McAfee ePolicy Orchestrator

セキュリティ プロフェッショナルにインスピレーションと力を与える

セキュリティ管理では、外部脅威の十分な可視性も得られない中で、様々なツールやデータをやりくりして状況を乗り越えるという難しい作業が求められます。このため、ツール間のギャップをついて多くの被害を出すチャンスを攻撃者に与えてしまっています。サイバーセキュリティの人材は限られているので、複雑なサイバーセキュリティ環境を簡単に構築できる方法が必要です。事後対応ではなく、攻撃の先を見越して事前に対応する必要があります。

組織では、あらゆる種類のデバイスへの脅威に迅速に対応して被害を最小限にとどめ、セキュリティが効果をあげている証拠を経営幹部に示さなければなりません。オンプレミスでもクラウド ベース (SaaS または IaaS の 2 つのモデルから選択) でも利用できる McAfee® ePolicy Orchestrator® (McAfee ePO™) 管理プラットフォームは、時間のかかる作業の効率を上げて人的エラーの回避を可能にします。またセキュリティ管理の担当者は、プロアクティブに、迅速に、高い実効性をもって対策を講じることができるようになります。McAfee ePO コンソール の独自の機能の 1 つに McAfee® MVISION Insights があります。これは組織が攻撃を受ける前にプロアクティブに脅威の優先度を決定し、組織が講じた対策で攻撃を阻止することができるかを予測し、脅威に対処するために何をすべきかを具体的に提示することのできる初めてのテクノロジです。

セキュリティの基礎

必要不可欠なものから見ていきましょう。セキュリティ アーキテクチャの中核となるのは、デバイスとシステムの健全性を監視しコントロールする機能です。Center for Internet Security (CIS) Controls and Benchmarks や、米国標準技術局 (NIST) の SP 800-53 セキュリティ及びプライバシー コントロールのような業界標準は、必須要件としてセキュリティ インフラストラクチャの監視とコントロールを挙げています。McAfee ePO コンソールを使うと、必要不可欠な可視性を入手でき、またポリシーの設定と自動執行が可能になります。これにより会社全体での健全なセキュリティ ポスチャが確保できます。単一コンソールから全社へのポリシー管理と執行ができるた

主な特徴

- 業界で評価の高い、作業をシンプルにする独自の統合インターフェースで集中管理 – クラウド及びオンプレミスで利用可能
- 攻撃者の一歩先を行くプロアクティブで実践的なインテリジェンス
- 自動化ワークフローで管理作業を効率化
- オープンな包括的プラットフォームで McAfee のソリューションと 150 以上のサードパーティ ソリューションを統合し、より迅速かつ正確な対応を実現
- 市場シェアの大きいデバイスの一般的なセキュリティ管理
- Windows Defender のような OS 内蔵のネイティブ コントロールを活用及び強化
- 数百のデバイスから数千のデバイスまで様々な規模に対応。デバイスからクラウドまでカバー

McAfee へアクセス

め、複数の製品を調整する複雑さが無くなります。MVISION Insights の拡張機能では、プロアクティブな強化策の提言と機能を、実践的なインテリジェンスとともに提供します。この必要不可欠なセキュリティ管理機能は、IT セキュリティ コンプライアンスの基礎となります。

シンプル化され、実績のある高度セキュリティ管理

McAfee ePO コンソールは 36,000 社以上のお客様でセキュリティの管理と、コンプライアンス プロセスの効率化と自動化を実現し、またデバイス、ネットワーク、セキュリティ オペレーションの全体的な可視性を向上させています。大企業では McAfee ePO コンソールの高度にスケーラブルなアーキテクチャを活用して、統合された一つのスクリーンから何十万ものノードを管理しています。このダッシュボード ビューでリスク管理の優先順位付けができ、デジタル領域全体のセキュリティ ポスチャのサマリーを視覚的に表示します。さらに、MVISION Insights は、組織にとって重大な外部脅威をプロアクティブに表示する独自の機能で、なすべき予防的なガイダンスを提供します。リアクティブな事後対応ではなくプロアクティブな事前対応を行うエンドポイント セキュリティを実現して、セキュリティ管理のストレスを軽減します。また、最新の脅威情報や調査結果を入手できる「セキュリティ リソース」エリアも提供されています。

