Trend Cyber Risk Assessment Service - Examples

August 2024

About the assessment service

- Our Risk Assessment Service is designed to provide your customers with a comprehensive understanding of their cybersecurity posture.
- The goal is to help businesses identify vulnerabilities, assess their risk levels, and take actionable steps to mitigate potential threats.

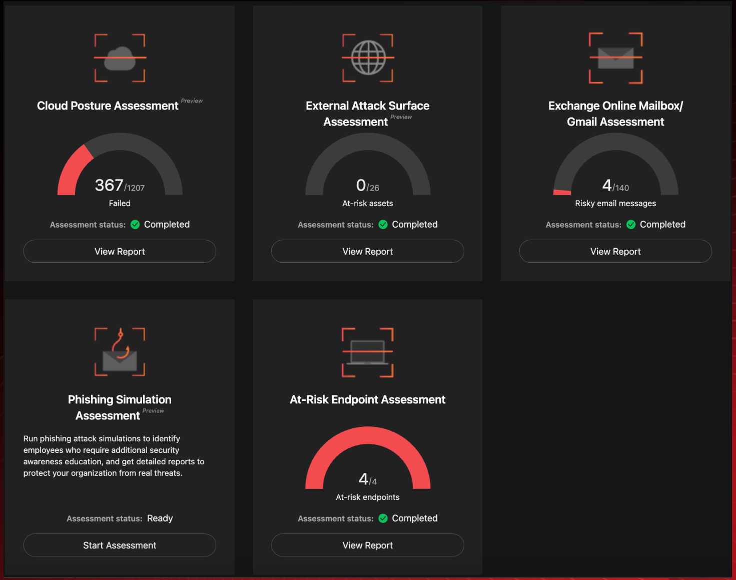
Available Assessments

What to expect?

- A Trend Micro technical advisor will give you an overview of each assessment
- You can select one or multiple assessments
- No sensor installation required for most assessments

Available Assessments – Trend Vison One

- Cloud Posture Assessment
  - No sensor installation required.
  - Discovers misconfigurations and corresponding risk levels in the cloud assets.
  - Scans organization's cloud infrastructure to identify misconfiguration, compliance, and security risks based on common standards and practices.
- External Attack Surface Assessment
  - No sensor installation required.
  - Discover risks hiding in customers' internet-facing assets by Simply entering the organization's domain.
  - Provides visibility of vulnerabilities, insecure connections, and unexpected services/ports within customers' environment.
- Exchange Online Mailbox/Gmail Assessment
  - Read-access only.
  - Discovers BEC messages, phishing messages, ransomware, malicious files, and malicious URLs.
  - Scans all messages sent and received in the last 15 to 30 days for all cloud mailbox users in customers' environment.



Cloud Posture Assessment Preview

367/1207 Failed

Assessment status: ✓ Completed

External Attack Surface Assessment Preview

0/26 At-risk assets

Assessment status: ✓ Completed

Exchange Online Mailbox/ Gmail Assessment

4/140 Risky email messages

Assessment status: ✓ Completed

Phishing Simulation Assessment Preview

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

Assessment status: Ready

At-Risk Endpoint Assessment

4/4 At-risk endpoints

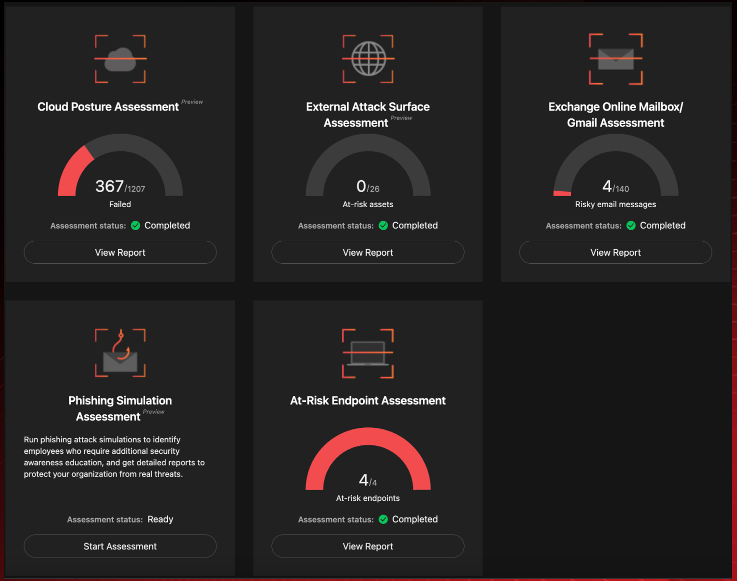
Assessment status: ✓ Completed

Available Assessments – Trend Vison One

- Phishing Simulation Assessment
  - Online service. No sensor installation required.
  - Simulates a phishing attack and gain insight into the human risk that exists within their organization.
  - Allows users to choose a phishing email template, select their employees, launch their simulation, and monitor the results.

- Vulnerability Assessment (Available by Request)
  - Sensor deployment needed.
  - Delivers custom tools to address new, specific common vulnerabilities and exposures (CVE).
  - Scans endpoints and/or server applications for the recent OpenSSL 3.x, Samba or Log4j (Log4Shell) CVEs.

- At-Risk Endpoint Assessment (Available by Request)
  - Sensor deployment needed.



Cloud Posture Assessment Preview

367/1207 Failed

Assessment status: Completed

External Attack Surface Assessment Preview

0/26 At-risk assets

Assessment status: Completed

Exchange Online Mailbox/ Gmail Assessment

4/140 Risky email messages

Assessment status: Completed

Phishing Simulation Assessment Preview

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

Assessment status: Ready

At-Risk Endpoint Assessment

4/4 At-risk endpoints

Assessment status: Completed

Assessment Guides and Report Samples

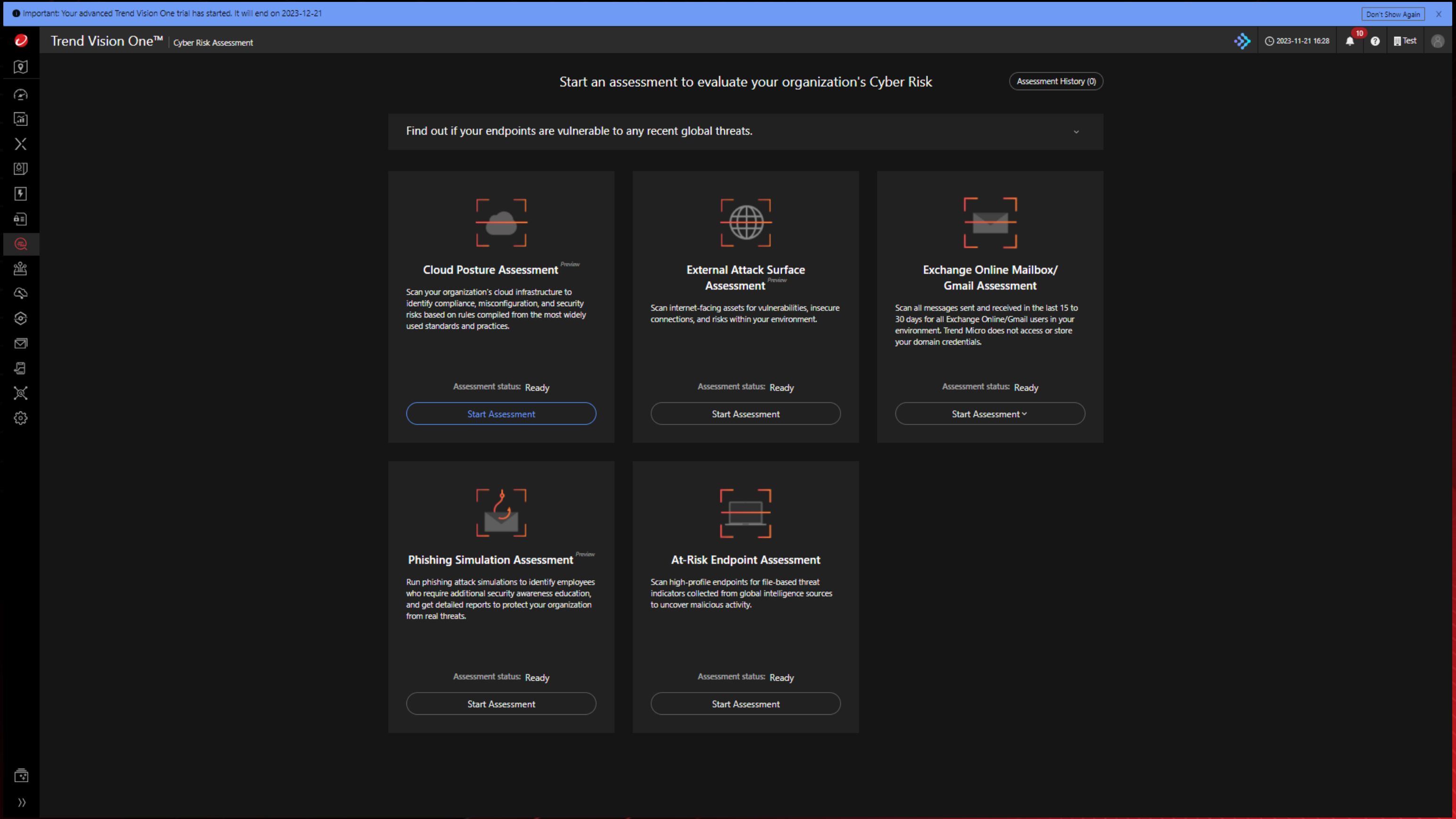
Click the links below to access each assessment's step-by-step guide and report samples:

1. Cloud Posture Assessment
2. External Attack Surface Assessment
3. Exchange Online Mailbox/Gmail Assessment
   1. Office 365
   2. Gmail
4. Phishing Simulation Assessment

Cloud Posture Assessment

Step-by-Step Assessment Walkthrough

- Click “Start Assessment”



Important: Your advanced Trend Vision One trial has started. It will end on 2023-12-21

Start an assessment to evaluate your organization's Cyber Risk

Find out if your endpoints are vulnerable to any recent global threats.

Cloud Posture Assessment

Scan your organization's cloud infrastructure to identify compliance, misconfiguration, and security risks based on rules compiled from the most widely used standards and practices.

Assessment status: Ready

External Attack Surface Assessment

Scan internet-facing assets for vulnerabilities, insecure connections, and risks within your environment.

Assessment status: Ready

Exchange Online Mailbox/ Gmail Assessment

Scan all messages sent and received in the last 15 to 30 days for all Exchange Online/Gmail users in your environment. Trend Micro does not access or store your domain credentials.

Assessment status: Ready

Phishing Simulation Assessment

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

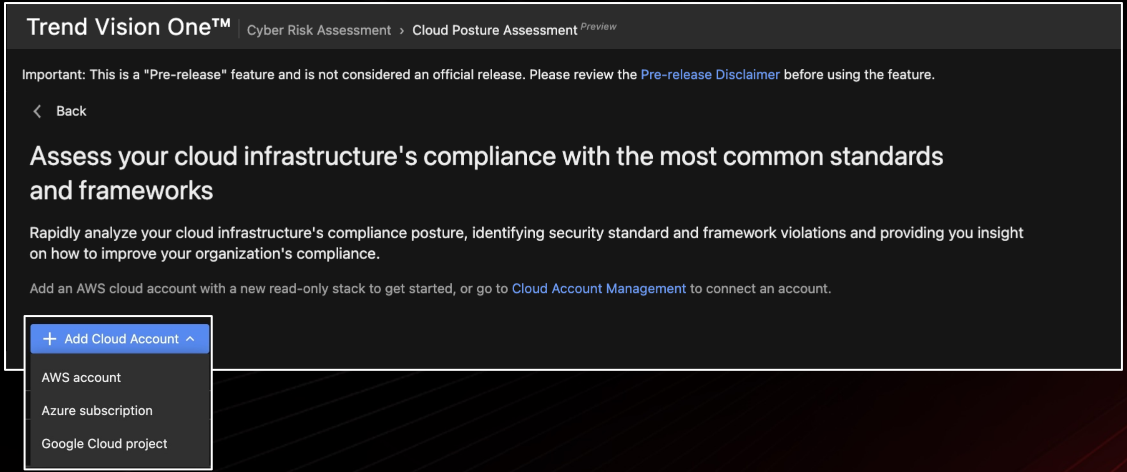
Assessment status: Ready

At-Risk Endpoint Assessment

Scan high-profile endpoints for file-based threat indicators collected from global intelligence sources to uncover malicious activity.

Assessment status: Ready

End to End Steps



Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

Assess your cloud infrastructure's compliance with the most common standards and frameworks

Rapidly analyze your cloud infrastructure's compliance posture, identifying security standard and framework violations and providing you insight on how to improve your organization's compliance.

Add an AWS cloud account with a new read-only stack to get started, or go to Cloud Account Management to connect an account.

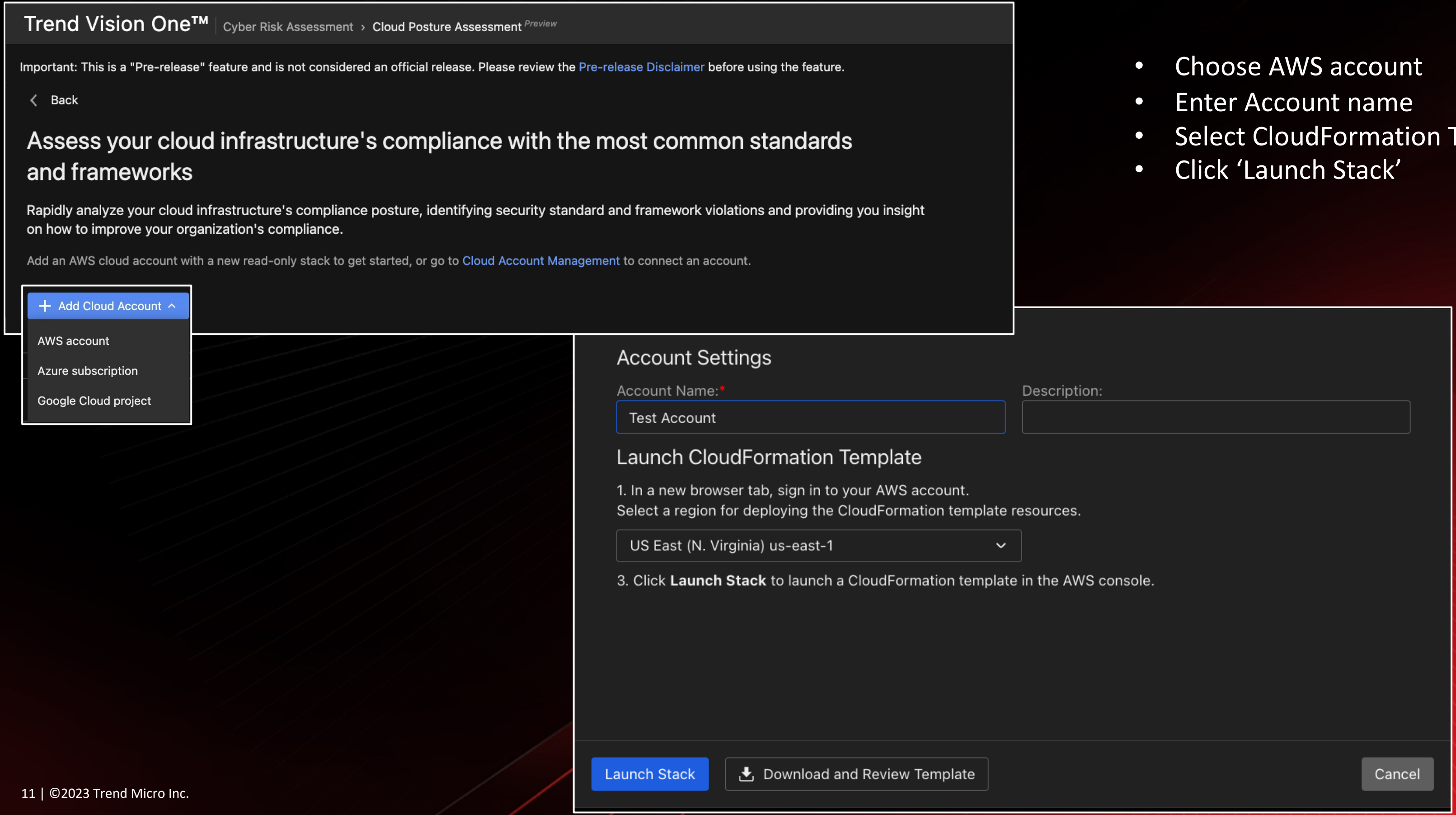
- Click “Add Cloud Account”
- Choose between “AWS Account”, “Azure Subscription” and “Google Cloud Project”

Cloud Posture Assessment

AWS Account

Step-by-Step Assessment Walkthrough

End to End Steps – AWS Account



Trend Vision One™ | Cyber Risk Assessment › Cloud Posture Assessment *Preview*

Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

‹ Back

Assess your cloud infrastructure's compliance with the most common standards and frameworks

Rapidly analyze your cloud infrastructure's compliance posture, identifying security standard and framework violations and providing you insight on how to improve your organization's compliance.

Add an AWS cloud account with a new read-only stack to get started, or go to Cloud Account Management to connect an account.

Account Settings

Account Name:* Test Account

Description:

Launch CloudFormation Template

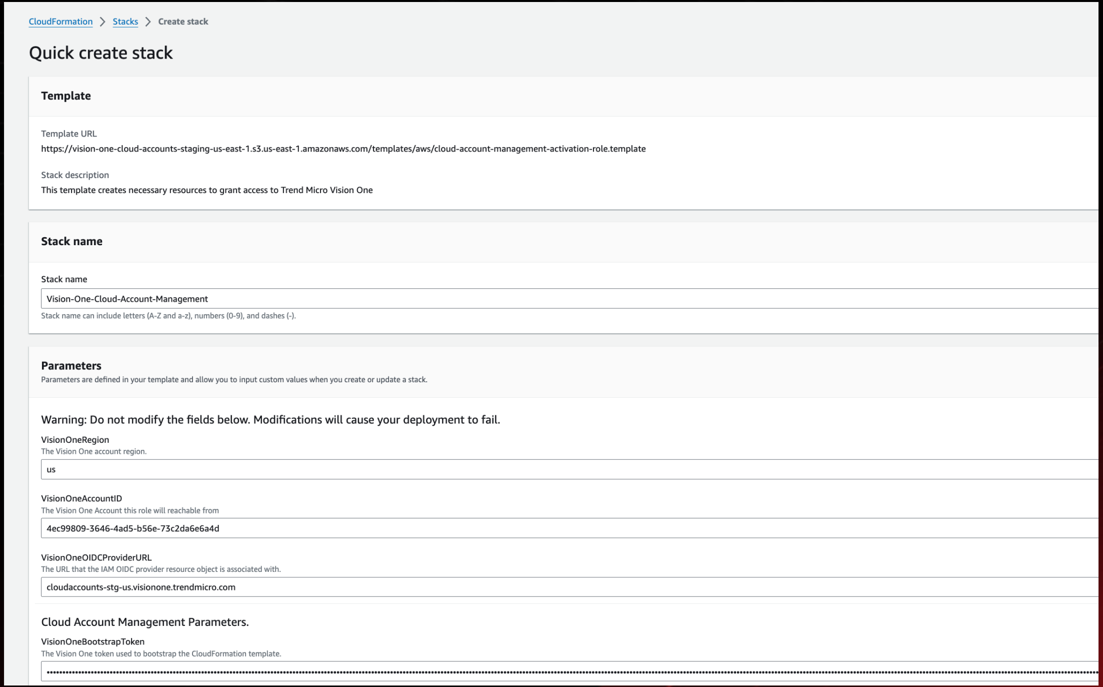
1. In a new browser tab, sign in to your AWS account.
Select a region for deploying the CloudFormation template resources.

US East (N. Virginia) us-east-1

3. Click **Launch Stack** to launch a CloudFormation template in the AWS console.

- Choose AWS account
- Enter Account name
- Select CloudFormation Template region
- Click ‘Launch Stack’

End to End Steps – AWS Account



CloudFormation > Stacks > Create stack

Quick create stack

Template

Template URL
https://vision-one-cloud-accounts-staging-us-east-1.s3.us-east-1.amazonaws.com/templates/aws/cloud-account-management-activation-role.template

Stack description
This template creates necessary resources to grant access to Trend Micro Vision One

Stack name

Stack name
Vision-One-Cloud-Account-Management
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Warning: Do not modify the fields below. Modifications will cause your deployment to fail.

VisionOneRegion
The Vision One account region.
us

VisionOneAccountID
The Vision One Account this role will reachable from
4ec99809-3646-4ad5-b56e-73c2da6e6a4d

VisionOneOIDCProviderURL
The URL that the IAM OIDC provider resource object is associated with.
cloudaccounts-stg-us.visionone.trendmicro.com

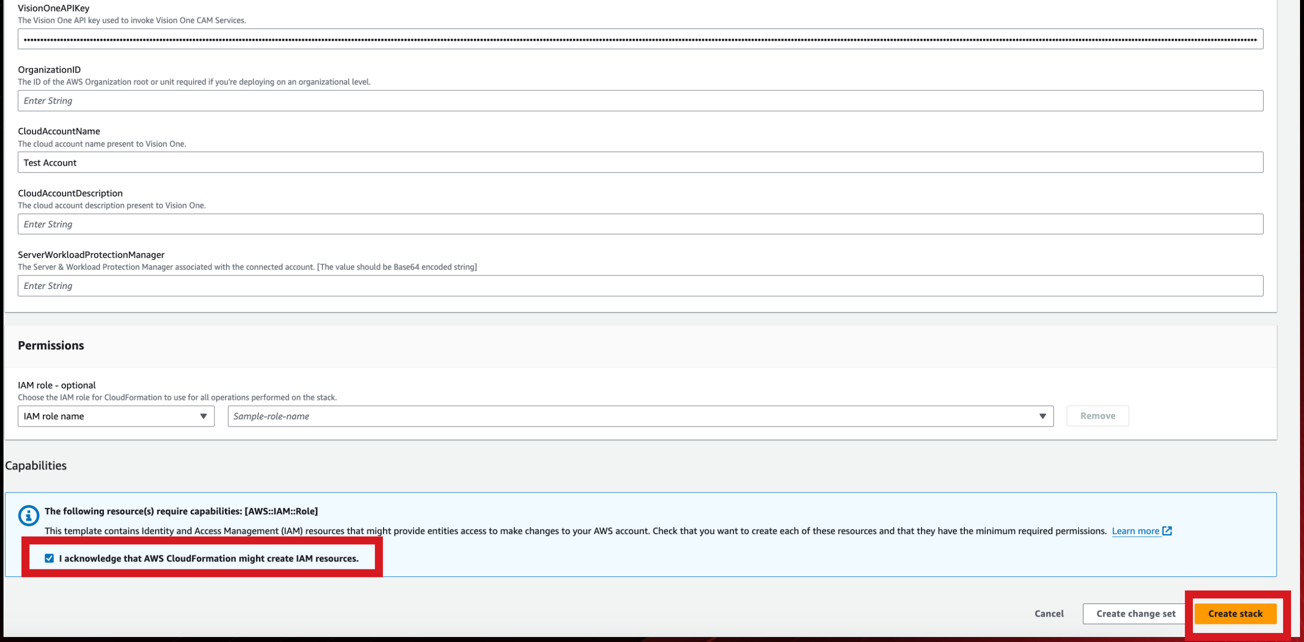
Cloud Account Management Parameters.

VisionOneBootstrapToken
The Vision One token used to bootstrap the CloudFormation template.
••

- AWS CloudFormation stacks page launches
- Review the information and scroll down

Check this link for the full steps if needed: Adding an AWS account | Trend Micro Service Central

End to End Steps – AWS Account



VisionOneAPIKey

The Vision One API key used to invoke Vision One CAM Services.

••

OrganizationID

The ID of the AWS Organization root or unit required if you're deploying on an organizational level.

Enter String

CloudAccountName

The cloud account name present to Vision One.

Test Account

CloudAccountDescription

The cloud account description present to Vision One.

Enter String

ServerWorkloadProtectionManager

The Server & Workload Protection Manager associated with the connected account. [The value should be Base64 encoded string]

Enter String

Permissions

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name ▼ | *Sample-role-name* ▼ | Remove

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

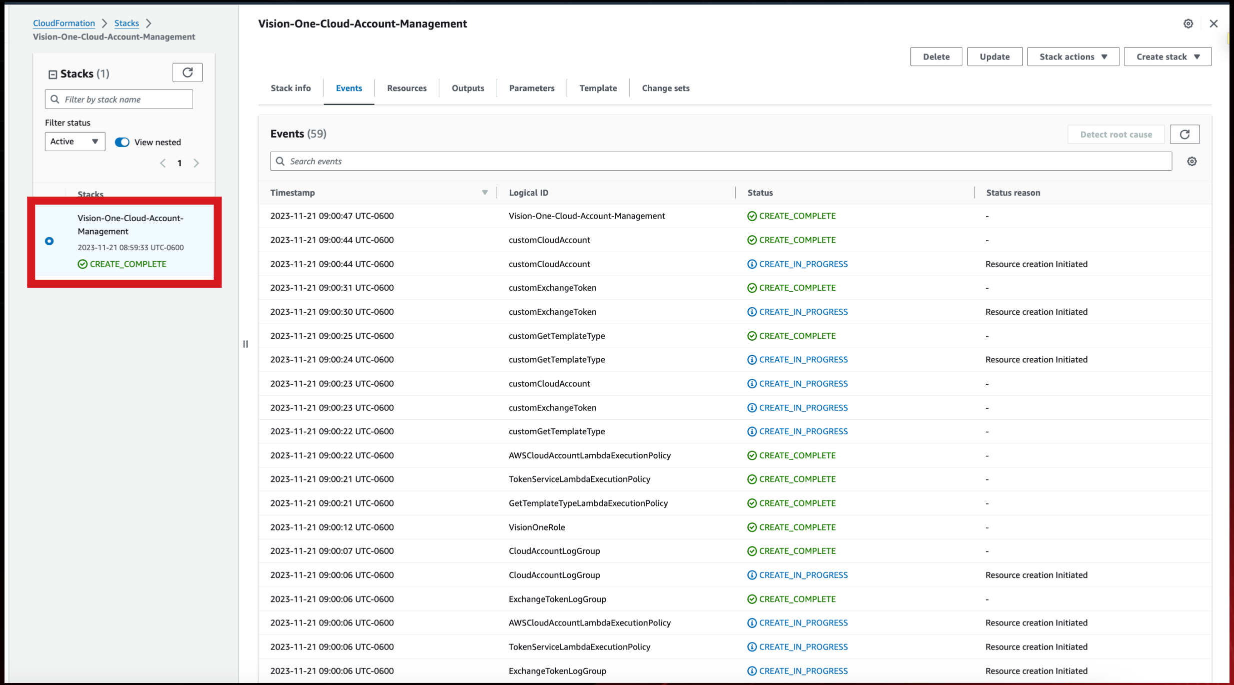
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more

☑ **I acknowledge that AWS CloudFormation might create IAM resources.**

- Confirm that checkbox highlighted is checked
- Click ‘Create Stack’

Check this link for the full steps if needed: [Adding an AWS account | Trend Micro Service Central]

End to End Steps – AWS Account



Vision-One-Cloud-Account-Management
2023-11-21 08:59:33 UTC-0600
CREATE_COMPLETE

Vision-One-Cloud-Account-Management

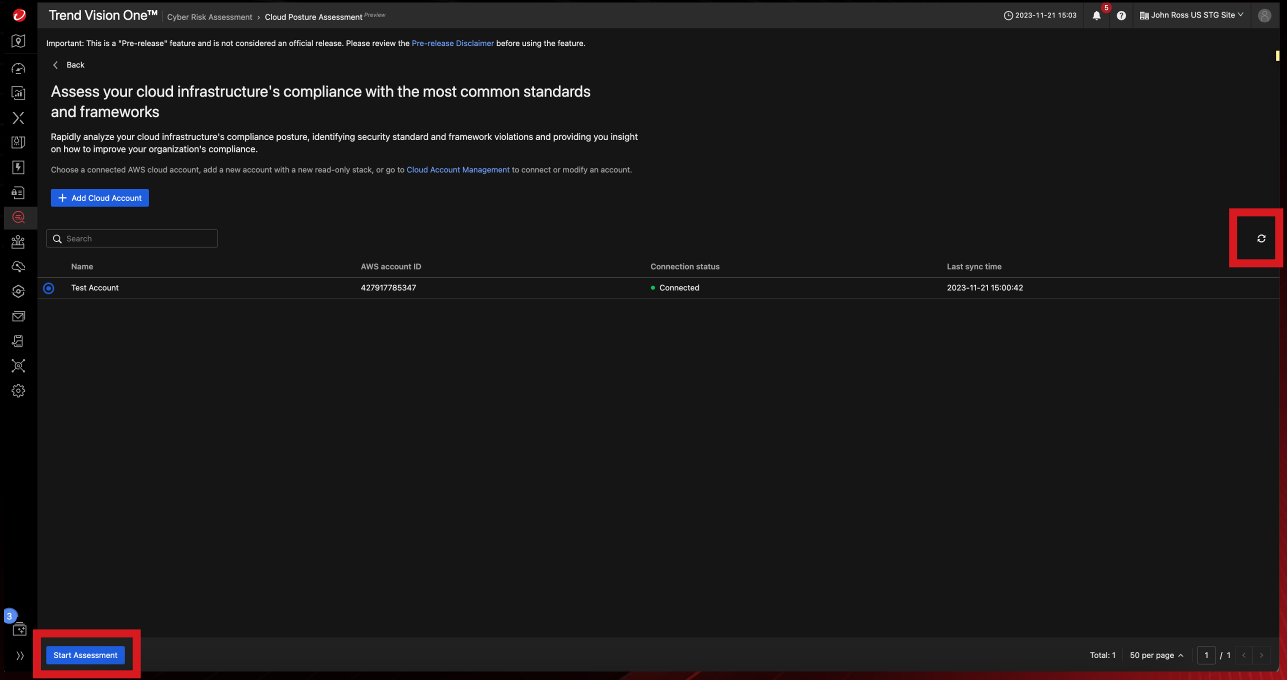
Events (59)

Timestamp	Logical ID	Status	Status reason
2023-11-21 09:00:47 UTC-0600	Vision-One-Cloud-Account-Management	✓ CREATE_COMPLETE	-
2023-11-21 09:00:44 UTC-0600	customCloudAccount	✓ CREATE_COMPLETE	-
2023-11-21 09:00:44 UTC-0600	customCloudAccount	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2023-11-21 09:00:31 UTC-0600	customExchangeToken	✓ CREATE_COMPLETE	-
2023-11-21 09:00:30 UTC-0600	customExchangeToken	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2023-11-21 09:00:25 UTC-0600	customGetTemplateType	✓ CREATE_COMPLETE	-
2023-11-21 09:00:24 UTC-0600	customGetTemplateType	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2023-11-21 09:00:23 UTC-0600	customCloudAccount	ⓘ CREATE_IN_PROGRESS	-
2023-11-21 09:00:23 UTC-0600	customExchangeToken	ⓘ CREATE_IN_PROGRESS	-
2023-11-21 09:00:22 UTC-0600	customGetTemplateType	ⓘ CREATE_IN_PROGRESS	-
2023-11-21 09:00:22 UTC-0600	AWSCloudAccountLambdaExecutionPolicy	✓ CREATE_COMPLETE	-
2023-11-21 09:00:21 UTC-0600	TokenServiceLambdaExecutionPolicy	✓ CREATE_COMPLETE	-
2023-11-21 09:00:21 UTC-0600	GetTemplateTypeLambdaExecutionPolicy	✓ CREATE_COMPLETE	-
2023-11-21 09:00:12 UTC-0600	VisionOneRole	✓ CREATE_COMPLETE	-
2023-11-21 09:00:07 UTC-0600	CloudAccountLogGroup	✓ CREATE_COMPLETE	-
2023-11-21 09:00:06 UTC-0600	CloudAccountLogGroup	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2023-11-21 09:00:06 UTC-0600	ExchangeTokenLogGroup	✓ CREATE_COMPLETE	-
2023-11-21 09:00:06 UTC-0600	AWSCloudAccountLambdaExecutionPolicy	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2023-11-21 09:00:06 UTC-0600	TokenServiceLambdaExecutionPolicy	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2023-11-21 09:00:06 UTC-0600	ExchangeTokenLogGroup	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated

- When stack shows 'CREATE_COMPLATE,' head back to our assessment page

Check this link for the full steps if needed: Adding an AWS account | Trend Micro Service Central

End to End Steps – AWS Account



Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

Assess your cloud infrastructure's compliance with the most common standards and frameworks

Rapidly analyze your cloud infrastructure's compliance posture, identifying security standard and framework violations and providing you insight on how to improve your organization's compliance.

Choose a connected AWS cloud account, add a new account with a new read-only stack, or go to Cloud Account Management to connect or modify an account.

	Name	AWS account ID	Connection status	Last sync time
●	Test Account	427917785347	● Connected	2023-11-21 15:00:42

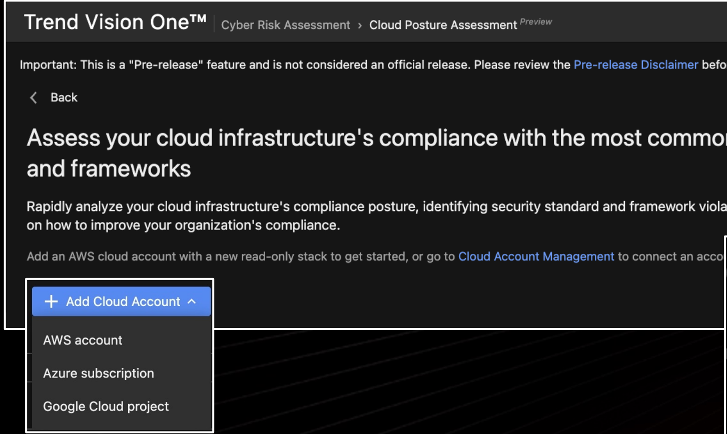
- Click the 'Refresh' button
- With the account selected, click 'Start Assessment'

Cloud Posture Assessment

Azure Subscription

Step-by-Step Assessment Walkthrough

End to End Steps – Azure Subscription



Trend Vision One™ Cyber Risk Assessment › Cloud Posture Assessment *Preview*

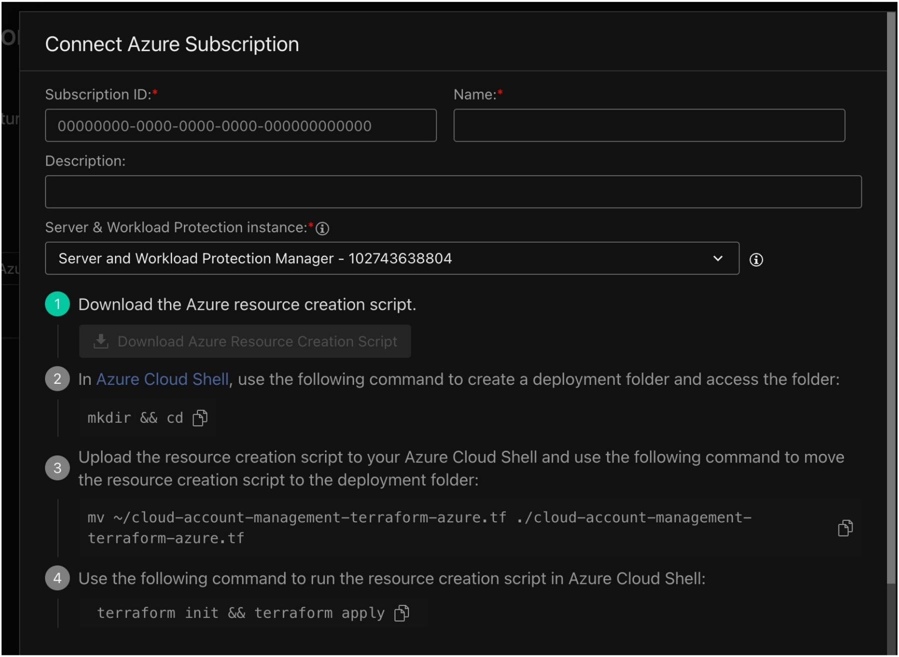
Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

< Back

Assess your cloud infrastructure's compliance with the most common standards and frameworks

Rapidly analyze your cloud infrastructure's compliance posture, identifying security standard and framework violations and providing you insight on how to improve your organization's compliance.

