Cloud Protection for Salesforce

Testing Guide

目次

第 章
1

はじめに

トピック :

本ガイドでは、WithSecure Cloud Protection for Salesforceをテストする方法について説明し、さらにテストを計画するためのヒントや便利な情報を提供します。

1.1 ソリューション概要

WithSecure Cloud Protection for Salesforceは、Salesforceプラットフォームの既存のセキュリティ機能を強化および拡張するように設計されたクラウドベースのセキュリティソリューションです。

WithSecure Cloud Protection for Salesforceは、Salesforce Cloudに出入りするコンテンツを分析します。これにより、Salesforce組織からアップロードまたはダウンロードされるファイルやURLが、会社、パートナー、顧客に対するサイバー攻撃に使用されることがなくなります。

このソリューションには、SalesforceアプリケーションとWithSecure Security Cloudが含まれています。WithSecure Security Cloud. WithSecure Security Cloudは、ファイルとWebサイトのレピュテーションとセキュリティサービスを提供します。WithSecure Cloud Protection for Salesforceアプリケーションは、会社が使用しているSalesforce Sales、Service、またはExperience Cloud（旧名「Community Cloud」）にインストールされます。 他のソフトウェアをインストールしたり、ネットワーク構成を変更したりする必要はありません。

WithSecure Security Cloudは、脅威を分析して対応するためのクラウドベースのシステムです。数百万のセンサー ノードから脅威インテリジェンスを収集し、デジタル脅威の大規模なデータベースを作成します。このデータベースは、世界的なサイバー脅威をリアルタイムで表示します。

WithSecure Cloud Protection for Salesforceは、このデータを使用して、グローバルまたはローカルの脅威状況の変化に迅速に対応します。たとえば、当社のヒューリスティック分析と動作分析によって新たなゼロデイ攻撃が検出された場合、当社はこの情報をすべての顧客と共有します。 これにより、高度な攻撃が最初に検出された直後に無効化することができます。

このソリューションは遅延を短縮するように設計されており、Salesforceの使用には影響しません。ファイルまたはコンテンツを分析する際、このソリューションはWithSecure Security Cloudを利用する多段階プロセスを使用します。このプロセス内のステップは、コンテンツのリスク プロファイルに基づいてアクティブ化されます。たとえば、ゼロデイ マルウェアやその他の高度な脅威を使用した攻撃を防ぐように設計されたSmart Cloud Sandboxingテクノロジーを使用して、リスクの高いファイルのみがより徹底的な分析を受けます。

1.2 テストオプション

WithSecureは、WithSecure Cloud Protection for Salesforceをテストするために3つの異なる方法を提供します。

1. WithSecureのライブデモを予約します。

   cloudprotection@WithSecure.comにメールを送信して、ソリューションのウォークスルーとライブデモセッションを予約してください。

2. 事前に設定されたSalesforceの組織でテストドライブ（試運転）をしてみましょう。

   Salesforce AppExchangeのテストドライブは、WithSecure Cloud Protection for Salesforceを簡単にテストする方法を提供します。ソリューションはすでにテスト組織にインストールされており、悪意のあるファイルのダウンロードまたはアップロード、悪意のある許可されていないURLのアップロードまたはクリックを試して、WithSecure Analytics（アナリティクス）、レポート、設定を詳しく調べることができます。

3. Salesforce組織に30日間の無料試用版をインストールします。

   より詳細なテストを行うには、WithSecure Cloud Protectionを自分のSalesforce組織にインストールします。Salesforce AppExchangeから数分でソリューションをインストールできます。その後、ソリューションは30日間の試用モードで自動的に実行されます。ソリューションをインストールするときは、WithSecureクイックインストールガイドに従ってください。

第 章
2

テストドライブでソリューションをテストする

トピック :

WithSecure Cloud Protection for Salesforceのテストをより簡単かつ便利に行うために、Anti-Malware Testfile (EICAR) とテスト用のWithSecure URLが含まれている、事前に構成されたSalesforce Test Drive組織があります。

注 : EICARはコンピュータに有害なマルウェア対策用のテストファイルです。詳細については、http://www.eicar.org/85-0-Download.htmlを参照してください。

2.1 テストドライブ組織を使い始める

次の手順に従って、テストドライブでCloud Protection for Salesforceのテストを開始します。

1. WithSecure Cloud Protectionアプリのリストで [**テストドライブ**] をクリックします。
2. Salesforceアカウントを使用してAppExchangeにログインします。
   Salesforce Test Drive組織にアクセスできるようになり、WithSecure Cloud Protection for Salesforce **Protection Dashboard**が表示されます。

2.2 ファイル保護の動作を確認する

次の手順に従って、ファイル保護がどのように機能するかの例を確認してください。

1. [**アプリランチャー**] に移動し、[**Sales**] を開きます。
2. [**アカウント**] をクリックし、[**WithSecure Demo Account**] を選択します。
   WithSecure Cloud Protection for Salesforceがアップロード時に悪意のあるファイルを削除し、テキストファイルで置き換えたことがわかります [有害なコンテンツは削除されました] `ExampleMaliciousFile`。
3. `ExampleMaliciousFile.docx`をダウンロードしてみてください。
   WithSecure Cloud Protection for Salesforceがダウンロードをブロックします。

2.3 URL 保護の動作を確認する

次の手順に従って、URL保護がどのように機能するかの例を確認してください。

1. [**アプリランチャー**] に移動し、[**Chatter**] を開きます。
   WithSecure Cloud Protection for Salesforceは、分析のために元のURLを書き換えました。
2. WithSecureのテストURLをクリックしてみてください。
   WithSecure Cloud Protection for Salesforceが有害で許可されていないWebサイトへのアクセスをブロックします。

2.4 アナリティクス分析情報を表示する

WithSecure Cloud Protection for Salesforceにはチェックしたファイルや URLのイベントをすべて確認できるアナリティクス分析セクションがあります。

1. [**アプリケーション ランチャー**] から [**Cloud Protection**] を開きます。
2. **アナリティクス** > **ファイル イベント** タブを開きます。
   すべてのファイル分析イベントが表示され、ファイルイベント履歴にアクセスできます。
3. イベントの [**履歴**] 列の [**表示**] をクリックします。
   [ファイルイベント履歴] ビューが開き、選択したファイルのアップロードおよびダウンロードアクションの詳細が表示されます。
4. **アナリティクス** > **URLイベント**タブを開きます。
   すべてのURL分析イベントが表示され、URLイベント履歴にアクセスできます。
5. イベントの [**履歴**] 列の [**表示**] をクリックします。
   [URLイベント履歴] ビューが開き、選択したURLの投稿と解決されていないアクションの詳細が表示されます。

2.5 要約ダッシュボードとレポートを表示する

[**概要**] タブには、Salesforceコンテンツの概要が表示されます。

[**概要**] タブをクリックします。
このダッシュボードには、WithSecure Cloud Protection for Salesforceがチェックした Salesforceコンテンツの完全な統計情報が表示されます。

注 : [その他のレポート] オプションは、ソリューションの試用版と製品版で利用できます。

2.6 ソリューション設定を表示する

テストドライブでは、WithSecure Cloud Protection for Salesforceの設定を変更することはできませんが、どのような設定が可能なのかを確認することができます。

[管理] タブを開きます。
ファイルおよびURL保護コンポーネントで使用できる設定と、ソリューションの一般的な設定が表示されます。

第 章
3

Salesforce組織でソリューションをテストする

トピック：

WithSecureは、すべてのSalesforceのお客様に30日間の無料試用期間を提供します。

WithSecure Cloud Protection for Salesforceは、Salesforce AppExchangeから直接、サンドボックス、開発、または本番組織に数分でインストールすることができます。

ソリューションをインストールする際は、クイックインストールガイドの指示に従ってください。

3.1 ファイル保護の動作を確認する

次の方法で Eicar テスト ファイルを使用してファイル保護の動作を確認できます。

1. `Eicar.com`テスト ファイルをhttps://www.eicar.org/?page_id=3950からダウンロードして、ファイル名を`Example_MaliciousFile.docx`に変更します。

   👉 **注:** `Eicar.com`は実際に脅威がないファイルですが、検証用にマルウェアとして認識されます。マルウェア対策ソフトがファイルをブロックした場合、特定のフォルダをリアルタイム スキャンから除外して `Eicar.com` ファイルをフォルダに入れてください。

2. `Example_MaliciousFile.docx` および安全なファイル を Salesforce *ファイル*または ***Chatter*** にアップロードします。
3. [**アプリケーション ランチャー**] から [**Cloud Protection**] を開きます。
4. **アナリティクス** > **ファイル イベント** タブを開きます。
   安全なファイルとブロックしたファイルが1ファイルずつあることが示されます。
5. 両方のファイルをダウンロードできるか試します。
   安全なファイルはダウンロードできますが、悪質なファイルはブロックされています。
6. **アナリティクス** > **ファイル イベント** タブに戻り、ダウンロード イベントを確認します。
7. [**表示**] をクリックするとイベント履歴を確認できます。
   選択したファイルに対するアップロード・ダウンロードのアクティビティが表示されます。

3.2 URL 保護の動作を確認する

次の方法でテスト ドメインを使用して URL 保護の動作を確認できます。

1. [**アプリケーション ランチャー**] から [**Cloud Protection**] を開きます。
2. **管理** > **URL 保護** タブを開きます。
3. このテストでは、[**許可していない カテゴリを選択**] で [*ギャンブル*] が選択されていることを確認してください。
4. 次の2つの URL `unsafe.fstestdomain.com` と `gambling.fstestdomain.info` を Salesforce ***Chatter*** に投稿します。
5. ***Chatter*** を開き、URL がある2つの新しい投稿を表示します。
6. **WithSecure Cloud Protection** に戻り、**アナリティクス** > **URL イベント** タブを開きます。
   Chatter の新規投稿が2つあります。
7. ***Chatter***に戻り、両方のリンクを開けるか試します。「***Web*** *サイトをブロックしました*」および「*許可していない* ***Web*** *サイトをブロックしました*」のブロック ページが表示されます。
8. **WithSecure Cloud Protection** に戻り、**アナリティクス** > **URL イベント** タブをもう一度開きます。
   URL を開いたイベントが2つ表示されます。
9. [**表示**] をクリックするとイベント履歴を確認できます。
   選択した URL に対するアクティビティ (投稿とリンクのアクセス) が表示されます。

3.3 要約ダッシュボードとレポートを表示する

[**概要**] タブには、Salesforce コンテンツの概要とレポートツールが表示されます。

1. [**概要**] タブをクリックします。
   このダッシュボードには、WithSecure Cloud Protection for Salesforceがチェックした Salesforce コンテンツの完全な統計情報が表示されます。
2. [**その他のレポート**] をクリックして、利用可能な組み込みレポートにアクセスします。
   このソリューションには、[**保護コンテンツアナリティクス**]、[**ファイル保護の詳細**]、および [**URL保護の詳細**] の3つの組み込みダッシュボードが含まれています。
   また、使用可能な属性を使用して、独自のダッシュボードやレポートを作成することもできます。
   ファイルレポートの属性⊠

- 作成者⊠フルネーム
- 作成日
- 日時
- ファイル拡張子
- ファイル名
- ファイルスキャンID
- ファイルサイズ
- ファイルタイプ
- IPアドレス
- 最終更新者⊠フルネーム
- 最終更新日
- 名前
- 所有者⊠フルネーム
- レコードID
- スキャンタイプ
- SHA1
- ロケーション
- ユーザ⊠フルネーム
- 評決
- 所有者⊠名、フルネーム、姓、所有者ID、電話、プロファイル⊠名前、ルール⊠名前、タイトル、ユーザ名、メールアドレス、エイリアス、アクティブ⊠
- 理由
- ファイルの普及度
- ファイルレピュテーション評価

URLレポートの属性⊠

- URLスキャン⊠ID
- URLスキャン⊠名前
- アクション
- カテゴリ
- 日時
- 方向
- IPアドレス
- ロケーション
- 理由
- 評判
- 評判の説明
- URL
- ユーザ
- 評決
- 所有者名
- 所有者エイリアス
- 所有者ロール
- 作成者
- 作成されたエイリアス
- 作成日
- 最終更新者
- 最終更新エイリアス
- 最終更新日

3.4 ソリューション設定を表示する

WithSecure Cloud Protection for Salesforce の試用版では、クイックインストールガイドに記載されている設定を変更することができます。

[管理] タブを開きます。
ファイルおよびURL保護コンポーネントで使用できる設定と、ソリューションの一般的な設定が表示されます。