



CloudGuard – AWS Control Tower Implementation

Implementation Guide

Date: July 6, 2020



Table of Contents

CloudGuard – AWS Control Tower Implementation	1
Introduction	3
Overview	3
CloudGuard – AWS Control Tower Architecture	5
Resources	5
Prerequisites	7
Deployment and Configuration.....	10
Implement CloudGuard Automatic On-Boarding	10
Enroll Accounts in AWS Control Tower.....	10
Compliance Assessments on CloudGuard	12
Best Practices.....	14
Estimated Pricing.....	14
Resources	15



Introduction

CloudGuard is an automation solution that secures your AWS environment. When deployed in cloud environments, companies need to enable a unified set of cloud native security tools to protect their cloud assets from breaches in a simple and unified way.

The purpose of this Implementation Guide is to enable every [AWS Marketplace](#) customer to seamlessly activate, deploy and configure the CloudGuard in an [AWS Control Tower](#) environment, while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Overview

CloudGuard is a comprehensive cloud native security platform for visibility, workload protection, and posture management of cloud workloads and services.

It has these main features:

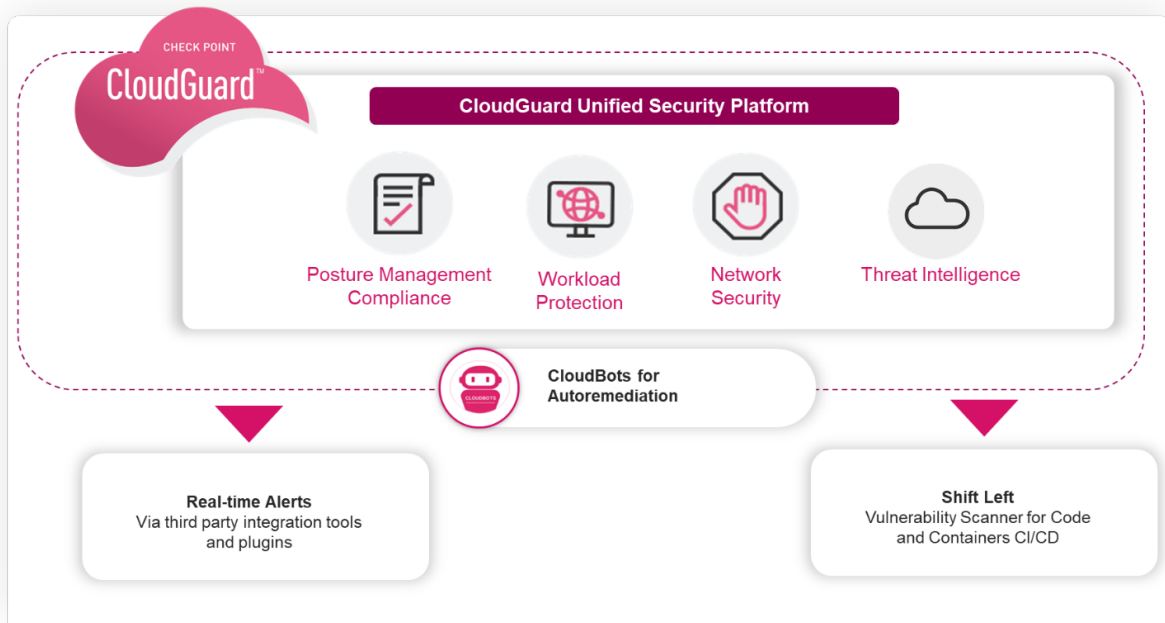
Clarity: this provides powerful visualization of cloud assets, including network topology, firewalls and more

Posture Management: this provides comprehensive compliance management including automated continuous compliance to help assess and enforce regulatory requirements and security best practices

CloudBots: these are open-source auto-remediation solutions that can be used together with Posture Management (or standalone), to accelerate the resolution of dangerous misconfigurations and enforce compliance

Tamper Protection: this provides continuous monitoring and automation reversion of unauthorized modifications to cloud accounts

Privileged Identity Protection: this is just-in-time privilege elevation with out-of-band authorization for IAM actions



CloudGuard – AWS Control Tower Architecture

Check Point CloudGuard provides unified cloud native security for all your assets workloads, giving you the confidence to automate security, prevent threats, and manage posture everywhere across your multi account environment.

With the integration of AWS Control Tower, we can seamlessly automate the customizations specific to your organizational needs upon the creation of a new account and cater to your use cases such as creating [AWS Identity and Access Management \(IAM\)](#) roles.

AWS Control Tower lifecycle events are a set of Amazon CloudWatch events that gets generated when an AWS account gets created using [Account Factory](#).

With every new AWS account created, the AWS Control Tower lifecycle event is going to trigger the [AWS Lambda](#). Lambda will create required IAM resources in child account, and automatically onboard this account to CloudGuard.

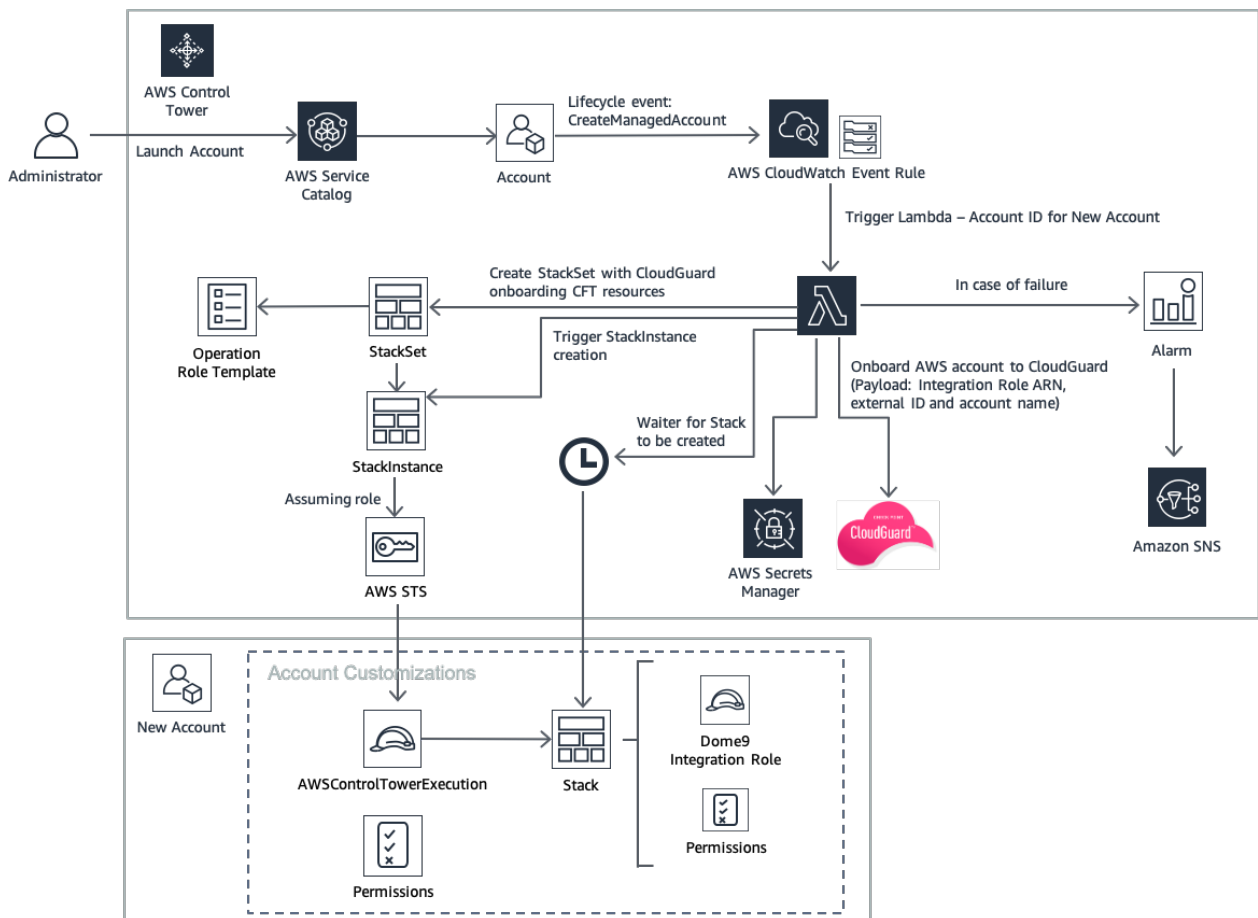


Figure 1: CloudGuard - Control Tower Architecture Diagram

Resources

Once the Serverless application is deployed, it creates the following resources (resources

names may be different as SAM adds a custom prefix) –

1. Dome9AutomationLambdaCWLifecycleEvent - CloudWatch event rule that is triggered by the CreateManagedAccount event in AWS Control Tower
2. Dome9AutomationLambdaCWLifecycleEventPermission – Allows [CloudWatch event](#) to trigger the Lambda.
3. Dome9ApiKeys – [AWS Secrets Manager](#) secret. Access ID and Secret for authentication with CloudGuard API.
4. Dome9AutomationLambda – The core component for this automation. It performs the following steps (as appeared in figure 1):
 - a. Creates stack set based on CloudGuard template
 - b. Creates stack instance with AWS Control Tower Execution role
 - c. Waits for stack instance to be finished (Stack was successfully deployed to child account)
 - d. Gets CloudGuard credentials from Secrets Manager secret.
 - e. Launches request to CloudGuard API with the required authentication and onboarding payload.
5. Dome9AutomationLambdaRole – Execution role for Lambda that will allow it to perform the following:
 - a. CloudFormation operations (Create/Delete stack sets, Create stack instances)
 - b. IAM Pass Role - Lambda Role should leverage AWSControlTowerStackSet role (created by AWS Control Tower during a Landing Zone set up)
 - c. Secrets Manager – Get secret value operation to the specific CloudGuard secret (created as part of the Serverless application installation)
 - d. Basic Lambda execution role
6. CreateManagedAccountDome9AutomationLambdaAlarm – CloudWatch alarm configured to be on when Lambda failures count is equal or greater than 1.
7. Dome9AutomationLambdaAlarmTopic – SNS topic gets message from the CloudWatch alarm and publishes notification to the provided “NotificationEmail” in the SAM installation part.

Note:

To on-board existing accounts to CloudGuard please follow the instructions listed [here](#).

In the next releases we will be adding support for existing AWS accounts onboarding.



Prerequisites

Subscribe to Check Point CloudGuard on AWS Marketplace.

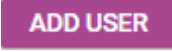
A recommended best practice is to subscribe from AWS Control Tower master account, but it can also be done from any AWS account, and will not affect the AWS Control Tower implementation.

Search for **Check Point-CloudGuard Dome9: Cloud Compliance for AWS** in the AWS Marketplace, here:

https://aws.amazon.com/marketplace/pp/B07Z5SZ9GG?qid=1590113047970&sr=0-10&ref=srh_res_product_title

The screenshot shows the AWS Marketplace product page for 'CloudGuard Dome9: Cloud Compliance for AWS'. The page header includes the AWS Marketplace logo and navigation links. The product title is 'CloudGuard Dome9: Cloud Compliance for AWS', sold by 'Check Point CloudGuard Dome9'. The description states: 'CloudGuard Dome9 SaaS platform allows you to easily manage security and compliance in your AWS environment. You can assess security posture, detect misconfigurations, actively Show more'. There are two buttons: 'Continue to Subscribe' (orange) and 'Save to list' (white). Below the product details, there is a 'Product Overview' section with text: 'CloudGuard Dome9 delivers security and compliance automation to enterprises as they scale in the public cloud. Using Dome9, security teams can visualize cloud assets, continuously assess the security posture, model and enforce gold standard policies, and manage compliance and governance in AWS/Azure/Google Cloud environments. Dome9 was acquired by Check Point, and is now part of the Check Point CloudGuard family of products.' To the right of the overview is a 'Highlights' section with a bullet point: 'End-to-end security and compliance capabilities that allow you to quickly assess security posture, identify risks and gaps, fix issues, actively enforce gold standard, and prove compliance in audits'.

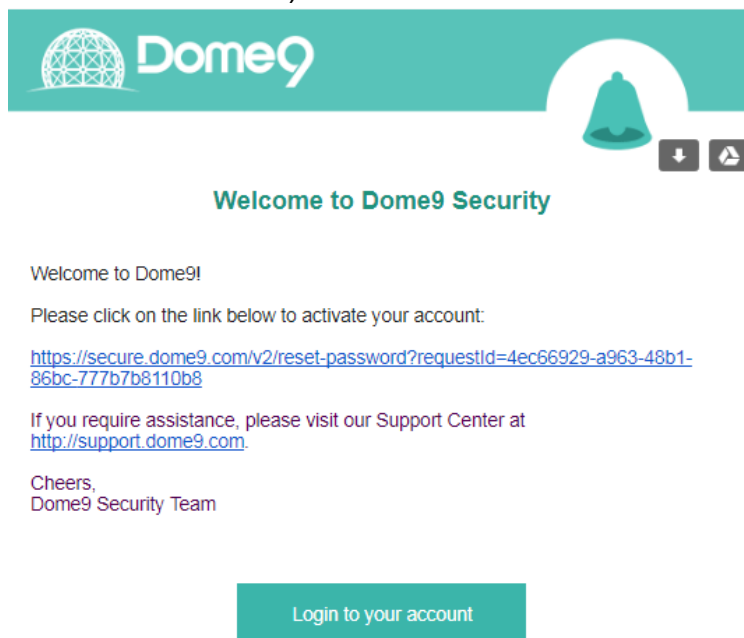
Click on the **Continue to Subscribe** button and follow these steps on your AWS account.

