Securing the Virtualized Environment: Meeting a New Class of Challenges with Check Point Security Gateway Virtual Edition

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Check Point
April 2011
Table of Contents

Executive Summary ........................................................................................................................................1
The Unique Challenges of Securing Virtualization .................................................................................1
Securing Virtualized Resources with Check Point Security Gateway Virtual Edition .......................2
  Extensible Software Blade Architecture ..................................................................................................3
  Flexibility in Modes of Deployment ......................................................................................................4
  Securing the Dynamic Virtualized Environment ....................................................................................5
  Centralized Administration, Unified with the Physical .........................................................................5
EMA Perspective .........................................................................................................................................6
About Check Point ....................................................................................................................................7
Executive Summary

Virtualization has seen wide adoption as a new and powerful range of tools for resource optimization and IT agility. Yet many organizations still do not recognize the significant differences between securing physical and virtualized environments. Legacy tools provide little control and often less visibility within the virtualized environment. Technologies are needed not only to extend protection to individual VMs, but to their interactions with each other.

But that is far from all that virtualization requires. For security and operations professionals alike, virtualization requires new ways of thinking about IT management—and IT risk. The virtualized data center can be a highly dynamic environment, with concepts such as live migration and the movement of running VMs for resource optimization posing entirely new challenges for security. New solutions are needed for these new demands—but they must also be compatible with existing strategy and investment to make the most of the opportunities virtualization offers the business.

In this paper, Enterprise Management Associates (EMA) examines the security challenges of virtualization, and explores the many ways in which Check Point Security Gateway Virtual Edition (VE) protects virtual machines (VMs) from external threats as well as from each other. Designed to integrate with security-enabling initiatives such as VMware’s VMsafe APIs, Security Gateway VE supports dynamic environments with a modular architecture and centralized administration that unifies security management across both physical and virtualized systems. This offers a solution that extends Check Point’s long-standing leadership in IT security with products that preserve and enhance the security investment while tackling the unique challenges of securing virtualization.

The Unique Challenges of Securing Virtualization

Although EMA research shows that security for virtualized environments is rated as a very important priority by nearly half (49 percent) of all enterprises, and is of average or above importance to nearly all (99 percent), many organizations have yet to fully recognize where their security strategies fall short when it comes to virtualization.

Current approaches in many enterprises are still predicated on legacy models such as the physical segmentation of resources. These models may break down when virtualized systems consolidate workloads having different security requirements on the same physical host. The logical segmentation of workloads based on security policy may still be limited largely to the physical network. Many organizations may have little control over issues such as inter-VM traffic, which raises questions regarding the security and effectiveness of segmentation among VMs on a shared physical host.

This highlights how virtualization introduces entirely new challenges for security. The hypervisor itself becomes a target—and a strategic one for the attacker, since the hypervisor is the focus of isolation and control for guest VMs. Though resource consolidation has its benefits, it has its risks as well, such as the increased security risk raised when multiple workloads can be targeted on a single virtualized physical host.

Securing the Virtualized Environment: Meeting a New Class of Challenges with Check Point Security Gateway Virtual Edition

Complexity is also increased with added layers of infrastructure, and the introduction of additional tools needed to manage them. These management tools may themselves lack sufficient maturity to address security concerns. Traditional approaches based on network segmentation may break down in the virtual realm, if policy is unable to recognize the nature of a specific virtual machine. Tools that fail to distinguish, for example, a virtual host used by a sales team from one used to manage sensitive intellectual property may inadvertently expose sensitive data to external networks. Management tools without this awareness may offer little or no distinction between the privileges of security personnel and virtual system managers, which raises concerns regarding separation-of-duties (SoD), accountability for administrative actions, and the implications for business priorities such as regulatory compliance. This highlights the blurring of traditional boundaries within IT that virtualization introduces—and not just between administrative roles, but also between servers and the network.

This reflects how virtualized environments may be physically resident on individual servers, but within those servers an entire architecture may be manifest: in networking, the server OS, storage and applications. Legacy approaches to IT security may fail if they do not embrace these distinctions, and the ways in which virtualization transforms the nature of security management. Firewalls alone will not deliver the needed depth within the virtualized environment, if they simply provide protection at the physical perimeter. Security for virtualized environments must be integral with a capable defense against intrusions and malware or protections against the exfiltration of sensitive data.

Virtualization is also a dynamic environment, which further raises the bar for protection. Virtual machines must be secured as they are brought online, with policy consistent with the nature of each individual VM. New environments and applications can be brought up, moved and changed in a virtualized environment much faster than before—and they must be protected from the moment they go “live.” Virtual workloads also have another characteristic unlike legacy systems: the ability to move running VMs when needed to optimize available resources, through techniques such as live migration and VMware’s vMotion technology. Security for virtualized environments must take these new dynamics into account as well. (This, however, suggests how virtualization can be a security advantage, highlighting the new way of thinking: Integrating security with the hypervisor can enable protection for these environments before they are deployed in operation and reduce gaps in coverage relative to legacy physical approaches.)

Securing Virtualized Resources with Check Point Security Gateway Virtual Edition

Answering these challenges, Check Point, long a pioneer in securing IT, has introduced Check Point Security Gateway Virtual Edition to protect dynamic virtual environments from threats both internal and external to the virtualized environment. Deployed as a virtual machine within a virtualized physical host, the Check Point Security Gateway VE delivers hypervisor-level security that provides:

- Network, intrusion prevention (IPS), antivirus and anti-malware security for individual guest VMs, without the need for agents deployed on each VM
- Security for inter-VM traffic between guest machines on a shared host
- Protection for VMs from threats arising from external networks
Securing the Virtualized Environment: Meeting a New Class of Challenges with Check Point Security Gateway Virtual Edition

- Policy that recognizes virtualization’s dynamic realities such as live migration
- Unified administration and a modular architecture that extends the security investment across both physical and virtualized environments.
- Deep auditing and visibility on virtualization configuration changes and VM network security
- Readily deployed functionality that secures all existent and newly provisioned VMs without changing the virtualized network topology.

Legacy approaches to technologies such as intrusion prevention may be blind to threats in the virtual environment without accommodations such as sending traffic to off-host appliances for inspection. Such an approach complicates the environment, effectively forcing a forward-looking virtualization strategy to bend to legacy implementations.

The Check Point solution was designed for virtualization, integrating security directly with the virtualized environment. Its options for deployment enhance the flexibility of how the solution is used, without dependence on adapting legacy approaches that may detract from the efficiencies and performance enterprises expect from virtualization.

**Extensible Software Blade Architecture**

Built on the same Software Blade Architecture that powers other Check Point products, Security Gateway VE is designed to be both comprehensive and extensible. Software Blades are modular components that each add a different aspect of functionality to Check Point products. Independently deployable but well integrated within the product architecture, each Software Blade is centrally managed. This strategy not only allows Check Point customers to tailor a deployment to their specific needs, but also enables future extensions of capability as security requirements evolve.

This Software Blade Architecture offers a significant advantage to Security Gateway VE customers: It enables them to deploy the same modules used to secure physical resources in virtualized environments, with functionality specifically designed and extended for virtualization. This brings Check Point’s wide range of 3D Security Software Blades to the virtual environment while preserving and extending the security investment across both physical and virtualized realms.

Software Blades for Security Gateway VE include:

- **Firewall:** Security Gateway VE extends Check Point leadership in firewall technology with highly granular policy-based protection, including protection from threats posed by other guest VMs on the same shared host and techniques such as strengthening anti-spoofing by linking a guest VM’s IP address with its UUID. Straightforward administration enables administrators to easily define security policy that follows VMs regardless where deployed within the virtualized data center, even in dynamic environments where VMware vMotion is a factor.

