WHITE PAPER

napatech

You can't secure what you can't see

Discover the value of network visibility for cybersecurity

Contents

YOU CAN'T SECURE WHAT YOU CAN'T SEE

Securing corporate networks has never been more challenging. Tried and tested methods, architectures and solutions no longer work, as cybercriminals become more sophisticated and more successful with their exploits.

However, just putting more money into the same approaches is not going to be enough. The game is changing and enterprise cybersecurity needs to change with it. This requires a rethink on how cybersecurity defences are architected and deployed. Not just from a technology point of view, but also from a return on investment point of view.

In this paper, we will look at the latest expert advice on how to design cybersecurity defences, the importance of continuous monitoring and analysis and, above all, on the new possibilities enabled by open-source cybersecurity software and FPGA-accelerated standard servers with specific examples of affordable, yet effective cybersecurity solutions.

More and more enterprises are leveraging these new possibilities to build their own cybersecurity monitoring solutions that can provide visibility and insight into more places in the network and enable the continuous monitoring and analytics required to combat cybercriminals.

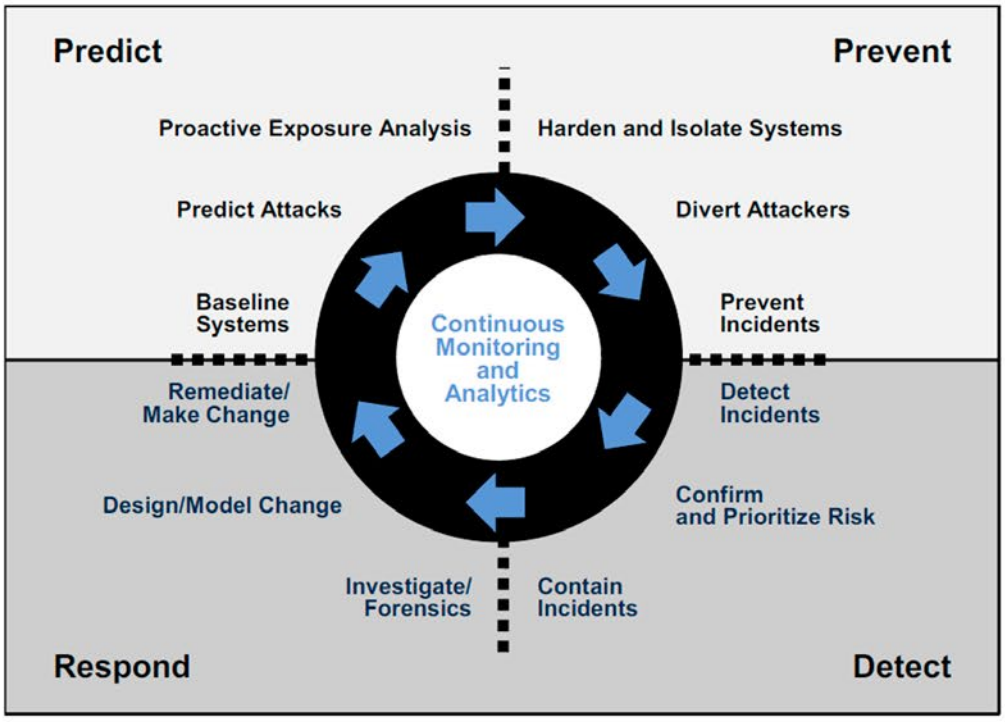
RELYING ON PERIMETER DEFENCES IS NO LONGER ENOUGH

According to security experts and analysts such as Gartner, traditional cybersecurity defences that rely on prevention alone are no longer enough to stop cybercriminals. Security threat prevention need to be complemented with solutions that can detect threats based on continuous monitoring and analysis of network and application behaviour. Security threat detection solutions and technologies will not prevent breaches from taking place, but will drastically reduce the time it takes to detect and react to a breach.

In “Designing an Adaptive Security Architecture for Protection from Advanced Attacks” from January 2016, Gartner described the concept of an adaptive security architecture. 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:



Source: Gartner (February 2014)

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

As one can see, in the detect and respond fields of the diagram, the focus is on detecting, containing and responding to security incidents. These capabilities recognize the fact that there will be breaches that will evade detection by security threat prevention solutions for one reason or another. It is therefore important to monitor activity to detect any anomalous behaviour that could indicate a breach.

MORE COMPLEX NETWORKS

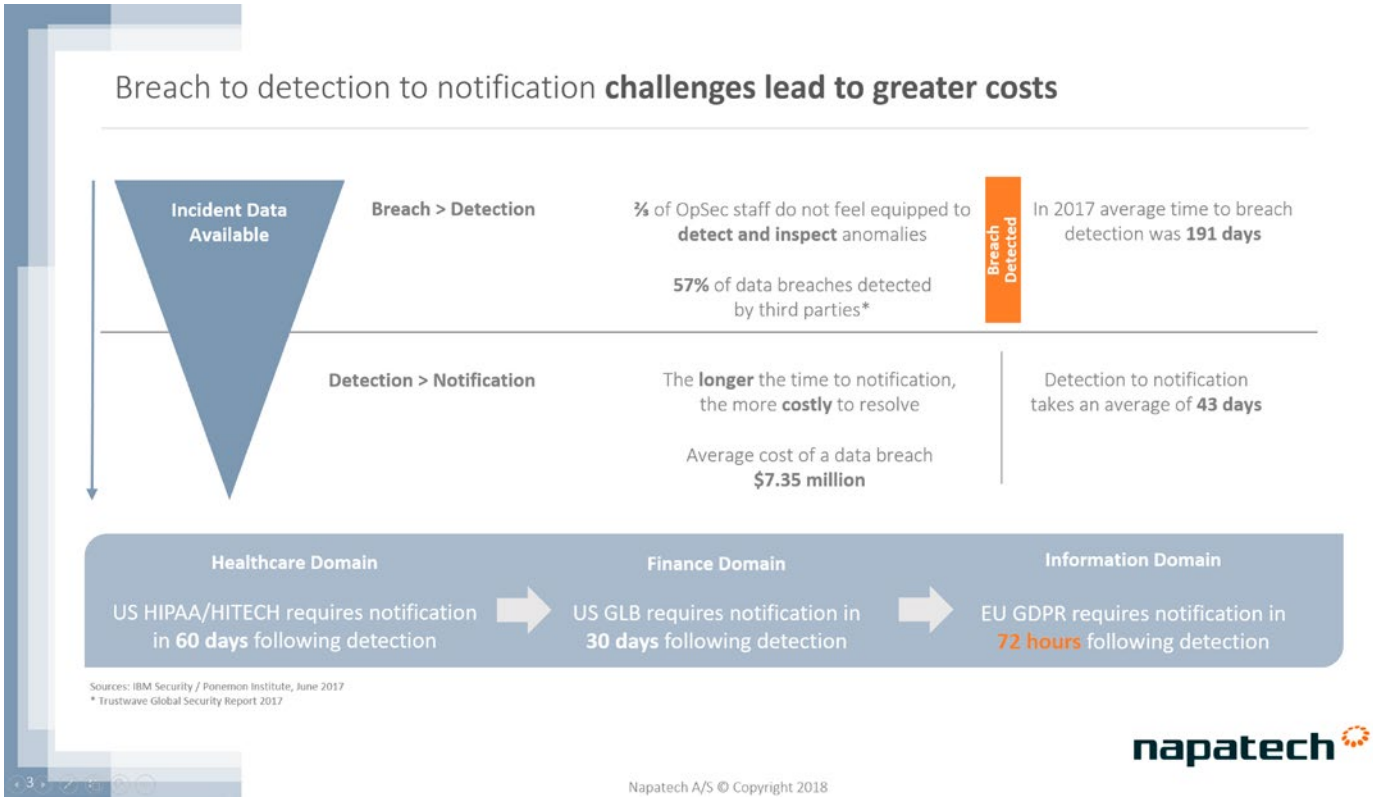
Enterprise networks are becoming more complex on a number of fronts. We now rely on the Internet for almost every aspect of corporate life, which has led to a broad range of new applications on the network. This ranges from simple email communications to Voice-over-IP (VoIP) telephony to video conferencing. In addition, the enterprise network has been extended to mobile devices and smartphones creating a new device-level complexity. This leads naturally to Bring Your Own Devices (BYOD), which has become a selling point for recruitment at some companies, but introduces a cybersecurity challenge. When it comes to the cloud, we of course see the increased use of cloud-based apps for corporate and personal use, but we are also seeing hybrid networks spanning in-house data-centres and hosted cloud services, which again adds to the complexity of the environment to be monitored.