1. Create a CloudGuard Account - the onboarding process connects your cloud account or cluster to CloudGuard. This is a first step in allowing CloudGuard to monitor and, optionally, manage your cloud account security posture. For Additional instructions click [here](#).
2. Create a CloudGuard User with onboarding permissions. Click [here](#) for more information.
3. [Add a new user](#)
 - a. Select the **User Administration** page in the **Settings** menu.
 - b. Click 
 - c. Enter details for user. The user will be identified by the email address. If the user will use Single Sign-on see [Single Sign-On](#).

- d. Select a Role and Permissions for the user. The permissions associated with the role are automatically granted to the user, so no need to assign these explicitly in the Permissions section. If you do not assign a role, you must assign the permissions for the user explicitly here.

Note: Super Users and Account Owner users can add new CloudGuard users to the account.

- e. Click **CLOSE**. An email will be sent to the new user (according to the email address entered for the user). Click on the link in the email to set the password.



- f. Assign On-Boarding Permissions to this user.

You can define roles with specific permissions that can be assigned to users. The roles you define are specific to your CloudGuard account.

Select the **Roles** page in the **Settings** menu.

Click **ADD ROLE**

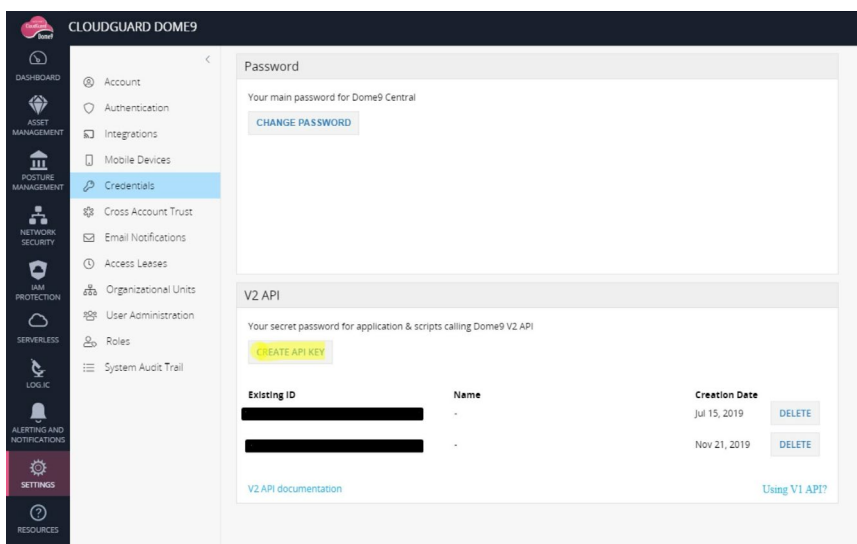
Assign On-Boarding Permissions to this user

Optionally, select users for the role. These users will be granted the permissions associated with the role

4. Generate API Key for the user you've created.

Follow the steps below to create a V2 API Key. You must be logged into the CloudGuard Web App as a user with All System Resources permission.

1. On the CloudGuard UI, navigate to the Credentials page in the Settings menu.
2. In the lower left menu, you will see 'V2 API.'
3. Select 'Create API Key'
4. Your new API Key will be created. A pop-up window will appear with your ID and secret.



