CHECK POINT | Google

CloudGuard

CloudGuard Network Security for Google Cloud

Hybrid Mesh Firewall for Dynamic Cloud Environments

AI-powered Threat Prevention and Unified Security Management

Security insertion and management have been significant hurdles 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, often leaving them vulnerable to sophisticated attacks from the Internet. Once a cloud network is breached, the lateral movement of attacks inside the cloud and externally to corporate networks is a major 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.

As the number of cloud networks grows, managing security becomes time consuming and error prone. It also becomes more complex and costly to manage. Each cloud vendor has their own network, virtualization, and load balancing mechanisms that security engineers must learn. Through API and software integration, Check Point unifies network security and policy management across all networks no matter where they are. This simplifies security operations and reduces risk from human error.

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 Google 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 hybrid mesh firewall security protecting cloud assets from attacks while enabling secure and scalable connectivity to Google Cloud.

Designed for the dynamic security requirements of cloud deployments, CloudGuard provides advanced threat protection and deep packet inspections for all traffic entering and leaving private subnets in Google Cloud. Fully integrated security features include Firewall, IPS, Application Control, IPsec VPN, Antivirus, Anti-Bot, Threat Extraction and Threat Emulation for zero-day protection. CloudGuard also provides consistent policy management, enforcement, and reporting, simplifying migration and security operations for Google Cloud environments.

AI-Powered Threat Prevention for Google Cloud

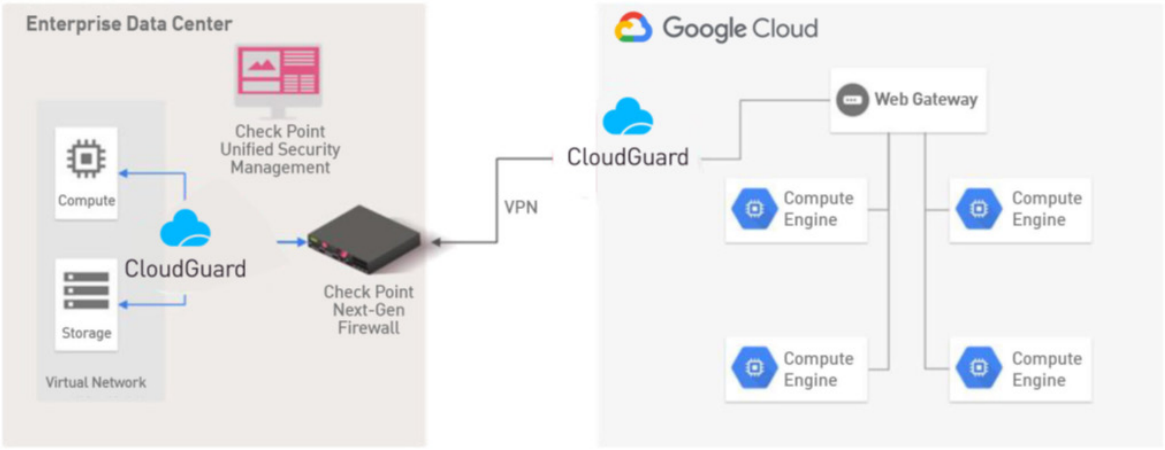
Check Point and Google have partnered to deliver a best-in-class experience for customers looking to extend advanced security protections to their Google public and hybrid cloud environments. Seamlessly integrating with Google Cloud, Check Point CloudGuard provides reliable connectivity to public and hybrid cloud assets while protecting applications and data with industry-leading automation, access control, and 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, Check Point complements Google Cloud security controls and technologies to enable customers to easily and seamlessly secure their assets in the cloud.

Complete Visibility and Control

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

- **Protection against security breaches and malware** in public cloud networks that may lead to private cloud or data center attacks
- **High availability and scalability** with Google Cloud Load Balancers and multiple regions/zones ensures efficient and comprehensive security for elastic environments 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** 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



Unified policy management and security that follows VMs as they migrate from the data center to Google Cloud networks

Comprehensive Security Capabilities

CloudGuard for Google Cloud provides industry-leading threat prevention and lowest false positives to keep Google Cloud networks safe from even the most sophisticated evasion 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 prevent 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
- **Zero-Day Protection** threat emulation and redmediation 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 Any Network, Anywhere

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.

