AI Defense

When you enable the integration with AI Defense you can secure your AI assets including the associated activity, types of connections, and number of identities accessing unsanctioned models. By utilizing this function with your Multicloud Defense tenant, you can discover models in your environment and apply AI Defense runtime protection. Once discovered, models can also be tested for safety and security using AI Defense validation. For more information on AI Defense and what it can do to improve your safety and security with AI, see AI Defense documentation.

AI Defense Integration with Multicloud Defense

Support and Limitations

Depending on how integrated you want your Multicloud Defense tenant and AI Defense to be, here are the requirements and limitations:

- You **must** have a Security Cloud Control account prior to accessing either AI Defense or Multicloud Defense.
- Only **egress** Multicloud Defense Gateways are currently compatible with AI Defense.
- If you want the full AI Defense experience with AI Runtime monitoring of LLM prompts and responses, you **must** "Secure Your Account" and add a Service VPC or VNet to your gateway.
- Profiles and rulesets created in Multicloud Defense directed to support your AI Defense integration **must** be modified in the Multicloud Defense Controller; you cannot delete or modify a Multicloud Defense policy or ruleset in the AI Defense dashboard.
- You must have an AI Defense license. See Administration for more information on AI Defense licenses.

Overview

The following list is an overview of the procedure to enable both aspects of these products to allow a secure integration:

1. Log into your Multicloud Defense tenant.
2. Generate an API Key with the Multicloud Defense dashboard.

3. Connect your Multicloud Defense tenant to AI Defense.
4. Onboard a cloud service provider to Multicloud Defense. Be sure to add the correct permissions to your AWS account to allow secure access and communication.
5. Enable Traffic Visibility.
6. Secure Your Account.
7. AI Guardrails Profile
8. Attach your profile to the policy ruleset of an egress gateway.