Increase Profitability and Cloud Relevance with Network Functions Platforms

Array Networks AVX Series for MSPs and CSPs

Foreword

by Rich Tehrani, CEO, TMC

As buying habits evolve and continual advancements take place, the business of selling technology solutions is changing rapidly. Consider:

- The software market is growing at a rate of 55%, yet hardware sales are declining (Forbes)
- IaaS is the fastest growing cloud segment at 36.6% YoY
- There are 77 million millennials. Of those working, the majority are in management roles (EY)
- WSJ reports millennial CIOs look to build long-term strategic partnerships with vendors

This data taken as a whole, shows MSPs and CSPs (xSPs) need to formulate a strategy to capitalize on these evolving demographic and technological trends. The good news is, this confluence allows providers to reduce reliance on single-digit-margin hardware. Instead, much of the customer spend can be converted to service revenues which can enjoy margins in the 25% range.

For a decade, xSPs have upgraded tape drives at their customer locations to backup appliances with an associated monthly cloud-storage fee. These cloud backups also functioned as a DR solution allowing employees to work remotely, even if the office systems were not usable. Such solutions were far better than fixed-function tape drives. By offering a better service, providers saw customers will not only pay more for hardware, they will budget for recurring expenses as well.

Likewise, technologies such as NFV, software and cloud allow these providers to take fixed-function appliances such as firewalls and ADCs and sell them as virtual network functions. There can be tremendous benefits to this model such as far higher margins, non-commoditized pricing, greater customer stickiness and the ability to sell additive services more easily. Researchers tell us in fact, that 20% to 30% of managed services delivered over physical appliances today are ripe to be picked off by NFV-based managed enterprise services.

Customers further benefit from this approach as they convert CAPEX to OPEX spending. They are also happy because they know their immediate service provider has more control over the services provided – the so called one-throat-to-choke philosophy. Another advantage of cloud is customers can burst when needed for added capacity or functionality. This flexibility allows them to upgrade their virtual appliances as needed without the current rip-and-replace headache. Cloud also allows them to pay for consumption as opposed to over-provisioning on-premise hardware in order to adequately serve their future peak demand.

Even non-millennials assign value to partners who can work with them to strategically solve their business problems. This shift is coming at a time when reliance on cloud is growing and NFV provisioning solutions and ecosystems are beginning to flourish. The forward-thinking xSP looks to be ahead of the curve while capturing a greater share of the customer spend on solutions. All this while providing a more flexible and customized service that fixed-function hardware cannot match.

In conclusion, customers are becoming accustomed to paying monthly for cloud services and will do so if the real and perceived benefits are greater than purchasing a fixed-function appliance. In addition, they want more from their xSP. They want to know they can put together a customized solution that meets their dynamic needs over time. By providing functionality that the customer values, providers are able to benefit by moving from commoditized hardware offerings to more lucrative service revenue.

Rich Tehrani, CEO, TMC

TABLE OF CONTENTS

Introduction

According to an Infonetics Research report[1], the vast majority of major communication service providers either plan to or already have rolled out network functions virtualization (NFV). The main reasons for this overwhelming trend are service agility and the resulting faster time to revenue, the ability to view network and service conditions through a single pane of glass, and simplified provisioning of new services, as well as network virtualization, with the resulting reduction in both CAPEX and OPEX.

For other cloud and managed service providers (collectively xSPs), what is holding back adoption of NFV? While the Infonetics Research report covered only major Telcos, it also exposed several barriers to deployment that are common across many service providers. Among them are:

- Skills deficits among existing staff, difficulty in finding and training staff, and potential organizational disruption among existing teams
- Lack of maturity of current NFV solutions, as well as incomplete standards
- Perceived difficulty in integrating NFV into existing network architectures
- Unknown total cost of ownership (TCO) and return on investment (ROI).

Another barrier to deployment, which has not yet risen to prominence in the NFV discussion but is certain to do so as NFV gains momentum, is the intrinsic nature of NFV infrastructure (NFVI).

By design, NFVI uses readily available commercial off-the-shelf (COTS) hardware, which is generic and thus inexpensive as compared to traditional physical/dedicated appliances. While COTS resources can easily run business-oriented applications and services, certain security and networking solutions – such as routers, WAF, NGFW, ADCs, WAN optimization and others – are highly I/O, switching and compute-intensive. Their performance will suffer in a shared-resource environment, thus impacting the ability to meet SLAs and generate revenues.

