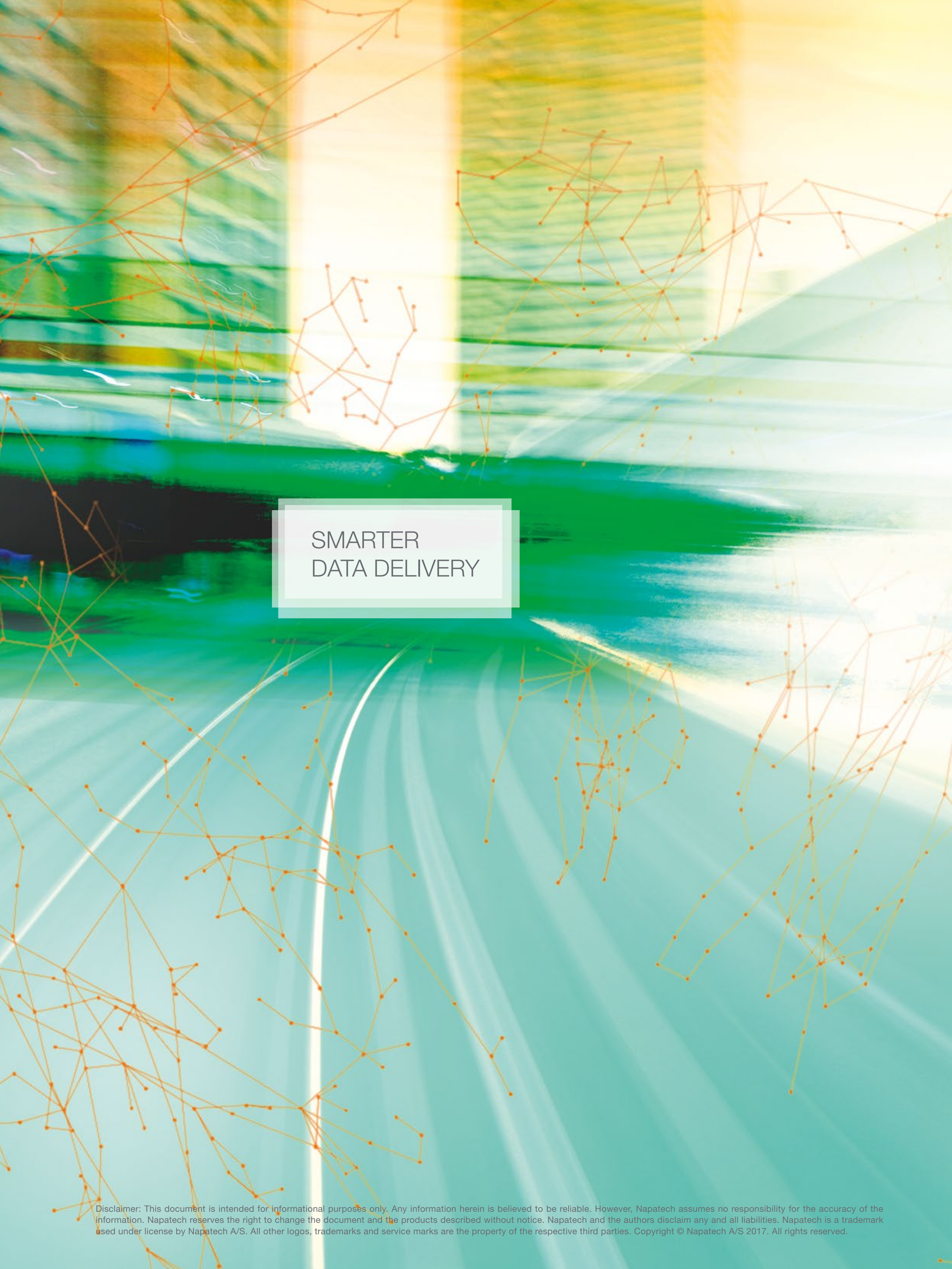
napatech

WHITE PAPER

PROVIDING SECURITY, AGILITY AND INSIGHT FOR DYNAMIC CLOUD CONNECTIVITY

May 2017



Disclaimer: This document is intended for informational purposes only. Any information herein is believed to be reliable. However, Napatech assumes no responsibility for the accuracy of the information. Napatech reserves the right to change the document and the products described without notice. Napatech and the authors disclaim any and all liabilities. Napatech is a trademark used under license by Napatech A/S. All other logos, trademarks and service marks are the property of the respective third parties. Copyright © Napatech A/S 2017. All rights reserved.

