures have prompted the cyber security community to reconsider how defenses are currently architected and deployed. In particular, the current over-reliance on prevention solutions to catch threats before they enter the network is no longer considered sufficient. We have learnt that building a taller, thicker wall does not prevent attackers from breaching our defenses and can often provide a false sense of security.

Experts in the cyber security community have called for a more holistic approach, relying on a combination of security prevention and detection solutions – rather than on prevention alone. This adaptive security approach does not claim to prevent all threats from breaching defenses, but it does promise to shorten the time to detect and react to a breach, which can prove crucial.

The foundation of an effective adaptive security solution is the ability to continuously monitor and analyze what is happening in the network to detect anomalous behavior. It also requires the ability to retain network data for forensic analysis for when past events need to be investigated in more detail. To re-create the anatomy of an attack, knowing exactly what happened when is vital. Without this learning, there is no basis for improving defenses to keep up with attacker's growing ingenuity and innovation.

In this white paper, we will look more closely at what adaptive security entails. We will explore the importance of security detection as a supplement to prevention – and outline its vital components.

## ADAPTIVE SECURITY

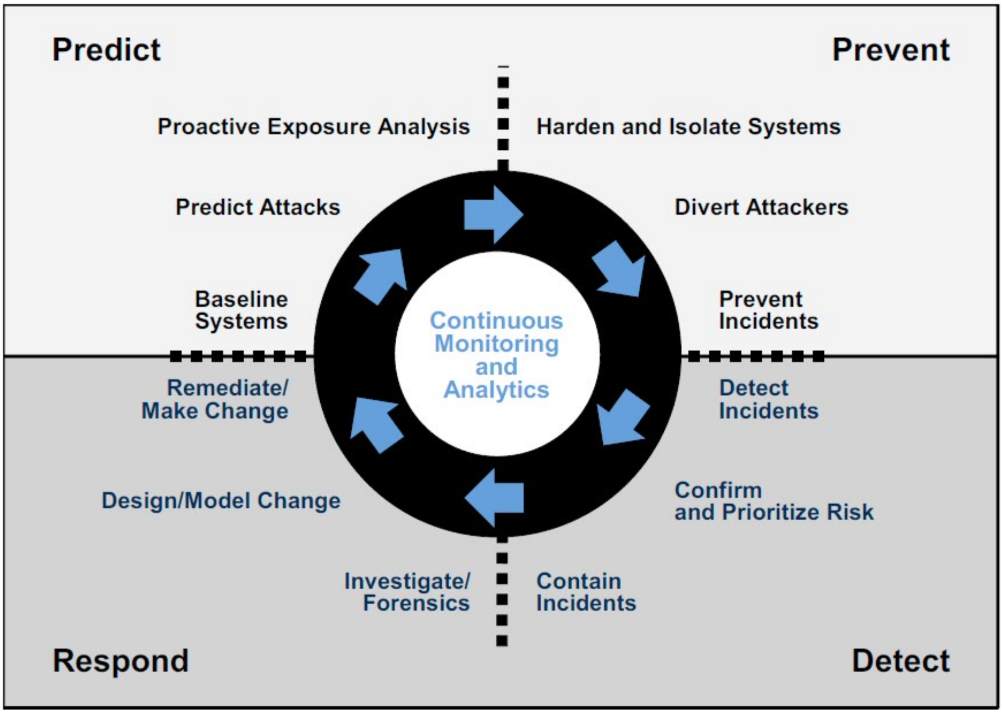
In “Designing an Adaptive Security Architecture for Protection from Advanced Attacks” from January 2016, Gartner elaborated on the concept of an adaptive security architecture first proposed in 2014. In the analysis, Gartner concluded that there is an over-reliance on security prevention solutions, which are insufficient to protect against motivated, advanced attackers. The alternative proposed was an adaptive security architecture based on the following critical capabilities:

- Preventive capabilities to stop attacks
- Detective capabilities to find attacks that have evaded preventive capabilities
- Retrospective capabilities to react to attacks and perform forensic analysis
- Predictive capabilities to learn from attacks and industry intelligence to improve capabilities and proactively predict potential new attacks

These recommendations are captured in the following diagram from the report:

The foundational and enabling capability underpinning the adaptive security architecture framework is the ability to perform continuous network monitoring and analysis.

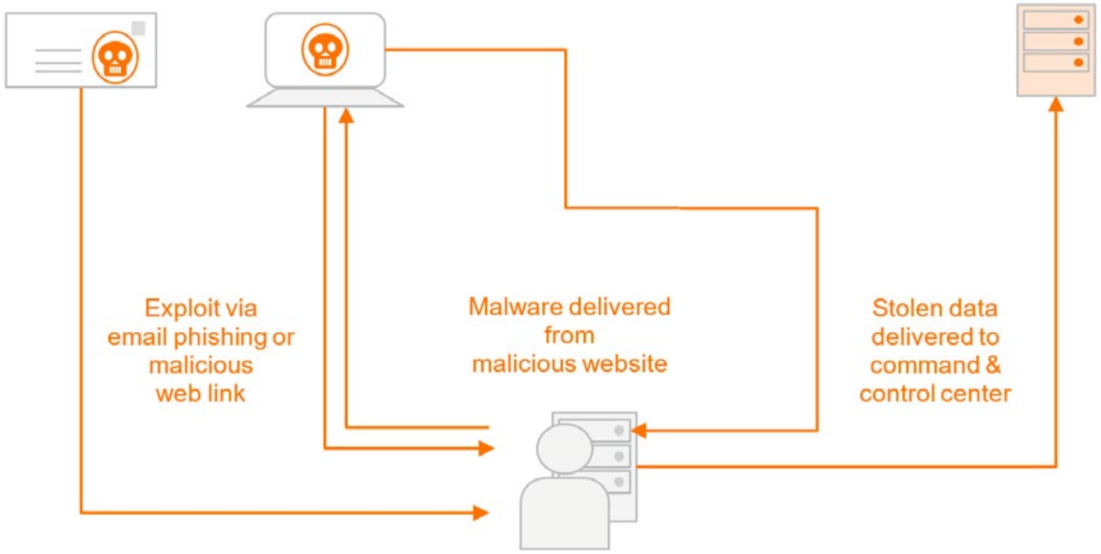
To understand how these capabilities can be applied to detect attacks, it is useful to walk through a typical example and explore how current prevention solutions are designed. We can then examine how attackers are circumventing these defenses and finally establish what detective, responsive and predictive solutions can be deployed to enable an adaptive security solution.



Source: Gartner (February 2014)

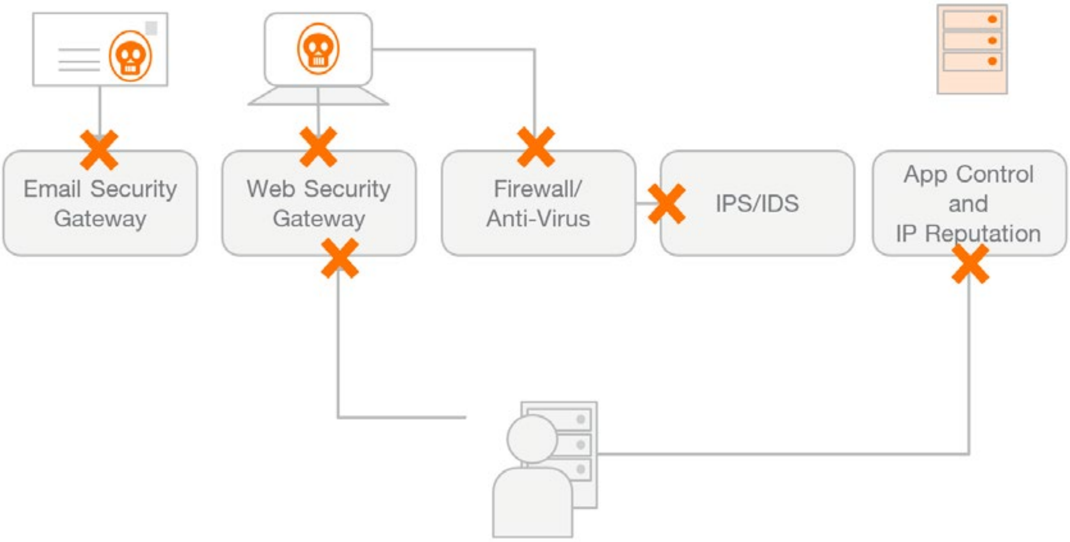
## THE ANATOMY OF AN ATTACK

To understand the significance of the capabilities recommended in the adaptive security architecture, it is useful to walk through a typical attack:


Exploit via email phishing or malicious web link
Malware delivered from malicious website
Stolen data delivered to command & control center