Add an AWS cloud account with a new read-only stack to get started, or go to Cloud Account Management to connect an acco



Connect Azure Subscription

Subscription ID:* 00000000-0000-0000-0000-000000000000

Name:*

Description:

Server & Workload Protection instance:* Server and Workload Protection Manager - 102743638804

1. Download the Azure resource creation script.

2. In Azure Cloud Shell, use the following command to create a deployment folder and access the folder:

```
mkdir && cd
```

3. Upload the resource creation script to your Azure Cloud Shell and use the following command to move the resource creation script to the deployment folder:

```
mv ~/cloud-account-management-terraform-azure.tf ./cloud-account-management-terraform-azure.tf
```

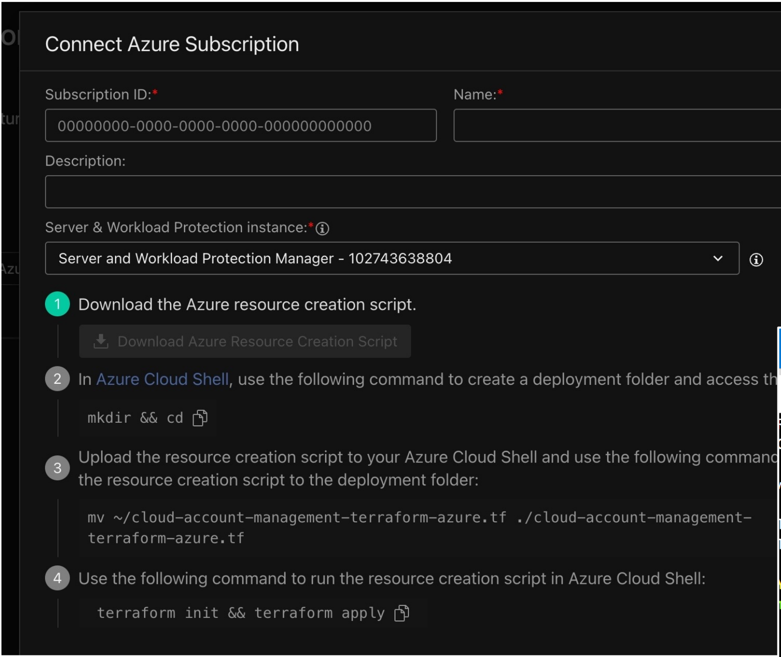
4. Use the following command to run the resource creation script in Azure Cloud Shell:

```
terraform init && terraform apply
```

- Choose Azure Subscription
- Enter Subscription ID
- Specify a **Name** for the subscription which appears in the Cloud Accounts list.
- Click **Download Azure Resource Creation Script**.

Check this link for the full steps if needed:
Adding an Azure subscription | Trend Micro Service Central

End to End Steps – Azure Subscription



Connect Azure Subscription

Subscription ID:* 00000000-0000-0000-0000-000000000000

Name:*

Description:

Server & Workload Protection instance:* Server and Workload Protection Manager - 102743638804

1 Download the Azure resource creation script.

2 In Azure Cloud Shell, use the following command to create a deployment folder and access th

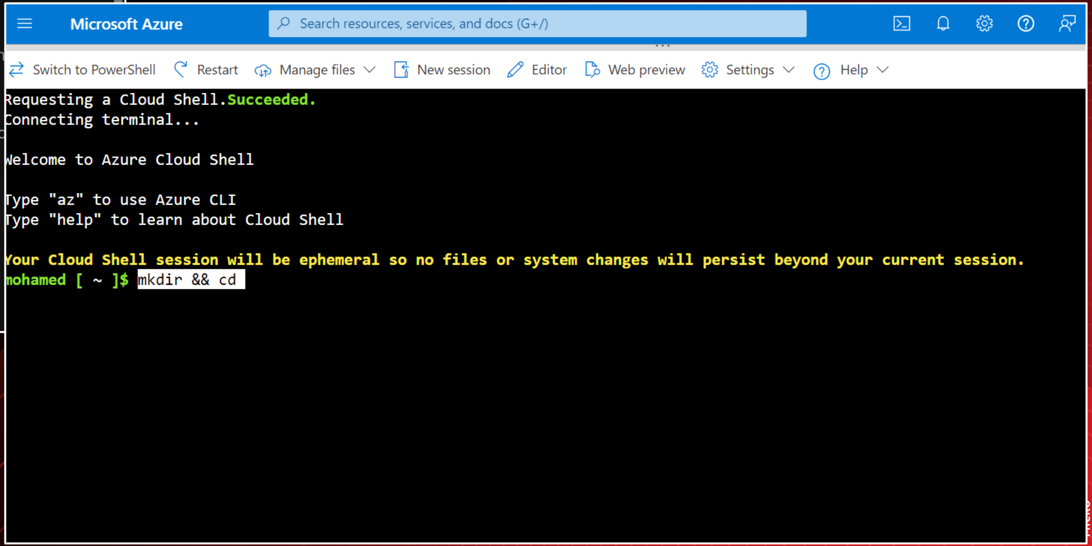
```
mkdir && cd
```

3 Upload the resource creation script to your Azure Cloud Shell and use the following command the resource creation script to the deployment folder:

```
mv ~/cloud-account-management-terraform-azure.tf ./cloud-account-management-
terraform-azure.tf
```

4 Use the following command to run the resource creation script in Azure Cloud Shell:

```
terraform init && terraform apply
```



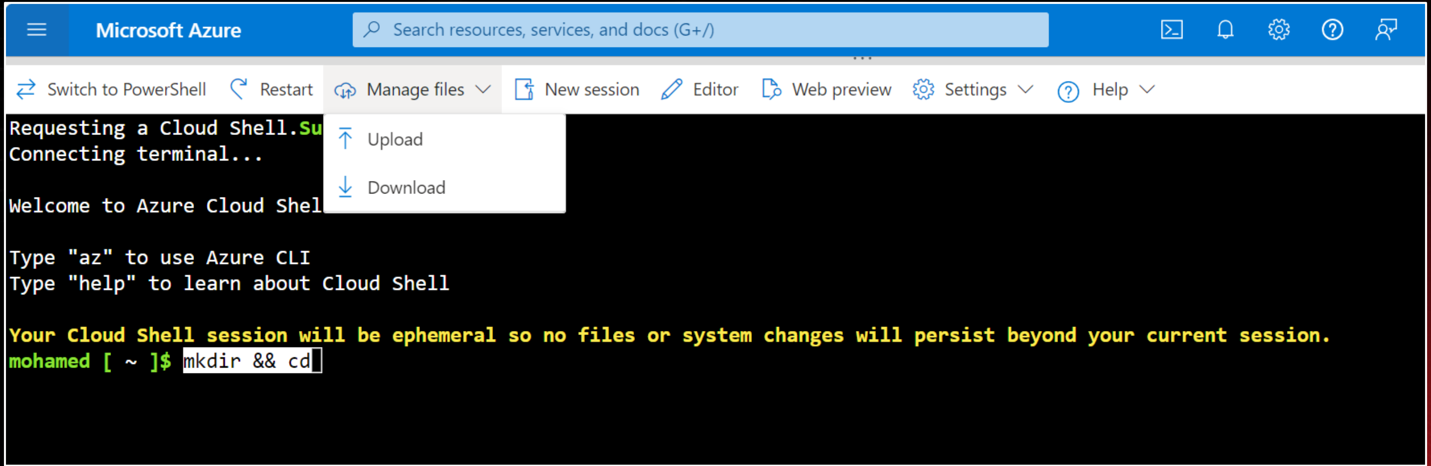
```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
mohamed [ ~ ]$ mkdir && cd
```

- In Azure Cloud Shell, access the command line interface.
- Create a new directory for the deployment folder and then access the folder.
- Copy the command or type **mkdir [directoryName] && cd [directoryName]**

Check this link for the full steps if needed: Adding an Azure subscription | Trend Micro Service Central

End to End Steps – Azure Subscription

- Upload the resource creation script to your Azure Cloud Shell. Azure Cloud Shell uploads the resource creation script to the root directory.

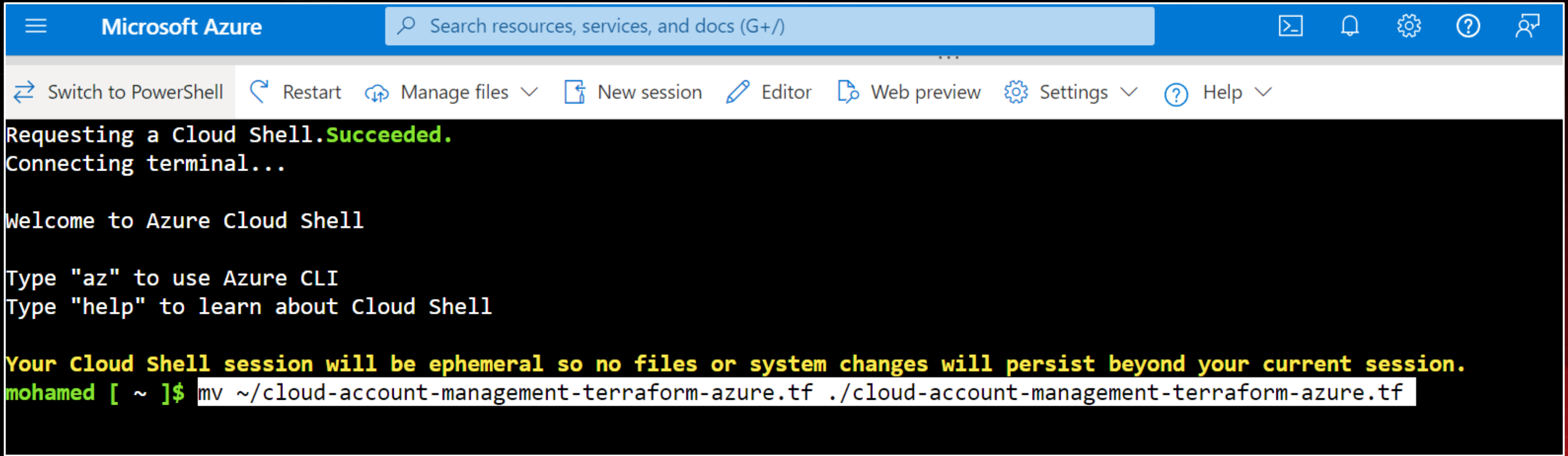


```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shel

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
mohamed [ ~ ]$ mkdir && cd
```

Check this link for the full steps if needed: Adding an Azure subscription | Trend Micro Service Central

End to End Steps – Azure Subscription

- Move the resource creation script to the deployment folder: Copy the command or type **mv ~/cloud-account-management-terraform.tf ./cloud-account-management-terraform.tf**

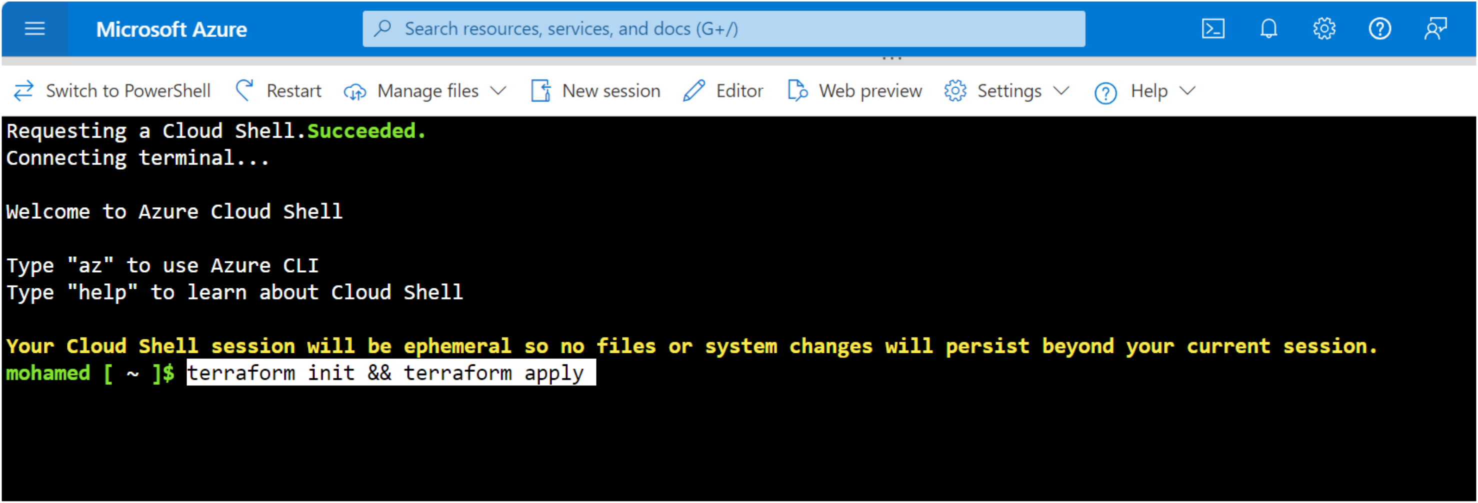


```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
mohamed [ ~ ]$ mv ~/cloud-account-management-terraform-azure.tf ./cloud-account-management-terraform-azure.tf
```

Check this link for the full steps if needed: Adding an Azure subscription | Trend Micro Service Central

End to End Steps – Azure Subscription

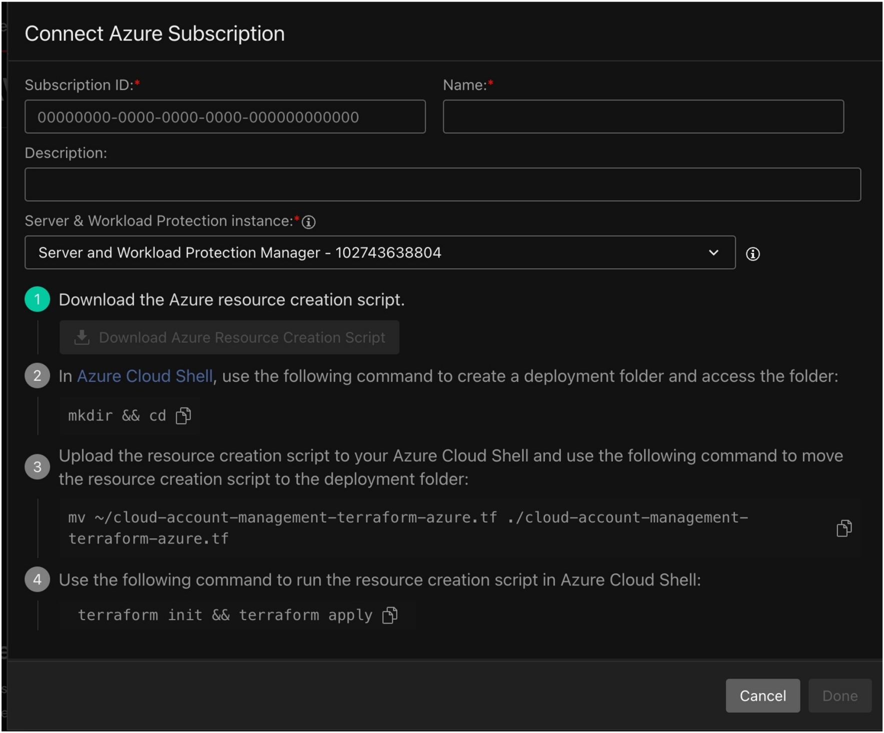
- Initiate Terraform and apply the resource creation script: Copy the command or type **terraform init && terraform apply**



```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
mohamed [ ~ ]$ terraform init && terraform apply
```

Check this link for the full steps if needed: Adding an Azure subscription | Trend Micro Service Central

End to End Steps – Azure Subscription



Connect Azure Subscription

Subscription ID:* 00000000-0000-0000-0000-000000000000

Name:*

Description:

Server & Workload Protection instance:* Server and Workload Protection Manager - 102743638804

1 Download the Azure resource creation script.

2 In Azure Cloud Shell, use the following command to create a deployment folder and access the folder:

```
mkdir  && cd
```

3 Upload the resource creation script to your Azure Cloud Shell and use the following command to move the resource creation script to the deployment folder:

```
mv ~/cloud-account-management-terraform-azure.tf ./cloud-account-management-terraform-azure.tf
```

4 Use the following command to run the resource creation script in Azure Cloud Shell:

```
terraform init && terraform apply
```

- In the Trend Vision One console, in the Connect Azure Subscription screen, click Done.
- The connection process might take a few moments to complete. You can refresh the Cloud Accounts screen to check the status of your added subscription.

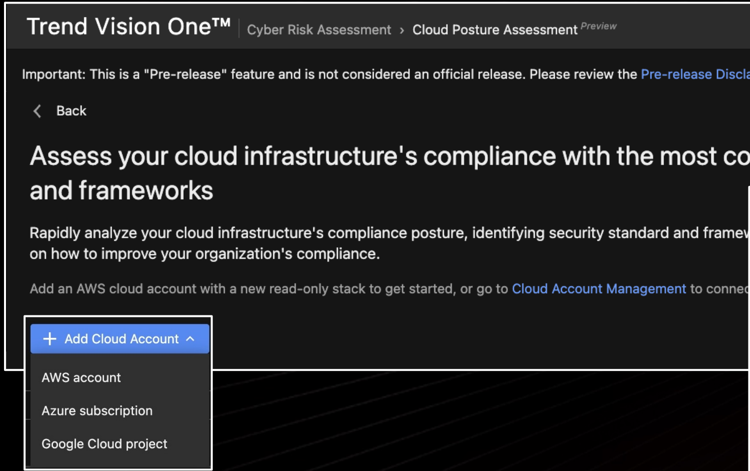
Check this link for the full steps if needed: Adding an Azure subscription | Trend Micro Service Central

Cloud Posture Assessment

Google Cloud Project

Step-by-Step Assessment Walkthrough

End to End Steps – Google Cloud Project



Trend Vision One™ | Cyber Risk Assessment › Cloud Posture Assessment Preview

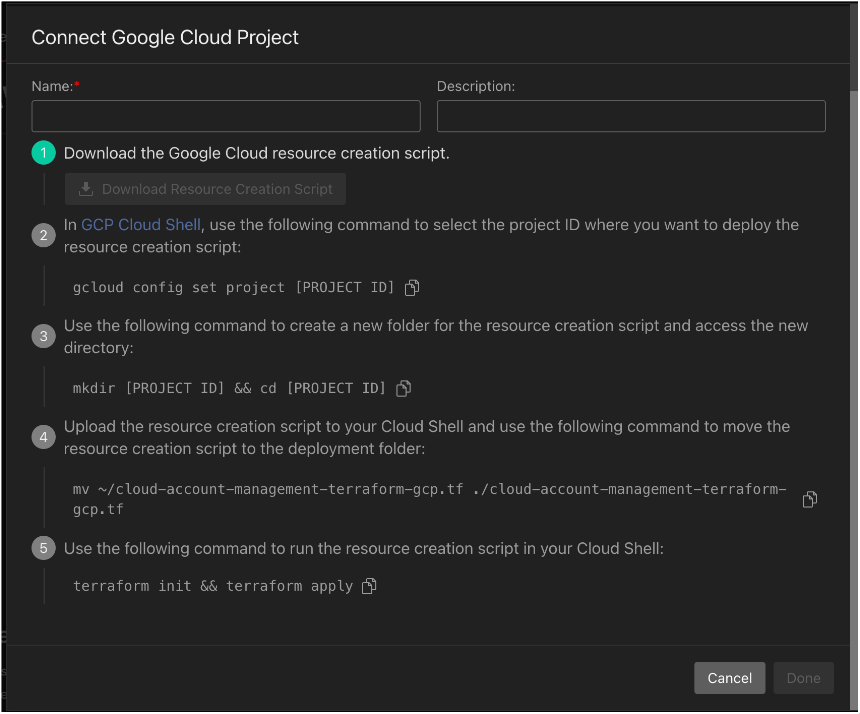
Important: This is a "Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

< Back

Assess your cloud infrastructure's compliance with the most common standards and frameworks

Rapidly analyze your cloud infrastructure's compliance posture, identifying security standard and framev on how to improve your organization's compliance.

Add an AWS cloud account with a new read-only stack to get started, or go to Cloud Account Management to connec



Connect Google Cloud Project

Name:*

Description:

1. Download the Google Cloud resource creation script.

   Download Resource Creation Script

2. In GCP Cloud Shell, use the following command to select the project ID where you want to deploy the resource creation script:

```
gcloud config set project [PROJECT ID]
```

3. Use the following command to create a new folder for the resource creation script and access the new directory:

```
mkdir [PROJECT ID] && cd [PROJECT ID]
```

4. Upload the resource creation script to your Cloud Shell and use the following command to move the resource creation script to the deployment folder:

```
mv ~/cloud-account-management-terraform-gcp.tf ./cloud-account-management-terraform-
gcp.tf
```

5. Use the following command to run the resource creation script in your Cloud Shell:

```
terraform init && terraform apply
```

- Choose Google Cloud Project.
- Specify a Name for the project which appears in the Cloud Accounts list.
- Click **Download Resource Creation Script**.

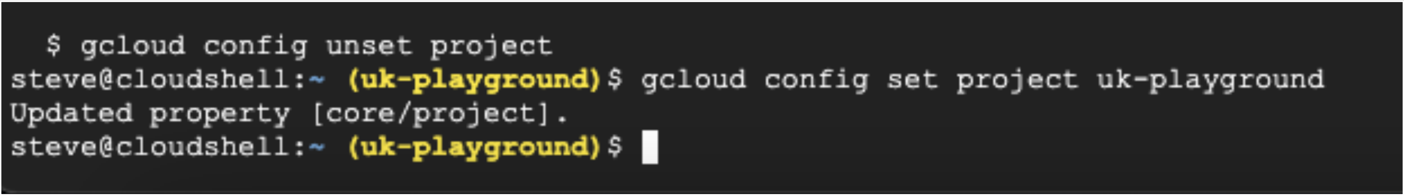
Check this link for the full steps if needed:

Adding a Google Cloud project | Trend Micro Service Central

End to End Steps – Google Cloud Project

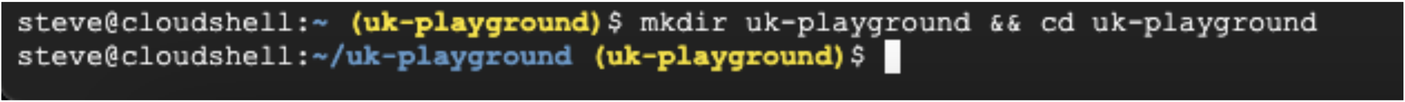
In Google Cloud Shell, access the command line interface.

- Access the project you want to connect: Copy the command or type **gcloud config set project [project ID] where [project ID]** is the Project ID you want to connect.



```
  $ gcloud config unset project
steve@cloudshell:~ (uk-playground)$ gcloud config set project uk-playground
Updated property [core/project].
steve@cloudshell:~ (uk-playground)$
```

- Create a new directory for the deployment folder within the project you want to connect, then access the folder: Copy the command or type **mkdir [Project ID] && cd [Project ID]**

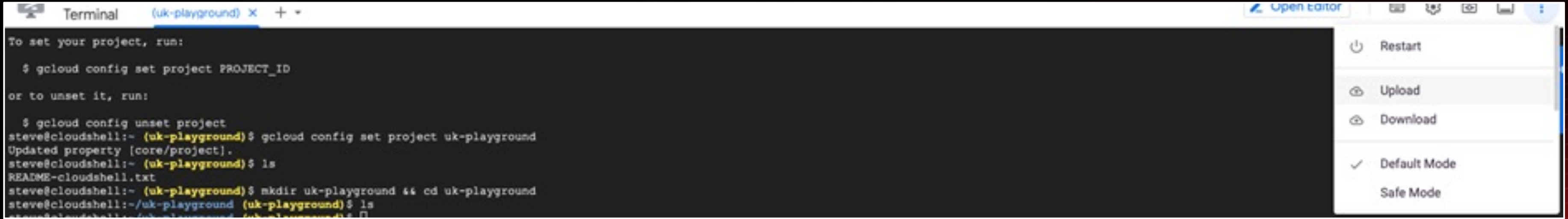


```
steve@cloudshell:~ (uk-playground)$ mkdir uk-playground && cd uk-playground
steve@cloudshell:~/uk-playground (uk-playground)$
```

Check this link for the full steps if needed: Adding a Google Cloud project | Trend Micro Service Central

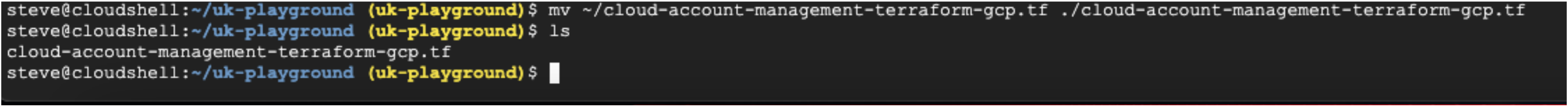
End to End Steps – Google Cloud Project

Upload the resource creation script to your Google Cloud Shell. Google Cloud Shell uploads the resource creation script to the root directory.



```
To set your project, run:

  $ gcloud config set project PROJECT_ID

or to unset it, run:

  $ gcloud config unset project
steve@cloudshell:~ (uk-playground)$ gcloud config set project uk-playground
Updated property [core/project].
steve@cloudshell:~ (uk-playground)$ ls
README-cloudshell.txt
steve@cloudshell:~ (uk-playground)$ mkdir uk-playground && cd uk-playground
steve@cloudshell:~/uk-playground (uk-playground)$ ls
steve@cloudshell:~/uk-playground (uk-playground)$
```

Move the resource creation script to the deployment folder: Copy the command or type **mv ~/cloud-account-management-terraform-gcp.tf ./cloud-account-management-terraform-gcp.tf**

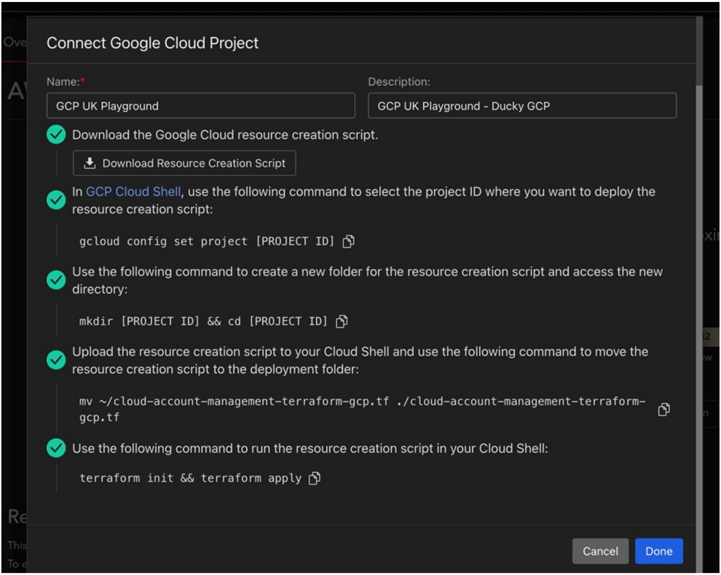


```
steve@cloudshell:~/uk-playground (uk-playground)$ mv ~/cloud-account-management-terraform-gcp.tf ./cloud-account-management-terraform-gcp.tf
steve@cloudshell:~/uk-playground (uk-playground)$ ls
cloud-account-management-terraform-gcp.tf
steve@cloudshell:~/uk-playground (uk-playground)$ █
```

Check this link for the full steps if needed: Adding a Google Cloud project | Trend Micro Service Central

End to End Steps – Google Cloud Project

- Initiate Terraform and apply the resource creation script: Copy the command or type **terraform init && terraform apply**
- In the Trend Vision One console, in the Connect Google Cloud Project screen, click **Done**.
- The connection process might take a few moments to complete. You can refresh the Cloud Accounts screen to check the status of your added project.



Connect Google Cloud Project

Name:* GCP UK Playground

Description: GCP UK Playground - Ducky GCP

✓ Download the Google Cloud resource creation script.

Download Resource Creation Script

✓ In GCP Cloud Shell, use the following command to select the project ID where you want to deploy the resource creation script:

```
gcloud config set project [PROJECT ID]
```

✓ Use the following command to create a new folder for the resource creation script and access the new directory:

```
mkdir [PROJECT ID] && cd [PROJECT ID]
```

✓ Upload the resource creation script to your Cloud Shell and use the following command to move the resource creation script to the deployment folder:

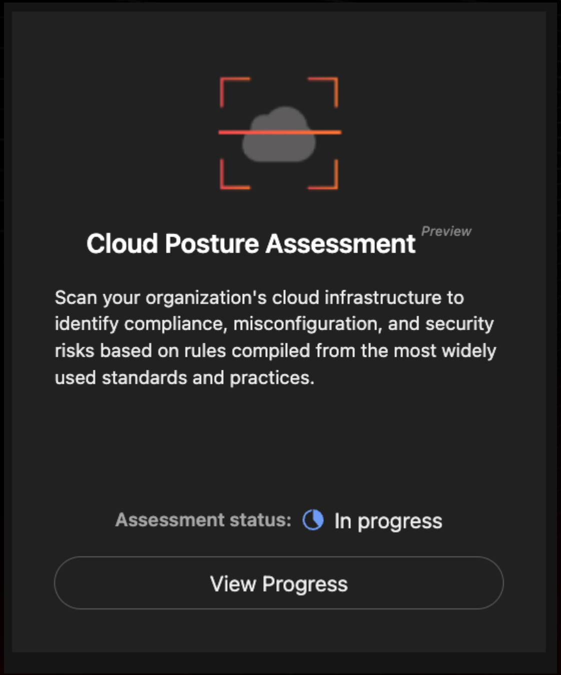
```
mv ~/cloud-account-management-terraform-gcp.tf ./cloud-account-management-terraform-gcp.tf
```

✓ Use the following command to run the resource creation script in your Cloud Shell:

```
terraform init && terraform apply
```

Check this link for the full steps if needed: [Adding a Google Cloud project | Trend Micro Service Central]

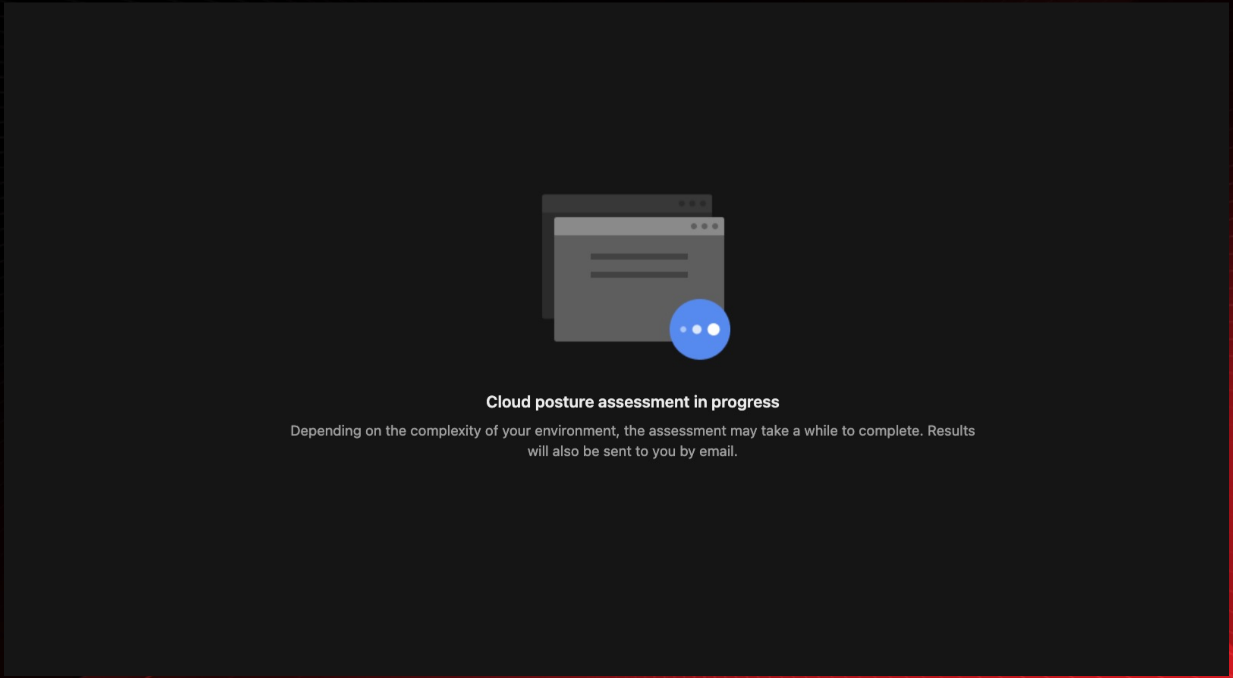
End to End Steps



Cloud Posture Assessment *Preview*

Scan your organization's cloud infrastructure to identify compliance, misconfiguration, and security risks based on rules compiled from the most widely used standards and practices.

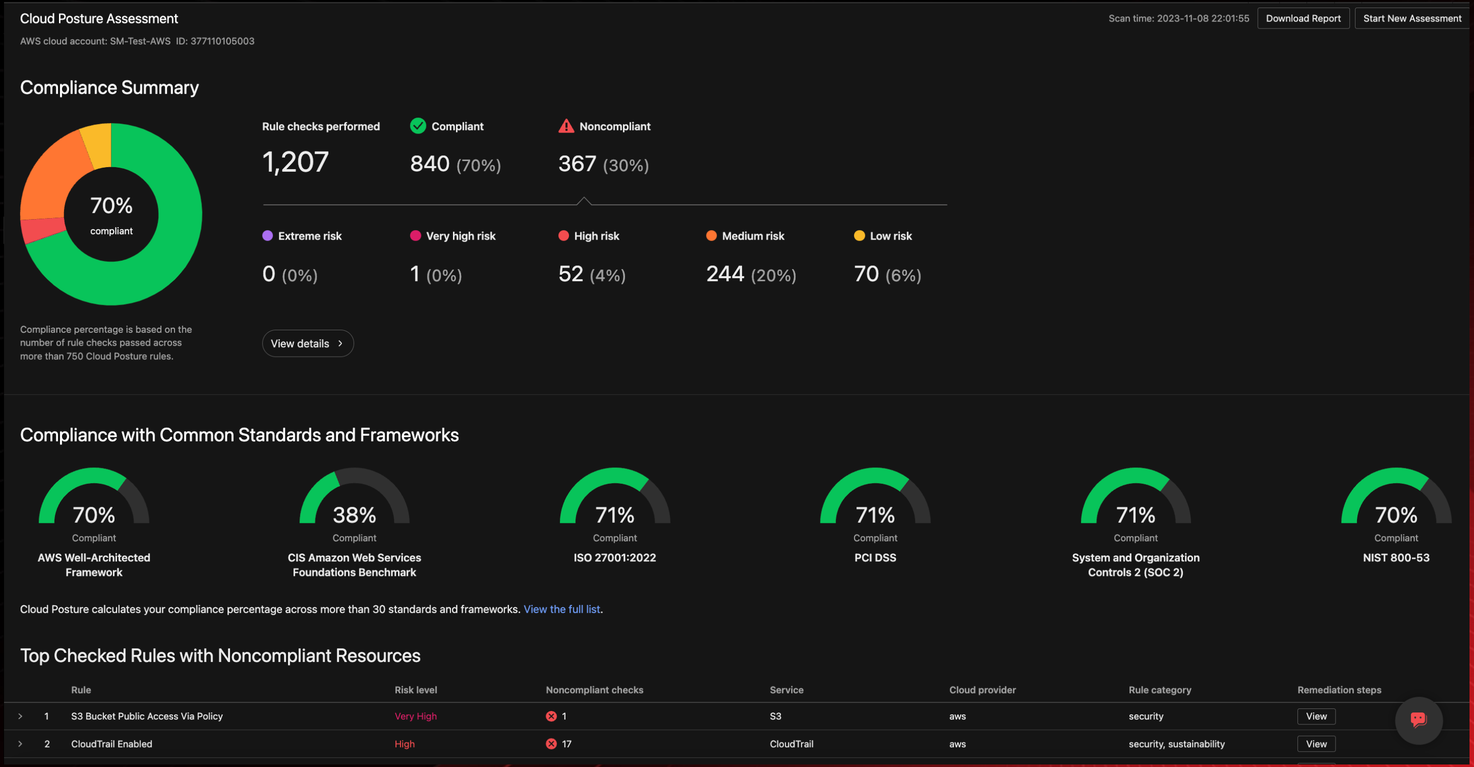
Assessment status: In progress



Cloud posture assessment in progress

Depending on the complexity of your environment, the assessment may take a while to complete. Results will also be sent to you by email.

Cloud Posture Assessment Sample Report



Cloud Posture Assessment

AWS cloud account: SM-Test-AWS ID: 377110105003

Scan time: 2023-11-08 22:01:55

Compliance Summary

Compliance percentage is based on the number of rule checks passed across more than 750 Cloud Posture rules.

