Secure Endpoint

ベストプラクティスガイド

バージョン 2.4

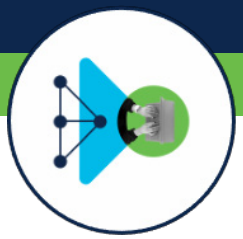
作成者：Secure Endpoint TME

対象者：初級者、専門職

リリース日：2021 年 6 月 11 日

テクニカルガイド

Cisco public



このドキュメントについて

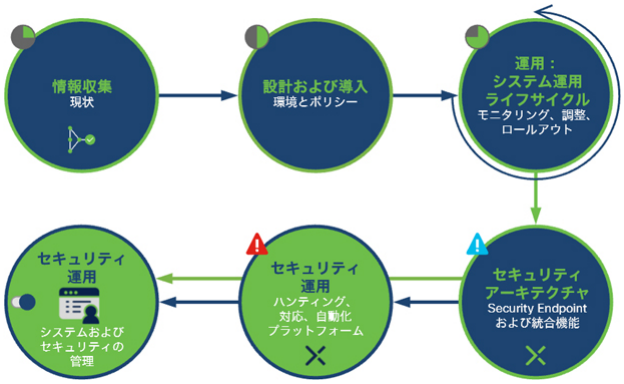
Cisco Secure Endpoint（旧 AMP for Endpoints）は、包括的なエンドポイント セキュリティ ソリューションです。スタンドアロンの Endpoint Detection & Response（EDR）製品として、また、Cisco SecureX EDR/XDR Architecture® の重要なコンポーネントとして機能するように設計されています。お客様やパートナーは、自社環境に Secure Endpoint を導入して設定する前に、多くのことを考慮する必要があります。このドキュメントの目的は、導入、セットアップ、設定のベストプラクティスに関するガイドを示すことです。

注：ベストプラクティスガイドは、既存の製品ドキュメントを補足するものとして設計されているため、すべての Secure Endpoint 設定オプションを取り上げているわけではありません。詳細な製品設定については、他の公式 Secure Endpoint ドキュメント（https://docs.amp.cisco.com/）を参照してください。

このドキュメントでは、Cisco Secure Endpoint を正しく導入するための推奨手順について説明します。このドキュメントのフローチャートは、汎用的なフレームワークとして、さまざまなお客様環境で利用できます。

以下の内容が含まれています。

- **情報収集：**環境に関する必要な情報を収集する。
- **設計および導入：**ポリシーおよびロールアウト計画を策定する。
- **運用ライフサイクル：**日々の製品運用、ポリシー適用、エンドポイントの更新/アップグレードを実施する。
- **セキュリティアーキテクチャ：**付属のハンティングツール（SecureX Threat Response、Real Time Endpoint Search など）を有効にする、Ribbon アプリを含む SecureX を有効にする、Pivot Menu を理解し、サードパーティの脅威情報を追加する、Secure Endpoint 製品に含まれる感染後タスク/機能を有効にする。
- **セキュリティ運用：**SecureX Orchestration を有効にし、セキュリティ運用を自動化/オーケストレーションする、既存のセキュリティアーキテクチャを統合して強化し、現在の SOC 環境に組み込む。



企業全体に導入する場合は、情報収集から統合設定まで、これらのステップを段階的に進めることを推奨します。継続的にレビューして改善していくことは、Secure Endpoint の導入を成功させるために不可欠です。

そうすることで、円滑に導入して正確に設定を調整し、パフォーマンス問題が顕在化する前にタイムリーに解決できます。お客様の環境はそれぞれ異なっているため、このフレームワークは推奨例としてのみ利用し、お客様の状況に応じて調整してください。

目次

情報収集 5

概要 5

環境情報 5

セキュリティ製品情報 5

監査およびコンプライアンス 6

準備 7

概要 7

設計と導入の計画 7

クラウド インフラストラクチャ - 機能とサービス 7

クラウド インフラストラクチャ – バックエンド インテリジェンス 8

クラウド インフラストラクチャ - エンドポイント接続 8

- クラウドとの通信 8
- クラウド通信：プロキシ環境 8
- クラウド通信：必要な帯域幅 8

オンプレミスコンポーネント 9

- Secure Endpoint アップデートサーバー 9

Endpoint Connector の基本的な設計 9

- ファイルスキャンシーケンス 10
- サポートされているオペレーティングシステム 11
- Windows Security Center の統合 11
- Windows Defender 11
- 競合製品 11

エンドポイントのグルーピング 11

ポリシーの設定計画 12

- ポリシーの設定計画 - ファイルスキャン 12
- ポリシーの設定計画 - ファイルスキャンの除外 12
- ポリシーの設定計画 - ネットワークモニタリング 12
- ポリシーの設定計画 - 保護エンジン 13
- ポリシーの設定計画 - Cisco Advanced Search（Orbital） 13

準備チェックリスト 13

Secure Endpoint - Console のセットアップ 14

ユーザーアカウントの設定 14

- 二要素認証 14
- SecureX プラットフォームと SecureX SSO を有効にする 15

Console セットアップのチェックリスト 15

ポリシーの設計および管理 - パフォーマンスとセキュリティ 16

ポリシーオブジェクト 16

ポリシー設定：最適なパフォーマンスとセキュリティ 17

- ポリシー設定：モードおよびエンジン 17
- ポリシー設定：除外リストの定義と管理 18
- ポリシー設定：除外リストとセキュリティ 18
- ポリシー設定：プロキシ 18
- ポリシー設定：Connector のパスワード（自己保護） 19
- ポリシー設定：ファイルとプロセスのスキャン 19
- ポリシー設定：キャッシュ 19
- ポリシー設定：ファイルスキャン - アーカイブファイルとパックファイルの違い 19

ポリシー設定：ワークステーション 20

ポリシー設定：サーバー 21

ポリシーセットアップのサマリー 22

Secure Endpoint のインストール、更新、運用ライフサイクル 23

Secure Endpoint：ソフトウェアのロールアウト 23

- 事前準備：簡易サマリー 23

Secure Endpoint のロールアウトに関するベストプラクティス ... 23
フェーズ 1：ラボ環境 - テストとロールアウト ... 24
フェーズ 2：ゴールドユーザーグループ ... 25
フェーズ 3：導入の準備 ... 25
フェーズ 4：ロールアウト ... 25
Secure Endpoint：運用ライフサイクル ... 26
インストールのテスト ... 26
新たなエンジンと機能 ... 26
カスタム除外リスト ... 26
Secure Endpoint：トラブルシューティング ... 26
ヘルスチェックツール ... 27
接続テストツール ... 27
Secure Endpoint 診断バンドルの分析 - Windows および macOS で CPU 使用率が高い場合 ... 27
エクスプロイト防止機能で保護されたプロセス ... 27
SecureX – EDR/XDR/MDR アーキテクチャ ... 28
Secure Endpoint：自動アクション ... 28
感染後自動アクション：コンピュータをグループに移動する ... 28
感染後自動アクション：エンドポイントをネットワークから分離する ... 28
Secure Endpoint：ファイル分析 ... 28
SecureX：統合モジュール ... 28
SecureX：Pivot Menu ... 29
SecureX：Threat Response ... 29
SecureX：Ribbon ... 29
付録 A：Secure Endpoint プライベートクラウド ... 30
考慮事項：パブリッククラウドとプライベート クラウド アプライアンスの違い ... 30
詳細：パブリッククラウドとプライベートクラウドの比較 ... 31
付録 B：仮想環境（VDI） ... 32
概要 - VDI とマルチユーザー環境 ... 32
エンドポイント仮想化とアプリケーション仮想化の比較 ... 32
VDI およびマルチユーザー環境に Secure Endpoint をインストールする ... 33
アイデンティティ永続化 ... 33
アイデンティティ永続化の設定 ... 33
Endpoint トレイアイコン ... 33
除外と機能の無効化 ... 34
ネイティブハイパーバイザの統合と Secure Endpoint ... 35
統合：ハイパーバイザごとのスキャン（VMware など） ... 37
統合：スキャン専用ノード（Hyper-V、Citrix、OpenStack など）によるスキャン ... 37
仮想環境でのオンデマンド/IOC スキャン ... 38
Microsoft Windows Terminal Server の推奨設定 ... 38
Microsoft Hyper-V の推奨設定 ... 39
VDI チェックリスト/サマリー ... 40
付録 C：/skiptetra を指定した後に Tetra を手動で追加 ... 41
手動で Tetra をエンドポイントに追加する ... 41
レジストリのキー値を生成するバッチファイル ... 41
付録 D：サードパーティ製品と Secure Endpoint の統合 ... 42
API コードによる Secure Endpoint の統合例 ... 42
GitHub の Cisco Security – サンプル統合コード ... 42
付録 E：除外リストの詳細 ... 43

情報収集

概要

情報収集は、Secure Endpoint を円滑に導入して設定するために、最初にすべきことです。このセクションでは、環境およびセキュリティ製品に関するデータやコンプライアンス要件を収集する際に重要な考慮事項について説明します。

- エンドポイントのオペレーティングシステム（Windows/Linux/macOS）
- エンドポイントの数
- 既存のセキュリティ製品とアーキテクチャ
- ソフトウェア導入プロセス
- カスタムアプリケーション
- プロキシの利用状況
- エンドポイントの接続情報（プロキシの要/不要、リモート（VPN）かローカルファイアウォールか）
- プライバシー要件

環境情報

最初のステップは、既存のセキュリティ態勢を把握して文書化することです。これには、既存の環境に関する情報を収集することも含まれます。すべて網羅されているわけではありませんが、次の点を確認することから始めるとよいでしょう。

- 保護する必要があるエンドポイントの数
- 導入されているオペレーティングシステムとアーキテクチャ
- Secure Endpoint をインストールするエンドポイントに、既存の EDR ソフトウェアは導入されているか
    - 導入されている場合、Secure Endpoint のインストール前後に削除するか
    - それとも、既存の EDR ソフトウェアと共存させるのか
- ミッションクリティカルなエンドポイントとソフトウェアはどれか
- ソフトウェアはエンドポイントにどのように配信されるか
- エンドポイントはアプリケーション/サービスとどのように接続されるか
- エンドポイントはプロキシを利用しているか
- エンドポイントは VPN 経由でローミングまたは接続しているか
- エンドポイントで使用されるソフトウェアのインベントリはあるか
- 必要なエンドポイントを含んだテスト用のラボ環境はあるか
- LAN/WAN リンクの帯域幅またはポートに関して、お客様が定義した制限はあるか

これらの確認事項（およびその他のビジネスプロセスやポリシー）は、導入に関して判断する際に役立ちます。この情報収集ステップでは、上記以外にも、お客様のエンドポイント管理に固有の情報はすべて収集する必要があります。

セキュリティ製品情報

多くの企業は、ビジネスに不可欠なソフトウェア、除外する必要がある対象、定義済みの導入プロセスなど、エンドポイント セキュリティ ソリューションに関する詳細なドキュメントをすでに作成しています。このドキュメントには、Cisco Secure Endpoint のポリシーに変換できる可能性のある情報が大量に含まれています。これらの情報を一から収集するのではなく、既存の情報を編集して現在の価値を評価し、Secure Endpoint のセットアッププロセスに活用します。

すべて網羅されているわけではありませんが、次の点を確認することから始めるとよいでしょう。

製品管理ユーザーに関して
- コンソールポータルにアクセスする必要があるのは誰か
- コンソールポータルへのアクセスに関して、各ユーザーにどのレベルの権限を付与する必要があるか

既存のエンドポイントセキュリティで使用されている機能は何か（以下の例参照）
- ネットワークアクティビティのブロック機能
- Secure Endpoint にすでに存在している機能
- その他のセキュリティ機能

既存のエンドポイントセキュリティにはどのような設定がなされているか（以下の例参照）
- 除外リスト
- アプリケーション ブロック リスト
- アプリケーション許可リスト
- IP アドレスブロックリスト

これらの情報を収集しながら、ポリシーとリストを調整していきます。ポリシーリストや機能を確認することで、必要なエンドポイントセキュリティを検証して整理できます。ポリシー項目を整理することで、エンドポイントのセキュリティが強化されます。

Cisco Secure Endpoint は、軽量のコネクタです。オプションで、他の EPP/EDR セキュリティ製品と連携できます。各製品が相互に阻害することなく適切に連携できるように、既存の設定と機能を確認する必要があります。

監査およびコンプライアンス

多くの組織は、監査およびコンプライアンス要件の対象となっています。組織は、これらの要件に対応するために、誰がアクセスして変更を行ったかや、それらの変更がいつ行われたかに関するデータ、およびエンドポイントセキュリティの過去のパフォーマンスに関するデータを維持していく必要があります。Cisco Secure Endpoint は、詳細なユーザー監査データとエンドポイントの履歴データを最大 30 日まで保持します。Event Streaming 機能を利用することで、さらに多くの履歴データを保持することも可能です。

新しい Secure Endpoint が必要な要件を満たしていることを確認するために、次の情報を入手することをお勧めします。
- 組織の監査要件
- 組織が対応すべき政府/自治体のコンプライアンス要件
- PCI DSS、GDPR 要件
- 履歴データの保管に関する組織の要件

情報
Cisco Trust Center：Cisco Trust Center – プライバシーシート
Cisco GDPR 関連情報 • 製品概要：https://www.cisco.com/c/ja_jp/about/trust-center/data-privacy.html • Secure Endpoint/AMP for Endpoints プライバシーデータシート：https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/security/cisco-amp-endpoints-privacy-data-sheet.pdf • Secure Endpoint/AMP for Endpoints データマップ：https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatamap/security/amp-privacy-data-map.pdf

準備

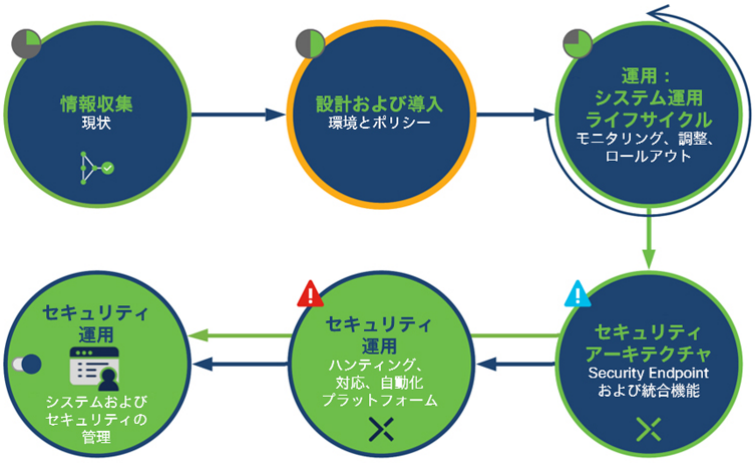
概要

プロセスの次のステップは、導入の準備です。準備には、導入計画とポリシー設定が含まれます。これらのステップは、収集した情報によって異なります。導入の準備中に、適切にポリシーを設定するためにいくつか確認するポイントがあります。場合によっては、テストを行ったり、パイロットユーザーグループと連携したりすることで、実際の環境でしか確認できないポイントを特定できます。

このセクションでは、Cisco Secure Endpoint のベースとなる情報を示します。この情報を確認することは、Cisco Secure Endpoint を正常に機能させるために必要です。

設計と導入の計画

準備における次のステップは、設計と導入の計画です。このステップでは、情報収集セクションで収集されたデータを活用して、Secure Endpoint の利用、設定計画、ポリシーセットアップに関する決定を行います。



クラウド インフラストラクチャ - 機能とサービス

Cisco SecureX と Cisco Secure Endpoint は、クラウドファーストのアプローチを採用しています。エンドポイントはクラウド インフラストラクチャと通信して、新しいポリシー更新情報、製品更新情報、ファイルの特性情報、ライブクエリ要求などを受け取ります。クラウドアーキテクチャは、さまざまな機能やサービスを提供します。

1. **Secure Endpoint Cloud：**エンドポイントに必要なすべてのサービスを提供します。Secure Endpoint は SecureX に完全に統合されるため、Endpoint 製品をアクティベートしたら、SecureX を有効にする必要があります。
    a. Endpoint ガイド：https://console.amp.cisco.com/docs/ https://console.eu.amp.cisco.com/docs/
    b. Secure Endpoint および Secure Malware Analytics（旧 Threat Grid）の適切な運用に必要なサーバーアドレス：https://www.cisco.com/c/ja_jp/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html
    c. Cisco Secure Endpoint サポートドキュメント：https://www.cisco.com/c/ja_jp/support/security/fireamp-endpoints/series.html
2. **Secure Endpoint Connector：**エンドポイントにインストールされるソフトウェアパッケージです。エンドポイントを保護し、Cloud Detection Engines 向けにテレメトリ情報を生成します。
3. **Secure Endpoint Orbital：**エンドポイントに関するリアルタイム調査情報を提供します。
4. **SecureX Platform：**Secure Endpoint ソリューションにさまざまなサービスを提供するプラットフォームです。
    a. **SSO：**すべての UI にシングルサインオンできます。
    b. **SecureX Threat Response：**特定の監視対象について、インフラストラクチャ全体を検索できる調査ツールです。
    c. **SecureX Orchestration：**適切なワークフローを構築してセキュリティを自動的に確立します。
    d. **統合モジュール：**Cisco Secure 製品およびサードパーティベンダー製品と統合して、脅威情報を収集します。さまざまなベンダーがコミュニティ サブスクリプションを提供しています（http://cs.co/threatresponseintegrations）。
    e. **SecureX Ribbon：**SecureX が提供するオーバーレイ アプリケーションとして、SecureX に統合された Cisco Secure Console で利用できます。Ribbon には、ケースブックアプリ、インシデントアプリ、Orbital アプリなど、エンドポイントでリアルタイムに調査するためのアプリが含まれています。
    f. **SecureX Pivot Menu：**SecureX をベースにしたセキュリティツールとして、多くの Cisco Secure 製品の UI で利用できます。Pivot Menu を利用すると、監視対象に関して製品間で共有できるレピュテーション情報を即座に取得し、インストール済みのシスコ製品やサードパーティ製品で、一般的な調査/対応アクションを非常に簡単に実行できます。
    g. **SecureX の詳細情報：**SecureX の詳細、機能、利点を把握できます。
    h. **SecureX のドキュメント：**http://cs.co/SXO_docs
    i. **SecureX ワークフローリポジトリ：**http://cs.co/SXO_repo
    j. **SecureX ビデオ：**http://cs.co/SecureX_videos
    k. **SecureX に関する FAQ：**http://cs.co/SecureX_faq
5. **Cognitive Analytics：**このサービスは、悪意のあるトラフィックに関して、標準の W3C ログデータを分析します。イベントは Secure Endpoint Events に直接送信されます。
6. **Secure Malware Analytics：**未知の独自なファイルを起動して、ふるまいに悪意の兆候がないかを判断するファイル分析プラットフォームです。

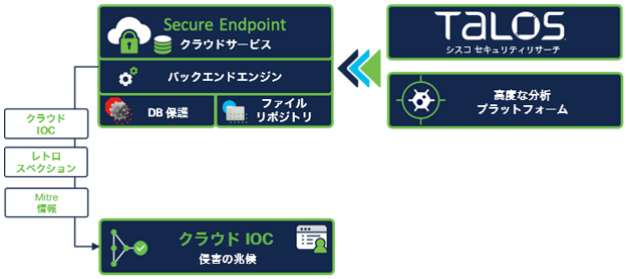
セキュリティアーキテクチャ：Secure Endpoint は、EDR アーキテクチャの一部として、一般的なエンドポイント保護機能に加え、さまざまな脅威ハンティング機能と脅威調査機能を備えています。

注：シスコは、高度なプライバシーニーズに対応するため、Secure Endpoint プライベート クラウド アプライアンスを提供しています。オンプレミスに導入することで、他のクラウド製品やサービスと統合することなく、プライバシーを確実に保護できます。詳細については、「付録 A：Secure Endpoint プライベートクラウド」を参照してください。

クラウド インフラストラクチャ – バックエンド インテリジェンス

Secure Endpoint のバックエンドエンジンは、Connector によって提供されたテレメトリデータを処理しています。バックエンドの規模は Connector 数によって自動的に決まり、収集されたテレメトリデータはリアルタイムで処理されます。また、7 日前にさかのぼって処理することもできます。その期間中またはリアルタイムの処理時に、Secure Endpoint のバックエンドは、最新の脅威情報を受信します。脅威情報は、エンドポイントから収集したすべてのテレメトリデータと関連付けられます。

リアルタイム処理とレトロスペクティブ分析によって、クラウド IOC イベントが出力されます。クラウド IOC は、悪意のあるふるまいを検出するロジックとインテリジェンスに基づいて生成されます。対象には悪意のあるファイルも含まれますが、多くの場合、悪意のあるファイルはエンドポイントの侵害には関与しません。脅威のコンテキスト情報を提供するために、シスコは、IOC に関する情報と MITRE 情報を加えています。クラウド IOC に関する主な特性は以下のとおりです。

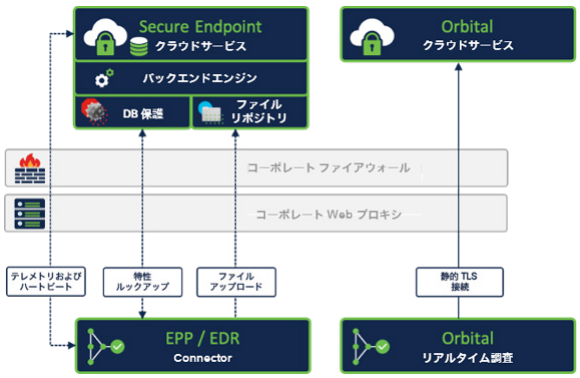


- リアルタイムおよびレトロスペクティブ IOC イベントは、感染後のタスクを自動化するために利用され（自動アクション）、デバイストラジェクトリで、侵害に関するエンドポイントのふるまいを示します。また、インテリジェンスを定期的に更新することで高度な検出を実現します。
- MITRE 情報は、IOC イベントに直接表示されます。

セキュリティアーキテクチャについて考える場合、クラウド IOC は、脅威ハンティングや脅威調査を開始したり、セキュリティの自動化を推進したりする上で非常に役立つ重要な情報です。

クラウド インフラストラクチャ - エンドポイント接続

Secure Endpoint がパブリッククラウドと通信するためには、適切に設定されたファイアウォール/プロキシシステムが必要です。パブリッククラウドと通信することで、特性の検索、バックエンド処理用のテレメトリデータの送信、ポリシー更新内容や定義の更新情報の受信ができます。Secure Endpoint では、Secure テクノロジーによって、エンドポイントとクラウド間の情報が保護されています。パブリッククラウドと通信できるように、ファイアウォールとプロキシを更新することをお勧めします。



クラウドとの通信

Secure Endpoint のトラブルシューティング テクニカルノーツは、cisco.com Web サイト：適切なエンドポイント/マルウェア分析に必要なサーバーアドレス（http://cs.co/AMP4EP_Required_URLS）を参照してください。

クラウド通信：プロキシ環境

プロキシを使用する環境では、TLS 通信がインターセプトされてパブリッククラウドへの通信が中断されないように、プロキシを設定する必要があります。ポリシーには、エンドポイントが使用できるプロキシ設定も含めなければなりません。Secure Endpoint は、システムまたはポリシーで定義されたプロキシのみを使用します。これにより、悪意のあるプロキシと通信することで通信が制限されたり、ブロックされたりするのを防げます。

ベストプラクティス：通信が中断されないように、Secure Endpoint 通信の TLS インターセプトを無効にします。

クラウド通信：必要な帯域幅

Secure Endpoint をインストールすると、AV シグネチャが更新されます。Secure Endpoint は、AV シグネチャの増分のみ更新しますが、導入直後は全体更新が必要です。帯域幅を節約するために、必要に応じて Secure Endpoint アップデートサーバーを導入することもできます。Connector がバックエンド処理用のテレメトリデータを生成する EDR 操作中は、帯域幅は少なくて済みます。詳細は以下の表を参照してください。

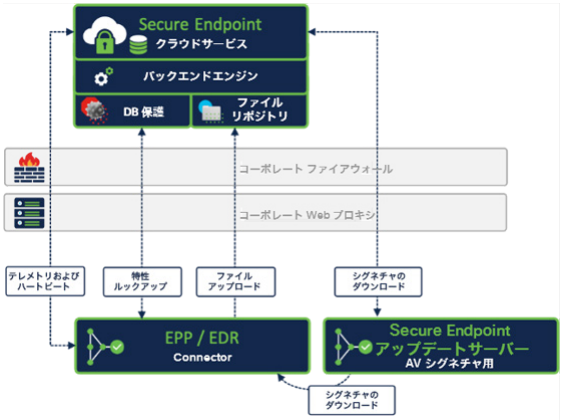
エンドポイントごとの更新に必要なサイズ	シグネチャの更新	通常の運用（エンドポイントテレメトリ）
~ 500MB	最初の AV シグネチャの更新	該当なし
1MB 未満～ 8MB	シグネチャの増分更新（1 日あたり 4 ～ 8 回） エンドポイントが 30 回を超えて増分更新できなかった場合、シグネチャ全体が更新されます。	該当なし
ルックアップあたり 最大 540 バイト	該当なし	1 日あたりの想定平均数：～ 54 クエリ/日 (該当エンドポイントですべてのエンジンが有効になっている場合)

オンプレミスコンポーネント

Secure Endpoint アップデートサーバー

帯域幅の要件が厳しい環境では、オプションで Secure Endpoint アップデートサーバーを利用して、オンプレミスに AV 定義を保存することもできます。アップデートサーバーは、パブリッククラウドで AV スキャンが有効になっていて、帯域幅が懸念される場合にのみ利用することをお勧めします。

Secure Endpoint アップデートサーバーの設定手順：
https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/213237-amp-tetra-on-prem-server-configuration-s.html



ベストプラクティス：ネットワーク帯域幅が豊富なパブリッククラウド環境や、エンドポイントが外部ネットワークに接続されている環境では、Secure Endpoint アップデートサーバーを利用しないことをお勧めします。

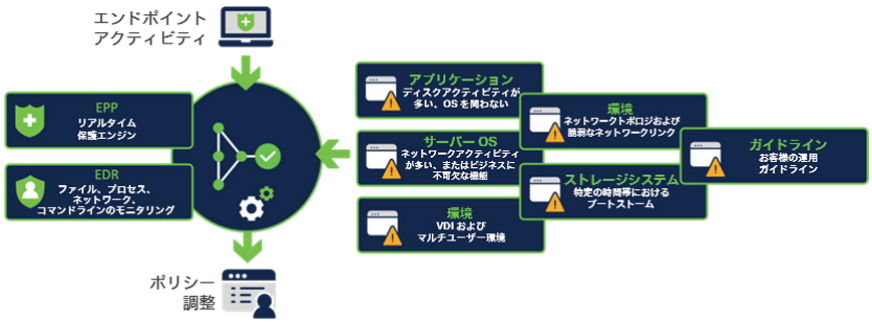
Endpoint Connector の基本的な設計

Secure Endpoint Connector は軽量のコネクタです。エンドポイントに対するシステム負荷を可能な限り最小限に抑えることが目的です。
EPP/EDR の観点では、Connector には主に以下の 2 つの領域があります。

- リアルタイム保護エンジン（EPP）
- エンドポイントモニタリング（EDR - バックエンド処理用テレメトリデータ）

Connector の仕組みを理解することは、ユーザビリティを確保しながら Endpoint Security を設計する上で重要です。Connector のパフォーマンスと信頼性に影響を与える可能性のある要因は多数あります。優れたパフォーマンスを得るには、適切に設定しなければなりません。

たとえば、EPP は、特定の特性を備えたアプリケーションに影響を与える可能性があります。また、特定のアプリケーションの特性により、Secure Endpoint Connector の CPU 使用率が高くなる場合があります。



ベストプラクティス：アプリケーションによる Connector への影響を考慮します。
結論：以下のように、一般的に CPU の負荷が高くなる状況がいくつかあります。
- 大量のディスク操作：Connector は、多数のファイルをスキャンしてハッシュ化する必要があります。
- アーカイブファイルのスキャン：アーカイブファイルの解凍には多くの CPU リソースが必要です。

ファイルスキャンシーケンス

ファイルスキャンは、エンドポイントで最も多くのリソースを消費するプロセスの 1 つです。Secure Endpoint は、ファイルやスクリプトのスキャン/検出/検疫、または圧縮ファイル内のスキャンのために多くのステップを実行します。

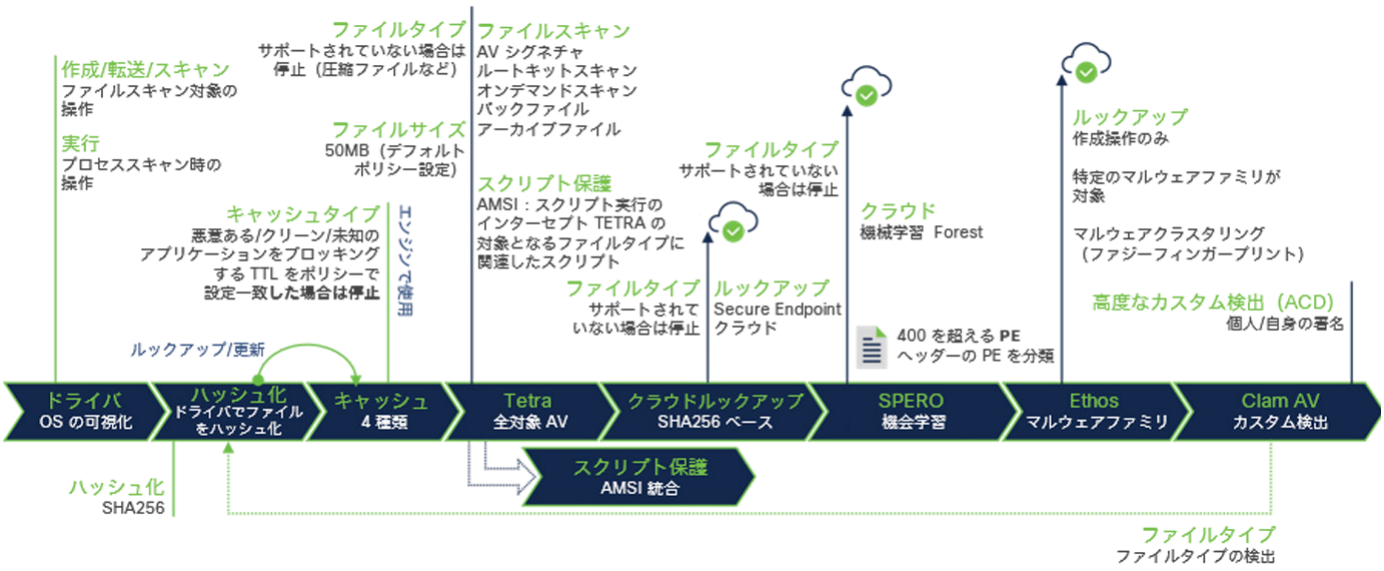
Secure Endpoint Connector は、次のシーケンスに基づいてディスク上のファイルをスキャンします（概要）。ファイルサイズ、ファイルタイプ、ポリシー設定などの多くの要因によって、シーケンスが変わる可能性があることに注意してください。ほとんどのケースで、すべてのシーケンスが処理されることはありません。Microsoft AMSI、Spero、Ethos に統合されるスクリプト保護エンジンなどは、Windows オペレーティングシステムでのみ利用されます。

1. **ドライバ：**ドライバは、OS を可視化するものです。Connector エンジンは、作成/転送/スキャン/実行操作をスキャンします。
2. **ハッシュ化：**ファイルはドライバによってハッシュ化され、ローカルキャッシュに追加されます。実際のファイルタイプの検出には、Clam AV エンジンの一部が使用されます。これは、他のすべての操作にとって重要です。
3. **キャッシュ：**Secure Endpoint には4 種類のキャッシュがあります。パフォーマンスを向上させるために、キャッシュにヒットした場合、ファイルスキャンプロセスは停止します。すべてのキャッシュタイプの TTL は、ポリシーで変更できます。
4. **AV スキャン：**キャッシュにヒットしない場合、AV スキャンが実行されます。AV エンジンは、アクセス時スキャン、オンデマンドスキャン、パケットファイルスキャン、アーカイブファイルスキャン、ルートキットスキャンに利用されます。
5. **スクリプト保護：**Secure Endpoint は、Microsoft Anti Malware Scanning Interface（AMSI）と連携し、Microsoft スクリプトインタープリタによって処理されたスクリプトファイルをスキャンします。
6. **クラウドルックアップ：**これまでに一致しなかった場合、エンドポイントはクラウドルックアップを実行して、特定のハッシュに関する脅威情報を取得します。
7. **SPERO（機械学習）：**機械学習の手法に基づいてファイルを分析します。
8. **Ethos、Malware Grouping エンジン：**未知のファイルにおける既知の悪意あるアクティビティをエンドポイントが検出できるようにします。
9. **ClamAV：**ClamAV は、Linux および macOS システムで OEM エンジンとして利用されます。Windows コネクタは、このエンジンをスキャンには使用しません。ClamAV は、カスタム検出とファイルタイプの検出に使用されます。

注：「停止」（以下の図を参照）は、検出シーケンス全体の停止を意味するわけではありません。どこで停止するかは状況によって異なります。

例：

- Tetra がスキャンを停止しても、シーケンスは停止しません。
- クラウドルックアップから返されるファイルの特性情報またはキャッシュされた結果が正常な場合、シーケンスは早い段階で終了します。
- エンドポイントの検出エンジンが脅威を検出しない場合でも、EDR 部分は、ファイル/プロセスに関するアクティビティのモニターを続け、クラウドエンジンはその情報を処理します。これにより、エンドポイントのリアルタイムエンジンで検出されなかった場合でも、クラウド IOC（侵害の兆候）が示される可能性があります。



ベストプラクティス - ファイルスキャン：パフォーマンスを向上させるために、ディスク操作の多いアプリケーションには注意してください。たとえば、データベースサーバー、Web サーバー、開発環境、インベントリソフトウェアなどです。サーバーまたはワークステーションのオペレーティングシステムがインストールされている場合、このガイドラインは当てはまりません。脅威の検出/保護または脅威リスクの軽減は、一度で終わるプロセスではありません。検出シーケンスによって製品に関するインサイトが得られ、必要に応じて製品を調整する方法をより詳細に理解できます。

注：高度なカスタム検出は、特性が不明なファイルに対してのみ機能します。

サポートされているオペレーティングシステム

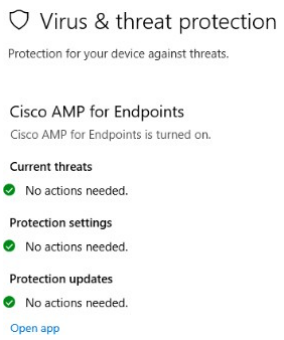
Secure Endpoint Connector は、Windows、Linux、macOS オペレーティングシステムで利用できます。Secure Endpoint Console は、監視モードの iOS デバイスと Android デバイスを統合することもできます。

公式にサポートされているバージョンは、cisco.com の Web サイトを参照してください。

- Windows：https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/214847-amp-for-endpoints-windows-connector-os-c.html
- Linux：https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/215163-amp-for-endpoints-linux-connector-os-com.html
- macOS：https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/214849-amp-for-endpoints-mac-connector-os-compa.html
- Security Connector の iOS 互換性：https://www.cisco.com/c/ja_jp/support/docs/security/security-connector/215337-cisco-security-connector-apple-ios-compa.html

Windows Security Center の統合

Secure Endpoint は、AV シグネチャ全体が更新された後、Windows Security Center for Virus and Threat Protection と統合します。登録プロセスが完了するまでしばらく時間がかかる場合があります。この時点で Connector は、他のすべてのエンジンやクラウドルックアップを含む保護機能をすでに提供しています。



Windows Defender

Connector のバージョンが 6.3.1 以降の Secure Endpoint には、Cisco Security Monitoring Service という新しいサービスが含まれています。このサービスによって、Windows Security Center（WSC）に Secure Endpoint が登録されます。詳細については、Secure Endpoint ユーザーガイドを参照してください。

バージョン 7.4.1.20439 以降では、インストール後に Connector が直接登録されるようになり、WSC への統合手順が変わっています。以前のバージョンでは、WSC に登録する前にシグネチャの全体更新が行われていました。

競合製品

- **削除：**Secure Endpoint は、インストールプロセス中に競合製品を削除しません。既存のセキュリティ製品を置き換えるには、次の 2 つの方法があります。
  - Secure Endpoint をインストールし、競合製品を削除します。その後、エンドポイントを再起動します。これにより、エンドポイントが常に保護されます。
  - 問題や製品間の競合がある場合は、まず競合製品を削除してからシステムを再起動し、再起動後に Secure Endpoint をインストールする必要があります。
- **非互換性：**互換性がないことがすでに判明している他のセキュリティ製品がいくつかあります。詳細は『Deployment Strategy Guide』（https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20Deployment%20Strategy.pdf）を参照してください。

エンドポイントのグルーピング

グループは、エンドポイントとそれぞれのポリシーを分類するために利用されます。同様のエンドポイントに同じポリシーを適用する場合、グループを定義することをお勧めします。エンドポイントをグループ化する属性には、次のようなものがあります。

- タイプ（サーバー、デスクトップ、ラップトップ）
- ロケーション（地域、ブランチ、リモートアクセス）
- インストールされているアプリケーションセット
- 利用されるサービスまたは運用機能
- 有効なセキュリティ機能およびオプション
- ユーザーグループ（早期導入者、開発者、パワーユーザー、一般ユーザー）
- 既存のグループ

サーバーとデスクトップは、使用方法、機能、アーキテクチャが異なるため、別々のポリシーに関連付けることをお勧めします。

ベストプラクティス：すべてのポリシーや機能（エンドポイントの分離や Orbital Real Time Search など）を含め、エンドポイントに関連するものはすべて、ポリシーオブジェクトに関連付けられます。エンドポイントを分離するのは、必要な場合に限ることを推奨します。そうすることで、エンドポイントの管理に必要な管理作業が軽減されます。

情報：ポリシーの更新：シスコのエンジニアリング部門は、グループ/ポリシーの処理を再設計するプロジェクトをすでに開始しています。この変更により、ポリシーオブジェクトのコンポーネントが分離されるため、ポリシー処理の柔軟性が大幅に向上します。

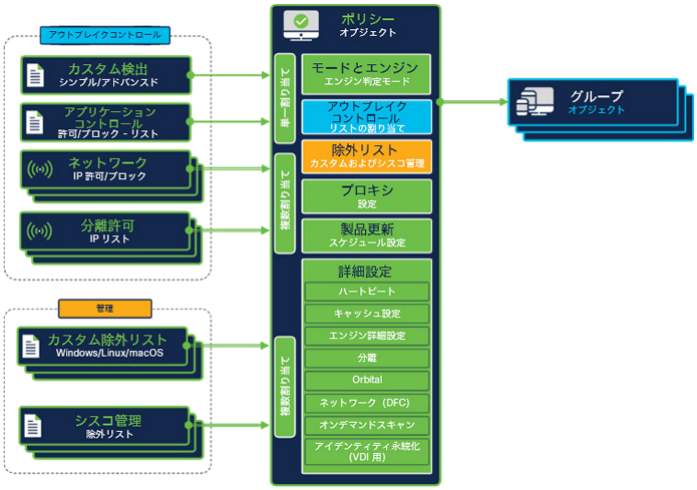
上記の情報に基づくエンドポイントのグループ化とは別に、グループにポリシーを割り当てる方法を検討することが重要です。ポリシーには、さまざまなタイプのリストを含められ、リストはポリシーに割り当てられます。リストタイプに基づいて、1 つのリストをポリシーオブジェクトに 1 回または複数回割り当てることができます。また、ポリシーオブジェクト内の設定と割り当てられたリストに基づいて、エンドポイントのポリシー情報が生成されます。何らかの変更があると、新しいバージョンのポリシーが作成され、次のハートビート中に、グループに割り当てられたエンドポイントに適用されます。

ポリシーの設定計画

Secure Endpoint のポリシーは、選択した機能が優れたエンドポイントセキュリティを実現し、ユーザーが機能やパフォーマンスに関する問題の影響を受けないように設定する必要があります。ポリシーは、エンドポイントのグループに関連付けられます。収集した情報とエンドポイントグループに基づいて、必要な機能と例外リストのポリシーを設定できます。

アウトブレイク コントロール リスト（[コンソール（Console）] → [アウトブレイクコントロール（Outbreak Control）]）：図に示すように、リストタイプに応じて、1 つのポリシーオブジェクトに 1 回または複数回割り当てられます。また、複数のポリシーオブジェクトに割り当てることもできます。

除外リスト（[コンソール（Console）] → [管理（Management）] → [除外（Exclusions）]）：各リストは、1 つのポリシーオブジェクトに複数回割り当てられます。また、複数のポリシーオブジェクトに割り当てることもできます。



ポリシーの設定計画 - ファイルスキャン

ファイルスキャンは、Secure Endpoint の中心的な機能です。このコアエンジンは、悪意あるファイルに対して動作し、悪意を示すシグネチャに関してファイルをスキャンします。ファイルスキャンにより、CPU 使用率、I/O、クラウドへのネットワーク要求がわずかに増加します。ファイルスキャン機能がなければ、ファイルの作成、転送、変更、実行を可視化できません。

悪意あるファイルによるエンドポイントの侵害から保護する機能や、侵害をさかのぼって検出する機能のために、ファイルスキャンを有効にすることをお勧めします。大量のファイル I/O が必要なアプリケーションを実行するエンドポイントは、ファイルスキャンの影響を受ける可能性があります。アプリケーションのパフォーマンスが影響を受ける場合は、ファイルスキャン対象から除外すれば、アプリケーションに干渉する I/O を削減できます。

ポリシーの設定計画 - ファイルスキャンの除外

Secure Endpoint には、2 種類の除外リストがあります。カスタム除外リストとシスコ管理除外リストの 2 つです。どちらもポリシーオブジェクトに複数回割り当てることができます。

基本的な除外管理について：http://cs.co/AMP4EP_Best_Practices_Exclusions

シスコ管理除外履歴：https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/214809-cisco-maintained-exclusion-list-changes.html

ベストプラクティス：除外リストは常に管理して整理します。複数の除外リストを作成する場合は、適切な名前をつけることで、管理が大幅にシンプルになります。

ポリシーの設定計画 - ネットワークモニタリング

ネットワークモニタリング機能を利用することで、Secure Endpoint は、エンドポイントと他の宛先間のアドレス情報を収集できます。この情報は、悪意のある宛先を特定して対処するために利用されます。ネットワークモニタリング機能により、CPU 使用率やクラウドに対するネットワーク要求がわずかに増加します。ネットワークモニタリング機能を利用しなければ、内部のネットワークリソースに関する情報しか得られないため、情報を外部情報と関連付ける必要があります。ネットワークモニタリング機能を利用すると、Cisco SecureX Architecture® を使用した統合調査が可能になります。

ネットワーク負荷が高くないエンドポイントでは、ネットワークモニタリング機能を有効にすることをお勧めします。プライマリ ワークステーションと、大量のネットワークトラフィックが発生しない一部のサーバーで有効にします。

ネットワークモニタリングがエンドポイントのネットワーク運用に影響する場合、ネットワークモニタリング機能を有効にしないポリシーをエンドポイントに適用するか、DFC コンポーネントなしで Connector をインストールします。

ベストプラクティス：ワークステーションとサーバーのどちらのオペレーティングシステムがインストールされているかに関係なく、ネットワーク負荷の高いシステム、ネットワークがチーミングされたシステム、多数の VLAN が設定されているシステムでは、ネットワークモニタリングを無効にすることをお勧めします。

ポリシーの設定計画 - 保護エンジン

その他の保護エンジン（オフラインエンジン、悪意あるアクティビティの防御エンジンなど）を利用することで、別の悪意あるふるまいから保護できます。各エンジンを有効にすると、Secure Endpoint の効果が向上します。有効にしたエンジンまたは設定によっては、パフォーマンスが低下する場合があります。エンジンの設定を有効にしたり変更したりする場合は、実稼働エンドポイントに適用する前に、変更内容をテストすることをお勧めします。

注：推奨設定と異なるセンシティブなシステムで新しいエンジンを有効にする場合は、監査モードで始めることをお勧めします。監査モードでは、Connector はイベントを生成しますが、ブロックすることはありません。

「v1.91 付録 B：非標準環境（VDI）」に、VDI 環境でファイルスキャンを有効にした場合の詳細情報が記載されています。

エンジンをテストしてから有効にすることをお勧めします。以下に、エンジンに対するポリシーの設定方法に関するオプションと考慮事項を示します。

エンジンポリシー設定	効果	パフォーマンスへの影響	その他のコメント
有効	効果大（以下によって異なる） • 有効にしたエンジンオプション • 除外対象（多すぎると効果が少ない）	影響大（以下によって異なる） • エンドポイントで実行されるアプリケーション • 除外対象（少なすぎると影響が大きい）	イベントは、可視化と一元的な調査のために Cisco SecureX Architecture® に送信される
無効	効果小	影響小	次のような場合にのみ推奨 • 別の製品が同等の機能を提供している • 有効にするとパフォーマンスに対する影響が大きすぎる • アプリケーションと互換性がない
設定変更	設定の変更内容によって異なる	設定の変更内容によって異なる	除外などの他の設定によっては、エンドポイントでのエンジンのパフォーマンスが向上する場合がある

ポリシーの設定計画 - Cisco Advanced Search（Orbital）

Cisco Advanced Search（Orbital）を利用すれば、エンドポイントでリアルタイムに調査ができます。Orbital クライアントは、Orbital クラウドサービスに静的に接続されます。脅威ハンティングまたはインシデント対応を強化するために、ポリシーで Orbital を有効にすることをお勧めします。CPU 使用率が上昇した場合に影響を受けやすいエンドポイントでは、テストを行う必要があります。上昇の影響が大きすぎる場合は、Orbital を無効にします。

Orbital でエンドポイントの価値を高める：https://blogs.cisco.com/security/getting-more-value-from-your-endpoint-security-tool-2-querying-tips-for-security-and-it-operations

Orbital に関する考慮事項

- Orbital は、エンドポイントでリアルタイムにクエリを実施するために追加するコンポーネントです。
- Orbital を利用するには適切なライセンスが必要です（https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/package-comparison.html）。
- ポリシーで Orbital を有効にしたら、Secure Endpoint がすべて自動で Orbital クライアントをインストールします。
- Orbital Endpoint（orbital.exe）は、TLS 1.2 で Orbital クラウドに静的に接続されます。
- Orbital は、フォレンジック スナップショットを生成します。スナップショットは、手動でも自動でも生成できます。
- Orbital は、SQL（Structured Query Language）を使用して、データベースに対するようにエンドポイントに対してクエリを実行します。

準備チェックリスト

Secure Endpoint の準備ステップのサマリーを確認してください。

- ☐ Secure Endpoint は SecureX Architecture に統合されます。使用可能なすべての機能を有効にしてください。このドキュメントの「クラウドアーキテクチャの概要」に記載されている全サービスのリストを参照してください。
- ☐ バックエンドエンジンは、ほぼリアルタイムにエンドポイントのテレメトリデータを処理します。7 日前にさかのぼって処理することもできます。
- ☐ プロキシ/ファイアウォールの設定を確認し、Connector がクラウドサービスと通信できるようにします。
- ☐ 最初の AV シグネチャの更新、または、実施されていない 30 回分の増分更新に必要な帯域幅があることを確認します。必要に応じて Secure Endpoint アップデートサーバーを導入します。
- ☐ Secure Endpoint は、アプリケーションのパフォーマンスに影響を与える可能性があります。また、アプリケーションの特性によっては、Connector のリソース消費に影響する場合があります。
- ☐ Secure Endpoint は Windows Defender の設定を変更せず、サードパーティのセキュリティ製品も削除しません。
- ☐ エンドポイントのグループ化、ポリシーの生成、リストの割り当ては、運用をシンプルにし、セキュリティを強化できるように適切に計画する必要があります。
- ☐ Cisco Advanced Search を利用すれば、SQL を使用してエンドポイントの情報を非常に簡単に検索できます。

Secure Endpoint - Console のセットアップ

Secure Endpoint Console のセットアップ：このセクションでは、ユーザーアカウントの設定、ポリシーとグループの作成および設定、感染/アウトブレイクコントロール機能の設定、除外リストの作成、感染後タスクの自動アクションの有効化に関する重要な情報を提供します。

以下の内容が含まれています。

- ユーザーアカウントの設定
- ポリシーとグループの作成および設定
- 感染/アウトブレイクコントロール機能の設定
- 除外リストの作成
- 自動アクションの有効化
- Secure Endpoint アップデートサーバーのセットアップ

Secure Endpoint アカウントのアクティベーションに関する電子メールを受信したら、記載されているリンクをクリックして、Cisco Security アカウントの初期セットアップを行います。詳細については、『Secure Endpoint Entitlement Guide』を参照してください。

ベストプラクティス：Secure Endpoint は、SecureX EDR/XDR/MDR アーキテクチャの重要なコンポーネントです。デバイストラジェクトリやファイルトラジェクトリなどのハンティング機能を備え、エンドポイントのテレメトリデータを処理してクラウド IOC を生成します。SecureX は、任意の Secure Endpoint ライセンスで利用でき、さまざまなハンティング機能や調査機能、セキュリティ自動化機能を備えています。Secure Endpoint Connector を導入してポリシーを設定する前に、Secure Endpoint Console を SecureX に接続し、提供されているすべてのハンティング機能および調査機能を有効にすることを強くお勧めします。サービスのリストは、「クラウド インフラストラクチャ - 機能とサービス」セクションで確認できます。

推奨のステップは次のとおりです。
- security.cisco.com にアクセスして SecureX を有効にします。
- visibility.amp.cisco.com にアクセスして SecureX Threat Response を有効にします。
- orbital.amp.cisco.com にアクセスして Secure Endpoint Advanced Search を有効にします。

詳細については、このドキュメントの「SecureX - EDR/XDR/MDR アーキテクチャ」セクションを参照してください。

ユーザーアカウントの設定

ユーザー管理の詳細については、『Secure Endpoint ユーザーガイド』の「アカウント」セクションを参照してください。Secure Endpoint には、ユーザーアカウントが適切に設定されていないと使用できない機能がいくつかありますので、注意してください。利用可能なすべての設定オプション、製品機能、秘密情報を利用できるようにするには、ユーザーが二要素認証を有効にする必要があります。

次の機能では二要素認証が必要です。

- リモートファイルの取得
- イベントでのコマンドラインの有効化
- 感染コントロール機能

二要素認証

ユーザーの二要素認証を適切に設定するには、Secure Endpoint UI の右上隅にある自分のアカウント名をクリックし、[マイアカウント（My Account）] を選択します。オプションで、[Secure Endpointユーザー管理（Secure Endpoint user management）] に移動します。

- [アカウント（Accounts）] → [ユーザー（Users）] の順にクリックし、自分のユーザー名を選択します。
- [二要素認証（Two-Factor authentication）] オプションの横にある [有効化（Enable）] をクリックし、画面の指示に従って、推奨アプリケーション（Duo、Authy、Google Authenticator）のいずれかに基づいて二要素認証を慎重に設定します。
- ユーザーページに戻ると、リモートファイル取得機能とコマンドラインが有効になっていることがわかります。

注：リカバリコードは安全な場所に保管してください。すでに Cisco SecureX SSO に移行している場合は、SSO サービスが SecureX プラットフォームに移行されているため、Secure Endpoint のバックエンドで二要素認証を変更することはできません。二要素認証を管理するには、https://me.security.cisco.com/（ユーザー ID 設定）に移動します。

SecureX プラットフォームと SecureX SSO を有効にする

SecureX プラットフォームは、任意のライセンスで利用できます。Secure Endpoint Console へのログインに慣れたら、**SecureX プラットフォームを有効にし、SecureX シングルサインオン（SSO）**に切り替えることを強くお勧めします。『SecureX Opt-In guide』に記載されている手順に従って、SecureX プラットフォームと SecureX SSO を有効にします。詳細については、SecureX SSO（SAML）の仕組みが記載されている『Cisco SecureX Sign-On クイックスタートガイド』を確認してください。

注：Secure Endpoint にログインすると、作成されるアカウントタイプは、Cisco Security アカウントになります。SecureX ログインページで新しい SecureX アカウントを**直接作成しない**でください。SecureX ログインページでアカウントを作成すると、SecureX で新しい ORG ID が生成されます。これは、Secure Endpoint の ORG ID とは異なります。SecureX に最初にログインする際は、SecureX ログイン用の Cisco Security アカウントを使用します。そうすることで、Secure Endpoint の ORG ID と同じ、正しい SecureX ORG ID が生成されます。

注：SecureX SSO を有効にすると、Secure Endpoint Console への従来のログイン情報は使用できなくなります。

シスコでは、ユーザー、SAML、二要素認証を管理するためのツールをいくつか用意しています。次の表に、参考の URL と設定オプションを示します。

プラットフォームおよびリンク	
Secure Endpoint	
https://castle.amp.cisco.com	Secure Endpoint ユーザーと SAML（SSO）設定を管理します。
SecureX	
https://sign-on.security.cisco.com/	Cisco SecureX プラットフォームにログイン
https://security.cisco.com/	Cisco SecureX プラットフォームにログイン
https://me.security.cisco.com	SecureX ユーザー ID の設定と多要素認証管理。組織名の変更や、最近のアカウントアクティビティの確認が可能
https://sso-apps.security.cisco.com/dashboard	SecureX アプリケーションポータル
https://www.cisco.com/c/ja_jp/td/docs/security/secure-sign-on/sso-quick-start-guide/sso-qsg-welcome.html	SecureX Sign-On クイックスタートガイド

Console セットアップのチェックリスト

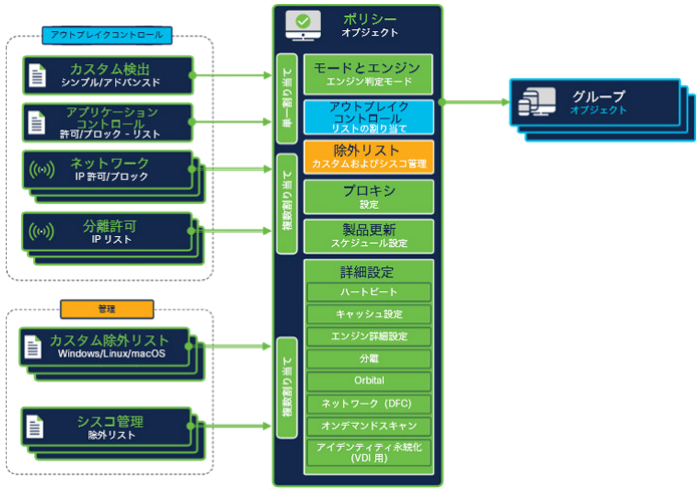
Console セットアップのサマリーを確認します。

- ☐ 最初のステップの 1 つとして、SecureX を有効にすることを強くお勧めします。「SecureX - EDR/XDR/MDR アーキテクチャ」セクションに、SecureX Architecture の詳細が記載されています。
- ☐ ユーザーがデータの秘密保持に関する確認や設定ができるように、二要素認証を有効にします。
- ☐ security.cisco.com にアクセスし、SecureX プラットフォームを有効にします。ガイドを確認して SecureX プラットフォームを有効にし、SecureX SSO に移行します。
- ☐ 前の章の「ポリシーの設定計画」および「Secure Endpoint Connector の設計」に基づいてポリシーを設定します。パフォーマンスとセキュリティの適切な設定方法については、「ポリシー設計 - パフォーマンスとセキュリティ」を参照してください。
- ☐ 「SecureX - EDR/XDR/MDR アーキテクチャ」で説明されているように、ファイル分析（感染状況）および感染後タスクを有効にします。

ポリシーの設計および管理 - パフォーマンスとセキュリティ

ポリシーの作成と管理は、Secure Endpoint の中核となる作業です。ポリシーは、Connector 機能の設定可能な部分すべてを制御します。そのため、新たに作成されたすべてのポリシーが、現在および将来の組織構造を考慮して作成されているかを確認することが重要です。この柔軟性を維持するために、組織のニーズに適切に対応する上で必要となるポリシーをいくつか作成することを推奨します。

このスクリーンショットは、Secure Endpoint のポリシーアーキテクチャを示しています。これを見れば、Secure Endpoint Console で設定可能なオブジェクトとポリシーオブジェクトとの関係を把握できます。このアーキテクチャでは、エントリが複数のリストで重複することはありません。左側には、ポリシーオブジェクトで直接使用できるオブジェクト（アウトブレイクコントロール、管理）が示されています。



アウトブレイクコントロール：カスタム検出（特性変化）、アプリケーション許可/ブロックリスト（実行）、ネットワーク IP 許可/ブロックリスト、分離許可リストがポリシーに割り当てられます。

Secure Endpoint Console には、管理者が構築するベースとなるポリシーがデフォルトでいくつか用意されています。デフォルトのポリシーは、エンドポイントのパフォーマンスへの影響を最小限に抑えながら、高いレベルのセキュリティを確保できるように設計されています。さまざまなエンドポイント機能に対するポリシー設定を決定する際に、シスコはお客様に対して、ポリシーページの推奨設定をそのまま使用し、組織のセキュリティニーズに対応するための変更は、最小限に留めるようにアドバイスしています。

デフォルトポリシーには主に、**監査**と**保護**の 2 つのタイプがあります。

- **監査**ポリシーでは、エンドポイントへの干渉を最低限に抑えながら Secure Endpoint Connector を導入できます。デフォルトの監査ポリシーでは、ファイルが検疫されたり、ネットワーク接続がブロックされたりすることはありません。そのため、初期導入時およびトラブルシューティング時にデータを収集して Connector を調整するのに役立ちます。
- **保護**ポリシーは、エンドポイントを強力に保護します。Connector は保護ポリシーを利用して、既知の悪意あるファイルの検疫や、C2 ネットワークトラフィックのブロックなどの保護アクションを実施します。

ベストプラクティス：ポリシー作成に関する Secure Endpoint のベストプラクティスでは、ベースとなる一連のポリシーを作成してからそのポリシーを複製し、同じポリシーのデバッグバージョンやアップデートバージョンを作成します。そうすることで、デバッグデータを収集したり、Connector をアップデートしたりする際に、一貫性を確保できます。

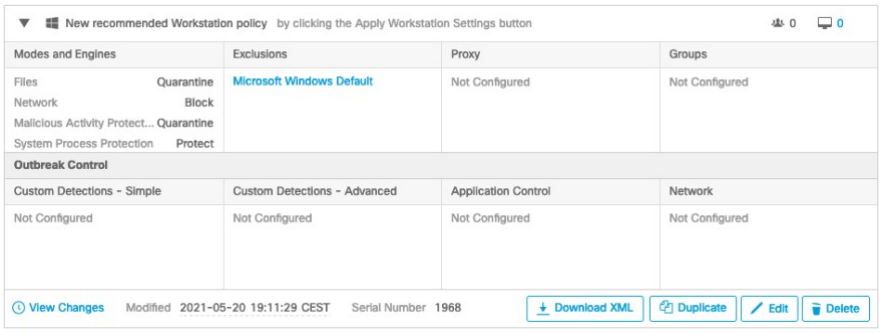
情報：Secure Endpoint Console には、管理者が構築するベースとなるポリシーがデフォルトでいくつか用意されています。事前に定義済みのグループとポリシーをそのまま使用すれば、製品テストを迅速かつ簡単に実施できます。

ポリシーオブジェクト

Secure Endpoint は、Windows/Linux/MAC、Android や iOS などのモバイルデバイス、ネットワークデバイス向けのポリシーを提供しています。ネットワークデバイスが Secure Endpoint クラウドに登録されていない場合、タブは表示されません。ポリシーオブジェクトは、[管理（Management）] → [ポリシー（Policies）] で確認できます。

ポリシービューには、ポリシーオブジェクトに関する以下のようなさまざまな情報が表示されます。

- エンジンの設定モード
- 割り当てられている除外リスト
- プロキシ設定
- ポリシーが適用されているグループ
- 割り当てられている検出リスト
- アプリケーション制御リスト
- ネットワークリスト（ホワイトリスト/許可）
- 最終更新日
- ポリシーのシリアル番号（変更するたびに増加）



[XMLのダウンロード（Download XML）] ボタン：ダウンロードしたファイルは、破損した Connector に追加できます。Connector は、Secure Endpoint がインストールされたローカルディレクトリにあります。この XML ファイルは、Connector が Secure Endpoint Cloud と通信できなくなった場合に役立ちます。Connector の policy.xml ファイルを置き換えるには、Connector サービスを停止して policy.xml を置き換え、Connector サービスを再開します。

新しいポリシーオブジェクトを生成すると、シスコが管理する除外リスト（**Microsoft Windows Default**）がポリシーオブジェクトにのみ追加されます。

ポリシー設定：最適なパフォーマンスとセキュリティ

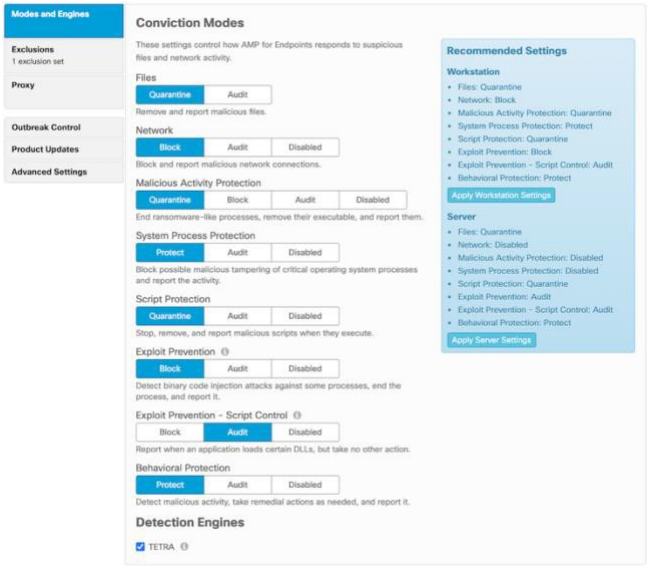
以下のステップでは、Secure Endpoint のポリシー設定に関するベストプラクティスを示します。ワークステーションとサーバーのオペレーティングシステムのどちらに Secure Endpoint をインストールしても、コードベースは同じで違いはありません。前の章では、Connector の基本的な機能について説明しました。このセクションでは、重要な情報について説明し、パフォーマンスとセキュリティのニーズに適したポリシーを構築できるようにします。そのために、ワークステーションとサーバーのポリシーを構築する際に役立つ情報を示します。

このガイドで説明されていない設定については、『**Secure Endpoint 製品ガイド**』（https://console.amp.com/docs）を参照し、この情報を注意深く確認してください。

ポリシー設定：モードおよびエンジン

[モードおよびエンジン（Modes and Engines）] エリアには、使用可能なすべてのエンジンとそのモードの概要が表示されます。また、サーバーとワークステーションの推奨設定も示されています。

注：すべてのエンジンがあらゆるオペレーティングシステムで利用できるわけではありません。



ファイルスキャン：悪意あるファイルのスキャンは、エンドポイント上の複数のエンジンがそれぞれ異なる手法を駆使して行います。ファイルスキャンの全体シーケンスでさえ固定されていません。ファイルの種類やキャッシュ情報などに応じて、ファイルのスキャン/検出ステップが多少なりとも変わります。詳細については、「ファイルスキャンシーケンス」情報を参照してください。ファイルスキャンを [監査（Audit）] モードに切り替えると、ファイルスキャンシーケンスでディスクからファイルが削除されることはありません。

推奨設定：図の青い背景の部分は、ワークステーションおよびサーバーのオペレーティングシステム用の推奨エンジン設定を示しています。推奨設定は、新しいポリシーを作成する際に適しています。エンジン判定モードに関して以下に注意してください。

- ポリシーでエンジンを無効にしても、ドライバはエンドポイントで引き続き使用できます。そのため、エンジンはいつでも簡単に有効にできます。
- /skipdfc や /skiptetra などのインストールスイッチを指定すると、ドライバはインストールされません。ドライバを再度有効にするには、Secure Endpoint を再インストールする必要があります。
- 自動アクション → コンピュータをグループに移動：悪意のあるアクティビティが検出された場合に、この感染後自動タスクによって、コンピュータは設定済みグループに移動されます。検出率を高めるために、このグループではすべてのエンジンを有効にしておきます。そのため、すべてのドライバがシステムにインストールされていなければなりません。
- AV-Engine ドライバがインストールされていない場合、システムでオンデマンドスキャンは利用できません。/skiptetra スイッチを指定した後に AV スキャンをシステムに追加する場合は、「v1.92 付録 C：/skiptetra を指定した後に Tetra を手動で追加」を確認してください。

ベストプラクティス：自社の環境内でファイルスキャンを設計する場合は、以下のステップを確認してください。
- 後から AV スキャンを有効にする予定がある場合は、/skiptetra インストールスイッチを指定しないでください。ドライバがインストールされなくなります。ポリシーを有効にしても、ドライバファイルはエンドポイントに追加されません。エンドポイントにドライバを追加するには、Secure Endpoint を再インストールする必要があります。
- VDI 環境でのファイルスキャンには、さらに注意が必要です。詳細については、「v1.91 付録 B：仮想環境（VDI）」を参照してください。
- 後から Windows エンドポイントに AV スキャンを手動で追加する方法があります。詳細については、「v1.92 付録 C：/skiptetra を指定した後に Tetra を手動で追加」を参照してください。

セキュリティのベストプラクティス：検出および保護機能
- AV スキャンの検出/検疫イベントがない場合、バックエンドエンジンがクラウド IOC を追加で生成することがあります。これは、エンドポイントが悪意あるファイルを検出したが、ディスクからファイルを削除する AV エンジンが存在しない場合に発生します。
- 自動アクション機能を利用すれば、ポリシーで AV スキャンが無効になっているシステムをクリーンアップできます。「v1.80 SecureX - EDR/XDR/MDR アーキテクチャ」を参照し、コンピュータを設定済みグループに移動して、最も優れた検出機能を適用する方法を確認してください。
- オンデマンドスキャンは、AV スキャンエンジンなしでは実行できません。
- **すべて検出するポリシー：**侵害の兆候に対して最も優れた検出機能を適用する必要がある場合は、AV エンジンを有効にする必要があります。

ポリシー設定：除外リストの定義と管理

多くの場合、時間が経つにつれて、Secure Endpoint Console にさまざまな除外リストが定義されるようになります。不要な除外リストは削除する必要があります。除外リストの管理をシンプルにするためのガイドラインを示します。

シスコが管理する除外リスト：シスコ管理のリストは、重要なファイルやプロセスを除外するのに役立ちます。シスコ管理の除外リストの履歴は、https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/214809-cisco-maintained-exclusion-list-changes.html を参照してください。

カスタム除外リスト：除外リストの管理をシンプルにするためのガイドラインに従います。

- **グローバル除外リスト：**ほとんどのシステムで必要なアプリケーションの除外リストです。たとえば、ほとんどのエンドポイントにインストールされているアプリケーションなどが対象です。このような除外リストは、多くのポリシーに割り当てられます。特定のアプリケーションを新たに除外する必要がある場合は、1 つの除外リストを更新して管理するだけで済みます。
- **除外リストの命名ルール：除外リストの管理がシンプルになるような名前をつけます。**アプリケーションにさまざまなバージョンが存在する場合、除外リストを分割し、除外リスト名にソフトウェアのバージョンを追加すれば、将来除外リストを簡単に整理できます。スクリーンショットに示されているように、ポリシーオブジェクトにはわかりやすい名前が付いています。

注：Secure Endpoint Connector の除外リストにはいくつか数に制限があり、この数は変更できません（Connector バージョン 6.0.5 以降）。すべての値は非常に大きいため、通常の運用中にこの値に達することはありません。

- プロセス除外リストの制限数は、除外リストセット全体で 100 です。
- 100 件を超えるプロセスが除外されているポリシーでは、最初の 100 件のみが適用されます。
- 除外対象はアルファベット順にソートされます。
- 推奨される除外件数の最大値は 300 です。
- policy.xml のサイズ制限は 40KB で、すべてのタイプの除外対象が含まれます。
- 除外対象の最大数は 1,000 です。

除外に関するベストプラクティス：通常、除外リストの制限に達することはありません。特定のエンドポイントに多くの除外対象がある場合は注意してください。グループ設計は、必要な除外リストの数を減らすのにも役立ちます。詳細については、『Secure Endpoint の除外リストに関するベストプラクティス』ガイド（https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/213681-best-practices-for-amp-for-endpoint-excl.html）を参照してください。
- 除外リストには適切な名前を付けます。
- 複数の除外リストを使用すると、古い除外リストを整理できます。
- シスコ管理の除外リストを利用すれば、除外リストの管理工数を削減できます。

ワイルドカードを利用した除外は、他の除外タイプよりも評価に多くのシステムリソースを必要とします。ワイルドカードでの除外はできるだけ少なくします。

ポリシー設定：除外リストとセキュリティ

除外リストは、製品の機能と信頼性にとって重要です。多くのお客様は、ビジネスに不可欠なアプリケーションを除外して、Endpoint Security による影響を回避しています。除外リストを効果的に定義する要素にはさまざまなものがあります。ハッシュ化は、エンジンでスキャンする前でもシステムリソースを消費します。

スキャンを除外すると、Connector がスキャンしたりモニターしたりするのも停止します。その結果、EPP/EDR のセキュリティレベルに関して、**除外されたエリアは、次のような状態になります。**

- ファイルはハッシュ化されず、キャッシュでも利用できません。また、スキャンもクラウドルックアップも行われません。
- アクティビティはモニターされず、バックエンドに送信されます。
- バックエンドエンジンに情報は提供されません。除外されたディレクトリの悪意あるアクティビティに関しては、クラウド IOC などの出力結果は生成されません。
- デバイストラジェクトリに情報は表示されません。
- Advanced Analysis にファイルはアップロードされません。

前後のその他のアクティビティは、使用可能なすべてのエンジンによってモニター/分析されます。

セキュリティのベストプラクティス：最高レベルのセキュリティを実現し、エンドポイントエンジンとバックエンドエンジンで最大限の効果を上げるために、必要な場合にのみ除外対象を追加することを推奨します。
- **フル検出ポリシー：**可能な限り除外対象をなくし、ディスク上のほとんどの領域をスキャンの対象にして、実行中のプロセスを保護します。

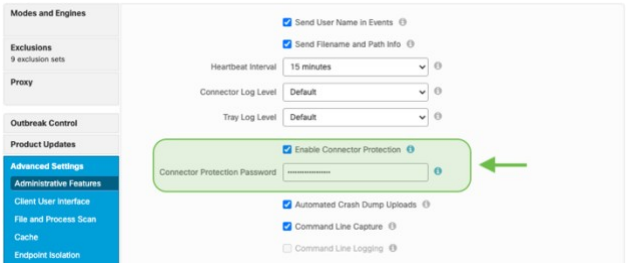
ポリシー設定：プロキシ

すでに説明したように、TLS1.2 接続内のプロトコルは HTTP ではありません。TLS がプロキシで終端すると、HTTP ではないため、プロキシはパッケージをドロップし、Secure Endpoint の通信が停止します。Connector は引き続きオフラインエンジンを使用しますが、オンラインエンジン、クラウドルックアップ、バックエンドエンジンなどの他のすべての機能は使用できなくなります。プロキシ接続に関していくつかガイドラインがあります。

- プロキシで TLS トラフィックを検査しないでください。クラウド通信が切断されます。
- プロキシ認証を利用する場合、サポートされていない NTLM 認証シナリオがいくつかあります（製品ドキュメントを参照してください）。
- プロキシサーバーが設定されている場合、すべての更新はプロキシを介して行われます。
- クラウド通信は動的であり、プロキシが使用できない場合は、直接通信に切り替わります。

ポリシー設定：Connector のパスワード（自己保護）

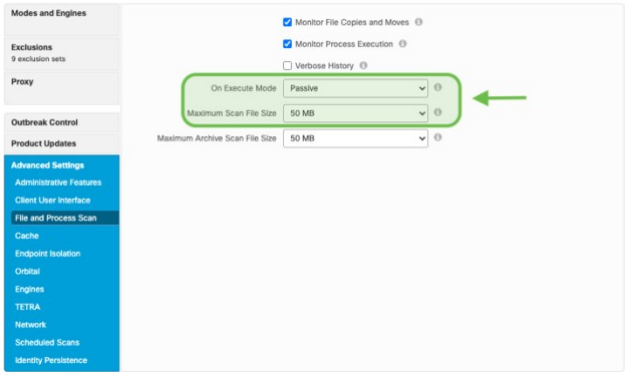
常にパスワードを設定します。これにより、不正なユーザーやマルウェアによって Connector が無効化されたり、アンインストールされたりしないように保護できます。



ポリシー設定：ファイルとプロセスのスキャン

[実行開始モード（On Execute Mode）]：[パッシブ（Passive）] のままにすることをお勧めします。
[アクティブ（Active）] に変更する場合は、以下の点に注意してください。

- [アクティブ（Active）] モードでは、ファイルやスクリプトに悪意があるかどうかが判断されるまで、またはタイムアウトになるまで、実行されないようブロックされます。
- クラウドルックアップも実行されません。



[スキャンファイルの最大サイズ（Maximum Scan File Size）]：ポリシーのデフォルト値は 50MB に設定されています。この値を小さくすることはできますが、大きくすることはできません。この値より大きいファイルは、Connector for EPP/EDR 機能で無視されます。この値が、セキュリティと製品機能のバランスをとる最大値です。マルウェアファイルのサイズが 50MB を超えることは通常ありません。50MB までであれば、ファイルをハッシュ化しても CPU にそれほど大きな負荷はかかりません。

セキュリティのベストプラクティス：自動アクションを使用して、**感染/侵害された**エンドポイントを定義済みグループに移動する場合は、次の設定を利用できます。
- できるだけ大きなファイルをスキャンする場合は、スキャンファイルの最大サイズを 50MB に設定します。ファイルが 50MB を超える場合でも、そのファイルに関するアクティビティは、バックエンドエンジンによってモニター、スキャン、処理されます。
- パフォーマンスよりもセキュリティを重視する場合は、[実行開始モード（On Execute Mode）] を [アクティブ（Active）] に設定します。

ポリシー設定：キャッシュ

キャッシュを利用することで、Connector のパフォーマンスが向上します。すでに利用できるハッシュがキャッシュにある場合、Connector はファイルをスキャンしません。

キャッシュは次のようにしてシステムでクリアできます。

1. Secure Endpoint Connector **サービスを停止**します。
2. ローカルディスク上の**キャッシュファイルを削除**します（Connector ディレクトリにあります）。
3. Secure Endpoint Connector サービスを**再開します。**

トラブルシューティング テクニカルノーツの「Windows 上の Secure Endpoint キャッシュファイルと履歴ファイルの削除」を参照してください。

セキュリティのベストプラクティス：キャッシュ設定によって、パフォーマンスとセキュリティに影響があります。
- Microsoft Office アプリケーション x64 のサイズは約 50MB です。この値を小さくするのは、Microsoft Office がインストールされていないエンドポイントを対象にする場合のみにします。
Microsoft 製品は、依然としてエンドポイントに対する大きな攻撃ベクトルです。
- **フル検出ポリシー：**すべてのキャッシュ値を最も低い値に設定します。

ポリシー設定：ファイルスキャン - アーカイブファイルとパックファイルの違い

これら 2 つの設定の違いを理解することが重要です。

アーカイブファイル：Secure Endpoint Connector は、圧縮されたファイルを開き、内容をスキャンします。Tetra は、ファイルとプロセスのスキャン設定の値を使用します。ファイルサイズのデフォルト値は 50MB ですが、アーカイブファイルのデフォルト値は 5MB です。一般的な圧縮ファイルのタイプは、7zip、arj、jar（Java アーカイブ）、tar、zip です。

アーカイブスキャンでは、システムが過負荷にならないように次の制限が適用されます。いくつかのガイドラインが含まれています。

- アーカイブファイルのスキャンは、上記のファイルサイズ内のものが対象です。
- アーカイブファイルのスキャンは、サポートされているタイプのファイルが対象です。
- 一括処理ファイル数は 1,000 です（圧縮ファイル内に 100 万ファイルが含まれる場合など）。

最大 5 つのレベルがありますが、1 つの圧縮ファイルから同時に 100 万ファイルをスキャンする場合を除き、同じレベルの zip 内のファイル数に制限はありません。つまり、1,000 ファイル単位で自動的にスキャンされます。

パックファイル：[パックファイルのスキャン（Scan Packed Files）] オプションを有効にすると、Tetra エンジンは、ASCII ファイルでも実行可能なファイルを検出します。例：*.JS ファイルは ASCII ファイルですが、実行できます（*.JS ファイルはそのままで実行可能ですが、他のファイル/コードで構成されているという意味でパッケージと見なされます）。

ベストプラクティス：ファイルの展開には多くのシステムリソースが必要です。特に、コンパイルされて非常に圧縮度の高いコードで動作する開発環境の場合に多くのリソースを利用します。そのため、このようなエンドポイントをグループ化し、特別な除外リストが設定されているポリシーを割り当てることを強くお勧めします。開発用エンドポイントは、一般的なエンドポイントとは異なる場合が多く、標準の除外リストは機能しない場合があります。パフォーマンスが低下しないようにするには、ポリシーで [アーカイブのスキャン（Scan Archives）] を無効にします。

セキュリティのベストプラクティス：最適な検出/保護のためのガイドラインに従います。
- [パックファイルのスキャン（Scan Packed Files）] 設定を無効にすると、Tetra は悪意のある JS ファイルを検出しなくなります。
- **フル検出ポリシー：**最高レベルの検出/保護機能を利用するには、両方の設定を有効にする必要があります。

ポリシー設定：ワークステーション

ワークステーションシステム用の新しいデフォルトポリシーを生成します。

- [管理（Management）] → [ポリシー（Policies）] で [新規ポリシー（New Policy）] ボタンをクリックし、新しいポリシーオブジェクトを生成します。
- ポリシーを生成するオペレーティングシステムを選択し、[新規ポリシー（New Policy）] をクリックします。
- わかりやすい名前を付け（オプションで説明を追加）、右側の [ワークステーション設定の適用（Apply Workstation Settings）] ボタンをクリックします。これで、シスコが推奨する設定が適用されます。
- すべてのエンジンがインストールされるように、コマンドラインスイッチを**指定せずに**（デフォルトインストール）、Secure Endpoint をインストールします。

最初の段階として最適なポリシーオブジェクトが生成されます。

- [ファイル（Files）]：[検疫（Quarantine）]
- [ネットワーク（Network）]：[ブロック（Block）]
- [悪意のあるアクティビティからの保護（Malicious Activity Protection）]：[検疫（Quarantine）]
- [システムプロセスの保護（System Process Protection）]：[保護（Protect）]
- [スクリプトの保護（Script Protection）]：[検疫（Quarantine）]
- [エクスプロイト防止（Exploit Prevention）]：[ブロック（Block）]
- [エクスプロイト防止-スクリプト制御（Exploit Prevention - Script Control）]：[監査（Audit）]
- [ふるまいの保護（Behavioral Protection）]：[保護（Protect）]

ポリシー導入チェックリスト：

- **除外リスト**：最適なセキュリティを確保するために本当に必要な場合にのみ、除外リストを追加します。「Secure Endpoint のインストール、更新、運用ライフサイクル」セクションで、追加が必要な除外対象を特定する方法を確認します。新たな除外対象を定義する場合は、パフォーマンスとセキュリティを考慮した、除外に関するベストプラクティスを確認します。

- **リスト：**Secure Endpoint Console の [アウトブレイクコントロール（Outbreak control）] で、カスタム検出（シンプル）、カスタム検出（アドバンスド）、アプリケーション制御（ブロック/許可）、ネットワーク - IP（ブロック/許可）用のリストを生成します。生成したら、リストをポリシーに割り当てます。これらのリストは、SecureX Pivot Menu でも利用できます。ポリシーの設定計画に関するベストプラクティスを確認してください。

- **エンドポイントの分離**：必要に応じてこの機能を有効にします。**手動**または**自動**（自動アクション機能を利用）でネットワークからエンドポイントを切断できます。詳細については、「v1.80 SecureX - EDR/XDR/MDR アーキテクチャ」セクションを参照してください。

- **Orbital**：Orbital を有効にして、エンドポイントでリアルタイム調査を実施できるようにします。Orbital は標準ライセンスでは利用できません。Secure Endpoint Advantage 以上のライセンスが必要です。

- **エンジン設定：**高度なエンジン設定：[エンジン（Engines）] → [エンジン一般設定（Common Engine Settings）] で、[Windowsのイベントトレースを有効にする（Enable Event Tracing for Windows）] を有効にします。これにより、ふるまい保護エンジンに対して Windows イベントログ情報が有効になります。この機能は、既存の Microsoft グループポリシー設定と競合する場合があります。この機能を有効にする場合は、情報フィールドを確認し、担当のワークプレイス/エンドポイント設計者に相談してください。

- **アイデンティティ永続化：**この機能はデフォルトでは利用できないため、TAC に有効にしてもらう必要があります。頻繁に再インストールされるエンドポイントに Secure Endpoint がインストールされていない場合、この機能は不要です。

- その他すべての設定の詳細については、「ポリシー設定：最適なパフォーマンスとセキュリティ」セクションを確認してください。

ポリシー設定：サーバー

サーバーシステム用の新しいデフォルトポリシーを生成します。

- [管理（Management）] → [ポリシー（Policies）] で [新規ポリシー（New Policy）] ボタンをクリックし、新しいポリシーオブジェクトを生成します。
- ポリシーを生成するオペレーティングシステムを選択し、[新規ポリシー（New Policy）] をクリックします。
- わかりやすい名前を付け（オプションで説明を追加）、右側の [サーバー設定の適用（Apply Server Settings）] ボタンをクリックします。これで、シスコが推奨する設定が適用されます。
- すべてのエンジンがインストールされるように、コマンドラインスイッチを**指定せずに**（デフォルトインストール）、Secure Endpoint をインストールします。

最初の段階として最適なポリシーオブジェクトが生成されます。

- [ファイル（Files）]：[検疫（Quarantine）]
- [ネットワーク（Network）]：[無効（Disabled）]
- [悪意のあるアクティビティからの保護（Malicious Activity Protection）]：[無効（Disabled）]
- [システムプロセスの保護（System Process Protection）]：[無効（Disabled）]
- [スクリプトの保護（Script Protection）]：[検疫（Quarantine）]
- [エクスプロイト防止（Exploit Prevention]：[監査（Audit）]
- [エクスプロイト防止-スクリプト制御（Exploit Prevention - Script Control）]：[監査（Audit）]
- [ふるまいの保護（Behavioral Protection）]：[保護（Protect）]

ポリシー導入チェックリスト：

- **除外リスト**：最適なセキュリティを確保するために本当に必要な場合にのみ、除外リストを追加します。「Secure Endpoint のインストール、更新、運用ライフサイクル」セクションで、追加が必要な除外対象を特定する方法を確認します。新たな除外対象を定義する場合は、パフォーマンスとセキュリティを考慮した、除外に関するベストプラクティスを確認します。
- **リスト：**Secure Endpoint Console の [アウトブレイクコントロール（Outbreak control）] で、カスタム検出（シンプル）、カスタム検出（アドバンスド）、アプリケーション制御（ブロック/許可）、ネットワーク - IP（ブロック/許可）用のリストを生成します。生成したら、リストをポリシーに割り当てます。これらのリストは、SecureX Pivot Menu でも利用できます。ベストプラクティスについては、「ポリシーの設計および管理 – パフォーマンスとセキュリティ」セクションを参照してください。
- **ネットワーク：**サーバー OS には、ほぼ常に、ワークステーション OS よりもはるかに多くのネットワーク負荷がかかります。そのため、[ネットワーク保護（Network Protection）] を [有効（Enabled）] にする場合は、いくつか注意が必要です。
    - ネットワークドライバなしで Connector をインストールする代わりに、この機能を無効にすることで、ネットワークのほとんどの問題を解決できます。
    - ネットワーク保護機能によって、ネットワークの動作が遅くなる可能性があります。サーバーアプリケーションがネットワークパフォーマンスや応答時間を重視する場合は、エンジンを有効にする際に注意が必要です。綿密にテストすることを強くお勧めします。
    - ネットワークをチーミングする場合や、1 つのサーバーネットワークカードに複数の VLAN を設定する場合など、特定のネットワーク設定を適用する場合は、慎重にテストする必要があります。このような状況では、ネットワーク保護機能を無効にすることをお勧めします。
    - それでもネットワークの問題が解消しない場合は、/skipdfc インストールスイッチを指定して Secure Endpoint を再インストールし、ネットワークドライバをインストールしないようにする必要があります。
- **システムプロセスの保護：**このエンジンは、「Mimikatz」のような攻撃を防御できるように設計されています。NTLMv1 の無効化などのグループポリシーや、その他の NTLM セキュリティが設定されている場合は、エンジンを無効にできます。エンジンを有効にする必要がある場合は、サーバーのパフォーマンスを慎重にモニターしてテストすることをお勧めします。
- **エクスプロイト防止：**エクスプロイト防止エンジンは、次の場合にトリガーされます。
  - プロセスが、保護されたプロセスのリストに表示されている（詳細については、『Secure Endpoint User Guide』を参照してください）。
  - プロセスが、エクスプロイト防止エンジンの保護リストに表示されている別のプロセスによって起動された。
  - プロセスが、エクスプロイト防止エンジンがモニターしているディレクトリから実行された。

  エクスプロイト防止エンジンがトリガーされると、軽量の DLL がプロセスにロードされ、このプロセスに関してメモリーが更新されます。このプロセスだけが、更新されたメモリーロケーションを認識します。サーバーシステム、特にドメインコントローラでは、メモリーが更新されると予期しないふるまいが発生する可能性があります。このエンジンを有効にした場合は、サーバーのパフォーマンスをモニターして慎重にテストすることを推奨します。
- その他すべての設定の詳細については、「ポリシー設定：最適なパフォーマンスとセキュリティ」セクションを確認してください。
- サポートされているサーバー OS で **Orbital** Real Time Search を有効にします。
- **エンドポイントの分離**機能を有効にして、侵害された可能性のあるサーバーをネットワークから切断します。

ポリシーセットアップのサマリー

Console セットアップのサマリーを確認します。

- ☐ 最初のステップの 1 つとして、SecureX を有効にすることを強くお勧めします。「SecureX - EDR/XDR/MDR アーキテクチャ」セクションに、SecureX Architecture の詳細が記載されています。
- ☐ ユーザーがデータの秘密保持に関する確認や設定ができるように、二要素認証を有効にします。
- ☐ security.cisco.com にアクセスし、SecureX プラットフォームを有効にします。ガイドを確認して SecureX プラットフォームを有効にし、SecureX SSO に移行します。
- ☐ ここでのガイドラインに従えば、エンドポイントに悪影響を与えずに機能するポリシーを定義できます。

情報：シスコは、Secure Endpoint のポリシーを再設計するプロジェクトを開始しました。これにより、ポリシー管理全体が大幅に改善されます。すべての変更は段階的に行われるため、移行全体の管理作業が最小限に抑えられます。

Secure Endpoint のインストール、更新、運用ライフサイクル

Secure Endpoint：ソフトウェアのロールアウト

他の大規模なソフトウェア導入と同様に、時間をかけて体系的に導入することをお勧めします。段階的に導入することで、どんな環境で問題が発生しても、比較的少数のエンドポイントにしか影響を与えずに解決できます。これらの注意点は、特にセキュリティソフトウェアに関連しています。そのため、シスコでは、段階的なアプローチで Secure Endpoint を導入することをベストプラクティスとしています。表に示すように、いくつかの一般的なアプローチ/例があります。

計画的 ロールアウト - シナリオ 1	計画的 ロールアウト - シナリオ 2	緊急 ロールアウト
お客様の導入戦略に準拠	お客様の導入戦略にほぼ準拠	導入戦略適用外
ロールアウトプロジェクト全体に十分時間をかけられる	ロールアウトを特定の日までに完了しなければならず、時間が限られている	緊急のためプロジェクト計画を策定している時間がほとんど、またはまったくない
エンドポイント用の標準ソフトウェアイメージを使用してテスト	エンドポイント用の標準ソフトウェアイメージを使用してテスト	ほとんど、またはまったくテストなし
アプリケーションとビジネスに不可欠なシステムをテスト	ほとんどのアプリケーションはテストし、一部のビジネスに不可欠なシステムは対象外	ビジネスに不可欠なシステムも対象外（最悪のシナリオ）
ロールアウト：標準イメージから開始し、段階的に重要なシステムを導入する。確実にロールアウトすることに重点を置いている。	**ロールアウト：**テスト後、使用可能なほとんどのシステムにソフトウェアをロールアウトする。ロールアウトの完了日に重点を置いている。	**ロールアウト：**緊急ロールアウトのため、セキュリティインシデント発生中に実際のセキュリティソリューションで保護できない、または EDR 機能がない。できるだけ速くロールアウトすることが必要。
⌄⌄	⌄⌄	⌄⌄
Secure Endpoint は、これらの各導入シナリオ（例）に対応しています。各シナリオにおいて、前の章で説明したベストプラクティスについて検討してください。		
時間にゆとりのある計画的なロールアウト。ビジネスに影響が及ぶリスクが最小。	ロールアウトはほぼ計画的に進められる。パフォーマンスに顕著な影響が及ぶ場合がある。ビジネスに影響が及ぶリスクが中程度。中断は、導入戦略として想定されている。	できるだけ速くロールアウトすることが必要。セキュリティまたは可視性を強化することが求められている。環境が侵害された場合のシナリオ。データ損失のリスクが、ソフトウェア導入によるリスクよりもはるかに高い場合に適用。EPP ソリューションしか導入されていない場合に、Cisco Incident Response サービスを適用する一般的な状況。ユーザーは中断を受け入れている。

注：これらは、セキュリティ製品のロールアウトに関するさまざまな状況を示すためのほんの一例です。

事前準備：簡易サマリー

1. 「Secure Endpoint の準備」セクションでは、Secure Endpoint アーキテクチャの概要、Connector がクラウドと通信する方法、Connector ソフトウェアのベースとなるアーキテクチャの概要、Secure Endpoint 環境を計画するためのベストプラクティスに関して多くの情報を示しました。Secure Endpoint は、SecureX Architecture に完全に統合されます。SecureX Architecture については、「SecureX – EDR/XDR/MDR アーキテクチャ」セクションで説明しています。
2. ポリシーの設計および管理 – パフォーマンスとセキュリティ」セクションでは、アカウントを有効にする方法や SecureX プラットフォームを有効にする方法および、ワークステーションまたはサーバーポリシーを構築するために役立つ情報を示しました。

Secure Endpoint のロールアウトに関するベストプラクティス

次のセクションでは、Secure Endpoint のロールアウトを成功させるためのインサイトとアイデアをいくつか示します。前の章ですでに説明したように、お客様の環境はそれぞれ異なっています。そのため、このフレームワークは、推奨例としてのみ利用し、お客様それぞれの状況に応じて調整する必要があります。

フェーズ 1：ラボ環境 - テストとロールアウト

ステップ 1：Secure Endpoint Console から Connector をダウンロードします。Connector をダウンロードする際、次の 2 つのことを検討します。

- 特定のバージョンの Connector でテストする場合は、次の 2 つのオプションがあります。
  - 最初に [アカウント（Accounts）] → [組織設定（Organization Settings）] で適切なバージョンを選択します（デフォルトは、最新の Connector バージョンです）。
  - ポリシー設定で Connector のバージョンを設定します。製品のアップグレードがポリシーに設定されていない場合は、[組織設定（Organization Setting）] が適用されます。
- ダウンロード時に、エンドポイントが属する**グループを選択**します。グループ ID は Connector パッケージに含まれています。インストール後、Connector はこの特定のグループに登録されます。

ベストプラクティス：Secure Endpoint Console の [アカウント（Accounts）] → [組織設定（Organization Settings）] で、自社の環境に定義されている Connector のバージョンを設定します。これで、全員が同じバージョンをインストールすることになります。それ以外の場合は、[管理（Management）] → [Connectorのダウンロード（Download Connector）] で、Secure Endpoint Console にアクセスできない管理者向けのダウンロード用 URL を生成します。

Windows、Linux、macOS に対する Connector の OS 互換性を確認します。

- **Windows**：ドキュメント ID：214847
- **Linux**：ドキュメント ID：215163
- **MacOS**：ドキュメント ID：214849
- その他の Secure Endpoint ドキュメント：cisco.com Web サイト参照

ステップ 2：ラボ内のマシンに Connector をインストールします。まずは標準的な企業イメージを使用してテストし、多数の企業エンドポイントから結果を収集します。できるだけ多くのソフトウェアコンポーネントをインストールしてみてください。

テスト手順

- 既存のセキュリティ製品を残す場合は、各製品が正常に機能していることを確認します。
- エンドポイントにログインし、ログインスクリプトが実行されていることを確認します。
- 標準アプリケーションを起動し、正常に機能していることを確認します。
- 専用プロキシまたはトランスペアレントプロキシを使用する場合は、プロキシ管理者に相談してください。
  - 企業ポリシーによって認証が要求される場合は、Secure Endpoint のプロキシ認証に専用のユーザーアカウントを使用します。サポートされていない NTLM 認証オプションについては、Secure Endpoint のヘルプを参照してください。
  - プロキシ管理者は、プロキシログから Secure Endpoint 接続を除外できます。特に、ログデータとコストを削減する必要があり、別のツール（splunk など）にログがアップロードされている場合は、除外して構いません。
- Secure Endpoint Console を開き、エンドポイントが Secure Endpoint クラウドに正常に接続されているかや、適切なポリシーがアクティブになっているかを確認します。また、Secure Endpoint Console で該当するイベントを確認します。
- 機能またはパフォーマンスの問題を特定します。これらの問題に対処する方法については、以下の「Connector 診断」セクションで説明します。

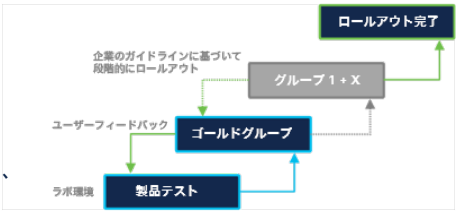
ベストプラクティス：常に既存の導入アーキテクチャ（Microsoft SCCM、Altiris など）に基づいてテストします。導入アーキテクチャでは、テスト用に多くのソフトウェアパッケージがすでに提供されています。ソフトウェアのインストールおよびアップグレード中には、インストーラによってシステム上の多くのファイルが変更されます。これらのファイルは Secure Endpoint のスキャン対象となります。また、ソフトウェアのインストールおよびアップグレードプロセス中にシステムパフォーマンスをモニターします。Secure Endpoint のインストール時に問題が発生した場合は、Windows インストーラの終了 コードを確認します。

ソフトウェア導入エージェントは、プロセスのスキャン対象から除外されます。セキュアなエリアでは、SHA-256 ハッシュも除外対象となります。

フェーズ 2：ゴールドユーザーグループ

ステップ 3：ビジネスに不可欠なアプリケーションを利用してテストするために、ゴールドユーザーグループを定義します。特定のアプリケーション機能によっては、ディスク上に新しいファイルが生成される場合があり、アプリケーションテストを IT 部門が行うことはできません。

- ゴールドユーザーは、特定のアプリケーション機能とパフォーマンスをテストします。
- ゴールドユーザーが簡単にフィードバックできるようにします。
- たとえば、モニタリングモードに設定されているグループに Connector を移動するなど、ユーザー向けの迅速なソリューションを検討します。



ヘルプデスク：ゴールドユーザーが実施するソフトウェアテストについて、ヘルプデスクに情報を提供します。ソフトウェアテストにヘルプデスクが参加できるよう、ゴールドグループにヘルプデスクユーザーを追加します。

IT 部門：ゴールドグループのテストに IT 部門のメンバーを追加しても構いません。IT 部門のメンバーは、技術的な知識が豊富で、適切なフィードバックを提供してくれることが多いからです。

システムオーナー：特定のエンドポイントのシステムオーナーについて検討します。システムオーナーと話し合って情報を伝え、システムの変更に参加してもらいます。製品の取り扱い方法、最悪の場合の対処方法、Secure Endpoint を無効にする方法を説明します。また、できるだけ早く、エンドポイントのアップグレード方法、アップグレードが可能な時期、必要な除外リストの設定方法に関する戦略を策定します。

ベストプラクティス：重要なソフトウェアは、適切なユーザーがテストする必要があります。ソフトウェア製品内の特定の機能には、特別な設定が必要な場合があります。重要なソフトウェアを単に起動しただけでは、必要な製品調整がわからない場合があります。

フェーズ 3：導入の準備

ステップ 4：導入用のパッケージを生成します。シスコでは、Microsoft SCCM、Altiris などの既存の導入アーキテクチャを使用することを推奨しています。

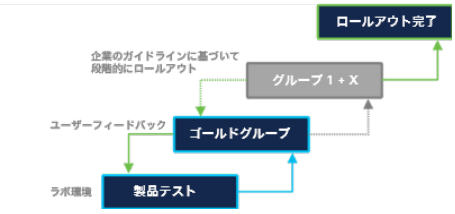
- 必要に応じて導入パッケージを定義します。
- 削除パッケージを定義します。
- 導入と削除のテストをします。

ベストプラクティス：Secure Endpoint Connector に指定可能なインストーラ コマンド ライン スイッチを確認します：
http://cs.co/AMP4E_Connector_Install_Switches

フェーズ 4：ロールアウト

ステップ 5：内部のガイドライン、ポリシー、定義された段階的なロールアウト方式に基づいて、環境内でロールアウトを開始します。必要に応じて、ロールアウトフェーズで新しい除外リストを追加します。

- ビジネスに不可欠なシステム：ビジネスに不可欠なシステムに Secure Endpoint を導入する場合は、まず監査モードにします。



ベストプラクティス：エンドポイントに新しいソフトウェアをインストールする際、Secure Endpoint でもその他のソフトウェアパッケージでも、問題が発生する可能性は常にあります。最悪な状況を想定して段階的にロールアウトすることで、インフラストラクチャへの影響を軽減できます。

Secure Endpoint：運用ライフサイクル

このセクションでは、Secure Endpoint の機能を最適化するための戦略について説明します。新しいオプション、機能、セキュリティ修正プログラムがリリースされたら、新しい Connector バージョンをレビューしてアップグレードし、保護機能を強化することをお勧めします。

インストールのテスト

- 正しく登録されていれば、Secure Endpoint Console でコンピュータ名を検索できます。

新たなエンジンと機能

Secure Endpoint の新機能がリリースされた際、新機能に新しいエンジンが含まれていたり、既存のエンジン用の新たなオプション設定が含まれていたりする場合があります。新しいリリースをテストする際は、既存の製品にはない新機能を有効にするか、Secure Endpoint で提供される機能を確認することをお勧めします。新しい機能を試す場合は、最初に監査設定を有効にしておくと便利です。ポリシーの変更、テスト、ロールアウトは、エンドポイントを中断せずに実施できます。

ベストプラクティス：Secure Endpoint によって CPU 負荷が大きくなる場合、非常に簡単かつ迅速に解決するには、各エンジンを段階的に無効にして、高負荷の原因となっているエンジンを特定します。特定の Secure Endpoint グループを作成すれば、影響を受けるエンドポイントに対してエンジンを無効にできます。

カスタム除外リスト

Secure Endpoint またはその他のパフォーマンスツールのログを確認することで、カスタム除外リストの対象を特定できます。

Secure Endpoint 診断パッケージを利用して除外対象を特定する手順は、次のとおりです。診断パッケージは、コマンドラインを使用してエンドポイント上で直接生成することも、Secure Endpoint Console のコンピュータプロパティから生成することもできます。

コマンドライン（Windows）：

- エンドポイントでデバッグロギングを開始します。デバッグロギングは、エンドポイント UI（Windows）で直接有効にできます。または、[詳細設定（Advanced Settings）] → [管理機能（Administrative Features）] → [Connectorログレベル（Connector Log Level）] のポリシーで有効にすることも可能です。
- 適切なコマンドラインパラメータを指定して、エンドポイントで **ipsupporttool.exe** を起動します。起動したら、適切な時刻を指定することで、問題を再現できます。ツール使用方法の詳細については、「Secure Endpoint のトラブルシューティング テクニカルノーツ」を参照してください。
- 結果ファイルは、デフォルトでユーザーのデスクトップに出力されます。

Secure Endpoint Console

- [管理（Management）] → [コンピュータ（Computers）] の順に選択し、コンピュータのプロパティに移動します。
- [診断（Diagnose）] ボタンをクリックします。
- ポップアップウィンドウでデバッグセッションの長さを選択し、[作成（Create）] ボタンをクリックします。
- Secure Endpoint Tray を開き、新しいポリシーを取得します。エンドポイントでデバッグロギングが自動的に有効になります。
- エンドポイントで問題を再現します。
- [分析（Analysis）] → [ファイルリポジトリ（File Repository）] で診断パッケージをダウンロードします。

診断パッケージの分析

- http://cs.co/AMP4E_Tuning_Tool からパフォーマンス チューニング ツールをダウンロードします。
- 診断パッケージとチューニングツールを同じディレクトリにコピーします。
- チューニングツールを実行し、結果を確認します。

ベストプラクティス：チューニングツールの結果を確認し、前の章のガイドラインに従って新しい除外対象を追加します。必要に応じて同じ手順を繰り返し、他に除外する必要のある対象を見つけます。

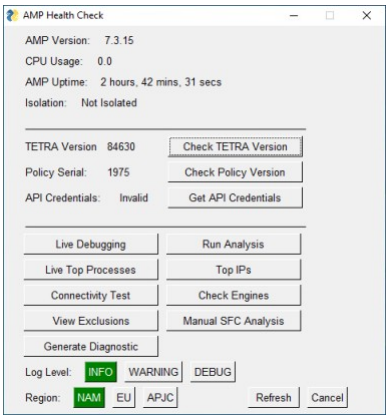
Secure Endpoint：トラブルシューティング

『Secure Endpoint Deployment Strategy Guide』には、トラブルシューティングに役立つ情報がすでに記載されています。

- パフォーマンス
- Outlook パフォーマンス
- クラウド接続
- デバイストラジェクトリに情報がない
- デバイストラジェクトリにネットワークイベントがない
- ポリシーが更新されない
- プロキシ
- Connector の重複
- シンプルカスタム検出
- アプリケーションブロック

ヘルスチェックツール

ヘルスチェックツールには、エンドポイントの問題を調査するための一連の機能が備わっています。ツールは、https://github.com/CiscoSecurity/amp-05-health-checker-windows からダウンロードできます。Live Debugging オプションを利用すれば、必要なスキャン除外対象を判断することもできます。

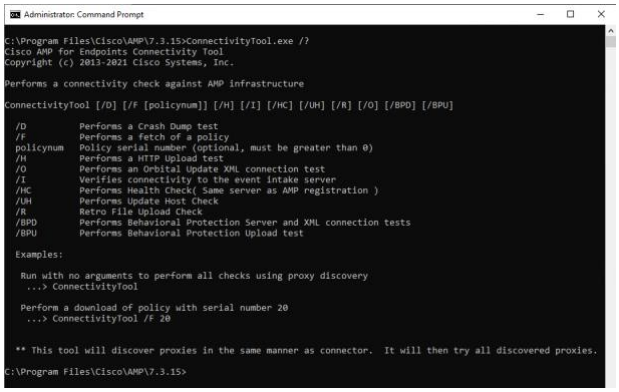


接続テストツール

このツールを利用すれば、ポリシーの取得、イベントのアップロード、Orbital の更新チェック、ふるまい保護エンジンのチェックなどをはじめ、いくつかの接続テストを実施できます。
すべての可能なオプションを表示するには以下の手順を実施します。

1. コマンドプロンプト（cmd）ウィンドウを開きます。
2. Connector のインストールディレクトリに移動します。
3. ConnectivityTool.exe /? と入力して Enter を押します。

利用可能なオプションについては、ヘルプを確認してください。



Secure Endpoint 診断バンドルの分析 - Windows および macOS で CPU 使用率が高い場合

CPU 使用率が高い場合のトラブルシューティング方法の詳細については、cisco.com の Web サイトを参照してください。

- Windows：https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/215261-analyze-amp-diagnostic-bundle-for-high-c.html
- macOS：https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/215570-analize-macos-amp-diagnostic-bundle-for.html

エクスプロイト防止機能で保護されたプロセス

エクスプロイト防止機能によって軽量の DLL が挿入され、メモリーが変更されると、アプリケーションがまれに予期しないふるまいをすることがあります。エクスプロイト防止機能の軽量 DLL が挿入された実行中のプロセスをすべてリストするには、Orbital を使用してエンドポイントを検索します。

- Orbital コンソールを開き、新しいクエリを開始します。
- **host:hostname** を検索対象として使用し、ホストを選択します。
- 次のカスタム SQL をコピーし、[ライブクエリ（Live Query）] ボタンをクリックします。

```
select DISTINCT p.pid, p.name AS "Process Name",
p.path AS "Process Path",
pm.path AS "DLL-Loaded-path",
sha256,
a.issuer_name AS "DLL-Cert-Issuer_Name",
a.subject_name AS "DLL-Cert-Subject_Name",
a.result
from processes p
LEFT JOIN process_memory_map pm ON p.pid=pm.pid
LEFT JOIN authenticode a ON pm.path = a.path
LEFT JOIN hash h ON pm.path = h.path
WHERE pm.path != ""
AND pm.path NOT LIKE "%windows\system32%"
AND pm.path LIKE "%.dll"
AND pm.path LIKE "%Protector64.dll%"
ORDER BY p.pid;
```

SecureX – EDR/XDR/MDR アーキテクチャ

Secure Endpoint は、SecureX プラットフォームに完全に統合されます。SecureX は、高度なハンティングツールとセキュリティ自動化機能を備え、エンドポイント製品を強化します。このアーキテクチャには、本ドキュメントの「クラウド インフラストラクチャ - 機能とサービス」セクションに記載されている機能が備わっています。最初のタスクの 1 つとして、SecureX を有効にすることを強くお勧めします。『SecureX Opt-In guide』に記載されている手順に従って、SecureX プラットフォームと SecureX SSO を有効にします。SecureX SSO の仕組みについては、『Cisco SecureX Sign-On クイックスタートガイド』を参照してください。

SecureX のその他の情報も確認してください。

- SecureX のドキュメント：http://cs.co/SXO_docs
- SecureX に関する FAQ：http://cs.co/SecureX_faq
- SecureX Youtube プレイリスト：http://cs.co/SecureX_videos
- SecureX Orchestration ワークフロー：http://cs.co/SXO_repo

ベストプラクティス：SecureX Architecture によっていかにセキュリティが強化され、セキュリティ調査がシンプルになるか考えてみましょう。SecureX および SecureX が提供する全機能は、任意の Secure Endpoint ライセンスで利用できます。

Secure Endpoint：自動アクション

Secure Endpoint には、4 種類の自動アクションが用意されています。機能の詳細については、『Secure Endpoint 製品ガイド』を参照してください。以下の自動アクションがあります。

- 侵害発生時にフォレンジック スナップショットを取得する
- 侵害発生時にコンピュータを分離する
- 検出時に Threat Grid に送信する
- 侵害発生時にコンピュータをグループに移動する

感染後自動アクション：コンピュータをグループに移動する

コンピュータをグループに移動するには、準備が必要です。感染後のタスクであるため、最高レベルの検出/保護を実現するポリシーを定義する必要があります。

- すべてのエンジンを有効にし、[保護（Protect）] または [検疫（Quarantine）] に設定します。詳細については、「ポリシー設定：最適なパフォーマンスとセキュリティ」セクションを確認してください。
- キャッシュを最も低い値に設定します。
- 可能な限り除外対象を削除します。
- ポリシーでオンデマンドスキャンを有効にします。

ベストプラクティス：グループシステムに適切なポリシーが適用されるように準備します。

感染後自動アクション：エンドポイントをネットワークから分離する

コンピュータをネットワークから分離する：Secure Endpoint 通信は対象から除外され、エンドポイントが分離されても常に機能します。この機能を有効にする前に、ロギングやリモートアクセスのための中央システムへの通信など、どの通信を機能したままにする必要があるかを検討します。

ベストプラクティス：この機能を有効にする前に分離 IP 許可リストを定義し、エンドポイントに必要な通信を確立しておきます。

Secure Endpoint：ファイル分析

Secure Endpoint のバックエンドプロセスがファイルを自動的に要求することはありません。Secure Endpoint の [分析（Analysis）] -> [感染状況（Prevalence）] -> [自動分析の設定（Configure Automatic Analysis）] で、感染状況分析を有効にする必要があります。

SecureX：統合モジュール

シスコは、シスコおよびサードパーティの製品とすぐに統合できる機能を用意しています。他製品と統合することで、ハンティング エクスペリエンスが大幅に向上します。

- 利用可能なシスコ製品用の統合モジュールを設定します。SecureX がサポートしている製品を確認してください。
- シスコがホストしているモジュールを利用して、サードパーティ製品との統合を設定します。これらのモジュールは、シスコとサードパーティベンダー間のデータを自動的に変換します。

ベストプラクティス：設定されたすべてのモジュールは、調査時の情報検索対象となります。利用可能なすべての統合モジュールを設定することを強くお勧めします。

SecureX：Pivot Menu

Pivot Menu は、SecureX をベースにしたセキュリティツールで、多くの Cisco Secure 製品の UI で利用できます（対象拡大予定）。Pivot Menu を使用すると、監視対象に関して製品間で相互に利用できるレピュテーション情報を即座に取得し、インストール済みの製品全体で、一般的な調査/対応アクションを非常に簡単に実行できます。

SecureX：Threat Response

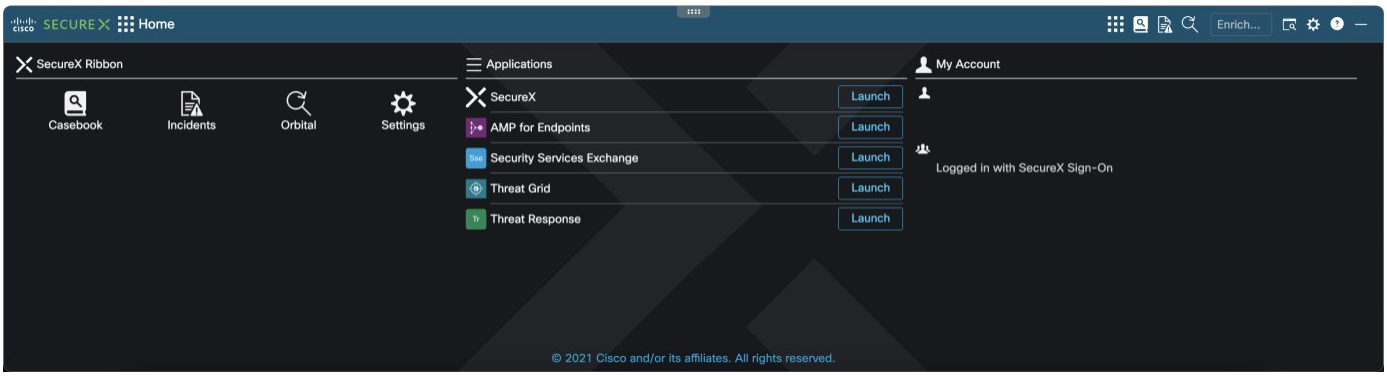
SecureX Threat Response を利用すれば、SecureX 統合製品の多くの領域から調査を行えます。ハッシュ、IP、ドメインなどのタイプの監視対象が UI に表示されるたびに、SecureX Threat Response を利用して直接調査できます。

ベストプラクティス：SecureX Threat Response を利用すれば、脅威を簡単に調査できるようになるため、有効にすることをお勧めします。

SecureX：Ribbon

Cisco SecureX は、一元化されたコンソールであり、さまざまな機能を統合したプラットフォームでもあります。可視化機能の統合、自動化、インシデント対応ワークフローの促進、脅威ハンティング機能の強化を実現します。これらの各種機能は、アプリケーション（アプリ）とツールの形で SecureX Ribbon に表示されます。SecureX ヘルプで SecureX Ribbon の詳細を確認してください。

- SecureX Ribbon - 概要
- SecureX Ribbon - ケースブックアプリ
- SecureX Ribbon - インシデントアプリ
- SecureX Ribbon - Orbital アプリ



付録 A：Secure Endpoint プライベートクラウド

プライベートクラウドとパブリッククラウドの主な違いは次のとおりです。

インフラストラクチャ	メリット	デメリット
パブリッククラウド	• エンドポイント機能が最初に導入される • ローミングエンドポイントはクラウドに接続したまま	• 内部ネットワークをパブリッククラウドサーバーに接続する必要がある
プライベートクラウド	• オンプレミスのクラウドサーバーを使用するため、エンドポイントのデータプライバシーが確保される • エンドポイントにサービスを提供するための専用リソースが使用される	• ハードウェアにより、サポートできるアクティブエンドポイントの数が制限される

考慮事項：パブリッククラウドとプライベート クラウド アプライアンスの違い

Secure Endpoint には、**パブリッククラウド**と**プライベート クラウド アプライアンス**の 2 つの導入オプションがあります。2 つのオプションの違いを理解して、自社の組織に最適なものを選択することが重要です。

パブリッククラウド

- Secure Endpoint パブリッククラウド（クラウド ネイティブ アプローチ）は、お客様が選択する最も一般的なオプションです。この導入方式では、エンドポイントを管理するためのサーバーリソースが不要で、新しい機能をすぐに利用できます。そのためシスコでは、柔軟性が高いこの方式を推奨しています。

プライベート クラウド アプライアンス

- Secure Endpoint プライベート クラウド アプライアンスは、お客様の環境内でホストされます。この導入オプションを選択すると、すべてのエンドポイント テレメトリ データを直接管理できるため、組織のプライバシーを確保できます。
- Secure Endpoint プライベート クラウド アプライアンスには、仮想アプライアンスと物理 UCS アプライアンスの 2 つの形態があります。各オプションには独自の要件があるため、購入を決定する前に慎重に評価する必要があります。
- Secure Endpoint プライベート クラウド アプライアンスのどちらのバージョンにも、主要な動作モードが 2 つあります。
    a. **プロキシモード：**企業の Web プロキシを使用してクラウドに接続する。
    b. **エアギャップモード：**クラウドには一切接続しない。
- Secure Endpoint プライベートクラウドのほとんどのお客様は、プロキシモードでアプライアンスを稼働させています。プロキシモードは、プライベートクラウドを導入する際に推奨される設定です。
- エアギャップモードは、仮想プライベートクラウド環境では利用できなくなっていて、利用するには物理 UCS HW を導入する必要があります。このモードは、厳格なプライバシー要件への対応が必要なお客様、または外部ネットワークに接続できないお客様向けのものです。

Secure Endpoint プライベートクラウドの詳細については、cisco.com の Web サイト（https://www.cisco.com/c/ja_jp/support/security/fireamp-private-cloud-virtual-appliance/series.html#~tab-documents）にあるドキュメントを参照してください。

詳細：パブリッククラウドとプライベートクラウドの比較

次の表に、Secure Endpoint のパブリッククラウドとプライベート クラウド アプライアンスの主な違いを示します。

機能	パブリッククラウド	プライベートクラウド	情報
導入			
ロケーション	クラウドの各リージョンの DC	仮想アプライアンスまたはハードウェアアプライアンス	Deployment Strategy Guide
プライバシー	マネージドクラウドサービス	プロキシモードまたはエアギャップモード	Cisco Trust Portal
導入規模	マネージドクラウドサービス	HW アプライアンスで 100,000 エンドポイントをサポート	仮想アプライアンスのサイジング
高可用性	マネージドクラウドサービス	コールドスタンバイ	
信頼性	マネージドクラウドサービス	バックアップおよび復元プロセス	
MSSP ポータル	利用可能	該当なし	
ポリシーおよび機能			
Connector のポリシー	利用可能な最新機能	○	
エンドポイントエンジン	利用可能な最新機能	○	
サポートされる OS	Win/Linux/macOS/iOS/Android	Win/Linux/macOS/iOS/	リリース ノート参照
アイデンティティ永続化	○	○	
エンドポイントの分離	○	○	
アクションの自動化	○	○	
→ グループに移動	○	○	
→ エンドポイントの分離	○	○	
→ 分析用にファイルを送信	○	○	
→ フォレンジック スナップショット	○	×	Orbital が必要*1
SecureX およびハンティングサービスへの統合			
SecureX	○	×	
Cognitive Analytics	○	×	
Threat Response	○	×	
Advanced Search（Orbital）	○	×	
Secure Malware Analytics			
クラウド	○	×	
オンプレミスアプライアンス	×	○	

*1：フォレンジック スナップショットには Orbital Cloud Service が必要です（オンプレミス環境では利用できません）。

付録 B：仮想環境（VDI）

概要 - VDI とマルチユーザー環境

仮想デスクトップ インフラストラクチャ（VDI）やマルチユーザー環境（Terminal Server、Hyper-V、VMware など）において、仮想プラットフォームを停止させたり、パフォーマンスを低下させたりせずに Secure Endpoint をインストールするには、詳細な計画が必要です。市場には非常に多くの仮想化オプションが存在しているため、すべてをここに記載することはできませんが、次のセクションで、仮想化環境の概要と、Endpoint の追加を慎重に計画する必要がある理由について簡単に説明します。

注：Microsoft、VMware、Citrix、Open Stack などの仮想化ベンダーが提供するベストプラクティスガイドを確認してください。

ベストプラクティス：仮想環境 OS のサポート
仮想デスクトップ オペレーティング システムがサポートされている場合、Secure Endpoint は VDI ベンダーに依存しません。Secure Endpoint が VDI 環境を停止させることなく機能するようにするには、仮想環境で特別な設定が必要です。

エンドポイント仮想化とアプリケーション仮想化の比較

- **エンドポイント仮想化：**仮想化プラットフォームによって、ユーザーは、**仮想デスクトップ機能をすべて**利用できます。IT 部門にとってのメリットは、デスクトップを簡単に再構築できることです。管理者は、いくつかの手順を実行するだけで、**ゴールデンイメージ**を利用して仮想エンドポイント全体を再導入できます。

  仮想化プラットフォームは、多くの場合、お客様の**導入戦略**で検討されています。新しいアプリケーションが必要な場合は、新たなバージョン番号の新しいゴールデンイメージを作成します。IT 部門は、最新の変更によって悪影響がある場合などに、新しいイメージをテストします。テストが完了すれば、すべてのエンドユーザー仮想システムを再導入できます。問題がある場合、IT 部門は、前のイメージに戻せます。

  ユーザープロファイルに保存されているユーザー**設定**を損なわず、ユーザーがどこからログオンしてもすべての設定を提供できるように、**ローミング ユーザー プロファイル**などの機能が利用されます。これらのプロファイルには、アプリケーション設定、ブラウザのお気に入りやキャッシュ、デスクトップアイコンなどのデータが含まれています。ログオン中、プロファイルは、ネットワーク共有ロケーションからローカルマシンにコピーされます。ユーザーがログオフすると、プロファイルはネットワーク共有ロケーションに戻されます。ユーザープロファイルに関する課題としては、ユーザーディレクトリに保存される**ファイルの数が多くなる**ことが挙げられます。多くの場合、ローミングプロファイルが保存されているネットワーク共有ロケーションへのアクセスには、**SMB プロトコル**が利用されます。

  エンドユーザーは、ローカルにインストールされたアプリケーションがなくても、適切に設定された Windows 10 エンドポイント（アクセスするためだけのデバイス）を使用して仮想デスクトップにアクセスできます。もう 1 つのオプションは、軽量のターミナルを使用する方法です。ターミナルは、仮想デスクトップにアクセスするクライアントを含む、軽量の Linux イメージをブートします。

  サマリー：エンドユーザーにとっては一般的な Windows 10 エンドポイントなどのように見えますが、バックエンドのアーキテクチャは、物理的なデスクトップやノートブックとはまったく異なります。

- **アプリケーション仮想化：**このアプローチは、アプリケーションのみが「仮想化」されるため、エンドポイントの仮想化とは異なります。つまり、アプリケーションはユーザーのエンドポイントにはインストールされず、仮想化プラットフォームから「ストリーミング」されます。
  例
  1. ユーザーは、デスクトップのアイコンからアプリケーションを起動します。
  2. 仮想化バックエンドでは、ユーザーは別のホストにログオンしています。たとえば Windows Terminal Server などです。アプリケーションを起動するエンドユーザーがこの仕組みを認識することはありません。
  3. バックエンドにログオンするとアプリケーションが開始され、ユーザーのデスクトップにストリーミングされます。

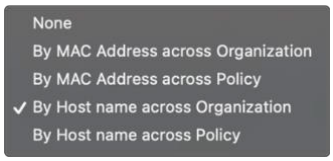
- **両方のアプローチの共通点：**現在はさまざまなアプローチがあります。2 つだけ例を取り上げます。どちらのシナリオでも、バックエンドで**ストレージシステム**を使用しています。ユーザーログオン時に **SMB プロトコル**を使用する場合、ストレージを仮想化ホストに接続する一般的な方法は **iSCSI** です。
  いずれにせよ、何らかの**ネットワークレイヤ通信**が発生します。ローカルディスクからのアクセスとネットワークレイヤからの**アクセスにかかる平均時間**は大きく異なります。仮想化環境とストレージシステムは、アクセス時間の問題を軽減するためのさまざまな機能を提供しています。
  このようなシナリオにおいて **Secure Endpoint を設定する際は**、特定のファイルをスキャンすることでパフォーマンスを低下させないようにする必要があります。

お客様サイトを担当している IT 管理者と連携し、仮想化環境を詳細に把握してから導入することをお勧めします。注：お客様サイトのさまざまなチームが仮想環境を担当する場合と、Cisco Secure Endpoint ソリューションを管理するチームが担当する場合があります。

VDI およびマルチユーザー環境に Secure Endpoint をインストールする

現時点では、Secure Endpoint と仮想化製品は互換性があります。サポートされている OS であれば、Secure Endpoint をインストールできます。適切に機能するように、Secure Endpoint にはいくつかの機能とオプションが用意されています。次のセクションでは、利用できるオプションを示します。まずはバックエンドの準備に関してです。

アイデンティティ永続化



さまざまなシステムが VDI のために頻繁に再導入されたり、IT サポートによってエンドポイントが再インストールされたりすることがよくあります。どちらの場合もシステム名は変更されず、レジストリ内に Secure Endpoint Connector の GUID が新たに生成されます。Endpoint のバックエンドでは、この新しい Connector GUID に基づいて、新しいコンピュータオブジェクトが生成されます。この問題は、Endpoint のバックエンドでアイデンティティ永続化機能を有効にすることで解決できます。この機能は **TAC が有効にする**必要があります。この機能が有効になれば、**Endpoint のポリシー**で新しいオプションを使用できるようになります。

Cisco Secure Endpoint でアイデンティティ永続化を有効にする：
https://www.cisco.com/c/ja_jp/support/docs/security/advanced-malware-protection-endpoints/200318-Deployment-of-Cisco-AMP-for-Endpoints-wi.html

アイデンティティ永続化の設定

- [管理（Management）] → [ポリシー（Policies）] に移動し、該当するポリシーを選択します。
- ポリシーで [詳細設定（Advanced Settings）] → [アイデンティティ永続化（Identity Persistence）] に移動し、適切な設定を行います。

この機能が不要な場合は有効にしないでください。

ベストプラクティス：アイデンティティ永続化が 1 つのグループで有効になっていて、他のグループでは無効になっている場合、グループ間でエンドポイントを移動する際には、注意してください。移動することで、コンピュータアカウントが重複する可能性があります。エンドポイントが自動的に別のグループに移動される、またはエンドポイントが頻繁に再インストールされる状況で自動アクションを利用する場合は、**すべてのグループでアイデンティティ永続化を有効にする**ことを強くお勧めします。

ベストプラクティス：アイデンティティ永続化は VDI のみに関連するものではなく、Secure Endpoint が仮想システムにインストールされている場合に一般的に利用されます。VDI 環境では、エンドポイントの再イメージングが頻繁に行われます。アイデンティティ永続化機能は、システムが頻繁に再導入される場合にいつでも利用できます。MAC アドレスまたはホスト名でシステムを特定し、環境に適したアプローチを検討してください。

ゴールデンイメージとエンドポイントの複製

- ゴールデンイメージを作成する必要がある場合は、**/goldenimage** コマンドラインスイッチを指定して Connector をインストールします。詳細については、https://www.cisco.com/c/ja_jp/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html を参照してください。
- Secure Endpoint がすでにインストールされているシステムを複製する場合は、必要な手順が異なります。こちら（https://www.cisco.com/c/ja_jp/support/security/fireamp-private-cloud-virtual-appliance/products-tech-notes-list.html）を参照してください。

注：Secure Endpoint は、30 回分までシグネチャの増分更新を行います。その後は、シグネチャセット全体がダウンロードされます。ゴールデンイメージは、長期間使用されることが多いため、増分更新の制限を超える場合があります。制限を超えている場合に、新しい VDI システムが該当のゴールデンイメージから導入されると、Secure Endpoint では常にシグネチャセット全体がダウンロードされます。このような場合は、クラウドへの通信の帯域幅を確保し、更新プロセスを速めるために、Tetra Update Server を導入します。

Endpoint トレイアイコン

Secure Endpoints の sfc.exe プロセスでは、トレイアイコン接続が 1 つしか認められていません。Terminal Server などのマルチユーザー環境では、ポリシーでトレイアイコンを完全に無効にします。無効にしないと、sfc.exe プロセスがトレイアイコンプロセスに接続できないため、トレイアイコンに誤った情報が表示されます。

ベストプラクティス：Terminal Server など、複数のユーザーが 1 つのシステムにログインしている環境では、ポリシーでトレイアイコンを無効にします。

除外と機能の無効化

以下に示す特定のタイプのアプリケーションを除外します。前の章で説明したように、ディスクアクティビティの多いプロセスを除外することで、バックエンドのストレージシステムのパフォーマンス低下を防ぎます。さらに、以下に示すように、ディスクアクティビティを多く生成する Secure Endpoint の機能を無効にします。

- スタートアップ集約型アプリケーションは除外します。
- プロファイリング/インベントリツールはホワイトリストに登録する必要があります。
- インストール時にフラッシュスキャンを無効にし、オンデマンドスキャンをなしにします。
- エンドポイント IOC スキャンをなしにします。
- 仮想化ベンダーが提供するすべてのプロセスを除外します。たとえば、アプリケーションを仮想化するすべての Citrix プロセスなどです。

Tetra エンジン：シスコでは、コマンドライン引数 **/skiptetra 1** を指定して Secure Endpoint をインストールすることで、仮想環境で Tetra AV を使用しないようにすることを推奨しています。AV スキャンが必要な場合は、段階的に Tetra をインストールし、新たなエンドポイントにインストールする前に、システムとストレージのパフォーマンスをモニターします。

ネットワーク（DFC）：仮想化するシステムは、多くのネットワーク帯域幅を必要とします。**/skipdfc 1** コマンドライン引数を指定して、ネットワーク DFC なしで Secure Endpoint をインストールします。

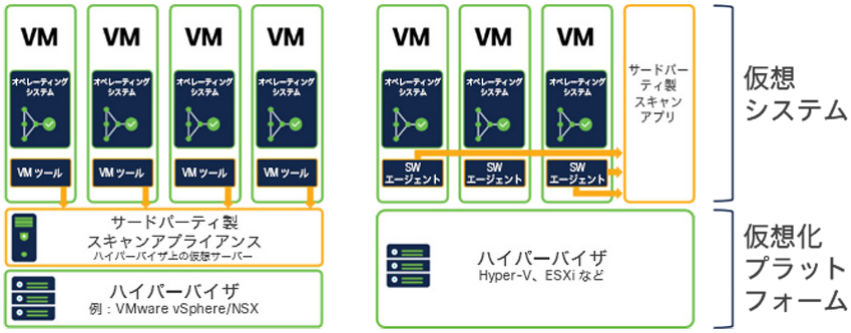
ブートストーム - 注：マルチユーザー環境に Tetra AV をインストールする場合は、エンドポイントが起動し、ユーザーがログインする際のブートストームについて考慮してください。

ベストプラクティス：ディスクパフォーマンスと Secure Endpoint の機能
→ **ベストプラクティス - パフォーマンス：**設定する際には、多くのファイルをスキャンすることで大量のディスクアクティビティが発生しないように考慮します。
→ **ベストプラクティス - ネットワークのパフォーマンスと安定性：**ネットワークドライバなしで Secure Endpoint Connector をインストールします。

ネイティブハイパーバイザの統合と Secure Endpoint

ネイティブ仮想化統合：ゲスト OS が Secure Endpoint でサポートされている場合、Secure Endpoint を仮想環境にインストールできます。仮想環境でファイルをスキャンするには、3 つの一般的な統合方法/アプローチがあります。各システムには、それぞれの観点からメリット/デメリットがあります。

- **オプション：**ハイパーバイザレベルで直接スキャン（例：VMware NSX）
- **オプション：**仮想スキャンアプライアンスを利用（スキャンプロセスは、VM 内のエージェントによってスキャンアプライアンスに移される）
- **オプション：**VM で Endpoint Security を直接実行



多くのお客様にとって、ファイルスキャンによるリソース消費は、導入する際の重要な考慮事項です。そのため多くの場合、スキャンプロセスは専用のアプライアンスに移されます。このようなアプローチはスキャンにしか当てはまらず、この設計では、EDR 機能やふるまいベースのエンジンが考慮されていません。そのため多くのベンダーが、仮想マシンにソフトウェアエージェントをインストールしています。

注：Secure Endpoint は常に仮想マシン内にインストールされます。現在シスコは、ハイパーバイザレベルでファイルを直接スキャンしていません。

次の表に、仮想化シナリオの主な違いを示します。シスコは、競合他社の製品や機能について、最新の変更内容やアプローチをすべて把握しているわけではありません。この表は、主な機能を理解するためのものです。常に最新の製品ドキュメントを調査し、お客様の IT チームと連携して慎重に計画してください。また、次の表には、サービスアプライアンスと追加のエンドポイントが導入されるハイブリッドソリューションは含まれていません。各アプローチの基本的な違いについて理解することが目的です。

	ハイパーバイザレベルのスキャン	サービスアプライアンスでのスキャン	VM 内でのスキャン	情報
導入				
Secure Endpoint の導入	×	×	○	
エンドポイントソフトウェア	VMware ツール	ソフトウェアエージェント	Secure Endpoint	
スキャンアプライアンスのインスタンス数	ハイパーバイザあたり 1	エンドポイントあたり 1	該当なし	
スキャンエンジンのロケーション	ハイパーバイザ（VM）	サービスアプライアンス（VM）	VM 内	
ファイルあたりのスキャン数（ワーストケース）	ハイパーバイザごとに 1 回	アプライアンスごとに 1 回	ホストごとに 1 回	← 同じファイルを複数回スキャンすると、ストレージシステムに高い負荷がかかり、遅延が発生する可能性があります。
スキャンサービスとの通信	IP ベース	IP ベース	VM 内のドライバ	VM とスキャンサービス間の通信
高可用性	×	○	該当なし	
停止時の影響	ハイパーバイザ上のすべての VM	アプライアンスに接続されているすべての VM	単一の VM	
リソース消費量	ハイパーバイザあたり 100 ～ 200MB	エンドポイントあたり 100 ～ 200MB	エンドポイントあたり 100MB	リソース消費量をどこまで削減できるかは、1 つのハイパーバイザでホストされるエンドポイントの数など、アーキテクチャによって異なります。多くの場合、どこまでリソースを削減できるかはお客様にとって重要な問題です。リソース消費量は、ハードウェアあたりの VM 密度の影響を受けます。
例：1000 VM（RAM 使用量）	1 ～ 2 GB RAM（ハイパーバイザあたり 100 VM）	アプライアンス用に 100 ～ 200 MB。1 GB（エンドポイントあたり 10 MB）	10 GB（VM あたり 100 MB）	仮想インフラストラクチャ上でのファイルスキャンに使用する RAM の量

	ハイパーバイザレベルのスキャン（EDR）	サービスアプライアンスでのスキャン（EDR）	VM 内でのスキャン（EDR）	情報
保護と EDR				
ファイルスキャン	○	○	○	
プロセス情報	×	一部	○	
オンデマンドスキャン	×	×	○	
機械学習	×	×	○	
ふるまいエンジン	×	×	○	エンドポイントのふるまいに関する詳細情報が必要です。
感染後タスク	×	×	○	
高可用性	×	○	該当なし	
リアルタイムフォレンジック	×	×	○	
リソース消費量	ハイパーバイザあたり 100 ～ 200MB	エンドポイントあたり 100 ～ 200MB	エンドポイントあたり 100MB	リソース消費量をどこまで削減できるかは、1 つのハイパーバイザでホストされるエンドポイントの数など、アーキテクチャによって異なります。多くの場合、どこまでリソースを削減できるかはお客様にとって重要な問題です。リソース消費量は、ハードウェアあたりの VM 密度の影響を受けます。
例：1000 VM（RAM 使用量）	1 ～ 2 GB RAM（ハイパーバイザあたり 100 VM）	アプライアンス用に 100 ～ 200 MB。1 GB（エンドポイントあたり 10 MB）	10 GB（VM あたり 100 MB）	仮想インフラストラクチャ上でのファイルスキャンに使用する RAM の量

サマリー：仮想化環境とのさまざまな統合機能によって、スキャン用リソースを専用システムに移行し、RAM と CPU の使用量を削減できます。エンドポイント コンポーネントを追加できないようなソリューションにはエンドポイント保護機能や EDR 機能がなく、以下のような感染後タスクも用意されていません。
- エンドポイントをネットワークから分離するタスク
- フォレンジック スナップショットを生成するタスク
- エンドポイントのふるまいによってトリガーされる高度なファイル分析タスク

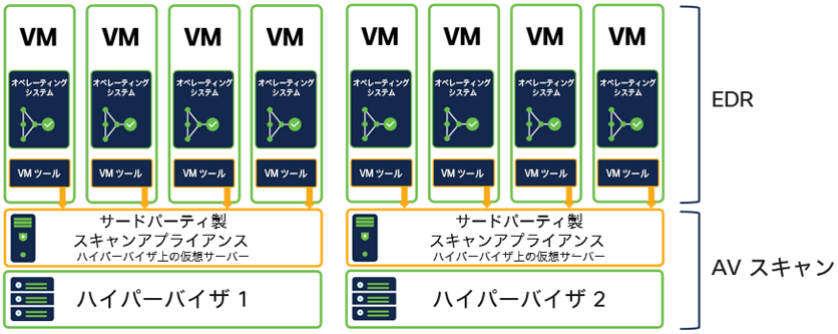
ベストプラクティス：エージェントレススキャン製品がすでに導入されている場合は、/skiptetra 1 インストールスイッチを指定して、Tetra エンジンなしで Secure Endpoint Connector をインストールします。Tetra が無効になっているポリシーを使用することも可能です。このポリシーを使用すると、Secure Endpoint を再インストールせずに AV スキャンを有効にできます。

統合：ハイパーバイザごとのスキャン（VMware など）

説明：サードパーティのスキャン用アプライアンスがハイパーバイザに導入されています。このアプライアンスは、AV スキャン専用です。

ハイパーバイザによる AV スキャンに関するインサイト

- スキャン用アプライアンスではプロセス情報は利用できません。
- オンデマンドスキャンはできません。
- 除外できるのはパスのみです。プロセスは除外できません。
- スキャン用アプライアンスを自動導入できます（ベンダーに依存）
- VMware ツールをインストールする必要があります。
- AV スキャンと EDR 以上の保護をするには、VM 内にソフトウェアコンポーネントを追加しなければなりません。



Secure Endpoint の導入

- /skiptetra 1 インストールスイッチを指定して、Tetra なしで Secure Endpoint をインストールします。
  - 重複スキャンは可能ですが、より多くのシステムリソースが必要になるため、推奨されません。
- 他のすべてのエンジンは、前のセクションのガイドラインに基づいてインストールできます。

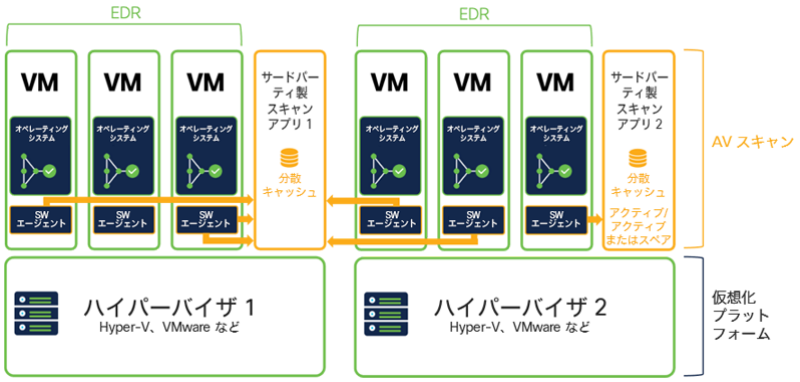
情報：VMware 社が Carbon Black 社と Lastline 社を買収しましたが、買収によって提供される新機能は、このドキュメントには含まれていません。

統合：スキャン専用ノード（Hyper-V、Citrix、OpenStack など）によるスキャン

説明：スキャン専用アプライアンスを使用して、複数のハイパーバイザにわたって仮想システムのコンテンツをスキャンします。1 つのアプライアンスを使用して、異なるハイパーバイザとバージョンでホストされている仮想エンドポイントをスキャンすることもできます。

専用アプライアンスによる AV スキャン

- ハイパーバイザ プラットフォーム全体で多くのエンドポイントを処理可能
- 分散キャッシュ（ベンダーに依存）
- VM のソフトウェアエージェントがスキャンのためにファイルを送信
- プロセスに基づいて除外可能（ベンダーに依存）
- オンデマンドスキャンなし



Secure Endpoint の導入

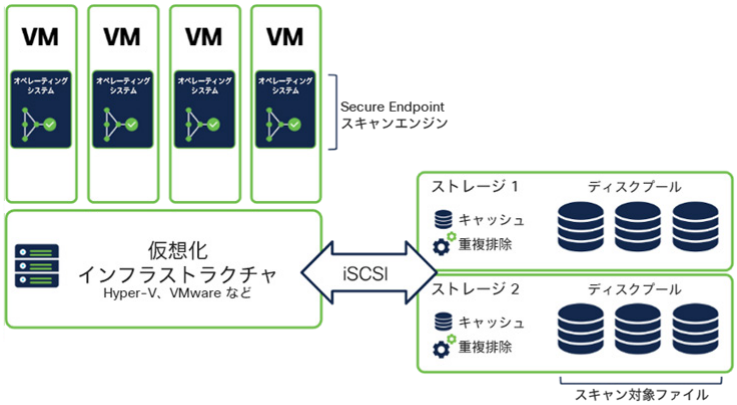
- /skiptetra 1 インストールスイッチを指定して、Tetra なしで Secure Endpoint をインストールします。
  - 重複スキャンは可能ですが、より多くのシステムリソースが必要になるため、推奨されません。
- 他のすべてのエンジンは、前のセクションのガイドラインに基づいてインストールできます。
- ファイルをスキャン用アプライアンスに転送するソフトウェアエージェントを除外します。

仮想環境でのオンデマンド/IOC スキャン

以下の図は、仮想環境の簡単な例を示しています。iSCSI を使用して 1 つ以上のストレージシステムがハイパーバイザに接続されています。また、複数の仮想システムがハイパーバイザによってホストされています。

- Secure Endpoint が仮想マシンのメモリーで実行されています。
- オペレーティング システム ファイルは、ストレージシステムに格納されています。

ファイルをスキャンするには、ストレージシステムから仮想マシンにすべてコピーする必要があります。同じファイルが複数の仮想システムで使用されている場合は、ファイルを複数回コピーしなければなりません。



ベストプラクティス - オンデマンドスキャン：仮想環境ではオンデマンドスキャン（ファイルスキャンと IOC スキャン）を実行しないようにします。お客様のセキュリティガイドラインとして OD スキャンが必要な場合は、エンドポイントを異なるグループに分け、すべてのエンドポイントでスキャンが同時に始まらないようにします。

Microsoft Windows Terminal Server の推奨設定

Microsoft Terminal Server にはいくつかの特殊な特性があるため、Secure Endpoint を適切に設定することが重要です。

特性：

- 一度に複数のユーザーセッションが発生する。
- 多くの場合、リモート ネットワーク ドライブに保存されているローミングプロファイルが利用される。その結果、ユーザーのログオン時とログオフ時にネットワーク帯域幅の使用量が多くなる。ローミングプロファイルには、ローカルドライブにコピーされる何千ものファイルが含まれている。
- 多くのログイン/ログアウトが同時に発生することで、Terminal Server システムに高い負荷がかかる。
- メモリー内で多数のアプリケーションが実行される。
- 実行中のアプリケーションによって多くのディスクアクティビティが生成される。

推奨設定

- Terminal Server 専用のグループおよびポリシーテンプレートを定義します。
- Microsoft Windows 用のシスコ管理除外リストを割り当てます。
- 仮想化システムに関連するプロセスを除外します。Microsoft 社の Web サイト（https://social.technet.microsoft.com/wiki/contents/articles/18439.terminal-server-antivirus-exclusions.aspx）で推奨されている、Terminal Server AV 除外リストを確認します。
- 上記のポリシーに従って、Secure Endpoint のトレイアイコンを無効にします。
- ポリシーでネットワーク保護を無効にします。それでもネットワークのパフォーマンスに問題がある場合は、**/skipdfc** インストールスイッチを指定して Endpoint を再インストールします。詳細については、導入ガイドを参照してください。概要は、このガイドの「Secure Endpoint の準備と運用ライフサイクル」セクションにまとめてあります。
- メモリーに対する変更によって Terminal Server 環境で問題が発生する可能性があるため、悪意あるアクティビティ防御エンジンとエクスプロイト防御エンジンは慎重にテストする必要があります。まずは監査モードで開始し、段階的に保護モードに切り替えます。
- ディスクパフォーマンスの問題が発生しないように、Terminal Server にはオンデマンドスキャンを実施しないでください。お客様が必要とされている場合は、Terminal Server にユーザーがログオンしていない時間帯に行います。スキャンプロセスのスピードを上げるために、ディスクの一部をスキャンするなど、オンデマンドスキャンの範囲を限定するさまざまなオプションを利用します。

Microsoft Hyper-V の推奨設定

Microsoft Hyper-V は、他のオペレーティングシステムを仮想化します。仮想デスクトップ オペレーティング システムがサポートされている場合、Secure Endpoint は VDI ベンダーに依存しません。仮想 VM はすでに保護されているため、パフォーマンス上の理由から、Hyper-V プラットフォームには Endpoint Security はインストールされていません。お客様の要件としてハイパーバイザ プラットフォームを保護する必要がある場合、Secure Endpoint を適切に設定する必要があります。

Microsoft Hyper-V 用ポリシーの構築

- Microsoft Hyper-V システム専用のグループおよびポリシーテンプレートを定義します。
- Microsoft Windows 用のシスコ管理除外リストを割り当てます。
- Microsoft 社が推奨する除外リストを追加します（https://docs.microsoft.com/en-us/troubleshoot/windows-server/virtualization/antivirus-exclusions-for-hyper-v-hosts）。
- ハイパーバイザがクラスタ化されている場合は、Microsoft 社の推奨（https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-exclusions-microsoft-defender-antivirus?view=o365-worldwide）に基づいて、クラスタ除外対象を追加します。
  - クォーラムディスクが設定されている場合は、パス全体をスキャン対象から除外する必要があります。クォーラムディスクに関する Microsoft 社の情報を確認してください（https://docs.microsoft.com/en-us/windows-server/failover-clustering/manage-cluster-quorum）。
- ポリシーでエクスプロイト防止機能と悪意あるアクティビティ防御機能を**無効にします。**
- Hyper-V システムでオンデマンドスキャンを**無効化/削除します。**
- ネットワークのパフォーマンスは、Hyper-V システムにとって重要です。**/skipdfc** インストールスイッチを指定して Secure Endpoint をインストールし、Secure Endpoint ネットワークドライバをインストールしないようにします。
  - **ポリシーで Secure Endpoint 製品の更新を無効**にします。内部機能を使用して Connector を更新する場合は、標準のインストールコマンドラインを使用できます。

ベストプラクティス：Microsoft Hypervisor System に Secure Endpoint をインストールする場合は、常に慎重にテストしてください。VM が実行されているシステムにはインストールしないでください。

SecureX Threat Hunt：お客様が仮想化プラットフォームで Microsoft Defender を使用している場合は、SecureX Microsoft Graph Security API モジュールを有効にできます。有効にすることで、SecureX Threat Response の Threat Hunt 実施中に Microsoft 社のセキュリティ情報を確認できます（https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWm9G4）。

パブリッククラウド環境の仮想システム

仮想ワークロードの OS がサポートされている場合、Secure Endpoint は任意の仮想化プラットフォームにインストールできます。Amazon Web Services（AWS）などのパブリッククラウド環境では、パフォーマンスに応じてコストが発生します。そのため、Secure Endpoint を適切に設定することで、コストを削減できます。

- パブリッククラウド環境の仮想 OS が Secure Endpoint でサポートされているかどうかを確認します。このドキュメントの「サポートされるオペレーティングシステム」セクションを確認してください。cisco.com の Web サイトでは、公式にサポートされている OS の情報をチェックできます。
- 「ポリシーの設計および管理 – パフォーマンスとセキュリティ」セクションを確認し、リソースへの影響が少なくなるように Secure Endpoint のポリシーを設定します。
- オンデマンドスキャンは、必要な場合、または侵害が想定される場合に**のみ**有効にします。そのような場合、自動アクション機能を有効にして、クラウド IOC が生成された後にコンピュータを適切なグループに移動します。
  エンドポイント IOC スキャンは、リソースを大量に消費し、時間がかかるため、必要な場合にのみ実行します。
- クラウドではシステムリソース使用量に応じてコストが発生するため、定期的にシステムパフォーマンスを確認する必要があります。「Secure Endpoint：トラブルシューティング」セクションを参照して、CPU 使用率が高くなっている原因を特定します。

VDI チェックリスト/サマリー

以下のサマリーを確認してから、VDI 環境に Secure Endpoint をインストールします。

- ☐ TAC ケースをオープンして、アイデンティティ永続化を有効にします。
- ☐ 仮想化プラットフォームのタイプを確認します。
- ☐ **/goldenimage** コマンドラインスイッチを指定して、ゴールデンイメージを生成します。イメージが完成する前に Secure Endpoint バックエンドに接続しないように注意してください。
- ☐ シグネチャは、30 回分までは増分更新され、その後は、シグネチャパッケージ全体がダウンロードされます。Secure Endpoint アップデートサーバーを導入し、ローカルネットワークにシグネチャファイルを保存します。
- ☐ sfc.exe プロセスでサポートされるトレイアイコン接続は 1 つです。マルチユーザー環境の場合、ポリシーでトレイアイコンを無効にします。
- ☐ Tetra を有効にする場合は、ストレージが過負荷にならないように、慎重にテストしながら段階的に有効にします。除外と機能の無効化に関するガイドラインを確認してください。
- ☐ ネットワーク負荷が高いシステムや、ネットワーク インターフェイスに多数の VLAN が設定されているシステムには、ネットワークドライバをインストールしないでください。
- ☐ Secure Endpoint は常に仮想 OS 内で実行されます。
- ☐ オンデマンドスキャンは、ストレージのパフォーマンスを低下させる可能性があります。日常運用でオンデマンドスキャンや IOC スキャンは実施しないようにします。
- ☐ VDI 環境を EDR/XDR/MDR アーキテクチャに統合する場合は、慎重に計画して、テストしてください。
- ☐ Microsoft Terminal Server、Hyper-V、パブリック クラウド インフラストラクチャ環境など、特定の環境に関する推奨事項を確認します。

付録 C：/skiptetra を指定した後に Tetra を手動で追加

これは**回避策**のため、グローバルにロールアウトする前に、必ずテスト環境でテストしてください。

手動で Tetra をエンドポイントに追加する

Connector バージョン 7.3.15 でテスト済み

/skiptetra 1 インストールスイッチを指定してインストールした場合は、次の手順を実行すれば、Tetra をエンドポイントに追加できます。

1. Connector を停止します。
2. C:\Program Files\Cisco\AMP\tetra to C:\Windows\System32\drivers から trufos.sys をコピーします。
3. HKLM\System\ControlSet001\Services\Trufos にレジストリを登録します。レジストリキーの値については以下を参照してください。
4. ポリシーで tetra が有効になっていることをポータルで確認します。
    a. [高度な設定（Advanced Settings）] → [TETRA] → [TETRA] チェックボックスをオンにします。
    b. [モデルとエンジン（Models and Engines）] → [TETRA] チェックボックスをオンにします。
5. Connector を起動します。

この作業に伴う影響が 1 つあります。これらの手順を実行した後、将来的に Secure Endpoint をアンインストールした場合、上記で作成した trufos.sys とレジストリエントリを手動で削除しなければなりません。ただし、ファイル/レジストリキーを削除しなくても、エンドポイントに影響はありません。

レジストリのキー値を生成するバッチファイル

次のテキストを .bat ファイルにコピーして、すべてのレジストリキーを一括で追加します。

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v DependOnService /t REG_MULTI_SZ /d FltMgr
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v DisplayName /t REG_SZ /d Trufos
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v ErrorControl /t REG_DWORD /d 1
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v Group /t REG_SZ /d "FSFilter Anti-Virus"
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v ImagePath /t REG_EXPAND_SZ /d "\??\C:\WINDOWS\System32\Drivers\trufos.sys"
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v Start /t REG_DWORD /d 3
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v Type /t REG_DWORD /d 2
```

ベストプラクティス：7.3.15 より新しいバージョンの Connector を使用している場合は、レジストリキーを変更したら常に慎重にテストしてください。

付録 D：サードパーティ製品と Secure Endpoint の統合

さまざまなサードパーティのセキュリティ企業が、Secure Endpoint と統合できる製品を開発しています。最新のリストについては、https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/AMP-endpoints-partners-integrations.html#~third-party-solutions を参照してください。

統合可能な製品リスト：

- Alert Logic
- Arctic Wolf Networks
- Blackpoint
- Cigent D3E
- Empow Cybersecurity
- Exabeam
- Fortinet FortiSOAR
- IBM BigFix
- IBM MaaS360
- IBM QRadar
- IBM Resilient
- Jask（Sumo Logic）
- LogicHub
- LogRhythm
- Palo Alto Networks Cortex XSOAR
- Panaseer
- Perch Security
- RSA NetWitness SIEM
- ServiceNow ITSM
- Siemplify
- Splunk Phantom
- Splunk SIEM
- Swimlane
- Syncurity
- TheHive SOAR

API コードによる Secure Endpoint の統合例

API のドキュメントについては、https://developer.cisco.com/amp-for-endpoints/ を参照してください。

GitHub の Cisco Security – サンプル統合コード

サンプル統合コード：https://github.com/CiscoSecurity?q=amp&type=&language=&sort=

付録 E：除外リストの詳細

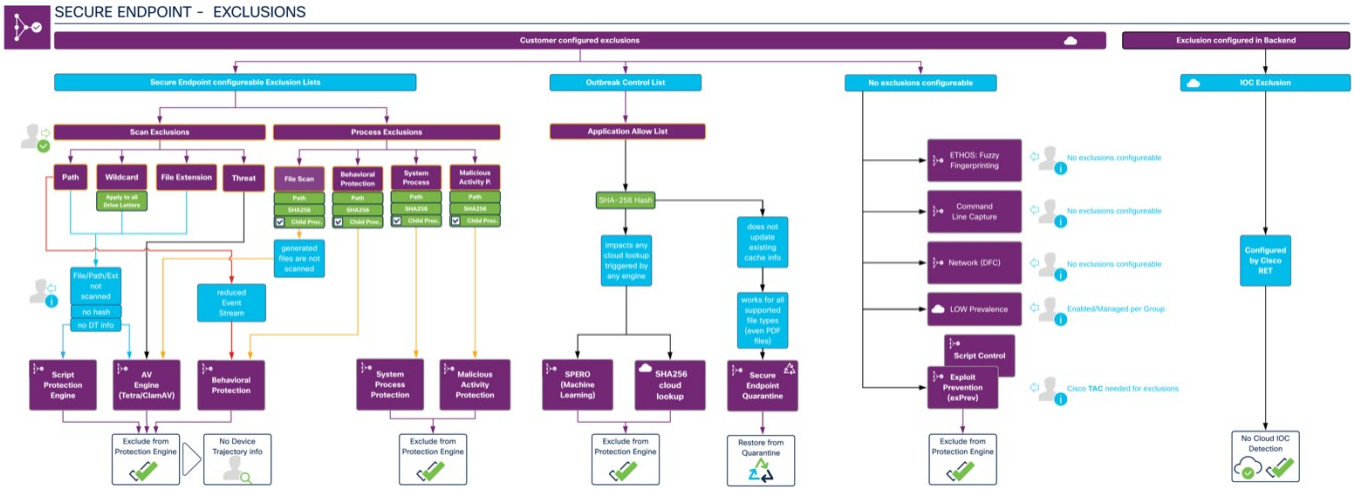
このガイドでは、Secure Endpoint の除外管理に関して、以下のように多くの有益な情報を提供しています。

- 「ポリシーの設定計画」セクションでは、ポリシーオブジェクトの概要と、リストオブジェクトがどのようにポリシーに割り当てられるかを示しています。
- 「ポリシー設定：除外リストの定義と管理」セクションでは、除外に関する既知の制限について説明しています。リストの管理と割り当てのベストプラクティスを参照してください。
- エンドポイントのトラブルシューティングを行い、必要な除外対象を判断します。その際、デバイストラジェクトリ機能を使用して、脅威を検出したエンジンを確認できます。
- 最高レベルのセキュリティを実現するために定期的に除外リストを整理します。
- できるだけ除外対象を少なくすることで、最高レベルのセキュリティを確保できます。

Secure Endpoint を利用してファイルを分析するプロセスや、その他のエンドポイントを保護するプロセスは、1 回だけでは終わりません。たとえば、ファイルスキャンでは、ファイルタイプやキャッシュステータスなどに基づいて、いくつかの段階を経る必要があります。詳細については、ファイルスキャンシーケンスを参照してください。

以下に概要を示します。

- **スキャンを除外**すると、AV スキャンとスクリプト保護エンジンに影響が及びます（パス/ワイルドカード/ファイル拡張子/脅威スキャン除外）。また、ふるまい保護エンジンのシステム アクティビティ モニターにも影響します。除外されたファイルはハッシュ化されず、バックエンドエンジン用のテレメトリも生成されません。除外されたプロセスは、コマンドライン アクティビティを除き、デバイストラジェクトリには表示されません。
- **プロセスの除外**は、単一のエンジンに非常に密接に関連します。
  - プロセス → ファイルスキャン：プロセスはスキャンされません。除外されたプロセスで生成されたファイルもスキャンされません。
  - プロセス → ふるまい保護：プロセスは、攻撃パターン検出エンジンから除外されます。
  - プロセス → システムプロセス保護または悪意あるアクティビティの防御：プロセスは特定のエンジンから除外されます。
- **アプリケーション許可リスト：**エントリは、Endpoint Connector の次の領域に影響します。
  - **ファイルタイプ：**Portable Executable およびその他のファイルタイプ（PDF ファイルなど）のエントリが処理されます。
  - SPERO（機会学習）：許可されたハッシュは、機械学習の検出対象から除外されます。
  - クラウドルックアップ：許可されたハッシュは、クラウドルックアップの対象から除外されます。クラウドルックアップの検出結果は、デバイストラジェクトリに **SHA エンジン**として表示されます。
  - ハッシュがアプリケーション許可リストに追加されている場合、**検疫フォルダ**のファイルは、ディスク上の元の場所に復元されます。
- クラウド IOC 検出除外は現在利用できません。除外対象は、シスコによってバックエンドに追加されます。クラウド IOC 検出の除外対象を追加するには、TAC ケースをオープンしてください。



ベストプラクティス：除外対象をできるだけ少なくして最高レベルのセキュリティを実現し、バックエンド検出エンジンで最大の効果を上げられるようにします。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp