McAfee Public Cloud Server Security Suite

AWSとAzureのクラウド ワークロードを保護する包括的なセキュリティ

データセンターからクラウド サーバーに移行する企業が増え、共通の責任モデル[1]の重要性が強く意識されるようになりました。Amazon Web Services（AWS）やMicrosoft Azureなどのパブリック クラウドプロバイダーは境界を保護していますが、コンテンツの保護はユーザーが行わなければなりません。このような先進的な企業が、クラウド戦略のコストを維持しながら、クラウド ワークロードに対するゼロデイ脅威や高度な持続型脅威（APT）を阻止するには何が必要でしょうか。クラウドを採用している企業は次のような課題を抱えています。

- ゼロデイ脅威や高度脅威への対応が難しくなっている。
- 可視化と集中管理が行われていないため、複数のクラウド インフラを保護するのは非常に困難になっている。
- クラウド ワークロードの保護でパフォーマンスの低下が問題になっている。

McAfee® Public Cloud Server Security Suiteは、総合的な脅威対策を継続的に実行し、パフォーマンスに対する影響を最小限に抑えながら、AWSとAzureのワークロードを迅速に検出して管理します。複数のクラウド データセンター、クラウド アカウント、仮想マシン、新しい脅威を検出できます。

主な特長

- AWSとAzureのワークロードに特化
- 迅速な検出
- セキュリティの評価と脅威の修復
- 拡張性の高いセキュリティ
- 包括的な保護対策
- 管理コンソールとしてMcAfee® ePolicy Orchestrator®（McAfee ePO™）を利用
- Chef、Puppet、OpsWorksなどの配備オプション
- コンプライアンスの状況を明示
- McAfeeの他のソリューションとの統合

図1. 1つの管理コンソールで複数のクラウド インフラとMcAfeeの技術を管理できます。

McAfee Public Cloud Server Security Suiteは包括的なセキュリティ対策を提供します。基本的なウイルス対策だけでなく、侵入防止や高度なホワイトリスト機能などにより、ゼロデイ脅威を阻止し、変更を管理してコンプライアンスを維持します。また、暗号化によってデータを保護します。1つのコンソールで複数のクラウドを簡単に管理し、ポリシーを施行できます。Chef、Puppet、OpsWorks DevOpsツールなど、柔軟な配備オプションが用意されているので、シームレスに利用できます。

クラウド インフラと脅威の検出

クラウド インフラと脅威を適切に管理するには、可視性を向上させる必要があります。

- AWS と Azure のクラウド インフラにある仮想ネットワークまたは仮想プライベート クラウド (VPC)、テンプレート、ワークロードをすべて数分で検出します。クラウド インフラを保護するには、クラウド インフラのアカウントに関する詳細情報を取得し、クラウド インフラにアクセスしているユーザーとアクセス対象を確認する必要があります。また、テンプレートと VPC にワークロードが割り当てられる方法を把握し、クラウド インフラに対応するシステム ツリーのスナップショットを取得しなければなりません。

対応プラットフォーム

- Windows Server 2008、2008 R2、2012、2012 R2
- Linux (Red Hat、CentOS、SUSE、Ubuntu、Amazon Linux)

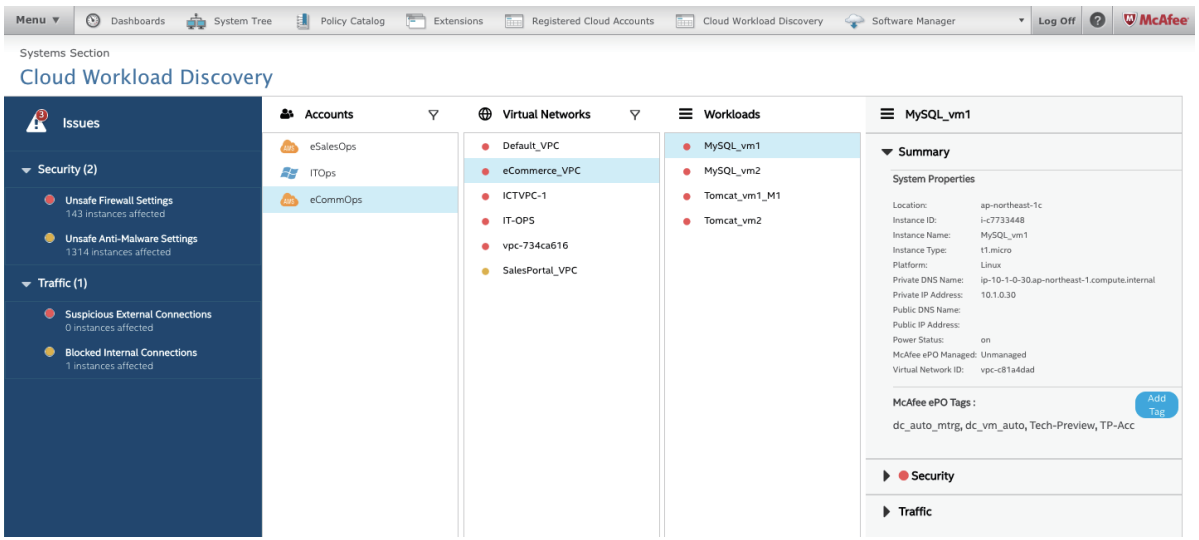

図2. 複数のクラウド インフラと新たな脅威を検出し、監視します。

- 複数のクラウドのセキュリティを 1 つの場所で管理します。セキュリティ統制を向上させるには、攻撃元などの脅威情報を利用する必要があります。
- ワークロードのトラフィックを表示し、情報の流れと外部からのアクセスを管理します。

