WHITE PAPER

Data Center
Network Monitoring and Cyber Security

You Can't Secure What You Can't See

Discover the value of network visibility for cybersecurity

Authors

Daniel Joseph Barry
VP of Strategy & Market Development
Napatech

Jeff Nigh
Sr. Technical Solution Specialist
Intel® Corporation
Programmable Solutions Group

Table of Contents

Introduction 1
Relying on perimeter defenses is no longer enough. 2
More complex networks 2
Detecting breaches faster. 3
Building your own visibility infrastructure 3
Is packet loss an issue? Absolutely! 4
FPGA acceleration for reliable cybersecurity 4
Field Programmable Gate Arrays 4
Various types of security solutions possible 5
Security Monitoring and Forensic Solution 5
Create adaptable security architectures. 5
The bottom line 6
FPGA technology from Intel and Napatech 6
Conclusion. 6
Where to get more information. 6

Introduction

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

Simply throwing more money at 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 defenses are architected and deployed. Not just from a technology point of view, but also from a return on investment perspective.

Figure 1. Traditional cybersecurity defenses that rely on prevention alone are no longer enough to stop cybercriminals.

In this paper, we will look at the latest expert advice on how to design cybersecurity defenses, the importance of continuous monitoring and analysis and, above all, the possibilities and cost benefits enabled by open source software and FPGA-accelerated standard servers.

We will be exploring why more and more enterprises are leveraging these new possibilities to build their own cybersecurity solutions, looking at how they provide insight into more places in the network and enable the continuous monitoring and analytics required to combat cybercriminals.

Example use cases will be described to demonstrate how open source software on standard servers with FPGA acceleration can be deployed to improve security postures. This will be validated through specific results achieved with Intel® FPGA Programmable Acceleration Cards Intel FPGA PACs and Napatech Link* Capture Software.

Relying on perimeter defenses is no longer enough

According to security experts and analysts such as Gartner, traditional cybersecurity defenses that rely on prevention alone are no longer enough to stop cybercriminals. Threat prevention needs to be complemented with solutions that can detect threats based on continuous network monitoring and analysis.

In "Designing an Adaptive Security Architecture for Protection from Advanced Attacks" (www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection), Gartner described the concept of an adaptive security architecture. In the analysis, Gartner concluded that there is an overreliance 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 Figure 2.

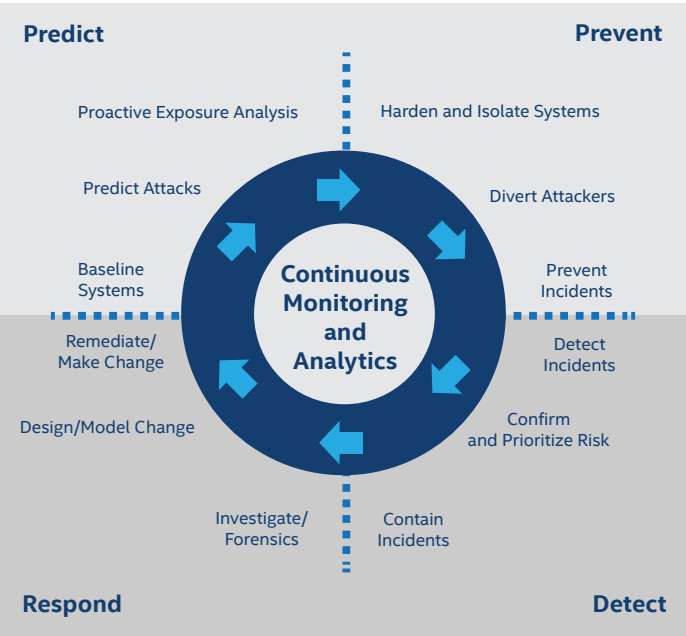

Figure 2. The four stages of an adaptive security architecture

Source. www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection

The key enabler underpinning the adaptive security architecture framework is the capability to perform continuous monitoring and analytics. 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 evade security threat prevention solutions for one reason or another. It is therefore important to monitor activity to detect any anomalous behavior that could indicate a breach.

