White Paper

Building Security Into CSP Cloud Transformation Strategies

Prepared by

Patrick Donegan
Chief Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.cisco.com

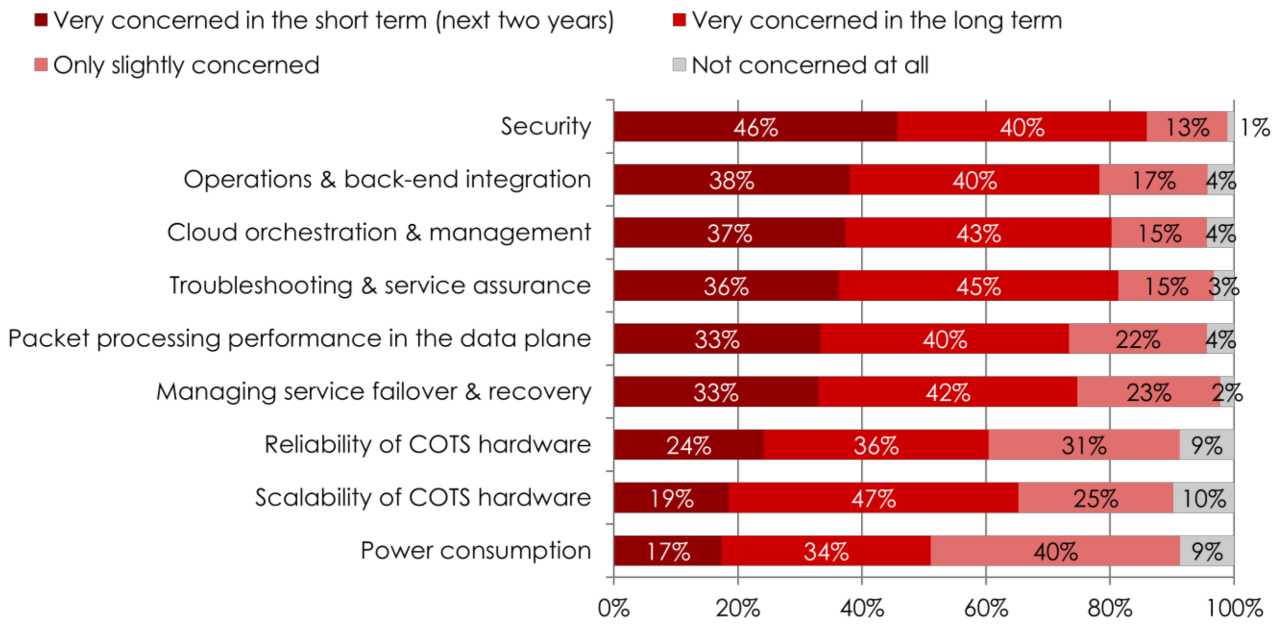
June 2016

Cloud Security: Realities & Imperatives for CSPs

The transformation of service provider networks to more virtualized or "cloudified" network architectures, leveraging network functions virtualization (NFV) and software-defined networking (SDN), is no longer a matter of "if" but of "how?," "how quickly? and "with what impact on business results?" These questions are certainly critical to the future of service providers in the digital economy. One could easily argue that these questions are even existential.

As shown in **Figure 1**, service providers throughout the world are clear that the way in which security is built into their evolving network architecture, technology platforms and operational processes is the single most critical factor that will answer the above questions. They understand that how well (or how poorly) they build security into their network transformation strategy will impact how successful (or unsuccessful) it proves to be – directly and significantly.

Figure 1: Concern About NFV's Technical Implementation Aspects



Source: Heavy Reading's NFV Survey, September 2015

Service Provider Security Strategies: Some Harsh Realities

The threat to ICT infrastructure from cyber attacks is increasing, and rapidly. Service providers can be successful in blocking most attacks, but a subset will inevitably get through. And when they do, the consequences can be devastating. In 2015, for example, one European ISP saw a third of its stock market valuation wiped out after a data breach.

The more open, software-centric environment enabled by SDN and NFV provides critical new capabilities for enhancing network security, but it also introduces significant new risks that service providers don't have experience of managing. In

Heavy Reading's May 2015 survey on "Network Security in the NFV & SDN Era," when asked about the new security challenges that worry them most, service providers identified hypervisor vulnerabilities; the single point of failure created by SDN controllers; and the opening up of network resources to end customers via open APIs.

Network transformation promises the opportunity to capture new revenues and break out of the generally flat revenue trajectory that service providers have endured for many years. But if senior management isn't satisfied with the underlying security of these new business models, they will remain on the drawing board, gathering dust, until the supporting security requirements are met.

Security initially takes a back seat to revenue generation and cost-saving considerations, but this is changing now. Whereas there have been tests and demonstrations of SDN and NFV showing revenue generation and cost savings going back three or four years, more recently we have started to see vendor proof points for building security into service providers' cloud transformation strategies.

Service Provider Security Strategies: Some Imperatives

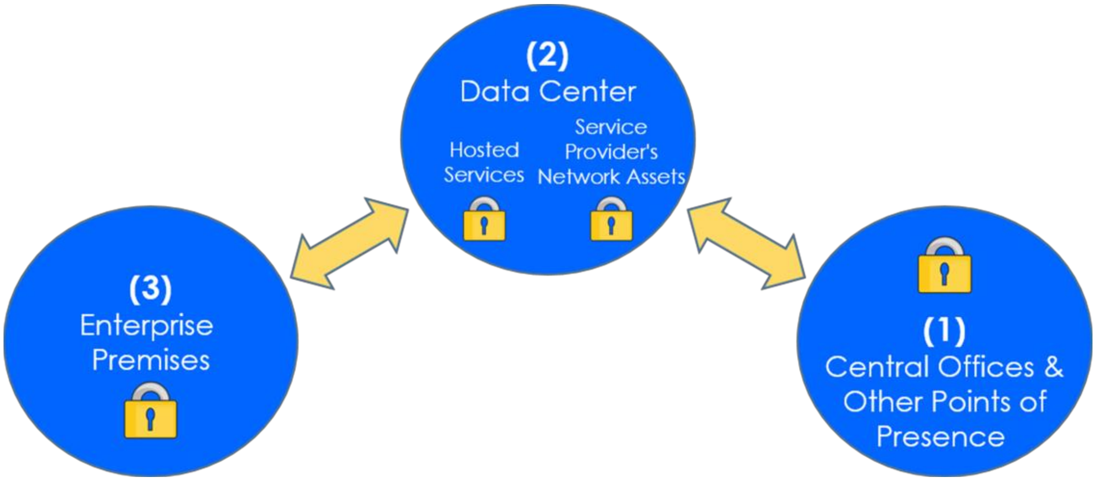
A common security policy framework across network domains: As service providers drive the migration of network assets from traditional central offices and other points of presence to large-scale, next-generation data centers in the cloud, a single security policy framework with common orchestration and common lifecycle management across both of these networking domains is essential. Having separate security frameworks for each domain would reinforce conventional security silos in the service provider organization when the express purpose of NFV and SDN is to break them down to drive stronger, more flexible and more efficient security. Service providers that are positioned as managed security service providers (MSSPs) delivering security services to enterprises should also consider the merits of extending that same set of security policy tools out to a third domain – the enterprise customer premises.

A common security policy framework across different network instances: For the next several years, service provider networks will comprise both conventional physical and new virtual network instances. Some firewall and DDoS protection requirements on particularly high capacity interfaces will continue to require conventional physical hardware instances. It will be some years before virtualized network functions (VNFs) are able to scale sufficiently to mitigate a 500 Gbit/s DDoS attack, for example. In other cases, security applications will increasingly be spun up as VNFs on industry standard servers. Where service providers want the same vendor for both physical and virtual instances of a given security application, they will require competitive differentiation and a consistent feature set across both physical and virtual instances.

A common security policy framework that integrates the contributions of the primary network infrastructure, not just the dedicated security infrastructure: The universal presence and visibility into network traffic that elements like switches and routers have, and the telemetry they generate, needs to be more tightly integrated with threat intelligence in support of superior threat detection outcomes. Switches and routers should also be enabled to participate more in the enforcement of security policy, allied with the spinning up of specialized security VNFs. They provide the security architecture with many more points of presence for a more distributed architecture, and at lower cost than specialized security infrastructure.

Cost containment: Being intent on accelerating new applications and services (each one with its own unique security profile), and with the quantity and sophistication of security threats inevitably increasing, service providers fear that the price of maintaining a competitive security stance in lockstep with rapid new service innovation could be a ballooning security budget. The service provider organization's strict financial disciplines won't allow this, however. While temporary increases in spending can be considered in some cases, the security budget has to be capped over the medium term at the very least.

Figure 2: The Three Domains of Service Provider Security


(2)
Data Center
Hosted Services
Service Provider's Network Assets
(3)
Enterprise Premises
(1)
Central Offices & Other Points of Presence

Source: Heavy Reading

Blocking, Detection & Mitigation of Threats

Blocking of threats at the perimeter via solutions like firewalls remains an important part of security strategy. They ensure that the majority of threats are stopped before they penetrate the network. However, the certainty that a minority of threats are always going to be sophisticated enough to escape detection at the perimeter, and the magnitude of the damage that some of these threats are proven to cause, means that threat blocking has the status of basic table stakes today.

Service providers' focus increasingly needs to be on the real-world success rate of their threat detection and threat mitigation capabilities. Of particular importance now are the mean time to detection and the mean time to mitigation of security threats. Whether it be serving a botnet or carrying out data exfiltration or some other attack type, the longer malware is left to reside and operate in the network, the more damage it will do. Hence, reducing the time to detection from months or weeks to days or hours is a priority security objective. Similarly, with something like a DDoS attack, where detection is likely to be comparatively rapid, the cost in lost revenue and cost penalties can be such that when it comes to time to mitigation, every minute – or even every second – counts.

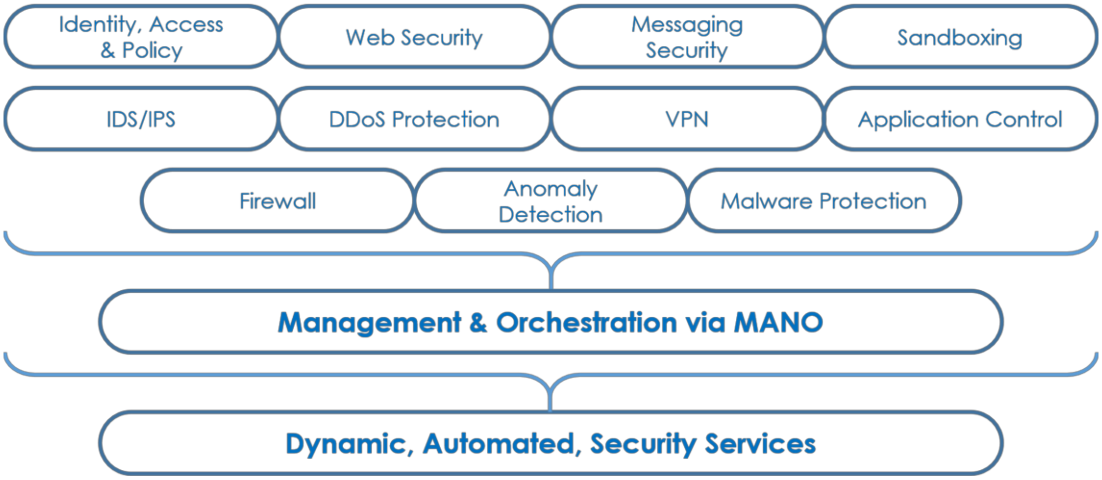
The following details key capabilities that are needed for reducing time to detection and time to mitigation. Some are universally applicable across the ICT sector. Some are unique to the service provider environment. Others originated in the cloud or data center and are now making their way into the service provider environment.

The State of the Art in Detection & Mitigation

There are several trends in the network security market that service providers need to align with in much the same way as any other organization must if it wants to dramatically reduce time to detection and time to mitigation. Among these are a focus on the following:

- **Access to the very best threat intelligence** from third-party partners with a global reach.
- **As previously mentioned, tight integration of threat intelligence** with both the security infrastructure layer and the primary infrastructure layer of switches, routers and other elements.
- **Application layer security at L5-L7.** Conventional L3/L4 network security is effective at blocking the large majority of attacks. But sophisticated attackers long ago figured out how to write apps that get past them, using techniques such as encryption and polymorphic code that mutates in order to avoid detection. An increasing number now focus on identifying specific vulnerabilities in server resources, such as the Domain Numbering System (DNS), Session Initiation Protocol (SIP) and HyperText Transfer Protocol (HTTP) with low volumes of malicious traffic.
- **Real-time anomaly detection leveraging behavioral analytics to detect previously unknown threats.** Conventional deterministic rules-based signature detection is effective at identifying most threats that conform to a generic template already seen in multiple instances all over the world. But many newer, more sophisticated attacks, some of which are expressly designed to exploit the unique vulnerabilities of a specific network, do not present a readily identifiable malicious signature. Anomaly detection techniques that leverage behavioral analytics to observe, store and correlate the unique traffic patterns in a specific network – and flag marked deviations from the norm – are therefore an increasingly important component of advanced threat detection and mitigation.
- **Secure sandboxing for cataloguing malware and malware behaviors** as well as allowing the safe investigation of unknown files.

Figure 3: Some Key Building Blocks in Service Provider Security



Source: Heavy Reading

Security Resources Unique to the Telecom Network Infrastructure

Service providers have unique insight into security threats by virtue of one of their primary functions being to transport traffic between network end points. This gives them early visibility into information about traffic and traffic patterns, which can be used to protect their own infrastructure, as well as that of their enterprise customers.

NetFlow has been used to that end for many years, but as service providers begin to leverage the capabilities of SDN and NFV, as shown below, new opportunities are opening up to aggregate not just NetFlow, but also other types of behavioral telemetry across the network. If that data can then be effectively rolled up into a powerful analytics engine, service providers can have far better visibility than they have had until now – and far better visibility than other actors in the cybersecurity ecosystem. That can enable them to detect and mitigate threats much more rapidly than they have traditionally been able to.

Security Best Practice Drawn From the Cloud

Much of the value in deploying leading-edge threat detection and mitigation capabilities can only be realized by service providers applying them in the context of their network transformation strategies, and by leveraging the key technologies and best practices associated with networking in the cloud or data center. Three key requirements stand out in this regard:

NFV

NFV enables the service provider to deploy security VNFs instantly at the closest possible point in the network to wherever the threat is first detected. This flexibility allows the service provider to be far more effective in minimizing the impact of an attack than today's model, which tends to consist of a handful of hardware-based security devices that are stationed permanently at the perimeter, often heavily over-provisioned, potentially several nodes or links away from the attack.

NFV flexibility also allows rapid time to market for new applications and services with the exact security policies they need for executive management to be willing to allow them to be launched. As shown in **Figure 4** (next page), a majority of service providers expect most network security applications to be deployed as VNFs. The same survey showed half or more respondents expecting to deploy firewalls, Web security, messaging security and intrusion detection systems/intrusion prevention systems (IDS/IPS) as VNFs to enterprise customers.

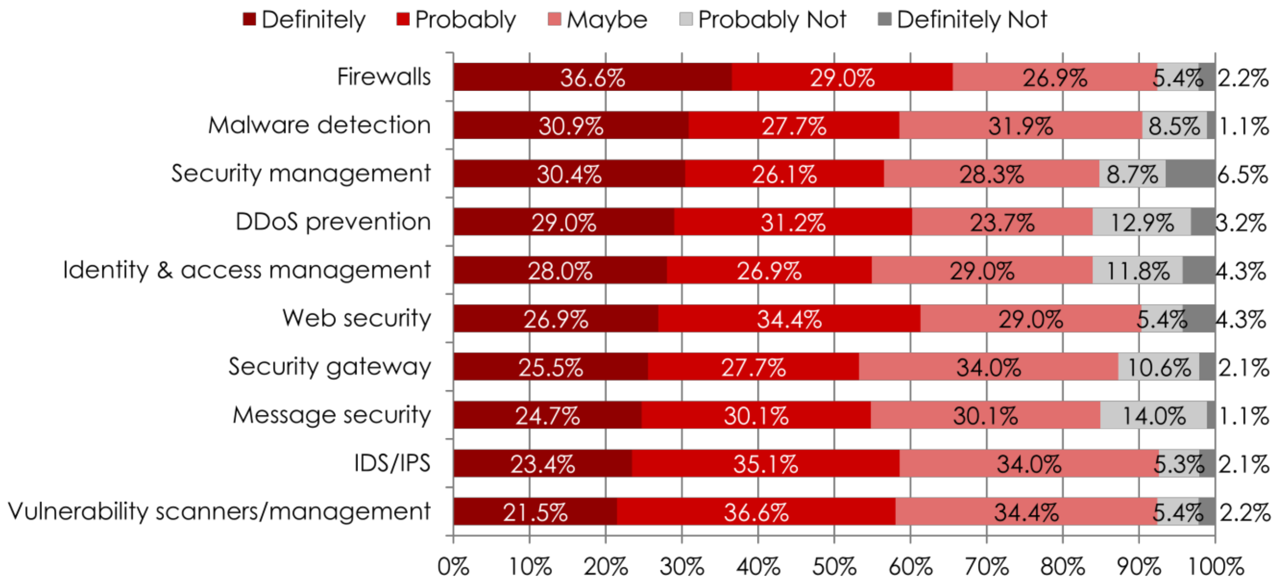
SDN

With its network-wide visibility into the control plane, no other networking device available to service providers is better able to support the aggregation of NetFlow and multiple other traffic-related data feeds for superior security outcomes than the SDN controller.

Security for East-West Traffic

A holistic approach to service provider security needs to take account of the patterns of both North-South traffic (traffic entering and exiting the data center, central office or other point of presence) and East-West traffic (traffic between application servers, typically in the data center). In the data center, East-West traffic is a lot higher than North-South traffic, typically by a factor of three or four to one. In central offices or other points of presence, the ratio typically favors North-South traffic. This is important from a solution standpoint, because some security solutions can scale well in either direction, whereas others are better suited to one or the other.

Figure 4: Service Provider Intent to Deploy Security Applications as VNFs



Source: Heavy Reading's "Network Security In The SDN And NFV Era," May 2015; n=97

Automation of Security Policy

It's often underappreciated just how small the security team in the service provider really is. Outside of the largest service providers, most security teams comprise no more than a handful of people – sometimes no more than three or four. Many small service providers don't even have a full-time person dedicated to security.

It's also underappreciated just how much of this small team's time is tied up with day-to-day security administration today. This includes things such as configuring firewall rules or undertaking manual investigations into security breaches and meeting to determine mitigation responses. In some cases, in may include manually generating their own attack signature relating to their unique network and network traffic characteristics. The vast majority of the security team's time is spent "firefighting" or "looking in the rearview mirror."

So the service provider's objective is to accelerate innovation in new services and applications supported by security; the sophistication of cyber threats is increasing; the already-small security team faces having more and more demands placed on it when it is already knee deep in firefighting; and the security budget can't increase much (if at all). If the security team is to have any chance of getting on the front foot and spending more time anticipating and preparing to combat the upcoming threats that are in the pipeline, something has to change.

This is where network automation comes in. If enabling the most rapid time to market with new services and the most rapid time to threat detection and mitigation are the ultimate security "ends" for service providers, then network automation is emerging as the ultimate "means" for delivering that end objective. Critically, automation promises the ability to improve the service provider's security stance and enable service agility while also keeping security spending under control.

Orchestration Is the Key to Automation

Orchestration is the key to driving successful automation of security policy in service provider networks. That means the ability to dynamically identify available hardware resources and dynamically spin up the right security VNFs wherever they are needed in the network. That can be in response to a specific security threat. Or it can be in an MSSP context, in which the service provider is managing multiples of the same security VNF for different enterprise clients off the same networking device.

Security orchestration needs to be common across conventional physical and new virtualized instances of security software; it needs to be common across the data center, central office and other points of presence (and potentially the enterprise customer premises as well); and it needs to be informed by real-time security threat intelligence as well as network behavior analytics.

Service Chaining With Multiple Vendors

Service chaining is closely linked with orchestration in the emerging service provider network architecture. In its basest form, it's not a new idea. In traditional network architectures, service chains are created in hardware. For example, in the security context, some traffic flows might be routed to a traditional dedicated firewall followed by a traditional IDS. The service chain is established – and fixed – in hardware.

As already shown, in a virtualized environment, orchestration provides the ability to spin up security VNFs anywhere in the network. Since this means that the service chain is no longer fixed – i.e., no longer changeable only via physical hardware changes – the role of service chaining evolves to one of dynamically establishing service chains on the fly in software. This means dynamically establishing the exact right chain of security VNFs in the exact right sequence in support of a given application or service.

The ability to dynamically generate services chains of network security software – in the right sequence and at scale – is therefore a key requirement for service providers as they seek to transform their networks. When executive management looks to sign off on the launch of new services and applications, service chaining is a layer of detail that must be looked into. It is key to driving network optimization – ensuring that each flow has applied to it the exact security policies that it requires, and no more. It is also key to monetization – providing the platform from which security can always remain in lockstep with new service deployment plans, rather than being an afterthought that delays time to market or even leads to the time-to-market window being missed altogether.

Consistent with that, service providers need to be able to compose service chains comprised of the security VNFs of multiple vendors. The service provider may prefer its virtualized firewall from one vendor, its virtualized IDS solution from a second, and its DDoS solution from a third – to protect either its own network, or that of its enterprise customer. Service chaining must be able to support these various security VNFs from different vendors and ensure that each one is activated in the correct sequence in the chain, and at scale.

Scalability & Performance

In importing SDN and virtualization concepts from the IT environment into the service provider environment, one of critical requirements that service providers have is that implementations in their environment must confirm to the higher standards of scalability and performance that their customers expect, and that their regulators also hold them to.

Understandably, when standard industry servers rather than proprietary hardware are used to power security VNFs, service providers need proof points that they will get the scalability and carrier-grade performance they need. Once again, while good progress has already been made in demonstrating scalability where many network functions are concerned, proof points regarding security VNFs have only begun to be offered up more recently. Among the key metrics that need to be demonstrated are throughput, capacity and the connection setup rate across both physical and virtual environments, as well as metrics for resiliency and failover.

Specific Performance Requirements for Supporting Multi-Tenancy

What applies with respect to performance requirements at the level of the network as a whole also applies in microcosm when it comes to supporting multi-tenancy in the context of being an MSSP delivering security services to enterprises. In this context, multi-tenancy refers to service providers as MSSPs leveraging the same server resources to host the security VNFs, such as firewall VNFs, of multiple different enterprise customers. The economies of scale that can be realized are one of the core value propositions of NFV.

Once again, however, these benefits can only be commercially exploited if the service provider is confident that it can guarantee the independence and security of each customer's own VNF. Specifically, service providers need to be able to see how groups of security VNFs can be successfully instantiated on the same server resources and that both hardware and software failover mechanisms perform well.

Summary

As they evolve their networks toward increasing software programmability, service providers need to maintain the baseline security they have always provided. They need to evolve security further to support the rollout of new revenue-generating services that have unique security requirements. SDN and NFV also transform the market opportunity for service providers to sell security as a service to large, medium and small enterprises.

In looking to leverage a unified, software programmable security architecture across central offices, the data center, other points of presence – and potentially the enterprise customer premises, as well – service providers need to be able to combine the very best in threat detection and mitigation capabilities with the very best in open, software-programmable networking solutions.

The ability to assemble a competitive suite of security applications from multiple best-of-breed networking and security vendors, and then integrate them and automate their deployment flexibly, with full orchestration and service chaining – and at scale – is critical to the success of any service provider achieving its network transformation goals.

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. For ongoing news, please go to thenetwork.cisco.com.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners.