アセットとインベントリの検出

検出は、Multicloud Defense の**「検出、展開、防御」**アプローチの重要なコンポーネントです。

検出は、オンボーディングされたクラウドアカウントに展開されている現在のリソースをリアルタイムで可視化します。さらに、VPC フローログと DNS ログ用のインターフェイスを提供し、クラウド展開の全体像を把握できます。Multicloud Defense Controller は、IAM ロール（AWS および OCI）、AD アプリケーション登録（Azure）、またはサービスアカウント（GCP）に付与された権限を介して、クラウドリソースを定期的にクロールし、変更を監視することでリソースの「常に新しい」インベントリモデルを維持します。

[検出（Discovery）] タブを使用すると、リソースの属性とそれらがどのように相互接続されているかを確認できます。Multicloud Defense はこの情報を照合し、設定およびトラフィックフローのコンテキストに関するすべてのリソースのセキュリティ態勢を簡潔なビューにまとめます。

検出の概要

[検出の概要（Discovery Summary）] ページは、使用可能なトラフィックとインベントリの概要を示すウィジェットを集めたものです。ページの上部にある [フィルタ（Filter）] を使用して、ウィジェットの履歴を変更できます。

トラフィックの概要ウィジェット

現在、Multicloud Defense は、1 つは DNS トラフィック用、もう 1 つは VPC および VNet フローログ用の 2 つのウィジェットで、トラフィックのブロックを簡略的に示します。トラフィックに関するこれらのウィンドウは、悪意のあるトラフィックと DNS または VPC/VNet トラフィックをそれぞれ区別します。特定の時間枠にズームインするには、これらのウィジェットのいずれかの内側をクリックします。

[ログ（Logs）] トグルをクリックするだけで、この概要ページから、これらのウィジェットのいずれかのログを有効化または無効化できます。これらのタイプのログとコンパイルされるトラフィックの詳細については、トラフィックのタイプ を参照してください。

検出の概要

検出の概要は、クラウド サービス プロバイダーに接続するときに、Multicloud Defense によって検出プロセスの一部として復旧される一連のインベントリのウィンドウです。これらの統計は、クイックプレビュー用に簡略的に表示されます。詳細を確認するには、インベントリ （2 ページ） を参照してください。

インベントリ

IAM ロール（AWS および OCI）、AD のアプリケーション登録（Azure）、またはサービスアカウント（GCP）に付与された権限により、Multicloud Defense は、高度なネットワークセキュリティの適用に関連し、クラウドサービスプロバイダーのアカウント、サブスクリプション、およびプロジェクトに存在する、クラウドリソースの「古くならない」インベントリモデルとリアルタイム検出を継続的に維持します。検出されたリソースは、管理者がセキュリティルールを迅速に展開し、公開中のアプリケーションのリスクの軽減を可能にするワークフローで使用できます。すべてのアクティビティは、Multicloud Defense Controller を介してすぐに報告されます。

インベントリが有効になっている場合、Multicloud Defense Controller は完全なインベントリ検出を定期的に実行します。デフォルトは 60 分ですが、調整可能です。リアルタイムのインベントリ検出は、CloudFormation テンプレートが展開されたリージョンで有効になります。

検出プロセスの一部では、各クラウドサービスが提供するログが強調表示されます。サービスプロバイダーごとに、次のタイプのログに注意してください。

- **AWS**：VPC フローログ、Mount53 フローログ、および DNS ログ。
- **Azure**：NSG フローログ。
- **GCP**：VPC フローログ。

Multicloud Defense は、すべてのクラウド サービス プロバイダーに同じレベルのサポートを提供することに注意してください。

アプリケーション

アプリケーションには、クラウドアカウントのすべてのロードバランサと API ゲートウェイが表示されます。[インベントリ（Inventory）] の [アプリケーション（Applications）] セクションには、[既知のタグ（Known Tags）]、[タグ（Tags）]、および [アプリケーション（Applications）] の 3 つのフィルタボタンがあります。[アプリケーション（Applications）] では、ユーザーがワークフローを呼び出して、特定のアプリケーションの保護を作成し、適用できます。

