

# CloudGuard Network Security on AWS

*Advanced Threat Prevention for AWS  
and Hybrid Clouds*



## Public Cloud Security Overview

The wide adoption of cloud architectures is being driven by the desire to transform businesses for greater efficiency, speed, agility, and cost controls. While cloud solutions offer many advantages over traditional IT infrastructure, legacy security approaches do not address the dynamic nature of cloud environments, and can expose organizations to a new set of security risks.

Security insertion and management is a significant challenge for the cloud. Organizations struggle to manage disparate security solutions for their premises and cloud environments, resulting in a lack of consistent policy enforcement that makes regulatory compliance difficult. At the same time, the frequency and sophistication of threats continues to increase. Security solutions protecting premises-based environments do not extend to the cloud, leaving them exposed and making them attractive targets for cyber criminals. Once a cloud environment is breached, attacks are able to spread laterally from instance to instance within the cloud and even extend externally to corporate networks.



### KEY PRODUCT BENEFITS

- Amazon Web Services (AWS) is a secure, dedicated cloud computing service. 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.
- CloudGuard Network Security on AWS delivers advanced, multi-layered security for the AWS cloud environment, protecting assets in the cloud from attacks while enabling secure connectivity from enterprise networks to the AWS cloud.
- Designed for the dynamic security requirements of cloud deployments, CloudGuard IaaS provides advanced threat protections to inspect traffic entering and leaving private subnets in the VPC. 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 AWS cloud painless.

CloudGuard Network Security on AWS delivers comprehensive security tailored to protect AWS, hybrid-cloud and on-premises cloud environments, so businesses can feel confident about extending their data center applications and workflows to the cloud.

## Advanced Threat Prevention for AWS cloud environments

Check Point and AWS have collaborated to deliver a best-in-class experience for customers looking to extend advanced security protections to their AWS public and hybrid environments. Supporting the AWS cloud infrastructure, CloudGuard provides reliable and secure connectivity to cloud assets while protecting applications and data with industry-leading threat prevention. Additionally, CloudGuard helps organizations by dramatically simplifying security management and policy enforcement across hybrid and public cloud networks. As a result, IT organizations can achieve an advanced security posture that moves with Virtual Applications as they migrate from data centers to AWS cloud environments.

## Complete Visibility and Control for AWS environments

CloudGuard Network Security on AWS gives businesses the confidence to securely extend their data center resources and workloads to AWS cloud, providing tangible customer benefits including:

- Protection against security breaches, malware, and zero-day attacks in the public cloud that may lead to hybrid cloud / data center breaches
- Unified security management, visibility, and reporting across both hybrid and AWS networks
- Elimination of the costs and loss of reputation associated with business disruptions and downtime
- Securely migrate sensitive workloads, applications and data to the cloud

## Comprehensive Security Protections

CloudGuard Network Security on AWS provides industry-leading threat prevention security to keep AWS cloud networks safe from even the most sophisticated attacks. Fully integrated security protections include:

- Firewall, Intrusion Prevention System (IPS), Antivirus, and Anti-Bot technology protect workloads in the cloud from unauthorized access and malicious network attacks
- IPSec VPN allows secure connectivity over a dedicated and encrypted tunnel between AWS Virtual Private Cloud (VPC) and the enterprise network
- Remote Access allows remote users to connect to AWS clouds 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 zeroday attacks

Lateral threat prevention internal to the AWS cloud can be achieved using the appropriate networking configuration to redirect traffic to the CloudGuard Network Security 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.



*Check Point unified security management provides real-time visibility into activity that spans the data center to the AWS cloud*

## Cloud-native integration with multiple AWS services

Check Point is an APN Advanced Technology Partner with Networking and Security Competencies.

Designed for the dynamic security requirements of cloud deployments, CloudGuard Network Security is cloud-native: it seamlessly integrates with native AWS controls to enable rapid deployment, while supporting network segmentation, auto-scaling and high availability across multiple Availability Zones.

CloudGuard Network Security on AWS integrates with a broad range of AWS services, including Amazon GuardDuty, Amazon CloudWatch, AWS Security Hub, AWS Gateway Load Balancer, AWS Traffic Mirroring, AWS Transit Gateway, AWS CloudTrail, VPC Ingress Routing and VPC Flow Logs.

