

McAfee MVISION Endpoint

Microsoft 環境向けの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、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。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。Windows 10 に内蔵されているセキュリティを、複数のコンソールで運用を複雑にすることなく、活用、強化、及び管理することが成功へのカギとなります。

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。また、一貫した集中コンソールで Windows Defender、McAfee のセキュリティ、そして Mac や Linux システムのポリシー管理ができるため、

ワークフローが複雑になることもありません。共通管理により重複入力の手間が省かれ、またエンドポイント環境の可視性も高くなります。

脅威対策を最大化

McAfee 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、認証情報窃盗監視、そしてロールバック修正で、Windows 10 OS に内蔵される基本的なセキュリティを大幅に強化し、高度なゼロデイ攻撃に効果的に対抗します。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。

主な特長

- 高度な脅威に対する高度な防御: 機械学習、認証情報窃盗防止、そしてロールバック修正で、Windows 10 の基本セキュリティを補完
- 複雑化を回避: Windows Defender と McAfee のセキュリティのポリシー管理の集中化

Windows 10 の基本セキュリティを活用し、強化し、管理する統合的防御

McAfee へアクセス



データシート

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。

McAfee 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。

可視性を高める

McAfee MVISION Endpoint は、脅威とコンプライアンスという両方の観点から環境を可視化する単一のインターフェースを使って管理できます。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。

管理の柔軟性

McAfee 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
 - ー 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。
 - ー 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。
 - ー 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。

短時間での利用開始が可能

- Defender 環境には既定のポリシーを適用
- 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
- クライアント サイズが小さいため、軽く速いダウンロード

データシート

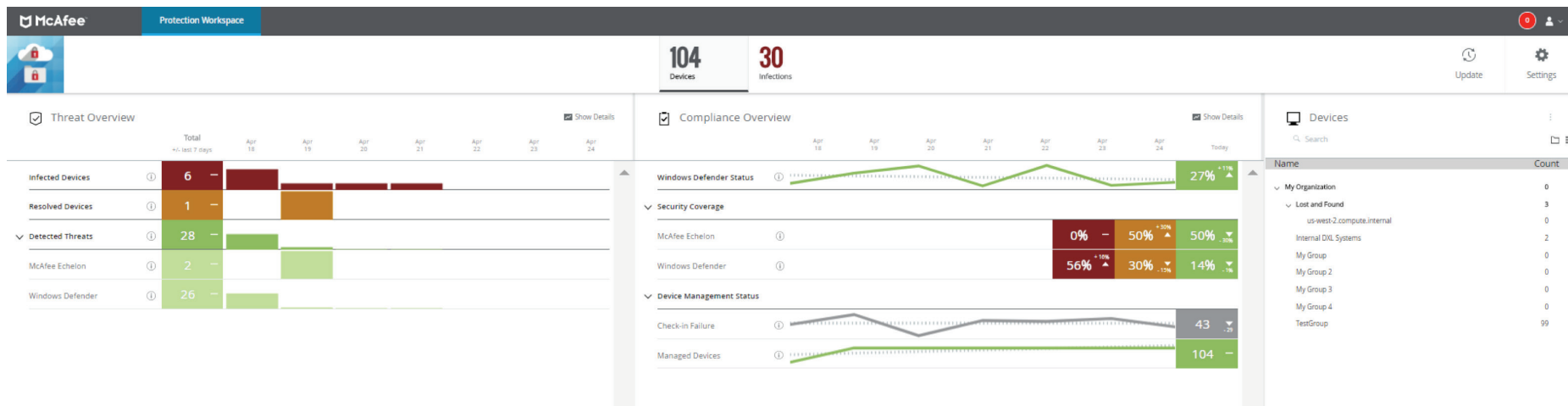


図 1 脅威保護のワークスペースでは、McAfeeとMicrosoftの両方の技術を使って脅威とコンプライアンスを確認できます。

パフォーマンスを重視したデザイン

McAfee 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。

McAfee MVISION の一部

環境全体の統一プラットフォーム

BYOD（個人所有機器の持ち込み）、モバイル、IoT デバイスの増加に伴い、多くの組織ではこれまでとは別の種類のオペレーティングシステムやデバイスへの保護が必要になってきています。ますます高まる複雑性に対応するため、McAfee は MVISION の提供を始めました。MVISION は新しい戦略的方针及び革新的なセキュリティ技術ポートフォリオで、管理を簡略化し、Windows セキュリティを強化し、機械学習を活用し、モバイルのセキュリティも網羅します。

McAfee MVISION 技術ポートフォリオでは、デバイスの保護にクラウドファーストのアプローチをとります。セキュリティプロフェッショナルは可視性とコントロールの集中化により、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をまとめて管理できます。

McAfee MVISION を使うと、デスクトップ、ラップトップ、タブレット、モバイル、物理サーバー、仮想サーバー、クラウドワークロード、IoTなどの攻撃対象すべてを保護できます。

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
- 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

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。<https://www.mcafee.com/enterprise/ja-jp/products/mvision-endpoint.html>.



〒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
www.mcafee.com/jp

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。

McAfee、マカフィーおよびMcAfeeのロゴは米国法人McAfee, LLCまたはその米国及びそれ以外の国の子会社の商標又は登録商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2018 McAfee, LLC.4071_0718
2018年7月