At-A-Glance

メリット

- 攻撃前、攻撃中、攻撃後の保護
- 隠れたマルウェアの迅速な検出、対応、修復
- 比類ないグローバルな脅威インテリジェンスと動的マルウェア分析
- セキュリティ侵害の発生源と範囲を詳細に把握
- より多くの情報に基づいたセキュリティの判断とより迅速な調査
- どこでも保護：ネットワーク、エンドポイント、モバイル デバイス、仮想環境、電子メール、および Web ゲートウェイ

Cisco Advanced Malware Protection

侵害を防御、検出、修復するための可視性と制御

組織は攻撃にさらされ、セキュリティ侵害は日々発生しています。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。これらのツールは拡張されたネットワークの入口でトラフィックを検査しますが、組織に侵入しようとするすべての脅威を 100 % 検出できるわけではありません。また、第一防衛線をすり抜けた脅威のアクティビティ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阻止することができないのです。

Cisco® Advanced Malware Protection（AMP）は、ポイントインタイム機能の域を超えて、攻撃前、攻撃中、攻撃後の各フェーズにまたがって組織を保護するように構築されています。

- **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 アクティビティ、プロセス、および通信を継続的に監視し、分析します。ファイルが悪意のある動作を示した場合は、AMP がそれを検出し、遡及的アラート、侵害の痕跡（IoC）、追跡、および分析を提供するので、セキュリティ チームは侵害を受けた部分をピンポイントで修復できます。

AMP 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

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

継続的な分析と遡及的セキュリティ

- Cisco AMP は、ファイルの初期検査の後も、すべてのファイル アクティビティと動作を、その性質に関係なく継続的に監視、分析、記録します。
- 以前は「不明」または「良好」とされていたファイルが悪意のある動作を示すようになった場合は、AMP が遡及的アラートを自動的に送信し、侵害範囲の特定と迅速な対応のために、そのファイルのアクティビティと動作の履歴を提供します。

可視性と制御

- 遡及的アラートは、ネットワーク上の誰がいつ感染したかをはじめとして、ファイルの性質のあらゆる変化をレポートします。
- ダッシュボードには、脅威がある正確な場所、動作の内容、および根本原因が表示されるので、脅威をすみやかに封じ込めて修復することができます。

柔軟性と幅広い選択肢

- Cisco AMP は、複数のプラットフォームに対応しており、エンドポイント、ネットワーク、モバイル デバイス、仮想環境などに導入可能です。そのため、各組織のニーズに適した方法で導入することができます。

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 AMP 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/amp をご覧ください。

AMP Threat Grid テクノロジーと Cisco AMP 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。

Cisco AMP は、ファイル、動作、テレメトリ データ、およびアクティビティをこの堅牢でコンテキストリッチなナレッジ ベースと関連付けることで、攻撃をブロックし、脅威に対する理解を深め、より迅速かつ容易に対応できるようにします。

継続的な分析と遡及的セキュリティ

Cisco AMP は、初期検査の後も、すべてのファイル 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。疑わしい、または悪意のあるアクティビティが見つかった場合は、セキュリティ チームにアラートと侵害の痕跡を送信します。また、優れた可視性によって状況を明確化します。セキュリティ チームは、脅威の詳しい履歴を確認し、セキュリティに関する次の重要な質問の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
- どのシステムが影響を受けたか
- 現在、脅威は何をしているのか？
- どのように脅威を止めるか？

セキュリティ チームはこの情報を基に、AMP の使いやすいブラウザベースの管理コンソールから迅速な対策を講じることができます。

柔軟な導入オプション

Cisco AMP のソリューションは、複数のプラットフォームに導入可能です（表 1 を参照）。

表 1. Cisco AMP 導入オプション

製品名	詳細
Cisco AMP for Endpoints	ユーザのパフォーマンスに影響を与えることなく、AMP の軽量コネクタを使用して、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、Android モバイル デバイス、および仮想環境を実行する PC を保護します。AMP for Endpoints は AnyConnect v4.1 からも起動できます。
Cisco AMP for Network	AMP を Cisco FirePOWER ™ ネットワーク セキュリティ アプライアンスに統合されたネットワークベースのソリューションとして導入するオプションです。
Cisco AMP on ASA with FirePOWER Services	AMP 機能を Cisco ASA ファイアウォールに統合したものです。
Cisco AMP プライベート クラウド仮想アプライアンス	パブリック クラウドの使用に制限のある、厳格なプライバシー要件を持つ組織のために構築されたオンプレミスのエアギャップ型ソリューションです。
Cisco AMP on CWS、ESA、または WSA	Cisco Cloud Web Security（CWS）、Cisco Email Security Appliance（ESA）、または Cisco Web Security Appliance（WSA）で AMP 機能を有効にして、遡及機能およびマルウェア分析を提供できます。
Cisco AMP Threat Grid	Cisco AMP に統合されている AMP Threat Grid によって、高度な動的マルウェア分析を行うことができます。スタンドアロンの高度なマルウェア分析および脅威インテリジェンス ソリューションとして、クラウド内またはアプライアンス上に導入することもできます。

C45-731876-02 11/15