McAfee Complete Endpoint Threat Protection

巧妙な攻撃を阻止する高度な脅威対策

主な特長

- 機械学習と動的隔離により、ゼロデイの脅威、ランサムウェア、グレーウェアを阻止します。
- アクションと分析の自動化により、問題を迅速に修復し、生産性を維持します。
- 集中管理により、管理作業を軽減し、配備を簡単に行うことができます。

組織が直面する脅威を阻止するには、高度な可視性を実現し、脅威対策のライフサイクル全体を管理できるツールが必要です。そのためには、セキュリティ担当者はより正確な情報に基づいて高度脅威の分析を行う必要があります。McAfee® Complete Endpoint Threat Protectionは、ゼロデイ脅威や巧妙な攻撃を検出・隔離する高度なセキュリティ機能を提供します。ゼロデイ攻撃や巧妙な攻撃にすぐにアクションを実行できます。コアとなるエンドポイント保護機能は、機械学習と動的隔離機能と連携し、ゼロデイ脅威をほぼリアルタイムで検出し、分類を行い、システムが感染する前にブロックします。有益なフォレンジック データとレポートを使用することで、アウトブレーク発生前に調査を行い、保護対策を強化できます。拡張性に優れたフレームワークが採用されているので、脅威状況の変化に応じて別の高度な脅威対策を簡単に追加できます。

自動化された高度な脅威対策

高度な脅威は侵入前にブロックする必要があります。McAfee Complete Endpoint Threat Protectionにはアプリケーションの動的隔離とReal Protect[1]の技術が搭載されています。アプリケーションの動的隔離は、不審な動作を検出すると、グレーウェアや不審なゼロデイ脅威を自動的に隔離します。これにより、システムへの感染とユーザーへの被害を未然に防ぐことができます。Real Protectは、機械学習を使用して脅威の調査と分類を行います。これにより、類似した脅威の検出時にアクションを自動的に実行できます。

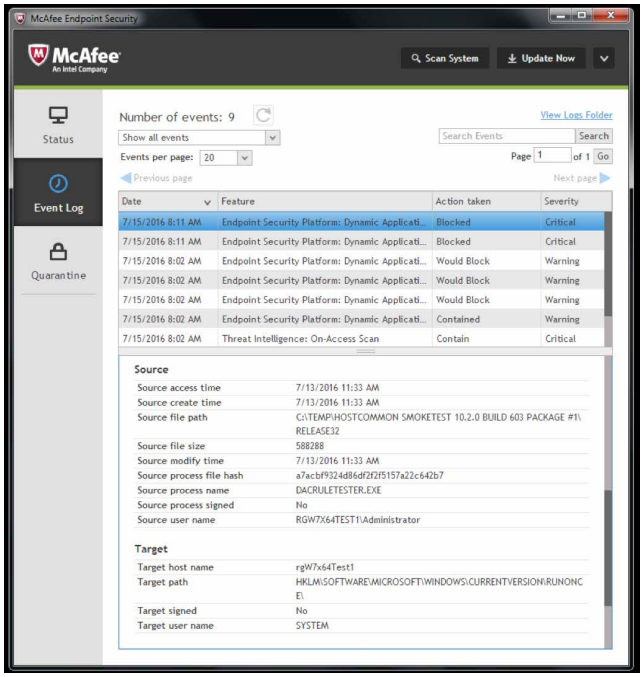

図1. アプリケーションの動的隔離が重大度に応じて脅威をブロックし、封じ込める。

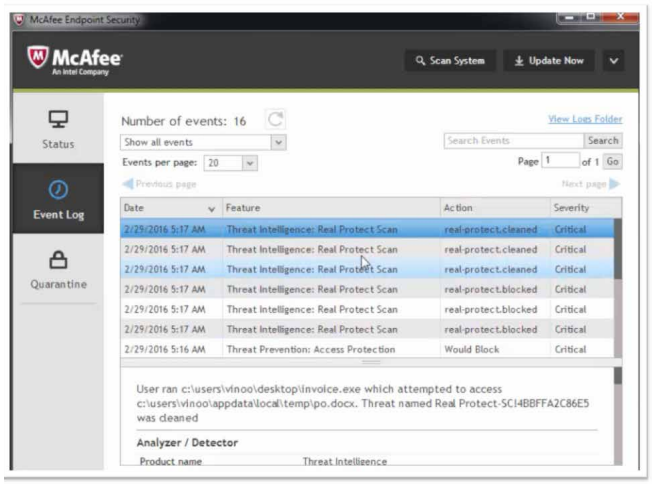

図2. Real Protectは、機械学習を使用してゼロデイ マルウェアをリアルタイムで検出する。このような脅威はシグネチャベースのスキャンで検出されないことが多い。

