Dell Threat Defense

インストールおよび管理者ガイド

Powered by Cylance

v17.11.06

2017-11-06

目次

概要

Threat Defense, powered by Cylance は、マルウェアがデバイスに影響を与え得る前にこれを検出し、ブロックします。Cylance は、マルウェアの識別に数学的アプローチを使用しており、反応型シグニチャ、信頼ベースのシステム、またはサンドボックスではなく、機械学習法を使用します。このアプローチにより、新しいマルウェア、ウイルス、ボット、および今後発生する変種を無効化します。Threat Defense は、オペレーティングシステムでのマルウェアの潜在的なファイルの実行を分析します。

本マニュアルは、Threat Defense コンソールの使い方、Threat Defense エージェントのインストール、およびこれらの設定方法について説明します。

機能

Threat Defense は、各ホストにインストールされ、クラウドベースのコンソールと通信する小規模エージェントで構成されます。これらのエージェントは、テスト済み数学モデルを使用してホスト上のマルウェアを検出して阻止します。継続的なクラウド接続または継続的なシグニチャのアップデートは必要としません。また、オープンネットワークおよび隔離ネットワークの両方で機能します。脅威の状況が発達するに従って、Threat Defense も進化します。莫大な、現実世界のデータセットで継続的なトレーニングを積むことによって、Threat Defense は、常に攻撃者の一歩先を行きます。

- **脅威**：脅威がデバイスにダウンロードされるか、または悪用が試みられている場合。
- **脅威の検出**：Threat Defense エージェントが脅威を識別する方法。
    - **プロセスのスキャン**：デバイスで実行されているプロセスをスキャンします。
    - **実行制御**：実行時のプロセスのみを分析します。これは、起動時に実行するファイル、自動実行するように設定されているファイル、ユーザーが手動で実行するファイルをすべて含みます。
- **分析**：悪意のあるファイルか安全なファイルかを識別する方法。
    - **脅威スコアのクラウドルックアップ**：クラウドの数学モデルはファイルのスコア決定に使用されます。
    - **ローカル**：エージェントに付属の数学モデル。デバイスがインターネットに接続していないときは、これを使用して分析できます。
- **アクション**：ファイルが脅威として識別された場合にエージェントが行うこと。
    - **グローバル**：グローバル隔離および安全リストを含んだ、ポリシー設定を確認します。
    - **ローカル**：隔離または除外のファイルを手動で確認します。

本ガイドについて

クラウドベースのコンソールについてよく理解してから、エンドポイントにエージェントをインストールすることが推奨されます。エンドポイントの管理方法について理解すると、これらの保護および維持が容易になります。このワークフローが推奨されますが、ユーザーは、理にかなった方法で使用環境への導入に取り組むことができます。

例：ゾーンは、組織内のグループのデバイスを助けます。たとえば、選択した基準（オペレーティングシステム、デバイス名、またはドメイン名など）に基づいて、新しいデバイスをゾーンに自動的に追加するゾーン規則を使用してゾーンを設定します。

メモ：エージェントのインストールに関する手順はポリシーおよびゾーンについて学習した後になります。ユーザーは、必要に応じてエージェントのインストールを開始できます。

コンソール

Threat Defense コンソールは、ログインして、組織の脅威に関する情報を表示するウェブサイトです。このコンソールを使用すると、デバイスをグループ（ゾーン）に分けて整理すること、デバイスで脅威を発見したときに実行するべきアクション（ポリシー）を設定すること、インストールファイル（エージェント）をダウンロードすることが容易になります。

Threat Defense コンソールは、次の言語をサポートしています。

フランス語	ドイツ語	イタリア語	日本語
ポルトガル語（ポルトガル）	韓国語	スペイン語	ポルトガル語（ブラジル）

表 *1*：サポートされている *Threat Defense* コンソールの言語

ログイン

アカウントをアクティブ化すると、Threat Defense コンソールのログイン情報が記載された電子メールを受信します。電子メール内のリンクをクリックしてログインページに移動するか、次のリンクをクリックしてください。

- 北アメリカ：http://dellthreatdefense.com
- ヨーロッパ：http://dellthreatdefense-eu.cylance.com

デバイスポリシー

エージェントが遭遇したマルウェアの処理方法を定めるポリシーです。たとえば、マルウェアを自動的に隔離するか、または特定のフォルダにある場合はそれを無視します。各デバイスは、ポリシーの範囲内である必要があり、デバイスに適用できるポリシーは 1 つのみです。デバイスを単一ポリシーに限定することにより、矛盾する機能（当該デバイスでは許可されるべきときに、ファイルをブロックするなど）を除外します。ポリシーが割り当てられていない場合、デフォルトポリシーが適用されます。

デフォルトポリシーでは、実行時のみプロセスを分析する、実行制御のみが有効になります。これによって、デバイスに基本的な保護が適用され、デバイスでの動作を中断しません。また、実稼働環境にポリシーを導入する前に、ポリシー機能をテストする時間を提供します。

ポリシーの追加方法

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。ポリシーを作成できるのは、管理者のみです。
2. **設定** > **デバイスポリシー** の順に選択します。
3. **新しいポリシーを追加** をクリックします。
4. ポリシー名を入力し、ポリシーのオプションを選択します。
5. **作成** をクリックします。

ファイルアクション

設定 > デバイスポリシー > *[ポリシーの選択]* > ファイルアクション

ファイルアクションは、Threat Defense で危険または異常と検出されるファイルを処理するさまざまなオプションを提供します。

ヒント：危険または異常なファイルの分類に関する詳細については、保護 - 脅威セクションを参照してください。

実行制御による自動隔離

この機能は危険または異常なファイルを隔離し、実行されないようにします。ファイルを隔離すると、ファイルが元の場所から隔離ディレクトリ、`C:\ProgramData\Cylance\Desktop\q` に移動します。

一部のマルウェアは、特定のディレクトリに他のファイルをドロップするように設計されています。このマルウェアは、ファイルのドロップに成功するまでドロップし続けます。Threat Defense は、ドロップされたファイルが実行されないように変更して、このタイプのマルウェアが削除されたファイルをドロップし続けないようにします。

ヒント：デルでは、本番環境で適用する前に少数のデバイスで自動隔離をテストすることを強くお勧めします。このテスト結果を確認して、ビジネスに不可欠なアプリケーションが実行時にブロックされないようにします。

自動アップロード

デルでは、ユーザーが 危険および異常なファイル両方の 自動アップロード を有効にすることを推奨します。Threat Defense は検出されたすべての危険または異常なファイルを Cylance Infinity Cloud に自動的にアップロードし、ファイルのより詳細な分析を実行し、追加の詳細情報を提供します。

Threat Defense は、未知の Portable Executable（PE）ファイルのみをアップロードし、分析します。組織内の複数のデバイスで同じ未知のファイルが発見された場合、Threat Defense は、デバイスごとに 1 ファイルではなく、1 ファイルだけを分析するためにアップロードします。

ポリシー安全リスト

ポリシーレベルで安全と見なされるファイルを追加します。エージェントは、このリストに含まれるファイルに対しては脅威アクションを適用しません。

さまざまなレベル（ローカル、ポリシーまたはグローバル）におけるファイルの除外（隔離または安全）の処理の詳細については、付録 B：を参照してください。除外処理を参照してください。

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。ポリシーを作成できるのは、管理者のみです。
2. **設定** > **デバイスポリシー** の順に選択します。
3. 新しいポリシーを追加するか、既存のポリシーを編集します。
4. ポリシー安全リスト で **ファイルの追加** をクリックします。
5. **SHA256** 情報を入力します。任意で、MD5 およびファイル名（既知の場合）を含めます。
6. **カテゴリ** を選択し、このファイルの内容を確認しやすくします。
7. このファイルを ポリシー安全リスト に追加する理由を入力します。
8. **送信** をクリックします。

保護設定

設定 > デバイスポリシー > *[ポリシーの選択]* > 保護設定

実行制御

Threat Defense は、悪意のあるプロセスが実行されないかどうかを常に監視し、何らかの危険または異常な試みが実行された場合は警告します。

デバイスからのサービスシャットダウンを阻止する

選択すると、Threat Defense サービスは、手動で、または別のプロセスのいずれかによってシャットダウンされないように保護されます。

マルウェアサンプルのコピー

マルウェアサンプルをコピーするネットワーク共有を指定できます。これにより、ユーザーは、Threat Defense が危険または異常と判断したファイルを自分で分析することができます。

- CIFS/SMB ネットワーク共有をサポートします。
- ネットワーク共有の場所を 1 つ指定します。例：`c:\test`。
- 基準を満たす全ファイル（重複を含む）がネットワーク共有にコピーされます。一意性テストは実行されません。
- ファイルは圧縮されません。
- ファイルはパスワードで保護されていません。

警告：ファイルはパスワードで保護されていません。悪意のあるファイルをうっかり実行しないように注意する必要があります。

スクリプト制御

スクリプト制御は、悪意のあるアクティブスクリプトおよび PowerShell スクリプトが実行されないようにブロックすることによってデバイスを保護します。

1. コンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **デバイスポリシー** の順に選択します。
3. ポリシーを選択し、**保護設定** をクリックします。
4. チェックボックスをオンにして、**スクリプト制御** を有効にします。
    a. **警告**：環境内で実行されるスクリプトを監視します。初期導入時にお勧めします。
    b. **ブロック**：特定フォルダからのスクリプトのみの実行を許可します。アラートモードでのテスト後に使用します。
    c. **これらのフォルダ（およびサブフォルダ）内のスクリプトを承認します**：スクリプト制御フォルダの除外は、フォルダの相対パスを指定する必要があります。
    d. **PowerShell コンソールの使用をブロック**：PowerShell コンソールの起動をブロックします。PowerShell ワンライナーの使用に対して保護することによって追加のセキュリティを提供します。

    メモ：スクリプトが、PowerShell コンソールを起動し、スクリプト制御が PowerShell コンソールをブロックするように設定されている場合は、スクリプトは失敗します。PowerShell スクリプトを起動し、PowerShell コンソールは起動しないようにユーザーがスクリプトを変更することをお勧めします。
5. **保存** をクリックします。

エージェントログ

設定 > デバイスポリシー > [ポリシーの選択] > エージェントログ

コンソールでエージェントログを有効にして、ログファイルをアップロードし、コンソールで表示できるようにします。

1. コンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **デバイスポリシー** の順に選択します。
3. ポリシーを選択し、**エージェントログ** をクリックします。ログファイルに選択されているデバイスが、確実にこのポリシーに割り当てられているようにします。
4. **ログファイルの自動アップロードを有効にする** を選択し、**保存** をクリックします。
5. **デバイス** タブをクリックし、デバイスを選択します。
6. **エージェントログ** をクリックします。ログファイルが表示されます。
7. ログファイルをクリックします。ログファイル名は、ログの日付です。

ポリシーに関するベストプラクティス

ポリシーを最初に作成したときは、段階的方法でポリシー機能を実装して、パフォーマンスおよび操作に影響を及ぼさないことを確認することが推奨されます。環境内で Threat Defense が機能する方法を理解するにつれて、より多くの機能を有効にした、新しいポリシーを作成します。

1. 初期のポリシーを作成する場合は、**自動アップロード** のみを有効にします。
    a. エージェントは、実行制御およびプロセスモニタを使用して、実行中のプロセスのみを分析します。

    これは、起動時に実行するファイル、自動実行するように設定されているファイル、ユーザーが手動で実行するファイルをすべて含みます。

    エージェントは、コンソールに対してアラートを送信するのみです。ブロックまたは隔離されるファイルはありません。

    b. 脅威アラートがないかどうかコンソールを確認します。

    目的は、脅威（異常または危険）と見なされるエンドポイントで実行される必要のあるすべてのアプリケーションまたはプロセスを見つけることです。

    このような場合（たとえば、ポリシーのフォルダを除外する、そのデバイスのファイルを 除外する、またファイルを安全リストに追加する）、ポリシーまたはコンソール設定をこれらを 許可する に設定します。

    c. この初期ポリシーを 1 日使用して、デバイスで通常使用されるアプリケーションおよびプロセスを実行し、分析できます。

重要：脅威と見なされるアプリケーションおよびプロセスが、デバイス上で定期的（たとえば、月 1 回）に実行される場合があります。この初期ポリシー中にこのようなアプリケーションおよびプロセスを実行するか、スケジュールどおり実行されるときにデバイスをモニタするように覚えておくかどうかは、ユーザーの考え方次第です。

2. 保護設定で、実行制御および監視プロセスの完了後に **実行中の危険なプロセスの強制終了** を有効にします。

   脅威（EXE または MSI）が検出された場合には、状態に関係なく、実行中の危険なプロセスおよびそのサブプロセスの強制終了によって、プロセス（およびサブプロセス）を強制終了させます。

3. ファイルアクションで、**自動隔離** をオンにします。

   自動隔離 は悪意のあるすべてのファイルを 隔離 フォルダに移動します。

4. 保護設定で、**スクリプト制御** をオンにします。

   スクリプト制御は、ユーザーがデバイスで悪意のあるスクリプトを実行しないように保護します。

   ユーザーは、指定フォルダに対してスクリプトの実行を承認できます。

   スクリプト制御フォルダの除外は、フォルダの相対パスを指定する必要があります（たとえば、**`\Cases\ScriptsAllowed`**）。

ゾーン

ゾーンは、デバイスを整理し、管理する方法です。たとえば、デバイスは、地理または機能に基づいて分類できます。必要不可欠なデバイスのグループが存在する場合、これらのデバイスをグループ化し、このゾーンに対して高い優先度を割り当てることができます。加えて、ポリシーはゾーンレベルで適用されるため、デバイスは、これらのデバイスに適用されるポリシーに基づいて 1 つのゾーンにグループ化することができます。

組織には、管理者のみがアクセスできるデフォルトゾーン（非ゾーン化）があります。デバイスをゾーンに自動的に割り当てる、ゾーン規則が存在しなければ、新しいデバイスは非ゾーン化に割り当てられます。

ゾーンマネージャおよびユーザーはゾーンに割り当てられることができ、ゾーンマネージャおよびユーザーはゾーンの設定方法を表示できます。これにより、ゾーンマネージャおよびユーザーは、担当するデバイスにアクセスできます。ゾーンマネージャおよびユーザーロールを持つユーザーがゾーンを表示できるようにするには、少なくとも 1 つのゾーンを作成する必要があります。

デバイスは複数のゾーンに属することができますが、デバイスに適用できるポリシーは 1 つのみです。複数のゾーンを許可すると、デバイスのグループ化方法に柔軟性が生じます。デバイスを単一ポリシーに限定することにより、矛盾する機能（たとえば、当該デバイスでは 許可 されるべきときにファイルをブロックする）を除外します。

次の理由により、デバイスが複数のゾーンに存在することがあります。

- デバイスが、手動で複数のゾーンに追加される。
- デバイスが、複数のゾーンの規則に適合する。
- デバイスは、あるゾーンに既に存在し、別のゾーンの規則に適合する。

推奨するゾーンの使用方法については、「ゾーン管理に関するベストプラクティス」を参照してください。

ゾーンの追加方法

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。ゾーンを作成できるのは、管理者のみです。
2. **ゾーン** をクリックします。
3. **新しいゾーンの追加** をクリックします。
4. ゾーン名を入力し、ポリシーを選択し、値を選択します。ゾーンには、ポリシーが関連付けられている必要があります。値は、ゾーンの優先度です。
5. **保存** をクリックします。

ゾーンへのデバイスの追加方法

1. 管理者またはゾーン管理アカウントを使用してコンソール（http://dellthreatdefense.com）にログインします。
2. **ゾーン** をクリックします。
3. ゾーンリスト で特定のゾーンをクリックします。そのゾーンの現在のデバイスが、ページの下部の ゾーンデバイスリスト に表示されます。
4. **ゾーンへのデバイスの追加** をクリックします。デバイスのリストが表示されます。
5. ゾーンに追加する各デバイスを選択し、**保存** をクリックします。オプションで **選択したデバイスにゾーンポリシーを適用する** を選択します。ゾーンにデバイスを追加しても、ゾーンポリシーは自動的に適用されません。これは、ゾーンが、これらのデバイスのポリシーを管理するためではなく、デバイスを整理するために使用されることがあるからです。

ゾーンの削除方法

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。ゾーンを削除できるのは、管理者のみです。
2. **ゾーン** をクリックします。
3. 削除するゾーンのチェックボックスをオンにします。

4. **削除** をクリックします。
5. 選択したゾーンの削除の確認を求めるメッセージが表示されたら、**はい** をクリックします。

ゾーンのプロパティ

ゾーンのプロパティは、必要に応じて編集できます。

ゾーンの優先度について

ゾーンには、そのゾーン内のデバイスの重要性または重大性を分類する、異なる優先レベル（低、標準、または高）を割り当てることができます。ダッシュボードのいくつかの領域では、デバイスは優先度ごとに表示されて、即時の対応を必要とするデバイスを識別しやすくします。

優先度は、ゾーンを作成するとき、またはゾーンを編集して優先度の値を変更するときに設定できます。

ゾーンのプロパティの編集方法

1. 管理者またはゾーン管理者としてコンソール（http://dellthreatdefense.com）にログインします。
2. **ゾーン** をクリックします。
3. ゾーンリスト で特定のゾーンをクリックします。
4. **名前** フィールドに新しい名前を入力して、ゾーン名を変更します。
5. **ポリシー** ドロップダウンメニューで別のポリシーを選択してポリシーを変更します。
6. **低**、**標準** または **高** の値を選択します。
7. **保存** をクリックします。

ゾーン規則

デバイスは、特定の基準に基づいてゾーンに自動的に割り当てることができます。この自動化は、ゾーンに多数のデバイスを追加するときに便利です。ゾーン規則に一致する新しいデバイスが追加されると、これらのデバイスは、自動的に該当するゾーンに割り当てられます。**すべての既存のデバイスに今すぐ適用** が選択されている場合は、規則に一致するすべての既存のデバイスがそのゾーンに追加されます。

メモ：ゾーン規則はデバイスをゾーンへ自動的に追加しますが、デバイスを削除することはできません。デバイスの IP アドレスまたはホスト名を変更しても、このデバイスはゾーンから削除されません。デバイスは、手動でゾーンから削除する必要があります。

ゾーン規則に一致した結果としてゾーンに追加されたデバイスにゾーンポリシーを適用するオプションがあります。つまり、デバイスの既存のポリシーの代わりに、指定したゾーンポリシーが適用されます。ゾーン規則に基づいたポリシーの自動適用は、注意して使用する必要があります。適切に管理されていない場合、ゾーン規則にデバイスが一致したために、デバイスが誤ったポリシーに割り当てられることがあります。

デバイスに適用されるポリシーを表示するには、コンソールで、デバイスの詳細 ページを表示します。

ゾーン規則の追加方法

1. 管理者またはゾーン管理者としてコンソール（http://dellthreatdefense.com）にログインします。
2. **ゾーン** をクリックして、ゾーンのリスト からゾーンを選択します。
3. ゾーン規則で **ルールの作成** をクリックします。
4. 選択したゾーンの基準を指定します。条件を更に追加するには、+ サインをクリックします。条件を削除するには、- サインをクリックします。
5. **保存** をクリックします。

ゾーン規則の基準

- **新しいデバイスが組織に追加されたとき**：ゾーン規則に合致する組織に追加されるすべての新しいデバイスは、ゾーンに追加されます。
- **デバイスの任意の属性が変更されたとき**：既存のデバイスの属性が変更され、ゾーン規則に合致する場合はその既存のデバイスはゾーンに追加されます。
- **範囲内の IPv4 アドレス**：IPv4 アドレスの範囲を入力します。
- **デバイス名**：
    - 開始：デバイス名はこの文字列で開始する必要があります。
    - 含む：デバイス名はこの文字列を含む必要がありますが、名前内の位置はどこでも構いません。
    - 終了：デバイス名はこの文字列で終了する必要があります。
- **オペレーティングシステム**：
    - である：オペレーティングシステムは、選択したシステムでなくてはいけません。
    - ではない：オペレーティングシステムは、選択したシステムではいけません。たとえば、唯一のゾーン規則がオペレーティングシステムは Windows 8 ではいけないと定める場合、非 Windows デバイスなど全オペレーティングシステムがこのゾーンに追加されます。

- **ドメイン名**：
    - 開始：ドメイン名はこの文字列で開始する必要があります。
    - 含む：ドメイン名はこの文字列を含む必要がありますが、名前内のどの位置でも構いません。
    - 終了：ドメイン名はこの文字列で終了する必要があります。
- **識別名**：
    - 開始：識別名はこの文字列で開始する必要があります。
    - 含む：識別名はこの文字列を含む必要がありますが、名前内のどの位置でも構いません。
    - 終了：識別名はこの文字列で終了する必要があります。
- **（LDAP）のメンバー**：
    - である：（グループ）のメンバーは、これに一致する必要があります。
    - 含む：（グループ）のメンバーは、これを含む必要があります。
- **次の条件が満たされている**：
    - すべて：デバイスを追加するには、ゾーン規則の全条件が一致する必要があります。
    - いずれか：デバイスを追加するには、ゾーン規則の少なくとも 1 つの条件が一致する必要があります。
- **ゾーンポリシーの適用**：
    - 適用しない：ゾーンにデバイスが追加されたときに、ゾーンポリシーを適用しません。
    - 適用：ゾーンにデバイスが追加されたときに、ゾーンポリシーを適用します。

      警告：ゾーンポリシーを自動的に適用すると、ネットワーク上のデバイスの一部に悪影響を及ぼす場合があります。ゾーン規則がこの特定のゾーンポリシーを必要とするデバイスを見つけた場合にのみゾーンポリシーを自動的に適用します。
- **すべての既存のデバイスに今すぐ適用**：ゾーン規則は組織内のすべてのデバイスに適用されます。ゾーンポリシーは適用されません。

識別名（*DN*）について

ゾーン規則で識別名（DN）を使用する場合には、DN に関するある程度の知識が必要です。

- ワイルドカードは使用できませんが、「含む」条件により同様の結果を得ることができます。
- エージェントに関する DN エラーおよび例外は、ログファイルに保存されます。
- エージェントがデバイスで DN 情報を検出した場合、この情報は、自動的にコンソールに送信されます。

- DN 情報を追加するときには、次のように適切な形式でなくてはいけません。
    - 例：CN=JDoe,OU=Sales,DC=dell,DC=COM
    - 例：OU=Demo,OU=SEngineering,OU=Sales

ゾーンデバイスリスト

ゾーンデバイスリスト には、このゾーンに割り当てられたすべてのデバイスが表示されます。デバイスは、複数のゾーンに属することがあります。**エクスポート** を使用して、ゾーンデバイスリスト のすべてのデバイス情報を含む CSV ファイルをダウンロードします。

メモ：ゾーンを表示する権限が存在しない場合に、ゾーンカラムのゾーンへのリンクをクリックすると、リソースが見つかりません ページが表示されます。

ゾーン管理に関するベストプラクティス

ゾーンはタグのように考えるのが最適であり、いずれのデバイスも複数のゾーンに属する（または複数のタグを持つ）ことができます。作成可能なゾーンの数に制約はありませんが、ベストプラクティスは、組織内のテスト、ポリシー、およびユーザーロールレベルという 3 種類の異なるゾーンメンバーシップであることが確認されています。

これらの 3 種類のゾーンは、以下で構成されます。

- アップデート管理
- ポリシー管理
- ロールベースのアクセス管理

アップデート管理向けのゾーン組織

ゾーンの一般的な使用法の 1 つは、エージェントアップデートの管理を支援することです。Threat Defense は、最新のエージェントバージョンおよび以前のバージョンをサポートしています。このため、企業は、フリーズしたウィンドウの変更をサポートし、新しいエージェントバージョンの徹底的なテストを行うことができます。

エージェントテストおよび本番稼働フェーズの管理および指定に使用される、推奨ゾーンタイプは、3 種類あります。

- **ゾーンのアップデート - テストグループ**：これらのゾーンには、組織内のデバイス（およびそれらのデバイスで使用されているソフトウェア）を適切に表示するテストデバイスが必要です。これにより、最新のエージェントをテストすることができ、このエージェントを本番稼働デバイスに導入しても、ビジネスプロセスを妨げないようにします。

- **ゾーンのアップデート - パイロットグループ**：このゾーンは、セカンダリテストゾーンまたはセカンダリ本番ゾーンとして使用できます。第 2 のテストゾーンとしては、本番稼働環境に投入する前に、より規模の大きいグループで新しいエージェントをテストできます。第 2 の本番稼働ゾーンとしては、2 つの異なるエージェントバージョンを実行できます。ただし、2 つの異なる本番稼働ゾーンを管理する必要があります。
- **ゾーンのアップデート - 本番**：ほとんどのデバイスは、本番に割り当てられるゾーンにある必要があります。

メモ：エージェントを本番ゾーンにアップデートするには、「エージェントのアップデート」を参照してください。

テストゾーンまたはパイロットゾーンの追加

1. 管理者またはゾーン管理アカウントを使用してコンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **エージェントのアップデート** の順に選択します。
3. テストゾーンまたはパイロットゾーンの場合：
    a. **テストゾーンの選択** または **パイロットのゾーンの選択** をクリックします。
    b. ゾーンをクリックします。

    本番ゾーンが **自動アップデート** に設定されている場合は、テストおよびパイロットゾーンは使用できません。本番稼働ゾーンで自動アップデートを他のオプションに変更すると、テストゾーンおよびパイロットゾーンを有効にすることができます。
4. **バージョンを選択してください** をクリックします。
5. テストゾーンまたはパイロットゾーンに適用するエージェントバージョンを選択します。
6. **適用** をクリックします。

ポリシー管理向けのゾーン組織

別のゾーンセットを作成すると、別のポリシーを別のタイプのエンドポイントに適用するのに役立ちます。次の例を検討してください。

- ポリシーゾーン – ワークステーション
- ポリシーゾーン – ワークステーション – 除外
- ポリシーゾーン – サーバー
- ポリシーゾーン – サーバー – 除外
- ポリシーゾーン – 幹部 – 高保護

これらの各ゾーンでこのポリシーゾーンに含まれる全デバイスにデフォルトでポリシーを適用することが推奨されます。1 つのデバイスを複数のポリシーゾーンに配置すると、適用するポリシーに関する競合が生じ得るため、複数のポリシーゾーンには配置しないでください。また、ゾーン規則エンジンでは、IP、ホスト名、オペレーティングシステム、およびドメインに応じてこれらのホストを自動的に整理できます。

ロールベースのアクセス管理向けのゾーン組織

ロールベースのアクセスを使用して管理を担当するデバイスのサブセットに、コンソールユーザーのアクセスを制限します。これは、IP 範囲、ホスト名、オペレーティングシステム、またはドメインによる分離を含むことがあります。地理的ロケーション、タイプ、またはその両方によるグループ化を検討してください。

例：

- RBAC ゾーン – デスクトップ – ヨーロッパ
- RBAC ゾーン – サーバー – アジア
- RBAC ゾーン – レッドカーペット（幹部）

上記のゾーンの例を使用して、ゾーン管理者は *RBAC* ゾーン - デスクトップ - ヨーロッパに割り当てられ、そのゾーン内のデバイスにのみアクセスできます。ゾーンマネージャユーザーが他のゾーンを表示しようとすると、これを表示する権限がないことを示すエラーメッセージが表示されます。デバイスが複数のゾーンに含まれている場合、ゾーンマネージャはこのデバイスを表示できますが、ゾーンマネージャがこのデバイスが関連付けられている他のゾーンを表示しようとすると許可されず、エラーメッセージが表示されます。

ダッシュボードなどのコンソールの他のパーツでは、*RBAC* ゾーン - デスクトップ - ヨーロッパのゾーン管理者もゾーンまたはそのゾーンに割り当てられたデバイスに関連する脅威およびその他の情報に制限されます。

同様の制限が、ゾーンに割り当てられたユーザーにも適用されます。

ユーザー管理

管理者にはグローバル許可があり、ユーザーの追加または削除、ゾーンへのユーザーの割り当て（ユーザーまたはゾーンマネージャのいずれかとして）、デバイスの追加または削除、ポリシーの作成、およびゾーンの作成を実行できます。管理者はまた、ユーザー、デバイス、ポリシー、およびゾーンをコンソールから永久に削除することができます。

ユーザーおよびゾーンマネージャは、割り当てられているゾーンに関するアクセスおよび権限のみを持っています。これは、ゾーンに割り当てられたデバイス、これらのデバイスで検出された脅威、およびダッシュボードの情報に適用されます。

各ユーザーに許可されたユーザー権限の全一覧については、付録 C: ユーザーのアクセス権を参照してください。

ユーザーの追加方法

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。ユーザーを作成できるのは、管理者のみです。
2. **設定** > **ユーザー管理** の順に選択します。
3. ユーザーの電子メールアドレスを入力します。

4. ロールドロップダウンメニューでロールを選択します。
5. ゾーン管理者またはユーザーを追加する際は、それらを割り当てるゾーンを選択します。
6. **追加** をクリックします。パスワードを作成するためのリンクが含まれた電子メールがユーザーに送信されます。

ユーザーロールの変更方法

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。ユーザーを作成できるのは、管理者のみです。
2. **設定** > **ユーザー管理** の順に選択します。
3. ユーザーをクリックします。ユーザーの詳細 ページが表示されます。
4. ロールを選択して、**保存** をクリックします。

ユーザーの削除方法

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。ユーザーを作成できるのは、管理者のみです。
2. **設定** > **ユーザー管理** の順に選択します。
3. 削除する 1 人または複数のユーザーのチェックボックスをオンにします。
4. **削除** をクリックします。
5. 削除の確認を求めるメッセージが表示されたら、**はい** をクリックします。

ネットワーク関連

ネットワークは、Threat Defense エージェントがインターネット上でコンソールと通信できるように設定します。本項は、ファイアウォール設定およびプロキシ設定について説明します。

ファイアウォール

デバイスの管理にオンプレミスソフトウェアは不要です。Threat Defense エージェントは、コンソール（クラウドベースのユーザーインタフェース）によって管理され、そこに報告します。ポート 443（HTTPS）は通信用に使用され、エージェントがコンソールと通信するために、ファイアウォールで開く必要があります。このコンソールは、Amazon Web サービス（AWS）によってホストされ、固定 IP アドレスがありません。エージェントが次のサイトと通信できることを確認します。

- login.cylance.com
- data.cylance.com
- my.cylance.com
- update.cylance.com

- api2.cylance.com
- download.cylance.com

あるいは、*.cylance.com への HTTPS トラフィックを許可します。

プロキシ

Threat Defense 向けのプロキシサポートは、レジストリエントリを通じて設定されます。プロキシが設定されると、エージェントは、コンソールサーバーに対するすべてのアウトバウンド通信についてレジストリエントリの IP アドレスおよびポートを使用します。

1. レジストリにアクセスします。

   メモ：エージェントがインストールされた方法に応じて昇格した権限またはレジストリの所有権を取得が必要な場合があります（保護モードが有効化されているかいないか）。

2. レジストリエディタで、**HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop** に移動します。
3. 新しい文字列値（REG_SZ）を次のように作成します。
   - 値の名前 = ProxyServer
   - 値のデータ = プロキシ設定（たとえば、http://123.45.67.89:8080）

エージェントは、現在ログイン中のユーザーの資格情報を使用して、認証された環境内でインターネットと通信しようとします。認証されたプロキシサーバーが設定されており、ユーザーがデバイスにログインしていない場合、エージェントはプロキシを認証できず、コンソールと通信できません。この場合は、次のいずれかを行います。

- プロキシを設定し、*.cylance.com への全トラフィックを許可する規則を追加します。
- 別のプロキシポリシーを使用し、Cylance ホスト（*.cylance.com）への許可されていないプロキシアクセスを可能にします。

これを行うことにより、どのユーザーも当該デバイスにログインしていない場合、エージェントは認証を必要とせずに、クラウドに接続し、コンソールと通信できます。

デバイス

エージェントがエンドポイントにインストールされると、コンソールでデバイスとして使用できるようになります。ポリシー（確認された脅威を処理するために）、グループデバイス（ゾーンを使用して）を割り当てることによってデバイスの管理を開始し、各デバイス（隔離および除外）に手動でアクションします。

デバイス管理

デバイスとは、Threat Defense エージェントがインストールされたコンピュータです。デバイスは、コンソールから管理します。

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。デバイスを管理できるのは、管理者のみです。
2. **デバイス** をクリックします。
3. 次のアクションを実行できるようにするには、デバイスのチェックボックスをオンにします。
    - **エクスポート**：CSV ファイルを作成しダウンロードします。このファイルには、組織内の全デバイスのデバイス情報（名前、状態、およびポリシー）が含まれています。
    - **削除**：デバイスリスト から選択したデバイスを削除します。この操作では、エージェントはデバイスからアンインストールされません。
    - **ポリシーの割り当て**：選択したデバイスをポリシーに割り当てることができます。
    - **ゾーンへの追加**：選択したデバイスをゾーンに追加することができます。
4. デバイスの詳細ページを表示するには、デバイスをクリックします。
    - **デバイス情報**：ホスト名、エージェントのバージョン、およびオペレーティングシステムのバージョンなどの情報を表示します。
    - **デバイスプロパティ**：デバイス名、ポリシー、ゾーン、ロギングレベルを変更できます。
    - **脅威 & アクティビティ**：デバイスに関連する脅威情報および他のアクティビティを表示します。
5. **新規デバイスの追加** をクリックして、インストールトークンとエージェントインストーラをダウンロードするリンクを含むダイアログを表示します。
6. ゾーンの詳細ページを表示するには、ゾーンカラムのゾーン名をクリックします。

脅威 & アクティビティ

選択したデバイスに関連する脅威情報および他のアクティビティを表示します。

脅威

デバイスで検出された脅威をすべて表示します。デフォルトでは、脅威はステータス（危険、異常、隔離、および除外）によってグループ化されます。

- **エクスポート**：選択したデバイスで見つかったすべての脅威の情報を含む CSV ファイルを作成し、ダウンロードします。脅威情報には、名前、ファイルパス、Cylance スコア、およびステータスなどの情報が含まれます。

- **隔離**：選択した脅威を隔離します。これはローカルの隔離です。つまりこの脅威はこのデバイス上でのみ隔離されます。組織内のすべてのデバイスの脅威を隔離するには、ファイルが隔離された際に、**また、この脅威はすべてのデバイスで見つかった場合は常に隔離する** チェックボックスを選択します（グローバル隔離）。
- **除外**：選択した脅威のステータスを 除外 に変更します。除外ファイルの実行が許可されます。これは、ローカルの除外です。つまりこのファイルはこのデバイス上でのみ許可されます。組織内のすべてのデバイスでこのファイルを許可するには、ファイルが除外された際に **また、すべてのデバイスで安全としてマークする** チェックボックスを選択します（セーフリスト）。

悪用の試み

デバイス上での悪用の試みをすべて表示します。プロセス名、ID、タイプ、および実行されるアクションに関する情報が含まれます。

エージェントログ

デバイス上のエージェントによってアップロードされたログファイルを表示します。ログファイル名は、ログの日付です。

エージェントログファイルの表示方法：

1. 単一デバイスの現在のログファイルをアップロードします。
   a. デバイス > エージェントログ の順にクリックします。
   b. **現在のログファイルのアップロード** をクリックします。ログファイルのサイズによっては、数分かかることがあります。

または

1. ポリシー設定：
   a. 設定 > デバイスポリシー > [ポリシーの選択] > エージェントログ の順にクリックします。
   b. ログファイルの自動アップロードを有効にする をクリックします。
   c. **保存** をクリックします。

詳細ログを表示するには、ログファイルをアップロードする前に、エージェントのロギングレベルを変更します。

1. コンソールで、**デバイス** > **[デバイスをクリックします]**、エージェントのロギングレベルドロップダウンメニューで **詳細** を選択し、**保存** をクリックします。詳細ログファイルをアップロードしたら、デルはエージェントのロギングレベルを 情報 に変更することをお勧めします。
2. デバイス上で、Threat Defense ユーザーインタフェースを閉じます（システムトレイの Threat Defense アイコンを右クリックしてから、**終了** をクリックします）。

または

1. 管理者としてコマンドラインを開きます。次のコマンドラインを入力してから、**Enter** を押します。

   ```
   cd C:\Program Files\Cylance\Desktop
   ```

2. 次のコマンドラインを入力してから、**Enter** を押します。

   ```
   Dell.ThreatDefense.exe –a
   ```

3. システムトレイに Threat Defense アイコンが表示されます。右クリックして、**ロギング** をクリックし、次に **すべて** をクリックします（コンソールの 詳細 と同じ）。

または（macOS の場合）

1. 現在実行中のユーザーインタフェースを終了させます。
2. ターミナルから次のコマンドを実行します。

   ```
   sudo /Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -a
   ```

3. 新しいユーザーインタフェースが開いたら、それを右クリックします。**ロギング** >**すべて** の順に選択します。

スクリプト制御

拒否されたスクリプトなどスクリプト制御に関連する全アクティビティを表示します。

重複デバイス

Threat Defense エージェントが最初にデバイスにインストールされたとき、このデバイスを識別および参照するためにコンソールによって使用される、一意の識別子が作成されます。しかし、仮想マシンイメージを使用して複数のシステムを作成するなど特定のイベントでは、同じデバイスに対して 2 つ目の識別子が作成されることがあります。コンソールの デバイス ページに重複エントリが表示される場合は、デバイスを選択して、**削除** をクリックします。

このようなデバイスを識別しやすくするためには、デバイス ページでカラムソート機能を使用して、通常、デバイス名によってデバイスをソートし、比較します。または、デバイスリストは .CSV ファイルとしてエクスポートできるため、強力な並べ替え / 整理機能を持つ Microsoft Excel または同様のものでも表示できます。

***Microsoft Excel* の使用例**

1. Microsoft Excel でデバイスの CSV ファイルを開きます。
2. このデバイス名のカラムを選択します。
3. ホーム タブから、条件付き書式 > セルの強調表示ルール > 重複する値 の順に選択します。
4. **重複** が選択されていることを確認し、次にハイライトオプションを選択します。
5. **OK** をクリックします。重複する項目が強調表示されます。

メモ：削除コマンドは、デバイスページからデバイスのみを削除します。Threat Defense エージェントに対してアンインストールコマンドを発行することはありません。エージェントは、エンドポイントでアンインストールする必要があります。

エージェントアップデート

Threat Defense エージェントのメンテナンスと管理は簡単です。エージェントは、コンソールからアップデートを自動的にダウンロードし、コンソールは Cylance によってメンテナンスされます。

エージェントは、1～2 分ごとにコンソールに問い合わせます。コンソールは、エージェントの現在の状態（オンライン または オフライン、危険 または 保護）、バージョン情報、オペレーティングシステム、および脅威のステータスを表示します。

Threat Defense は、毎月エージェントにアップデートをリリースします。これらのアップデートは、構成リビジョン、新モジュール、およびプログラム変更を含むことがあります。エージェントアップデートが使用可能になると（設定 > エージェントアップデートでコンソールによって報告される）、エージェントはアップデートを自動的にダウンロードし、適用します。エージェントアップデート中のネットワークトラフィックを制御するために、全組織が、最大 1000 デバイスの同時アップデートに対応できるように設定されています。ユーザーは、希望する場合は、自動アップデートを無効にできます。

メモ：同時アップデートのデバイスの最大数は、デルサポートで変更することができます。

ゾーンベースのアップデート

ゾーンベースのアップデートによって、組織は、デバイスのサブセットで新しいエージェントを評価してから、（本番稼働）環境全体に導入できます。本番稼働とは異なるエージェントを使用できる 2 つのテストゾーン（テストおよびパイロット）のうちの 1 つに、1 つまたは複数の現在のゾーンを一時的に追加することができます。

ゾーンベースのアップデートの設定方法

1. 管理者アカウントを使用して、コンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **エージェントのアップデート** の順に選択します。3 つの最新のエージェントバージョンが表示されます。

   本番ゾーンが **自動アップデート** に設定されている場合は、テストおよびパイロットゾーンは使用できません。本番稼働ゾーンで自動アップデートを他のオプションに変更すると、テストゾーンおよびパイロットゾーンを有効にすることができます。
3. 本番稼働ドロップダウンリストで特定のエージェントバージョンを選択します。
4. 本番稼働では、自動アップデート または 更新しない も選択します。
   a. **自動更新** により、すべての本番デバイスは サポートされているエージェントのバージョンのリスト の最新のバージョンに自動的にアップデートされます。
   b. **更新しない** はすべての本番デバイスがエージェントをアップデートすることを禁止します。

5. テストゾーンでは、ゾーンドロップダウンリストから 1 つまたは複数のゾーンを選択してから、バージョンドロップダウンリストで特定のエージェントバージョンを選択します。
6. 必要に応じて、パイロットゾーンに対して手順 5 を繰り返します。

メモ：デバイスが、テストまたはパイロットゾーンの一部であるゾーンに追加されると、そのデバイスはテストまたはパイロットゾーンのエージェントのバージョンを使用して起動します。デバイスが複数のゾーンに属し、これらのゾーンのうちの 1 つがテストゾーンまたはパイロットゾーンに属する場合、テストゾーンまたはパイロットゾーンのエージェントバージョンが優先されます。

エージェントアップデートのトリガ方法

次の 1 時間間隔前にエージェントアップデートをトリガするには、次の手順を実行します。

1. システムトレイで Threat Defense エージェント アイコンを右クリックし、**アップデートのチェック** を選択します。
2. Threat Defense サービスを再起動します。これによって、コンソールへの問い合わせがただちに行われます。

または

- アップデートは、コマンドラインから開始できます。Cylance ディレクトリから次のコマンドを実行します。

  ```
  Dell.ThreatDefense.exe – update
  ```

ダッシュボード

Defense コンソールにログインすると、ダッシュボード ページが表示されます。ダッシュボードは、環境内の脅威の概要を示し、1 つのページから異なるコンソール情報にアクセスできます。

脅威統計

脅威統計は過去 *24* 時間以内に検出された脅威の数および組織の合計を表示します。脅威統計 をクリックして 保護 ページに移動し、その統計に関連する脅威の一覧を表示します。

- **実行中の脅威**：組織内のデバイス上で現在実行されている脅威として確認されたファイルです。
- **自動実行脅威**：自動的に実行される脅威です。
- **隔離された脅威**：過去 24 時間以内に隔離された脅威とその合計です。
- **Cylance 固有**：他のアンチウイルスソースではなく、Cylance によって確認された脅威です。

保護割合

脅威保護およびデバイス保護の割合を表示します。

- **脅威保護**：アクションが実行された脅威の割合です（隔離、グローバル隔離、除外 および安全リスト）。
- **デバイスの保護**：自動隔離が有効になったポリシーに関連するデバイスの割合です。

優先度別の脅威

アクションを必要としている脅威の合計数です（隔離、グローバル隔離、除外 および 安全リスト）です。これらの脅威は、優先度別（高、中、および低）でグループ化されます。この概要は、アクションを必要とする脅威の合計数を表示し、この合計を優先度で分け、割合の合計および影響を受けるデバイスの数を示します。

脅威は、ダッシュボード ページの左下隅に優先度別にリスト表示されます。優先度分類によってグループ化された組織内の脅威の合計数が特定されます。

脅威は次の属性の数値に基づいて低、中、高に分類されます。

- ファイルの Cylance スコアが 80 を超えている。
- ファイルが現在実行中である。
- 以前に実行されたことがあるファイルである。
- ファイルが自動実行されるように設定されている。
- 脅威が検出されたゾーンの優先度。

この分類は、どの脅威およびデバイスに最初に対処するべきかを管理者が判断するのに役立ちます。脅威およびデバイスの詳細を表示するには、脅威またはデバイス数をクリックします。

脅威イベント

直近 30 日間に検出された脅威の数を示す線グラフを表示します。線は、危険、異常、隔離、除外 およびクリアされたファイルによって色分けされています。

- 詳細を表示するには、グラフ上の点にマウスを置きます。
- 線を表示する、または非表示にするには、凡例内の色の 1 つをクリックします。

脅威の分類

ウイルスまたはマルウェアなど組織内で検出された脅威タイプのヒートマップを表示します。保護 ページに移動し、該当するタイプの脅威のリストを表示するには、ヒートマップで項目をクリックします。

トップ 5 リスト

組織内で最も多くのデバイスで検出されたトップ 5 脅威、最も多くの脅威が検出されたトップ 5 デバイス、最も多くの脅威が検出されたトップ 5 ゾーンのリストが表示されます。詳細を表示するには、リスト項目をクリックします。

ダッシュボードの上位 5 つのリストで、隔離または除外など組織内の処理されていない危険な脅威がハイライト表示されます。これらのリストは、ほとんど常に空であるべきです。異常な脅威の処理中に、上位 5 つのリストは重大な脅威であることを示します。

保護 – 脅威

Threat Defense は、ファイルを危険または異常に分類するだけではありません。ファイルの静的および動的な特徴の詳細が提供されます。それによって、管理者は脅威をブロックできるだけでなく、脅威の緩和や対応を強化するために、脅威の動作も理解できます。

ファイルタイプ

危険：スコアが 60～100 のファイル。危険ファイルは、Threat Defense エンジンによってマルウェアによく似た属性が検出されたファイルです。

異常：スコアが 1～59 のファイル。異常のファイルにもマルウェアの属性はありますが、危険ファイルより少ないため、マルウェアである可能性は低くなります。

メモ：ファイルの表示されたスコアが分類の範囲に一致しなくても、危険 または 異常 に分類されることがあります。これは、最初の検出後に新しい発見があったり、ファイル分析が追加された結果です。最新の分析にするには、デバイスポリシーで自動アップロードを有効にします。

Cylance スコア

Cylance スコアは異常または危険とみなされる各ファイルに割り当てられます。このスコアは、ファイルがマルウェアである確実性のレベルを表します。この数値が大きいほど、確実性が高くなります。

脅威情報の表示

コンソールの 保護 タブには、詳細な脅威情報、脅威が検出されたデバイス、およびこれらの脅威に対してこれらのデバイスで実行されたアクションが表示されます。

メモ：保護 タブの脅威リストには設定可能なカラムがあります。任意のカラムでドロップダウン矢印をクリックしてメニューにアクセスしてから、さまざまな脅威の詳細を表示 / 非表示にします。このメニューには、フィルタリングサブメニューが含まれています。

脅威の詳細の表示方法

1. コンソール（http://dellthreatdefense.com）にログインします。
2. **保護** タブをクリックして、その組織で検出された脅威のリストを表示します。
3. 左メニューバーのフィルタを使用して優先度（高、中または低）およびステータス（隔離、除外、危険または異常）によってフィルタリングします。

   メモ：左ペインに赤色で表示される数字は、隔離または除外されていない目立った脅威を示します。分析を必要とするファイルのリストを表示するには、これらの項目をフィルタリングします。

4. カラムを追加して、追加の脅威情報を表示できるようにするには、カラム名のうちの 1 つの隣にある下矢印をクリックしてから、カラム名を選択します。

5. 特定の脅威に関する追加情報を表示するには、脅威名のリンクをクリックするか（新しいページに詳細が表示されます）、脅威の行の任意の場所をクリックします（ページの下部に詳細が表示されます）。表示内容は両方とも同じですが、プレゼンテーションのスタイルが異なります。詳細には、ファイルメタデータの概要、脅威に感染したデバイスのリスト、エビデンスレポートなどが含まれます。

    a. ファイルメタデータ

        - 分類［Cylance Advanced Threat and Alert Management（ATAM）チームによる割り当て]
        - Cylance スコア（確実性のレベル）
        - AV 業界による裏付け（他のベンダーとの比較用の VirusTotal.com へのリンク）
        - 初回検出日、最新検出日
        - SHA256
        - MD5
        - ファイル情報（作成者、説明、バージョンなど）
        - 署名の詳細

    b. デバイス

        脅威のデバイス / ゾーンリストは、脅威の状態（危険、隔離、除外および異常）によってフィルタリングできます。その状態の脅威が存在するデバイスを表示するには、状態フィルタのリンクをクリックします。

        - 危険：ファイルは危険に分類されましたが、何のアクションも実行されていません。
        - 隔離：ポリシー設定により、ファイルはすでに隔離されました。
        - 除外：ファイルは管理者により、除外またはホワイトリスト化されました。
        - 異常：ファイルは異常に分類されましたが、何のアクションも実行されていません。

    c. エビデンスレポート

        - **脅威のインジケータ**：Cylance Infinity エンジンが分析したファイルの観測です。これらのインジケータは、ファイルの分類の理由を理解しやすくし、ファイルの属性と動作を知る上での手がかりを提供します。脅威インジケータは、コンテキストに役立つカテゴリに分類されます。
        - **詳細脅威データ**：詳細脅威データ には、追加ファイルメタデータ、ファイル構造の詳細、動的動作（ファイルの削除、レジストリキーの作成または変更など）、ファイルの通信試行先の URL など、ファイルの静的および動的特徴の包括的サマリが表示されます。

脅威インジケータを表示するには、次の手順を実行します。

1. コンソール（http://dellthreatdefense.com）にログインします。
2. トップメニューで **保護** をクリックして、脅威の一覧を表示します（または **デバイス** をクリックしてデバイスを選択します）。
3. 任意の脅威の名前をクリックします。脅威の詳細 ページが表示されます。
4. **エビデンスレポート** をクリックします。

脅威インジケータのカテゴリ：

各カテゴリは、悪意のあるソフトウェアによくある領域を示しています。これは、1 億を超えるバイナリを深く分析した結果に基づいています。脅威インジケータレポートは、ファイル内に存在するこれらのカテゴリの数を示します。

異常

ファイルには、何らかの非一貫性または異常を示す要素が含まれています。ファイルの構造に非一貫性が存在することが多くあります。

収集

ファイルには、データ収集のエビデンスが存在します。デバイス構成の列挙または機密情報の収集などが挙げられます。

データロス

ファイルには、データ引き出しのエビデンスが存在します。外部ネットワーク接続、ブラウザとして作用したエビデンス、または他のネットワーク通信などが挙げられます。

欺瞞

ファイルには、騙そうとした試みのエビデンスが存在します。隠しセクション、検出回避コードの含有、またはメタデータもしくは他のセクションでの不適切なラベル表示などの形態をとることがあります。

破壊

ファイルには、破壊機能のエビデンスが存在します。ファイルまたはディレクトリなどデバイスリソースの削除機能が挙げられます。

その他

他のカテゴリに適合しない他のすべてのインジケータです。

メモ：時折、脅威インジケータ および詳細な脅威のデータ セクションに結果がない、または使用できない場合があります。これは、ファイルがアップロードされていないときに発生します。デバッグログは、ファイルがアップロードされていない理由に関する手がかりを提供することがあります。

脅威への対応

一部の脅威に対して実行するアクションのタイプは、デバイスの割り当てられたユーザーによって異なることがあります。脅威に適用されるアクションは、デバイスレベルまたはグローバルレベルで適用できます。検出された脅威またはファイルに対して実行されるさまざまなアクションは次の通りです。

- **隔離**：特定のファイルを隔離すると、ファイルはこのデバイスで実行されなくなります。

  メモ：デバイスでコマンドラインを使用して、脅威を隔離することができます。これは Windows エージェントのみで使用できます。詳細については、「コマンドラインによる隔離」を参照してください。

- **グローバル隔離**：ファイルをグローバル隔離すると、組織全体のすべてのデバイスでファイルが実行されなくなります。

  メモ：ファイルを隔離すると、ファイルは元の場所から隔離ディレクトリ（**C:\ProgramData\Cylance\Desktop\q**）に移動します。

- **除外**：ファイルを除外すると、そのファイルをデバイスで実行できるようになります。
- **グローバル安全**：ファイルをグローバル安全リストに掲載されたファイルは、組織のどのデバイスでも実行できます。

  メモ：Threat Defense によって、「正常な」ファイルを隔離または報告される場合もあります（ファイルの機能が悪意のあるファイルに非常に似ている場合に起こります）。これらのインスタンスでは、ファイルの除外またはグローバル安全リストへの掲載が有用なことがあります。

- **ファイルのアップロード**：ファイルを手動で Cylance Infinity にアップロードして分析します。自動アップロードが有効である場合、新しいファイル（Cylance による分析が済んでいないファイル）は、Cylance Infinity に自動的にアップロードされます。Cylance Infinity にファイルが存在する場合、ファイルのアップロード ボタンは使用できません（灰色になります）。

- **ファイルのダウンロード**：独自のテスト目的でファイルをダウンロードします。組織でこの機能が有効になっている必要があります。ユーザーは、管理者である必要があります。脅威は、バージョン 1320 以上のエージェントを使用して検出する必要があります。

  メモ：ファイルは、Cylance Infinity で使用可能な必要があり、すべての 3 つのハッシュ（SHA256、SHA1 および MD5）が Cylance Infinity およびエージェントに一致する必要があります。一致しない場合、ファイルのダウンロード ボタンは使用できません。

特定デバイスでの脅威への対応

1. 管理者またはゾーン管理者としてコンソール（http://dellthreatdefense.com）にログインします。
2. **デバイス** タブをクリックします。

3. デバイスを検索し、選択します。
4. あるいは、関連する脅威のリストに掲載されている場合、デバイスへのリンクを保護タブから使用できることがあります。
5. このデバイス上のすべての脅威が、ページの下部のリストに表示されます。脅威をデバイス上の隔離または除外ファイルのいずれかに選択します。

脅威へのグローバルな対応

グローバル隔離リスト または グローバル安全リスト に追加されたファイルは、すべてのゾーン内のすべてのデバイス上の隔離または許可のいずれかです。

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **グローバルリスト** の順にクリックします。
3. グローバル隔離 または 安全 をクリックします。
4. **ファイルの追加** をクリックします。
5. ファイルの SHA256（必須）、MD5、名前およびグローバルリストに配置された理由を追加します。
6. **送信** をクリックします。

保護 – スクリプト制御

Threat Defense は、ブロックされた、またはアラートを受けたアクティブスクリプトおよび PowerShell スクリプトに関する詳細を提供します。スクリプト制御を有効にすると、保護 ページのスクリプト制御 タブに結果が表示されます。ここでは、スクリプトおよび影響を受けたデバイスに関する詳細が提供されます。

スクリプト制御の結果の表示方法

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。
2. 保護 をクリックします。
3. スクリプト制御 をクリックします。
4. 表でスクリプトを選択します。これにより、影響を受けたデバイスのリストを含む 詳細 テーブルがアップデートされます。

スクリプト制御カラムの説明

- **ファイル名**：スクリプトの名前です。
- **インタプリタ**：スクリプトを確認するスクリプトの制御機能です。

- **最新検出**：スクリプトが最後に実行された日付と時刻です。
- **ドライブタイプ**：スクリプトが検出されたドライブのタイプです（例：内蔵ハードドライブ）。
- **SHA256**：スクリプトの SHA 256 ハッシュです。
- **デバイスの数**：このスクリプトによって影響を受けるデバイスの数です。
- **警告**：スクリプトが警告された回数です。これは、同一デバイスに対して複数回のことがあります。
- **ブロック**：スクリプトがブロックされた回数です。これは、同一デバイスに対して複数回のことがあります。

詳細カラムの説明

- **デバイス名**：スクリプトに影響されるデバイスの名前です。デバイスの詳細 ページを表示するには、デバイス名をクリックします。
- **状態**：デバイスの状態です（オンラインまたはオフライン）。
- **エージェントバージョン**：現在デバイスにインストールされているエージェントのバージョンです。
- **ファイルパス**：スクリプトの実行元であるファイルのパスです。
- **日時**：スクリプトが実行された日付と時刻です。
- **ユーザー名**：スクリプトが実行されたときにログインしたユーザーの名前です。
- **アクション**：スクリプトに行われたアクション（警告またはブロック）です。

グローバルリスト

グローバルリスト で、ファイルを隔離にマークするかまたはこれらのファイルを組織内のすべてのデバイスで許可することができます。

- **グローバル隔離：**組織内のすべてのエージェントは、デバイス上で検出されたすべてのファイルをグローバル隔離リストに隔離します。
- **安全：**組織内のすべてのエージェントは、デバイス上で検出された安全リスト上のすべてのファイルを許可します。
- **未割り当て：**組織内で確認された、グローバル隔離または安全リストに割り当てられていないすべての脅威です。

脅威ステータスの変更

脅威ステータス（グローバル隔離、安全 または未割り当て）を変更するには：

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **グローバルリスト** の順に選択します。

3. 脅威が割り当てられている最新のリストを選択します。たとえば、未割り当て をクリックして未割り当ての脅威をグローバル隔離 または 安全 に変更します。
4. 変更する脅威のチェックボックスを選択し、ステータスのボタンをクリックします。
    a. 安全：ファイルを 安全リスト に移動します。
    b. グローバル隔離：ファイルを グローバル隔離リスト に移動します。
    c. リストから削除するには：ファイルを 未割り当てリスト に移動します。

ファイルの追加

ファイルを グローバル隔離 または 安全リスト に手動で移動します。追加されるファイルの SHA256 ハッシュ情報は必須です。

1. 管理者としてコンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **グローバルリスト** の順に選択します。
3. ファイルを追加するリスト（グローバル隔離 または 安全リスト）を選択します。
4. **ファイルの追加** をクリックします。
5. SHA256 情報を入力します。任意で、MD5 およびファイル名情報を入力します。
6. このファイルの追加理由を入力します。
7. **送信** をクリックします。

証明書による安全リストへの掲載

お客様は、署名された証明書別にファイルを安全リストに掲載することができます。これにより適切に署名されたカスタムソフトウェアは、中断することなく実行できます。

メモ：この機能は、現在 Windows オペレーティングシステムでのみ動作します。

- この機能によって、お客様は、証明書の SHA1 サムプリントによって表示される署名された証明書による ホワイトリスト / 安全リスト を確立できます。
- 証明書情報（タイムスタンプ、件名、発行者、および拇印）は、コンソールによって抽出されます。証明書は、コンソールにアップロードされたり、コンソールに保存されたりすることはありません。
- 証明書のタイムスタンプは、証明書の作成日時を示します。
- コンソールは、証明書が最新か、有効期限切れであるかを確認しません。
- 証明書が変更された（たとえば、更新された、または新しい）場合、コンソールの 安全リスト に追加する必要があります。

1. 証明書リポジトリに証明書の詳細を追加します。

    a. 署名付き Portable Executable（PE）の証明書拇印を識別します。

    b. **設定** > **証明書** の順にクリックします。

    c. **証明書の追加** をクリックします。

    d. **追加する証明書を参照** をクリックするか、または証明書をメッセージボックスにドラッグ & ドロップします。

    e. 証明書を参照する場合、ウィンドウが開き、証明書を選択できます。

    f. 任意で、この証明書に関するメモを追加します。

    g. **送信** をクリックします。発行者、件名、拇印、およびメモ（入力した場合）が、リポジトリに追加されます。

2. 証明書を 安全リスト に追加します。

    a. **設定** > **グローバルリスト** の順に選択します。

    b. **安全** タブを選択します。

    c. **証明書** をクリックします。

    d. **証明書の追加** をクリックします。

    e. 証明書を 安全リスト から選択します。任意で、カテゴリを選択し、この証明書の追加理由を追加します。

    f. **送信** をクリックします。

脅威の拇印の表示

保護 タブでは、脅威の詳細に証明書の拇印が表示されるようになりました。画面で、**証明書の追加** を選択して証明書をリポジトリに追加します。

権限

証明書の追加 は、管理者のみが使用できる機能です。証明書がすでに証明書リポジトリに追加されている場合、コンソールには、**証明書に移動** が表示されます。証明書は、**証明書に移動** オプションを参照できるゾーン管理者のみに表示されます。

プロファイル

プロファイルメニュー（右上隅）では、アカウントの管理、コンソール監査ログの表示、製品ヘルプへのアクセスを実行できます。

My Account

パスワードおよび電子メール通知の設定は、My Account ページで変更します。

1. コンソール（http://dellthreatdefense.com）にログインします。
2. 右上隅のプロファイルメニューをクリックし、**マイアカウント** を選択します。
3. パスワードを変更するには、次の手順を実行します。
    a. パスワードの変更 をクリックします。
    b. 古いパスワードを入力します。
    c. 新しいパスワードを入力し、確認のためにもう 1 度入力します。
    d. アップデート をクリックします。
4. 電子メール通知 を有効にする、または無効にするには、チェックボックスを選択するか、その選択を解除します。チェックボックスの有効化および無効化は、自動的に保存されます。電子メール通知 は、管理者のみが使用できます。

監査ロギング

ユーザーアイコンドロップダウンリスト（コンソールの右上隅）

監査ログには、コンソールから実行された次のアクションに関する情報が含まれています。

- ログイン（成功、失敗）
- ポリシー（追加、編集、削除）
- デバイス（編集、削除）
- 脅威（隔離、免除、グローバル隔離、安全リスト）
- ユーザー（追加、編集、削除）
- エージェントアップデート（編集）

監査ログは、コンソールの右上側にあるプロファイルドロップダウンリストに移動し、**監査ログ** を選択するとコンソールに表示されます。監査ログは、管理者のみが使用できます。

設定

設定 ページには、アプリケーション、ユーザー管理、デバイスポリシー、グローバルリスト、および エージェントアップデート の各タブが表示されます。設定 メニューは、管理者のみが使用できます。

アプリケーション

Threat Defense エージェント

デバイスは、Threat Defense エージェントを各エンドポイントにインストールすることによって組織に追加されます。コンソールに接続すると、（識別された脅威を管理するために）ポリシーを適用し、組織のニーズに基づいてデバイスを整理します。

Threat Defense エージェントは、最小限のシステムリソースを使用するように設計されています。エージェントは、実行ファイルまたはプロセスを優先して取り扱います。これは、これらが悪意のあるものであり得るためです。ディスク上に単に存在するファイル（実行ファイルではなく、ストレージに存在するファイル）は、悪意のあるものである可能性はあるものの、差し迫った脅威をもたらすものではないため、これらの優先度は低くなります。

Windows エージェント

システム要件

エンドポイントハードウェア（CPU、GPU など）は、ターゲットオペレーティングシステムの推奨要件を満たすか、それ以上であることが推奨されます。例外は、下記の通りです（RAM、使用可能なハードドライブ容量、および追加ソフトウェア要件）。

オペレーティングシステム	• Windows 7（*32* ビットまたは *64* ビット） • Windows Embedded Standard 7（*32* ビット）および Windows Embedded Standard 7 Pro（*64* ビット） • Windows 8 および 8.1（*32* ビットおよび *64* ビット）* • Windows 10（*32* ビットおよび *64* ビット）** • Windows Server 2008 および 2008 R2（*32* ビットおよび *64* ビット）*** • Windows Server 2012 および 2012 R2（*64* ビット）*** • Windows Server 2016 – Standard、Data Center および Essentials****
RAM	• 2 GB
使用可能なハードドライブ容量	• 300 MB
追加ソフトウェア / 要件	• .NET Framework 3.5（SP1）以上（*Windows* のみ） • インターネットブラウザ • ログイン、インストーラへのアクセス、製品の登録を行うためのインターネットアクセス • ソフトウェアをインストールするためのローカル管理者権限
その他の要件	• TLS 1.2 はエージェントの 1422 以降でサポートされており、.NET Framework 4.5 以降が必要です。

表 *2*：*Windows* のシステム要件

*非対応：Windows 8.1 RT

**Windows 10 Anniversary Update には、Agent 1402 以降が必要です。

***非対応：Server Core（2008 および 2012）および Minimal Server（2012）。

****Agent 1412 以降が必要です。

インストールファイルのダウンロード方法

1. コンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **アプリケーション** の順に選択します。
3. **インストールトークン** をコピーします。

   インストールトークンは、エージェントがコンソール上で割り当てられたアカウントに報告できるようにする、ランダムに生成された文字列です。インストールトークンは、インストール中に（インストールウィザードで、またはインストールパラメータ設定としてのいずれかで）要求されます。
4. インストーラをダウンロードします。
   a. オペレーティングシステムを選択します。
   b. ダウンロードするファイルタイプを選択します。

      Windows の場合は、エージェントのインストールに MSI ファイルを使用することが推奨されます。

ヒント：ゾーン規則が設定されている場合、デバイスがゾーン規則の基準と一致する場合は、デバイスはゾーンに自動的に割り当てることができます。

エージェントのインストール – Windows

Threat Defense をインストールする前に、すべての前提条件が満たされていることを確認します。システム要件を参照してください。

1. DellThreatDefenseSetup.exe（または MSI）をダブルクリックして、インストールを開始します。
2. Threat Defense セットアップウィンドウで **インストール** をクリックします。
3. Threat Defense テナントから提供されたインストールトークンを入力します。**次へ** をクリックします。

   メモ：インストールトークンにアクセスできない場合は、Threat Defense 管理者に連絡するか、KB 文書「方法：Threat Defense の管理（英語）」を参照してください。
4. 任意で、Threat Defense の宛先フォルダを変更します。

   OK をクリックしてインストールを開始します。
5. **完了** をクリックしてインストールを終了します。Threat Defense を起動するには、チェックボックスをオンにします。

Windows のインストールパラメータ

エージェントは、GPO、（SCCM として一般に知られる）Microsoft System Center Configuration Manager、および MSIEXEC を使用して、対話形式でまたは非対話形式でインストールできます。MSI は（下記に示す）ビルトインパラメータでカスタマイズできます。または、パラメータはコマンドラインから提供されることができます。

プロパティ	値	説明
PIDKEY	<インストールトークン>	インストールトークンが自動入力されます。
LAUNCHAPP	0 または 1	0: システムトレイアイコンおよびスタートメニューフォルダは、実行時に非表示です。 1: システムトレイアイコンおよびスタートメニューフォルダは、実行時に非表示ではありません（デフォルト）。
SELFPROTECTIONLEVEL	1 または 2	1: ローカル管理者のみがレジストリおよびサービスを変更できます。 2：システム管理者のみがレジストリおよびサービスを変更できます（デフォルト）。
APPFOLDER	<インストール先フォルダ>	エージェントのインストールディレクトリを指定します。 デフォルトの場所は C:\Program Files\Cylance\Desktop です
VenueZone	「ゾーン名」	Agent のバージョン 1382 以降が必要です •ゾーンへのデバイスの追加 •ゾーンが存在しない場合は、ゾーンが入力した名前を使用して作成されます。 •ゾーン名を、既存のゾーンまたは作成するゾーンの名前に置き換えます。 **警告**：ゾーン名の前または後にスペースを追加すると、新しいゾーンが作成されます。

表 *3*：*Windows* のインストールパラメータ

次のコマンドライン例は、Microsoft Windows インストーラツール（MSIEXEC）を実行し、PIDKEY、APPFOLDER、および LAUNCHAPP の各インストールパラメータを渡す方法を示します。

```
msiexec /i DellThreatDefenseSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN>
LAUNCHAPP=0 /L*v C:\temp\install.log
```

