# AI Defense

AI Defense との統合を有効にすると、関連するアクティビティ、接続のタイプ、および許可されていないモデルにアクセスするアイデンティティの数を含む AI アセットを保護できます。Multicloud Defense テナントでこの機能を利用することで、環境内でモデルを検出し、AI Defense ランタイム保護を適用できます。検出したら、AI Defense 検証を使用してモデルの安全性とセキュリティをテストすることもできます。AI Defense の詳細および、AI で安全性とセキュリティを向上させるためにできることについては、AI Defense のマニュアルを参照してください。


- Multicloud Defense の AI Defenseとの統合 （1 ページ）


# Multicloud Defense の AI Defenseとの統合

### 制限事項と制約事項

Multicloud Defense テナントと AI Defense の統合方法に応じて、次の要件と制限事項が課されます。

- AI Defenseまたは Multicloud Defense にアクセスする前に、Security Cloud Control アカウントが**必要です** 。
- 現在、AI Defense と互換性があるのは**出力** Multicloud Defense Gateway のみです。
- LLM プロンプトと応答の AI ランタイムモニタリングを含む完全な AI Defense エクスペリエンスを得るには、「アカウントを保護」し、サービス VPC または VNet をゲートウェイに追加する**必要があります**。
- AI Defense 統合をサポートするために Multicloud Defense で作成されたプロファイルとルールセットは、Multicloud Defense Controller で変更する**必要があります**。 AI Defense ダッシュボードで Multicloud Defense ポリシーまたはルールセットを削除または変更することはできません。
- AI Defense ライセンスが必要です。AI Defense ライセンスの詳細については、「管理」を参照してください。
- AWS および Azure でアセットの AI の検出が行われます。

## 概要

次のリストは、これらの製品の両方の側面から安全な統合を可能にする手順の概要を示しています。

1. Multicloud Defense テナントにログインします。
2. Multicloud Defense ダッシュボードを使用してAPI キーを生成します 。
3. Multicloud Defense テナントを AI Defense に接続します。
4. クラウド サービス プロバイダーを Multicloud Defense に導入準備します。セキュアなアクセスと通信を許可するために、AWS アカウントに 適切な権限を追加してください。
5. トラフィックの可視性を有効化します。
6. アカウントを保護します。
7. AI ガードレールプロファイル
8. 出力ゲートウェイのポリシールールセットにプロファイルを添付します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。