ジェネレーティブAIおよびChatGPTに対するDLPおよびCASBサポートの設定

内容

[はじめに](#)
[概要](#)

はじめに

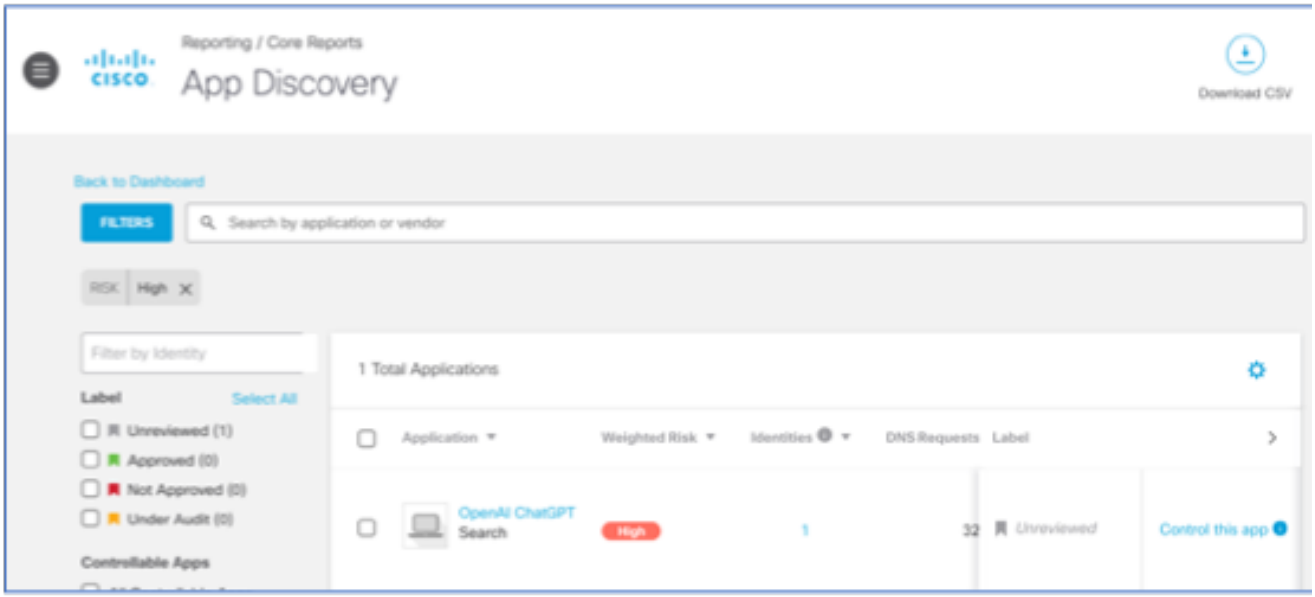
このドキュメントでは、ジェネレーティブAIおよびChatGPTに対するCloud Access Security Broker(CASB)およびデータ損失防止(DLP)のサポートについて説明します。

概要

シスコは、Umbrella製品スイートに新しいCloud Access Security Broker(CASB)とデータ損失防止(DLP)の機能拡張をリリースしました。これは、お客様が組織内でChatGPTの使用をより効果的に管理できるように設計されています。
これらの機能拡張により、お客様は従業員がChatGPTを責任を持って安全に使用し、機密情報を潜在的なリスクから保護することができます。

