# Cisco Advanced Malware Protection

## 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

**利点**

- 類を見ないグローバルな脅威インテリジェンスを活用して、最前線での防御を強化
- セキュリティ侵害の発生源と範囲を詳細に把握
- マルウェアの迅速な検出、対応、修復
- 再感染による修復のコストが不要に
- 攻撃前、攻撃中、攻撃後の各フェーズにわたってあらゆる場所（ネットワーク、エンドポイント、モバイル デバイス、電子メール、Web）を保護

組織は常に攻撃にさらされており、セキュリティ侵害がよくニュースの見出しを飾っています。今日では、世界に広がる攻撃者コミュニティが高度なマルウェアを生み出し、多様な攻撃ベクトルを通じて、このようなマルウェアをさまざまな組織に送り込んでいます。こうした多面的な標的型攻撃は、最良の防止ツールすらも出し抜くことができます。このようなツールは、ネットワークへの進入時点でトラフィックやファイルの検査を行い、既知の脅威をブロックしますが、「問題のない」または「不明な」ファイルのネットワークへの侵入は防ぎません。残念なことに、分析が行われるのはそこまでです。隠されたマルウェア ファイルがこれらの防御をすり抜ける場合、これらのツールではシステム上で脅威の活動をほとんど可視化できません。そのため、重大な損害が発生する前に、セキュリティ プロフェショナルがセキュリティ侵害の範囲を予測したり、迅速にマルウェアの動作を検出し、迅速に対応、封じ込め、除外したりすることが困難な状況です。

Cisco® Advanced Malware Protection（AMP）は、高度なマルウェアのライフサイクル全体を視野に入れたセキュリティ ソリューションです。セキュリティ侵害を防止するだけではなく、最前線の防御をすり抜けた脅威を迅速に検出、封じ込め、修復するために必要な可視性、コンテキスト、および制御機能を備えています。しかも、コスト効率に優れ、運用効率に悪影響を与えることはありません。

## 製品概要

AMP は、インテリジェンスを活用した、企業向けの高度な統合マルウェア分析/防御ソリューションです。攻撃前、攻撃中、攻撃後の各フェーズにわたって、組織を包括的に保護します。

- **攻撃前**:シスコの Talos Security Intelligence and Research Group および Threat Grid の脅威インテリジェンス フィードによるグローバルな脅威インテリジェンスを使用して、既知の脅威および新たな脅威に対する防御と保護を強化します。
- **攻撃中**:前述のインテリジェンスと、既知のファイルのシグニチャおよび Cisco Threat Grid のダイナミック マルウェア分析テクノロジーを組み合わせて使用することで、ポリシーに違反するファイル タイプや、ネットワークへの侵入を試みるエクスプロイトおよび悪意のあるファイルを特定し、ブロックします。
- **攻撃後(またはファイルの初期検査後)**:ポイントインタイム検出機能に加えて、あらゆる種類の活動やトラフィックを、現時点での評価に関係なく継続的に監視および分析して、悪意のある活動の徴候を探します。不明なファイル、または以前は「問題ない」と見られていたファイルが不正な動作を開始した場合は、AMP はその活動を検出し、即座にセキュリティ チームに対してセキュリティ侵害の兆候を警告します。このソリューションは、マルウェアの発生源、影響を受けるシステム、マルウェアの動作に関する可視性を提供します。また、侵入にすみやかに対処し、わずか数クリックで修復できる制御機能も備えています。これにより、セキュリティ チームはすみやかに攻撃を検出し、セキュリティ侵害の範囲を特定し、損害が発生する前にマルウェアを閉じ込めるために必要な、深いレベルでの可視性と制御機能を利用することができます。

## グローバルな脅威インテリジェンスとダイナミック マルウェア分析

AMP は、非常に優れたセキュリティ インテリジェンスとダイナミック マルウェア分析を基盤としています。シスコの Talos Security Intelligence and Research Group および Threat Grid の脅威インテリジェンス フィードという、業界トップクラスのリアルタイムの脅威インテリジェンスとビッグデータ分析を組み合わせて活用します。このデータはクラウドから AMP クライアントにプッシュされるため、最新の脅威インテリジェンスを活用してプロアクティブな脅威対策を講じることができます。お客様にとってのメリット:

- 150 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 日あたり 100 TB のデータ
- 130 億件の Web 要求
- エンジニア、技術者、および研究者で構成されるグローバル チーム
- 24 時間運用

AMP は、システム上のファイルや行動やテレメトリ データや活動を、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、すみやかにマルウェアを検出します。セキュリティ チームは、AMP の自動分析機能を活用することで、セキュリティ侵害活動を検索する時間を節約するとともに、常に最新の脅威インテリジェンスを利用して、高度な攻撃を迅速に把握、優先順位付け、ブロックできます。

シスコの Threat Grid テクノロジーを AMP に統合すると、さらに次のメリットがあります。

- 非常に正確でコンテキストリッチなインテリジェンス フィードが標準フォーマットで提供されるため、既存のセキュリティ テクノロジーとスムーズに統合できます。
- 毎月数百万のサンプルを 700 を超える動作指標に照らして分析し、数十億のアーティファクトを生成できます。
- セキュリティ チームは、わかりやすい脅威スコアを使用して、脅威を優先順位付けすることができます。

AMP は、これらのインテリジェンスと分析に基づいて、セキュリティ関連の意思決定に役立つ情報を提供し、自動的な対策を可能にします。たとえば、継続的に更新されるインテリジェンスに基づいて、既知のマルウェアやポリシーに違反するファイル タイプを自動的にブロックし、悪意があると判明している接続を動的にブラックリストに設定し、悪意があると分類された Web サイトやドメインからのファイルのダウンロードをブロックできます。

## 継続的な分析とレトロスペクティブ セキュリティ

ほとんどのネットワークおよびエンドポイント ベースのマルウェア対策システムは、拡張ネットワークへの制御ポイントを通過する時点でのみファイルを検査します。分析が行われるのはそこまでです。しかし、マルウェアは高度化してきており、このような初期検査を巧みにすり抜けます。スリープ、多態、暗号化、未知のプロトコルの使用などは、マルウェアが検査をすり抜けるテクニックのごく一部です。見えないものは防御できないため、主なセキュリティ侵害のほとんどはこのような形で始まります。セキュリティ チームは脅威の侵入を見逃し、その後も存在に気付かないままです。侵入した脅威をすみやかに検出して封じ込めるための可視性もないので、気が付いたときにはすでにマルウェアが目的を達成し、損害が発生している、という具合です。

Cisco AMP はこのようなシステムとは異なります。AMP システムでは、ポイントインタイム方式のプリエンプティブな検出/ブロック手法は 100 % 確実なものではないという認識に立ち、初期検査以降も継続的にファイルおよびトラフィックを分析します。AMP は、エンドポイント、モバイル デバイス、ネットワーク上のすべてのファイルの活動および通信を監視、分析、記録して、疑わしい行動や悪意のある行動を示す、ステルス性の高い脅威をすばやく発見します。問題の徴候が見つかったら、AMP はセキュリティ チームに警告を送り、脅威の動作についての詳細情報を提供します。これにより、次のようなセキュリティ上の重要なポイントが明らかになります。

- 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
- マルウェアはどこに潜んでおり、どのシステムが影響を受けるか
- 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

この情報によって、セキュリティ チームはすばやく現状を把握し、AMP の封じ込めおよび修復機能を使用して対策を講じることができます。管理者は、AMP の使いやすいブラウザ ベースの管理コンソールで数クリックするだけで、問題のファイルがこれ以上他のエンドポイントに作用しないようにブロックし、マルウェアを封じ込めることができます。AMP は、問題のファイルがどこに存在していたかを把握しているため、そのファイルをメモリから除去し、他のすべてのユーザから隔離できます。マルウェアが侵入した場合でも、セキュリティ チームはシステム全体をイメージから再度回復してマルウェアを除去する必要はありません。このような方法は、時間やコストやリソースの負担が大きいうえに、重要な業務システムを中断させることにもなります。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。

これは、継続的な分析、継続的な検出、レトロスペクティブ セキュリティによるものです。これらの機能は、システム内のすべてのファイルの活動を記録し、「問題ない」と思われていたファイルが「問題のある」活動の徴候を見せた場合に、そのファイルを検出して、記録されている履歴を過去にさかのぼって確認し、脅威の発生源と行動の詳細を把握できます。そして、AMP では、組み込みの対応および修復機能によって、脅威を取り除くことができます。また、AMP は、脅威のシグニチャからファイルの行動に至るまで、把握したすべてのデータを AMP の脅威インテリジェンス データベースに記録し、最前線での防御をさらに強化します。これにより、過去に発生した脅威や類似のファイルは、それ以降は初期検査をすり抜けることができなくなります。

セキュリティ チームは、このような AMP の機能によって、攻撃を迅速かつ効率的に検出し、ステルス性の高いマルウェアを発見するために必要な深いレベルの可視性と制御機能を手に入れることができます。また、セキュリティ侵害とその影響範囲を把握し、（ゼロデイ攻撃であっても）損害が発生する前にマルウェアをすばやく封じ込めて修復し、今後同様の攻撃を防止できます。

## 主な機能

AMP の継続的な分析とレトロスペクティブ セキュリティ機能は、次のような強固な機能に基づいて実現されます。

- **包括的なグローバル脅威インテリジェンス**：Cisco Talos Security Intelligence and Research Group および Threat Grid の脅威インテリジェンス フィードは、業界最大のリアルタイムな脅威インテリジェンスの集合体です。最高レベルの可視性とフットプリントに加え、複数のセキュリティ プラットフォームわたって実行できる機能を備えています。
- **侵入の痕跡（IoC）**：ファイルやテレメトリ イベントを関連付け、アクティブなセキュリティ侵害の可能性が大きい順に優先順位を付けます。AMP は、複数のソースからのセキュリティ イベント データ（侵入やマルウェアなどのイベント）を自動的に関連付け、イベントをより大規模な組織的攻撃に結び付けたり、リスクの高いイベントの優先順位を付けたりできるようにします。
- **ファイルのレピュテーション**：高度な分析と集合型インテリジェンスの組み合わせによって、ファイルが悪意のあるものであるかどうかを判断し、より正確な検出につなげることができます。
- **組み込み AV エンジン**：導入されている AMP for Endpoints には、組み込み AV 検出エンジンが搭載されています。ルートキット スキャン、ローカル IOC スキャン、デバイス フロー モニタリングを使用して、シグニチャ ベースの検出を実行します。シグニチャベースの AV および高度なエンドポイント保護機能を 1 つのエージェントに統合する必要があるお客様は、このエンジンを有効にして利用できます。組み込み AV エンジンには、大型エンドポイント AV スイートの追加機能（パーソナル ファイアウォールなど）はありません。
- **静的および動的なマルウェア分析**：非常にセキュアなサンドボックス環境でマルウェアを実行、分析、テストして、未知のゼロデイ脅威を検出できます。AMP ソリューションには、Threat Grid のサンドボックスおよび静的/動的なマルウェア分析テクノロジーが統合されているため、より多くの動作指標に対してチェックを行う包括的な分析を実施できます。
- **レトロスペクティブな検出**：広範な分析によってファイルの評価が変化したときは、アラートが送信され、最初の防御をすり抜けたマルウェアについて注意喚起され、問題のファイルが可視化されます。
- **ファイル追跡機能**：環境全体にわたるファイル伝播を継続的に追跡することで、ファイルの可視性を実現し、マルウェアによるセキュリティ侵害の範囲をすみやかに特定できるようにします。
- **デバイス追跡機能**：デバイス上およびシステム レベルでの活動や通信を継続的に追跡することで、根本原因をすみやかに把握し、セキュリティ侵害の前後のイベント履歴を把握できます。
- **柔軟な検索**：ファイル、テレメトリ、および集合型セキュリティ インテリジェンスに対してシームレスな検索を実行でき、IoC や悪意のあるアプリケーションにさらされているコンテキストと範囲をすばやく把握できます。
- **拡散の程度**：組織内で実行されたすべてのファイルを、拡散度が低い順に並べて表示することで、少数のユーザのみが影響を受ける、以前は検出できなかった脅威を浮かび上がらせることができます。少数のユーザのみが実行するファイルでも、拡張ネットワーク内で実行することが望ましくない、悪意のあるアプリケーション（ターゲット型の高度な永続的脅威など）や疑わしいアプリケーションである場合があります。
- **エンドポイント IoC**：ユーザは、ユーザ独自の IoC を提出して、ターゲット型攻撃を捕捉できます。セキュリティ チームは、これらのエンドポイント IoC を利用して、環境内のアプリケーションに固有の、あまり知られていない高度な脅威を詳細に調査できます。
- **脆弱性**：システム内の脆弱性があるソフトウェア、脆弱性のあるソフトウェアを含むホスト、セキュリティ侵害を受ける危険性が高いホストのリストを表示します。AMP は、シスコの脅威インテリジェンスおよびセキュリティ分析によって、マルウェアの攻撃対象となっている脆弱性のあるソフトウェアや、エクスプロイトの可能性がある現象を特定し、パッチを適用すべきホストを優先度の高い順に示します。

- **アウトブレイク制御**:コンテンツの更新を待つことなく、疑わしいファイルや脅威の拡大を制御し、感染を修復できます。アウトブレイク制御機能には、次の内容が含まれています。
  - シンプルでカスタマイズ可能な検出機能により、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できます。
  - 高度なカスタムのシグネチャにより、多相性マルウェア ファミリをブロックできます。
  - アプリケーションのブロック リストによって、アプリケーション ポリシーを適用したり、マルウェアの侵入口として利用されているセキュリティ侵害されたアプリケーションの封じ込めを行って、再感染サイクルに歯止めをかけることができます。
  - カスタムのホワイトリストにより、安全なカスタムのミッションクリティカル アプリケーションを継続的に動作させることができます。
  - デバイス フローの関連付けによって、マルウェアによるコールバック通信を発信元で阻止します。特に、企業ネットワークの外部にあるリモート エンドポイントへのコールバック対策に有効です。

## さまざまな場所の保護に対応した導入オプション

サイバー犯罪者は、さまざまな進入口から組織に攻撃を仕掛けます。ステルス性の高い攻撃を効果的に検出するには、可能な限り多くのベクトルに対して可視性を確保しておく必要があります。そのため、AMP ソリューションには、拡張ネットワークのさまざまな制御ポイントに導入可能なオプションが用意されています。組織固有のセキュリティ ニーズに合わせて、さまざまな方法でさまざまな場所に導入できます。使用可能なオプションを次に示します。

| 製品名 | 詳細 |
|---|---|
| **Cisco AMP for Endpoints** | AMP の軽量コネクタによって、Windows、Mac、Linux システムを実行する PC と、Android モバイル デバイスを保護できます。ユーザのパフォーマンスに悪影響を与えることはありません。Cisco AMP for Endpoints は、AnyConnect v4.1 からも起動できます。 |
| **Cisco AMP for Networks** | AMP を Cisco FirePOWER NGIPS 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します。 |
| **Cisco AMP on Firewalls and ASA with FirePOWER Services** | Cisco NGFW または ASA 適応型セキュリティ アプライアンス ファイアウォールに統合された AMP 機能を導入します。 |
| **Cisco AMP Private Cloud Virtual Appliance** | 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 ESA または WSA** | Cisco Email Security Appliance（ESA）または Cisco Web Security Appliance（WSA）で AMP 機能を有効にして、レトロスペクティブ機能およびマルウェア分析を提供できます。 |
| **Cisco AMP for Meraki MX** | AMP を Meraki MX セキュリティ アプライアンスの一部として導入し、高度な脅威管理機能を備えたシンプルなクラウドベースのセキュリティ管理を実現します。 |
| **Cisco Threat Grid** | Cisco AMP に統合されている Threat Grid によって、高度な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またはアプライアンスに導入することもできます。 |

Cisco Advanced Malware Protection は、まさに「あらゆる場所」をカバーしています。このような複数の攻撃ベクトル全体（ネットワーク エッジからエンドポイントまで）にわたる可視性と制御により、隠されたマルウェアをすばやく検出して排除することが可能になります。ただし、徹底的かつ迅速な措置を講じるには、セキュリティ インフラストラクチャ全体にわたって情報を共有できなければなりません。ここで注目すべきことは、これらすべてのソリューション間での相互接続、通信、および統合の重要性です。これらのソリューションは単独で利用するポイント製品ではありません。組み合わせて導入することで、ソリューションが連動し、脅威に体系的かつ迅速に対応する統合された防御が実現します。導入したすべての AMP ソリューションで脅威インテリジェンス、侵入の痕跡、イベント情報、隔離情報が自動的に共有されるエコシステムが構築されます。AMP の「あらゆる場所を監視する」機能により、組織はマルウェアの検出および修復に要する時間を劇的に短縮できます。

## サードパーティ テストをリードする Cisco AMP

シスコは、2016 年の「NSS Labs Breach Detection Systems Comparative Analysis Report（NSS Labs 侵害検出システム（BDS）比較分析レポート）」で、3 年連続で NSS Labs Breach Detection Systems Security Value Map（NSS Labs 侵害検出システム セキュリティ バリュー マップ）の首位を獲得しています。2016 年の NSS ラボによる製品比較テストに、Cisco AMP のテスト結果が詳しく記載されています。

- 100 % のセキュリティ効果を達成しました。これは、テスト対象のすべてのベンダーの中で最高の評価です。
- シスコはテスト中、すべてのマルウェア エクスプロイトと回避テクニックを 100 % 検出してブロックした唯一のベンダーです。
- テストされた他のどのベンダーよりも短時間で検出しました。
- エンドポイントやアプリケーションの遅延に対する影響を最小限にとどめながら、優れた性能を維持しました。

## シスコが選ばれる理由

現在の状況では、もはや侵害されるかどうかではなく、いつ侵害されるかが問題となっています。防止ツールだけでは、すべての攻撃を先制して 100 % 検出しブロックすることはできません。侵入を完全に阻止することはできません。したがって、セキュリティが侵害された場合に、すみやかに侵入を検出し、対応および修復を行うことができるツールが必要です。

Cisco AMP は、インテリジェンスを活用した、企業向けの高度な統合マルウェア分析/防御ソリューションです。ネットワークの防御機能を強化するグローバルな脅威インテリジェンスと、悪意のあるファイルをリアルタイムにブロックする分析エンジンに加えて、あらゆる行動とトラフィックを最初の検査後も継続的に監視および分析する機能を備えています。これらの機能によって、脅威となる可能性がある活動についての高度な可視性を確保するとともに、マルウェアを制御し、迅速に検出、封じ込め、除去できます。

## Cisco Capital

**目標達成を支援するファイナンス**

Cisco Capital® ファイナンスは、目標を達成して競争力を維持するために必要なテクノロジーのご購入をお手伝いします。お客様の CapEx を削減し、成功を加速させ、投資金額と ROI を最適化します。Cisco Capital ファイナンス プログラムは、お客様がハードウェア、ソフトウェア、サービス、および補完的なサードパーティ製機器を柔軟に取得できるようにします。また、それらの購入を 1 つにまとめた計画的なお支払い方法をご用意しています。Cisco Capital は 100 ヵ国以上でサービスを利用できます。詳細はこちら。

## 次のステップ

Cisco AMP の詳細については、http://www.cisco.com/jp/go/amp を参照してください。この簡単な概要ビデオをご覧ください。また、テクノロジーに関する簡単なデモや詳細なデモ、お客様の声、AMP の競合製品との比較も用意しています。シスコのセールス担当者にお問い合わせいただければ、Cisco AMP の専門家との POV を設定いたします。



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

C22-734228-04JA 17.03