

Implementation Guide:

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

Table of Contents

Foreword.....	3
Solution overview and features	4
Architecture diagram	4
Pre-requisites	5
Deployment and Configuration Steps	6
Software as a Service (SaaS).....	6
Amazon Machine Image & Quick Start	10
Best Practices	15
Solution Estimated Pricing	15
FAQs	15
Additional resources	15
Partner contact information	15

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 AWS EC2 API endpoint and IAM automate discovery and visibility into workloads in every AWS account, while SNS provides a mechanism to programmatically respond to security events at scale. The Lifecycle Hook solution provides a CloudFormation template which, when launched in the 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 leverages the CloudWatch Event Triggered when a managed account is created to trigger customization of the member account. The ControlTowerExecutionRole in each account is then used to create access for Workload Security.

This integration deploys a CloudWatch Events Rule, a Secrets Manager secret, 2 lambdas, 1 s3 bucket, and IAM lambda execution roles into the master account to support creation of IAM cross account roles in each Control Tower account.

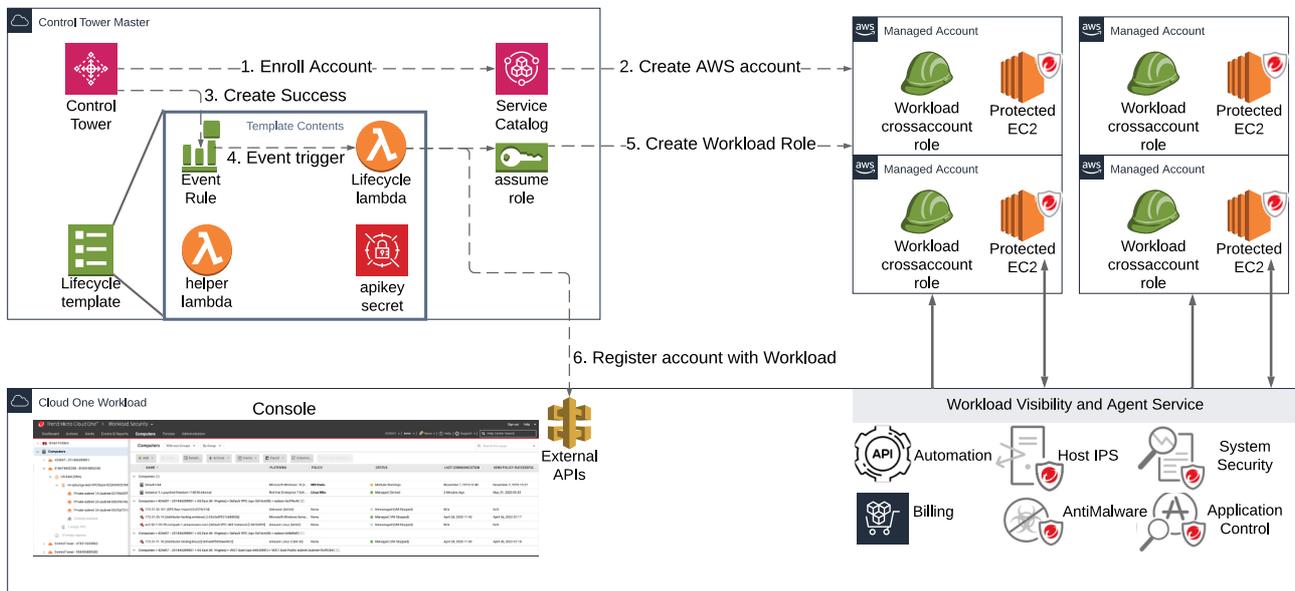


Figure 1 Trend Micro Cloud One – Workload Security Architecture Diagram

During stack launch, the lifecycle lambda will be executed for each existing Control Tower Account, including the Control Tower Master, Audit, and Log accounts. After launch, a CloudWatch event rule will trigger the lifecycle lambda for each successful 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 ControlTowerExecution 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 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/>.

