McAfee Application Control

未承認のアプリケーションによるリスクからエンドポイント、サーバー、専用デバイスを保護。

リモート攻撃またはソーシャル エンジニアリングを利用する高度な持続型脅威（APT）により、ビジネスの保護は一段と難しくなっています。McAfee® Application Controlを利用すると、サイバー犯罪を未然に防ぎ、生産性を維持しながらビジネスを保護できます。McAfeeのこのソリューションは、動的な信用モデルと革新的なセキュリティ機能（ローカルとグローバルのレピュテーション情報、リアルタイムの動作分析、エンドポイントの自動保護など）を使用してAPTを迅速に阻止します。手間のかかるリスト管理やシグネチャの更新は不要です。McAfee Application Controlを使用すると、ゼロデイ脅威を未然に防ぐことができます。

インテリジェントなホワイトリスト

McAfee Application Controlは、未承認のアプリケーションの実行をブロックし、ゼロデイ攻撃とAPT攻撃を阻止します。インベントリ機能により、アプリケーションに関連するファイルを簡単に確認し、管理できます。組織内のすべてのバイナリ（EXE、DLL、ドライバー、スクリプト）がアプリケーションまたはベンダーごとにグループ化され、階層的に表示されます。また、アプリケーションが状態（正常、不正、不明）別に自動的に分類されます。正常なことが確認され、ホワイトリストに登録されたアプリケーションだけに実行が許可されるので、未知のマルウェアによる攻撃も阻止できます。

適切なセキュリティ ポスチャの実施

ソーシャルやクラウドがビジネスに欠かせない存在となり、アプリケーションの利用形態に柔軟性が求められています。McAfee Application Controlには次の3つのオプションがあり、柔軟な脅威対策が可能です。

図1. 柔軟なホワイトリスト戦略が可能な3つのオプション

主な特長

- シグネチャの更新なしでゼロデイやAPTを阻止
- McAfee Global Threat IntelligenceとMcAfee Threat Intelligence Exchangeの利用により、ファイルとアプリケーションに関するグローバルとローカルのレピュテーションを提供
- 動的ホワイトリストにより、信用されたチャネルで追加されたアプリケーションを自動的に承認し、セキュリティの強化と総所有コストの削減を実現
- マカフィー セキュリティ ソリューションの集中管理プラットフォームであるMcAfee® ePolicy Orchestrator®（McAfee ePO™）ソフトウェアによりアプリケーションアクセスを効率的に制御
- 安全なホワイトリストと高度なメモリー保護機能でパッチの適用サイクルを短縮
- 信用された更新プログラムで最新のパッチを適用し、システムを常に最新の状態に維持
- 接続または切断状態のサーバー、仮想マシン、エンドポイント、POSなどの専用デバイス、Microsoft Windows XPなどのレガシー システムを保護

強力な提案機能

インベントリ検索や事前定義のレポートにより、環境内に存在する脆弱性、コンプライアンス違反、セキュリティ問題を迅速に検出し、修復できます。最近追加されたアプリケーション、未承認のバイナリ、レピュテーション不明のファイル、古いバージョンのソフトウェアが実行されているシステムなどをすばやく突き止め、ソフトウェア ライセンスの問題を検証できます。

完全で迅速な対応

ホワイトリスト機能はMcAfee Global Threat Intelligence (McAfee GTI) から取得したグローバル脅威情報を使用します。McAfee の独自の技術で、世界中に存在する数百万台のセンサーを利用し、ファイル、メッセージ、送信者のレピュテーションをリアルタイムで追跡します。McAfee Application Controlは、この情報を使用して環境内に存在するファイルのレピュテーションを確認し、ファイルを正常、不正、未知のいずれかに分類します。

McAfee Application Controlを別売りのオプション モジュールであるMcAfee Threat Intelligence Exchangeと一緒に配備すると、ローカルのレピュテーション情報に基づいてホワイトリストを更新し、脅威を迅速にブロックできます。McAfee Application Controlは、McAfee Advanced Threat Defenseと連携し、McAfee Threat Intelligence Exchangeを使用して、サンドボックスで未知のアプリケーションの動作を動的に分析し、新たに検出されたマルウェアからエンドポイントを自動的に保護します。

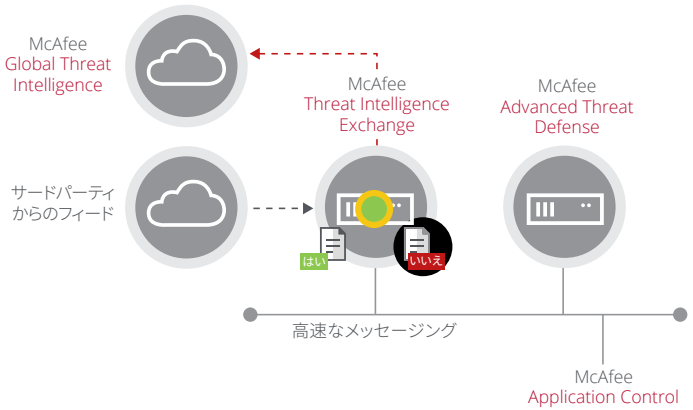

図2. McAfee GTIがファイルと送信者のレピュテーションを継続的に監視。McAfee Threat Intelligence Exchangeと一緒に配備すると、McAfee Application Controlがローカルのレピュテーション情報に基づいてホワイトリストを自動的に更新します。ファイルに関する情報がさらに必要な場合にはMcAfee Advanced Threat Defenseと連携します。

