IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

# Moving Toward Seamless Security

*November 2016*

Adapted from *Worldwide Virtual Firewall/UTM Security Forecast, 2016–2020* by Elizabeth Corr, Robert Ayoub, et al., IDC #US41219416

Sponsored by Check Point

*Security at the perimeter is no longer adequate for today's networks. Most modern unified threat management (UTM)/firewall solutions provide a breadth of security functions, but if the solutions don't provide complete visibility into all network traffic, attacks are still likely to get through. Virtualized infrastructures in particular have been a blind spot for security because traffic between virtual machines (VMs) is not easily monitored. This paper examines the need for virtual security gateways that can apply advanced security functionality to all virtual infrastructures. It also looks at the role Check Point's vSEC product can play in protecting the wide range of virtual and cloud platforms on the market today.*

## Introduction

The move to virtualized infrastructures has been a significant part of the digital transformation for many enterprises. Whether enterprises are adopting virtualized servers to improve computing density or moving workloads to public or private clouds, virtualized environments play an important part in the porting of applications and data into repositories that allow easy access for end users.

Enterprises moving toward digital transformation aggressively look to take advantage of the hybrid cloud, leverage both public and private clouds to optimize the organization's resources, and speed time to market. To improve their business agility and operational flexibility, enterprises want the ability to migrate applications between clouds, attaining cost savings and tapping unique platform capabilities in the process.

Today, the physical devices on the network are usually well protected. Administrators are accustomed to implementing patches as well as managing and monitoring physical devices on a regular basis. On the other hand, virtual devices pose a new set of complexities and challenges.

## Virtual Infrastructures Create Significant Security Challenges

One of the key advantages of virtualization is the ability to easily move virtual machines in order to optimize hardware resource usage. Likewise, for cloud, the ability to quickly spin up and down virtual machines on demand based on usage is seen as a primary advantage in creating a flexible infrastructure that can adapt to the demands on the enterprise. However, this fluidity brings great challenges for security.

### *Lack of Visibility into Traffic as It Travels Within Virtual Infrastructures*

Securing virtual machines is difficult. It is virtually impossible to know exactly where a machine might reside. The traffic from servers may never exit the enterprise; rather, it may move from virtual machine to virtual machine, thereby avoiding inspection and allowing attackers unrestricted access to

the virtual environment. If organizations are relying on static security technologies, they will miss traffic as it moves between virtual machines.

A virtual infrastructure also poses challenges for traditional patching. In the cloud, machines may spin up for only minutes at a time, thereby avoiding most scan cycles. Many virtual environments are difficult to scan or patch in the first place because of the always-on nature of the environments.

## Benefits of Comprehensive Security

Comprehensive security is a key requirement of the 3rd Platform. As the constant drumbeat of breaches continues, it is evident that existing security controls are inadequate and do not address the wide breadth of vectors available for attack. The modern security stack must be broad and apply advanced threat protection across a wide variety of vectors. Organizations should not be forced to deploy only a subset of threat prevention technologies based on cost or complexity but should have the ability to provide the required security across data and devices based on flexible requirements.

There is no "one size fits all" approach to security, and organizations should be able to choose from protection technologies and apply those technologies as needed to both physical and virtual environments regardless of vendor or provider. Enterprises should have the choice to select security functions as needed for a particular device, function, or workflow. A complete security platform should provide the following functions:

- Traditional security functions such as firewall, IPS, antivirus, and anti-bot
- Virtual private network (VPN) technology to allow secure communication into cloud resources
- Sandboxing protection to detect unknown malware and zero-day attacks
- Mobile security to allow mobile users to securely connect to the cloud using encrypted connections and additional authentication
- Data loss prevention to protect sensitive data from theft or unintentional loss
- Application control to prevent application layer denial-of-service attacks and protect cloud services

By providing a comprehensive security architecture that addresses both physical and virtual environments, organizations can be assured that they have the ability and security capabilities necessary to address attacks as they flow through the network, not just attempt to stop all attacks at the perimeter. Centralized management of on-premise and public cloud infrastructures can also significantly improve the ability of organizations to protect against attacks.

Policy management is simplified with centralized configuration and monitoring of cloud and on-premise security from a single console. This ensures that the right level of protection is applied consistently across both hybrid cloud and physical networks. Hybrid cloud workload traffic is logged and can be easily viewed within the same dashboard as other logs.

## Virtualization Security Trends

Enterprises are moving their data applications to virtual and cloud platforms at an increasingly rapid pace. This shift has enterprises evaluating security solutions. Enterprises are more apt to utilize virtualized security from their existing security provider if it is available and if the performance of the virtualized solution is similar to the performance of what they have in place. However, enterprises are extremely worried about the protection of their data. In a recent IDC survey, phishing was perceived as the top cyberattack being experienced in enterprise networks, with 63% of respondents indicating it as a top problem, followed by ransomware (59%) and spyware (50%). Attackers are improving their

social engineering tactics, crafting convincing email messages associated with their phishing campaigns. As a result, enterprises are continually looking for better ways to protect their data, wherever it resides.[1] Enterprises are also seeking easily tailored security without complex licensing. They want security that works across any platform. Additionally, they require security that can provide centralized management and consolidation of log data, policies, and reporting across all locations – both physical and virtual.

Enterprises also want to protect data, applications, users, and devices. The perimeter has vanished and enterprise security groups need a platform that can consistently address multiple attack vectors across an increasingly complex environment. Attackers are persistent and continually change their tactics. The enterprise's security posture must also follow the latest attack patterns.

## Considering Check Point

Check Point's vSEC is a family of products that delivers advanced threat prevention security to public, private, and hybrid clouds as well as software-defined datacenters. vSEC gateways protect virtualized environments from internal and external threats by securing applications, VMs, and virtualized networks with a comprehensive suite of security protections designed for the elastic and dynamic nature of cloud-based environments.

Check Point vSEC supports multiple hypervisors including VMware ESX, Microsoft Hyper-V, and KVM, as well as leading network virtualization solutions such as VMware NSX and vCenter, Cisco ACI, and OpenStack. In addition, vSEC supports the leading public and hybrid cloud environments such as Amazon Web Services, Microsoft Azure, and VMware vCloud Air.

Check Point vSEC provides proactive protection for even the most sophisticated threats with a comprehensive suite of advanced security capabilities, including:

- Firewall, IPS, Antivirus, and Anti-Bot protect services in the public cloud from unauthorized access and attacks.
- IPsec VPN allows secure communication into cloud resources.
- SandBlast Zero-Day Protection provides comprehensive protection against malware and zero-day attacks.
- Mobile Access allows mobile users to connect to the cloud using an SSL encrypted connection with two-factor authentication and device pairing.
- Data Loss Prevention protects sensitive data from theft or unintentional loss.
- Application Control helps prevent application layer denial-of-service attacks and protects cloud services.

### *Ease of Deployment and Centralized Management*

By supporting a large number of network virtualization platforms and integrating directly into the AWS and Azure marketplaces, Check Point's vSEC is easy for enterprises to obtain and deploy. What's more, vSEC integrates with popular cloud and software-defined networking (SDN) orchestration tools to facilitate automated security service insertion workflows. Check Point vSEC supports both pay-as-you-go (PAYG) and bring-your-own-license (BYOL) options for AWS and Azure, allowing enterprises to choose the model that works best for them, as well as attractive licensing options for all supported private cloud and SDN solutions.

[1] *Security Survey Analysis: Growing Interest in Data Security, Endpoint Security, and Network Security Products,* IDC #US41694116, September 2016

Once deployed, vSEC automatically integrates with existing Check Point management solutions on the network (including R80), allowing for immediate deployment of existing policies, centralized management of policies and devices, and a centralized location in which to collect and analyze logs. Check Point management also enables context sharing of security groups, tags, and threat information and supports automated quarantine and remediation workflows of infected VMs. vSEC provides customers with consistent policy management as well as visibility into the logging and reporting of all traffic in virtual and physical networks while securely enabling connectivity from enterprise networks to public and hybrid cloud environments.

### *Challenges for Check Point*

Even though Check Point's vSEC product is comprehensive, it is Check Point centric. Customers who may want to leverage other existing solutions in their network will find that Check Point's vSEC does not manage products from other vendors today. However, the Check Point management platform does provide open APIs, allowing it to integrate with a variety of solutions, which lets customers write their own scripts to have their security management integrate with and/or potentially manage other cloud-based products. Enterprises will need to settle on the Check Point architecture in order to take advantage of all the features and functionality.

## Conclusion

IDC believes enterprises need a comprehensive platform that can deploy advanced security functions across any platform — both virtual and on-premise. The Check Point vSEC product provides that functionality, giving enterprises a platform that can secure and manage corporate data whether it resides on-premise, is distributed among virtual machines, or is in a public, private, or hybrid cloud. As enterprises look for a security solution that can provide advanced security functions across a wide variety of virtualized platforms, they should consider Check Point vSEC.

---




Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com