McAfee MVISION Endpoint

Windowsデスクトップとサーバーを保護する高度なエンドポイント セキュリティ

フル機能のエンドポイント セキュリティ プラットフォーム (EPP) よりもシンプルで手ごろな価格の代替策として、Microsoft Windows Defender のようなネイティブのセキュリティが利用されています。Windows Defender は必要不可欠な基本的保護機能は提供しますが、最新のファイルレス及びゼロデイ マルウェアの脅威に十分に対抗するためには、機械学習のような最新の対策が必要になります。複数のコンソールを利用することなく、Windowsデスクトップ/サーバー環境にすでに組み込まれているセキュリティ機能[1]を管理し、強化できるかどうかが成功のカギになります。McAfee® MVISION Insights[2] は、攻撃が広がる前に先を見越したセキュリティ分析や対策を提供して、組織のセキュリティ体制を強化します。

セキュリティを強化すると複雑に

これらのツールは通常個別に管理されるため、セキュリティ チームは、セキュリティ保護を強化すると運用が複雑になるというジレンマに陥ります。これはまた大抵の場合、財政的及び運用上の節約もできないということを意味します。

より良い選択: 高度な保護機能と統合管理

McAfee® MVISION Endpoint を用いると、有効性と効率性の両方を手に入れることができるのでジレンマに悩む必要はありません。ファイル、ファイルレス、及び行動機械学習分析で高度な脅威検出ができ、また環境内のすべてのエンドポイントを集中管理できるようになります。複雑なワークフローは不要です。1つのコンソールでWindows Defenderウイルス対策、Defender Exploit Guard、Windowsファイアウォール、McAfeeのセキュリティ、Mac、Linuxシステムを管理できます。共同管理とポリシーの統合により、入力作業の手間が省けるだけでなく、エンドポイント環境の可視化も向上します。

脅威対策と防止策を最大化

MVISION Endpoint は、多くの検出機能と修正機能を提供して、常に最新のネイティブのセキュリティ コントロールを補完します。機械学習、認証情報窃盗のモニタリング、修復のロールバック機能により、Windowsデスクトップ/サーバーのオペレーティング システム (OS) に組み込まれている基本的なセキュリティ機能を大幅に強化し、高度なゼロデイ脅威に効果的な対応が可能になります。このアプローチをすれば、ネイティブのセキュリティ技術に投資するかサードパーティ技術に投資するかという選択に悩むことなく、両方の良い部分を活用することができます。組織のセキュリティ体制を更新して脅威対策を強化し、攻撃が始まる前に、特に優先される潜在的な脅威に対処する必要があります。

主な特長

- **高度な脅威に対する高度な防御:** 機械学習、認証情報の窃盗防止、修復のロールバックがWindowsデスクトップ/サーバーシステムの基本的なセキュリティ機能を補完します。
- **複雑化を回避:** McAfeeのテクノロジー、Windows Defenderウイルス対策のポリシー、Defender Exploit Guard、Windowsファイアウォールの設定を1つのポリシーとコンソールで管理
- **MVISION Insights:** 最新の実用的なセキュリティ インテリジェンス ソリューションで、標的となるセクターや地域に基づき優先度が高いと判断される潜在的な脅威キャンペーンに即時に対応。保護が不十分なエンドポイントを予測して、脅威の検出を向上させる対処法を提供します。

