napatech

# TIME TO RETHINK NETWORK SECURITY

There are three major trends currently unfolding that promise increased efficiency and effectiveness in how we do business. These are cloud computing, big data analysis and mobility. However, with these benefits there are also vulnerabilities that need to be addressed, not least of which is ensuring that valuable data is available and secure. The challenge is to provide this security without handicapping the adoption of these trends and undermining the potential benefits they provide. What is required is a holistic view of network security based on correlation of both network and security information in real time.

# TIME TO RETHINK NETWORK SECURITY

**Cloud computing, big data analysis and mobility are three current trends that promise increased efficiency and effectiveness. In short, access to real-time decision data anytime, anywhere on any device. Unfortunately, these benefits come at a cost. To provide this kind of access opens vulnerabilities that cybercriminals are more than motivated to exploit. How can we secure valuable and critical data without compromising efficiency?**

No single product can address this challenge, but by combining the strengths of existing products we can build an effective security solution. By combining network and security information, a more holistic solution can be adopted that can address vulnerabilities with certainty and precision. By understanding the behavior of the network, using this information to detect anomalies and then comparing this information with security events, it is possible to act immediately in addressing potential attacks.

In the following, we will take a closer look at the major trends and the expected growth in data that these will partly drive. We will also look at the security challenge as highly organized cyber criminals target the vulnerabilities that these trends expose. A solution is proposed based on available products. We will focus on some of the challenges that vendors of these products must address in order to be effective in meeting the security challenges identified. We will also evaluate what technologies are available today that can help both now and in the future.

## UNDERSTANDING THE BENEFITS OF CLOUD COMPUTING, BIG DATA ANALYSIS AND MOBILITY

The combined benefit of cloud computing, big data analysis and mobility is the availability of real-time data for decision-making at anytime, anywhere, accessible from any device.

Cloud computing provides the ability to centralize data in a way that makes it accessible at anytime from anywhere. Mobility increases this accessibility adding a level of convenience and efficiency for cloud service users. The centralization of data, that is the essence of cloud computing, enables real-time analysis in relation to historical data to identify trends and opportunities. This big data analysis provides an efficient overview of key data to support decision making, which can form the basis for highly effective reactions in real time to unfolding events and opportunities.

These three trends combined promise to revolutionize digital services making them more user friendly and responsive.

## UNDERSTANDING THE VULNERABILITIES OF CLOUD COMPUTING, BIG DATA ANALYSIS AND MOBILITY

The underlying enabling foundation of all three trends is the ubiquity and accessibility of the Internet. Once you have access to the Internet, you can take advantage of these three trends. But, this is also the basis for the vulnerability of these trends, as this accessibility is also available to cyber criminals.

The centralization of data in cloud data centers provides fewer, but more attractive locations to target. In this sense, life just got easier and at the same time more challenging for the cyber criminal. But then again, the challenge is part of the appeal. Instead of many, small cyber villages, we now have a few cyber castles. Let the siege begin!

Mobility is the potential weakness in the defense as access to the cloud computing services is made available on a wider range of mobile devices that are sometimes beyond the control of the cloud service provider or the client enterprise. The Bring Your Own Device (BYOD) trend is a case in point where it is efficient to allow access to data for employee owned devices, but opens potential vulnerabilities as they are not as strictly controlled and managed as other access devices, such as corporate laptops.


FIGURE 1
How to secure availability without compromising efficiency?