アプリケーションタグ

アプリケーションの識別に使用する [アプリケーションタグ（Application Tags）] のリストを作成します。インベントリ検出段階では、指定されたタグを持つ検出されたすべてのロードバランサが、アプリケーションとして扱われます。

たとえば、アプリケーションとして機能するすべてのロードバランサに [アプリケーションタグ（Application Tags）] を割り当てることができます。このタグの値は、検出されたインベントリの [アプリケーションタグ（Application Tags）] として表示されます。視覚的に表した例として、次のテーブルを参照してください。

ロード バランサ	タグ	値
ロードバランサ 1	ApplicationName	課金
ロード バランサ 2	ApplicationName	UserManagement

検出されたインベントリには、検出されたアプリケーションアセットの [課金情報（Billing）] および [ユーザー管理（UserManagement）] アプリケーションが表示されます。

[アプリケーションタグ（Application Tags）] のリストを作成するには、[作成（Create）] をクリックします。

パラメータ	説明
名前	事前に入力されます。
説明	ユーザー指定の説明です。
値	使用されるタグ値は、ロードバランサに割り当てられます。

アプリケーションタグの詳細については、アプリケーションタグを参照してください。

既知のタグ

[既知のタグ（Known Tags）] には、クラウドアカウントのアプリケーション ロード バランサによって識別され、管理者が既知のタグによって識別したアプリケーションが表示されます。これらの既知のタグは、**[設定（Settings）]**>**[管理（Management）]**>**[アカウント（Account）]**>**[アプリケーションタグ（Application Tags）]**にリストされています。

タグ（Tags）

タグには、アプリケーション ロード バランサによって識別されたすべてのアプリケーションと、タグキーとタグ値、およびこれらのアプリケーションが Multicloud Defense Gateway によって保護されているかどうかを示すフィールドが表示されます。

検出されたアセット

クラウドアカウントのリージョンでインベントリ検出を有効にすると、Multicloud Defense Controller は継続的にクラウドアセットを検出します。検出されたアセットを確認するには、[検出（Discover）] または**[管理（Manage）]** > **[インベントリ（Inventory）]**に移動します。デフォルトのビューには、すべてのクラウドアカウントで検出されたアセットが表示されます。特定のクラウドアカウントにフィルタリングするには、[アカウントの選択（Select Account）] を使用して特定のクラウドアカウントを指定し、検出されたアセットを表示します。

検出されるアセットのカテゴリとそれが示す内容は次のとおりです。

- セキュリティグループ：AWS セキュリティグループ（SG）および Azure ネットワーク セキュリティ グループ（NSG）。
- ネットワーク ACL：AWS ネットワークアクセス制御リスト（NACL）。
- サブネット。
- ルートテーブル。
- ネットワーク インターフェイス。
- VPC/VNet：AWS VPC、Azure VNet、および GCP VPC。
- アプリケーション：アプリケーションは、AWS アプリケーション ロードバランサ（ALB）によって識別されます。
- ロードバランサ。
- インスタンス：AWS インスタンス、Azure 仮想マシン、および GCP コンピューティング インスタンス。
- タグ：AWS タグ、Azure タグ、および GCP ラベル。
- 証明書：AWS Certificates Manager（ACM）証明書。

アセット検出とインベントリの有効化

クラウドアカウントでアセットの検出を有効にするには、次の手順を実行します。

手順

ステップ 1 **[管理（Management）]** > **[アカウント（Accounts）]**に移動します。

ステップ 2 クラウドアカウントの横にあるチェックボックスをオンにし、[インベントリの管理（Manage Inventory）] をクリックします。

ステップ 3 Multicloud Defense で検出するクラウドアセットが配置されている**リージョン**をセレクトします。更新間隔は、インベントリが更新されるまでの分単位の時間です（推奨されるデフォルトは 60 分）。Multicloud Defense は、定期的なポーリングの代わりに、クラウド サービス プロバイダーの API とイベントを使用し

て継続的な検出も実行します。ここで指定する更新間隔の時間は、完全な再クロール用であり、これによりリアルタイム検出中に欠落したイベントのすべてのアセットが調整されます。

新しい行を追加して対象のリージョンを選択することで、リージョンごとに異なる更新間隔を定義できます。1 つのリージョンには単一の更新間隔のみを指定することができます。

ステップ 4 [完了（Finish）] をクリックして保存します。

（注）
保存するとすぐに、Multicloud Defense Controller は新しく追加されたリージョンのアセットインベントリを要求します。

次のタスク

検出されたアセットを確認するには、**[管理（Manage）]**>**[インベントリ（Inventory）]**に移動します。

セキュリティに関するインサイト

インサイトは、AWS、Azure、および GCP で検出されたアセットのルールベースの評価であり、調査結果として表示されます。インサイトは、Multicloud Defense Controller によって提供される定期的かつリアルタイムのインベントリモニタリングで動作するため、Multicloud Defense Gateway を展開せずに使用できます。

手順

ステップ 1 Multicloud Defense Controller インターフェイスで、[アカウントの追加（Add Account）] をクリックします。別の方法として、簡単セットアップウィザードを使用してアカウントに接続することを強くお勧めします。各手順を進めてアカウントを接続します。

ステップ 2 アカウントが接続され、オンボーディングされたら、アセット検出とインベントリの有効化します。

ステップ 3 **[検出（Discover）]** > **[検出の概要（Discovery Summary）]**に移動します。このページには、検出されたすべてのアセットと**インサイトの調査結果**の概要ビューが表示されます。

セキュリティに関するインサイトの種類

次のセキュリティインサイトのタイプに関する説明を読み、ダッシュボードで何ができるかを理解しましょう。

セキュリティ グループ

お客様が**セキュリティグループ**の急増に苦慮することはよくあります。セキュリティグループは、多くの場合、リスクをもたらす可能性のあるリソース間で共有されます。特定のリソースを対象としてセキュリティグループに加えられた変更が、より大規模なリソースグループに影響を与える可能性があります。

セキュリティグループには、すべてのセキュリティグループ、その詳細、およびセキュリティグループを使用するリソースのセットのリストが含まれます。[インバウンドパブリックである（Is Inbound Public）] フィールドと [アウトバウンドパブリックである（Is Outbound Public）] フィールドは、セキュリティグループが 0.0.0.0/0 で設定されていることを示します。

検索ウィンドウで、検索条件に基づいてルールを作成するオプションを使用して、フィールドとその値に基づいて検索条件を定義します。

ルール（Rule）

ルールは、設定されたインバウンドルールとアウトバウンドルールに基づいてセキュリティグループのビューを提供します。

ポート

ポートは、設定されたインバウンドポートとアウトバウンドポートに基づいてセキュリティグループのビューを提供します。

アプリケーションのセキュリティ グループ

[アプリケーションセキュリティグループ（Application Security Groups）] は、AWS セキュリティグループに似た Azure 構造の 1 つです。Azure アプリケーション セキュリティ グループには、そのシステムとそのインターフェイスを含むセキュリティグループのメンバーが存在します。メンバーシップとセキュリティの両方を制御できます。その結果、Multicloud Defense はこのメンバーシップ構造を使用して動的なポリシーを構築できます。Azure 環境内でアプリケーション セキュリティ グループを作成して使用すると、Multicloud Defense は変更を認識し、変更を組み込むようにポリシーを適応させます。

Azure のアプリケーション セキュリティ グループとその動作の詳細については、Microsoft Azure のドキュメントを参照してください。

Network ACL

ネットワークアクセス制御リスト（ACL）は、すべてのネットワーク ACL とその詳細のリストを提供します。[インバウンドパブリックである（Is Inbound Public）] フィールドと [アウトバウンドパブリックである（Is Outbound Public）] フィールドは、ネットワーク ACL が 0.0.0.0/0 で設定されていることを示します。

