Achieving Visibility, Versatility and Value with Network Functions Platforms

Array Networks AVX Series for Security

Foreword

by Michael Suby, Frost & Sullivan

Cybersecurity is at a must-change crossroads. Consider the state that many organizations find themselves. Over time they have accumulated numerous stand-alone security appliances to defend against a broadening range of attack vectors. These independent appliances, while well intended, step up administrative overhead while hoping for operational efficacy that seldom materializes – neither at the individual appliance level nor across scattered appliances. Simultaneously, the number of alerts generated from this appliance sprawl – plus servers and networking gear – creates perpetual alert overload, which contributes to the very real and rising potential that true security incidents are overlooked until it is too late. In essence, there is no facility to avert damage before it occurs.

The direness of this situation is further compounded by:

- A perennial shortage in skilled security practitioners
- An insistence that security be effective without adding latency to end-to-end processing
- The accelerating pace of change demanding that all technology disciplines – compute and storage, networking, and security – operate with the same high degree of agility as software development, individually and collectively

At this crossroad, we recommend that enterprises veer right and seriously consider using virtual network functions, with those functions operating in a purpose-built network functions platform. As described in this white paper, a network functions platform is explicitly designed to deliver isolation with modularity, uncompromising processing speed, and cross-discipline automation. Let us explain:

- **Isolation with modularity** – With intensifying scrutiny on data privacy, organizations must take appropriate precautions to inspect encrypted traffic for malicious intent, but without exposing private data outside an isolated and auditable container. A network functions platform is designed to run various inline inspection functions within a sandwiched container of de-encryption and re-encryption.
- **Uncompromising processing speed** – Built for speed, a network functions platform anticipates the properties required for compute-intensive security functions. Administrators merely define the workload's requirements and dedicated resources are instantly provisioned. Similar to air traffic control where a plane is not allowed to take off unless approved to land, a network functions platform reserves a dedicated lane of resources to the workload until that workload ceases.
- **Cross-discipline automation** – While theoretically desirable to have each technology discipline gain expertise in other disciplines for the purposes of rapid and seamless cross-discipline orchestration, the reality is that each discipline has its hands full just staying current. A network functions platform, however, addresses this desired state by automating routine tasks of other disciplines. For example, rather than calling on peers to size, test and provision server and networking hardware, the platform accomplishes this through in-platform automation – a direct contributor to improved agility.

Turning back the appliance sprawl in security and, with that, simplifying and improving the efficacy of the security discipline is not an overnight occurrence. Yet, a network functions platform is an important step that can be taken now. We recommend you read on to gain an even greater appreciation of what this type of platform can do for you.

Michael Suby, VP of Research, Frost & Sullivan

FROST & SULLIVAN

TABLE OF CONTENTS

Security is a constantly evolving challenge for IT teams – evildoers continually change their tactics and explore new threat vectors in an attempt to exploit enterprise assets and personal information. To successfully defend against these chameleon-like threats requires approaches that are equally versatile and provide broader and deeper levels of visibility.

Virtualizing networking and security functions – commonly described as NFV – holds significant promise for a more adaptive approach to security; however, adoption has been slowed due to operational, organizational and ROI concerns, among others.

Recently, a new class of products, referred to as Network Functions Platforms, has started to receive coverage by the IT industry press. The name hints at something to do with NFV, but that's only part of the story. A deeper dive will help clarify just what this solution category can do for enterprise security as a whole, and shine a light on some compelling new security use cases.

First, it is important to understand the current virtualization landscape as it relates to networking, security and enterprise adoption.

- Consensus among recent market surveys and analyst reports indicates that although only a small number of enterprises have implemented virtualized networking and security in their production networks, greater than half of all businesses are currently analyzing strategies and vendors.
- The key driving factors for considering virtual networking are 1) a desire to accelerate the provisioning of services and 2) to gain greater agility and efficiency in leveraging IT infrastructure. Additional business drivers include anticipated reductions in CAPEX and OPEX – all factors that hold particular relevance for IT security.
- Standing in the way of faster and more widespread adoption are concerns around 1) organizational disruption among server, virtualization, networking and security teams, 2) skills deficits with respect to new technology, 3) the lack of maturity of current solutions, 4) inability to clearly define ROI and 5) ensuring enterprise-class performance and security.

The takeaway is that there is a clear interest in virtualizing networking and security functions on the part of enterprises, driven by the need to become more 'cloudy' and software-centric in their approach to supporting IT requirements. Enter the Network Functions Platform, a virtualized hardware platform that is purpose-built to run networking and security virtual appliances (VAs), while at the same time addressing challenges to NFV adoption and providing enhanced visibility and greater versatility in responding to today's continually evolving security landscape.

What is a Network Functions Platform?

Think of the Network Functions Platform as a virtualized server on steroids, a compute environment specifically designed to run security and networking workloads. Because security functions such as next-generation firewalls, Web application firewalls, DDoS protection and SSL VPNs are more compute-intensive as compared to application workloads, the Network Functions Platform is engineered from both a hardware and software perspective for scalability and performance SLAs.

Service agility with guaranteed performance is a combination not previously available to IT managers. Virtual appliances offer great agility, but because they typically run on commercial off-the-shelf (COTS) servers, performance suffers – especially for resource-consuming security VAs. Conversely, while dedicated hardware appliances offer the guaranteed performance required by security services, they do not provide the agility needed in dynamic environments. Thus, Network Functions Platforms offer the best of both worlds: the flexibility of software and the performance guarantees of hardware.

Importantly, the Network Functions Platform is also designed to mitigate organizational disruption and skill deficit concerns by abstracting and automating tasks that otherwise would entail complicated server, virtualization and network configuration.

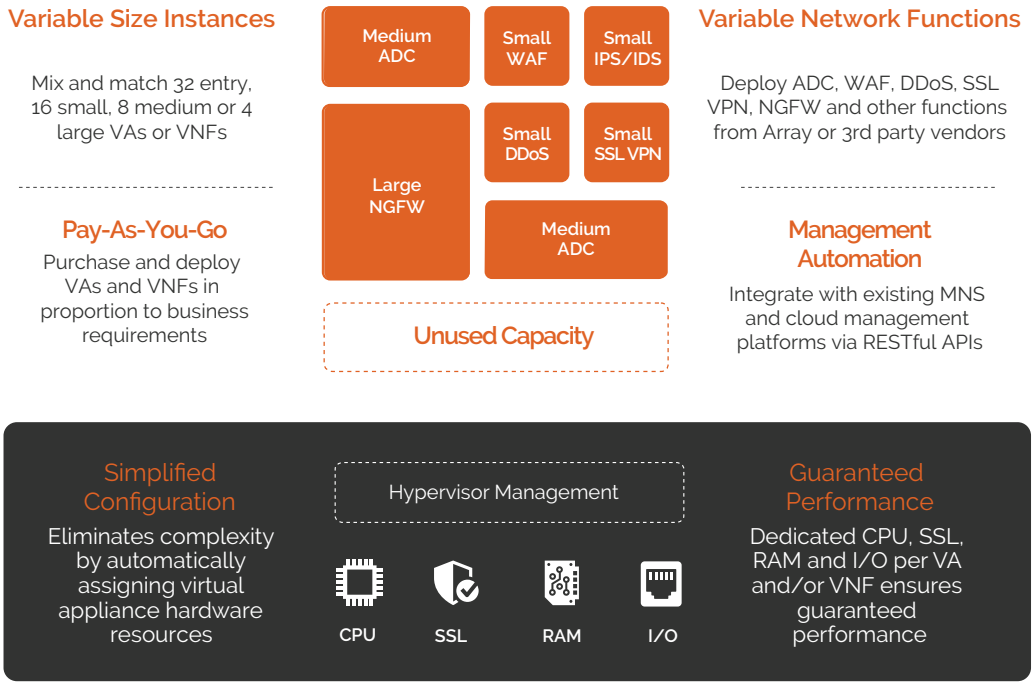
Let's look at three primary inhibitors to broader adoption of networking and security virtualization, and how they are resolved by Network Functions Platforms.

1. Organizational Silos – The concern is that security teams have a strong core competency in security, but in many cases operate independent of networking, server and virtualization teams. NFV initiatives can span multiple areas of operation and as a result run the risk of devolving into organizational gridlock.

   The Network Functions Platform is an appliance that may be purchased and deployed by the security team, without the need to involve network, server or virtualization teams. Because the platform is purpose-built, preconfigured and highly automated, the security team most likely possesses all necessary skills, and will not need to reply upon networking, server or virtualization groups for assistance.

2. Skills Deficits – As mentioned, virtualizing networking and security functions requires new skill sets, knowledge beyond the domain of some security teams (and perhaps not even possessed by server and virtualization teams in some instances). This includes everything from selecting server configuration, to resource allocation, to service chaining. Without the requisite knowledge, any initiative will ultimately fail.

Network Functions Platform



The Network Functions Platform fully automates and abstracts tasks such as hypervisor management, CPU pinning, NUMA boundary settings, SR-IOV, DPDK, driver considerations, physical and virtual port mapping and many other factors; all that is left for the security team to do is select a desired function and an appropriately-sized instance.

In addition, the intuitive WebUI management system provided by the Network Functions Platform simplifies creation of service flows between hosted security VAs – for example, one or more ADC instances performing SSL decryption and encryption and load balancing traffic flows across multiple IPS/IDS, DDoS, WAF and data loss prevention instances on the same Network Functions Platform – eliminating the need for specialized skills or involving server and virtualization teams. The Network Functions Platforms allow security teams, and the business, to become more software-centric in the near term with minimum operational or organizational disruption.

3. **Performance and SLAs** – Many security services are business-critical and are often subject to high-volume traffic and complex configurations, as well as the need to consider their impact on the end-user experience. Anticipated virtualization benefits such as reducing time to deploy or becoming more agile and efficient in the use of IT infrastructure do not outweigh the cost to the business should a solution underperform.

As mentioned, commodity virtualized servers were designed for application workloads, not security workloads. General-purpose hardware, hypervisor overhead, VM contention and virtual switches can all conspire to rob security services of the performance needed to meet and maintain necessary SLAs.

In contrast, the Network Functions Platform provides performance for VAs that is on par with hardware-based security appliances, and is also capable of providing guaranteed performance for each VA deployed on the platform.

Boasting a system architecture that is purpose-built for networking and security, the Network Functions Platform partitions hypervisor management resources such that they do not impact or become impacted by hosted VAs.

In addition, each VA is assigned dedicated resources (CPU cores, hardware SSL, memory, virtual ports and physical interfaces) that are unavailable to other hosted functions. The result is a solution that combines the agility of cloud and virtualization with the performance of dedicated hardware appliances.

Array Networks AVX Series Network Functions Platforms for Security

A significant concern regarding networking and security virtualization is the need to establish demonstrable ROI. Perhaps the best way to build a business case for broader and more rapid adoption is to identify solutions that are simple and self-contained – solutions that solve immediate security requirements, while at the same time laying a foundation and migration path to more advanced NFV implementations in the future.

Security is a use case where Network Functions Platforms can provide a compelling alternative deployment model – one that provides visibility to SSL-encrypted traffic, protects against DDoS and other application-level attacks, and allows services to be securely interconnected within a high-performance, self-contained environment.

First, we'll look at using a Network Functions Platform as a method for gaining visibility to encrypted traffic by using SSL intercept in combination with service-chained security functions. Next, we'll look at using Array's platform to guard against DDoS and other application level attacks. Finally, we'll look at the platform as a means to concentrate security services such as SSL VPN and next-generation firewalls.