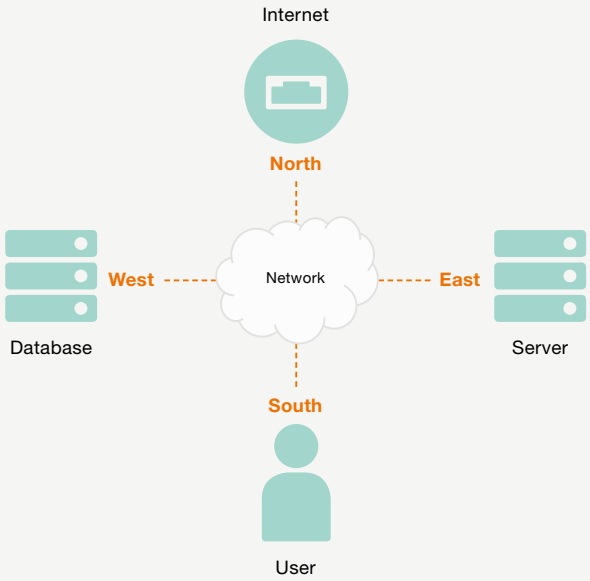



FIGURE 2
Traditional north-south traffic now complemented by east-west traffic

Big data, in this regard, merely ups the stakes. It is the treasure that the cyber criminals want to get their hands on or, at the very least, prevent access to. As we rely on the Internet for all manner of services including financial transactions and customer database access, the value of this big data is only set to increase. This is what makes mounting the siege worthwhile.

## UNDERSTANDING THE CHALLENGES

Cloud computing centralizes large amounts of data in fewer locations. This increases the amount of data being handled and thereby the speeds at which this data is being transported. In short, this means more data at higher speeds. On the positive side, the centralization of data also leads to the centralization of IT competence. Cloud service providers should thus be in a position to invest and attract the expertise to implement world-class security solutions. From this perspective, outsourcing IT processes to cloud service providers should make your data more secure if you are a small-to-medium enterprise.

Big data analysis adds the extra dimension that traffic flows within the network are prone to change. Traditionally, traffic has flowed in a “north-south” direction from the interface to the external internet connection in the “north” to the user on their PC client in the “south”. With big data analysis, large amounts of critical data is now being exchanged between storage databases in the “west” and servers in the “east” of the network. There are therefore traffic flows in all directions, which complicate the situation and demand a rethink with regard to which points in the network need to be monitored and secured.

Mobility adds the extra complexity that the “south” interfaces are also moving. One can no longer assume that a particular user will use a stationary PC client to access services. The user could turn up anywhere in the network using a mobile device to access services.

From a network security point of view, the challenges can thus be summarized as understanding the new network profile and identifying where network security solutions are required, monitoring these critical points and ensuring that the products used can keep up with increasing speeds and data loads.

## INCREASING LOADS, SPEEDS AND ATTACKS

It comes as no surprise that data loads are on the increase, but few consider the implications. We rarely feel the impact in our daily lives beyond waiting for a web page to download. Most enterprise networks are over-dimensioned to ensure that there is bandwidth overhead to handle high-load situations.

In other words, we plan for worst case scenarios and throw bandwidth at the problem. On average, this works, as communication services can be prioritized so the most

sensitive services are guaranteed bandwidth and other services can accept data re-transmissions in the event that packets are dropped due to congestion.

However, if you need to monitor and analyze data on a particular connection in real time, you cannot afford to drop packets. Increasing loads is therefore an issue that cannot be ignored and network appliances, be they for performance monitoring or network security, need to ensure that they can see the entire picture in real time otherwise the analysis of the real-time situation is incomplete. For example, Distributed Denial of Service Attacks (DDoS) can seek to exploit throughput limitations by bombarding in-line security appliances with data to such an extent that the security appliance must surrender and lower the drawbridge or deny services to users. Ideally, the appliances used in the network should have the capacity to handle the theoretical maximum amount of data and flows that could be expected to be generated so that this type of attack will not succeed.

As data loads increase, data speeds will also increase as we enhance the capacity of connections and aggregate these into even higher speed connections. So, not only do you need to handle more data, but you also have to do it at higher speeds. Higher loads and speeds are challenging enough, but then we also need to consider that the number and types of attacks are also growing exponentially. Cyber criminals are continuously innovating new ways to succeed in penetrating defenses, often using a combination of attacks. For example, using a DDoS attack as a diversion for introducing a Trojan horse or other malware into the network.

To successfully defend against such multi-layered attacks, it is important to think holistically and use all means available to identify and address breaches in security. The key is establishing the network-wide view of what is happening on a real-time basis so the right defensive measures can be brought to bear where they are needed most.

