エンドポイント セキュリティをよりシンプルに

デバイスからクラウドまで、すべてのエンドポイントを保護する統合セキュリティ対策の構築

サイバーセキュリティは矛盾した問題を抱えています。脅威の数は増加の一途をたどり、巧妙化が急速に進んでいます。また、侵害により多大な被害も発生しています。一方で、このような状況に対応できる経験豊富なアナリストの数は以前よりも少なくなっています。

このような複雑なセキュリティ問題をより少ない時間とリソースで解決できる方法を提供するのがMcAfee®エンドポイント保護ポートフォリオです。このソリューションは業界最先端の分析機能と機械学習機能を利用し、150を超えるベンダーの製品と連携が可能です。デバイスからクラウドまでを網羅するセキュリティを実現するため、McAfeeは、よりシンプルでスマート、かつ柔軟な統合セキュリティ システムの構築に注力しています。

主な特長

- エクスプロイト防止、ファイアウォール、Web管理、機械学習でエンドポイントを保護
- フィッシング詐欺、ゼロデイ攻撃、データ漏洩からiOS/Androidデバイスをリアルタイムで保護。オフラインでもデバイスを保護
- AIを活用した調査機能により、脅威検知、調査、対応を強化
- オペレーティング システムの基本的なセキュリティ機能に機械学習、認証情報の窃盗防止、修復のロールバック機能を追加
- 1つの管理コンソールでセキュリティ対策を管理
- SaaSベースのMVISION ePOかオンプレミスのMcAfee® ePO™を選択可能

McAfeeとつながる

エンタープライズ環境で使用されるエンドポイントの数は増加し続けています。その種類も多様化し、複雑さを増しています。企業はいま難しい判断に迫られています。従来のウイルス対策のみに依存して良いのか。この状態を続けていては、ランサムウェアやボットネットなど、最新の脅威を防ぐことはできないのではないか。あるいは、複数のベンダーのソリューションを組み合わせて脅威対策を強化するべきか。しかし、これによってプロセスが遅くなったり、重大なダウンタイムが発生することはないのか。こうした脅威対策と運用効率の問題を解決するのがMcAfeeのエンドポイント保護ソリューションです。

McAfee Endpoint Security

集中管理と分析情報の共有

この統合エンドポイント保護プラットフォームは、1つのエージェントで脅威対策、ファイアウォール、Web管理、適応脅威対策などの複数の技術を一元管理します。複雑な環境でもセキュリティを容易に管理できます。

従来のウイルス対策と異なり、McAfee Endpoint Securityはローカル エンドポイントとクラウドのMcAfee® Global Threat Intelligenceの接続を利用し、ゼロデイ脅威をほぼリアルタイムで検出します。どこで脅威が検出されても、すぐに識別できます。高度なエクスプロイト対策と分析情報を共有することで、McAfee Endpoint Securityのゼロデイ脅威の検出率はMcAfee® VirusScan® Enterpriseよりも25%向上しています。独立調査機関のテストで、McAfee Endpoint Securityは99.98%の検出率と誤検知ゼロの結果を残しています。

メンテナンスを自動化し、効率的に修復

McAfee Endpoint Securityでは、高度な自動化機能と機械学習機能を利用できます。このプラットフォームは機械学習により動作の分類を行います。これにより、ゼロデイ脅威をほぼリアルタイムで検出し、有効な脅威インテリジェンスを提供します。この機能は時間とともに進化していきます。新しい動作を学習し、ルールを追加していくので、今後発生する攻撃も識別できます。

攻撃が発生すると、管理者は感染場所をすぐに特定し、エンドポイントが攻撃を受けていた期間を確認できます。状況をすぐに把握できるので、より迅速な対応が可能になります。Real Protect機能は、対象のエンドポイントを最後に確認された良好な状態に修復します。感染をすぐに防止できるので管理者の負担が少なくなります。また、アプリケーションの動的隔離が、最初のエンドポイントの感染前にランサムウェアやグレーウェアを阻止します。

McAfee ePOプラットフォームとMcAfee Endpoint Securityを組み合わせることで、環境の可視化を強化し、ITスタッフの作業効率を改善することができます。また、セキュリティ対策が統合され、オペレーションが省力化されるので、コストの削減にもつながります。McAfee Endpoint Securityに移行した結果、セキュリティ管理にかかる時間が週に40時間短縮されています。従業員の生産性が低下することもありません。スキャンはデバイスがアイドル状態のときに実行され、処理もすぐに終了します。再起動やシャットダウン後もシームレスに再開します。McAfee Endpoint Securityは軽量で、クラウドへの接続も必要ありません。オフラインでもユーザーを保護します。