Rule checks performed	✓ Compliant	⚠ Noncompliant
1,207	840 (70%)	367 (30%)

● Extreme risk	● Very high risk	● High risk	● Medium risk	● Low risk
0 (0%)	1 (0%)	52 (4%)	244 (20%)	70 (6%)

Compliance with Common Standards and Frameworks

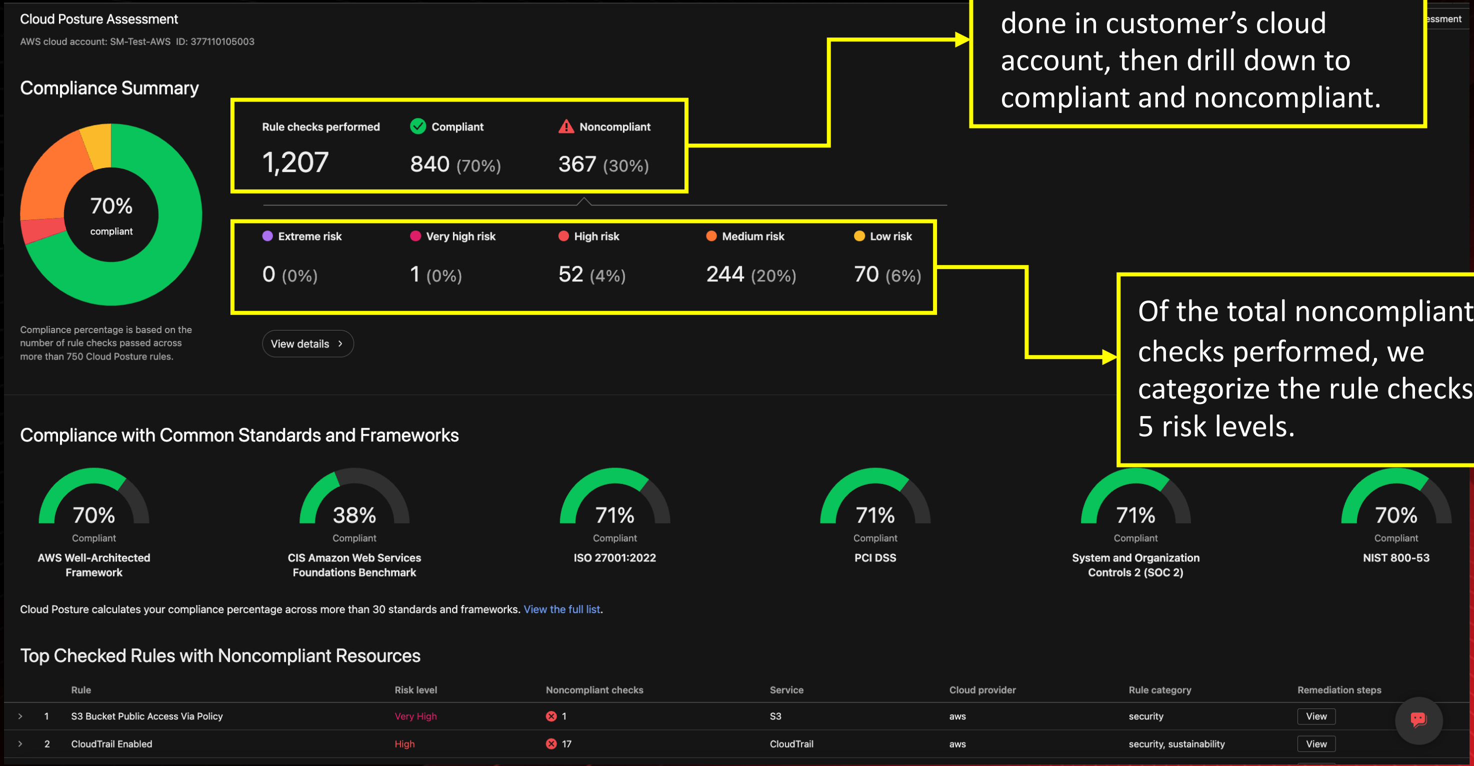
AWS Well-Architected Framework	CIS Amazon Web Services Foundations Benchmark	ISO 27001:2022	PCI DSS	System and Organization Controls 2 (SOC 2)	NIST 800-53
70% Compliant	38% Compliant	71% Compliant	71% Compliant	71% Compliant	70% Compliant

Cloud Posture calculates your compliance percentage across more than 30 standards and frameworks. View the full list.

Top Checked Rules with Noncompliant Resources

		Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
›	1	S3 Bucket Public Access Via Policy	Very High	✖ 1	S3	aws	security	View
›	2	CloudTrail Enabled	High	✖ 17	CloudTrail	aws	security, sustainability	View

Cloud Posture Assessment Report



Cloud Posture Assessment

AWS cloud account: SM-Test-AWS ID: 377110105003

essment

Compliance Summary

Rule checks performed	✓ Compliant	⚠ Noncompliant
1,207	840 (70%)	367 (30%)

● Extreme risk	● Very high risk	● High risk	● Medium risk	● Low risk
0 (0%)	1 (0%)	52 (4%)	244 (20%)	70 (6%)

Compliance percentage is based on the number of rule checks passed across more than 750 Cloud Posture rules.

View details ›

Compliance with Common Standards and Frameworks

70% Compliant	38% Compliant	71% Compliant	71% Compliant	71% Compliant	70% Compliant
AWS Well-Architected Framework	CIS Amazon Web Services Foundations Benchmark	ISO 27001:2022	PCI DSS	System and Organization Controls 2 (SOC 2)	NIST 800-53

Cloud Posture calculates your compliance percentage across more than 30 standards and frameworks. View the full list.

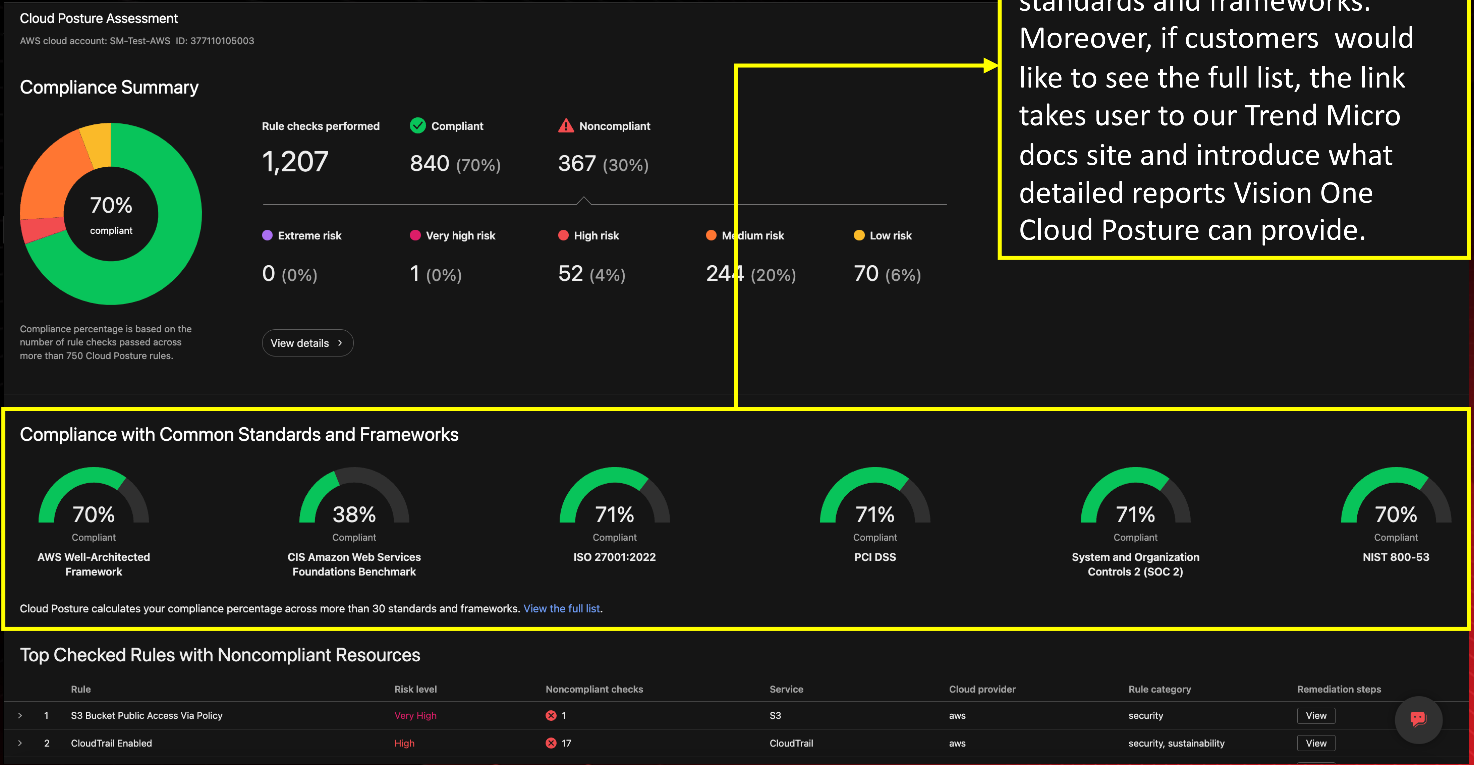
Top Checked Rules with Noncompliant Resources

		Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
›	1	S3 Bucket Public Access Via Policy	Very High	⊗ 1	S3	aws	security	View
›	2	CloudTrail Enabled	High	⊗ 17	CloudTrail	aws	security, sustainability	View

Total number of rule checks done in customer's cloud account, then drill down to compliant and noncompliant.

Of the total noncompliant rule checks performed, we categorize the rule checks into 5 risk levels.

Cloud Posture Assessment Report



Cloud Posture Assessment

AWS cloud account: SM-Test-AWS ID: 377110105003

Compliance Summary

Rule checks performed: 1,207

✓ Compliant: 840 (70%)

⚠ Noncompliant: 367 (30%)

● Extreme risk	● Very high risk	● High risk	● Medium risk	● Low risk
0 (0%)	1 (0%)	52 (4%)	244 (20%)	70 (6%)

Compliance percentage is based on the number of rule checks passed across more than 750 Cloud Posture rules.

View details ›

Compliance with Common Standards and Frameworks

AWS Well-Architected Framework	CIS Amazon Web Services Foundations Benchmark	ISO 27001:2022	PCI DSS	System and Organization Controls 2 (SOC 2)	NIST 800-53
70% Compliant	38% Compliant	71% Compliant	71% Compliant	71% Compliant	70% Compliant

Cloud Posture calculates your compliance percentage across more than 30 standards and frameworks. View the full list.

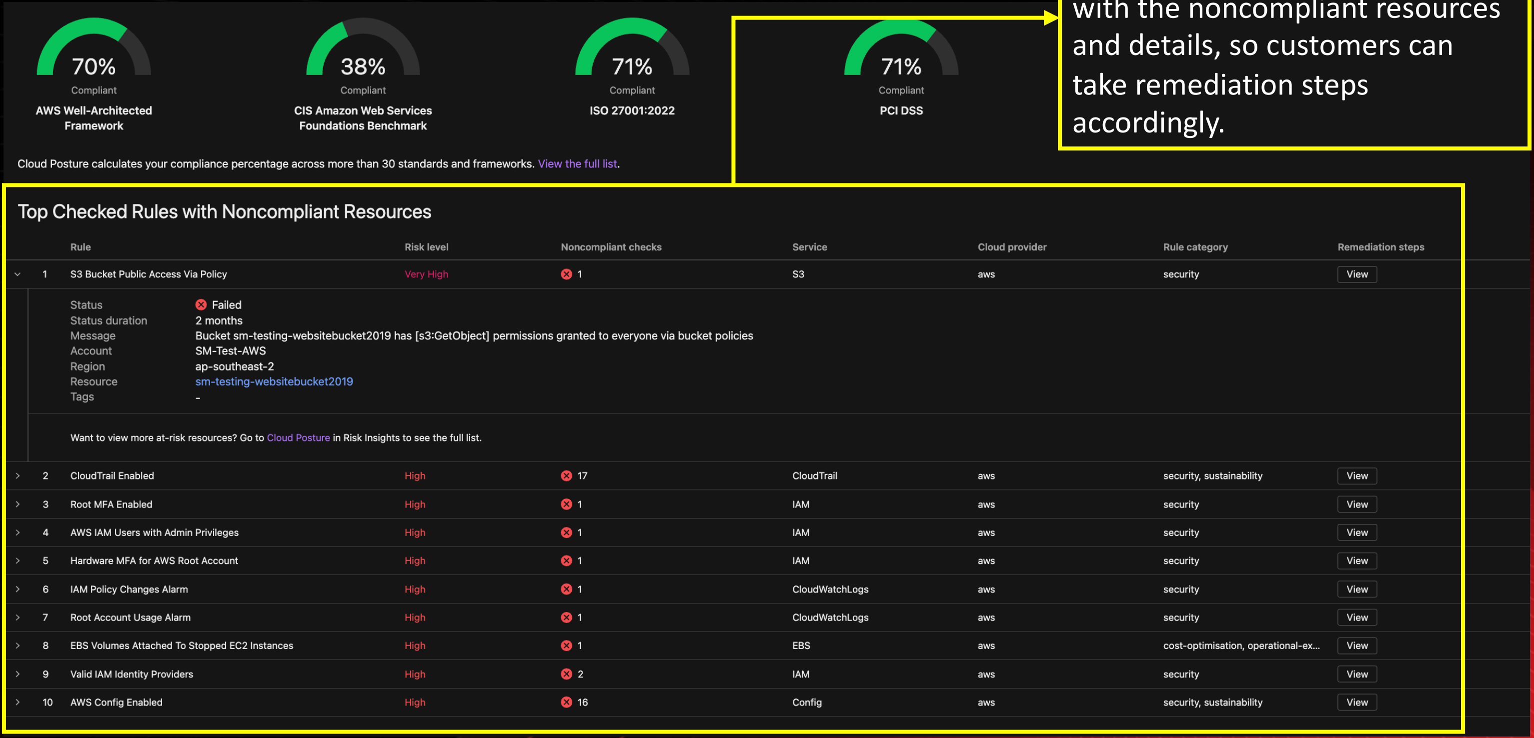
Top Checked Rules with Noncompliant Resources

		Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
›	1	S3 Bucket Public Access Via Policy	Very High	☒ 1	S3	aws	security	View
›	2	CloudTrail Enabled	High	☒ 17	CloudTrail	aws	security, sustainability	View

This section shows compliance percentage against common standards and frameworks. Moreover, if customers would like to see the full list, the link takes user to our Trend Micro docs site and introduce what detailed reports Vision One Cloud Posture can provide.

Cloud Posture Assessment Report

This section shows the top checked rules, order by risk level, with the noncompliant resources and details, so customers can take remediation steps accordingly.



70% Compliant	38% Compliant	71% Compliant	71% Compliant
AWS Well-Architected Framework	CIS Amazon Web Services Foundations Benchmark	ISO 27001:2022	PCI DSS

Cloud Posture calculates your compliance percentage across more than 30 standards and frameworks. View the full list.

Top Checked Rules with Noncompliant Resources

		Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
˅	1	S3 Bucket Public Access Via Policy	Very High	✗ 1	S3	aws	security	View

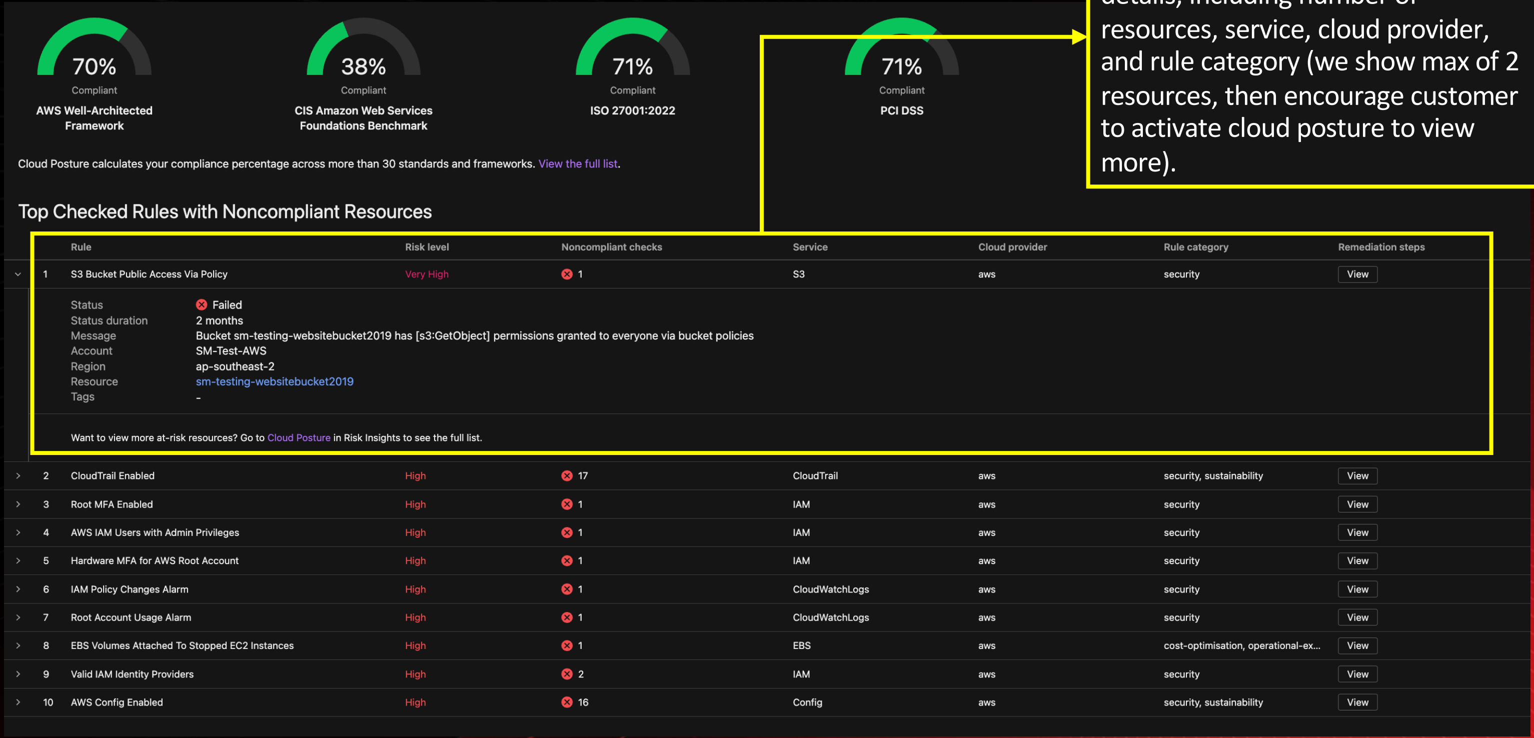
Status	✗ Failed
Status duration	2 months
Message	Bucket sm-testing-websitebucket2019 has [s3:GetObject] permissions granted to everyone via bucket policies
Account	SM-Test-AWS
Region	ap-southeast-2
Resource	sm-testing-websitebucket2019
Tags	-

Want to view more at-risk resources? Go to Cloud Posture in Risk Insights to see the full list.

		Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
›	2	CloudTrail Enabled	High	✗ 17	CloudTrail	aws	security, sustainability	View
›	3	Root MFA Enabled	High	✗ 1	IAM	aws	security	View
›	4	AWS IAM Users with Admin Privileges	High	✗ 1	IAM	aws	security	View
›	5	Hardware MFA for AWS Root Account	High	✗ 1	IAM	aws	security	View
›	6	IAM Policy Changes Alarm	High	✗ 1	CloudWatchLogs	aws	security	View
›	7	Root Account Usage Alarm	High	✗ 1	CloudWatchLogs	aws	security	View
›	8	EBS Volumes Attached To Stopped EC2 Instances	High	✗ 1	EBS	aws	cost-optimisation, operational-ex...	View
›	9	Valid IAM Identity Providers	High	✗ 2	IAM	aws	security	View
›	10	AWS Config Enabled	High	✗ 16	Config	aws	security, sustainability	View

Cloud Posture Assessment Report

Customer can click on the arrow on the left to view each failed rule in details, including number of resources, service, cloud provider, and rule category (we show max of 2 resources, then encourage customer to activate cloud posture to view more).



70% Compliant
AWS Well-Architected Framework

38% Compliant
CIS Amazon Web Services Foundations Benchmark

71% Compliant
ISO 27001:2022

71% Compliant
PCI DSS

Cloud Posture calculates your compliance percentage across more than 30 standards and frameworks. View the full list.

Top Checked Rules with Noncompliant Resources

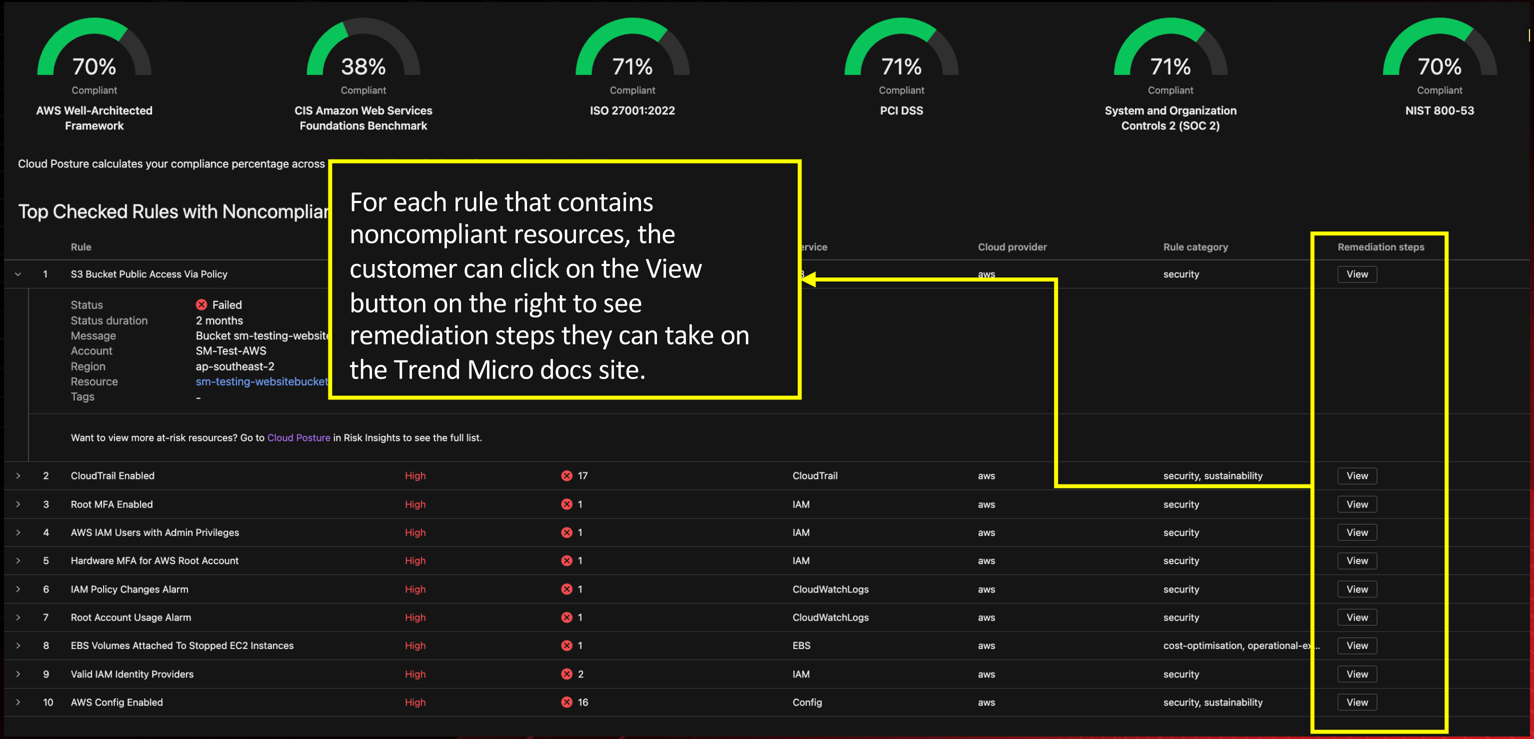
	Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
1	S3 Bucket Public Access Via Policy	Very High	☒ 1	S3	aws	security	View

Status: ☒ Failed
Status duration: 2 months
Message: Bucket sm-testing-websitebucket2019 has [s3:GetObject] permissions granted to everyone via bucket policies
Account: SM-Test-AWS
Region: ap-southeast-2
Resource: sm-testing-websitebucket2019
Tags: -

Want to view more at-risk resources? Go to Cloud Posture in Risk Insights to see the full list.

	Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
2	CloudTrail Enabled	High	☒ 17	CloudTrail	aws	security, sustainability	View
3	Root MFA Enabled	High	☒ 1	IAM	aws	security	View
4	AWS IAM Users with Admin Privileges	High	☒ 1	IAM	aws	security	View
5	Hardware MFA for AWS Root Account	High	☒ 1	IAM	aws	security	View
6	IAM Policy Changes Alarm	High	☒ 1	CloudWatchLogs	aws	security	View
7	Root Account Usage Alarm	High	☒ 1	CloudWatchLogs	aws	security	View
8	EBS Volumes Attached To Stopped EC2 Instances	High	☒ 1	EBS	aws	cost-optimisation, operational-ex...	View
9	Valid IAM Identity Providers	High	☒ 2	IAM	aws	security	View
10	AWS Config Enabled	High	☒ 16	Config	aws	security, sustainability	View

Cloud Posture Assessment Report



70% Compliant **AWS Well-Architected Framework**	38% Compliant **CIS Amazon Web Services Foundations Benchmark**	71% Compliant **ISO 27001:2022**	71% Compliant **PCI DSS**	71% Compliant **System and Organization Controls 2 (SOC 2)**	70% Compliant **NIST 800-53**

Cloud Posture calculates your compliance percentage across

Top Checked Rules with Noncomplian

		Rule			ervice	Cloud provider	Rule category	Remediation steps
⌄	1	S3 Bucket Public Access Via Policy			3	aws	security	View
›	2	CloudTrail Enabled	High	☒ 17	CloudTrail	aws	security, sustainability	View
›	3	Root MFA Enabled	High	☒ 1	IAM	aws	security	View
›	4	AWS IAM Users with Admin Privileges	High	☒ 1	IAM	aws	security	View
›	5	Hardware MFA for AWS Root Account	High	☒ 1	IAM	aws	security	View
›	6	IAM Policy Changes Alarm	High	☒ 1	CloudWatchLogs	aws	security	View
›	7	Root Account Usage Alarm	High	☒ 1	CloudWatchLogs	aws	security	View
›	8	EBS Volumes Attached To Stopped EC2 Instances	High	☒ 1	EBS	aws	cost-optimisation, operational-ex...	View
›	9	Valid IAM Identity Providers	High	☒ 2	IAM	aws	security	View
›	10	AWS Config Enabled	High	☒ 16	Config	aws	security, sustainability	View

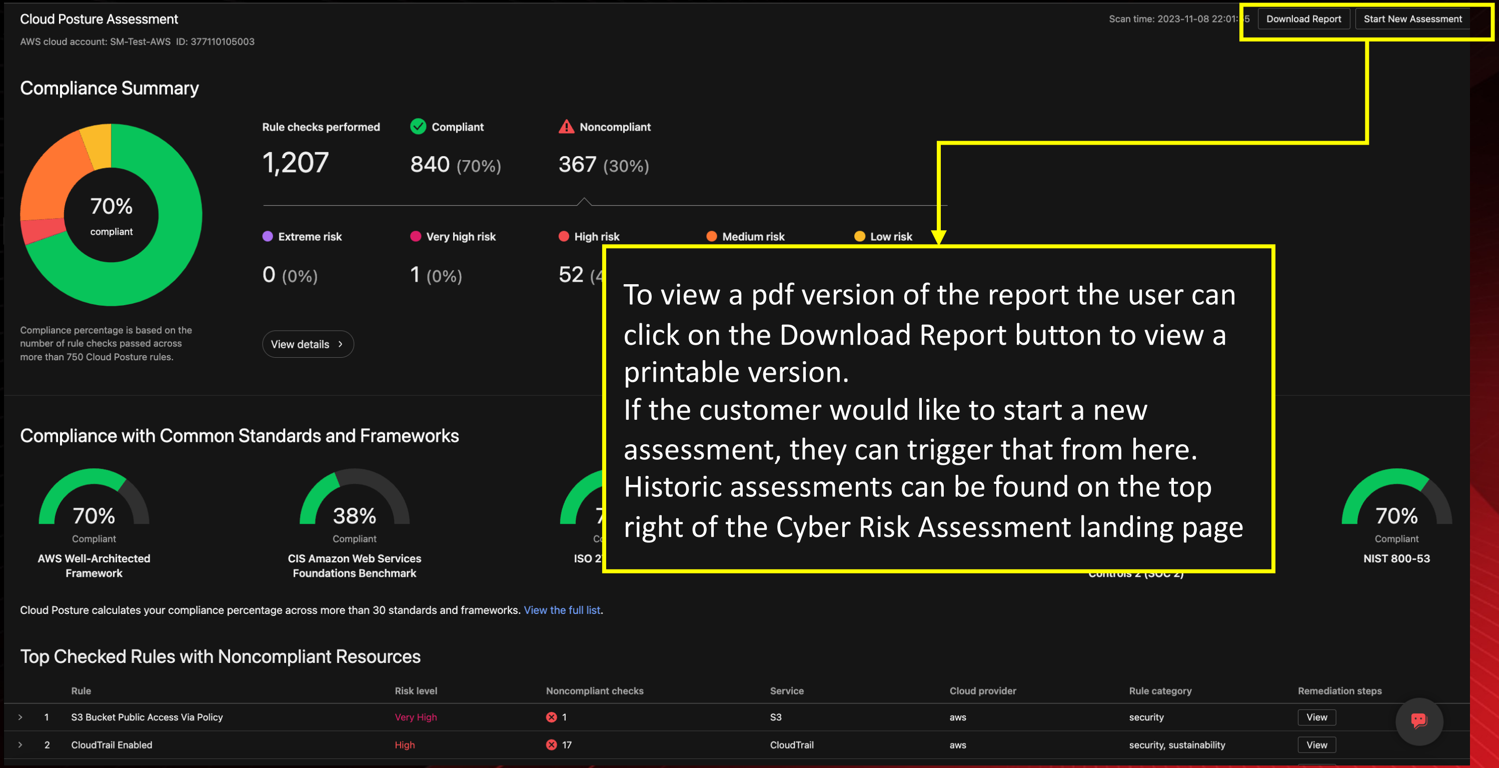
Row 1 details:

Status	☒ Failed
Status duration	2 months
Message	Bucket sm-testing-website
Account	SM-Test-AWS
Region	ap-southeast-2
Resource	sm-testing-websitebucket
Tags	-

Want to view more at-risk resources? Go to Cloud Posture in Risk Insights to see the full list.

For each rule that contains noncompliant resources, the customer can click on the View button on the right to see remediation steps they can take on the Trend Micro docs site.

End to End Flow



Cloud Posture Assessment

AWS cloud account: SM-Test-AWS ID: 377110105003

Scan time: 2023-11-08 22:01:5

Compliance Summary

Compliance percentage is based on the number of rule checks passed across more than 750 Cloud Posture rules.

Rule checks performed	✓ Compliant	⚠ Noncompliant
1,207	840 (70%)	367 (30%)

● Extreme risk	● Very high risk	● High risk	● Medium risk	● Low risk
0 (0%)	1 (0%)	52 (4		

Compliance with Common Standards and Frameworks

70%
Compliant
AWS Well-Architected Framework
38%
Compliant
CIS Amazon Web Services Foundations Benchmark
7
Co
ISO 2
Controls 2 (SOC 2)
70%
Compliant
NIST 800-53

Cloud Posture calculates your compliance percentage across more than 30 standards and frameworks. View the full list.

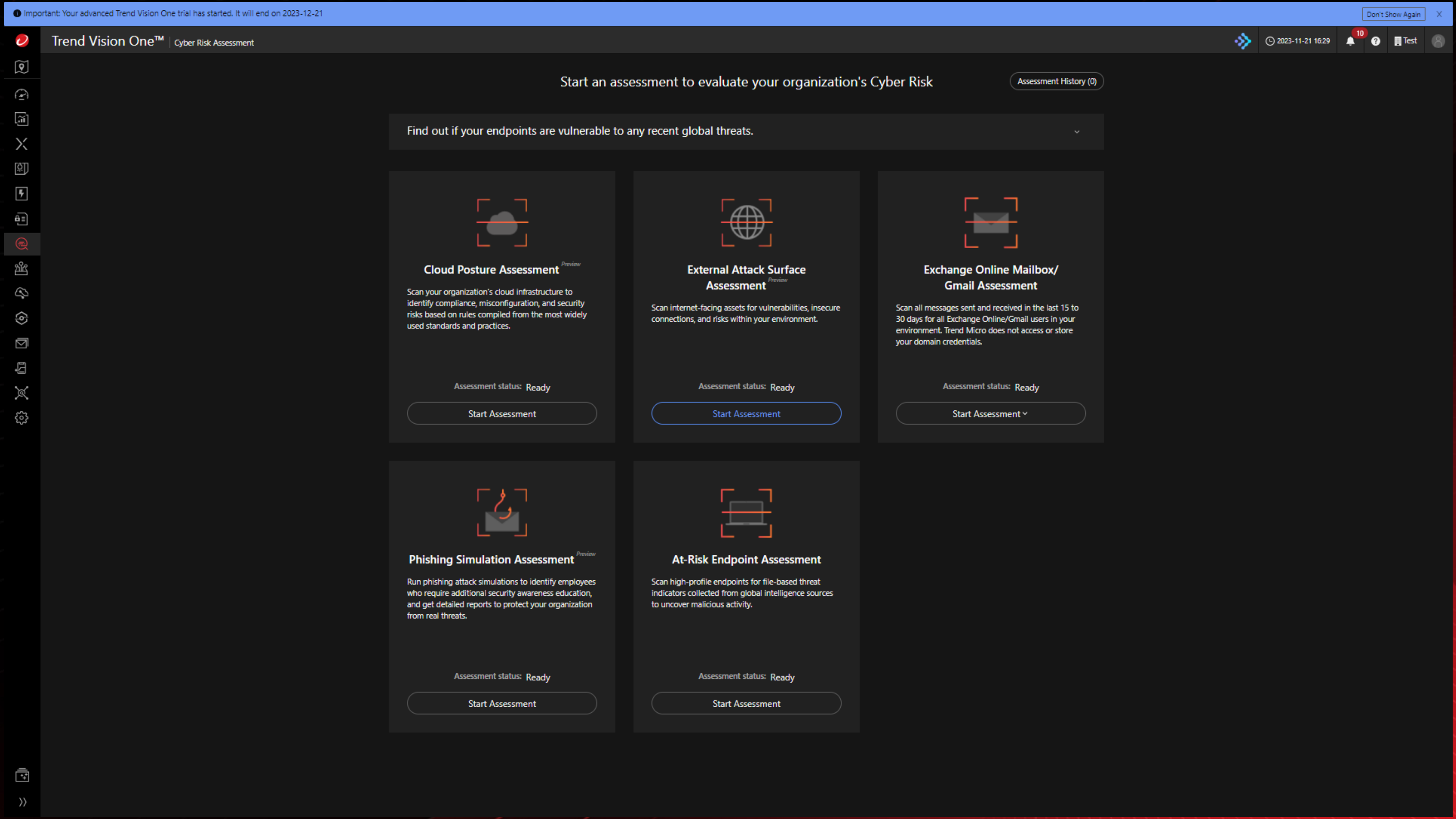
Top Checked Rules with Noncompliant Resources

		Rule	Risk level	Noncompliant checks	Service	Cloud provider	Rule category	Remediation steps
›	1	S3 Bucket Public Access Via Policy	Very High	☒ 1	S3	aws	security	View
›	2	CloudTrail Enabled	High	☒ 17	CloudTrail	aws	security, sustainability	View

To view a pdf version of the report the user can click on the Download Report button to view a printable version.
If the customer would like to start a new assessment, they can trigger that from here.
Historic assessments can be found on the top right of the Cyber Risk Assessment landing page

External Attack Surface Assessment

Step-by-Step Assessment Walkthrough



Important: Your advanced Trend Vision One trial has started. It will end on 2023-12-21

Start an assessment to evaluate your organization's Cyber Risk

Find out if your endpoints are vulnerable to any recent global threats.

Cloud Posture Assessment *Preview*

Scan your organization's cloud infrastructure to identify compliance, misconfiguration, and security risks based on rules compiled from the most widely used standards and practices.

Assessment status: Ready

External Attack Surface Assessment *Preview*

Scan internet-facing assets for vulnerabilities, insecure connections, and risks within your environment.

Assessment status: Ready

Exchange Online Mailbox/ Gmail Assessment

Scan all messages sent and received in the last 15 to 30 days for all Exchange Online/Gmail users in your environment. Trend Micro does not access or store your domain credentials.

Assessment status: Ready

Phishing Simulation Assessment *Preview*

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

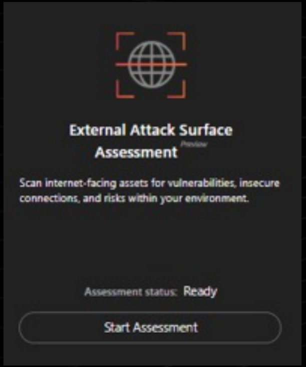
Assessment status: Ready

At-Risk Endpoint Assessment

Scan high-profile endpoints for file-based threat indicators collected from global intelligence sources to uncover malicious activity.

Assessment status: Ready

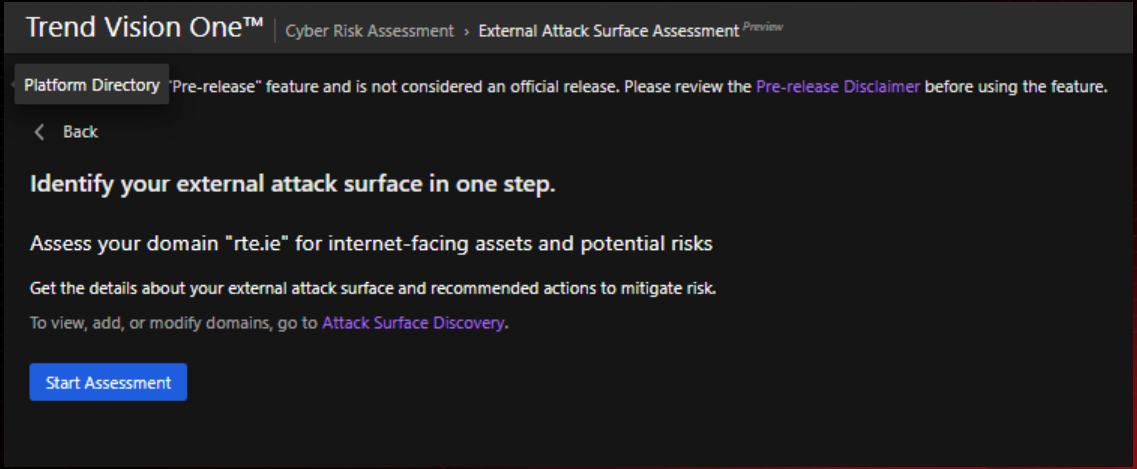
End to End Flow



External Attack Surface Assessment Preview

Scan internet-facing assets for vulnerabilities, insecure connections, and risks within your environment.

