McAfee MVISION Cloud

ビジネスを加速化するクラウド セキュリティ

McAfee® MVISION Cloud はクラウド ネイティブのセキュリティ対策です。SaaS、PaaS、IaaS のセキュリティを一元管理し、クラウドのデータを脅威から保護します。

可視化

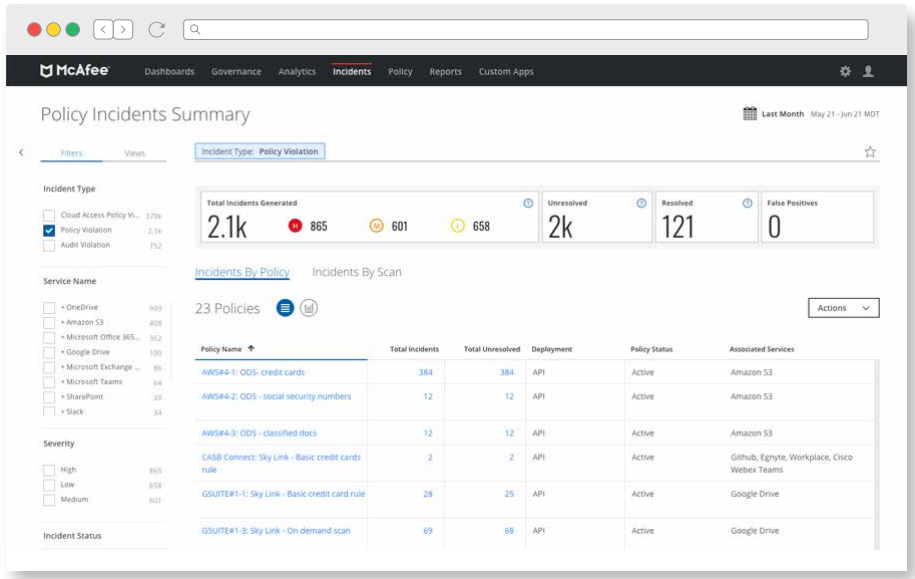
クラウドの使用状況とデータをすべて可視化します。

コントロール

任意のソースからのデータとクラウド アクティビティをコントロールします。

保護

クラウドの脅威を阻止し、誤設定を防ぎます。



主な特徴

- クラウド上のデータにデータ損失防止（DLP）ポリシーを適用し、エンドポイントの DLP と同期します。
- 未承認ユーザーとの機密データの共有を防ぎます。
- 個人所有のデバイスで会社のデータのダウンロードと同期をブロックします。
- 乗っ取られたアカウント、内部脅威、マルウェアを検出します。
- 暗号化キーでクラウド上のデータを暗号化し、第三者によるアクセスを阻止します。
- 未承認のアプリケーションを可視化し、その機能をコントロールします。
- 業界標準のベンチマークを使用して誤設定を調査し、設定を自動的に変更します。

McAfee とつながる

MVISION Cloud プラットフォーム

ポリシー エンジンの統合

同じポリシーをすべてのクラウド サービスに適用できます。保存されているデータにも送信中のデータにも同じポリシーが適用されます。既存のソリューションからポリシーをインポートすることも、新しいポリシーを作成することもできます。

事前定義のポリシー テンプレート

すぐに使えるポリシー テンプレートが用意されています。ビジネス要件、コンプライアンス、業種、クラウド サービス、サードパーティのベンチマークに合わせて選択できます。