According to IHS Markit[1] , 57% of surveyed enterprises expected to operate a mix of on-premise and managed security services using 11 different cloud service providers.

It is clear that in such a complex network and application environment that the number of potential sources of attack have multiplied and that attacks can now occur from within the enterprise network circumventing perimeter defences.

DETECTING BREACHES FASTER

Research shows that the faster one can detect and react to a breach, the lower the impact and associated cost, which is an increasing concern given very high profile breaches of late and C-level exposure in such circumstances.



Corporate boards and executives are increasingly aware of the cost of data breaches, which now average over $7m per breach, but increased regulation is also increasing the stakes. For example, the new GDPR regulations in Europe, which stipulate that organizations that have experienced a breach affecting the private data of clients need to notify affected clients of that breach within 72 hours! Considering that the average time from detection to notification of a breach today is 43 days, this would appear to be a very challenging requirement!

Therefore, the establishment of a continuous monitoring and analytics infrastructure, particularly for the network, is of critical importance. However, providing visibility at all the locations that are required can be an expensive proposition and while there are many commercial offerings to choose between, finding the solution that provides exactly what you need, at exactly the price you can afford, can be difficult.

[1] IHS Markit "Cloud Service Strategies & Leadership Survey North America" and "Next Gen Threat Prevention Strategies and Vendor Leadership Survey North America", from 2017

BUILDING YOUR OWN VISIBILITY INFRASTRUCTURE

Mitigating the increasing number of potential threat sources requires a broader visibility into what is happening in the networks with more points of visibility. However, it can be cost prohibitive to use commercial solutions at all relevant points in the network.

This is why more and more enterprises are exploring the option of building their own cybersecurity probes and appliances. Never before has it been more viable to pursue this option. There are a broad range of open-source software offerings, such as Snort, Suricata and Bro that have reached a high level of maturity and enable powerful security monitoring solutions. Indeed, they are often the basis of many commercial offerings available!

The advantage of building your own cybersecurity probe or appliance is that it can provide exactly the level of visibility and insight that you need, where you need it. It can include exactly the features you require, including capabilities important for your environment and network. Finding a commercial solution that can provide exactly what you need, at a price you are willing to pay can be a challenge, so building your probe or appliance provides a compelling alternative that can stretch your cybersecurity budget dollars.

What has been an issue in the past is finding the right compute platform on which to deploy open-source, commercial or in-house developed cybersecurity software applications. Conventional standard servers using standard Network Interface Cards (NICs) provide a “good-enough” solution for lower speed rates, but face challenges once you move beyond 1G speed rates.

One of the big challenges is packet loss. Whether the security monitoring solution being designed is inline or passively snooping traffic on a tap or switch SPAN port, packet loss poses an issue, as, once lost, packets cannot be retrieved. This is because monitoring solutions should not interfere with communications unless a threat is detected. So, normal mechanisms for re-sending traffic that is not received, such as TCP re-transmission, cannot be used.

IS PACKET LOSS AN ISSUE? ABSOLUTELY!

When packet loss issues arise, it is not just one packet here or there, but a number of packets lost at the same time. This can mean that the entire session is compromised from an analysis point of view, rather like missing the part of the crime movie that reveals the identity of the villain. In cybersecurity terms, this is doubly true, as one tactic to obfuscate malicious activity is to overwhelm defenses with bursts of data.

In other words, you lose packets at precisely the time when you needed to gain more insight into what is happening. An irony that is not lost on the cybercriminal.

Therefore, assuring zero-packet loss is essential to ensuring that cybersecurity defenses are up to the task when they are needed most.

FPGA-BASED SMARTNICS FOR RELIABLE CYBERSECURITY

To assure zero-packet loss, it is important to use NICs, which are designed for this task. FPGA-based SmartNICs are ideal for this purpose as they not only provide the raw throughput and deterministic performance required, but can also provide the intelligent processing of data on the SmartNIC that will address all aspects of packet loss.

An FPGA-based SmartNIC solution includes two important parts; the SmartNIC hardware with FPGA-chip on-board that replaces the standard NIC and the FPGA "image" software that implements the features and capabilities to be executed on the FPGA. For more info on what an FPGA is and how it works, see the info box.

Packet loss can occur in multiple locations in the server. It can be at the network port or in the processing pipeline of the NIC, but can also occur due to congestion over the server PCIe interface, incorect memory management and data transfer over the NUMA node QPI interface.

