Consolidating and Supercharging vADCs with Network Functions Platforms

Array Networks AVX Series for App Delivery

Foreword
by IDC Analyst Brad Casemore

Software-defined networking (SDN) burst onto the scene earlier this decade as an architectural approach closely aligned with the needs of cloud-era agility. Shortly thereafter, the concept of network functions virtualization (NFV) first surfaced. NFV was advanced by large communications service providers (Comm SPs) and defined formally under the auspices of the European Telecommunications Standards Institute (ETSI).

Although NFV was promulgated by ETSI by and for telecommunications service providers, many of its objectives are equally applicable to enterprise IT departments. In virtualizing network functions to run on industry-standard server hardware, NFV aspired to deliver greater operational and network agility, to reduce opex and capex expenditures, and to enable dynamic provisioning of new services as market requirements evolved. While these objectives clearly remain important to service providers, they are of strong interest to many enterprises as they pursue the imperative of digital transformation.

While the term "enterprise NFV" has since emerged, most enterprise IT departments remain at a nascent stage in their adoption of virtual network functions (VNFs), much less a full-scale embrace of automated and orchestrated VNFs within a complete NFV framework. For example, IDC market data indicates that the software/virtual form factor (vADCs) accounted for less than 19% of overall revenue derived from sales of application delivery controllers to enterprises in 2016. ADCs sold as physical appliances still predominate in the enterprise. Percentages are similar for other network and security services offered to enterprise as both physical appliances and in virtual form factors.

This relatively modest level of NFV adoption, however, does not result from a paucity of enterprise interest in NFV principles and practices. To the contrary, IDC's interactions with enterprise customers and IDC survey results demonstrate that a growing percentage of enterprises – especially those that have deployed or intend to deploy SDN or network automation – intend to adopt virtualized network and security services. Among the chief reasons cited for doing so include expediting service provisioning, gaining network agility, enhancing operational efficiency, and lowering capex and opex costs.

Notwithstanding such intent – as well as an appreciation of the benefits that enterprise NFV can confer – IT departments often struggle to make their plans actionable. One inhibitor is confusion and even conflict over roles and responsibilities within the IT department. Indeed, the introduction of network and security VNFs that run on servers can blur traditional lines of demarcation between siloed IT teams that deal respectively with networks, servers, virtualization, and security. Another common challenge is a dearth of skillsets in areas such as network virtualization, while yet another inhibitor is concern about a potential performance compromise that might result from the adoption of virtualized network and security services on industry-standard servers. In addition, many enterprise IT departments struggle to build a business case for enterprise NFV.

It's in this context that the Network Functions Platform has been advanced. It can be seen as an attempt to provide enterprise IT with a path of least resistance to NFV, an approach that seeks to address questions about the overall business case for the technology as well as concerns about operational friction, skills gaps, and the satisfactory performance of virtualized network and security services.

Brad Casemore, Research Director, Datacenter Networks, IDC

IDC
Analyze the Future

TABLE OF CONTENTS

Introduction

Recently, a new class of products, referred to as Network Functions Platforms, has been making headlines in the IT industry press. The name hints at something to do with Network Functions Virtualization (NFV), which it does, but that's only part of the overall story. A deeper dive will help clarify just what this new solution category can do for an enterprise IT manager, in addition to shining a light on some compelling new application delivery use cases.

First, it is important to understand the current NFV landscape, particularly as it relates to enterprise NFV adoption.

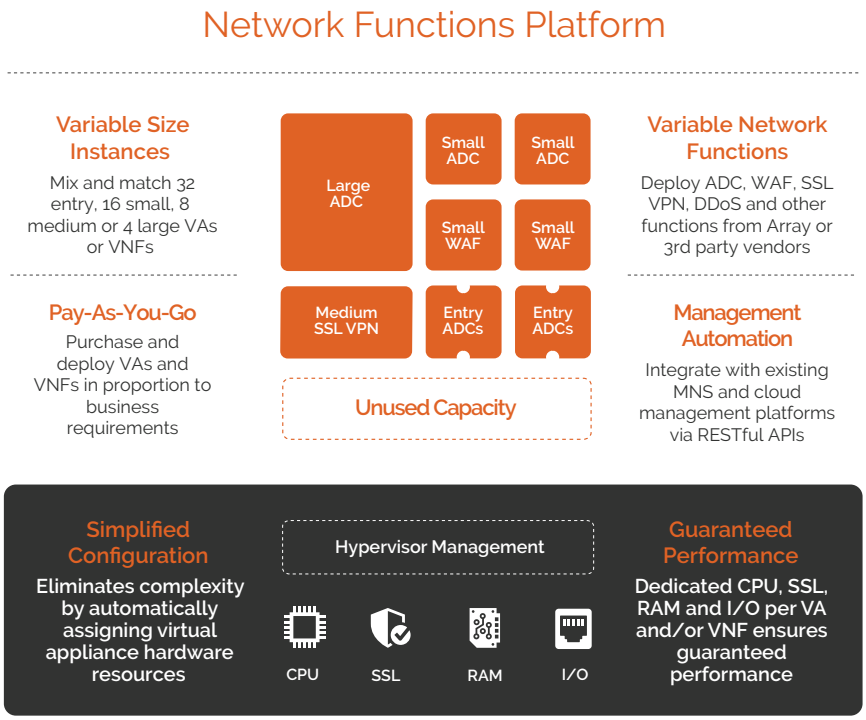
- Consensus among recent market surveys and analyst reports indicates that although only a small number of enterprises have implemented NFV in their production networks, greater than half of all businesses are currently analyzing NFV strategies and vendors.
- The key driving factors for consideration of NFV 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 over time.
- Standing in the way of quicker, more widespread adoption of NFV 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 NFV 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 NFV 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 appliances (VAs) and virtual network functions (VNFs), while at the same time addressing the most pressing challenges to enterprise NFV adoption.

What is a Network Functions Platform?

Think of the Network Functions Platform as a virtualized server on steroids. Because networking and security workloads (ADC, WAF and DDoS for example) are much more compute-intensive as compared to application workloads, the Network Functions Platform is engineered from both a hardware and software perspective to deliver both scalable performance and guaranteed performance.

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 critical NFV inhibitors and how they are resolved by Network Functions Platforms.



- **Organizational Disruption** – The concern is that networking teams have a strong core competency in networking, but often operate independent of server and virtualization teams. NFV spans multiple areas of operation and as a result runs the risk of devolving into organizational gridlock.

  The Network Functions Platform is an appliance that may be purchased and deployed by the networking team, without the need to involve server and virtualization teams. Because the platform is already purpose-built for NFV and because complex virtualization configuration is automated, the networking team most likely possesses all skills necessary, and will not need to rely upon server or virtualization groups for help.

- **Skills Deficits** – As mentioned, NFV requires new skill sets, knowledge beyond the domain of some network teams (and perhaps not 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, NFV initiatives will ultimately fail.

  Server specifications, hypervisor management, CPU pinning, NUMA boundary settings, SR-IOV, drivers, physical and virtual port mapping and many other factors are fully automated and abstracted by the Network Functions Platform; all that is left for the networking 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 allows for simplified creation of service flows between VAs and VNFs (for example, one or more ADC instances load balancing traffic across multiple WAF instances on the same Network Functions Platform) – again eliminating the need for specialized skills or involving server and virtualization teams. The Network Functions Platforms allow networking teams, and the business, to become more software-centric in the near term with minimum operational or organizational disruption.

- **Performance and SLAs** – Many enterprise applications are business-critical, and feature high-volume traffic, complex configurations and/or strict requirements for the end-user experience. Anticipated NFV benefits such as reducing the time needed to deploy services or becoming more agile and efficient in the use of IT infrastructure do not outweigh the cost to the business should applications go offline or underperform.

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

  In contrast, the Network Functions Platform provides performance for VAs and VNFs that is on par with hardware-based networking and security appliances, and is also capable of providing guaranteed performance for each VA/VNF 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 and VNFs. In addition, each VA and VNF is assigned dedicated resources (such as CPU cores, hardware-accelerated 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.