An entirely new product class, called Network Functions Platforms, has recently arisen to address these and other barriers to deployment for NFV, and to enable xSPs to monetize and expand their service offerings. In this white paper, we'll examine how Network Functions Platforms can help xSPs become more agile and software-centric in their approach to supporting customer requirements, pave the path to NFV, and open new markets for service offerings.

What is a Network Functions Platform?

Simply put, a Network Functions Platform is a virtualized hardware appliance that is purpose-built to run networking and security virtual appliances (VAs) and virtual network functions (VNFs). As mentioned previously, these types of workloads (e.g. firewalls, load balancers, VPNs, etc.) require more compute, I/O and switching resources than typical business applications, and must meet performance requirements in order to meet SLAs.

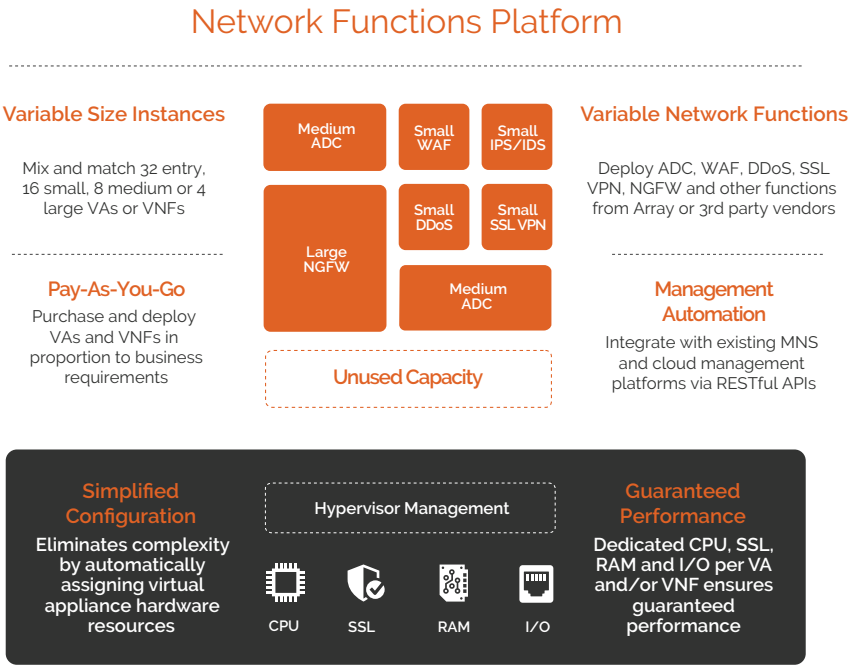

Figure 1: Key Network Functions Platform Features

1 Infonetics Research, SDN and NFV Strategies: Global Service Provider Survey

The Network Functions Platform is engineered from both a hardware and software perspective to deliver guaranteed performance for multiple VAs/VNFs, and further, to scale them up or down as needed to meet requirements. Each VNF/VA instance has its own CPU, memory, I/O, and SSL resources, and hypervisor management is similarly assigned dedicated resources, and separated from hosted functions, to minimize resource conflicts (i.e. the "hypervisor tax") – thus ensuring performance. Segregation of resources also helps meet end-customer and regulatory requirements to protect data and other resources.

Network Functions Platforms can host variable-sized instances as well, ranging from entry-level (which is equivalent to the performance of a lower-end standalone networking or security appliance), to large – the equivalent of a high-end dedicated appliance. In addition, instance sizes can be mixed and matched to right-size resources as needed.

Perhaps most importantly for xSPs, however, is that the Network Functions Platform is designed to mitigate organizational disruption, skill-set deficits, implementation difficulty and other barriers. By abstracting and automating configuration tasks, the Network Functions Platform streamlines NFV deployment that would otherwise require highly complex server, virtualization and network configurations, multiple functional teams, and in many cases, additional training or staff.

Breaking Down Barriers to NFV

xSP product managers and/or network operations teams that are tasked with implementing NFV can leverage Network Functions Platforms to overcome several key obstacles. Among them are:

- **Organizational Disruption and Skills Deficits** – One of the chief concerns for xSP product managers and network operations teams is that while the networking team has a strong core competency in networking – and the same is true of security, application and server virtualization teams in their own respective areas – NFV spans multiple IT disciplines, and thus carries a high risk of causing organizational disruption because of distributed competencies and/or ownership.

  Network Functions Platforms, however, can be deployed by any IT team, regardless of background or area of expertise. Because the platform is purpose-built for NFV, and complex virtualization configuration is automated, any IT team from any discipline will more than likely have the skill set needed to execute on the product manager's or network operations team's vision for software-centric service creation.

