McAfee Advanced Threat Defense

高度な標的型攻撃を検出

Intel Security®が提供するMcAfee® Advanced Threat Defenseは、現在の高度な標的型攻撃を検出し、収集した脅威情報から迅速にアクションを実行して組織を保護します。従来のサンドボックスと異なり、高度な検査機能により、回避技術を駆使した脅威も検出します。ネットワークからエンドポイントまでを網羅しているIntel Securityのソリューションとの緊密な統合により、環境全体で脅威情報を迅速に共有し、保護機能と検査機能を強化できます。

McAfee Advanced Threat Defenseの主な差別化要因

Intel Securityソリューションとの緊密な統合

- 検出から封じ込めまでの時間を短縮し、組織全体を保護できます。
- ワークフローが簡素化され、対応と修復にかかる時間を短縮できます。

強力な分析機能

- 強力な解凍機能により、正確な分析を行います。
- 高度な静的コード分析と動的分析により、豊富なデータで正確な分析を行います。

マルウェア分析の集中管理

- 分析結果の共有によりネットワークで必要なデバイスが少なくなり、コストを抑えることができます。
- 配備が簡単です。

ネットワークからエンドポイントまでの保護対策に高度なマルウェア分析機能を統合し、IT環境全体で脅威情報を共有することで、脅威の検出方法が大きく変わります。管理システム、ネットワーク、エンドポイントで脅威情報を共有することで、攻撃を速やかに遮断し、感染システムを隔離できます。同一または類似した脅威を阻止するだけでなく、影響を受けた可能性がある場所を特定し、修復することもできます。

McAfee Advanced Threat Defense: 高度脅威の検出

McAfee Advanced Threat Defenseは、多層型の革新的なアプローチで現在のステルス型攻撃やゼロデイ マルウェアを検出します。ウイルス対策のシグネチャ、レピュテーション、リアルタイム エミュレーションと詳細な静的コード分析、動的分析（サンドボックス）を組み合わせ、実際の挙動を分析します。このソリューションは市場で最も強力で高度なマルウェア対策技術を提供するので、保護対策とパフォーマンスのバランスを維持できます。

既知のマルウェアは、シグネチャとリアルタイム エミュレーションで検出し、パフォーマンスを向上させています。回避技術を駆使した巧妙な脅威は完全な静的コード分析とサンドボックスで阻止します。また、詳細なマルウェア分類情報により、既知のマルウェア ファミリとの類似性を評価します。コードを解凍して詳細な静的コード分析を行うので、サンドボックス回避技術を駆使し、すぐには実行されないコードも検出します。

マルウェアの作成者はパッキングでコードの構成を変更したり、検出を回避しようとします。大半の製品は元の実行コードを正しく解凍できませんが、McAfee Advanced Threat Defenseの高度な解凍機能を使用すると、難読化を解除し、元の実行コードを確認することができます。また、静的コード分析では、ファイル属性と命令セットを解析してコードの挙動を特定します。

静的コード分析と動的分析により、マルウェアの疑いがあるコードを正確に評価します。

統合されるソリューション

- **McAfee Active Response**
- **McAfee Application Control**
- **McAfee Enterprise Security Manager**
- **McAfee ePolicy Orchestrator**
- **McAfee Network Security Platform**
- **McAfee Threat Intelligence Exchange**
- **McAfee Web Gateway**

ターゲットに合わせたサンドボックスで検出の正確性を向上

環境変数やカスタム アプリケーションを狙った攻撃の多くはサンドボックスで検出されません。このような攻撃を検出するため、McAfee Advanced Threat Defenseはカスタム イメージの分析にも対応しています。組織に最適なオペレーティング システムやアプリケーションを決めるだけでなく、バージョンも指定できます。これにより、汎用的なイメージではなく、実際のホスト プロファイルの条件で脅威を分析できるので、より正確なリスク評価が可能になります。

同じネットワーク上で複数のホスト プロファイルを実行している場合でも、McAfee Advanced Threat DefenseはMcAfee ePolicy Orchestrator®（McAfee ePO™）と連携し、ホストのオペレーティング システムとアプリケーションを特定します。さらに、ターゲット ホストの条件で不審なファイルを分析します。

保護の強化

高度なマルウェアを検出することは重要です。しかし、レポートを作成したり、アラートを通知するだけでは管理者の負担が増すだけで、ネットワークは保護された状態になりません。

McAfee Advanced Threat Defenseは、ネットワークからエンドポイントまでのセキュリティ デバイスと緊密に統合されているので、McAfee Advanced Threat Defenseが不審なファイルを検出するとすぐにアクションを実行できます。このように検出と保護が緊密かつ自動的に統合されている点が非常に重要です。

McAfee Advanced Threat Defenseは、特定のセキュリティ ソリューションと直接統合することも、McAfee Threat Intelligence Exchange経由で統合することもできます。

直接統合した場合、McAfee Advanced Threat Defenseが検出したファイルにIntel Securityのソリューションがアクションをすぐに実行します。脅威情報を既存のポリシー施行プロセスに組み込み、同一または類似したファイルをネットワーク全体でブロックすることができます。

McAfee Advanced Threat Defenseの検出結果が統合製品のログとダッシュボードに表示されるので、分析全体が一つの環境で実行されているように見えます。これにより、ワークフローが簡素化されるので、1つのインターフェースでアラートを効率よく管理できます。

McAfee Threat Intelligence Exchangeとの統合により、McAfee Endpoint Protectionなどの保護対策とMcAfee Advanced Threat Defenseが連動し、分析結果と侵入の痕跡が共有されます。McAfee Advanced Threat Defenseが不審なファイルを検出すると、McAfee Threat Intelligence Exchangeがレピュテーションを更新し、最新の脅威情報を組織内の統合セキュリティに配信します。

McAfee Threat Intelligence Exchangeを使用するエンドポイントは、新しいマルウェアの感染をブロックし、同じファイルによる攻撃を未然に防ぎます。McAfee Threat Intelligence Exchangeに統合されたゲートウェイは、組織への不審なファイルの侵入を阻止します。また、McAfee Threat Intelligence Exchangeを使用するエンドポイントは、社内ネットワークに接続していない場合でもファイルの検出情報を受信し、ペイロードの拡散を防ぎます。

感染システムの検出と修復

攻撃に対して適切な判断と対応を行うには、優先度を含む実用的な情報で組織全体を可視化する必要があります。マカフィーの複数のソリューションを併用すると、組織の状況を正確に把握することができます。

McAfee Enterprise Security Managerは、McAfee Advanced Threat Defenseなどからファイル レピュテーションと実行イベントを収集し、相関分析を行います。高度なアラートと履歴ビューにより、詳細な情報からセキュリティ状況をリアルタイムで把握し、リスクの優先度を判断できます。McAfee Advanced Threat Defenseが検出した痕跡データはMcAfee Enterprise Security Managerが6か月間管理し、ネットワークやシステムの分析に使用されます。これにより、新たに識別されたマルウェアの発生源と以前に通信を行っていたシステムも特定できます。McAfee Enterprise Security Managerではリスクを明確に把握し、訂正処置をすぐに実行できます。McAfee Endpoint Protection、McAfee Threat Intelligence

Exchange、McAfee Active Responseの緊密な統合により、的確なセキュリティ オペレーションを実施できます。新しい構成の送信、新しいポリシーの実装、ファイルの削除、ソフトウェア更新の配備などを行い、リスクを回避できます。ネットワーク内で感染したエンドポイントはMcAfee Active Responseによって自動的に識別され、McAfee Advanced Threat Defenseレポートに表示されるので、的確なアクションをすぐに実行できます。

配備

McAfee Advanced Threat Defenseは、高度なマルウェア分析を行うアプライアンスとして配備され、既存のマカフィー セキュリティにシームレスに統合されます。McAfee Advanced Threat Defenseは、Intel Securityの複数のデバイスで共有されるので、無駄な費用をかけずにネットワークを拡張できます。

セキュリティ オペレーション センターとマルウェアの分析者もMcAfee Advanced Threat Defenseを使用して分析を行うことができます。

McAfee Advanced Threat Defenseは次のような高度な機能を提供します。

- ユーザー対話モード: マルウェアのサンプルを直接使用しながら分析を行うことができます。
- 高度な解凍機能: 数日かかっていた調査も数分で終わります。
- 完全な論理パス: 標準的なサンドボックス環境で休眠状態のサンプルを追加の論理パスで強制的に実行し、詳しい分析を行うことができます。
- 複数の仮想環境へのサンプルの送信: ファイルの実行に必要な環境変数を特定し、調査時間を短縮できます。
- 関数の関係図、埋め込みファイルやドロップされたファイルの情報を含む詳細レポート: 脅威の分析者に重要な情報を提供します。

McAfee Advanced Threat Defenseの評価をご希望の方は、弊社の営業担当までご連絡いただくか、**www.mcafee.com/jp/products/advanced-threat-defense.aspx**をご覧ください。

McAfee Advanced Threat Defenseの仕様	**ATD-3000**	**ATD-6000**
サイズ	1Uラックマウント	2Uラックマウント
検出	**ATD-3000/ATD-6000**	
対応のファイル/メディア タイプ	PEファイル、Adobeファイル、Microsoft Officeファイル、イメージ ファイル、アーカイブ、Java、Androidアプリケーション パッケージ	
分析方法	McAfee Anti-Malware Engine、GTIレピュテーション（ファイル/URL/IP）、Gateway Anti-Malware（エミュレーションと動作分析）、動的分析（サンドボックス）、静的コード分析	
対応OS	Windows 8（32ビット/64ビット）、Windows 7（32ビット/64ビット）、Windows XP（32ビット/64ビット）、Windows Server 2003、Windows Server 2008（64ビット）、Android 次の言語のすべてのWindowsオペレーティング システム: 英語、ドイツ語、イタリア語、日本語、中国語（簡体字）	

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒150-0043 東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店　〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810-0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com