McAfee Cloud Threat Detection

高度なマルウェアや潜伏する脅威の検出でMcAfee®のセキュリティ対策を簡単に強化

McAfeeは、機械学習などの最新の分析技術を応用することで、マルウェアを識別してアクションを実行できます。また、セキュリティ対策を自動的に更新し、将来の類似した攻撃にも対応することができます。

主な利点:

- 未知の脅威によるビジネスへのリスクを軽減
- ビッグデータと機械学習を利用
- セキュリティに対する投資を最適化
- 高度な脅威分析を簡単に配備

従来の保護対策を回避する巧妙なマルウェアが増加しています。組織は苦しい戦いを強いられています。高度な検出ソリューションも存在しますが、セキュリティ要員やリソースに制約がある組織にとっては、このようなソリューションは複雑で、高価なものとなります。また、大半の組織は保護インフラを統合していないため、担当者が対応に追われ、脆弱性が解決されずに残っています。

求められる機能とは？この問題を解決するには、使いやすく配備が簡単で、コスト効率の良い高度な検出機能が必要です：McAfee® Cloud Threat Detection。この新しいサービスは、既存のMcAfeeソリューションのプラグインとして機能し、高度なマルウェアや回避技術を駆使する脅威を検出します。クラウド サービスとして提供されるので、大量の計算リソースを必要とする最新の分析技術も簡単に利用することができます。検出能力を強化するだけでなく、既存のセキュリティ対策を最適化することもできます。

検出と保護の統合

McAfeeのソリューションは最前線の防衛ラインとして、列挙やレピュテーションなどの高度なツールを利用して既知のマルウェアやマルウェアの可能性のあるコードを識別します。不正なファイルとして確定できない場合には、クラウドに送信され、より詳しい分析が実行されます。

回避技術を駆使する新しいマルウェアの阻止

McAfee Cloud Threat Detectionでは、静的分析エンジンを使用してファイルの詳細情報を抽出します。様々なファイルタイプに対応しているので、グレー ファイルの分析に必要なコンテキスト情報を収集し、不正なファイルと正常なファイルを効率的に識別します。また、サンドボックス環境でファイルを実行して動作分析を行います。マルウェアが実行した処理はすべて記録され、不正な意図がないかどうか評価されます。ファイルがランダムなフォルダーを生成し、そこに新しいファイルを書き込み、元のファイルを削除していないかどうか。Google、Amazon、Facebookなどの既知のサイトへのトラフィックを装い、未知または不審なURLに誘導していないかどうか。これらは、McAfee Cloud Threat Detectionサービスが不明なファイルの分類で使用する動作分析の一例です。このサービスはメタデータ、URL、ファイル名、フォルダーの場所などの情報を抽出します。他のコンピューターが感染していないかどうかを調査できるように、これらの情報をユーザーに戻します。

機械学習の利用

分析サイクルではビッグデータや機械学習を利用しています。これらの機能は、McAfee Labsが管理し、調整しています。クラウド上のビッグデータ システムでは、25年以上に渡って蓄積されたデータと20億個のファイルを使用して分類モデルの構築と調整が行われています。また、進行中の研究結果や調査結果も機械学習に反映されます。マルウェア技術や動作の変化や調査の進展に合わせて、このモデルは進化していきます。

正確性を重視

経験上、誤検知や非検知は大きな問題となることが分かっています。このため、弊社で使用しているシステムでは、信頼できる診断を適時に行えるように、最も重要なシステム ファイルと署名用の証明書に対して抑制と均衡を重視しています。高度な分析で新たな脅威を検出しながら、マルウェア、動作、コンテキスト属性を相互に参照して関連付け、誤検知を最小限に抑えています。これは、クラウド上で分析と様々なマルウェア対策リソースを使用する利点の一つです。

検出とアクション

McAfee Cloud Threat Detectionは、その都度、マシンの隔離や類似した攻撃を阻止する対策の有効化などのポリシーを施行する元のシステムにも通知を行います。詳しい調査や攻撃後の対応に役立つ詳細なインジケータ(IoC)を提供します。McAfee Global Threat Intelligence (McAfee GTI) のレピュテーションを更新し、McAfee GTI対応のソリューションを使用しているすべての組織の保護を強化します。手動による調査によって、アナリストは、簡単に単発の分析ファイルを更新できます。

手頃な価格で迅速な対応が可能な小規模ビジネス向けのソリューション

クラウド ベースのサービスのため、統合されたMcAfee製品から暗号化された共有キーを入力するだけで利用できます。迅速なプロビジョニングが可能です。分散システムの場合、データセンターにトラフィックを戻す必要はありません。クラウドに送信するだけで完了します。弊社の専門家が継続的に保守を行い、更新とアップグレードを実行します。McAfeeの統合されたソリューションは、すべてボリューム単位のサブスクリプション料金で利用できます。事前の設備投資は不要です。

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

統合されるソリューション

- McAfee® ePolicy Orchestrator® Cloud
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Endpoint Protection
- McAfee Web GatewayおよびWeb Gateway Cloud Service

〒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