McAfee Advanced Threat Defense

高度な標的型攻撃を検出

McAfee® Advanced Threat Defenseを使用すると、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できます。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セキュリティ 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。柔軟な配備オプションが用意され、様々なネットワークに配備できます。

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、シグネチャなどの静的分析だけでなく、動的分析（サンドボックス）によるリアルタイム エミュレーションを行い、実際の動作を分析します。コードの静的分析でファイルの属性と命令セットを検査し、意図と動作を特定して既知のマルウェアファミリとの類似性を評価します。分析の最終段階で、McAfee Advanced Threat Defenseはディープ ニューラル ネットワーク経由で機械学習を利用し、不正な兆候を確認します。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し、パフォーマンスを低下させずに高度な調査を行います。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、パフォーマンスの低下を防ぎます。回避技術を駆使した巧妙な脅威は、機械学習の結果を利用した詳細な静的コード分析とサンドボックスで阻止します。不正な兆候は、詳細な静的コード分析と機械学習の結果から特定します。

McAfee Advanced Threat Defenseの主な差別化要因

McAfeeソリューションの緊密な統合

- 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。
- 詳細な静的コード分析、動的分析、機械学習により、豊富なデータで正確な分析を行います。

柔軟で一元管理された配備

- 複数のプロトコルに対応した集中配備でコストを削減できます。
- 柔軟な配備オプションが用意され、様々なネットワークに配備できます。

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の高度な解凍機能は、難読化を解除し、元の実行コードを確認します。また、詳細な静的コード分析でファイルの属性と命令セットを解析し、コードの挙動を特定します。

静的コード分析、機械学習、動的分析により、マルウェアの疑いがあるコードが正確に評価されます。高度な分析結果から生成されたサマリー レポートで状況を確認し、優先度に従ってアクションを実行できます。また、詳細レポートにより、マルウェアの詳しい分析結果を確認できます。

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は様々な方法で統合できます。特定のセキュリティ ソリューションに直接統合することも、McAfee Threat Intelligence ExchangeやMcAfee Advanced Threat Defense Email Connectorを介して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McAfee 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。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。

統合されるソリューション

- McAfee Active Response
- McAfee Advanced Threat Defense Email Connector
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator®
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Application Control
  - McAfee Endpoint Protection
  - McAfee Security for Email Servers
  - McAfee Server Security
- McAfee Web Gateway

McAfee Advanced Threat Defense Email Connectorを利用すると、McAfee Advanced Threat Defenseはメールゲートウェイからメールの添付ファイルを受信し、分析することができます。McAfee Advanced Threat Defenseは添付ファイルを分析し、メッセージのヘッダーに分析結果を挿入してメール ゲートウェイに戻します。メール ゲートウェイは、ポリシーに従ってアクション（添付メールの削除や隔離など）を実行し、内部ネットワークへのマルウェアの侵入を阻止します。McAfee Threat Intelligence ExchangeをMcAfee Advanced Threat DefenseとMcAfee Security for Email Serversを統合することで、メール サーバーで高度な検出を行います。

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。McAfee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を特定できます。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、的確な対策をすぐに実行できます。

配備

高度な脅威分析には柔軟な配備オプションが用意され、様々なネットワークに配備できます。McAfee Advanced Threat Defenseは、オンプレミス アプライアンスまたは仮想のフォーム ファクターとして使用できます。いずれのフォーム ファクターもMcAfee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、効率的に拡張できます。

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。

- 設定可能なオペレーティング システム / アプリケーション サポート : 特定の環境変数で分析を調整し、 脅威の検証と調査のサポートを行うことができます。
- 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、調査にかかる時間を短縮できます。
- 逆アセンブル出力やメモリー ダンプ、関数呼び出しの関係図、埋め込みファイルやドロップされたファイル、ユーザー API のログ、PCAP 情報など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		
物理フォーム ファクター	ATD-3100 1Uラックマウント	ATD-6100 1Uラックマウント
仮想フォーム ファクター	v1008、v1016、v3032、v6064 ESXi 5.5, 6.0	v1008、v1016、v3032、v6064 ESXi 5.5, 6.0
検出		
対応のファイル/サンプル 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、URL	
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）、詳細なコード分析、カスタムYARAルール、機械学習、ディープ ニューラル ネットワーク	
対応OS	Windows 10（64ビット）、Windows 8.1（64ビット）、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 2016、Windows Server 2012、Windows Server 2012 R2、Windows Server 2008、Windows Server 2003、Android すべての言語のWindowsオペレーティング システム。	
出力形式	STIX、OpenIOC、XML、JSON、HTML、PDF、テキスト	
送信方法	ポイント製品との統合、RESTful API、手動送信、McAfee Advanced Threat Defense Email Connector（SMTP）	

〒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（代表）
www.mcafee.com/jp