ポリシー作成ウィザード

ブール論理によるルールの組み合わせ、除外対象、インシデントの重大度に応じた修復アクションを使用して、カスタム ポリシーを定義できます。

ポリシー インシデントの管理

統一されたインターフェースでインシデントをレビューし、アクションを手動で実行できます。修復の自動ロールバックにより、ファイルとその権限を復元できます。

クラウド レジストリ

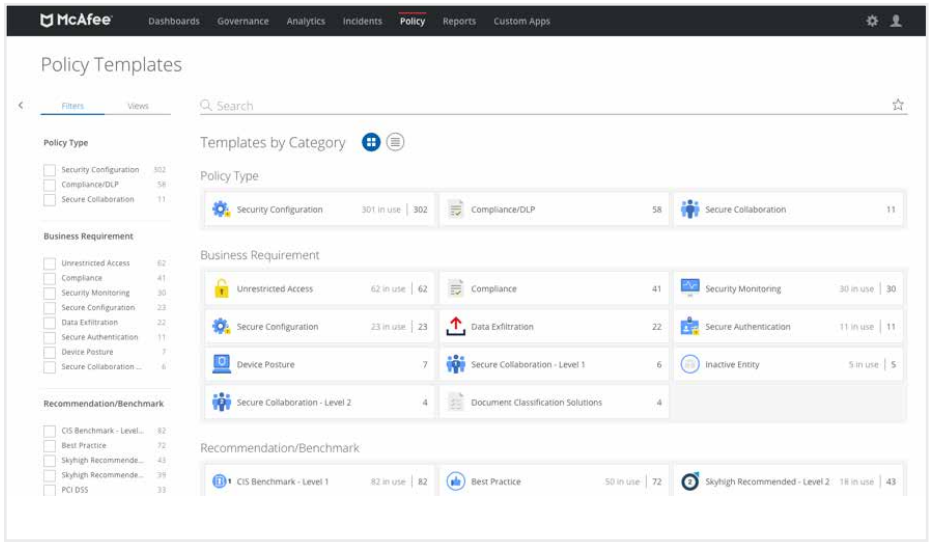
世界最大で最も正確なクラウド レジストリを提供します。クラウド サービスのリスクを 261 の項目で診断し、クラウドの信頼性を 10 段階で評価します。

プライバシーの保護

不可逆的な一方行のプロセスでオンプレミスのユーザー情報をトークン化し、企業の情報を難読化します。

自律的な修復

ポリシー インシデントの修正をユーザーに指示します。修正すると、インシデント アラートが自動的に解決されます。インシデントのレビューを手動で行う必要はありません。



アプリ内でのコーチング

インシデントが発生したメール、メッセージング、コラボレーション アプリケーション内でリアルタイムで対応を指示します。

AI を利用したアクティビティ マッパー

人工知能を利用してアプリの状態を把握し、ユーザーのアクションを一定のアクティビティにマッピングします。標準化された方法でアプリのモニタリングと制御が可能になります。

マルチクラウドに対応

統一されたセキュリティ ポリシーをすべてのクラウド サービスに適用します。これにより、ポリシー違反を関連付け、個々のサービスでアクティビティ、異常、脅威を調査できます。

クラウドの使用状況とデータをすべて可視化

コンテンツの分析

キーワード、事前定義の英数字パターン、正規表現、ファイルのメタデータ、ドキュメントとデータベースのフィンガープリントを利用して、クラウド サービスで使用されている機密データを特定します。

コラボレーションの分析

共有されているファイルとフォルダに対するユーザーや組織のアクセス権（閲覧者、編集者、所有者など）を検出します。

アクセスの分析

デバイスのオペレーティング システム、デバイスの管理状況、場所、企業 / 個人のアカウントなどのアクセス コンテキストを分析します。

クラウドの使用状況の分析

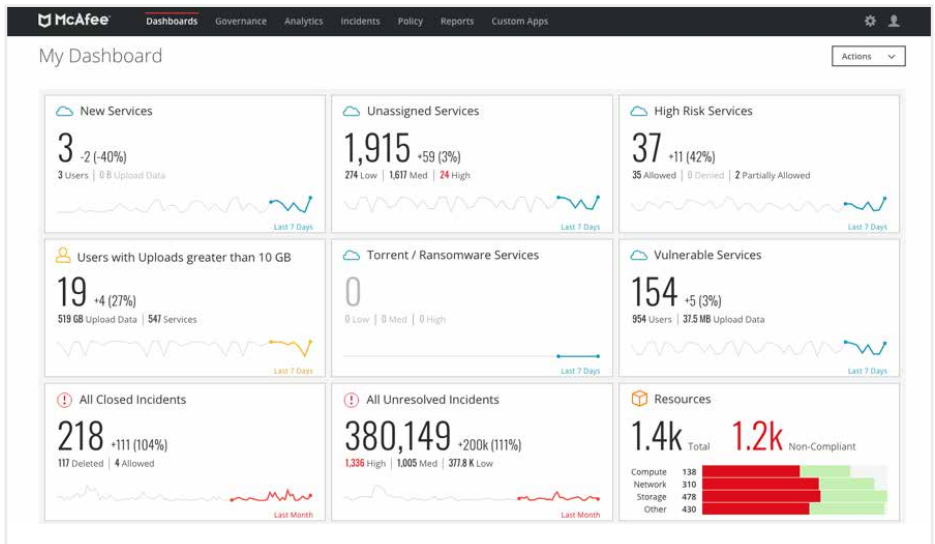
ユーザーが使用しているクラウド サービス、データ量、アップロード数、アクセス数、許可 / 拒否アクティビティなど、一定期間のクラウドの使用状況を要約して表示します。

クラウド アクティビティのモニタリング

インシデント発生後の調査とフォレンジックで利用できるように、すべてのユーザーと管理者のアクティビティを収集し、包括的な監査証跡を保存します。

「McAfee MVISION Cloud で IT サービスのギャップを見つけています。傾向やパターンをすぐに把握できるので、ユーザーに対するサービス品質の向上につながっています。また、長期的な戦略と投資計画でより的確な意思決定を行うことができます。」

— David Stevens
マリコパ郡最高情報責任者



クラウド上のデータとアクティビティをコントロール

クラウド データ損失防止（DLP）

独自のコンテンツ ルールに基づいてポリシーを適用し、クラウド アプリケーション、インフラ、ファイルからのデータ漏えいを防ぎます。構造化データだけでなく、非構造化データにも対応しています。オンプレミスの McAfee® Data Loss Prevention（DLP）コンテンツ ルールとポリシーを MVISION Cloud と同期し、クラウド サービスに適用できます。

マルチソース コントロール

クラウドにアップロードされるデータだけでなく、クラウドで作成されたデータ、共同作業者と共有しているデータ、クラウド サービス間で共有しているデータ、クラウドからダウンロードされるデータに DLP ポリシーを適用できます。

多層的な対応

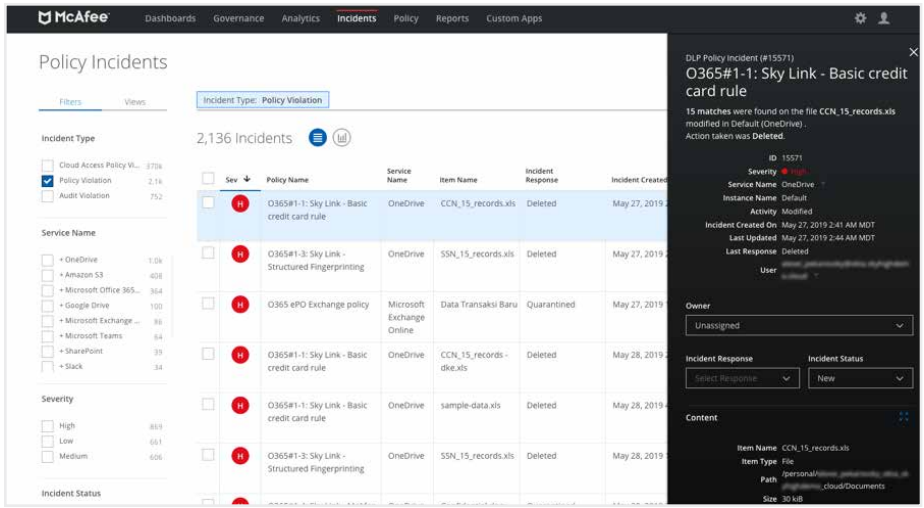
重大度別のポリシーを定義し、インシデントの重大度に応じて個別の対応を行うことができます。DLP スキャンなどの監査で誤設定が見つかると、対応アクションを自動的に実行します。

隔離

クラウド サービス内のセキュアな管理領域でポリシーをトリガーしたファイルを隔離します。McAfee が隔離ファイルを保存することはありません。

暗号化

顧客側で管理されるキーによる暗号化とでピアレビューで機密データを保護します。構造化データだけでなく、非構造化データも暗号化されます。



情報の権限管理

機密データが常に保護されるように、クラウド サービスにアップロードされるファイルやクラウド サービスからダウンロードされるファイルに権限管理の保護機能を適用します。

コラボレーションの制御

ファイルやフォルダーに対するユーザー権限を編集者または閲覧者に格下げしたり、権限の削除や共有リンクの取り消しを行うことができます。データの機密性に応じて権限を設定できます。

アプリケーションの接続

承認済みのクラウド サービスと接続するサードパーティ アプリケーション（マーケットプレイスのアプリなど）を可視化します。特定のユーザー、アプリケーション、アクセス権限に基づいてサードパーティ アプリケーションの動作をポリシーでコントロールします。

「クラウド用に設計された McAfee のソリューションで、データ損失防止（DLP）、権限管理、データ分類、脅威対策、暗号化などのセキュリティ ポリシーをクラウド環境に適用しています。」

– Mauro Loda
DuPont クラウド セキュリティ チーフアーキテクト

削除
コンプライアンス ポリシーに違反するクラウド サービスからデータを完全に削除します。

コンテキスト対応のアクセス制御
サービス レベルのリスクやデバイス タイプに基づいてアクセスを許可またはブロックします。また、アクティビティ レベルできめ細かい制御を行い、データのアップロードとダウンロードを防ぎます。

適応型の認証
アクセス制御ポリシーに基づいて ID 管理ソリューションを統合し、追加の認証手順をリアルタイムで実施できます。

クラウド アプリケーションのコントロール
非承認のクラウド サービスに対してきめ細かいポリシーを設定できます。たとえば、MVISION Cloud コンソールから未承認テナントに対するアクティビティを許可またはブロックできます。

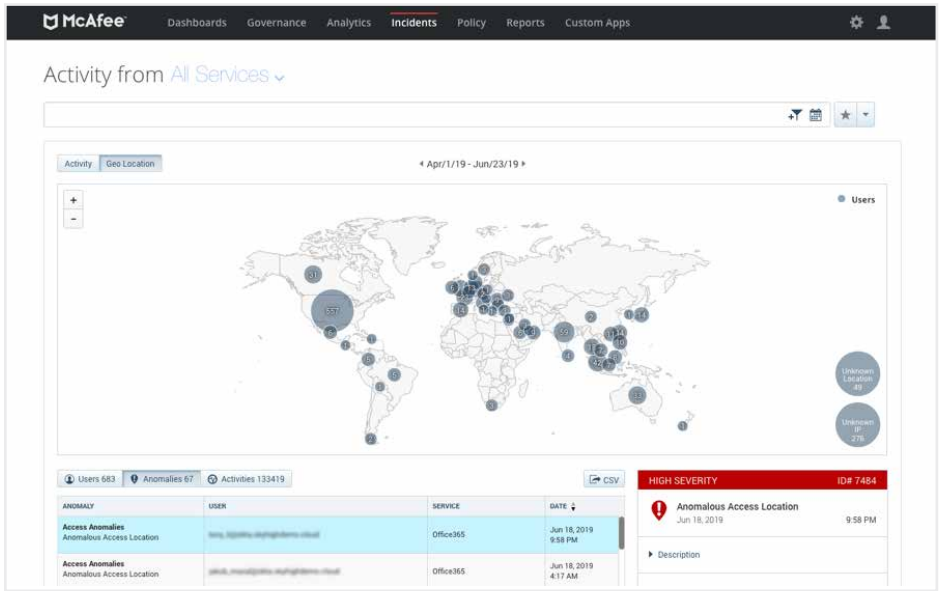
クラウドに対する脅威の阻止と誤設定の防止

セキュリティ構成の監査
クラウド アプリケーションとインフラのセキュリティ設定を確認し、CIS（Center for Internet Security）Benchmark などの業界標準に基づいてセキュリティの改善方法を提示します。コードを IaaS に配備する前に監査を行い、リスクをプリエンプティブに回避できます。

