エンドポイント向け Cisco AMP（高度なマルウェア防御）

製品概要

組織は絶え間ないサイバー攻撃を受けており、セキュリティ侵害は毎日発生しています。Cisco Advanced Malware Protection（AMP）for Endpoints は、クラウド管理エンドポイント セキュリティ ソリューションであり、サイバー攻撃を防止し、最前線の防御をすり抜けた高度な脅威が損害を引き起こす前に、このような脅威を迅速に検出、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。また、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。

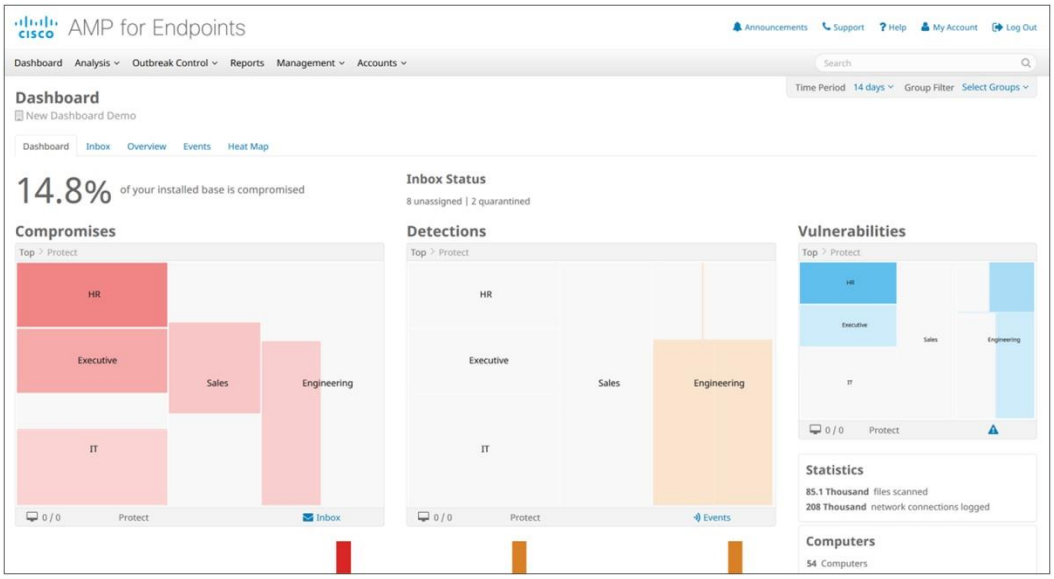
AMP for Endpoints は、保護を強化する最新のグローバル脅威インテリジェンス、攻撃を侵入時点で検出してブロックする組み込みウィルス対策（AV）エンジン、不明なファイルを分析する組み込みサンドボックス テクノロジー、および攻撃パスを遮断し脆弱性を最小限に抑えるプロアクティブな保護機能を備えており、攻撃を防止します。ただしマルウェアがこのような防止対策をすり抜けて侵入した場合、AMP for Endpoints はすべてのファイル アクティビティを継続的に監視、記録することで、悪意のある動作を迅速に検出し、セキュリティ チームに遡って警告を出し、深いレベルの可視性と、経時的にマルウェアの動作を詳しく記録した履歴（どこから侵入し、どこに潜んでおり、何を行っているか）を提供します。AMPは、脅威を自動的に封じ込め修復します。AMP は、Windows、Mac OS、Linux、およびモバイル デバイスが稼働するエンドポイントを防御します。4 分でわかる AMP for Endpoints [英語]

次のメリットが得られます。

- **防止を超える保護**：Cisco AMP for Endpoints は単なる攻撃の防止を超えた機能を提供します。ファイルとトラフィックを継続的に分析します。レトロスペクティブ セキュリティを実現します。レトロスペクティブ セキュリティでは、過去に遡って、プロセス、ファイル アクティビティ、および通信を追跡します。これにより、感染の全体像を把握して根本原因を明らかにし、修復を実行できるようになります。結果として、組織全体にわたって保護の効果および効率が向上します。
- **最高レベルの可視性を実現するモニタリング**：Cisco AMP for Endpoint は、レトロスペクションを超える機能を提供します。また、さまざまな形態のレトロスペクションを一連のアクティビティと関連付け、リアルタイムでの分析を行う、新しいレベルのインテリジェンスが導入されています。さらに、個々のエンドポイント、またはエンドポイントが存在する環境全体にわたって悪意のある動作パターンを見つけ出すことができます。
- **経時的に動作を監視する高度な分析**：Cisco AMP for Endpoint は、高度な動作検出機能により自動化を実現します。この機能は、侵害およびリスクのある上位領域について、優先順位を付けて並べたビューを提供します。
- **受動的な調査から能動的な調査への移行**：Cisco AMP for Endpoint のアクティビティは、調査の一環として事実と手がかりを探すレベルから、マルウェア検出や動作における侵害の痕跡（IoC）などの実際のイベントに基づき、集中的に侵害を探し出すレベルに達しています。
- **非常にシンプルな封じ込め**：Cisco AMP for Endpoint では、イベントのチェーンが可視化され、ダッシュボードとトラジェクトリ ビューを補完するコンテキストが提供されます。AMP は、特定のアプリケーション、ファイル、マルウェア、その他の根本原因をターゲットにすることができ、迅速かつ簡単に攻撃チェーンを断ち切ることができます。
- **コンテキストに応じた実用的なダッシュボード**：レポートの機能は、イベントの列挙や集約だけではありません。Cisco AMP for Endpoints の実用的なダッシュボードにより、合理化された管理と高速な対応が実現します。（図 1 を参照）

- **連携によって機能が強化される統合プラットフォーム**：Cisco AMP for Endpoints は、Cisco AMP for Network ソリューションおよび導入されているその他の AMP との完全な統合により、組織全体の可視性と制御を高めることができます。

図 1. コンテキストを提供する実用性の高いダッシュボード



可視性、コンテキスト、制御を高めて効果的なセキュリティを実現

高度なマルウェアの問題にライフサイクル全体を通じて効果的に対処できるソリューションが求められています。このソリューションでは、予算を圧迫せず、業務効率も犠牲にせずに、最新の脅威に対して保護、インシデントへの対応、修復を実現できる必要があります。課題の一部は、検出およびブロックのためのテクノロジーと、インシデント対応および修復のためのテクノロジーとが連携しておらず、インテリジェントな対応が不足していることに原因があります。

多くの場合、こうしたインテリジェンスの不足により、感染の範囲や深度を完全に把握できないため、インシデント対応や修復は感染の後に行われることになります。さらに、連携不足により、インシデント対応や修復中に感染しているシステムや根本原因が見過ごされ、再感染が際限なく繰り返される場合もあります。

結果として多くの場合、セキュリティ プロフェッショナルは、ネットワーク中の高度なマルウェアの範囲を十分に認識できず、感染後のマルウェアの封じ込めや修復にのみ注力し、以下のような基本的な疑問を解決できなくなります。

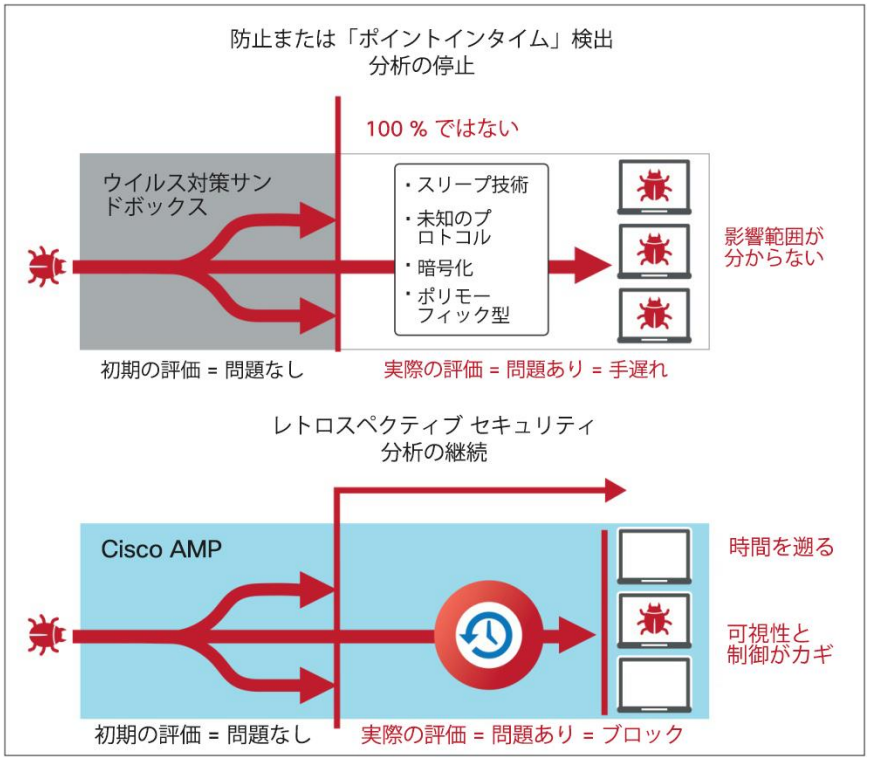
- 攻撃がどのような方法で行われ、どこから侵入したのか
- どのシステムが侵害を受けたか
- その脅威によってどのような被害があったか?
- 脅威を阻止して根本原因を除去することはできるか
- 攻撃から回復するにはどうすればよいか
- 再発を防止するにはどうすればよいか

