McAfee Threat Intelligence Exchange

脅威情報を共有して標的型攻撃を阻止

McAfee® Threat Intelligence Exchangeを使用すると、エンドポイント、ゲートウェイ、ネットワーク、データセンターを保護するソリューションの間でセキュリティ情報をリアルタイムに交換し、適応型の脅威検出と対応が可能になります。ローカルで収集された情報とグローバルの脅威情報が共有され、複数のセキュリティ対策が1つの統合ソリューションのように機能します。McAfee Threat Intelligence Exchangeは、数日～数か月かかる脅威の検出から封じ込めまでをわずか数ミリ秒で行います。

主な特長

- 高度な標的型脅威の検出から封じ込めまでにかかる時間を大幅に短縮し（数日～数か月から数ミリ秒）、脅威対策を最適化します。
- グローバルなデータソースから脅威情報を収集し、ローカルの脅威情報と組み合わせて総合的な脅威情報を提供します。
- 高度な標的型攻撃を迅速に検知します。
- エンドポイント、ゲートウェイ、ネットワーク、データセンターを保護するセキュリティソリューションで、関連するセキュリティ情報がリアルタイムで共有されます。

脅威情報エコシステムを構築

McAfee Threat Intelligence Exchangeは、McAfee Data Exchange Layerを経由して情報を共有し、セキュリティ コンポーネントを統合します。接続しているすべてのセキュリティ ソリューションで、複数の情報源から収集した脅威情報が共有されます。他社製のソリューションも例外ではありません。

複数のセキュリティ コンポーネントが1つのソリューションのように機能するので、脅威の検出と対策に役立つ関連情報が環境内のエンドポイント、ゲートウェイ、データセンター、クラウド、他のセキュリティ制御ポイントでリアルタイムで共有されます。McAfee Data Exchange Layerで簡単に統合できるので、セキュリティを効率的に管理し、実装と運用にかかる費用を大幅に削減できます。

McAfee Data Exchange Layerはオープン フレームワークとして設計されています。他社製を含むすべてのセキュリティ ソリューションをMcAfee Threat Intelligence Exchangeエコシステムに動的に接続できます。セキュリティ コンポーネントの間で必要な情報が交換されるので、総所有コストを抑えることができます。既存のセキュリティ製品やソリューションに対する投資が無駄になることはありません。

個々のシステムが連携する適応型の脅威対策は、企業のITセキュリティにとって全く新しいアプローチです。セキュリティ チームは、組織や予算の壁を超えるため、脅威情報を自動的に取得し、保護ポリシーとセキュリティ対策をプロアクティブに適用できるシステムを必要としています。

セキュリティ インフラを相互に連携するシステムに変えることで、脅威情報の共有と環境の保護が可能になります。McAfee Threat Intelligence Exchangeでセキュリティを強化することで、巧妙さを増す新たな標的型攻撃にも対応することができます。

主な特長（続き）

- エンドポイントのコンテキスト（ファイル、プロセス、環境属性）と総合的な脅威情報で未知のファイルに対して適切な判断を行うことができます。
- McAfee Data Exchange Layerで簡単に統合できます。Intel Securityとそれ以外のセキュリティ ソリューションが統合され、脅威情報がリアルタイムで共有されるので、実装と運用のコストを削減できます。

脅威への適応と無効化

標的型攻撃に迅速に対応するには、脅威情報を共有し、ネットワークのどの部分でも脅威を検出できるようにする必要があります。これらの脅威は特定の組織を標的とするため、ローカルに監視システムを配備して脅威の傾向を把握し、攻撃を検知する必要があります。このようなコンテキストデータとグローバル脅威情報を組み合わせることで、これまで検出できなかった脅威を識別し、短時間での阻止が可能になります。

ネットワーク上で検出された未確認のファイルは、McAfee Threat Intelligence Exchangeが評価し、その結果をすべてのシステムにリアルタイムで配信します。ローカルの脅威情報は今後の検出のために保存されます。同じ脅威が別のデバイスやサーバーで見つかった場合、すぐに識別されます。不明と判定されることはありません。

