McAfee Cloud Workload Security

ハイブリッド インフラのワークロード保護をより迅速、確実、簡単に

企業のデータセンターは日々進化し、より多くのワークロードがクラウド環境に移行されています。多くの企業がコンテナーやオンプレミスとクラウドを併用するハイブリッド環境を選択しています。この傾向は今後も続くでしょう。この状況で新たなセキュリティ問題が浮き彫りになりました。クラウド環境（プライベート、パブリック）を保護するには、新しいアプローチやツールが必要になります。誤設定、マルウェア、データ侵害に対する包括的なセキュリティ対策で、すべてのクラウド ワークロードの保護を一元的に管理する必要があります。

McAfee® Cloud Workload Security（McAfee® CWS）は、エラスティックなワークロードとコンテナーを自動的に検出し、保護します。高度な保護対策により、セキュリティの盲点をなくし、複数のクラウドを効率的に管理できます。プライベート クラウド、パブリック クラウド、マルチクラウドにワークロードを移行しても1つのポリシーが自動的に適用されるので、サイバーセキュリティ チームはワークロードを効率的に保護することができます。

最新のワークロード セキュリティ: ユースケース

自動検出

管理対象外のワークロード インスタンスやDockerコンテナーが存在すると徹底したセキュリティ管理はできません。攻撃者はこのような隙間を見逃さず、組織への侵入を試みます。McAfee CWSは、Amazon Web Services（AWS）、Microsoft Azure、OpenStack、VMware環境でエラスティックなワークロード インスタンスやDockerコンテナーを検出し、新しいインスタンスを継続的に監視します。1つのビューで環境全体を監視できるので、組織を危険にさらす運用上の盲点やセキュリティの穴をなくすことができます。

ネットワーク トラフィックの分析情報を取得

McAfee CWSは、クラウド ワークロードから提供されるネイティブのネットワーク トラフィックを利用し、McAfee® Global Threat Intelligence（McAfee® GTI）のデータフィードの情報を適用します。これにより、リスク スコア、位置情報、他のネットワーク情報などのプロパティを表示できます。この情報から自動修復アクションを作成し、ワークロードを保護できます。

主な特長

- 手間のかかるポリシー配備を自動化し、エラスティックなワークロード インスタンスの可視性を常に維持することで、セキュリティ オペレーションの盲点をなくします。
- 一元管理とワークフローの自動化により、ハイブリッドなマルチクラウド環境を保護する複雑さを解消します。
- エージェントレスでネットワークの脅威を可視化し、検出します。
- 仮想マシン用に最適化された脅威対策で多層的な保護を実現します。
- Chef、Puppetなどの自動化ツールとの統合で、配備時にパブリック クラウドとプライベート クラウドのワークロードにセキュリティを適用します。

McAfeeとつながる

配備フレームワークへの統合

McAfee CWSは、クラウド ワークロードにMcAfee®エージェントを自動的に配備し、管理する配備スクリプトを作成します。このスクリプトにより、Chef、Puppetなどのツールや他のDevOpsフレームワークと統合し、AWSやMicrosoft Azureなどのクラウド プロバイダーによって実行されるワークロードにMcAfeeエージェントを配備できます。

イベントの統合

McAfee CWSでは、1つのインターフェースでオンプレミスとクラウド環境の様々な対策技術を管理できます。また、AWS GuardDuty、McAfee® Policy Auditor、McAfee® Network Security Platformなどの技術との統合も可能です。

