

McAfee Server Security Suite Advanced

ホワイトリスト機能と変更管理を搭載し、物理環境、仮想環境、クラウド環境のサーバーを保護するセキュリティ対策

現代の複雑な IT 環境では、包括的なアプローチなしに、ますます洗練されていく脅威から新しいサーバーやクラウド ワークロードを保護することは困難になってきています。McAfee® Server Security Suite Advanced は、物理環境、仮想環境、パブリック クラウドで一貫したセキュリティを継続的に提供します。包括的なセキュリティには、基礎的なウイルス対策、ファイアウォール、侵入防止、ゼロデイ脅威から保護するためのホワイトリスト機能、および法規制の要件を満たすための変更管理が含まれています。高度な保護により、物理サーバーおよび仮想サーバーのパフォーマンスへの影響を最小限にし、クラウドの動的ワークロードと自動拡張します。

迅速な検出と制御

McAfee Server Security Suite Advanced の主な特長である、ハイブリッド クラウド用 Cloud Workload Discovery があれば、拡大し続けるハイブリッド データセンターでセキュリティギャップを追跡することは必ずしも難しくはありません。ハイブリッド クラウド向けの Cloud Workload Discovery は、VMware、OpenStack、AWS、および Microsoft Azure に対応し、すべてのワークロードとそのプラットフォームの完全な可視化を実現します。脆弱なセキュリティ統制、安全でないファイアウォールや暗号化の設定、脅威の兆候（不審なトラフィックなど）を分析し、より迅速に検出します。McAfee® ePolicy Orchestrator® (McAfee ePO™) ソフトウェアまたは DevOps ツールは、迅速な修復を可能にします。

ユニークなリスク プロファイルとセキュリティ要件のある様々なクラウド ワークロードがあるため、クラウドのセキュリティは、困難になる場合があります。Cloud Workload Discovery のポリシーに基づいた評価なら、このような多様なワークロードが求めるセキュリティ管理と、それらのワークロードが実際に持っているものを正確かつ簡単に比較できるため、十分な保護とコンプライアンスを確保できます。セキュリティ リスクを検出すると、わずか数クリックで完全な保護対策に移動できます。

McAfee ePO の管理コンソールと Cloud Workload Discovery の統合により、組織は物理環境、仮想環境、およびクラウド環境全体でセキュリティで保護されたソリューションを実装するための効果的な管理が可能になります。この統合により、セキュリティ管理者は簡素化したワークフローで単一の管理

主な特長

- エンドポイント、ネットワーク、データ、McAfee のコンプライアンス ソリューションのセキュリティを一元管理できるほか、McAfee ePO ソフトウェアによってサードパーティのソリューションも管理できます
- ハイブリッド クラウド用 Cloud Workload Discovery によって、深い可視性、リスク評価、および修復が可能です
- 高度なホワイトリスト機能を使ったブラックリストと侵入防止を変更管理と組み合わせて、物理サーバーと仮想サーバーをマルウェアから保護します
 - 不要なアプリケーションの実行を防止することにより、未知の脅威から保護します
 - 分散環境とリモートでのシステムレベルの変更を常に監視し、コンプライアンスを維持します
- ローカルのレピュテーション情報とサンドボックス分析により、数秒でゼロデイの未知の脅威をブロックします
- パフォーマンスへの影響は最小限に抑え、物理サーバーと仮想サーバーのセキュリティを最適化します

データシート

プラットフォームを使って、脅威アラートへの対応、ポリシーの実行、セキュリティ問題の識別と解決の時間短縮を行います。

McAfee Server Security Suite Advanced は、DevOps をサポートする動的なクラウド環境が敏捷性のためにセキュリティを犠牲にしないことを保証します。弊社のセキュリティはクラウドワークロードに柔軟に対応し、常に保護されるようにします。プライベートクラウドでの柔軟なプロビジョニングによって、ワークロードの上下に合わせてリソースプールからオフラインスキャンサーバーを自動的に追加または削除できます。AWS と Azure のワークロードの場合、ワークロードの変化に合わせて自動スケールするように、テンプレートレベルでセキュリティを構成できます。

包括的な保護対策

McAfee Server Security Suite Advanced は、物理環境、仮想環境、クラウド環境のサーバーを保護する最も包括的なセキュリティを提供します。さらに、ブラックリスト、ホワイトリスト、および変更管理のユニークな組み合わせと、Windows 32 ビットおよび 64 ビットシステムのメモリ



図 1. Cloud Workload Discovery で持続可能なメリットを実現。

バッファオーバーフロー攻撃への保護は、業界で比類ないものです。このスイートには次の製品が含まれています。

- **McAfee Application Control for Servers:** このホワイトリストソリューションでは、未知のマルウェアや、ゼロデイと高度な脅威から保護するために、承認されたソフトウェアのみをサーバーで実行することを許可します。この一元管理されたホワイトリストソリューションは、動的な信用モデルを使って労力のかかるリスト管理の手間を省きます。
- **McAfee Change Control for Servers:** 分散環境とリモート環境全体でシステムレベルの変更を継続的に検出し、サーベンス オクスリー法やクレジットカード業界のデータセキュリティ基準 (PCI DSS) などの法令規則の遵守に役立ちます。
- **McAfee Endpoint Security 脅威対策:** ゼロデイ攻撃と高度な攻撃から Microsoft Windows および Linux サーバーを保護する、協調型の拡張可能なフレームワークの一部です。
- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus):** このマルウェア対策ソリューションは、仮想環境用に設計されています。VMware NSX と VMware vCNS 用に調整された、エージェントを使用しないオプションとして、および Microsoft Hyper-V、VMware、KVM、Xen などすべての主要ハイパーバイザーで展開できるマルチプラットフォーム対応のオプションとして利用可能です。
- **McAfee Host Intrusion Prevention for Server:** サーバー上のコードの動作を監視し、不審な活動がないかイベントを分析することによって、複雑なセキュリティの脅威からビジネスを保護します。

データシート

- **McAfee Endpoint Security ファイアウォール**: ネットワークとインターネットのトラフィックを監視し、不審な通信を遮断します。

McAfee Server Security Suite Advanced は、別売の追加モジュールである McAfee Threat Intelligence Exchange からのローカル データを使って、McAfee Global Threat Intelligence (McAfee GTI) からのグローバル レピュテーション情報を強化し、増加し続けるユニークなマルウェアサンプルを瞬時に特定および阻止できます。McAfee Threat Intelligence Exchange を使ってスイートのソリューションは McAfee Advanced Threat Defense と連携し、サンドボックスで未知のアプリケーションの動作を動的に分析して、すべてのエンドポイントを新たに検出されたマルウェアから自動的に保護します。

McAfee は、Rapid7 と提携して脆弱性管理を行います。Rapid7 の Nexpose ソリューションは、脆弱性を検出および優先順位付けし、露出が修復されたことを確認します。

パフォーマンスへの影響は最小限

多くの企業においてセキュリティは優先事項であるものの、一部の企業はパフォーマンスへの影響を懸念してサーバーの保護を促進させるのを躊躇しています。McAfee Server Security Suite Advanced なら、マルウェアのスキャン中ですらパフォーマンスを犠牲にせず、物理サーバーと仮想サーバーを保護できます。

多くのマルウェア対策製品とは異なり、McAfee Endpoint Security と McAfee MOVE AntiVirus はコンピューティングリソースに多大な負荷を与えません。McAfee Endpoint Security は高速スキャンを行い、他のマルウェア対策製品よりも優れた保護を実現しながら CPU とメモリの使用量を最適化します。McAfee MOVE AntiVirus は仮想マシンのマルウェア スキャンをメモリと処理への影響が少ない迅速な保護にオフロードします。オンアクセス スキャンとオンデマンド スキャンに個別のポリシーを設けることで、パフォーマンスの動きとセキュリティをより詳細に制御できます。

サーバー セキュリティとビジネスの最適化

仮想化とクラウド コンピューティングが持つ様々な可能性を実現するには、これらの環境を適切に保護しなければなりません。弊社が提供するサーバー セキュリティソリューションは企業の成長をサポートします。物理環境、仮想環境、またはクラウド環境のいずれであれ、ますます動的になる環境でサーバーとクラウド ワークロードを保護する一連のソリューションを提供しています。

データシート

機能	利点
単一コンソールでの管理	<ul style="list-style-type: none">物理環境、仮想環境、およびクラウド環境を一元管理することで、すべてのプラットフォームでのポリシーの管理、展開、可視性、およびセキュリティ管理を含め、セキュリティをより詳細に制御できます。操作が簡単で、作業時間を短縮し、負荷を軽減できます。
迅速な検出と制御	<ul style="list-style-type: none">物理サーバーを発見し、VMware vSphere、OpenStack、AWS、Microsoft Azure のワークロードおよびプラットフォームの完全なビューを取得します。クラウドの動的ワークロードに柔軟に対応するセキュリティで常に保護されます。
仮想化のセキュリティ	<ul style="list-style-type: none">仮想インフラのセキュリティを最適化します。パフォーマンスやリソース利用量に影響を及ぼすことはありません。マルチプラットフォーム (すべての主要なハイパーバイザー) または VMware NSX と VMware vCNS のエージェントを使用しない配備を選んで、素晴らしいパフォーマンスと仮想マシン密度を実現します。
パブリック クラウドのセキュリティ	<ul style="list-style-type: none">ファイアウォールと暗号化の設定を含む、AWS と Microsoft Azure 用監査プラットフォームのセキュリティ。AWS のトラフィックとネットワーク脅威の可視性によって完全な保護を確保します。
アプリケーション ホワイトリスト	<ul style="list-style-type: none">従来のサーバー セキュリティに比べて、ホストのパフォーマンスに対する影響は大幅に減少しています。ゼロデイ攻撃や高度な持続型脅威 (APT) を阻止します。シグネチャの更新が必要ないため、迅速な対応が可能です。動的なホワイトリスト機能で動作負荷を軽減します。
変更管理	<ul style="list-style-type: none">重要なシステム ファイル、ディレクトリ、設定に対する未承認の変更をブロックし、ファイルの改ざんを防ぎます。セキュリティ侵害が発生した場合でも、トラブルシューティングが短時間で可能です。サーバーに対する変更をリアルタイムに追跡し、検証します。時間枠、変更元、承認済みの作業チケットに基づいてポリシーを変更します。
コア サーバーの保護	<ul style="list-style-type: none">ゼロデイ攻撃と高度な攻撃から保護するマルウェア対策保護を実装します。McAfee Host Intrusion Prevention System によって、侵入を試みる複合型の脅威から保護します。
ローカル レピュテーション情報	<ul style="list-style-type: none">McAfee Threat Intelligence Exchange (別売追加モジュール) との統合により、数秒でゼロデイの未知の脅威をブロックします。

詳細を見る

McAfee Server Security Suite Advanced を使用する利点についてさらに詳しくは、<http://www.mcafee.com/jp/products/server-security-suite-advanced.aspx> をご覧ください。



〒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

McAfee、McAfee のロゴ、ePolicy Orchestrator、McAfee ePO は米国法人 McAfee, LLC または米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2017 McAfee, LLC. 2719_0317
2017年3月