PROVIDING SECURITY IN NFV

CHALLENGES AND OPPORTUNITIES

STRATEGIC WHITE PAPER | NFV INSIGHTS SERIES

While Network Functions Virtualization (NFV) introduces new challenges to security, it also presents unique opportunities for addressing security problems because of the unprecedented scale, flexibility and central control it affords. Compute, storage and network resources can be optimally allocated and stitched together, as required by the security policy. A recursive divide-and-conquer approach can be used to address NFV security, with security schemes applied at the platform, virtualized network zones and application levels. To reduce complexity, a centralized approach that leverages automation capabilities is recommended. Alcatel-Lucent CloudBand™ enables this approach.

About the NFV Insights Series

NFV represents a major shift in the telecommunications and networking industry. NFV applies virtualization and cloud principles to the telecommunications domain, something that appeared to be impossible until recently due to the stringent performance, availability, reliability, and security requirements in communication networks. Many service providers are now keen to implement NFV to help them become more agile in delivering services, and to reduce equipment and operational cost. This series of whitepapers addresses some of the key technical and business challenges on the road to NFV.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Network Functions Virtualization (NFV) has been positioned to revolutionize both the construction and operation of telecommunication networks. Among the major expected benefits of NFV are the savings that result from using general-purpose hardware and increased automation—which in turn decreases time to market. NFV will also create an environment that is particularly favorable to innovation.

No doubt, NFV introduces new challenges to security, but at the same time it provides unprecedented opportunities for developing novel security solutions and improving the inherent security properties of on-boarded applications.

Among the key security challenges—all introduced by virtualization—are:

- Reliance on additional software (that is, hypervisors and modules for management and orchestration) and hence a longer chain of trust
- Reduced isolation of network functions
- Fate-sharing due to resource pooling and multi-tenancy
- Effective key escrow for hosted network functions

The good news is that there are mechanisms and tools to deal with these challenges. Furthermore, the unprecedented scale, flexibility and central control afforded by NFV dramatically improve the effectiveness of the key mechanisms, such as automation, analytics, virtual security appliances and hypervisor-based introspection.

A recursive divide-and-conquer approach can be applied to address NFV security. When this is done, it is clear that the opportunities NFV creates for improving overall security outweigh potential problems. Alcatel-Lucent CloudBand™ provides a critical enabler for this approach, offering a platform on which network functions can become more secure than ever. In particular, CloudBand facilitates a policy-driven approach to orchestration, security zoning and workload placement. That includes the user's ability to specify security policy using the standard OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) language.

As a result, compute, storage and network resources can be optimally allocated and stitched together, as required by the security policy. If, for example, the policy requires that certain virtual network functions (vNF) components be separated physically, they will be placed on different hosts. Similarly, virtual security appliances can be spun up automatically and chained together according to the provider's policy.

CloudBand aims to support state-of-the-art security analytics to enable security anomaly prediction, detection and isolation. Together with its built-in automation capabilities, it can proactively and reactively remediate security problems. Finally, CloudBand is designed to be an enabling platform for security as a service, which carriers can offer to hosted providers.

INTRODUCTION

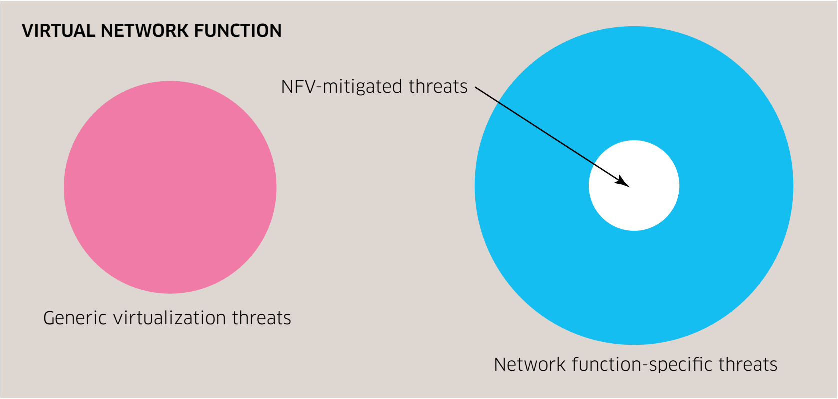
NFV is an initiative that was spearheaded by major network operators [1]. It deals with virtualization and relatively centralized management of various network modules previously deployed as physical devices.

It is an adage in the security community that technological evolution drives evolution in the threat landscape as well. New layers, components, interfaces and capabilities can give rise to new chances for attack by malicious agents. Nonetheless, new technologies also make possible novel security solutions. In the case of NFV, the opportunities are expected to outweigh any potential problems. This paper reviews the security threats, challenges and opportunities in NFV, and outlines a blueprint for achieving comprehensive security in an NFV environment. It also highlights Alcatel-Lucent CloudBand's role in effecting security improvements as specified in the blueprint.

SECURITY THREATS AND THE MITIGATION STRATEGY

The first question to ask when considering the security of NFV is which threats apply to a vNF? Figure 1 shows a diagram to answer this question.

Figure 1. Threat diagram for virtual network functions


VIRTUAL NETWORK FUNCTION
NFV-mitigated threats
Generic virtualization threats
Network function-specific threats

In the simplest case, a vNF is a network function running on a virtual machine (VM). The overall set of security threats to a given vNF can be, at the first approximation, viewed as a combination of all generic virtualization threats and those threats specific to the network function software. The generic virtualization threats are governed by the security properties of the virtualization platform consisting of software and hardware. The network function-specific threats are determined by the quality of the network function's design and software implementation. But virtualization provides an added security benefit: the potential to eliminate or mitigate some threats inherent to the network function software through new mechanisms such as hypervisor introspection [2] and centralized security management.

For example, by using hypervisor introspection, root-kits can be eliminated. Further, run-time memory analysis can improve the security posture of the vNF. Centralized security management, on the other hand, allows network functions to be configured and protected effectively according to a common policy as opposed to a collection of per-NF security procedures that may not always be consistent and up-to-date. It follows then that the strategy for improving security of a vNF must be two-pronged so as to combine:

1) Shrinking the circle on the left in Figure 1 as much as possible by securing the virtualization platform, and
2) Carving as large a hole as possible out of the circle on the right by applying NFV-enabled security mechanisms such as hypervisor-based introspection.

Specific threats are, of course, deployment-dependant. The sections below describe four NFV deployment models: private, exposed, hybrid, and community. Each model adds security threats to those in the previous model. This taxonomy is consistent with both the NIST model [3] and the present taxonomy of the ETSI NFV Security Expert Group [4].

Private NFV deployment model

In the private NFV deployment model, the carrier exclusively owns the cloud, network function software, and service portal. The network functions do not face subscribers or provide any external access, although they may be managed by the respective carrier business units. In this rather sterile environment, the attack surface is relatively contained, with the main threats coming from insiders. However, something as simple as a configuration error can expose a network function to the public Internet. Furthermore, a rogue insider can cause considerable damage, especially when regulations require that the different business units are responsible for separate network functions. Insider attacks can be mitigated through identity and access management techniques (specifically, role-based access control [5]) and application of the principles of the "least privilege" and "separation of duties" to ensure that personnel are assigned to distinct roles with constrained authority. In concert with this, analytics applied to access logs can provide early indications of suspicious activities.

Other threats in the private NFV deployment model include exploits caused by flaws in virtualization software and vulnerabilities of image files. Applying the defense-in-depth principle to employ multi-facet and multi-layer security controls can help mitigate these types of threats. More specifically, to counter these threats, the Cloud Security Alliance (CSA) has developed a comprehensive set of security controls [6].

Exposed NFV deployment model

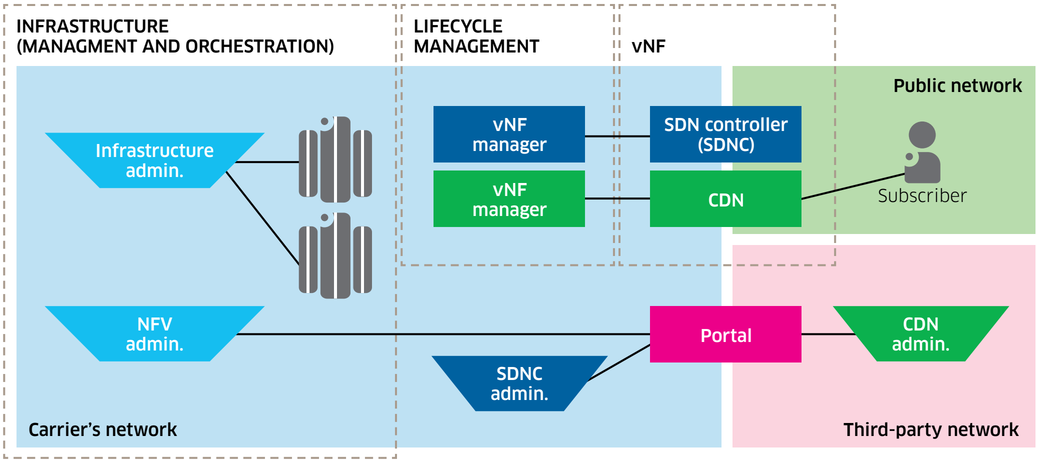
The exposed NFV deployment model differs from the private model in that some network functions (for example, the Content Delivery Network (CDN) server) are exposed to subscribers directly and are accessible from the public network. In this model, all threats of the private NFV deployment model apply, further amplified by the public Internet access. A major problem is that an infiltration or compromise of a public-facing network function may further spread to the NFV manager and the rest of the infrastructure. The key additional defense mechanisms that apply here include hardening of the network function augmented by employing security zoning, hypervisor introspection and analytics.

Hybrid NFV deployment model

The hybrid NFV model, which further exposes the infrastructure to outside access, is shown in Figure 2 (where bold font is used to emphasize new virtualization-specific threats). In this model, vNFs may be managed from a third-party network (such as an enterprise network) via a portal. It is evident that third-party access to the portal provides a vector for an attack on the carrier's network. Again, mitigation of these types of attacks can be achieved through systematic implementation of identity and access management (which limits the extent of the third-party's actions), hardening of the portal, and other well-known security best practices.

Having a third-party vNF also presents a new security problem—an involuntary potential for the escrow of cryptographic keys (since those are visible to the hypervisor). Here the keys that are part of the vNF image (and possibly other sensitive data) are visible to the hypervisor, and thus to anyone who has access to it. In other words, the carrier or NFV provider has access to the keys. In certain jurisdictions, a valid digital signature must have the attribute that it is under the sole control of the user. Key escrow does not meet this requirement, limiting the services that the carrier can provide. Ideally, the carrier should not have control of cryptographic keys (for both signing and encryption). One solution to this end is for the carrier to offer key storage and cryptographic services in specialized hardware security modules (HSM).

Figure 2. Hybrid NFV deployment



Threats:

- Exploitation or violation due to:
  - ¬ administrative error
  - ¬ native vulnerabilities of vNFs
  - ¬ **vulnerabilities of virtualization software**
  - ¬ **vulnerabilities of images**
  - ¬ vulnerabilities of hardware or firmware
  - ¬ denial of service
  - ¬ rogue insider
  - ¬ **(involuntary) key escrow**

Community NFV deployment model

The most exposed NFV deployment model is the community NFV deployment. Here the carrier hosts network functions that are deployed and managed by different parties via the Internet (for example, when an enterprise's services are hosted in the carrier's cloud). All the previous threats apply. In addition, there are the potential threats of an attack by a malicious vNF or other application, which can ripple through the carrier's whole infrastructure. Such threats can be mitigated by employing mechanisms such as security zoning and firewalls.

A byproduct of hosting a malicious vNF is what Berkeley [7] calls reputation fate sharing. The behavior of a single cloud customer can affect the reputation of the cloud as a whole. For example, reputational blacklisting of the IP address of a malicious vNF could also have the effect of blacklisting innocent vNFs as collateral damage.

In the community NFV deployment, as is the case with a public cloud, there is a duality of purpose. It is in the interest of a customer to keep the environment secure, but it is all the more in the interest of the cloud provider to keep the customer secure so that the whole environment stays healthy. In addition, security services offered to customers are another source of revenue, while offering those services requires little new infrastructure. In fact, the cloud infrastructure is in itself a perfect medium for offering new services.

NFV SECURITY CHALLENGES AND OPPORTUNITIES

There are several key security challenges with NFV, when compared with classical deployments of network functions, including:

- Reliance on additional software (that is, the hypervisor and modules for management and orchestration) and hence a longer chain of trust
- Reduced isolation of network functions
- Fate-sharing due to resource pooling and multi-tenancy
- Effective key escrow for hosted network functions

The good news is that there are mechanisms and tools to deal with these challenges. Furthermore, there are unique opportunities in NFV when it comes to security, including:

- **Lower cost of ownership**: NFV holds the promise of lower total cost of ownership through lowering CAPEX by migrating functions from proprietary to commodity hardware, and from dedicated boxes to virtual machines. This is as true for security appliances and functions as for other network products and applications.
- **Streamlined security operations**: In a cloud environment, multi-tenancy drives the need for logical separation of virtual resources among tenants. Through orchestration, certain vNFs can be deployed on separate compute nodes, and they can be further segregated by using separate networks. In addition, the use of security zones allows vNFs to be deployed on—or migrated to—hosts that satisfy security-pertinent criteria such as location and level of hardening (for example, some hosts may employ the trusted computing technology).
- **Patch management**: NFV can ease the operational impact of deploying security updates. An upgraded instance of the vNF can be launched and tested while the previous instance remains active. Services and customers can then be migrated to the upgraded instance over a period of time (shorter or longer as dictated by operational needs). The older instance with the un-patched security flaw can be retired once this is complete.
- **Incident response**: NFV opens up new possibilities in incident response owing to the inherent flexibility it introduces. For example, automated incident response could include rapid and flexible re-configuration of virtual resources.

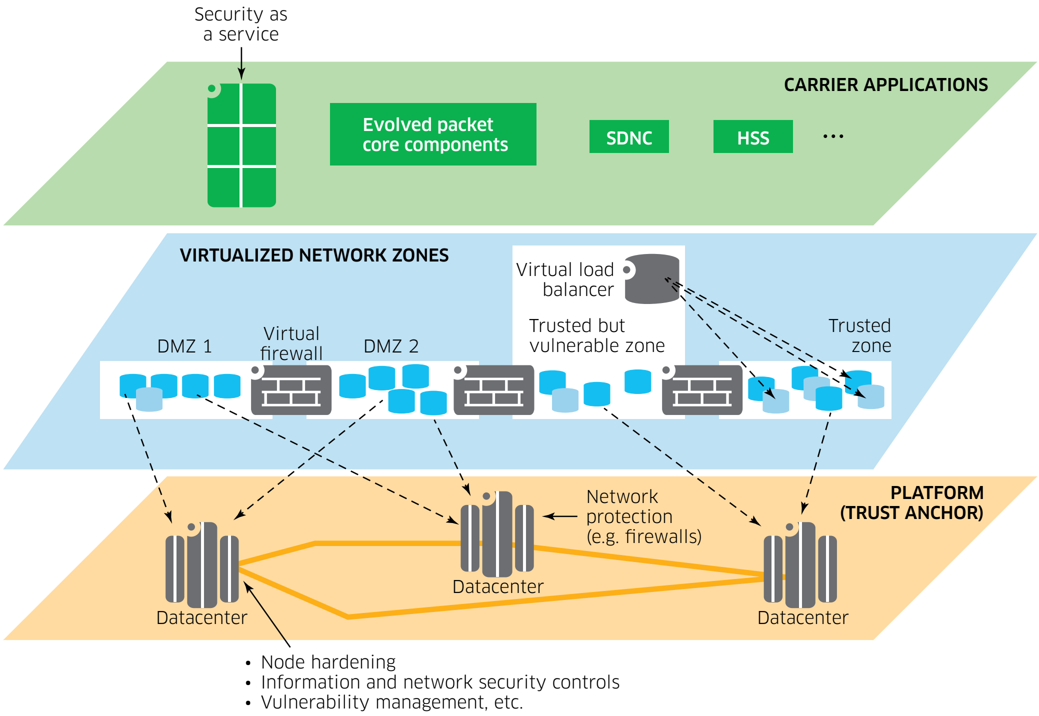
Another characteristic of network function virtualization that leads to improved incident response is the relative ease of decommissioning and re-commissioning vNFs. If a vNF is suspected of having been compromised (for example, through unauthorized access via a back door), an uncompromised version can be instantiated to replace it and the compromised version can be decommissioned and a copy of it made for forensic analysis.

BUILDING UP COMPREHENSIVE SECURITY WITH NFV

Service providers will likely want to undertake a systematic approach to developing security in an NFV environment. The major underlying scheme is recursive in its nature—a build-up of more complex services on top of the elementary ones. As depicted in Figure 3, security is applied at three distinct layers:

1. NVF platform
2. Virtualized network zones
3. Carrier applications

Figure 3. Building up comprehensive security



Security as a service
CARRIER APPLICATIONS
Evolved packet core components
SDNC
HSS
...
VIRTUALIZED NETWORK ZONES
Virtual load balancer
Trusted but vulnerable zone
DMZ 1
Virtual firewall
DMZ 2
Trusted zone
PLATFORM (TRUST ANCHOR)
Network protection (e.g. firewalls)
Datacenter
Datacenter
Datacenter
• Node hardening
• Information and network security controls
• Vulnerability management, etc.

NFV platform security

The foundation is the NFV platform, which includes the datacenters with basic compute capabilities, the networks that interconnect them, and the operations and management systems, including the management and orchestration modules. The first order of business is to ensure platform security through known controls and to achieve physical and logical zoning.

The tasks for ensuring platform security can be grouped according to what they are securing:

- Physical cloud nodes (for compute, storage and networking)
- Management systems (that is, lifecycle, orchestration and API access)
- Connectivity

When orchestration allows cloud bursting, cloud federation controls should apply. As described earlier, controls have been published by the Cloud Security Alliance. For OpenStack®-based clouds, the OpenStack Community has published a comprehensive security guide for bolstering platform security [8].

Virtualized network zone security

The second security layer in the NFV environment is the deployment of virtual security appliances. For instance, virtual firewalls can be deployed to establish new network zones. The result is as secure as it would be with physical firewalls, but at much higher speed, lower cost, and with unprecedented flexibility. This new, virtualized environment, which may include visibly separate networks—offered as a service—can be much more complex than that of any carrier's network now, yet its security is backed by the platform controls.

Carrier application security

The third NFV security layer is the application level. Virtualized functions in support of applications, such as the Evolved Packet Core, SDNC, and Home Subscriber Service (HSS), are placed in the established security zones. The security of that deployment is assured by a combination of native application security controls and those provided at Layer 2. This is then further enhanced by the platform capabilities. Once deployed, the security services provided by the applications can be recursively used to further improve platform security. For instance, the virtualized HSS can be used to provide an extra authentication factor for access to platform software [9].

Building the case for automation

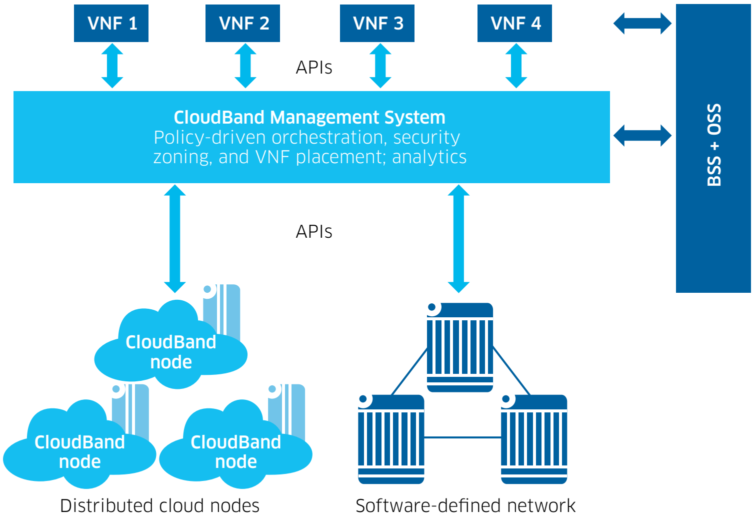
One problem with this multi-layered approach is the seeming complexity of the resulting system. Even with all security processes and policies properly documented and the datacenter personnel trained, there is far too much information to be left to manual processing. Hence the security processes need to be automated and implemented as part of the management system that oversees the cloud environment in all datacenters and compute nodes. A centralized management system for command and control can ensure systematic and consistent implementation of security.

Security monitoring appliances [10] can be extremely beneficial. Interworking with hypervisors, these appliances can provide fine-grained inspection of virtual machines' memory without modifying virtual machines themselves. By using analytics on the data collected from the platform and multiple security appliances, the centralized management system can assess, in near-real time, the state of security in the whole cloud, and then—when necessary—quickly take an enforcement action combined with remediation through auto-healing. Similarly, virtual load balancers and virtual DNS servers (in addition to their main purposes) can be deployed to further mitigate DOS attacks, complementing other anti-DOS measures.

ALCATEL-LUCENT CLOUDBAND

Alcatel-Lucent CloudBand is an NFV platform designed for carrier requirements. CloudBand consists of a centralized management system and distributed cloud nodes (see Figure 4).

Figure 4. Alcatel-Lucent CloudBand, a secure NFV platform



Alcatel-Lucent CloudBand takes a holistic approach to security. It adheres to the pertinent best practices as outlined earlier in this paper. It also exploits various mechanisms to provide a platform on which network functions can become more secure than ever. To begin with, the CloudBand Node and its networking have been secured, according to the industry practices. In addition, CloudBand takes a policy-driven approach to orchestration, security zoning and workload placement. That approach includes user’s ability to specify security policy using the standard TOSCA language. As a result, compute, storage and network resources can be optimally allocated and stitched together, according to the security policy. If, for example, the policy requires that vNFs be separated physically, they will be placed on different hosts. Similarly, virtual security appliances can be spun up automatically and chained together according to the carrier’s policy. Through integration with the OSS and BSS, the relevant policies from those systems can be taken into account as well.

CloudBand also aims to support state-of-the-art security analytics to enable security anomaly prediction, detection and isolation. Together with its built-in automation capabilities, it will be able to proactively and reactively remediate security problems in an unmatched fashion. Finally, CloudBand is designed to be an enabling platform for security as a service. This allows carriers to host network elements with enhanced security for enterprises and other carriers.

CONCLUSION

As far as security is concerned, NFV presents unique opportunities for addressing security problems because of the unprecedented scale, flexibility and central control it affords. The “recursive build-up” approach described in this white paper is one structured way to achieve improved NFV security. Alcatel-Lucent CloudBand is a critical enabler in this approach, offering a platform on which network functions can become more secure than ever.

For more information please contact: David Amzallag (David.Amzallag@alcatel-lucent.com), Igor Faynberg (Igor.Faynberg@alcatel-lucent.com), Huilan Lu (Huilan.Lu@alcatel-lucent.com)

REFERENCES

[1] White paper by network operators on “Network Functions Virtualisation,” October 2012, <http://portal.etsi.org/nfv/nfv_white_paper.pdf>.

[2] T. Garfinkel and M. Rosenblum, “A Virtual Machine Introspection Based Architecture for Intrusion Detection,” Proceedings of the Network and Distributed Systems Security Symposium, February 2003.

[3] P. Mell and T. Grance, “The NIST definition of cloud computing”, NIST special publication 800-145, September 2011.

[4] ETSI NFV Security Problem Statement, <http://docbox.etsi.org/ISG/NFV/Open/Latest_Drafts/nfv-sec001v009-NFV_Security_Problem_Statement.pdf>.

[5] I. Faynberg, H. Lu, and H. Ristock. “On dynamic access control in Web 2.0 and beyond: Trends and technologies,” Bell Labs Technical Journal, vol. 16, no. 2 (2011), 199-218.

[6] Cloud Security Alliance, “Cloud Control Matrix,” <https://cloudsecurityalliance.org/research/ccm/>.

[7] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica. “Above the clouds: A Berkeley view of cloud computing,” Dept. Electrical Engineering and Computer Sciences, University of California, Berkeley, Rep. UCB/EECS 28 (2009), <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>.

[8] OpenStack Community, “OpenStack Security Guide,” 2014, <http://docs.openstack.org/sec/>.

[9] I. Faynberg, M. A. Hartman, H. Lu, and D. W. Varney, “On New Security Mechanisms for Identity Management: Recognizing and Meeting Telecom Operator and Enterprise Needs,” Bell Labs Technical Journal, vol. 15, no. 1 (2010), 95–113.

[10] Ibrahim, A.S.; Hamlyn-Harris, J.; Grundy, John; Almorsy, M., “CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model,” 5th International Conference on Network and System Security (NSS), ISBN: 978-1-4577-0458-1, pp.113-120, 6-8 Sept. 2011.

ACRONYMS

API	Application programming interface
BSS	Business support system
CAPEX	Capital expenditures
CDN	Content Delivery Network
CSA	Cloud Security Alliance
DOS	Denial of Service
HSM	Hardware security modules
HSS	Home Subscriber Service
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OSS	Operating support system
SDNC	Software-Defined Networking Controller
TOSCA	Topology and Orchestration Specification for Cloud Applications
VM	Virtual machine
vNF	Virtual network function