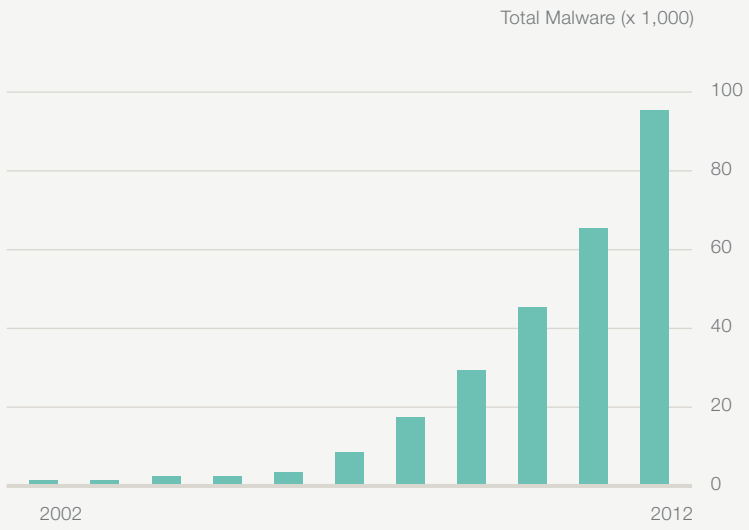
## SECURING THE NETWORK STEP-BY-STEP

Most networks already have network or application performance monitoring appliances installed. These are capable of providing real-time information on network and application usage. By collecting and analyzing this data, it is possible to build a profile of usage over time. This is a type of network behavior analysis that can provide insight into typical traffic flows and application usage at different times of the day and days of the year.

Monitoring the network in real time can help detect anomalies. An example could be an increase in traffic between two nodes that do not normally communicate with each other. This can be the first sign of an attack and at the very least demands closer scrutiny.

As mentioned earlier, traffic flows are likely to change and real-time monitoring in this way can provide the first signs that a new traffic flow profile is being established and that there is potentially a need for extra bandwidth or a need to provide increased security at these points in the network. Particularly, big data analysis could result in critical data being transported over network links that are not normally

**FIGURE 3**
Number of attacks growing (source: AV-Test GmbH)



protected or have limited bandwidth. Real-time monitoring helps to identify these needs early, allowing action to be taken before it affects customer service level agreements.

Introducing Security Information and Event Management (SIEM) as a concept on top of this network behavior monitoring allows correlation of information from the various network security appliance solutions with network behavior information. With SIEM, network behavior anomalies can be compared against information from network security appliances to identify if an attack is underway or not.

If network security appliances cannot provide confirmation, then the attack could potentially be a zero-day threat, which has not been seen before and has evaded detection. With this real-time information it is possible to react immediately to take the necessary actions to limit the extent of the attack.

Conversely, the network security appliance can indicate that an attack is taking place, but the network behavior analysis indicates that no anomalies are seen in the network. This could be an indication of a false positive in the network security appliance, which can occur, often to the irritation of users who cannot understand why their legitimate transaction is not being processed.

## OPPORTUNITY TO RETHINK NETWORK SECURITY APPLIANCE DESIGN

By thinking holistically, we can begin to see network security in a new light. Network security products today are functionally focused with different appliances providing different functions that in combination provide increased security. For example, network security solutions would normally comprise of a firewall, Intrusion Detection or Prevention System (IDS/IPS), a web and/or email security gateway, Data Loss Prevention (DLP) system and other more focused network security appliances.

We have seen a desire to consolidate this functionality into one appliance with Universal Threat Management (UTM) appliances and recently next-generation firewalls. There are also vendors with “software blade” concepts that allow different types of security functionality to be introduced on the same platform on a need basis.

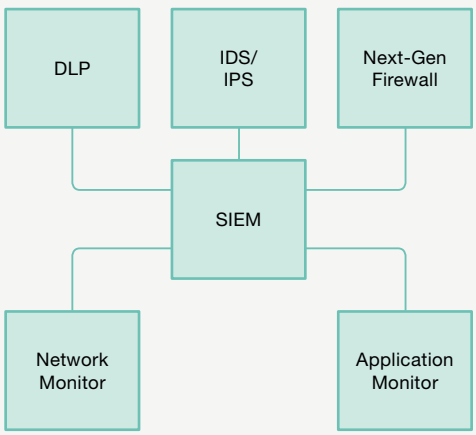
What is important is the ability to introduce the functionality needed as quickly and easily as possible at different locations in the network in line with shifts in traffic profiles. It is therefore advantageous if the functionality in some way can be disassociated from the underlying hardware allowing multiple functions to be introduced at the same location or easily moved.