主な機能は次のとおりです。

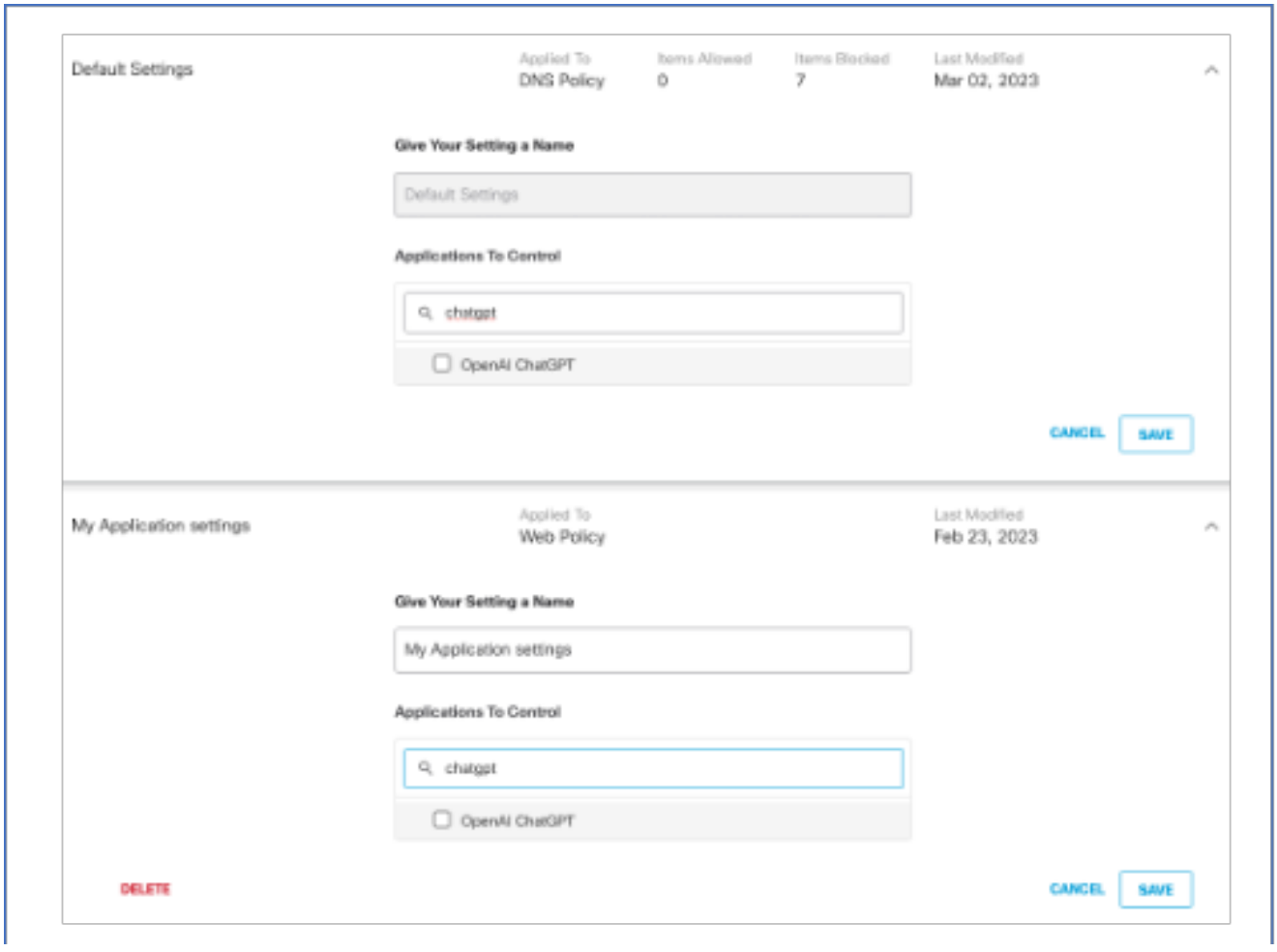
1. 組織内でのChatGPTの使用状況の検出：
   App Discoveryレポート(Reports -> Core Reports)を使用すると、お客様は組織全体のChatGPT使用状況を特定して監視できます。
   これにより、従業員がどのようにツールを使用しているかについての貴重な洞察が得られ、ツールの使用を最適化して社内ポリシーへのコンプライアンスを確保できます。