McAfee へアクセス

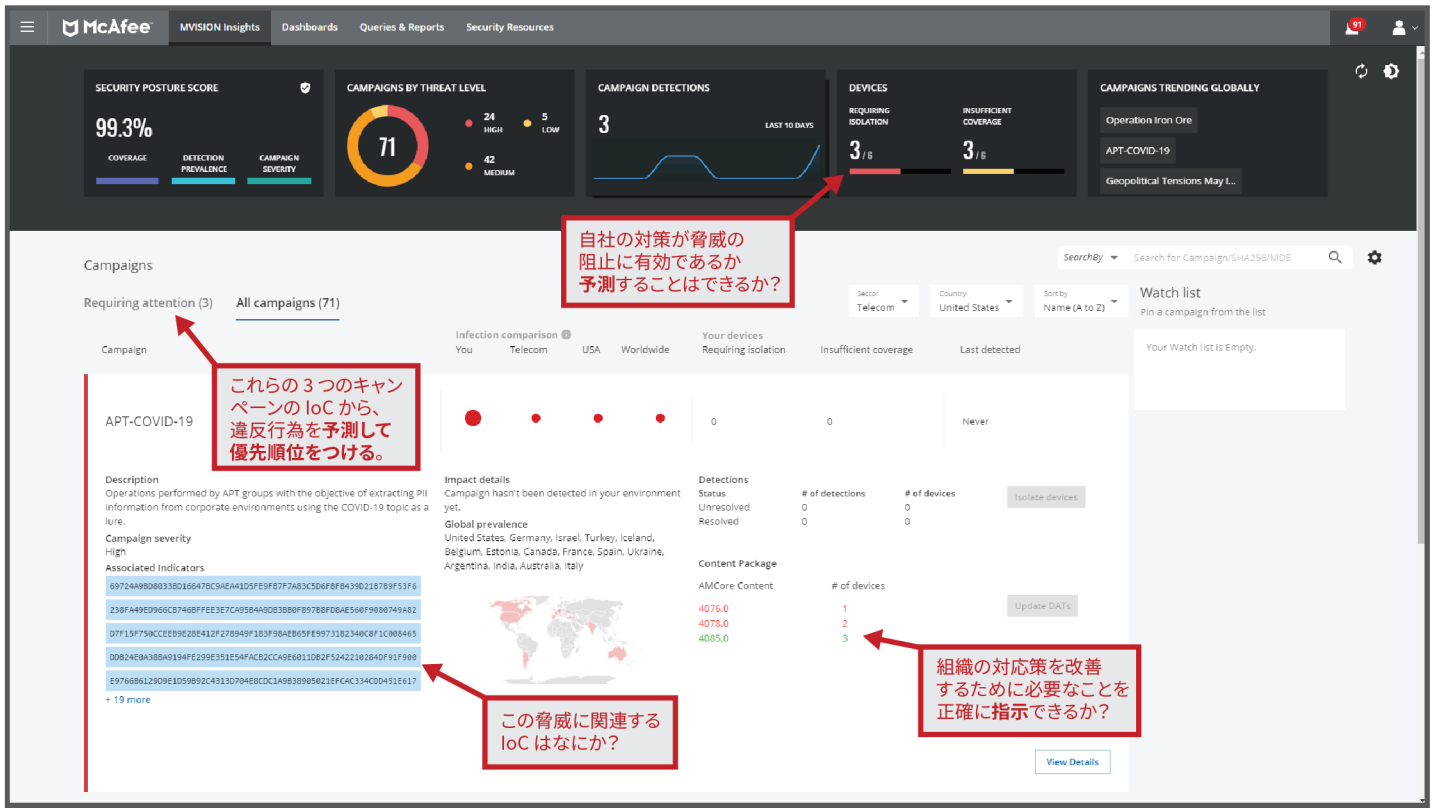

図1. MVISION Insights は、統一的なダッシュボードを使って重要な事項に対する回答を示し、先を見越したサイバー セキュリティ対策を提供します。

リカバリー時間

McAfee の機械学習技術を使うと、シグネチャ ベースよりも検出率が高くなり、また競合ソリューションよりも誤検出率が低くなります。このため管理者は誤検出の確認に時間をとられることなく、真の脅威への対応にフォーカスすることができます。

MVISION Endpoint はまた、不審なプロセスによって影響を受けたファイルを監視し元の状態に戻すことができます。その他の不正ファイルやプロセスの除去も可能です。修復やリカバリーのダウンタイムがなくなるので、ユーザーは生産性を維持できます。そして不正アクセスされたエンドポイントを復元したりイメージングを再度行ったりといった作業がなくなるため、管理者は組織の生産性を高める仕事に時間を費やすことができます。