  NFV can be complex to set up, requiring the administrator to select server configurations, allocate resources, link services

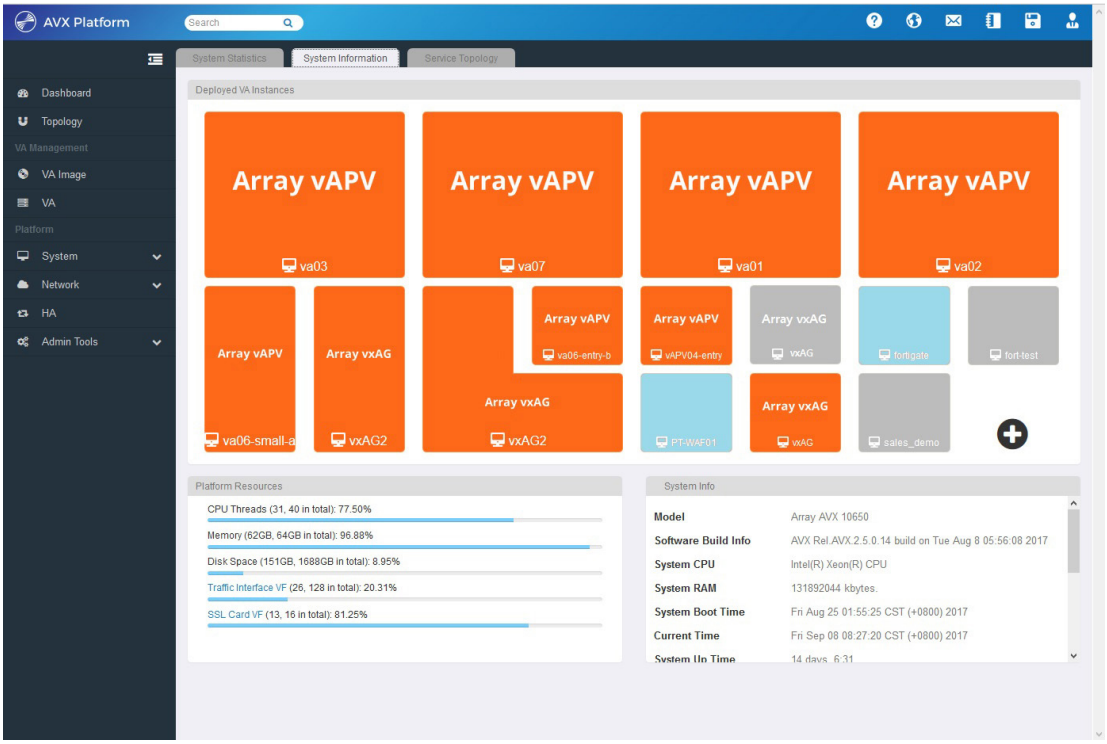

Figure 2: Network Functions Platform WebUI

and ensure compatibility for many disparate elements. To mitigate these potential pitfalls, Network Functions Platforms automate and abstract essential NFV-related configuration elements including hypervisor management, CPU pinning, NUMA boundary settings, SR-IOV, drivers and physical/virtual port mapping. The IT staff needs only to select the desired functions and appropriately size the instances.

In addition, the Network Functions Platform's intuitive WebUI management portal simplifies creation of service flows between VNFs/VAs – for example, one or more ADC instances load balancing traffic across multiple WAF or NGFW instances within the same Network Functions Platform – thus eliminating the need for special skills or involving multiple IT teams. With Network Functions Platforms, IT teams as well as the service provider can become software-centric sooner rather than later, with minimal operational or organization disruption and no specialized training.

- **Performance and SLAs** – Network Functions Platforms offer performance for networking and security VAs that equals that of hardware-based appliances, while also providing guaranteed performance for each VA instance. Purpose-built for networking and security services, the Network Functions Platform partitions off the hypervisor management resources so that they do not impact – and also are not impacted by – the hosted VNFs and VAs.

  In addition, each instance is assigned dedicated resources (including CPU cores, hardware-accelerated SSL resources, memory, virtual ports and physical interfaces) that are separate from those of any other hosted functions. The end result is a solution that combines the agility of cloud and virtualization with the performance of traditional dedicated appliances.

Especially when serving larger enterprise customers, the ability to meet and maintain SLAs is critical. Network Functions Platforms provide a dashboard with a detailed view of current status for a range of system and function parameters, as well as the eCloud™ RESTful API for integration with cloud management, orchestration and automation systems to manage and monitor both the platforms and the hosted VAs/VNFs. OpenStack support offers another alternative for management and monitoring, and includes support for OpenStack Neutron load-balancing-as-a-service (LBaaS). The AVX platform can also be represented as a compute node within OpenStack Nova.

