Check Point CloudGuard Virtual Edition

Comprehensive Security Protections for Software-Designed Data Centers

Virtualized Security Overview

The wide adoption of virtualization and cloud-based architectures is being driven by the desire to transform businesses for greater efficiency, speed, agility, and cost controls. While virtualized solutions offer many advantages over traditional IT infrastructure, legacy security approaches do not address the dynamic needs of these new compute and network environments, exposing organizations to a host of unique security risks.

Security insertion and management is a significant challenge for cloud enabled environments like virtualized data centers, branch offices and other multi-tenant infrastructures. Organizations struggle to manage disparate security solutions for their physical and virtual environments, resulting in a lack of consistent policy enforcement that makes management and auditing difficult. At the same time, the frequency and sophistication of cyber threats continues to increase. Traditional security approaches protecting physical networks fail to adequately extend to virtual environments, leaving them exposed and making them attractive targets for cyber criminals. Once a virtual machine (VM) is breached, attacks are able to spread laterally from VM to VM within the virtual network and even extend externally across the entire corporate network.

Check Point CloudGuard Network Security Virtual Edition (VE) delivers comprehensive security tailored to protect hypervisor-based virtual networks so businesses can feel confident about extending their applications and workflows to cloudenabled environments.

Check Point CloudGuard Network Security Virtual Edition (VE) gateways protect dynamic virtualized environments from internal and external threats by securing virtual machines (VMs) and applications with the full range of protections of the Check Point Software Blade architecture. Check Point's virtualization security supports multiple hypervisors including VMware ESX, Microsoft Hyper-V and KVM.

Designed for the dynamic requirements of data center, branch office and other multi-tenant deployments, CloudGuard VE provides the most advanced threat prevention security to inspect traffic entering and leaving subnets in virtual environments. Fully integrated security features include: Firewall, IPS, Application Control, IPsec VPN, Anti-Virus and Anti-Bot. SandBlast adds Threat Extraction and Threat Emulation for zero-day protections.

CloudGuard VE provides consistent security policy management, enforcement, and reporting, making migration to virtualized cloud environments painless. Additionally, CloudGuard VE allows for an elastic licensing model (virtual core compute-based with automated distribution from a shared pool) ideal for environments with dynamic workloads.

Threat Prevention For Virtualized Networks

Check Point's flagship cloud security solution CloudGuard Network Security Virtual Edition (VE) protects dynamic virtualized environments from internal and external threats by securing virtual machines (VMs) and applications with industry-leading advanced threat prevention security. CloudGuard VE seamlessly integrates with leading hypervisors such as VMware ESX, Microsoft Hyper-V and KVM. Additionally, CloudGuard VE provides reliable and secure connectivity to public cloud assets while protecting applications and data with industry-leading security while helping organizations dramatically simply security management and policy enforcement across private, hybrid, and public cloud networks.

Business agility and robust security

CloudGuard VE gives organizations the confidence to securely deploy workloads to virtualized cloud networks, providing tangible customer benefits including:

- Protection against security breaches, malware, and zero-day attacks in the public cloud that may lead to private cloud / data center breaches
- Unified security management, visibility, and reporting across both private and public cloud networks
- Elimination of the costs and loss of reputation associated with business disruptions and downtime
- Securely migrate sensitive workloads, applications and data to the cloud

Fully integrated security protections

CloudGuard VE provides industry-leading threat prevention security to keep virtualized cloud networks safe from even the most sophisticated attacks. Fully integrated security protections include:

- **Firewall, Intrusion Prevention System (IPS), Anti-Virus, and Anti-Bot** technology protects services in the cloud from unauthorized access and prevents attacks
- **Application Control** helps to prevent application-layer Denial of Service (DoS) attacks and protect hybrid cloud services
- **Mobile Access** allows mobile users to connect to hybrid clouds using an SSL encrypted connection with two-factor authentication and device pairing
- **Data Loss Prevention** protects sensitive data from theft or unintentional loss
- **SandBlast Zero-Day Protection** sandbox technology provides the most advanced protection against malware and zero-day attacks

Unified management of physical and virtual infrastructures

With all aspects of security management such as policy management, logging, monitoring, event analysis and reporting centralized via a single dashboard, security administrators get a holistic view of their security posture across the entire organization. CloudGuard VE gives organizations complete threat visibility and consistent enforcement for virtual cloud infrastructures.

Policy management is simplified with centralized configuration and monitoring of both physical and cloud-based networks, allowing for a consistent security footprint for all corporate data. A layered approach to policy management allows administrators to segment a single policy into sub-policies for customized protections and delegation of duties per application or segment. This ensures that the right level of protection is applied across both physical and cloud networks.

Consolidated logs and reporting

Check Point SmartEvent, part of the Unified Security Management platform, consolidates monitoring, logging and reporting across virtual and physical networks. Virtualized cloud workload traffic is also logged and can be easily viewed within the same dashboard as other logs. Security reports specific to virtualized workloads can be generated to track security compliance across cloud-based infrastructures, dramatically simplifying compliance reporting and audits.

Dynamic security policies

CloudGuard can be configured for integration with a controller component as part of the Security Management platform. The CloudGuard controller integrates with cloud management solutions to include the sharing of context, allowing cloud objects to be imported and reused within Check Point security policies. This reduces security policy creation time from minutes to seconds. Real-time context sharing of cloud objects is maintained so that any changes or new additions are automatically tracked without the need for administrator intervention. Check Point logs are further enriched with cloud context including cloud object names. For example, in a VMware environment, vCenter objects like virtual machine identities and network elements are available in security policies and are populated in logs and reports.

Elastic licensing with automated distribution

Licensing is compute based (virtual cores in-use by any CloudGuard VE gateway) and allows for dynamic distribution of CloudGuard VE gateway instances from a shared and centralized license pool. This elastic licensing model is facilitated by Check Point Unified Security Management and is ideal for dynamic workloads.

Seamless integration in private cloud networks

Check Point CloudGuard VE can be deployed as a security gateway to protect the ingress-egress point of a virtual network or virtual segment as well as inter-VM protection using standard routing configurations. CloudGuard can be delivered as a service when integrated with SDN controllers using service chaining to perform transparent traffic redirection. This provides a smooth and seamless integration into private cloud environments built on SDN and NFV frameworks. Likewise, advanced capabilities like secure microsegmentation for lateral (east-west) traffic protection, the ability to isolate (auto-quarantine) infected hosts are also supported.

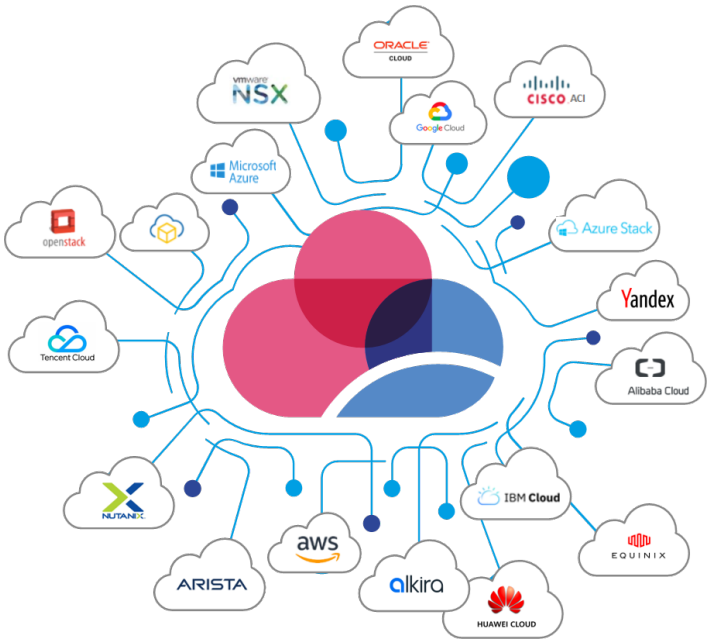
Security automation and orchestration

In virtualized data center environments, there is often a need to integrate different systems that manage the security workflow. Also, repetitive manual tasks must be automated to streamline security operations. Check Point's security management API allows for granular privilege controls, so that edit privileges can be scoped down to a specific rule or object within the policy, thus restricting what an automated task or integration can access and change. This ability to automatically provision trusted connectivity provides security teams with the confidence to automate and streamline the entire security workflow. In addition, predefined Check Point security templates automate the security of newly provisioned virtual applications. This makes it much easier to deploy advanced security in virtualized networks.

Solution Components

CloudGuard Network Security gateway

The CloudGuard gateway is a security gateway running inside a virtual machine (VM). It provides industry-leading advanced threat prevention security and is deployed into the virtualized network to provide perimeter protection and prevent lateral threat movement between applications inside the datacenter.



CloudGuard supports the broadest range of cloud infrastructures and hypervisors

Check Point Unified Security Management with CloudGuard controller

The Check Point CloudGuard Network Security controller integrates with virtual infrastructure managers, cloud management systems and SDN controllers. It supports the import of cloud management and networking objects (vCenter, OpenStack, NSX, ACI), dynamically tracks object changes and allows using cloud networking security groups in the Check Point security policy and logs. It allows for optimized network security service deployment, provisioning and automation.

Virtualization hypervisor and manager

The virtualization hypervisor provides a high performance server virtualization platform for the software-defined data center. The virtualization infrastructure manager like vCenter provides centralized configuration and management of the server virtualization environment. Check Point's CloudGuard VE supports multiple hypervisors including VMware ESX, Microsoft Hyper-V and KVM in addition to SR_IOV network interface support.

Cloud networking fabric and controller (optional)

The cloud networking fabric provides a high performance network virtualization platform for the software-defined data center. The controller provides centralized configuration and management of the network fabric. It allows for advanced network security service insertion (L4-L7) and automation.

Cloud management (optional)

The cloud manager provides automation and orchestration platform for centralized management, provisioning for all components in the software defined data center. It allows for advanced network security service insertion (L4-L7) and automation.

Key Features And Benefits

- Protect the most demanding and business critical virtualized environments using Check Point's advanced threat protection with highest malware catch rates
- Comprehensive security protections fully integrated into a single security gateway
- Optimally deployed in virtual data centers, branch offices and multi-tenant environments
- Support for leading hypervisors including VMware ESXi, Microsoft Hyper-V and KVM
- Unified security management for control and visibility across virtual and physical networks
- Security services provisioned in minutes for fast application deployments
- Shared security context to enable better alignment across security controls
- Elastic licensing model with automated and centralized distribution
- Seamless integration into private cloud environments for advanced and automated security deployments

Summary

Check Point CloudGuard Network Security Virtual Edition delivers accelerated, automated and simplified provisioning and deployment of Check Point's advanced security services in next generation virtualized cloud networks. The integration enables better collaboration among security and infrastructure teams while providing full control and visibility across both physical and virtual infrastructure. CloudGuard also integrates with a wide variety of public clouds (including AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud and more) as well as private cloud environments including those built on SDN technology and NFV frameworks commonly deployed in the SDDC including VMware NSX, Cisco ACI and OpenStack.

To learn more about how Check Point CloudGuard Network Security VE provides the most advanced security protections for virtualized cloud networks, download a free trial of CloudGuard Virtual Edition at https://supportcenter.checkpoint.com or contact your Check Point partner or sales representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com