EVOLVING CLOUD SERVICE DEMANDS AND THE NEED FOR SECURITY, AGILITY AND INSIGHT

Since the turn of the century, cloud computing has evolved to address a wider range of needs. Applications that one never imagined would leave the premises are now supported by cloud services. Indeed, it is hard to imagine any application that could not be supported using a cloud model.

Ironically, the one reason why many have been reluctant to use the cloud in the past, could well be the main reason why many will choose cloud services in the future; namely security. With the growing sophistication of security attacks and the cost of building and maintaining the required defenses, there is now a strong case for relying on large cloud service providers with professional security teams.

This is just one example of how end-user demands are evolving. As more business-critical applications are moving to the cloud, end users are expecting more from all related partners. This includes the cloud service providers themselves, but also data center hosting/co-location providers as well as connectivity providers.

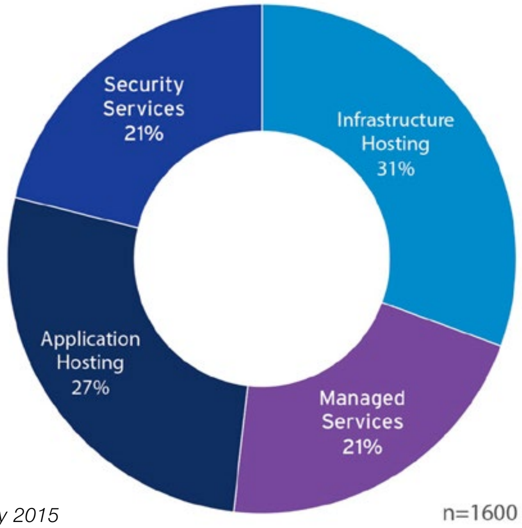
This has been captured succinctly by 451 Advisors in their report “Cloud 2.0: New Challenges, New Opportunities For Cloud Service Providers” from Dec 2015. In this report, they stated: “Increasingly, users are demanding that their CSPs deliver enterprise-ready, value-added, easily scaled services with security baked deeply within… the hallmarks of cloud now are speed and agility, but most of all, services.”

As we can see, security is now a fundamental requirement, but speed and agility are also extremely important as now the cloud is directly supporting the speed at which business is conducted. Service requirements are therefore maturing as shown in Figure 1 from the same report:

Infrastructure Hosting, the familiar Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) offerings are being commoditized, making way for more sophisticated services, such as Managed Services and Security Services.

So, there is no doubt that end-user demands are increasing and becoming more sophisticated. Cloud service providers and others have not been slow to respond with a host of new offerings that not only address these requirements, but also address the fact that sophisticated services require sophisticated connectivity solutions.

Figure 1: The CSP Opportunity



Source: 451 Research, Hosting and Cloud Study 2015

PUBLIC INTERNET CONNECTIVITY NO LONGER ENOUGH

According to the Rightscale "2017 State of the Cloud Report", 95% of respondents use cloud services with 67% adopting a hybrid-cloud strategy. The fact that 67% of respondents use a hybrid-cloud strategy is significant as it shows that the transition to cloud services takes time and will be almost application-specific. Less critical workloads can be supported with public cloud services, while more business-critical services will continue to use private-cloud service offerings.

Cloud service providers and datacentre hosting service providers are fully alert to these needs and have shown nimbleness and ingenuity in their response. Their new offerings not only provide choices and flexibility for customers, they also bring a realization that public Internet connectivity is no longer enough to meet end-user needs.

The response from cloud service providers has been to offer best-performance, direct connectivity solutions to minimize these performance issues. Examples include Amazon Web Services (AWS) Direct Connect, Microsoft Azure ExpressRoute, Google Cloud Interconnect and SalesForce.com ExpressConnect, to name a few.

To make this work, the cloud service providers have partnered with both telecom service providers and data center hosing service providers, who now offer complementary connectivity services. Telecom service provider examples include BT Cloud Connect, AT&T Netbond and Verizon Secure Cloud Interconnect.

The traditional data center hosting service providers have taken these services one step further, leveraging the footprint they have across the globe. Since many already host the majority of cloud service provider offerings in their data centers at multiple locations across the globe, they can offer a brokerage solution ensuring fast connectivity and physical proximity no matter where you need to connect. This can address many of the performance issues associated with accessing cloud services over the Public Internet.

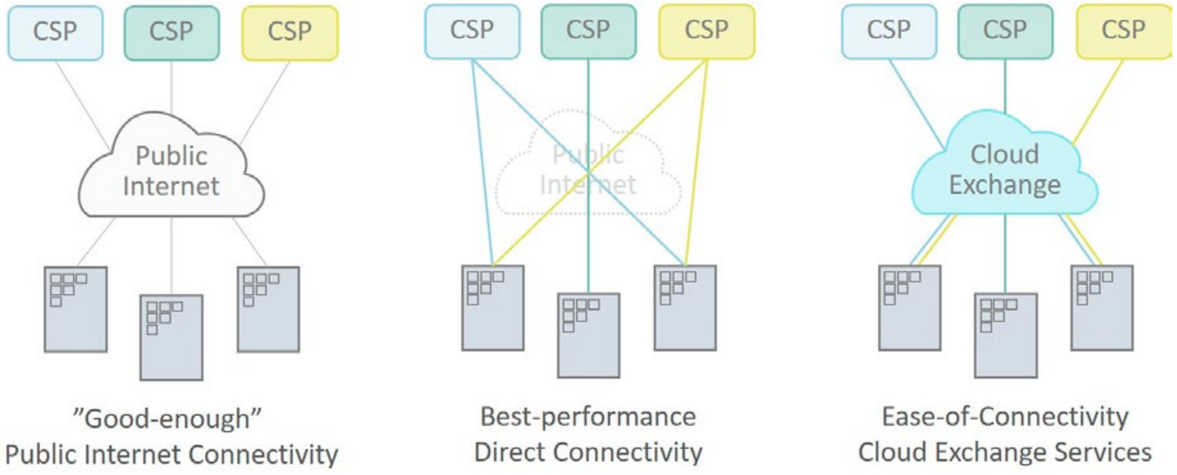


Figure 2: The evolution of cloud connectivity solutions

The original concept for cloud services was to rely on public Internet connectivity as this was deemed "good-enough". End users did not complain, as the alternative was to use more expensive telecom services such as leased lines, MPLS or Carrier Ethernet services. Another reason was that the initial workloads and applications moving to the cloud were not business-critical or demanding. Good-enough was good enough.

But, as the workloads and applications migrating to the cloud became more sophisticated, good-enough quickly became inadequate. In addition, increased end-user usage of cloud-based services, such as Skype for Business, Webex and even Microsoft365, to name a few, began to unveil the downsides of good-enough connectivity as latency, jitter and other distance-related performance issues demanded better solutions.

Examples of these services include Equinix Cloud Exchange, Digital Realty Service Exchange and CoreSite Any2Exchange.

CLOUD CO-OPETITION FOR CONNECTIVITY

Cloud service providers, data center hosting service providers and telecom service providers are all responding to emerging end-user demands with new offerings. Many are partnering to help end-user customers achieve success. But, be under no illusions; they are also competing to be the preferred partner and first point-of-contact for these end-user customers.

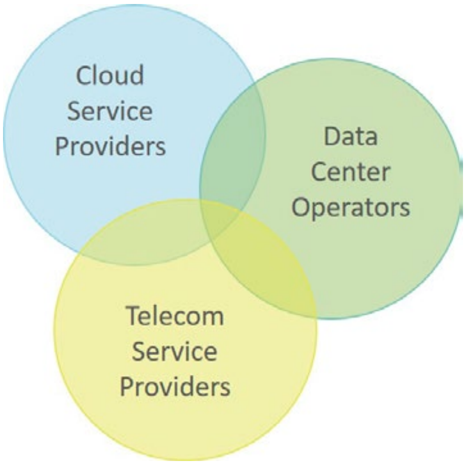


Figure 3: Cloud co-opetition for connectivity

It could be argued that the key to success for these three very different players is the ability to provide the best connectivity solution with service security embedded. This must be done in an agile, responsive manner providing full insight for the end user on what is happening and how their service and supporting elements are performing. These are some of the key incentives for considering Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) approaches to realize particular connectivity solutions.

PROVIDING SECURITY, AGILITY AND INSIGHT WITH SDN/NFV

To understand how SDN/NFV could meet the needs for security, agility and insight, consider a case for a global enterprise adding a new local office in a specific location and needing to quickly turn up the required cloud services.

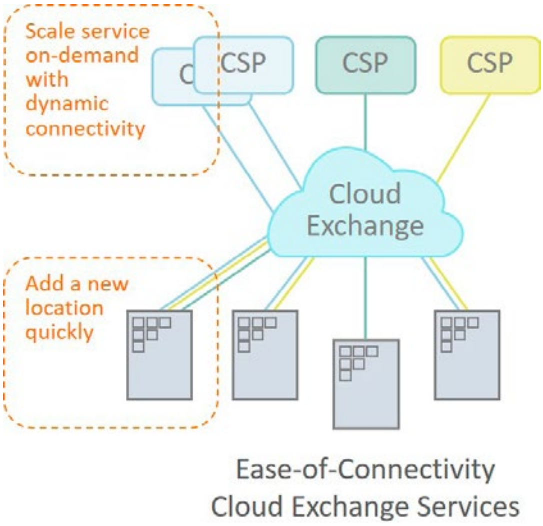

Scale service on-demand with dynamic connectivity
C
CSP
CSP
CSP
Cloud Exchange
Add a new location quickly
Ease-of-Connectivity Cloud Exchange Services

Figure 4: Quick turn up of cloud services at a new location

The first challenge is establishing connectivity to the various cloud services. As we have seen, there are a number of options, but let us assume a type of cloud exchange service is used. This will ensure a secure and dedicated connection as well as access to the cloud services with close proximity, high-speed and low latency and jitter. But, how is this achieved in reality?

