Check Point
SOFTWARE TECHNOLOGIES

AUTOMATE YOUR CLOUD COMPLIANCE JOURNEY IN 6 STEPS

TABLE OF CONTENTS

INTRODUCTION

Securing cloud environments is different from securing traditional data centers and endpoints. The dynamic nature of the cloud requires continuous assessment and automation to avoid misconfigurations, compromises, and breaches.

It can also be difficult to gain complete visibility across dynamic and rapidly changing cloud environments — limiting your ability to enforce security at scale. On top of these challenges, cloud governance is critical to maintain compliance with regulatory requirements and security policies as they evolve.

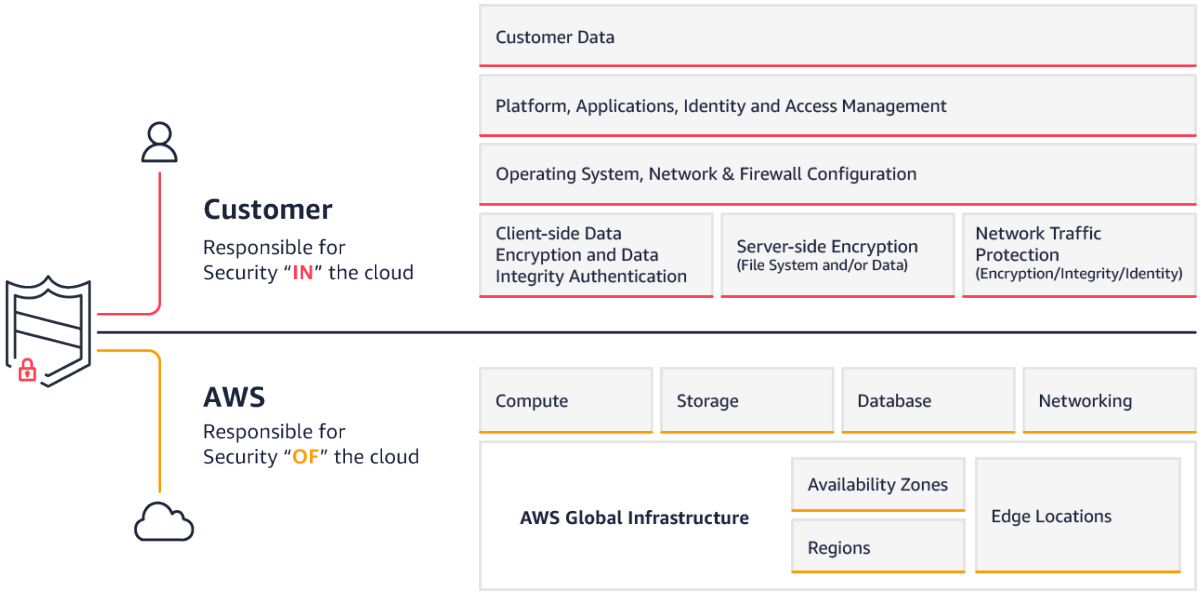
Because cloud deployments are not just implemented once and left untouched, organizations need to consider how to integrate security into their CI/CD pipeline and software development lifecycle. Implementing a security solution that addresses cloud challenges requires deep security and cloud expertise that organizations often do not have.

Once in the cloud, organizations manage and create environments via automation, adapt their workloads to changes by automatically provisioning resources, and use the newest technologies that drive innovation. The cloud era brings a new paradigm to the way organizations manage security and control their environments. They need to automate cloud governance, security and compliance, while also incorporating those features as early as possible into their software development life cycle.

Taking cloud security to the next maturity level begins with continuous security governance and compliance, and a prevention-focused state of mind.

UNDERSTANDING YOUR SECURITY POSTURE ON AWS

SHARED RESPONSIBILITY MODEL



When evaluating your cloud security posture, it is important to understand the principle of the Shared Responsibility Model.

Amazon Web Services (AWS) is responsible for the security "OF" the cloud. As the customer, it is up to you to secure your workloads and applications "IN" the cloud.

To evaluate your security controls and compliance in the cloud, start with gaining visibility into your environment and understanding your current security posture.

Once you understand your cloud environment and its configurations, you can start monitoring and enforcing security policies to address your unique needs.

SCALING SECURITY TO MATCH CLOUD USAGE

As new technologies evolve from on-premises to cloud, and now to containerized and serverless architectures, organizations are challenged with securing these environments and scaling their security controls. Cloud Security Operations teams are unable to keep up with deploying, maintaining, and updating security policies across each environment. Additionally, it can be difficult to remediate misconfigurations before a breach occurs due to the dynamic nature of the cloud environments.

This eBook will walk you through the steps to achieving robust security and compliance at scale through automation, and how Check Point CloudGuard can assist through each step.

6 STEPS TO COMPLIANCE AUTOMATION

STEP 1: GAIN VISIBILITY

Securing cloud environments begins with understanding them. Since you cannot secure what you cannot see, obtaining visibility is crucial to determining how environments should be protected. Having clear, intuitive visibility of the traffic and configurations within your environment allows you to classify objects by exposure level and understand your organization's needs.

Visualizing your environment is not an easy task. Your cloud operations/security and compliance teams need to know what they are looking for and how to use the information they are given. Many organizations struggle to understand what assets are public facing in the cloud. Having a tool that provides a clear, detailed map of your overall architecture will help your team understand how the cloud environment operates and what security measures need to be taken.

Key aspects to consider for obtaining visibility into your cloud security architecture include:

Cloud assets configuration

Identify which applications and workloads you have running on the cloud vs. on-premises.

Public exposure levels

Understand the applications and workloads that are public-facing and more vulnerable to threats.

Network topology

Review your network layout and understand areas prone to threat exposure.

Security groups

Discover and classify your security groups by the varying exposure levels.

Traffic and user activity

Review how applications and workloads interact and the traffic in between them.

Visualizing these aspects can help you create a better plan tailored for your specific policies, as well as identify misconfigurations that can leave your organization vulnerable to breaches, potential attacks, and insider threats.

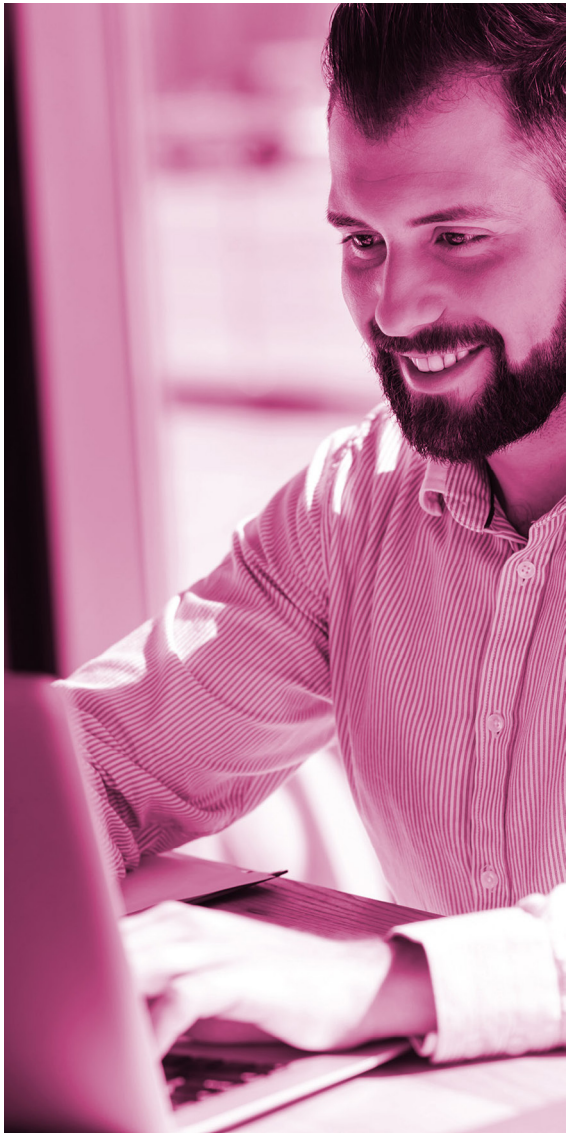
STEP 2: SELECT COMPLIANCE FRAMEWORK AND SCOPE

After evaluating the landscape of your environment and current security posture, you can begin building a new compliance program. As part of this effort, you should focus on the following:

1. **Select relevant compliance framework:**
   Focus on the framework that is aligned to your organization's and industry needs. Different industries have specific regulatory requirements related to security such as ISO27001, PCI DSS, SOC2 and GDPR.