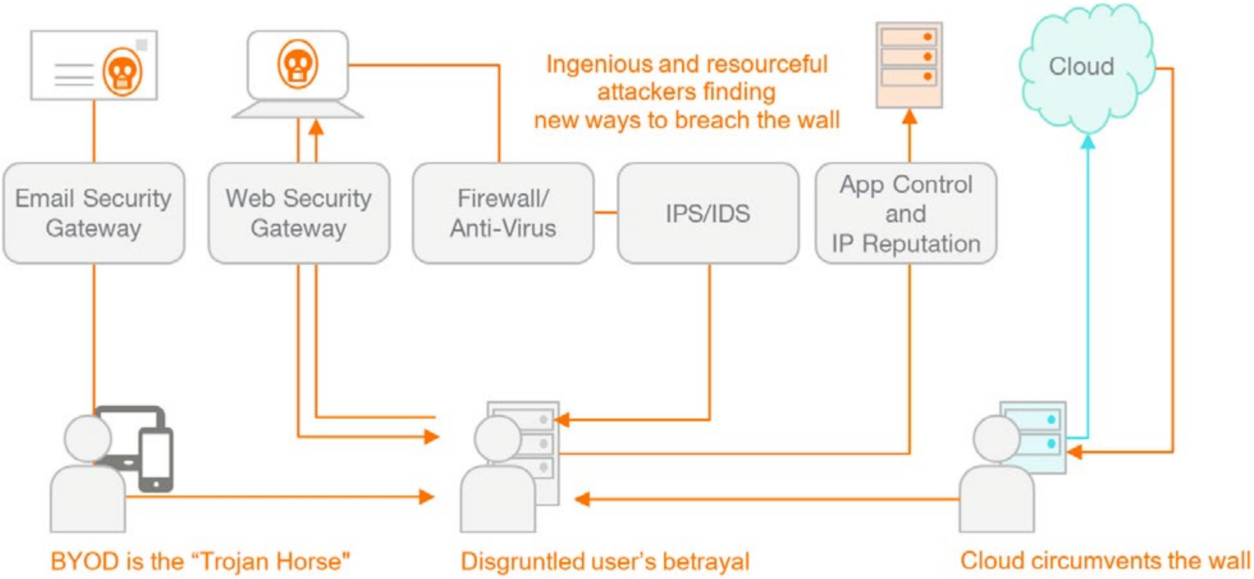
A typical attack strategy is to send a phishing email or malicious web-link to the user who unwittingly clicks on the link, causing malware to be downloaded to his computer. The malware can then search for and deliver valuable information to an external command and control center owned by the attacker.

It is the job of security prevention solutions to stop these attacks at various stages of its execution:



Email security gateways are designed to prevent phishing mails from being delivered to the user. If, however, a phishing mail is delivered, web security gateways, firewalls and IPS/IDS solutions are designed to prevent the download of malware to the user's computer. Should a user's computer become infected despite these steps, application control and IP reputation solutions should prevent stolen data from being delivered to the attacker's command and control center.

It is easy to understand why organizations would feel that this multi-stage architecture designed to address each step of the attack should be sufficient to foil attackers. Nevertheless, the fact remains that breaches are happening because several measures are undermining the effectiveness of security prevention solutions:


Ingenious and resourceful attackers finding new ways to breach the wall
Cloud
Email Security Gateway
Web Security Gateway
Firewall/ Anti-Virus
IPS/IDS
App Control and IP Reputation
BYOD is the "Trojan Horse"
Disgruntled user's betrayal
Cloud circumvents the wall

Many users are now demanding that they can bring their own devices to work. This potentially opens opportunities for attackers as users are perhaps not as vigilant in updating their personal devices and would typically not have the same kind of security prevention solutions at home and certainly not on the road.

Individual users can also become disgruntled and take active part in an attack by stealing data themselves or enabling others to do so. But it is not always a conscious betrayal. Today, many security breaches are still based on users unwittingly providing access to attackers they believe to be part of the organization or consultants hired to perform maintenance on the network or facilities in general.

The advent of cloud computing also provides new opportunities for attackers as various departments and individuals use cloud services for personal and corporate activities. Few of us consider the security of these services as we place more value on the efficiency and ease-of-use that they provide.

Finally, attackers are ingenious and resourceful – constantly looking for new ways to breach the wall by exploiting vulnerabilities. One of the latest developments is the non-malware attack. In this type of attack, no malware is downloaded to the user's computer. Instead, a malware script is activated that exploits vulnerabilities in flash, web browsers and other existing tools. As many of the prevention solutions installed on the computer will be focusing on preventing malware download, this attack effectively nullifies the effectiveness of a large part of the security architecture.

