Cloud Protection for Salesforce

Testing Guide

目次

1 はじめに 5
1.1 ソリューション概要 5
1.2 テストオプション 5
2 テストドライブでのソリューションのテスト 7
2.1 テストドライブ組織の使い始め 7
2.2 ファイル保護の動作を確認する 7
2.3 URL保護のテスト 7
2.4 アナリティクスの表示 8
2.5 サマリーダッシュボードとレポートの表示 8
2.6 ソリューション設定の表示 8
3 自社のSalesforce組織でのソリューションのテスト 9
3.1 ファイル保護のテスト 9
3.2 URL保護のテスト 9
3.3 サマリーダッシュボードとレポートの表示 10
3.4 ソリューション設定の表示 11

第 1 章 はじめに

本ガイドでは、Cloud Protection for Salesforceをテストする方法について説明し、今後のテストを計画する際に活用できるヒントや手法を提供します。

1.1 ソリューション概要

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。

Cloud Protection for Salesforce は、Salesforce クラウドに進入または進入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、貴社、パートナー、またはお客様に対するサイバー攻撃に使用されないように保護します。

本ソリューションには、Salesforce アプリケーションと WithSecure Security Cloud が含まれます。WithSecure Security Cloud は、ファイルおよびウェブサイトの評判（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。Cloud Protection for Salesforce アプリケーションは、貴社が使用している Salesforce Sales Cloud、Service Cloud、または Experience Cloud（旧称 Community Cloud）にインストールします。その他のソフトウェアをインストールしたり、ネットワーク設定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、デジタル脅威の大型データベースを構築します。このデータベースにより、グローバルなサイバー脅威のリアルタイムなビューが提供されます。

Cloud Protection for Salesforce は、このデータを活用して、グローバルまたはローカルな脅威環境の変化に迅速に対応します。例えば、ヒューリスティック分析や行動分析によって新しいゼロデイ攻撃が検知された場合、その情報はすべての不特定多数のお客様と共有されます。これにより、高度な攻撃が最初に検知されてから短時間で無効化することができます。

本ソリューションは、遅延を低減し、Salesforce の利用に影響を与えないよう設計されています。ファイルやコンテンツを分析する際、ソリューションは WithSecure Security Cloud を活用したマルチステージ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。例えば、高リスクのファイルのみが、ゼロデイマルウェアやその他の高度な脅威による攻撃を防ぐように設計された Cloud Sandboxing テクノロジーによる詳細な分析を受けます。

1.2 テストオプション

Cloud Protection by WithSecure は、Cloud Protection for Salesforce をテストするための3つの方法を提供しています。

1. ライブデモを予約する

   japan-sales@cloudprotection.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およびライブデモセッションを予約します。
2. 事前設定された Salesforce 組織で テストドライブを行う

   Salesforce AgentExchange Test Drive は、WithSecure Cloud Protection for Salesforce を簡単にテストできる方法です。 ソリューションはテスト組織にすで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

ロードやアップロード、悪意のあるURLや不許可のURLのアップロードやクリックを試したり、WithSecure アナリティクス、レポート、設定を詳細に確認したりできます。

3. ご自身の Salesforce 組織に 15日間の無料トライアルをインストールする。

   より詳細なテストを行うために、ご自身の Salesforce 組織に WithSecure Cloud Protection を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、インストール後は自動的に15日間のトライアルモードで動作します。ソリューションをインストールする際は、『Quick Installation Guide』に従ってください。

第 2 章 テストドライブでのソリューションのテスト

Cloud Protection for Salesforce のテストをより簡単かつ便利にするために、アンチマルウェアテストファイル（EICAR）とテスト用の URL が含まれる事前設定済みの Salesforce テストドライブ 組織が用意されています。

> 注：ICAR はアンチマルウェアテストファイルであり、コンピューターに危害を加えるものではありません。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の使い始め

テストドライブで Cloud Protection for Salesforce のテストを開始するには、次の手順に従います。

1. Cloud Protection アプリのリスティングで [Take a Test Drive] をクリックします。
2. Salesforce アカウントを使用して AgentExchange にログインします。
   これで Salesforce テストドライブ 組織にアクセスできるようになり、Cloud Protection for Salesforce の保護ダッシュボードが表示されます。

2.2 ファイル保護のテスト

ファイル保護がどのように機能するか例を確認するには、次の手順に従います。

1. [App Launcher]（アプリ起動ツール）に移動し、[Sales] を開きます。
2. [Accounts]（取引先）をクリックし、[Demo Account] を選択します。
   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 [HARMFUL CONTENT REMOVED] Example_MaliciousFile に置き換えたことが確認できます。
3. Example_MaliciousFile.docx のダウンロードを試みます。
   Cloud Protection for Salesforce がダウンロードをブロックします。

2.3 URL保護のテスト

URL保護がどのように機能するか例を確認するには、次の手順に従います。

1. [App Launcher]（アプリ起動ツール）に移動し、[Chatter] を開きます。
   Cloud Protection for Salesforce は、分析目的で元の URL を書き換えています。
2. テスト URL をクリックしてみます。
   Cloud Protection for Salesforce は、有害なウェブサイトおよび許可されていないウェブサイトへのアクセスをブロックします。