2. **Get a clear understanding of your compliance scope:**
   Determine which cloud assets/accounts have sensitive information, what are the most sensitive development and business processes running, and what regions are relevant for your compliance program.

With an understanding of your cloud environment, relevant scope, and compliance landscape, you can begin prioritizing cloud compliance efforts and create a high-level assessment plan for your organization.



STEP 3: EVALUATE INITIAL RESULTS AND PLAN

In order to evaluate results and define your compliance automation plan, you should consider the following:

1. Initial assessments

Based on the selected framework and scope, run an initial cloud security/compliance assessment. This will allow compliance and cloud security operations teams to evaluate initial results and better understand specific rules and policies.

2. Applying exclusions

Once the initial findings have been evaluated, you can begin applying exceptions to eliminate irrelevant alerts. This will help you narrow down your future notifications to only those that require an immediate action. These exceptions must be captured in a detailed log for future reference and audits.

3. Adding customizations

When you are comfortable with the initial results and have applied exceptions, you can start adding custom compliance and security rules that represent your unique security needs.

STEP 4: MONITOR YOUR CONTINUOUS COMPLIANCE PROGRAM

After the evaluation of initial results is complete, you can start defining your compliance monitoring and remediation plan. In order to transition from ad-hoc assessments to a continuous compliance process, you need to run them on an ongoing basis and set up real-time notifications for non-compliant resources.

The key steps for automated compliance monitoring are:

1. **Define frequency:**
   The frequency of your assessment should be tailored to your processes. You can run reports daily, weekly, monthly, or on a custom schedule.

2. **Identify owners:**
   Define individuals or teams who will be notified of any findings or errors. You can have multiple owners for different types of reports, cloud accounts, or services that are being assessed (i.e., summary, detailed, PCI DSS 3.2/ISO27001/CIS Benchmarks, etc.).

3. **Integrate with other internal processes and supporting tools:**
   Results and remediation plans for your compliance assessment findings can be consumed via your existing internal tools. Compliance monitoring can be done using email, SNS, or third- party IT Management Suite (ITMS) system such as JIRA, PagerDuty, or ServiceNow.

STEP 5: AUTOMATE REMEDIATION

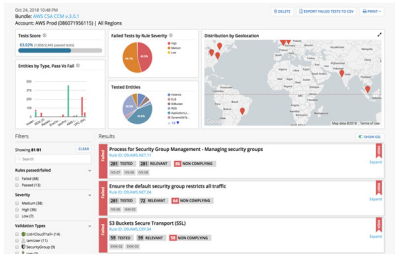
The next step in your cloud compliance automation journey is to automate the remediation activities for active prevention.

With continuous compliance monitoring you can set up real-time notifications for security or compliance policy violations. For some organizations, that is enough. However, those above a certain scale and cloud maturity level, prefer to automate remediation. Automation helps reduce the load on the security operations team and drastically reduces time-to-resolution of security issues.

Automatic remediation should start with addressing the most important findings. This can include closing public-facing security groups or enabling Amazon Simple Storage Service bucket encryption.

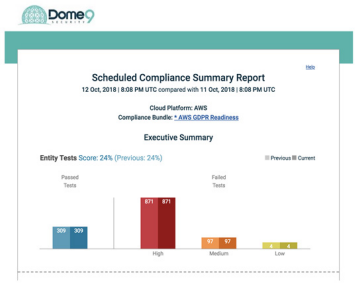
Automated actions are executed upon discovery of a new finding. These actions range from tagging misconfigured resources, to enabling certain security policies, or automatically changing configurations.