More complex networks

Enterprise networks are becoming more complex on several 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 datacenters and hosted cloud services, which again add to the complexity of the environment to be monitored.

According to IHS Markit (IHS Markit "Cloud Service Strategies & Leadership Survey North America" and "Next Gen Threat Prevention Strategies and Vendor Leadership Survey North America", from 2017), 57% of surveyed enterprises expected to operate a mix of on-premise and managed security services using 11 different cloud service providers.

In such a complex environment, the number of potential sources of attack have multiplied and attacks can now occur from within the enterprise network, circumventing perimeter defenses.

Detecting breaches faster

Research shows that the faster one can detect and react to a breach, the lower the impact and associated cost.

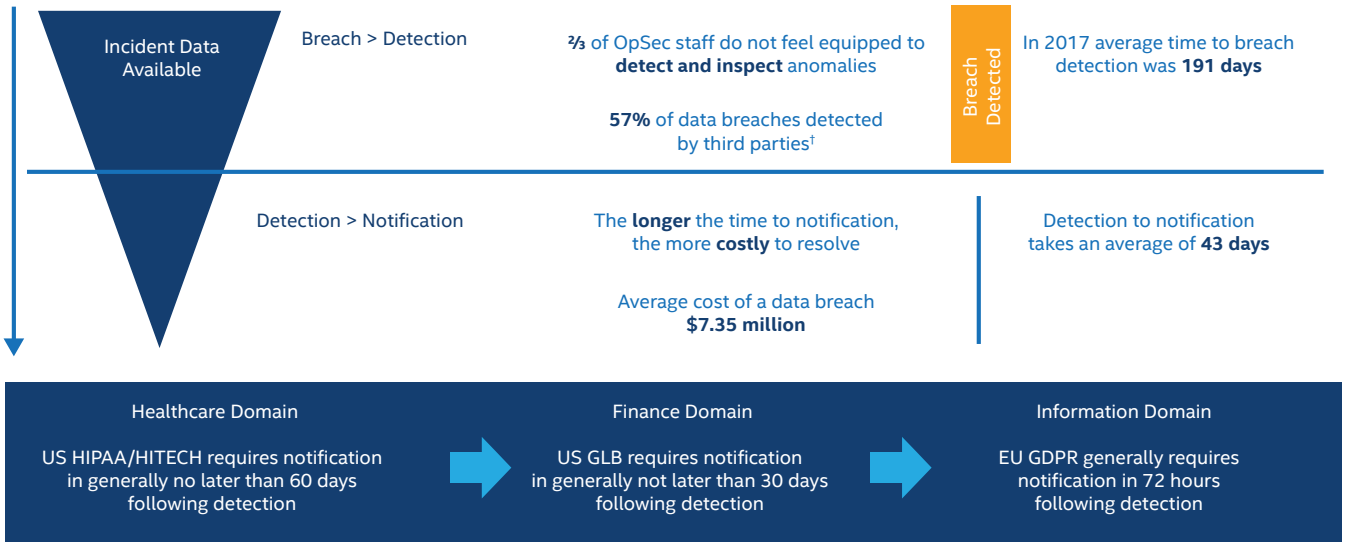

Figure 3. Average time from breach detection to notification
Source. IBM Security / Ponemon Institute, June 2017
† Trustwave Global Security Report

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

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

Building your own visibility infrastructure

Because most commercial solutions are cost prohibitive, more and more enterprises are exploring the option of building their own cybersecurity probes and appliances. Never has it been more viable to pursue this option. There is 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. In fact, these tools are often the basis of commercial offerings as well.

The advantage of building your own probe or appliance is that it can provide exactly the level of visibility and insight you need, where you need it – and include precisely the features you require, nothing more, nothing less. Considering the cost of commercial solutions, this provides a compelling alternative that can greatly 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 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.

One of the big challenges is packet loss. Whether the security monitoring solution 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.

Figure 4. Building your own probe provides exactly the level of visibility and insight you need, where you need it.

Is packet loss an issue? Absolutely!

When packet loss issues arise, it is not just a question of one packet here or there, but several packets lost at the same time. This can compromise the entire session 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 need to gain more insight into what is happening. An irony that is not lost on the cybercriminal. Therefore, zero packet loss is essential to ensure that defenses are up to the task when needed most.

FPGA acceleration for reliable cybersecurity

To ensure zero packet loss, it is important to use NICs that are designed for the task. FPGA-based accelerator cards, also referred to as an FPGA Accelerated NIC, are ideal for this purpose as they not only deliver the raw throughput and deterministic performance required, but also provide the intelligent processing of data that will address all aspects of packet loss.

An FPGA Accelerated NIC solution includes two important parts; the PCI Express* (PCIe*) card with FPGA-chip onboard that replaces the standard NIC and the FPGA "image" software that implements the features and capabilities to be executed on the FPGA.

Field Programmable Gate Arrays

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.

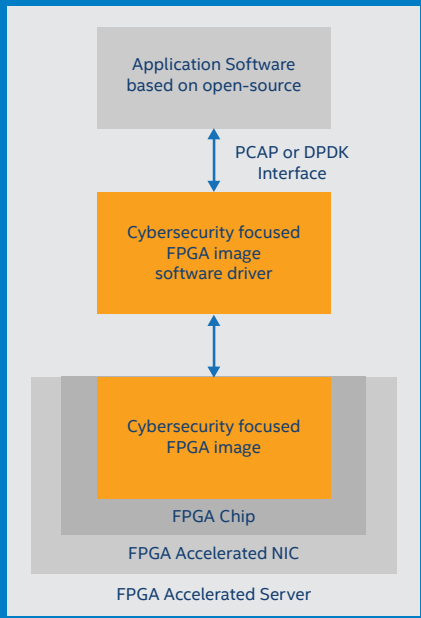

Figure 5. What is an FPGA?

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

Solutions based on an FPGA Accelerated NIC 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 divide the processing and analysis of data over multiple CPU cores leading to a higher level of performance.

In short, by replacing standard NICs with FPGA Accelerated NICs, it is possible to ensure zero packet loss, improve performance significantly and enable high-speed probes and appliances built to support open source applications like Snort, Suricata, and Bro.

Various types of security solutions possible

Several types of security monitoring solutions are possible using open source software running on standard servers with FPGA Accelerated NICs 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

Figure 6 shows an example of a cybersecurity solution combining some of the above capabilities. It involves two servers, each with their own FPGA Accelerated NIC and dedicated FPGA image software. In the first server, we are using a Suricata-based IDS application to examine data in real time and identify any suspicious traffic. In the second server, we are using a security forensics application and network recorder to capture all the network data to disk with zero packet loss for retrospective 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.

Security Monitoring and Forensic Solution

1. Network tap provides data to servers with FPGA Accelerated NIC 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. Application software 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.

