Check Point SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY

openstack

CHECK POINT + OPENSTACK

Comprehensive Security Protections for Cloud-based Datacenters

OpenStack is an open standard cloud computing platform for public and private clouds. It is designed by a global community of developers and organizations to address today's need to build a scalable and flexible cloud infrastructure to enable agility and to deliver speed and time-to-market advantages for the delivery of new services.

Check Point is a contributing member of the OpenStack community and integrates with OpenStack to protect and secure cloud environments.

Check Point CloudGuard for OpenStack protects OpenStack cloud environments from internal and external threats with the full range of protections available in the Check Point threat prevention architecture. CloudGuard for OpenStack delivers best-of-breed security protection and management so your organization can focus on architecting dynamic cloud environments

Designed for the dynamic security requirements of cloud deployments, CloudGuard provides the most advanced threat protections to inspect traffic entering and leaving tenant subnets in the cloud. CloudGuard also provides consistent security policy management, enforcement, and reporting, making migration to OpenStack cloud environments painless.

Check Point CloudGuard IaaS has been validated and integrated with ecosystem partners in OpenStack cloud environments.

VIRTUAL DATACENTER SECURITY OVERVIEW

The wide adoption of cloud architectures—whether public, private or hybrid—is being driven by the desire to transform businesses for greater efficiency, speed, agility and cost controls particularly in the carrier and large enterprise networks which are primarily used for application delivery to large user base including customers and lines of business. OpenStack cloud networks helps CSPs and large enterprises thrive in this increasingly fast-paced environment by accelerating the journey from traditional networks built on monolithic, proprietary appliances to more agile cloud networks enabled by Network Functions Virtualization (NFV). Now enterprises and carriers can move to a virtualized network and instantly add capacity and manage the entire network from a single, unified control application and can achieve true agility in network configuration and management.

While the cloud offers many advantages over traditional infrastructure it also exposes enterprises and carriers and their end users to a whole new set of security challenges. The built-in security controls in the cloud lack advanced threat protection. The operational challenge of provisioning security for workloads is a manual operation that is complex, slow and error-prone. The cloud hosts multi-tenant environments where application workloads critically need to be isolated and protected from each other. The traditional approach to securing a data center with a perimeter gateway only provides visibility and control into north-south traffic. All internal or east-west traffic is unprotected and allows threats to spread laterally once a weaker system has been compromised.

DYNAMIC THREAT PREVENTION SECURITY FOR OPENSTACK

Check Point CloudGuard IaaS for OpenStack delivers industry leading threat prevention security fully integrated and validated on OpenStack, allowing CSPs and enterprises to deliver comprehensive protections from fifth generation internal and external threats targeting virtual datacenter environments. Using CloudGuard for Openstack, enterprises can focus on developing a fully automated and centrally orchestrated cloud environment that empowers line of business users to self-provision resources.

What's more, the OpenStack ecosystem of validated and integrated virtualized functions give carriers the freedom to quickly and easily deploy best-in-class applications like Check Point CloudGuard in production networks.

March 2020

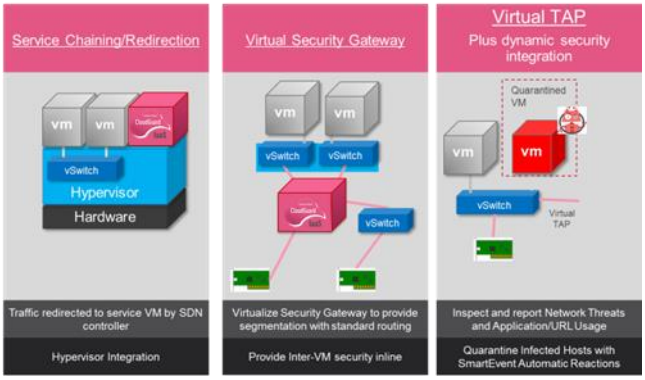
Comprehensive threat prevention

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

- **Firewall, Intrusion Prevention System (IPS), Antivirus, and Anti-Bot** technology protects services in the cloud from unauthorized access and prevents attacks
- **Application Control** helps to prevention application-layer Denial of Service (DoS) attacks
- **IPSec VPN** allows secure connectivity over a dedicated and encrypted tunnel between Azure Virtual Networks (VNET) and the Enterprise network
- **Remote Access** allows remote users to connect to Azure 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

Security orchestration and automation

OpenStack provides the framework to allow automated policy-based service insertion from a single-pane-of-glass management platform. The integration automates and simplifies the provisioning of CloudGuard gateways into the OpenStack controlled networking fabric to protect east-west traffic from lateral movement of threats. The integration of OpenStack and CloudGuard allows for single-click provisioning using HEAT (YAML) templates and the ability to configure security gateway via RESTful APIs, as well as gateway auto registration with defined policies for dynamic segmentation.

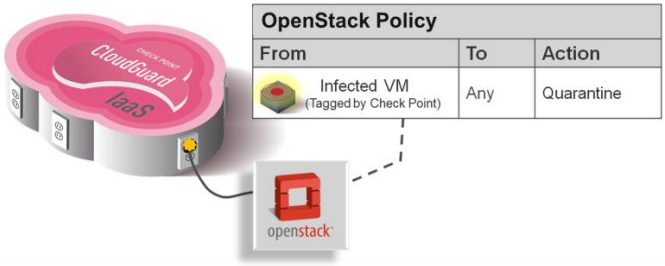


Context-aware security policies

The integration with OpenStack cloud controller shares context with the Check Point CloudGuard controller allowing OpenStack Metadata like security groups 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 security groups is maintained so that any changes or new additions are automatically tracked without the need for administrator intervention.

Auto-quarantine of infected hosts

Hosts identified by CloudGuard as infected can be automatically isolated and quarantined. This is accomplished by CloudGuard tagging the infected hosts and sharing this information with the OpenStack controller. Additionally, automated remediation services can be triggered by an orchestration platform. Threats can be quickly contained and the appropriate remediation service can be applied to the infected VM.



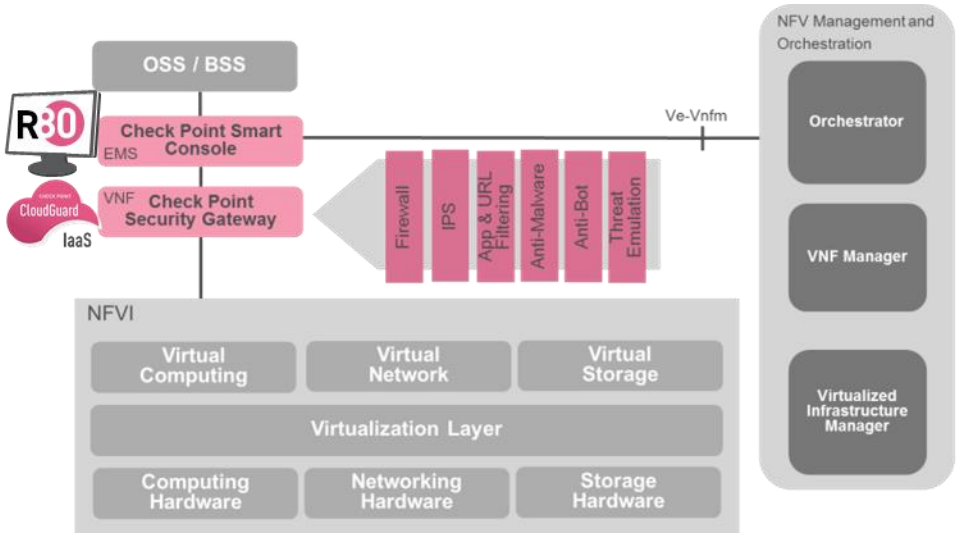
Centralized visibility and control

Check Point CloudGuard for OpenStack provides simplified and centralized security management across cloud environments. Manage CloudGuard for OpenStack using your existing Check Point Unified Security Management solution. Enforce a consistent security policy across both virtual and physical, on-premises and cloud infrastructures all from a single console.

Unified logs and reporting

CloudGuard for OpenStack gives organizations complete threat visibility and enforcement across their entire cloud-based infrastructure. Check Point SmartEvent software consolidates monitoring, logging, and reporting across cloud networks. Check Point logs are further enriched with OpenStack context including security group tags. Security reports specific to cloud workload traffic can be generated to track security compliance across the cloud network, simplifying reporting, compliance and audits.

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. CSPs can provide automatically scheduled, periodic reports to their customers using the Check Point SmartEvent software.



Check Point CloudGuard for OpenStack Integraton with NFV infrastructure

KEY FEATURES AND BENEFITS

- Dynamic insertion and orchestration of Check Point's advanced threat protection with highest malware catch rates
- Operationally feasible micro-segmentation for East-West traffic protection
- Fine-grained security policies tied to OpenStack defined objects, tags and more
- Openstack object context-awareness in security logs and data center specific reports
- Tagging infected hosts as a means for network isolation (auto-quarantine) or remediation
- SmartEvent Logging provides incident tracking and threat analysis for both the perimeter and data center traffic
- Unified security management for control and visibility across virtual and physical environments including multi tenancy support
- Ability to use context from multiple cloud management systems such as Cisco ACI, OpenStack and VMware vCenter in the same security policy
- Rapid Deployment of security policies through the complete application deployment lifecycle
- Reduced OPEX due to accelerated application and security deployment with increased efficiency in service provisioning and network security segmentation

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT OPENSTACK

The OpenStack (www.openstack.org) project is a global collaboration of developers and cloud computing technologists producing the open and scalable standard cloud computing platform for both public and private clouds. The open source project is built by a vibrant community of developers in collaboration with users and some of the biggest names in the industry. OpenStack works with popular enterprise and open source technologies making it ideal for heterogeneous infrastructure. Hundreds of the world's largest brands rely on OpenStack to run their businesses every day, reducing costs and helping them move faster.