Automated Compliance



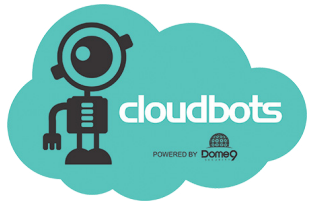
1 Compliance at the click of a button

2 Continuous Alerts and Notifications



4 Automated Remediation

3 Integration with ITMS tools



STEP 6: REPORTING AND AUDITING

At this point in your compliance journey, your focus should be on maintaining up-to-date reports. In order to meet your industry-specific regulations, many will require you to provide compliance reports at any given moment, for any given time period.

These reports are required in order to understand the current security and compliance posture of your cloud environment and will lead to better decision making when it comes to evolving your security posture.

Due to the complexity and everchanging nature of the cloud, continuous snapshots of your compliance assessment results should be taken and stored for future reference.

CHECK POINT CLOUDGUARD OVERVIEW

Check Point CloudGuard on AWS is a scalable solution that helps organizations gain visibility and manage the security and compliance of their cloud environments. The automated and continuous visibility, governance, and compliance help fulfill your part of the Shared Responsibility Model. As a preventative solution that allows organizations to assess their security posture, detect misconfigurations, and actively enforce security best practices, CloudGuard helps organizations stay ahead of potential breaches. With CloudGuard, protecting cloud workloads and services is no longer complex, and you gain access to features that provide:

Network security

Continuous compliance

Privileged identity protection

Cloud threat intelligence

DevSecOps can establish guardrails with automated protection and remediation of cloud configurations. With a single pane view, organizations can deploy, automate and manage security policies across all of their cloud environments with just a few clicks.

In addition, CloudGuard offers CloudBots, an automated remediation solution built for AWS on top of continuous compliance capabilities. Using CloudBots, you can trigger automated remediation actions upon the discovery of new events and breaches.

CloudGuard provides the automated assessment and remediation tools organizations need to maintain a strong security posture and automate their cloud compliance journey.

SOLUTION FEATURES:

- Compliance Engine: Automatically and continuously assess security configurations with out of the box test suites
- Cloud Inventory: Combine cloud inventory and configuration information with real-time monitoring data
- Visualization of cloud assets and traffic: Automatically construct a real-time topology of your cloud security posture
- Auto-remediation: Detect and remediate critical issues in your cloud environment
- Tamper-protection: Continuously monitor and automate the revision of unauthorized modifications
- Privileged identity protection: Grant just-in-time privileged elevation for your AWS IAM users and roles
- Cloud Threat Intelligence: Gain access to cloud intrusion detection, network traffic visualization, and user activity analytics technologies
- Network Security: Leverage IaaS and SaaS network security controls, offering complete visibility, control, and threat protection

CUSTOMER SUCCESS STORY

Customer implemented a scalable security solution that provided single pane of glass visibility and improved their security posture by over 35%.

CHALLENGES

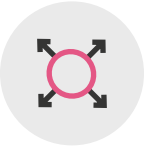
Customer needed a way to rapidly scale to meet growing customer demands, while implementing tighter controls across all their AWS accounts.

SOLUTION

Check Point proved to be the ideal choice. After running through different proof of concepts (POCs), the customer realized that CloudGuard was the only solution that could securely scale at the pace needed for their business. In order to keep up with the growing demand for cloud resources, the customer had created 40-50 different AWS accounts; CloudGuard was able to integrate all of them and apply the same controls across all the environments. With CloudGuard's ability to take this effort from POC to launch in a matter of weeks, the customer was able to better visualize their cloud environment security posture.

By the end of the first 10 months using Check Point's CloudGuard, the customer was able to improve their overall security posture by over 35%.

SOLUTION BENEFITS



Scale easily to manage dozens of accounts via APIs from a single pane of glass.

Monitor and generate reports on all accounts with ease.

Pro-actively remediate misconfigurations using CloudBots.

GETTING STARTED

Check Point offers multiple ways in which you can get started with CloudGuard on AWS. Choose from one of the options below to learn how you can get started on your cloud automation journey.

Request a demo with a Check Point expert>

Visit Check Point CloudGuard listing on AWS Marketplace>

Contact Check Point Technologies>

Visit Check Point on AWS MarketPlace

aws marketplace


Check Point®
SOFTWARE TECHNOLOGIES