Consolidated Logs and Reporting

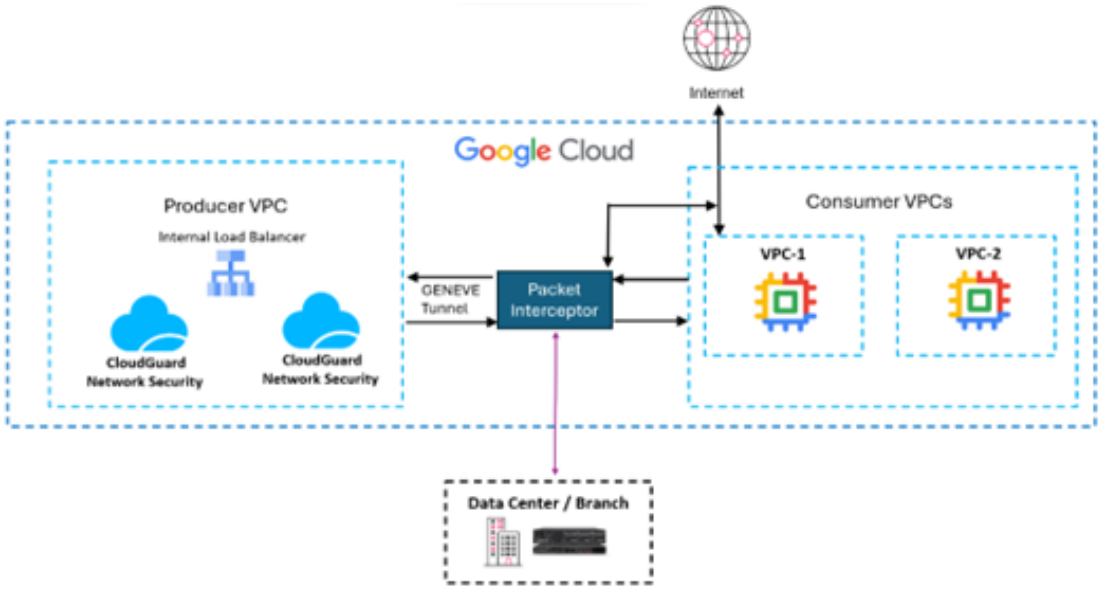
CloudGuard Network Security for Google Cloud gives organizations complete threat visibility and enforcement for hybrid cloud infrastructures. Check Point SmartEvents consolidates monitoring, logging, and reporting across cloud and on-premises networks. SmartEvent logs can also be exported to 3rd party 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 In-Band 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. Quickly deploy and provision CloudGuard firewalls using Terraform-based Infrastructure Manager templates. Network security policies can auto-adapt based on security groups so new assets are automatically given the correct security policy eliminating the need for human intervention, reducing operating costs and chance for error.

Check Point also supports Google Cloud Network Security Integration. This integration leverages Generic Network Virtualization Encapsulation (GENEVE) tunneling technology to securely deliver traffic to CloudGuard Network Security in-band inspection gateways and firewalls while preserving original packet integrity, ensuring both security and performance. The integration delivers exactly what is needed by network security teams seeking to economically secure network traffic without impacting performance.



All network traffic flows: ingress, egress, north-south and east-west, go through in-band deep packet inspection

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 public cloud.

CloudGuard Network Security 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 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 providing future flexibility and choice.

To learn more about Check Point advanced security protection for public and hybrid cloud networks, start a free trial of CloudGuard Network Security for Google Cloud, request a live demo, or contact your Check Point, Google, or partner sales representative.

About Check Point

Check Point Software Technologies Ltd. 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 Google Cloud

Google Cloud is a suite of public cloud computing services offered by Google 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.