McAfee Cloud Workload Security

プライベート クラウドとパブリック クラウドのワークロード保護をより安全、高速、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。セキュリティの盲点をなくし、高度な保護対策を実現します。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、ハイブリッド 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。

リアルタイムでの可視化

自動検出

未確認のワークロード 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 Cloud Workload Securityは、Amazon Web Services（AWS）、Microsoft Azure、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。

最新のワークロード セキュリティ

高度な脅威対策

McAfee Cloud Workload Security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。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できます。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。

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。
- 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。
- 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。
- 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。
- 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

イベントの統合

McAfee Cloud Workload Security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。AWS GuardDutyなどの他社の技術もサポートしています。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 Cloud Workload SecurityのユーザーはMcAfee Cloud Workload Security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 Cloud Workload Securityが検出したトラフィックに一致すると、GuardDutyのネットワーク接続イベントがフローのグラフに関連付けられます。

優れた仮想化セキュリティ

McAfee Cloud Workload Securityは、基盤となるリソースに影響を及ぼすことなく、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。運用コストが増加することもありません。このソリューションのマルウェア対策は、リソースを大量に消費するタスクのスケジュールを自動的に設定します。たとえば、ハイパーバイザーの負荷が過剰でないときにオンデマンド スキャンを実行します。

ネットワー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により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。

ファイル整合性モニタリング（FIM）

FIM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。

アプリケーション管理

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。アプリケーション管理は、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。

簡単な管理

集中管理による一貫性

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。

自動配備

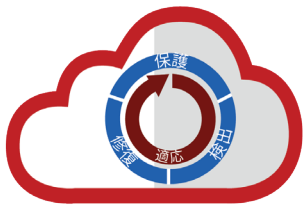
Chef、Puppet、Ansibleなどの自動配備ツールに対応しているので、複数のクラウド環境にセキュリティ技術を自動的に配備できます。

保護範囲の拡大

McAfee Cloud Workload Security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。

主な特長（続き）

- 使いやすい高度なマルウェア対策と侵入防止で多層的な保護を提供します。
- 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。
- ソリューション内から直接訂正処置を実行できます。



Cloud Workload Security

包括的な
可視性と**統制**

機能	Cloud Workload Security Basic	Cloud Workload Security Essentials	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、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	✓	✓	✓
サーバーOS（Windows、Linux）の脅威対策	✓	✓	✓
ホスト侵入防止とエクスプロイト防止	✓	✓	✓
クラウド暗号化の管理	✓	✓	✓
AWSと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	✓	✓	✓
McAfee® Management for Optimized Virtual Environments（エージェントレス/マルチプラットフォーム）	✓	✓	✓
ホスト ベースのファイアウォール	✓	✓	✓
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		✓	✓
Global Threat Intelligence レピュテーション スコアを利用したクラウド ネイティブ ネットワークのトラフィック分析		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
McAfee® Virtual Network Security Platformの統合		✓	✓

詳細情報

詳細は、www.mcafee.com/jp/products/cloud-workload-security.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