SSL Intercept

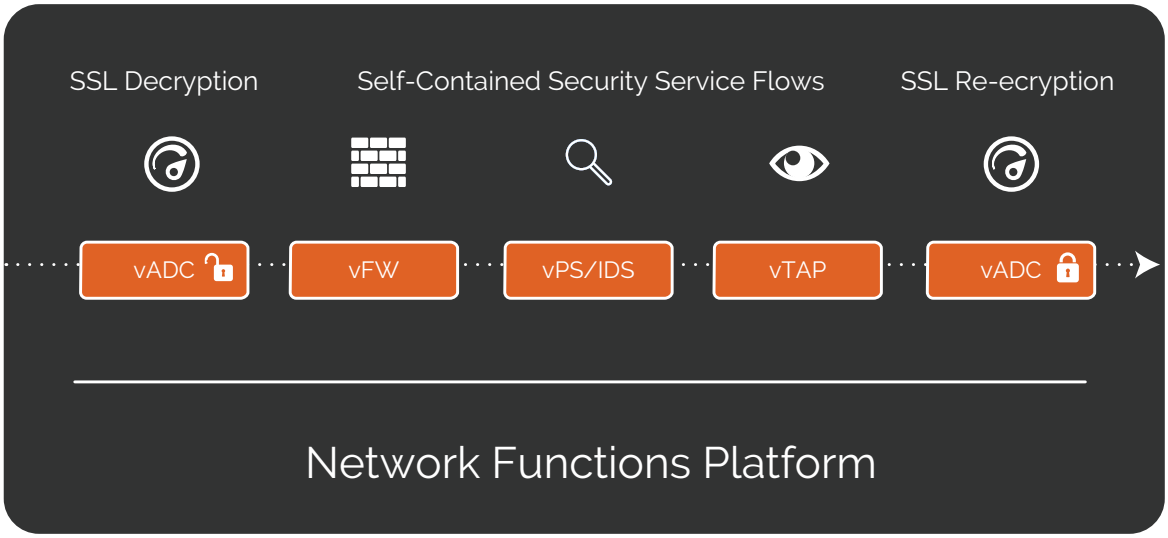
Scalable Visibility and Security for SSL-Encrypted Traffic

An increasing majority of web traffic is secured using SSL, and while encryption improves security, hackers are using SSL as a cloak to deliver malicious payloads. Because firewalls, IDS/IPS, data loss prevention and similar solutions often lack visibility into encrypted traffic, they can allow malware and other threats to traverse the network uninspected and therefore un-remediated. For solutions that do support decryption, high-volume SSL traffic commonly overwhelms system resources and impacts performance.

To address these challenges of visibility, flexibility and performance scalability, Array's SSL intercept (SSLi) solution decrypts SSL traffic to allow inspection and remediation by virtualized security functions running on the Network Functions Platform. Once inspected for attacks, intrusion and data exfiltration attempts, traffic is re-encrypted and forwarded to its final destination.

In the SSLi solution architecture shown below, two virtual ADCs are deployed as bookends on the Network Functions Platform – one for decryption and one for re-encryption. Each virtual ADC benefits from hardware-accelerated SSL, effectively offloading this compute-intensive function from the security VAs to ensure solution scalability. Multiple security virtual appliances are then service chained between the virtual ADCs to create a fully secure, self-contained solution for inspecting temporary clear-text traffic.

In addition to providing scalable visibility to encrypted traffic, the SSL intercept solution load balances traffic across hosted security virtual appliances to assure service availability and supports a unique Web classification capability aimed at providing selective decryption for sensitive traffic. For example, HIPAA and other regulations require that traffic to and from medical, financial and certain other sites remain intact to protect sensitive personal information. As an added value, SSLi consolidates security services on a single streamlined platform that reduces CapEx and OpEx costs associated with space, power, cooling and provisioning.



