



CREATING A DEVSECOPS CULTURE IN YOUR COMPANY



Available in
AWS Marketplace

Table of Contents

Introductions	2
Challenges	3
The Shared Responsibility Model.....	5
Check Point CloudGuard on AWS	6
• Features	7
• What it Does	9
• Benefits	10
• How it Works	12
Xero Case Study.....	15
Resources/Next Steps.....	17

CREATING A DEVSECOPS CULTURE IN YOUR COMPANY

Introduction

Companies looking to adopt a cloud architecture are doing so for the opportunity to transform their business into one that is agile, scalable, and cost-efficient. Cloud solutions offer many advantages over traditional on-premise infrastructure, but legacy security solutions do not address the dynamic nature of cloud environments and can expose organizations to new security risks.

Furthermore, compiling a number of disparate security solutions can not only expose environments to bad actors internally and externally, but can also slow down the development of new products and security response times.

Companies pursuing methods of securing their apps and data need to find solutions that take into account both on-premise and cloud-based environments. In doing so, these companies can better comply with regulatory requirements, enforce consistent policy, and proactively defend against cyber attacks.

This is why many companies are switching to a DevSecOps approach to combat the obstacles they face with infrastructure and data security. At its core, DevSecOps means **every stakeholder in the software development lifecycle is responsible for security**. A DevSecOps approach is more critical than ever because software development is no longer a siloed part of the company; it affects every part of a business.

Check Point Software Technologies provides solutions that protect customers from cyber attacks, malware, and other threats. For over 28 years, Check Point has helped over 100,000 organizations of all sizes protect their environments. Check Point offers comprehensive infrastructure security with its Infinity architecture across network, cloud, mobile, and endpoint, which provides the highest level of threat prevention against both known and unknown targeted attacks, as well as intuitive security management.

IN THIS EBOOK WE WILL COVER:

- The Shared Responsibility Model and how to fulfill your part of it
- Check Point CloudGuard Network Security on AWS, Check Point's comprehensive security solution that seamlessly integrates with your infrastructure
- The story of how CloudGuard is helping Xero expand rapidly without compromising compliance or security

A hand is holding a bright red life preserver. Through the circular opening in the center of the life preserver, a person is seen struggling in the ocean, with white-capped waves crashing around them. The background of the entire image is a soft, out-of-focus view of the ocean under a bright sky.

CHALLENGES

There are a number of hurdles that can slow down your cloud adoption journey

CHALLENGES

Non-Transferrable Security:

On-premise network security solutions don't translate well to cloud architectures

Speed over Security:

Sacrificing security for speed and agility

Slow Processes:

Legacy solutions slow down developer processes

Inconsistent Protection:

Using disparate protections and solutions making it difficult to manage

Lateral Threats:

Facing lateral spread of threats with new generation of cyber attacks

Sophisticated Threats:

Threats and malware are becoming increasingly sophisticated

Lacking a Consolidated View:

