データシート

McAfee Endpoint Threat Defense and Responseファミリ

ゼロデイ マルウェアを検出して高度な攻撃を未然に防ぐ

急激に進化するサイバー脅威からエンドポイントを保護するには、新しい次元のセキュリティ対策が必要です。脅威が高度化し、未知の脆弱性に対するリスクが高まっているため、多くの企業は複数のセキュリティ ソリューションを導入しています。これらのソリューションは相互に関連性もなく、機能が重複している場合もあります。このため、可視化が制限され、セキュリティ環境は複雑さを増しています。この問題を解決するため、McAfeeはMcAfee® Endpoint Threat DefenseとMcAfee Endpoint Threat Defense and Responseを提供しています。いずれのソリューションも静的分析と動作分析を利用し、脅威情報を統合して、新たに発生する脅威の検出と対応、問題の修復を行います。統合されたセキュリティ コンポーネントが1つのソリューションのように機能し、脅威情報の共有と簡素化されたワークフローにより環境の可視化を強化します。統合されたセキュリティ機能とフォレンジックにより、安全なインフラを実現し、潜在的な脅威を迅速に検出して被害を未然に防ぎます。

ゼロデイ マルウェア、グレーウェア、ランサムウェアを阻止

静的分析と動的分析により、新たに発生する脅威を未然に防ぎます。高度なレピュテーションと動作分析により潜在的な攻撃を検出します。McAfee Threat Intelligence Exchangeと脅威情報を共有し、脅威を迅速にブロックして封じ込めます。また、レピュテーション情報を迅速に更新し、新たな攻撃を阻止します。

McAfee Endpoint Threat DefenseとMcAfee Endpoint Threat Defense and Responseは、クラウド（米国のデータセンター）を使用して不正な動作とReal Protectの脅威モデルの類似性を識別し、ゼロデイ マルウェアを阻止します。この動作分類技術は、他のセキュリティ ソフトウェアで検出されない脅威の根絶に使用されます。McAfee ePolicy Orchestratorから実用的な脅威情報を提供し、ゼロデイ脅威の検出とリアルタイムの修復を可能にします。動作分類は動的な機械学習により自動的に進化します。これにより、セキュリティの欠陥を減らしながら、保護レベルを向上させることができます。

主な特長

- ゼロデイ マルウェア、グレーウェア、ランサムウェアの検出、保護、問題の修正を行います。
- 動的なレピュテーション、動作分析、機械学習により、効果的な保護を行います。
- ユーザーや信頼できるアプリケーションの影響を最小限に抑えながら、保護機能を強化します。
- セキュリティ エコシステムで脅威情報を共有することで、より多くの脅威に迅速に対応できます。
- ワークフローの統合とMcAfee® ePolicy Orchestrator® (McAfee ePO™) の管理コンソールにより、インシデント調査と修復作業を簡単に行うことができます。

イベント数を減らして問題の解決を迅速に

セキュリティ イベントの数を減らし、自動的に識別できる脅威が増えるので、最も重要な問題に迅速に対応できます。また、脅威情報を共有し、プロアクティブなアラートを利用して自動応答を定義します。調査や問題解決の労力を軽減するため、ワークフローが簡素化されています。これにより、イベントに迅速に対応し、セキュリティ機能を拡張しながら組織全体の保護レベルを強化できます。

接続されたコンポーネントがMcAfee Data Exchange Layer経由で重要なセキュリティ情報を自動的に共有します。McAfee Threat Intelligence Exchangeでは、McAfee Global Threat Intelligenceやサードパーティの情報源など、エコシステム全体で包括的な脅威情報を共有し、保護対策で自動的に活用することができます。

最初の攻撃を未然に防ぐ

ゼロデイ マルウェアを検出し、エンドポイントに対する変更を阻止します。アプリケーションの動的隔離がグレーウェアの動作を監視し、不正な変更を阻止します。これにより、攻撃を実行する前にエクスプロイトを効率的に阻止します。ネットワーク上にないエンドポイントも保護し、不正な動作を封じ込めます。このような保護機能をユーザーが意識することはありません。

セキュリティ プロセスの拡大と採用を可能に

ポリシー施行、インシデントの調査、修復をMcAfee ePOで簡単に行うことができます。この管理コンソールを使用すると、すべてのシステムの状況を把握し、エンドポイントのセキュリティ状況を簡単に診断できます。また、保護対策をリアルタイムで有効にできます。ワークフローの統合とワンクリックの修復により、1つのエンドポイントでもインフラ全体でもモニタリング、検索、対応を簡単に行うことができます。McAfee Endpoint Threat DefenseとMcAfee Endpoint Threat Defense and Responseでは、機械学習機能を利用して動作分類モデルを自動的に更新し、すべてのセキュリティ コンポーネントで脅威情報を迅速に共有します。これらのコンポーネントは1つの統合されたシステムとして機能し、新たに発生する脅威を阻止します。事前に設定した対応で潜在的な脅威を阻止できるので、セキュリティ管理で優先度の高い他の作業にスタッフを振り分けることができます。