構成の自動修復
監査で不適切な設定が見つかると、ポリシーによって修復が自動的に行われます。たとえば、IaaS ストレージ バケットに対するパブリック アクセスを自動的に無効にします。

ユーザー / エンティティ動作分析（UEBA）
複数のヒューリスティック分析と機械学習により自己学習モデルを自動的に構築し、複数のクラウド サービスで脅威の兆候を示すユーザーの行動パターンを特定します。

ガイド付き学習
システムが検知した異常に対する影響度の変化をリアルタイムでプレビューできます。この情報は、機械学習モデルへの入力として使用できます。



乗っ取られたアカウントの検出
ログイン試行を分析し、許可されていないリージョン間のアクセス、総当たり攻撃、信頼されていない場所からのアクセスなど、アカウントの乗っ取りを示す兆候を特定します。

内部脅威の検出
機械学習を利用し、内部ユーザーによる機密情報の流出など、過失または故意による不正行為を検出します。

特権ユーザーの分析
過剰なユーザー権限、アクティブでないアカウント、不適切なアクセス、権限の不当なエスカレーション、ユーザーのプロビジョニングなどを特定します。

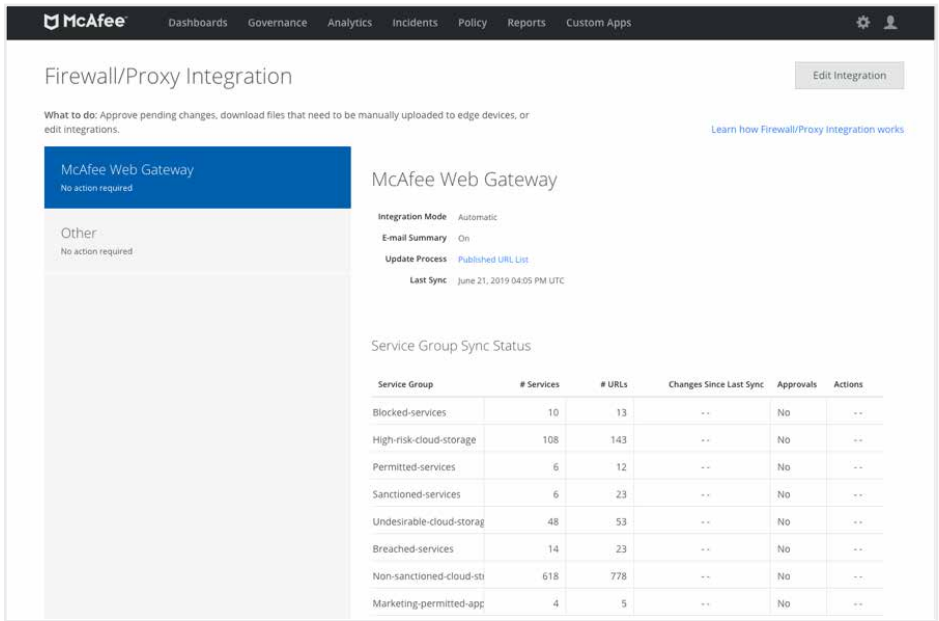
マルウェアの検出
クラウド サービスからデータを送出するマルウェアの挙動を検出します。クラウド サービスをリアルタイムまたはオンデマンドでスキャンします。

マルウェアの駆除
マルウェアを完全に無害化して駆除し、高度な脅威を排除します。

「McAfee のソリューションにより、従業員がどのように Salesforce を利用しているのかを把握しています。内部脅威、感染、認証情報、過剰な権限の付与などを確認できます。」