複雑性の解消

複雑さは効率の敵です。インターフェースや管理コンソールが異なる単体製品をいくつも管理する必要はありません。McAfee Complete Endpoint Threat Protectionは、McAfee® ePolicy Orchestrator®（McAfee ePO™）で管理します。これにより、1つの画面ですべてを管理できるので、配備時間を短縮し、管理作業の負担を軽減できます。環境内で複数のオペレーティング システムが実行されている場合でも、Microsoft Windows、Apple Macintosh、Linuxシステムに適用できるクロスプラットホーム ポリシーを使用できます。

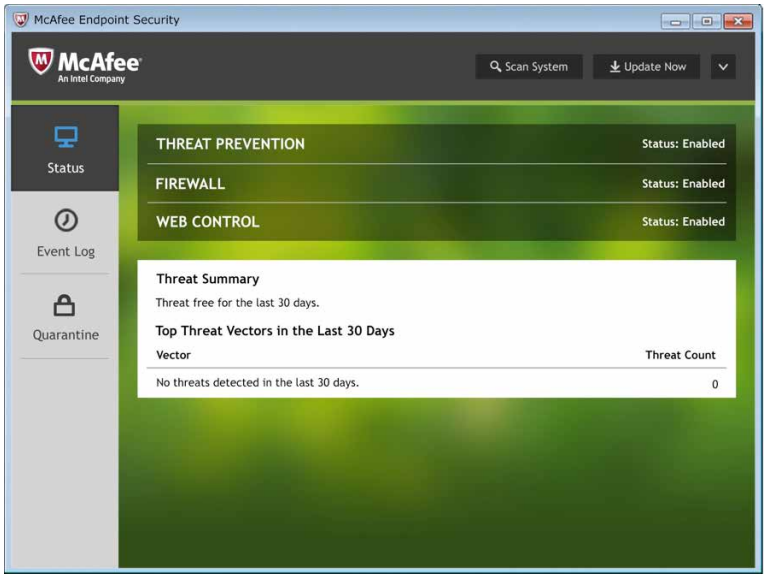

図3. 管理者にもユーザーにも分かりやすいユーザー インターフェース

現在だけでなく将来にも対応した柔軟なフレームワーク

McAfee Complete Endpoint Threat Protectionでは、協調型のフレームワークが採用され、複数の保護技術がリアルタイムで連携します。これにより、脅威分析を強化するだけでなく、収集されたフォレンジック データを他の保護機能と共有し、インテリジェントな対応が可能になります。コアとなるエンドポイント保護機能が、共通の通信レイヤーを使用して高度な脅威対策に接続し、初めて検出した脅威を的確に識別します。

このアプローチでは、配備も柔軟に行うことができます。購入時にすべての機能をインストールし、後で設定する機能を決めることもできます。また、ポリシーを変更することで、機能を簡単に有効にすることができます。