ビジネスの妨げにならない

ビジネスの継続性を妨げないように、レピュテーションに従って新しいアプリケーションが自動的に許可されます。レピュテーションが不明な場合、エンドポイントの実行パターンに応じて新しい推奨ポリシーがインターフェースに表示されます。ブロックされたアプリケーションの管理も重要です。ブロックされたアプリケーションの詳細と確認してから、ホワイトリストに登録されたファイルを承認したり、ファイルを無視してアプリケーションをブロックします。

主な特長 (続き)

- アプリケーションの評価や自己承認によって新しいアプリケーションを許可し、ビジネスの継続性を向上
- オーバーヘッドが少なく、ユーザーの生産性とサーバー パフォーマンスを維持
- レガシー システムと最新技術に対する投資を保護

対応プラットフォーム

Microsoft Windows (32ビット/64ビット)

- 組み込み: Windows XPE、7 Embedded、WEPOS、POSReady 2009、WES 2009、Embedded 8、8.1 Industry、10
- サーバー: Windows Server 2008、2008 R2、2012、2012 R2
- デスクトップ: Windows NT、2000、XP、Vista、7、8、8.1、10

Linux

- Red Hat/CentOS 5、6、7
- SUSE/openSUSE 10、11
- Oracle Enterprise Linux 5、6、7
- Ubuntu 12.04

ユーザーに対する通知

アプリケーションのレピュテーションが不明な場合、McAfee Application Controlは次の方法で新しいアプリケーションのインストールを許可します。:

- **ユーザー通知** — 分かりやすいポップアップ メッセージを送信し、未承認のアプリケーションが拒否された理由を説明します。ユーザーは、このメッセージの内容を確認して、メールまたはヘルプデスクで承認依頼を行うことができます。
- **ユーザーの自己承認** — 特権ユーザーは、IT部門の承認を待たずに新しいソフトウェアをインストールできます。IT部門はこれらの自己承認を検証し、企業全体に適用されるポリシーを作成して、すべてのシステムでアプリを禁止または許可できます。

システムを常に最新の状態にする

システムに最新のパッチを適用し、常に最新の状態にしておく必要があります。このため、弊社では、業務の妨げにならずにシステムを自動的に更新する動的信用モデルを提供しています。このモデルでは、信用されたユーザー、証明書、プロセス、ディレクトリを使用してシステムの状態を維持します。また、McAfee Application Controlでは、ホワイトリストに登録されたアプリケーションをMicrosoft Windows（32ビット/64ビット）に対するメモリーバッファー オーバーフロー攻撃から保護します。

高度に実行を制御する

保護機能の強化のために、McAfee Application Controlにより、ファイル名、プロセス名、親機能のプロセス名、コマンドラインパラメータ、ユーザ名に基づいたルールを設定することができます。高度な実行の制御を利用して、ファイルの入出力(I/O)、システムインタープリター向け対話モードのブロックなどの攻撃を阻止し、システムツールによる搾取を防ぐことができます。さらに、ポリシーを作成するためにより強力で、信頼性の高いSHA-256アルゴリズムが取得できます。

McAfee ePolicy Orchestrator Software: 一元管理

McAfee ePOは様々な管理機能を搭載し、セキュリティ対策を一元管理します。また、企業全体のセキュリティをきめ細かく監視します。この実績豊富なプラットフォームには、McAfee Application Control、McAfee Host Intrusion Prevention、マルウェア対策などのマカフィー セキュリティ製品が統合されています。McAfee Application Controlのインストールと更新はMicrosoft System Centerから簡単に実行できます。

監視モードでの監視

監視モードを使用すると、ホワイトリストをロックせずに、動的なデスクトップ環境のポリシーを検出できます。McAfee Application Controlを本稼働前の環境や早期に段階的に配備できます。McAfee Application Controlを使用すると、管理者は1つのポリシー検出ページで、監視要求または自己承認要求のポリシーを定義できます。

レガシー システムと最新技術に対する投資を保護

Microsoft Windows NT、Windows 2000、Windows XPなどのサポート対象外の古いオペレーティング システムも保護する必要があります。Microsoftや他のセキュリティ ベンダーは、これらのレガシー アプリケーションに対するサポートを終了していますが、McAfee Application Controlはこれらのソフトウェアも保護します。McAfee Application Controlは、Microsoft Windows 10などの最新のオペレーティング システムにも対応しています。

次のステップ

詳細については、**http://www.mcafee.com/jp/products/application-control.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