McAfee Endpoint Security の主な特長

- ゼロデイ脅威をほぼリアルタイムで検出
- マルウェア対策エンジンを継続的に更新
- ウイルス対策、エクスプロイト防止、ファイアウォール、Web管理を統合
- エンドポイントを最後に確認された正常な状態に修復
- オフライン状態でもエンドポイントで悪質なアプリケーションとプロセスを隔離
- アラートに優先度を設定し、イベントを再現
- 使いやすい統合ツールで、脅威ハンティングとインシデント対応が容易に
- ワンクリックでインシデント対応が可能

McAfee MVISION EDR

平均的なIT部門は数千台のエンドポイントを管理しています。管理対象はデスクトップやサーバーだけでなく、スマートフォンやスマート ウォッチ、IoTデバイスなど多岐にわたります。現在のEDRソリューションは大量の情報を生成するため、熟練のアナリストでないと的確な分析ができません。帯域幅に制約があり、人材が不足している現状では、これは効果的なアプローチとはいえません。

MVISION EDRは、ウイルス対策や従来のEDRソリューションが無効になっている場所を特定します。この統合エンドポイント セキュリティ ソリューションでは、大量のアラートを効率的に管理できます。脅威の兆候を示すエンドポイントをモニタリングし、アクティビティ データを収集できます。環境全体を可視化し、必要なコンテキスト情報を取得できます。AIを活用した対応と分析機能がデータを分析して脅威のパターンを識別し、脅威を自動的にブロックまたは隔離してセキュリティ担当者に通知します。また、フォレンジックと分析ツールにより、識別した脅威と不審なアクティビティを調査します。

人工知能（AI）を活用した調査機能

従来のEDRは、未加工のデータ、コンテキスト、検索機能を提供しますが、これらの情報や機能を活用して調査・分析を行うには、相当な経験と知識が必要になります。MVISION EDRではガイド付きの調査機能を利用できるので、熟練の担当者でなくても、短い時間で調査を行うことができます。また、インシデントのリスクや根本原因をより迅速に特定することができます。

AIを活用した調査機能が、攻撃の発生源と対象、攻撃パターンなどのデータを様々な情報源から自動的に収集して処理します。ベテランのアナリストが経験の浅いメンバーに質問をしていくように、アラートに対する仮説を自動的に提示し、複数の情報源からエビデンスを収集して要約し、視覚的に提供します。MVISION EDRはエビデンスに基づいて仮説に関連する質問に回答を提示します。アナリストは、質問を継続してデータを収集するかどうかを判断し、問題を解決済みにしたり、エスカレーションします。

これにより、アナリストの経験値を引き上げ、大量のアラートを効率的に管理できるようになります。調査時間を短縮するだけでなく、調査の品質も向上します。経験の少ないアナリストでも脅威分析が可能になるため、経験豊富なアナリストはより多くの時間を脅威ハンティングに費やすことができます。

迅速な識別と対応

また、強力な検索機能とデータの常時収集機能を使用することで、調査範囲を広げ、より詳しい調査を行うことができます。MVISION EDRでは、エンドポイントのアクティブ プロセス、ネットワーク接続、サービス、自動実行エントリのスナップショットを作成できます。これにより、過去のデータを検索するだけでなく、リアルタイム検索で迅速な調査を行うことができます。このデータはクラウドにもストリーミングされるので、新しい分析エンジンと技術も迅速に採用できます。また、動作ベースの検出結果がMITRE ATTACKフレームワークにマッピングされるので、脅威のフェーズとリスクを判定し、優先度に従って対応することが可能になります。

McAfee MVISION EDR の主な特長

- すぐに利用できる的確な脅威検出情報
- 迅速な分析により、復旧までの時間を短縮
- AIを活用して攻撃を分析
- 既存のスタッフの能力を最大限に活用
- メンテナンスに手間がかからないクラウド ソリューション
- 業界で評価の高いセキュリティ管理プラットフォームであるMVISION ePO（SaaSベース）またはMcAfee ePO（オンプレミス、IaaSベース）を利用
- 煩雑な管理作業が解消され、アナリストは戦略的なインシデント対応に専念できる