2.4 アナリティクスの表示

Cloud Protection for Salesforce には、チェックされたファイルや URL のすべてのイベントを確認できるアナリティクスセクションが含まれています。

1. [App Launcher] (アプリ起動ツール) に移動し、[Cloud Protection] を開きます。
2. [Analytics] (アナリティクス) > [File Events] (ファイルイベント) タブに移動します。
   すべてのファイルアナリティクス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 [History] (履歴) 列にある [View] (表示) をクリックします。
   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を示す [File Event History] (ファイルイベント履歴) ビューが開きます。
4. [Analytics] (アナリティクス) > [URL Events] (URLイベント) タブに移動します。
   すべての URL アナリティクス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 [History] (履歴) 列にある [View] (表示) をクリックします。
   選択した URL の投稿およびオープンアクションの詳細を示す [URL Event History] (URLイベント履歴) ビューが開きます。

2.5 サマリーダッシュボードとレポートの表示

[Summary] (サマリー) タブには、Salesforce コンテンツの概要が表示されます。

[Summary] (サマリー) タブをクリックします。
このダッシュボードにはCloud Protection for Salesforce がチェックした Salesforce コンテンツの完全な統計が表示されます。

> 注 : [More reports] (その他のレポート) オプションは、ソリューションのトライアル版および製品版で利用できます。

2.6ソリューション設定の表示

テストドライブでは、では、WithSecure Cloud Protection for Salesforce の設定を変更することはできませんが、利用可能な設定を確認することができます

[Administration] (管理) タブをクリックします。
ここには、ファイルおよび URL 保護コンポーネントで利用可能な設定と、ソリューションの全般的な設定が表示されます。

第3章 自社のSalesforce組織でのソリューションのテスト

Cloud Protection by WithSecure は、すべての Salesforce のお客様に 15日間の無料トライアルテスト期間を提供しています。

Salesforce AgentExchange から直接、サンドボックス、開発者、または本番組織に Cloud Protection for Salesforce を数分でインストールできます。

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手順に従ってください。

3.1 ファイル保護のテスト

Eicar テストファイルを使用してファイル保護をテストするには、次の手順に従います。

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

   注：有害ではありませんが、Eicar.com はテスト目的でマルウェアとして識別されます。アンチマルウェア保護によってファイルがブロックされる場合は、リアルタイムスキャンからフォルダを除外し、そこに Eicar.com ファイルを配置してください。
2. Example_MaliciousFile.docx とクリーンなファイルを Salesforce の [Files]（ファイル）または [Chatter] にアップロードします。
3. [App Launcher]（アプリ起動ツール）に移動し、[Cloud Protection] を開きます。
4. [Analytics]（アナリティクス）> [File Events]（ファイルイベント）タブに移動します。
   ここには、1つのクリーンなファイルと1つのブロックされたファイルが表示されます。
5. 両方のファイルをダウンロードしてみます。
   クリーンなファイルはダウンロードできますが、悪意のあるファイルはブロックされます。
6. 再び [Analytics]（アナリティクス）> [File Events]（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. [View]（表示）をクリックして、完全なイベント履歴を確認します。
   選択したファイルのすべてのアップロードおよびダウンロードアクションが表示されます。

3.2 URL保護のテスト

テストドメインを使用して URL 保護をテストするには、次の手順に従います。

1. [App Launcher]（アプリ起動ツール）に移動し、[Cloud Protection] を開きます。
2. [Administration]（管理）> [URL Protection]（URL保護）タブに移動します。
3. このテストでは、[Select disallowed categories]（許可しないカテゴリの選択）リストで [Gambling] が選択されていることを確認します。
4. 2つのサンプル URL unsafe.fstestdomain.com と gambling.fstestdomain.info を Salesforce [Chatter] に投稿します。
5. [Chatter] を開くと、URL が書き換えられた2つの新しい投稿が表示されます。
6. Cloud Protection に戻り、[Analytics]（アナリティクス）> [URL Events]（URLイベント）タブに移動します。
   2つの新しい Chatter 投稿が表示されます。

7. [Chatter] に戻り、両方のリンクを開いてみます。[Harmful website blocked] (有害なウェブサイトがブロックされました) および [Disallowed website blocked] (許可されていないウェブサイトがブロックされました) のブロックページが表示されます。
8. 再び Cloud Protection に戻り、[Analytics] (アナリティクス) > [URL Events] (URLイベント) タブに移動します。
   2つの URL オープンイベントが表示されます。
9. [View] (表示) をクリックして、完全なイベント履歴を確認します。
   選択した URL のすべての投稿およびオープンアクションが表示されます。。

3.3 サマリーダッシュボードとレポートの表示

[Summary] (サマリー) 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. [Summary] (サマリー) 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が表示されます。
2. [利用可能な組み込みレポートにアクセスするには、[More reports] (その他のレポート) をクリックします。
   本ソリューションには、Protected Content Analytics、File Protection Details、URL Protection Details の3つの組み込みダッシュボードが含まれています。
   利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の表示

Cloud Protection for Salesforce のトライアル版では、Quick Installation Guide に記載されている設定を変更できます。

[Administration] (管理) タブをクリックします。
ここには、ファイルおよび URL 保護コンポーネントで利用可能な設定と、ソリューションの全般的な設定が表示されます。