Implementation Guide:

Trend Micro Cloud One™ – Conformity
for AWS Control Tower
# Table of Contents

Foreword ........................................................................................................................................... 3
Solution overview and features ....................................................................................................... 4
Architecture diagram ....................................................................................................................... 4
Pre-requisites ..................................................................................................................................... 6
Deployment and Configuration Steps ............................................................................................... 6
Removing the solution ...................................................................................................................... 9
Self-Hosting ....................................................................................................................................... 10
Best Practices ................................................................................................................................... 11
Solution Estimated Pricing ............................................................................................................. 11
FAQs ................................................................................................................................................. 11
Additional resources ...................................................................................................................... 11
Partner contact information ............................................................................................................ 11
Foreword

The Trend Micro Cloud One – Conformity service for Cloud compliance performs continuous assessment of the security posture across multiple accounts on the AWS cloud. Implementing this solution, you will have assurance that your cloud infrastructure is configured and deployed securely according to the Well-Architected Framework best practices.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Conformity in AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.
Solution overview and features

Trend Micro Cloud One – Conformity provides continuous security, compliance, and governance in a SaaS platform, designed to help you manage misconfigurations of cloud resources in your AWS environment by mapping to the AWS Well-Architected Framework and leading compliance frameworks.

Optional integration with Amazon EventBridge can enhance scheduled scans into real time visibility, and our auto-remediation project enhances the solution with AWS Lambda and Amazon SNS resources running inside the managed account to enable misconfigurations to be resolved programmatically further reducing improving the posture of environments.

Trend Micro Cloud One – Conformity helps you to continuously improve your security and compliance posture for AWS infrastructure through automated checks and clear remediation steps. The core platform provides over 550 out-of-the-box, real-time AWS infrastructure best practice rule checks with manual remediation and self-healing capability. The platform enables continuous detection and correction of all best practice violations.

With Trend Micro Cloud One – Conformity you can:

- Continuously build your cloud infrastructure to best practices by mapping the current environment state to the AWS Well-Architected Framework.
- Audit your AWS deployments with numerous compliance standards, including PCI, GDPR, HIPAA, AICPA SOC, CIS, and NIST 800-53.
- Manage compliance at scale in the cloud by monitoring activity and changes to the environment in real time.
- Connect with your preferred ticketing or notification providers, including Slack, JIRA, Amazon Simple Notification Service (SNS), and ServiceNow.
- Run exportable reports on your cloud environments for internal and external audits against benchmark standards.

Architecture diagram

Many businesses are faced with the challenge of protecting their cloud assets and ensuring compliance with regulatory requirements and best practices across multiple AWS accounts. With Trend Micro Cloud One – Conformity, continuous assessment of the security posture allows businesses to confidently maintain compliance across multiple accounts across their AWS environments.

This integration leverages the Amazon EventBridge Event triggered when a managed account is created to trigger customization of that account. The AWSControlTowerExecution role in each account is then used to create access for Conformity.

This integration deploys an EventBridge rule, AWS Secrets Manager secret, AWS KMS customer-managed key, AWS Lambda function, and AWS Identity and Access Management (IAM) Lambda execution role in the management account to support creation of IAM cross-account roles in each AWS Control Tower managed account.
During stack creation, the lifecycle function will be executed on each account currently managed by AWS Control Tower, including the AWS Control Tower Management, Audit, and Log accounts. The lifecycle function will retrieve the Conformity ApiKey from Secrets Manager, then get the External ID for your organization from the Conformity API. Next the function will assume the AWSControlTowerExecution role in the target Managed Account in order to create the necessary cross account role and associated policy. Finally, a call will be made to the Conformity API to enable protection for this Managed Account.

After launch, an EventBridge event rule will trigger the lifecycle function for each successful AWS Control Tower CreateManagedAccount event and execute the same flow to automatically adopt new accounts.
Pre-requisites

Access to the AWS Control Tower Management Account with permission to create AWS CloudFormation, IAM, AWS Lambda, and Amazon Simple Storage Service (Amazon S3) resources.

A Trend Micro Cloud One – Conformity account.

If you are new to AWS, see Getting Started with AWS: https://aws.amazon.com/getting-started/.

For additional information on AWS Marketplace, see https://aws.amazon.com/marketplace/help/about-us?ref=footer_nav_about_aws_marketplace.

To get started with AWS Control Tower, check out the https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html

Deployment and Configuration Steps

**Step 1.1: Subscribe to Trend Micro Cloud One on AWS Marketplace.**


Click on the Continue to Subscribe button.
Step 1.2: Subscribe to Trend Micro Cloud One consumption billing

In the new screen, you can review the consumption based pricing and End User License Agreement.