ルール（Rule）

ルールは、設定されたインバウンドルールとアウトバウンドルールに基づいてネットワーク ACL のビューを提供します。

サブネット

[サブネット（Subnets）] には、すべてのサブネットとその詳細のリストが表示されます。[パブリックである（Is Public）] フィールドは、パブリック IP の自動割り当てが有効になっているかどうかに基づいて、パブリックアクセス可能なサブネットを示します。

ルートテーブル

[ルートテーブル（Route Tables）] には、すべてのルートテーブルとその詳細のリストが表示されます。[インバウンドパブリックである（Is Inbound Public）] フィールドと [アウトバウンドパブリックである（Is Outbound Public）] フィールドは、インターネットへのデフォルトアクセスを提供するように設定されたルートテーブルを示します。

ネットワーク インターフェイス

[ネットワークインターフェイス（Network Interfaces）] には、すべてのネットワーク インターフェイスとその詳細のリストが表示されます。[インバウンドパブリックである（Is Inbound Public）] フィールドと [アウトバウンドパブリックである（Is Outbound Public）] フィールドは、オープンなセキュリティグループ（0.0.0.0/0）で設定されたネットワークインターフェイス、またはインターネットへのデフォルトアクセスを許可するルートテーブルを示します。

VPC\VNet

[VPC/VNet] には、すべての VPC/VNet とその詳細のリストが表示されます。

アプリケーション

アプリケーションには、展開されたすべてのアプリケーション ロード バランサとその詳細のリストが表示されます。[保護済み（Secured）] フィールドは、Multicloud Defense Gateway とセキュリティポリシーがアプリケーションを保護するために適用されているかどうかを示し、アプリケーションを保護するためのワークフローを呼び出す機能を提供します。

ロード バランサ

ロードバランサは、通常、応答時間を増やし、ネットワーク遅延を短縮することで、アプリケーションのパフォーマンスを向上させます。サーバー間で負荷を均等に分散してアプリケーションのパフォーマンスを向上させたり、クライアント要求を地理的に近いサーバーにリダイレクトして遅延を短縮したりするなど、いくつかの重要なタスクを実行します。

ロードバランサとサポートされているクラウド サービス プロバイダー

現時点では、AWS ゲートウェイのロードバランサを設定できます。

Multicloud Defense でロードバランサを設定すると、[パブリック（Public）] フィールドに、リソースがインターネット側のロードバランサであるかどうかが表示されます。[CSP WAFが有効（CSP WAF Enabled）] は、CSP WAF がアプリケーション ロード バランサに対して有効になっているかどうかを示します。

Instances

[インスタンス（Instances）] には、すべてのインスタンスのリストと、リソースに割り当てられて設定されているセキュリティグループとインターフェイスの数に関するサマリー情報が表示されます。[インバウンドパブリックである（Is Inbound Public）] フィールドと [アウトバウンドパブリックである（Is Outbound Public）] フィールドは、オープンなセキュリティグループ（0.0.0.0/0）で設定されたネットワークインターフェイスを持つインスタンス、またはインターネットへのデフォルトアクセスを許可するルートテーブルを示します。

タグ

[タグ（Tags）] には、タグが設定されているすべての VPC/VNet、サブネット、セキュリティグループ、インスタンス、およびロードバランサのリストが表示されます。

証明書

[証明書（Certificates）] には、AWS 証明書マネージャで使用可能なすべての証明書のリストと、発行者、ドメイン名、および有効期限に関する概要情報が表示されます。

トポロジ

このタブには、クラウドアカウントのクラウドアセットのリージョン別の概要マップビューが表示されます。画面の上部にある [フィルタ（Filter）] バーを使用して、表示を微調整できます。ここから、データを取得するクラウドサービスプロバイダーのアカウント、リージョン、特定の VNet または VPC、インスタンス、および履歴の期間を決定できます。

