データシート

McAfee Virtual Network Security Platform

クラウド ネットワークを狙う脅威を確実に阻止

McAfee® Virtual Network Security Platformは、プライベート クラウドとパブリック クラウド固有の要件を満たすネットワーク脅威/侵入防止システム（IPS）ソリューションです。クラウド アーキテクチャに侵入する巧妙な脅威を正確に検知し、迅速にブロックします。コンプライアンスを維持し、確実なクラウド セキュリティを実施できます。このソリューションは、シグネチャレスの検知、インライン エミュレーション、シグネチャを利用した脆弱性の修復、Amazon Web Services（AWS）やネットワーク仮想化のサポートなど、高度な技術を搭載しています。効率的なワークフローが用意され、複数の統合オプションと分かりやすいライセンス体系が用意されているため、複雑なクラウド アーキテクチャでも、セキュリティの管理と拡張を簡単に行うことができます。

高度なセキュリティ技術でパブリック クラウドを保護

パブリック クラウドは利便性が高く、導入でコストを削減するだけでなく、設備投資型から運用コスト型への転換を図ることができます。しかし、新しい次元のリスクも存在します。どこからでもアクセスできるソフトウェアの脆弱性が悪用され、クラウドが使用不能になったり、重要な情報が盗まれる可能性があります。また、同じサービスを利用している他のテナントに顧客情報が誤って露出する可能性もあります。McAfee Virtual Network Security Platformは、主要なパブリック クラウド サービスであるAWSにも対応し、インターネット ゲートウェイを通過するデータだけでなく、データセンター内部で転送されるデータに対しても脅威の可視化を実現します。この侵入防止システム（IPS）プラットフォームにより、パブリック クラウド アーキテクチャでセキュリティ コンプライアンスを維持することができます。

仮想化環境の保護

プライベート クラウドやパブリック クラウドなど、仮想インフラを採用する企業が急速に増えています。仮想環境では、物理的なサーバーが複数の仮想マシン（VM）を同時にホスティングし、実行しています。また、仮想化されたワークロード全体がホスティングされている場合もあります。VM間の通信でワークロードの移行、複製、バックアップが迅速に行われるため、プライベート/パブリック クラウドやSDDC内部で大量のトラフィックが発生しています。ネットワークの仮想化で、トラフィック フローの柔軟性が増し、予測不能な状態

主な特長

最高の高度脅威対策

- シグネチャを使用しない高度なマルウェア分析
- クロスサイト スクリプティングとSQLインジェクションの阻止
- ボットネット コールバックとマルウェアを検出する高度な機能
- 動作分析と分散サービス拒否攻撃（DDoS）対策
- McAfee Advanced Threat Defenseとの統合
- IPSと侵入検出システム（IDS）の配備
- VMware ESXの常時保護 ― McAfee Virtual Network Security Platform ソリューション

クラウドレディのアーキテクチャ

- 1つのライセンスで、パブリック クラウドとプライベート クラウドの任意の組み合わせでスループットを共有できます。
- 革新的なAWS検査アプローチにより、パブリック クラウド内のトラフィックを保護します。

になっています。この状況に対応するため、仮想環境を保護するセキュリティ ソリューションは柔軟性と拡張性に優れていなければなりません。また、持続時間の短いVMやワークロードの調整を行うソフトウェア定義ネットワーク（SDN）のプラットフォームでもシームレスに機能しなければなりません。

プライベート クラウドへの対応

McAfee Virtual Network Security Platformは、VMware NSX、OpenStackベースのSDN環境などの主要なプライベート クラウド プラットフォームにシームレスに統合されています。McAfee Virtual Network Security Platformは、VMware NSX.での動作が保証されている唯一の仮想環境専用IPSソリューションです、VMのマイクロセグメンテーションとトラフィックのディープ インスペクションが仮想環境で自動的に行われます。

最高の脅威対策

McAfee Virtual Network Security Platformは、次世代の検査アーキテクチャをベースにし、仮想ネットワークのトラフィックを詳細に検査します。完全なプロトコル分析、脅威レピュテーション、動作分析、高度なマルウェア分析などの調査技術により、ネットワーク上の既知の脅威とゼロデイ攻撃を検出し、被害を未然に防ぎます。

単独のマルウェア検出技術だけではすべての攻撃を防ぐことはできません。McAfee Virtual Network Security Platformは複数のシグネチャを多層的に利用します。また、シグネチャを使用しない検出エンジンでクラウドへのマルウェアの侵入を防ぎます。ブラウザー、JavaScript、Adobeファイルのインライン エミュレーション、ボットネットとマルウェアのコールバック検出、挙動によるDDoS検出、クロスサイト スクリプティングやSQLインジェクションなどの高度攻撃の阻止など、様々な検査技術を搭載しています。また、McAfee Virtual Network Security Platformは、詳細な動作分析を行うMcAfee Advanced Threat Defenseとの統合により、ステルス性の高い脅威を識別し、ブロックします。McAfee Advanced Threat Defenseは、静的なコード分析（マルウェア サンドボックス）と機械学習を組み合わせて、回避技術を駆使したゼロデイ脅威やランサムウェアの検出能力を強化しています。

クラウドでのライセンス共有も簡単に

自社のITリソースとインフラを複数のクラウドやプラットフォームに分散する企業が増えています。古いアプリケーションを利用する、特定のベンダーへの依存度を下げる、システムに冗長性を持たせる、コストを削減するなど、その理由は様々です。仮想環境のセキュリティ ソリューションは、ライセンスが複雑で高額になる場合もあります。プライベート クラウドとパブリック クラウドでライセンスが別であったり、SDNプラットフォームの種類ごとにライセンスが必要になることもあります。

McAfeeは、クラウド ライセンス共有という新しい概念を導入し、ライセンス体系を簡素化しました。これにより、パブリック クラウドとプライベート クラウドのプラットフォームをどのように組み合わせても、McAfee Virtual Network Security Platformのスループットとライセンスを共有できます。クラウド ライセンス共有でセキュリティも向上します。手間のかかる調達手順を踏むことなく、クラウド内でトラフィックの保護と仮想ワークロードのマイクロセグメンテーションを迅速に行うことができます。

優れたワークフローと分析機能

巧妙な高度脅威も簡単に検出し、ブロックできます。McAfee Virtual Network Security Platformは高度な分析機能を搭載しています。また、別のセキュリティ ソリューションと統合することで、ネットワーク脅威を検知・回避する包括的なプラットフォームを構築できます。

- VMware NSXとOpenStackベースのSDN環境に対応し、プライベート クラウドのワークロード間でのトラフィックのマイクロセグメンテーションと検査を自動的に行います。
- VMwareとの統合により、ダッシュボードからVMに隔離機能を実行できます。
- 1つの集中管理コンソールで、物理センサー、仮想センサー、オンプレミス、クラウドを保護できます。

インテリジェントなセキュリティ管理

- 1つのコンソールでオンプレミスとクラウドのセンサーを管理
- 高度なアラート相関と優先度の設定
- マルウェアの検査情報を表示するダッシュボード
- 事前定義の検査ワークフロー
- 拡張性に優れたWebベースの管理機能

可視性と制御

- アプリケーションの識別
- ユーザーの識別
- デバイスの識別
- AWS内のすべてのVMの保護状態を把握

最近の脅威は大量のアラートを生成します。この中から重要な兆候を見つけ出し、追跡することは容易ではありません。個々の情報を短時間で関連付け、分析できなければ、脅威を未然に防ぐことはできません。McAfee Virtual Network Security Platformの高度な分析機能と実用的なワークフローにより、複数のIPSアラートから1つの有益なイベントが生成されるので、関連する有益な情報をすぐに取得することができます。

集中管理とリアルタイム制御

1つのMcAfee Network Security Managerアプライアンスで、Webベースの集中管理を簡単に行うことができます。最先端のコンソールと洗練されたグラフィカル ユーザー インターフェースにより、リアルタイムなデータで管理できます。1つのコンソールで物理ネットワーク、プライベート クラウド、パブリック クラウドにあるMcAfee Network Security PlatformアプライアンスとMcAfee Network Threat Behavior Analysisアプライアンスの管理、設定、モニタリングを簡単に行うことができます。分かりやすいWebベースの管理インターフェースにより、単体のデバイスだけでなく、広範囲に分散したミッション クリティカルなクラスターを管理できます。また、VMware ESXサーバーやAWS内にMcAfee Network Security Managerを仮想インスタンスとして配備することもできます。

高可用性と障害時復旧

McAfee Network Security Managerは、アクティブなコントローラーとスタンバイ状態のコントローラーを判別します。アクティブなコントローラーが使用不能になると、スタンバイ状態のコントローラーがアクティブになります。AWS環境では、このようなコントローラーの高可用性（HA）が用意され、常に1つのコントローラーが有効で接続可能な状態になっています。スタンバイ状態のMcAfee Network Security Managerは、AWS環境に障害時復旧機能を提供します。