16221272854164

16221291406100

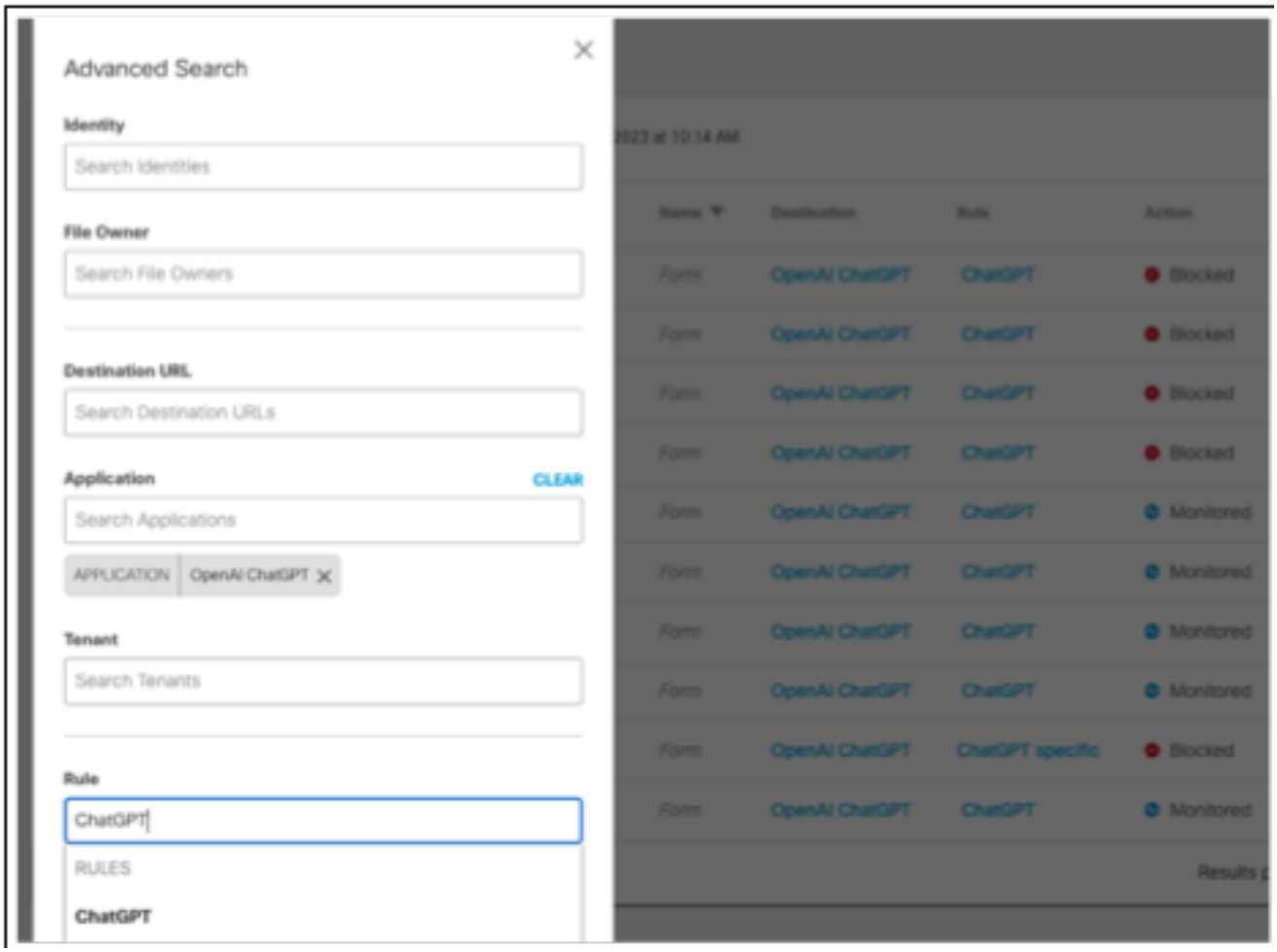
2. ChatGPTアクセスのきめ細かい制御：
すべてのユーザがChatGPTにアクセスできないようにしたり、特定のユーザまたはユーザグループにのみアクセスを許可したりできるようになりました。
この細かい制御により、セキュリティとコンプライアンスの要件に従ってChatGPTの使用を管理できます。 アプリケーションの設定でopenAI ChatGPTを選択すると、DNSポリシーとWebポリシーの両方を通じてブロックが可能になります。



16221268217748

3. DLPによるChatGPT使用リスクの評価：
リアルタイムDLPを使用すると、送信されChatGPTと共有される機密情報の種類を監視で

きます。これは、ChatGPTの使用に関連するリスクを評価し、データの漏洩や侵害の可能性を軽減するための適切な措置を講じるのに役立ちます.
ChatGPTのDLPモニタリングを有効にするには、宛先をAll Destinationsに設定したリアルタイムルールを使用するか、利用可能なアプリケーションのリストから特にopenAI ChatGPTを選択します。



16221283948052

4. DLPを使用したChatGPTの安全な使用の許可：
シスコのDLPソリューションを使用すると、機密情報を含むChatGPTへのプロンプトをブロックできます。これにより、従業員は潜在的なリスクにさらされることなく、安全かつ安全にChatGPTを使用し続けることができます。
ChatGPTのDLPブロッキングを有効にするには、宛先をAll Destinationsに設定したリアルタイムルールを使用するか、利用可能なアプリケーションのリストから特にopenAI ChatGPTを選択します。

16221311959572

5. DLPを使用したChatGPTへのソースコード漏えいの防止：
   新しいソースコードデータIDを使用すると、DLPを使用してChatGPTとのソースコード共有を監視および停止し、貴重な知的財産(IP)を保護できます。

6. 新しいジェネレーティブAIアプリケーションカテゴリ：
   新しいジェネレーティブAIアプリケーションカテゴリが導入され、より広範なツールの使用の検出と防止に取り組みました。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。