技術概要 : McAfee MVISION Endpoint と MVISION ePO

進化を続ける脅威、セキュリティ人材の不足、管理ツールの増加などが、McAfee® Device Security ポートフォリオ、とりわけ最新の革新的な McAfee® MVISION 製品を推進する力となっています。エンドポイントやサーバー、モバイル、クラウドそして IoT デバイスに広がるソリューションによって、McAfee は、お客様のセキュリティチームのストレスを軽減しながら、同時により効果的な業務の実現を目指します。この文書では、以下の 2 つの McAfee MVISION ソリューションの技術概要を紹介しています : McAfee® MVISION ePO ™ および McAfee® MVISION Endpoint。

McAfeeとつながる

McAfee MVISION ePolicy Orchestrator (MVISION ePO)

McAfee MVISION ePolicy Orchestrator® (MVISION ePO) は、クラウドベースのシステムで、1 つのコンソールからデジタル領域全体に迅速に配備され、監視、管理を行います。自動化ワークフローや優先順位に従ったリスク評価によって、トリアージ、調査およびセキュリティインシデントへの対応にかかる時間とタスクを軽減します。

導入とセットアップ

MVISION ePO は McAfee がホスティングする Software-as-a-Service (SaaS) 管理ツールで、常に最新の状態に保たれています。McAfee のマルチテナントホステッドバージョンのセットアップには数分しかかかりません。ブラウザーを開いて、アカウントの作成、ネットワークの構成を行うだけです。裏にあるインフラを管理する必要はありません。セキュリティに集中するだけです。さまざまなシナリオが組み込まれていることから開始から完全な形で動作する一方で、豊富なカスタマイズ機能によって独自の環境に合わせた微調整も可能です。このアーキテクチャは 1 つのサーバーで何十万台ものデバイスや複雑な環境へと拡大できます。

ダッシュボードとレポートのカスタマイズ

「脅威対策ワークスペース」と呼ばれる操作が容易なダッシュボードを使うと、数表やアラートリストよりもかなり高速に視覚化の処理を行うことができます。また、簡略化されたワークフローにより脅威の監視、コンプライアンス情報の表示、デバイスの管理を行うことができます。