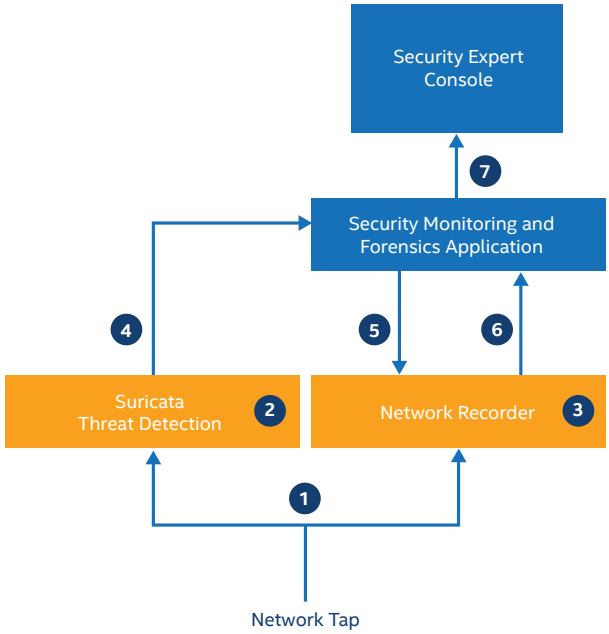

Figure 6. Security monitoring and forensic solution

Create adaptable security architectures

As a standard server with an FPGA Accelerated NIC can support a wide range of cybersecurity solutions, it is possible to extend defenses and implement an adaptable security architecture purely by using different software applications.

IDS applications can provide the detection capabilities needed. 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 these solutions can be based on the same reconfigurable platform: a standard server with an FPGA Accelerated NIC and 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 infrastructure with broad network visibility, it is possible to quickly determine if an incident is in fact a breach or merely a false positive.

This is a crucial point, as a typical security expert needs to examine up to 17,000 alerts in just one week (Ponemon Institute "The cost of malware containment"). Many of the largest cyberattacks have been successful; not because the breach was not detected by security defenses, but because the security team was overburdened and lacked the tools and insight to quickly determine whether an incident was indeed a breach.

By building your own infrastructure using open source applications on standard servers with FPGA acceleration, you can attain the network visibility required to focus your efforts where they are needed.

FPGA technology from Intel and Napatech

Intel FPGA PACswith Napatech Link Capture Software is uniquely suited for this type of deployment. The solution guarantees zero packet loss and more than doubles the performance of cybersecurity applications like Suricata even when using a full signature set. What that means, in practice, is that less than half of the server CPU power is now required to run the same application. This is achieved by offloading burdensome processes and workloads related to high-speed packet processing, thus freeing up valuable compute resources and returning them to the applications.

If we do the math, this could very well be the decisive factor between purchasing a dual-socket or a quad-socket server, with the latter costing about four times more, i.e. $20,000. As relatively few applications need quad-socket servers, volumes are lower, and the motherboard is a lot more expensive. 2X the price, the reality is the price x4. In other words, halving the number of cores is a significant saving: up to $15,000 per server.

Intel FPGA PACs with Napatech Link Capture Software has been benchmarked across a wide range of other cybersecurity applications, covering open source, custom-developed, as well as commercial tools. Common to all is a dramatic performance improvement achieved from FPGA acceleration, compared to servers with standard NIC configurations. Complete solution configurations, installation guides and performance results are available today for Suricata, n2disk, TRex, and Wireshark.

Conclusion

As we have seen, threat prevention is no longer enough to protect against motivated, advanced attackers. An adaptive security architecture must be complemented with improved capabilities to detect, contain, and respond to an incident – and this requires complete visibility.

Numerous commercial offerings are available, but many are cost prohibitive and leave little room for customization. Enterprises are therefore looking at building their own monitoring solution based on off-the-shelf servers, but with just a standard NIC deployment, the risk of packet loss is severe.

The solution is to use a standard server with FPGA acceleration, which brings the following benefits:

- Firstly, the right FPGA acceleration technology will ensure that not a single packet is lost, thus guaranteeing complete visibility, strengthening your threat detection capabilities – and potentially saving your company millions.
- Secondly, the right FPGA solution will allow you to maximize your CPU utilization and multiply application performance. This again will enable a more robust security posture while also yielding significant savings at a system level.

Where to get more information

- Find more information about Intel Programmable Acceleration Cards, visit www.intel.com/content/www/us/en/programmable/products/boards_and_kits/dev-kits/altera/acceleration-card-arria-10-gx/overview.html
- Find more information about the Napatech Link Capture Software, visit www.napatech.com/products/link-capture-software-for-intel/

† Tests measure performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks.