AMP for Endpoints のクイックスタート

最終更新日：2020 年 9 月 25 日

第 1 章

概要

AMP for Endpoints（Cisco Advanced Malware Protection for Endpoints）はウイルスを検出するだけでなく、当社や他のベンダーが見過ごしたウイルスをクリーニングする機能を提供します。誤検出（FP）を防ぐための許可されたアプリケーションリスト、マルウェアの感染を管理するシンプルカスタム検出、高度で持続的な脅威を追跡および除去するために独自の検出を記述できる高度なカスタム検出を作成することができます。レポート機能では、コンピュータの一般的なセキュリティ状態を把握し、ネットワークに侵入するウイルスのソースを割り出し、ご使用の環境でのセキュリティ問題を洗い出すことができます。また、システムを縦断している一連の異なるファイル タイプを追跡し、環境におけるマルウェアの感染の影響を理解するための強力なタイムラインを提供します。

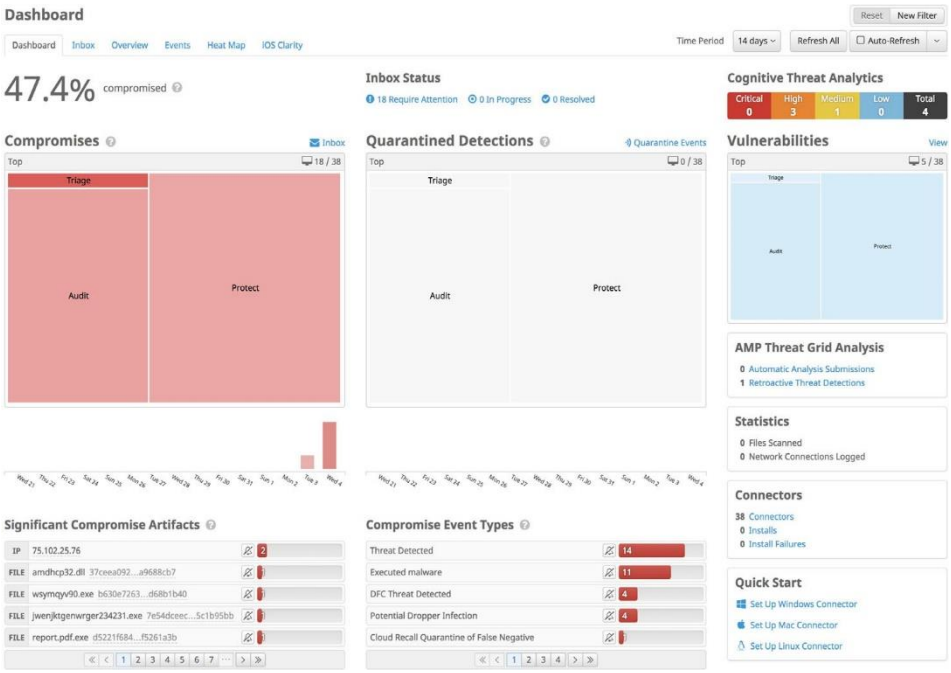
AMP for Endpoints の使用を開始するには、https://console.amp.cisco.com からログインし、コネクタをダウンロードして、ポリシーを設定する必要があります。その後、コンソールで、検疫されたファイルの復元、許可されたアプリケーションリストへの追加、シンプルカスタム検出の作成、およびコネクタのインストールをコンピュータにプッシュするなどの諸機能を試すことができます。

導入ウィザード

AMP for Endpoints コンソールに初めてログインすると、導入ウィザードが表示されます。このウィザードは、ウイルス対策製品の除外項目の作成、プロキシのセットアップ、ポリシーの設定、グループの作成など、AMP for Endpoints 環境をすばやく設定するための手順を説明します。

ダッシュボード

AMP for Endpoints ダッシュボードには、マルウェアやネットワークの脅威の検出に関する更新とともに環境内のデバイスの問題箇所の概要が表示されます。ダッシュボード ページでは、イベントにドリルダウンしてより詳細な情報を収集することによって、潜在的な侵害に対処することができます。



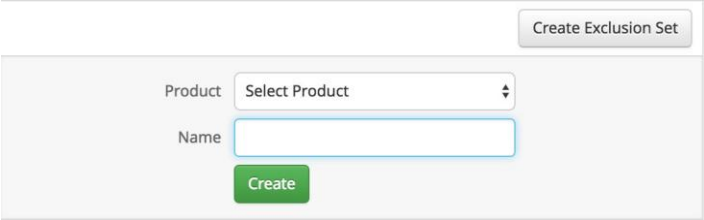
ウィルス対策製品の除外項目の作成

AMP for Endpoints Windows コネクタとウイルス対策またはその他のセキュリティソフトウェア間での競合を避けるには、コネクタがウイルス対策ソフトウェアのディレクトリをスキャンせず、かつウイルス対策ソフトウェアがコネクタのディレクトリをスキャンしないように除外項目を作成する必要があります。コネクタが悪意があるか、または検疫済みのファイルに伴う問題であると判断した文字列がウイルス対策署名に含まれている場合、問題になる可能性があります。

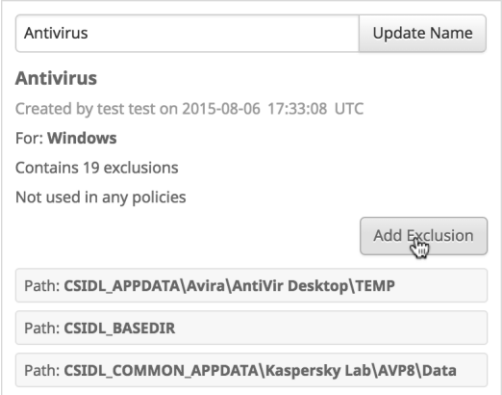
AMP for Endpoints Windows コネクタでのウイルス対策除外項目の作成

最初のステップは、AMP for Endpoints コンソールで [Management] > [Exclusions] に移動して、除外項目を作成することです。

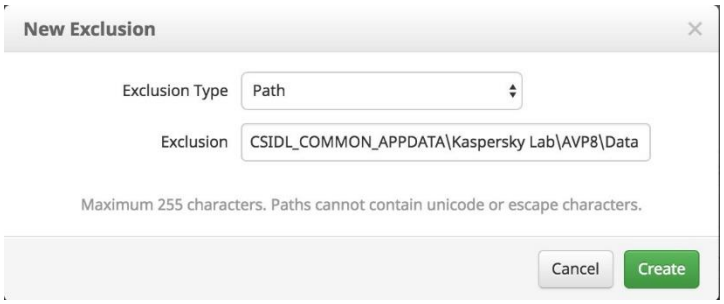
[Create Exclusion Set] をクリックして、新しい除外項目のリストを作成します。リストの名前を入力し、AMP for Endpoints Windows コネクタまたは AMP for Endpoints Mac コネクタ のどちらにするかを選択し、[Create] をクリックします。



次に、[Add Exclusion] をクリックして、除外項目をリストに追加します。



その後で、除外のパスを入力するように要求されます。エンドポイントにインストールしたセキュリティ製品の CSIDL を入力し、[Create] を作成します。



重要事項：英語以外の一部の言語では、パスの区切り文字に異なる文字が使用されている場合があります。コネクタの除外項目設定で使用できる有効なパスの区切り文字は「\」だけです。

この手順をセキュリティ アプリケーションに関連付けられたパスごとに繰り返します。共通の CSIDL には次が含まれます。

Kaspersky

- CSIDL_COMMON_APPDATA\Kaspersky Lab\AVP8\Data

McAfee VirusScan Enterprise

- CSIDL_PROGRAM_FILES\McAfee
- CSIDL_PROGRAM_FILESX86\McAfee
- CSIDL_PROGRAM_FILES\Common Files\McAfee
- CSIDL_COMMON_APPDATA\McAfee
- CSIDL_PROGRAM_FILES\VSE
- CSIDL_COMMON_APPDATA\VSE
- CSIDL_PROGRAM_FILES\Common Files\VSE

Microsoft ForeFront

- CSIDL_PROGRAM_FILES\Microsoft Forefront
- CSIDL_PROGRAM_FILESX86\Microsoft Forefont

Microsoft Security Client

- CSIDL_PROGRAM_FILES\Microsoft Security Client
- CSIDL_PROGRAM_FILESX86\Microsoft Security Client

Sophos

- CSIDL_PROGRAM_FILES\Sophos
- CSIDL_PROGRAM_FILESX86\Sophos
- CSIDL_COMMON_APPDATA\Sophos\Sophos Anti-Virus\

Splunk

- CSIDL_PROGRAM_FILES\Splunk

Symantec Endpoint Protection

- CSIDL_COMMON_APPDATA\Symantec
- CSIDL_PROGRAM_FILES\Symantec\Symantec End Point Protection
- CSIDL_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection

エンドポイントに必要な除外項目をすべて追加した後、ポリシーに除外項目設定を追加する必要があります。

重要事項：CSIDL では、大文字と小文字が区別されます。

ウイルス対策ソフトウェアでの AMP for Endpoints Windows コネクタの除外項目の作成

AMP for Endpoints コネクタでウイルス対策製品用の除外項目を作成する以外に、エンドポイント上で実行しているウイルス対策製品でも AMP for Endpoints コネクタ用の除外項目を作成する必要があります。一般的なウイルス対策製品でこれを実行する手順は次のとおりです。

McAfee ePolicy Orchestrator 4.6 での除外の作成

1. ePolicy Orchestrator にログインします。
2. メニューから [Policy] > [Policy Catalog] を選択します。
3. [Product] プルダウンから VirusScan Enterprise の適切なバージョンを選択します。
4. On-Access High-Risk Processes ポリシーを編集します。
5. [Exclusions] タブを選択して、[Add] ボタンをクリックします。
6. [By Pattern] フィールドで、AMP for Endpoints コネクタのインストール環境（デフォルトで、バージョン 5.1.1 以上の場合は C:\Program Files\Cisco、それより前のバージョンの場合は C:\Program Files\Sourcefire）へのパスを入力し、[Also exclude subfolders] ボックスをオンにします。
7. [OK] をクリックします。
8. [Save] をクリックします。
9. On-Access Low-Risk Processes ポリシーを編集します。
10. このポリシーに対してステップ 5 ～ 8 を繰り返します。

McAfee VirusScan Enterprise 8.8 での除外の作成

1. VirusScan コンソールを開きます。
2. [Task] メニューで、[On-Access Scanner Properties] を選択します。
3. 左ペインで、[All Processes] を選択します。
4. [Exclusions] タブを選択します。
5. [Exclusions] ボタンをクリックします。
6. [Set Exclusions] ダイアログで、[Add] ボタンをクリックします。
7. [Browse] ボタンをクリックして、AMP for Endpoints コネクタのインストールディレクトリ（デフォルトで、バージョン 5.1.1 以上の場合は C:\Program Files\Cisco、それより前のバージョンの場合は C:\Program Files\Sourcefire）を選択し、[Also exclude subfolders] ボックスをオンにします。
8. [OK] をクリックします。
9. [Set Exclusions] ダイアログで、[OK] をクリックします。
10. [On-Access Scanner Properties] ダイアログで [OK] をクリックします。

Managed Symantec Enterprise Protection 12.1 での除外の作成

1. Symantec Endpoint Protection Manager にログインします。
2. 左ペインで、[Policies] をクリックします。
3. [Policies] リストで、[Exceptions] エントリを選択します。
4. 新しい例外ポリシーを追加するか、既存のポリシーを編集できます。
5. ポリシーを開いたら、[Exceptions] をクリックします。
6. [Add] ボタンをクリックして、リストから [Windows Exceptions] を選択し、サブメニューから [Folder] を選択します。
7. [Add Security Risk Folder Exception] ダイアログで、[Prefix variable] ドロップダウンメニューから [PROGRAM_FILES] を選択して、[Folder] フィールドに「Cisco」を入力します。[Include subfolders] がオンになっていることを確認します。
8. このフォルダメニューを除外するスキャンのタイプを指定して、[All] を選択します。
9. [OK] をクリックします。
10. この例外が、AMP for Endpoints コネクタがインストールされている組織内のすべてのコンピュータで使用されていることを確認します。

Unmanaged Symantec Enterprise Protection 12.1 での除外の作成

1. SEP を開いて、左側のペインで [Change Settings] をクリックします。
2. [Exceptions] エントリの隣にある [Configure Settings] をクリックします。
3. [Exceptions] ダイアログで [Add] ボタンをクリックします。
4. [Security Risk Exception] サブメニューで、[Folders] を選択します。
5. ダイアログで AMP for Endpoints コネクタのインストールフォルダ（デフォルトでは、バージョン 5.1.1 以降の場合は C:\Program Files\Cisco、それより前のバージョンの場合は C:\Program Files\Sourcefire）を選択し、[OK] をクリックします。
6. [Exceptions] ダイアログで [Add] ボタンをクリックします。
7. [SONAR Exception] サブメニューで、[Folder] を選択します。
8. ダイアログで AMP for Endpoints コネクタのインストールフォルダ（デフォルトでは、バージョン 5.1.1 以降の場合は C:\Program Files\Cisco、それより前のバージョンの場合は C:\Program Files\Sourcefire）を選択し、[OK] をクリックします。
9. [Close] ボタンをクリックします。

Microsoft Security Essentials での AMP for Endpoints コネクタの除外項目の作成

1. Microsoft Security Essentials を開き、[Settings] タブをクリックします。
2. 左側のペインで、[Excluded files and locations] を選択します。
3. [Browse] ボタンをクリックして、AMP for Endpoints コネクタのインストール フォルダ（デフォルトで、バージョン 5.1.1 以上の場合は C:\Program Files\Cisco、それより前のバージョンの場合は C:\Program Files\Sourcefire）に移動して、[OK] をクリックします。
4. [Add] ボタンをクリックし、[Save changes] をクリックします。
5. 左側のペインで [Excluded processes] を選択します。
6. [Browse] ボタンをクリックして、sfc.exe ファイル（デフォルトで、バージョン 5.1.1 以上の場合は C:\Program Files\Sourcefire\FireAMP\x.x.x\sfc.exe、それより前のバージョンの場合は C:\Program Files\Sourcefire\FireAMP\x.x.x\sfc.exe。「x.x.x」は AMP for Endpoints コネクタのバージョン番号）に移動し、[OK] をクリックします。
7. [Add] ボタンをクリックし、[Save changes] をクリックします。

重要事項：Microsoft Security Essentials の除外プロセスでは sfc.exe ファイルへの具体的なパスが必要なため、AMP for Endpoints コネクタを新しいバージョンにアップグレードするたびに、この除外もアップデートする必要があります。

ポリシーの設定

ポリシーとは、AMP for Endpoints コネクタを展開するグループごとにセットアップする構成時の設定です。メニューから [Management] > [Policies] を選択して、[Policy creation and configuration] ページに移動します。

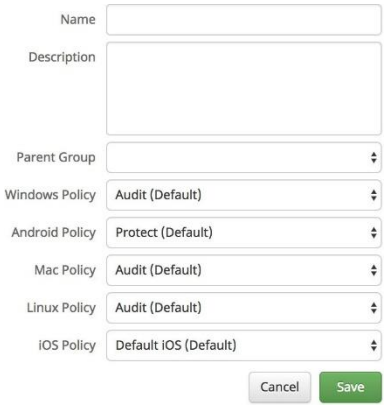
[New Policy...] をクリックして新しいポリシーを作成するか、[Duplicate] をクリックして既存のポリシーに基づいて新しいポリシーを作成します。新しいポリシーのプラットフォームを選択して [New Policy] をクリックすると、新しいポリシーを保存する前に完了しなければならない一連の設定ページが表示されます。設定を入力して [Next] をクリックし、ページを進めます。アンチウイルスの除外で作成したカスタム除外セットをこのポリシーに追加します。詳細については、オンライン マニュアルを参照してください。

構成設定を選択したら、[Save] ボタンをクリックしてポリシーを作成します。

グループの作成

ポリシーを作成した後、ポリシーが適用されるグループを作成できます。グループでは、機能、場所、または管理者が決定する他の条件によって組織のコンピュータを管理できます。

新しいグループを作成するには、[Create Group] をクリックします。グループに名前を割り当てて説明を加えた後、すでに作成済みのポリシーを割り当てます。



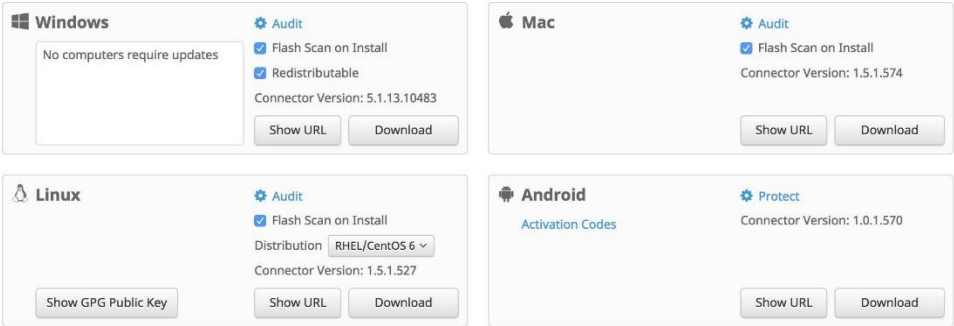
展開で必要な数のグループに対して、この手順を繰り返します。

コネクタの導入

エンドポイントに AMP for Endpoints Windows コネクタを展開するには、AMP for Endpoints コネクタインストーラを使用します。インストーラにアクセスするには、［Management］ > ［Download Connector］ に移動します。

コネクタインストーラのダウンロード

[Download the Connector] 画面が表示されます。前の手順で作成したいずれかのグループを選択し、[Download] ボタンをクリックして AMP for Endpoints Windows インストーラをダウンロードします。



重要事項：AMP for Endpoints Mac、AMP for Endpoints Linux、および AMP for Endpoints Android コネクタのインストール手順については、『AMP for Endpoints User Guide』を参照してください。

Flash Scan on Install

このチェックボックスをオンにすると、AMP for Endpoints Windows コネクタのインストールが完了してクラウドに接続された後、自動的にフラッシュスキャンが実行されます。フラッシュスキャンは、実行プロセスと関連レジストリエントリのクイックスキャンです。

再頒布

AMP for Endpoints Windows コネクタの 32 ビットおよび 64 ビットの両方のバージョンを含むインストーラをダウンロードします。このファイルは、コネクタを複数のコンピュータにインストールするために、ネットワーク共有に配置するか、System Center Configuration Manager などのツールでグループ内のすべてのコンピュータにプッシュすることができます。

インストーラオプションを選択した後、[Download] ボタンをクリックします。ファイルをローカルコンピュータまたはコネクタをインストールするコンピュータからアクセス可能なネットワーク共有に保存します。

重要事項：Microsoft System Center Configuration Manager（SCCM）を使用してコネクタ を Windows XP コンピュータに導入する場合は、追加の手順を実行する必要があります。AMP for Endpoints コネクタインストーラを右クリックして、コンテキストメニューから [Properties] を選択します。[Environment] タブで、[Allow users to interact with this program] ボックスをオンにして、[OK] をクリックします。

コネクタのインストール

コネクタをインストールするコンピュータからインストーラをダブルクリックします。独自の展開ソフトウェアがある場合、展開を自動化するためにコマンド ライン スイッチを使用することもできます。使用可能なスイッチは次のとおりです。

- /S：インストーラをサイレント モードにします。

  重要事項：これは、最初のパラメータとして指定する必要があります。

- /desktopicon 0：コネクタ用のデスクトップアイコンが作成されません。
- /desktopicon 1：コネクタ用のデスクトップアイコンが作成されます。
- /startmenu 0：[Start Menu] ショートカットが作成されません。
- /startmenu 1：[Start Menu] ショートカットが作成されます。
- /contextmenu 0：右クリックのコンテキスト メニューから [Scan Now] が無効になります。
- /contextmenu 1：右クリックのコンテキスト メニューから [Scan Now] が有効になります。
- /remove 0：コネクタはアンインストールされますが、後で再インストールできるようにファイルは残されます。
- /remove 1：コネクタがアンインストールされ、すべての関連ファイルが削除されます。
- /uninstallpassword [Connector Protection Password]：ポリシーで [Connector Protection] を有効にした場合にコネクタをアンインストールできます。このスイッチと共に [Connector Protection] のパスワードを提供する必要があります。
- /skipdfc 1：DFC ドライバのインストールが省略されます。

  重要事項：このフラグを使用してインストールされたコネクタは、[Modes and Engines] > [Network] が [Disabled] に設定されたポリシーを使用するグループに含める必要があります。

- /skiptetra 1：TETRA ドライバのインストールをスキップします。

  重要事項：このフラグを使用してインストールされたコネクタは、[Modes and Engines] > [TETRA] がオフに設定されたポリシーを使用するグループに含める必要があります。

- /D=[PATH]：インストール先ディレクトリを指定するために使用します。たとえば、/D = C:\tmp は C:\tmp にインストールします。

  重要事項：これは、最後のパラメータとして指定する必要があります。

- /overridepolicy 1：以前のコネクタのインストール環境にインストールする場合に、既存の policy.xml ファイルを置き換えます。
- /overridepolicy 0：以前のコネクタのインストール環境にインストールする場合に、既存の policy.xml ファイルを置き換えません。
- /temppath：コネクタのインストール時に作成される一時ファイルのパスを指定します。たとえば、/temppath C:\somepath\temporaryfolder のように指定します。このスイッチは、AMP for Endpoints Windows コネクタ 5.0 以降でのみ使用できます。

AMP for Endpoints Windows コネクタ 5.1.3 以降には、5.1.1 より前のバージョンから 5.1.3 以降にアップグレードする場合に、インストールディレクトリを「Sourcefire」から「Cisco」に移行することをオプトイン（またはオプトアウト）できるコマンドラインスイッチがあります。その方法を次に示します。

- /renameinstalldir 1 は、インストールディレクトリを Sourcefire から Cisco に変更します。
- /renameinstalldir 0 は、インストールディレクトリを変更しません。

重要事項：デフォルトでは、/renameinstalldir 1 が使用されます。

どのスイッチも指定せずにコマンド ライン インストーラを実行することと、/desktopicon 0 /startmenu 1 /contextmenu 1 /skipdfc 0 /skiptetra 0 は等価です。

AMP for Endpoints Windows コネクタ 6.0.5 以降には、Microsoft Security Advisory 3033929 の確認をスキップするためのコマンドラインスイッチがあります。

- /skipexprevprereqcheck 1：Microsoft Windows KB3033929 の確認をスキップします。
- /skipexprevprereqcheck 0：Microsoft Windows KB3033929 を確認します（デフォルト）。

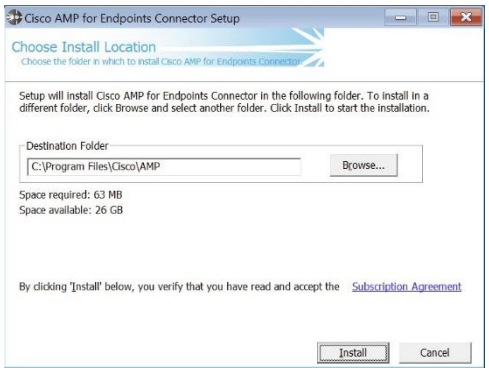
重要事項：このスイッチを使用しても、この KB、または Windows 7 および Windows Server 2008 R2 の SHA-2 コード署名サポートを有効にする Windows の更新がインストールされていない場合は、Cisco Cloud への接続に問題が発生します。

コマンドラインスイッチを使用して AMP for Endpoints コネクタをインストールする場合、終了コードも知っておく必要があります。終了コードは、%TEMP% フォルダの immpro_install.log ファイルにあります。

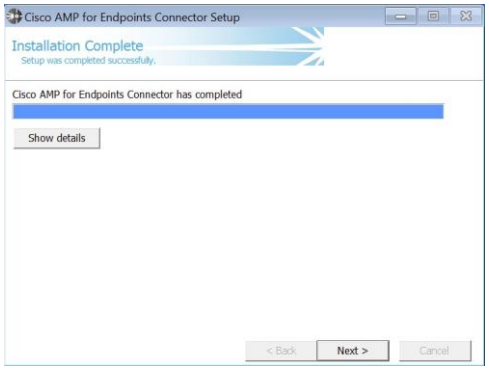
- 0：成功
- 1500：インストーラがすでに実行中
- 1618：別のインストールがすでに進行中
- 1633：サポートされていないプラットフォーム（例：64 ビットへの 32 ビット版のインストールまたはその逆）
- 1638：このバージョンまたは新しいバージョンの製品がすでに存在します。
- 1801：無効なインストール パス

- 3010：成功（リブートが必要 - アップグレードでのみ使用されます）
- 16001：試用版インストールの期限が切れています。
- 16002：インストールする前に完了している必要のあるリブートがユーザのシステム上で保留になっています。
- 16003：サポートされていないオペレーティング システム（例：XP SP2、Win2000）
- 16004：無効なユーザ権限（admin として動作しません）
- 16005：既存の AMP for Endpoints コネクタがすでに停止されているか、またはコネクタ保護が使用されていますが、パスワードが指定されていません。
- 16006：Windows コネクタと干渉する PoS OS の特定の機能（Enhanced Write Filter（EWF）または File-Based Write Filter（FBWF））が、現在有効になっています。これらの機能を無効にしてからやり直してください。PoS OS は公式にはサポートされていません。
- 16007：コネクタのアップグレードを完了するには再起動が必要ですが、[Block Reboot] オプションがポリシーに設定されています。
- 16008：コンピュータで必要な再起動が保留されているため、コネクタのアップグレードがブロックされました。
- 16009：Windows 7 および Windows Server 2008 R2 の SHA-2 コード署名サポート用のパッチがありません（KB3033929）。

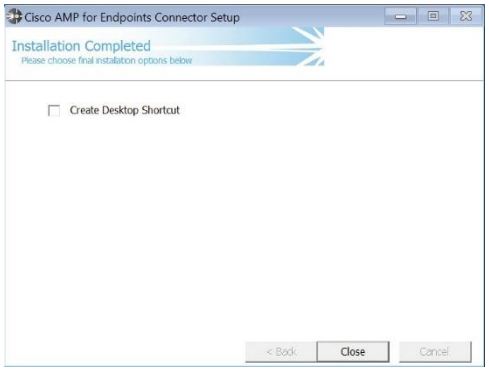
Windows User Access Control（UAC）が有効になっている場合は、プロンプトが表示されます。[Yes] をクリックして続行します。



次に、インストールの場所に関するダイアログが表示されます。ほとんどの場合、デフォルトの場所が最良の選択肢です。[Connector End User License Agreement and Privacy Policy] へのリンクも表示されます。[Install] をクリックして続行します。



インストールが完了したら、[Next] ボタンをクリックして続行します。



チェックボックスをオンのままにすると、デスクトップにコネクタのアイコンが作成されます。[Close] ボタンをクリックしてインストールを終了します。インストール時にフラッシュスキャンを実行するオプションが選択された場合は、ここでスキャンが実行されます。コネクタに適用されたポリシーで [Cloud Notifications] を選択していた場合、Windows のシステムトレイアイコンで、Cisco Cloud に接続されているかどうかも示されます。

重要事項：この時点で、AMP for Endpoints コネクタのディレクトリ用に、ウイルス対策、侵入防御など、インストール済みのすべてのセキュリティ製品でフォルダの除外が作成されているのを確認することが非常に重要です。手順については、アンチウイルス ソフトウェアのドキュメントを参照してください。逆に、すべてのセキュリティおよびバックアップアプリケーションについて、AMP for Endpoints のデフォルトポリシーにカスタム除外セットを追加して、AMP for Endpoints コネクタ内に除外を作成する必要があります。

ファイアウォール接続

AMP for Endpoints コネクタが Cisco システムと通信するには、ファイアウォールでクライアントが特定のポートから特定のサーバに接続できる必要があります。組織の所在地に応じて、3 組のサーバ（欧州向け、アジア太平洋地域、日本、および中華圏向け、その他の地域向け）から選択できます。

重要事項：ファイアウォールでの IP アドレスの例外設定が必要な場合は、この「Cisco TechNote 」を参照してください。

北米のファイアウォールの例外

北米内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベントサーバ**：intake.amp.cisco.com
- **管理サーバ**：mgmt.amp.cisco.com
- **ポリシーサーバ**：policy.amp.cisco.com
- **エラーレポート**：crash.amp.cisco.com
- **エンドポイント IOC ダウンロード**：ioc.amp.cisco.com
- **高度なカスタムシグニチャ**：custom-signatures.amp.cisco.com
- **コネクタのアップグレード**：upgrades.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.amp.cisco.com

ファイルとネットワークの分類・検索目的でシスコ クラウド サーバとの通信をコネクタに許可するには、ファイアウォール上で、クライアントから次のサーバへの TCP 443 接続を許可する必要があります。

- **クラウドホスト**：cloud-ec.amp.cisco.com

AMP for Endpoints Windows バージョン 5.0 以降の場合は、代わりに次のクラウドホストアドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウドホスト**：cloud-ec-asn.amp.cisco.com

- **登録サーバ**：cloud-ec-est.amp.cisco.com

AMP for Endpoints コネクタのいずれかで TETRA を有効にした場合は、シグニチャ更新用として TCP 80 および 443 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：tetra-defs.amp.cisco.com

AMP for Endpoints コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新用として TCP 80 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.amp.cisco.com

欧州連合のファイアウォールの例外

EU 内にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベントサーバ：**intake.eu.amp.cisco.com
- **管理サーバ：**mgmt.eu.amp.cisco.com
- **ポリシーサーバ**：policy.eu.amp.cisco.com
- **エラーレポート**：crash.eu.amp.cisco.com
- **エンドポイント IOC ダウンロード**：ioc.eu.amp.cisco.com
- **高度なカスタムシグニチャ**：custom-signatures.eu.amp.cisco.com
- **コネクタのアップグレード**：upgrades.eu.amp.cisco.com (TCP 80 and 443)
- **リモートファイル取得**：rff.eu.amp.cisco.com

ファイルおよびネットワーク ディスポジション ルックアップのためにコネクタが Cisco Cloud サーバと通信するには、クライアントが TCP 443（デフォルト）または TCP 32137 で次のサーバに接続することをファイアウォールが許可する必要があります。

- **クラウドホスト**：cloud-ec.eu.amp.cisco.com

AMP for Endpoints Windows バージョン 5.0 以降の場合は、代わりに次のクラウドホストアドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウドホスト**：cloud-ec-asn.eu.amp.cisco.com
- **登録サーバ**：cloud-ec-est.eu.amp.cisco.com

AMP for Endpoints コネクタのいずれかで TETRA を有効にした場合は、シグニチャ更新用として TCP 80 および 443 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：tetra-defs.eu.amp.cisco.com

AMP for Endpoints コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新用として TCP 80 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.eu.amp.cisco.com

アジア太平洋地域、日本、および中華圏のファイアウォールの例外

アジア太平洋地域、日本、および中華圏にある組織は、コネクタから次のサーバまでの間で HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベントサーバ**：intake.apjc.amp.cisco.com
- **管理サーバ**：mgmt.apjc.amp.cisco.com
- **ポリシーサーバ：**policy.apjc.amp.cisco.com
- **エラーレポート**：crash.apjc.amp.cisco.com
- **エンドポイント IOC ダウンロード**：ioc.apjc.amp.cisco.com
- **高度なカスタムシグニチャ**：custom-signatures.apjc.amp.cisco.com
- **コネクタのアップグレード**：upgrades.apjc.amp.cisco.com（TCP 80 および 443）
- **リモートファイル取得**：rff.apjc.amp.cisco.com

ファイルおよびネットワーク ディスポジション ルックアップのためにコネクタが Cisco Cloud サーバと通信するには、クライアントが TCP 443（デフォルト）または TCP 32137 で次のサーバに接続することをファイアウォールが許可する必要があります。

- **クラウドホスト**：cloud-ec.apjc.amp.cisco.com

AMP for Endpoints Windows バージョン 5.0 以降の場合は、代わりに次のクラウドホストアドレスおよび登録サーバ（両方とも TCP 443）を使用する必要があります。

- **クラウドホスト**：cloud-ec-asn.apjc.amp.cisco.com
- **登録サーバ**：cloud-ec-est.apjc.amp.cisco.com

AMP for Endpoints コネクタのいずれかで TETRA を有効にした場合は、シグニチャ更新用として TCP 80 および 443 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：tetra-defs.apjc.amp.cisco.com

AMP for Endpoints コネクタのいずれかで ClamAV を有効にした場合は、シグニチャ更新用として TCP 80 経由での次のサーバへのアクセスを許可する必要があります。

- **更新サーバ**：clam-defs.apjc.amp.cisco.com

プロキシ

コネクタでは、複数のメカニズムを使ってプロキシサーバをサポートできます。特定のプロキシサーバまたはプロキシ自動設定（PAC）ファイルへのパスをポリシーで定義することも、コネクタが Windows レジストリからエンドポイントプロキシ設定を検出することもできます。

AMP for Endpoints コネクタは、エンドポイントプロキシ設定を自動的に検出するように設定できます。コネクタはプロキシ設定情報を検出すると、AMP for Endpoints 管理サーバに接続にして、プロキシサーバの設定が正しいことを確認しようとします。コネクタは、ポリシーで指定されたプロキシ設定を最初に使用します。コネクタが sourcefire.com への接続を確立することができなかった場合、エンドポイントの Windows レジストリからプロキ

シ設定を取得しようとします。コネクタは、ユーザ単位の設定ではなく、システム全体の設定からのみ設定を取得します。

コネクタは、Windows レジストリからプロキシ設定を取得できない場合、プロキシ自動設定（PAC）ファイルを検索します。この動作は、ポリシー設定で指定することも、Web プロキシ自動検出プロトコル（WPAD）を使用して決定することもできます。ポリシーで PAC ファイルの場所が指定されている場合、http または https で始まる必要があります。サポートされる PAC ファイルは、ECMAScript ベースのみであることに注意してください。すべてのコネクタの通信はすでに暗号化されているため、https プロキシはサポートされていません。コネクタのバージョン 3.0.6 では、PAC ファイルを使用して SOCKS プロキシ設定を指定できません。

クラウド検索に一定回数失敗すると、コネクタはプロキシ設定を再検出します。これは、ラップトップがエンタープライズ ネットワークの外部に存在する場合に、ネットワークプロキシ設定が変更されてもコネクタが接続できるようにするためです。

第 2 章

AMP FOR ENDPOINTS の詳細

前章ではポリシーを設定して、コネクタをインストールしました。次は、AMP for Endpoints の他の機能について取り上げます。

コンソール メニュー

最上部のメニュー バーは、インストールの総数と過去 7 日間のマルウェアの検出数を示します。ページの最上部には、現在のシステム アナウンスの数とともに、1 つ前のアナウンスを表示するリンクも表示されます。メニュー項目は、後述するように、ダッシュボード、分析、感染管理、レポート、管理、およびアカウントに誘導します。また、サポートに連絡するためのリンク、ヘルプ システム、およびセッションを終了するためのログアウトリンクもあります。[My Account] リンクをクリックすると、自分のアカウントの [Users] ページに直接移動するため、変更を加えることができます。

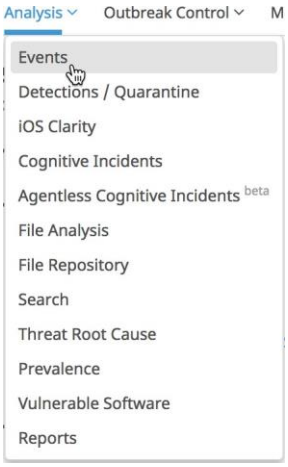
メニューバーの検索ボックスを使用して、任意のページから検索を実行できます。さらに、ダッシュボードの [Overview] タブ、[Heat Map] タブ、[Threat Root Cause] ページ、および [Deployment Summary] ページにはさらに詳細なビューを提供するグローバル グループ フィルタもあります。

- [Dashboard]：悪意のあるファイルの検出と AMP for Endpoints コネクタの展開内で実行されている検疫に関する最新の情報を提供します。
- [Analysis]：このメニューにはご使用の環境における脅威の分析に関連した項目が含まれます。

- [Outbreak Control]：このセクションでは、管理者が AMP for Endpoints 展開内で発生した悪意のあるファイルの感染に対処するために必要なツールを提供します。
- [Reports]：データに基づいた PDF レポートを作成できます。
- [Management]：このメニューには、AMP for Endpoints コネクタを管理するための項目が含まれます。
- [Accounts]：このセクションでは、AMP for Endpoints Web インターフェイスにアクセスできるユーザを管理します。

Event

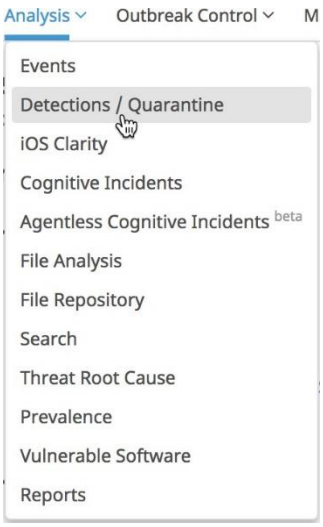
イベントとは、AMP for Endpoints 展開内でトラッキングおよび記録されているすべてのアクティビティを指します。検出、検疫、およびソフトウェアのインストールなどの情報は、ここに表示することができます。この情報は、システム内に存在する大部分のレポート機能の基盤となっています。イベントにフィルタを適用してビューを絞り込むことができます。



メニューから [Analysis] > [Events] を選択すると、[Event View] ページが表示されます。

検出/検疫

検出および検疫は、ご使用の展開内で悪意のあるファイルが検出されるたびにトラッキングを行う特定のタイプのイベントです。また、悪意のあるファイルの検疫が成功したか失敗したかを表示します。リストにフィルタを適用してビューを絞り込むことができます。



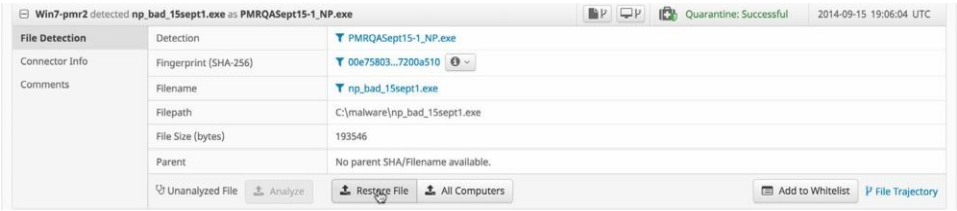
メニューから [Analysis] > [Detections/Quarantine] を選択すると、[Detections and Quarantine Events] ページが表示されます。

検疫からファイルを復元する

悪意のあるファイルの検出および検疫が行われたときに、誤検出であれば、ファイルを復元する必要があります。これは、AMP for Endpoints Web インターフェイスからのみ実行できます。

次に、イベントの例を示します。

イベントをクリックすると、検疫されたファイルの詳細が示されます。



イベントで示されたコンピュータのファイルを復元するには、イベントエントリの [Restore File] をクリックします。そのファイルを検疫したすべてのコンピュータでそのファイルを復元するには、[Restore File on all Computers] をクリックします。ファイルは 30 日間隔離保管され、その後は復元できません。

重要事項：復元要求を送信してからファイルが実際にコンピュータに復元されるまでに、最大で 30 分の時間差があります。

感染管理

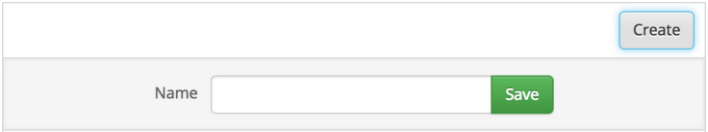
AMP for Endpoints には、アウトブレイクコントロールに分類される、ニーズに合わせてカスタマイズ可能な多様なリストがあります。主なリストには、シンプルカスタム検出、アプリケーションブロック、許可されたアプリケーションリスト、高度なカスタム検出、IP ブロック/許可リストなどがあります。

アプリケーション制御：許可されたアプリケーション

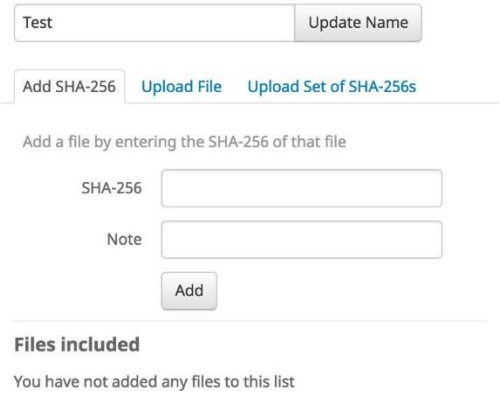
アプリケーションリストは、AMP for Endpoints システムが安全または悪意がないと想定するように指示されている、ユーザ定義のファイルリストです。

[Outbreak Control] > [Allowed Applications] を選択すると、リストの作成と設定を行う画面が表示されます。

許可されたアプリケーションリストを作成するには、下記の [Create] ボタンをクリックし、[Name] に名前の情報を入力して、[Save] をクリックします。



リストを構成するには、[Edit] をクリックします。下記のオプションでは、リストの設定の選択肢が示されています。



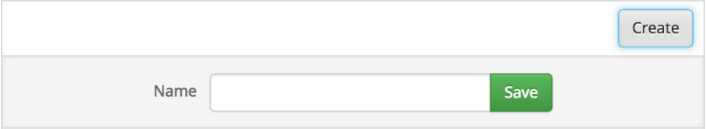
許可するコンピュータ上のファイルのベースラインを作成するには、 sha256deep などのアプリケーションを使用してハッシュをファイルに書き出し、そのファイルをアップロードすることができます。推奨される使用方法：

```
sha2563deep.exe -q -s -r -oe c:\*.*
```

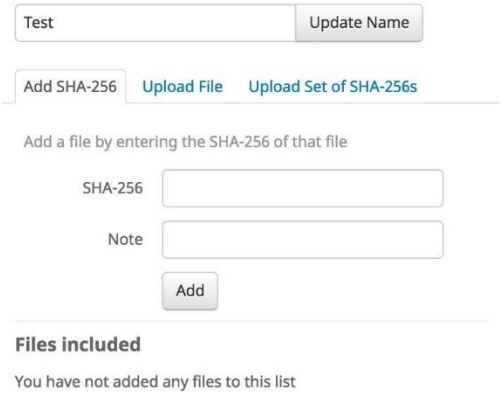
カスタム検出：簡易

シンプルカスタム検出リストはブロックリストと同じです。これらは、ユーザによって検疫が求められているファイルです。シンプルカスタム検出のエントリは、今後新しく作成されるファイルを検疫するだけでなく、レトロスペクティブ機能を通じて、サービスがすでに検出した PC のファイルも検疫します。

簡易カスタム検出リストを作成するには、[Outbreak Control] > [Simple] に移動します。[Create] をクリックして新しいシンプルカスタム検出を作成し、名前を付けて、[Save] をクリックします。



検出をリストに追加するには [Edit] をクリックします。下記のオプションでは、シンプルカスタム検出の設定の選択肢が示されています。



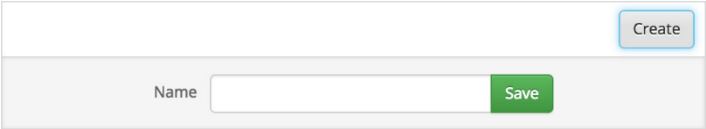
カスタム検出：高度

高度なカスタム検出は、従来型のウイルス対策シグニチャに類似していますが、ユーザにより作成される点が異なります。これらのシグネチャは、ファイルのさまざまな側面を検査し、異なるシグネチャの形式を使用できます。使用可能なシグニチャの形式の一部を以下に示します。

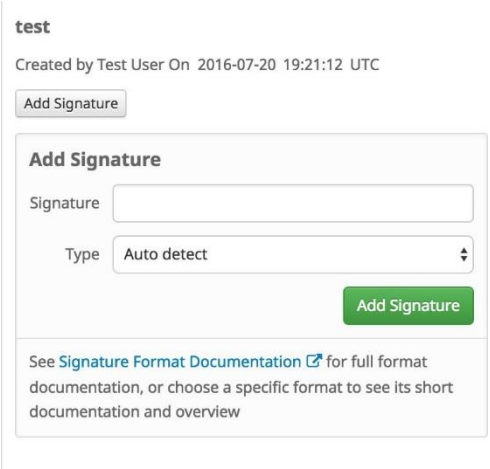
- MD5 シグニチャ
- MD5、PE セクション ベースのシグニチャ
- ファイル本文ベースのシグニチャ
- 拡張シグニチャ形式（オフセット、ワイルドカード、正規表現）
- 論理的シグニチャ
- アイコン シグニチャ

シグネチャの形式の詳細については、http://www.clamav.net/doc/latest/signatures.pdf を参照してください。これらのシグネチャは、エンドポイントにダウンロードできるファイルにコンパイルされています。

高度なカスタム検出を作成するには、[Outbreak Control] > [Advanced] に移動します。そこから [Create Signature Set] をクリックして高度なカスタム検出セットを新規作成し、名前を付けた後、[Create] をクリックします。



高度なカスタム検出セットを作成してから、[Edit] をクリックすると、[Add a signature] リンクが表示されます。シグネチャの名前を入力した後、[Create] をクリックします。



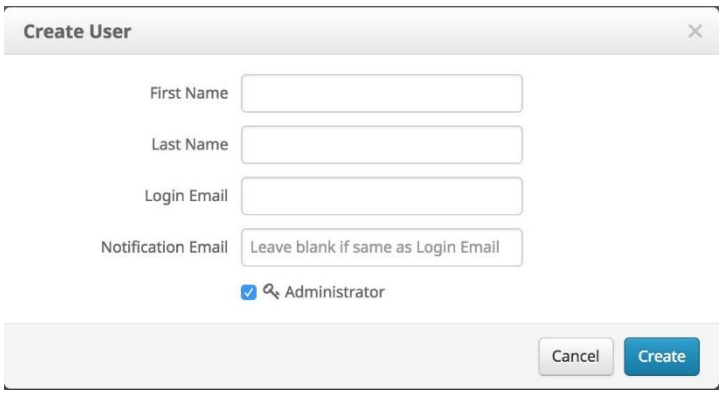
すべてのシグネチャがリストされていれば、[Build a Database from Signature Set] を選択します。不要なシグネチャを誤って追加した場合、[Remove] をクリックして削除できます。

重要事項：シグネチャを追加するか削除した場合は、必ず [Build a Database from Signature Set] をクリックする必要があります。

追加のユーザ アカウントの作成

[Users] 画面では、アカウントを管理し、そのアカウントの通知やサブスクリプションを表示するだけでなく、追加のユーザ アカウントを作成できます。新しいユーザを作成するには、メニューから [Accounts] > [Users] に移動します。

[New User] をクリックして、AMP for Endpoints コンソールの新しいユーザアカウントを作成します。アカウント アクティベーション電子メールを受信するために、有効な電子メール アドレスが必要です。たとえば、作成されるすべての通知を配布リストに送信する場合は、通知を受信するための別の電子メール アドレスを追加することもできます。ユーザを管理者にするか、非特権ユーザにするかを決定する必要もあります。管理者には、組織内のすべてのグループに対するフル コントロールが付与されます。[Administrator] ボックスをオフにすると、そのユーザは自分のグループに関するデータしか表示できなくなります。後からアカウントを編集することによって、ユーザの特権とグループ アクセス権を変更できます。



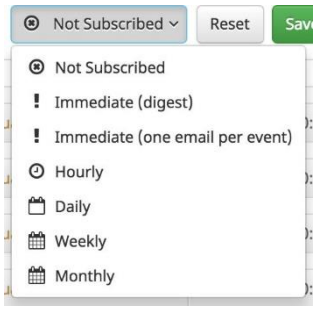
新しいユーザに、アクティベーション用電子メールが送信されます。メールには、クリックしてアカウントのアクティベーションとパスワードのセットアップを行うためのリンクが記載されています。

フィルタおよびサブスクリプション

フィルタは、[Events] タブの最上部に表示されます。右側にあるドロップダウンから過去に保存されたフィルタを選択することも、既存のイベントからのイベントタイプ、グループ、または特定のフィルタを追加することもできます。フィルタ基準を削除するには、削除する項目の横にある [x] をクリックします。[Events] リストは、ドロップダウンリストからの基準に基づいて昇順または降順にソートすることもできます。すべてのフィルタ基準を削除するには [Reset] ボタンをクリックします。現在のフィルタ処理されたビューを保存するには [Save Filter As] ボタンをクリックします。

保存されたフィルタを表示中に、フィルタを更新して [Save New] をクリックし、変更を新しいフィルタとして保存したり、[Update] をクリックして既存のフィルタを上書きしたりできます。

フィルタ ビューをサブスクライブするには、[Not Subscribed] ボタンをクリックして、サブスクリプション タイミング オプション付きのメニューを表示します。イベントは、即時、毎時、毎日、毎週、または毎月の通知でサブスクライブできます。



通知頻度を選択したら、[Update] をクリックして設定を保存します。フィルタ ビューの通知を受け取る必要がなくなった場合、通知の頻度を [Not Subscribed] に切り替えて、[Update] をクリックします。

デモ データ

デモデータを使用すれば、実際のマルウェア感染から再現されたデータをコンソールで読み込んで AMP for Endpoints の動作を確認できます。これは、製品を評価し、コンピュータを感染させることなくその機能を実証するのに役立ちます。

デモデータを有効にすると、AMP for Endpoints コンソールにコンピュータとイベントが追加され、マルウェアが検出されたときのダッシュボード、ファイルトラジェクトリ、デバイストラジェクトリ、脅威の根本原因、検出、およびイベントの動作を確認できます。デモデータは、AMP for Endpoints 展開からのライブデータと共存できますが、デモデータに重大度の高いマルウェアがある場合に、特定のビュー（ダッシュボードの侵害の兆候ウィジェットなど）で本物のイベントがわかりにくくなる可能性があります。

デモデータをコンソールに読み込ませるには、[Enable Demo Data] をクリックします。

デモデータが有効になっている場合は、[Disable Demo Data] をクリックすることによって再度削除することができます。

[Refresh Demo Data] はデモデータの有効化と同様です。デモ データが有効になっている場合、リフレッシュすると、すべてのイベントがリフレッシュされて現在の日のイベントに表示されます。

付録 A

脅威の説明

AMP for Endpoints には、独自のネットワーク検出イベントタイプと侵害の兆候が定義されています。ここでは、これらの検出タイプについて説明します。

重要事項：脅威名の説明については、AMP 命名規則を参照してください。

Indications of Compromise

AMP for Endpoints は、過去 7 日間にわたって観察されたイベントに基づく Indications of Compromise を使用してデバイスを評価します。悪意のあるファイルの検出、悪意のあるファイルを繰り返しダウンロードしている親ファイル（ドロッパー感染の可能性）、悪意あるファイルをダウンロードしている複数の親ファイル（複数の感染したファイル）などのイベントはすべて寄与因子です。Indications of Compromise には以下が含まれます。

- 脅威の検出：コンピュータ上で 1 つ以上のマルウェアの検出がトリガーされました。
- ドロッパー感染の可能性：ドロッパー感染の可能性は、1 つのファイルが繰り返しコンピュータにマルウェアをダウンロードしようとしていることを示しています。
- 複数の感染したファイル：複数の感染したファイルは、コンピュータ上の複数のファイルがマルウェアをダウンロードしようとしていることを示しています。
- 実行されたマルウェア：既知のマルウェア サンプルがコンピュータ上で実行されました。この場合は、マルウェアがペイロードを実行した可能性があるため、単純な脅威検出より深刻です。
- 疑わしいボットネット接続：コンピュータが疑わしいボットネット コマンドと制御システムへの外部接続を確立しました。

- [Application] 侵害：疑わしいポータブル実行可能ファイルが Adobe Reader Compromise などの名前のアプリケーションによってダウンロードされ、実行されました。
- [Application] によるシェルの起動：指定されたアプリケーションが不明なアプリケーションを実行し、コマンド シェルが起動されました。Java によるシェルの起動など。
- 汎用 IOC：コンピュータが侵害された可能性を示す疑わしい動作です。
- 疑わしいダウンロード：疑わしい URL から実行ファイルをダウンロードしようとしました。ただし、必ずしも URL やファイルに悪意がある（またはエンドポイントが侵害されている）とは限りません。動作の原因を理解するために、ダウンロードの背景やダウンロードしようとしたアプリケーションを詳細に調査する必要があります。
- Cscript の疑わしい起動：Internet Explorer がコマンド プロンプトを起動し、それによって cscript.exe（Windows Script Host）が実行されました。このイベントのシーケンスは一般的に、ブラウザ サンドボックス エスケープの結果として悪意のある Visual Basic スクリプトが実行されたことを意味しています。
- 疑わしいランサムウェア：既知のランサムウェアに関連付けられた特定のパターンを含むファイル名がコンピュータで確認されました。たとえば、help_decrypt.<filename> という名前のファイルがみつかりました。
- 考えられる webshell：IIS ワーカー プロセス（w3wp）が、powershell.exe などの別のプロセスを起動しました。これは、コンピュータがセキュリティ侵害を受けており、攻撃者へのリモート アクセスが許可されたことを示唆する可能性があります。
- コグニティブ脅威：Cisco Cognitive Threat Analytics は高度なアルゴリズム、機械学習、および人工知能を使用して、ユーザおよびネットワークデバイスによって生成されたネットワークトラフィックを関連付けます。これにより、コマンドアンドコントロール トラフィック、データ漏えい、および悪意のあるアプリケーションを識別します。Cognitive Threat Indication of Compromise イベントは、疑わしいまたは異常なトラフィックが組織内で検出された場合に生成されます。CTA により重大度 7 以上を割り当てられた脅威のみが AMP for Endpoints に送信されます。

重要事項：正規のアプリケーションのアクティビティが Indication of Compromise をトリガーする場合があります。正規のアプリケーションは検疫またはブロックされませんが、今後侵害の兆候がトリガーされるのを防ぐために、アプリケーションを [Application Control] > [Allowed Applications] に追加してください。

DFC 検出

デバイス フロー コリレーション（DFC）を使用すると、疑わしいネットワークアクティビティにフラグを立てたり、ブロックしたりできます。ポリシーを使用すると、疑わしい接続が検出されたときの AMP for Endpoints コネクタの動作に加え、コネクタがアドレスを使

用すべき場所（Cisco Intelligence Feed、作成したカスタム IP リスト、または両方の組み合わせ）を指定できます。DFC 検出には以下が含まれます。

- DFC.CustomIPList：コンピュータが、DFC IP ブロックリストで定義された IP アドレスへの接続を確立しました。
- Infected.Bothost.LowRisk：コンピュータが、ボットネットへの既知の参加者であるコンピュータに属していると見られる IP アドレスへの接続を確立しました。
- CnC.Host.MediumRisk：コンピュータが、過去にボット コマンドと制御チャネルとして使用されたことがわかっている IP アドレスへの接続を確立しました。このコンピュータのデバイス トラジェクトリをチェックして、このホストからファイルがダウンロードされ、その後実行されたかどうかを確認してください。
- ZeroAccess.CnC.HighRisk：コンピュータが、既知の ZeroAccess コマンドと制御チャネルへの接続を確立しました。
- Zbot.P2PCnC.HighRisk：コンピュータが、そのピアツーピア コマンドと制御チャネルを使用して既知の Zbot ピアへの接続を確立しました。
- Phishing.Hoster.MediumRisk：コンピュータが、フィッシング サイトをホストしている可能性のある IP アドレスへの接続を確立しました。コンピュータ フィッシング サイトの多くは他の Web サイトもホストしており、このような無害なサイトのいずれかに接続された可能性もあります。

重要事項：DFC は、VPN などのネットワークトンネリングを行うアプリケーションには対応していません。

付録 B
補助ドキュメント

ダウンロード可能な補助ドキュメントは次のとおりです。

Cisco AMP for Endpoints ユーザガイド

次のリンクから、ユーザ ガイドの最新バージョンをダウンロードできます。

ユーザ ガイドをダウンロードする

Cisco AMP for Endpoints クイック スタート ガイド

このガイドでは、グループ、ポリシー、および除外のセットアップ方法と AMP for Endpoints コネクタの展開方法について説明します。このガイドは、AMP for Endpoints の評価に役立ちます。

クイック スタート ガイドをダウンロードする

Cisco AMP for Endpoints 展開戦略ガイド

このガイドでは、AMP for Endpoints の本番展開に向けた準備と計画の詳細に加えて、ベストプラクティスとトラブルシューティングのヒントについて説明します。

導入戦略ガイドをダウンロードする

Cisco AMP for Endpoints サポート ドキュメンテーション

AMP for Endpoints の設定、保守、トラブルシューティングに関する TechNotes です。

サポート ドキュメンテーション

Cisco エンドポイント IOC 属性

Endpoint IOC の属性に関するドキュメントには、AMP for Endpoints コネクタに搭載された Endpoint IOC スキャナでサポートされる IOC の属性が詳しく説明されています。AMP for Endpoints コンソールにアップロードできるサンプルの IOC ドキュメントも含まれています。

エンドポイント IOC 属性をダウンロードする

Cisco AMP for Endpoints API のドキュメンテーション

API を使用すると、コンソールにログインしなくても、AMP for Endpoints データおよびイベントにアクセスできます。マニュアルは、使用可能なインターフェイス、パラメータ、および例について説明しています。

API マニュアルを参照する

Cisco AMP for Endpoints リリース ノート

このリリースノートには AMP for Endpoints の変更ログが含まれています。

リリース ノートをダウンロードする

デモンストレーション データ提案エンドポイント向け Cisco AMP

デモデータストーリーでは、AMP for Endpoints でデモデータが有効になっている場合に表示される一部の例について説明します。

SFEICAR ドキュメントをダウンロードする

ZAccess ドキュメントをダウンロードする

ZBot ドキュメントを ダウンロードする

CozyDuke ドキュメントを ダウンロードする

Upatre ドキュメントを ダウンロードする

PlugX ドキュメントを ダウンロードする

Cryptowall ドキュメントを ダウンロードする

Low Prevalence Executable ドキュメントをダウンロードする

コマンドラインのキャプチャに関するドキュメントをダウンロードする

Cognitive Threat Analytics（CTA）のドキュメントをダウンロードする

WannaCry ランサムウェアのドキュメントをダウンロードする

FriedEx ドキュメントをダウンロードする

付録 B

シスコユニバーサルクラウド契約

クラウドオファーの利用規約