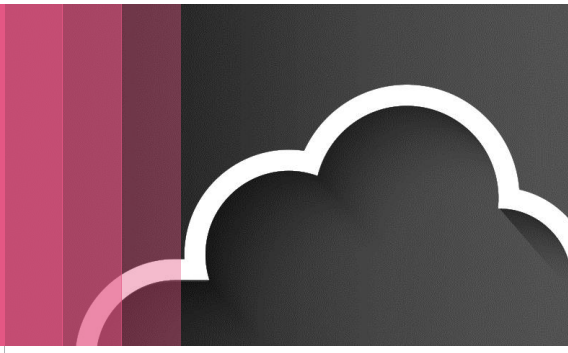
CHECK POINT CLOUDGUARD ADAPTIVE SECURITY FOR PRIVATE AND PUBLIC CLOUDS



EVOLVING TOWARDS PRIVATE CLOUD DATACENTERS

The modern data center is undergoing rapid change. Virtualization is paving the way to the private cloud, enabling applications to be delivered at a fraction of the cost and time. Virtualization separates workloads from hardware for the pooling of resources to be dynamically allocated on-demand. This resource pooling enables the virtualized data center, and is a critical foundation for the Private Cloud. Private Clouds are implemented internally within the corporate firewall, and controlled by the IT department, bringing with them an element of trust that is less inherent in public clouds.

Following these developments is the emergence of a supporting architecture called Software-Defined Networking (SDN), which separates the network control plane from the forwarding plane, enabling a centralized and programmable way to configure, manage, secure and optimize the network.

The next step in this ongoing evolution is the Software-Defined Data Center (SDDC), where all the infrastructure elements - networking, storage, CPU and security – are virtualized and delivered as a service. The entire infrastructure is automated by software, orchestrating user-defined services and integrating security and agility into the data center.

CHALLENGES SECURING THE PRIVATE CLOUD

These emerging technology trends, with their increased agility, flexibility and efficiency, also give rise to new security challenges:

The static security policy: The Private Cloud is a dynamic environment. New applications are instantly deployed, the environment scales up and down, and applications move around the data center. Security services must keep pace with these rapid changes and take into account elastic scaling. This requires automation; otherwise security will either be neglected or become a bottleneck in the process of provisioning applications.

Internal traffic visibility: Private clouds and their mobile workloads mean a shift in data traffic growth inside the virtualized data center. In addition to protecting traffic inside and outside of the data center, security for virtualized networks must also be able to inspect and enforce security policies for traffic moving laterally inside the data center.

Comprehensive security automation and orchestration for Private Cloud/IaaS environments

“Thanks to Check Point, we have a Virtual Security solution that fully integrates into our dynamic virtualized environment with all the performance, security and functionality we expected from our physical Check Point gateways for years”

Luc Steens
Team Leader Security Managed Services, Getronics

Limits of traditional segmentation: Traditionally, security segments have been tightly coupled with the physical network topology. This resulted in exceedingly manual, process-intensive networking configurations. However, deploying security within virtualized environments means these physical boundaries are now logical and automated, adversely impacting static network security processes, contributing to operational overhead and impacting network agility.

Advanced threats: Sophisticated, fifth generation (GenV) cyber-attacks target the weakest systems on the network; they obtain control of the infected machine using a Command and Control (C&C) server, and then move laterally from virtual machine (VM-to-VM) to steal valuable data without ever being detected. The threats are no longer just at the network perimeter; advanced protection is also needed to minimize and mitigate post-breach propagation within the datacener.

SOLUTION OVERVIEW

In order to optimize the benefits of the Private Cloud, security requirements must be addressed in a new way. As enterprises move their network infrastructures to private clouds, it is essential for security to overcome the challenges outlined above and integrate with SDN architectures, network virtualization and orchestration platforms. The solution must be built on five key principles:

1. **Automated security services insertion into the network**. Security service-chaining enables security for all traffic in the data center automatically. Now we can create security policies that implicitly configure the network in the background.

2. **Policy and context-awareness**. Understand the state of the applications and the context by integrating into cloud orchestration and IT tools, like ticketing systems, user directories, and SDN controllers. Learn and apply the best policy based on state and context. This also enables secure, scalable deployments and allows you to grow the number of applications in the data center safely.

3. **Trusted automation and orchestration**. To effectively enable automation, it needs to be trusted. Trust-based APIs enable self-service integrations with third-party systems and automate policy changes within the scope of their privileges. This means administrators can allow changes to specific rules within the policy.

4. **Compliance and threat visibility**. If a compromised virtual machine is detected, it must be quarantined with options for remediation. Reporting and analytics are necessary to uncover and understand traffic trends.

5. **Centralized management**. Security management is simplified with unified administration and monitoring of physical and virtual security gateways, and public IAAS such as AWS, Azure, Google Cloud Platform and more.

Check Point CloudGuard IaaS includes:

- Interoperability with VMware vSphere 5.5, vCenter Server, vCloud Suite & VMware NSX
- Centralized security management for virtual & physical gateways
- Inspection of inter-VM traffic without changing network topology
- Automated deployment of CloudGuard gateways
- Automated protection of new VMs
- Use of SDN-defined objects in Check Point policy
- VM migration without breaking application connectivity & security

ADAPTIVE SECURITY FOR THE VIRTUALIZED DATACENTER

Check Point CloudGuard IaaS security gateways deliver industry-leading advanced threat prevention security to protect dynamic virtual environments from external and internal threats, including those propagating via inter-VM traffic. Comprehensive security protections include; firewall, IPS, anti-bot, anti-malware, a host of other features. Check Point CloudGuard IaaS is also designed to protect communications between applications in the private cloud through tight integration with leading private cloud platform including VMware NSX and Cisco ACI.

Additionally, CloudGuard IaaS supports and protects all popular hypervisors from VMware, Microsoft, KVM and Xen. The solution supports open Application Programming Interfaces (APIs) allowing it to interface with popular SDN solutions such as VMware NSX, Cisco ACI and OpenStack to enable intelligent routing and transparent communication between applications for monitoring traffic.

Tightly integrated with VMware NSX and vCenter as well as the Cisco ACI APIC controller, Check Point CloudGuard gateways adapt to all changes in the virtual environment, providing dynamic and dedicated protection depending on the type of applications, network locations and their levels of risk. What's more, CloudGuard supports automated control of all physical and virtual defenses while maintaining complete separation of duties.

CloudGuard IaaS supports the broadest range cloud environments including all leading public, private and hybrid cloud platforms. Advanced features such as auto-provisioning and auto-scaling along with automatic policy updates ensures security protections keep pace with all changes to your cloud. Additionally, CloudGuard IaaS supports a single unified console for consistent visibility, policy management, logging, reporting and control across all cloud environments.

Automated Security Provisioning for Fast-Scaling Data Center

Elastic scaling security addresses the growing number of applications in the data center. When a new application or server is added to the virtual datacenter, security capacity can now be automatically added to it. Check Point automatically secures newly provisioned VMs as well as migrated VMs without breaking application connectivity. In addition, automatic CloudGuard IaaS deployments instantly secure all VMs on new ESX host members without requiring changes to the virtual network topology.

Centralized Management for Virtual and Physical Gateways

Security management is unified across both physical and virtual systems, allowing IT to set security policies for both environments from one central location. This ensures consistent security across all gateways without the expense of separate management consoles. Check Point security management is also integrated with all leading cloud management solutions. A policy that uses cloud-defined objects, including Security Groups, can be pushed to both Check Point CloudGuard IaaS (for East-West traffic inspection) and to physical Check Point appliances (for North-South traffic inspection).

CloudGuard IaaS supports all leading SDN, SDDC and server virtualization solutions to seamlessly deliver advanced threat prevention security to keep private datacenters free from even the most sophisticated GenV cyber threats.

CHECK POINT DATACENTER SECURITY ARCHITECTURE

Check Point offers an end-to-end security architecture combining high-performance network security devices with real-time proactive protections for North-South and East-West traffic. Our robust architecture provides the flexibility to custom-fit security enforcements in the modern data center while maintaining the flexibility, elasticity and automation virtual environment provide. This portfolio includes:

- **Check Point Data Center Appliances** – Advanced Threat Prevention for North-South traffic
- **Check Point Virtual Systems** – Insulate zones (Production, Integration, R&D, DMZ, Partners) by consolidating multiple virtual security gateways on the same Check Point appliances.
- **Check Point CloudGuard IaaS Private Cloud gateways** – Secure East-West traffic inside the virtual data center and support micro-segmentation. Check Point CloudGuard management integrates with Cloud Orchestration Management platforms such as VMware NSX and vCenter, Cisco ACI, Nokia Nuage and more to allow for security service insertion.
- **Check Point CloudGuard IaaS Public Cloud Gateway** – Securely extend your data center to Public IaaS (AWS, Azure, Google Cloud Platform, Oracle Cloud Infrastructure, Alibaba Cloud, and more) by securing the communication and the Public IaaS workloads.
- **Check Point Security Management** – Unified management for virtual, physical and public IaaS gateways with policy layers and pre-defined policy templates to secure dynamic cloud environments.
- **Check Point Trusted API** – Trusted REST APIs allow automation with granular & scoped privileges.

SUMMARY

Without the proper network security controls, IT organizations simply cannot realize the benefits of a cloud-base infrastructure. Uncormpromised East-West traffic security, automated provisioning and orchestration, and central management for both physical and virtual environments are essential security requirements in the virtualized datacenter. When combined with leading network virtualization platforms, Check Point CloudGuard IaaS provides a simple yet comprehensive solution to secure, manage and automate cloud environments.

Check Point delivers a complete solution for securing both North-South and East-West traffic. With Check Point, you can embrace an entirely new approach to deploying, provisioning and managing a full range of security services. Check Point is committed to protecting the modern data center from advanced attacks and lateral-moving threats across the private cloud environment. IT organizations get all the security they need without compromising any of the benefits of network virtualization.

To learn more about Check Point CloudGuard Private and Public Cloud Security solutions, visit www.checkpoint.com.

CONTACT US

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