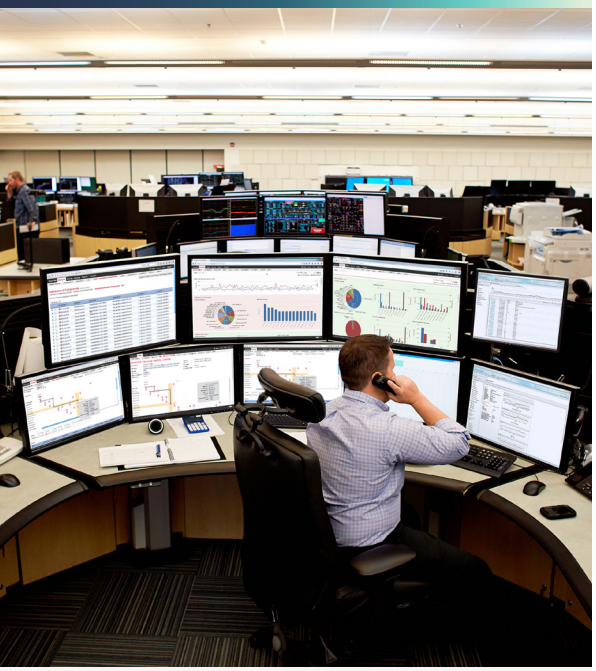
At-a-Glance



# ネットワーク向け Cisco AMP (高度なマルウェア防御)

## メリット

- 攻撃、悪意のあるファイル、ポリシーに違反するファイルの**検出とブロック**
- マルウェアの拡大を追跡し、危害の範囲を特定するための**継続的なファイル アクティビティの分析および記録**
- **離散型イベント**をコーディナテッド アタックに相関づけ
- 侵害をすばやく検出、分析、格納するための**高度な可視性と制御**
- ネットワーク防御を強化する**優れたグローバル脅威情報へのアクセス**
- AMP の使いやすい Web ブラウザ ベースのコンソール、FireSIGHT Management Center を使用した**ソリューションの管理**

## 実世界での 侵害の防止、検出、対応

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、ファイアウォール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、ネットワークへのエントリ ポイントでトラフィックを検査しますが、組織への侵入を試みるすべての脅威を検出する点では 100% 有効ではありません。また、第一線の防御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) for Networks 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を使用してネットワーク防御を強化します。
- **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を使用して、ネットワークへの侵入を試みるマルウェアをブロックします。
- **攻撃後**、またはファイルがネットワークを通過した後、AMP はすべてのファイル アクティビティとトラフィックを継続的に監視および分析します。ファイルが悪意のある動作を示した場合、AMP は脅威のアクティビティの高度な可視性と、迅速に対応して阻止するための制御を提供します。

AMP for Networks は、侵害防止機能だけなく、侵入が検出されなかった場合は、迅速な侵害の検出、対応、格納機能を提供します。すべての機能はコストパフォーマンスに優れ、運用の効率性に影響しません。

## 脅威インテリジェンスおよび動的マルウェア分析

AMP for Networks は、Cisco Collective Security Intelligence、Talos Security Intelligence and Research Group 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大規模なコレクションをベースに構築されています。組織にとって以下のようなメリットがあります：

- 110 万件の着信マルウェアのサンプル（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**：ファイルがネットワーク制御ポイントを通過した後でも、AMP はファイル アクティビティと動作を継続的に監視、分析、記録し、最前線の防御をすり抜けたマルウェアを迅速に検出します。

**レトロスペクティブ セキュリティ**：以前は「不明」または「良好」だったファイルが悪意のある動作を示す場合、AMP は、レトロスペクティブ アラートを送信し、侵害の範囲を特定して迅速に対応できるように、ファイル アクティビティの記録履歴を表示します。

**Cisco FireSIGHT Management Center**：脅威のアクティビティ、ホスト、オペレーティング システム、アプリケーション、ユーザ、ファイルおよび位置情報を表示する単一のコンソールを通じて環境を可視化することができます。

**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、広範な動作インジケーター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。

**痕跡（Indications of compromise：IoCs）**：AMP は、ファイル、テレメトリ、侵入、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、アクティブな侵害の可能性があるものとして優先度を設定します。これにより、セキュリティ チームは、イベントをより大きな調整攻撃に関連付け、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。

**ファイルの軌跡**：ファイルの伝播は長期的に追跡され、可視性が提供されます。これにより、マルウェアの侵害の範囲を特定するのに必要な時間が短縮されます。

**エンドポイント用 Cisco AMP の統合**：エンドポイントで実行可能なアクティビティの可視性をさらに高め、ネットワーク イベントをエンドポイント イベントに相関付けるために、AMP for Networks は AMP for Endpoints と互換性があります。

この情報を使用して、AMP は、セキュリティ チームが対応に優先順位を付けるのに役立つ脅威スコアなどの実行可能なインテリジェンスを提供します。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豊富なナレッジ ベースに自動的に相関付けることにより、ネットワークへの侵入を試みる脅威をブロックします。これにより、セキュリティ チームはネットワーク内の脅威をより高度に認識し、より迅速かつ容易にインシデントに対応することができます。

## 継続的な分析およびレトロスペクティブ セキュリティ

AMP for Networks は、ネットワーク制御ポイントでの初期検査の後も、配置に関係なく、すべてのファイル アクティビティを監視、分析、記録します。AMP が疑わしいアクティビティや悪意のあるアクティビティを観察したり、以前は「良好」だったファイルが「不正」に変わったりすると、セキュリティ チームにレトロスペクティブ アラートおよび危害の通知が送信されます。AMP は、厳密に何が発生したかを可視化します。セキュリティ チームは、マルウェアに関して実質的に時間をロールバックすることにより、完全に記録された脅威の履歴を確認し、セキュリティに関する重要な質問に対する答えを迅速に得ることができます。たとえば、次のような質問です。

- マルウェアがどこから来たか
- 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

ファイル軌跡機能を使用すると、セキュリティ チームは、長期的なファイル転送のビジュアル表示およびファイルに関する他の情報を表示することにより、ネットワーク全体でファイルの送信を追跡することができます。その後、それらの悪意のあるファイルのブロックと、単純なポリシー更新およびカスタム検出リストの操作を簡単に行うことができます。ベンダーが提供する更新を待つことなくいつでも行動を取ることができるため、セキュリティ チームは強化されます。

継続的な分析およびレトロスペクティブ セキュリティが実施されるため、セキュリティ チームには、迅速に脅威を検出、対応、阻止するための可視性と制御が与えられます。

## 展開

AMP for Networks は、使いやすい Web ベースの管理コンソールである Cisco FireSIGHT ™ Management Center を使用して管理します。これは、広範なネットワーク機能や処理機能を持つ Cisco FirePOWER next-generation intrusion prevention system (NGIPS) のサブスクリプションとして導入されます。

## 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 for Networks 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。



C45-731875-01 08/15