DDoS Protection

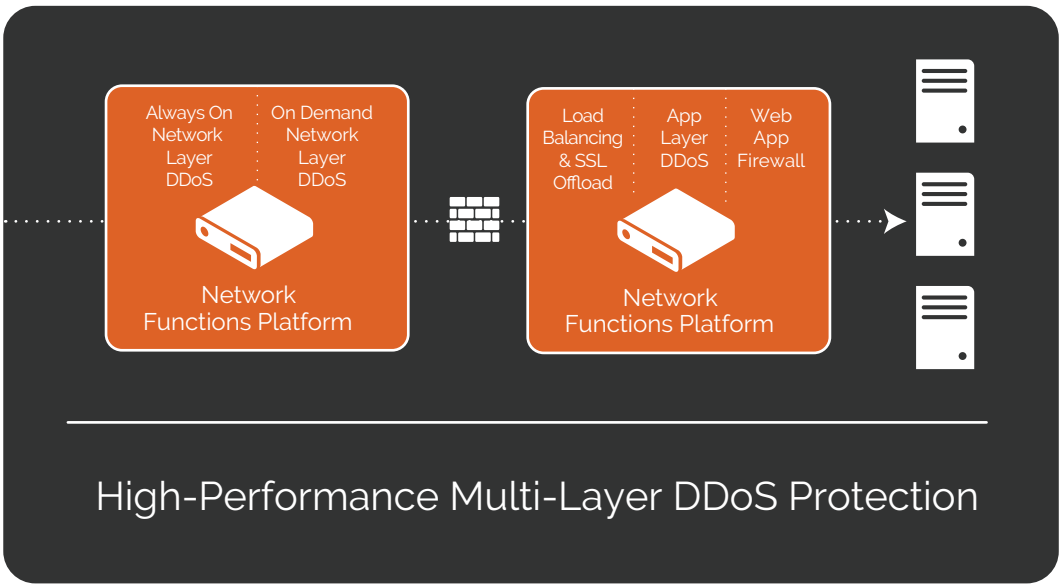
High-Performance, Multi-Layer Attack Prevention

DDoS attacks can be an IT department's worst nightmare. Because they combine high-volume traffic clogging with application-targeted techniques, these stealthy attacks can disrupt services for legitimate users and even take down applications or entire networks.

While there are proven techniques to mitigate DDoS attacks, there is a downside that many vendors prefer not to mention: each technique is compute-intensive; in other words, they can each warrant an entire hardware-based appliance in order to run in their power band. By activating them simultaneously on a single appliance integrated with other functions such as web application firewalls (WAF), the ability to protect against DDoS attacks in a scalable manner suffers.

By contrast, Array's Network Functions Platform supports compute-intensive DDoS capabilities with guaranteed, hardware-like high performance. By using separate virtual appliances for network, session and application layer protection, and separate virtual appliances for security-enhancing load balancing, SSL offload and WAF capabilities, multiple lines of defense can be established without negatively impacting the end-user experience.

DDoS protection supports both always-on (inline) and on-demand configuration, and may be deployed in front of firewalls for network-layer scrubbing, or behind firewalls – closer to servers – for application-layer scrubbing. Network Functions Platforms may be used to host Array's DDoS, WAF and ADC services with built-in machine learning, or best-of-breed 3rd-party DDoS virtual appliances.



Service Concentration

Consolidating Next-Generation Firewalls and SSL VPNs

Over time, many larger organizations and service providers accumulate a fleet of firewalls, SSL VPNs and other dedicated security appliances. This is driven by the demand from individual use cases, applications, departments and customers for separation that keeps their operations secure, and for performance undisturbed by competing demands.

For security and network operations teams, the downside to this approach is the fixed and inflexible nature of hardware appliances, as well as the CAPEX cost of expensive hardware and the OPEX cost of space, power and cooling.

By contrast, Network Functions Platforms enable a multi-tenant approach that maintains hardware-like isolation and guaranteed performance. Each security virtual appliance is fully separate, with reserved CPU, SSL, memory and I/O resources that provide guaranteed performance. Both CAPEX and OPEX can be reduced without sacrificing security, availability or performance.

Through the use of Network Functions Platforms, security teams experience tremendous gains in terms of service concentration and consolidation.

For example, the equivalent of up to 16 dedicated firewall appliances can be consolidated on a single Network Function Platform – while maintaining an equivalent level of performance for each service. In addition, by consolidating security services

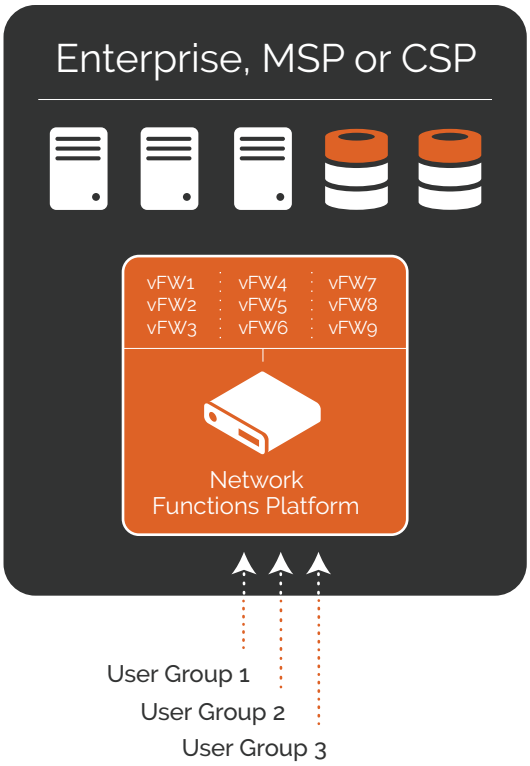
on Array platforms, operations teams gain the ability to remotely provision on-demand services, scale up or out as needed, repurpose resources to meet the changing requirements of various applications, departments and customers, and integrate with management automation and orchestration systems for enhanced business agility.

A Seamless Migration Path to NFV

Beyond benefits such as visibility into application traffic, multi-layer DDoS protection, service concentration, business agility, guaranteed performance SLAs and cost savings, Network Functions Platforms have a very significant additional benefit – they provide a migration path toward broader, more software-centric security infrastructure.

Security teams can experiment with and deploy a wide range of services on the platform. With greater familiarity, more complex service chains will emerge to meet the requirements of specific applications and use cases. In time, integration with management frameworks will centralize, orchestrate and automate platform and function provisioning within larger private and hybrid cloud architectures.

Most importantly, Network Functions Platforms allow businesses to take the journey toward software-centric security infrastructure on their own terms. By achieving ROI through solving pressing security challenges, and by mitigating NFV concerns such as organizational disruption and skills deficits, Network Functions Platforms provide an ideal starting point for IT to chart a course toward increased business agility.



About Array Networks

Array Networks, the network functions platform company, solves performance and complexity challenges for businesses moving toward virtualized networking, security and application delivery. Headquartered in Silicon Valley, Array addresses the growing market demand for network functions virtualization (NFV), cloud computing and software-centric networking.

Proven at more than 5,000 worldwide customer deployments, Array is recognized by leading analysts, enterprises, service providers and partners for pioneering next-generation technology that delivers agility at scale.

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA
rschmit@arraynetworks.com
+32 2 6336382

China
support@arraynetworks.com.cn
+010-84446688

France and North Africa
infosfrance@arraynetworks.com
+33 6 07 511 868

India
isales@arraynetworks.com
+91-080-41329296

Japan
sales-japan@arraynetworks.com
+81-44-589-8315

To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866 MY-ARRAY (692-7729) or authorized reseller.