Check Point CloudGuard for Cisco ACI

Comprehensive Security Protections for Software-Designed Data Centers

Modern Data Center Security Overview

Organizations today demand an agile data center environment to reduce IT costs, increase business agility and remain competitive. At the same time, the shift from a hardware-centric to an application-focused infrastructure has led to a dramatic increase in network traffic going east-west, or laterally, between applications in the data center.

Security has traditionally been focused on protecting perimeter, or north-south traffic, going into and out of the data center while east-west traffic between applications inside the data center is not inspected. This presents a host of new challenges where threats introduced into the data center can traverse unimpeded since they no longer pass through the security gateway.

What's more, traditional security approaches are manual, operationally complex, slow and unable to keep pace with dynamic changes and rapid application provisioning. Check Point CloudGuard Network Security for Cisco ACI addresses these challenges delivering comprehensive and dynamic security specifically architected for Cisco ACI enabled data centers.

Cisco Application Centric Infrastructure (ACI) is a comprehensive software defined networking (SDN) architecture that supports a business-relevant application policy language to accelerate application delivery, reduce operating costs and greatly increase business agility. Cisco ACI helps customers dramatically reduce application deployment times from weeks to minutes while improving IT alignment with business objectives and policy requirements.

CloudGuard Network Security for Cisco delivers advanced threat prevention security for Cisco ACI software-defined data centers. Designed for the dynamic requirements of Cisco ACI deployments, 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 by the gold standard in security management, CloudGuard provides consistent security policy enforcement, full threat visibility across physical and virtual data center network environments.

Dynamic Threat Prevention Security for Cisco ACI

Cisco ACI provides effective micro-segmentation for next generation data centers through the integration of physical and virtual environments under a common policy model for networks, servers, storage and security. Cisco ACI's application-aware policy model and native security capabilities are leveraged by Check Point CloudGuard to dynamically insert, deploy and orchestrate advanced security protections within software-defined data centers.

Together, Cisco and Check Point provide a powerful solution that gives customers complete traffic visibility and reporting in addition to proactive protection from even the most advanced threats within virtual network environments. The joint solution forms the foundation of an intelligent application delivery network architecture where security seamlessly follows application workloads and accelerates application deployment while maintaining reliability, multi-tenancy and operational workflows.

Comprehensive Threat Prevention

CloudGuard for Cisco ACI provides industry-leading threat prevention security to keep data centers protected from the lateral movement of threats and other sophisticated attacks. Fully integrated multi-layer 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, along with threat emulation and URL filtering capabilities
- **Application Control** helps prevent application layer denial-of-service (DoS) attacks, thus protecting the next-generation data center
- **IPSec VPN and Mobile Access** allow secure communication into cloud resources
- **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

Automated Security Provisioning

Cisco ACI provides the framework to allow automated policy-based service insertion from a single-pane-of-glass management platform. The integration of Cisco ACI and CloudGuard automates and simplifies the provisioning of CloudGuard gateways into the ACI fabric to protect east-west traffic from lateral movement of threats.

Context-Aware Security Policies

The integration with Cisco's Application Policy Infrastructure Controller (APIC) shares context with the Check Point CloudGuard controller allowing end point groups (EPG) 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 end point groups is maintained so that any changes or new additions are automatically tracked without the need for administrator intervention.

Check Point Access Policy				
Rule	**From**	**To**	**Application**	**Action**
3	Finance_App1 (vCenterObject)	Database_Group (ACI EPG)	MSSQL	Allow
4	HR_Appw (ACI EPG)	Database_Group (ACI EPG)	CRM	Allow
5	User_ID	SAP_App (vCenter Object)	SAP	Allow

Complete Visibility and Control

CloudGuard for Cisco ACI provides consolidated logging and reporting of threats and security events. Check Point logs are further enriched with ACI context including EPG names and security tags. Additionally, the Check Point SmartEvent platform provides advanced incident tracking and threat analysis across both the physical and virtual data center network traffic.

Centralized and Unified Management

Security management is simplified with centralized configuration and monitoring of Check Point CloudGuard. Traffic is logged and can be easily viewed within the same dashboard as other gateways. Security reports can be generated to track security compliance across the data center 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 security posture across their organization.

Solution Components

Check Point CloudGuard for Cisco ACI Gateways

The CloudGuard gateway provides industry-leading advanced threat prevention security and is deployed into the ACI fabric to prevent lateral threat movement between applications inside the data center.

Check Point Smart Center with CloudGuard Controller

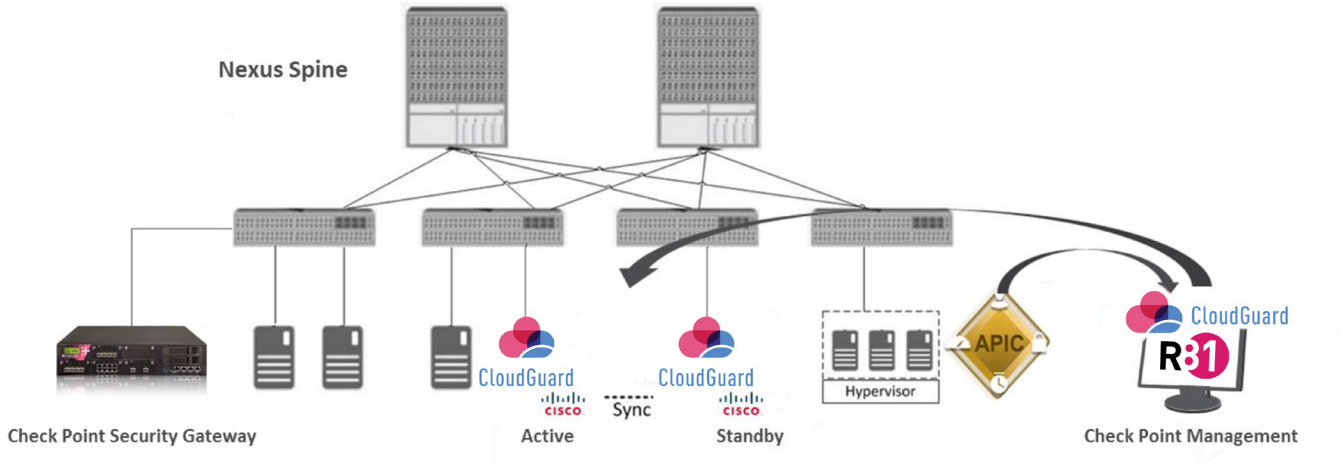
The CloudGuard controller integrates with SDN and cloud controllers like the Cisco APIC. It supports the import of ACI objects, dynamically tracks object changes and allows using ACI objects (EPGs) in the Check Point security policy and logs.

Cisco ACI Fabric and APIC

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

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 ACI End Point Groups (EPGs)
- ACI 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 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



Summary

Check Point CloudGuard Network Security for Cisco ACI delivers accelerated, automated, simplified provisioning and deployment of Check Point's advanced security services in next generation, software defined data centers built on Cisco ACI technology. The CloudGuard integration with Cisco ACI enables customers to have the same level of security for traffic inside the data center as Check Point provides at the perimeter. As a result, customers are able to facilitate better collaboration among security and infrastructure teams while providing full control and visibility across both physical and virtual data center infrastructure.

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 Cisco

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Cisco powers the world's Internet experiences and connects people, processes, data and things to enable innovation that benefits business and society. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.cisco.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