Need greater visibility across the entire organization, on-premise and in cloud



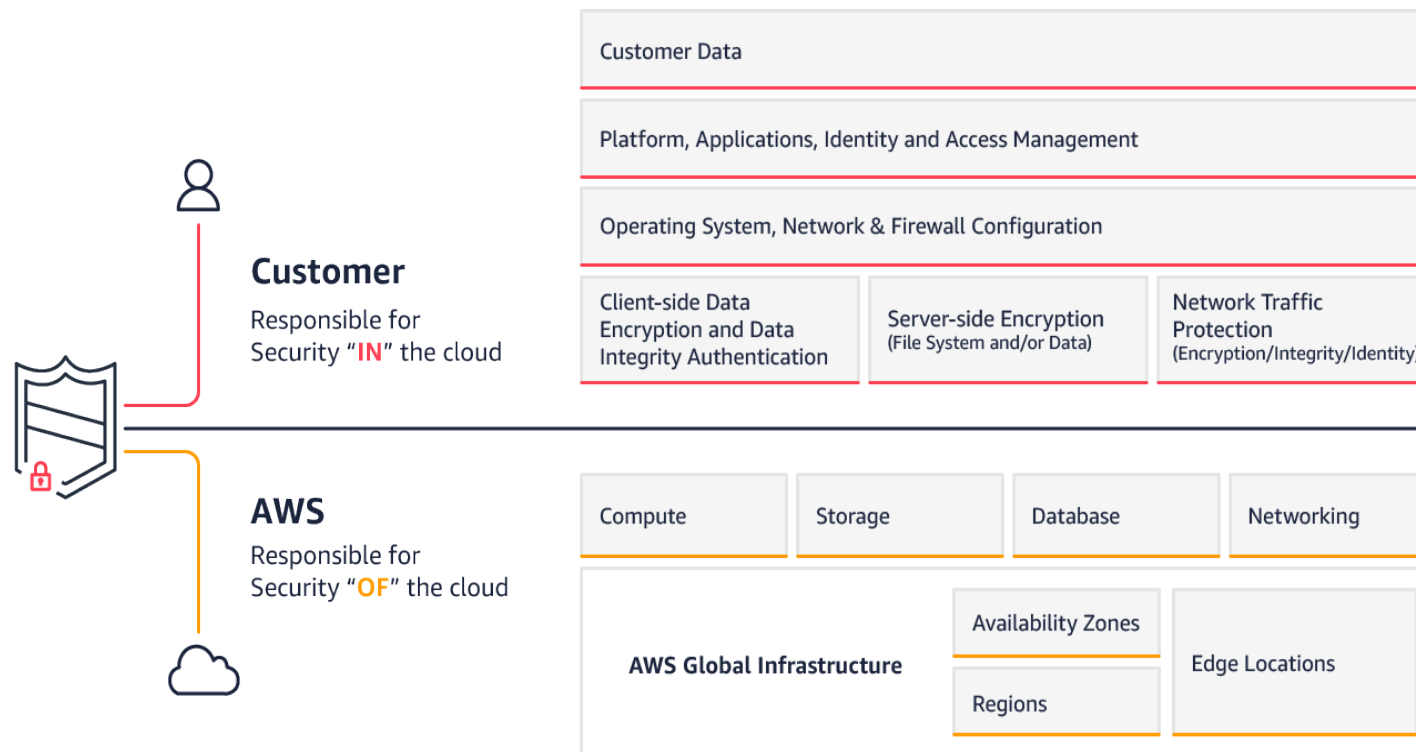
The Shared Responsibility Model

Security and compliance is a shared responsibility between Amazon Web Services (AWS) and you. Although AWS is responsible for the security **of the cloud**, you are responsible for the security **in the cloud**.

It is imperative to carefully choose how you will secure your data on AWS, and make sure you pick a solution that has the flexibility and security you need.

Holding your end of the Shared Responsibility Model can be difficult for a number of reasons. Strongly securing integral parts of your business such as customer data, the operating system, and applications could mean hiring full time in-house experts. This could increase your operational costs or take budget away from creating products and business value. However, solutions like Check Point CloudGuard can make fulfilling your part of the Shared Responsibility Model easier.

THE SHARED RESPONSIBILITY MODEL: CUSTOMER VS. CLOUD PROVIDER



Check Point CloudGuard on AWS

Adopting public cloud infrastructure means security is now shared between you and your cloud provider. Check Point CloudGuard on AWS delivers automated and elastic security to keep assets and data protected while staying aligned to the dynamic needs of public cloud environments.

Check Point CloudGuard on AWS offers the same robust protections that we provide for on-premise environments. Check Point has been developing security solutions for the last 28 years. This allows you to confidently extend your applications and workflows to the cloud, protect them, and connect to them securely, without sacrificing go-to-market speed, agility, or high quality customer experiences.



FEATURES

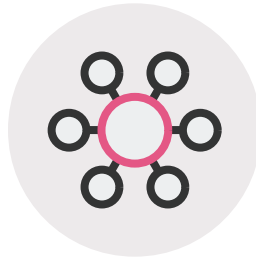


FEATURES



AUTOMATED & AGILE

Auto-provisioning and auto-scaling, along with automatic policy updates, ensures security protections keep pace with all changes to your cloud.



UNIFIED MANAGEMENT

Single unified console delivers consistent visibility, policy management, logging, reporting, and control across all cloud environments and networks.



ANY CLOUD, ANYWHERE

Support for the broadest range of cloud infrastructures, including: AWS, VMware Cloud on AWS, and more.

