McAfee Network Threat Behavior Analysis

ネットワーク動作と脅威を完全に可視化

McAfee® Network Threat Behavior Analysis は、McAfee の製品サービスの一部である McAfee Network Security Platform に統合されたコンポーネントです。ネットワーク インフラの状況をリアルタイムで把握し、脅威対策を管理できます。スイッチとルーターからのトラフィックを分析することによって、McAfee Network Threat Behavior Analysis はネットワーク上の危険な動作を特定して、ステルス型攻撃を効果的に防ぐことができます。ネットワーク レベルの脅威を評価し、ネットワーク要素の全体的な動作を識別します。マルウェア、ゼロデイ攻撃、ボットネット、ワームなど、疑いのあるアノマリまたは攻撃の種類を迅速に検知します。また、McAfee Network Threat Behavior Analysis はシグネチャなしでマルウェアを特定するリアルタイムのエミュレーション エンジンを含む McAfee Network Security Platform の一部の高度なエンジンが含まれています。

現代のステルス型攻撃に対応する高度な可視性

従来の検出方法を回避し、ネットワークに多大な被害をもたらす高度なステルス型攻撃が増えています。McAfee Network Threat Behavior Analysis は、スイッチとルーターからのネットワーク トラフィックを分析して異常な動作を監視し、報告します。これにより、ネットワークへの攻撃を検知し、迅速に対応することができます。

McAfee Network Threat Behavior Analysis アプライアンスは NetFlow と JFlow データを活用して、侵入防止システム（IPS）の典型的な境界を越えて脅威を検出します。クアッドコア プロセッサー、RAID ディスク アレイ、ギガビット イーサネット接続を完備したアプライアンスです。また、オフライン ストレージ エリア ネットワーク（SAN）接続を提供します。独立したフロー能力で、大量のネットワーク トラフィックを処理し、トラフィックの分析を迅速化できます。

ネットワークの優れた可視性と分析

McAfee Network Threat Behavior Analysis があれば、ネットワーク上のアプリケーションとプロトコルに関する豊富な情報を利用して判断を下せます。異常なネットワーク動作を監視および報告し、動作に基づいたアルゴリズムによって脅威を識別します。ホストとアプリケーションの動作を分析することによって、ゼロデイ攻撃、スパム、

主な特長

ネットワークを保護する可視性

- ネットワークのトラフィック解析により、異常なネットワーク動作を監視および報告
- プロアクティブで、動作に基づいた脅威検出
- 未知の脅威の効果的な検出
- ゼロデイ、スパム、ボットネット、偵察攻撃などのアノマリ検出

包括的なマルウェア対策

- 不正なファイルのリアルタイム エミュレーションでマルウェアを阻止
- ボットネット活動検出のためのネットワーク全体の高度な相関分析
- エンドポイント情報と、ネットワーク フローおよびイベントの相関関係

ボットネット、および偵察攻撃のアノマリ検出を行います。包括的なフロー分析で、未承認のアプリケーションの使用状況を確認し、問題のあるネットワーク セグメントを特定します。

マルウェアの蔓延を防止

McAfee Network Threat Behavior Analysis は McAfee Network Security Platform と連携して、高度な検査と不審なファイルのブロックを行うリアルタイム エミュレーションを提供します。リアルタイム エミュレーション エンジンは不審なファイルを検出し、不正な動作をブロックします。複数の IPS とネットワーク デバイス間の高度な相関分析により、McAfee Network Threat Behavior Analysis は伝統的なシグネチャ ベースの防御を回避するステルス型のボットネットを発見します。McAfee Endpoint Intelligence Agent を使用して、正当なネットワーク トラフィックを装った不正なトラフィックを送信する、感染エンドポイントを検出して制御します。レピュテーションに基づくエンドポイント活動分析により、データ侵害を制限して、マルウェアの蔓延を防ぎます。

セキュリティ操作を簡素化し、コストを削減

McAfee Network Threat Behavior Analysis は、費用対効果の高いセキュリティ管理に必要となる実用的な洞察を提供します。アプライアンスは、インシデントの対応時間を短縮し、ネットワークのパフォーマンスを効率化すると同時に、ネットワークの脅威や侵害によって業務が中断されることを防止します。

追加機能

- McAfee Global Threat Intelligence（McAfee GTI）との統合によるセキュリティ強化
- 費用対効果の高い実装のための仮想版
- McAfee ePolicy Orchestrator®（McAfee ePO™）、McAfee Enterprise Security Manager、および McAfee Vulnerability Manager との統合により強化された可視性と相関分析
- ネットワーク トラフィックの簡単な整理と分析
- フローごとのメタデータ（アプリ ID、ファイル、URL）ダッシュボード
- 包括的な隔離オプションでセキュリティ体制を向上
- 詳細なホストの脅威要素の評価による外部ホストの可視性
- Cisco と Juniper のスイッチおよびルーター（NetFlow v5 と v9、JFlow v5 と v9）との互換性

	NTBA T-600	NTBA T-1200
仕様		
1秒あたりのフロー	最大60,000	最大100,000
Cisco NetFlow	v5とv9	v5とv9
Juniper JFlow	v5とv9	v5とv9
プロセッサー	Xeon E5-2658 x1	Xeon E5-2658 x2
メモリー	46 GB	96 GB
使用可能なストレージ	4.4 TB/Raid 10	8.8 TB/Raid 10
ネットワーク インターフェース	銅線（10/100/1,000）x4	銅線（10/100/1,000）x4
環境		
フォーム ファクタ	1U	2U
幅	438 mm	438 mm
奥行	709.37 mm	707.8 mm
高さ	43.2 mm	87.6 mm
最大重量	14.96 kg	21.6 kg
推定インレット電源使用率（最悪のシナリオ）	402 W	667 W
冗長電源	750 W	750 W
システム冷却要件（BTU/時間）	1370 BTU/時	2280 BTU/時
動作温度	+10°C～+35°C（変化率が1時間あたり10°Cを超えないように）	

仮想 NTBA 仕様	T-VM	T-100VM	T-200VM
推奨RAM	16 GB	8 GB	16 GB
推奨CPU	4	4	4
1秒あたりのフロー	最大25,000 fps	最大10,000 fps	最大25,000 fps

〒 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

60839ds_ntba_0214B
2014 年 2 月