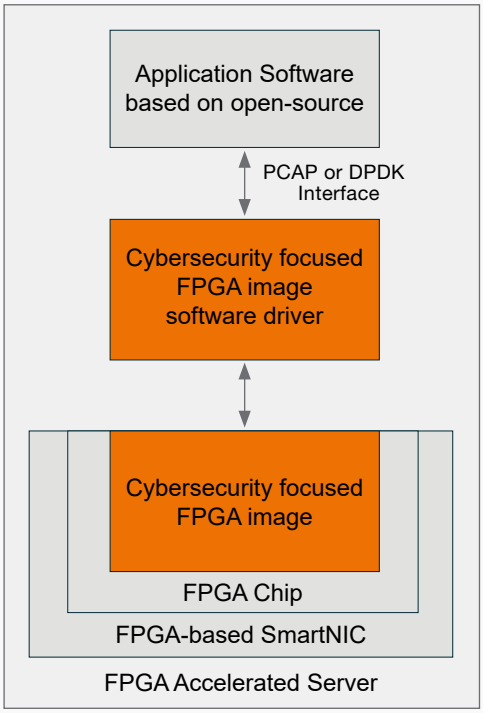
Solutions based on FPGA-based SmartNICs not only ensure that their network ports and internal pipeline have the capacity to receive and transmit data traffic at highest theoretical rates, but also provide on-board buffering to ensure that no packets are lost due to network, PCIe bus or CPU congestion. Direct and optimized transfer of data to CPU cache memory ensures that packets are processed as fast as possible. Intelligent classification and multi-CPU load distribution divides the processing and analysis of data over multiple CPU cores leading to a high level of performance.

In short, by replacing standard NICs with FPGA-based SmartNICs and FPGA image software designed for security monitoring applications, it is possible to assure zero packet loss, improve performance significantly and enable high-speed probes and appliances that are built to support open-source applications like Snort, Suricata and Bro.

A Field Programmable Gate Array (FPGA) is a reconfigurable chip that provides a set of logical components and memory that can be combined to perform a specific computational task. How the logical components and memory are combined is defined using a software configuration file called an FPGA image.

FPGAs can support almost any conceivable computational task where the data path and computations can be completely customized to the task that needs to be performed. As the FPGA is defined using software, it can also be reconfigured, on-the-fly, remotely allowing the same hardware to have new capabilities on-demand.

One of the key attractive attributes of FPGAs that set them apart from other programmable processing chips is determinism. Once the data path is configured in the FPGA, the time it takes to process that data is the same no matter the load. This makes FPGAs ideal for low-latency and low-jitter applications and applications that require guaranteed performance under all conditions.



VARIOUS TYPES OF SECURITY SOLUTIONS POSSIBLE

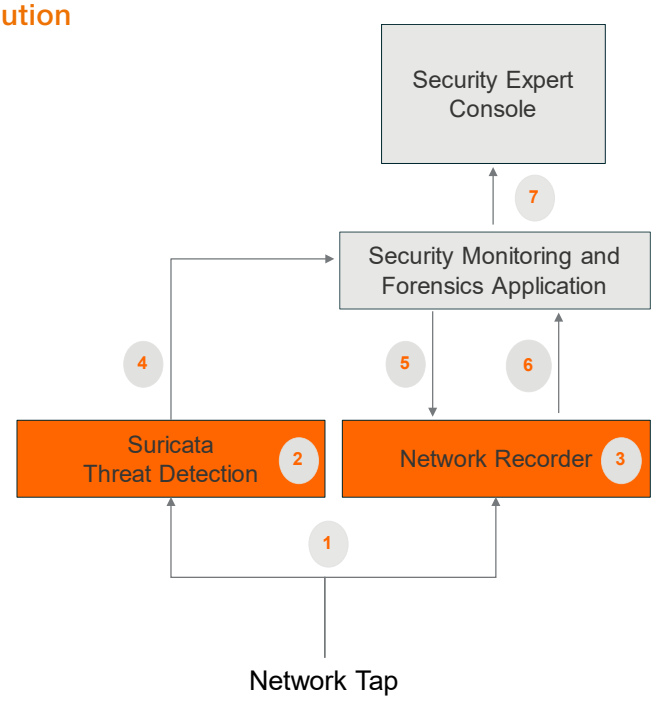
Several types of security monitoring solutions are possible using open-source software running on standard servers with FPGA-based SmartNICs and cybersecurity focused FPGA image software:

- Intrusion Detection Systems (IDS) that can detect if a breach has occurred internally in the network and not just at the perimeter
- Internal Network Advanced Threat Detection (ATD) systems that can analyze the pattern of behavior of networks to determine if a zero day threat has eluded perimeter defenses
- Security forensics solutions that can record network data for deeper analysis should a breach be detected
- Dynamic Distributed Denial of Service (DDos) mitigation solutions that can detect DDoS attacks and redirect traffic for scrubbing
- Security testing solutions that can generate traffic at full theoretical limits to stress test cybersecurity defenses

Here is an example of a cybersecurity solution combining some of the above capabilities:

Security Monitoring and Forensic Solution

1. Network tap provides data to servers with FPGA-based SmartNICs and FPGA image software
2. Suricata-based threat detection server monitors all traffic with zero packet loss
3. Network recorder server stores all traffic to disk with zero packet loss
4. Suricata alerts of security incident
5. App SW queries network recorder for related data
6. Network recorder responds with relevant data
7. This enables security expert to quickly determine if security incident is a breach



It involves two servers, each with their own FPGA-based SmartNIC and dedicated FPGA image software. In the first server, we are using a Suricata-based IDS threat detection application to examine data in real-time to determine if there is any suspicious traffic. In the second server, we are using a security forensics application and network recorder to record all the network data to disk with zero packet loss for later analysis. If the Suricata engine finds suspicious traffic, it sends an alert to the security monitoring and forensics application that either automatically, or on demand from a user, retrieves network data related to the security incident from the recorded network data. This enables the security expert to make a fast determination of the veracity and severity of the security incident.

CREATE ADAPTABLE SECURITY ARCHITECTURE WITH RECONFIGURABLE HARDWARE

As the standard server with FPGA-based SmartNIC solution can support a wide range of cybersecurity solutions, it is possible to extend cybersecurity defences and implement an adaptable security architecture purely by using different software applications.

IDS and threat detection applications can provide the security detection solutions required. A security forensics application can be used to quickly investigate and react to breaches and security testing solutions can be used for hardening defenses. All of these solutions can be based on the same reconfigurable platform, the standard server with FPGA-based SmartNIC with cybersecurity focused FPGA image software.

THE BOTTOM LINE

As stated earlier, faster detection and reaction to breaches saves money. Up to $7 million. By establishing the appropriate continuous monitoring and analysis infrastructure with broad network visibility, it is possible to see more, but also determine fast whether a security incident is a breach or not.

This is important, as a typical security expert needs to examine up to 17,000 security alerts a week[2]. Many of the largest breaches have succeeded, not because the breach was not detected by security defenses, but that the security incident could not be examined properly and in time due to the security experts being overwhelmed with incidents and not having the tools and insight available to determine if an incident was a breach fast enough.

Commercial solutions are needed to form the backbone of your cybersecurity defenses, but enabling visibility at all the locations you need can become cost prohibitive using available commercial solutions. By using open-source applications on standard servers with FPGA-based Smart NICs with FPGA image software designed for high-performance security monitoring, it is possible to build a more affordable solution with exactly the capabilities required to provide the visibility you need, when and where you need it.

For example, Napatech has shown that it is possible to double the performance of applications like Suricata even when using a full signature set. What that means, in practice, is that half of the server CPU power is now required to run the same application.

If we do the numbers, what we see is that this can be the difference between purchasing a dual-socket or a quad-socket server. The price for a dual-socket server is around $5,000, while a quad-socket server is actually 4 times more expensive at around $20,000!! This is because there are not many applications that need quad-socket servers, which means volumes are lower, and the motherboard is a lot more expensive. So, while one might expect that 2 more cores means 2x the price, it actually means 4x the price! So, halving the number of cores is a significant saving of up to $15,000 per server!

So, if you are an enterprise who needs a more affordable solution for providing insight into all your network activity, then take a look at the benefits of using standard servers with FPGA-based SmartNICs and FPGA image software designed for high-performance security monitoring as the platform of choice for your open-source, commercial or in-house developed cybersecurity solution deployments.