Assessment status: Ready



Trend Vision One™
Cyber Risk Assessment › External Attack Surface Assessment Preview
Platform Directory
Back
Start Assessment

"Pre-release" feature and is not considered an official release. Please review the Pre-release Disclaimer before using the feature.

Identify your external attack surface in one step.

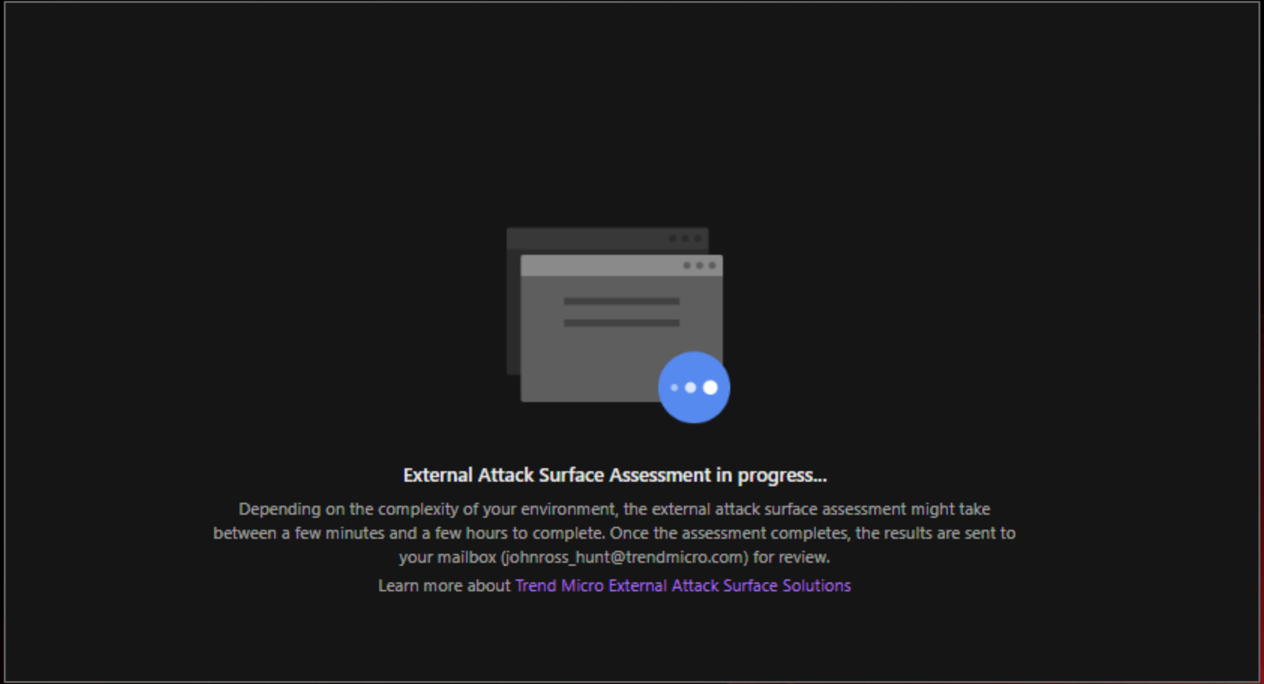
Assess your domain "rte.ie" for internet-facing assets and potential risks

Get the details about your external attack surface and recommended actions to mitigate risk.

To view, add, or modify domains, go to Attack Surface Discovery.

- After entering the EAS Assessment, the customer's email domain is automatically added.
- Additional domains cannot be added from within the assessment.
- If the customer would like to add additional domains, this can be done from the Attack Surface Discovery app.
  - Note: Customers will need to assign credits or start a trial to access the ASD app.

End to End Flow



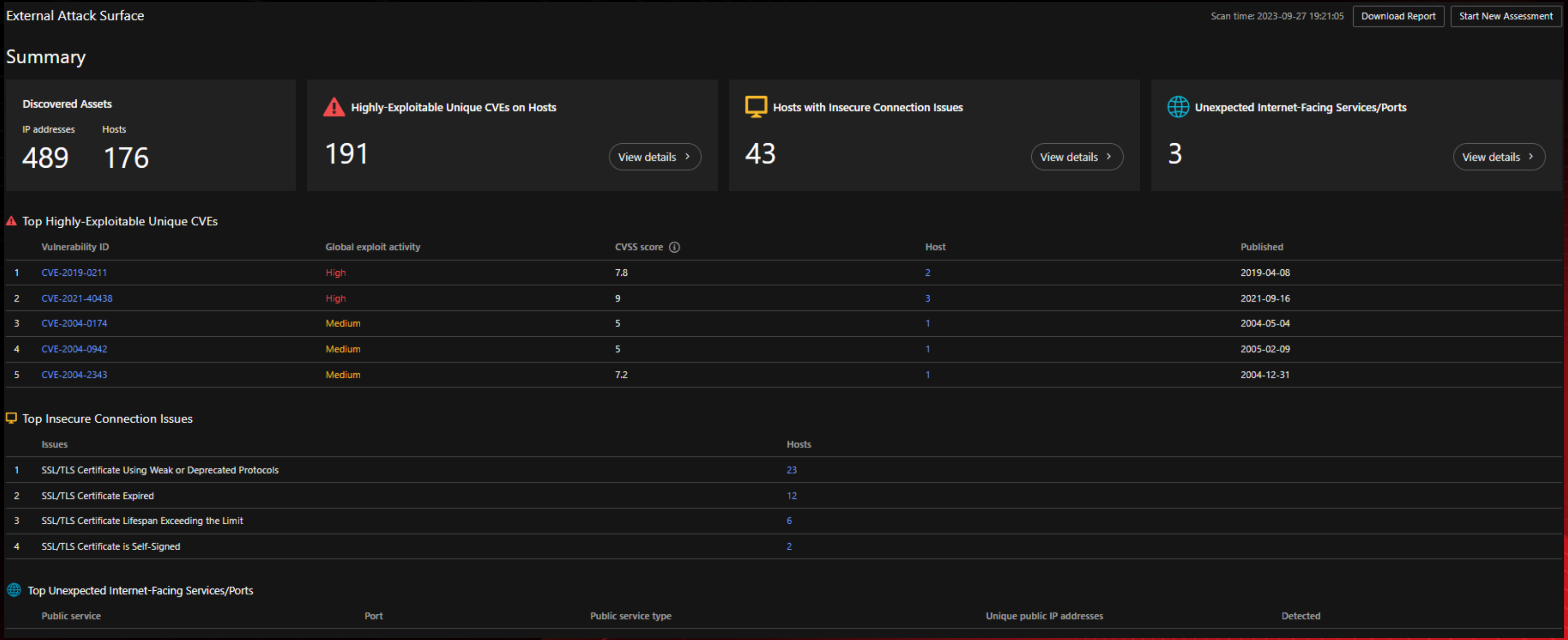
External Attack Surface Assessment in progress...

Depending on the complexity of your environment, the external attack surface assessment might take between a few minutes and a few hours to complete. Once the assessment completes, the results are sent to your mailbox (johnross_hunt@trendmicro.com) for review.

Learn more about Trend Micro External Attack Surface Solutions

- Depending on the complexity of the customer’s environment and the number of assets discovered the scan could take some time to complete.
- The user will receive an email notification once the results are ready.

EAS Assessment Report



External Attack Surface

Scan time: 2023-09-27 19:21:05

Summary

Discovered Assets

IP addresses 489

Hosts 176

Highly-Exploitable Unique CVEs on Hosts

191

Hosts with Insecure Connection Issues

43

Unexpected Internet-Facing Services/Ports

3

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score ⓘ	Host	Published
1	CVE-2019-0211	High	7.8	2	2019-04-08
2	CVE-2021-40438	High	9	3	2021-09-16
3	CVE-2004-0174	Medium	5	1	2004-05-04
4	CVE-2004-0942	Medium	5	1	2005-02-09
5	CVE-2004-2343	Medium	7.2	1	2004-12-31

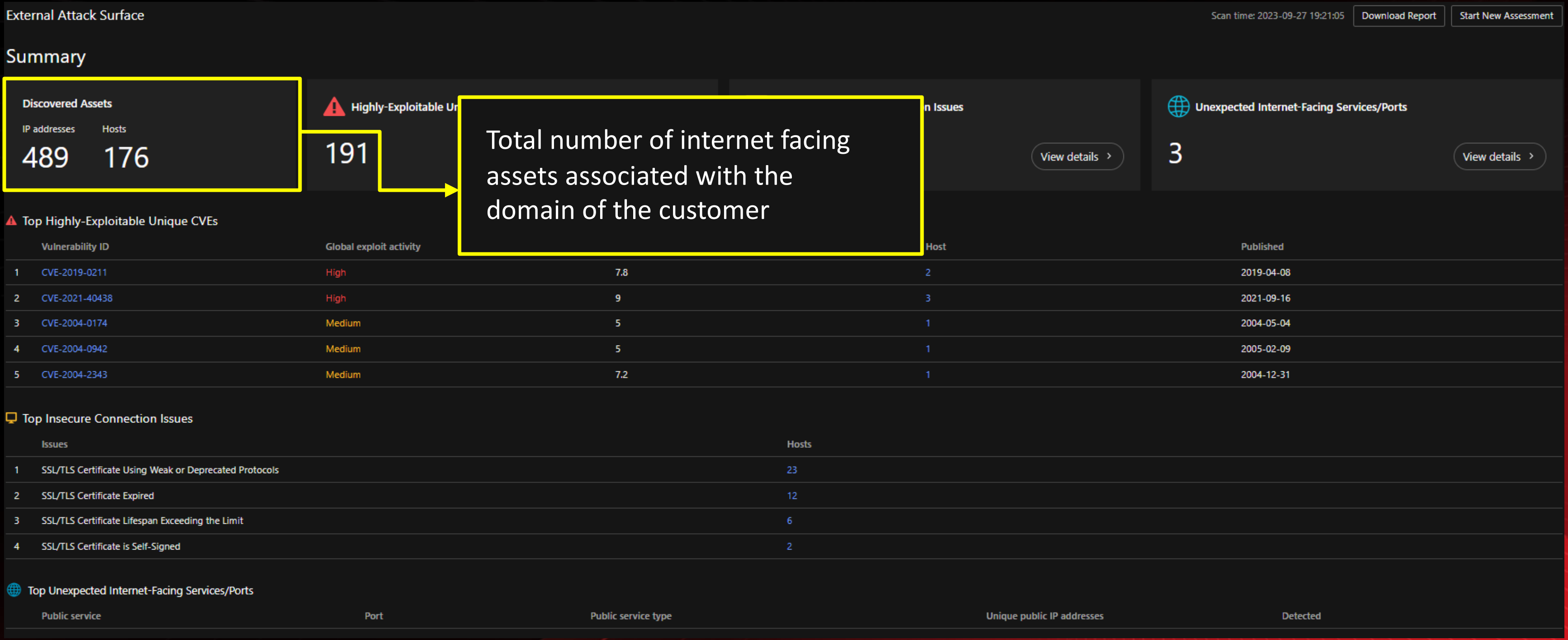
Top Insecure Connection Issues

	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

Public service	Port	Public service type	Unique public IP addresses	Detected

EAS Assessment Report



External Attack Surface

Scan time: 2023-09-27 19:21:05 | Download Report | Start New Assessment

Summary

Discovered Assets

IP addresses 489

Hosts 176

Highly-Exploitable Un

191

n Issues

View details ›

Unexpected Internet-Facing Services/Ports

3

View details ›

Total number of internet facing assets associated with the domain of the customer

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity		Host	Published
1	CVE-2019-0211	High	7.8	2	2019-04-08
2	CVE-2021-40438	High	9	3	2021-09-16
3	CVE-2004-0174	Medium	5	1	2004-05-04
4	CVE-2004-0942	Medium	5	1	2005-02-09
5	CVE-2004-2343	Medium	7.2	1	2004-12-31

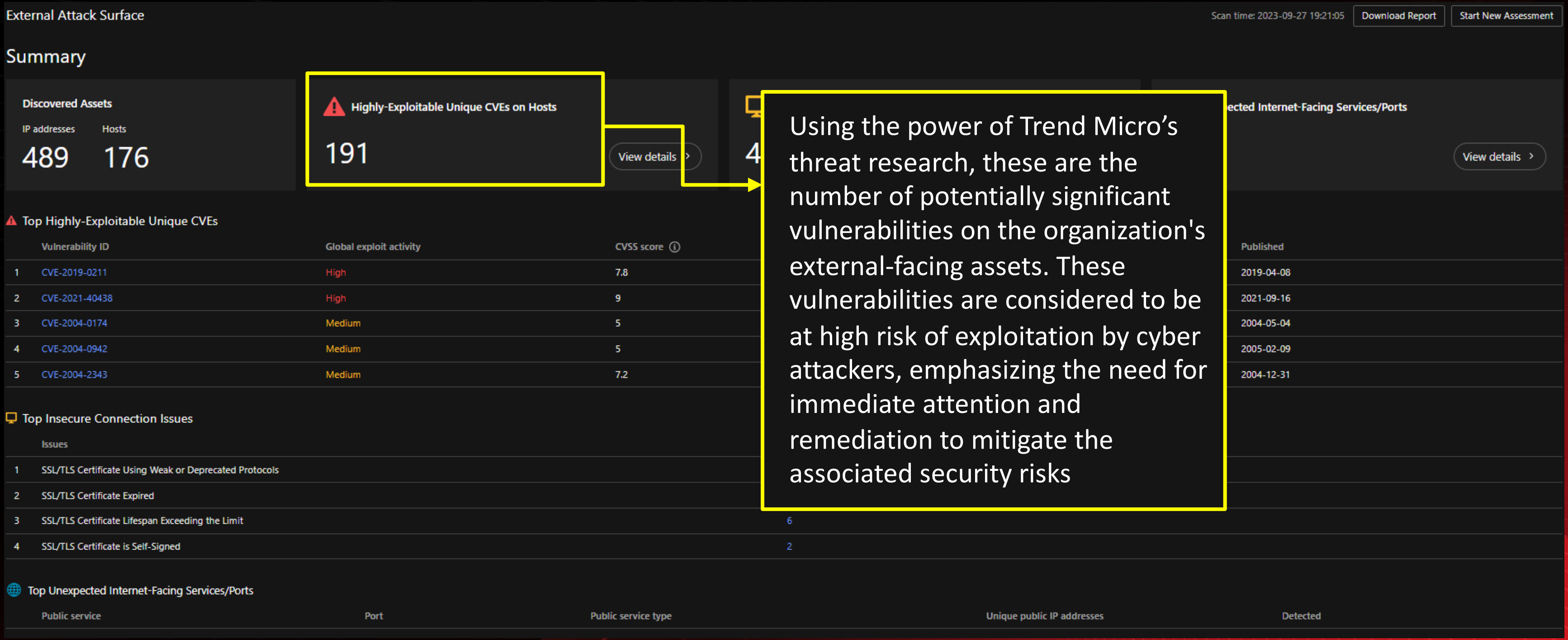
Top Insecure Connection Issues

	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

Public service	Port	Public service type	Unique public IP addresses	Detected

EAS Assessment Report



External Attack Surface

Scan time: 2023-09-27 19:21:05

Summary

Discovered Assets

IP addresses 489

Hosts 176

Highly-Exploitable Unique CVEs on Hosts

191

ected Internet-Facing Services/Ports

Using the power of Trend Micro's threat research, these are the number of potentially significant vulnerabilities on the organization's external-facing assets. These vulnerabilities are considered to be at high risk of exploitation by cyber attackers, emphasizing the need for immediate attention and remediation to mitigate the associated security risks

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score ⓘ	Published
1	CVE-2019-0211	High	7.8	2019-04-08
2	CVE-2021-40438	High	9	2021-09-16
3	CVE-2004-0174	Medium	5	2004-05-04
4	CVE-2004-0942	Medium	5	2005-02-09
5	CVE-2004-2343	Medium	7.2	2004-12-31

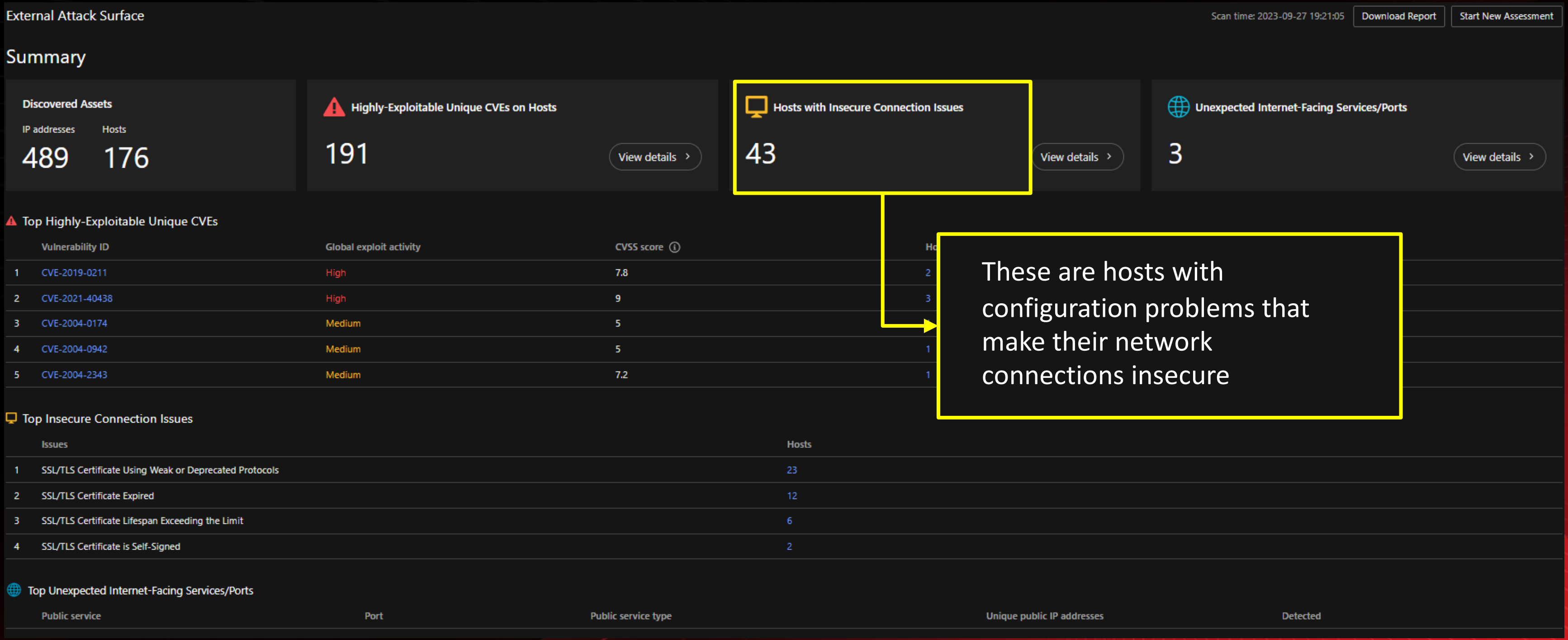
Top Insecure Connection Issues

	Issues	
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	
2	SSL/TLS Certificate Expired	
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

Public service	Port	Public service type	Unique public IP addresses	Detected

EAS Assessment Report



External Attack Surface

Scan time: 2023-09-27 19:21:05 | Download Report | Start New Assessment

Summary

Discovered Assets

IP addresses	Hosts
489	176

Highly-Exploitable Unique CVEs on Hosts

191

View details ›

Hosts with Insecure Connection Issues

43

View details ›

Unexpected Internet-Facing Services/Ports

3

View details ›

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score ⓘ	Ho
1	CVE-2019-0211	High	7.8	2
2	CVE-2021-40438	High	9	3
3	CVE-2004-0174	Medium	5	
4	CVE-2004-0942	Medium	5	1
5	CVE-2004-2343	Medium	7.2	1

These are hosts with configuration problems that make their network connections insecure

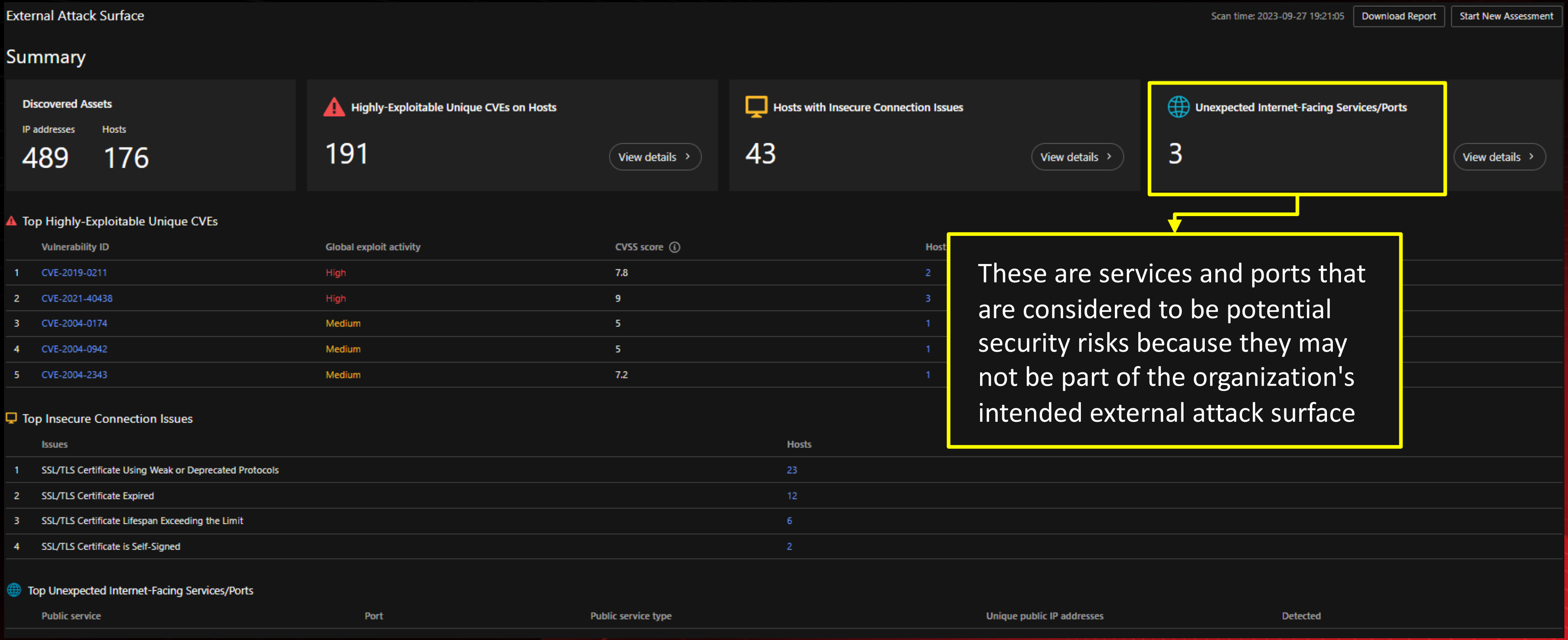
Top Insecure Connection Issues

	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

Public service	Port	Public service type	Unique public IP addresses	Detected

EAS Assessment Report



External Attack Surface

Scan time: 2023-09-27 19:21:05

Summary

Discovered Assets

IP addresses	Hosts
489	176

Highly-Exploitable Unique CVEs on Hosts: 191

Hosts with Insecure Connection Issues: 43

Unexpected Internet-Facing Services/Ports: 3

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score	Host
1	CVE-2019-0211	High	7.8	2
2	CVE-2021-40438	High	9	3
3	CVE-2004-0174	Medium	5	1
4	CVE-2004-0942	Medium	5	1
5	CVE-2004-2343	Medium	7.2	1

Top Insecure Connection Issues

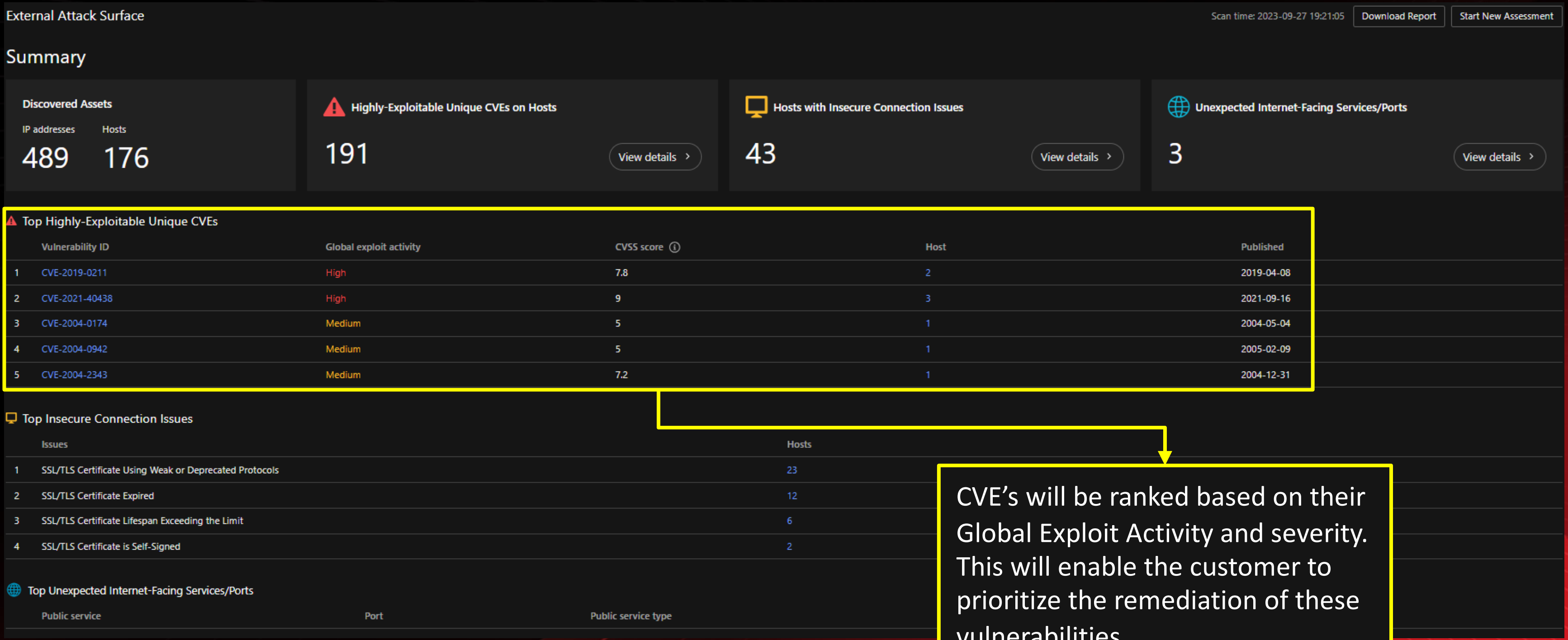
	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

Public service	Port	Public service type	Unique public IP addresses	Detected

These are services and ports that are considered to be potential security risks because they may not be part of the organization's intended external attack surface

EAS Assessment Report



External Attack Surface

Scan time: 2023-09-27 19:21:05

Summary

Discovered Assets		Highly-Exploitable Unique CVEs on Hosts	Hosts with Insecure Connection Issues	Unexpected Internet-Facing Services/Ports
IP addresses	Hosts			
489	176	191	43	3

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score ⓘ	Host	Published
1	CVE-2019-0211	High	7.8	2	2019-04-08
2	CVE-2021-40438	High	9	3	2021-09-16
3	CVE-2004-0174	Medium	5	1	2004-05-04
4	CVE-2004-0942	Medium	5	1	2005-02-09
5	CVE-2004-2343	Medium	7.2	1	2004-12-31

Top Insecure Connection Issues

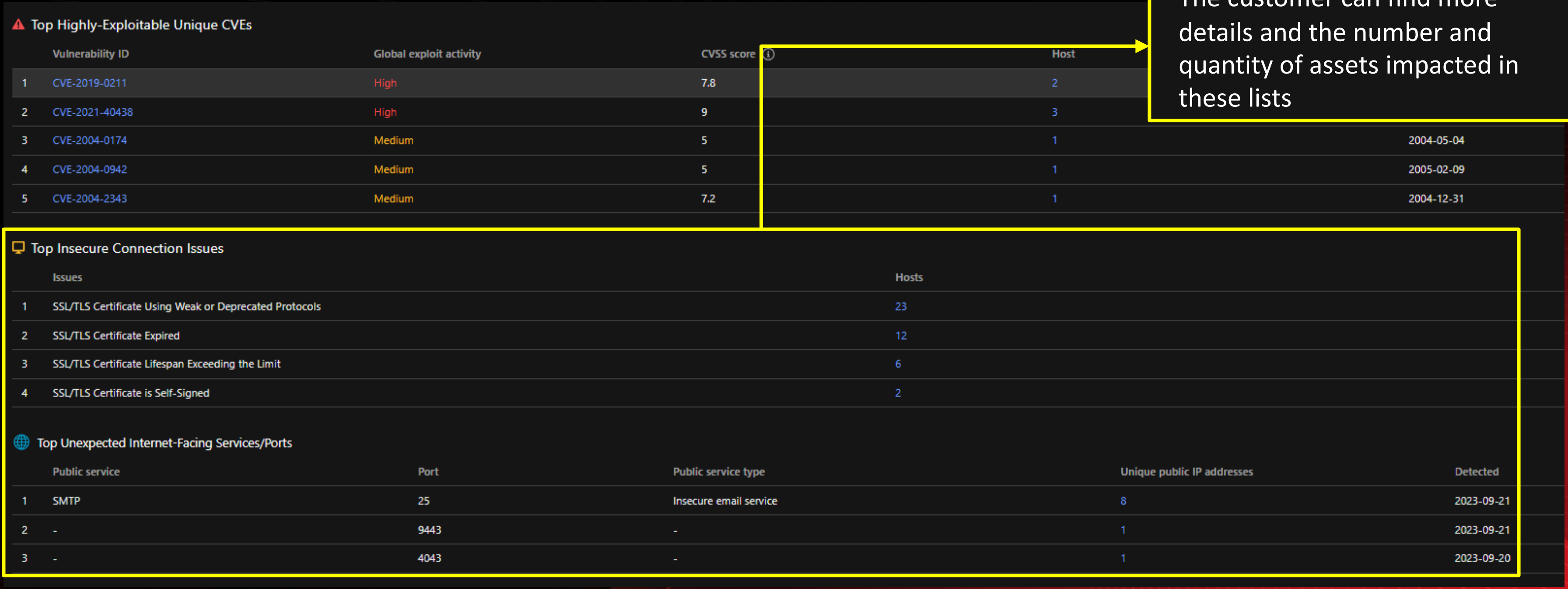
	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

Public service	Port	Public service type

CVE's will be ranked based on their Global Exploit Activity and severity. This will enable the customer to prioritize the remediation of these vulnerabilities

EAS Assessment Report



The customer can find more details and the number and quantity of assets impacted in these lists

⚠ Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score ⓘ	Host	
1	CVE-2019-0211	High	7.8	2	
2	CVE-2021-40438	High	9	3	
3	CVE-2004-0174	Medium	5	1	2004-05-04
4	CVE-2004-0942	Medium	5	1	2005-02-09
5	CVE-2004-2343	Medium	7.2	1	2004-12-31

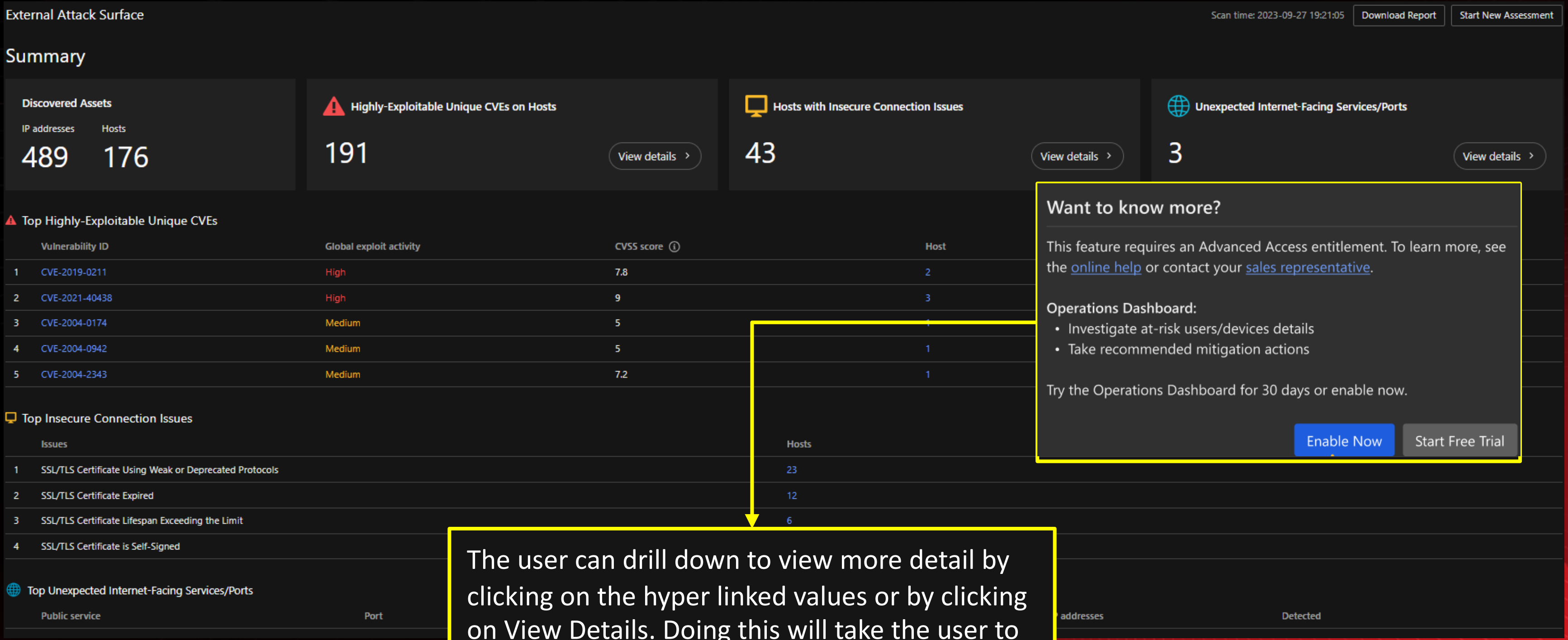
Top Insecure Connection Issues

	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

	Public service	Port	Public service type	Unique public IP addresses	Detected
1	SMTP	25	Insecure email service	8	2023-09-21
2	-	9443	-	1	2023-09-21
3	-	4043	-	1	2023-09-20

End to End Flow



External Attack Surface

Scan time: 2023-09-27 19:21:05

Summary

Discovered Assets

IP addresses 489

Hosts 176

Highly-Exploitable Unique CVEs on Hosts: 191

Hosts with Insecure Connection Issues: 43

Unexpected Internet-Facing Services/Ports: 3

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score ⓘ	Host
1	CVE-2019-0211	High	7.8	2
2	CVE-2021-40438	High	9	3
3	CVE-2004-0174	Medium	5	1
4	CVE-2004-0942	Medium	5	1
5	CVE-2004-2343	Medium	7.2	1

Top Insecure Connection Issues

	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	

Top Unexpected Internet-Facing Services/Ports

Public service	Port	addresses	Detected

Want to know more?

This feature requires an Advanced Access entitlement. To learn more, see the online help or contact your sales representative.

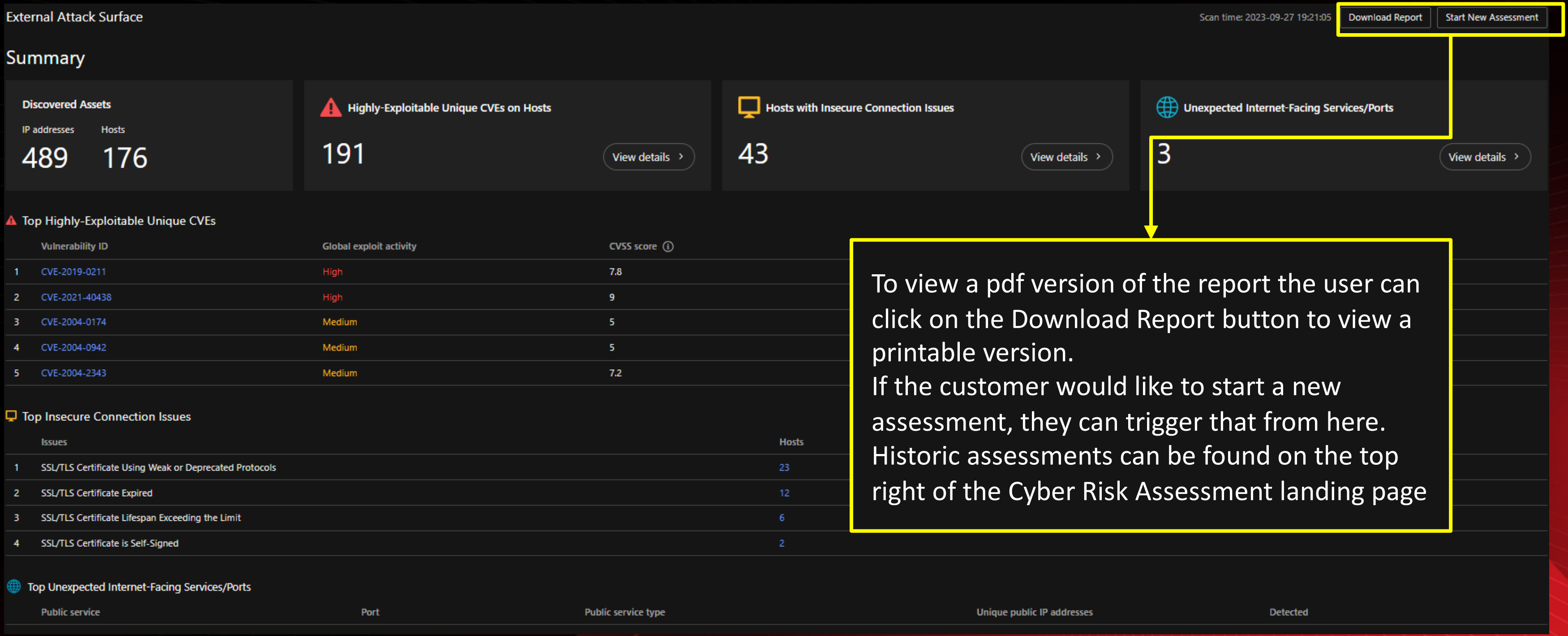
Operations Dashboard:

- Investigate at-risk users/devices details
- Take recommended mitigation actions

Try the Operations Dashboard for 30 days or enable now.

The user can drill down to view more detail by clicking on the hyper linked values or by clicking on View Details. Doing this will take the user to our Attack Surface Risk management trial and once that is started they can view all the detail in the Operations Dashboard.

End to End Flow



External Attack Surface

Scan time: 2023-09-27 19:21:05

Summary

Discovered Assets

IP addresses	Hosts
489	176

Highly-Exploitable Unique CVEs on Hosts

191

Hosts with Insecure Connection Issues

43

Unexpected Internet-Facing Services/Ports

3

Top Highly-Exploitable Unique CVEs

	Vulnerability ID	Global exploit activity	CVSS score ⓘ
1	CVE-2019-0211	High	7.8
2	CVE-2021-40438	High	9
3	CVE-2004-0174	Medium	5
4	CVE-2004-0942	Medium	5
5	CVE-2004-2343	Medium	7.2

Top Insecure Connection Issues

	Issues	Hosts
1	SSL/TLS Certificate Using Weak or Deprecated Protocols	23
2	SSL/TLS Certificate Expired	12
3	SSL/TLS Certificate Lifespan Exceeding the Limit	6
4	SSL/TLS Certificate is Self-Signed	2

Top Unexpected Internet-Facing Services/Ports

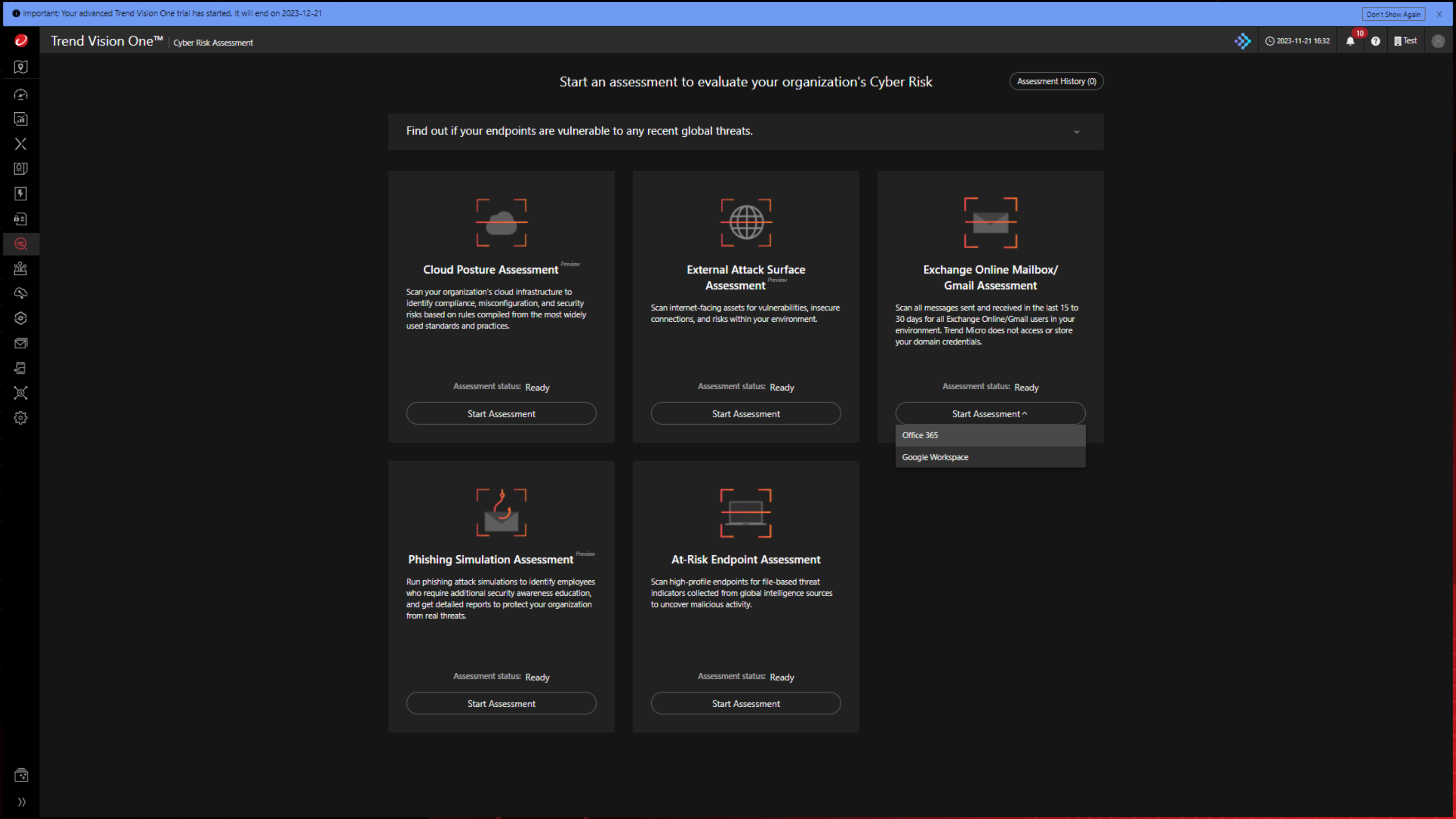
Public service	Port	Public service type	Unique public IP addresses	Detected

To view a pdf version of the report the user can click on the Download Report button to view a printable version.
If the customer would like to start a new assessment, they can trigger that from here.
Historic assessments can be found on the top right of the Cyber Risk Assessment landing page

Exchange Online Mailbox/Gmail Assessment – Office 365

Step-by-Step Assessment Walkthrough

Select Office 365, through “Exchange Online Mailbox/Gmail Assessment”



Important: Your advanced Trend Vision One trial has started. It will end on 2023-12-21

Don't Show Again

Trend Vision One™ | Cyber Risk Assessment

2023-11-21 16:32

Test

Start an assessment to evaluate your organization's Cyber Risk

Assessment History (0)

Find out if your endpoints are vulnerable to any recent global threats.

Cloud Posture Assessment Preview

Scan your organization's cloud infrastructure to identify compliance, misconfiguration, and security risks based on rules compiled from the most widely used standards and practices.

Assessment status: Ready

Start Assessment

External Attack Surface Assessment Preview

Scan internet-facing assets for vulnerabilities, insecure connections, and risks within your environment.

Assessment status: Ready

Start Assessment

Exchange Online Mailbox/ Gmail Assessment

Scan all messages sent and received in the last 15 to 30 days for all Exchange Online/Gmail users in your environment. Trend Micro does not access or store your domain credentials.

Assessment status: Ready

Start Assessment ^

- Office 365
- Google Workspace

Phishing Simulation Assessment Preview

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

Assessment status: Ready

Start Assessment

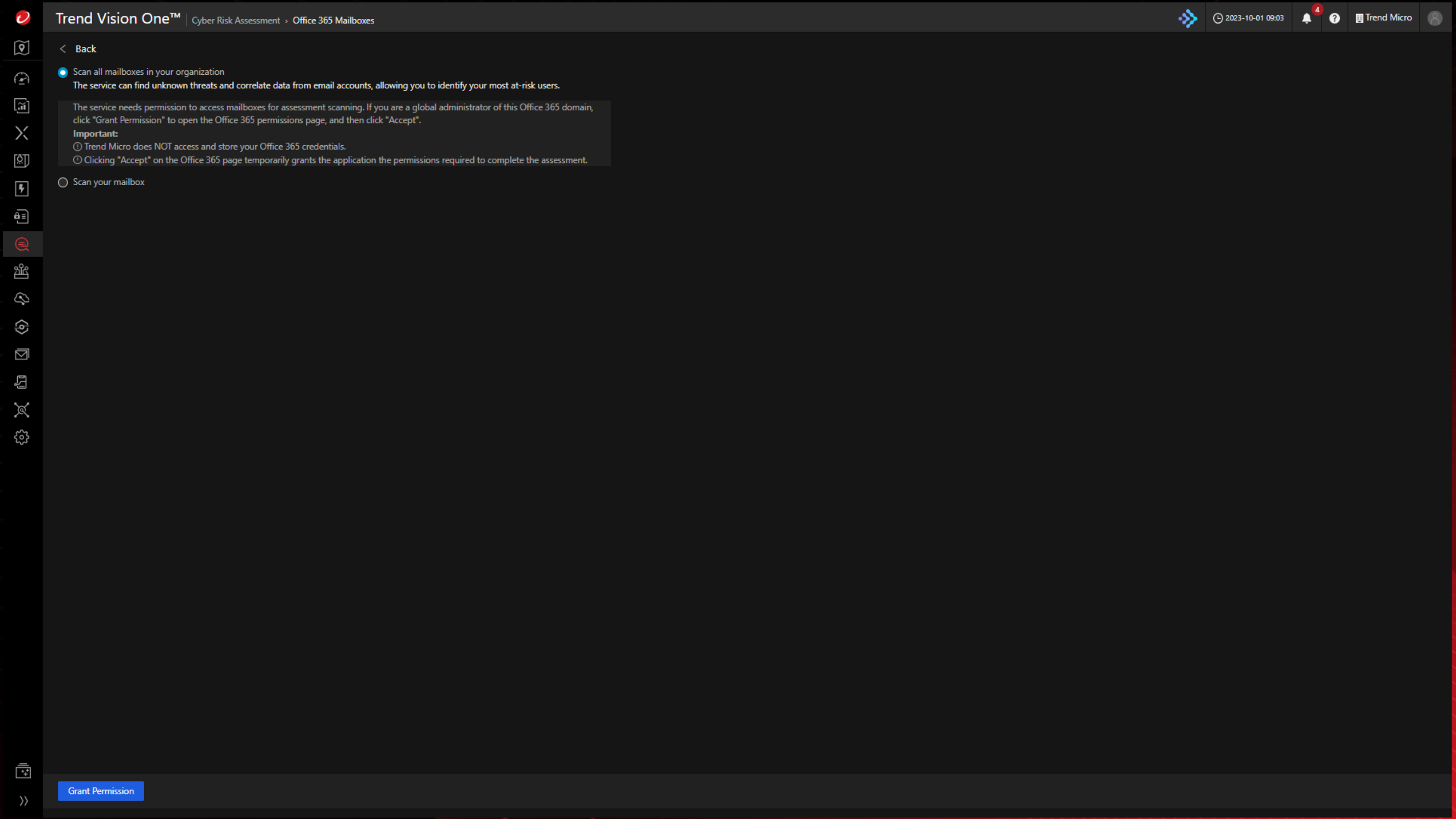
At-Risk Endpoint Assessment

Scan high-profile endpoints for file-based threat indicators collected from global intelligence sources to uncover malicious activity.

Assessment status: Ready

Start Assessment

Select assessment scope and grant permission



Trend Vision One™ | Cyber Risk Assessment › Office 365 Mailboxes

● Scan all mailboxes in your organization

The service can find unknown threats and correlate data from email accounts, allowing you to identify your most at-risk users.

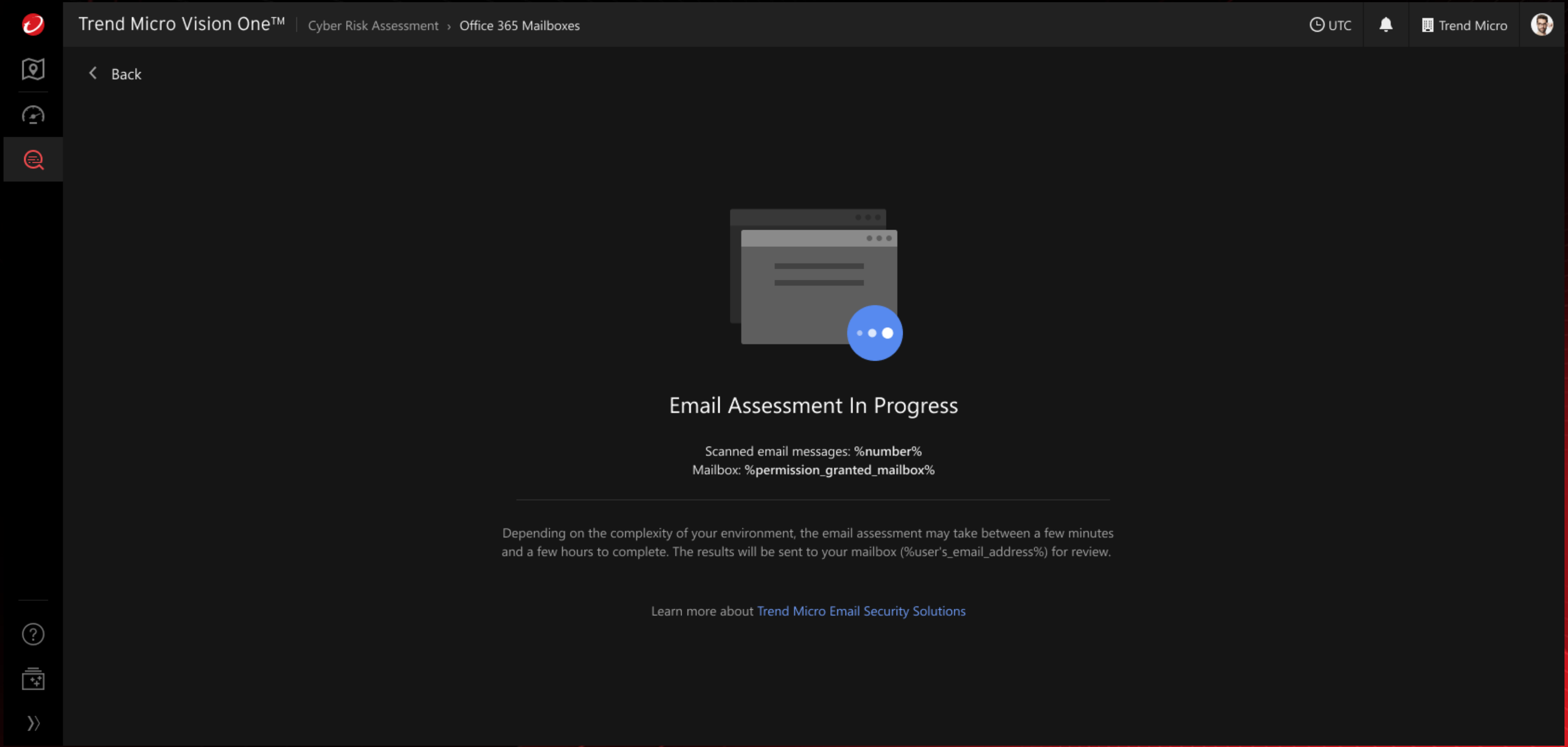
The service needs permission to access mailboxes for assessment scanning. If you are a global administrator of this Office 365 domain, click "Grant Permission" to open the Office 365 permissions page, and then click "Accept".

Important:

ⓘ Trend Micro does NOT access and store your Office 365 credentials.

ⓘ Clicking "Accept" on the Office 365 page temporarily grants the application the permissions required to complete the assessment.

○ Scan your mailbox



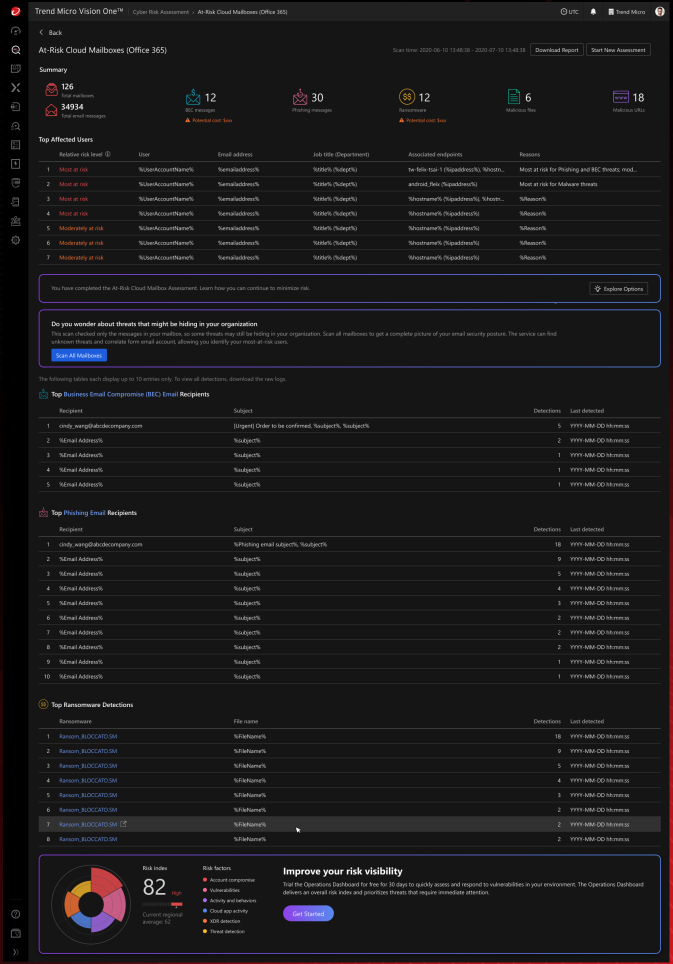
Email Assessment In Progress

Scanned email messages: **%number%**
Mailbox: **%permission_granted_mailbox%**

Depending on the complexity of your environment, the email assessment may take between a few minutes and a few hours to complete. The results will be sent to your mailbox (%user's_email_address%) for review.

Learn more about Trend Micro Email Security Solutions

Office 365 Assessment Report



Trend Micro Vision One™
Cyber Risk Assessment › At-Risk Cloud Mailboxes (Office 365)
UTC
Trend Micro
Back

At-Risk Cloud Mailboxes (Office 365)

Scan time: 2020-06-10 13:48:38 - 2020-07-10 13:48:38

Summary

126	Total mailboxes
34934	Total email messages
12	BEC messages ⚠ Potential cost: $xxx
30	Phishing messages
12	Ransomware ⚠ Potential cost: $xxx
6	Malicious files
18	Malicious URLs

Top Affected Users

	Relative risk level ⓘ	User	Email address	Job title (Department)	Associated endpoints	Reasons
1	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	tw-felix-tsai-1 (%ipaddress%), %hostn...	Most at risk for Phishing and BEC threats; mod...
2	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	android_fleix (%ipaddress%)	Most at risk for Malware threats
3	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%), %hostn...	%Reason%
4	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%
5	Moderately at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%
6	Moderately at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%
7	Moderately at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%

You have completed the At-Risk Cloud Mailbox Assessment. Learn how you can continue to minimize risk.

Do you wonder about threats that might be hiding in your organization

This scan checked only the messages in your mailbox, so some threats may still be hiding in your organization. Scan all mailboxes to get a complete picture of your email security posture. The service can find unknown threats and correlate form email account, allowing you identify your most-at-risk users.

The following tables each display up to 10 entries only. To view all detections, download the raw logs.

Top Business Email Compromise (BEC) Email Recipients

	Recipient	Subject	Detections	Last detected
1	cindy_wang@abcdecompany.com	[Urgent] Order to be confirmed, %subject%, %subject%	5	YYYY-MM-DD hh:mm:ss
2	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
3	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss
4	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss
5	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss

Top Phishing Email Recipients

	Recipient	Subject	Detections	Last detected
1	cindy_wang@abcdecompany.com	%Phishing email subject%, %subject%	18	YYYY-MM-DD hh:mm:ss
2	%Email Address%	%subject%	9	YYYY-MM-DD hh:mm:ss
3	%Email Address%	%subject%	5	YYYY-MM-DD hh:mm:ss
4	%Email Address%	%subject%	4	YYYY-MM-DD hh:mm:ss
5	%Email Address%	%subject%	3	YYYY-MM-DD hh:mm:ss
6	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
7	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
8	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
9	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss
10	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss

Top Ransomware Detections

	Ransomware	File name	Detections	Last detected
1	Ransom_BLOCCATO.SM	%FileName%	18	YYYY-MM-DD hh:mm:ss
2	Ransom_BLOCCATO.SM	%FileName%	9	YYYY-MM-DD hh:mm:ss
3	Ransom_BLOCCATO.SM	%FileName%	5	YYYY-MM-DD hh:mm:ss
4	Ransom_BLOCCATO.SM	%FileName%	4	YYYY-MM-DD hh:mm:ss
5	Ransom_BLOCCATO.SM	%FileName%	3	YYYY-MM-DD hh:mm:ss
6	Ransom_BLOCCATO.SM	%FileName%	2	YYYY-MM-DD hh:mm:ss
7	Ransom_BLOCCATO.SM	%FileName%	2	YYYY-MM-DD hh:mm:ss
8	Ransom_BLOCCATO.SM	%FileName%	2	YYYY-MM-DD hh:mm:ss

Risk index

82 High

Current regional average: 62

Risk factors

- ● Account compromise
- ● Vulnerabilities
- ● Activity and behaviors
- ● Cloud app activity
- ● XDR detection
- ● Threat detection

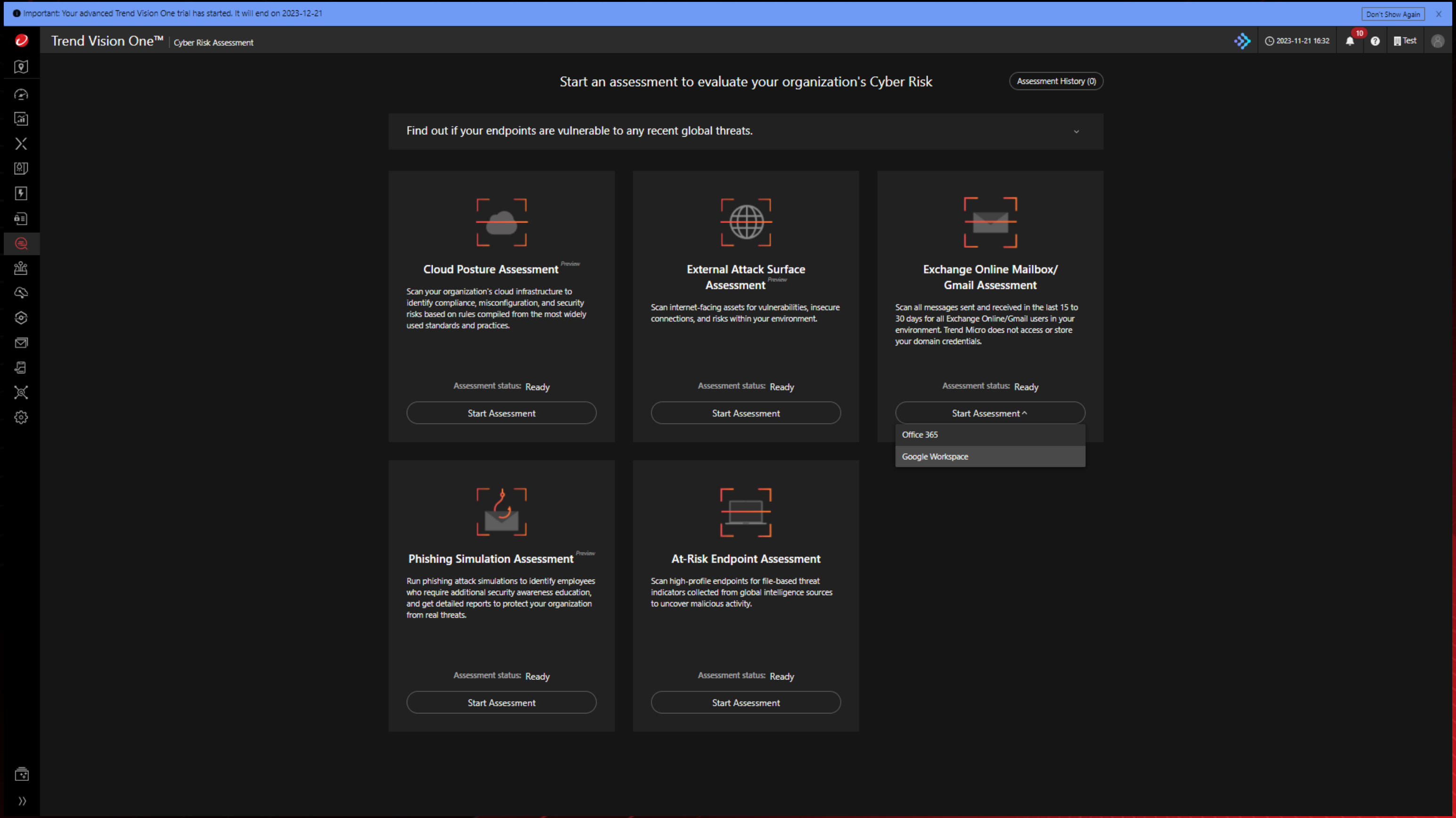
Improve your risk visibility

Trial the Operations Dashboard for free for 30 days to quickly assess and respond to vulnerabilities in your environment. The Operations Dashboard delivers an overall risk index and prioritizes threats that require immediate attention.

Exchange Online Mailbox/Gmail Assessment – Gmail

Step-by-Step Assessment Walkthrough

Select Google Workplace, through “Exchange Online Mailbox/Gmail Assessment”



Important: Your advanced Trend Vision One trial has started. It will end on 2023-12-21

Start an assessment to evaluate your organization's Cyber Risk

Find out if your endpoints are vulnerable to any recent global threats.

Cloud Posture Assessment Preview

Scan your organization's cloud infrastructure to identify compliance, misconfiguration, and security risks based on rules compiled from the most widely used standards and practices.

Assessment status: Ready

Start Assessment

External Attack Surface Assessment Preview

Scan internet-facing assets for vulnerabilities, insecure connections, and risks within your environment.

Assessment status: Ready

Start Assessment

Exchange Online Mailbox/ Gmail Assessment

Scan all messages sent and received in the last 15 to 30 days for all Exchange Online/Gmail users in your environment. Trend Micro does not access or store your domain credentials.

Assessment status: Ready

Start Assessment ^

- Office 365
- Google Workspace

Phishing Simulation Assessment Preview

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

Assessment status: Ready

Start Assessment

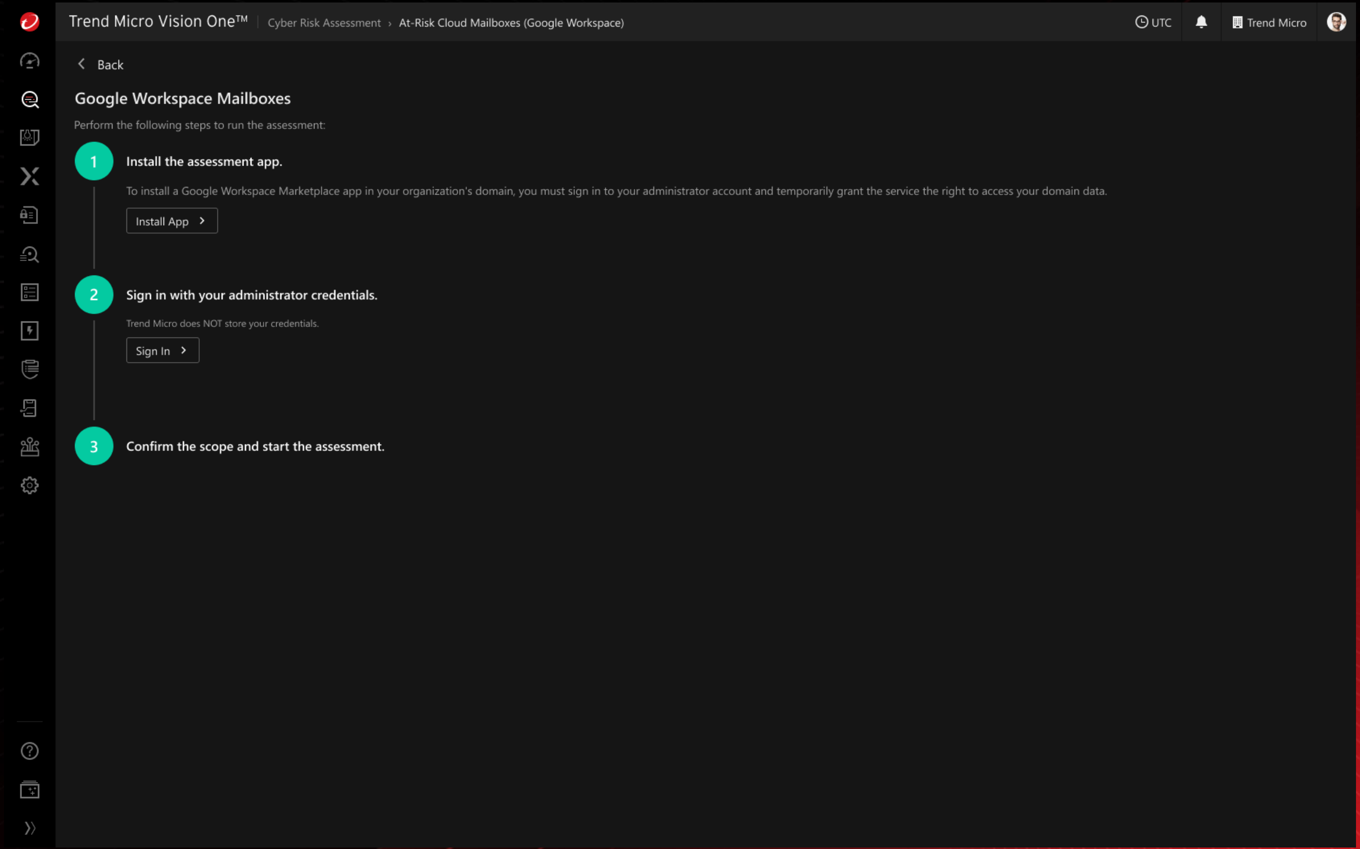
At-Risk Endpoint Assessment

Scan high-profile endpoints for file-based threat indicators collected from global intelligence sources to uncover malicious activity.

Assessment status: Ready

Start Assessment

Install App



Trend Micro Vision One™
Cyber Risk Assessment › At-Risk Cloud Mailboxes (Google Workspace)
UTC
Trend Micro
Back

Google Workspace Mailboxes

Perform the following steps to run the assessment:

1. **Install the assessment app.**

   To install a Google Workspace Marketplace app in your organization's domain, you must sign in to your administrator account and temporarily grant the service the right to access your domain data.

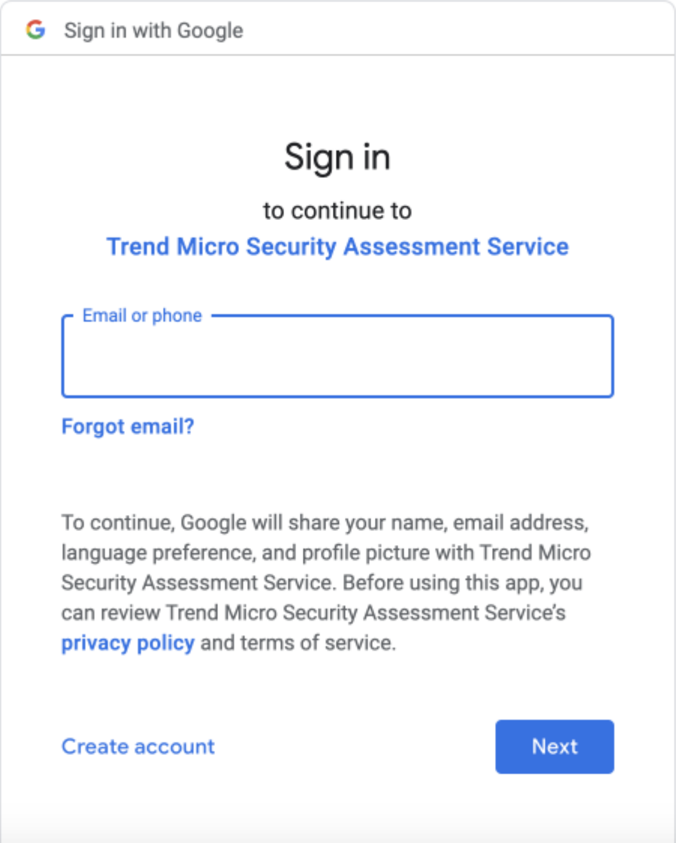
   Install App ›

2. **Sign in with your administrator credentials.**

   Trend Micro does NOT store your credentials.

   Sign In ›

3. **Confirm the scope and start the assessment.**



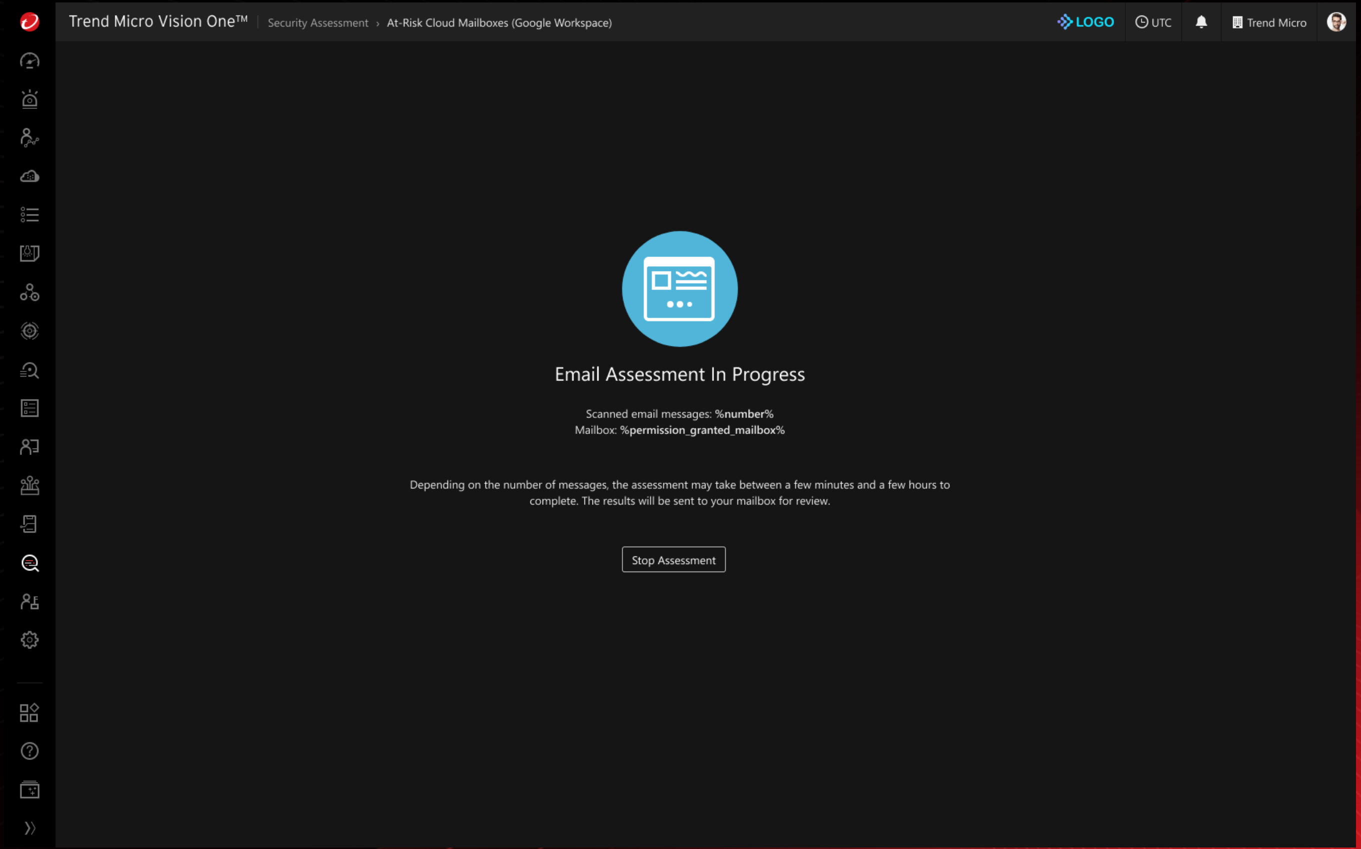
Sign in with Google

Sign in

to continue to

Trend Micro Security Assessment Service

To continue, Google will share your name, email address, language preference, and profile picture with Trend Micro Security Assessment Service. Before using this app, you can review Trend Micro Security Assessment Service's privacy policy and terms of service.



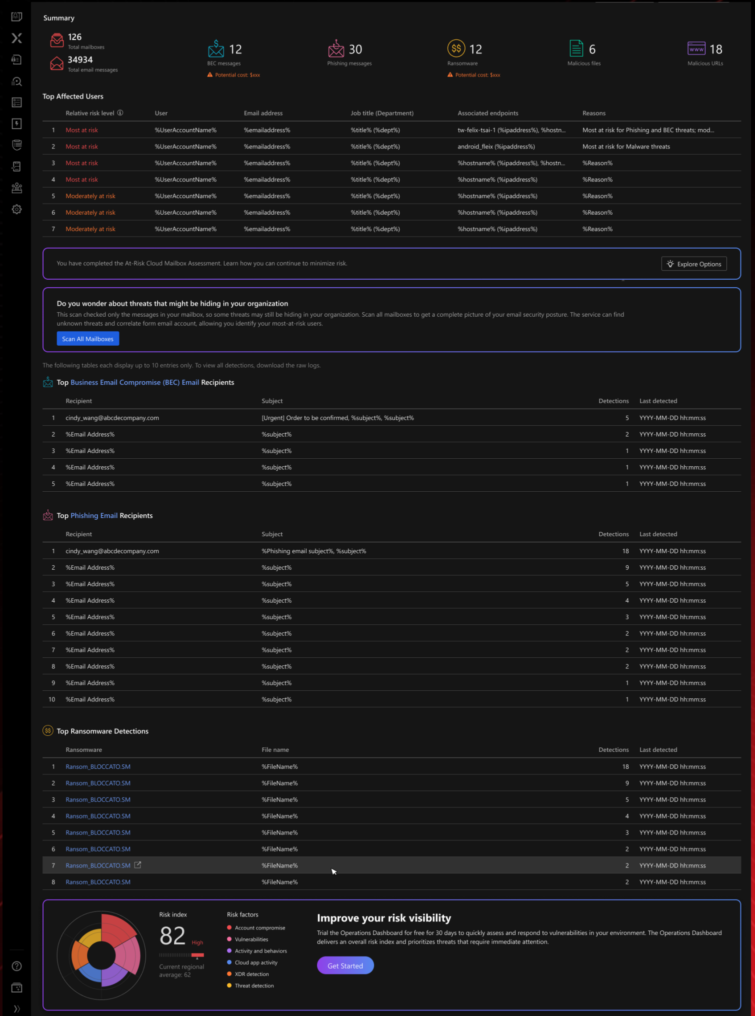
Trend Micro Vision One™
Security Assessment › At-Risk Cloud Mailboxes (Google Workspace)
LOGO
UTC
Trend Micro

Email Assessment In Progress

Scanned email messages: **%number%**
Mailbox: **%permission_granted_mailbox%**

Depending on the number of messages, the assessment may take between a few minutes and a few hours to complete. The results will be sent to your mailbox for review.

Gmail Assessment Report



Summary

126 Total mailboxes

34934 Total email messages

12 BEC messages
⚠ Potential cost: $xxx

30 Phishing messages

12 Ransomware
⚠ Potential cost: $xxx

6 Malicious files

18 Malicious URLs

Top Affected Users

	Relative risk level ⓘ	User	Email address	Job title (Department)	Associated endpoints	Reasons
1	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	tw-felix-tsai-1 (%ipaddress%), %hostn...	Most at risk for Phishing and BEC threats; mod...
2	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	android_fleix (%ipaddress%)	Most at risk for Malware threats
3	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%), %hostn...	%Reason%
4	Most at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%
5	Moderately at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%
6	Moderately at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%
7	Moderately at risk	%UserAccountName%	%emailaddress%	%title% (%dept%)	%hostname% (%ipaddress%)	%Reason%

You have completed the At-Risk Cloud Mailbox Assessment. Learn how you can continue to minimize risk.

Do you wonder about threats that might be hiding in your organization

This scan checked only the messages in your mailbox, so some threats may still be hiding in your organization. Scan all mailboxes to get a complete picture of your email security posture. The service can find unknown threats and correlate form email account, allowing you identify your most-at-risk users.

The following tables each display up to 10 entries only. To view all detections, download the raw logs.

Top Business Email Compromise (BEC) Email Recipients

	Recipient	Subject	Detections	Last detected
1	cindy_wang@abcdecompany.com	[Urgent] Order to be confirmed, %subject%, %subject%	5	YYYY-MM-DD hh:mm:ss
2	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
3	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss
4	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss
5	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss

Top Phishing Email Recipients

	Recipient	Subject	Detections	Last detected
1	cindy_wang@abcdecompany.com	%Phishing email subject%, %subject%	18	YYYY-MM-DD hh:mm:ss
2	%Email Address%	%subject%	9	YYYY-MM-DD hh:mm:ss
3	%Email Address%	%subject%	5	YYYY-MM-DD hh:mm:ss
4	%Email Address%	%subject%	4	YYYY-MM-DD hh:mm:ss
5	%Email Address%	%subject%	3	YYYY-MM-DD hh:mm:ss
6	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
7	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
8	%Email Address%	%subject%	2	YYYY-MM-DD hh:mm:ss
9	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss
10	%Email Address%	%subject%	1	YYYY-MM-DD hh:mm:ss

Top Ransomware Detections

	Ransomware	File name	Detections	Last detected
1	Ransom_BLOCCATO.SM	%FileName%	18	YYYY-MM-DD hh:mm:ss
2	Ransom_BLOCCATO.SM	%FileName%	9	YYYY-MM-DD hh:mm:ss
3	Ransom_BLOCCATO.SM	%FileName%	5	YYYY-MM-DD hh:mm:ss
4	Ransom_BLOCCATO.SM	%FileName%	4	YYYY-MM-DD hh:mm:ss
5	Ransom_BLOCCATO.SM	%FileName%	3	YYYY-MM-DD hh:mm:ss
6	Ransom_BLOCCATO.SM	%FileName%	2	YYYY-MM-DD hh:mm:ss
7	Ransom_BLOCCATO.SM	%FileName%	2	YYYY-MM-DD hh:mm:ss
8	Ransom_BLOCCATO.SM	%FileName%	2	YYYY-MM-DD hh:mm:ss

Risk index

82 High

Current regional average: 62

Risk factors

- ● Account compromise
- ● Vulnerabilities
- ● Activity and behaviors
- ● Cloud app activity
- ● XDR detection
- ● Threat detection

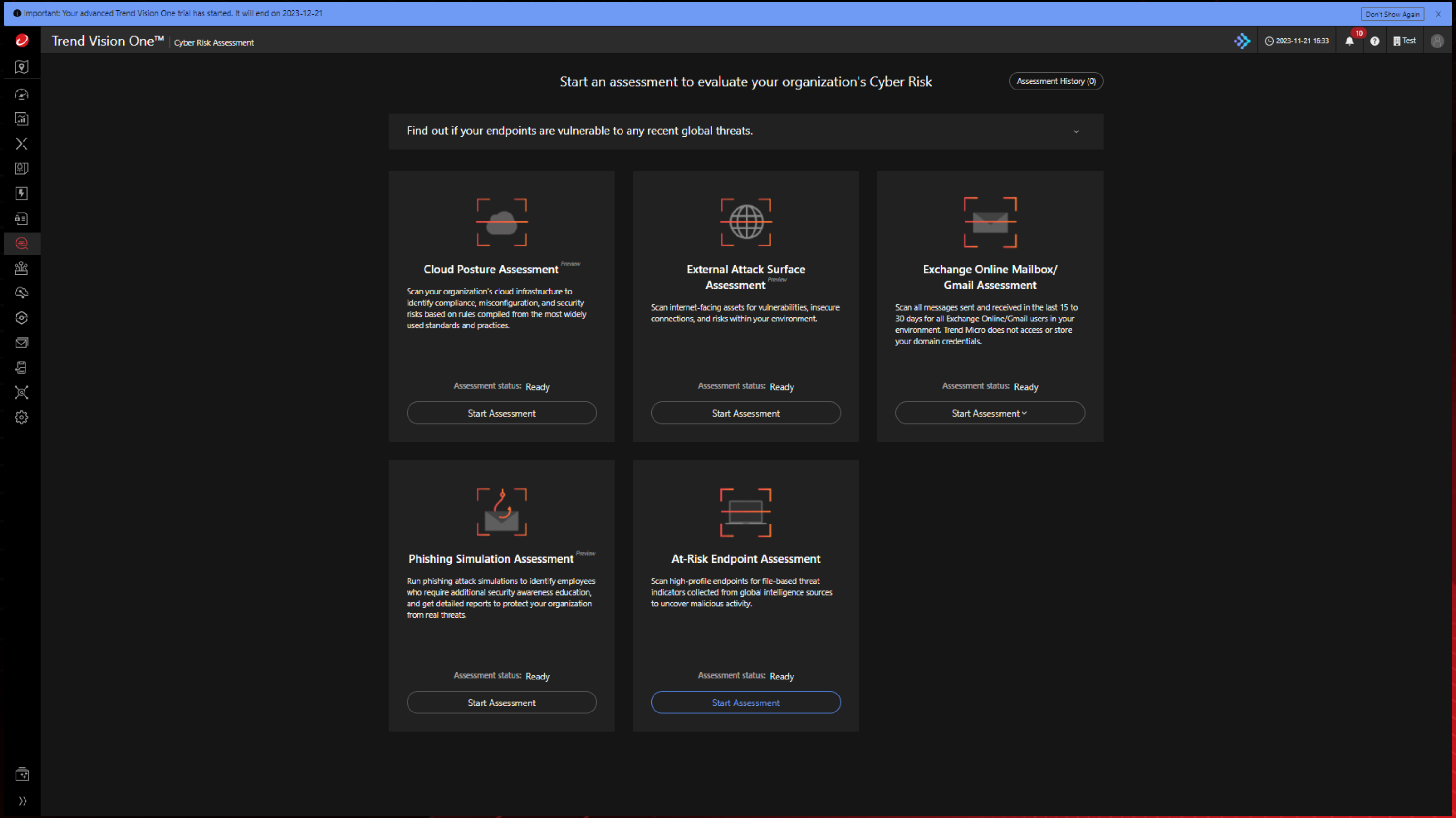
Improve your risk visibility

Trial the Operations Dashboard for free for 30 days to quickly assess and respond to vulnerabilities in your environment. The Operations Dashboard delivers an overall risk index and prioritizes threats that require immediate attention.

At-Risk Endpoint Assessment

Step-by-Step Assessment Walkthrough

Select "At-Risk Endpoint Assessment"



Important: Your advanced Trend Vision One trial has started. It will end on 2023-12-21

Trend Vision One™ | Cyber Risk Assessment

Start an assessment to evaluate your organization's Cyber Risk

Find out if your endpoints are vulnerable to any recent global threats.

Cloud Posture Assessment *Preview*

Scan your organization's cloud infrastructure to identify compliance, misconfiguration, and security risks based on rules compiled from the most widely used standards and practices.

Assessment status: Ready

External Attack Surface Assessment *Preview*

Scan internet-facing assets for vulnerabilities, insecure connections, and risks within your environment.

Assessment status: Ready

Exchange Online Mailbox/ Gmail Assessment

Scan all messages sent and received in the last 15 to 30 days for all Exchange Online/Gmail users in your environment. Trend Micro does not access or store your domain credentials.

Assessment status: Ready

Phishing Simulation Assessment *Preview*

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

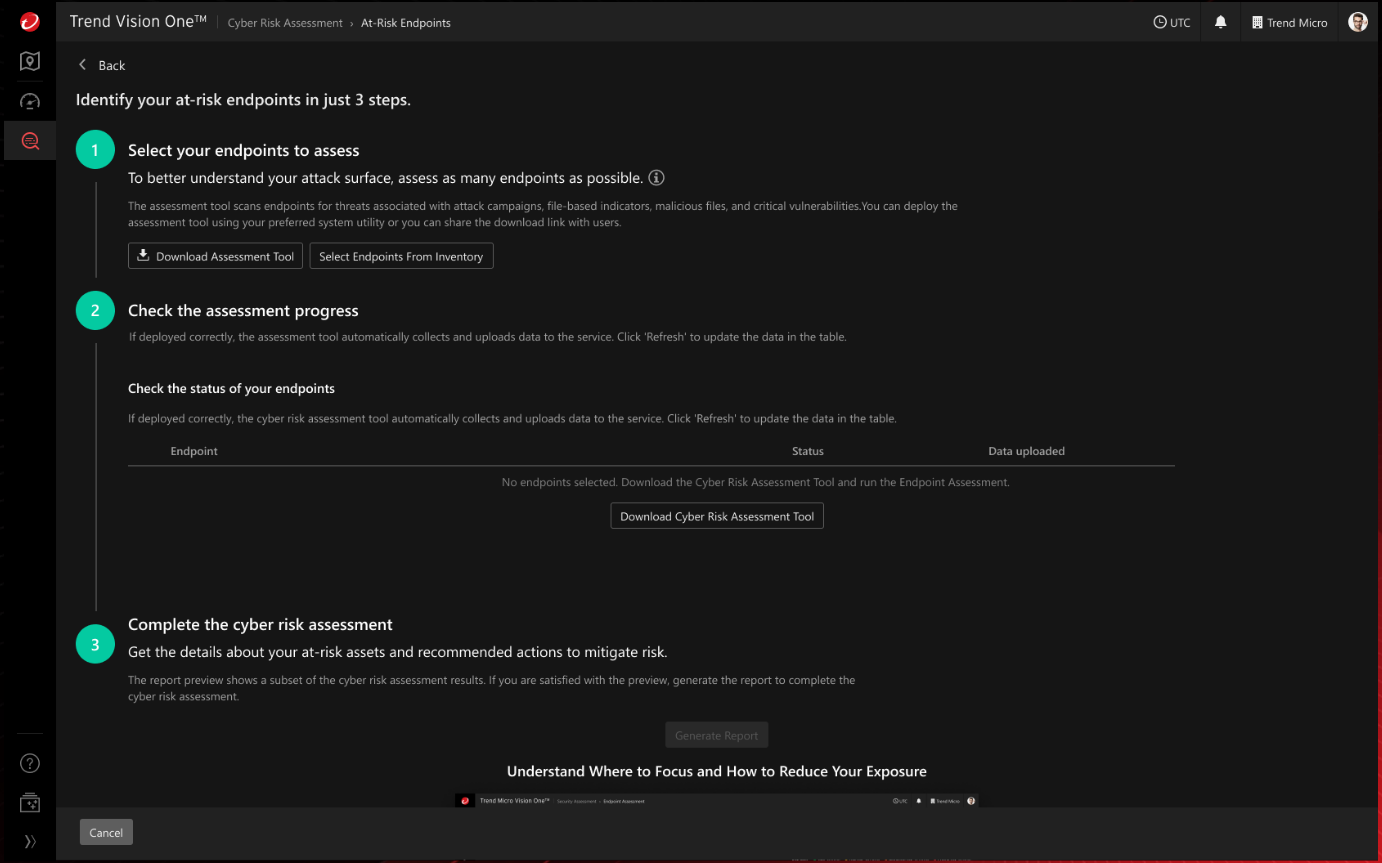
Assessment status: Ready

At-Risk Endpoint Assessment

Scan high-profile endpoints for file-based threat indicators collected from global intelligence sources to uncover malicious activity.

Assessment status: Ready

Select your endpoints to assess



Identify your at-risk endpoints in just 3 steps.

1 Select your endpoints to assess

To better understand your attack surface, assess as many endpoints as possible.

The assessment tool scans endpoints for threats associated with attack campaigns, file-based indicators, malicious files, and critical vulnerabilities.You can deploy the assessment tool using your preferred system utility or you can share the download link with users.

2 Check the assessment progress

If deployed correctly, the assessment tool automatically collects and uploads data to the service. Click 'Refresh' to update the data in the table.

Check the status of your endpoints

If deployed correctly, the cyber risk assessment tool automatically collects and uploads data to the service. Click 'Refresh' to update the data in the table.

Endpoint	Status	Data uploaded

No endpoints selected. Download the Cyber Risk Assessment Tool and run the Endpoint Assessment.

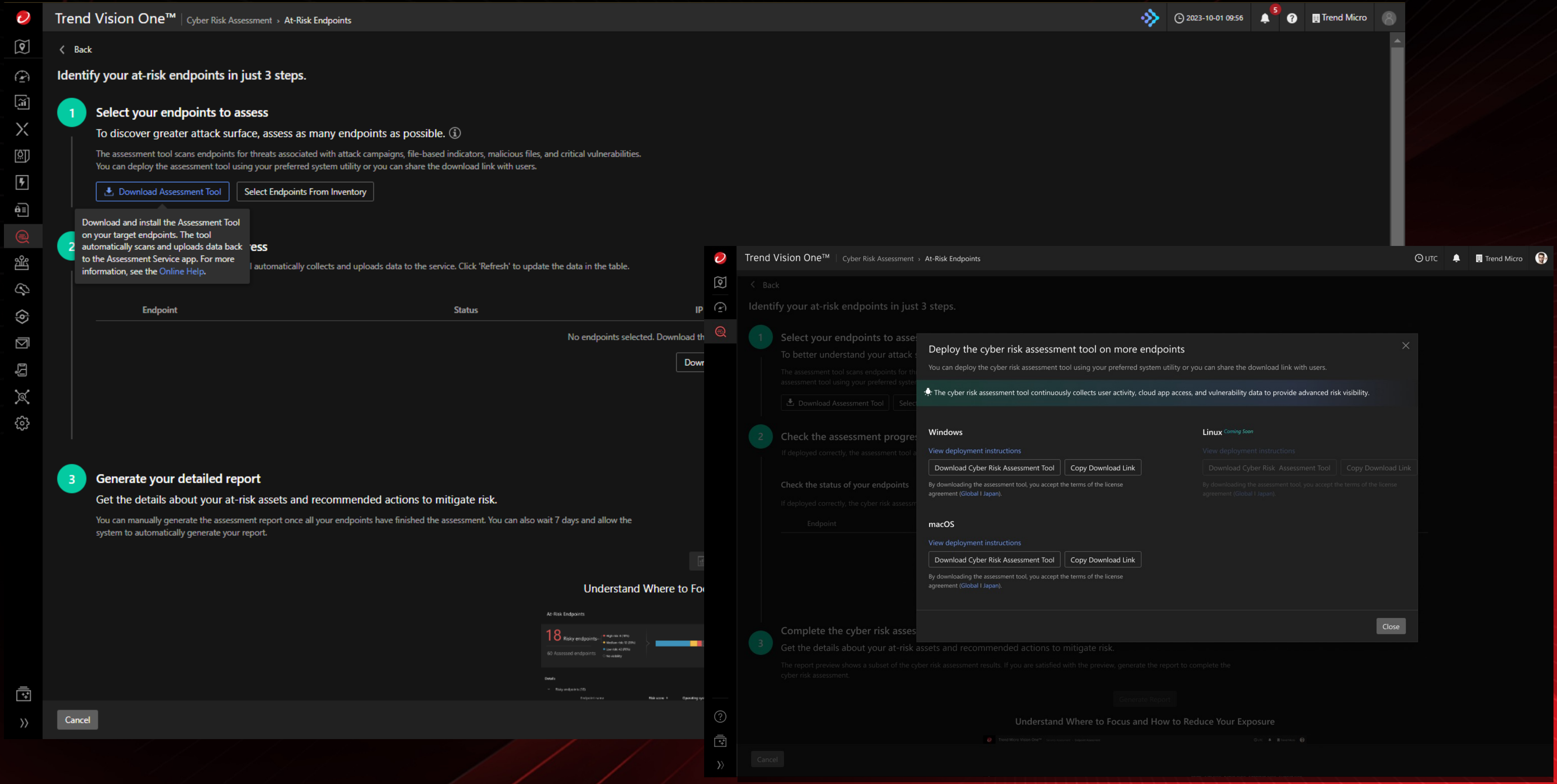
3 Complete the cyber risk assessment

Get the details about your at-risk assets and recommended actions to mitigate risk.

The report preview shows a subset of the cyber risk assessment results. If you are satisfied with the preview, generate the report to complete the cyber risk assessment.

Understand Where to Focus and How to Reduce Your Exposure

Option 1: select "Download Assessment Tool"



Identify your at-risk endpoints in just 3 steps.

1 Select your endpoints to assess

To discover greater attack surface, assess as many endpoints as possible.

The assessment tool scans endpoints for threats associated with attack campaigns, file-based indicators, malicious files, and critical vulnerabilities. You can deploy the assessment tool using your preferred system utility or you can share the download link with users.

Download and install the Assessment Tool on your target endpoints. The tool automatically scans and uploads data back to the Assessment Service app. For more information, see the Online Help.

2 …ess

…l automatically collects and uploads data to the service. Click 'Refresh' to update the data in the table.

Endpoint	Status	IP

No endpoints selected. Download th

3 Generate your detailed report

Get the details about your at-risk assets and recommended actions to mitigate risk.

You can manually generate the assessment report once all your endpoints have finished the assessment. You can also wait 7 days and allow the system to automatically generate your report.

Understand Where to Fo

Deploy the cyber risk assessment tool on more endpoints

You can deploy the cyber risk assessment tool using your preferred system utility or you can share the download link with users.

The cyber risk assessment tool continuously collects user activity, cloud app access, and vulnerability data to provide advanced risk visibility.

Windows

View deployment instructions

By downloading the assessment tool, you accept the terms of the license agreement (Global I Japan).

Linux *Coming Soon*

View deployment instructions

By downloading the assessment tool, you accept the terms of the license agreement (Global I Japan).

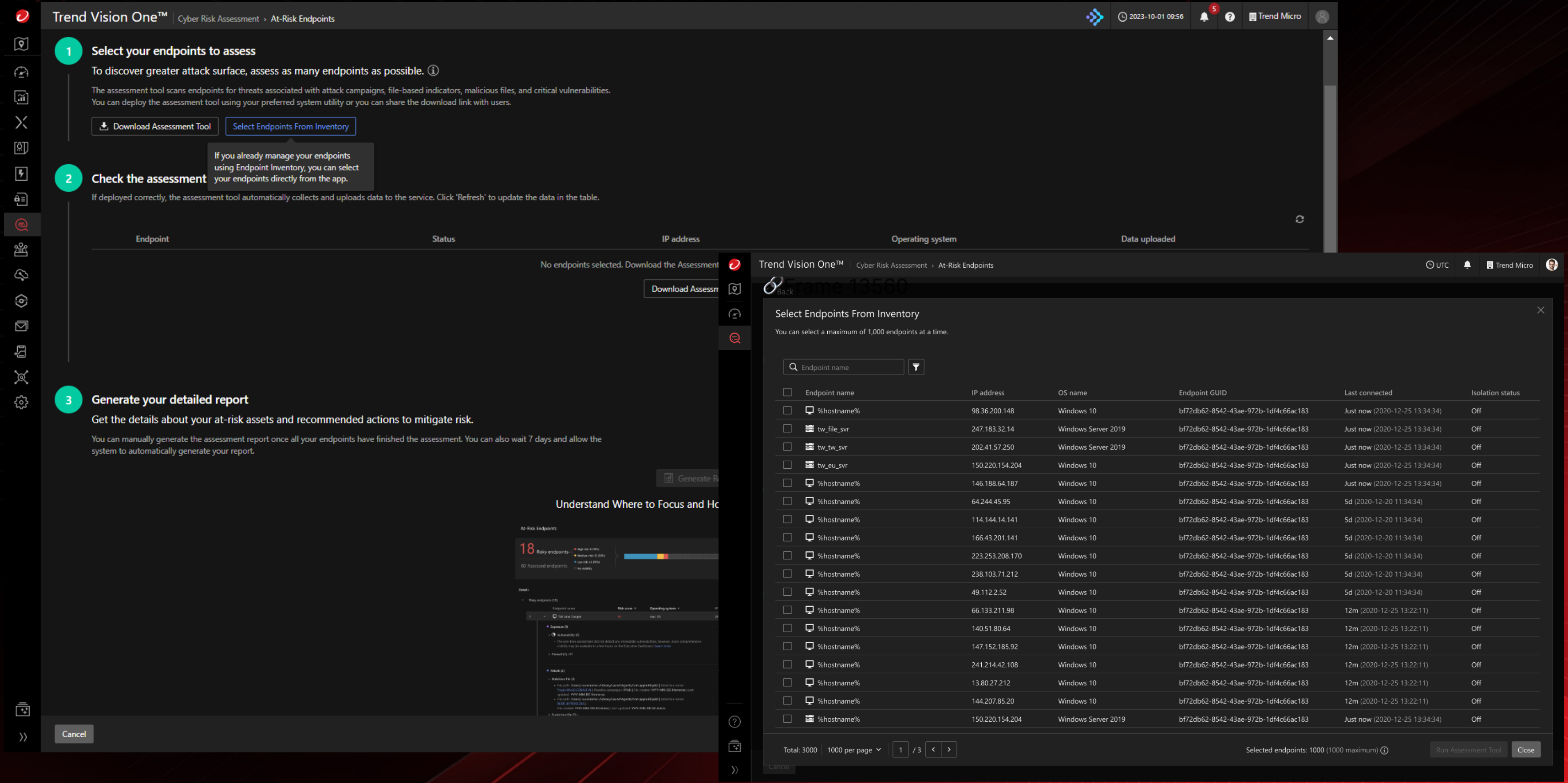
macOS

View deployment instructions

By downloading the assessment tool, you accept the terms of the license agreement (Global I Japan).

Understand Where to Focus and How to Reduce Your Exposure

Option 2: select "Select Endpoints From Inventory"



1 **Select your endpoints to assess**

To discover greater attack surface, assess as many endpoints as possible.

The assessment tool scans endpoints for threats associated with attack campaigns, file-based indicators, malicious files, and critical vulnerabilities. You can deploy the assessment tool using your preferred system utility or you can share the download link with users.

If you already manage your endpoints using Endpoint Inventory, you can select your endpoints directly from the app.

2 **Check the assessment**

If deployed correctly, the assessment tool automatically collects and uploads data to the service. Click 'Refresh' to update the data in the table.

Endpoint	Status	IP address	Operating system	Data uploaded

No endpoints selected. Download the Assessment

3 **Generate your detailed report**

Get the details about your at-risk assets and recommended actions to mitigate risk.

You can manually generate the assessment report once all your endpoints have finished the assessment. You can also wait 7 days and allow the system to automatically generate your report.

Select Endpoints From Inventory

You can select a maximum of 1,000 endpoints at a time.

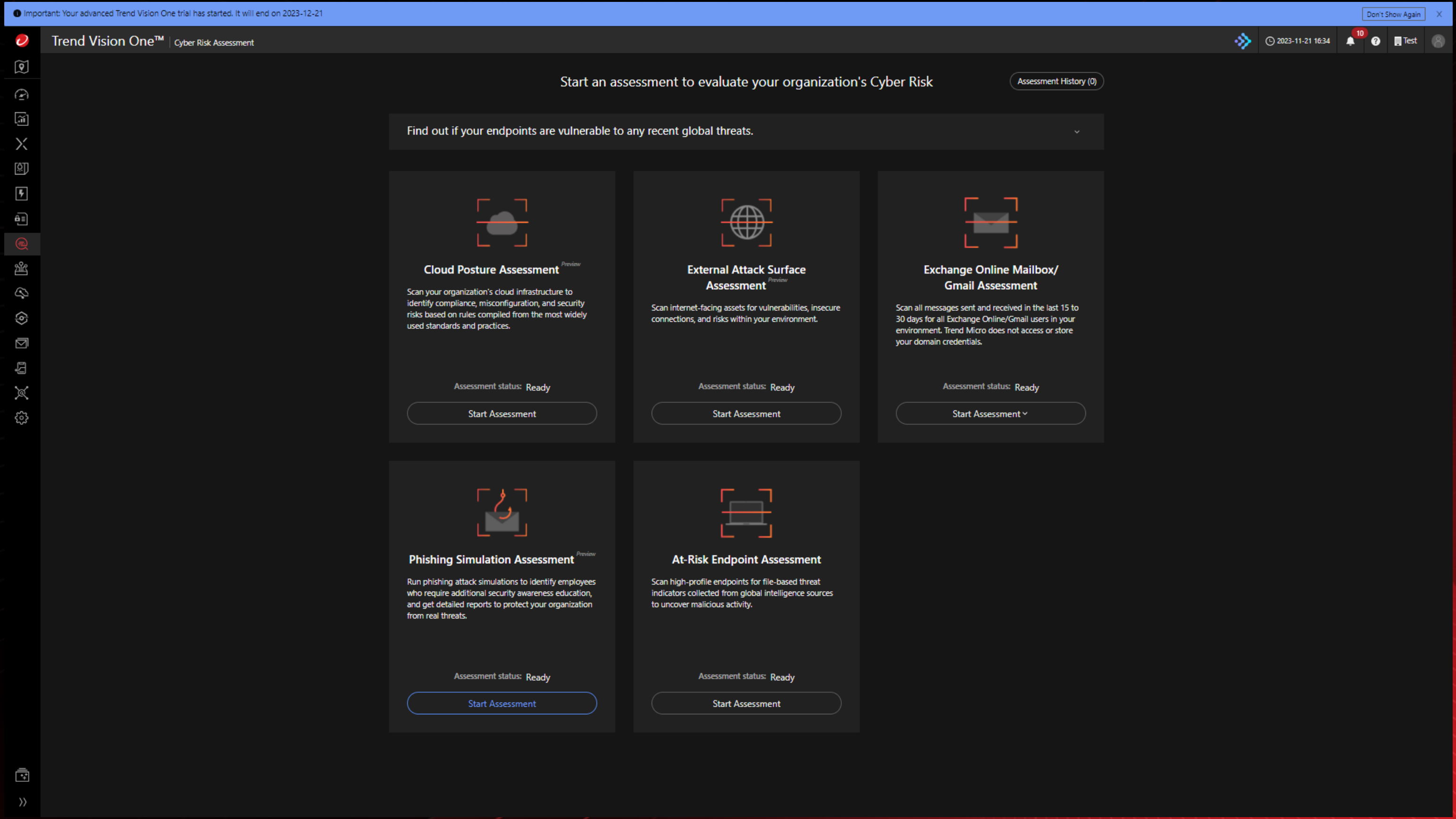
□	Endpoint name	IP address	OS name	Endpoint GUID	Last connected	Isolation status
□	%hostname%	98.36.200.148	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	Just now (2020-12-25 13:34:34)	Off
□	tw_file_svr	247.183.32.14	Windows Server 2019	bf72db62-8542-43ae-972b-1df4c66ac183	Just now (2020-12-25 13:34:34)	Off
□	tw_tw_svr	202.41.57.250	Windows Server 2019	bf72db62-8542-43ae-972b-1df4c66ac183	Just now (2020-12-25 13:34:34)	Off
□	tw_eu_svr	150.220.154.204	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	Just now (2020-12-25 13:34:34)	Off
□	%hostname%	146.188.64.187	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	Just now (2020-12-25 13:34:34)	Off
□	%hostname%	64.244.45.95	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	5d (2020-12-20 11:34:34)	Off
□	%hostname%	114.144.14.141	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	5d (2020-12-20 11:34:34)	Off
□	%hostname%	166.43.201.141	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	5d (2020-12-20 11:34:34)	Off
□	%hostname%	223.253.208.170	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	5d (2020-12-20 11:34:34)	Off
□	%hostname%	238.103.71.212	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	5d (2020-12-20 11:34:34)	Off
□	%hostname%	49.112.2.52	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	5d (2020-12-20 11:34:34)	Off
□	%hostname%	66.133.211.98	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	12m (2020-12-25 13:22:11)	Off
□	%hostname%	140.51.80.64	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	12m (2020-12-25 13:22:11)	Off
□	%hostname%	147.152.185.92	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	12m (2020-12-25 13:22:11)	Off
□	%hostname%	241.214.42.108	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	12m (2020-12-25 13:22:11)	Off
□	%hostname%	13.80.27.212	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	12m (2020-12-25 13:22:11)	Off
□	%hostname%	144.207.85.20	Windows 10	bf72db62-8542-43ae-972b-1df4c66ac183	12m (2020-12-25 13:22:11)	Off
□	%hostname%	150.220.154.204	Windows Server 2019	bf72db62-8542-43ae-972b-1df4c66ac183	Just now (2020-12-25 13:34:34)	Off

Total: 3000 1000 per page 1 / 3

Selected endpoints: 1000 (1000 maximum)

Phishing Simulation Assessment

Step-by-Step Assessment Walkthrough



Important: Your advanced Trend Vision One trial has started. It will end on 2023-12-21

Start an assessment to evaluate your organization's Cyber Risk

Find out if your endpoints are vulnerable to any recent global threats.

Cloud Posture Assessment Preview

Scan your organization's cloud infrastructure to identify compliance, misconfiguration, and security risks based on rules compiled from the most widely used standards and practices.

Assessment status: Ready

External Attack Surface Assessment Preview

Scan internet-facing assets for vulnerabilities, insecure connections, and risks within your environment.

Assessment status: Ready

Exchange Online Mailbox/ Gmail Assessment

Scan all messages sent and received in the last 15 to 30 days for all Exchange Online/Gmail users in your environment. Trend Micro does not access or store your domain credentials.

Assessment status: Ready

Phishing Simulation Assessment Preview

Run phishing attack simulations to identify employees who require additional security awareness education, and get detailed reports to protect your organization from real threats.

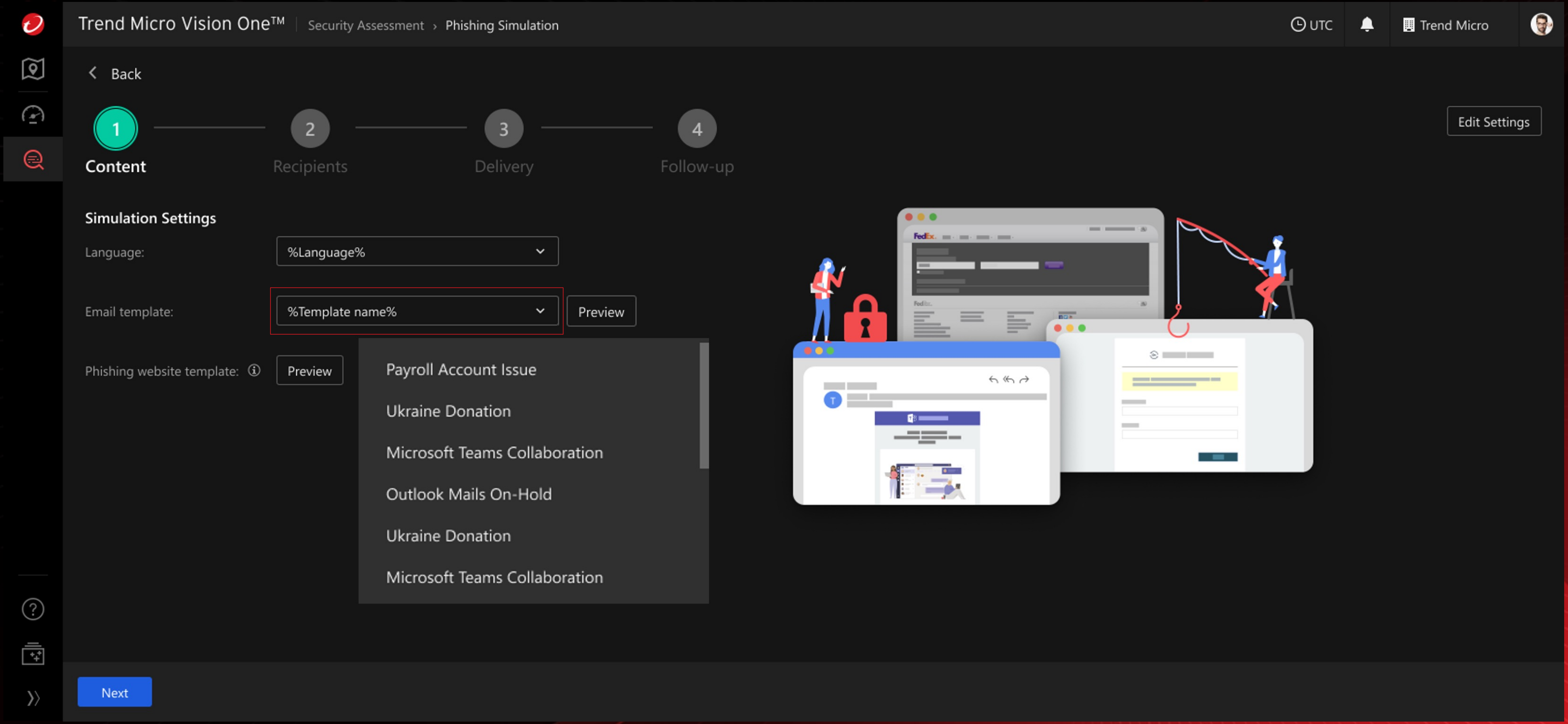
Assessment status: Ready

At-Risk Endpoint Assessment

Scan high-profile endpoints for file-based threat indicators collected from global intelligence sources to uncover malicious activity.

Assessment status: Ready

- Choose and select an email template
- Click “Preview” and then you can edit the template to customize it if needed



Simulation Settings

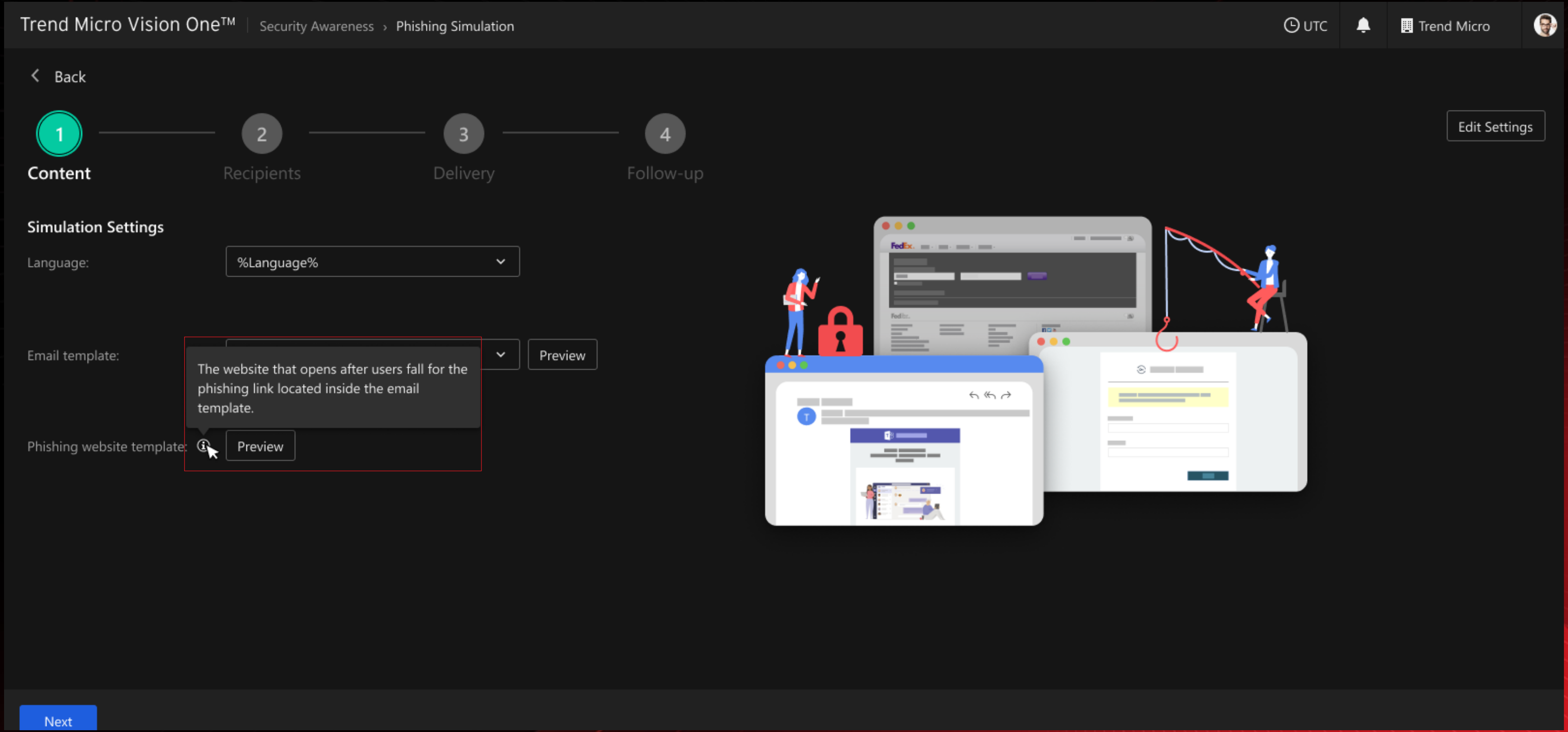
Language: %Language%

Email template: %Template name%

Phishing website template:

- Payroll Account Issue
- Ukraine Donation
- Microsoft Teams Collaboration
- Outlook Mails On-Hold
- Ukraine Donation
- Microsoft Teams Collaboration

Preview how the website would look like if the employees clicked the phishing link in the email template



Trend Micro Vision One™ | Security Awareness › Phishing Simulation

Simulation Settings

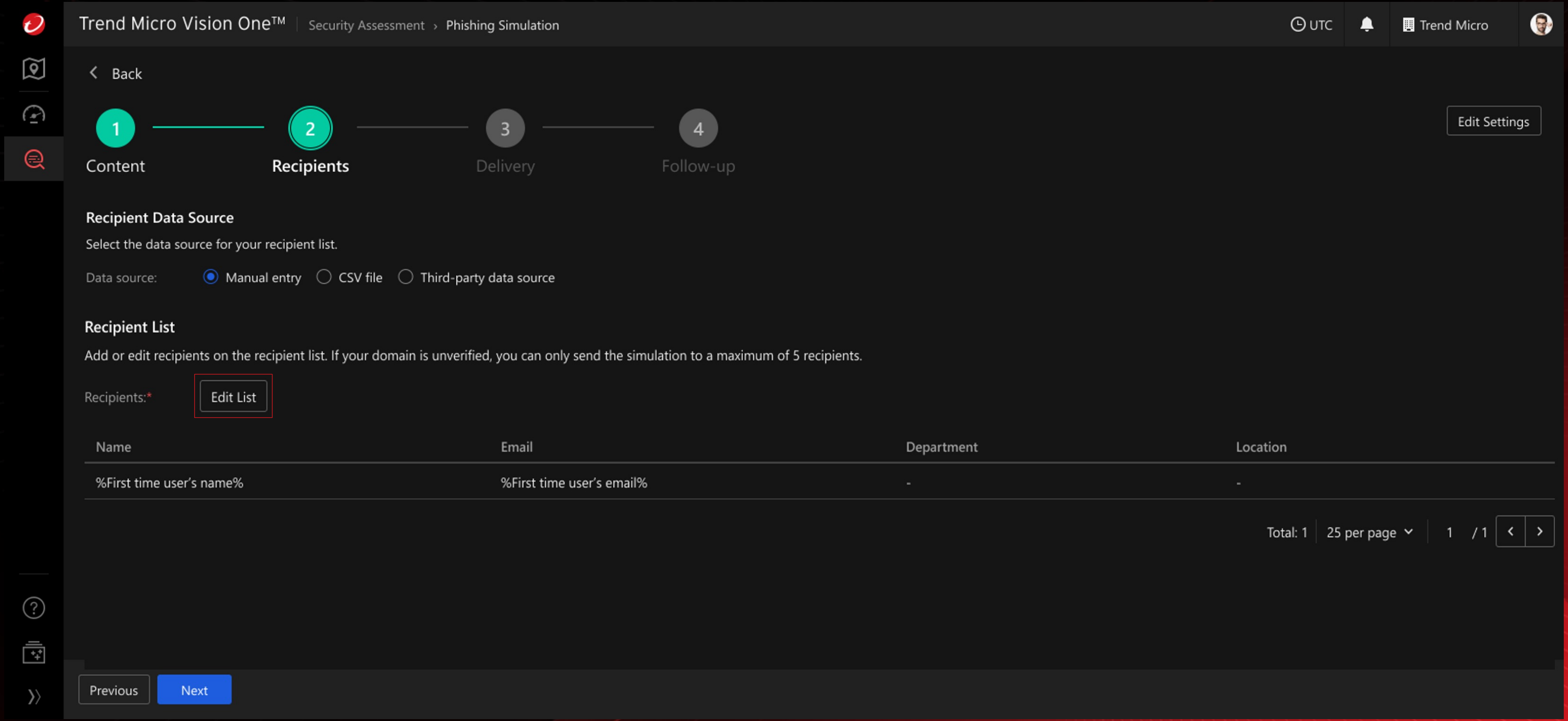
Language: %Language%

Email template:

The website that opens after users fall for the phishing link located inside the email template.

Phishing website template:

- The first way to include the recipient list is manually
- Choose “Manual entry”, Click “Edit List”, then click “Next”



Recipient Data Source

Select the data source for your recipient list.

Data source: ● Manual entry ○ CSV file ○ Third-party data source

Recipient List

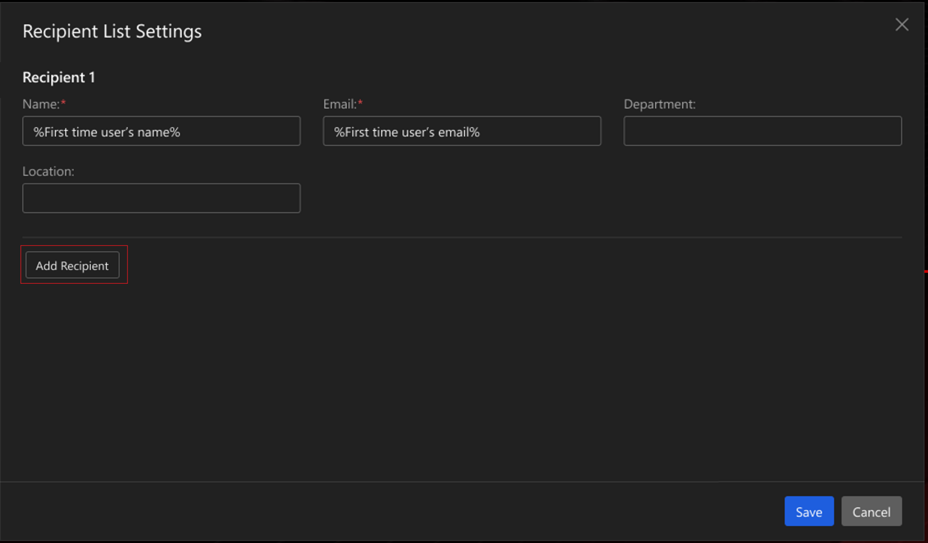
Add or edit recipients on the recipient list. If your domain is unverified, you can only send the simulation to a maximum of 5 recipients.

Recipients:* Edit List

Name	Email	Department	Location
%First time user's name%	%First time user's email%	-	-

Total: 1 25 per page 1 / 1

- The “Name” and “Email” fields are mandatory
- The email domain for recipients must be the same as your sign-up account or verified domain
- Click “Add Recipient” to add the information of the second recipient, and so on
- Once finished inserting the data, click “Save”



Recipient List Settings

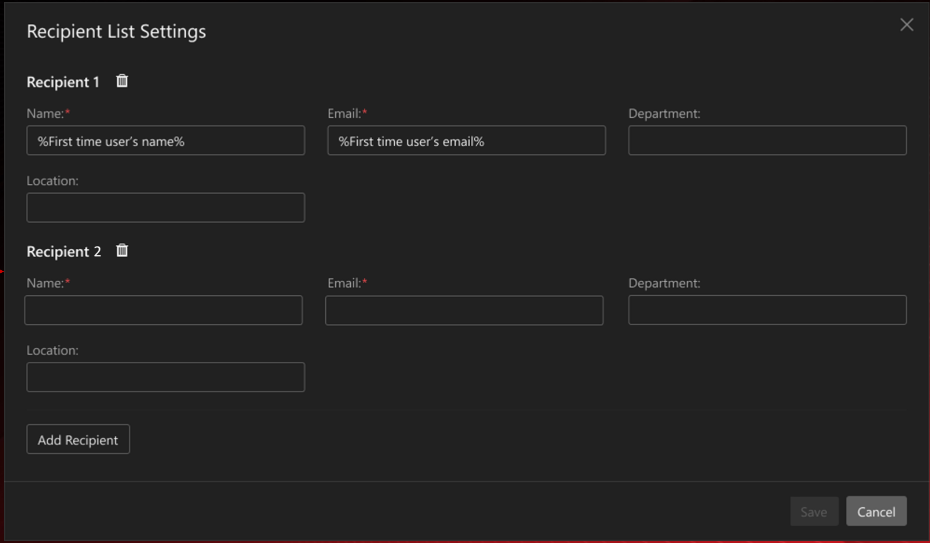
Recipient 1

Name:* %First time user’s name%

Email:* %First time user’s email%

Department:

Location:



Recipient List Settings

Recipient 1

Name:* %First time user’s name%

Email:* %First time user’s email%

Department:

Location:

Recipient 2

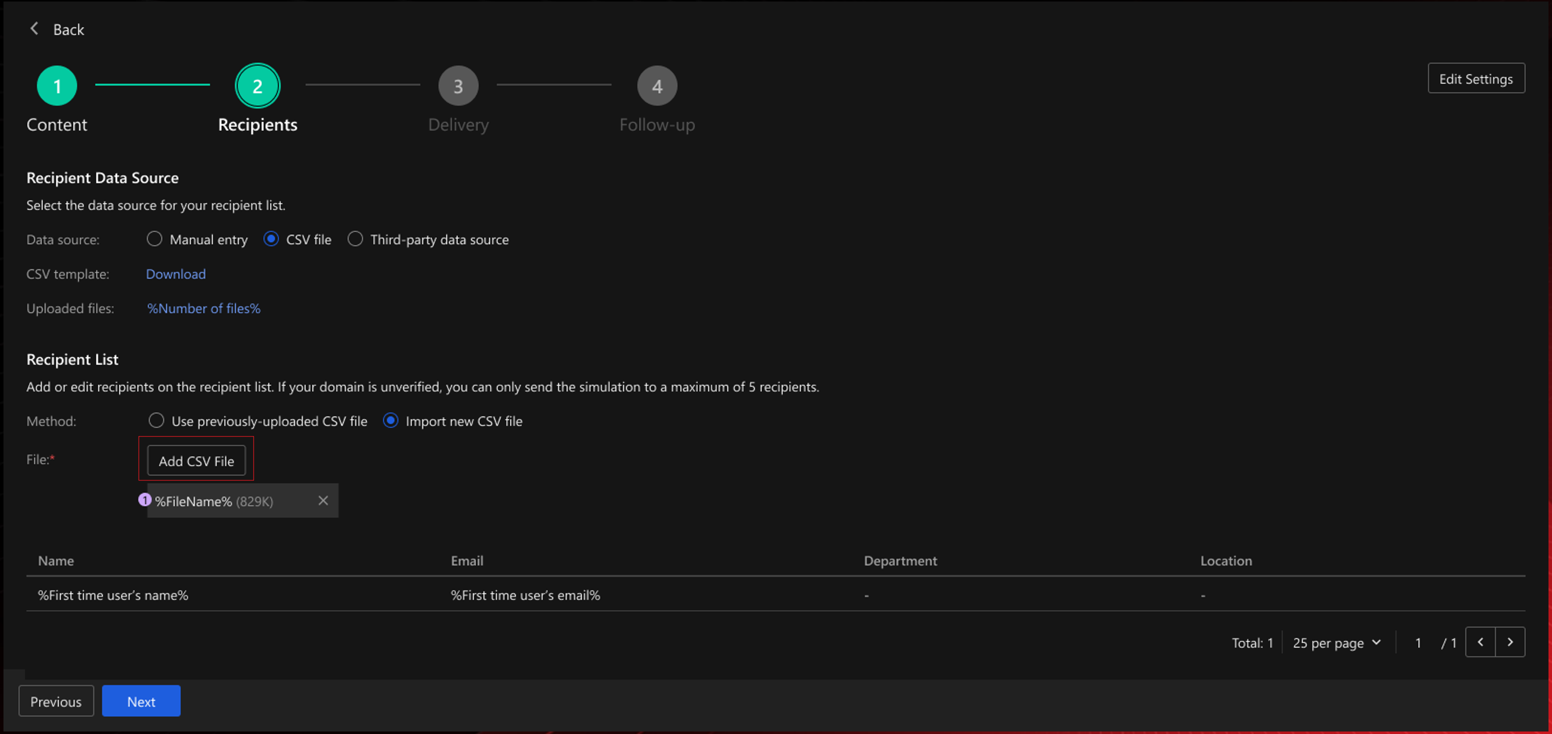
Name:*

Email:*

Department:

Location:

- The second way to include the recipient list is using a CSV file
- Choose “CSV file” as a data source, select “Import new CSV file” and then select “Add CSV file”
- Upload the file and click “Next”
- Please note that there is a CSV template for you to download



Recipient Data Source

Select the data source for your recipient list.

Data source: ○ Manual entry ● CSV file ○ Third-party data source

CSV template: Download

Uploaded files: %Number of files%

Recipient List

Add or edit recipients on the recipient list. If your domain is unverified, you can only send the simulation to a maximum of 5 recipients.

Method: ○ Use previously-uploaded CSV file ● Import new CSV file

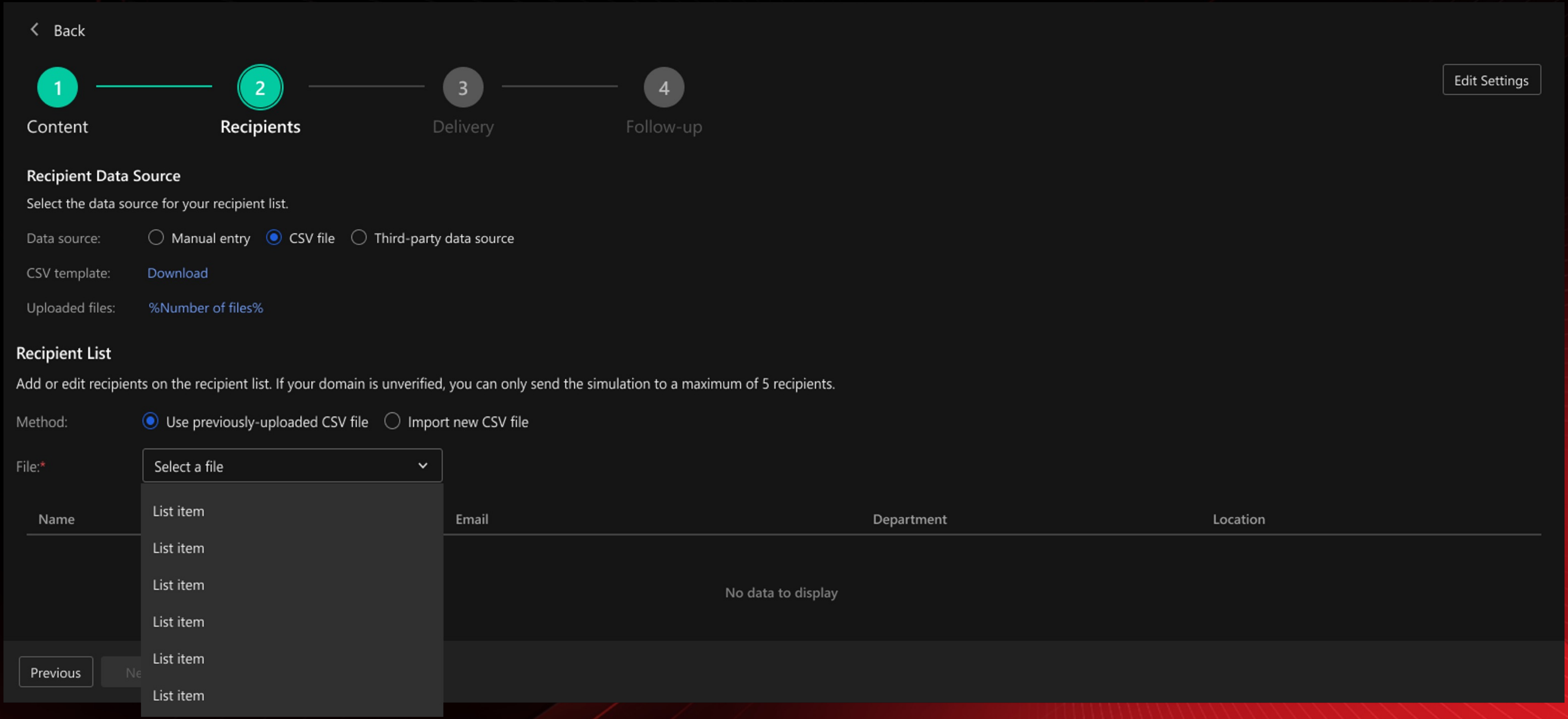
File:* Add CSV File

%FileName% (829K) ×

Name	Email	Department	Location
%First time user’s name%	%First time user’s email%	-	-

Total: 1 | 25 per page | 1 / 1

You can use a previously-uploaded CSV file



Recipient Data Source

Select the data source for your recipient list.

Data source: ○ Manual entry ● CSV file ○ Third-party data source

CSV template: Download

Uploaded files: %Number of files%

Recipient List

Add or edit recipients on the recipient list. If your domain is unverified, you can only send the simulation to a maximum of 5 recipients.

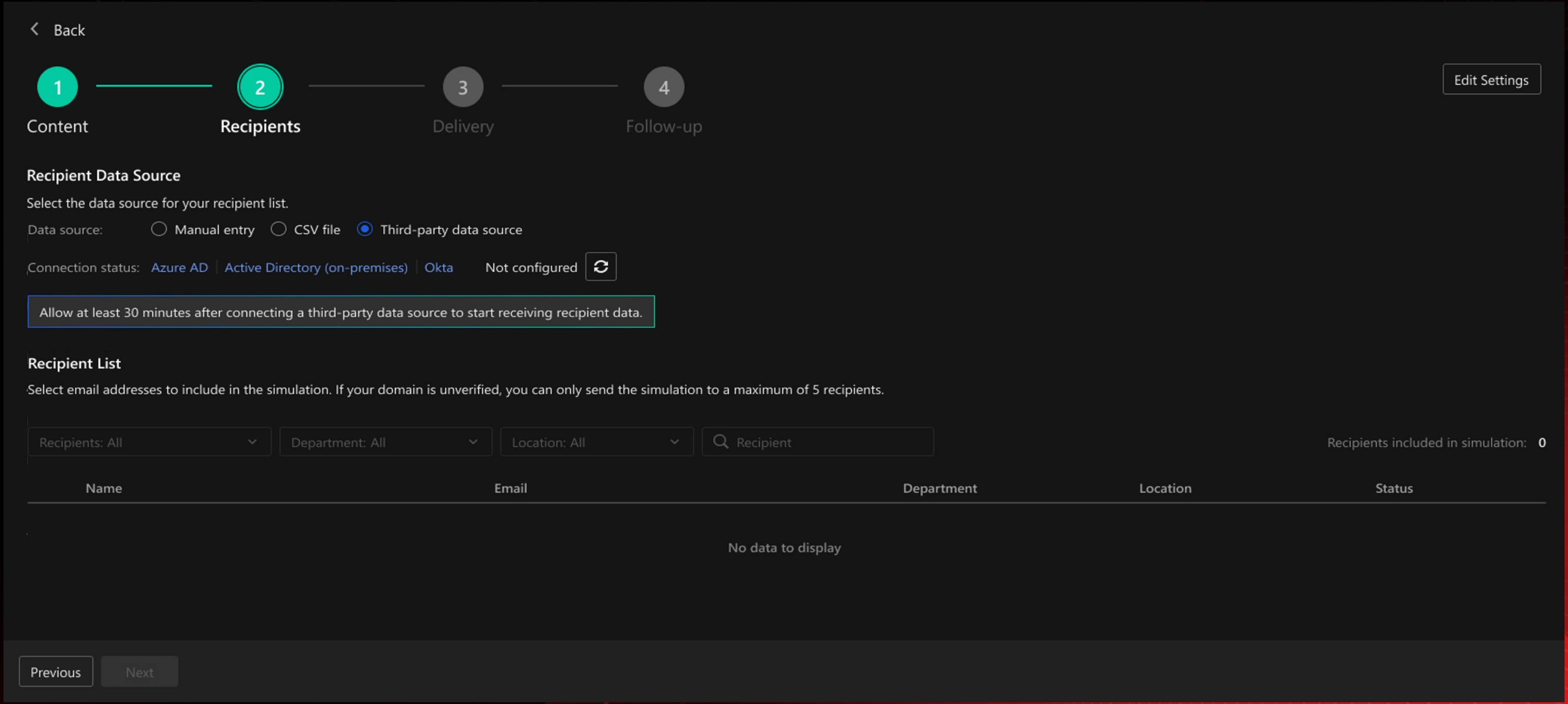
Method: ● Use previously-uploaded CSV file ○ Import new CSV file

File:* Select a file

Name	Email	Department	Location

No data to display

The third way to include the recipient list is using a Third-party data source



Recipient Data Source

Select the data source for your recipient list.

Data source: ○ Manual entry ○ CSV file ● Third-party data source

Connection status: Azure AD | Active Directory (on-premises) | Okta   Not configured

Allow at least 30 minutes after connecting a third-party data source to start receiving recipient data.

Recipient List

Select email addresses to include in the simulation. If your domain is unverified, you can only send the simulation to a maximum of 5 recipients.

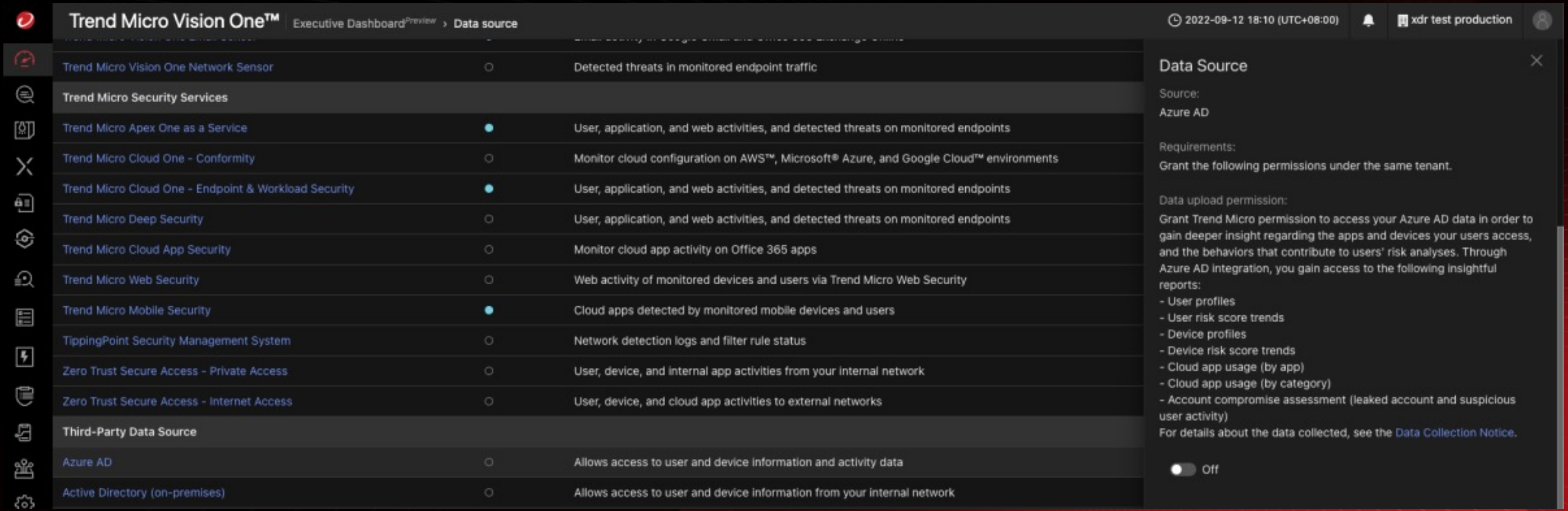
Recipients: All | Department: All | Location: All | Recipient

Recipients included in simulation: 0

Name	Email	Department	Location	Status

No data to display

Data source: Azure AD



Trend Micro Vision One™
Executive Dashboard Preview › Data source
2022-09-12 18:10 (UTC+08:00)
xdr test production

Trend Micro Vision One Network Sensor	○	Detected threats in monitored endpoint traffic
Trend Micro Security Services		
Trend Micro Apex One as a Service	●	User, application, and web activities, and detected threats on monitored endpoints
Trend Micro Cloud One - Conformity	○	Monitor cloud configuration on AWS™, Microsoft® Azure, and Google Cloud™ environments
Trend Micro Cloud One - Endpoint & Workload Security	●	User, application, and web activities, and detected threats on monitored endpoints
Trend Micro Deep Security	○	User, application, and web activities, and detected threats on monitored endpoints
Trend Micro Cloud App Security	○	Monitor cloud app activity on Office 365 apps
Trend Micro Web Security	○	Web activity of monitored devices and users via Trend Micro Web Security
Trend Micro Mobile Security	●	Cloud apps detected by monitored mobile devices and users
TippingPoint Security Management System	○	Network detection logs and filter rule status
Zero Trust Secure Access - Private Access	○	User, device, and internal app activities from your internal network
Zero Trust Secure Access - Internet Access	○	User, device, and cloud app activities to external networks
Third-Party Data Source		
Azure AD	○	Allows access to user and device information and activity data
Active Directory (on-premises)	○	Allows access to user and device information from your internal network

Data Source

Source:
Azure AD

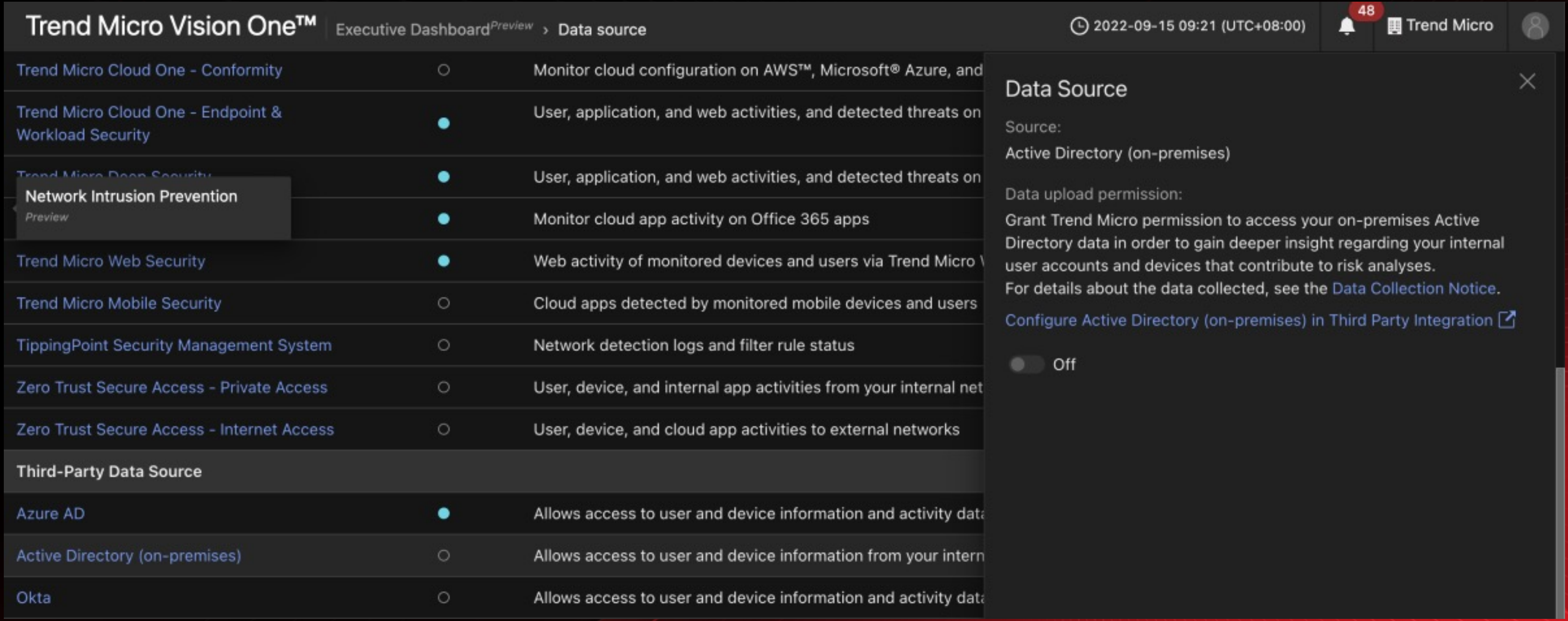
Requirements:
Grant the following permissions under the same tenant.

Data upload permission:
Grant Trend Micro permission to access your Azure AD data in order to gain deeper insight regarding the apps and devices your users access, and the behaviors that contribute to users' risk analyses. Through Azure AD integration, you gain access to the following insightful reports:
- User profiles
- User risk score trends
- Device profiles
- Device risk score trends
- Cloud app usage (by app)
- Cloud app usage (by category)
- Account compromise assessment (leaked account and suspicious user activity)

For details about the data collected, see the Data Collection Notice.

○ Off

Data source: Active Directory (on-premises)



Trend Micro Vision One™
Executive Dashboard Preview › Data source
2022-09-15 09:21 (UTC+08:00)
48
Trend Micro

Trend Micro Cloud One - Conformity	○	Monitor cloud configuration on AWS™, Microsoft® Azure, and
Trend Micro Cloud One - Endpoint & Workload Security	●	User, application, and web activities, and detected threats on
Trend Micro Deep Security	●	User, application, and web activities, and detected threats on
Network Intrusion Prevention *Preview*	●	Monitor cloud app activity on Office 365 apps
Trend Micro Web Security	●	Web activity of monitored devices and users via Trend Micro \
Trend Micro Mobile Security	○	Cloud apps detected by monitored mobile devices and users
TippingPoint Security Management System	○	Network detection logs and filter rule status
Zero Trust Secure Access - Private Access	○	User, device, and internal app activities from your internal net
Zero Trust Secure Access - Internet Access	○	User, device, and cloud app activities to external networks
Third-Party Data Source		
Azure AD	●	Allows access to user and device information and activity data
Active Directory (on-premises)	○	Allows access to user and device information from your intern
Okta	○	Allows access to user and device information and activity data

Data Source

Source:

Active Directory (on-premises)

Data upload permission:

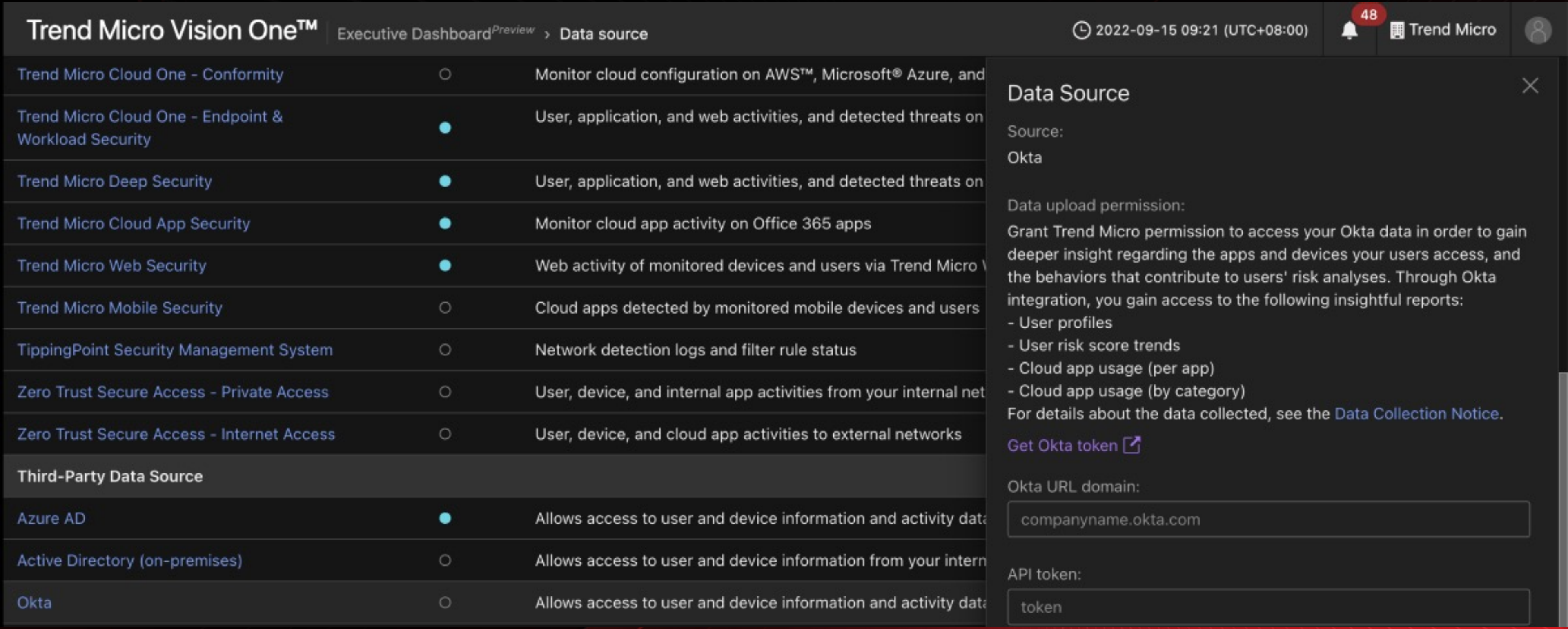
Grant Trend Micro permission to access your on-premises Active Directory data in order to gain deeper insight regarding your internal user accounts and devices that contribute to risk analyses.

For details about the data collected, see the Data Collection Notice.

Configure Active Directory (on-premises) in Third Party Integration

Off

Data source: Okta



Trend Micro Vision One™
Executive Dashboard Preview › Data source
2022-09-15 09:21 (UTC+08:00)
48
Trend Micro

Trend Micro Cloud One - Conformity	○	Monitor cloud configuration on AWS™, Microsoft® Azure, and
Trend Micro Cloud One - Endpoint & Workload Security	●	User, application, and web activities, and detected threats on
Trend Micro Deep Security	●	User, application, and web activities, and detected threats on
Trend Micro Cloud App Security	●	Monitor cloud app activity on Office 365 apps
Trend Micro Web Security	●	Web activity of monitored devices and users via Trend Micro \
Trend Micro Mobile Security	○	Cloud apps detected by monitored mobile devices and users
TippingPoint Security Management System	○	Network detection logs and filter rule status
Zero Trust Secure Access - Private Access	○	User, device, and internal app activities from your internal net
Zero Trust Secure Access - Internet Access	○	User, device, and cloud app activities to external networks
Third-Party Data Source		
Azure AD	●	Allows access to user and device information and activity data
Active Directory (on-premises)	○	Allows access to user and device information from your intern
Okta	○	Allows access to user and device information and activity data

Data Source

Source:

Okta

Data upload permission:

Grant Trend Micro permission to access your Okta data in order to gain deeper insight regarding the apps and devices your users access, and the behaviors that contribute to users' risk analyses. Through Okta integration, you gain access to the following insightful reports:
- User profiles
- User risk score trends
- Cloud app usage (per app)
- Cloud app usage (by category)

For details about the data collected, see the Data Collection Notice.