These are just the most obvious issues that security teams need to deal with. But they clearly show that a reliance on prevention alone is not enough. The answer is to complement security prevention solutions with security detection.

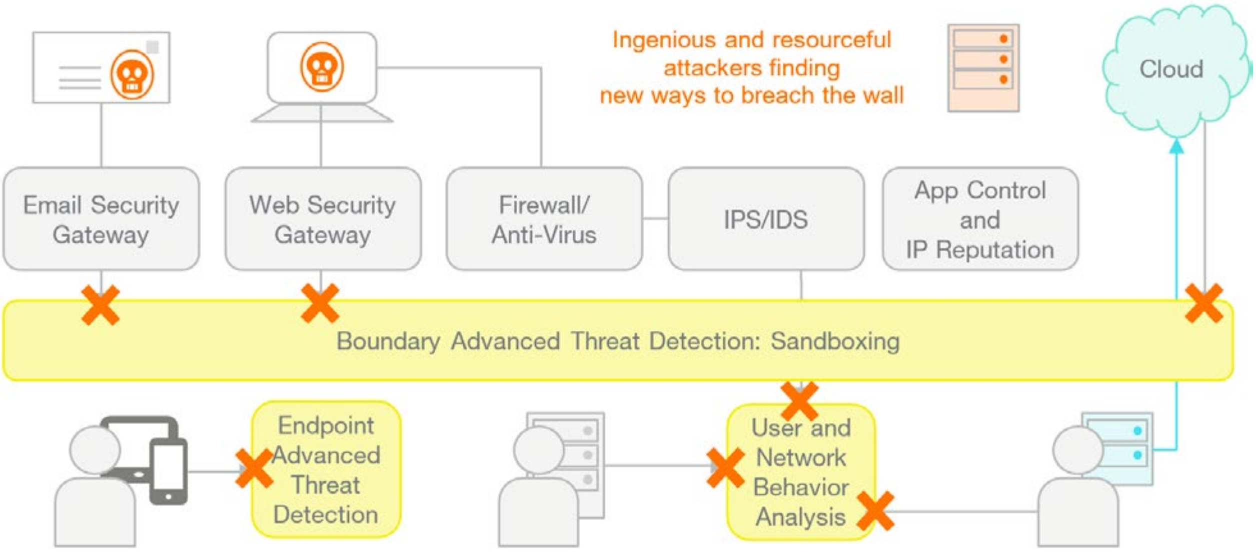
## DETECTING BREACHES QUICKLY

Security solutions like firewalls and intrusion prevention systems are designed to avert known attacks. In the case of intrusion prevention systems, pattern matching is used to recognize the "signature" of a known attack. But, what happens if it is a zero-day-threat that has never been seen before? How can we detect that a breach has taken place?

Unfortunately, our confidence in security prevention solutions often leads to situations where breaches go undetected for months, even years. According to the "2016 Cost of Data Breach Study, Global Analysis" by the Ponemon Institute, the average time to identify a malicious attack is now 229 days, while the average time to contain the attack is 82 days!

This can prove commercially damaging as the average cost of a data breach is reported to be $4 million or $158 per stolen record. Over the last few years, high profile cases have been prominent in the news and, in some cases, have cost C-level executives their jobs.

To combat this situation, a number of "advanced threat detection" solutions have been introduced. These solutions are designed to detect breaches that have penetrated security prevention solutions:


Ingenious and resourceful
attackers finding
new ways to breach the wall
Cloud
Email Security Gateway
Web Security Gateway
Firewall/ Anti-Virus
IPS/IDS
App Control and IP Reputation
Boundary Advanced Threat Detection: Sandboxing
Endpoint Advanced Threat Detection
User and Network Behavior Analysis

The first category of solutions can be considered boundary advanced threat detection solutions, often known as sandboxes. They are designed to catch threats that security gateways, firewalls and intrusion prevention solutions miss. With sandboxing, suspicious data is sent to a safe environment where the behavior of the software can be observed and determined safe or unsafe. Needless to say, this is not a real-time determination, but compared to the average of 229 days to detect a breach, it is lightning fast!

It is clear that sandboxes do not prevent threats from taking place, but like other advanced threat detection solutions, the goal is to shorten the time it takes to detect and respond. The Ponemon Institute found that the average cost to identify a malicious attack is 26% lower if identified within 100 days and the average cost to contain a malicious attack is 26% lower if contained within 30 days.

Other detection solutions include endpoint advanced threat detection solutions. These are centrally managed security solutions installed on different types of endpoint devices including smartphones and tablets. They allow the security team to detect and track an attacker's actions and offer a first step towards containing the attack.

But, even with these solutions, attackers can go undetected. As a supplement, an additional layer of advanced threat detection can be deployed based on user and network behavior analysis. Such internal advanced threat detection solutions rely on continuous monitoring of network activity to first establish a profile of normal network behavior and then compare

real-time activity to this profile to detect anomalous behavior. When used in conjunction with the information from other security solutions, it can provide the first indication that a breach has taken place.

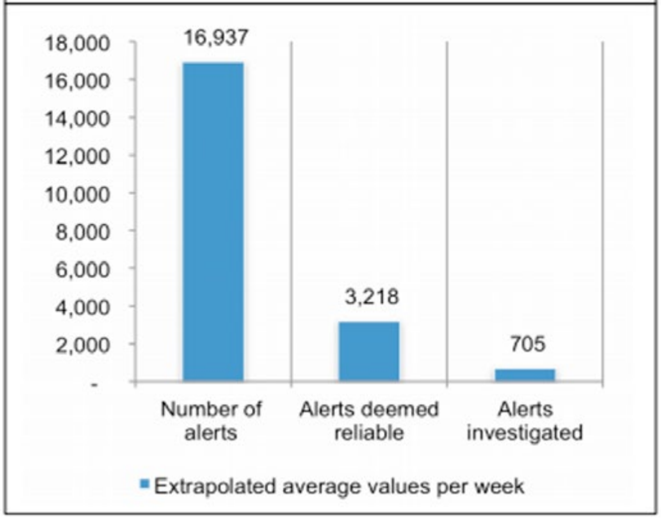
This solution is particularly effective in combating non-malware attacks as it does not rely on detecting file downloads, but on detecting activities that are out-of-the-ordinary, giving the security team the basis for further investigation.

## INFORMATION OVERLOAD LEADING TO UNDETECTED BREACHES

With the introduction of advanced threat detection solutions, a comprehensive security infrastructure is now in place to prevent and detect advanced threats. However, the complexity of the solution has reached new heights, which means there is more for the security team to monitor and more information that needs to be processed. Unfortunately, this amount of information can be more than most teams can handle, which in itself can lead to threats.

According to “The Cost of Malware Containment” report by the Ponemon Institute from January 2015, the average number of malware alerts investigated by security teams was just 4% of the number of nearly 17,000 alerts received:

**Figure 1. Extrapolated average malware alerts for organizations participating in this study**



Source: Ponemon Institute “The Cost of Malware Containment”, January 2015

This just shows the pressure that security teams with limited resource are experiencing. There are also examples that very high profile breaches went undetected – not because of systems failing to detect the breach, but because the breach alert received such a low priority that the security team never got around to investigating further.

To address this issue, solutions are being developed to automate the process of correlating alert information from various systems to provide security teams with better root cause analyses of potential breaches. The next generation Security Information and Event Management (SIEM) systems are now including machine learning and artificial intelligence capabilities to improve intelligence and automation, thereby providing a single pane of glass for the security team to effectively manage the security of their networks.

But, what if the worst happens and a threat is detected too late? What steps can be taken and what solutions do we need to react effectively?