管理者は特定のイベントの内容を確認するために掘り下げて調査ができます。このサマリービューを使えばレポートの作成や手持ちデータの合理化にかかる時間を削減でき、またマニュアル作業での間違いが起こる可能性も低減できます。McAfee ePO コンソールで、セキュリティ管理者のポリシー管理もシンプルになります。業界をリードする McAfee のメッセージング ファブリックである「Data Exchange Layer (DXL)」を活用してサードパーティ脅威インテリジェンスを取り込むことも、また、各種ポリシーと様々な製品との双方向の統合も可能です。これらの運用効率化でプロセスとデータ共有作業を削減し、より早く正確な対応ができるようになります。

サポート センターでは、McAfee 製品の情報に簡単にアクセスできます。お使いの環境の McAfee ePO サーバーの状態を確認することもできます。これは、オンプレミスの McAfee ePO コンソールでも、Amazon Web Services (AWS) 用の McAfee ePO コンソールでも利用可能です。McAfee ePO コンソール内からサポート情報や製品情報をプロアクティブに受信し、McAfee のコンテンツ リポジトリを検索できます。また、ベストプラクティスや操作方法などの情報も確認できます。ご使用の McAfee ePO インフラストラクチャの状態も簡単に管理できます。システムの状態をすばやく取得し、推奨改善手順も確認できます。

アナリストは、顧客が McAfee を採用し使い続けている理由は McAfee ePO ソフトウェアにあると説明しています。

統合プラットフォームの利点
統合プラットフォームを使用している組織のほうが、保護能力が高く、迅速な対応を行っています。

統合プラットフォームを採用している組織
- 78% の組織で、前年のセキュリティ侵害数が 5 件以下。
- 80% の組織で、脅威を 8 時間以内に検出。

統合プラットフォームを採用していない組織
- 前年のセキュリティ侵害数が 5 件以下だったのはわずか55%。
- 脅威を 8 時間以内に検出したのはわずか 54%。

(出典: 2016年 Penn Schoen Berland)

オープン プラットフォームの効果で不規則性を排除

ESGの調査によると、大量に発生する新しい脅威やデバイスを管理するため、40% の組織が 10～25 のツールを使用し、30% の組織が 26～50 のツールを使用しています。多くの製品を使用すると複雑性が増すため、統合管理 (インストールからレポーティングまで) が可能になれば運用上の見返りは何倍にもなることが期待できます。半数以上の組織は、セキュリティ ツールの統合により効率性が 20% 向上すると推定しています (出典：2018年 MSI リサーチ)。

McAfee はオープン プラットフォームでのセキュリティ管理の統合で、これらの要件に対応します。これにより様々な資産を保護し、脅威インテリジェンスをサポートし、オープンソースのデータを管理し、サードパーティ製品を統合できます。McAfee はコンプライアンスと様々なセキュリティ製品の管理を集中コントロールします。これによりアナリストは、複数の製品から瞬時に重要なデータを見つけ、必要なアクションをとることができます。また、McAfee ePOを使用すると、既存の資産と次世代の技術を1つのフレームワークに統合することができます。

オープン プラットフォームでは様々な統合アプローチ (スクリプティング、アプリケーション プログラミング インターフェース (API)、非API、オープンソース DXL メッセージング ファブリックを使った最小労力のアプローチ) から、ニーズに合った、またカスタマイズやサービスが少なくて済むベストなものを選択できます。当社は McAfee® Security Innovation Alliance プログラムを通じて、相互運用可能なセキュリティ製品の開発を促進し、これらの製品を複雑な顧客環境で簡単に統合できるように支援しています。これにより、既存の投資が無駄にならない、真に統合されたセキュリティ エコシステムを提供することができます。McAfee Security Innovation Alliance プログラムには、現在 150 社以上のパートナーが参加しています。

さらに、DXL の通信ファブリックを利用すると、複数ベンダーのセキュリティ製品や、社内で開発したソリューション、そしてオープンソースのソリューションを相互に連携させ、最適化することができます。Cisco pxGrid と DXL による統合で、50 種類のセキュリティ技術からどのようなデータにもアクセスできるようになります。McAfee ePO コンソールは堅固なオープン プラットフォーム管理の主要コンポーネントです。