— Mike Bartholomy
Western Union 情報セキュリティ シニア マネージャー

エンタープライズ テクノロジーの連携
- データ損失防止（DLP）
- セキュリティ情報 / イベント管理（SIEM）
- セキュアな Web ゲートウェイ（SWG）
- 次世代ファイアウォール（NGFW）
- 鍵管理システム（KMS）
- ID とアクセスの管理（IAM）
- 情報権限管理（IRM）
- エンタープライズ モビリティ管理（EMM/MDM）
- ディレクトリ サービス（LDAP）



配備モード

McAfee Sky Link

クラウド サービス API に接続して、データとユーザー アクティビティを可視化します。アップロードまたは共有されているデータと保存されているデータにポリシーを適用します。

McAfee Lightning Link

クラウド サービスと帯域外接続を直接確立し、データ、ユーザー、デバイスにリアルタイムでポリシーを適用します。

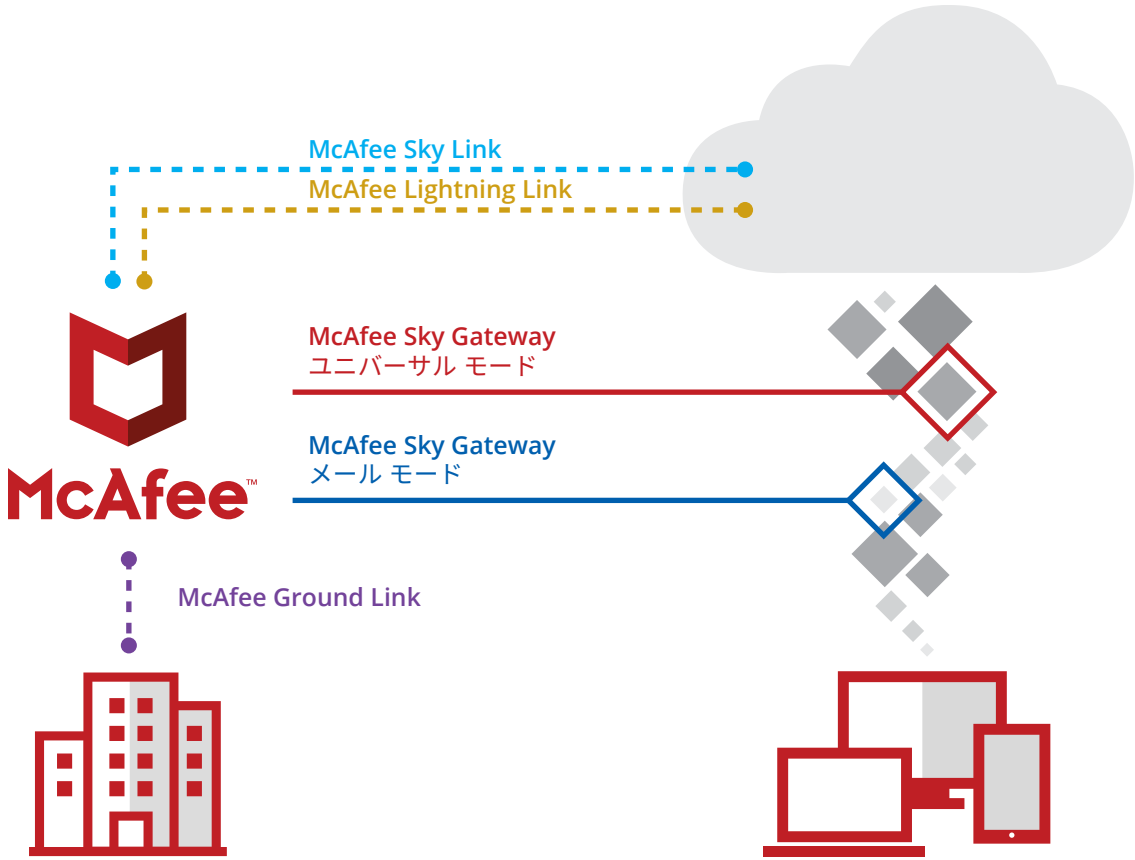
McAfee Ground Link

オンプレミスの LDAP ディレクトリ サービス、DLP ソリューション、プロキシ、ファイアウォール、鍵管理サービスと McAfee との接続を仲介します。

McAfee Sky Gateway

移動中のデータにリアルタイムでポリシーを適用します。

- **メール モード :** ネイティブのメール フローを利用し、Exchange Online からインラインまたはパッシブ監視モードで送信されるメッセージにポリシーを適用します。