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

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>).



TREND MICRO

Trend Micro Cloud One - Workload Security (formerly DSaaS)

Sold by: [Trend Micro](#)

Cloud security simplified with Workload Security. The most threat defense techniques across the broadest set of platforms, no matter where your workloads or containers live. Seamlessly

[Show more](#)

★★★★☆ 17 AWS reviews | 16 external reviews ⓘ

[Continue to Subscribe](#)

[Save to list](#)

[Overview](#)

[Pricing](#)

[Usage](#)

[Support](#)

[Reviews](#)

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.

[Continue to Subscribe](#)

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.

Subscribe

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also agree and acknowledge 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 is subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services

Pricing Details

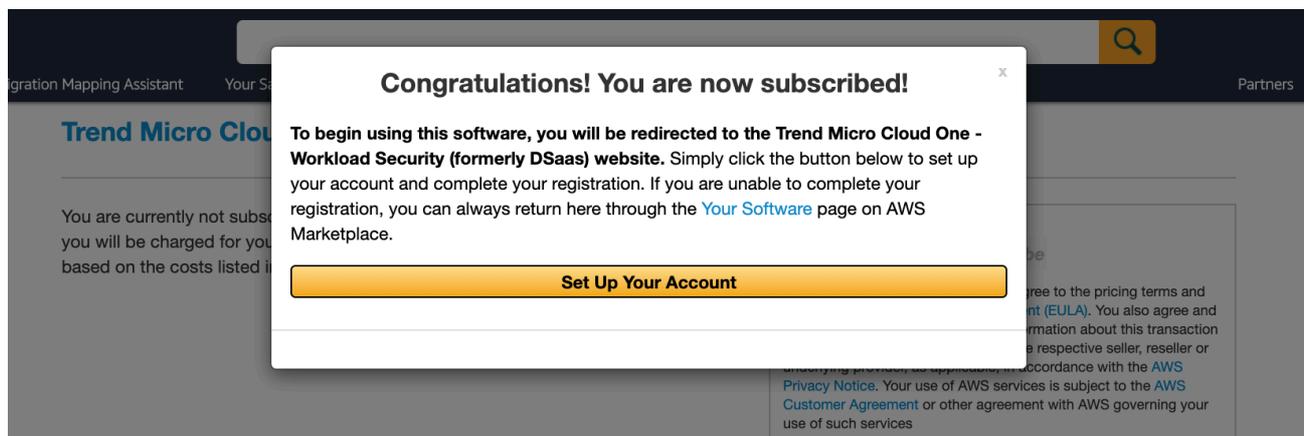
Software Fees

Additional taxes may apply.

UNITS	COST
Any Micro, Small or Medium EC2 instance types	\$0.01 / host / hour
Any Large EC2 instance types	\$0.03 / host / hour
Any Xlarge or larger EC2 instance types	\$0.06 / host / hour

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.

Create A New Account

Already have an account? [Click here to sign in to an existing account.](#)

Simply complete and submit the form and you'll be up and running in minutes.

First Name:	<input type="text"/>	Email:	<input type="text"/>
Last Name:	<input type="text"/>	Country:	<input type="text" value="United States"/>
Company/Account:	<input type="text"/>	Language:	<input type="text" value="English (US)"/>
Password:	<input type="password"/>	Time Zone:	<input type="text" value="(UTC-5.00) Eastern Standard Time (U..."/>
Confirm Password:	<input type="password"/>		
Password Strength:	No Password		

I'm not a robot  reCAPTCHA
Privacy - Terms

I agree to the [License Agreement](#)

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 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 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 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 <github repo>, 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>

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 Control Tower was deployed, and launch the lifecycle template:

<https://us-east-1.console.aws.amazon.com/CloudFormation/home?region=us-east-1#/stacks/create/review?templateURL=https://s3.amazonaws.com/trend-micro-cloud-one-workload-controltower-lifecycle/Trend-Micro-Workload-LifeCycle.yaml&stackName=WorkloadLifeCycleHook>.

