Multicloud Defense について

Multicloud Defense について

Multicloud Defense（MCD）は、Multicloud Defense Controller と Multicloud Defense Gateway の 2 つの主要コンポーネントで構成される包括的なセキュリティソリューションです。これらのコンポーネントが連携してセキュアなマルチクラウド環境を確立します。

Multicloud Defense は現在、Amazon Web Services（AWS）、Azure、Google Cloud Platform（GCP）、および Oracle OCI クラウドアカウントをサポートしています。これらのプラットフォームのサポート範囲はさまざまです。

本質的に、Multicloud Defense は高機能の合理化されたセキュリティフレームワークを提供し、コントローラのオーケストレーション、ゲートウェイ通信、および最適化されたデータパス処理を調和させ、堅牢で効率的なマルチクラウド保護メカニズムを実現します。

このドキュメントは、パブリック クラウド ネットワーキングとセキュリティの概念の基本を理解するために準備されており、以下を含むさまざまな職務チームに参加する実務者を対象としています。

- 開発（DevOps および DevSecOps）
- セキュリティ オペレーション センター（SOC）
- セキュリティアーキテクト情報
- セキュリティ アーキテクト クラウド アーキテクト

Multicloud Defense に関するその他の資料

Multicloud Defense の詳細については、次のドキュメントを参照してください。

- Multicloud Defense Release Notes

Multicloud Defense の命名規則

Multicloud Defense はさまざまなクラウド サービス プロバイダーと対話するため、プラットフォーム全体で普遍的なエクスペリエンスを提供するために、ゲートウェイとオブジェクトの作成時の文字数に制限を設けています。Multicloud Defense の外部に存在するゲートウェイとオブジェクトには、名前の前に `ciscomcd` が付加されます。そのため、元のゲートウェイまたはオブジェクトの名前が長すぎると、問題が発生する可能性があります。

Multicloud Defense の内部と外部のどちらであっても、ゲートウェイまたはオブジェクトに名前を付ける場合は、次の文字数制限を考慮してください。

表 *1*: 命名規則の文字数制限

Multicloud Defense の機能	文字制限
ゲートウェイインスタンス	55
オブジェクト名	63

（注） 上記の値は、Multicloud Defense タグが付加されて**いない**名前の文字数制限を示します。ゲートウェイまたはオブジェクトに名前を付けるときにタグを含める必要はありません。

サポート対象のリージョン

Multicloud Defense は次のリージョンをサポートします。

- 米国（US）：us-west-2
- 欧州（EU）：eu-central-1
- 東京（APJ）：ap-northeast-1
- シドニー（APJ）：ap-southeast-2
- ムンバイ（APJ）：ap-south-1

Multicloud Defense コンポーネントの推奨バージョン

機能拡張や新機能、およびバグ修正のための最新のアップグレードおよび更新を使用して、コンポーネントを最新の状態に保つことをお勧めします。利用可能な更新やアップグレード、および各パッケージで扱う内容の詳細については、『Cisco Multicloud Defense リリースノート』を参照してください。

サードパーティ製品のサポートとバージョン管理

Multicloud Defense では追加の製品と機能を利用しています。最適な動作のために、リストされている適切なバージョンを使用することを検討してください。

インターネットブラウザ

現時点で、Multicloud Defense は、コントローラダッシュボードを表示する際に **Chrome** ブラウザの使用をサポートおよび推奨しています。

AWS でのインスタンス メタデータ サービス

インスタンス メタデータ サービス（IMDS）は、Amazon EC2 インスタンスからインスタンス メタデータにアクセスするために使用されます。Multicloud Defense Controller バージョン 23.10 では、対応する Multicloud Defense Gateway バージョンに応じて IMDSv2 が [必須（Required）] または [任意（Optional）] に設定されます。

Amazon EC2 インスタンスで最適なセキュリティを確保するために、[必須（Required）] モードの IMDSv2 を特にサポートする Multicloud Defense Gateway バージョンにアップグレードすることを**強く**お勧めします。

（注） Multicloud Defense Controller バージョン23.10 では、Multicloud Defense Gateway バージョン 23.04 以降は EC2 インスタンス向けに IMDSv2 が強制的にデフォルトに設定されます。

次の表を使用して、お使いの環境の EC2 インスタンス内で設定される IMDS のバージョンを判断してください。

Multicloud Defense Gateway バージョン	必要な IMDS バージョン
23.08	IMDSv2（必須）
23.06	IMDSv2（必須）
23.04	IMDSv2（必須）
23.02	IMDSv1 IMDSv2（任意）
22.12	IMDSv1 IMDSv2（任意）

IMDS のバージョンと、選択したバージョンへの移行方法の詳細については、AWS のドキュメントを参照してください。

サポートされるディスクサイズ

適切なゲートウェイバージョンに対する次のディスクサイズのサポートを検討してください。

表 *2:* ゲートウェイバージョンごとのディスクサイズ

ゲートウェイバージョン	サポートされるディスクサイズ
23.12 以降	128GB
23.10 まで	256GB

Cisco Security Provisioning and Administration でのMulticloud Defense

Security Provisioning and Administration は、Cisco Security Cloud 全体で Cisco Secure 製品インスタンス、ユーザーアイデンティティ、およびユーザーアクセス管理を集中管理できる Web アプリケーションです。Security Provisioning and Administration の管理者は、新しい Security Cloud エンタープライズの作成、エンタープライズ内のユーザーの管理、ドメインの要求、組織の SSO アイデンティティプロバイダーの統合などのタスクを実行できます。