- **ユニバーサル モード :** ユーザーとクラウド サービスの間にインラインで配置され、認証後にトラフィックを誘導します。エージェントを使用せずにすべてのユーザーとデバイスに対応します。

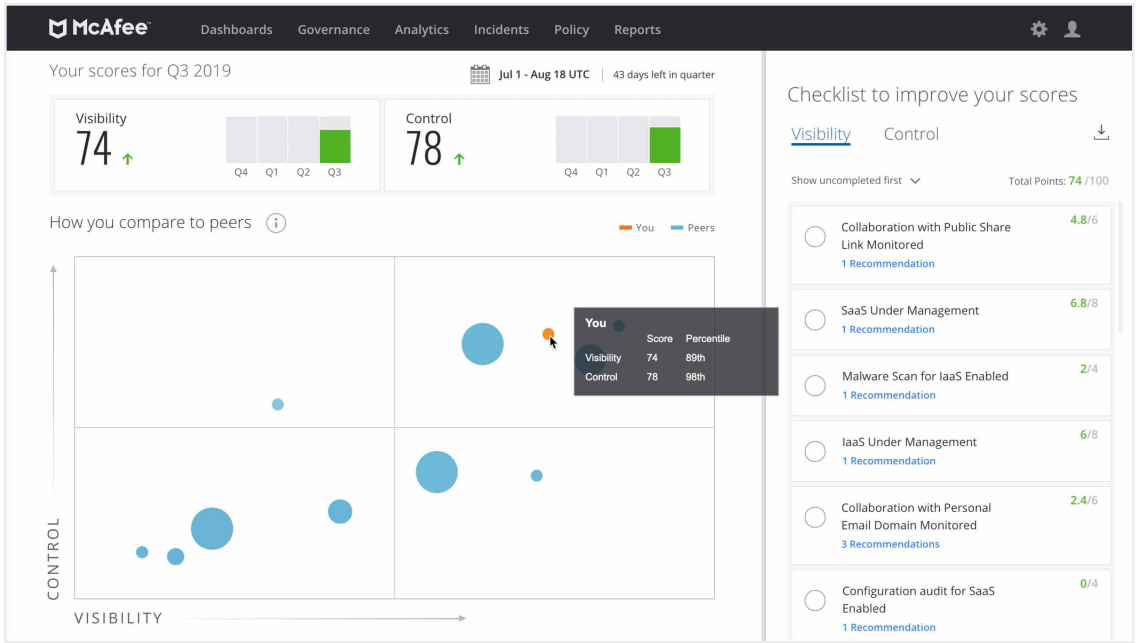


Cloud Security Advisor

Cloud Security Advisor は MVISION Cloud Security プラットフォームのポータルで、クラウド セキュリティの状況を確認できます。クラウド セキュリティの管理で優先して行うべき作業を推奨します。

Cloud Security Advisor は次のものから構成されます。

- **クラウド セキュリティ レポート :** 重要な使用統計の概要が表示されます。クラウド フットプリント、インシデント、危険なデータ、ユーザー数など、重要なセキュリティ指標が表示されます。
- **Cloud Security Advisor スコア / クアドラント :** 可視化とコントロールの評価スコア（100 点満点）が表示されます。この評価は、クラウド セキュリティの指標、実装の進捗状況、同規模の業界関係者との比較に基づいて行われます。
- **クラウド セキュリティの推奨事項 :** クラウド セキュリティの向上に必要な作業を重要度に応じて推奨します。推奨事項は、潜在的な影響の大きさに基づいて優先度が設定されます。