What this requires is the ability to quickly scale out the cloud services for the new number of users and then establish dynamic, on-demand connectivity to these services.

This is where SDN and NFV come in. With SDN switching and controllers coupled with NFV orchestration, it is possible to deploy and scale the necessary network virtual functions and software-defined switching instances to direct traffic to and from the new location to the right cloud services quickly and easily. What's more, if the particular service chain of network virtual functions is not providing the required level of performance, NFV orchestration can move or re-deploy virtual functions around in the data center to achieve the required performance.

Which brings us to the next question; how will you know if the service is not performing as expected? How can you redeploy network virtual functions quickly and easily?
This is where insight comes in. The ability to monitor virtual traffic in the data center is essential to both assuring service performance, but also security. With insight, a real-time picture of what is happening can be provided to the SDN controllers and NFV orchestrators, which can allow them to quickly re-allocate resources to optimize performance or to

contain potential security breaches. However, for these requirements to be met, we need a well-functioning Management and Orchestration (MANO) solution and framework, which, until recently, has proven to be a challenge.

SDN/NFV MANO SOLUTIONS EMERGING FOR SERVICE AUTOMATION

One of the major stumbling blocks to broader adoption of SDN/NFV has been, and indeed still is in many respects, the lack of a common framework and solutions for Management and Orchestration (MANO). This is essential for realizing the goals of agility and automation in how services are deployed and connectivity established.

Nevertheless, important strides have been made in overcoming these challenges. One in particular promises to provide the guidance that has been missing and to catalyze broader SDN/NFV deployments, namely the MEF Lifecycle Service Orchestration (LSO) framework.