Windows 10、Windows Server 2016、Windows Server 2019システムの基本的なセキュリティ機能を補完し、強化する統合セキュリティ

短時間での利用開始が可能

- 組織にとって重要な意味を持つ脅威をすぐに確認して行動に移すことができます。
- すぐに使えるポリシーをWindows Defenderウイルス対策に適用し、Defender Exploit Guardで最も重要なルールを管理。ベストプラクティス ルールの設定をWindowsファイアウォールに適用。
- 既存のマカフィーの管理機能を利用するか、SaaS ベースのコンソールを使って短時間で配備完了
- Story Graph により、脅威とそれに対するアクションを視覚的に確認できます。これにより、エンドポイントを保護し、将来の攻撃に備えることができます。
- クライアント サイズが小さいため、軽くて速いダウンロード

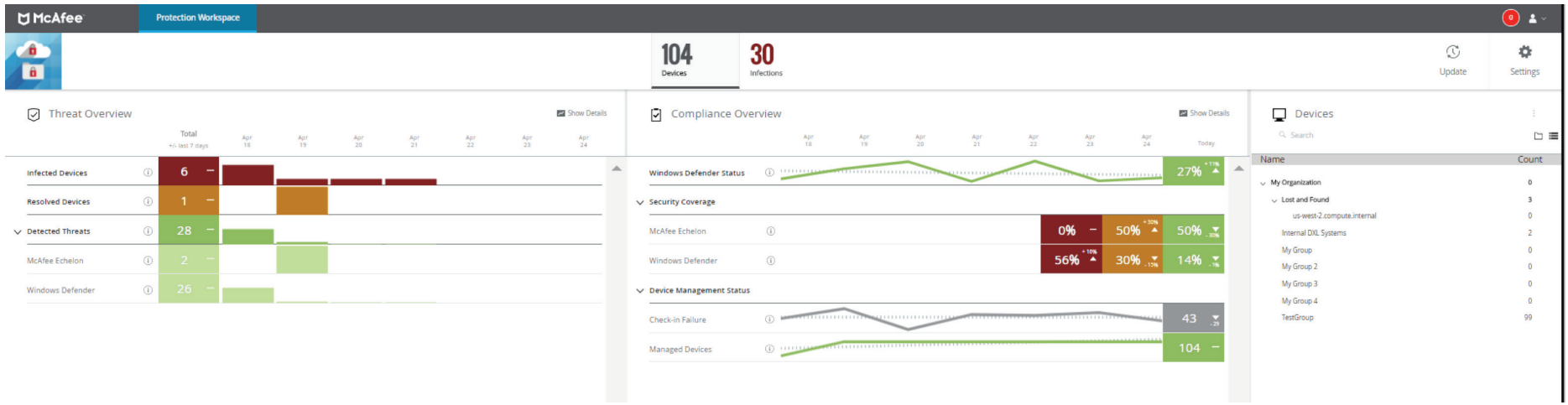

図2. 脅威保護のワークスペースでは、McAfee と Microsoft の両方の技術を使って脅威とコンプライアンスを確認できます。

可視性を高める

MVISION　Endpointは、1つのコンソールで集中管理されます。環境全体を可視化し、脅威とコンプライアンスの状態を把握できます。また、BitLockerによる暗号化状態も確認できます。何がどこで何をして脅威イベントが発生したのかという点と点をつなげるために、あちこちのコンソールを見る必要はありません。使いやすいダッシュボードと自分で設定できるアラートで、最も重要なデータを簡単に入手できます。

Story Graph 機能により、調査作業をより効率的に行い、エンドポイントのセキュリティを強化できます。脅威イベントの元になったアクションの追跡情報を使用してアクションを分析し、脅威の原因を突き止めることができます。

管理の柔軟性

MVISION Endpoint には以下の選択肢があります:

- **純粋なSaaS管理:** 複数のテナント、グローバル規模、McAfee が維持運用
  - メリット: いつでもどこでも管理コンソールにアクセスでき、自動アップデートや管理サービスで TCO (総所有コスト) を削減できます。
- **仮想配備:** Amazon Web Services (AWS) 環境での配備では、1時間以内にすべてが利用可能になります。
  - メリット: すでに行っている仮想環境への投資を活用して、配備費用やメンテナンス費用を抑えます。コントロールは自由にカスタマイズできます。

- **オンプレミス配備:** オンサイトのサーバーに管理ソフトウェアをローカルでインストールします。
  - メリット: 既存の環境を使いながら、複数のMcAfeeの技術を集中管理できます。

パフォーマンスを重視したデザイン

MVISION Endpoint の多くの機能はクラウド ベースのサービスのため、システム占有領域は非常に小さく、また軽くできています。そのため短時間で利用を開始できます。クライアント ファイルのサイズも小さいのでダウンロードにも時間がかからず、ネットワークへの負荷も少なく済みます。

一度インストールされるとアップデート作業は必要ありません。自動でアップデートがインストールされるので管理者が作業を行う必要もありません。

常時稼働ではなく必要に応じてコンピューターとネットワークの使用量を変化させる機能があるため、エンドポイントとユーザーへの影響は最小限にとどめられます。

環境全体の統一プラットフォーム

BYOD、モバイル、IoT機器が増加し、保護するオペレーティング システムやデバイスの種類が多様化しています。この煩雑さを解消するため、McAfeeは革新的なMVISIONテクノロジーを導入しました。これにより、管理作業を省力化し、Windowsセキュリティ、モバイル、IoT機器のセキュリティを強化するという戦略的なビジョンが実現されます。

McAfee MVISIONテクノロジーは、デバイスのセキュリティにクラウド ファーストのアプローチを採用しています。セキュリティ担当者は、McAfee、サードパーティ、ネイティブのオペレーティング システム (OS) を1つのコンソールから管理できます。

McAfee Device Security ポートフォリオにより、デスクトップ、ラップトップ、タブレット、モバイル、物理/仮想サーバー、クラウド ワークロード、IoTを網羅する保護対策を利用できます。

ビジネス上のメリット

- すべてのデバイスを集中管理
- 先進、ファイル、ファイルレス、行動機械学習保護
- Mac、Linux、IoT、モバイル デバイスの保護
- サイバーセキュリティ対策を攻撃前にシフト レフト (早期対応に) する
- TCOの削減とワークフローの合理化

McAfeeを選ぶ理由

- より多くを、より速く、より少ない作業で実現
- ネイティブ コントロールのための統合管理とチューニング済みの先進的保護機能を提供する業界で唯一のベンダー
- デバイス環境全体への可視性の提供
- 統合による、大規模でオープンなエコシステム
- 独自のプロアクティブなエンドポイント セキュリティ対策

詳細を見る

詳細については、下記のサイトをご覧ください。**www.mcafee.com/enterprise/ja-jp/products/mvision-endpoint.html**.

1. Microsoft Windows 10、Microsoft Windows Server 2016、Microsoft Windows Server 2019システム
2. このドキュメントには、製品、サービス、または開発中のプロセスに関する情報が含まれています。ドキュメントに記載のある特徴はシステム構成に依存します。機能を十分に活用するため、対応するハードウェア、ソフトウェア、サービスの利用が必要になる場合があります。ここに記載されている情報は、McAfee の判断で予告なしに変更される可能性があります。最新の予測、スケジュール、仕様、ロードマップを入手するには、お近くの McAfee 窓口にお問い合わせください。

ご説明したコスト及び時間削減のシナリオでは、これらのMcAfee製品が最適化された設定及び配備によって、将来のコストにどう影響を与え、また時間とコストをどう削減できる可能性があるかという例をお見せすることを目的としています。状況及び結果は設定や配備状況によって異なることがあります。McAfeeは時間やコスト削減を保証しません。

マカフィー株式会社　www.mcafee.com/jp
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