

**Implementation Guide:** 

Trend Micro Cloud One™ – Workload Security for AWS Control Tower

# Table of Contents

Foreword	3
Solution overview and features	
Architecture diagram	4
Pre-requisites	5
Deployment and Configuration Steps	5
Software as a Service (SaaS)	
Amazon Machine Image & Quick Start	10
Best Practices	14
Solution Estimated Pricing	14
FAQs	14
Additional resources	14
Partner contact information	12

# Foreword

The Trend Micro Cloud One<sup>™</sup> – 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 programmatically 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.

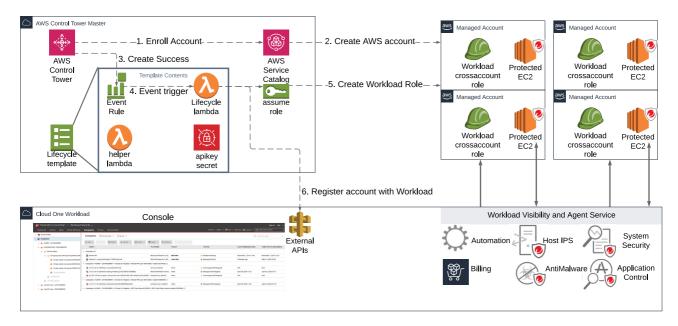


Figure 1 Trend Micro Cloud One – Workload Security Architecture Diagram

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: <a href="https://aws.amazon.com/getting-started/">https://aws.amazon.com/getting-started/</a>.

For additional information on AWS Marketplace, see <a href="https://aws.amazon.com/marketplace/help/about-us?ref">https://aws.amazon.com/marketplace/help/about-us?ref</a> = footer nav about aws marketplace.

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

# 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)

Step 1.1: Subscribe to Trend Micro Cloud One – Workload Security on AWS Marketplace.



# Locate the Workload Security in the AWS Marketplace

(https://aws.amazon.com/marketplace/pp/B01LXMNGHB).



# **Product Overview**

Simplify your life with Workload Security, a part of Trend Micro Cloud One, a security services platform for cloud builders. Previously called Deep Security as a Service, this hosted solution means there's no set up or configuration and we handle all the product and kernel updates for you. Workload Security seamlessly defends your AWS workloads and containers against threats, malware and vulnerabilities. Pay for what you use with hourly pricing and manage IPS/IDS, anti-malware, application control and more in a single solution and console.

Workload security defends against network attacks with intrusion detection and prevention, hardens your servers and speeds patching and response to zero-day issues like WannaCry, Shellshock and Heartbleed. Workload Security protects Windows and Linux workloads from malware, monitors unplanned or suspicious changes to your systems, stops SQL injection and XSS attacks on your applications. Gain immediate visibility into your workloads and speed compliance with a SaaS that is PCI-DSS Level 1 compliant.

Trend Micro Cloud One is a security services platform for organizations building in the cloud. Comprised of 6 cloud security services, it delivers the broadest and deepest cloud security offering in one solution. Workload Security is available now via this listing, and new Cloud One services including Application and Network security will be available on this listing soon and can be deployed from the Cloud One management console.

# Highlights

- Cloud security simplified with Workload Security as a Service
- Speed PCI-DSS and regulatory compliance with multiple security controls in one product.
- Defend against network threats with Intrusion detection and prevention (IDS/IPS).

Click on the Continue to Subscribe button.

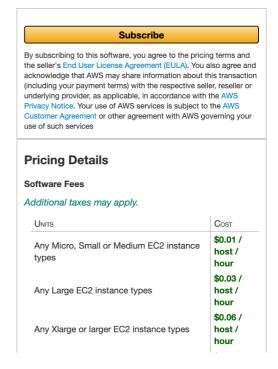


#### Step 1.2: Pricing and purchase agreement

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.

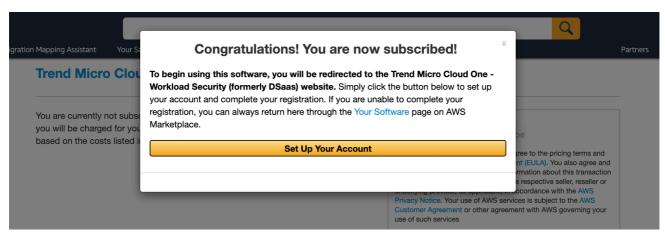
#### Trend Micro Cloud One - Workload Security (formerly DSaas)

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.



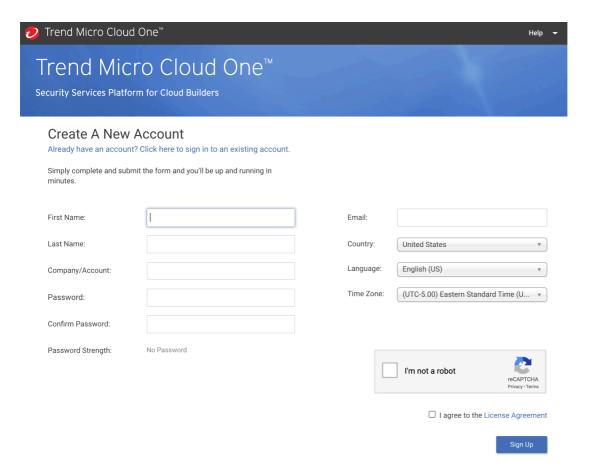
#### Step 1.3: Set up Trend Micro Cloud One account

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: <a href="https://help.deepsecurity.trendmicro.com/api-key.html?Highlight=API%20key">https://help.deepsecurity.trendmicro.com/api-key.html?Highlight=API%20key</a>.

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

**Step 3.3:** Login in to Master 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: <a href="https://console.aws.amazon.com/cloudformation#/stacks/new?templateURL=https://S3.amazonaws.com/trend-micro-cloud-one-workload-controltower-lifecycle/Trend-Micro-Workload-LifeCycle.yaml&stackName=WorkloadLifeCycleHook.">https://sa.amazonaws.com/trend-micro-cloud-one-workload-controltower-lifecycle/Trend-Micro-Workload-LifeCycle.yaml&stackName=WorkloadLifeCycleHook.</a>



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.

-Script Deployment: <a href="https://help.deepsecurity.trendmicro.com/computers-add-deployment-scripts.html">https://help.deepsecurity.trendmicro.com/computers-add-deployment-scripts.html</a>

-Baking: <a href="https://help.deepsecurity.trendmicro.com/agent-baked-in.html">https://help.deepsecurity.trendmicro.com/agent-baked-in.html</a>

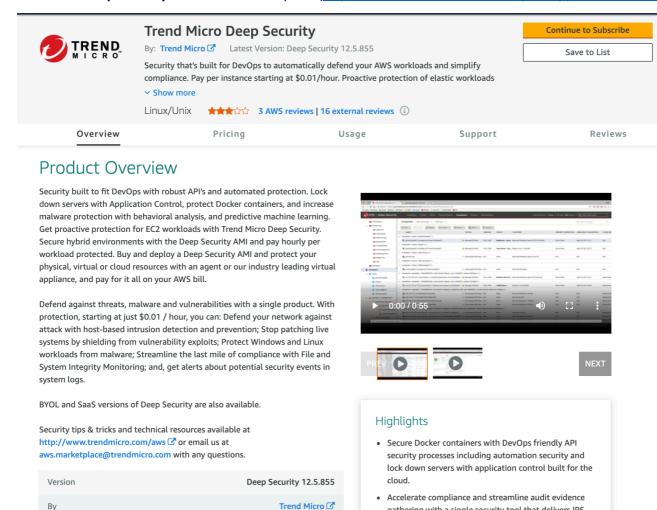


# Amazon Machine Image & Quick Start

#### Step 1.1: Subscribe to Trend Micro Deep Security on AWS Marketplace.

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.

Locate the Deep Security in the AWS Marketplace (https://aws.amazon.com/marketplace/pp/B01AVYHVHO)



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.

gathering with a single security tool that delivers IPS.

Thank you for subscribing to this product! You can now configure your software.