高度脅威の検出、優先度の判定、修復

McAfee Endpoint Threat Defense and Responseを使用すると、攻撃元、範囲、影響を判断できます。このソリューションは、McAfee Active Response技術を使用し、インフラ内のエンドポイントの現在の状況と履歴を表示します。攻撃の兆候を識別し、コンテキスト情報を元に優先度を設定するので、迅速な対応が可能になります。

正確、高速、迅速な保護機能により、現在広まっている脅威だけでなく、潜伏する脅威や回避技術を駆使する脅威をプロアクティブに阻止します。質の高い情報と可視化により、脅威の侵入口をピンポイントで特定できるので、脅威をすぐに封じ込め、問題を修復できます。これまで数か月かかっていた修復作業を数分または数ミリ秒で行うことができます。

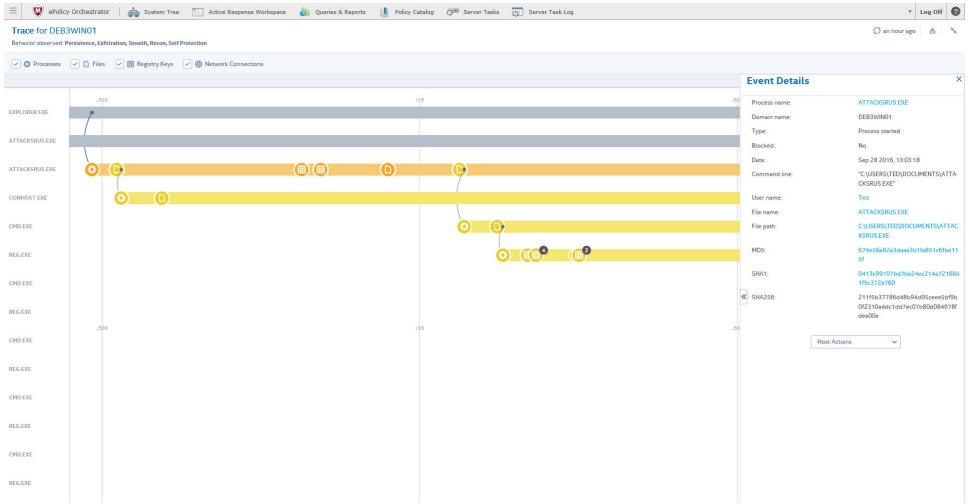

図1. ワークスペースで不審なインシデントの発生源や動作を追跡できるので、インシデント対応を迅速に行うことができる。

McAfee Endpoint Threat Defense and Response ファミリの機能

コンポーネント	利点	顧客のメリット	差別化	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
アプリケーションの動的隔離[1]	ネットワーク内外のエンドポイントに対する不正な変更を阻止し、グレーウェアによる被害を未然に防ぎます。	▪ 実際に攻撃を受ける前に、潜在的な脅威を分析し、検出します。 ▪ ユーザーや信頼されたアプリケーションに影響を及ぼすことなく、保護機能を強化できます。 ▪ ユーザーによる操作を必要最低限に抑え、検出から封じ込めまでの時間を短縮します。 ▪ エンドポイントの生産性を低下させずに、脅威を隔離し、攻撃を未然に防ぎます。	▪ McAfeeのインフラの中核として機能し、保護対策の最適化と効率化を行います。 ▪ インターネット接続の有無に関係なく動作します。外部からの入力や分析も不要です。 ▪ ユーザーに透過的に機能します。 ▪ 監視モードにより、環境内でエクスプロイトの可能性のある動作を迅速に識別します。	√	√