Get Okta token

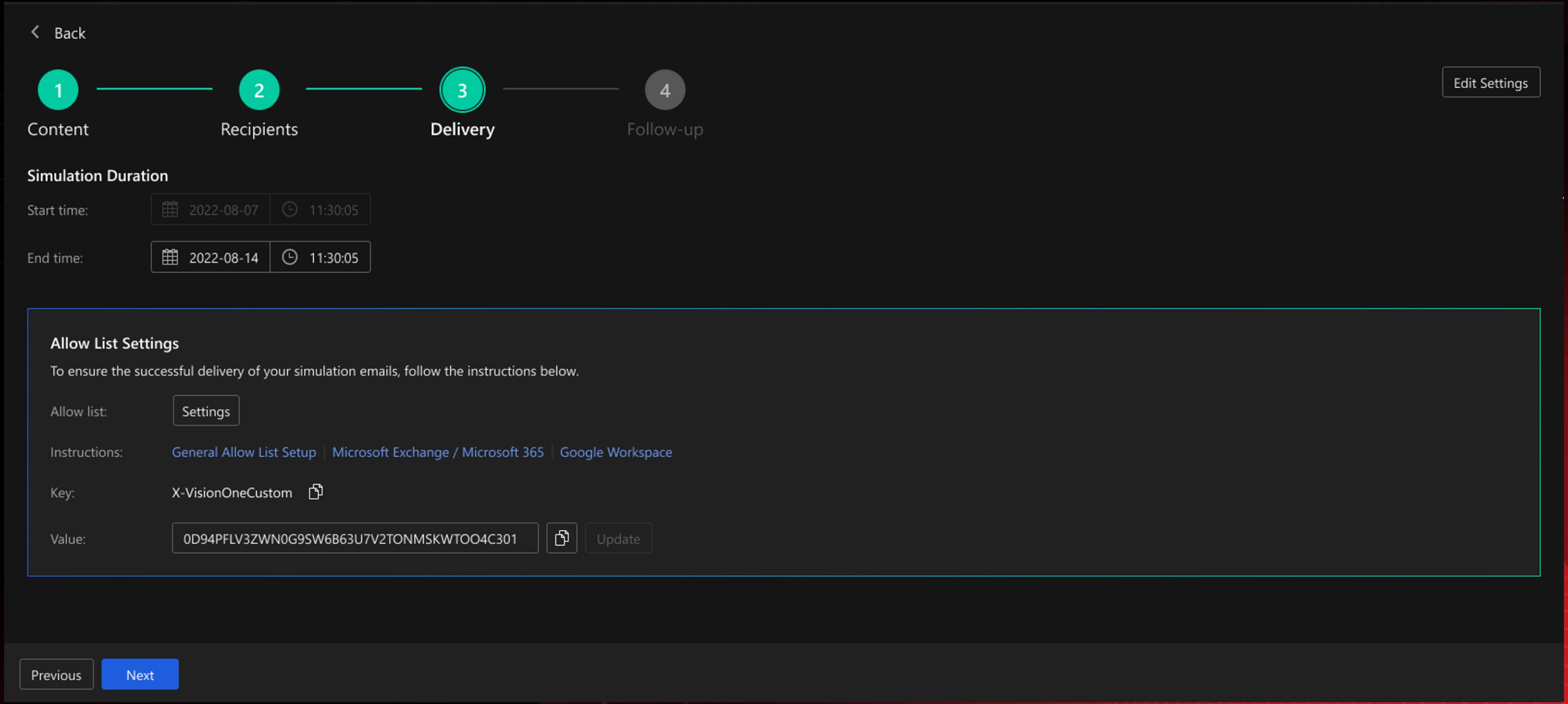
Okta URL domain:

companyname.okta.com

API token:

token

- Now you finished the “Recipients” step, and you have your list ready (through one of the three ways that we mentioned in the previous slides)
- In the “Delivery” step, set the end time of your campaign



Simulation Duration

Start time: 2022-08-07 11:30:05

End time: 2022-08-14 11:30:05

Allow List Settings

To ensure the successful delivery of your simulation emails, follow the instructions below.

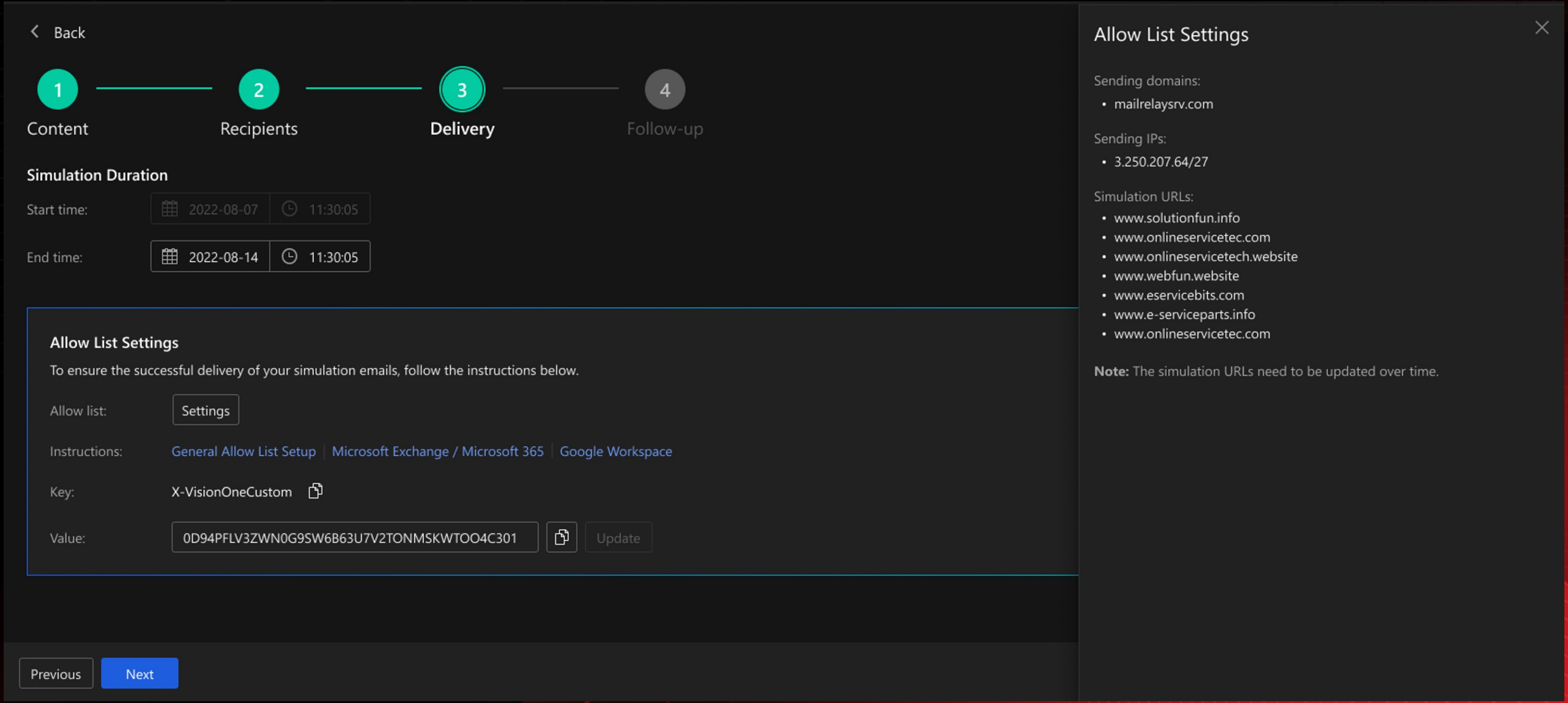
Allow list: Settings

Instructions: General Allow List Setup | Microsoft Exchange / Microsoft 365 | Google Workspace

Key: X-VisionOneCustom

Value: 0D94PFLV3ZWN0G9SW6B63U7V2TONMSKWTOO4C301

- Allow List Settings
- This is a vital step to ensure that the simulation emails are delivered to the inbox
- Check the Instructions links



Simulation Duration

Start time: 2022-08-07 11:30:05

End time: 2022-08-14 11:30:05

Allow List Settings

To ensure the successful delivery of your simulation emails, follow the instructions below.

Allow list: Settings

Instructions: General Allow List Setup | Microsoft Exchange / Microsoft 365 | Google Workspace

Key: X-VisionOneCustom

Value: 0D94PFLV3ZWN0G9SW6B63U7V2TONMSKWTOO4C301

Allow List Settings

Sending domains:

- mailrelaysrv.com

Sending IPs:

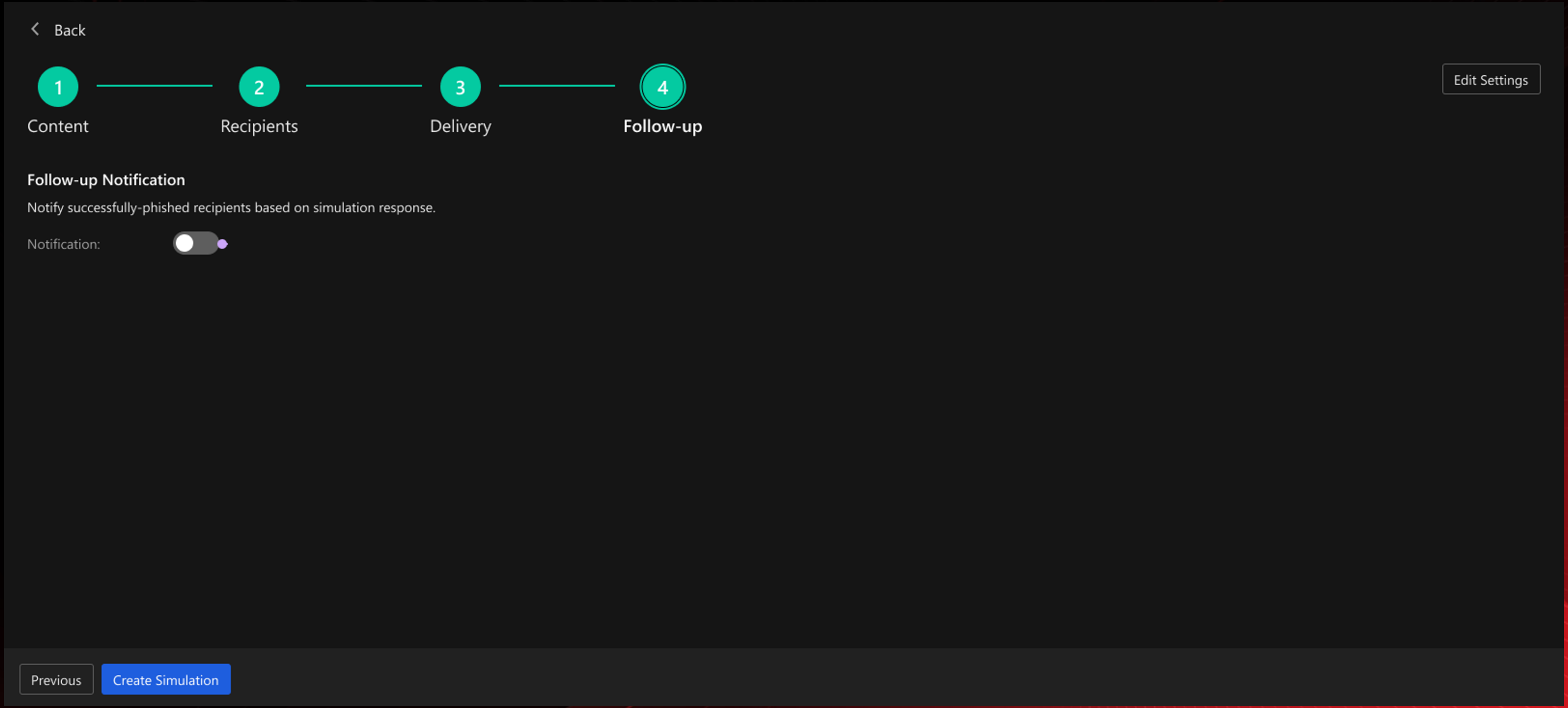
- 3.250.207.64/27

Simulation URLs:

- www.solutionfun.info
- www.onlineservicetec.com
- www.onlineservicetech.website
- www.webfun.website
- www.eservicebits.com
- www.e-serviceparts.info
- www.onlineservicetec.com

Note: The simulation URLs need to be updated over time.

In this final step, you can turn on the Follow-up Notification, that will allow the phished recipients to receive an email with some instructions to avoid any future risks

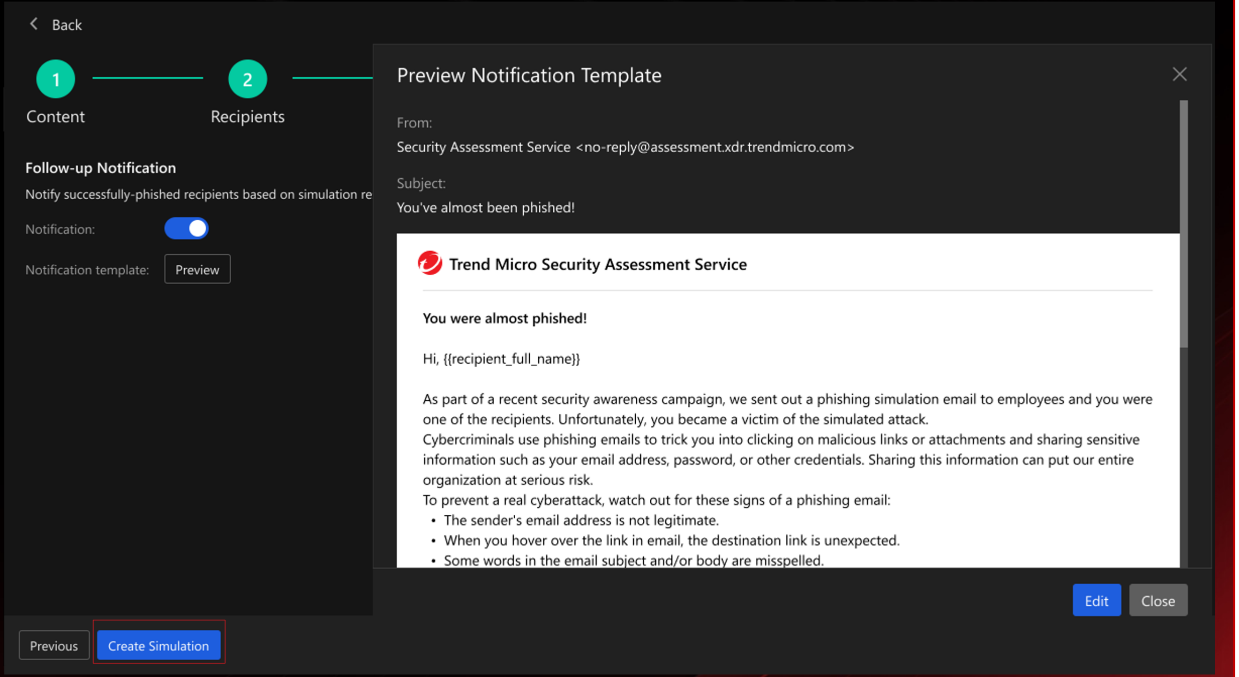


Follow-up Notification

Notify successfully-phished recipients based on simulation response.

Notification: ○

Customize the notification email template if needed



Follow-up Notification

Notify successfully-phished recipients based on simulation re

Notification:

Notification template: Preview

Preview Notification Template

From:
Security Assessment Service <no-reply@assessment.xdr.trendmicro.com>

Subject:
You've almost been phished!

Trend Micro Security Assessment Service

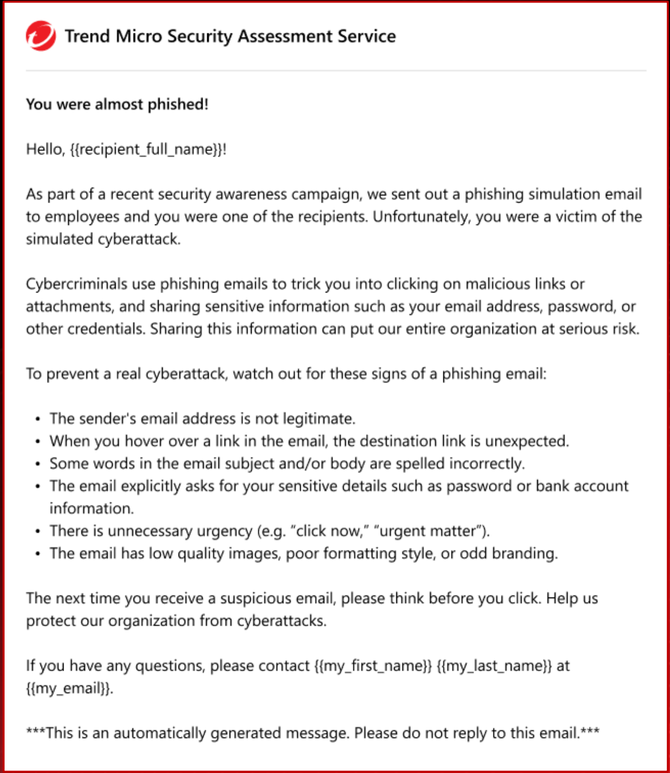
You were almost phished!

Hi, {{recipient_full_name}}

As part of a recent security awareness campaign, we sent out a phishing simulation email to employees and you were one of the recipients. Unfortunately, you became a victim of the simulated attack.
Cybercriminals use phishing emails to trick you into clicking on malicious links or attachments and sharing sensitive information such as your email address, password, or other credentials. Sharing this information can put our entire organization at serious risk.
To prevent a real cyberattack, watch out for these signs of a phishing email:

- The sender's email address is not legitimate.
- When you hover over the link in email, the destination link is unexpected.
- Some words in the email subject and/or body are misspelled.

Notification Template:



Trend Micro Security Assessment Service

You were almost phished!

Hello, {{recipient_full_name}}!

As part of a recent security awareness campaign, we sent out a phishing simulation email to employees and you were one of the recipients. Unfortunately, you were a victim of the simulated cyberattack.

Cybercriminals use phishing emails to trick you into clicking on malicious links or attachments, and sharing sensitive information such as your email address, password, or other credentials. Sharing this information can put our entire organization at serious risk.

To prevent a real cyberattack, watch out for these signs of a phishing email:

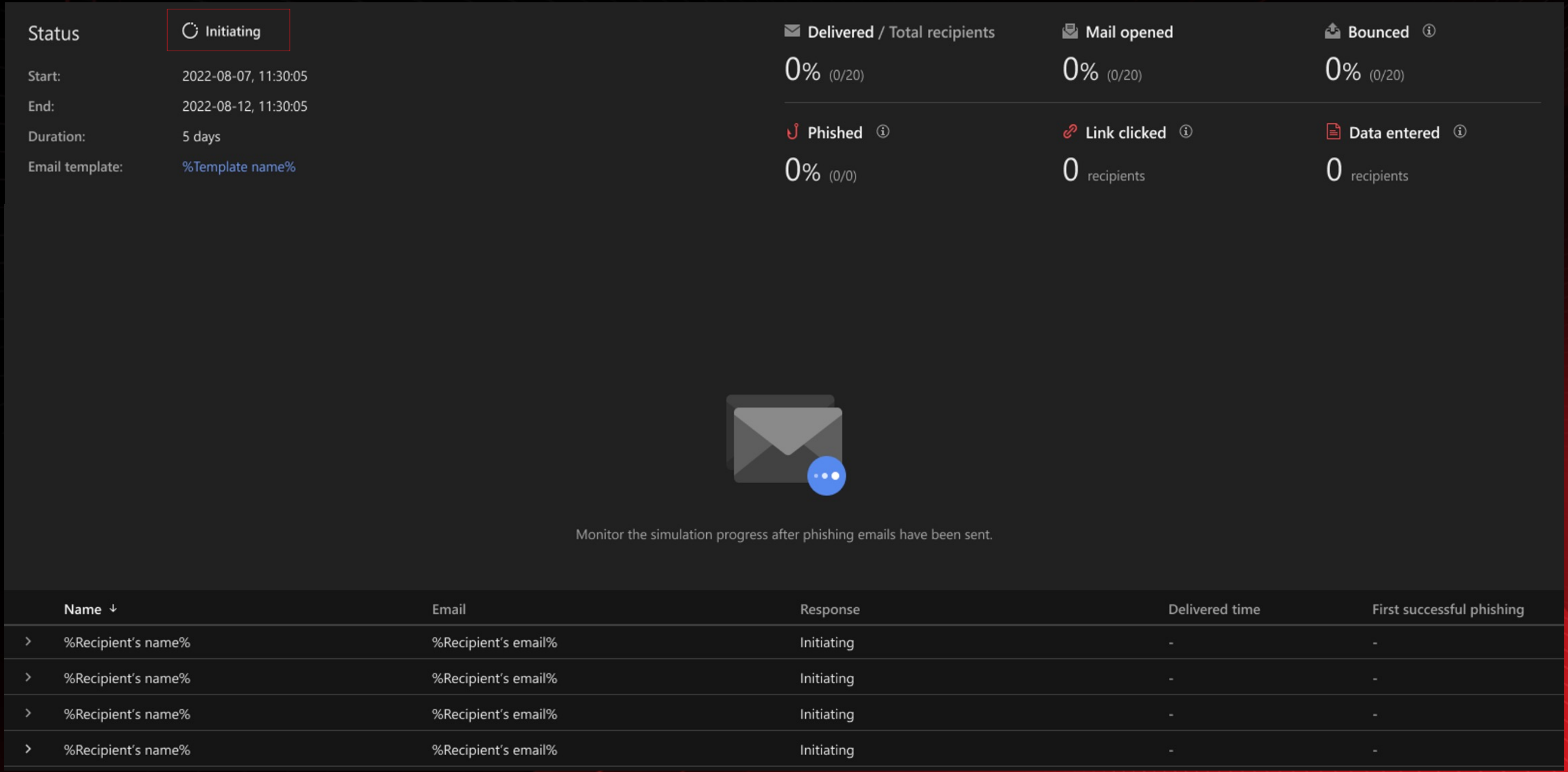
- The sender's email address is not legitimate.
- When you hover over a link in the email, the destination link is unexpected.
- Some words in the email subject and/or body are spelled incorrectly.
- The email explicitly asks for your sensitive details such as password or bank account information.
- There is unnecessary urgency (e.g. "click now," "urgent matter").
- The email has low quality images, poor formatting style, or odd branding.

The next time you receive a suspicious email, please think before you click. Help us protect our organization from cyberattacks.

If you have any questions, please contact {{my_first_name}} {{my_last_name}} at {{my_email}}.

This is an automatically generated message. Please do not reply to this email.

You can now monitor the simulation progress



Status | Initiating

Start: 2022-08-07, 11:30:05

End: 2022-08-12, 11:30:05

Duration: 5 days

Email template: %Template name%

Delivered / Total recipients: 0% (0/20)

Mail opened: 0% (0/20)

Bounced ⓘ: 0% (0/20)

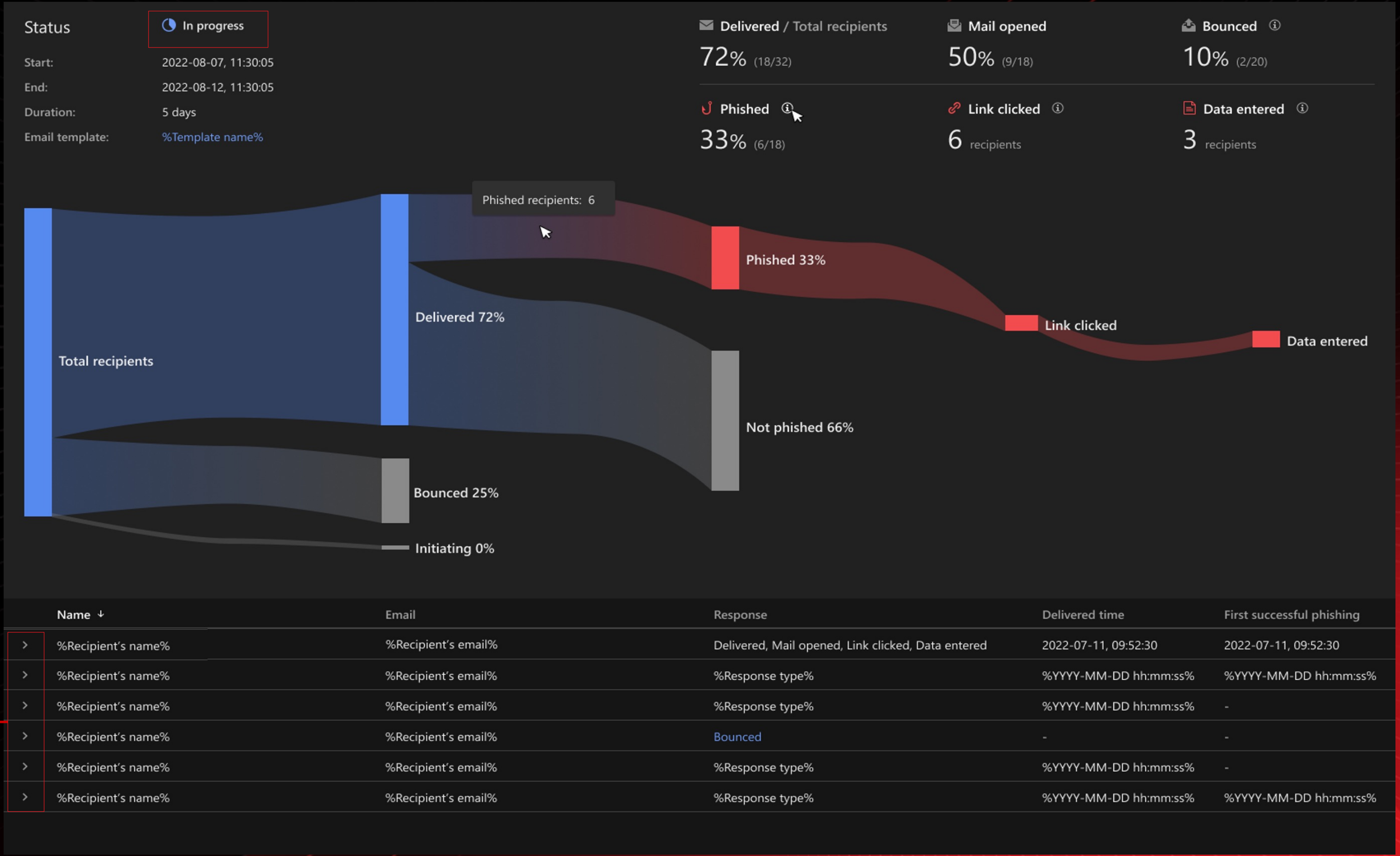
Phished ⓘ: 0% (0/0)

Link clicked ⓘ: 0 recipients

Data entered ⓘ: 0 recipients

Monitor the simulation progress after phishing emails have been sent.

	Name ↓	Email	Response	Delivered time	First successful phishing
›	%Recipient's name%	%Recipient's email%	Initiating	-	-
›	%Recipient's name%	%Recipient's email%	Initiating	-	-
›	%Recipient's name%	%Recipient's email%	Initiating	-	-
›	%Recipient's name%	%Recipient's email%	Initiating	-	-



Status: In progress

Start: 2022-08-07, 11:30:05

End: 2022-08-12, 11:30:05

Duration: 5 days

Email template: %Template name%

Delivered / Total recipients 72% (18/32)

Mail opened 50% (9/18)

Bounced 10% (2/20)

Phished 33% (6/18)

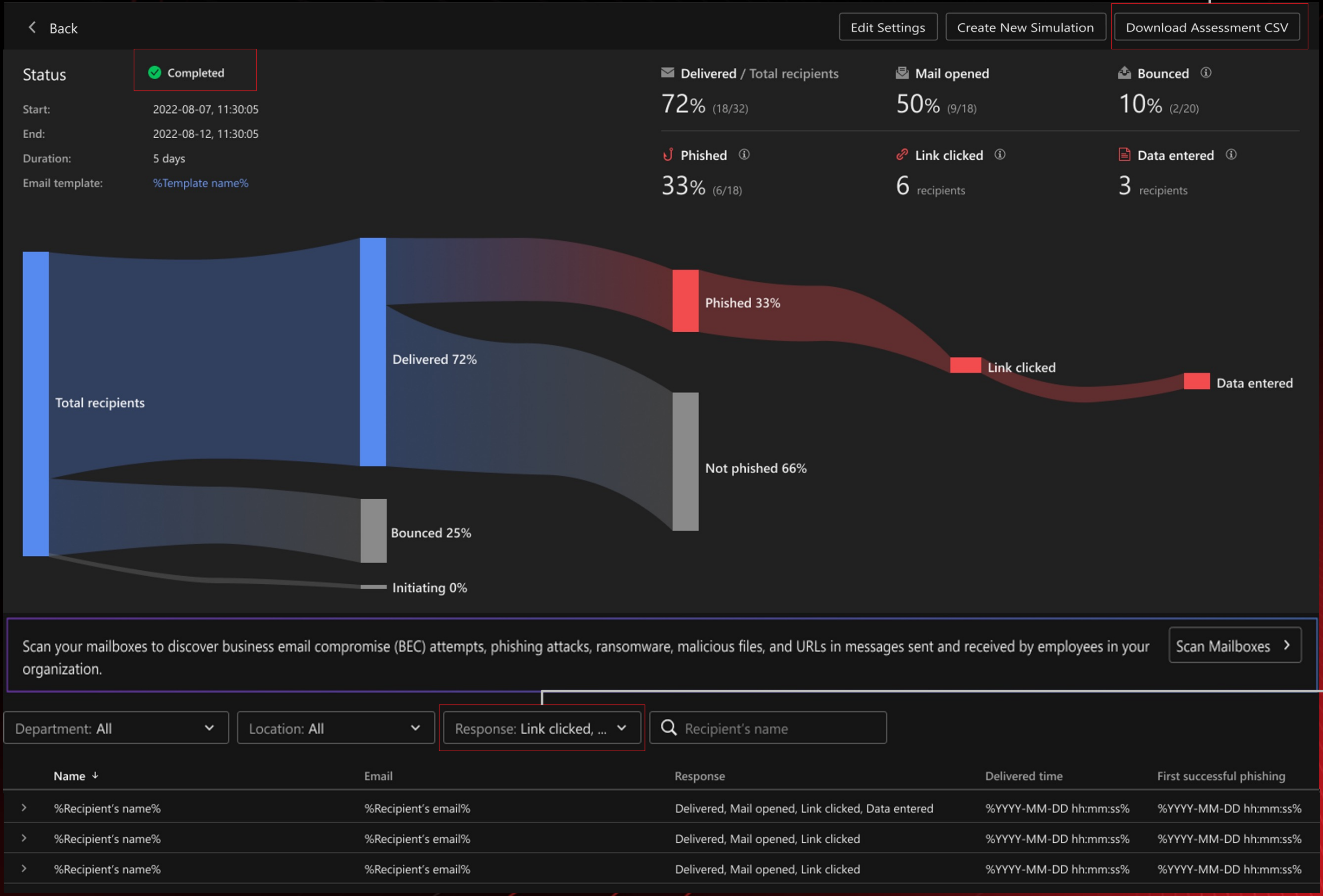
Link clicked 6 recipients

Data entered 3 recipients

	Name ↓	Email	Response	Delivered time	First successful phishing
>	%Recipient's name%	%Recipient's email%	Delivered, Mail opened, Link clicked, Data entered	2022-07-11, 09:52:30	2022-07-11, 09:52:30
>	%Recipient's name%	%Recipient's email%	%Response type%	%YYYY-MM-DD hh:mm:ss%	%YYYY-MM-DD hh:mm:ss%
>	%Recipient's name%	%Recipient's email%	%Response type%	%YYYY-MM-DD hh:mm:ss%	-
>	%Recipient's name%	%Recipient's email%	Bounced	-	-
>	%Recipient's name%	%Recipient's email%	%Response type%	%YYYY-MM-DD hh:mm:ss%	-
>	%Recipient's name%	%Recipient's email%	%Response type%	%YYYY-MM-DD hh:mm:ss%	%YYYY-MM-DD hh:mm:ss%

Expand for more details about each recipient

Phishing Simulation Assessment Report



Status: Completed

Start: 2022-08-07, 11:30:05

End: 2022-08-12, 11:30:05

Duration: 5 days

Email template: %Template name%

Delivered / Total recipients: 72% (18/32)

Mail opened: 50% (9/18)

Bounced: 10% (2/20)

Phished: 33% (6/18)

Link clicked: 6 recipients

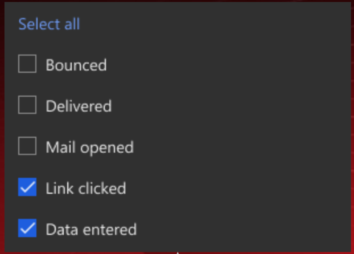
Data entered: 3 recipients

Scan your mailboxes to discover business email compromise (BEC) attempts, phishing attacks, ransomware, malicious files, and URLs in messages sent and received by employees in your organization.

Name ↓	Email	Response	Delivered time	First successful phishing
%Recipient's name%	%Recipient's email%	Delivered, Mail opened, Link clicked, Data entered	%YYYY-MM-DD hh:mm:ss%	%YYYY-MM-DD hh:mm:ss%
%Recipient's name%	%Recipient's email%	Delivered, Mail opened, Link clicked	%YYYY-MM-DD hh:mm:ss%	%YYYY-MM-DD hh:mm:ss%
%Recipient's name%	%Recipient's email%	Delivered, Mail opened, Link clicked	%YYYY-MM-DD hh:mm:ss%	%YYYY-MM-DD hh:mm:ss%

Download the assessment CSV report for the full simulation results

Filter the results based on the response type:

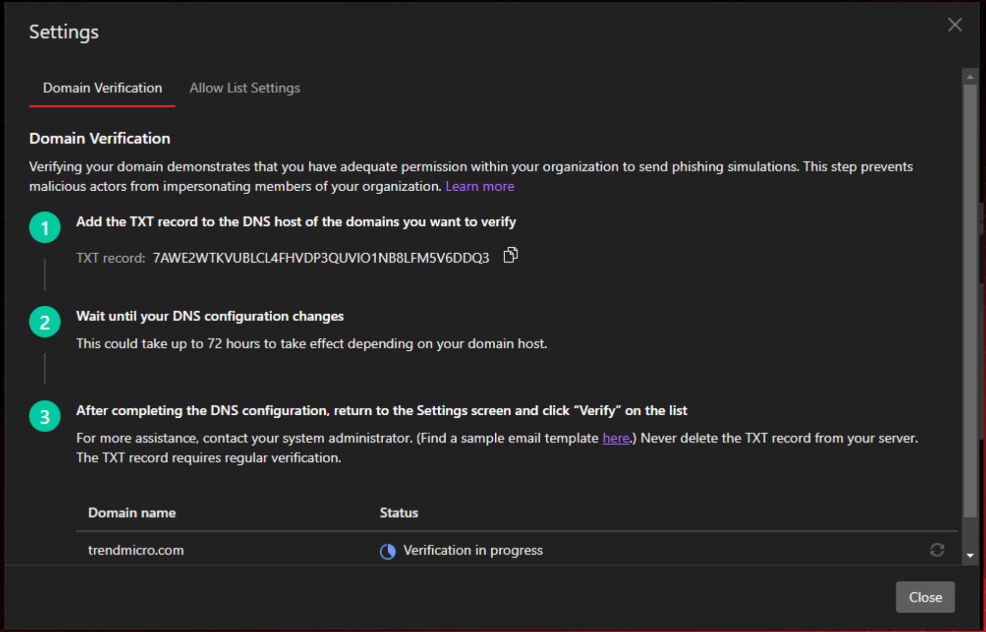

Select all

- ☐ Bounced
- ☐ Delivered
- ☐ Mail opened
- ☑ Link clicked
- ☑ Data entered

TREND MICRO

Security control - Verifying your domain

- A user can send a phishing simulation to up to 5 employees when first using the phishing simulator.
- You can only send a phishing simulation to employees with the same domain as the Vision One user.
- To send a Phishing simulation to more than 5 employees the user needs to verify their domain.
- Click “Edit Settings” on the top right of your screen and follow the instructions to verify your domain



Domain Verification

Verifying your domain demonstrates that you have adequate permission within your organization to send phishing simulations. This step prevents malicious actors from impersonating members of your organization. Learn more

1. **Add the TXT record to the DNS host of the domains you want to verify**

   TXT record: 7AWE2WTKVUBLCL4FHVDP3QUVIO1NB8LFM5V6DDQ3

2. **Wait until your DNS configuration changes**

   This could take up to 72 hours to take effect depending on your domain host.

3. **After completing the DNS configuration, return to the Settings screen and click “Verify” on the list**

   For more assistance, contact your system administrator. (Find a sample email template here.) Never delete the TXT record from your server. The TXT record requires regular verification.

Domain name	Status
trendmicro.com	Verification in progress

partnersupport@trendmicro.com