- **Intrusion prevention (IPS):** With intelligence backed by Check Point Research and Response Centers, Check Point’s multi-tier Threat Detection Engine combines a range of IPS techniques including signatures, anomaly detection, behavioral analysis, protocol validation, and other methods for identifying and defeating network-borne threats. These techniques are optimized to enable Check Point IPS to filter most network traffic without the performance impact of deep inspection.
Securing the Virtualized Environment: Meeting a New Class of Challenges with Check Point Security Gateway Virtual Edition

- **Antivirus and anti-malware:** The Check Point Antivirus and Anti-Spyware Software Blade provides both signature and anomaly-based protection to help defend systems from threats transmitted via a number of common network protocols.

- **Web security:** As Web technologies continue to shape modern IT, protection for the entire Web ecosystem becomes increasingly important. Check Point Software Blades offer protection for many common server-side Web risks as well as for client-side URL filtration and “safe surfing.” This helps protect virtualized environments regardless whether they improve resource utilization for server functions, or extend the benefits of virtualization to end users.

- **VPN:** The Check Point VPN Software Blade enables organizations to consolidate network security gateway functions to include secure communications for both remote access and site-to-site VPNs, combining protection for sensitive network content with defense against network-borne threats.

**Flexibility in Modes of Deployment**

The Check Point Security Gateway Virtual Edition offers “plug-and-play” security for virtual machines through the deployment of a virtual appliance delivered in the widely adopted Open Virtual Format (OVF). Security Gateway VE requires no network changes—regardless whether to VMs, VLANs, virtual switches or physical networks—and is compatible with popular virtual networking implementations such as Distributed Virtual Switch (DVS) and the Cisco Nexus 1000V virtual switch.

Security Gateway VE delivers protection through two deployment modes:

- **Hypervisor mode:** In this mode, Check Point Security Gateway VE provides inspection for all VM traffic in VMware environments, through the tight hypervisor integration enabled by VMware VMsafe technology. All virtual machines on the VMware ESX host are protected, without any change to the virtual network.

- **Network mode:** In this mode, Security Gateway VE is deployed as a virtual network device. This supports more traditional Layer 3 topologies, with traffic inspected by Security Gateway VE, but without requiring explicit network routing or bridging.

These options enable administrators to choose the set of capability that best meets their needs. Both alternatives enable inter-VM traffic inspection within a vSwitch, and protect virtual environments from external threats.

In hypervisor mode, security is integrated seamlessly and directly with the hypervisor. This enables immediate protection of any new VM brought up on the protected physical host. In network mode, security can be deployed in more traditional topologies, which allows for greater flexibility in designing security configuration that best answers specific requirements. This can help, for example, to reduce the cost of securing virtualization for small office or branch office environments and can help simplify branch off perimeter network security. Network mode anti-virus protection also offers additional functionality relative to hypervisor mode.

This flexibility in deployment modes enables organizations to choose the right balance of capability to fit their needs. Security Gateway VE in hypervisor mode delivers protection for all VMs on an ESX host, making the most of virtualized resource optimization. Network mode enables flexibility
in topology design as well as the advanced capabilities needed in many virtualized environments, including anti-spam and email security, advanced networking, and support for Check Point ClusterXL. Both modes provide a comprehensive range of firewall, IDS/IPS, antivirus/anti-malware, and Web security capabilities. Users simply choose the set of Software Blades that they require, regardless of deployment mode.

Securing the Dynamic Virtualized Environment

One of the advantages of virtualization is that it enables high agility in deploying, moving and retiring virtual machines on demand. This allows modern IT organizations to deliver a wide range of business benefits, from better performance, availability and resource optimization to “just in time” activation of VMs as needed for specific tasks.

Check Point Security Gateway VE responds with capability that directly tackles the security implications of live migration and distributed virtualization resource management, with support for VMware vMotion and Distributed Resource Scheduler (DRS). When new VMs are brought online, protection is applied to them immediately, with no downtime. This helps to ensure that newly added machines are protected automatically. When a running VM is vMotion-migrated to a different ESX host, existing connections related with the original virtual IP address continue to have their security policy enforced as defined on the original ESX host. This allows established connectivity to proceed without interruption, and defends the moved VM against communications restricted or prohibited by the original security policy. This further improves the transparence of security management by enabling a one-to-one correspondence between security policy and a specific VM, regardless on which physical platform it may be hosted.

This is important, particularly in light of the evolution of regulatory requirements such as those of the PCI Data Security Standard, which increasingly expect virtualized environments to preserve well-established security concepts such as the segmentation of network security zones. Check Point Security Gateway VE allows administrators to define multiple policy zones that can be applied to specific categories of VMs. These policies follow VMs regardless where they may be provisioned physically, helping to assure that resource segregation based on policy or sensitivity is preserved in both physical and virtual environments.

Centralized Administration, Unified with the Physical

The administration of Check Point Security Gateway VE is not only centralized for all of an organization’s virtual environments, but is unified with Check Point physical security technologies as well. Security Gateway VE is managed from the same Security Management or Multi-Domain Management (MDM) console as other Check Point products. This provides two specific benefits:

• It enables consistency in the creation, distribution and management a security policy across the entire IT environment, both virtualized and physical. This limits potential gaps in security coverage and assures more efficient management, enhanced with technologies that specifically recognize the new demands of securing virtualization.
Securing the Virtualized Environment: Meeting a New Class of Challenges with Check Point Security Gateway Virtual Edition

- It keeps security management in the hands of the security team, regardless whether the protected environment is physical or virtual. This upholds the separations of duties often required by regulatory mandates, and relieves uncertainties caused by tools that blur distinctions between the administration of security for virtualized environments with the administration of virtualization itself.

Check Point security management tools help support compliance requirements for monitoring and reporting that affect both virtual and physical environments. Event alerting includes the ability to integrate messages from ESX logs directly into the Check Point management console. For example, any time a new VM is created or configuration changes are made to a vNIC, vSwitch, VLAN or port group, the event will trigger an alert in Check Point management tools. This keeps security teams informed when events from the comprehensive environment have an impact on virtualization security.

EMA Perspective

As the pioneer of stateful inspection firewalls, Check Point has long been a leader in network protection that is simple to deploy and administer. Today, Check Point extends this leadership to virtualized environments with Security Gateway Virtual Edition, which recognizes the challenges of virtualization security with solutions that are both conveniently extensible and easy to deploy, and with minimal impact on the protected environment. This approach offers a number of business benefits for security administration.

The unification of virtualization security management with the same administrative console that manages other Check Point products protects and extends the security investment. Check Point’s Software Blade Architecture eases the application of security functionality for security teams, since Security Gateway VE enables them to deploy the same protection modules regardless whether the target is a physical or virtualized system. Because it integrates with the virtualized environment, Security Gateway VE also keeps the preservation of security intact in the event of a disaster that affects the virtualized data center. As with ESX systems themselves, Security Gateway VE can be re-deployed on recovery platforms just as readily as in the primary environment, reflecting the disaster recovery and business continuity advantages of virtualization.

These benefits would not be realized, however, if Security Gateway VE did not address the unique requirements of virtualization that call for a new generation of security tools. Security Gateway VE hypervisor integration leverages VMware’s VMsafe initiative and enables essential visibility and control within the virtualized environment. This provides detection and prevention of threats to individual VMs, with improved data and endpoint security for each. It offers control for multiple zones and policy requirements, and protection that follows the dynamic movement of virtual machines. Security Gateway VE goes well beyond these fundamentals, however. Compatibility with VMware vSphere Cluster, for example, is in tune with organizations that seek to make the most of virtualization.
With these capabilities, Check Point extends protection specific to the virtualized environment, defending VMs from security threats in external environments—as well as from each other. Security teams must keep all these priorities in mind when weighing the strategies for securing virtualization, considering that VMs can be compromised by malicious software and actions as well as through inadequate defenses that fail to recognize the realities of virtualization. The continued evolution of regulatory requirements such as the PCI Data Security Standard clearly indicate that organizations will need to keep pace with these realities, as leaders such as Check Point continue to define defense for the intangible enterprise.

**About Check Point**

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) provides customers with protection against threats, reduces security complexity and lowers total cost of ownership. Check Point was an industry pioneer with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the security needs of any organization. Check Point 3D Security combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies. Check Point’s award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.
About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2011 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com