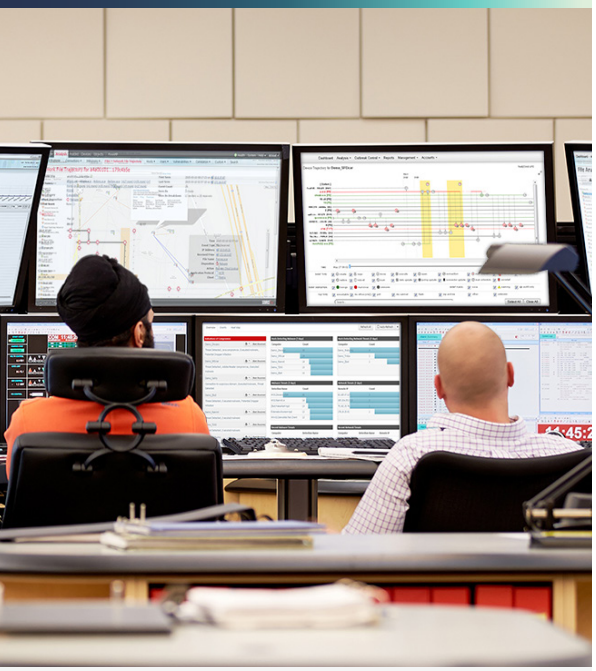
At-A-Glance



メリット

- マルウェアの継続的な検出と監視を迅速かつ遡及的に実施
- Windows オペレーティング システム、Mac、モバイル デバイス、および仮想環境の保護
- マルウェアの拡散を追跡し、侵害の範囲を特定するための長期的なファイル活動の記録
- 離散型イベントをコーディナテッド アタックに相関付け
- ネットワーク防御を強化するグローバル脅威情報へのアクセス
- 侵害をすばやく検出、分析、修復するための高度な可視性と制御

Cisco Advanced Malware Protection for Endpoints

現実社会におけるセキュリティ侵害の防御、検出、対応、および修復

ハッカーは、ウィルス対策や侵入防御システムなど、最強のポイントインタイム検出ツールでさえすり抜ける高度なマルウェアを作成しています。これらのツールは、すべての脅威を検出する点で 100 % 有効ではありません。また、最初の防御をすり抜けた脅威の活動を可視化することもほぼできません。この結果、IT セキュリティ チームは潜在的な危害の範囲を認識することができず、損害を与える前にすばやくマルウェアを検出および修復することができないのです。

Cisco Advanced Malware Protection（AMP）for Endpoints は、ポイントインタイム機能の域を超えて、攻撃前、攻撃中、攻撃後に組織を保護します。

- **攻撃前**：AMP は最適なグローバル脅威インテリジェンスに基づいて防御を強化します。
- **攻撃中**:AMP はインテリジェンス、既知のシグニチャ、および動的ファイル分析テクノロジーに基づいて、IT 環境への侵入を試みるマルウェアをブロックします。
- **攻撃後**：AMP はすべてのファイルと実行可能なアクティビティを監視して、初回の検出を回避したマルウェアを捕捉し、迅速に修復するための可視性と制御を提供します。

Cisco AMP for Endpoints は、侵入を防御するだけはありません。仮に第一防衛線が突破された場合でも、コスト効率の高い方法で、運用効率に影響を与えることなく、脅威を迅速に検出、阻止、修復できます。

脅威インテリジェンスおよび動的マルウェア分析

Cisco AMP は、Cisco 集合型セキュリティ インテリジェンス、Talos Security Intelligence and Research Group、および AMP Threat Grid インテリジェンス フィードから提供される、リアルタイムの脅威インテリジェンスと動的マルウェア分析の広範なコレクションをベースに構築されています。

この脅威インテリジェンスは、以下のソースから提供される情報に基づいています。

- 110 万件のマルウェア受信(1 日あたり)
- 160 万個のグローバル センサー
- 1 日で 100 テラバイトのデータ
- 130 億件の Web 要求
- 600 名のエンジニア､技術者､および研究者
- 24 時間運用

機能

継続的な分析および遡及的セキュリティ：AMP は、ファイル アクティビティを継続的に監視、分析、記録し、最前線の防御をすり抜けるマルウェアを迅速に検出します。これは、侵害の範囲を特定して、迅速に対応するのに役立ちます。

動的なマルウェア分析とサンドボックス：**高度なセキュリティで保護された環境では、広範な動作指標を使用してマルウェアの分析を開始し、以前は不明だったゼロデイ脅威を発見することができます。**

侵害の痕跡（Indications of compromise：IoC）：ファイルおよびテレメトリ イベントは相関付けられ、アクティブな侵害の可能性があるものとして優先度が設定されます。AMP は侵害やマルウェア イベントなどのマルチソース セキュリティ イベント データを自動的に相関付けます。これにより、セキュリティ チームは、イベントをコーディナテッド アタックに関連付け、リスクが高いイベントの優先度を設定することができます。

デバイス トラジェクトリ：デバイスおよびシステム レベルで、実行可能なアクティビティや通信を継続的に追跡することができます。これにより、根本原因を迅速に理解し、侵害に至ったイベントや侵害後のイベントの履歴を確認することができます。

普及率：AMP は、組織全体で実行されているすべてのファイルを普及率順に表示します。これは、少数のユーザのみが確認した、以前は検出されていなかった脅威を表面化させるのに役立ちます。少数のユーザのみによって開かれたファイルは、悪意がある場合があります。

脆弱性：AMP は、システム上の脆弱性のあるソフトウェア、そのソフトウェアを格納するホスト、および侵害を受けた可能性が高いホストの一覧を表示します。AMP は、標的にされている脆弱性のあるソフトウェアと、悪用の可能性があるものを特定し、パッチを適用するホストの一覧を優先度とともに提供します。

アウトブレイク制御：AMP は、疑わしいファイルやアウトブレイクに対する制御を取得し、コンテンツの更新を待つことなく修復を実行するのを助けます。また、

- すべてのシステムまたは選択したシステムで特定のファイルを迅速にブロックする
- ポリモーフィック型マルウェアのファミリをブロックする
- マルウェア ゲートウェイとして使用されている侵害を受けたアプリケーションを阻止し、再感染サイクルを止める
- 企業ネットワーク外のリモート エンドポイントでも、マルウェアのコールバック通信をソースで停止する
- ミッション クリティカルなアプリケーションがどのような事態でも継続して実行できるようにする

他の機能については、AMP for Endpoints のデータシートを参照してください。

AMP Threat Grid テクノロジーと Cisco AMP for Endpoints との統合は、コンテキストリッチなインテリジェント フィードを実現します。このテクノロジーは、毎月数百万のサンプルを 350 個以上の指標に照らして分析します。その結果、セキュリティ チームが対応の優先度を設定するのに役立つ、数十億のアーチファクトや理解しやすい脅威スコアが生成されます。

継続的な分析と遡及的セキュリティ

Cisco AMP for Endpoints は、初期検査の後も、すべてのファイルと実行可能なアクティビティを、その性質に関係なく継続的に監視、分析、記録します。AMP が疑わしいアクティビティを発見すると、セキュリティ チームにアラートが送信されます。セキュリティ チームは、脅威の完全な履歴を確認して、次の質問に対する答えを迅速に得ることができます。

- マルウェアの発生源はどこか
- 攻撃はどのような方法で行われ、どこから侵入したのか
- どこにあったか どのシステムが影響を受けたか
- 脅威は過去および現在にどのような活動を行っているか
- 脅威を阻止して根本原因を除去するにはどうすればよいか

AMP のブラウザベースの管理コンソールを数回クリックするだけで、ファイルが別のエンドポイントで実行されるのをブロックできます。Cisco AMP は過去にファイルが通過した他のすべてのエンドポイントを把握しているため、ファイルをメモリから取り出し、すべてのユーザから隔離することができます。マルウェアを排除するために、従来のようにセキュリティ チームがシステム全体を再イメージする必要はもはやありません。その方法には多大な時間、コスト、リソースがかかっていました。AMP では、マルウェアのみを対象にピンポイントで修復を行うことができるため、IT システムやビジネスに付随的な損害が生じることはありません。

また AMP は、脅威の署名からファイルの動作まで、確認した内容をすべて記憶しており、そのデータを AMP の脅威インテリジェンス データベースに記録します。これにより第一防衛線がさらに強化されるため、そのファイル（および類似ファイル）は初期検出を回避できなくなります。

導入

Cisco AMP for Endpoints は、使いやすい Web ベースのコンソールを使用して管理します。AMP の軽量エンドポイント コネクタを使用して導入されるため、ユーザのパフォーマンスには影響ありません。分析はエンドポイントではなくクラウドで行われます。このソリューションは、Windows、Windows POS オペレーティング システム（2015 年 6 月末より使用可能）、Mac、モバイル デバイス、および仮想システムを対象とする、エンドポイントでのサブスクリプションとして提供されます。AMP for Endpoints は AnyConnect v4.1 からも起動できます。

次のステップ

高度なサイバー攻撃から組織を保護するのに Cisco AMP for Endpoints がどのように役立つかについては、シスコの営業担当者またはチャネル パートナーにお問い合わせください。詳細については、www.cisco.com/jp/go/ampendpoint を参照してください。

C45-731874-04 01/16