ホワイトペーパー

McAfee MVISION CNAPP

マルチクラウド セキュリティのシングル プラットフォーム

目次

McAfee MVISION CNAPP

マルチクラウド セキュリティのシングル プラットフォーム

マルチクラウド IaaS（Infrastructure-as-a-Service）の採用とリスク

クラウド プラットフォームを採用する企業が急速に増えています。McAfee® のレポートによると、複数の IaaS プロバイダーを利用していると回答した企業は全体の 76% でした。しかし、実際のクラウドの利用状況のデータを調べてみると、92% が複数のクラウドを利用しており、その数は昨年よりも 18% 増えています。IaaS 環境に存在するデータの性質を考えると、この 16% は大きな意味を持ちます。通常、IaaS 環境にはビジネスに不可欠なアプリケーションが移行され、その多くは顧客向けのアプリです。クラウドを利用する主なメリットは、スケーラブルな IT 環境を迅速かつ柔軟、またエラスティックに実現できる点にあります。しかし、この柔軟性、スケーラビリティ、エラスティックな特長が、複数のクラウド プラットフォームを利用する際のセキュリティに重大な影響を及ぼしています。

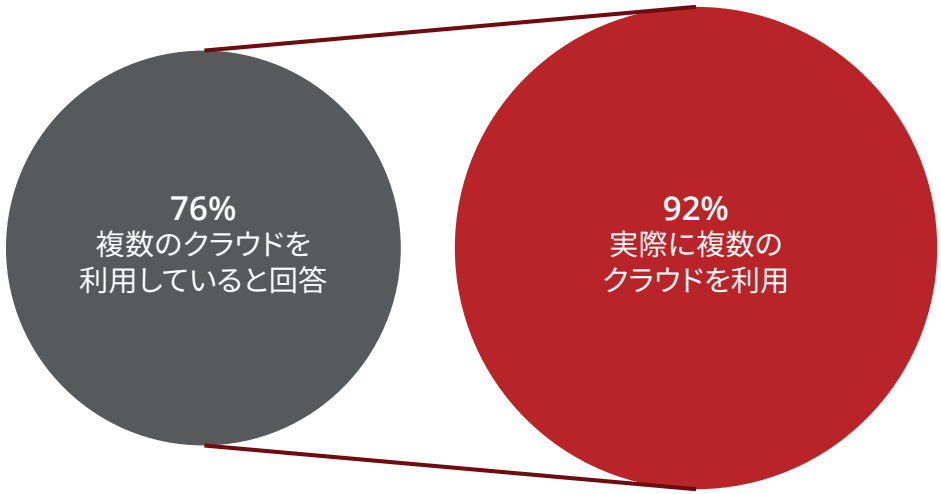

図 1. 複数の IaaS プロバイダーの利用状況

マルチクラウド保護の課題

マルチクラウドを保護するための主な課題は 5 つあります。

セキュリティの一元管理

多くの場合、マルチクラウド環境では複数のセキュリティ管理ツールが使用されています。セキュリティ管理が一元化されていないと、効率的な運用を行うことはできません。構成ミスが起きやすくなり、脅威の早期発見も難しくなります。また、インシデント対応にかかる時間も長くなり、結果として人件費も増加します。

構成のコンプライアンス

多くの組織にとって構成のコンプライアンスも課題となっています。ネットワーク、サーバー、アプリケーション、ユーザー、ストレージの構成についてクラウド サービスのリスクを評価し、特定できる能力は、現在のビジネス環境において必要不可欠な要素です。不適切な構成のクラウド サービスが 1 つあるだけで、会社全体がセキュリティ侵害の被害を被る可能性があります。マルチクラウド戦略の採用は、構成ミスや脆弱性に関するリスクにより、さらに難しいものとなっています。たとえば、毎日数百個（数千ではない）の変更を行っている企業では、クラウド サービスのチェックを継続的に行う必要があります。また、発見された構成ミスは、発見後すぐに修正する必要があります。すでに多くの作業に追われている管理者が解決するのを待っているようでは遅すぎます。

データ セキュリティ

マルチクラウドを採用すると、エンタープライズ データ セキュリティの点で新たなリスクと課題に直面します。たとえば、複数のクラウド サービスとインフラ間で、一貫したデータ セキュリティ ポリシーを使用して会社と顧客のデータを保護しなければなりません。また、1 つのダッシュボードですべてのインシデントを一元管理し、タスクを自動化する必要があります。また、各国の法規制に対応するため、記録を保持しなければなりません。セキュリティ管理を自動化し、マルチクラウドの状況を把握できなければ、コンプライアンス対応は一層難しいものとなります。

DevOps の統合

DevOps により IT 組織の機能が変わりました。IaaS（Infrastructure-as-a-Service）は、業務用や顧客向けのアプリケーションを構築し、ホスティングする標準の IT 環境として様々な規模の企業で利用されています。DevOps は、製品の開発と配布をより安全に、より迅速に行うことを目標としています。DevOps パイプラインの整備は、マルチクラウド戦略を成功させる上で最も重要な部分といえるかもしれません。DevOps はスピードを重視し、非常に短いサイクルで開発を行うことを主眼としています。コードの作成や更新に比べると、コードのレビューに時間がかかることもあります。スピードを重視するあまり、構成ミスや脆弱性、欠陥が修正されないままソフトウェアが公開されることも少なくありません。

クラウド インシデントへの対応

これまで、インシデント対応はオンプレミス環境を中心に考えられてきました。しかし、クラウド環境は多くの点でオンプレミスとは異なります。クラウド インシデントへの対応には多くの課題があります。データをどのように収集、取得、分析し、インシデントの調査を行うかが問題になります。また、インシデント対応における共有責任について理解し、インシデントの可視化を行う必要があります。

マルチクラウドの保護に実績のある McAfee MVISION Cloud

McAfee® MVISION ™は、単一のクラウド ネイティブの施行ポイントを使用して、マルチクラウドの複雑さを解消します。これは、マルチクラウド インフラ間で企業と顧客のデータ、資産、アプリケーションを高度なセキュリティ脅威やサイバー攻撃から保護する包括的なクラウド セキュリティ ソリューションです。

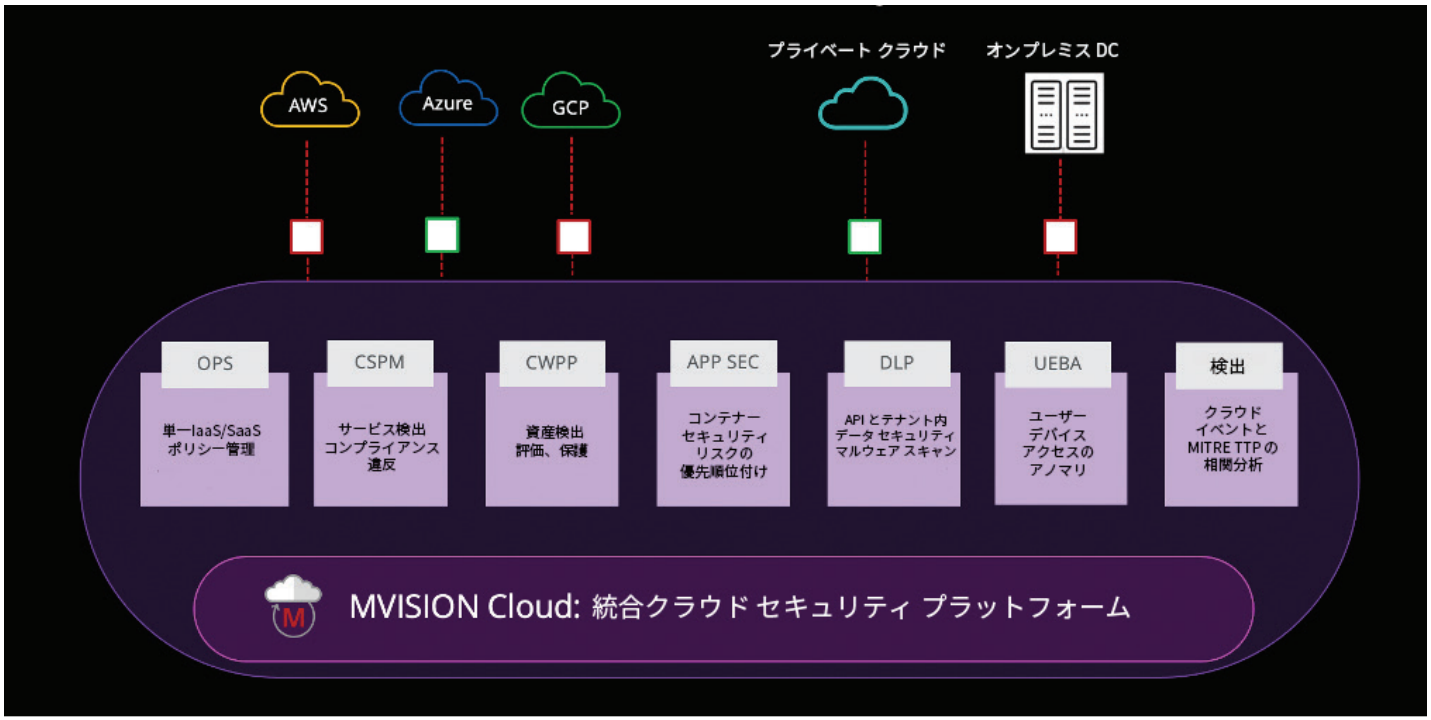

図 2. McAfee MVISION Cloud: マルチクラウド セキュリティ アーキテクチャ

マルチクラウドの保護に McAfee MVISION Cloud を使用すべき 5 つの理由

セキュリティの一元管理

McAfee MVISION Cloud は、Amazon Web Services、Microsoft Azure、Google Cloud Platform など、最先端の IaaS プラットフォームに対応しています。統合された管理インターフェースにより、統一されたセキュリティ ポリシーをすべての CSP に適用します。これにより、個々のサービス レベルでポリシー違反、脆弱性、調査活動、異常、脅威を関連付けることができます。

主な機能 :

- 1 つのクラウド セキュリティ プラットフォームからプロビジョニング、構成、管理を行います。
- ポリシー違反のすべてのインシデントを中央のリポジトリに格納します。
- すべての CSP 内の各リソースを完全に可視化し、コンプライアンス状況を提供します。
- Cloud Security Advisor がセキュリティ指標の測定方法と推奨事項を提供します。
- Data Jurisdiction により、ロールベースの完全なアクセス制御を提供します。

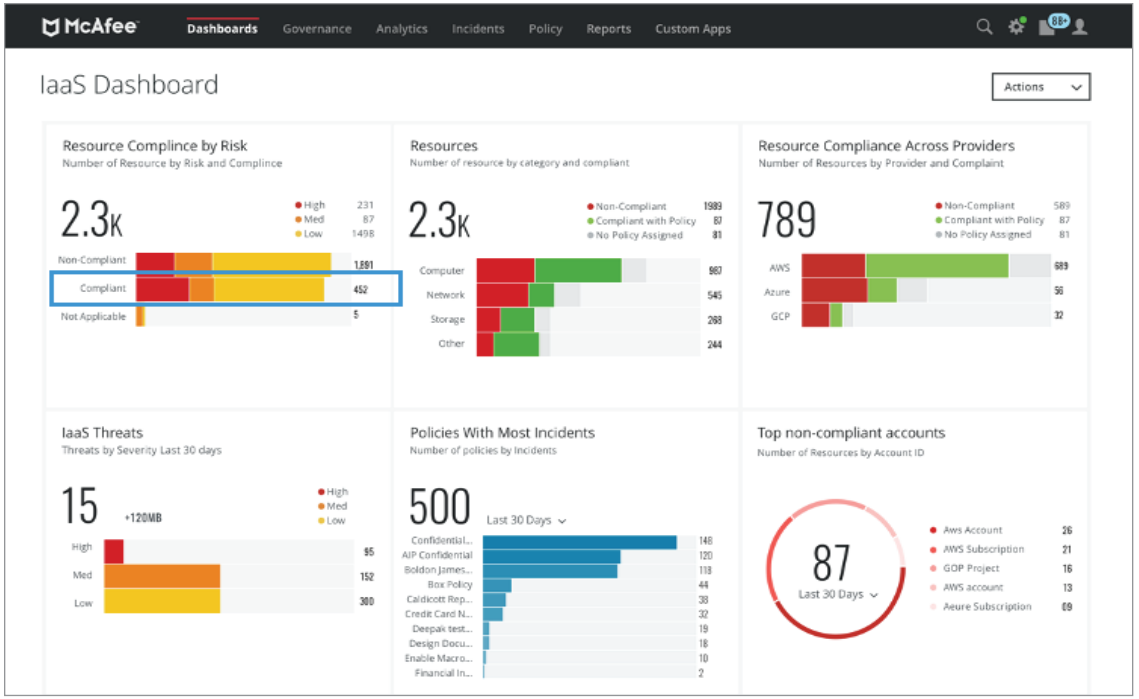

図 3. IaaS ダッシュボード

マルチクラウド セキュリティ ポスチャー マネジメント

マルチクラウドを保護するには McAfee MVISION Cloud が最適なソリューションです。Amazon Web Services、Microsoft Azure、Google Cloud Platform 向けの Cloud Security Posture Management（CSPM）機能により、適切なセキュリティ ガイドラインンを使用して評価を自動的に行います。これにより、複数のポリシーと CIS ベンチマークを管理する際の煩雑さが解消され、構成ミスによるデータ損失を防ぎ、マルチクラウドのコンプライアンスを維持できます。

McAfee MVISION Cloud では、マルチクラウド IaaS 環境を継続してモニタリングし、報告されたセキュリティ ポリシーと実際のセキュリティ ポスチャとの乖離を特定できます。CSPM の中核となるのが、クラウド構成のミスに起因する脆弱性の検知です。これらの脆弱性により、コンプライアンス違反やデータ侵害が発生する可能性があります。このソリューションには、次のよう利点があります。

- 複数のクラウド環境を継続的に可視化し、ポリシー違反を検出します。
- 構成ミスを自動的に修復します。
- CIS Foundations Benchmarks、PCI、NIST 800-53、HIPAA など、標準規格やベンチマークのコンプライアンス ライブラリが事前にビルドされています。
- 構成の問題を識別し、重大な問題が発生する前に、DevSecOps、ワークロード、コンテナー、その他のサービスを停止します。
- 構成監査ポリシー ビルダーにより、組織の要件に合わせてセキュリティ構成監査のカスタム ポリシーを作成できます。Amazon Web Services、Microsoft Azure、Google Cloud Platform のカスタム ポリシーをサポートします。

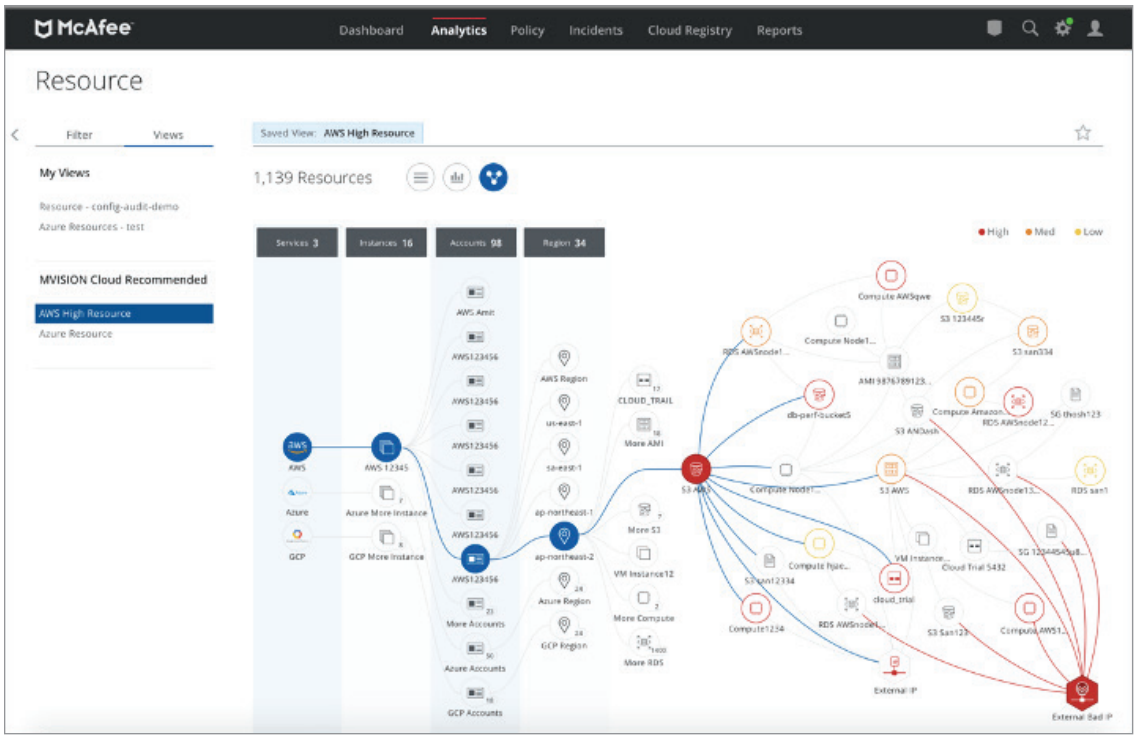

図 4. リソースの可視化とリスク分析

データ セキュリティ ポリシーの一元管理

McAfee MVISION Cloud では、Amazon Simple Storage Service（S3）、Microsoft Azure ブロブ ストレージ、Google Cloud ストレージ バケットに保存されている重要なデータや機密データを可視化し、クラウド環境で使用されるデータを適切に保護できます。MVISION Cloud のコンテンツ エンジンが重要な情報を自動的に識別し、分類します。機密データを削除または隔離し、データの流出を防ぎます。

主な機能 :

- Amazon Web Services、Microsoft Azure、Google Cloud Platform のデータを可視化し、保護します。
- SaaS と複数の IaaS プラットフォーム、Amazon Web Services、Microsoft Azure、Google Cloud Platform 間でデータ損失防止（DLP）ポリシーが適用されます。
- クラウド サービス内のポリシー違反やセキュリティ脅威をほぼリアルタイムで検出します。

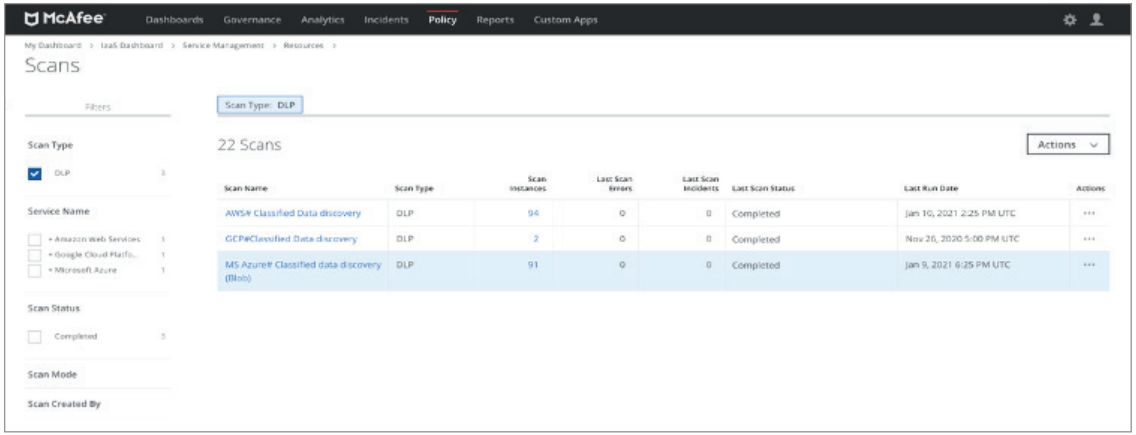

図 5. ポリシー スキャン

インシデントの一元管理

[Policy Incidents Summary] ページに、統合されたサマリー情報が表示されます。すべての DLP とセキュリティ構成監査ポリシーのインシデントに関する情報が表示されます。これにより、個々のポリシーの効果を確認できます。生成されたインシデント数と比較して DLP と構成監査ポリシーの評価精度を修正し、修復アクションを調整できます。

主な機能 :

- マルチクラウドの統合インシデント ダッシュボード。DLP、マルウェア、脅威アノマリ、脆弱性、セキュリティ構成監査の情報が表示されます。
- MITRE ダッシュボードで、AWS、Azure、GCP などのクラウド サービス インフラに悪影響を及ぼす可能性がある、様々なアクティビティの全体的な状況を把握できます。
- 検出されたアノマリをセキュリティ情報 / イベント管理（SIEM）に公開します。
- ServiceNow などのチケッティング システムとの連携。
- ロールベースのアクセス レベルにより、システムの重要領域に対するユーザーのアクセスを制限したり、特定の権限を持つユーザー専用のワークフローを作成できます。

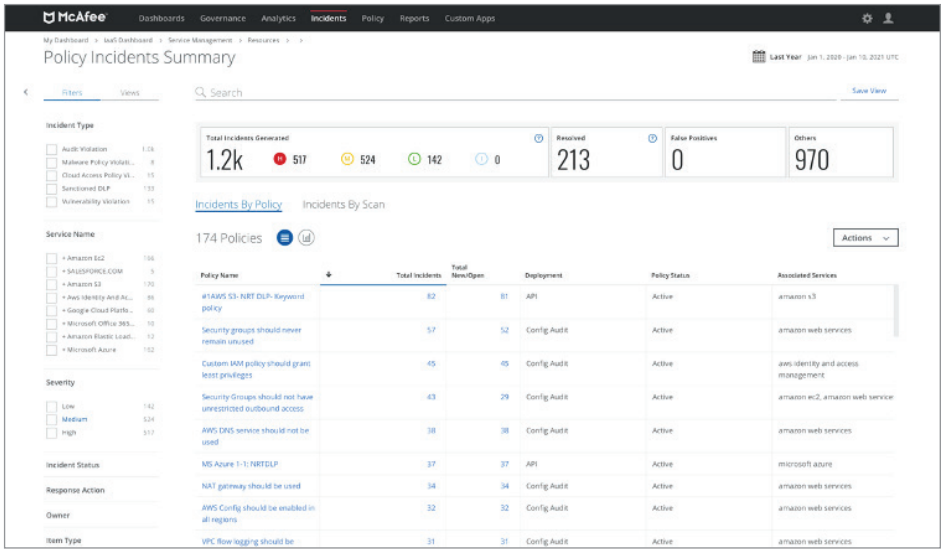

図 6. ポリシー インシデントのサマリー

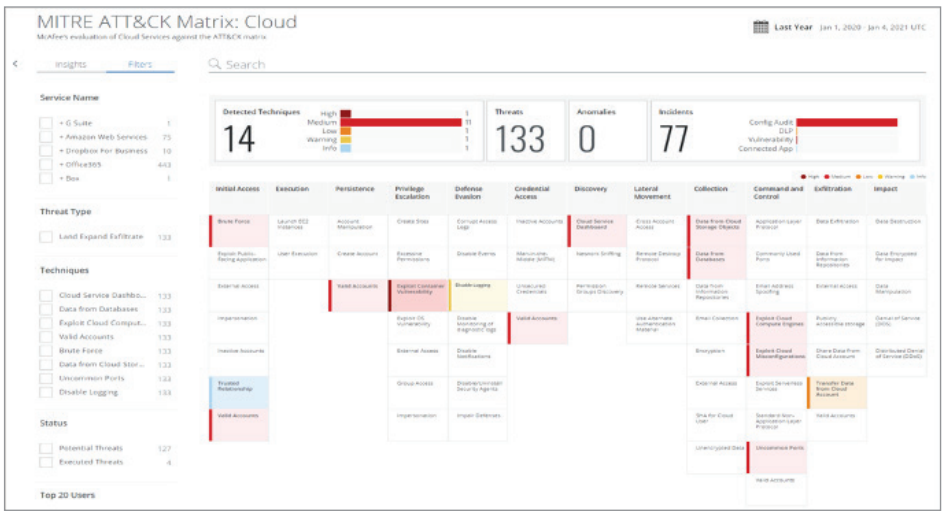

図 7. MITRE ATT&CK マトリックス：クラウド

クラウド ネイティブ アプリケーション

McAfee MVISION Cloud Native Application Protection Platform（CNAPP）は、パブリック クラウド インフラストラクチャ向けの Cloud Security Posture Management（CSPM）と Cloud Workload Protection Platform（CWPP）を統合し、アプリケーションとデータのコンテキストを使用して、ホストとワークロード（VM、コンテナー、サーバーレス機能など）を保護します。また、オフラインとインラインの両方のモードで DevOps テンプレートを評価できるセキュリティ ソリューションを提供します。

このソリューションでは、Amazon Web Services と Microsoft Azure（Terraform サポートを含む）の DevOps テンプレートを評価できます。McAfee Cloud Workload Protection Platform（CWPP）はクラウド ネイティブ アプリケーションを保護するソリューションの一つです。マカフィーでは、これとは別のアプローチも提供しています。マカフィーの究極の目標は次のとおりです。

- 様々な問題に対応するため、技術的な解決策でなく、ビジネス上の成果を重視する。
- すべてのワークロード、環境、クラウド サービス プロバイダーのデータを保護できる包括的なソリューションを提供する。
- 機能やワークフローのタイプで分けるのではなく、ユーザーのワークフローを現状に融合し、管理の煩雑さを削減する。

セキュリティの観点から、McAfee CWPP は、5 つの柱に基づいてこれらの目標を実現します。

- **検出してリスクベースで分類する：**見えないものは保護できません。タイプや場所に関係なく、ワークロードを検出することからリスク管理が始まります。次に、組織に対するリスクに基づいてアカウントとワークロードの脆弱性を分類します。このような相対的なリスクを迅速に把握できれば、修復作業の優先度をすばやく判断し、全体のリスクを軽減することができます。
- **セキュリティを開発プロセスの早い段階で実行する（シフトレフト）：**McAfee MVISION CNAPP を使用すると、オフラインとインラインの両方のモードで DevOps テンプレートを評価できます。インライン モードでは、Github/BitBucket コード リポジトリと Jenkins などの CI/CD ツールを MVISION CNAPP と連携できます。インライン API をシフトレフトして、DevOps テンプレート ファイルに存在する脆弱性を確認します。
- **ゼロ トラスト ポリシーの制御：**McAfee MVISION CNAPP ソリューションは、ゼロ トラストのネットワーク / ワークロード ポリシーを中心としています。このアプローチでは、環境にアクセスしているものとその方法（SOC 戦略の重要な部分）に関する分析だけでなく、必要なタスクを実行できるようにユーザーとサービスに適切な権限を付与できます。

- **脅威対策の統合：** CWPP は、クラウドとオンプレミスのワークロードを保護する脅威対策を統合します。また、ワークロード保護とアカウント権限を連携します。クラウド ネイティブ アプリケーションの保護と McAfee XDR を連携することで、オンプレミスとクラウド インフラを完全に可視化し、リスク管理と修復を行うことができます。
- **ガバナンスとコンプライアンス：** クラウド ネイティブ アプリケーションの保護に理想的なソリューションには、特権アクセスを管理し、場所に関係なくワークロードと機密データを保護する機能が必要です。

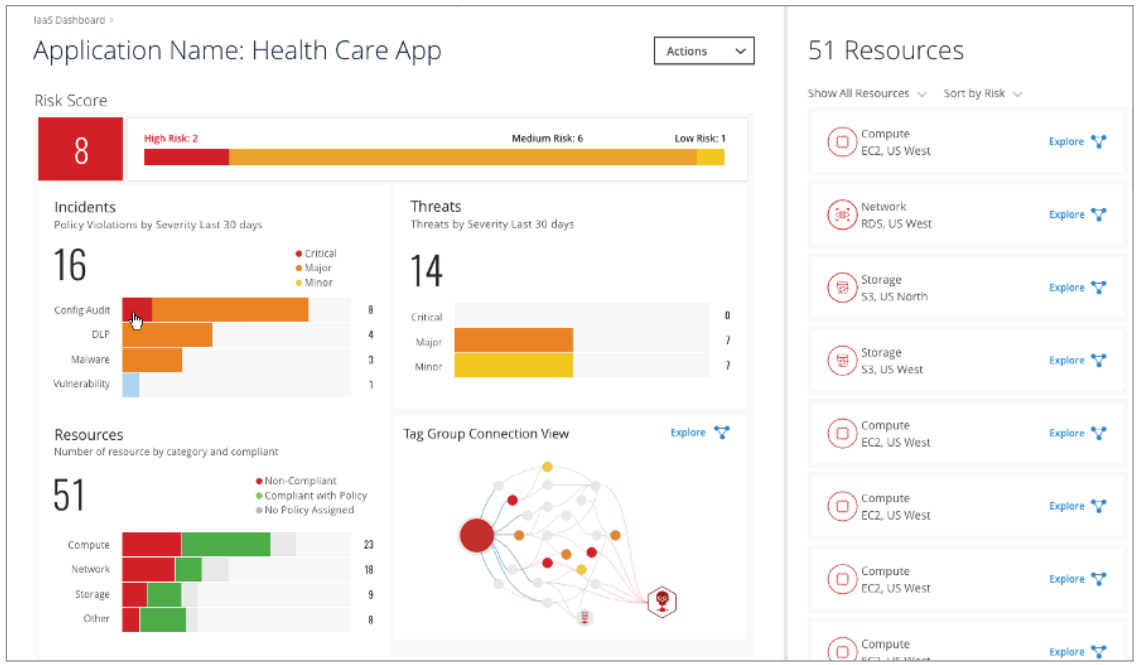

図 8. リスクに基づく優先度の設定。

まとめ

McAfee MVISION Cloud は、クラウド ネイティブに強力なセキュリティを提供するシングル プラットフォームです。McAfee MVISION Cloud は、データ保護、マルウェア検知、脅威対策、ガバナンス、コンプライアンスなどの機能で、新しいクラウド ネイティブ アプリケーションのニーズに包括的に対応します。これにより、セキュリティ機能の向上とマルチクラウド セキュリティの総所有コスト（TCO）の削減を実現することができます。

McAfee について

McAfee は、デバイスからクラウドまでを保護するサイバーセキュリティ企業です。McAfee では、より安全なデジタル世界を構築するため、個々の力を結集し、企業と個人を保護するソリューションを提供しています。他社の製品と連携するソリューションを構築することで、真に統合されたサイバーセキュリティ環境を整備し、脅威の対策、検出、修復を連動して行うことができます。McAfee の個人向けのソリューションは、すべての種類のデバイスに対応しています。自宅でも外出先でも、安心してデジタル ライフを楽しむことができます。McAfee では、他のセキュリティ企業との連携を強化し、力を合わせてサイバー犯罪者と戦っています。

www.mcafee.com/jp

〒 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
www.mcafee.com/jp