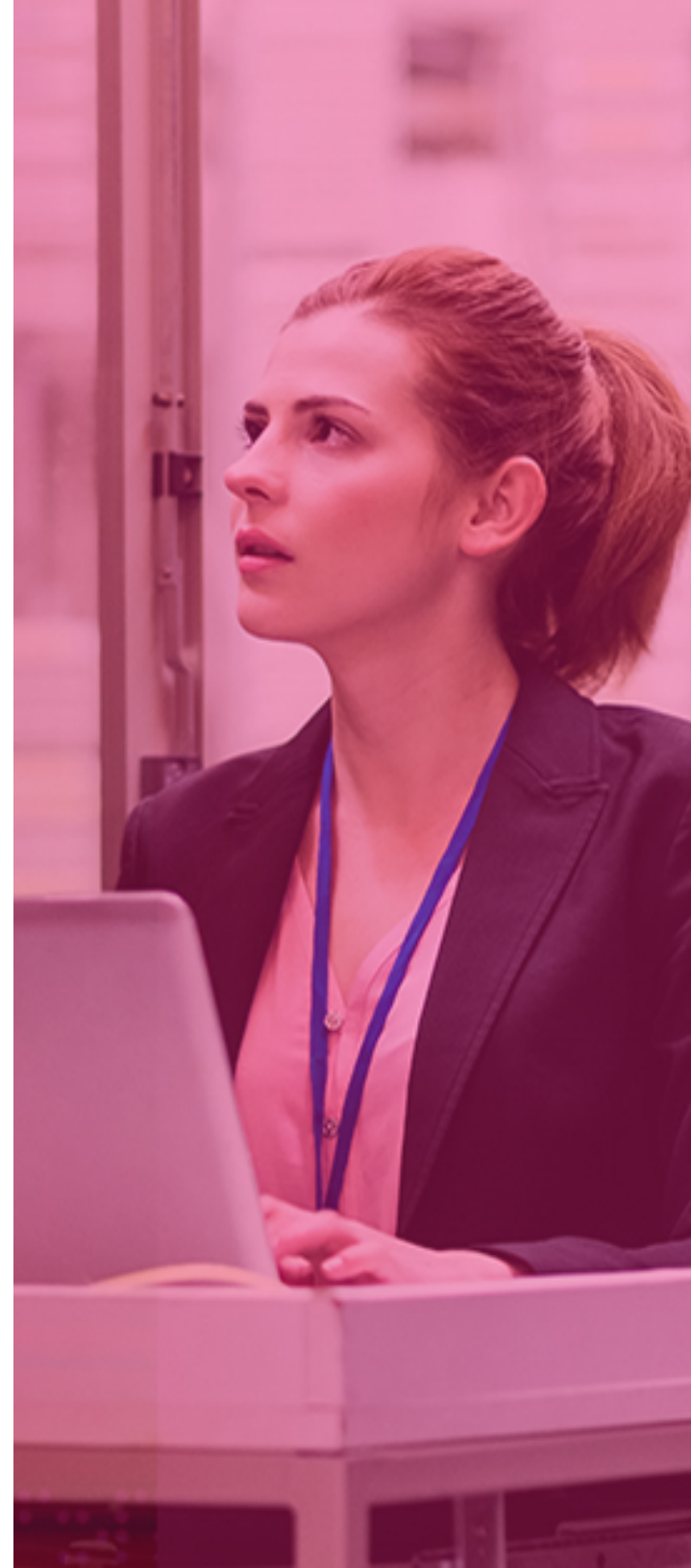
What CloudGuard Does

Check Point CloudGuard on AWS extends its comprehensive enterprise-grade security to AWS, including:

- Zero-day threat protection
- HTTPS inspection
- Intrusion prevention system (IPS)
- Complete application and identity awareness

CLOUDGUARD ALSO:

- Protects your assets on the cloud from attacks while enabling secure connectivity; lets you enforce consistent security policies across your entire organization.
- Integrates with Amazon GuardDuty to provide a self-service, automatic and adaptive solution that detects and prevents malicious activity in real time.
- Reports Security Gateway statistics as metrics to Amazon CloudWatch, which can be used to monitor Gateway health as well as trigger auto scale events.
- Provides a library of CloudGuard CloudFormation templates (CFTs) to simplify deployment.

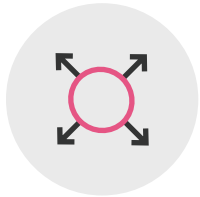


A person is lying on their back on a wooden deck, holding a smartphone in their hands. They are wearing a light blue long-sleeved shirt and blue pants. The background is a bright sunset or sunrise with a warm orange and yellow glow. The word "BENEFITS" is written in large, black, sans-serif capital letters on the right side of the image.

