McAfee Cloud Threat Detection

高度なマルウェアや回避技術を駆使する脅威の検出で Intel Securityのセキュリティ対策を強化

機械学習などの最新の分析技術は、マルウェアの識別やアクションの実行に役立っています。また、これらの技術を応用することで、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、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。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。

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。この条件を満たすのがMcAfee® Cloud Threat Detectionです。この新しいサービスは、既存のIntel® Security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の最適化にも役立ちます。

検出と保護の統合

Intel Security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があるコードを識別しています。不正なファイルとして確定できない場合には、クラウドに送信し、より詳しい分析を実行します。

回避技術を駆使する新しいマルウェアの阻止

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をすべて記録し、不正な意図がないかどうか評価します。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。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、このサービスが抽出したメタデータ、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はよく理解しています。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、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送信し、詳しい調査や攻撃後の対応に役立つ詳細なIoCを提供します。また、McAfee Global Threat Intelligence（GTI）のレピュテーションを更新し、GTI対応のソリューションを使用している組織の保護を強化します。

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、クラウドに送信するだけで、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。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。ボリューム単位のサブスクリプション料金で利用できるので、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。

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