CloudGuard Network Security for Google Cloud

Advanced Threat Prevention Security for Public, Private and Hybrid Clouds

Google Public Cloud Security Overview

The wide adoption of cloud is being driven by the desire to transform businesses for greater efficiency, speed, agility, and cost controls. While cloud providers have secured the underlying infrastructure with necessary built-in controls and data isolation needed in multi-tenant environment, they have given enterprises the flexibility to innovate and at the same time the responsibility to protect their data and workloads hosted in the cloud.

Security insertion and management has been a significant hurdle for customers migrating to the public cloud. Organizations struggle to manage disparate security and traffic monitoring solutions for their on-premises and cloud environments, resulting in a lack of consistent policy enforcement that makes regulatory compliance difficult. At the same time, the number of breaches and sophistication of cyber threats continues to increase. Enterprises are challenged with extending the same level of protection and control deployed on-premises to the cloud, leaving them vulnerable to attacks from the Internet. Once an environment is breached, the lateral movement of attacks inside the cloud and externally to corporate networks remains a potential threat. Remote access to the public cloud is another challenge where organizations need to securely connect on-premises applications inside the Data Center with public cloud infrastructure.

Check Point CloudGuard Network Security for Google Cloud delivers comprehensive security tailored to protect public and hybrid cloud environments, allowing businesses to confidently extend their data center applications and workflows to the cloud.

Google Cloud is a secure, dedicated public cloud computing service operated by Google.

The service supports existing workloads and third-party applications as well as new application development, giving IT a common platform for seamlessly extending its data center to the cloud.

Check Point CloudGuard Network Security for Google Cloud delivers advanced, multi-layered security for the Google cloud environment, protecting assets in the cloud from attacks while enabling secure connectivity from enterprise networks to the Google cloud (hybrid networks).

Designed for the dynamic security requirements of cloud deployments, CloudGuard provides advanced threat protections to inspect traffic entering and leaving private subnets in the cloud network. Fully integrated security features include: Firewall, IPS, Application Control, IPsec VPN, Antivirus, Anti-Bot. SandBlast adds Threat Extraction and Threat Emulation for zero-day protections

CloudGuard provides consistent security policy management, enforcement, and reporting, making migration to the Google cloud painless.

Dynamic Threat Prevention Security for Google Cloud

Check Point and Google have partnered to deliver a best-in-class experience for customers looking to extend advanced security protections to their Google public and hybrid cloud environments. Seamlessly integrating with Google Cloud, CloudGuard provides reliable connectivity to public and hybrid cloud assets while protecting applications and data with industry-leading threat prevention. Additionally, CloudGuard dramatically simplifies security management and policy enforcement across private, hybrid, and public cloud networks. As a result, IT organizations can achieve an advanced security posture with consistent visibility that moves with Virtual Applications as they migrate from data centers to Google hybrid cloud environments.

As a Google technology partner, CloudGuard complements Google Cloud security controls to enable customers to easily and seamlessly secure their assets in the cloud.

Complete Visibility and Control

CloudGuard for Google Cloud gives businesses the confidence to securely extend their data center resources and workloads to public clouds, providing tangible customer benefits including:

- Protection against security breaches and malware in the public cloud that may lead to private cloud /data center breaches

- High availability and scalability with Cloud Load Balancers and multiple zones/regions which enables security that grows with an elastic environment and changing business requirements

- Unified security management across on-premises and cloud workloads, improve visibility and automated dynamic security policies integrating Google Cloud Objects into logs and reports

- Automated workflows and orchestration to minimize configuration errors for increased agility and reduced operational costs

- Elimination of the costs and loss of reputation associated with business disruptions and downtime

- Migrate sensitive workloads, applications and data to the public cloud with confidence while maintaining compliance

Comprehensive Security Protections

CloudGuard for Google Cloud provides industry-leading threat prevention security to keep Google Cloud 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 Google Cloud networks and the Enterprise network
- **Remote Access** allows remote users to connect to Google Cloud environments 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

Lateral threat prevention inside the public cloud can be achieved using the appropriate networking configuration to redirect internal traffic to the CloudGuard gateway for inspection.

Centralized Management of On-premises and Public Cloud Infrastructures

Policy management is simplified with centralized configuration and monitoring of cloud and on-premises security from a single console. This ensures that the right level of protection is applied consistently across both hybrid cloud and physical networks. Hybrid cloud workload traffic is logged and can be easily viewed within the same dashboard as other logs.

The Check Point Smart Dashboard provides real-time visibility into activity that spans the data center to the Google public cloud

Consolidated Logs and Reporting

CloudGuard for Google Cloud gives organizations complete threat visibility and enforcement for hybrid cloud infrastructures. Check Point SmartEvents software consolidates monitoring, logging, and reporting across cloud and on-premises networks. SmartEvent logs can also be exported to 3rd party SIEM platforms. Enhanced logging, forensics, and reporting that leverages Google Cloud defined objects improves visibility into the hybrid cloud.