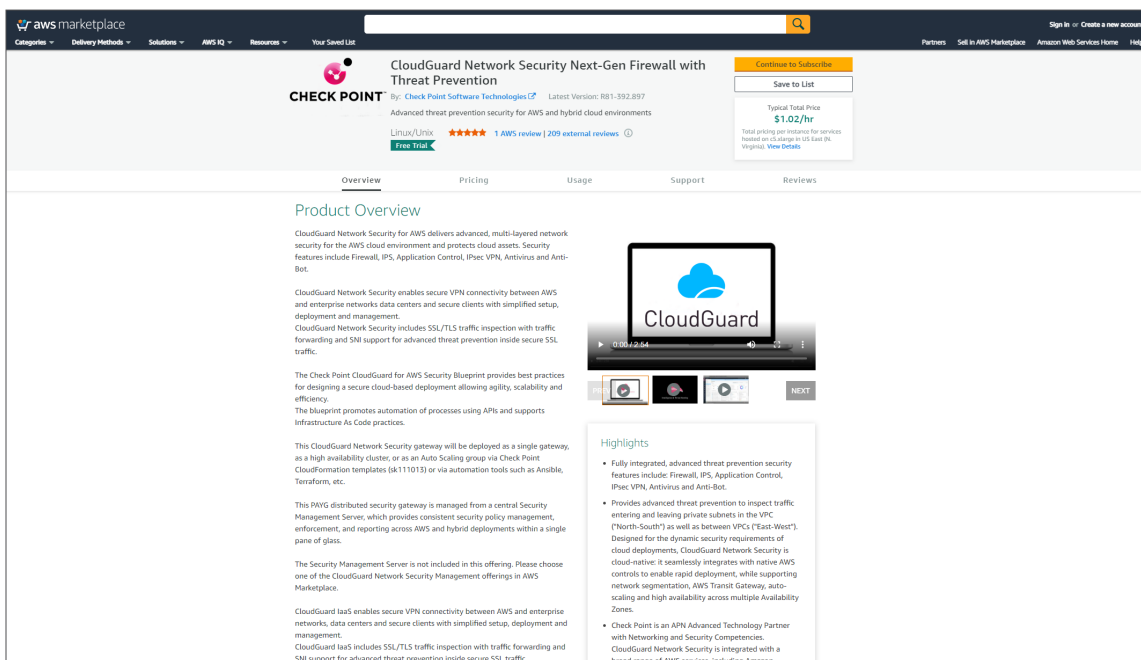
## Consolidated Logs and Reporting

CloudGuard Network Security on AWS environments gives organizations complete threat visibility and enforcement for hybrid cloud infrastructures. Check Point SmartEvent software consolidates monitoring, logging, and reporting across cloud and on-premises networks. SmartEvent logs can also be exported to 3rd party SIEM platforms.

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. 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 their security posture across the entire organization.

## Rapid and flexible deployment

Easily and affordably extend security to your Amazon cloud using rapid one-click deployment of CloudGuard Network Security, available in [AWS Marketplace](#) in on-demand per-hour (PAYG) or Bring Your Own License (BYOL) options. Rapidly deploy and provision CloudGuard using AWS CloudFormation templates and quickly customize security protections to your specific business needs using Check Point advanced threat prevention suite of security technologies.

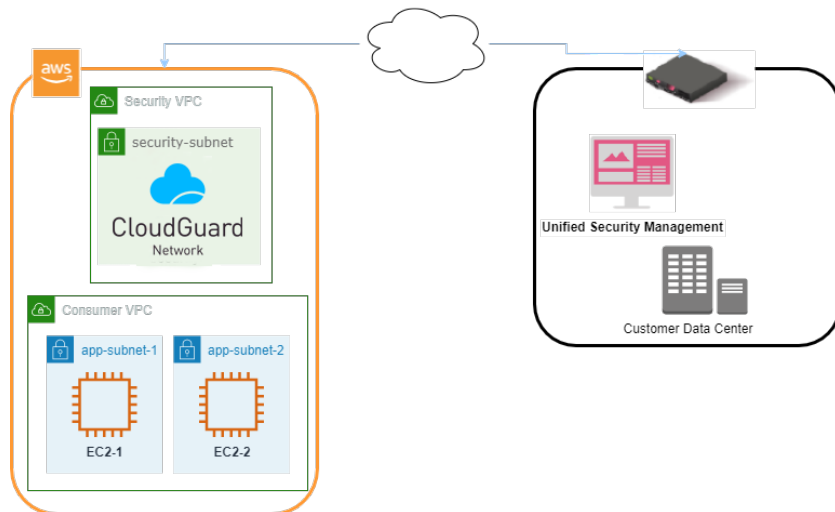


*Check Point CloudGuard Network Security gateway, available on AWS Marketplace*

CloudGuard Network Security is also available in [AWS Quick Starts](#) to help deploy CloudGuard quickly and easily, based on AWS best practices for security and high availability.



**AWS Quick Starts**



*Unified policy management and security that follows instances as they migrate from the data center to AWS 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 on Amazon Web Services for Amazon Web Services takes advantage of the cost efficiencies and automation of AWS while tightly integrating advanced security features designed to meet the efficiency and scalability requirements of large deployments in the AWS cloud.

CloudGuard Network Security for AWS environments enables customers to confidently extend security to their AWS cloud infrastructure with the full range of protections of the Check Point Infinity threat prevention architecture. CloudGuard Network Security for AWS environments prevents network attacks and data breaches while enabling secure connectivity to AWS cloud environments.

To learn more about how CloudGuard Network Security provides advanced security protections for AWS and hybrid cloud networks, deploy a free trial of CloudGuard Network Security for AWS environments from the AWS Marketplace, or contact your Check Point or AWS partner or sales representative.

### Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

### U.S. Headquarters

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

[www.checkpoint.com](http://www.checkpoint.com)