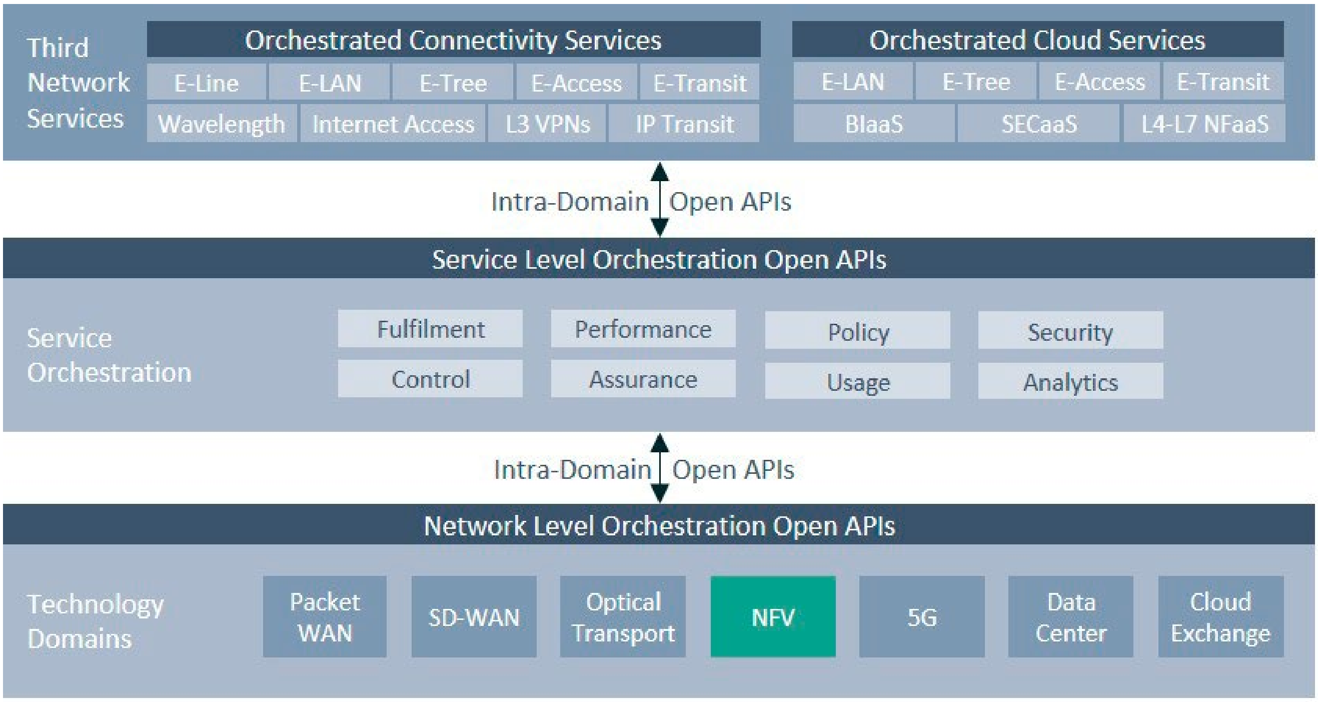


Figure 5: MEF Lifecycle Service Orchestration framework

Adapted from various MEF LSO presentations

Since its introduction in March 2016, this framework has received widespread approval and adoption by major carriers. AT&T in particular has been a driver and user/ beneficiary of the LSO - deploying it as the framework behind their ECOMP open-source MANO solution recently merged with the Open-O initiative to form the new Open Network Automation Platform (ONAP). In addition, there are other open-source initiatives, such as the OpenMano spearheaded by Telefonica, also offering MANO solutions.

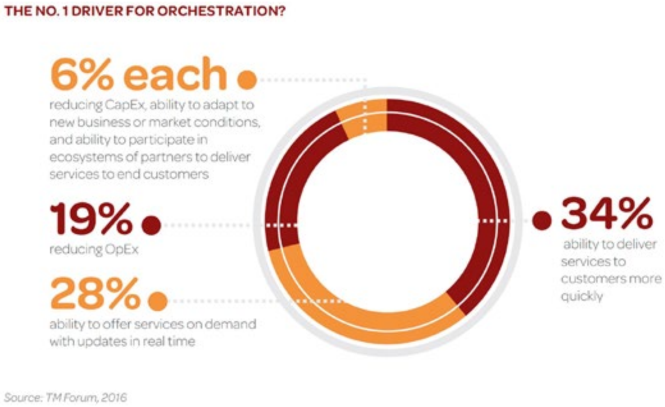
With a common framework like MEF LSO, it is now possible for different companies to agree on basic structures, architectures and interfaces where important information can be exchanged. This is what will enable cross-organizational, cross-domain connections to be established, maintained and secured.

As can be seen, the service orchestration part of the LSO framework includes a number of different functions related to fulfilment, performance, policy, control, assurance, usage, analytics and, of course, security. But, the one thing all these functions will rely on is insight; insight into what is happening in the technology domains.

It is also important to note that even though the MEF LSO now provides a framework for automated service agility, it will not be possible to implement without a similarly automated infrastructure and especially the NetworkFunctions Virtualization Infrastructure (NFVI). It is therefore important and timely to consider how such an NFVI can be implemented.

SERVICE SECURITY AND AGILITY REQUIRES AUTOMATED NFVI

According to the TMForum “Insights Research Report” from September 2016, the number one driver for most carriers to orchestrate their networks is either the ability to deliver services to customers faster or the ability to offer services on demand with updates in real time.



Source: TM Forum, 2016

Figure 6: The number one driver for orchestration

In other words, service agility tops OpEx and CapEx savings as the motivation for service orchestration. However, this assumes that the underlying NFVI is itself agile and automated. Is this the case?

To fully support agility, the NFVI must both be automated and driven by real-time insight into what is happening. Real-time insight provides a picture of what is happening right now, thus allowing SDN controllers and NFV orchestrators to make decisions on when to make changes to improve performance or where to instantiate resources for a new service chain.

For example, one case could be the need to test whether the planned deployment of an NFV service chain will result in a data path that can support latency and jitter requirements. With real-time insight capabilities, such a test can help orchestration make informed decisions. This all has to happen on demand if it is to support service agility requirements.

From a security perspective, experts are now asserting that relying on security prevention techniques based on firewalls and intrusion prevention systems is no longer enough. Some very high-profile breaches have shown that attacks are circumventing these defenses. To provide more comprehensive security, prevention techniques need to be accompanied with advanced detection techniques, such as network behavior analysis. This allows the establishment of normal network behavior profiles that can be matched to real-time monitoring of network behavior to detect anomalies that can be the sign of malicious attacks.

Here also, real-time network insight plays an important role as it provides both the basis for establishing network behavior profiles as well as the ability to detect malicious behavior in real time. It should be noted that this capability is based on virtual probes and appliances that analyze aggregate traffic rather than virtual appliances that are provided as part of a service chain. This is an important distinction.

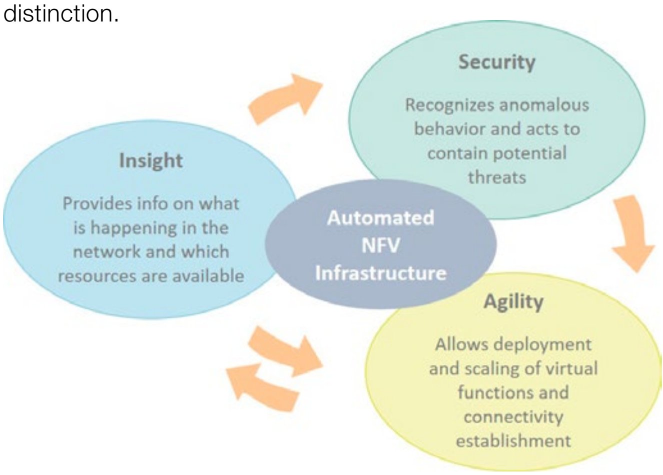

Security
Recognizes anomalous behavior and acts to contain potential threats
Insight
Provides info on what is happening in the network and which resources are available
Automated NFV Infrastructure
Agility
Allows deployment and scaling of virtual functions and connectivity establishment

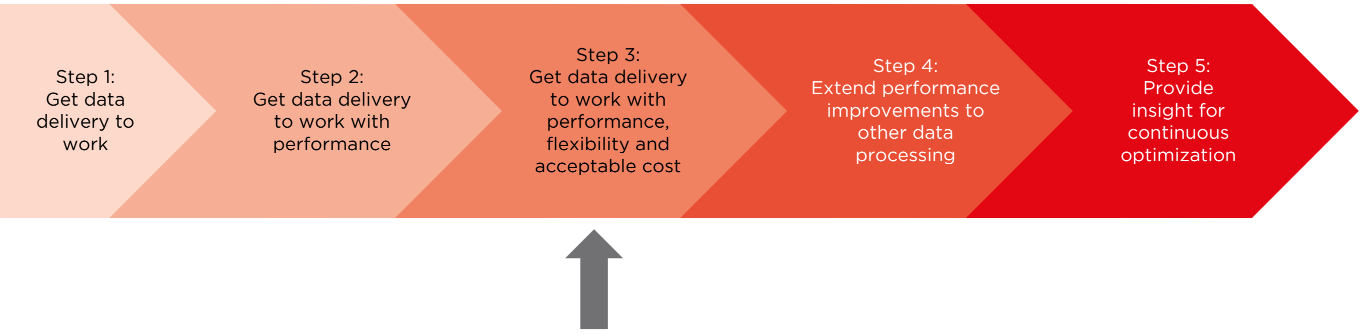
Figure 7: How an automated NFVI driven by insight supports agility and security

With an automated NFVI with built-in real-time insight capabilities, it is possible to provide the agility in the NFVI to support agile service deployment as well as the insight and analysis to support more robust security.

But, is the NFVI ready for automation today? Are the capabilities to provide insight available? We believe that it isn’t, but we are on the path to providing the automation and insight required. We are on step 3 of a 5-step journey to building the right NFVI.

FIVE STEPS TO BUILDING AN AUTOMATED NFVI

The following sections outline the necessary steps in implementing an automated NFVI. The first steps have already been taken and we are now on step 3. But, more work needs to be done. Fortunately, solutions are emerging to address these steps and enable the automated NFVI that is essential to service agility.


Step 1:
Get data delivery to work
Step 2:
Get data delivery to work with performance
Step 3:
Get data delivery to work with performance, flexibility and acceptable cost
Step 4:
Extend performance improvements to other data processing
Step 5:
Provide insight for continuous optimization

This is the challenge that needs to be addressed now to enable automation and support service agility

Figure 8: The 5 steps to automated NFVI

STEP 1. GET DATA DELIVERY TO WORK

Not long after the publication of the first NFV white paper by 13 of the world's largest network operators in late 2012, the Intel Open Network Platform (ONP) emerged as an important conceptual framework for making the transition from traditional physical appliance-based networks to software-based virtualized networks. The ONP server reference architecture provides hardware and software components that are optimized for NFV and SDN deployments. It has a common hardware platform that is based on standard Intel x86 servers and standard NICs, as well as a hypervisor and virtual switch that abstract the hardware from the software. And true to the ethos of ETSI's NFV efforts, the ONP framework is built on open standards and open source software, including the OpenStack cloud operating system, OpenDaylight SDN controller and Open vSwitch (OVS) virtual switch.

With the inclusion of OVS and hypervisor, the ONP framework represents the first step in building an automated NFVI. OVS is a virtualized software implementation of a traditional network switch. It provides the connectivity in virtualized environments and can be deployed across multiple servers. As VNFs are distributed on different servers, the hypervisor and OVS switch traffic among them wherever they are implemented. This ability to instantiate and move VNFs anywhere in the network enables the flexibility and agility in NFV service chain creation.

ONP is a good starting point for automated NFVI, but it does have drawbacks in performance and cost efficiency. Generally, vSwitch performance is a common source of frustration for network operators, and it has been a bottleneck in NFV implementations. While vSwitch performance may not reach exactly the same levels as hardware appliances, it does need to be better than what it is today, where OVS throughput performance falls below industry expectations. In addition, efforts to improve OVS performance typically result in very high server Central Processing Unit (CPU) core consumption, which makes it expensive to run. The more cores OVS consumes, the less will be available for other data processing workloads including hosted virtual functions. Operators will end up paying for additional capacity just to achieve the same performance and functionality that they have today, which defeats the cost efficiency aims of NFV.

STEP 2. GET DATA DELIVERY TO WORK WITH PERFORMANCE

To overcome the performance shortcomings of OVS, the industry looked to an alternative approach with Single Root Input/Output Virtualization (SR-IOV). This is a familiar network interface in enterprise networking, but relatively new to telecom networks. SR-IOV does improve throughput performance, but it sacrifices flexibility and adds complexity.

SR-IOV bypasses the vSwitch and hypervisor and directly interfaces between VNFs and NICs that support SR-IOV. In other words, physical NICs are linked directly to specific virtual functions on the same server, thereby improving throughput performance. But by tying the NIC hardware to the VNF software in this way, SR-IOV effectively removes the abstraction layer that separated the hardware from software in the NFVI, which makes moving VNFs very difficult. The effect can be described as taking the virtualization out of NFV. Also, since there is no standard way to implement the SR-IOV mechanism, vendor-specific versions can add further complexity when it comes to integrating with other elements of the NFVI as well as legacy telco systems.

VNF mobility is important not only because it enables flexibility and service agility, but also because it is essential to the NFV business case. With the ability to easily move VNFs among servers within the data center or to different data center locations as NFV-based services mature, operators can consolidate virtual functions onto fewer servers and optimize server resource utilization. In data centers, the biggest costs are power and cooling. If operators can minimize the number of servers needed for NFV by optimizing where the VNFs run, then they can reduce data center operating costs.

The upshot is that SR-IOV resolves the performance issue, but undermines VNF mobility and flexibility. Nonetheless, it is an important step on the path to NFVI automation.

STEP 3. GET DATA DELIVERY TO WORK WITH PERFORMANCE, FLEXIBILITY AND ACCEPTABLE COST

The next step to enabling automation on a common hardware platform is OVS Acceleration. This improves the throughput performance of the virtual switch without the need for hypervisor bypass solutions (e.g., SR-IOV), thereby ensuring VNF mobility as well as cost efficiency for network operators. The technique is similar to Intel's ONP in that it uses OVS and relies on the data plane development kit (DPDK) as the interface to VNFs. The unique piece in the OVS Acceleration solution is a field-programmable gate array (FPGA)-based NIC designed specifically for the requirements of NFV. The solution offloads some of the functionality of OVS onto the NFV NIC so that the virtual switch uses fewer CPU cores and clocks higher overall throughput.

An NFV NIC operates like any standard NIC, providing input and output for traffic coming in and out of standard servers. The way it boosts performance is by creating Continuous Packet Batches that allow thousands of Ethernet frames and IP packets to be transferred at once. An NFV NIC with OVS Acceleration reduces the number actions that the OVS has to perform and increases overall throughput. Most of the OVS functionality remains running in software, but having a smaller workload means that the OVS will use fewer CPU cores.

By not tying the NIC to specific VNFs (as the SR-IOV mechanism does), OVS Acceleration ensures that network operators have the VNF mobility they need for agile service chain creation while also increasing throughput performance. Also, by offloading some of the OVS workload onto the NFV NIC, OVS Acceleration reduces the number of CPU cores that OVS consumes. These freed-up server resources enable operators to increase the density of VNFs per server to run more revenue-generating service functions per server as well as use less server capacity overall, which will lower network operating costs.

A recent case study illustrates the potential cost savings. In a data center with 10,000 servers, it was found that OVS Acceleration with DPDK on an NFV NIC would use eight times fewer CPU cores per server than OVS with DPDK on a standard Intel NIC. OVS Acceleration can provide full 40 Gbps throughput using just one CPU core. This corresponds to a saving of seven CPU cores per server, which translates into 3,890 fewer 18-core CPU chips and 1,945 fewer dual-socket servers. The resulting total capex and opex savings for network operators related to this reduction corresponds to $8 million over four years. In terms of performance, OVS can be accelerated by up to seven times compared to standard NIC solutions that support OVS and DPDK.