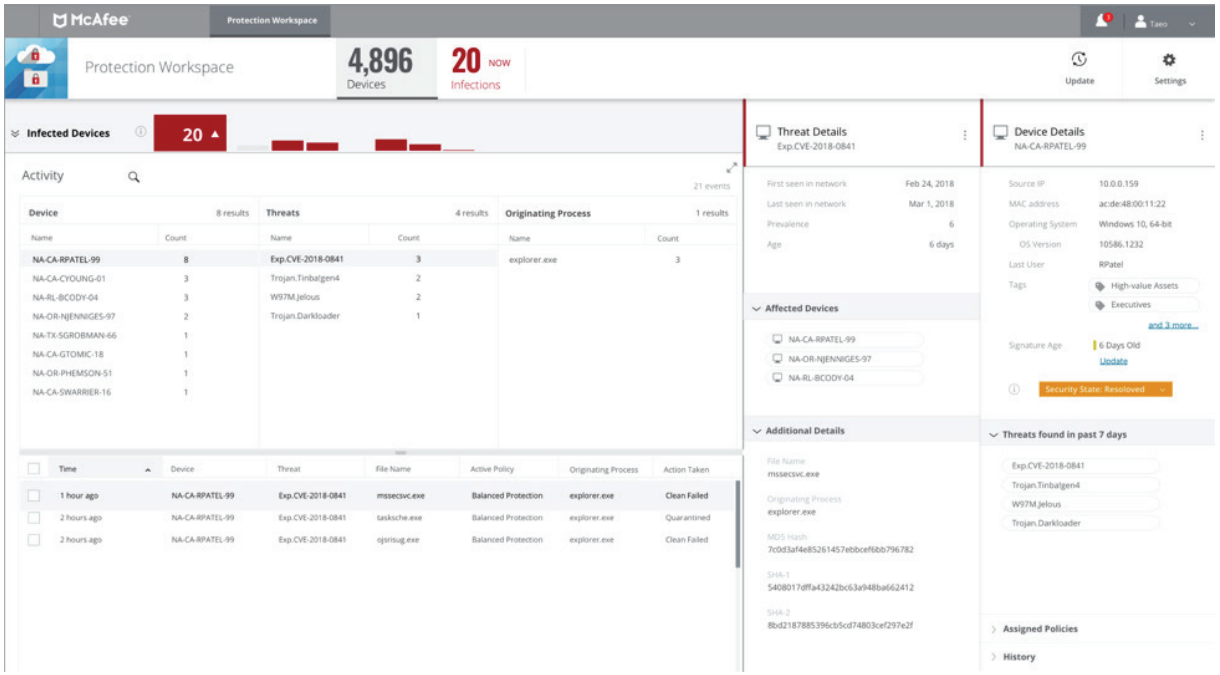

図 1 MVISION ePO には事前に定義され、カスタマイズ可能なダッシュボード、統合ビュー、脅威データの優先順位が含まれます。

MVISION ePO には、事前定義されカスタマイズ可能で強力なダッシュボードとレポートも含まれており、お気に入りのデータを明確に表示しながら環境を監視し続けることができます。直観的にカラーコード化されたグラフと図によって、潜在的な脅威の調査と修復をすばやく行うことができます。また、インストールされているソフトウェアバージョンまたはマルウェアスキャンのようなコンプライアンス指標やベストプラクティスを問い合わせることができ、コンプライアンス要件やヒストリカルトレンドに関する詳細なレポートも入手できます。MVISION ePO によってグループ、サブネットまたはデバイスにすばやくナビゲートできるようになり、詳細なログを確認して、ただちに修正処理を行うことができます。

MVISION Endpoint

Microsoft Windows 10 向けの高度な防御

McAfee MVISION Endpoint は、ローカルおよびクラウドベースの技術を追加して、高度なゼロデイ脅威を分析して対処することで Windows 10 システムのネイティブなセキュリティ機能と連動します。McAfee 技術を Microsoft Windows Defender Antivirus、Defender Exploit Guard、 および Microsoft Windows Firewall の設定に沿って管理するために軽量エージェントが使用されています。McAfee の機械学習分析では Windows 10、Server 2016 および Server 2019 の基本的なマルウェア検出機能をすり抜けた脅威を検出します。他の方法では見逃される可能性のあるファイルベース、ファイルレスおよびゼロデイ脅威がエンドポイントを侵害するのを防止します。

データ盗難とシステムロールバック

残念ながら、お客様のユーザーがフィッシングやソーシャルエンジニアリングの犠牲にならないとは保証できません。MVISION Endpoint には、認証情報の盗難監視やロールバック修復が含まれており、違反を防いだり、ユーザーの生産性を維持したりするのに役立ち、さらにはサポートチケットや感染したマシンの再イメージ化に費やす時間を減らすことができるようになります。ランサムウェアに感染して失われる可能性のあったファイルも復元できます。

統一ポリシーと管理

Windows Defender Antivirus、Defender Exploit Guard、Windows Firewall および MVISION Endpoint のポリシーを 1 つの領域で定義することで作業の重複を回避します。すぐ使用できるベストプラクティスルールによって、お客様の環境に最適な Windows Firewall ルールを適用し、管理することが容易になります。また、24 時間以内に Windows Defender Firewall ルールによってブロックされたイベント数や MVISION ePO のエンドポイントからのコンプライアンスデータについてビジビリティも取得できます。

脅威やそれに対するアクションについて迅速に視覚化したりインサイトを取得したりするもうひとつの方法は「ストーリーグラフ」機能です。これは、脅威イベントの検出につながったアクションについての追跡情報を提供するもので、ユーザーがこのアクションを確認したり、脅威の原因をより良く探ることができるようになります。

配備オプション

MVISION Endpoint の配備と管理は、ローカルにインストールされた SaaS (MVISION ePO) または Amazon Web Services (AWS) 上に配備された McAfee ePolicy Orchestrator ソフトウェアを使用して行われます。自動化されたタスクにより、エンドポイントソフトウェアが個別に選択されたシステムまたはシステムグループに配備されます。自動更新機能により、ユーザーの介入や管理オーバーヘッドを生じることなくソフトウェアクライアントを最新の状態に維持します。

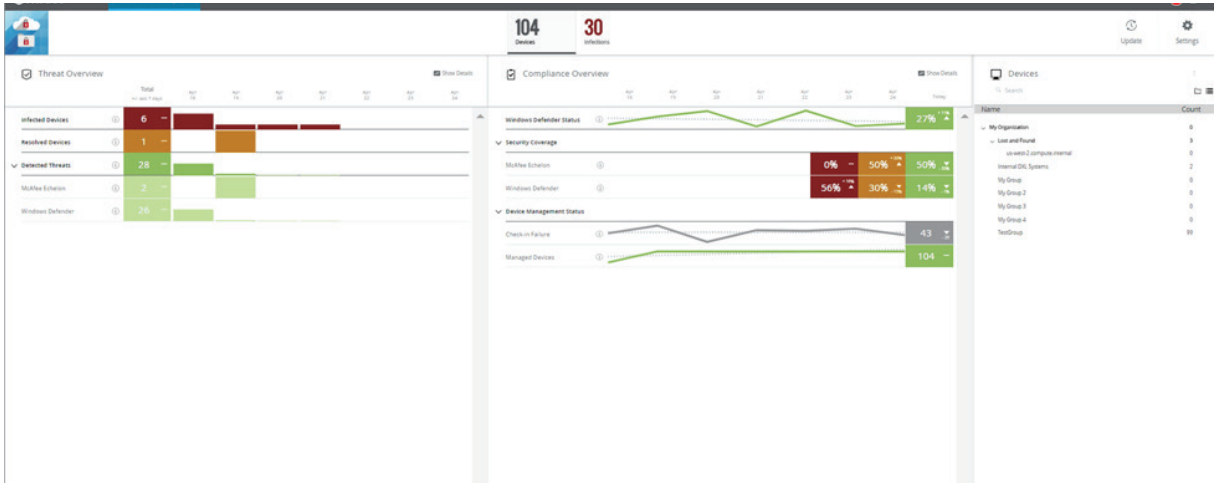

図 2 1 つのエリアで McAfee と Microsoft の技術についての脅威とコンプライアンス状態をご覧いただけます。

MVISION および McAfee Device Security の提供

脅威が複雑だからといって、セキュリティも複雑になる必要はありません

攻撃者はさまざまな攻撃手法を使って、複数のデバイスタイプを標的にします。そして、デジタル領域全体にわたって、さまざまな戦術を使って組織的攻撃を仕掛け、足がかりを築いて攻撃を持続し、保護されていない資産を利用するために攻撃の幅を広げます。McAfee Device Security では、以下を提供することにより、寄せ集めの製品や分散されたコンソールから発生する複雑さを避けながら、このような攻撃に対する効果的な防御を構築するために必要な統合管理、ビジビリティおよび多層化施策などを提供します。

- McAfee ePO ソフトウェア（SaaS、クラウドおよびオンプレミスのオプション含む）のシンプルな単一コンソールによる運用オーバーヘッドの削減
- ファイルレス攻撃やマルウェアベースの攻撃の両方を阻止するためのスマートで階層化された対策を講じ、さまざまな脅威に対して保護を強化
- フルスタックの防御または高度な対策オーバーレイをエンドポイントのネイティブコントロールに柔軟に配備することで最新のデバイスやレガシーデバイスの両方を保護する単一のソリューション
- McAfee、ネイティブコントロールおよびポリシーの統合による管理の簡素化
- 従来のエンドポイント、モバイルおよび固定機能システムなど複数のデバイスタイプを包括的に保護

McAfee MVISION 製品の詳細については、
www.mcafee.com/MVISION をご覧ください。

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