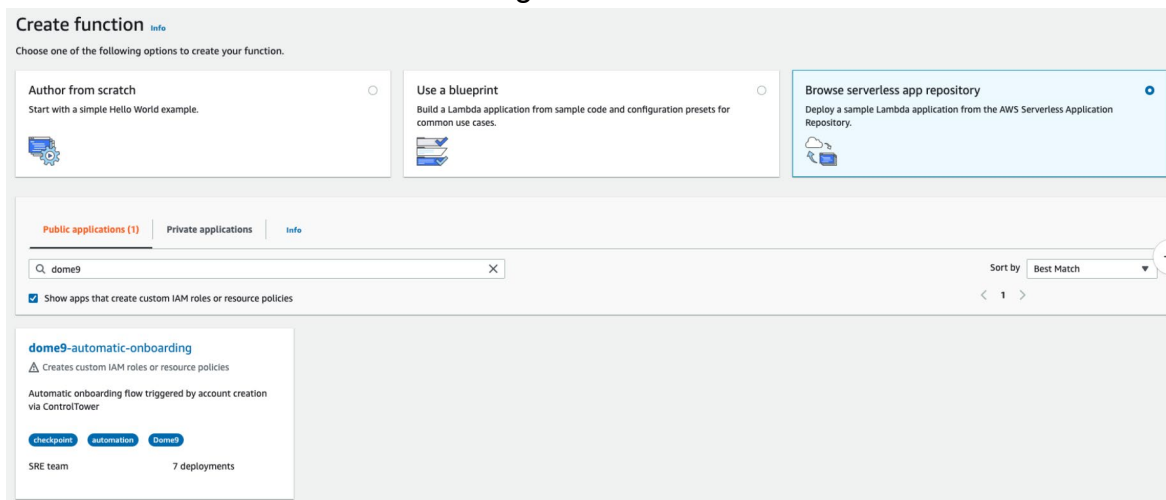
NOTE: Write down and record both the ID and secret that you are provided. While you will be able to view your ID in the console, you will not be able to retrieve the API secret once this window is closed.

Deployment and Configuration

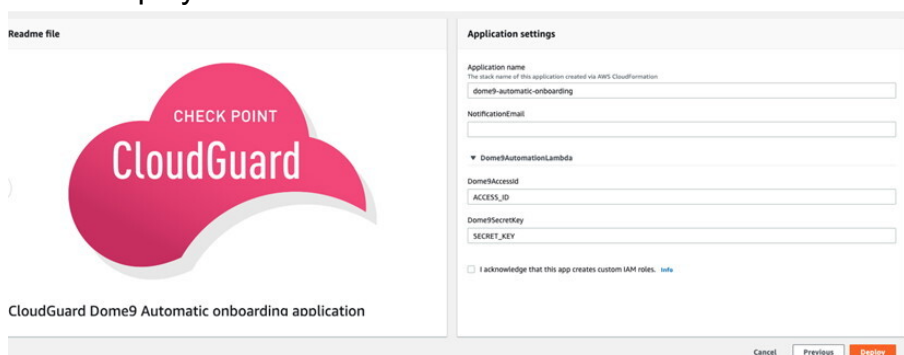
The following procedures explain how to configure CloudGuard in your AWS Control Tower environment.

Implement CloudGuard Automatic On-Boarding

1. Navigate to the Lambda service from your AWS master account.
2. Click “Create Function”.
3. Select “Browse serverless app repository”.
4. Enter “dome9” in the search box.
5. Check the “Show app that” checkbox.
6. Select “dome9-automatic-onboarding”.