弊社のフレームワークは、新しい技術を追加できるアーキテクチャを採用しているので、必要に応じて保護機能の拡張が可能です。

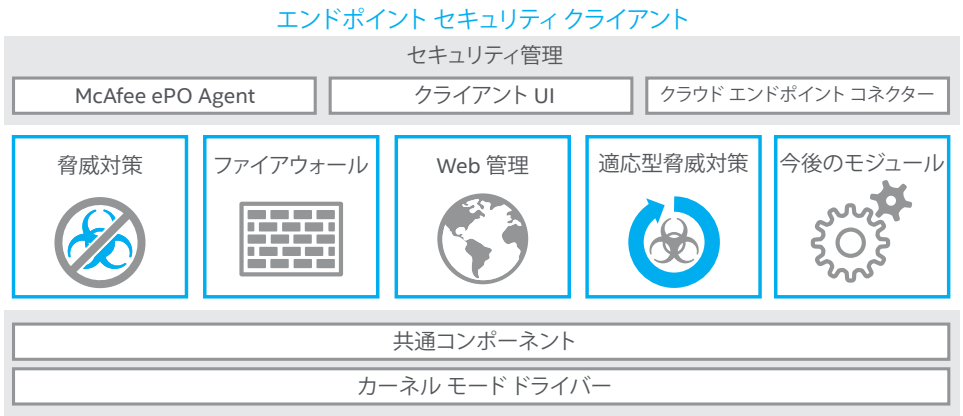

図4. McAfee エンドポイント セキュリティ クライアント フレームワーク

対応プラットフォーム

- Microsoft Windows: 7、To Go、8、8.1、10、10 November、10 Anniversary
- Mac OS X 10.5以降
- Linux 32/64ビット プラットフォーム: RHEL、SUSE、CentOS、OEL、Amazon Linux、Ubuntuの最新バージョン

サーバー:

- 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

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

コンポーネント	利点	顧客のメリット	差別化
アプリケーションの動的隔離	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。	• エンド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。 • ネットワークに対する攻撃を未然に防ぎ、脅威を隔離します。	• 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できます。
Real Protect	機械学習による動作分類を行い、ゼロデイの脅威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。	• 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。
脅威対策	多層型の保護対策でマルウェアの検出、封じ込め、修復を迅速に行う包括的なセキュリティです。	• ヒューリスティック、動作分析、オンアクセス スキャンにより、既知または未知のマルウェアも検出します。 • ポリシーと配備を単純化し、Windows、Mac、Linuxが稼働するデスクトップやサーバーを保護します。 • 信頼されたプロセスにはスキャンを実行せず、不審な対象に優先度を設定します。これにより、パフォーマンスが最適化されます。	Webの保護やファイアウォールと連携して分析能力を強化し、脅威対策を実行する多層型のマルウェア対策です。
統合ファイアウォール	ボットネット、分散型サービス拒否（DDoS）攻撃、信頼されていない実行ファイル、高度な持続型脅威、危険なWeb接続からエンドポイントを保護します。	• ポリシーを施行してユーザーを保護し、生産性を維持します。 • 不要な受信接続をブロックし、送信要求を制御することで帯域幅を保護します。 • 信頼されたネットワークや実行ファイル、危険なファイルや接続をユーザーに通知します。	社内ネットワークに接続していないノートPCやデスクトップも、アプリケーション ポリシーと位置情報ポリシーで保護します。
Web管理	Web保護とフィルタリングにより、エンドポイントでのWeb閲覧を保護します。	• 不正なサイトに移動する前に警告を表示するので、リスクを軽減し、コンプライアンスを遵守できます。 • Webサイトへのアクセスを許可またはブロックすることで、脅威を阻止し、生産性を維持できます。 • 危険なダウンロードは、ダウンロードが開始する前にブロックします。	Windows、Mac、複数のブラウザーを保護します。
McAfee Data Exchange Layer	セキュリティを統合し、Intel Security製品や他社製品間の通信を簡素化します。	• 統合により、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。	セキュリティ製品間で最も重要な脅威情報を共有できます。
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。 • 可視化と柔軟性を強化し、安心してアクションを実行できるようにします。 • カスタマイズ可能なポリシー施行で1つのエージェントを迅速に配備し、管理できます。 • 分かりやすいダッシュボードとレポートを使用して、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。また、コストの削減も可能です。 • 業界で広く知られた優れたインターフェースを利用できます。 • ドラッグアンドドロップに対応したダッシュボードでセキュリティ エコシステムを管理できます。 • オープン プラットフォームを利用しているので、新しいセキュリティ技術をすぐに導入できます。

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

1. このソリューションでは、米国に存在するデータセンターを利用して、ファイル レピュテーションを確認したり、不審なファイルに関連するデータを保存しています。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。アプリケーションの動的隔離と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。