世界地図の [グローバルビュー（Global View）] では、スクロールすることで上記のフィルタバーで指定した特定のリージョンを詳しく確認できます。マップのすぐ左側で、表示するトラフィックとインベントリのタイプを指定できます。表示する項目のチェックボックスを適宜オンまたはオフにします。

インサイト

インサイトは、AWS、Azure、および GCP で検出されたアセットのルールベースの評価であり、調査結果として表示されます。

ルール（Rule）

ルールは、検出されたアセットの調査結果を特定するための評価のセットです。Multicloud Defense は、デフォルトルールのセットを提供します。新しいルールを作成するには、インベントリカテゴリ（セキュリティグループ、アプリケーション、ロードバランサ、タグなど）を選択し、検索条件を定義し、[ルールの追加（Add Rule）] を選択して、必要な追加情報を指定します。**[インサイト（Insights）]** > **[ルール（Rules）]**に移動して、新しいルールを表示します。そこから、既存のアセットと新しく検出されたアセットを操作できます。

調査結果

調査結果とは、定義されたルールのセットに一致する検出されたアセットのリストです。

ルールと調査結果

クラウドリソースにチェックとガードレールを配置するようにルールを設定できます。

ルールと調査結果

クラウドリソースにチェックとガードレールを配置するようにルールを設定できます。

定義済みルール

Multicloud Defense Controller には、以下に示すような基本的な定義済みルールがいくつかあります。

- クラウド サービス プロバイダーの WAF が有効になっていないアプリケーション ロード バランサ。
- 入力ポートが開いていて、インスタンスがほとんどない（5 個未満）セキュリティグループ。使用率の低いセキュリティグループが多数あると、認識されにくいギャップが生まれ、簡単にエクスプロイトできるようになる可能性があります。
- 2 つ以上のネットワークインターフェイスを持つインスタンス。
- オープンなアウトバウンド（0.0.0.0/0）アクセスを持つセキュリティグループ。
- パブリックサブネット：[パブリックIPの自動割り当て（Auto-Assign Public IP）] が有効になっているすべての AWS サブネット。
- インターネットに対して開いている出力ポートが多すぎる（25 個以上）セキュリティグループ。
- インターネットに対して開いている入力ポートが多すぎる（5 個以上）セキュリティポート。
- パブリックアクセスが有効で、入力用に 65,535 個のポートが開いているセキュリティグループ。
- 30 日後に期限切れになる証明書：AWS Certificate Manager のみ。

ルールに一致するクラウドリソースには、重大度が一致する結果としてフラグが付けられます。

カスタムルールについては、定義済みルール （9 ページ） を参照してください。

シスコの規則

ユーザーは、リソースに追加のルールを設定できます。

1. **[検出（Discovery）]** > **[インベントリ（Inventory）]**に移動し、リソース（ロードバランサなど）を選択します。
2. テキストエリアでルール条件を作成し、[ルールの追加（Add Rule）] を選択します。
3. 次の項目の内容と、ルール条件を満たす検出結果の数を入力します。
   - 名前
   - 説明
   - 重大度
   - デフォルト アクション
   - Type
   - アカウント
4. [保存（Save）] をクリックします。

ルールのデフォルトアクションは、[情報（Info）] または [アラート（Alert）] のいずれかです。デフォルトアクションが「アラート」に設定されているルールの場合、ルールに新しい検出結果が見つかると、Multicloud Defense Controller からアラート通知が送信されます。デフォルトアクションをアラートにする場合は、次の設定が必要です。

- [アラートプロファイル（Alert Profile）] を設定し、ユーザーが ServiceNow、PagerDuty、または Webhook 通知を希望するかどうかを指定します。
- [検出タイプのアラートルール（Alert Rule of type Discovery）] と [インサイトルール（Insights Rule）] のサブタイプを、指定の重大度レベルと一緒に設定します。

調査結果

事前定義されたルールとカスタムルールに基づいて、リソースの調査結果を表示できます。簡単にアクセスできるように、[調査結果の概要（Findings Summary）] がダッシュボードおよび [インベントリ（Inventory）] タブの [概要（Summary）] ビューにも配置されています。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。