包括クラウドマルウェア検出一般提供

内容

はじめに

このドキュメントでは、Umbrellaクラウドマルウェア検出の一般的なアベイラビリティについて説明します。

背景説明

Cisco UmbrellaがCASBのビジョンに基づいて継続的に取り組む中、シスコはUmbrella Cloud Malware Detectionの一般提供を開始しました。

マルウェアはさまざまな方法で組織に侵入する可能性があります。市場の既存のセキュリティソリューションのギャップはクラウドプラットフォームです。マルウェアを含むファイルはクラウド内で実際の被害を受けることはありませんが、ユーザのエンドポイントにダウンロードすると被害を受ける可能性があります。

クラウドマルウェア検出とは

認定されたクラウドアプリケーション内の悪意のあるファイルを検出して修復する機能。この機能を追加することで、セキュリティ管理者は報告されたマルウェア（Cisco AMPおよびその他のUmbrella AVツールで見つかった休眠マルウェア）を調査し、それらのファイルを隔離または削除することを選択して環境を保護できます。

クラウドマルウェア検出により、組織は次のことが可能になります。

- クラウドの変革を安全に共有およびサポート
- クラウドマルウェア感染の拡大を防止
- クラウドマルウェアインシデントのレポート

サポートされるアプリケーション

Office365、Box、Dropbox、Webex Teams、およびGoogle（近日提供予定）がサポート対象アプリケーションです。

クラウドマルウェア検出は、製品のどこで確認できますか。

クラウドマルウェア検出は次の場所にあります。

レポート>クラウドマルウェア

Admin > Authentication（セルフオンボーディングフロー）

関連情報

- レポート文書
- オンボーディングドキュメント
- デモビデオ
- シスコのテクニカルサポートとダウンロード

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。