## THE IMPORTANCE OF POST-BREACH ANALYSIS

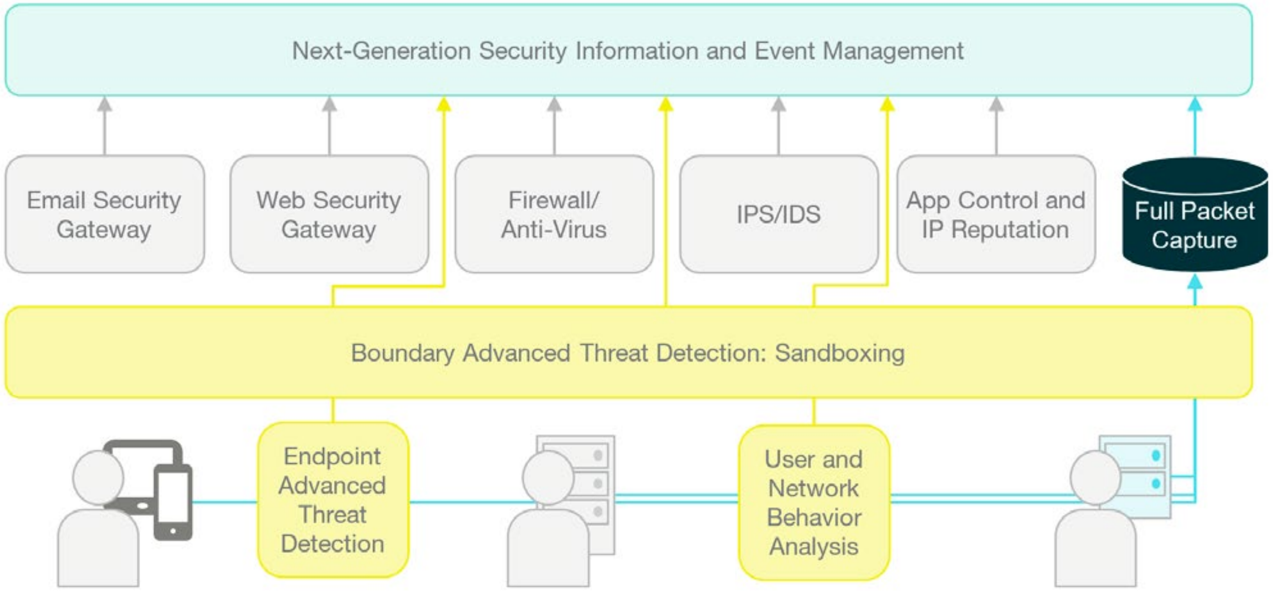
According to the Ponemon Institute, 70% of breaches are often detected by third parties outside the organization. This is the call that every C-level executive dreads and the immediate concern is to determine the extent of the breach and the company’s exposure. The C-level executive will expect his security team to be able to report exactly what happened, when it happened and why it happened within a matter of hours.

Unfortunately, most security solutions today are built to prevent and detect attacks in real-time or near-real-time. The ability to reconstruct the anatomy of an attack in detail is often impossible, especially if the attack took place up to half a year ago!

There is therefore a strong case to be made for establishing the capability to record network traffic in a way that will allow the reconstruction of a breach even months after the fact.

## THE BASIS FOR ADAPTIVE SECURITY

By adding advanced threat detection solutions, next generation SIEM solutions and packet capture capabilities to the security architecture, we now have in place the infrastructure to support an adaptive security framework:



Next-Generation Security Information and Event Management
Email Security Gateway
Web Security Gateway
Firewall/ Anti-Virus
IPS/IDS
App Control and IP Reputation
Full Packet Capture
Boundary Advanced Threat Detection: Sandboxing
Endpoint Advanced Threat Detection
User and Network Behavior Analysis

With this infrastructure, it is possible to prevent known attacks, detect zero-day-threats and pinpoint anomalous behavior. The various alerts are correlated and condensed by solutions like SIEM systems, enabling security teams to quickly focus their attention on the most important threats.

Should the worst happen and a breach be detected late, the ability to fully capture and record each data packet allows the anatomy of an attack to be recreated. This enables fast determination of the extent and impact of the breach and provides a source to learn and prevent such a breach from happening again.

Fortunately, the needed technologies to implement such solutions are available today.

## FULL PACKET CAPTURE

A key enabling capability for successful adaptive security as outlined above is the ability to continuously monitor and analyze network activity. To do this effectively, it is necessary to capture each data packet no matter the network speed or load. The packets can then be used for real-time analysis of the network activity or can be recorded to disk for later forensic analysis.

Napatech provides a full range of packet capture solutions that enable customers to build high-performance security appliances and solutions.

### NAPATECH SMARTNICS

Napatech SmartNICs are widely considered the most advanced and reliable packet capture network adapters available on the market today. With port speeds ranging from 1G to 100G, Napatech can provide a wide range of hardware configuration options all accessible through a common Application Programming Interface (API) that can be based on open standards such as PCAP or DPDK or the Napatech advanced NTAPI interface. The common API allows a single analysis application development effort that can support a variety of hardware.

Napatech SmartNICs are designed to support full theoretical throughput at 64 bytes even at speeds up to 100 Gbps, but also include extensive filtering, de-duplication and slicing capabilities. They offer the ability to direct specific data flows to specific applications and server CPU cores for processing, providing the developer with full control over the data to be analyzed.

To find out more, visit www.napatech.com

## NOTES

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

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

**NORTH AMERICA**
Napatech Inc.
Portsmouth, New Hampshire
Los Altos, California

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

**APAC**
ntapacsales@napatech.com
www.napatech.com