コンポーネント	利点	顧客のメリット	差別化	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Real Protect	機械学習による動作分類を行い、ゼロデイ マルウェアの実行を未然に防ぎます。以前に検出を回避した脅威も検出し、実行を阻止します。	▪ ランサムウェアなど、検出が難しいゼロデイ マルウェアも簡単に検出できます。 ▪ 脅威の識別と分析、問題の修復を自動的に行います。ユーザーの操作は必要ありません。 ▪ 接続されたセキュリティ インフラを使用し、自動的に分類を行います。	▪ 静的と動的の両方の動作分析を行い、保護対策を強化します。 ▪ 動的な動作分析でしか検出できないマルウェアを検出します。 ▪ リアルタイムでレピュテーションを更新し、すべてのセキュリティ コンポーネントの効率性を強化します。	√	√
McAfee Threat Intelligence Exchange	セキュリティ コンポーネントを接続し、コンテキスト情報を共有します。組織全体を可視化し、適応型の脅威対策を行います。	▪ 最初の攻撃を確認すると、その情報をセキュリティ システム間で共有し、更なる感染を未然に防ぎます。 ▪ 総所有コストを削減し、効率的なエンドポイント セキュリティを運用できます。 ▪ セキュリティ コンポーネントを統合し、完結した保護システムを実現します。個々のセキュリティ技術を1つのシステムに統合します。	▪ McAfee Global Threat Intelligenceのフィード、サードパーティの情報、ローカルの脅威情報を統合できます。 ▪ ローカルまたはサードパーティの情報を使用して、信用できる対象かどうかを定義します。 ▪ エンドポイント、Web、ネットワーク、クラウド製品から脅威のレピュテーション情報を迅速に取得します。 ▪ 実用的な脅威情報をレポートを抽出し、保護対策に適用します。	√	√
McAfee Data Exchange Layer	セキュリティを統合し、McAfee製品や他社製品間の通信を簡素化します。	▪ リスクを軽減し、対応時間を短縮できます。 ▪ オーバーヘッドが減少し、運用スタッフのコストを削減できます。 ▪ プロセスを最適化し、実用的な推奨事項を利用できます。	▪ すべてのセキュリティ製品間で脅威情報を共有します。 ▪ 他のすべてのエンドポイントと脅威情報を迅速に共有し、脅威を未然に防ぐだけでなく、保護機能も更新できます。	√	√
McAfee ePO による管理	拡張性と柔軟性に優れた管理機能で、セキュリティポリシーを1つのコンソールで管理し、セキュリティ問題の識別と対応を行うことができます。	▪ セキュリティ ワークフローを統合して簡素化しています。 ▪ すべてのシステムを可視化し、セキュリティの状況をすぐに把握し、リアルタイムで保護対策を実行できます。 ▪ カスタマイズ可能なポリシー施行でMcAfeeのセキュリティ対策を迅速に配備し、管理できます。 ▪ 動的で自動的なクエリー、ダッシュボード、対応により、情報の取得から対応までの時間を短縮できます。	▪ 1つのコンソールできめ細かい制御を行い、セキュリティ管理作業を迅速に実行できます。コストの削減も可能です。 ▪ ドラッグアンドドロップに対応したダッシュボードにより、エコシステム全体の状況をリアルタイムで把握できます。 ▪ オープン プラットフォームのSDK（ソフトウェア開発キット）により、新しいセキュリティ技術をすぐに採用できます。	√	√
McAfee Active Response	脅威の可視化、タイムライン、ライブ情報と履歴情報により、アクションをすぐに実行し、保護を実行することができます。	▪ 現在の脅威データと履歴データを迅速に検索し、攻撃の範囲を特定できます。調査を効率的に行い、対応までの時間を短縮できます。 ▪ 脅威対応を自動的に実行します。ユーザーの操作は不要です。 ▪ 脅威に優先度を設定します。 ▪ 継続監視とカスタマイズ可能なコレクターにより、攻撃の兆候を検出します。実行中の攻撃だけでなく、休眠中や削除された脅威も検出できます。	▪ 保護技術で検出されなかった未知のエクスプロイトや危険な動作をすぐに把握できます。 ▪ 他のエンドポイントの情報を検索しながら、イベントのタイムラインを調査できます。 ▪ ワンクリックで保護や修復などのアクションを実行できます。複数のツールを使用したり、複数の操作を行う必要はありません。		√

仕様

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
対応プラットフォーム:	**対応プラットフォーム:**
▪ Microsoft Windows: 7、To Go、8、8.1、10、10 November、10 Anniversary	▪ Microsoft Windows: 7、8、8.1、10、10 Anniversary
▪ Mac OS X 10.5以降	▪ RedHat 6.5
▪ Linux: RHEL、SUSE、CentOS、OEL、Amazon Linux、Ubuntuの最新バージョン	▪ CentOS 6.5
サーバー:	▪ Windows Server 2008、2012、2016
▪ Windows Server（2003 SP2以降、2008 SP2以降、2012）、Windows Server 2016	
▪ Windows Embedded（Standard 2009、Point of Service 1.1 SP3以降）	
▪ Citrix Xen Guest	
▪ Citrix XenApp 5.0以降	

1. McAfee Endpoint Threat Defense and Responseでは、米国に存在するデータセンターを利用して、顧客の認証検証、ファイル レピュテーションの確認、不審なファイルに関連するデータの保存を行います。必須ではありませんが、アプリケーションの動的隔離がクラウドに接続する場合があります。McAfee Active Response、アプリケーションの動的隔離、Real Protectのすべての機能を利用するには、クラウド アクセスとアクティブ サポートが必要になります。これらの機能を利用するには、クラウド サービスの利用条件に同意する必要があります。

詳細情報

McAfee Endpoint Threat Defenseの詳細については、**www.mcafee.com/jp/products/endpoint-threat-defense.aspx**をご覧ください。

McAfee Endpoint Threat Defense and Responseの利点については、**http://www.mcafee.com/jp/products/endpoint-threat-defense-response.aspx**をご覧ください。

〒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