NFV Adoption for Application Delivery

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

Application delivery (advanced load balancing, Layer-4/7 services and Layer-7 security) is an area where Network Functions Platforms can provide an alternative deployment model – one that keeps applications fast, available and secure, while at the same time introducing improvements in agility, efficiency and affordability as compared to legacy approaches to load balancing. First, we'll look at using a Network Functions Platform as a means to support ADC multi-tenancy and consolidation. Second, we'll look at using a Network Functions Platform to supercharge complex virtual application delivery and security configurations in a manner that ensures guaranteed application SLAs.

ADC Multi-Tenancy & Consolidation

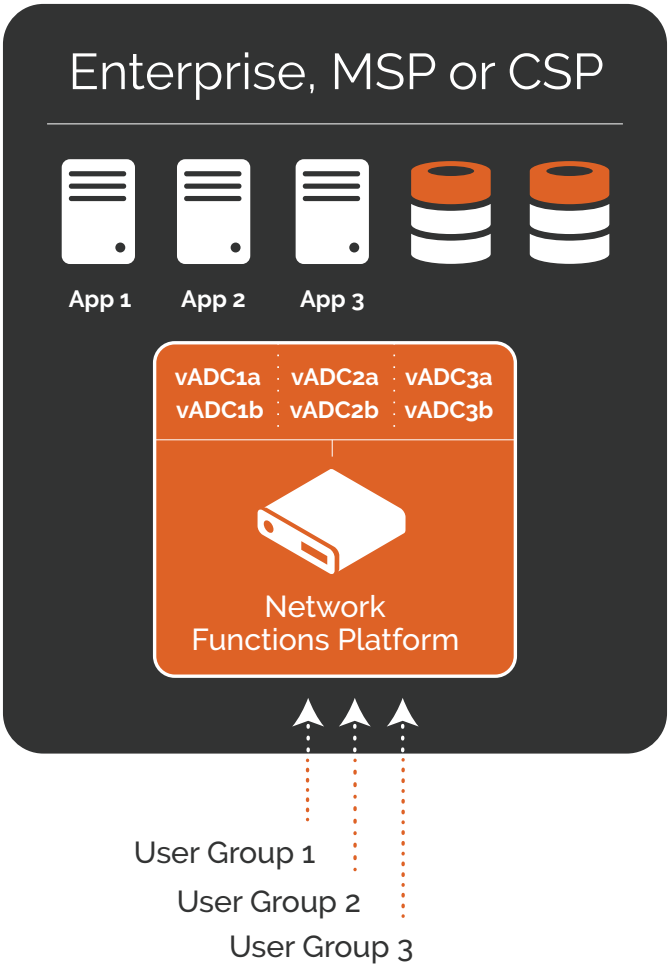
Superior Privacy, Greater Flexibility & Increased Efficiency for Layer-4/7 Services

Many larger organizations and service providers accumulate a fleet of dedicated ADCs or load balancers over time; it is not uncommon for pairs of ADCs to be assigned to individual applications, internal departments and/or customers. This is driven by the demand from each entity for separation that keeps their operations secure, and for performance undisturbed by competing demands.

For 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. While some ADC vendors claim to support multi-tenancy, none support multi-tenancy in a way that truly isolates or guarantees performance for ADC instances.

In contrast, Network Functions Platforms support ADC multi-tenancy with both true isolation and guaranteed performance. Each virtual ADC instance is fully separate, running in its own VM with reserved CPU, SSL, memory and I/O resources that provide guaranteed, hardware-like performance. Both CAPEX and OPEX can be reduced without sacrificing security, availability or performance.

In addition, network operations teams experience tremendous gains in terms of flexibility, such as being able to remotely provision on-demand Layer-4/7 services, scale up or out as needed, repurpose resources to meet the changing requirements of various applications, departments and customers, and integrate with cloud management systems to orchestrate and automate app delivery.