COMPANY PROFILE

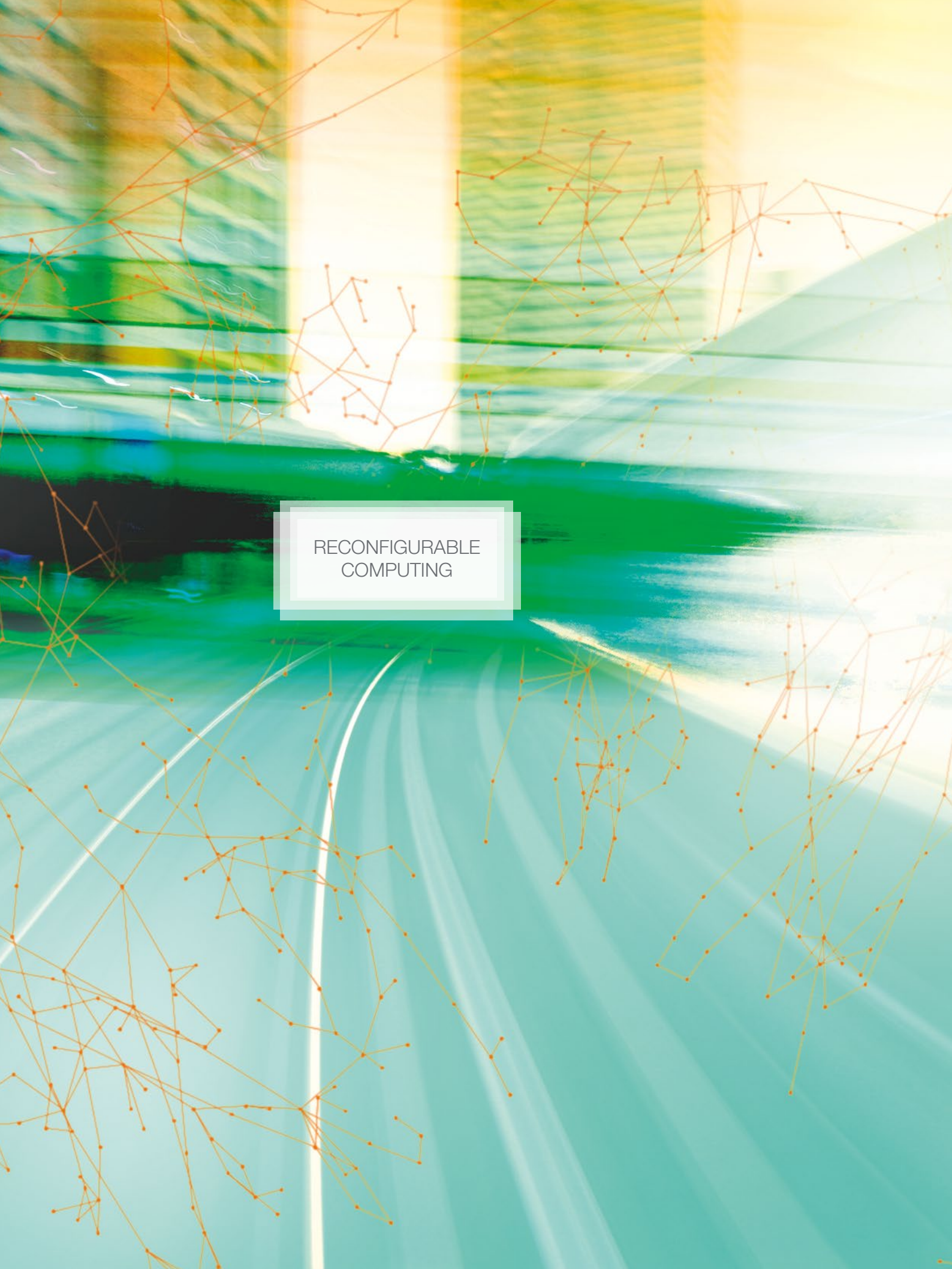
Napatech helps companies to reimagine their business by bringing hyperscale computing benefits to IT organizations of every size. We enhance open and standard virtualized servers to boost innovation and release valuable computing resources that improve services and increase revenue. Our Reconfigurable Computing Platform™ is based on a broad set of FPGA software for leading IT compute, network and security applications that are supported on a wide array of FPGA hardware designs.

Additional information is available at www.napatech.com

Napatech. RECONFIGURABLE COMPUTING

[2] Source: ponemon institute “the cost of malware containment”, january 2015

NOTES


RECONFIGURABLE
COMPUTING

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

DN-1183 Rev. 2