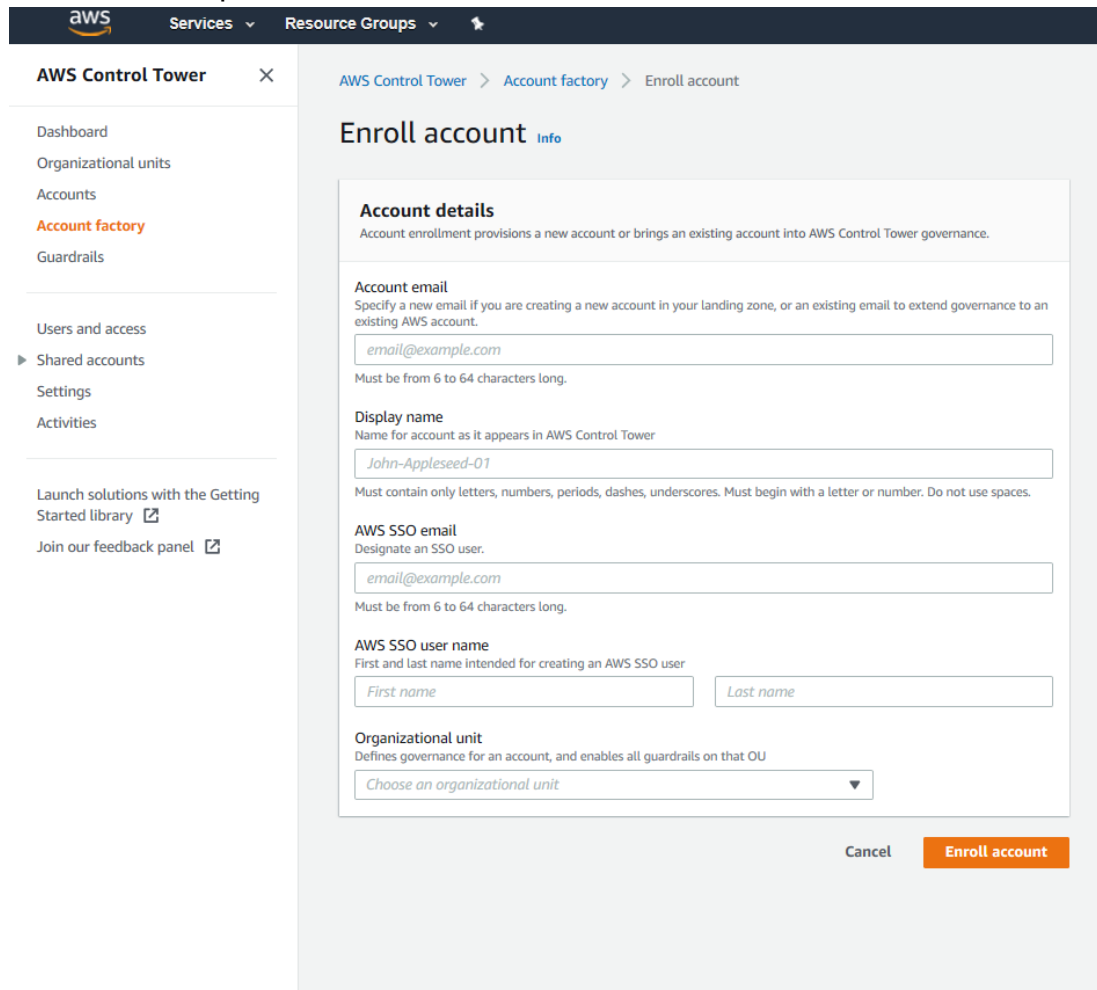
7. Fill the required parameters (NotificationEmail, Dome9AccessId, Dome9SecretKey). Please refer to [Step 4](#) from Pre-requisites.
8. Check the “I acknowledge that this app creates custom IAM roles”.
9. Click “Deploy”



Enroll Accounts in AWS Control Tower

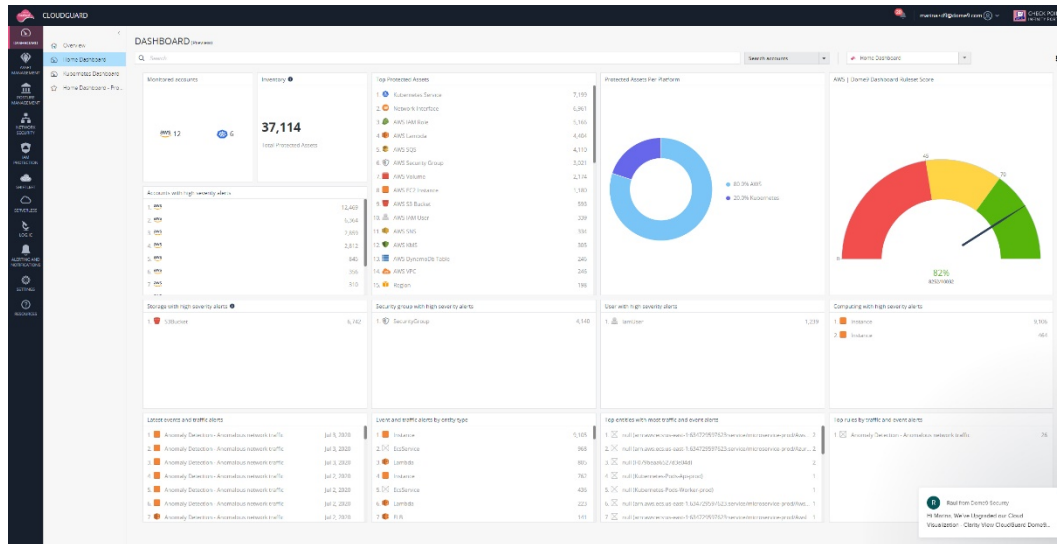
1. In the AWS console, navigate to “Control Tower”.

2. On the left sidebar, select “Account factory”.
3. Provide the required information.



4. On clicking on Enroll Account, AWS Control Tower will enroll a new or an existing account. Once the account creation is complete (usually takes about 30 min), CreateManagedAccount event is published. This event will trigger the Lambda function created by the CloudGuard serverless app.
5. Once the Lambda function triggers successfully, the account will be enrolled in CloudGuard. The CloudGuard Dashboards provide a powerful view showing summary and aggregate data from different CloudGuard data sources, including: Compliance and Posture Management Alerts, Protected assets, Serverless, and Kubernetes. CloudGuard users can create custom dashboards, and arrange the layout of widgets in them.


6. To validate the account is on-boarded you can review the CloudGuard Dashboard.



Compliance Assessments on CloudGuard

CloudGuard Posture Management evaluates your cloud environments for compliance against industry standards and best practices, or your organization's own security policies, using rules that you define, or using sets of rules (rulesets) developed by CloudGuard such as PCI-DSS and HIPAA 5.

To run a ruleset on a selected cloud account from CloudGuard, follow these steps:

1. In CloudGuard, navigate to the Compliance Rulesets tab in the Posture Management menu.
2. Select the ruleset to be run.
3. Click  in the upper right.
4. Select the Environment tab.
5. Select the Cloud account, region, and VPC on which the policy will be run, and then click RUN. The assessment will take from a few seconds to a few minutes (depending on the complexity of the ruleset and the number of rules). When completed, the results

will be displayed.

Details for each rule are shown. This shows that number entities tested (Tests), the number that were included in the scope of the rule (Relevant), the number of entities that were excluded (if **SHOW EXCLUSIONS** is selected), and the number of failed tests (Failed tests).

6. Click **Expand** to show more detail, including details for the rule, and a list of the failed entities.



Best Practices

- Securely store the API Keys** - Application developers can access functionality from within applications using the CloudGuard Dome9 API. With version 2 of this API, developers can access functions using RESTful HTTP requests. For more information please see: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk144514&partition=General&product=CloudGuard
- Ensure to have MFA enabled on your CloudGuard Account** - IAM Safety protects AWS services or specific actions for these services. You can configure your CloudGuard account to use Multi-Factor Authentication. For more information, please see: https://sc1.checkpoint.com/documents/CloudGuard_Dome9/Documentation/Settings/Security_Features.htm?tocpath=Settings%7C6
- Set an account lockout threshold** for failed attempts to login to your CloudGuard Account- Users who enter an incorrect password more than a set number of times, when logging in, will be locked out of their account. Their account can be unlocked by a super user, in the Users page. For more information, please see: https://sc1.checkpoint.com/documents/CloudGuard_Dome9/Documentation/Settings/Users-Roles.html?tocpath=Settings%7C1
- Idle session timeout** should be set following inactivity in order to logout your CloudGuard Account - Super users can set the session idle timeout time (after which an idle session is logged out) For more information, please see: https://sc1.checkpoint.com/documents/CloudGuard_Dome9/Documentation/Settings/Security_Features.htm?tocpath=Settings%7C6

Estimated Pricing

Pricing Information

Below are the total costs for these different subscription durations. Additional taxes or fees may apply.

CloudGuard Dome9: Cloud Compliance for AWS					
Units	Description	1 MONTH	12 MONTHS	24 MONTHS	36 MONTHS
CP-CGD9-CNP-100	Dome9 Compliance & Network Security, 100 Assets	\$2,235	\$21,450	\$42,900	\$64,350
CP-CGD9-CNX-100	Dome9 Compliance, Network Sec. & IAM Safety, 100 Assets	\$2,925	\$28,050	\$56,100	\$84,150



Resources

Community

<https://community.checkpoint.com/t5/Cloud-Security-Posture/bdp/cloudguard-dome9>

Additional Resources

CloudGuard Documentation:

https://sc1.checkpoint.com/documents/CloudGuard_Dome9/Documentation/DocHome.html?tocpath=1

Partner contact information

<https://www.checkpoint.com/about-us/contact-us/>

Support Information

CloudGuard: Cloud Compliance for AWS

<http://support.dome9.com/>

24x7 email support with emergency phone number. Premier support is available for enterprise customers.