McAfee Virtual Network Security Platformは、マネージャーの障害時復旧（MDR）、コントローラーの高可用性（HA）、仮想IPS Sensorの自動スケーリング機能により高可用性を実現しています。これにより、McAfee Virtual Network Security Platformは中断なくシームレスに機能します。MDRソリューションでは、プライマリManagerが停止するとセカンダリManagerに制御が引き継がれます。コントローラーのHAペアでは、1つのコントローラーが常にアクティブになり、接続可能な状態になります。これにより、ネットワークのダウンタイムを回避します。Sensorのインスタンスが停止すると、仮想IPS Sensorの自動スケーリング機能により、新しい仮想IPS Sensorが生成されます。また、ネットワーク トラフィックの増加時には負荷分散が行われます。

統合防御アーキテクチャ

巧妙な攻撃はインフラのギャップ、特に、セキュリティ製品間のギャップを攻めてきます。McAfee Virtual Network Security Platformは、複数のセキュリティ製品を統合し、製品間のギャップを解消する唯一のIPSです。結果として、投資効果を高め、総所有コストを抑えることができます。次のセキュリティ製品と統合が可能です。

- **McAfee ePolicy Orchestrator® (McAfee ePO™):** エンドポイントのすべてのIPSイベントとアラートを完全に可視化します。
- **McAfee Endpoint Intelligence Agent:** ネットワークとエンドポイントを監視し、データの流出を阻止します。
- **McAfee Enterprise Security Manager:** 詳細なデータを共有し、IPSアラートで隔離を行うことができます。
- **McAfee Threat Intelligence Exchange:** 異なる種類のデバイスで情報を共有できます。
- **McAfee Global Threat Intelligence:** 世界最大規模の包括的なレピュテーション サービスです。

- **McAfee Network Threat Behavior Analysis:** ネットワークの可視性を強化します。
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments（McAfee MOVE）**
- **サードパーティの脆弱性スキャナー:** エンドポイントのリスクを分析します。

追加機能

高度な脅威対策

- McAfee Gateway Anti-Malwareエミュレーション エンジン
- JavaScriptを含むPDFのエミュレーション エンジン（軽量のサンドボックス）
- Adobe Flash動作分析エンジン
- 高度な回避技術の阻止

ボットネット/マルウェア コールバック対策

- ドメイン名サーバー（DNS）/ドメイン生成アルゴリズム（DGA）Fast-Fluxコールバック検出
- DNSシンクホール
- ボットのヒューリスティック検出
- 複数の攻撃を相関分析
- 指令制御サーバーのデータベース

高度な侵入防止

- IPデフラグとTCPストリームの再構築
- マカフィー、ユーザー定義、オープンソースのシグネチャを使用
- ホスト隔離とレート制限
- 仮想環境の検査
- サービス拒否（DoS）/DDoS対策
- しきい値とヒューリスティックによる検出
- ホストベースの接続制限
- 自己学習、プロファイル ベースの検出

McAfee Global Threat Intelligence

- ファイル レピュテーション
- IPレピュテーション
- 位置情報によるアクセス制御
- IPアドレスによるアクセス制御

	センサーの種類1	センサーの種類2	センサーの種類3
プラットフォーム	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
仮想IPS Sensorモデル	IPS-VM100	IPS-VM600	IPS-VM100-VSS[1]
仮想IPS環境の種類	スタンドアロン	スタンドアロン	分散型
VMware NSXのサポート	なし	なし	あり
AWSのサポート	なし	なし	あり
論理CPUコア数[2]	3	4	3
必要なメモリー[3]	4 GB	6 GB	5 GB
仮想センサーの仕様			
最大スループット[4]	最大500 Mbps	最大1 Gbps	最大500 Mbps
同時接続数	200,000	600,000	200,000
1秒当たりの確立接続数	6,000	20,000	6,000
サポートされるUDPフロー	39,168	254,208	39,168
モニタリング ポート ペア数	2	3	1[5]
Sensor当たりの仮想インターフェース（VIDS）	32	100	32
DoSプロファイル	100	300	100
マネジメント ポート	あり	あり	あり
レスポンス ポート	あり	あり	なし
配備モード	VM間の検査、物理環境とVM間での検査、物理環境間での検査、SPANポートの検査		VMware NSXインライン検査

1. 挿入サービスとしてVMware NSX環境でのみ使用した場合
2. VMのリソース要件はリリースによって異なる場合があります。各リリースのドキュメントをご覧ください。
3. 同上
4. 理想的なテスト条件下で1518バイトのUDPパケットを使用して測定
5. 仮想環境との入出力カーネル レイヤーのVMware NSXでの検査

〒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