McAfee Server Security Suite Advanced

ホワイトリスト機能を搭載し、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

主な特長

- すべての物理サーバーと仮想サーバーを検出し、単一のコンソールで管理できます。クラウド環境のサーバーも管理できます。
- ブラックリストとホワイトリストで、物理環境と仮想環境のサーバーをマルウェアから保護します。
  - 動的ホワイトリストにより、未知の脅威を阻止します。McAfee Application Control for Serversにより、未承認のアプリケーションの実行を阻止し、ホストを保護します。
  - 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。

この2、3年、データセンターのストレージ、サーバー、ネットワーク、アプリケーションに大きな変化が起きています。多くのデータセンターがクラウド コンピューティングの導入を開始し、この環境を保護する新たな方法が求められています。組織のIT部門とセキュリティ担当者は、ビジネスの敏捷性とコスト効率を維持するため、物理環境、仮想環境とクラウドを統合管理できるセキュリティを構築する必要があります。Intel® Securityの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包括的なセキュリティです。ホワイトリスト、変更管理など、高度なサーバー セキュリティ機能を提供し、コンプライアンス対応の負担を軽減します。

すべてのワークロードを検出

すべてのワークロードを検出して適切なセキュリティ ポリシーを適用することは簡単なことではありません。弊社のソリューションを利用すると、スキャン レポートで未保護のエンドポイントを検出し、セキュリティ状況を確認できるので、管理作業の負担が軽減されます。McAfee Server Security Suite Advancedは、McAfee® ePolicy Orchestrator®（McAfee ePO™）との統合により、プライベート クラウドとパブリック クラウド上のすべての物理サーバーと仮想サーバーを検出します。また、McAfee Data Center Connector for VMware vSphere、Amazon Web Services、OpenStack、Microsoft Azureも用意されています。これにより、オンプレミスとクラウドの仮想マシンを監視し、適切なセキュリティ ポリシーを適用して強固なセキュリティを維持できます。また、オペレーティング システムのメモリー保護、ハイパーバイザー ホストと仮想マシンの関連付け、仮想マシンの場所などをダッシュボードで確認できます。

サーバーの保護

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対策で、変更管理機能と業界最高のブラックリスト/ホワイトリスト技術を搭載しています。

intel Security

主な特長（続き）

- McAfee MOVE AntiVirusにより、最適化された仮想化セキュリティを実現します。
- McAfee Data Center Connector for VMware vSphere、Amazon Web Services、OpenStack、Microsoft Azureにより、プライベート クラウドとパブリック クラウドにあるすべての仮想マシンのセキュリティを確認できます。

McAfee Server Security Suite AdvancedのMcAfee Application Control for Serversは、承認されたソフトウェアだけにサーバー上での実行を許可するホワイトリスト ソリューションです。このソリューションは、ホワイトリストを一元管理し、動的な信用モデルと革新的なセキュリティ機能により未承認のアプリケーションをブロックし、高度な持続型脅威を阻止します。ホワイトリストではシグネチャの更新が不要なため、脅威対策のホストへの影響が大幅に減少しています。

このスイートはコア サーバーの保護対策として、McAfee VirusScan® Enterpriseなど、Microsoft WindowsサーバーとLinuxサーバーを保護する従来のマルウェア対策を搭載しています。このマルウェア対策は、ゼロデイ エクスプロイトと検出回避技術に対するNSS Labsの性能評価で最高の結果を残しています。従来のマルウェア対策だけでなく、仮想環境に特化したソリューションも用意されています。McAfee Management for Optimized Virtual Environments (MOVE) AntiVirusは、仮想環境用に最適化されたウイルス対策で、大規模な環境でもパフォーマンスに影響を及ぼすことはありません。また、主要なハイパーバイザーをすべてサポートしています。McAfee MOVE AntiVirusはエージェントレスで機能し、VMware環境だけでなく、KVM、Microsoft Hyper-V、VMware、Xenベースのハイパーバイザー環境にも配備できます。

ウイルス対策は重要なセキュリティ対策ですが、高度な脅威を阻止するには別のソリューションも必要になります。McAfee Host Intrusion Preventionは、侵入を試みる複合型の脅威を阻止し、ビジネスを保護します。

クラウドへの展開

クラウドに移行すると、新しいワークロードに適切なセキュリティ ポリシーを適用するのが非常に難しくなります。マカフィーのソリューションを使用すると、プライベート クラウドとパブリック クラウド上で実行中の仮想マシンと停止している仮想マシンを自動的に検出できます。McAfee ePOプラットフォームでパブリック クラウド アカウントを登録すると、適切なセキュリティ ポリシーで仮想マシンが自動的に保護されます。また、マカフィーのデータセンター セキュリティのダッシュボードでは、プライベート クラウドとパブリック クラウドのセキュリティ状況を確認し、インシデントに対応できます。

サーバー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。マカフィーのソリューションは、柔軟性を維持しながら物理環境、仮想環境、クラウド環境のサーバーを保護します。McAfee Server Security Suite Advancedは、高度なソリューションで物理環境、仮想環境、クラウド環境のサーバーを保護し、組織全体のセキュリティ状況を強化します。

McAfee Server Security Suite Advancedの詳細については、次のサイトをご覧ください。

http://www.mcafee.com/jp/products/server-security-suite-advanced.aspx

機能	利点
アプリケーション ホワイトリスト	• 従来のエンドポイント 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を使用するので、従来のホワイトリストに比べると、オーバーヘッドが少なくなっています。
変更管理	• 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を短時間で行うことができます。 • 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。 • 突発的な変更や未承認の変更による影響を最小限に抑えます。
単一コンソールでの管理	• 物理サーバーと仮想サーバーを1つのウィンドウで管理できます。プライベート クラウドとパブリック クラウドも同時に管理できるので、セキュリティの可視性が強化されます。 • 操作が簡単になるため、管理作業の時間を短縮し、負荷を軽減できます。 • 必要なサーバー フットプリントが小さくなるため、ハードウェアのコストを抑えることができます。
コア サーバーの保護	• 物理サーバーに対してNSS Labsが実施したゼロデイ エクスプロイトと検出回避技術の性能評価[1]で最高の評価を得ています。 • Host Intrusion Preventionが、侵入を試みる複合型脅威を阻止し、ビジネスを保護します。
仮想化のセキュリティ	• 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に影響を及ぼすことはありません。 • データセンターの複数のハイパーバイザーに対応しています。すべてのハイパーバイザーのセキュリティ状況を確認できます。 • VMware環境にエージェントレスで配備されるので、VMのパフォーマンスを向上します。
プライベート クラウドとパブリック クラウド上にある仮想マシンの完全な可視性	• 物理サーバーだけでなく、VMware vSphere、Amazon AWS、OpenStack、Microsoft Azure環境のハイパーバイザーと仮想マシンも検出できます。保護が必要な対象をすべて把握できます。 • プロビジョニングが完了した仮想マシンを検出すると、セキュリティ ポリシーを自動的に適用して保護するため、適切なセキュリティ状態を維持できます。

1. NSS Labs, Inc.による保護対策テスト(2013年)

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒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）FAX 03-5428-1480
西日本支店　〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F
TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F
TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810-0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F
TEL 092-287-9674（代）
www.intelsecurity.com

62337ds_sss-adv_0316