デバイス セキュリティの拡大：ネイティブ セキュリティ ツールの管理

McAfee ePO の拡張可能なプラットフォームは、ネイティブ コントロール デバイスを含む多数のデバイスを管理します。Microsoft Windows 10 内蔵のセキュリティを強化及び共同管理して保護を最適化し、またネイティブの Microsoft システムの機能の活用が可能になります。McAfee ePO コンソールは McAfee® MVISION Endpoint を管理して、Microsoft OS ネイティブのセキュリティ向けに調整された高度な機械学習を提供します。また、管理コンソールが増えないため、複雑性やコストの上昇を抑えられます。McAfee ePO ソフトウェア は Microsoft Windows 10 デバイスと異種混合環境のすべてのデバイスに共通ポリシーを提供し、一貫したシンプルな管理を実現します。

時間の短縮

2018 年の MSI リサーチの調査によると、顧客は、セキュリティ ツールが統合されると最大 20% 時間の節減ができると考えています。

統合の価値

- ツールとプロセスの効果増大: 61%
- 複雑さと手作業の削減 — これによりセキュリティ プロフェッショナルはクリティカル シンキングの必要なタスクに集中: 61%
- パターンとコンテキストでデータを表示して可視性を向上: 58%
- ワークフローを効率化してレスポンス時間を短縮: 57%

(出典: 2018年 MSI リサーチ)

自動化ワークフローによる一貫性

McAfee ePO コンソールは柔軟で自動化された管理機能を提供し、脆弱性、セキュリティ ポスチャの変更、そして既知の脅威を、一つのコンソールで迅速に識別、管理、対応できるようにします。McAfee からの依頼で MSI リサーチが 2018 年に行った調査によると、企業は繰り返しのタスクを自動化すれば約 25% の時間の節約ができると期待していることがわかりました。

McAfee ePO ソフトウェアでは、この単一インターフェースを使用して一連の論理ステップにそってクリックするだけで、セキュリティ ポリシーを展開し執行できます。関連するコンテキストは、管理者がタスクに取り組んで、各ステップと、それが他にどう関係しているかを調べることで見えてきます。これで複雑さやエラーの可能性を減らすことができます。管理者は、環境、ポリシー、ツールに関するセキュリティ イベントの種類と重要度に応じて McAfee ePO コンソールがどのようにアラートの発信とセキュリティの対応をするかを定義できます。

開発業務とセキュリティ オペレーションに対応するため、McAfee ePOプラットフォームではセキュリティとITオペレーション システム間のワークフローを自動化し、問題の修復を迅速に行うことができます。McAfee ePO コンソールを使って、より厳しいポリシーの割り当てなどといった IT 運用システムの修復アクションをトリガーすることができます。Webアプリケーション プログラミング インターフェース (API) を利用することで、手動操作を減らすことができます。新しい、またはアップデートされたポリシーやタスクが展開される前に、間違いが起こる可能性を減らし品質管理をするために承認プロセスを設けるかを選択できます。

MVISION Insights では、特徴的ともいえるプロアクティブな自動化ワークフローが提供されます。業界や地域インテリジェンスに基づき MVISION Insights ダッシュボードで自動的にアラートが出され優先度が付けられた外部脅威や未知の脅威を、コモン ビューで確認することができます。これにより現在のセキュリティ ポスチャが脅威に対応できるのかを予測的に判断します。さらに、.DAT ファイルのアップデートや分離といった具体的なアクションが提示されます。

一般的なユースケース

- セキュリティ コンプライアンス レポートを定期的に作成して問題に対応することで、時間を節約し、労働集約型の作業を減らすことができます。
- MVISION Insights を活用して、プロアクティブに業界や地域の脅威状況を把握し、現行のセキュリティ ポスチャで脅威に対処できるのか、そして対処できない場合の対応策など、実践的な知見を得ることができます。
- 堅固な API を使って McAfee ePO コンソールを既存ビジネス プロセス及び機能に簡単に統合し、より多くの情報を入手しワークフローの実行を速めます。例えば McAfee ePO コンソールは、チケット発行システム、Web アプリケーション、さらにセルフサービス ポータルなどと統合します。
- McAfee ePO コンソールと Microsoft Active Directory を同期させ、新しいマシンがネットワークに追加される際にエージェントまたは機械学習セキュリティ ソリューションを配備して、セキュリティ ポスチャを維持します。

「McAfee ePO (ソフトウェア) は、**自動化とオーケストレーションを最初に実現した統合セキュリティの一つです。**...現在のセキュリティ担当者は、従来の (McAfee) ePO (ソフトウェア) をよりシンプルに利用でき、効果と効率性を向上できる方法を求めています...SaaSとして提供される MVISION は、大企業や中堅企業向けに、分析、ポリシー管理、イベント処理を統合しています。」