BENEFITS

Bringing DevOps and security together for
better and safer business outcomes

BENEFITS



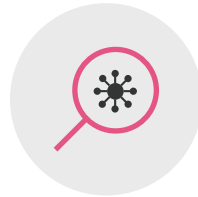
FAST DEPLOYMENT

Use single-click deployment from AWS Marketplace, automated AWS CloudFormation templates, and AWS QuickStart to get started with Check Point quickly.



AGILE

Use automation, orchestration, auto scaling, and integration tools for security as well as DevOps.



THREAT PREVENTION

Leverage the Check Point Infinity Architecture that protects against Gen V mega-cyber attacks and threats across all networks and platforms.



ROBUST SECURITY

Secure all traffic between applications inside your AWS environment and across your hybrid environments. Comprehensive protections include next generation firewalls and zero-day protections.



EASY TO MANAGE

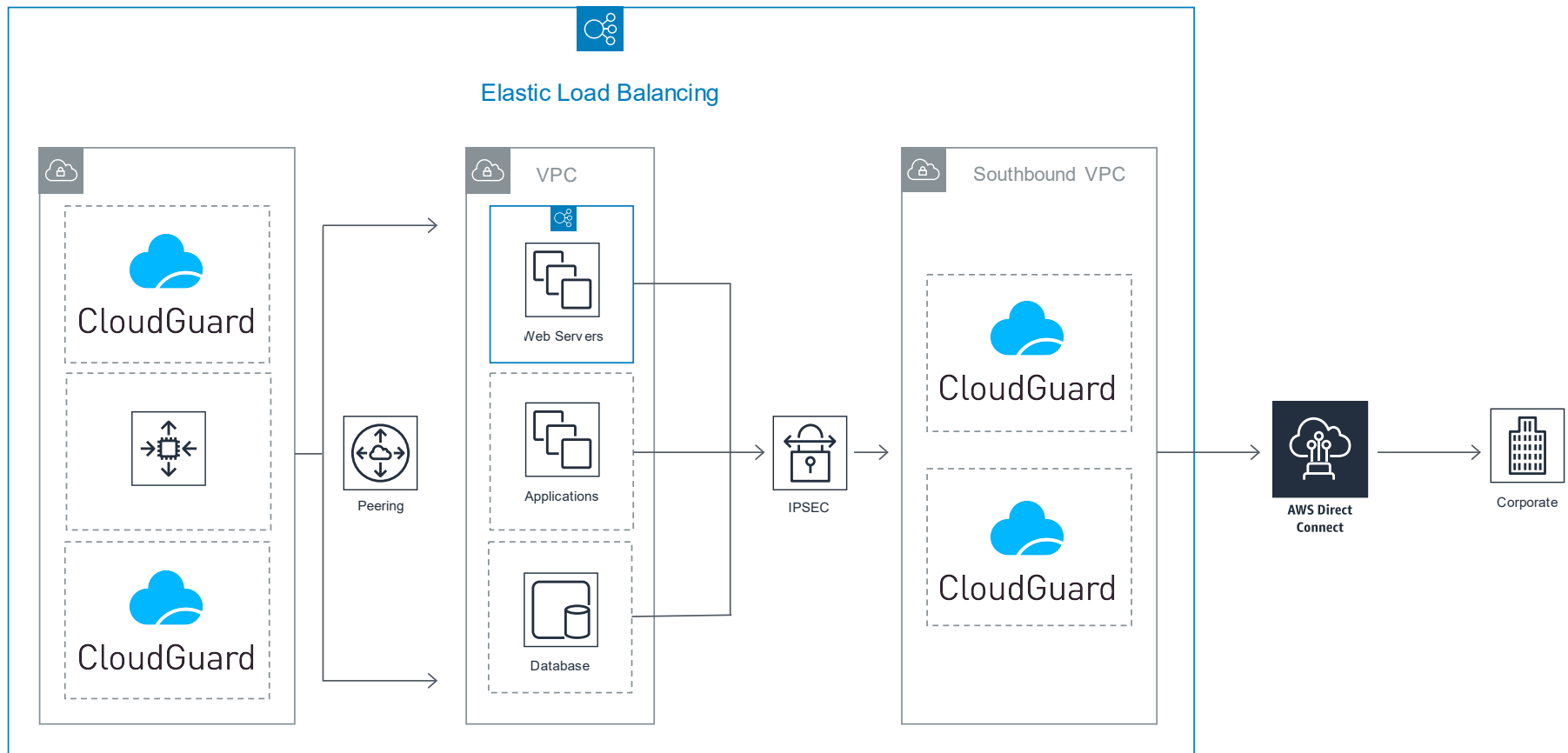
Gain automated security, unified management, consolidated logging, and consistent reporting across all clouds.

