Protecting Critical Assets in Public Clouds

Understanding the Shared Responsibility Model

The growth and popularity of public cloud continues to drive more data beyond traditional IT security protections—into data center environments no longer owned, managed or controlled by corporate IT. On-premises IT security controls do not touch the cloud, leaving customer data at risk from the same types of threats targeting assets and applications in corporate data centers. What's more, malware introduced into the cloud can easily propagate among VMs, attack virtual segments or even ride unimpeded over VPN links back to corporate networks.

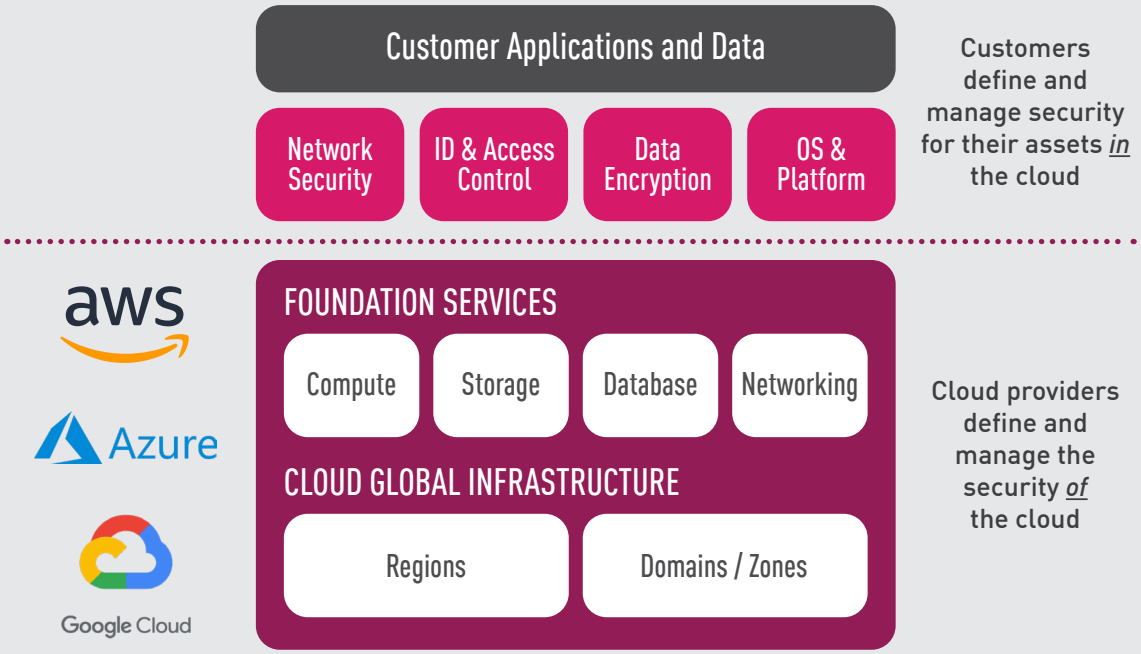
Public cloud networks are built upon a unified, multi-tenant platform utilizing a shared infrastructure to support millions of simultaneous customers world-wide. Foundational to public cloud environments are enhanced security, operational management and threat mitigation practices that protect the infrastructure, cloud fabric, hypervisors, services and tenant environments.

While public cloud providers deliver strong security controls to protect the cloud fabric, they have no knowledge of "normal" customer traffic and thus are unable to determine malicious content from benign. This presents a big challenge to security administrators to provide the same security protections against the latest fifth generation (GenV) cyber-attacks targeting the cloud as they do on-premises. A defense-in-depth strategy for the cloud should also include protecting all workloads and data from exploits, malware and other sophisticated attacks.

KEY PRODUCT BENEFITS

- Fulfill your shared security responsibility in public cloud networks
- Protect all your cloud assets and data from even the most sophisticated threats and malware
- Seamlessly extend the same protections safeguarding your on-premises network to any public cloud environment

© 2023 Check Point Software Technologies Ltd. All rights reserved.



The cloud shared responsibility model defines specific security boundaries for customers and providers.

To fully embrace the cloud, businesses need to understand where the balance of responsibilities lie between protecting the cloud infrastructure (incumbent upon the cloud provider) and protecting the data that resides in the cloud (incumbent upon the customer). This is what public cloud providers refer to as the shared responsibility model.

Fulfill Your Shared Security Responsibility with Check Point CloudGuard

To help customers deal with the security issues that fall under their responsibility, Check Point has partnered with the leading public cloud providers to seamlessly bring the same comprehensive security protections customers enjoy on their premises networks to their cloud environments. Check Point's CloudGuard Network Security solution provides industry-leading threat prevention security to keep customer data in public cloud networks safe from even the most sophisticated attacks. Additionally, Check Point CloudGuard enhances the native segmentation and elastic networking of public cloud environments to dynamically deliver advanced security and consistent policy enforcement that automatically grows and scales with customer environments while providing reliable and secure connectivity across public and hybrid cloud environments.

©2023 Check Point Software Technologies Ltd. All rights reserved.

	Public Cloud Provider Security Controls (AWS, Azure, Google Cloud Platform)	Cloud Security Enhanced with Check Point CloudGuard
Highly Scalable and Available Compute Platform	✓	
Logical Isolation of Customer Workloads through Fabric Controller	✓	
Key Vault for storage of cloud app security keys	✓	
Distributed Denial-of-Service (DDoS) Protection	Protection for cloud platform only	Protection for customer environment
Security groups or logical virtual network segmentation with stateful ACLs	✓	✓
FEDRAMP Authorized (AWS GovCloud, Azure Commercial, Azure Government)	✓	✓ Via platform certifications
Encryption of certain data at rest in cloud	✓	✓
Full support of Automation and Orchestration tools for Security	✓	✓
Virtual Private Network (VPN) connectivity to the cloud	✓	✓
Unified management of VPN connectivity across multiple cloud platforms		✓
Unified Security Management of Public Cloud, Private SDN and Traditional Data Center		✓
Industry-leading Threat Prevention in real time (L4-L7 protections)		✓
Identity-based Authentication Access to Applications within Cloud Workloads		✓
URL Filtering with Integrated and Unified Management		✓
Threat Extraction and Zero-day Sandboxing with Integrated and Unified Management*		✓
File Based Protection that encrypts, tracks and protects Office Documents and PDF files inside AND outside the cloud environment*		✓

** Requires additional Check Point products to enable full protections.*

© 2023 Check Point Software Technologies Ltd. All rights reserved.

Understanding the customer responsibility role versus the role of public cloud providers helps organizations make the best decisions concerning the security of their cloud environments. It also ensures that an organization's cybersecurity strategy efficiently and cost-effectively aligns with the rest of the business goals while delivering consistent protections for all corporate data both on-premises and in the cloud.

Check Point CloudGuard compliments native cloud service provider (CSP) security controls to ensure public cloud customers can fulfill their shared security responsibilities. With Check Point CloudGuard, customers can secure their workloads and applications running in hybrid and public cloud infrastructures, minimizing threats from breaches, data leakage as well as GenV cyber threats. Whether your cloud strategy centers around public or hybrid cloud, VPN replacement, multi-cloud routing, or cloud DMZ, Check Point CloudGuard helps secure all your cloud assets while fully supporting the elastic, dynamic and cost effective nature of the cloud.

What's more, only Check Point gives you a single pane-of-glass experience when managing physical, virtual and cloud-based security, complete with consolidated logs and reporting across all network environments. With Check Point, you can enforce a consistent security policy for corporate assets across both public cloud and on-premises infrastructures, dramatically simplifying compliance with regulatory mandates.

Check Point CloudGuard provides comprehensive threat prevention security, access, identity, strong authentication, compliance reporting and multi-cloud connectivity to help organizations embrace the cloud with confidence. CloudGuard seamlessly integrates with the leading cloud platforms and orchestration tools allowing it to be deployed in minutes while supporting key features such as dynamic security policies and elastic scalability. These powerful capabilities allow you to grow your cloud security elastically with the changing capacity requirements of your dynamic business environment.

For more information, please visit www.checkpoint.com/products/cloud-security/

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555

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

www.checkpoint.com

© 2023 Check Point Software Technologies Ltd. All rights reserved.