— Frank Dickinson、IDC セキュリティ製品リサーチ担当バイスプレジデント

迅速な回避と修復

McAfee ePOプラットフォームには高度な機能が組み込まれています。セキュリティ オペレーションの担当者は、これらの機能を使用して脅威の回避や対策を効率的に行うことができます。McAfee ePO コンソールの自動対応機能は、発生したイベントに基づいてアクションを自動で開始します。アクションは単なる通知の場合もあれば、修復の承認の場合もあります。

自動対応の一般的なユースケース

- 新しい脅威、アップデートの失敗、または優先度の高いエラーを、事前に決定した閾値をもとに判断し、メールまたはSMS で管理者に通知します。
- ホストに不正アクセスがあった場合に外部コミュニケーションを阻止 (コマンドやコントロールを拒否) するポリシーや、または管理者がポリシーをリセットするまでデータ引き出し/外部転送を阻止するポリシーなど、クライアントまたは脅威イベントに基づいてポリシーを適用します。
- 脅威が検出された際のオンデマンド メモリースキャンなど、システムのタグ付けや修復追加タスクの実行をします。
- サービスデスクでのチケット作成や他のビジネスプロセスへの統合など、サーバー コマンドや外部スクリプトを実行する登録済みの実行可能ファイルを始動します。
- ワークロードやコンテナー (デバイス) を、より制限の厳しいポリシーに基づいて自動的に隔離します。

クラウド ベースのセキュリティ管理

組織では、高度な脅威対策ソリューションの配備をシンプルにして促進する必要があるため、オンプレミス インフラストラクチャのコストとメンテナンス作業をなくすことができるクラウド ベースのセキュリティ管理が注目を集めています。McAfee ePO コンソールはいつでもどこからでもクラウドで実装できます。クラウドには 2 つのオプションがあります: AWS 用の McAfee ePO ソフトウェア または McAfee® MVISION ePO™ です。これは両方とも 1 時間以内に稼働を開始できます。

- AWS 用の McAfee ePO ソフトウェアを使用すると、自動スケーリングなどの AWS ネイティブのサービスや、個別のデータベースの購入や管理が不要な Amazon RDS を活用できるようになります。これにより管理者は、インフラストラクチャではなく重要なセキュリティ タスクに集中することができるようになります。AWS 用の McAfee ePO ソフトウェアは McAfee® Endpoint Security、McAfee® Data Loss Prevention、McAfee® Cloud Workload Security、DXL、そして McAfee ePO ソフトウェアに統合されたサードパーティ ソリューションを管理します。
- MVISION ePO はソフトウェア アズ ア サービス (SaaS) の McAfee ePO の強みをベースに構築されています。これはプラットフォームの管理を劇的にシンプルにするので、管理者は重要なセキュリティ タスクに集中できます。プラットフォームへのアップデートは継続的に行われ、管理者はその内容をいつでも確認できます。エージェントが配備されるとデバイス セキュリティが自動的に会社全体に配備されるので、各デバイスに個別にマニュアルでインストールやアップデートをする必要はありません。またこれによって脅威に対してより強固な対策ができるようになります。McAfee MVISION Endpoint と DXL はどこからでも単一コンソールで管理できます。

「McAfee ePOは傑出しています。この製品があれば、社内のすべてのエンドポイントのセキュリティを管理できます。社内に導入しているすべてのMcAfee製品を1つの画面でチェックできます。ダッシュボードは使いやすく、可視化、レポート、配備、更新、メンテナンス、意思決定など、必要な機能がすべて揃っています。」

—Christopher Sacharok、情報セキュリティ エンジニア、Computer Sciences Corporation

MVISION ePO を使うと、デバイスは、セキュリティ情報及びイベント管理 (SIEM) ソリューションへ関係するデータを送り、アナリストはその情報を分析してさらに正確に脅威の確認や修正ができるようになります。さらに、オンプレミスまたはハイブリッド クラウドの McAfee ePO ソフトウェアの既存のユーザーは、時間をかけることなく簡単に MVISION ePO に移行できます。SaaS ベースのセキュリティ管理プラットフォームによる効率性や利点を十分に活用していただけます。

McAfee ePO ソフトウェアで管理される McAfee 製品

McAfee 製品*
McAfee® Endpoint Protection (脅威対策、ファイアウォール、Web 管理)
McAfee® MVISION Endpoint は高度な脅威対策で Microsoft Windows Defender を補完
McAfee® MVISION Mobile
McAfee® MVISION Insights
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee® MOVE)
McAfee® Data Loss Prevention (McAfee® DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

*オンプレミスの McAfee ePO ソフトウェア用

柔軟な配備

配備	主な利点
オンプレミスの McAfee ePO	データと機能セットの完全なコントロール
AWS 用 McAfee ePO	オンプレミスでは必要となるハードウェア メンテナンスが不要
McAfee® MVISION ePO ソフトウェア アズ ア サービス*	複数テナントの SaaS オファリングで、インフラストラクチャのメンテナンスとアップグレードが不要

* McAfee MVISION ePO では McAfee ePO ソフトウェアの一部の機能は提供されていません。

ユースケース: McAfee ePO コンソールがセキュリティ集中管理を可能に

製品と技術	ユースケース	利点
MVISION ePO MVISION Endpoint Microsoft Windows 10	McAfee MVISION ePO ソフトウェアは McAfee MVISION Endpoint を管理して、Microsoft Windows 10 ネイティブ コントロールを高度な保護機能で補強します。共通管理プラットフォームと、Microsoft Windows 及び McAfee Endpoint Security 向けの一貫したポリシーで、高度な脅威を簡単に検出し管理できます。	Microsoft Windows のネイティブ コントロールの保護の強化と効果的な実績ある管理
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Securityにより、エンドポイントで既知の不正なファイルが検出されます。McAfee ePOコンソールで、より厳格なポリシーをエンドポイントに設定し、脅威を隔離します。これは共通管理インターフェースで行います。	感染したエンドポイントの迅速な隔離
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Managerでエンドポイントからの重要データの流出が検出されます。McAfee ePOコンソールでこのエンドポイントにタグを付けます。McAfee ePOコンソールでデータ損失防止ポリシーを適用してデータをブロックし、ユーザーにコンプライアンス違反を通知します。	データ損失ポリシーの自動執行
McAfee ePO MVISION ePO McAfee Endpoint McAfee MVISION EDR McAfee MVISION Insights	McAfee MVISION Insights は、優先度が高く攻撃が予期される外部脅威に関して実践的な情報を提供します。MVISION Insights から McAfee® MVISION EDR に切り替え、提供された侵害の兆候 (IoC) を使って自社の環境に IoC が存在するかを検索できます。存在が確認された場合は、関連するキャンペーンの情報や必要なアクションが詳細に提供されます。	迅速な調査と問題解決

統合の例

製品と技術	統合の例	利点
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Securityで不審なホストにフラグが設定されます。McAfee ePOコンソールで追加のスキャンを実行できます。これは PxGrid 経由で Cisco ISE に伝えられ、また McAfee ePO コンソール経由で DXL エクスチェンジに伝えられます。ホストが許容可能と判断されるまで、Cisco ISEがホストを隔離します。	プロアクティブな保護の強化
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO は Nexpose とアセット リストを共有します。これにより McAfee ePO コンソールからリスク ポスチャを確認でき、管理者はそれに沿ってポリシーを設定できるようになります。DXLベンダー コミュニティと脆弱性データを共有します。	▪ 複雑さの解消 ▪ 1つのダッシュボードで全体のセキュリティ状況を正確に把握し、優先順位に従ってアクションを実行できるので、リスクを最小限に抑えることが可能です。
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	この統合により、ネットワークやエンドポイント間でリアルタイムの脅威情報を双方向で共有できます。 イベントは DXL コミュニティでも共有されます。 Check Point Anti-Bot ソフトウェア ブレード はコマンド & コントロール (C&C) トラフィックをブロックし、McAfee ePO ソフトウェア及び統合されたその他のサードパーティ セキュリティ ソリューションに、共通の DXL 関連のアラートを送ります。McAfee はこのインテリジェンスをもとに、エンドポイント デバイスに対して関連する修正ワークフローを自動的に開始します。Check Point と McAfee はまた、ゼロデイ攻撃を検出、防止し、これを既知の攻撃として記録します。これがネットワークからの攻撃なのかエンドポイントからの攻撃なのかは関係ありません。統合された製品は重要なインテリジェンスをリアルタイムでやり取りすることによって、自動的に脅威を検出、ブロック、そして修正できるようになります。	▪ 検出までの時間を短縮 ▪ 攻撃をブロックして修復

〒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