たとえば、ゲートウェイで検出された不正なファイルの情報は、McAfee Data Exchange Layer経由でMcAfee Threat Intelligence Exchangeに送信され、さらにエンドポイントやデータセンターに転送されます。これにより、防御に必要な情報を事前に取得できます。また、エンドポイントでマルウェアの攻撃がブロックされると、この情報がすぐにゲートウェイや他のセキュリティ コンポーネントと共有されるので、脅威を境界で阻止することができます。

脅威情報をリアルタイムで統合

McAfee Global Threat Intelligence（McAfee GTI）などのグローバルな情報源、外部の脅威情報、STIX（Structured Threat Information eXpression）ファイルで記述された侵害の兆候（IoC）などの統合が可能です。McAfee Global Threat Intelligenceは、エンドポイント、データセンター、ゲートウェイ、ネットワークのセキュリティ ソリューションや、McAfee Advanced Threat Defenseのサンドボックスからリアルタイム データと履歴データを収集します。このようなグローバルの脅威データとローカルの情報が統合され、セキュリティ エコシステム全体ですぐに共有されます。

McAfee Threat Intelligence Exchangeを使用すると、McAfee GTIなどから取得した総合的な脅威情報とSTIXファイルを簡単に統合できます。これらの情報に、エンドポイント、ゲートウェイ、サンドボックスのソリューション、他のセキュリティ コンポーネントから収集したローカルの脅威情報（リアルタイム データとイベント データ）も統合できます。セキュリティ管理者は、環境や組織に合わせて脅威情報を調整し、保護対策をカスタマイズできます（たとえば、ファイルと証明書、組織が提供する証明書のブラックリストとホワイトリストなど）。

ローカルで脅威情報を調整し、優先順位を設定できるので、今後発生する脅威にも迅速に対応できます。重要なオブジェクトを記述したメタデータも保持され、収集した情報に反映されます。SIEM（セキュリティ情報/イベント管理）製品を使用すると、収集された情報と過去の不正なアクティビティから、攻撃を受けた可能性の高いシステムをすぐに特定できます。

最先端のエンドポイント保護

McAfee Threat Intelligence Exchangeは、McAfee Threat Intelligence Exchange VirusScan® Enterpriseモジュールを使用して革新的なエンドポイント保護を提供します。このモジュールは、設定可能なルールを使用してファイルの実行を制御します。また、ローカルのエンドポイント コンテキスト（ファイル、プロセス、環境属性など）と現在使用可能な脅威情報（組織の感染状況、経過時間、レピュテーションなど）の両方を使用します。

エンドポイントのリスク許容度に基づいてMcAfee Threat Intelligence Exchange VirusScan Enterpriseモジュールをカスタマイズするときに、特定の要件に合わせて実行条件を柔軟に設定できます。たとえば、既知の許容範囲のレピュテーションがない限りファイルへのアクセスを許可しないルールを設定すると、不明なファイルやグレーなファイルを拒否する厳格なポリシーを設定できます。

時間と場所を問わないエンドポイント管理

McAfee Threat Intelligence Exchangeは、どこでも利用できる適応型の脅威対策とセキュリティ管理を提供します。エンドポイントの場所に関係なく、脅威ポリシー、検出、セキュリティ更新、リモート調査を管理できます。セキュリティ コンポーネントは、物理的な場所に関係なく、1つのソリューションとして機能します。エンドポイント、ゲートウェイ、他のセキュリティ製品間で関連するセキュリティ データをリアルタイムで共有し、適応型の脅威対策を行います。

高度な標的型攻撃は現実の問題

標的型攻撃は、検出を回避して組織内に長期間潜伏し、重要なデータを盗み出します。最近発表された『Verizon 2015 Data Breach and Investigations Report』(2015年データ侵害調査報告書)によると、マルウェア サンプルの70%から90%は特定の組織を狙ったもので、このような脅威の検出は大きな課題となっています[1]。

