McAfee Network Security Platform

ほう包括的、インテリジェントで、高度な脅威対策プラットフォーム

McAfee® Network Security Platformは、ネットワーク上の高度なマルウェアを検出し、ブロックする次世代の侵入検知/防止システム（IDPS）です。単なるパターンの比較を超えた高度な検出機能とエミュレーション技術により、ステルス型攻撃を非常に高い精度で検出し、被害を未然に防ぎます。このプラットフォームは、条件の厳しいネットワークでも1台のデバイスで30 Gbpsを超える処理速度に対応できます（スタックで最大で100 Gbpsに対応）。McAfeeの統合ソリューションにより、脅威情報がMcAfee® Global Threat Intelligenceからリアルタイムで提供されます。ユーザー、デバイス、アプリケーションに関するコンテキスト データにより、ネットワークに対する攻撃を迅速に検出し、的確な対応を行うことができます。

ステルス型脅威の阻止

デジタル化の流れはセキュリティを取り巻く環境を劇的に変化させています。クラウド、モビリティ、IoTなど、新しい接続形態が次々に登場し、保護すべき領域に境界はなくなりました。脅威の量は指数関数的に増え、深刻度は急速に増しています。多くの企業がデータ保護の強化に取り組む中、強力なネットワーク セキュリティ戦略が重要な役割を果たすようになっています。従来の検出方法を回避し、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。万全な防御に必要なツールと技術を導入して管理するには多大な費用とリソースが必要になります。大半の企業はこの点が課題となっています。

McAfee Network Security Platformは、インテリジェントな脅威対策と使いやすい管理機能を搭載した統合ネットワーク セキュリティ プラットフォームです。これにより、検出精度が向上し、セキュリティ管理の負担が軽減されます。1つのマルウェア検出技術だけですべての攻撃を防ぐことはできません。McAfee Network Security Platformは複数のシグネチャを多層的に利用します。シグネチャを使用しない検出エンジンも使用します。完全なプロトコル分析、脅威レピュテーション、動作分析などの高度な技術でネットワーク トラフィックを分析し、マルウェアのコールバック、サービス拒否攻撃（DoS）、ゼロデイ攻撃などの高度な脅威を阻止します。

統合セキュリティ

McAfee Network Security Platformは、McAfee® Advanced Threat Defenseの統合により、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、回避技術を駆使する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。McAfee Network Security Platformは、McAfee Global Threat Intelligenceからファイル レピュテーションを取得し、McAfee® ePolicy Orchestrator®とMcAfee® Enterprise

主な特長

- 脅威を迅速に検出してブロックし、アプリケーションとデータを保護
- 環境の変化に対応できる、高性能でスケーラブルなソリューション
- 可視性と統制を一元管理
- シグネチャレスのマルウェア分析を含む高度な検出
- 送受信トラフィックのSSLを復号化し、ネットワーク トラフィックを検査
- 高可用性と障害時復旧
- 仮想アプライアンスも使用可能
- 他のMcAfeeソリューションとの統合でデバイスからクラウドまでを保護

Miercom CERTIFIED SECURE™

McAfeeとつながる

Security Managerを利用して、ネットワーク イベントの相関分析をリアルタイムで行います。これにより、デバイスの詳細、ユーザーの情報、エンドポイント セキュリティの状況、脆弱性評価などの情報を利用し、脅威の状況とビジネスに対するリスク要因を正確に把握します。

パフォーマンスと可用性

McAfee Network Security Platformは、高性能を維持しながら高度なセキュリティを提供します。このソリューションは、シングルパスでプロトコル別の検査アーキテクチャを高度な専用デバイスで実行し、100 Gbpsを超えるトラフィックを検査します。キュリティの設定に関係なく、パフォーマンスを維持できます。他のIPSでは、パフォーマンスよりもセキュリティを重視したポリシーを使用するとスループットが最大で50%低下します。

McAfee Network Security Platformはアクティブ/アクティブとアクティブ/パッシブのステートフル フェールオーバー構成を提供し、高可用性のSLAを実現しています。アプライアンスの性能が低下したり、単独のソリューションが過負荷状態になることはありません。

スケーラブルなハードウェア プラットフォームで投資を保護

McAfee NS7500 および NS9500 シリーズ アプライアンスは柔軟性に優れているため、お客様は今必要なものを購入することができるだけではなく、必要性が生じれば、ソフトウェア ライセンスを通じて簡単にスループットを拡張することができます。McAfee NS9500 アプライアンスは、複数の McAfee NS9500 アプライアンスを加えることでさらに機能を追加できます。

可視性と統制

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選択を行う必要があります。McAfee Network Security Platformは、業界で初めて高度脅威対策とアプリケーション認識を1つのセキュリティ エンジンに統合したIDPSソリューションでした。アプリケーションの利用状況と脅威のアクティビティを関連付けて分析します。たとえば、第7層で実行されている2,000以上のアプリケーションとプロトコルを視覚的に管理し、ネットワークで許可するアプリケーションを選択できます。

McAfee Network Security Platformは、アプリケーションだけでなく、ユーザーとデバイスも識別します。ネットワークの異常動作を識別し、アクティブなボットネットなど、危険なホストとユーザーに優先的に対応できます。

インテリジェントで、スケーラブルなセキュリティ管理

セキュリティに対する投資を無駄にしないため、インテリジェントなネットワーク セキュリティを利用する必要があります。McAfee Network Security Managerの拡張性に優れたWebベースのコンソールを使用すると、2台から数百台のネットワーク セキュリティ アプライアンスを管理できます。分かりやすいワークフローでアラートをすぐに確認できます。セキュリティ ダッシュボードでは、セキュリティと関連性に基づいてイベントの優先度が自動的に設定されます。

追加機能

高度な脅威対策

- 受信SSL（Secure Sockets Layer）の復号化は、エージェントベースの共有キーを使用し、Diffie-Hellman（DH）暗号とElliptic-Curve Diffie–Hellman（ECDH）暗号に対応します。センサーのパフォーマンスに影響を及ぼすことはありません（NSシリーズ用の機能で、特許出願中です）。
- 送信SSL復号化（NSシリーズ）
- McAfee® Gateway Anti-Malwareエミュレーション エンジン
- PDF JavaScriptエミュレーション エンジン
- Adobe Flash動作分析エンジン
- Microsoft Office のファイルに対する詳細検査エンジン
- 高度な回避技術の阻止
- モバイル脅威のレピュテーションとクラウド分析

ボットネット/マルウェア コールバック対策

- DNS/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）
- Snortシグネチャのネイティブ サポート（NSシリーズ）
- STIX（Structured Threat Information eXpression）のサポートで許可リスト/ブロックリストの機能強化（McAfee NS シリーズ）
- ホストの隔離とレート制限
- 仮想環境の検査
- McAfee Advanced Threat Defenseとの統合
- HTTP応答圧縮解除サポート

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、IP および URL のレピュテーション
- アプリケーションとプロトコルのレピュテーション
- 位置情報
- McAfee Global Threat Intelligence のカテゴリに基づく許可リスト

高可用性

- アクティブ/アクティブとアクティブ/パッシブのステートフルフェールオーバー
- 外部フェールオープン（アクティブ）
- 組み込みのフェールオープン

プロトコル トンネリング サポート

- IPv6
- V4-in-V4、V4-in-V6、V6-in-V4、V6-in-V6トンネル
- MPLS
- GRE
- Q-in-QダブルVLAN

McAfee® Network Security Manager

- 多層型の管理（最大1,000台のセンサー）
- ユーザー認証（RADIUS、LDAP）
- 自動フェールオーバー/フェールバック
- 重要な構成データの障害時復旧
- ポリシーを階層的に一元管理
- ダッシュボードにデバイスのメモリー使用率を表示

詳細情報

詳細と物理アプリケーションのオプションについては、McAfee Network Security Platform仕様シートをご覧ください。

IDPS (侵入検知 / 防止システム) に求められる機能の詳細について

〒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