In short, what is required is a universal hardware platform that is capable of supporting multiple functions, but can be scaled independently of functionality in-line with network speeds and loads.

## STANDARD SERVERS RISING TO THE TASK

Standard servers are now in a position to support the need for a universal hardware platform and can today support more than 100 Gbps of throughput. The strong roadmaps of

**FIGURE 4**
A holistic approach to network security



leading server CPU vendors promises annual improvement in performance by as much as 30%. This, combined with the fact that these vendors are also some of the first to adopt new manufacturing geometries, makes it very hard to compete with this kind of roadmap.

With standard servers, performance can be scaled on a per CPU core basis. This means that if the network security application is designed for multi-threaded performance on a standard server architecture, then it is possible to improve performance by adding more CPU cores to the server. If that is not enough, then it is possible to port the application to a newer server with more powerful CPU cores.

Using standard servers effectively decouples the network security application from the underlying hardware allowing scalability and flexibility.

But, to reap these benefits, it is also important to have the right data input/output solution.

> Napatech accelerators are designed for applications that need to monitor and analyze large amounts of data in real time

## ASSURING MONITORING AND ANALYSIS PERFORMANCE

Napatech accelerators for network management and security applications are designed for applications that need to monitor and analyze large amounts of data in real time. This includes the network and application performance appliances needed to understand network behavior, but also many network security appliances. This is because these appliances face some of the same challenges of analyzing large amounts of data in real time in an effective way.

There are basically two deployment modes for network security appliances that need to be considered. Many appliances are deployed in an off-line, passive mode where data is captured in real time for analysis. An example of this type of security appliance is an Intrusion Detection Systems (IDS). The second kind of deployment is in-line where the appliance is receiving traffic, analyzing the traffic in real time and then transmitting the traffic onwards. An example of this type of appliance is an Intrusion Prevention System (IPS), which provides the same functionality as an IDS, but has the capability to block traffic immediately.

For Data Loss Prevention (DLP) appliances, there are examples of appliances that that can be deployed in a passive off-line mode and others that are deployed in-line.

Napatech accelerators are available for both off-line and in-line modes including bypass options for in-line deployments. What is common for both is the ability to receive data at full line-rate even when network links are fully loaded. The accelerators have the ability to identify flows up to layer 4 including tunneled fragmented traffic. These flows can then be intelligently distributed to the various CPU cores in the server.

With this capability, it is possible to develop multi-threaded network security applications that can run on the multiple powerful CPU cores available in the standard server. Today, network security appliance vendors are implementing various products, such as IDS/IPS, DLP, Secure Web Gateways and other security solutions using this approach.

In addition, SIEM vendors also use this approach to implement dedicated probes for network behavior analysis, which is an alternative to using network and application performance analysis probes from other vendors.

## CONSOLIDATING MULTIPLE FUNCTIONS

Not all links in the network need to run at 10 Gbps, though more consolidation of services in larger data centers will drive higher data loads and network speeds. Nevertheless, there will be opportunities to combine functionality into a single physical server. This can be driven by a need to offer multiple functions at one location, but can also be driven by a need to scale an analysis application to higher network speeds, where the application software is not capable of handling this amount of data today. In this case, multiple instances can be run simultaneously on the same server.