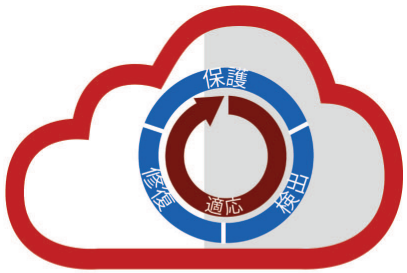
- AWS GuardDutyが識別した未承認の動作を継続的に監視できるので、脅威の可視化が強化されます。この統合により、McAfee CWSのユーザーはMcAfee CWSのコンソールから、EC2インスタンスのネットワーク接続、ポート プローブ、DNS要求などのGuardDutyイベントを確認できます。
- McAfee Policy Auditorは、既知またはユーザー定義の構成監査にエージェントベースの検査を実行します。これにより、HIPAA (Health Insurance Portability and Accountability Act)、PCI-DSS (Payment Card Industry Data Security Standard)、CIS Benchmark (Center for Internet Security Benchmark) などの業界標準への対応状況を確認できます。McAfee CWSは失敗した監査を報告するため、クラウド内のワークロードの構成エラーをすぐに確認できます。
- McAfee Network Security Platformもクラウド セキュリティ プラットフォームの一つで、ハイブリッド環境、AWS、Microsoft Azureなどの環境でネットワーク トラフィックを検査します。ネットワーク トラフィックをパケット レベルで詳細な検査を実行し、不一致を報告したり、McAfee CWS経由で警告を行います。これにより、マルチクラウド環境を一元管理し、問題を修復できます。

ネットワーク セキュリティ ネットワーク グループの適用

McAfee CWSでは、ユーザーや管理者がベースラインとなるセキュリティ グループ ポリシーを作成し、ワークロードで実行されているポリシーの監査を行うことができます。ベースラインからの逸脱や変更が見つかると、McAfee CWSコンソールにアラートが表示され、問題の修復を行うことができます。管理者は、McAfee CWSからネイティブのネットワーク セキュリティ グループを手動で設定し、クラウド ネイティブのセキュリティ グループ ポリシーを直接制御できます。

主な特長 (続き)

- 使いやすい多層型の保護対策で、高度なマルウェアや侵入を阻止します。
- Dockerコネテナーを検出してモニタリングし、マイクロセグメンテーションで保護します。
- ソリューション内から訂正処置を直接実行できます。



Cloud Workload Security

全体的な**可視化**と**コントロール**

McAfee Cloud Workload Securityのメリット: 主な機能と技術

クラウド ネイティブのビルド サポート

McAfee CWSでは、AWS EC2、Microsoft Azure 仮想マシン、OpenStack、VMware vCenterなど、複数のパブリック/クラウド環境を1つのコンソールで管理できます。Amazon Elastic Container Service for Kubernetes (Amazon EKS) とMicrosoft Azure Kubernetes Service (AKS) の新しいクラウド ネイティブのビルド サポートにより、ユーザーをクラウドにインポートし、実行を許可できます。

簡単な統合管理

複数のクラウド環境でも、1つのコンソールですべてのサーバー、仮想サーバー、クラウド ワークロードを管理できます。一貫したセキュリティ ポリシーを適用し、セキュリティを一元管理できます。管理者はMcAfee® ePolicy Orchestrator® (McAfee ePO™) で役割別の複数の権限を作成し、ユーザーの役割をより細かく定義できます。

マクロセグメンテーションによるネットワークの可視化

クラウド ネイティブのネットワーク可視化、優先順位に基づくリスク警告、マイクロセグメンテーションで可視化と制御を行うことで、仮想環境内での脅威の拡散と外部から攻撃を阻止します。1回のクリックでシャットダウンまたは隔離できるので、設定ミスを防ぎ、修復を効率的に行うことができます。

優れた仮想化セキュリティ

McAfee CWSスイートでは、McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus) を使用して、プライベート クラウドの仮想マシンをマルウェアから保護します。基盤となるリソースに影響を及ぼしたり、運用コストが増加することもありません。McAfee MOVE AntiVirusは、専用の仮想マシンにセキュリティをオフロードし、仮想環境のスキャンを最適化します。

ユーザーは、McAfee® Endpoint Security for Serversのマルウェア対策で保護されます。このソリューションは、オンデマンド スキャンなど、多くのリソースを必要とするタスクのスケジュールを自動的に調整し、重要なビジネス プロセスへの影響を回避します。

タグとワークフロー セキュリティの自動化

すべてのワークロードに適切なポリシーを自動的に割り当てます。AWSとAzureのタグ情報をMcAfee ePOにインポートし、これらのタグに基づいてポリシーを割り当てることができます。AWSとMicrosoft Azureの既存のタグをMcAfee ePOのタグと同期し、自動的に管理します。

自動修復

McAfee CWSは、ユーザーが定義したMcAfee ePOのポリシーで保護されていないシステムを検出し、そのシステムがマルウェアやウイルスに感染していると、このシステムを自動的に隔離します。

適応脅威対策

McAfee CWSは、機械学習、アプリケーションの隔離、仮想マシン用に最適化されたマルウェア対策、ホワイトリスト、ファイル整合性モニタリング、マイクロセグメンテーションなどの保護対策を統合し、ランサムウェアや標的型攻撃などの脅威からワークロードを保護します。McAfee® Advanced Threat Protectionは、機械学習を利用した高度な脅威対策により、コードの属性や挙動に基づいて不正なペイロードを特定します。これにより、これまで検出されなかった巧妙な攻撃も識別されます。

アプリケーション制御

アプリケーション ホワイトリストにより、信頼されたアプリケーションにのみ実行を許可し、未承認のペイロードをブロックします。既知の攻撃だけでなく、未知の攻撃も防ぐことができます。McAfee® Application Controlは、ローカルとグローバルの脅威情報に基づいて動的な保護を行います。セキュリティ機能を無効にすることなく、システムを常に最新の状態にしておくことができます。

ファイル整合性モニタリング（FIM）

McAfee®ファイル整合性モニタリングは、マルウェア、ハッカー、悪意のある内部ユーザーによってシステム ファイルとディレクトリが改ざんされていないかどうか継続的な監視を行います。サーバー ワークロードで変更されているファイルの数を通知し、攻撃の発生を警告します。

マルチクラウド環境を適切に保護するセキュリティ

McAfee CWSでは、クラウドのメリットを利用しながら最高のセキュリティ品質を維持できます。複数の保護技術に対応しているので、セキュリティ管理の負担を軽減できます。ビジネスに影響を及ぼすサイバー脅威を阻止し、ビジネスの成長に専念することができます。使用可能なパッケージ オプションと機能は次のとおりです。

機能	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
一元管理（McAfee ePOプラットフォーム）	✓	✓	✓
複数のクラウドに対応（AWS、Microsoft Azure、VMware）	✓	✓	✓
マイクロセグメンテーションによるワークロードとコンテナーの隔離	✓	✓	✓
McAfee MOVE（エージェントレス、マルチプラットフォーム）	✓	✓	✓
サーバーOS（Windows、Linux）を保護するMcAfee Endpoint Security脅威対策	✓	✓	✓
ホスト ベースのファイアウォール	✓	✓	✓
AWSとMicrosoft Azure（セキュリティ グループ）のネイティブ ファイアウォールの管理	✓	✓	✓
ホスト侵入防止とエクスプロイト防止	✓	✓	✓
AWSとMicrosoft Azureのタグ情報をMcAfee ePOにインポート	✓	✓	✓
非対応のワークロードでの自動修復	✓	✓	✓
機械学習を利用した適応脅威対策		✓	✓
ネットワーク トラフィックの可視化とマイクロセグメンテーション		✓	✓
クラウド ネイティブのネットワーク トラフィック分析とMcAfee GTI レピュテーション スコア		✓	✓
McAfee® Virtual Network Security Platform（McAfee® vNSP）の統合		✓	✓
McAfee Application Control 経由でサーバーを動的にホワイトリストに登録			✓
McAfeeファイル整合性モニタリングによる継続的な監査ロギング			✓
McAfee® Change Control for Serversによるファイルとフォルダーの保護			✓

詳細情報

詳細については、**www.mcafee.com/enterprise/ja-jp/products/cloud-workload-security.html**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