McAfee Virtual Network Security Platform

クラウド ネットワークを保護する完全な脅威検知と侵入防止

McAfee® Virtual Network Security Platform（McAfee® vNSP）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検出 / 侵入防止システム（IPS）です。クラウド アーキテクチャに侵入する巧妙な脅威を的確に検知し、迅速にブロックします。ワークロードを保護し、コンプライアンスを維持できます。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など、高度な技術を搭載しています。自動スケーリングを実現する効率的なワークフローサポート、柔軟な統合オプション、そして簡略化されたライセンス体系が用意されているため、組織はセキュリティの管理や拡張を容易に行うことができます。また現在のニーズだけでなく将来のニーズにも対応できます。

完全なパブリック クラウド セキュリティ

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、Amazon Web Services（AWS）、Microsoft Azure、Oracle Cloud Infrastructure（OCI）などの主要なパブリック クラウド サービスに対応しています。脅威を完全に可視化し、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、サーバー間で移動するデータ（East-West トラフィック）も保護します。

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 クラウドやソフトウェア定義データセンター（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。

主な特長

- プライベート クラウドとパブリック クラウド（AWS、Azure、OCI）を保護する包括的なセキュリティ
- インライン IPS/ 侵入検知システム (IDS) 運用モード
- East-West トラフィック保護
- 統一ポリシーおよび管理ワークフロー
- 既知の脅威だけでなく、未知の脅威も阻止する高度な検査技術
- 高可用性、障害時復旧、負荷分散
- クラウド ライセンスの共有で、プライベート クラウドとパブリック クラウドに柔軟にアクセス
- 他の McAfee ポートフォリオとの統合で、デバイスからクラウドまでを網羅
- AWS Marketplace で使用可能
- Azure Marketplace で使用可能

McAfee とつながる

プライベート クラウドへの対応

McAfee Virtual Network Security Platform は、VMware ESX サーバー上の仮想アプライアンスとして配備し、プライベートクラウド インフラストラクチャ内の仮想ネットワークを保護することができます。Open Virtualization Format (OVF) イメージとして使用可能な仮想アプライアンスは、特に ESX ホスト上の VM 間を流れるトラフィックだけでなく、異なる ESX ホストや物理ネットワークを通過するトラフィックも検査することができます。

高度な脅威対策

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未知の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。そしてブラウザー、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、行動ベースの分散型サービス拒否 (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な攻撃を阻止する様々な検査技術を搭載しています。

McAfee Virtual Network Security Platform は、McAfee® Advanced Threat Defense との統合により、ステルス性の高いファイルを識別し、ブロックします。一方、ブロックされたファイルに対しては行動分析がおこなわれます。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機能を強化しています。McAfee では、マルウェア対策でネイティブの Snort シグネチャもサポートしています。

柔軟なクラウド ライセンス共有

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があります。ほとんどのベンダーでプライベート クラウドとパブリック クラウドの種類ごとにライセンスが必要になるためです。

McAfee はクラウド ライセンス共有によりライセンス体系を簡略化し、コストを抑えます。これによりさまざまな組織がパブリッククラウドとプライベートクラウドのどのような組み合わせでも McAfee Virtual Network Security Platform ライセンスを共有することができます。クラウド ライセンス共有で柔軟性だけでなく、セキュリティも向上します。複雑なライセンスを管理したり、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

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。対応に手間取れば、実際の脅威を見逃してしまうこともあります。McAfee Virtual Network Security Platform には、高度な分析機能と有益なワークフローが搭載されています。複数の IPS アラートが相関分析されて 1 つの有益なイベントとして提供されるため、関連情報を迅速に把握できます。また、他の McAfee セキュリティ ソリューションとの統合により、ネットワークの脅威を検知・回避する真に包括的なプラットフォームを構築できます。

統一ポリシーおよび管理ワークフロー

VMware ESX サーバーや、AWS/Azure/OCI 環境に McAfee® Network Security Manager を仮想インスタンスとして配備することができます。これにより、ワークロードがクラウド プラットフォームに移行するため、セキュリティ管理者はハイブリットデータセンター全体で一貫したオンプレミスのセキュリティ プロファイルの拡張が可能となり、一元的な管理コンソールとワークフローを使って管理できるようになります。McAfee Virtual Network Security Platform は AWS Identity and Access Management（IAM）に対応しています。特定のユーザーとグループの権限に基づいて、AWS サービスとリソースに対するアクセスを簡単かつ安全に管理できます。

高可用性、障害時復旧、負荷分散

McAfee Virtual Network Security Platform は、複数の方法で中断のない管理、保護、パフォーマンスを自動的に提供します。McAfee Network Security Manager は、環境をプロアクティブにモニタリングすることで、高可用性を実現しています。例えば、アクティブ コントローラーが使用できないときに新しいコントローラー インスタンスを起動します。さらに、障害時復旧のために、スタンバイ状態の McAfee Network Security Manager を AWS、Azure、OCI 環境に配備できます。

McAfee Virtual Network Security Platform は、IPS センサー向けに高可用性も提供します。センサーが使用不能になると、自動スケーリング機能により、新しい仮想 IPS センサーがシームレスに生成され、中断のないセキュリティを提供します。ネットワーク トラフィックが増加すると、センサー間で自動的に負荷分散が実行され、最適なパフォーマンスを維持します。また、必要なスループット要件を満たすために、追加のセンサーを自動的に配備できます。

統合セキュリティ

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シームレスに統合する唯一の IPS です。ソリューション間でデータとワークフローを効率的に利用することで、セキュリティを強化し、ROI を増加できます。統合可能な McAfee セキュリティ ソリューションとしては、次のようなものがあります。

- **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
- **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
- **McAfee® Enterprise Security Manager:** 詳細なデータを共有し、IPS アラートで隔離
- **McAfee® Threat Intelligence Exchange:** 異なる種類のデバイスで情報を共有
- **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
- **McAfee® Network Threat Behavior Analysis:** ネットワークの可視性を強化
- **McAfee® Virtual Advanced Threat Defense:** 詳細な調査により、検出を回避する脅威を検知
- **McAfee® Management for Optimized Virtual Environments (McAfee® MOVE):** 仮想環境のウイルス対策ソリューション
- **サードパーティの脆弱性スキャナー :** ホストとエンドポイントのリスクを分析

追加機能

高度な脅威対策

- 高度なマルウェア対策
- ネイティブなインバウンド SSL 検査
- Microsoft Office ファイルの詳細検査
- PDF JavaScript 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
- 様々なシグネチャを使用（McAfee 提供、ユーザー定義、オープンソース）
- ホストの隔離とレート制限
- 仮想環境の検査
- サービス拒否 (DoS)/ 分散サービス拒否（DDoS）対策
- Structured Threat Information eXpression（STIX）のサポートにおける許可 / ブロックリスト
- 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
- Snort シグネチャのネイティブ サポート
- 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
- URL/ ドメイン レピュテーション
- 位置情報によるアクセス制御
- ジオロケーション ベースのアクセス制御

	センサーの種類 1	センサーの種類 2
プラットフォーム	VMware ESX	AWS Azure OCI
仮想 IPS Sensor モデル	IPS-VM600	IPS-VM600-VSS
仮想 IPS 環境の種類	スタンドアロン	分散型
AWS のサポート	いいえ	はい
Azure のサポート	いいえ	はい
OCI サポート	いいえ	はい
論理 CPU コア数	4	4
必要なメモリー	8 GB	8 GB
ストレージ	40 GB	40 GB
仮想センサーの仕様		
最大スループット	最大 1 Gbps	最大 1 Gbps
モニタリング ポート ペア数	3	1（ポート ペアでなくモニタリング ポート）
1 センサー当たりの仮想インターフェース（VIDS）	100	100
DoS プロファイル	300	300
マネジメント ポート	はい	はい
レスポンス ポート	いいえ	いいえ
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/ インライン ポートの検査	

詳細を見る

- Amazon Web Services 仮想ネットワークの保護
- Microsoft Azure 仮想ネットワークの保護

〒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

2021年1月