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様々なツールとデータを利用しなければならず、手間がかかります。そのため、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。

管理者は、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。McAfee® ePolicy Orchestrator® (McAfee ePO™) は、オンプレミスでもクラウドでも利用できる管理プラットフォームです (クラウド版にはSaaS用とIaaS用のモデルがあります)。このプラットフォームを利用すると、手間のかかる管理作業を省力化し、ヒューマン　エラーの発生を防ぐことができます。これにより、セキュリティ対応を迅速かつ効率的に実施できます。

基本的セキュリティ

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™ と 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め、複数の製品を調整する複雑さが無くなります。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。

主な特長

- 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
- 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 内臓のネイティブ 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とつながる

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タスク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。[セキュリティ リソース] ページでは、最新の脅威情報や研究成果をすぐに利用できます。

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 コンソールによりセキュリティ管理者はポリシー管理をシンプル化できます。これは当社の業界最先端のメッセージング 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の脅威インテリジェンスと連携し、また様々な製品において双方向でポリシーを統合することで実現しています。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。お客様の環境のePOサーバーの状態を確認することもできます。これは、オンプレミス版のePOとAWS用ePOで利用できます。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ePOインフラ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、状況改善のおすすめの手順を確認できます。

オープン プラットフォームの効果で不規則性を排除

ESG リサーチによると、何十億もの脅威とデバイスに対応するために、40% の組織で 10 から 25のツールを利用しており、また 30% の組織では 26 から 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 (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に集中コントロールを提供します。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。McAfee ePO コンソールを使うと、次世代技術を採用し、それを1つのフレームワーク内で既存システムと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、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150 社以上のパートナーが参加しています。

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
統合されたプラットフォームを使用すると、使用していない場合よりも保護が強化され、対応も速くなります。

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

さらに、Data Exchange Layer (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 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 ソフトウェアは 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有ポリシーを提供し、一貫性がありシンプルな管理を実現します。

自動化ワークフローによる一貫性

McAfee ePO ソフトウェア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。開発作業とセキュリティ オペレーションをサポートするため、McAfee ePO プラットフォームでは、問題の迅速な修正にむけてセキュリティシステムと IT 運用システムの間のワークフローを自動化できます。McAfee ePO コンソールを使って、厳密な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) を活用するとマニュアル作業を減らせます。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。

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

一般的なユースケース

- 各関係者のニーズに合ったセキュリティ コンプライアンス レポート作成をスケジューリングして時間を節約し、不必要で労力のかかる作業を排除します。
- 堅固なアプリケーション 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。例えばチケット発行システム、Web アプリケーション、またはセルフサービス 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。

迅速な脅威の緩和と修正

McAfee ePO プラットフォームには、セキュリティ運用スタッフが脅威を緩和、またはコンプライアンスの復元のために変更を実行する際の、効率性を上げる高度な機能が内蔵されています。McAfee ePO 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。アクションは簡単な通知や承認された修正作業などです。

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、より限定的な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 ソフトウェア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: Amazon Web Services (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。

「McAfee ePO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ePOの能力を維持しながら、より簡単で効果的なセキュリティ管理を求めています...SaaSとして提供されるMVISIONは、大企業や中堅企業が適切な対応を行えるように、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

- 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、Data Exchange Layer、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。
- McAfee® 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 Data Exchange Layer はどこからでも単一コンソールで管理できるようになります。McAfee 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。

McAfee ePO 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 先進的な脅威保護 で Windows Defender を補完
McAfee® MVISION Mobile
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 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 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 ePO の一部の機能は提供されていません

「McAfee ePO ソフトウェアは他のソリューションと比べて傑出しており、エンドポイント保護のワンストップ ショップになっています。使用しているMcAfee製品の必要な情報は、すべて一つのスクリーンから見られます。使いやすいダッシュボードと内蔵機能のおかげで、可視性、レポーティング、配備、アップデート、メンテナンス、意思決定などすべてが非常に簡単になりました。」

— Computer Sciences Corporation インフォメーション セキュリティ エンジニア Christopher Sacharok 氏

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

製品及び技術	ユースケース	利点
McAfee MVISION ePO McAfee 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、最新の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 はエンドポイント上の既知の不正ファイルを検出します。McAfee ePO コンソールはエンドポイントに、より厳密なポリシーを設定して隔離します。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 は、McAfee ePO コンソールでエンドポイントでの大量のデータ引き出しを検知しタグ付けします。McAfee ePO コンソールはデータ損失防止ポリシーを適用してデータ引き出しをブロックし、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

統合例

製品及び技術	統合のユースケース	利点
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security が不審なホストにフラグを付けます。McAfee ePO コンソールが追加スキャンを始動させます。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。Cisco ISE は安全だと判断されるまでホストを隔離します。	プロアクティブな保護強化
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。脆弱性データはベンダーの DXL コミュニティで共有されます。	▪ 複雑さの解消 ▪ 包括的かつ信頼できるポスチャを実現し、またリスクを最小化するために単一ダッシュボードからアクションの優先順位付けを実行
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	この統合により、ネットワークとエンドポイントの間の双方向のリアルタイムな情報共有が可能になります。 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 ▪ 攻撃をブロックし修正

〒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