McAfee® Enterprise Security Managerなどのセキュリティ情報/イベント管理（SIEM）ソリューションと統合することで、MVISION EDRの調査分析能力をさらに高めることができます。これにより、ネットワーク情報やSIEMが収集したデータを利用してエンドポイントの修復が可能になります。

McAfee MVISION Endpoint

MVISION Endpointは、高度な検出・修復機能により、エンドポイントの保護を強化します。このソリューションはオペレーティング システム（OS）固有の保護機能を強化するように設計されています。Windows 10やWindows Server 2016/2019に搭載されているウイルス対策、ファイアウォール、エクスプロイト防止機能を補い、Microsoft Defenderで検出されなかった高度な脅威を検出します。

よりスマートなエンドポイント対策

機械学習による分析のみに頼る他の製品と異なり、MVISION Endpointは静的分析、動作分析、ファイレス マルウェアの分析を併用し、誤検知の少ない、より強固な脅威対策を実現しています。このソリューションは、実際の動作を機械学習で分析し、他のマルウェアと同じ特徴が見られるファイルを脅威と判断します。また、高度なロールバック機能により、ランサムウェアの影響を受けたシステムを最後に確認された正常な状態に修復します。

クラウドベースのセキュリティ1つのコンソールで管理

最も重要な点は、MVISION Endpointが統合管理機能を備えていることです。ポリシー管理を二重に行うことなく、Windows Defenderウイルス対策、Exploit Guard、Windowsファイアウォールの設定、McAfeeポリシーを一元的に管理できます。McAfee MVISION EndpointとMcAfee ePOまたはMVISION ePOを展開することで、真に統合されたセキュリティを実現できます。McAfee ePOとMVISION ePOは、サードパーティの統合にも対応しています。追加の保護対策をコンソールに追加し、セキュリティの強化とカスタマイズを行うことができます。

これは非常に軽量なエージェントです。従来のセキュリティツールよりも高速で、強力な機能を提供します。更新はクライアントに自動的に適用されるので、クライアントが最新の状態かどうか気にする必要はありません。デバイスのフットプリントも小さく、バランスの取れた処理を行うため、ユーザーの邪魔になることはありません。

McAfee MVISION Endpointの主な特長

- Windows 10、Windows Server 2016/2019を一元管理
- 脅威（ファイル、ファイルレス）と動作の分析に機械学習を利用
- 総所有コスト（TCO）を低減し、ワークフローを簡素化
- 認証情報の窃盗防止と修復のロールバック
- McAfeeとMicrosoftの保護対策のポリシーを1つのコンソールで一元管理

McAfee MVISION Mobile

McAfee MVISION Mobileは、Apple iOSデバイスやAndroidデバイスの脅威と脆弱性を検出します。また、これらのデバイスが接続するネットワークや、ユーザーがダウンロードしたアプリケーションを識別します。このソリューションは、エンタープライズ向けの集中管理プラットフォームであるMcAfee ePOと統合されています。他のエンドポイントと同様にモバイル デバイスを管理できます。MVISION Mobileは、McAfee® Device Securityの統合コンポーネントで、McAfeeが管理するデバイスと同じコンソールでモバイル デバイスを可視化し、管理できます。

よりインテリジェントに脅威を警戒

クラウドベースのモバイル セキュリティ ソリューションは、アプリのサンドボックス化やトラフィックのトンネル化でデバイスを保護していますが、MVISION Mobileは違います。モバイル デバイス上に常に存在し、会社のネットワーク、公共のアクセス ポイント、モバイル通信など、どのような方法でネットワークに接続してもモバイル デバイスを保護します。オフラインのデバイスも保護します。

MVISION Mobileは、数百万台のデバイスから収集したデータと機械学習アルゴリズムを使用して、既知の脅威だけでなく、これから発生する可能性のある脅威や攻撃を識別します。デバイスの通常の動作からの逸脱を分析して侵害の兆候を把握し、デバイス、アプリケーション、ネットワークに対する高度な攻撃を正確に識別します。包括的なアプリケーション情報により、セキュリティとプライバシーのリスクを回避し、データ漏洩の可能性を減らします。また、ネットワーク保護通知により、デバイスが危険なネットワークや保護されていないネットワークに接続しているかどうかを確認し、攻撃を防止します。

McAfee MVISION Mobileの主な特長

- デバイス上でリアルタイムで保護
- モバイルの脅威を検出し、ゼロデイ攻撃を阻止
- プライバシー リスクを強調表示し、ユーザーにアプリケーションの危険性を通知
- エンタープライズ クラスのモバイル脅威インテリジェンスで対応を効率的に実施
- コンプライアンス コントロールにより、場所や時間に関係なく、どのデバイスでも安全に作業が可能
- フィッシング詐欺対策により、SMS、ソーシャル メディア アプリ、メールに含まれている有害なリンクを検出
- エンタープライズ モビリティ管理（EMM）ソリューションと統合、BYOD（bring your own device）にも対応
- 詳細な脅威フォレンジックにより、感染デバイスからの大量拡散を未然に防止

McAfee MVISION ePO

業界で評価の高いMcAfee MVISION ePOは、McAfeeソリューションを管理するだけでなく、オペレーティング システムに組み込まれているネイティブなセキュリティ機能も強化するように設計されています。これは、実績豊富なMcAfee ePOをマルチテナント対応のSaaSバージョンにしたもので、ポリシーの適用とコンプライアンス プロセスを自動的に行い、環境全体の可視化を強化します。このソリューションでは数十万台のデバイスを管理できます。ネイティブのセキュリティ機能と競合することもありません。オンプレミス アーキテクチャの管理を複雑にすることなく、デバイスからクラウドまでを保護することができます。

シンプルなセキュリティ

拡張性に優れたMVISION ePOのプラットフォームでは、Microsoft Windows 10デバイスを含むすべてのデバイスに同じ操作で共有ポリシーを適用できます。異種環境でも一貫した管理作業を簡単に行うことができます。MVISION ePOでは、環境全体の状況を一目で確認できるので、複数の製品を使用する場合の煩雑さや調整作業はありません。アジャイルな自動管理機能により、ユーザーは脆弱性を迅速に識別して管理し、対応できます。セキュリティ状況はブラウザー経由でどこからでも確認できます。また、簡単な手順で企業全体にセキュリティ ポリシーを展開し、適用できます。

保護ワークスペースには、デジタル領域の概要が1つのグラフィカルなグラフで表示されます。管理者はリスクの優先度を判断し、特定のイベントをドリルダウンしてより詳細な分析情報を表示できます。このビューにより、レポートの作成とデータの分析に必要な時間が短縮されます。操作が必要な場合でもエラーの発生を防ぐことができます。リスク管理とインシデント分析の両方を行うことで、デバイスからSIEMに重要な分析情報が提供されます。これにより、脅威ハンティングや修復作業を効率的に行うことができます。

さらなる効率化

Gartner Magic Quadrantエンドポイント保護部門の評価結果を見ると、多くの企業がMcAfee製品を採用している理由としてMcAfee ePOの存在を挙げています。この実績豊富な技術がSaaS形式で提供されるようになり、セキュリティ担当者はすべてのデバイスをモニタリングし、コントロールすることが可能になりました。MVISION ePOは、オンプレミスのセキュリティ インフラのようにセットアップやメンテナンスを行う必要がなく、環境全体でデバイス セキュリティを自動的に配備し、継続的にアップデートすることができます。これにより、安定性が向上し、管理作業にかかる時間が短縮されます。セキュリティ オペレーションを効率化する高度な機能により、以前よりもはるかに短い時間で脅威対策やコンプライアンス対応を行うことができます。

MVISION ePOの機能をお試しください。こちらをクリックすると、無料トライアルをご利用いただけます。

McAfee MVISION ePOの主な特長

- 業界で評価された集中管理機能
- どこからでも簡単にセキュリティを管理
- オンプレミスのセキュリティ プラットフォームのメンテナンスに伴う煩雑さを解消
- 共通のビューでリスク管理とインシデント分析が可能
- McAfee製品とオペレーティング システム固有のセキュリティ機能の両方を管理できる包括的なプラットフォーム
- ワークフローの自動化で管理作業を効率的に実施
- インシデントの調査/修復を省力化
- 市場で最も普及しているデバイスを共通のセキュリティ対策で管理
- 数百から数千台のデバイスに対応
- デバイスからクラウドまでを保護

ケーススタディ

MGM Resorts International
世界20か所のリゾート施設で20,000以上のノードを管理

- **課題:** リスクを事前に回避できず、ゼロデイ攻撃を受けている。基幹アプリケーションを常時稼働させておくため、複雑な攻撃パターンを把握し、脅威を阻止する必要がある。新しいテクノロジを導入しても、SecOpsのコスト削減につながらない。
- **ソリューション:** McAfee® Enterprise Security Manager、McAfee® Investigator、MVISION EDR、McAfee® Web Gateway、McAfee Endpoint Security、McAfee Data Loss Prevention、DXL、McAfee® Professional Services
- **結果:** 脅威の封じ込め、調査、修復にかかる時間を短縮。SecOpsチームのスキルが向上。