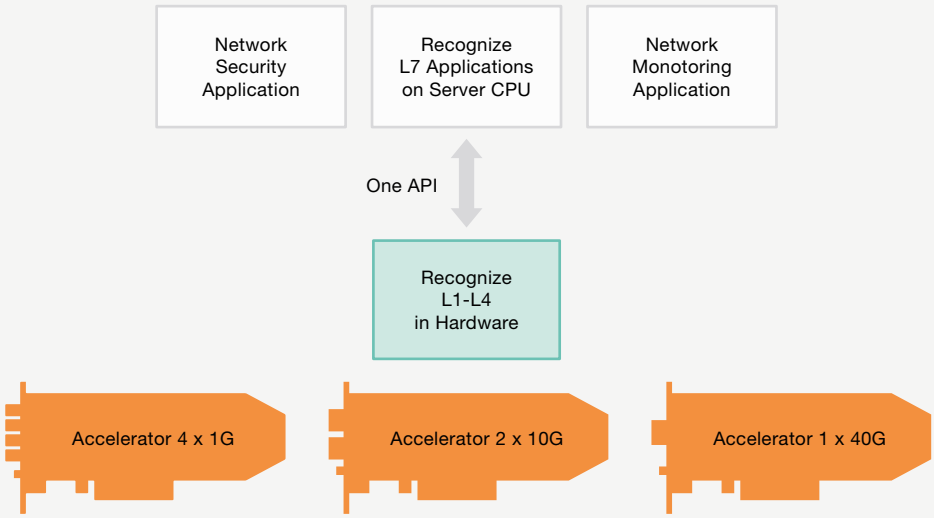



**FIGURE 5**
Rethinking network appliance design for scale and flexibility

Napatech accelerators support these consolidation cases by providing data merging and sharing capabilities. Data from multiple ports on multiple accelerators can be merged into a single analysis stream that can then be shared amongst multiple applications. The stream is shared and not replicated, which allows this solution to be used in high speed, high data load environments.

As mentioned earlier, the data stream can be intelligently distributed to multiple CPU cores based on the type of traffic detected. However, it can also be load balanced providing an equal load to each CPU core.

This approach allows multiple simultaneous applications to run on the same server and lends itself to the software blade approach of offering optional application packages.

Another option is to virtualize application software. In this case, each application can be run in its own virtual machine. The advantage of this approach is that application software from various appliances with different environments and operating systems can be run on the same server, with each application seeing an environment that is familiar despite the fact that it is now running on a new server. This is very useful in porting existing solutions to a consolidated server.

By using standard servers, we thus decouple the generic hardware from the application-specific software allowing new combinations of functionality in a more modular fashion that lends itself well to the increasingly dynamic nature of networks that we expect to see in the near future.

## THINK HOLISTICALLY AND RETHINK SPECIFICALLY

It is possible to build a highly responsive network security solution by using all the appliances at our disposal, and the information they provide, in a more holistic fashion. Using SIEM as a driving concept, it is possible to provide a correlation of network behavior information with information from security appliances to build an accurate picture of what is happening in real time. This enables the ability to respond immediately to any anomalies detected.

By ensuring that each individual appliance has the capacity to handle the data load and speeds, OEM vendors can ensure that these appliances are available and are providing actionable information. By basing development of these appliances on standard servers with accelerators, it is possible to take advantage of strong roadmaps to keep up with increasing data loads and speeds.

In addition, standard servers provide the opportunity to decouple applications from hardware allowing a re-think on what kind of functions can be offered and how they can be provided in a more flexible, modular manner.

## DISCOVER THE POWER OF NAPATECH

Napatech accelerators are designed to handle the maximum theoretical throughput of data for a given port speed. Napatech offers a range of accelerators supporting speeds from 10 Mbps to 100 Gbps. A single, common Application Programming Interface (API) allows application software to be developed once and used with a broad range of Napatech accelerators. This allows combinations of different accelerators with different port speeds to be installed in the same server. Additional features include:

- Napatech accelerators can identify, filter and distribute flows to up to 32 CPU cores
- Data merging functionality allows flows from different ports on different accelerators to be merged for analysis
- Data sharing functionality allows multiple applications to access the same data at the same time
- All of this can be performed with very low server CPU load

## CHOOSE THE MARKET LEADER

Napatech is the market leading provider of accelerators for network management and security applications. Napatech provides global sales and support from local offices in all major continents, which is included in the price of the accelerator. This means that our highly experienced support resources are available for design and integration support, as well as field support without extra charge.

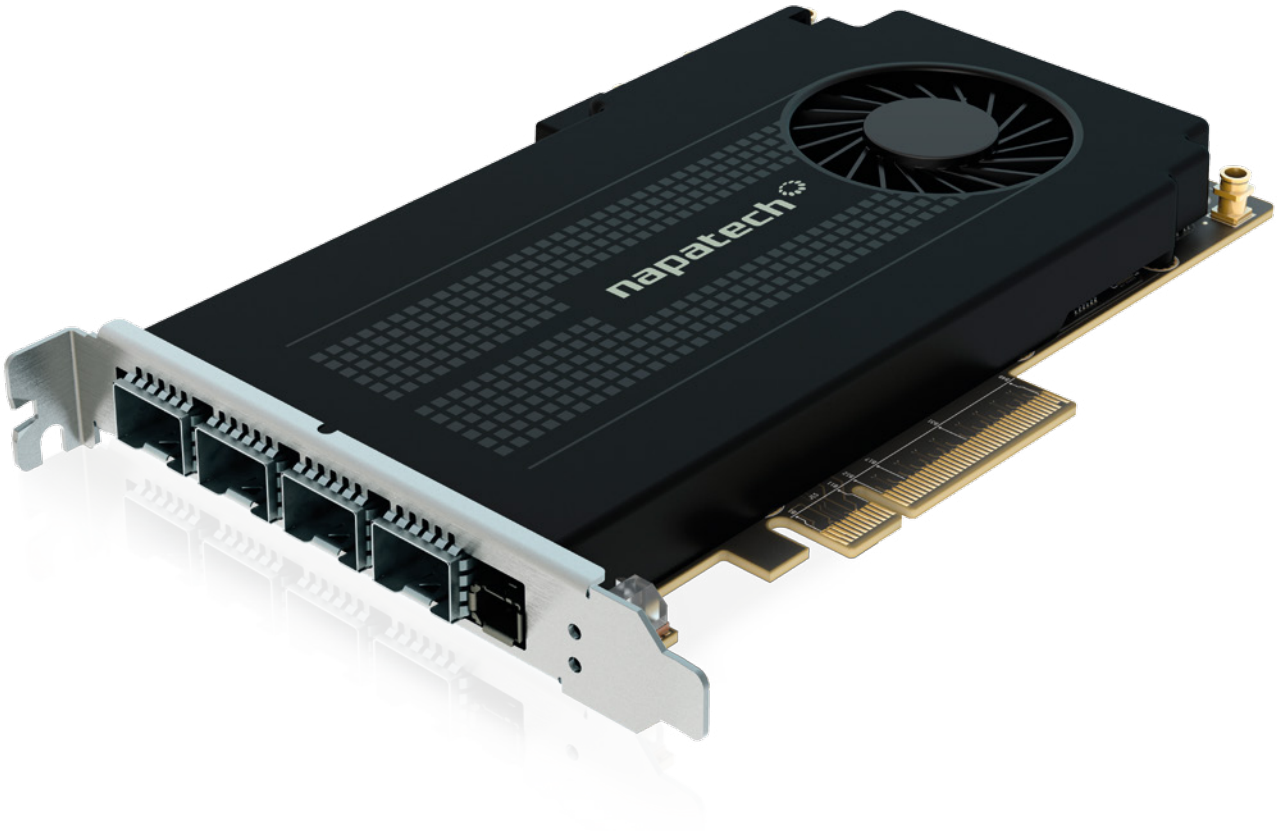
Napatech accelerators are manufactured to the highest standards by outsourced manufacturers in Switzerland and the USA supporting all major certifications including NEBS for telecom applications.

