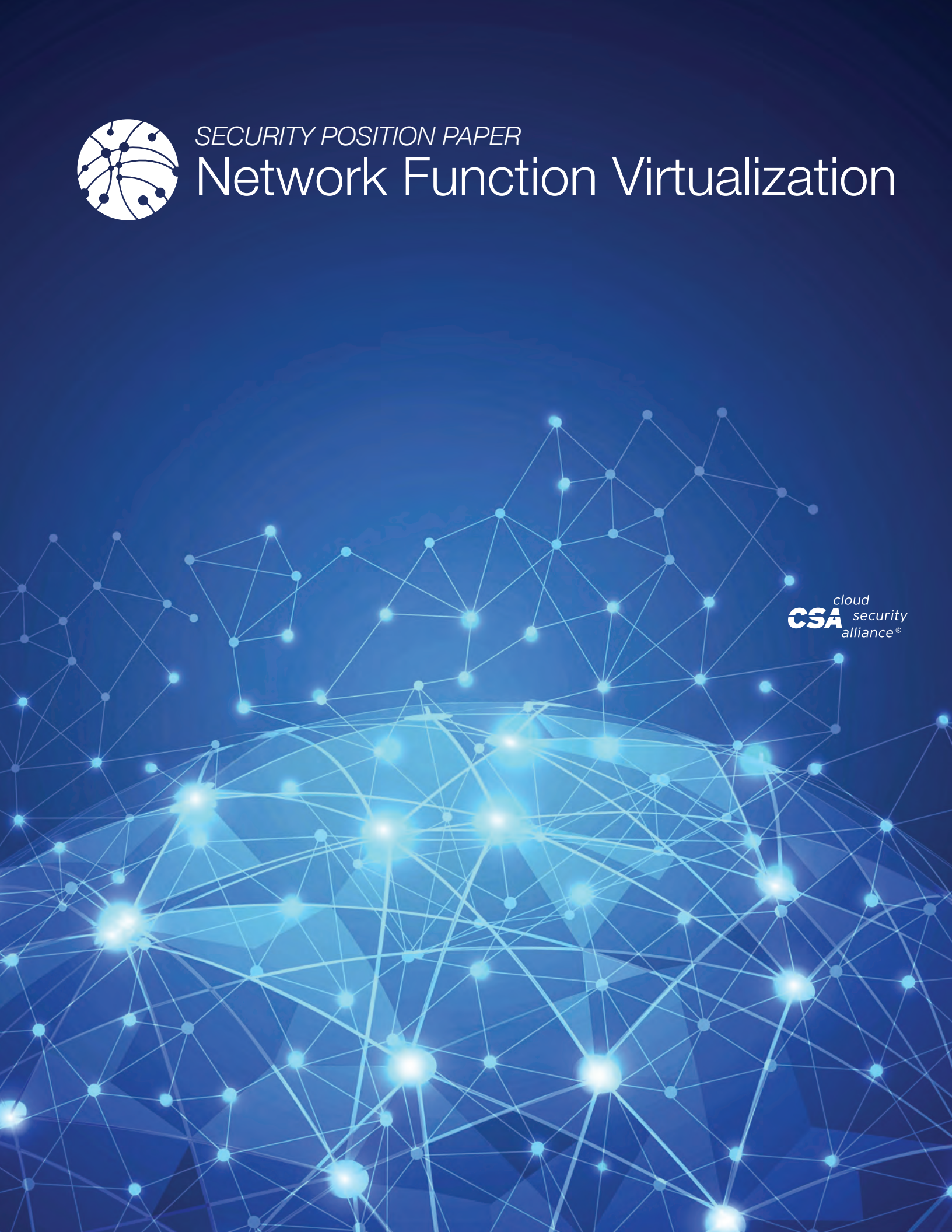


SECURITY POSITION PAPER

Network Function Virtualization

cloud security alliance®

© 2016 Cloud Security Alliance – All Rights Reserved

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Security Position Paper Network Function Virtualization" at https://cloudsecurityalliance.org/download/security-position-paper-network-function-virtualization/, subject to the following: (a) the Paper may be used solely for your personal, informational, non-commercial use; (b) the Paper may not be modified or altered in any way; (c) the Paper may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Paper as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance "Security Position Paper Network Function Virtualization".

ACKNOWLEDGMENTS

CO-CHAIRS
Kapil Raina
Saif Chaudhry

CONTRIBUTORS
Aleksandar Milenkoski
Bernd Jaeger
Kapil Raina
Mason Harris
Saif Chaudhry
Sivadon Chasiri
Veronica David
Wenmao Liu

CSA GLOBAL STAFF
Victor Chin, Research Analyst

©2016 Cloud Security Alliance - All Rights Reserved.

TABLE OF CONTENTS

Acknowledgments 3

Table of Contents 4

Section 1. Introduction 5

Audience and Scope 6

Section 2. Network Function Virtualization and Software- Defined Networks 7

Section 2.1. Network Function Virtualization (NFV) 8

Section 2.2. NFV vs. Traditional Networking 9

Section 3. Security Issues and Concerns 10

Section 3.1. NFV Security Challenges 10

Section 3.2. NFV and SDN: Risks in the Cloud 12

Section 4. NFV Security Framework: Opportunities 13

Section 5. NFV Security Framework: Addressing Security Risk 14

Section 5.1. NFV Security Framework 15

Section 5.2 Securing NFV-based Environments 17

Section 5.2.1 Securing the NFV Security Framework 18

Section 5.2.2 Important Elements 19

Trust Management/Technical Platform(s) 22

Conclusion 23

References 24

Acronyms 25

Appendix 1-SDN: Risks, Comparison and Existing Literature 25

Software-Defined Networks Versus Traditional Networks 27

Software-Defined Network Reports 27

©2016 Cloud Security Alliance - All Rights Reserved.

SECTION 1.

INTRODUCTION

In the last five years, cloud infrastructures have evolved dramatically in capability and complexity. Security risks have risen at least as commensurately.

While virtualization, per se, is not new, the idea that now almost anyone can virtualize resources such as compute, storage, networking, and applications increases the impact and velocity of security threats. Furthermore, the global geopolitical landscape has shifted from cyber attacks driven by opportunity, to well-funded nation-state campaigns.

The Cloud Security Alliance (CSA) has observed this trend and believes it is an appropriate time to convene another forum of experts to help network and data center technologists understand how to secure virtual infrastructure.

Since virtualization covers a range of technologies, the CSA Virtualization Working Group has decided to divide its efforts among several key areas: compute, network, containers and storage. There are plans underway to produce research on containers and storage virtualization security. The working group has already defined guidelines for compute virtualization, since it is a mature technology. Network virtualization is still a relatively new landscape, and requires a precursor to delivering a risk model or a step-by-step practitioner's guide.

This white paper is that precursor. The paper discusses some of the potential security issues and concerns, and offers guidance for securing a Virtual Network Function (NFV) based architecture, whereby security services are provisioned in the form of Virtual Network Functions (VNFs). We refer to such an NFV-based architecture as the NFV Security Framework. This paper also references Software-Defined Networking (SDN) concepts, since SDN is a critical virtualization-enabling technology.

This white paper consists of 5 sections.

Section 1 provides a basic overview.

Section 2 introduces NFV concepts, and briefly discusses SDN.

Section 3 expounds on some of the security issues and concerns when introducing NFV into a cloud environment.

Section 4 explains the benefits and opportunities of an NFV Security Framework.

Section 5 expounds on the challenges and important elements of the NFV Security Framework.

[1] https://virtualizationreview.com/articles/2015/03/20/security-top-reason-for-cloud-hesitancy.aspx
[2] http://www.oracle.com/us/products/middleware/data-integration/ioug-di-for-cloud-survey-2596248.pdf
[3] "With cloud, these practices have become more complex. And they've shifted from leading practices to critical core disciplines. Integration stability and reliability was the number two challenge in a recent survey on cloud adoption, trailing only security concerns." - source: http://dupress.com/articles/2014-tech-trends-cloud-orchestration/
[4] https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf

cloud security alliance®

©2016 Cloud Security Alliance - All Rights Reserved.

AUDIENCE AND SCOPE

The audience for this white paper is virtualization, security, and network architects interested in deploying NFV infrastructure. By virtualizing network functions, cloud service providers (CSPs) can launch revenue-generating network services more quickly than ever before and with fewer hardware dependencies. Enterprises can benefit from reduced operational and capital expenditures.

Today's CSPs and enterprises must address unique and complex security considerations. CSPs and enterprises must consider how adopting NFV infrastructure will affect their risk profiles and how the dynamic aspects of NFV will impact their overall security frameworks. This white paper helps CSPs and enterprises better understand both of these considerations, at the same time also presents an approach that addresses technical and non-technical NFV security controls. While primarily written for a technical audience, this paper can also help business stakeholders understand these concepts.

This paper does not present deployment scenarios, detailed implementation blueprints, or mitigation techniques. In the future, the CSA Virtualization Working Group will release a detailed risk model and security risk mitigation guide as follow up to this paper.

SECTION 2.

NETWORK FUNCTION VIRTUALIZATION AND SOFTWARE- DEFINED NETWORKS

Software defined networks (SDN) allow dynamic changes of network configuration that can alter network function characteristics and behaviors. For example, SDN can render real-time topological changes of a network path. Although NFV and SDN can each be used on their own, an SDN-enabled network provides a platform on which to implement a dynamic chain of virtualized network services that make up an end-to-end network service (see Figure 1).

Figure 1 - End-to-end network service example using SDN to dynamically chain VNFs

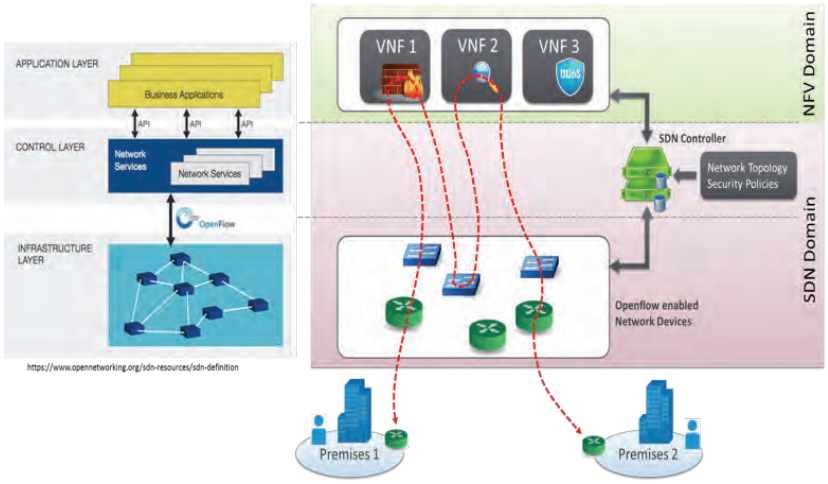


Figure 1 maps the Open Networking Foundation (ONF) SDN architecture on the left to an use-case example on the right. Here, an enterprise has established a secure connection between Premises 1 and Premises 2. The SDN-enabled network is shown as a red dotted line. Under non-SDN circumstances, this path traverses a fixed high-bandwidth virtual network firewall service (VNF 1) provided by a network provider. This is severely limiting in the face of a security incident that demands a nimble response (e.g., responding to an intrusion, or discovery of a zero day vulnerability of a software product). With SDN, an additional virtual security function, VNF 2 (e.g., IPS or malware filter) can be logically inserted into the network path – on demand.

Since a large body of work has already been written on SDN this document focuses on NFV. For more on SDN, refer to Appendix 1 - SDN: Risks, Comparison and Existing Literature.

[5] https://www.opennetworking.org/sdn-resources/sdn-definition

©2016 Cloud Security Alliance - All Rights Reserved.

SECTION 2.1.

NETWORK FUNCTION VIRTUALIZATION (NFV)

NFV represents a decoupling of the software implementation of network functions from the underlying hardware by leveraging virtualization techniques. NFV offers a variety of network functions and elements, including routing, content delivery networks, network address translation, virtual private networks (VPNs), load balancing, intrusion detection and prevention systems (IDPS), and firewalls. Multiple network functions can be consolidated into the same hardware or server. NFV allows network operators and users to provision and execute on-demand network functions on commodity hardware or CSP platforms.

NFV does not depend on SDN (and vice-versa) and can be implemented without it. However, SDN can improve performance and enable a rich feature set known as Dynamic Virtual Network Function Service Chaining (or VNF Service Chaining). This capability simplifies and accelerates deployment of NFV-based network functions.

cloud security alliance®

©2016 Cloud Security Alliance - All Rights Reserved.

SECTION 2.2.

NFV VS. TRADITIONAL NETWORKING

Traditionally, network functions are tied to proprietary hardware deployed as network appliances. As network appliances proliferate, deploying new network services and applications becomes increasingly difficult and costly. Provisioning is inefficient when constantly accommodating fluctuating traffic and changing requirements. In contrast, NFV decouples network functions from underlying hardware and platforms, and allows them to be provisioned on demand. Deploying new network services and applications is quick and easy with NFV.

cloud security alliance®

©2016 Cloud Security Alliance - All Rights Reserved.

SECURITY ISSUES AND CONCERNS

SECTION 3.1. NFV SECURITY CHALLENGES

NFV divides the network into components that can run on off-the-shelf systems (e.g., x86). Securing these components requires embedded security. Because network components are virtualized, NFV networks contain a level of abstraction that does not appear in traditional networks. There is complexity around the hypervisor, related controls and protocols, as well as in the boundaries between the virtual and physical networks.

Securing this environment is challenging for at least the following reasons:

1. **Hypervisor dependencies:** Today, only a few hypervisor vendors dominate the marketplace, with many vendors hoping to become market players. Like their operating system vendor counterparts, these vendors must address security vulnerabilities in their code. Diligent patching is critical. These vendors must also understand the underlying architecture, e.g., how packets flow within the network fabric, various types of encryption and so forth.

2. **Elastic network boundaries:** In NFV, the network fabric accommodates multiple functions. Placement of physical controls are limited by location and cable length. These boundaries are blurred or non-existent in NFV architecture, which complicates security matters due to the unclear boundaries. VLANs are not traditionally considered secure, so physical segregation may still be required for some purposes.

3. **Dynamic workloads:** NFV's appeal is in its agility and dynamic capabilities. Traditional security models are static and unable to evolve as network topology changes in response to demand. Inserting security services into NFV often involves relying on an overlay model that does not easily coexist across vendor boundaries.

4. **Service insertion:** NFV promises elastic, transparent networks since the fabric intelligently routes packets that meet configurable criteria. Traditional security controls are deployed logically and physically inline. With NFV, there is often no simple insertion point for security services that are not already layered into the hypervisor.

5. **Stateful versus stateless inspection:** Today's networks require redundancy at a system level and along a network path. This path redundancy cause asymmetric flows that pose challenges for stateful devices that need to see every packet in order to provide access controls. Security operations during the last decade have been based on the premise that stateful inspection is more advanced and superior to stateless access controls. NFV may add complexity where security controls cannot deal with the asymmetries created by multiple, redundant network paths and devices.

6. **Scalability of available resources:** As earlier noted, NFV's appeal lies in its ability to do more with less data center rack space, power, and cooling.

©2016 Cloud Security Alliance - All Rights Reserved.

Dedicating cores to workloads and network resources enables resource consolidation. Deeper inspection technologies—next-generation firewalls and Transport Layer Security (TLS) decryption, for example—are resource intensive and do not always scale without offload capability. Security controls must be pervasive to be effective, and they often require significant compute resources.

Together, SDN and NFV create additional complexity and challenges for security controls. It is not uncommon to couple an SDN model with some method of centralized control to deploy network services in the virtual layer. This approach leverages both SDN and NFV as part of the current trend toward data center consolidation.

©2016 Cloud Security Alliance - All Rights Reserved.

NFV AND SDN: RISKS IN THE CLOUD

Introducing NFV and SDN into the cloud environment is challenging for the following reasons:

1. **NFV and hypervisor compatibility:** Although not purely a security issue, porting a physical appliance to a virtual appliance is challenging for two reasons. First, appliances such as firewalls and intrusion prevention systems use custom drivers and kernels. If they are deployed on the general infrastructure-as-a-service (IaaS) hypervisors of compute nodes, they will likely not function. Second, some IaaS systems provide custom hypervisor application program interfaces (APIs) for traffic steering. This may mean that NFV providers must do significant work to make their virtual appliances compatible.

2. **System availability:** Although virtual security appliances offer great convenience to the cloud, there may be trade-offs among physical and virtual NFV functions. Even when an NFV appliance is optimized for a corresponding hypervisor, its performance may still not match up to that of a physical appliance.

3. **SDN architecture:** SDN is centralized, while cloud computing is elastic and distributed by nature. The combination of the centralized SDN implementation, its requisite support for the elastic and distributed nature of the cloud, and multi-tenancy in the cloud environment can lead to complications and incoherences.

4. **SDN implementation:** SDN architecture includes application, controllers, switches and management systems. All have vulnerabilities that can be used by adversaries to gain unauthorized access to or intercept and manipulate traffic. For example, many current white-box (commodity) switches run on Linux. Some are pre-configured for cleartext shell access with default credentials. Others use outdated and vulnerable SSL implementations. These put the entire SDN system at risk.

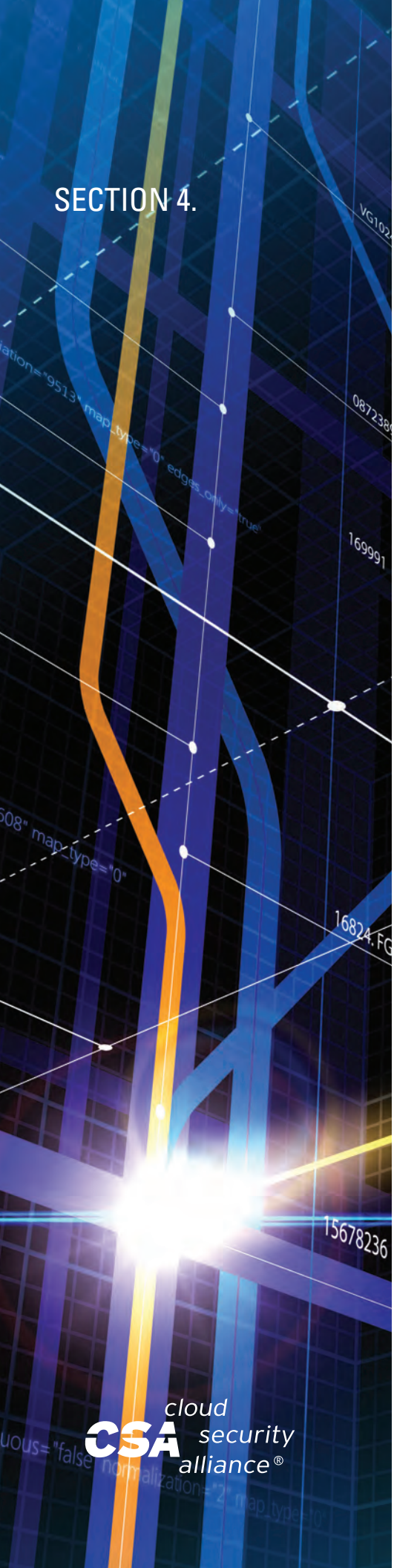
   The introduction of virtual network functions (VNFs) can increase the attack surface. A security breach in these applications may enable an attacker to bypass isolation mechanisms and compromise the overall network or perform unauthorized actions on other networks.

   In some cloud architectures, the data network may be shared with a management or control network. This shared architecture may lead to a compromise of the SDN or the Infrastructure-as-a-service (IaaS) control nodes. A successful intruder can manipulate underlying routes to bypass NFV security devices.

5. **Policy consistency:** If the SDN controller lacks a mechanism to check for consistent policies, a malicious user may construct multiple policies (e.g., network address translation rules with OpenFlow), that transform malicious flows, forbidden by access control-linked NFV devices, into "normal" traffic. Porras et al. (2015) describes such issues.

6. **Compatibility with IaaS:** IaaS network virtualization modules are responsible for isolating tenant resources such as network traffic,. However, if an independent SDN controller without IaaS awareness is introduced to manage traffic on virtual switches, resource isolation is violated because the SDN controller does not know how to map tenant traffic. For example, if a Cloud Service Provider wants to interconnect cloud networks operating on different platforms, the SDN controller needs to be aware of the networks components involved.

©2016 Cloud Security Alliance - All Rights Reserved.



NFV SECURITY FRAMEWORK: OPPORTUNITIES

Using the NFV Security Framework —that is, deploying the network security functions we consider VNFs—offers multiple benefits when compared to deploying them as hardware network appliances. Some of the primary benefits include:

- **Reduced deployment and management resources:** Many of traditional network security functions are performed by expensive, hard-to-manage hardware network appliances. With NFV, it is easy to deploy and manage these functions as virtualized software on commodity hardware, significantly reducing cost and effort. In addition, leveraging SDN technology to manage traffic destined for or originating from VNFs further reduces cost and effort (see Figure 2a).

- **Flexibility:** The NFV Security Framework increases flexibility when compared to conventional network security infrastructure:

  - **On-demand deployment and scalability:** NFV allows on-demand deployment and scaling of security function capabilities that are part of the NFV Security Framework. For instance, provided that VNFs featuring intrusion detection and prevention are deployed in VMs, they can be migrated to improve traffic analysis at an egress point, for example. Alternatively, if VMs are already in place, they can be cloned to scale traffic analysis significantly.

  - **Dynamic threat response:** The NFV Security Framework offers dynamic, real-time response to threats.. This can be particularly effective when it is used in conjunction with SDN. For example, SDN can be used to rearrange service chains to optimize performance and efficacy of VNFs.

  - **Global and real-time view:** With its centralized architecture, the SDN controller offers a real-time, global network view, including topology, routes, and traffic statistics. This capability is useful for responding to DDoS attacks and detecting network anomalies.

  - **Flexible response:** A security service provider can quickly provision a large number of firewalls when online business bursts—Black Friday (a big ecommerce shopping day in the U.S.), for example. During the rest of the year, the provider can save resources by maintaining a minimum number of security appliances.

  - **NFV and SDN enabling software-defined security:** Together, SDN and NFV offer a fast and scalable approach to building on-demand security solutions. The NFV control plane can quickly provision different types of virtual security appliances, while the SDN controller can steer, intercept, or mirror the desired traffic for security inspection, thereby creating a security service chain. Security resources and traffic control are both determined by a northbound security application, making the solution flexible and fast.

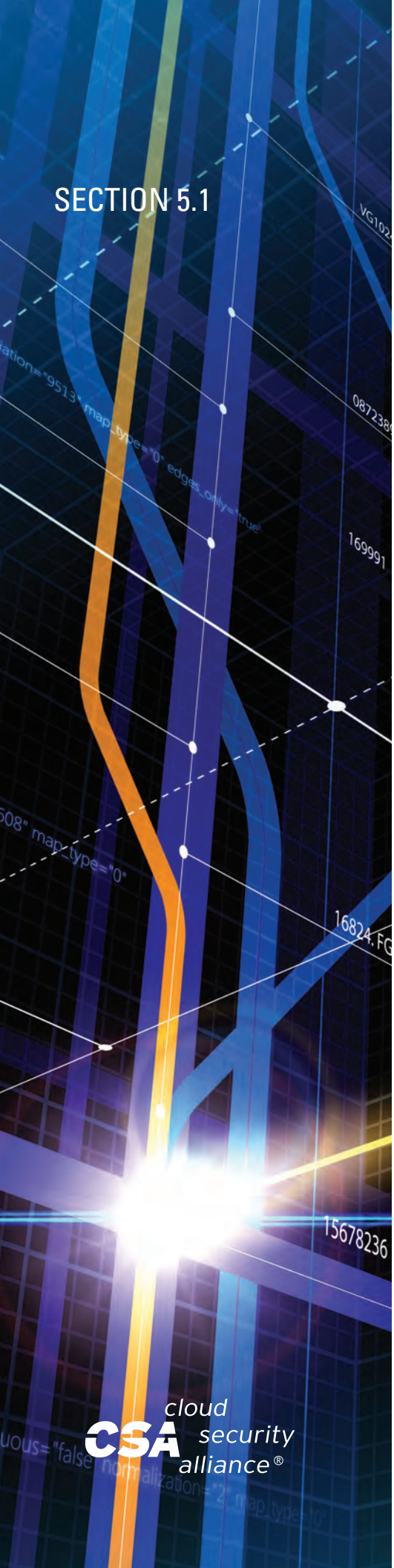
Despite these benefits, using the NFV Security Framework creates security challenges, which are relevant when virtualizing network functions in general.

©2016 Cloud Security Alliance - All Rights Reserved.

NFV SECURITY FRAMEWORK: ADDRESSING SECURITY RISK

In order to better understand how to address NFV security challenges, Section 5.1 describes a preliminary framework—the NFV Security Framework—and the benefits it delivers when securing and hardening an infrastructure Section 5.2 presents the security challenges created by using NFV for security- and non-security purposes, and also discusses important elements for securing such an architecture.

©2016 Cloud Security Alliance - All Rights Reserved.



NFV SECURITY FRAMEWORK

As mentioned earlier, the adoption of virtualization technology has encouraged the deployment of a variety of network security functions—intrusion detection and prevention (IDPS), access control, and identity management, for example—running on virtual machines (VMs) or in Linux containers. The architecture of the preliminary NFV Security Framework focuses on the functions most commonly seen in production infrastructures:

- **Intrusion detection and prevention.** Network IDPS solutions characterized according to various properties. Examples include solutions that analyze traffic using deep packet inspection and those that use shallow (stateful) packet inspection.

- **Access control.** Systems that evaluate network traffic against access control policies. Examples include conventional firewalls performing stateful packet inspection and next-generation firewalls performing deeper, context-related traffic analysis.

- **Malware protection.** Conventional anti-virus or anti-spyware systems. This category includes systems that detect the spread malicious software (e.g., viruses, spyware) at ingress and egress points, and block transit or storage of infected files.

- **Denial-of-service (DoS) protection.** Systems deployed and/or configured specifically for detecting and defending against DoS attacks, in particular against non-distributed DoS attacks targeting network protocol or application design flaws. This protection primarily includes DoS defense systems, many of which perform traffic analysis and enforce access control and flow policies. It also includes, for example, switches or routers with traffic rate-limiting capabilities.

- **Cryptography:** Systems that provide cryptographic services to ensure the confidentiality and integrity of data in transit and at rest. This category includes systems that provide cryptographic services at layers 2, 3, and 4 of the Open Systems Interconnection (OSI) reference model. Cryptographic services are normally deployed as specialized hardware appliances primarily for performance reasons and for key storage. The deployment of cryptographic services as VNFs is a challenge that calls for novel approaches. Organizations may need to determine whether speed (i.e. no encryption, imperfect encryption, smaller key sizes, etc) or confidentiality (i.e. forward-secrecy, larger key sizes, stronger algorithms, etc) is more important to focus on. This decision should be made in accordance with pre-determined classification of the data (sensitive, top secret, etc.) to be transmitted or stored.

- **Identity and access management.** Systems that enable managing and enforcing authentication, authorization, and audit policies, such as single sign-on. This applies to both users and systems (APIs).

©2016 Cloud Security Alliance - All Rights Reserved.

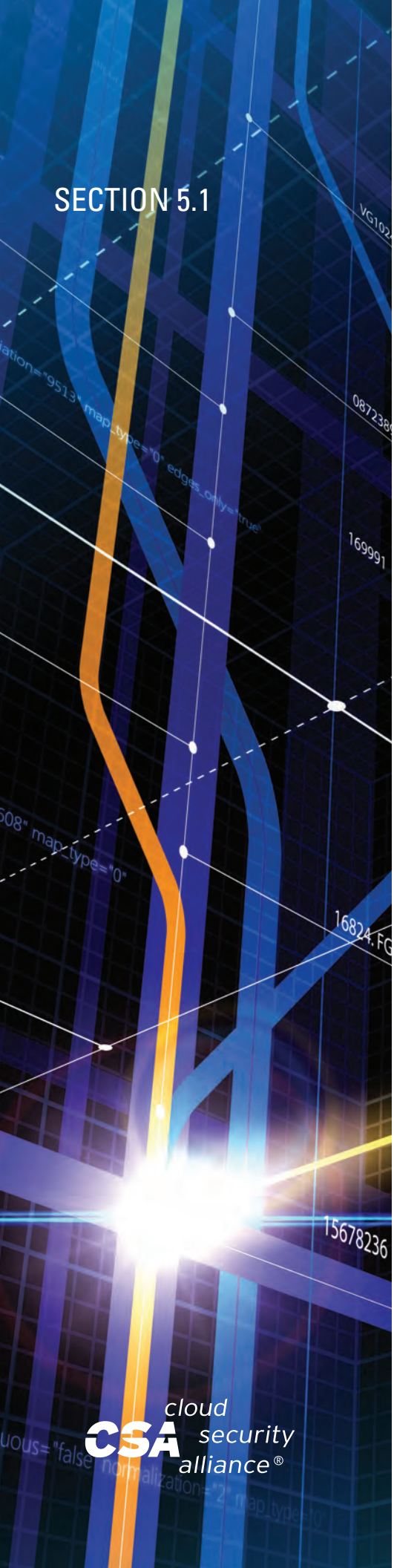


Figure 2a. Example Deployment Scenario of the NFV Security Framework

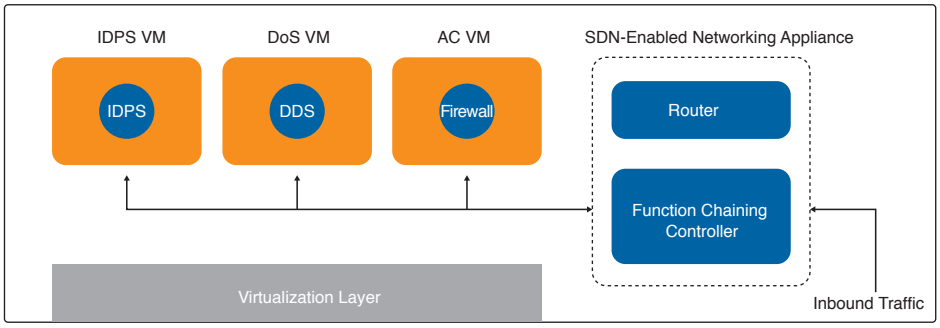
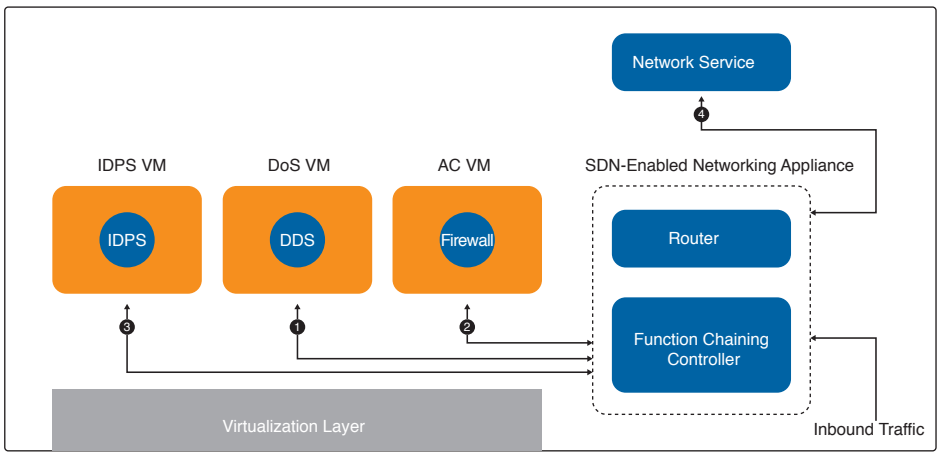


Figure 2b. Virtual Network Function Chaining in a DDoS flooding Attack



Deploying the security functions via VNFs assumes that virtualized software systems are available to perform the VNF operations. Figure 2a depicts a sample deployment of the NFV Security Framework, where systems that perform intrusion detection and prevention (IDP), data distribution service (DDS), and firewall—are deployed in virtual machines. In this scenario, inbound traffic is managed by an SDN-enabled network appliance, which directs flows to the deployed VNFs as configured by a network administrator. Inbound traffic is first directed to the firewall, then to the DDS and so on. We refer to this activity as network function chaining. The networking appliance depicted in Figure 2a performs network function chaining through its components, which have routing and function chaining capabilities.

To illustrate the benefits of using SDN in conjunction with the NFV Security Framework, we present an example scenario in Figure 2b. In the case of a distributed denial-of-service (DDoS) attack targeted at a network service, an SDN-enabled networking appliance can be reconfigured using orchestration functions such that inbound traffic destined for the network service is first directed to the DDS at point 1. The traffic is then directed to the firewall and the IDPS at points 2 and 3, and finally to its destination at point 4. The goal is achieving optimal efficacy of the deployed VNFs by filtering out malicious DDoS traffic before it reaches the firewall, the IDPS, and the targeted network service.

©2016 Cloud Security Alliance - All Rights Reserved.

SECTION 5.2

SECURING NFV-BASED ENVIRONMENTS

The simplified NFV architecture in Figure 2 shows the main components, their interfaces, and how they interact with and depend on each other.

Figure 3. Simplified NFV Architecture

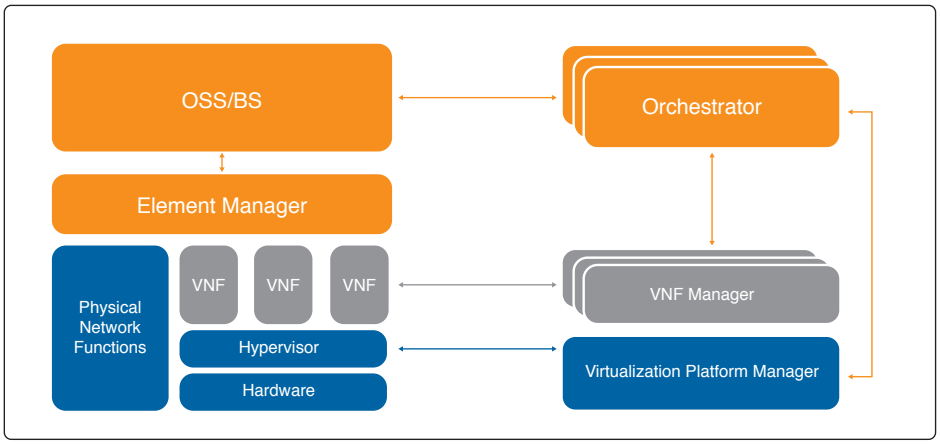


Figure 3 presents a static view of the technical aspects of an NFV infrastructure and the elements that must be secured. The successful deployment and operation of such a complex end-to-end network service model that uses SDN to dynamically chain several VNFs into the network path requires that dynamic aspects of NFV, as well as organizational and process challenges, be addressed. Section 5.2.2 discusses important elements that must be taken into account when securing the NFV Security Framework.

©2016 Cloud Security Alliance - All Rights Reserved.

SECTION 5.2.1

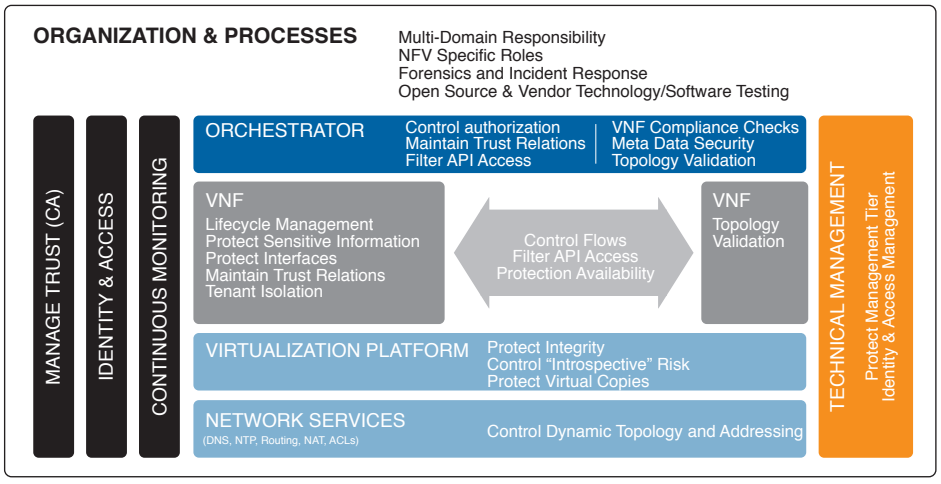
SECURING THE NFV SECURITY FRAMEWORK

The NFV Security Framework comprises the technical layer of a VNF environment, including core elements such as the VNFs, their management systems, and elements on which a VNF depends. These elements include the virtualization platform or general network service functions, which may also be virtualized.

The framework also considers non-technical aspects such as lifecycle management for NFV components, and the impact of a dynamically changing network for security monitoring and incident response purposes.

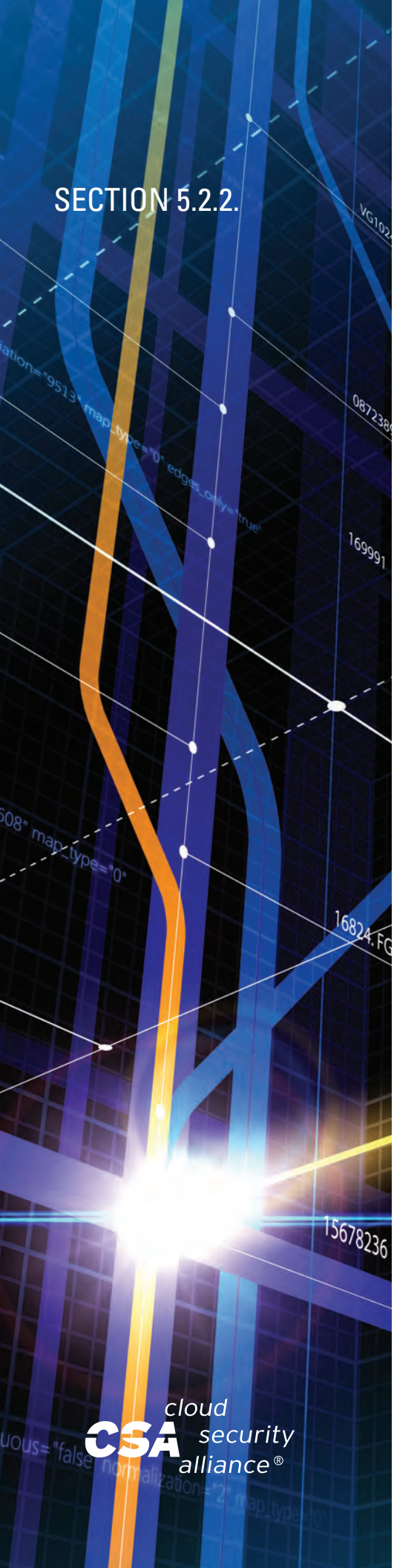
Figure 4 is a high-level view of framework elements that are discussed in the next section.

Figure 4. High-Level View of NFV Security Framework Elements



The framework's technical aspects and controls are embedded in organizational structures and processes that contain elements not found in traditional network operations. For example, the design, build, and operation of a VNF crosses network, hypervisor, compute, storage, SDN, and multiple management and orchestration domains, while in the past network teams dealt with only "their" systems and likely did not consider integrating their routers into the anti-virus protection process. They may not have thought about cloned network device certificates until their hardware appliances had become virtual machines or their customer premises equipment virtual function within the core network.

©2016 Cloud Security Alliance - All Rights Reserved.



IMPORTANT ELEMENTS

Following is a comprehensive list of the primary elements of a security framework, focusing on specific NFV requirements:

ORGANIZATION AND PROCESSES

- **Multi-domain responsibilities and new processes:** Building and operating virtualized networks includes many administrative domains and may require NFV- specific roles and the need for fine-grained controls that separate not only role but also function and scope. Life-cycle management, security monitoring, incident response and forensics, lawful interception, and other processes must be adapted to work in a more dynamic environment with fast-changing network topology, data flow paths, and network addresses.
- **Paradigm shift:** A part of the traditional network will become non-physical and will thus lose its natural defense against threats such as malware. The NFV security framework needs to be amended with additional processes to address this change.

VNF SECURITY LIFE-CYCLE

- **Creation and deployment:** Before a VNF is deployed, the orchestration or management system should verify compliance with its build-configuration standards. A check can include but is not limited to:

  - Security of the configuration
  - Whether the package contains only trusted and expected components
  - Whether trusted components have been altered (integrity)

  Because deploying a virtual router is much easier than a physical network device, controls should be put in place at the orchestration layer to avoid VNF sprawl, unintended topology, and network flow path changes.

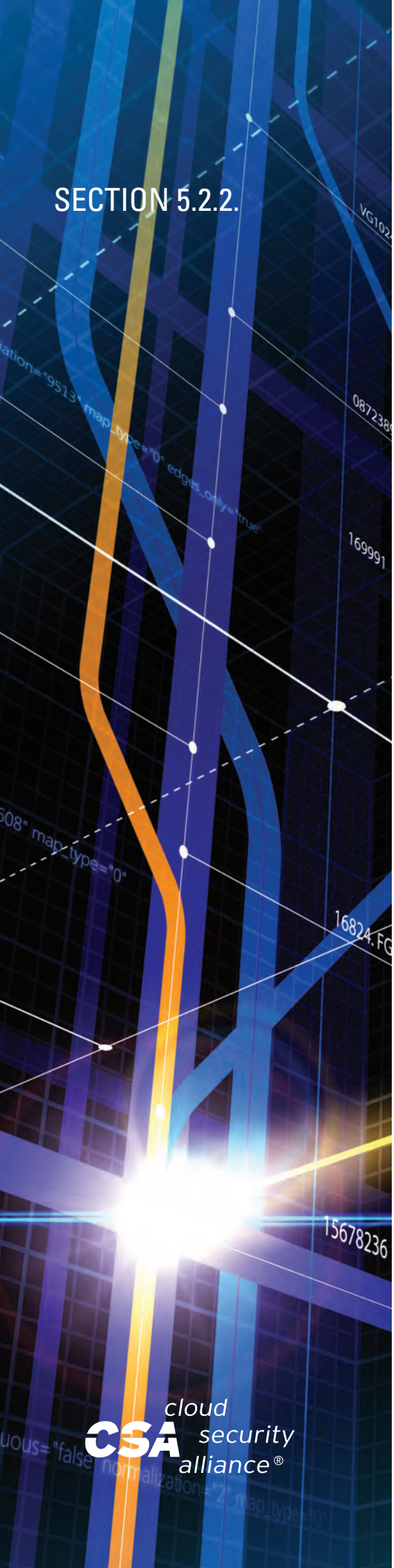
- **Cloning and moving/migrating virtual devices:** Virtual network devices can easily be cloned and instantiated. As a result, a security framework must address the following elements:

  - Depending on the migration technique, certificates, accounts, media access control addresses, or hardware IDs will look identical after cloning. Depending on the situation— "I need a second device 'B' with a similar configuration as 'A' but not the same certificate, or 'A' will be moved but should keep its identity" — this may not be desirable. If certificates are based on those attributes, the orchestration layer may inject and correct them if and when required.

  - Trusted platform modules (e.g., Intel's Trusted Execution Technology, or TXT) may be required to ensure that virtual devices can provide attestation or a true status of the security of the underlying hardware and physical location.

- **Dynamic state management.** Security framework requirements are quite similar to the cloud compute layer one. Virtual network components can change their state from hibernation, sleep, resumption, abort, restore, power-on, and power-off dynamically. An outdated or a poorly configured or tempered device that suddenly "re-spawns" in a network can easily compromise security. Thus, the orchestration layer should conduct similar compliance checks as for a first-time deployment. Sources and targets should be verified for integrity.

©2016 Cloud Security Alliance - All Rights Reserved.



- Snapshots, backups, and deletions (virtual secure decommissioning). Virtual network devices contain the same sensitive information as their physical counterparts. Examples include device certificates, VPN and encryption keys, admin accounts, and API keys. While secure wiping of a physical network device and secure handling of device configuration backups are standard, virtualization adds new requirements to an NFV security framework:

    - Snapshots will copy device RAM content into a file and backups may be stored at different locations. Content may include decrypted data and must be protected during transport and rest.

    - Clones of VMs may also be need to be considered, because they may be legitimate when deploying (i.e., based on a master image), or counterfeit, as when a malicious insider or hacker attempts to steal them or insert a corrupted system.

    - Device instances deleted at the orchestration layer may exist on the host's file system for some time and thus be recoverable.

    - A virtual router is easier to delete than a physical one, which may increase the risk of accidental or intentional DoS attacks.

The security framework elements addressed in this section are party technical and partly organizational. Any stored file—clones, data, or snapshots, for example—can be protected at the virtualization layer with encryption. If encryption is not an option, processes must be put in place to securely manage backups or VNF files.

MANAGING STATIC AND DYNAMIC TOPOLOGY

- **Visibility of virtual components and their management systems:** Technical and non-technical measures must be put in place to control access. These measures can include:

    - Role-based access controls (separation of duties, least privilege, workflow escalation)
    - Security architecture that describes interfaces, flows, and protection (filter) functions
    - Hypervisor isolation functions
    - Controlled, (i.e., wrapper, proxy) multi-tenant aware access to virtualization layer details that ensures side-channel and related security risks do not exist

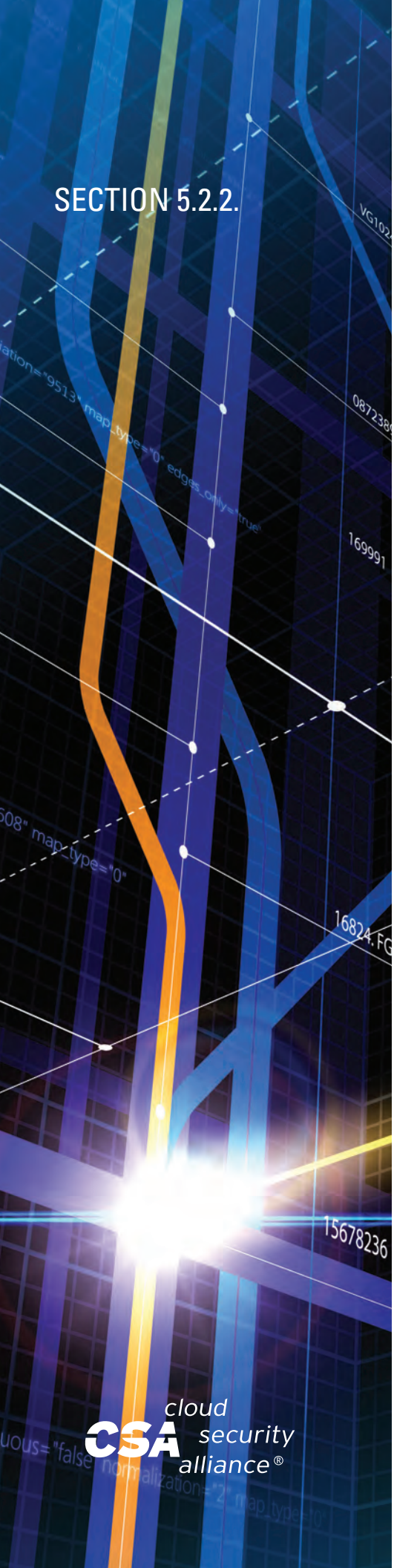
- **Topology validation:** An advantage of using SDN is the ability to dynamically reconfigure the network path to include an additional VNF security function in service chaining. This ability introduces the threat of unwanted topology changes resulting in loss of communication or unintended, direct traffic flow that circumvents filters or access controls. Thus, topology validation should be enforced at the orchestration layer and at a VNF level. Note that VNFs should check their new peer entity and determine whether or not to trust the validation.

LOGGING, MONITORING, SECURITY INFORMATION AND EVENT MANAGEMENT, AND CONFIGURATION MANAGEMENT

Given the dynamic nature of virtualized networks, it is important to consider the following:

- To identify anomalies in a complex NFV environment, security information from all layers must be collected and correlated to create strong audit trails

©2016 Cloud Security Alliance - All Rights Reserved.



for forensic and compliance assessments.

- Modern security information and event management and the intrusion analyst mindset is likely still influenced by static network. In NFV, IP addresses can change fast and creating a hard copy listing, as is the practice with static networks, may no longer be feasible. New metrics and analytics may be required. As presented in the section below titled "Cloning and moving/migrating virtual devices", the new virtual resources can dynamically or programmatically be created or cloned. These new resources and their associated security policies must be discoverable by the auditing mechanisms in order to generate appropriate audit trails. This could need some interactions between orchestration and lifecycle management components and the auditing framework.

- The end-to-end network path for a particular traffic flow or network route makes packet capture or inspection more difficult. This challenge should be addressed using topology validation and enforcement as noted in the earlier section titled "Managing static and dynamic topology."

- Forensic processes will likely need adaptation. While the acquisition of a forensic image may become easier—as compared to physically collecting a device—timeline and network log analysis may require changes in techniques, and analysts will need access to more systems and logs for a complete forensic picture. In addition, it will be critical to obtain complete and unaltered administrator audit logs to determine if threats were created by an administrator (e.g., insider threat), or if procedures were not followed (e.g., failure to log out of a session), or if the administrator's account was compromised (e.g., through botnet, malware, etc.).

- To ensure real-time physical and virtual system compliance, continuous monitoring should be considered.

- Implement the two-person rule—sometimes also called the "four-eyes principle" —to enforce dual authority on important tasks or sensitive actions, such as deleting virtual objects.

©2016 Cloud Security Alliance - All Rights Reserved.

TRUST MANAGEMENT

As earlier noted, trust management is a crucial security control in any dynamic network. The following bi-directional trust relations are particularly relevant in the NFV Security Framework:

- VNF to VNF
- VNF to external entities (i.e. DNS, NTP, routing)
- VNF to VNF-Manager
- VNF to Element Management System (EMS)
- VNF Manager to VNF Orchestrator and VNF Infrastructure Manager

It is important to put end-to-end trust management in place in the orchestration and management domain. Trust can be established based on hardware and software elements such as the status of the trusted compute base (e.g., Trust Platform Module or TPM) or secure boot and package source and/or integrity. Digital certificates can be used for security validation.

TECHNICAL PLATFORM(S)

Last, but hardly least, platform security should be determined based on the technical platform on which it runs. Critical aspects include:

- **Virtualization platform security.** This platform protects the hypervisor, the management domain, and APIs.
- **NFV identity and access management.** This system should be able to manage VNF accounts and credentials regardless of whether they are newly instantiated, hibernated, or retired. The system should also be able to manage privileged access including roles and entities that allow "Introspection" and provide extensive logs of any activities within these components.

©2016 Cloud Security Alliance - All Rights Reserved.

CONCLUSION

NFV and SDN technologies hold great promise for transforming the modern network. This white paper has established a basic framework for security awareness in this context. Future deliverables from the CSA Virtualization Working Group will offer further, practical steps that NFV/SDN technologists can leverage to simplify the process of securing their infrastructures.

[7] Element Management Systems perform the typical management functionality for one or several VNFs (ETSI, 2013)

©2016 Cloud Security Alliance - All Rights Reserved.

REFERENCES

1. Keith Ward. (2015). Survey: Security is Top Reason for Cloud Hesitancy. Virtualization Review. Retrieved: https://virtualizationreview.com/articles/2015/03/20/security-top-reason-for-cloud-hesitancy.aspx

2. Joseph McKendrick. (2015). Data Integration for Cloud Survey. Independent Oracle Users Group. Retrieved: http://www.oracle.com/us/products/middleware/data-integration/ioug-di-for-cloud-survey-2596248.pdf

3. Andy Main and John Peto. (2014). Tech Trends 2014, Cloud Orchestration. Deloitte University Press. Retrieved: http://dupress.com/articles/2014-tech-trends-cloud-orchestration/

4. Mario Maawad Marcos et al. (2015). How Cloud is Being Used in the Financial Sector: Survey Report. Cloud Security Alliance. Retrieved: https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf

5. Open Networking Foundation. Software-Defined Networking (SDN) Definition. Retrieved: https://www.opennetworking.org/sdn-resources/sdn-definition

6. P. Porras, S. Cheung, M. Fong, K. Skinner, and V. Yegneswaran. (2015). Securing the Software-Defined Network Control Layer. Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS).

7. European Telecommunications Standards Institute (ETSI). (2013). ETSI GS NFV 002 V1.1.1 - Network Functions Virtualization (NFV); Architectural Framework

8. McBride, M. C. (2013). SDN Security Considerations in the Data Center. Open Networking Foundation. ONF SOLUTION BRIEF.

9. Kreutz, D., Ramos, F. M., & Verissimo, P. (2013). Towards Secure and Dependable Software-Defined Networks. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 55-60). ACM.

10. Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2013). SDN security: A survey. Future Networks and Services (SDN4FNS), 2013 IEEE SDN for (pp. 1-7). IEEE.

11. European Telecommunications Standards Institute (ETSI). (2014). ETSI GS NFV-SEC 003 V1.1.1 - Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance.

cloud CSA security alliance®

©2016 Cloud Security Alliance - All Rights Reserved.

ACRONYMS

CM	Continuous Monitoring
CPE	Customer Premises Equipment
CSP	Cloud Service Provider
EMS	Element Management System
IAM	Identity and Access Management
IR	Incident Response
SIEM	Security Information and Event Management
OSS	Operations Support Systems
BSS	Business Support Systems
MSS	Managed Security Service

©2016 Cloud Security Alliance - All Rights Reserved.

APPENDIX

Appendix 1-SDN: Risks, Comparison and Existing Literature

1. SDN controller dependencies: In nearly every form of SDN, there is a model based on the use of APIs for north- and southbound communications to objects. These objects are then deployed as needed by the service contracts in place. This model emphasizes trust on the controller, because bi-directional communication is critical to the management of the objects. Security controls must account for separation of duties and provide fine-grained access control—to uphold the principle of least-access privilege on the control plane—to the control and data planes. In traditional physical networks, these planes are separated through the use of management networks and other entities. The SDN model has different boundaries than traditional physical networks, given the nature of access required by the controller. This vector represents a threat to the environment.

2. API security and best practices: APIs, by their nature, are open and extensible to encourage communication between entities. The number of API programmatic language options today is staggering. Security controls depend on the underlying API library to allow the API to perform its duties securely. Many of these libraries have had their own security challenges, leading one to conclude that underlying API structure influences the ability to secure it. This is a challenge for security operations. The API endpoint and its services represent an attack vector into the entire back-end environment. Therefore, appropriate controls should be applied to protect the API endpoint from incoming attack, from launching outgoing attacks (if compromised), and controls should prevent the API endpoint from allowing further access into the network (in the simplest form, via a DMZ).

3. Evolving standards: The pace of development and NFV/SDN evolution present an incredible challenge because they are outpacing the ability to fully understand security issues and provide effective controls. Furthermore, the lack of consistent standards among SDN implementations can create further gaps in security.

©2016 Cloud Security Alliance - All Rights Reserved.

Software-Defined Networks Versus Traditional Networks

Installing and configuring a traditional network requires skilled technicians. Tightly integrating the control and data planes of a network node makes it difficult for operators to scale the network dynamically.

With the ability to separate the control and data planes as well as programmability and centralized control, SDN network operators can manage packet flows, while gaining visibility into the network. This enables them to adjust network configuration to meet changing traffic demands and ultimately to improve overall network performance.

Software-Defined Network Reports

The Open Networking Foundation, which guides SDN standardization, published SDN Security Considerations in the Data Center (McBride, 2013) . The report notes that existing security solutions, such as firewalls and IDPS, are difficult to deploy, manage, program, and secure in the cloud, because policies are tightly coupled with physical resources. In addition, vendor-specific network components can limit the capabilities of security solutions. The report presents the benefits of OpenFlow-based SDN and its ability to address the security challenges of these environments.

In 2013, Kreutz, Ramos, and Verissimo revealed threat vectors caused by network programmability and control logic centralization. Network programmability can allow bugs and malicious code to attack network traffic and components, while software or users can disrupt centralized control. Major SDN-specific security attacks target control plane communications and SDN controllers. The lack of mechanisms to create trust among SDN controllers and management applications make it possible to easily deploy harmful applications.

Scott-Hayward et al. (Scott-Hayward, O'Callaghan, & Sezer, 2013) have presented the results of a survey of SDN security issues. They group these issues into six classes: unauthorized access, data leakage, data modification, malicious applications, denial of service, and configuration-related issues.

In contrast, NFV is an emerging technology; security issues and challenges have not been well studied. Recently, though, the European Telecommunications Standards Institute, which leads NFV standardization, published a report listing NFV threat vectors and providing security and trust guidance [European Telecommunications Standards Institute (ETSI), 2014] .

©2016 Cloud Security Alliance - All Rights Reserved.