Atrius Health
29以上のサイトで9,000台のエンドポイントが存在、ユーザー数は65,000人を超える

- **課題:** ランサムウェアとフィッシング詐欺。検出から対応までの時間を短縮。ビジネスを成長を妨げずに組織を保護する。
- **ソリューション:** McAfee Enterprise Security Manager、McAfee Endpoint Security
- **結果:** 運用コストの削減。フルタイム従業員を増やさずに検出から対応までの時間を短縮。仮想環境のセキュリティが向上。

Florida International University
2か所のメインキャンパスと海外のサテライトキャンパスを合わせて55,000名の学生と15,000名のスタッフ

- **課題:** BYODの普及。脅威対策が十分でない。不注意によるマルウェア感染の拡大。広範囲の可視化。
- **ソリューション:** McAfee Enterprise Security Manager、McAfee Endpoint Security
- **結果:** 不審なファイルや攻撃の封じ込めにかかる時間を短縮。スタッフを増強せずに全体のセキュリティ レベルを向上。ユーザーへの影響を最小限に抑えながらエンドポイントの保護を強化。組織全体の可視化を強化し、管理作業を省力化。

Banco Delta
400台のエンドポイント

- **課題:** セキュリティ管理作業の負担。巧妙な攻撃を阻止できる強固な防御態勢。今後のセキュリティ戦略計画（クラウドへの移行を含む）
- **ソリューション:** McAfee ePO プラットフォーム、McAfee Enterprise Security Manager、McAfee Endpoint Security
- **結果:** 侵害のリスクや感染を大幅に削減。

米国の保険会社
12か所に6,000台のデスクトップと2.000台のサーバー

- **課題:** 顧客の個人情報の保護。カスタマー エクスペリエンスを損なうことなく強固なセキュリティ対策を実施。
- **ソリューション:** McAfee Endpoint Security、McAfee Data Loss Prevention、McAfee Web Gateway
- **結果:** CPU使用率の急増が95%から30/35%に減少。数日かかっていたスキャンが数時間で完了。サイバーセキュリティ エンジニアの1週間の作業時間が大幅に短縮。ユーザーとSecOpsの生産性が向上。セキュリティ状況の改善。

世界的な大手銀行（EMEA）
40か国以上に45,000台のエンドポイント、2か所のデータセンター

- **課題:** ランサムウェアとゼロデイ脅威の阻止。ユーザーの動作に起因する脅威のブロック。セキュリティ管理作業の効率化。
- **ソリューション:** McAfee Endpoint Security、McAfee ePO プラットフォーム、McAfee Web Gateway
- **結果:** エンドポイントの保護対策が強化され、以前よりも多くのマルウェアを検知。ゼロデイ脅威に対する防御能力も向上。統合セキュリティ ソリューションで脅威情報をほぼリアルタイムで共有。保護までの時間を短縮。管理作業の効率化とインシデント数の減少で、運用コストの削減に成功。

受賞歴と評価

McAfee Endpoint Security

- 2019 Cybersecurity Excellence Awardsのエンドポイント セキュリティ カテゴリで銀賞を受賞
- AV-ComparativesのApproved Business Product Awardを受賞
- AV-TEST: McAfeeがユーザビリティで満点を獲得

MVISION Endpoint

- 2019 Cybersecurity Excellence Awardsのエンドポイント セキュリティ カテゴリで銀賞を受賞
- 2018 Tech Innovator Award for Endpoint Securityを受賞

MVISION Mobile

- 2019年Cybersecurity Excellence Awardsのモバイル セキュリティ カテゴリで銀賞を受賞

McAfee エンドポイント製品の実績

- 合計で6億2,200万台のエンドポイント
- 合計で9,700万台のエンドポイント（企業ユーザー）
- 合計で5億2,500万台のエンドポイント（個人ユーザー）
- 69,000の企業ユーザー
- 7,000名の従業員
- 189か国
- Fortune 100の80%で採用
- Fortune 500の75%で採用
- Global 2000の64%で採用
- 世界の大手金融機関の87%で採用
- 大手小売業上位50社の54%で採用
- 世界でセキュリティ関連の特許を1,550件以上取得

「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...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必要としています...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、イベント処理が統合されています。」

— 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

〒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