Cisco AMP for Endpoint による高度なマルウェアの検出、分析、ブロック、修復

予防的セキュリティ ツールだけでは、すべての攻撃を 100 % 防止することはできません。検出を回避して環境を危険にさらすには、たった 1 つの脅威で十分です。巧妙な攻撃者は、標的型でコンテキスト認識型のマルウェアを使用し、予防的防御を欺いて、いつでも、どのような組織に対しても攻撃をしかけられるだけのリソース、技能、そして粘り強さを持っています。さらに、防止ツール（または「ポイントインタイム」検出ツール）は、感染の後では、どこまで侵害されているのか認識できないため、拡散を阻止できず、類似攻撃の再発を防ぐことができません。

Cisco AMP for Endpoints は攻撃を防止し、マルウェアが侵入した際には単なる防止機能を超えた継続的な監視、検出、対応機能を提供します。ビッグデータ分析との組み合わせにより格子状に張り巡らした検出を実現し、エンドポイントでファイルとトラフィックを継続的に分析して、高度なマルウェアが存在するかどうかを判断します（図 2）。また、高度な機械学習手法により、各ファイルに関連付けられた 400 以上の特長を評価し、高度なマルウェアを分析およびブロックします。これらの機能の組み合わせにより、従来の防御機能を超える保護が可能になります。また、攻撃の経過を遡るレトロスペクティブ セキュリティ機能によって、侵入後に悪意のある活動を開始したファイルを検出し、警告を出すことができます。

図 2. 防止（または「ポイントインタイム検出」）ツールと継続的な分析/レトロスペクティブ セキュリティとの比較



これまでにない機能で高度なマルウェアを制御

現在のマルウェアはこれまでになく巧妙になっています。素早い進化を見せるマルウェアは、システムを侵害した後に検出をすり抜けられるようになっています。粘り強い攻撃者はこのマルウェアを起点に組織のネットワーク内を自由に移動します。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。Cisco AMP for Endpoint の継続的な分析とレトロスペクティブ セキュリティの機能は、とらえにくいマルウェアを発見し、高度な脅威対策のカギとなる、次のような疑問への答えを示します。

- 攻撃がどのような方法で行われ、どこから侵入したのか、どのシステムが侵害を受けたか

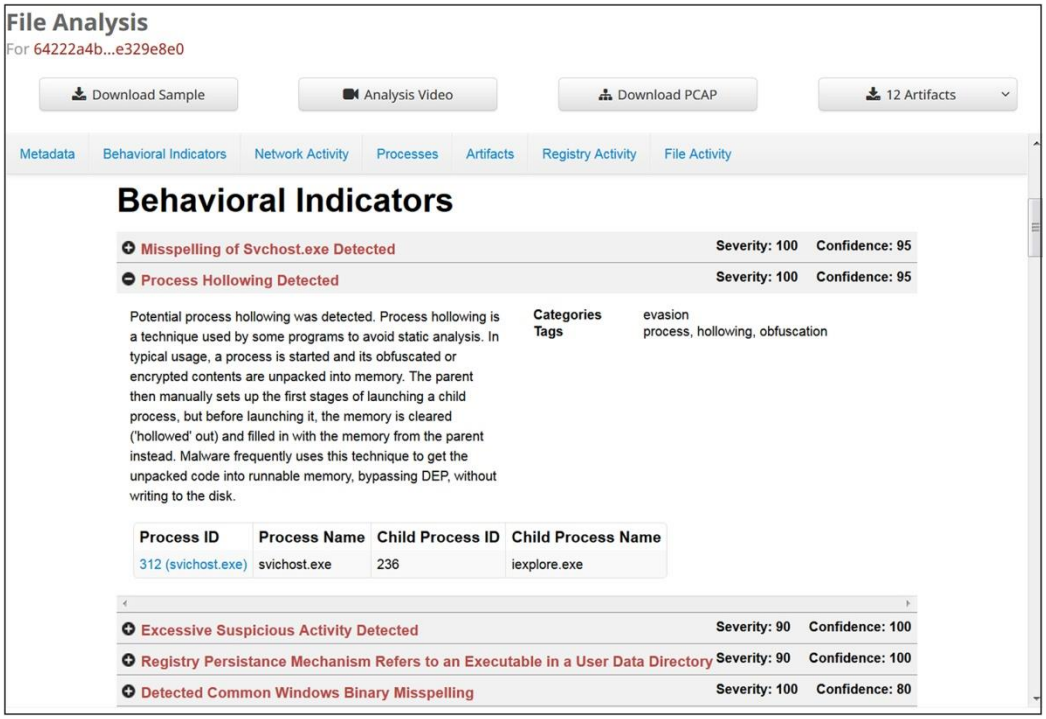
  ファイル トラジェクトリやデバイス トラジェクトリなどの強力なイノベーション（図 3）は、AMP のビッグデータ分析と継続的な分析の機能を使用し、マルウェアに感染したシステムを明らかにします。この感染システムには、潜在的な侵害に関連する感染源や根本原因が含まれます。これらの機能により、マルウェアのゲートウェイと、攻撃者が他のシステムに侵入するための足掛かりを得る目的で使用している経路を特定し、問題の範囲を素早く把握することができます。

図 3. デバイス トラジェクトリによる詳細な分析

- **その脅威によってどのような被害があったか**

  Cisco AMP for Endpoints のファイル分析（図 4）は、Talos Security Intelligence and Research Group に支えられており、AMP の組み込みサンドボックス技術（Threat Grid）を利用して、安全で高度にセキュアなサンドボックス環境を提供し、マルウェアや不審なファイルの動作の分析を可能にします。ファイル分析は、動作の重大度、元のファイル名、実行されているマルウェアのスクリーンショット、サンプル パケットのキャプチャなど、ファイルの動作に関する詳細な情報を提供します。この情報を手に入れることで、流行の封じ込めと将来の攻撃の阻止に何が必要かをよりよく理解することができるのです。

図 4. ファイル分析



デバイス トラジェクトリは、エンドポイントのファイルやネットワーク活動を時系列順に追跡することで、コンピュータ上で脅威となるアクティビティの素早い分析をサポートします。発生したイベントを完全に可視化することで、親プロセス、リモート ホストへの接続、マルウェアがダウンロードした可能性のある未知のファイルなどの痕跡を見つけ出して追跡できます。

侵害の痕跡（IoC）は、多くの場合曖昧で、消去される前にただちに調査しないと、攻撃が次の段階に移ります。Cisco AMP for Endpoints には、エンドポイントをスキャンしたり新たにデータを収集することなく迅速に結果を引き出せるシンプルで柔軟性に優れた検索機能があり、セキュリティ チームはこの機能を利用して攻撃の影響範囲を迅速に特定できます。

- **脅威を阻止し、根本原因を除去し、再発を防止することはできるか**

  Cisco AMP for Endpoint の感染制御は、マルウェアやマルウェア関連アクティビティ（コールバック通信やドロップファイルの実行）などの拡散を効果的に阻止する機能セットを提供します。セキュリティ ベンダーの更新を待つ必要はありません。これらの機能により、わずか数クリックで調査から制御に移行して時間を大幅に節約できるため、脅威の拡散や被害の拡大を抑えることができます。

  さらに、AMP はフルスキャンなしにシステムを自動的に修復できます。この技術は、過去に分析されたファイルを最新の脅威インテリジェンスと継続的に相互参照し、以前には問題がない、または、未知とみなされていても新たに脅威であることが判明したすべてのファイルを隔離します。

PC、Mac、Linux、モバイル デバイス、およびネットワークの保護

Cisco AMP for Endpoints は、PC、Mac、Linux、モバイル デバイスなど、すべてのエンドポイントを高度なマルウェアから保護し、セキュリティ インテリジェンスを向上させます。軽量コネクタ アーキテクチャがビッグデータ分析を使用し、多層防御の要件を簡素化し、高度なマルウェアに対処します。

また、Cisco AMP for Endpoints は Cisco AMP for Network および導入されているその他の AMP との統合により、一元化されたビューを通じて、拡張されたネットワークとエンドポイント全体において包括的な保護を提供します。継続的な分析、レトロスペクティブ セキュリティ、侵害のマルチソース指標を使用することで、エンドポイントからネットワーク レベルでインライン展開しようとするステルス攻撃を特定し、これらのイベントを相互に関連付けて対応を迅速化し、可視性と制御を向上することができます。

エンタープライズ向けに保護を拡大

AMP は、大企業向けに最適化されています。プライバシーの観点から、Cisco AMP for Endpoint のすべてのコネクタは、メタデータで分析を行います。分析では実際のファイルは不要であるため、ファイルが分析用にクラウドに送信されることはありません。プライバシー要件の厳しい組織では、プライベート クラウドのオプションも利用できます。このオンプレミスのシングル ソリューションは、オンプレミスでローカルに保存されたビッグデータ分析、継続的な分析、セキュリティ インテリジェンスを使用して、包括的で高度なマルウェア対策を提供します。

管理の容易性という点では、Cisco AMP for Endpoints コンソール インターフェイスは、管理、導入、ポリシー設定、および Windows システムや Mac、モバイル デバイスへの報告といった機能をすべて備えています。

性能という点では、PC、Mac、Linux、モバイル デバイスに導入される Cisco AMP for Endpoints は軽量コネクタ アーキテクチャを使用しているため、ストレージや処理能力、メモリの要件が他のセキュリティ ソリューションに比べて少なくて済み、攻撃に対して迅速な防御が可能です。

真に包括的なセキュリティ インテリジェンスを獲得

Cisco AMP for Endpoint はビッグデータと比類のないセキュリティ インテリジェンスをベースにしています。Cisco Talos Security Intelligence and Research Group および AMP 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。このデータはクラウドから AMP for Endpoints クライアントにプッシュされるため、常に最新の脅威インテリジェンスを活用できます。

シスコの Threat Grid サンドボックス技術は、AMP for Endpoints との統合により、700 を超える独自の動作指標によりファイル送信の構造だけでなく処理も評価し、関連する HTTP および DNS トラフィック、TCP/IP ストリーム、影響を受けるプロセス、レジストリ アクティビティを含む未知のマルウェアへの知見を提供します。

また、Threat Grid はコンテキストリッチな実用的コンテンツを毎日提供しており、毎月 800 万以上のサンプルを分析し、アーティファクトの数は数十億にも上ります。最後に、Threat Grid の非常に正確なコンテンツ フィードは、既存のセキュリティ テクノロジーとシームレスに統合できるよう標準形式で提供されているため、それぞれの組織固有のコンテキストリッチなインテリジェンスを生成できます。

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。

表 1 に、Cisco AMP for Endpoints の最高クラスの機能を示します。表 2 に、ソフトウェア要件を示します。

表 1. Cisco AMP for Endpoint の機能とメリット

機能	利点
継続的な分析	ファイルがエンドポイントに入ってくると、どのようなファイルだとしても、そのファイルのアクティビティを AMP for Endpoints が観測、分析、記録し続けます。悪意のある動作が検出されると、AMP は、マルウェアのそれまでの動作を時系列で記録したものをユーザに提示します。それは、マルウェアがどこからきたか、どこにいるのか、何をしているのかを示しています。これにより、セキュリティ侵害の範囲を特定し、迅速に対応できます。4 分でわかる継続的分析 [英語]
レトロスペクティブ セキュリティ	レトロスペクティブ セキュリティとは、過去に遡って、プロセス、ファイル アクティビティ、および通信を追跡する機能です。これにより、感染の全体像を把握し、根本原因を明らかにしたうえで修復を実行できます。イベント トリガー、ファイル評価の変更、IoC トリガーなど、IoC が見られたときに、レトロスペクティブ セキュリティの必要性が生じます。
ダッシュボード	シングルペインを通して環境を可視化：ホスト、デバイス、アプリケーション、ユーザ、ファイル、地理位置情報だけでなく、高度な永続的脅威（APT）、驚異の根本原因、その他の脆弱性のビューを考慮した包括的でコンテキストに応じた視点により、十分な情報に基づいてセキュリティの意思決定を行えます。
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	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。これにより、セキュリティ チームはマルウェア インシデントを迅速に特定し、より大規模な組織的攻撃に結び付けることができます。
ファイル 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	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。
ファイル分析とサンドボックス	非常にセキュアな環境でマルウェア動作を実行、分析、テストして、未知のゼロデイ脅威を検出できます。Threat Grid のサンドボックス技術を AMP for Endpoints に統合することで、より大きな動作指標のセットとの照合を行い、より動的な分析が可能になります。
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 トラジェクトリ（感染経路追跡）	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 トラジェクトリ（感染経路追跡）	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。
エンドポイント検索	シンプルなインターフェイスにより、すべてのエンドポイントを対象として、マルウェア エコシステムの一部として残されたアーティファクトを容易かつ迅速に検索でき、検索機能をクラウドに保存されているデータからエンドポイント自体に拡張されます。
拡散度の低い実行ファイル	組織全体にわたって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、標的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。

機能	利点
脆弱性	脆弱なソフトウェアを特定し、攻撃パスを遮断します。この機能は、脆弱性のあるソフトウェアを含むホストのリスト、各ホストの脆弱性のあるソフトウェアのリスト、侵害を受ける可能性が高いホストを表示します。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を特定し、エクスプロイトの可能性がある現象を明らかにし、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。
コマンドラインの可視化	この機能により、実行ファイルの起動に使用されるコマンドライン引数を確認できます。コマンドライン引数を調べ、Windows ユーティリティなどの正当なアプリケーションが悪意のある目的で使用されているかどうかを判断します。たとえば、シャドー コピーの削除に vssadmin が使用されているかどうか、または vssadmin によりセーフ ブートが無効にされているかどうかの確認、PowerShell ベースのエクスプロイトの確認、特権エスカレーション、アクセス コントロール リスト（ACL）の改ざん、およびシステム列挙の試行の調査などです。
アプリケーション プログラミング インターフェイス（API）	AMP for Endpoints で双方向(読み取りおよび書き込み）API が有効になっている場合、ユーザはサードパーティのセキュリティ ツールや SIBM と容易に統合でき、管理コンソールにログインせずに、各自の AMP for Endpoints アカウントでデータとイベントにアクセスできます。
アウトブレイク制御	不審なファイルやアウトブレイクの制御を実現し、コンテンツの更新を待つことなく、感染の封じ込めと修復を素早く外科的に実行します。アウトブレイク制御機能では、シンプルなカスタム検出により、特定のファイルをすべてのシステムまたは選択したシステムで素早くブロックできます。詳細なカスタム署名は、ポリモーフィック型マルウェアの亜種をブロックします。アプリケーションのブロック リストは、アプリケーション ポリシーを適用するか、マルウェアのゲートウェイとして使用される侵害されたアプリケーションを封じ込め、再感染のサイクルを停止します。カスタム ホワイトリストは、安全なアプリケーション、カスタム アプリケーション、またはミッション クリティカルなアプリケーションがどのような状況でも継続的に稼働されるようにします。デバイス フローの関連付けは、特に組織のネットワーク外のリモート エンドポイントを対象に、マルウェアによるコールバック通信を防ぎます。
Threat Grid との統合	Threat Grid のサンドボックス テクノロジーと高度なマルウェア分析機能が統合されており、ファイルの活動を分析する 700 以上ものユニークな動作指標と、わかりやすい脅威スコア、さらに世界中の脅威から幅広い範囲で収集された数十億に及ぶマルウェア アーティファクトを利用できます。サードパーティのサンドボックスを導入する必要がなく、外部統合のタイプを懸念する必要がありません。
Cognitive Threat Analytics（CTA）との統合	AMP for Endpoints が互換性のある Web プロキシ（Cisco WSA または Blue Coat ProxySG などのサードパーティ Web プロキシ）と共に導入されている場合にはエージェントレス検出が可能環境内で平均 30 % 以上の感染を認識。ファイルレスまたはメモリ専用マルウェアや Web ブラウザだけで有効な感染を検出。マルウェアが OS レベルでセキュリティを侵害する前にマルウェアを捕捉。AMP for Endpoints コネクタがインストールされていないデバイスを可視化。AMP for Endpoints 管理コンソールで CTA 検出イベントを確認。
切断モードのサポート	AMP for Endpoints コネクタがクラウドにアクセスできない場合、通常は追跡されクラウドに記録されるアクティビティはすべて、コネクタが AMP Cloud との接続を確立するまでエンドポイントのキャッシュに入れられます。その後、キャッシュに入れられたアクティビティがすべて送信され、コネクタが切断していた間の盲点を排除できます。（2017 年 1 月末予定）現在、コネクタは企業ネットワークにアクセスできない場合にハッシュ情報をインターネット経由で送信します。
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、オンプレミス型の遮断ソリューションとして構築された AMP for Endpoints も用意されています。
AnyConnect v4.1 からの起動	Cisco AnyConnect v4.1 リモート アクセス VPN クライアントをインストールすれば、そのリモート エンドポイント上でエンドポイント コネクタ用 AMP を起動できます。これにより、VPN 対応エンドポイントに対してエンドポイントの脅威防御をすみやかに広げ、リモート ホストからの攻撃の可能性を最小限に抑えることが可能となります。リモート エンドポイントに関する洞察をより多く入手して、攻撃中や攻撃後の修復を迅速に実施できるようにします。

表 2. ソフトウェア要件

Cisco AMP for Endpoint	• Microsoft Windows XP（Service Pack 3 以降） • Microsoft Windows Vista（Service Pack 2 以降） • Microsoft Windows 7 • Microsoft Windows 8 および 8.1 • Microsoft Windows 10 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Mac OS X 10.7 以降 • Linux Red Hat 6.5 および 6.6 • Linux CentOS 6.4、6.5、および 6.6
Android モバイル デバイス向け Cisco AMP for Endpoint	• Android バージョン 2.1 以降

プラットフォーム サポートと互換性

Cisco AMP for Endpoints には、Cisco AMP for Endpoints のライセンスとサブスクリプション（1、3、5 年オプション）および軽量コネクタが含まれます。Cisco AMP for Endpoints は、Cisco AMP for Network およびその他の導入されている AMP と互換性があります。また、リモート エンドポイントで Cisco AnyConnect v4.1 から Cisco AMP for Endpoints を起動することもできます。

保証に関する情報

保証については、Cisco.com の製品保証のページ [英語] を参照してください。

発注情報

Cisco AMP for Endpoints は、該当するライセンスおよびサブスクリプションの製品番号を使用して発注できます。

1. 最初に AMP for Endpoints のライセンス製品番号 FP-AMP-LIC= を検索します。
2. 購入する AMP for Endpoints コネクタ数に相当する数量を入力します。
3. 数量を入力すると、正しいサブスクリプション製品番号が自動的に選択されます。デフォルトは、1 年間のサブスクリプションです。
4. AMP for Endpoints アカウントは、1 年、3 年、または 5 年の期間ベースのサブスクリプションとなっています。3 年間または 5 年間の場合、FP-AMP-LIC= 製品番号でサービス/サブスクリプション期間を編集する必要があります。

図 5 に、AMP for Endpoints の製品番号の構造を示します。

図 5. AMP for Endpoints サブスクリプションの製品番号の例

発注を行うには、シスコ発注ホームページにアクセスするか、シスコのセールス担当者または 800 553-6387 までお問い合わせください。

Cisco Capital

目標の達成を支援するファイナンス

Cisco Capital では、目標を達成し、競争力を維持するために必要なテクノロジーの取得を支援します。設備コストの削減、成長促進、投資と ROI の最適化を支援します。Cisco Capital のファイナンス プログラムにより、ハードウェア、ソフトウェア、サービス、および関連するサードパーティ製機器を柔軟に購入することができます。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

関連情報

詳細については、以下のリンクを参照してください。

- エンドポイント向け Cisco AMP

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

C78-733181-07JA 17.03