Hardware-Accelerated vADCs

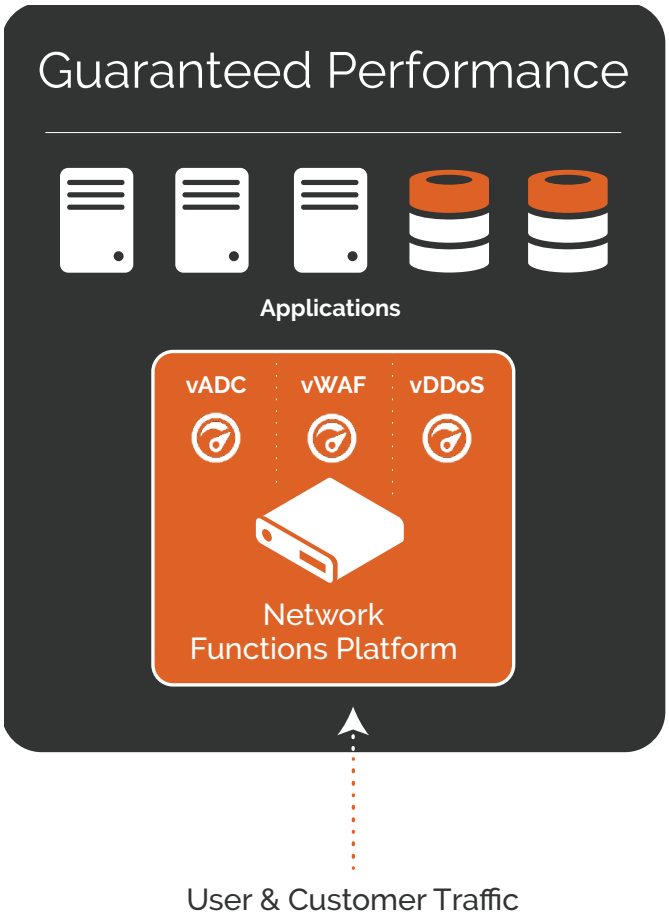
Guaranteed Performance for Compute-Intensive App Delivery and Security Services

Application delivery has evolved considerably over the last 15 years. Whereas load balancers were initially deployed to provide high availability, today's ADCs support significant additional capabilities including acceleration and advanced security. For instance, load balancing (ADC) and web application firewall (WAF) are frequently deployed together on the same hardware appliance.

While on paper these solutions make a lot of sense, there is a downside that many ADC vendors prefer not to mention: Each of these application delivery and security capabilities are compute-intensive; in other words, they each warrant an entire appliance in order to run in their power band. By activating them simultaneously on a single integrated appliance, performance and application SLAs typically suffersignificantly.

In contrast, Network Functions Platforms support compute-intensive advanced application delivery and security services with guaranteed, hardware-like high performance. Services such as ADC, WAF and DDoS, whether provided by Array or a 3rd-party vendor, each run as a fully isolated VA or VNF instance, each with the reserved CPU, SSL, memory and I/O resources they require.

Another little secret common to many vertically integrated ADC vendors is that while they maintain a broad product portfolio, they are typically only good at one or two core application delivery and security services. Network Functions Platforms avoid this vendor lock-in, enabling the deployment of true best-of-breed solutions that provide a superior mix of capabilities and consistent application SLAs.



A Seamless Migration Path to Enterprise NFV

Beyond application delivery benefits such as multi-tenancy, guaranteed performance, best-of-breed capabilities, operational efficiency and cost savings, Network Functions Platforms have a very significant additional benefit – they provide a migration path toward more comprehensive enterprise NFV initiatives.

Networking teams can experiment with and deploy a broader range of services on the platform, as can security teams. With greater familiarity, more complex service chains will emerge to meet the requirements of specific applications and end-users. In time, integration with management frameworks will centralize, orchestrate and automate platform and function provisioning within larger private cloud architectures.

Most importantly, Network Functions Platforms allow enterprises to take the journey toward NFV on their own terms. By achieving ROI, by solving existing application delivery challenges, and by mitigating NFV concerns such as organizational disruption and skills deficits, Network Functions Platforms provide an ideal starting point for enterprises to chart a course toward NFV and 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.