Security reports specific to cloud workload traffic can be generated to track security compliance across the hybrid cloud network, simplifying reporting and audits and making it easy to demonstrate compliance with industry regulations. Security administrators get a holistic view of their security posture across the entire organization via a single dashboard.

Rapid and Flexible Deployment

Easily and affordably extend security to your Google public cloud using rapid one-click deployment of the CloudGuard gateway which is available in the Google Cloud Launcher delivered using on-demand per-hour (PAYG) or Bring Your Own License (BYOL) options. Customize security protections to your specific business needs using Check Point Software Blade Technology.Quickly deploy and provision CloudGuard using Google Cloud Deployment Manager templates. Context sharing of security groups is maintained so that any changes or new additions are automatically tracked without the need for administrator intervention.
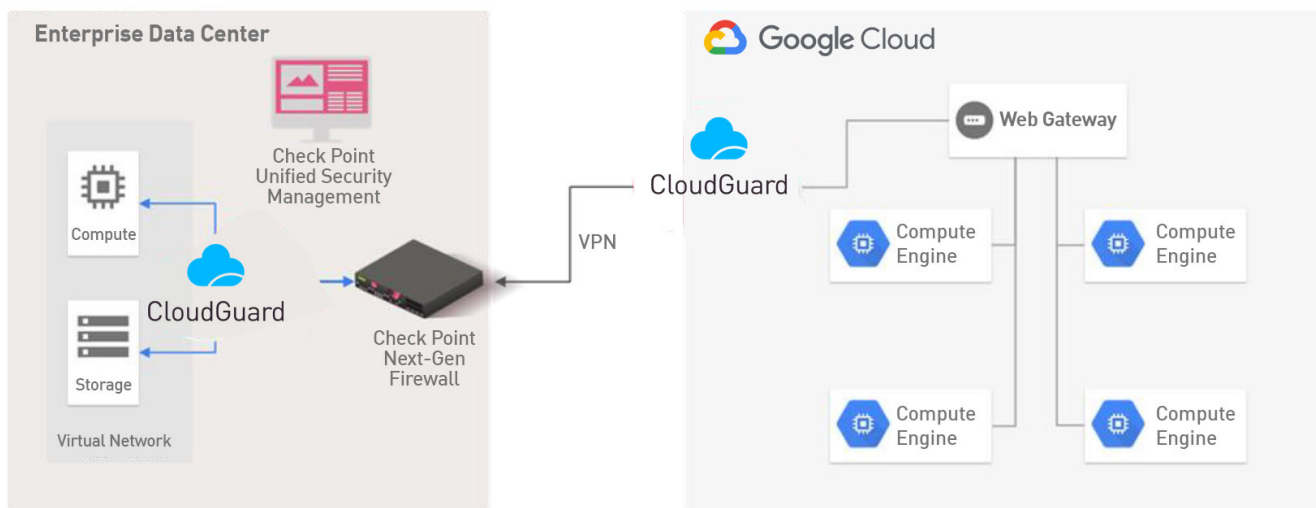
Unified policy management and security that follows VMs as they migrate from the data center to Google Cloud networks

Summary

Check Point Software Technologies provides uncompromising protection against all types of cyberattacks while dramatically simplifying IT security management. Check Point CloudGuard Network Security for Google Cloud takes advantage of the cost efficiencies and automation of Google Cloud while tightly integrating advanced security features designed to meet the efficiency and scalability requirements of large deployments in the public cloud.

Check Point CloudGuard for Google Cloud enables customers to confidently extend security to their Google Cloud infrastructure with the full range of protections of the Check Point threat prevention architecture. CloudGuard for Google Cloud prevents network attacks and data breaches while enabling secure connectivity to Google multitenant environments. CloudGuard also integrates with a wide variety of public cloud and private cloud environments.

To learn more about how Check Point CloudGuard and Google Cloud provides advanced security protections forpublic and hybrid cloud networks, download a free trial of CloudGuard for Google Cloud at www.checkpoint.com or contact your Check Point or Google partner or sales representative.

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 100,000organizations of all sizes.

About Google Cloud

Google Cloud (cloud.google.com)is a suite of public cloud computing services offered by Google (www.google.com) including a range of hosted services for compute, storage and application development that run on Google hardware that are used by software developers, cloud administrators and enterprise IT professionals. Google is a leading public cloud computing services provider, delivering a highly reliable, scalable, low-cost computing platform in the cloud that powers thousands of businesses around the world. With a global presence, customers across all industries are using Google's cloud computing platform to launch applications across a wide variety of use cases taking advantage of the following benefits offered by Google Cloud: low cost, performance, agility, high availability, security, openness and global footprint.