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: <https://help.deepsecurity.trendmicro.com/computers-add-deployment-scripts.html>

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

Amazon Machine Image & Quick Start

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

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



Trend Micro Deep Security

By: [Trend Micro](#) Latest Version: Deep Security 12.5.855

Security that's built for DevOps to automatically defend your AWS workloads and simplify compliance. Pay per instance starting at \$0.01/hour. Proactive protection of elastic workloads

[Show more](#)

Linux/Unix ★★★★☆ [3 AWS reviews](#) | [16 external reviews](#)

[Continue to Subscribe](#)

[Save to List](#)

[Overview](#) [Pricing](#) [Usage](#) [Support](#) [Reviews](#)

Product Overview

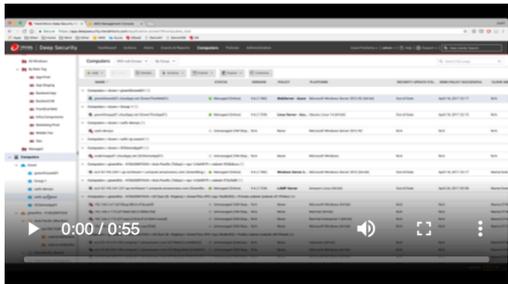
Security built to fit DevOps with robust API's and automated protection. Lock down servers with Application Control, protect Docker containers, and increase malware protection with behavioral analysis, and predictive machine learning. Get proactive protection for EC2 workloads with Trend Micro Deep Security. 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.

Version	Deep Security 12.5.855
By	Trend Micro



[PREV](#) [NEXT](#)

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.



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

The following table shows pricing information for the listed software components. You're charged separately for your use of each component.

Product	Unit type	Cost/host/hour
Trend Micro Deep Security	Any Micro, Small or Medium EC2 instance types	\$0.01
	Any Large EC2 instance types	\$0.03
	Any Xlarge or larger EC2 instance types	\$0.06
	Other Cloud - 1 Core	\$0.01
	Other Cloud - 2 Cores	\$0.03
	Other Cloud - 4+ Cores	\$0.06
	Data Center	\$0.06
	Amazon Workspace	\$0.01

[End User License 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.



< Product Detail Subscribe Configure

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Delivery Method

CloudFormation Template

AWS Quick Start - Trend Micro Deep Security

Software Version

Deep Security 12.5.855 (May 03, 2020)

Whats in This Version

Trend Micro Deep Security
running on m4.2xlarge

[Learn more](#)

Region

US East (N. Virginia)

Product code: cqcvf9f0ugw8rkgmf1c9dtxu

CloudFormation Template
Deploy a complete solution configuration using a CloudFormation template

Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

Trend Micro Deep Security	\$0.01 Cost/host/hour
running on m4.2xlarge	

Step 1.4: Launch Software



< Product Detail Subscribe Configure Launch

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)

[Usage Instructions](#)

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

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

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 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 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 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 <github repo>, 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>

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 Control Tower was deployed, and launch the lifecycle template:

<https://us-east-1.console.aws.amazon.com/CloudFormation/home?region=us-east-1#/stacks/create/review?templateURL=https://s3.amazonaws.com/trend-micro-cloud-one-workload-controltower-lifecycle/Trend-Micro-Workload-LifeCycle.yaml&stackName=WorkloadLifeCycleHook>.

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 *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
<https://help.deepsecurity.trendmicro.com/event-based-tasks.html?Highlight=event%20based%20task>
- Use the Recommendation Scan capability to automate and manage assignment of IPS, Log Inspection, and Integrity Monitoring rules to protect each system
<https://help.deepsecurity.trendmicro.com/recommendation-scans.html?Highlight=recommendation%20scan>
- 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/>