< Product Detail Subscribe

#### Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

#### Terms and Conditions

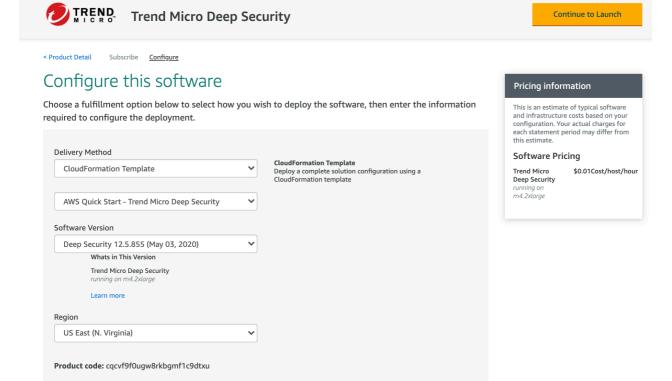
#### Trend Micro Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) . You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice . Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

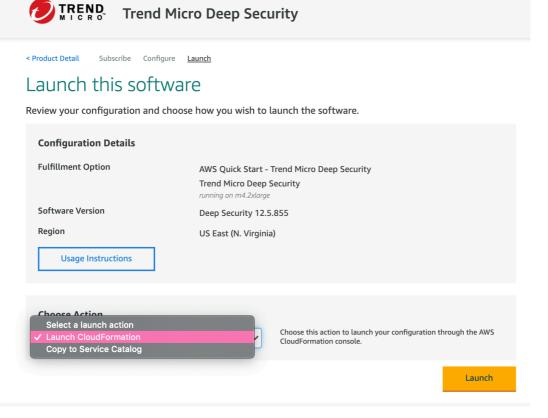
Product	Effective date	Expiration date	Action
Trend Micro Deep Security	6/12/2020	N/A	↑ Hide Details
		,	mananta Vaulra
The following table shows pricing information for the listed software components. You're charged separately for your use of each component.			
Trend Micro Deep Security	nd Micro Deep Security Additional taxes or fees may apply.		
	Trend Micro Deep Security		
	Unit type	Cost/host/ho	ur
	Any Micro, Small o Medium EC2 instar types		
	Any Large EC2 instance types	\$0.03	
	Any Xlarge or large EC2 instance types	%() ()h	
	Other Cloud - 1 Co	re \$0.01	
	Other Cloud - 2 Cores	\$0.03	
	Other Cloud - 4+ Cores	\$0.06	
	Data Center	\$0.06	
	Amazon Workspac	e \$0.01	
	♣ End User License	e Agreement	

# 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



Step 1.5: Set up Account



After completing the subscription, deploy Deep Security Manager to the AWS Control Tower designated shared security account. Trend Micro recommends using the quickstart deployment method. Additional documentation can be found here: <a href="https://docs.aws.amazon.com/quickstart/latest/deep-security/welcome.html">https://docs.aws.amazon.com/quickstart/latest/deep-security/welcome.html</a>.

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: <a href="https://help.deepsecurity.trendmicro.com/api-key.html?Highlight=API%20key">https://help.deepsecurity.trendmicro.com/api-key.html?Highlight=API%20key</a>.

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

**Step 3.3:** Login in to Master 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: <a href="https://console.aws.amazon.com/cloudformation#/stacks/new?templateURL=https://S3.amazonaws.com/trend-micro-cloud-one-workload-controltower-lifecycle/Trend-Micro-Workload-LifeCycle.yaml&stackName=WorkloadLifeCycleHook.</a>

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.
- -Script Deployment: https://help.deepsecurity.trendmicro.com/computers-add-deployment-scripts.html
- -Baking: https://help.deepsecurity.trendmicro.com/agent-baked-in.html



# **Best Practices**

- Leverage Event Based Tasks to automate policy assignment based on EC2 instance tags <a href="https://help.deepsecurity.trendmicro.com/event-based-tasks.html?Highlight=event%20based%20task">https://help.deepsecurity.trendmicro.com/event-based-tasks.html?Highlight=event%20based%20task</a>
- Use the Recommendation Scan capability to automate and manage assignment of IPS, Log Inspection, and Integrity Monitoring rules to protect each system <a href="https://help.deepsecurity.trendmicro.com/recommendation-scans.html?Highlight=recommendation%20scan">https://help.deepsecurity.trendmicro.com/recommendation-scans.html?Highlight=recommendation%20scan</a>
- 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: <a href="https://aws.amazon.com/marketplace/pp/801AVYHVHO">https://aws.amazon.com/marketplace/pp/801AVYHVHO</a>

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/