STEP 4. EXTEND PERFORMANCE IMPROVEMENTS TO OTHER DATA PROCESSING

OVS Acceleration resolves a major performance problem facing operators today while also meeting operator requirements for flexibility and cost efficiency. But the traffic demands on communications networks are unrelenting, and CSPs need to be equipped to cope with the cost of increasing data loads in the long term as well as shorter term performance improvements. As operating costs typically increase in line with data traffic load, CSPs need new ways of lowering the cost-per-bit. This market reality leads to the next step in NFVI automation, which is extending the performance improvements gained through OVS Acceleration to other common data processing functions.

With an FPGA-based NFV NIC, the same common hardware platform used for OVS Acceleration can be used to accelerate heavy data processing tasks, such as encryption and compression. FPGA-based hardware can be programmed and upgraded remotely, which creates a versatile platform that can serve other functions in an NFV environment. The flexibility of FPGA technology also allows third party IP to be dropped in to the NIC platform to perform a variety of functions. This hardware acceleration approach is essential for building automated NFVI because software-based solutions are typically too costly and resource intensive.

Data compression and encryption are particularly heavy data processing functions that consume a disproportionate amount of CPU cores. But CSPs are having to process increasing amounts of both traffic types. Encrypted traffic is on the rise worldwide. Network policy control vendor Sandvine estimates that 70% of Internet traffic is encrypted across Europe, Latin America and North America.

In the case of data compression, higher data traffic loads and demands for faster data service delivery are pressuring CSPs to store more data in the data center and closer to where customers are located. To mitigate storage costs, CSPs are compressing the data. But processing compressed data in a virtualized environment is resource intensive and consumes too many CPU cores, which ultimately increases data center operating costs.

CSPs can overcome the high cost of processing compressed and encrypted traffic through hardware acceleration on an NFV NIC. For example, hardware acceleration on an NFV NIC uses 40 times less CPU cores compared to software acceleration on server CPUs. In a data center with 10,000 servers, assuming 10% of servers need hardware acceleration, the total capex and opex saving corresponds to $4 million over four years.

STEP 5. PROVIDE INSIGHT FOR CONTINUOUS OPTIMIZATION AND SECURITY

Once the NFVI is running more cost efficiently through hardware-accelerated data processing, the next step is to implement effective network monitoring to enable continuous optimization as well as security solutions. In traditional physical networks, CSPs could monitor traffic by adding a passive Test Access Point (TAP) to the connection that needed to be monitored between two network nodes. Based on a mechanical relay or optical splitter, the TAP ensures that a copy of all traffic is sent to network appliances dedicated to network monitoring or security. Alternatively, routers and switches provide a Switch Port Analyser (SPAN) port, which makes a copy of the traffic activity of one or more switch ports so that it can be analyzed.

But in virtualized networks, these techniques are difficult to replicate. Virtual TAPs are challenged by VNF mobility whereby virtual functions can be moved around and instantiated on different virtual machines. In addition, virtual TAPs or SPAN ports require the duplication of all traffic in the virtual switch so that it can be analyzed by another virtual function. As virtual switching today is performed in software, this effectively means that double the amount of server CPU cores are required when a virtual switch needs to provide TAP or SPAN port functionality.

A more cost efficient way to monitor virtualized networks is to take advantage of the fact that the OVS Acceleration solution implemented on the NFV NIC already sees all the traffic in the virtual switch and can replicate this traffic efficiently without using any server CPU cores. This allows a copy of all traffic to be delivered to another location, whether another virtual appliance or function on the same server or on another server.

By offloading the traffic monitoring functionality onto a common hardware platform, CSPs will not only reduce operating costs through minimized CPU core use, they will also have constant insight into the network performance, enabling further optimization of the NFVI as well as the services and applications they are delivering to customers – and supporting security functions.

CONCLUSION

As cloud end-user demands become more sophisticated, cloud service providers, data center hosting service providers and telecom service providers are both competing and cooperating to assure dynamic connectivity. SDN/NFV are valuable technologies for enabling dynamic connectivity, but to be useful, they must support service agility, security and insight.

With the MEF LSO, the framework for SDN/NFV orchestration solutions is now agreed upon and open-source solutions are available. However, the crucial service agility that orchestration promises will not be realizable without a complementary automation of the NFV Infrastructure.

We are now on step 3 of a 5-step process to automating the NFV Infrastructure and solutions are emerging to enable the final steps. With this in place, the NFV Infrastructure can provide the automation and insight to support service agility with built-in security.

NOTES

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

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

NORTH AMERICA
Napatech Inc.
Boston, Massachusetts
Los Altos, California
Washington D.C.
USA

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

APAC
Napatech China/South Asia
Taipei City, Taiwan
Tel. +886 2 28164533 Ext. 319

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