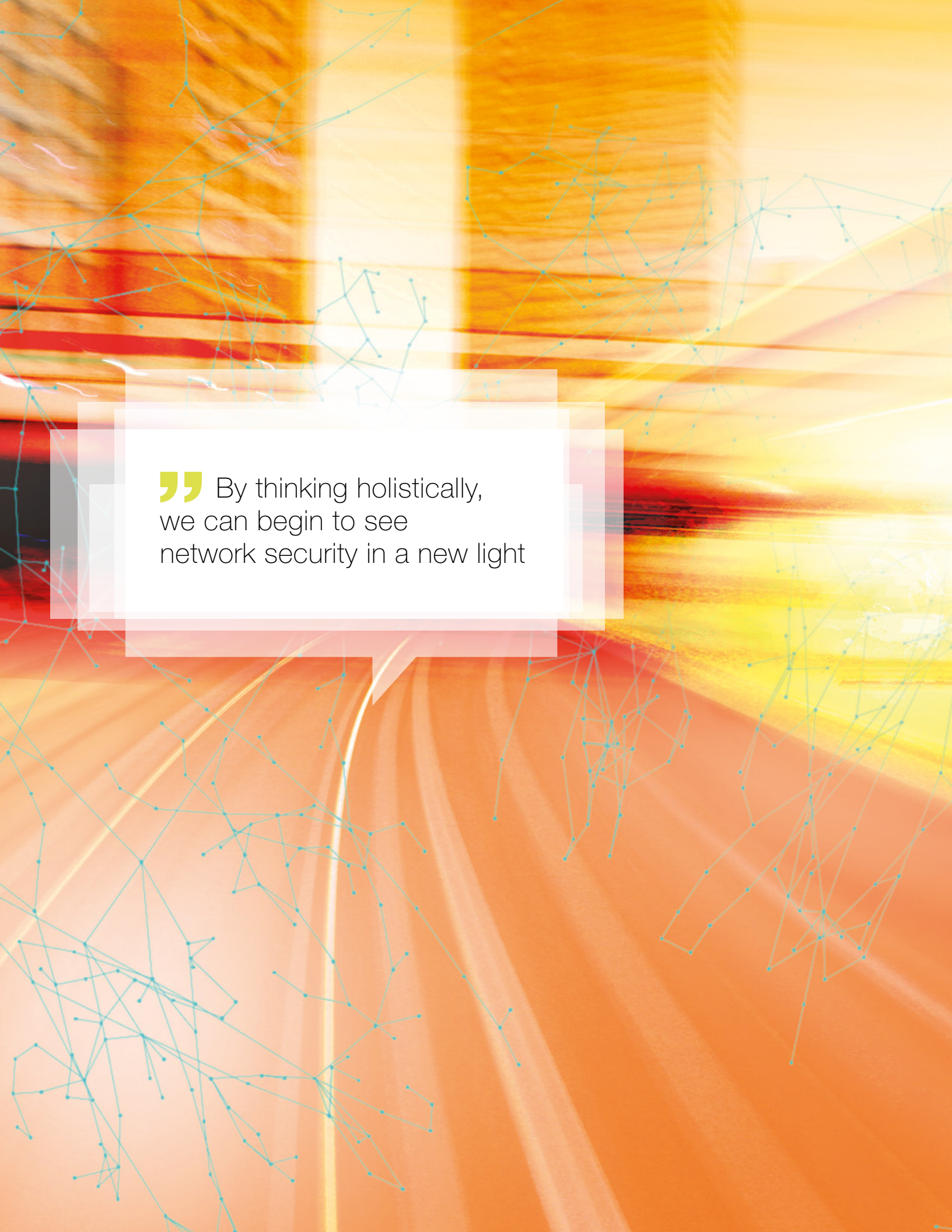
## COMPANY PROFILE

Napatech is the world leader in accelerating network management and security applications. As data volume and complexity grow, the performance of these applications needs to stay ahead of the speed of networks in order to do their jobs. We make this possible, for even the most demanding financial, telecom, corporate and government networks.

Now and in the future, we enable our customers' applications to run faster than the networks they need to manage and protect.

**Napatech. FASTER THAN THE FUTURE**




By thinking holistically,
we can begin to see
network security in a new light


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

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

**NORTH AMERICA**
Napatech Inc.
Boston, Massachusetts
Mountain View, California
Washington D.C.

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

**SOUTH AMERICA**
Napatech
São Paulo, Brazil

Tel. +55 11 2127 0782
ntsouthamericasales@napatech.com
www.napatech.com

**APAC**
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