HOW IT WORKS



HOW IT WORKS

This best-practices approach allows an organization to take advantage of AWS with its notable benefits (e.g. agility, elasticity, and efficiency), allowing the organization to maintain security controls and visibility as well as safeguard the environment's health.



HOW IT WORKS

This transit VPC architectural concept is based on a “hub and spoke” model where all spokes are connected to a central broker (hub) and all traffic to and from the spokes traverses through the broker.

CloudGuard Network Security also supports AWS Transit Gateway and AWS Gateway Load Balancer.

The **northbound hub** is used for monitoring and controlling traffic arriving into the environment from the Internet. This is used mainly for exposing services in the environment to the public.

The traffic in the northbound hub is usually web-based {HTTP/S}, prompting deployment of the northbound hub with the CloudGuard auto-scaling solution. It enables flexibility in terms of supporting the business through performance fluctuations, achieving business availability through growing business demand, and efficient operational cost when demand rises.

The **southbound hub** is used to monitor and control traffic in the following flows:

- East-west traffic inside of the environment (between spoke VPC's)
- Inbound/outbound, to/from on-premise network
- Outbound access to the Internet (e.g. for software updates)

Spoke VPCs are connected to the southbound VPC via IPsec tunnels, utilizing route-based VPN connectivity. IPsec endpoints on Spoke VPCs are done using AWS Virtual Private Gateways (VGWs).

In the northbound VPC, the AWS CFT deploys an auto scaling group and an internal load balancer, serving the published applications in the spoke VPCs. Elastic Load Balancing (ELB), Network Load Balancer {NLB}, or Application Load Balancer (ALB) may be deployed as an external load balancer to the environment. In the southbound VPC, the AWS CFT deploys two security gateways in separate Availability Zones (AZs) to serve the spoke VPCs in high availability mode.

A woman with curly hair, wearing a dark jacket, a red scarf, and denim shorts, is captured mid-jump over a large rock on a hilltop. She is smiling and has her right hand raised. The background shows a cityscape under a bright, hazy sky with a lens flare effect.

Case Study: Xero

**“CHECK POINT AND AWS HAVE
RELEASED XERO FROM THE
CONSTRAINTS OF TRADITIONAL
MANAGEMENT AND SECURITY
PRACTICES.”**

—Aaron McKeown, Head of Security
Engineering and Architecture, Xero

How Xero Transformed Their Business

Xero leveraged Check Point CloudGuard on AWS to embrace DevOps and modernize their application lifecycle.

CHALLENGES

Xero needed to build an agile and responsive infrastructure to support the next wave of growth, where the systems could scale up and down depending on market demands and an environment where infrastructure build times could be cut from weeks to days and hours to minutes. This new environment was planned to not only maintain, but also improve security.

OPPORTUNITIES

- Modernize application infrastructure to enable rapid innovation
- Adopt a DevSecOps culture to facilitate product and security team collaboration
- Build for global scale

QUICK FACTS ABOUT XERO:

- 1,400,000+ customers
- 2,000+ staff
- 1+ trillion transactions in last year

PROCESS

- Ignite active collaboration between Xero, Check Point, and AWS to build next generation architecture
- Implement greater visibility and control with DevOps teams
- Create a DevSecOps culture in the organization

OUTCOMES

- A culture of security across their organization
- DevSecOps teams with greater visibility and control
- Increased agility and the ability to scale, allowing them to expand rapidly and build better platforms at quicker rates
- The ability to do more with less, resulting in cost savings, faster growth and the achievement of new customer milestones

Resources and Next Steps

- [Check Point CloudGuard Network Security](#)
- [Check Point CloudGuard on AWS – Solution Brief](#)
- [Check Point CloudGuard on AWS Quick Start](#)
- [Check Point CloudGuard on AWS – Security Blueprint](#)
- [Check Point CloudGuard on AWS- Free Trial](#)
- [Video on Secure Transit VPC](#)
- [CloudGuard on AWS Transit VPC Deployment Guide](#)

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

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, endpoint 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.

For a free security assessment or trial, please contact: US Sales: +1-866-488-6691 International Sales: +44-203-608-7492

CONTACT US

Worldwide Headquarters

Check Point Software Technologies Ltd.
5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: +972-3-753-4555

U.S. Headquarters

Check Point Software Technologies, Inc.
959 Skyway Road, Suite 300
San Carlos, CA 94070 USA
Tel: +1-800-429-4391