クラウドの監視とセキュリティ アラートによる迅速な対応

以前にも増して迅速な修復が求められています。このソリューションを使用すると、セキュリティ問題の詳細な分析を迅速に行い、すぐに対策を講じることができます。

- 色別の脅威情報を使用し、緊急度の高い問題を特定し、適切な処置を行うことができます。
- カスタム タグを作成して、組織固有の要件に合わせてワークロードに割り当てることができます。
- セキュリティ問題を抑止する是正処置を行い、ポリシーを適用できます。脅威のレピュテーションを定義し、新たなセキュリティ インシデントからインフラを保護できます。
- カスタム ポリシーでクラウド ファイアウォールを管理し、個々のワークロードまたはワークロードのグループを保護します。AWS セキュリティ グループのポリシーを管理し、1 つ以上のインスタンスのトラフィックを制御できます。
- VPC で発生した不審なトラフィックを識別し、修正処置を行って犯罪者から重要な情報を保護できます。

包括的な脅威対策

McAfee Public Cloud Server Security Suiteでは、1つのエージェントで多層型のセキュリティを実現します。複数のクラウド プラットフォームを1つのコンソールで管理できます。DevOpsなどのツールと一緒に配備できるので、最適な環境を構築することができます。

図3. パブリック クラウドのワークロードを保護する包括的なセキュリティ

機能	利点
Chef、Puppet、AWS OpsWorksの配備オプション	・DevOps対応の配備ツールにより、セキュリティを簡単に配備し、脅威を未然に防ぐことができます。 ・セキュリティをオペレーションに組み込むこともできます。
クラウド ワークロードの検出	・クラウド インフラを可視化し、仮想データセンター、クラウド ワークロード、クラウド ファイアウォールを検出します。 ・セキュリティ ポスチャの評価を自動的に行い、脅威アラートを迅速に通知します。 ・脅威の重大度に基づいてアラートに優先度を設定し、修復作業を迅速に行うことができます。
McAfee ePOの管理コンソールで複数のクラウド インフラのセキュリティを管理	・ハイブリッド環境に対応できます。 ・1つのウィンドウで物理環境、仮想環境、クラウド ワークロードとポリシーを管理できます。 ・McAfeeやパートナーが提供するクラウド/オンプレミス セキュリティ技術を統合できます。 ・セキュリティ プロセスの統合と迅速な対応により、総所有コストを低減できます。
マルウェア対策	・最高のマルウェア対策を利用できます。 ・ウイルス、スパイウェア、ワーム、トロイの木馬などのリスクからシステムとファイルを保護します。 ・マルウェアを検出して駆除するだけでなく、隔離項目を管理するポリシーも簡単に設定できます。
ホスト ファイアウォール	・未承認のアクセスや攻撃からワークロードを保護します。
ホスト侵入防止	・不要または有害なネットワーク トラフィックをブロックし、特許取得済みの技術を利用してゼロデイ攻撃と既知の攻撃を防ぎます。 ・指定したポート、ファイル、共有、レジストリ キー、レジストリ値へのアクセスを制限し、ワークロードに対する望ましくない変更を阻止します。 ・メモリー保護により、不正なプログラムや脅威によるバッファー境界を超えた書き込みや、隣接するメモリーの上書きを阻止します。バッファ オーバーフローが悪用されると、コンピューターで任意のコードが実行される可能性があります。
アプリケーション ホワイトリスト	・シグネチャの更新なしでゼロデイ脅威や高度な持続型脅威を阻止します。 ・動的ホワイトリストにより、信用されたチャネルで追加されたアプリケーションを自動的に承認し、セキュリティの強化と総所有コストの削減を実現します。 ・安全なアプリケーション ホワイトリストと高度なメモリー保護機能でパッチの適用サイクルを短縮します。

機能	利点
ファイル整合性監視	▪ 分散環境やリモート環境でのシステム レベルの変更を常時監視し、検出します。 ▪ 重要なシステム ファイル、ディレクトリ、設定情報に対する不正な変更を阻止し、改ざんを防ぎます。 ▪ ワークロード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。
暗号化の管理	▪ AWS EBSボリュームに保存されたデータをAWS AES（Advanced Encryption Standard）で暗号化します。 ▪ すでにデータが存在するボリュームも簡単に暗号化できます。 ▪ AmazonのKey Management Service（KMS）を統合し、暗号化を行います。

詳細情報

製品ページ:

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

購入は、**AWS Marketplace**をご覧ください。

1. http://www.mcafee.com/us/resources/white-papers/wp-cloud-security-primer-techtarget.pdf

〒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