これはサイレントインストールであり、インストールログは **C:\temp** に保存されます。エージェントの実行時には、システムトレイアイコンおよび スタート メニューの Threat Defense フォルダは、どちらも非表示です。MSIEXEC で使用可能なさまざまなコマンドラインスイッチに関する追加情報は、KB 227091 を参照してください。

Wyse Device Manager（WDM）を使用した Windows エージェントのインストール

本項は、インストールスクリプトの作成方法、WDM 用 RSP パッケージの作成方法、および WDM にこのパッケージを追加して、ユーザー操作なしで多数のシンクライアントに同時にインストールする方法について説明します。

Threat Defense のコマンドラインインストールを実行するバッチファイルスクリプトを作成します。WDM は、導入中にこのスクリプトを実行します。

1. メモ帳を開きます。上記のコマンドラインパラメータを使用して、次のコマンドラインを入力し、

   <INSTALLATION TOKEN> を提供されたインストールトークンと置き換えます。

   msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<INSTALLATION TOKEN> /q

   このフォルダはインストール中にシンクライアントのこの場所にコピーされるため、**C:\TDx86** は弊社のディレクトリに使用されます。

2. **.bat** 拡張子をつけたファイルを TDx86 フォルダに保存します。例：**TDx86_Install.bat**。

   ユーザーの操作なしに複数のシンクライアントに同時にインストールすることができる Threat Defense エージェントを使用して RSP パッケージを作成します。

3. WDM をインストール済みのコンピュータで Scriptbuilder を開きます。

4. パッケージ名 および パッケージの説明 を入力します。

   - パッケージカテゴリ で 他のパッケージ を選択します。
   - オペレーティングシステム で Windows Embedded Standard 7 を選択します。

5. スクリプトコマンドを追加して、ターゲットシステムが WES7 または WES7p であることを確認します。

   - スクリプトコマンド で オペレーティングシステムの確認（CO） を選択します。
   - デバイス OS 値には、適切なオペレーティングシステムを入力します。

6. アイテムを追加するには、二重矢印を使用します。

7. プロンプトで **OK** を押します。

8. コマンドを追加してシンクライアントをロックし、ユーザー操作を阻止します。

   - **スクリプトコマンド** > **ロックアウトユーザー（LU）** の順に選択します。値は必要ありません。ただし、この例では、インストーラが失敗したか、エラーが発生した場合には、スプラッシュ画面が削除されるように**はい**の**値**が入力されます。

9. コマンドを追加して、シンクライアントにファイルをコピーします。
    - スクリプトコマンドの **X Copy（XC）** を選択します。
    - **リポジトリディレクトリ**値には、***** を既存の **<regroot>** の最後に追加します。
    - **デバイスディレクトリ**値には、宛先のシンクライアント上にコピーされるファイルのパスを入力します。この例では、パッケージ名が使用されます。
10. コマンドを追加して、.bat インストールスクリプトを実行します。
    - **スクリプトコマンド** > **デバイスで実行（EX）** の順に選択します。
    - デバイスファイル名の値には、パス **C:\TDx86\TDx86_install.bat** を入力します。以前のコマンド XC により、TDx86 フォルダがコピーされます。
    - 同期の実行値として **+** を追加します。これにより、実行されているファイルが完了するまで待ち、続行するように WDM に通知されます。
11. コマンドを追加して、シンクライアントからコピーされたファイルを削除します。
    - スクリプトコマンドの **ツリーの削除（DT）** を追加します。
12. コマンドを追加して、ロックアウトを無効にします。
    - スクリプトコマンドの **ロックアウトの終了（EL）** を追加します。
13. 見直しのために、スクリプトパッケージは次のように見えるはずです。
    - Threat Defense を WES7P システムに導入している場合、オペレーティングシステムセクションを WES7P にアップデートします。そうしない場合、パッケージはインストールに失敗します。
14. パッケージを保存します。
    - **保存** をクリックして、**TDx86** フォルダの場所を参照します。これらの指示に従っている場合、フォルダはデスクトップにあります。
15. Scriptbuilder を閉じます。
16. **WyseDeviceManager** を起動してパッケージを WDM に追加します。
17. **WyseDeviceManager** > **Package Manager** > **その他のパッケージ** の順に参照します。
18. メニューバーで **アクション** > **新規** > **パッケージ** の順に選択します。
19. **スクリプトファイルからのパッケージの登録（RSP）** を選択し、**次へ** をクリックします。
20. これまでの手順で作成した RSP ファイルの場所を参照し、**次へ** をクリックします。
21. **有効** が選択されていることを確認し、**次へ** をクリックします。

22. WDM をパッケージに登録する準備ができたら、**次へ** をクリックします。
23. パッケージが正常に登録されたら、**終了** をクリックします。
24. パッケージは **その他のパッケージ** に表示されます。
25. パッケージの内容を確認します。
    - ファイルエクスプローラを開き、**C:\inetpub\ftproot\Rapport** を参照し、**TDx86 folder** を見つけます。
    - TDx86 フォルダを開き、このフォルダにインストーラおよび .bat ファイルが含まれていることを確認します。

パッケージは、WDM で使用可能になりました。WDM は、ユーザー操作なしで多数の WES7 シンクライアントに Threat Defense を導入することができます。

コマンドラインを使用した隔離

デバイスでコマンドラインを使用して、ファイルを隔離することができます。これには、脅威に対する SHA256 ハッシュの知識が必要です。

メモ：この機能は Windows 専用であり、エージェント 1432 以上が必要です。

1. Windows デバイス上で、コマンドラインを開きます。例：スタートメニューから、cmd.exe を検索します。
2. 引数 **-q:<hash>** をつけて Dell.ThreatDefense.exe を呼び出します。ここで <hash> はファイルの SHA256 ハッシュです。こうすることでエージェントから、ファイルを隔離フォルダに送信することが求められます。

   コマンドラインの例（Dell Threat Defense がデフォルトの位置にインストールされている場合）：

   ```
   "C:\Program Files\Cylance\Desktop\Dell.ThreatDefense.exe" -q:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```

エージェントのアンインストール

Windows システム上のエージェントをアンインストールするには、プログラムの追加 / 削除機能を使用するか、コマンドラインを使用します。

エージェントをアンインストールしても、コンソールからデバイスは削除されません。手動でコンソールからデバイスを削除する必要があります。

エージェントをアンインストールする前に、次の手順を実行してください。

- **エージェントのアンインストールにパスワードを必要とする** が有効な場合、アンインストールに必要なパスワードを確認します。
- **デバイスからのサービスシャットダウンを阻止する** が有効な場合、ポリシーで無効化するか、エージェントをアンインストールするデバイスに別のポリシーを適用します。

追加 / 削除プログラムを使用したアンインストール

1. **スタート** > **コントロールパネル** を選択します。
2. **プログラムのアンインストール** をクリックします。カテゴリではなくアイコンが表示されている場合は、プログラムと機能 をクリックします。
3. **Dell Threat Defense** を選択して、**アンインストール** をクリックします。

コマンドラインの使用

1. 管理者としてコマンドプロンプトを開きます。
2. エージェントのインストールに使用したインストールパッケージに応じて、次のコマンドを使用します。
    a. DellThreatDefense_x64.msi
        i. 標準的なアンインストール：msiexec /uninstall DellThreatDefense_x64.msi
        ii. Windows インストーラ：msiexec /x DellThreatDefense_x64.msi
    b. DellThreatDefense_x86.msi
        i. 標準的なアンインストール：msiexec /uninstall DellThreatDefense_x86.msi
        ii. Windows インストーラ：msiexec /x DellThreatDefense_x86.msi
3. 次のコマンドはオプションです。
    a. Quiet モードでアンインストールを実行：/quiet
    b. Quiet モードかつ非表示で実行：/qn
    c. パスワード保護されたアンインストール：UNINSTALLKEY=<パスワード>
    d. ログファイルのアンインストール：/Lxv* <パス>
        i. ファイル名を含む指定したパス（<パス>）にログファイルが作成されます。
        ii. 例：C:\Temp\Uninstall.log

macOS エージェント

システム要件

エンドポイントハードウェア（CPU、GPU など）は、ターゲットオペレーティングシステムの推奨要件を満たすか、それ以上であることが推奨されます。例外は、下記の通りです（RAM、使用可能なハードドライブ容量、および追加ソフトウェア要件）。

オペレーティングシステム	• Mac OS X 10.9 • Mac OS X 10.10 • Mac OS X 10.11 • macOS 10.12* • macOS 10.13**
RAM	• 2 GB
使用可能なハードドライブ容量	• 300 MB

表 *4*：*macOS* のシステム要件

*Agent 1412 以降が必要です。

**Agent 1452 以降が必要です。

インストールファイルのダウンロード方法

1. コンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **アプリケーション** の順に選択します。
3. **インストールトークン** をコピーします。

   インストールトークンは、エージェントがコンソール上で割り当てられたアカウントに報告できるようにする、ランダムに生成された文字列です。インストールトークンは、インストール中に（インストールウィザードで、またはインストールパラメータ設定としてのいずれかで）要求されます。
4. インストーラをダウンロードします。
   a. オペレーティングシステムを選択します。
   b. ダウンロードするファイルタイプを選択します。

ヒント：ゾーン規則が設定されている場合、デバイスがゾーン規則の基準と一致する場合は、デバイスはゾーンに自動的に割り当てることができます。

エージェントのインストール - macOS

Threat Defense をインストールする前に、すべての前提条件が満たされていることを確認します。システム要件 を参照してください。

メモ： macOS Agent は、将来のリリースではデルのブランドになります。

1. **`DellThreatDefense.dmg`** をダブルクリックして、インストーラをマウントします。
2. PROTECT ユーザーインタフェースで 保護 アイコンをダブルクリックして、インストールを開始します。
3. **続行** をクリックして、オペレーティングシステムおよびハードウェアが要件を満たしていることを確認します。
4. 導入画面で **続行** をクリックします。
5. Threat Defense テナントから提供されたインストールトークンを入力します。**続行** をクリックします。

メモ： インストールトークンにアクセスできない場合は、Threat Defense 管理者に連絡するか、KB 文書「方法：Threat Defense の管理（英語）」を参照してください。

6. 任意で、Threat Defense のインストール場所を変更します。

   インストール をクリックしてインストールを開始します。
7. 管理者のユーザー名およびパスワードを入力します。**ソフトウェアのインストール** をクリックします。
8. 概要画面で **終了** をクリックします。

macOS のインストールパラメータ

Threat Defense エージェントは、ターミナルでコマンドラインオプションを使用してインストールできます。下記の例では、PKG インストーラを使用します。DMG の場合は、単純にコマンドのファイル拡張子を変更してください。

メモ：ターゲットエンドポイントがシステム要件を満たしていること、およびソフトウェアをインストールする人にソフトウェアをインストールするための適切な資格情報があることを確認します。

プロパティ	値	説明
InstallToken		インストールトークンは、コンソールで入手できます。
NoCylanceUI		起動時には、エージェントアイコンは表示されません。デフォルトは、表示されます。
SelfProtectionLevel	0 または 1	1: ローカル管理者のみがレジストリおよびサービスを変更できます。 2：システム管理者のみがレジストリおよびサービスを変更できます（デフォルト）。

プロパティ	値	説明
LogLevel	0、1、2、または 3	0: エラー – エラーメッセージのみがロギングされます。 1: 警告 – エラーメッセージおよび警告メッセージがロギングされます。 2：情報（デフォルト） – エラーメッセージ、警告メッセージおよび情報メッセージがロギングされます。これは、トラブルシューティング中に詳細を提供します。 3: 詳細 – すべてのメッセージがロギングされます。トラブルシューティング時には、このログレベルが推奨されます。しかし、詳細ログファイルのサイズは非常に大きくなります。トラブルシューティング中は詳細をオンにし、トラブルシューティングが終了したら情報に戻すことが推奨されます。
VenueZone	「ゾーン名」	Agent のバージョン 1382 以降が必要です •ゾーンへのデバイスの追加 •ゾーンが存在しない場合は、ゾーンが入力した名前を使用して作成されます。 •ゾーン名を、既存のゾーンまたは作成するゾーンの名前に置き換えます。 **警告**：ゾーン名の前または後にスペースを追加すると、新しいゾーンが作成されます。

表 *5*：*macOS* のインストールパラメータ

エージェントのインストール

インストールトークンを使用しないインストール

```
sudo installer -pkg DellThreatDefense.pkg -target/
```

インストールトークンを使用したインストール

```
echo [install_token] > cyagent_install_token

sudo installer -pkg DellThreatDefense.pkg -target/
```

メモ：**[install_token]** をインストールトークンと置き換えます。echo コマンドは、1 行あたり 1 つのインストールオプションを含むテキストファイルである **cyagent_install_token** ファイルを出力します。このファイルは、インストールパッケージと同じフォルダに存在する必要があります。ファイル拡張子に注意します。上記の例では、cyagent_install_token ファイルに拡張子が表示されていません。macOS のデフォルト設定では、拡張子は非表示です。テキストエディットまたは他のテキストエディタを使用してこのファイルを手動で構築すると、削除する必要のある拡張子が自動的に追加されます。

任意のインストールパラメータ

ターミナルに次を入力して、インストーラが入力されるオプションの適用に使用するファイル（**cyagent_install_token**）を作成します。各パラメータは、それ自身の行に含まれている必要があります。このファイルは、インストールパッケージと同じフォルダに存在する必要があります。

次に例を示します。すべてのパラメータがファイルに含まれる必要はありません。ターミナルには、ファイル内の単一の引用に含まれているすべてが含まれています。各パラメータの後ろでは Enter/Return を必ず押して、各パラメータがファイルのそれ自身の行で維持されるようにします。

テキストエディタを使用して、各パラメータを（それ自身の行に）含むファイルを作成することもできます。このファイルは、インストールパッケージと同じフォルダに存在する必要があります。

例：

```
echo 'InstallToken

NoCylanceUI

SelfProtectionLevel=2

LogLevel=2'> cyagent_install_token

sudo installer -pkg DellThreatDefense.pkg -target/
```

エージェントのアンインストール

パスワードを使用しないアンインストール

```
sudo
/Applications/Cylance/Uninstall\ DellThreatDefense.app/Contents/MacOS/
Uninstall\ DellThreatDefense
```

パスワードを使用したアンインストール

```
sudo
/Applications/Cylance/Uninstall\ DellThreatDefense.app/Contents/MacOS/
Uninstall\ DellThreatDefense --password=thisismypassword
```

メモ：**thisismypassword** をコンソールで作成したアンインストールパスワードと置き換えます。

エージェントサービス

サービスの開始

```
sudo launchctl load
/Library/launchdaemons/com.cylance.agent_service.plist
```

サービスの停止

```
sudo launchctl unload
/Library/launchdaemons/com.cylance.agent_service.plist
```

インストールの検証

次のファイルをチェックして、エージェントが正常にインストールされたことを検証します。

1. プログラムフォルダが作成されました。
    - Windows のデフォルト：**C:\Program Files\Cylance\Desktop**
    - macOS のデフォルト：**/Applications/DellThreatDefense/**
2. Threat Defense アイコンが、ターゲットデバイスのシステムトレイに表示されます。

    これは、パラメータ LAUNCHAPP=0（Windows）または NoCylanceUI（macOS）が使用されている場合には該当しません。
3. ターゲットデバイスの Start Menu\All Programs の下に Threat Defense フォルダが存在します。

    これは、パラメータ LAUNCHAPP=0（Windows）または NoCylanceUI（macOS）が使用されている場合には該当しません。
4. Threat Defense サービスが追加され、現在実行中です。ターゲットデバイスの Windows Service パネルに実行中としてリスト表示されている Threat Defense サービスが存在するはずです。
5. Dell.ThreatDefense.exe プロセスが実行中です。Dell.ThreatDefense.exe プロセスが、ターゲットデバイスの Windows タスクマネージャのプロセスタブの下にリスト表示されているはずです。
6. デバイスは、コンソールに報告しています。コンソールにログインし、デバイス タブをクリックします。ターゲットデバイスが表示され、オンライン状態でリスト表示されるはずです。

エージェントのユーザーインタフェース

エージェントのユーザーインタフェースは、デフォルトで有効になっています。表示するには、システムトレイで エージェント アイコンをクリックします。あるいは、エージェントは、エージェント アイコンがシステムトレイに表示されないようにインストールすることもできます。

脅威 タブ

デバイスで検出されたすべての脅威および実行されたアクションを表示します。危険とは脅威に対して何のアクションも実行されていないことを意味します。隔離とは脅威が変更（ファイルの実行を防ぐため）され、隔離 フォルダに移動されたことを意味します。除外 とはファイルが管理者によって安全とみなされ、デバイス上での実行が 許可 されることを意味します。

イベント タブ

デバイスで発生したすべての脅威イベントを表示します。

スクリプト タブ

デバイスで実行された、すべての悪意のあるスクリプトおよびスクリプトで実行されたすべてのアクションを表示します。

エージェントメニュー

エージェントメニューでは、Threat Defense のヘルプおよびアップデートにアクセスできます。より多くのメニューオプションを提供する、高度なユーザーインタフェースへのアクセスも提供されます。

エージェントメニュー

エージェントメニューでは、ユーザーがデバイスでアクションを実行できます。エージェント アイコンを右クリックすると、メニューが表示されます。

- **アップデートの確認**：エージェントは利用可能なすべてのアップデートを確認し、インストールします。アップデートは、デバイスが属するゾーンに許可されているアップデートバージョンに限定されます。
- **ポリシーアップデートのチェック**：ポリシーアップデートが利用可能かどうかをエージェントが点検します。これには、既存のポリシーまたはエージェントに適用されている別のポリシーの変更が含まれます。

  メモ：ポリシーアップデートの点検は、Windows ではバージョン 1422（またはそれ以降）で、また macOS ではバージョン 1432（またはそれ以降）でサポートされています。
- **バージョン情報**：エージェントのバージョン、デバイスに割り当てられたポリシーの名前、エージェントが最後にアップデートを確認した日付、およびインストール中に使用されるインストールトークンを含むダイアログが表示されます。
- **終了**：システムトレイでエージェントアイコンを終了します。Threat Defense サービスがオフになることはありません。
- **オプション** > **通知の表示**：このオプションを選択して、すべての新しいイベントを通知として表示します。

エージェントユーザーインタフェースの高度なオプションの有効化

Threat Defense エージェントは、ユーザーインタフェースを介して高度なオプションを提供して、コンソールに接続せずにデバイス上で機能を提供します。高度なオプションを有効にするときは、CylanceSVC.exe を実行している必要があります。

Windows

1. システムトレイにエージェントアイコンが表示されている場合は、アイコンを右クリックし、**終了** を選択します。
2. コマンドプロンプトを起動し、次のコマンドを入力します。完了したら、Enter を押します。

   cd C:\Program Files\Cylance\desktop

   アプリケーションが別の場所にインストールされている場合は、コマンドプロンプトでその場所に移動します。

3. 次のコマンドを入力し、完了したら、Enter を押します。

   Dell.ThreatDefense.exe –a

   システムトレイに エージェント アイコンが表示されます。

4. アイコンを右クリックします。ロギング、検出を実行 および 脅威の管理 オプションが表示されます。

macOS

1. トップメニューにエージェントアイコンが表示されている場合は、アイコンを右クリックし、**終了** を選択します。
2. ターミナルを開いて実行します

   a. Sudo /Applications/DellThreatDefense/DellThreatDefense.app/Contents/MacOS/DellThreatDefenseUI –a

   メモ：これは、Dell Threat Defense のデフォルトのインストールパスです。パスを編集して環境に一致させる必要がある場合があります。

3. エージェントの UI が追加オプションで表示されます。

ロギング

エージェントから収集するログ情報のレベルを選択します。デフォルトは情報です。トラブルシューティング時には、ログレベルをすべて（詳細）に設定することが推奨されます。トラブルシューティングが完了したら、これを情報に戻します（すべての情報をロギングすると、非常に大きいログファイルが生成されることがあります）。

検出の実行

ユーザーは、脅威をスキャンするフォルダを指定できます。

1. **検出を実行** > **フォルダの指定** の順に選択します。
2. スキャンするフォルダを選択し、**OK** をクリックします。検出されたすべての脅威が、エージェントのユーザーインタフェースに表示されます。

脅威管理

ユーザーはデバイス上の隔離ファイルを削除できます。

1. **脅威の管理** > **隔離の削除** の順に選択します。
2. **OK** をクリックして確認します。

仮想マシン

仮想マシンイメージで Threat Defense エージェントを使用する場合には、次のことが推奨されます。

テンプレートとして使用する仮想マシンイメージを作成するときは、仮想マシンのネットワーク設定との接続を切断してからエージェントをインストールします。これにより、エージェントがコンソールと通信し、デバイスの詳細を設定しないようにします。また、コンソールでのデバイスの重複を防止します。

パスワード保護されたアンインストール

設定 > アプリケーション

管理者は、エージェントのアンインストールにパスワードを要求することができます。パスワードを使用してエージェントをアンインストールする場合は、次のようになります。

- MSI インストーラを使用してインストールした場合、MSI を使用するか、コントロールパネルを使用するかのいずれかでアンインストールします。
- EXE インストーラを使用した場合、EXE を使用してアンインストールします。EXE インストーラを使用した場合には、コントロールパネルを使用しても機能せず、アンインストールにはパスワードが要求されます。
- コマンドラインを使用して案インストールする場合、アンインストール文字列 **`UNINSTALLKEY = [MyUninstallPassword]`**。

アンインストールパスワードの作成方法

1. 管理者アカウントを使用して、コンソール（http://dellthreatdefense.com）にログインします。
2. **設定** > **アプリケーション** の順に選択します。
3. **エージェントのアンインストールにパスワードを必要とする** チェックボックスを選択します。
4. パスワードを入力します。
5. **保存** をクリックします。

統合

Threat Defense コンソールは、一部のサードパーティプログラムと統合できます。

Syslog/SIEM

Threat Defense は、Syslog 機能を使用して Security Information Event Management（SIEM）ソフトウェアと統合できます。Syslog イベントは、エージェントイベントがコンソールに報告されるのと同時に報告されます。

Syslog メッセージの最新の IP アドレスについては、デルサポートにお問い合わせください。

イベントタイプ

監査ログ

コンソール（ウェブサイト）で実行されたユーザーアクションの監査ログを Syslog サーバーに送信するには、このオプションを選択します。このオプションがオフであっても、監査ログイベントは、常に監査ログ画面に表示されます。

Syslog に転送された監査ログのメッセージ例

デバイス

Syslog サーバーにデバイスイベントを送信するには、このオプションを選択します。

- 新しいデバイスが登録されると、このイベントに関する 2 種類のメッセージ（登録およびシステムセキュリティ）が受信されます。

  デバイスの登録イベントのメッセージ例

- デバイスが削除された場合

  デバイスの削除イベントのメッセージ例

- デバイスのポリシー、ゾーン、名前、またはロギングレベルが変更された場合

  デバイスのアップデートイベントのメッセージ例

脅威

新たに検出された任意の脅威または任意の既存の脅威について検出された変更を Syslog サーバーにロギングするには、このオプションを選択します。変更には、削除済み、隔離済み、除外済み、または実行済みである脅威が含まれます。

次の 5 種類の脅威イベントがあります。

- **threat_found**：新しい脅威が危険な状態で検出されました。
- **threat_removed**：既存の脅威が削除されました。
- **threat_quarantined**：新しい脅威が隔離ステータスで検出されました。
- **threat_waived**：新しい脅威が除外ステータスで検出されました。
- **threat_changed**：既存の脅威の動作が変更されました（例：スコア、隔離ステータス、実行中ステータス）。
- **threat_cleared**：脅威が除外され、安全リストに追加されるかまたはデバイスの隔離から削除されました。

脅威イベントのメッセージ例

脅威の分類

何百もの脅威が、マルウェアまたは潜在的な迷惑プログラム（PUP）として毎日分類されます。このオプションがオンの場合、これらのイベントの発生時に通知を受けるように登録されます。

脅威分類のメッセージ例

SIEM（Security Information and Event Management）

イベントが送信される Syslog サーバーまたは SIEM のタイプを指定します。

プロトコル

Syslog サーバーで設定したプロトコルと一致する必要があります。UDP または TCP を選択します。UDP は、メッセージ配信を保証しないため、一般に推奨されません。TCP（デフォルト）が推奨されます。

TLS/SSL

指定されたプロトコルが TCP である場合にのみ使用できます。TLS/SSL は、Threat Defense から Syslog サーバーへの移動中に Syslog メッセージが暗号化されるようにします。このオプションを選択することが推奨されます。Syslog サーバーは、TLS/SSL メッセージを開くように設定します。

***IP/* ドメイン**

セットアップした Syslog サーバーの IP アドレスまたは完全修飾ドメイン名を指定します。社内のネットワーク専門家に相談して、ファイアウォールおよびドメイン設定が適切に設定されるようにします。

ポート

Syslog サーバーがメッセージを開く、デバイス上のポート番号を指定します。1 ～ 65535 の数字である必要があります。通常の値は次のとおりです。UDP の場合は 512、TCP の場合は 1235 または 1468、および 固定 TCP の場合は 6514（例：TLS/SSL が有効な TCP）。

重大度

Syslog サーバーに表示されるべきメッセージの重大度を指定します。これは、主観的フィールドであり、任意の好ましいレベルに設定できます。重大度の値によって Syslog に転送されるメッセージが変更されることはありません。

ファシリティ

メッセージをロギングするアプリケーションタイプを指定します。デフォルトは、内部（または Syslog）です。これを使用して、Syslog サーバーでの受信時にメッセージを分類します。

接続のテスト

IP / ドメイン、ポートおよびプロトコルの設定をテストするには、**接続テスト** をクリックします。有効な値を入力すると、数分後に、成功の確認が表示されます。

カスタム認証

外部 ID プロバイダ（IdP）を使用してコンソールにログインします。このためには、IdP ログインを検証するために X.509 証明書および URL を取得するように IdP を設定する必要があります。Microsoft SAML 2.0 では、カスタム認証が機能します。この機能は、OneLogin、OKTA、Microsoft Azure、および PingOne で機能することが確認されています。この機能はまた、カスタム設定を提供し、Microsoft SAML 2.0 に従う他の ID プロバイダでも機能するはずです。

メモ：カスタム認証は、Active Directory Federation Service（ADFS）はサポートしていません。

- **強力な認証**：マルチファクタ認証アクセスを提供します。
- **シングルサインオン**：シングルサインオン（SSO）アクセスを提供します。

  メモ：すべての構成設定は ID プロバイダ（IdP）によって処理されるため、強力な認証またはシングルサインオンはカスタム認証設定に影響しません。
- **パスワードによるログインを許可する**：このオプションを選択して、SSO を使用してコンソールに直接ログインできます。このオプションでは、コンソールからロックアウトされることなく、SSO 設定をテストできます。SSO を使用して正常にコンソールにログインできたら、この機能を無効にすることが推奨されます。
- **プロバイダ：**カスタムの認証用のサービスプロバイダを選択します。
- **X.509 証明書**：X.509 認証情報を入力します。
- **ログイン URL**：カスタム認証用の URL を入力します。

脅威データレポート

組織に関する次の情報を含むスプレッドシートです。

- **脅威**：組織内で検出されたすべての脅威をリストします。この情報には、ファイル名とファイルのステータス（危険、異常、除外済み、隔離済み）が含まれます。
- **デバイス**：組織内の Threat Defense Agent がインストールされているすべてのデバイスをリストします。この情報には、デバイス名、オペレーティングシステムバージョン、エージェントバージョン、および適用されるポリシーが含まれます。
- **脅威のインジケータ**：各脅威および関連付けられている脅威の特性がリストされます。
- **クリア**：組織でクリアされているすべてのファイルがリストされます。この情報には、除外されたファイル、安全リストに追加されたファイル、またはデバイスの隔離フォルダから削除されたファイルが含まれます。
- **イベント**：ダッシュボードには、過去 30 日間の脅威イベントグラフに関連するすべてのイベントがリストされます。この情報は、ファイルハッシュ、デバイス名、ファイルパス、およびイベントの発生日を含みます。

この機能が有効な場合、レポートは 1:00AM 太平洋標準時（PST）に自動的にアップデートされます。**レポートの再生成** をクリックして手動でアップデートを生成します。

脅威データレポートは、コンソールへのログインを必要とせずにレポートのダウンロードに使用できる URL およびトークンを提供します。トークンはまた、必要に応じて削除したり、再生成したりできます。これにより、レポートにアクセスできるユーザーを制御できます。

トラブルシューティング

本項は、Threat Defense で不具合のトラブルシューティングを行うときに回答するべき質問および収集するべきファイルのリストを提供します。この情報は、不具合を解決する際にデルサポートの支援することができます。

本項には、一般的な不具合および提案される解決策も含まれます。

サポート

インストールパラメータ

- インストール方法とは何ですか ? 使用するパラメータを指定します。
    - 例 - Windows の場合：コマンドラインからインストールして、実行時にエージェントアイコンとスタートメニューフォルダを非表示にするときは、LAUCHAPP=0 を使用します。
    - 例 - macOS の場合：コマンドラインからインストールして、エージェントで自己保護を無効にするときは、SelfProtectionLevel=1 を使用します。
- インストールのどの手順を検証できますか ?
    - 例 - Windows の場合：MSI または EXE インストーラを使用しましたか?
    - 例 - 任意の OS：コマンドラインオプションを使用しましたか? Quiet Mode または No Agent ユーザーインタフェースなど。
- インストール向けの詳細ロギングを有効にします。

パフォーマンス上の懸念事項

- Threat Defense プロセスおよびメモリ消費を示す、タスクマネージャ（Windows）またはアクティビティモニタ（macOS）のスクリーンショットをキャプチャします。
- Threat Defense プロセスのダンプをキャプチャします。
- デバッグログを収集します。

- 不具合発生時のシステム情報の出力を収集します。
    - Windows の場合：msinfo32 または winmsd
    - macOS の場合：システム情報
- 関連するイベントログ（Windows）またはコンソール情報（macOS）をすべて収集します。

アップデート、ステータス、および接続の不具合

- ポート 443 がファイアウォールで開いており、デバイスが Cylance.com サイトを解決し、これに接続できることを確認します。
- このデバイスは、コンソールの デバイス ページにリスト表示されますか？オンラインですか、オフラインですか？最終接続時刻はいつですか？
- デバイスは、インターネットへの接続にプロキシを使用していますか？資格情報はプロキシで適切に設定されていますか？
- コンソールへの接続を試行するように、Threat Defense サービスを再起動します。
- デバッグログを収集します。
- 不具合発生時のシステム情報の出力を収集します。
    - Windows の場合：msinfo32 または winmsd
    - macOS の場合：システム情報

デバッグロギングの有効化

デフォルトでは、Threat Defense はログファイルを **`C:\Program Files\Cylance\Desktop\log`** に保存します。トラブルシューティングのために、Threat Defense がより詳細なログを生成するように設定することができます。

スクリプト制御の非互換性

不具合*:*

あるデバイスでスクリプト制御が有効になっているとき、これらのデバイスで実行している他のソフトウェアとの競合が生じることがあります。この競合は、通常、他のソフトウェアによって呼び出されている特定のプロセスに挿入されているエージェントが原因です。

解決策*:*

ソフトウェアによっては、この不具合は、コンソールでデバイスポリシーに特定プロセスの除外を追加することにより解決できます。別のオプションとしては、影響を受けた各デバイスで互換モード（レジストリキー）を有効にすることが挙げられます。しかし、除外が機能しない場合、デバイスに影響するデバイスポリシーでスクリプト制御を無効にして、標準デバイス機能を復元することが推奨されます。

メモ：この互換モードのソリューションは、Agent バージョン 1370 用です。Agent 1382 以降では、インジェクションプロセスが他の製品との互換性のためにアップデートされました。

互換モード

互換モードを有効にするには、次のレジストリキーを追加します。

1. レジストリエディタを使用して、**HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop** に移動します。
2. **デスクトップ** を右クリックして、**許可** をクリックし、所有権を得て自分自身に**フルコントロール**を付与します。**OK** をクリックします。
3. **デスクトップ** を右クリックし、**新規** > **バイナリ値** の順に選択します。
4. ファイルを **CompatibilityMode** という名前にします。
5. レジストリの設定を開いて、値を **01** に変更します。
6. **OK** をクリックして、レジストリエディタを閉じます。
7. デバイスの再起動が必要な場合があります。

コマンドラインオプション

Psexec を使用する場合

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE
\Cylance\Desktop /v CompatibilityMode /t REG_BINARY /d 01
```

多数のデバイスでコマンドを実行する場合は、**Invoke-Command cmdlet** を使用します。

```
$servers = “testComp1",”testComp2",”textComp3"

$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -
ScriptBlock {New-Item -Path HKCU:\Software\Cylance\Desktop -Name
CompatibilityMode -Type REG_BINARY -Value 01}
```

付録 A：用語集

異常	マルウェアの可能性が小さい低スコア（1～59）の疑わしいファイル。
管理者	Threat Defense のテナントマネージャ。
エージェント	コンソールと通信する、Threat Defense エンドポイントホスト。
監査ログ	Threat Defense コンソールから実行されたアクションを記録するログ。

自動隔離	危険および / または異常なすべてのファイルの実行を自動的に防止します。
自動アップロード	危険または異常と検出された、不明なすべての Portable Executable（PE）を自動的に Cylance Infinity Cloud にアップロードして分析します。
コンソール	Threat Defense 管理ユーザーインタフェース。
デバイスポリシー	組織の管理者によって設定され、全デバイスでの脅威の処理方法を定めた、Threat Defense ポリシー。
グローバル隔離	グローバルに（組織内の全デバイスにわたって）ファイルの実行を阻止します。
グローバル安全リスト	グローバルに（組織内の全デバイスにわたって）ファイルの実行を許可します。
Infinity	ファイルのスコア決定に使用される数学モデル。
組織	Threat Defense サービスを使用するテナントアカウント。
隔離	ローカルに（特定のデバイス上で）ファイルの実行を阻止します。
脅威	Threat Defense に検出された悪意のある可能性のあるファイルは危険または異常のいずれかに分類されます。
危険	マルウェアの可能性が大きい高スコア（60 ～100）の疑わしいファイル。
免除	ローカルに（特定のデバイス上で）ファイルの実行を許可します。
ゾーン	優先度、機能などに従って組織内のデバイスを整理し、グループ化する方法。
ゾーン規則	IP アドレス、オペレーティングシステム、およびデバイス名に基づいてデバイスの特定ゾーンへの割り当てを自動化できる機能。

付録 B：例外の処理

ユーザーが手動でファイルを隔離または許可（除外）する必要がある場合があります。Threat Defense は、各デバイス（ローカル）、デバイスのグループ（ポリシー）、または組織全体（グローバル）の例外を処理する方法を提供します。

ファイル

ローカル：デバイス上のファイルを隔離または除外（安全リスト）します。ファイルを分析するまで一時的にブロックまたは許可することも有用です。デバイスが、ファイルの実行を許可される必要のある唯一のデバイスである場合は、デバイス上のファイルを除外することも有用です。このアクションを複数のデバイスに対して実行する必要がある場合は、デルはポリシーまたはグローバルの使用をお勧めします。

ポリシー：ポリシーに割り当てられているすべてのデバイス上のファイルを安全リストにリストします。デバイスのグループにファイルを許可する場合に便利です（たとえば、IT デバイスに PsExec など悪意のある目的で使用され得るツールの実行を許可する）。ポリシーレベルが使用できないファイルを隔離します。

グローバル：組織のファイルを隔離または安全リストにリストします。組織内の既知の悪意のあるファイルを隔離します。正常であり、組織で使用されていますが、エージェントが悪意があるとフラグを立てたファイルを安全リストにリストします。

スクリプト

ポリシー：スクリプト制御によって指定のフォルダから実行するスクリプトを承認します。フォルダに対してスクリプトの実行を許可すると、サブフォルダにあるスクリプトも許可することになります。

証明書

グローバル：コンソールに証明書を追加し、次にそれらをグローバル安全リストに追加します。これにより、この証明書の署名付きアプリケーションを組織で実行できます。

証明書を追加するには、**設定** > **証明書** の順に選択し、**証明書の追加** をクリックします。

証明書を グローバル安全リスト に追加するには、**設定** > **グローバルリスト** の順に選択し、**安全** タブ、**証明書** タブの順に選択して、**証明書の追加** をクリックします。

付録 C：ユーザー許可

ユーザーが実行できるアクションは、割り当てられたユーザー許可（ロール）によって異なります。一般に、管理者は組織内の任意の場所でアクションを実行できます。ゾーンマネージャおよびユーザーは、割り当てられたゾーンに制限されます。この制限としては、ゾーン内のデバイスにのみアクセスできること、およびこれらのデバイスに関連する脅威データのみ表示できることが挙げられます。ゾーンマネージャまたはユーザーがデバイスまたは脅威を表示できない場合、そのデバイスが割り当てられたゾーンに属していない可能性があります。

	ユーザー	ゾーンマネージャ	管理者
エージェントアップデート			
表示 / 編集			X
監査ロギング			
表示			X
デバイス			
デバイスの追加 – グローバル			X
ゾーンへのデバイスの追加			X
デバイスの削除 – グローバル			X
ゾーンからのデバイスの削除		X	X
デバイス名の編集		X	X

	ユーザー	ゾーンマネージャ	管理者
ゾーン			
ゾーンの作成			X
ゾーンの削除			X
ゾーン名の編集 – いずれか			X
割り当てられたゾーン名の編集		X	X
ポリシー			
ポリシーの作成 – グローバル			X
ゾーンのポリシーの作成			X
ポリシーの追加 – グローバル			X
ゾーンへのポリシーの追加		X	X
ポリシーの削除 – グローバル			X
ゾーンからのポリシーの削除		X	X
脅威			
ファイルの隔離 – グローバル			X
ゾーンでのファイルの隔離	X	X	X
ファイルの免除 – グローバル			X
ゾーンでのファイルの免除	X	X	X
グローバル隔離 / 安全			X
設定			
インストールトークンの生成または削除			X
招待用 URL の生成または削除			X
インストールトークンのコピー	X	X	X
招待用 URL のコピー			X
ユーザー管理			
任意のゾーンへのユーザーの割り当て			X
管理対象ゾーンへのユーザーの割り当て		X	X
ゾーンマネージャの割り当て – グローバル			X
管理対象ゾーンへのゾーンマネージャの割り当て		X	X
コンソールからのユーザーの削除			X
ゾーンからのユーザーの削除 – グローバル			X
管理対象ゾーンからのユーザーの削除		X	X

付録 D：ファイルベースの書き込みフィルタ

Dell Threat Defense Agent は、Windows Embedded Standard 7（シンクライアント）を実行しているシステムにインストールできます。内蔵されたデバイス上では、システムのストレージへの書き込みは許可されないことがあります。この場合、システムはファイルベースの書き込みフィルタ（FBWF）を使用してシステムのメモリ内のキャッシュにシステムのストレージへの書き込みをリダイレクトしている場合があります。これはエージェントが、システムが再起動されるたびに変更を失うことによって発生する問題です。

内蔵されたシステムでエージェントを使用する場合は、次の手順に従います。

1. エージェントをインストールする前に、次のコマンドを使用して FBWF を無効にします：`fbwfmgr /disable`。
2. システムを再起動します。これで FBWF が無効になります。
3. Dell Threat Defense Agent をインストールします。
4. エージェントのインストール後、次のコマンドを使用して FBWF を再び有効にします：`fbwfmgr /enable`。
5. システムを再起動します。これで FBWF が有効になります。
6. FBWF で、次のフォルダを除外します。
    a. C:\Program Files\Cylance\Desktop – このフォルダを除外するとエージェントはシステムの再起動後もアップデートを保持します。
7. 次のコマンドを使用して、デスクトップフォルダを除外します：`fbwfmgr /addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. これはデフォルトのディレクトリにインストールすることを前提にしています。エージェントをインストールしたフォルダの除外を変更します。
8. エージェントに対するテストのためにマシン上に脅威を保管する場合は、FBWF からも保管場所を除外してください（例：`C:\Samples`）。