Check Point + VMware

Automated and Agile Threat Prevention Security for Software-Defined Data Centers

Challenges of Securing Modern Data Centers

Organizations today demand an agile data center environment to reduce IT costs, increase business agility and remain competitive. At the same time, integrated applications, increasing utilization of virtualization technology and dynamic environments have led to a dramatic increase in network traffic going east-west, or laterally within the data center. When it comes to security, the focus has mainly been on protecting the perimeter — or north-south traffic — going into and out of the data center. There are few controls to secure east-west traffic inside the data center. This presents a security risk where threats can traverse unimpeded once inside the data center. Traditional security approaches to this problem are manual, operationally complex and slow, and are unable to keep pace with dynamic virtual network changes and rapid virtual application provisioning.

VMware NSX is an industry leading network virtualization platform that delivers the same benefits to the network that VMware delivered for compute. Virtual networks can be programmatically managed and created on demand. The result is dramatically simplified network and security operations, fast provisioning of networking and security services — from weeks to minutes, and fundamentally better data center security. With the recent announcement of VMware Cloud on AWS, customers can now bring VMware's enterprise-class Software-Defined Data Center (SDDC) software seamlessly to their AWS cloud.

Check Point CloudGuard Network Security for VMware NSX delivers advanced threat prevention security to VMware NSX SDDC environments. Designed for the dynamic requirements of cloud-based data centers, CloudGuard provides automated security provisioning coupled with the most comprehensive protections. 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.

Centrally managed across hybrid infrastructures, CloudGuard provides consistent security policy enforcement, full threat visibility across physical data centers, SDDCs and public cloud environments.

Automated Threat Prevention Security For Software-Defined Data Centers

VMware NSX native security capabilities, automation and extensibility framework are leveraged by Check Point to dynamically insert, deploy and orchestrate advanced security services inside the Software-Defined Data Center. Network isolation and segmentation inherent to the NSX platform enable feasible micro-segmentation, allowing the SDDC to deliver a fundamentally more secure approach to data security. Policy is enforced at the virtual interface, and security policies follow workloads.

The integration of Check Point CloudGuard Network Security with NSX brings consistent policy management and enforcement of advanced security protections automatically deployed and dynamically orchestrated into software-defined data center environments. CloudGuard provides industry-leading threat prevention security to keep data centers protected from even the most sophisticated threats. Fully integrated multi-layered security protections include:

- Stateful Firewall, Intrusion Prevention System (IPS), Anti-Virus and Anti-Bot technology to protect data centers against lateral movement
- SandBlast Zero-Day Protection sandbox technology provides the most advanced protection against malware and zero-day attacks
- Application Control to help prevent application layer Denial of Service (DoS) attacks and by that protect the software-defined data center
- Data Loss Prevention protects sensitive data from theft or unintentional loss

Automation and Orchestration

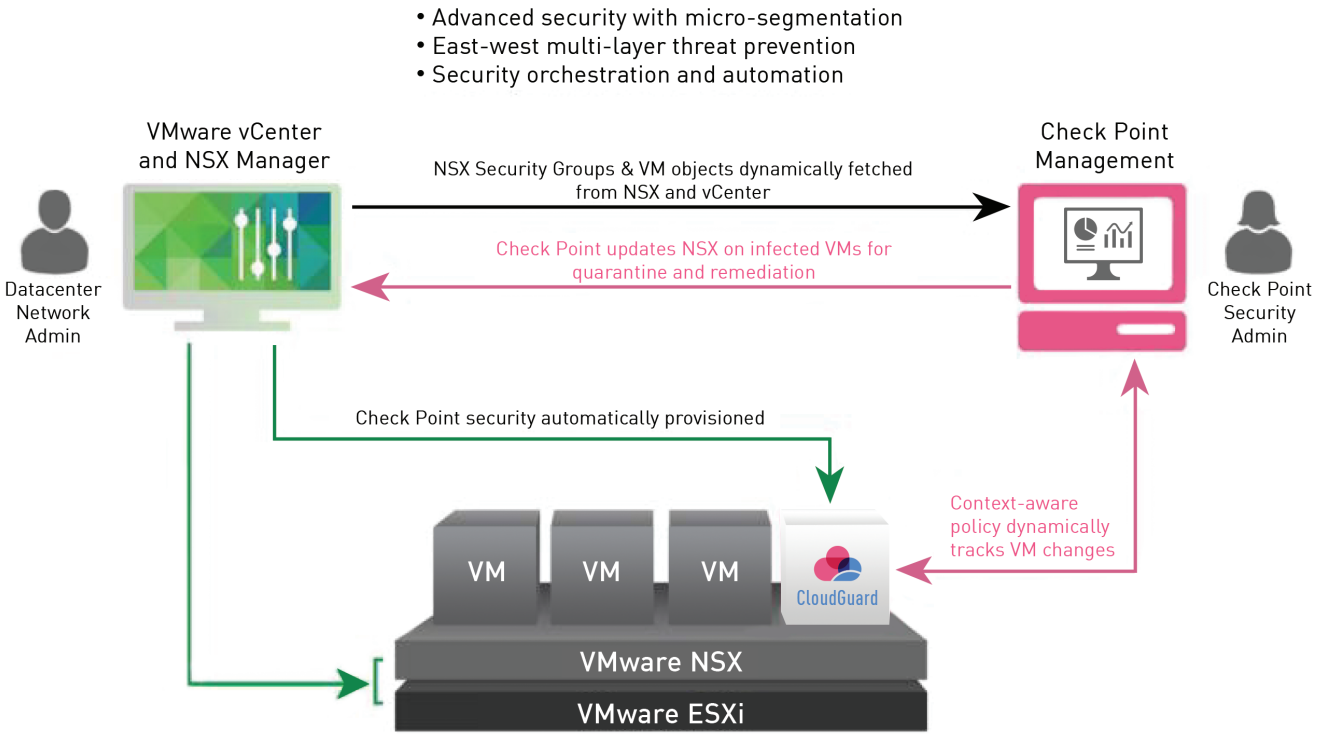
Check Point CloudGuard leverages NSX security automation for dynamic distribution and orchestration of CloudGuard for protecting east-west traffic. In the data center environment, there is often a need to integrate different systems that manage the security workflow. Also, repetitive manual tasks must 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, 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.

Ubiquitous Security Enforcement

Check Point CloudGuard integration with VMware NSX allows dynamic insertion of advanced security protection between workloads enabling distributed enforcement at every virtual interface. The integration automates and simplifies the provisioning of CloudGuard gateways into the NSX virtual fabric to protect east-west traffic from lateral movement of threats enabling feasible micro-segmentation. NSX basic fire-walling capability can be extended with Check Point's CloudGuard, whose layered security policy approach makes it easy to segment a policy, and provide granular rule definitions specific to network segments.

Automation and Orchestration

Check Point CloudGuard leverages NSX security automation for dynamic distribution and orchestration of CloudGuard for protecting east-west traffic. In the data center environment, 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, 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.

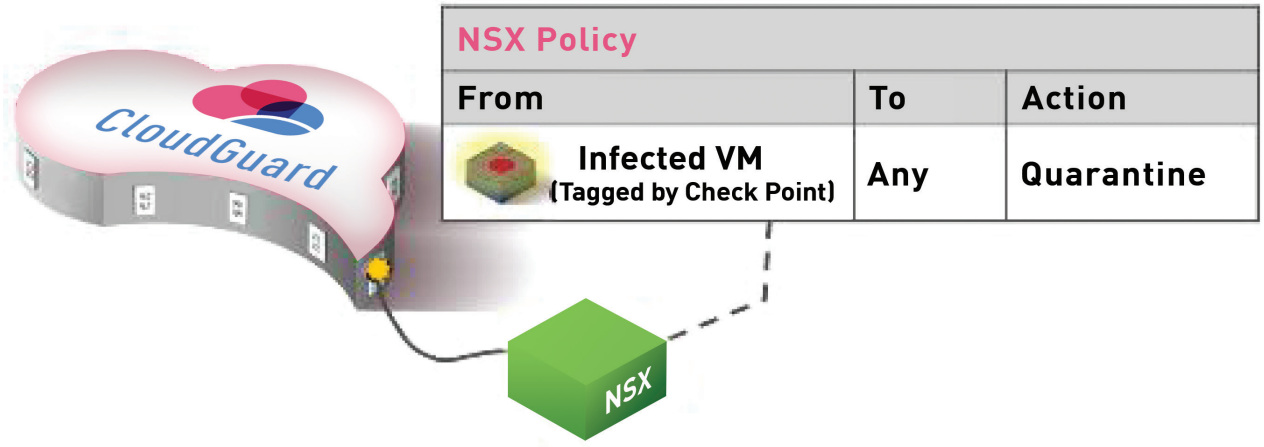


Ubiquitous Security Enforcement

Check Point CloudGuard integration with VMware NSX allows dynamic insertion of advanced security protection between workloads enabling distributed enforcement at every virtual interface. The integration automates and simplifies the provisioning of CloudGuard gateways into the NSX virtual fabric to protect east-west traffic from lateral movement of threats enabling feasible micro-segmentation. NSX basic fire-walling capability can be extended with Check Point's CloudGuard, whose layered security policy approach makes it easy to segment a policy, and provide granular rule definitions specific to network segments.

Context-Aware Security Policies

The integration with VMware NSX controller and vCenter shares context with the Check Point CloudGuard controller allowing security groups and VM identities 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 additions to the infrastructure are automatically tracked without the need for administrator intervention. Security protections are dynamically applied to newly created applications regardless of where they are hosted.



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 NSX controller. Additionally, automated remediation services can be triggered by an orchestration platform. Threats are quickly contained and the appropriate remediation service can be applied to the infected VM.

CHECK POINT ACCESS POLICY				
Rule	From	To	Application	Action
3	Finance_App1 (vCenter Object)	Database_Group (NSX Object)	MSSQL	Allow
4	HR_App2 (NSX Security Group)	Finance_Group (ACI EPG)	CRM	Allow
5	User_ID	SAP_App (vCenter Object)	SAP	Allow

Centralized Security Management

Security management becomes dramatically simplified with centralized configuration and monitoring of CloudGuard. Traffic is logged and can be easily viewed within a common dashboard. Security reports can be generated to track security compliance across both the data center and hybrid network. 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. 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 the security posture across their entire organization – from legacy premises to SDDC to hybrid cloud.

Key Features And Benefits

- Dynamic insertion and orchestration of Check Point's advanced threat prevention security
- Operationally feasible secure micro-segmentation for east-west traffic protection
- Fine-grained access control policies tied to NSX defined objects, security groups and virtual machines
- Unified security management and visibility across physical networks, SDDCs and hybrid cloud environments
- Security services provisioned in minutes for fast application deployments
- Shared security context to enable better alignment across security controls
- Isolation and auto-remediation of infected virtual machines
- Improved day-to-day operational efficiencies by automating routine tasks and integrating security into workflow and change management processes
- Advanced security services seamlessly provisioned and orchestrated at the speed of DevOps processes.

Solution Components

Check Point CloudGuard gateway

The CloudGuard gateway provides industry-leading advanced threat prevention security and is deployed into the NSX fabric as well as on customer AWS virtual private clouds (VPCs) to prevent malware and other sophisticated threats from affecting customer cloud environments.

Check Point Smart Center with CloudGuard controller

The Check Point CloudGuard controller integrates with NSX Manager, vCenter and AWS. It supports the import of NSX, vCenter and AWS objects, dynamically tracks object changes and allows using security groups in the Check Point security policies, reports and logs.

VMware NSX Fabric and Controller

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

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 multi-level 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 VMware

VMware is a leader in cloud infrastructure and business mobility. Build on VMware's industry-leading virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant and more secure. Customers can innovate faster by rapidly developing, automatically delivering and more safely consuming any application. VMware has more than 500,000 customers and 75,000 partners. The company is head-quartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

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