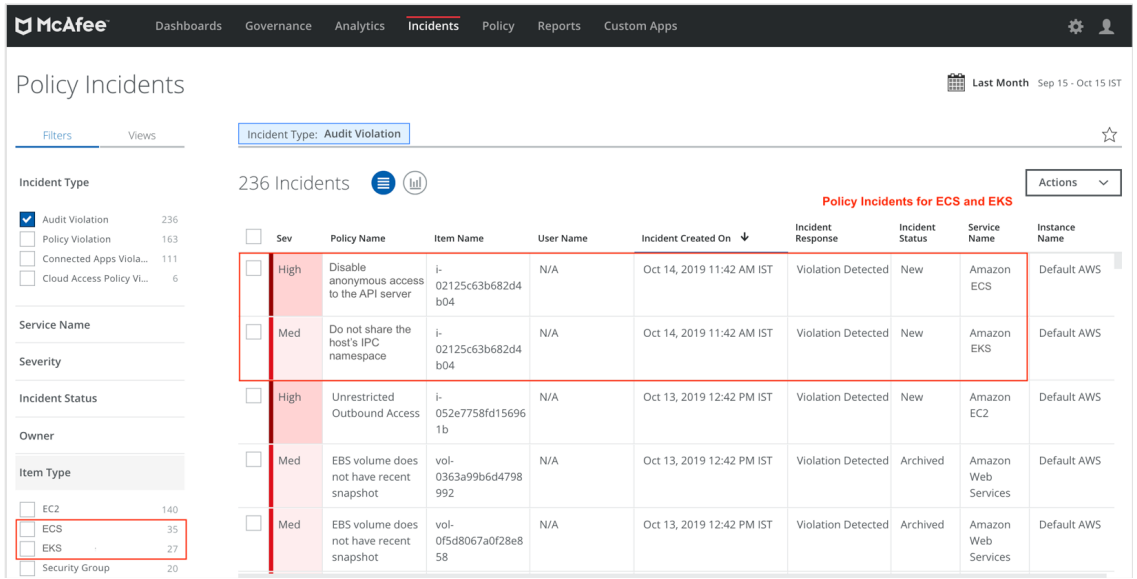


MVISION Cloud for Containers

仮想化ではコンテナ技術が主流となり、クラウドのメリットを最大限に活用できるように最適化されています。MVISION Cloud Container Security は、コンテナ向けに最適化された統合クラウド セキュリティ プラットフォームにより、動的で常に変化するコンテナ ワークロードとその展開先であるインフラを保護します。

MVISION Cloud for Containers の機能は次のとおりです。

- コンテナ コンポーネントの**脆弱性診断**
  - コンテナに組み込まれたコードを定期的に診断します。これにより、既知のリスクが存在するかどうか確認したり、リスクを回避してコンテナ ワークロードに対する攻撃を未然に防ぐことができます。この診断はビルド時にも行われます。
- Kubernetes などのコンテナ インフラ / オーケストレーション システムの**クラウド セキュリティの管理**
  - 環境の構成がリスク源にならないように管理します。
  - 環境の構成に対する変更で予期しないリスクが発生しないようにします。
- コンテナ間通信の**ナノ セグメンテーション**
  - ゼロトラスト : 何も信頼せず、常に確認します。コンテナのエフェメラルな特性に対応し、IP アドレスなどの外部要因に依存しない方法で、コンテナ プロセス間で発生するネットワーク通信をモニタリングします。



- 異常な通信を検出した場合、ユーザーの設定に基づいて通信を通知またはブロックします。
- アプリケーションは常に進化を続けています。このため、コンテナのバージョン間で通信パターンが変化することもあります。このような変化も見逃さず、検出します。
- 誤った構成を継続するのではなく、既知の正常な構成に戻し、ワークロードを保護します。

McAfee Together is power.

〒 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