![Subscribe](image)

You are currently not subscribed to this product. Once you begin your subscription, you will be charged for your accumulated usage at the end of your next billing cycle based on the costs listed in Pricing information on the right.

Pricing Details

<table>
<thead>
<tr>
<th>Software Fees</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>$0.01/7</td>
</tr>
<tr>
<td>Workload: Per Micro-Mod EC2 Instance, Workspace, Other Cloud 1 - CPU/hr</td>
<td>$0.02/7</td>
</tr>
<tr>
<td>Workload: Large EC2 instance, Other Cloud 2 - CPU/hr</td>
<td>$0.03/7</td>
</tr>
<tr>
<td>Workload: Per XL &amp; larger EC2 Instance, Other Cloud 3 - CPU/hr</td>
<td>$0.04/7</td>
</tr>
<tr>
<td>Workload: Data Center / Not Cloud instance - hr</td>
<td>$0.04/7</td>
</tr>
<tr>
<td>Network: per gigabyte (Gb) inspected</td>
<td>$0.01/7</td>
</tr>
<tr>
<td>Application: Per 1000 serverless invocations - /hr</td>
<td>$0.006/7</td>
</tr>
<tr>
<td>Container: Per node - hr</td>
<td>$0.016/7</td>
</tr>
<tr>
<td>Container: Per serverless container - hr</td>
<td>$0.01/7</td>
</tr>
<tr>
<td>File Storage: Per bucket with 2-1000 inspected files</td>
<td>$0.009/7</td>
</tr>
<tr>
<td>File Storage: Per bucket with 201-1000 inspected files</td>
<td>$0.009/7</td>
</tr>
<tr>
<td>File Storage: Per bucket with 1001+ inspected files</td>
<td>$0.01/7</td>
</tr>
<tr>
<td>Concurrency: Per AWS account with less than 1000 resources/hr</td>
<td>$0.007/7</td>
</tr>
<tr>
<td>Concurrency: Per AWS account with 1000 to 5000 resources/hr</td>
<td>$0.008/7</td>
</tr>
<tr>
<td>Concurrency: Per AWS account with 5001+ resources/hr</td>
<td>$0.005/7</td>
</tr>
</tbody>
</table>

Note: This software is priced along a consumption dimension. Your bill will be determined by the number of units you use.

Step 1.3: Set up Account

To begin using this software, you will be redirected to the Trend Micro Cloud One website. Simply click the button below to set up your account and complete your registration. If you are unable to complete your registration, you can always return here through the Your Software page on AWS Marketplace.

Set Up Your Account

![Set Up Your Account](image)

After redirection to the Cloud One portal, continue to create your account. During the account creation process you will be prompted to choose a region in which to host your data. Most organizations choose the region closest to the majority of their workloads. Some other organizations may have compliance requirements which drive their region selection.
Step 2.1: Log into the Cloud One console

Once your account has been created, you can log into the UI. From the Cloud One home page, select the Conformity tile. Skip the wizard which prompts addition of your first AWS account; the AWS Control Tower integration will manage this on your behalf.

Step 2.2: Getting Started

Instead of using the wizard in the console, we will be automating the process of adding all current and future AWS Control Tower Accounts to the Conformity console.

Step 3.1: In the Conformity console, click the arrow next to your name in the top right corner, then select ‘User settings’ followed by ‘API Keys’ from the left navigation and create a new API key. Be sure to save this string as it cannot be retrieved later. This key will be used to authenticate the automation from the AWS Control Tower Management Account to the Conformity API. More details on generating an API key can be found here: https://cloudconformity.atlassian.net/wiki/spaces/HELP/pages/77463659/Public+API+-+API+Keys.

Step 3.2: The code for this project can be downloaded from https://github.com/aws-quickstart/quickstart-ct-trend-micro-cloud-one-conformity/

Step 3.3: Login in to Management account in AWS Control Tower as an admin. Navigate to the CloudFormation Service, select the region in which AWS Control Tower was deployed, and launch the lifecycle template:

The template requires 2 parameters; the first is the API Key generated in step 3.1, and the second is the region selected when creating your Conformity account. Be sure to check the box acknowledging that CloudFormation might create IAM resources. Select Create stack, and the integration will start adding your AWS accounts to Conformity.

Step 4.1: Verify

When the CloudFormation template launches successfully, return to the Conformity console and all of your accounts will have been imported and the Conformity bot will have begun scanning all of your AWS accounts to alert you about any misconfigurations or posture concerns!