詳細については、**www.mcafee.com/jp/products/threat-intelligence-exchange.aspx**をご覧ください。

他のセキュリティ管理ソリューションでは、ポリシーの変更、コンテンツ、プログラムの更新をエンドポイントにすぐに配布することはできません。これでは組織に対するリスクが増大します。McAfee Threat Intelligence ExchangeはMcAfee Data Exchange Layerを利用することで、ネットワークの問題に影響を受けることなく接続を維持します。これにより、リスク ギャップがなくなり、エンドポイントの保護状態を維持できます。

連携のメリット

ワンクリックでレピュテーションを取得

組織内のセキュリティ コンポーネント(ゲートウェイ、エンドポイントまたはネットワーク)が不明なファイルを検出した場合、属性や脅威情報に基づいてレピュテーションをすぐに確認できます。

高度な脅威分析

ファイルに関する詳細な情報が必要になると、ファイルがMcAfee Threat Intelligence ExchangeからMcAfee Advanced Threat Defenseに自動的に転送され、脅威の分析がすぐに実行されます。静的または動的なコード分析を行い、問題のファイルのレピュテーションを評価します。この処理はすべて自動的に実行され、結果が記録されます。この情報はMcAfee Data Exchange Layer経由で共有され、セキュリティ エコシステム全体の保護に利用されます。

セキュリティ イベントの管理

McAfee Enterprise Security Managerを使用すると、McAfee Threat Intelligence Exchangeから取得したIoCを詳しく分析できます。セキュリティの履歴情報を使用し、ウォッチリストを自動的に作成できるので、組織のセキュリティを効率的に管理できます。

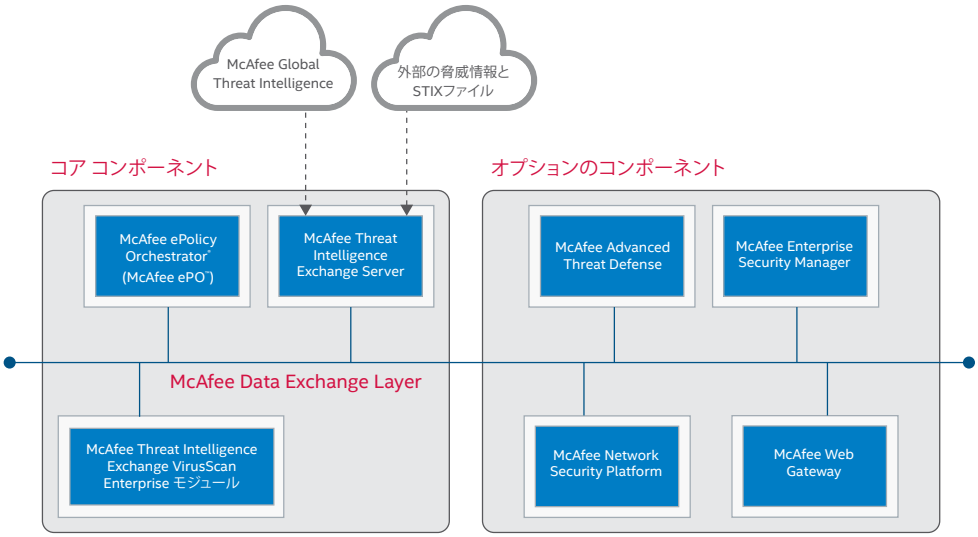

図 1. McAfee Data Exchange Layerで簡単に統合できるので、実装と運用にかかる費用を大幅に削減できます。Security Connectedプラットフォームの進化により、効率的な管理が可能になります。

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee. Part of Intel Security.
マカフィー株式会社
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
名古屋営業所 〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233 (代) FAX 052-551-6236
福岡営業所 〒810-0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674 (代)
www.intelsecurity.com

62276ds_threat-intelligence-exchange_0216_kgs