Thus, CSPs and MSPs can leverage the Network Functions Platforms to meet the SLA requirements of larger customers, and to open new markets for a range of networking and security services.

TCO & ROI

A significant concern among xSP product managers and/or network operations teams in regard to NFV is the need to establish demonstrable ROI and justifiable TCO. While smaller customers can be served via virtual appliances, larger enterprise-class customers will require the higher performance that only dedicated/physical appliances can provide.

For many xSPs, the margins on networking and security services delivered via physical appliances are incredibly thin and, compounding the problem, enterprise-class customers are knowledgeable about the cost of dedicated networking and security gear and can use this leverage to apply even more pricing pressure on providers.

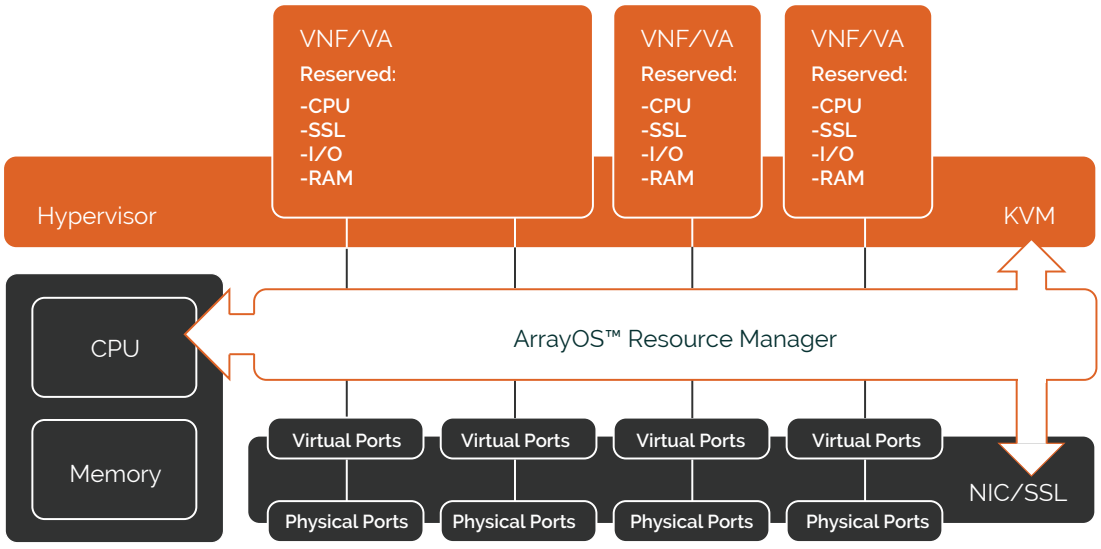

Figure 3: High-Level Network Functions Platform Architecture

With Network Functions Platforms, CSPs and MSPs can build out networking and security services to serve higher-end customers, but with significantly less investment in terms of both CAPEX and OPEX. Further, the cost of goods (i.e. the Network Functions Platform and the VNFs/VAs it supports) is largely opaque to end-users – thus resulting in the ability to offer services that deliver a far more generous profit margin. In addition, Network Functions Platforms can help 'level the playing field' with large public cloud providers such as AWS and Azure, all of whom are using NFV as part of their software-centric and agile approach.

Opening New Markets

As discussed previously, many xSPs have built their business models on supporting SMB-type customers that are well served by VAs running on general-purpose COTS servers. However, many providers want to expand their business to offer networking and security services to larger and more lucrative enterprise customers – but enterprises have higher standards for performance, security and SLAs.

In the past, the only options providers had were to either purchase high-dollar, inflexible dedicated appliances in order to serve the higher-tier market, or to simply forgo serving this market entirely. By contrast, the Network Functions Platform provides a mix of performance and agility that allows CSPs/MSPs to offer the on-demand provisioning that enterprises expect of cloud services, while also delivering the performance and security that enterprise customers demand, as well as the ability to support SLAs.

With the Network Functions Platform, xSPs are no longer limited as to the customer types they can serve with networking and security services, and can open new and profitable markets with the assurance of guaranteed performance and the ability to scale up or down services as needed to meet customer requirements.

Consolidation & Multi-Tenancy

In situations where xSPs are currently supporting higher-end customers with dedicated standalone appliances, or see dedicated standalone appliances as the only (expensive) option for providing services to higher-tier enterprise customers, the Network Functions Platform provides an ideal alternative.

In many cases, the Network Functions Platform can consolidate the equivalent of 16 standalone dedicated appliances into a single rack unit – significantly reducing costs for rack space, power and cooling at data centers and co-lo facilities where space is at a premium. Network Functions Platforms achieve this while maintaining hardware-like, guaranteed performance with demonstrable security and separation for each and every customer and service.

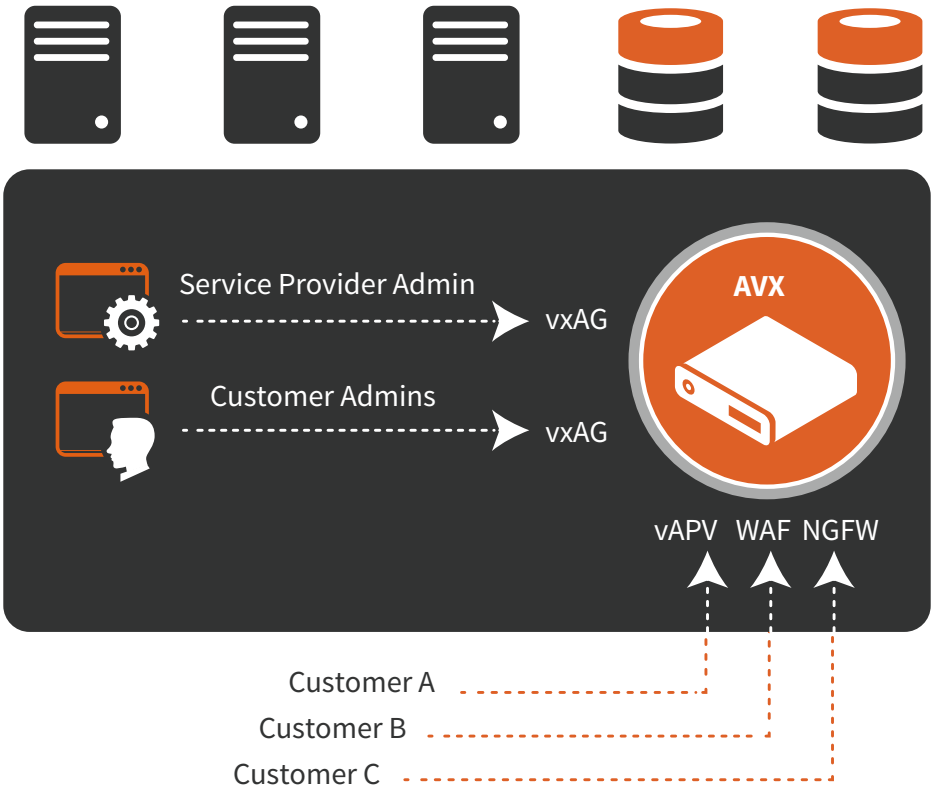

Figure 4: Data Center Consolidation Example

Best-of-Breed Services Platform

Many solutions on the market attempt to provide a range of networking and security services from an all-in-one type appliance, either virtual or dedicated. While this approach offers some benefits in terms of simplified management, these benefits are overshadowed by the performance degradation that occurs if multiple networking and security services are enabled simultaneously. In addition, it is very difficult for networking and security vendors to excel in more than one or two technology areas – in other words, a couple of integrated functions may be best-of-breed, while the rest are simply bolted on as an afterthought.

With the Network Functions Platform, almost any best-of-breed vendor's products may be used to offer network and security services – with each service running on its own virtual machine with guaranteed, hardware-like performance. Importantly, networking and security products can be service chained in order to optimize security and the performance of VAs. For example, one or more load balancer instances can distribute traffic among multiple WAF instances; or load balancers can decrypt SSL traffic, distribute it across multiple NGFWs, which then pass suspicious traffic to IDS/IPS instances for further inspection – before returning the traffic to load balancers for re-encryption and forwarding to application servers.

A Seamless Migration Path to NFV

Beyond benefits such as guaranteed performance, support for best-of-breed solutions, operational efficiency, multi-tenancy, data center consolidation and overall cost savings, Network Functions Platforms have a very significant additional advantage – they provide a migration path toward more comprehensive CSP/MSP 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 customers. In time, integration with management frameworks will centralize, orchestrate and automate platform and function provisioning.

Most importantly, Network Functions Platforms allow xSPs to initiate the journey toward NFV on their own terms. By achieving ROI and holding the line on TCO, by solving existing application delivery and security challenges, and by mitigating NFV concerns such as organizational disruption and skills deficits, Network Functions Platforms provide an ideal starting point for service providers to chart a course towards NFV, software-centric agility and new markets.

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.