AI Defense Assets

Integrates with Cisco Multicloud Defense to detect all AI workloads in your environment, including AI models, agents, and knowledge bases.

Once you've created an AI Defense connection to Multicloud Defense, AI Defense crawls your environment to detect all AI Assets (models, agents, and knowledge bases). Once a model has been discovered, it appears in the AI Assets: Cloud Visibility tab, and you can test it for vulnerabilities in the Validation tab.

The AI Assets page has:

- **Cloud visibility**: Provides an overview of your cloud environment, focusing on AI-related activities and assets.
- **External assets**: Designed to track and manage AI resources that exist outside the organization's direct cloud infrastructure.

Cloud Visibility

Cloud Visibility provides an overview of AI activities and assets within your cloud infrastructure, helping organizations identify models, applications, and resources in use. It offers insights into usage patterns, potential risks, and compliance status while monitoring hosting regions and VPC instances. This feature enhances transparency and control over AI workloads across multi-cloud environments.

- **Discovered AI assets**: Shows a count of the models, agents, and knowledge bases discovered.
- **Model validation status**: Indicates progress in validating the models in your environment. See the Validation page for test run results.
- **AI assets table**: Lists the discovered AI assets. For each, details are shown in the columns:
  - **AI Asset Name**: A clickable link directing you to the inspection page for the discovered asset. Select the link to access the **AI Asset** Details page.
  - **Asset Type**: Specifies the category of the asset, such as **Custom Model** or **Foundational Model**
  - **Discovered Date**: The date when the asset was first detected during a scan.
  - **Regions**: Identifies the cloud region where the asset is hosted.
  - **Last Validation**: Displays the timestamp of the most recent test performed on the asset. Click the timestamp to review the corresponding **Test Report**.
  - **Action**: Provides the option to initiate or re-run a test for the asset.

- **AI asset details**: Provides details that AI Defense has discovered about this asset. To re-run the validation scan, click the **Validate** button near the top of the screen.

External Assets

External Assets tracks and manages third-party AI resources, including generative AI applications and external knowledge bases. It offers visibility into their usage, risk scores, and protection status, ensuring organizations can secure external AI dependencies and mitigate the risks posed by shadow AI or unmonitored assets.

We detect traffic that goes to third-party models hosted outside your AWS cloud. For these, no validation is run, but AI Defense can show details about the network traffic to the model.

This data comes from Cisco Multicloud Defense. For an explanation of these fields, see the MCD documentation.

For each instance in your cloud that connects to an external AI model, the **Instances connecting to external assets** table shows:

- **Resource Name:** Displays the AWS VPC, subnet, and instance involved in the connection to an external model.
- **Account:** Identifies the AWS account associated with the instance that initiated the model connection.
- **Region:** Specifies the cloud region where the instance initiating the model connection is located.
- **VPC ID:** Indicates the unique identifier of the VPC hosting the instance that established the model connection.
- **Last Detected Date:** Shows the most recent timestamp when this resource connected to the external model.
- **Source IP:** Lists the IP address used by the instance to connect to the model.
- **Instances:** Provides details about the specific instances involved in the connection.

Initial Configuration of AI Assets

Remember

Prerequisite: Your organization must have a Multicloud Defense (MCD) tenant for use by AI Defense. If you don't have an MCD tenant available, see below:

Configuring Multicloud Defense for AI Defense Integration.

To set up AI Assets detection:

1. Create an API key in Multicloud Defense. Capture the API Key ID and API Key Secret for use in the next step. See Cisco Multicloud Defense User Guide - Management [Cisco Defense Orchestrator]
2. Open the AI Defense Administration tab, go to the Multicloud Defense card, and click Connect, and provide the API key details to complete the connection. See the AI Defense Administration documentation for details.
3. Return to Multicloud Defense and use the Connect Account button to connect Multicloud Defense to your cloud account. See Cisco Multicloud Defense User Guide - Setup with the Multicloud Defense Wizard [Cisco Defense Orchestrator]

4. In Multicloud Defense, you must either Enable Traffic Visibility, Secure Your Account, or both. See Cisco Multicloud Defense User Guide - Setup with the Multicloud Defense Wizard [Cisco Defense Orchestrator] and Cisco Multicloud Defense User Guide - Setup with the Multicloud Defense Wizard [Cisco Defense Orchestrator]

Note AWS is supported for early access

After Multicloud Defense has completed its scan, the AI Assets tab in AI Defense will display the AI Models in your cloud and the external models that call into instances in your cloud.

Configuring Multicloud Defense for AI Defense Integration

If your organization does not have a Multicloud Defense tenant available, follow the instructions below to create a new Multicloud Defense tenant:

Set Up Multicloud Defense (MCD) within Security Cloud Control (SCC)

If You Already Have Both SCC and MCD Accounts

- Login to SCC: Access your account.
- Navigate to MCD Management:

  Left-hand pane → Administration → Multicloud Defense Management.

If You Have an SCC Account but Haven't Activated MCD

- Login to SCC: Access your account.
- Activate MCD: Follow the steps below to enable MCD.

If You Do Not Have an SCC Account

- Create an SCC Account:

  Visit https://getcdo.com/.

  Follow the instructions to create an account.
- Enable MCD: After account creation, proceed with the steps below.

Enable Multicloud Defense

- Access MCD Management:

  Left-hand pane → Administration → Multicloud Defense Management (accept the EULA).
- Initiate Cloud Protection:

  Click the rocket ship icon (top right) → Select Protect cloud assets.
- Enable Multicloud Defense:

  Click Enable Multicloud Defense.

  Follow the on-screen prompts to create an MCD tenant (takes a few minutes)

Next Step

Return to the preceding section, Initial Configuration of AI Assets to connect AI Defense to your MCD tenant.