Step 4.2: As Conformity starts scanning your AWS accounts, most organizations will choose to prioritize high severity findings for investigation and remediation.
Step 5 - Keeping the Conformity role up to date: The Conformity bot is continuously improved to enhance visibility or add coverage for new AWS services. On occasion a new IAM permission may be required for the role in each protected account. When a new role is available, organizations using this Conformity for AWS Control Tower integration can simply update the CloudFormation stack using the template URL in step 3.2, and the role in all current and future enrolled accounts will be updated to the most recent version of the Conformity role.

Removing the solution

To remove the Control Tower lifecycle hook, identify and delete the CloudFormation stack. Protection for Managed Accounts which have already been added will remain in place. See the Conformity documentation for details on removing an account subscription.

If you would like to remove all of the protection for managed accounts, you can send a remove_all invocation event to the lifecycle hook before deleting the CloudFormation stack.

1. Log in to the AWS console for your organization’s Control Tower Management account.
2. Open the CloudFormation console.
3. Find the ConformityLifeCycleHook stack and open the Resources tab.
4. Find the LifecycleEventHandler row. It will have a Type value of AWS::Lambda::Function and there will be a link to the function. Click the link to open the Lambda console for the function.
5. In the Lambda function console, open the Test tab and create a new event with the event payload below:

   ```json
   {"InvokeAction":"remove_all"}
   ```

6. Click Invoke to trigger the lifecycle hook with the remove_all event payload.

You can verify that removal has been triggered for each account in your organization by reviewing the output logs.
Self-Hosting

Some customers may wish to self-host the Quick Start content; one popular reason for doing so is to ensure that the code you have reviewed is the code you deploy.

If you want to self-host this Quick Start, you will need to:

1. Create a bucket in the region where your AWS Control Tower is deployed. The bucket can be owned by any account as long as your Control Tower management account can access the content.

   🚨 WARNING: If your bucket is not in the same region where your AWS Control Tower is deployed, the stack deployment will fail.

2. Copy the CloudFormation template into your bucket. We recommend using the key quickstart-ct-trend-micro-cloud-one-conformity/templates/Trend-Micro-Cloud-One-Conformity-Lifecycle-QS.yaml.

3. Copy the Lambda function deployment package into your bucket. You can choose your own prefix, but the object path must end in functions/packages/c1c-controltower-lifecycle.zip. We recommend that you use quickstart-ct-trend-micro-cloud-one-conformity/functions/packages/c1c-controltower-lifecycle.zip.

   ℹ TIP: You can use the AWS command-line interface to copy the content:

   ```
   aws s3 cp --recursive \
   s3://aws-quickstart/quickstart-ct-trend-micro-cloud-one-conformity \
   s3://your-bucket/quickstart-ct-trend-micro-cloud-one-conformity
   ```

4. Review the content following your organization’s practices. You may want to read through the details of the CloudFormation stack to see exactly what it creates and what properties each resource has, and you may want to read through the source code for the Lambda function to see what it does.

5. Launch the CloudFormation stack in the same region where your AWS Control Tower is deployed, providing the URL to the template. In the parameters, replace the default value for the Quick Start S3 bucket name and the Quick Start S3 key prefix with the name of your bucket and the prefix within the bucket where the content is stored. In the examples above, the prefix is the default, quickstart-ct-trend-micro-cloud-one-conformity/.

   🚨 WARNING: If you deploy the stack in a different region than your AWS Control Tower, the lifecycle function will not receive events when new accounts are created or removed and will not automatically add or remove accounts in Conformity.
Best Practices

Configure SAML to manage access to your Conformity account.  
https://cloudconformity.atlassian.net/wiki/spaces/HELP/pages/134086850/Set+up+SAML+SSO+integration+for+Cloud+Conformity

Configure notification to Security Teams for high severity violations through integrations like PagerDuty or Amazon SNS.  
https://cloudconformity.atlassian.net/wiki/spaces/HELP/pages/58982475/Communication+Channels

Distribute responsibility for account remediation and visibility to account owners by configuring integrations with tools like Zendesk and Service Now for operations teams, or Jira and Slack for development teams.

Configure custom profiles to tailor monitoring for your security policy or individual accounts. Engage account owners to determine if specific frameworks like SOC2 or PCI should be included in evaluation.  
https://cloudconformity.atlassian.net/wiki/spaces/HELP/pages/142278677/Profiles

Solution Estimated Pricing

Public pricing for Conformity available on AWS Marketplace:  

Conformity is charged on a per AWS account basis and supports customers of all sizes. Please contact us for more information and pricing: https://www.cloudconformity.com/contact-us.html

FAQs

https://www.cloudconformity.com/frequently-asked-questions.html

Additional resources

https://www.cloudconformity.com/help/

Partner contact information

https://www.cloudconformity.com/contact-us.html