Implementation Guide:

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>3</td>
</tr>
<tr>
<td>Solution overview and features</td>
<td>4</td>
</tr>
<tr>
<td>Architecture diagram</td>
<td>4</td>
</tr>
<tr>
<td>Pre-requisites</td>
<td>5</td>
</tr>
<tr>
<td>Deployment and Configuration Steps</td>
<td>5</td>
</tr>
<tr>
<td>Software as a Service (SaaS)</td>
<td>5</td>
</tr>
<tr>
<td>Amazon Machine Image &amp; Quick Start</td>
<td>10</td>
</tr>
<tr>
<td>Best Practices</td>
<td>14</td>
</tr>
<tr>
<td>Solution Estimated Pricing</td>
<td>14</td>
</tr>
<tr>
<td>FAQs</td>
<td>14</td>
</tr>
<tr>
<td>Additional resources</td>
<td>14</td>
</tr>
<tr>
<td>Partner contact information</td>
<td>14</td>
</tr>
</tbody>
</table>
Foreword

The Trend Micro Cloud One™ – Workload Security service for Workload visibility and protection performs automated security deployment and management on the AWS cloud. Implementing this solution, you can automatically protect against vulnerabilities, malware, and unauthorized changes with a wide range of security capabilities across multiple AWS accounts.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure the Workload Security 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 – Workload Security helps to detect and protect against malware, exploitation of vulnerabilities, and unauthorized changes to your Windows and Linux systems as well as containers.

With a rich set of REST APIs, Workload Security facilitates deployment, policy management, health checks, and compliance reporting. Integrations with Amazon EC2 API endpoint and AWS Identity and Access Management (IAM) automate discovery and visibility into workloads in every AWS account, while Amazon SNS provides a mechanism to programatically respond to security events at scale. The Lifecycle Hook solution provides AWS CloudFormation template which, when launched in the AWS Control Tower Master Account, deploys AWS infrastructure to ensure Workload Security monitors each Account Factory AWS account automatically.

With Trend Micro you can:

- Automate security policies across multiple accounts and environments, such as data center and cloud, as you migrate or create new workloads.
- Protect EC2 instances across multiple accounts with Intrusion prevention, anti-malware, machine learning, behavioral analysis, application control, integrity monitoring, web reputation, firewall, and log inspection.
- Demonstrate compliance with a number of regulatory requirements, including GDPR, PCI DSS, HIPAA, NIST, FedRAMP, and more.
- Automate protection with API-first, developer-friendly tools to help you ensure that security controls are baked into DevOps processes.
- Connect security with existing environments and DevOps tools with integration for leading SIEM, security management, orchestration, monitoring, pipeline, and IT service management tools

Architecture diagram

When migrating or building in the cloud, organizations require security that will automatically monitor and protect their workloads across multiple AWS accounts, starting at development through production.

Trend Micro Cloud One - Workload Security provides a single service that is purpose-built for cloud, server, and container environments, providing visibility across your entire hybrid cloud. Security is automated with DevOps toolchain integration and a rich set of REST APIs, which facilitates deployment, policy management, health checks, and compliance reporting.

This integration configures Workload Security integration for each AWS Control Tower managed account during launch, then leverages the CloudWatch Event Triggered when a managed account is created to trigger customization of the member account. The AWSControlTowerExecutionRole in each account is then used to create access for Workload Security.

This integration deploys a CloudWatch Events Rule, an AWS Secrets Manager secret, 2 AWS Lambdas, 1 Amazon S3 bucket, and IAM Lambda execution roles into the master account to support creation of IAM cross account roles in each AWS Control Tower account.
During stack launch, the lifecycle lambda will be executed for each existing AWS Control Tower Account, including the AWS Control Tower Master, Audit, and Log accounts. After launch, an Amazon CloudWatch event rule will trigger the lifecycle Lambda for each successful AWS Control Tower CreateManagedAccount event. The lifecycle lambda function will retrieve the Workload ApiKey from AWS Secrets Manager, then get the External ID for your organization from the Workload API. Next the Lambda 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 Workload API to add this Managed Account to your Workload Security tenant.

Pre-requisites

Access to the AWS Control Tower Master Account with permission to create CloudFormation, IAM, Lambda, and S3 resources.

A Trend Micro Cloud One account.

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


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

Trend Micro offers both SaaS and AMI solutions. Please follow the deployment and configuration steps for the chosen product type.

Software as a Service (SaaS)


Click on the **Continue to Subscribe** button.

**Step 1.2: Pricing and purchase agreement**

In the new screen, you will be provided the subscription pricing based on the size of EC2 instance per hour of usage. Review pricing and click on Subscribe.
Step 1.3: Set up Trend Micro Cloud One account

You are now subscribed through AWS Marketplace, click on Set up your Account to create your Trend Micro Cloud One account.

Step 1.4: Set up Account

After redirection to the Trend Micro Cloud One portal, continue to create your account.
Step 2.1: Log into the Security Console

Once your account has been created, you can log into the UI. 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 Trend Micro Cloud One – Workload Security console

Step 3.1:

In the Workload Security console, navigate to Administration > User Management > API Keys and click new. Select a name for the key and Full Access Role. 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 Master to the console API. More details on generating an API key can be found here: https://help.deepsecurity.trendmicro.com/api-key.html?Highlight=API%20key.


The template requires 2 parameters; the first is the API Key generated in step 3.1. The second is the fqdn of your console. For Workload Security SaaS deployments, leave the default unchanged. Be sure to check the box acknowledging that AWS CloudFormation might create IAM resources. Select create stack, and the integration will start adding your AWS accounts to Workload Security.

**Step 4.1:** When the CloudFormation template launches successfully, return to the Workload Security console and all of your accounts will have been imported. You will already have visibility into any ec2 instances running in these accounts and the structure of VPCs and subnets across all regions.

**Step 4.2:** Next teams will need to start looking at how to deploy agents. Prioritize working with teams supporting high risk workloads like public facing systems or infrastructure supporting critical workloads. The agent can be deployed quickly with a script found in console at Help > Deployment Scripts, but for long term scale it is recommended to build agent deployment into AMI baking, application build pipelines, or other automation already in use within account owner teams.

Amazon Machine Image & Quick Start


Log into the AWS account in which the Deep Security manager should be deployed. For most AWS Control Tower environments, this will be the Audit account.


Product Overview

Security built to fit DevOps with robust APIs and automated protection. Lock down servers with Application Control, protect Docker containers, and increase malware protection with behavioral analysis, and predictive machine learning. Get proactive protection for EC2 workloads with Trend Micro Deep Security. Secure hybrid environments with the Deep Security AMI and pay hourly per workload protected. Buy and deploy a Deep Security AMI and protect your physical, virtual or cloud resources with an agent or our industry leading virtual appliance, and pay for it all on your AWS bill.

Defend against threats, malware and vulnerabilities with a single product. With protection, starting at just $0.01 / hour, you can: Defend your network against attack with host-based intrusion detection and prevention; Stop patching live systems by shielding from vulnerability exploits; Protect Windows and Linux workloads from malware; Streamline the last mile of compliance with File and System Integrity Monitoring; and, get alerts about potential security events in system logs.

BYOL and SaaS versions of Deep Security are also available.

Security tips & tricks and technical resources available at http://www.trendmicro.com/aws or email us at aws.marketplace@trendmicro.com with any questions.

Highlights

- Secure Docker containers with DevOps friendly API security processes including automation security and lock down servers with application control built for the cloud.
- Accelerate compliance and streamline audit evidence gathering with a single security tool that delivers IPS.

Step 1.2: Pricing and purchase agreement

In the new screen, you will be provided the subscription pricing based on the size of EC2 instance per hour of usage.
Step 1.3: Select configuration settings

Choose a fulfillment option to select how you wish to deploy the software, then enter the information required to configure the deployment.
Step 1.4: Launch Software

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option
AWS Quick Start - Trend Micro Deep Security
Trend Micro Deep Security
running on m4.2xlarge

Software Version
Deep Security 12.5.855

Region
US East (N. Virginia)

Choose Action

Select a launch action
- Launch CloudFormation
- Copy to Service Catalog

Choose this action to launch your configuration through the AWS CloudFormation console.

Launch

Step 1.5: Set up Account

When the CloudFormation stack has launched successfully, record the DeepSecurityConsole value from outputs of the top level CloudFormation template. You will need this URL to log into the console and to configure the multi-account integration.

**Step 2.1: Log into the Security Console**

Once your account has been created, you can log into the UI. Next we’ll work on creating access for the AWS Control Tower integration to manage accounts 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 Trend Micro Deep Security console.

**Step 3.1:**

In the Deep Security console, navigate to Administration > User Management > API Keys and click new. Select a name for the key and Full Access Role. 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 Master to the console API. More details on generating an API key can be found here: https://help.deepsecurity.trendmicro.com/api-key.html?Highlight=API%20key.

**Step 3.2:** The code for this project can be downloaded from https://github.com/trendmicro/cloudone-workload-controltower-lifecycle, or deployed from a Trend Micro S3 bucket at https://S3.amazonaws.com/trend-micro-cloud-one-workload-controltower-lifecycle/Trend-Micro-Workload-LifeCycle.yaml


The template requires 2 parameters; the first is the API Key generated in step 3.1. The second is the fqdn of your console. Use the fqdn (without https://) found in the DeepSecurityConsole value recorded in step 1.5. Be sure to check the box acknowledging that AWS CloudFormation might create IAM resources. Select create stack, and the integration will start adding your AWS accounts to Workload Security.

**Step 4.1:** When the CloudFormation template launches successfully, return to the Deep Security console and all of your accounts will have been imported. You will already have visibility into any ec2 instances running in these accounts and the structure of VPCs and subnets across all regions.

**Step 4.2:** Next teams will need to start looking at how to deploy agents. Prioritize working with teams supporting high risk workloads like public facing systems or infrastructure supporting critical workloads. The agent can be deployed quickly with a script found in console at Help > Deployment Scripts, but for long term scale it is recommended to build agent deployment into AMI baking, application build pipelines, or other automation already in use within account owner teams.


Best Practices

- Leverage Event Based Tasks to automate policy assignment based on EC2 instance tags
- Use the Recommendation Scan capability to automate and manage assignment of IPS, Log Inspection, and Integrity Monitoring rules to protect each system
- Learn about opportunities to further automate provisioning, protection, and reporting through in product and open source projects
  [https://help.deepsecurity.trendmicro.com/devops.html]

Solution Estimated Pricing

Public pricing is available on AWS Marketplace:

- SaaS: [https://aws.amazon.com/marketplace/pp/B01LXMNGHB]
- Software AMI: [https://aws.amazon.com/marketplace/pp/B01AVYHVHO]

Pricing for these services is consumption based, only pay for what you use. Pricing is charges based on the size of EC2 instance per hour of usage. Please contact us for more information and pricing:
  [https://www.trendmicro.com/aws/contact/]

FAQs

See FAQ at [https://help.deepsecurity.trendmicro.com/]

Additional resources

[https://help.deepsecurity.trendmicro.com/]
[https://automation.deepsecurity.trendmicro.com]

Partner contact information

[https://www.trendmicro.com/aws/contact/]