Multicloud Defense に登録すると、エンタープライズ全体をより適切に管理するため、Security Provisioning and Administration はデフォルトでテナントのアカウントを作成します。Security Cloud エンタープライズは、ライセンスを購入してすでに Multicloud Defense アカウントを持っている場合、およびライセンスを購入したが現在 Multicloud Defense アカウントを持って**いない**場合をサポートします。

Note that

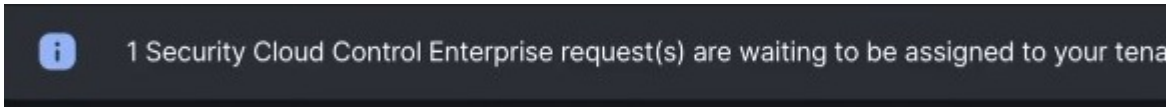
Security Provisioning and Administration ダッシュボードで次の手順を実行する必要があります。これらの手順の詳細については、『Cisco Security Provisioning and Administration ユーザーガイド』を参照してください。

1. サブスクリプションライセンスを購入します。購入が完了すると、お客様または指定されたシステム管理者に、サブスクリプション**要求コード**が記載された電子メールが送信されます。この電子メールは失くさないようにしてください。
2. サブスクリプションを要求します。上記の電子メールに記載されている要求コードが必要です。詳細については、『製品およびサブスクリプションの管理』を参照してください。
3. インスタンスをアクティブ化します。この「インスタンス」は、Cisco Defense Orchestrator のテナントにアタッチされている Multicloud Defense アカウントを指します。詳細については、『製品インスタンスのアクティブ化』を参照してください。

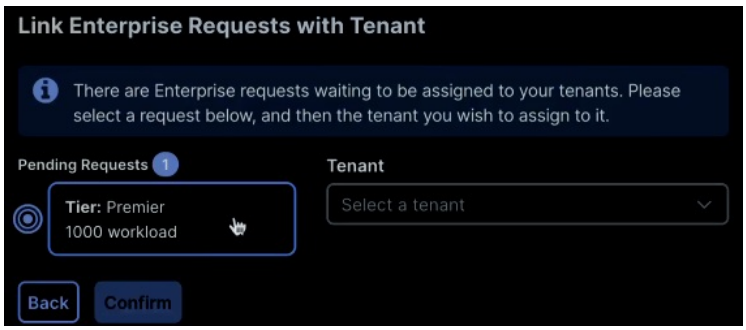
警告 新規または既存のインスタンスをアクティブ化するように求められます。エンタープライズにまだ存在**しない** Multicloud Defense アカウントにライセンスを適用するには、[新しいインスタンスのアクティブ化（Activate a new instance）] を選択します。[既存のインスタンスにライセンスを適用（Apply license to an existing instance）] オプションは、Security Cloud エンタープライズにすでに登録されている Multicloud Defense インスタンスにライセンスを適用します。

（注） CDO テナントに関連付けられた Multicloud Defense アカウントが**まだない**場合は、「`Do you have an existing Cisco Defense Orchestrator Account to associate with your Multicloud Defense License?`」というメッセージが表示されたら、[いいえ（No）] を選択します。これにより、CDO テナントの要求が生成され、Multicloud Defense を要求して有効にすることができます。[いいえ（No）] を選択した場合は、手順 4 を無視します。

4. アクティベーションを確認します。この手順はCDOで行います。アクティベーションボタンをクリックしてアクティベーションを確認する**必要があります**。このボタンは、次に示すように、ダッシュボード画面の上部付近に新しいバナーとして表示されます。



（注） アクティベーションを確認したら、Multicloud Defense アカウントのパフォーマンス階層を選択する必要があります。製品のトライアルライセンスかフルライセンスかによって、表示されるオプションは次のスクリーンショットと異なる場合があります。



Multicloud Defense のコンポーネント

Multicloud Defense は、パブリッククラウドとソフトウェア定義型ネットワーキング（SDN）の共通原則を使用して、コントロールプレーンとデータプレーンを分離し、Multicloud Defense Controller と Multicloud Defense Gateway の 2 つのソリューション コンポーネントに変換します。

Multicloud Defense Controller

Multicloud Defense Controller は、管理プレーンとコントロールプレーンを提供する、信頼性の高い拡張性に優れた集中型コントローラです。これは Software-as-a-Service（SaaS）として実行され、Multicloud Defenseによって完全に管理および保守されます。お客様は、Web ポータルにアクセスして Multicloud Defense Controllerを利用するか、Terraform の Multicloud Defense プロ

バイダーを使用して、DevOps /DevSecOps プロセスにセキュリティをインスタンス化することもできます。

Multicloud Defense Gateway

Multicloud Defense Gateway は、Multicloud Defense Controller によって顧客のパブリック クラウド アカウントに Platform as a Service（PaaS）として展開される Multicloud Defense ソフトウェアの自動スケーリングフリートです。これにより、外部からの攻撃を防御し、出力データの漏洩を防ぎ、攻撃のラテラルムーブメントを防ぐための高度なインラインセキュリティ保護が提供されます。Multicloud Defense Gateway には、TLS 復号、侵入検知および侵入防御（IDS/IPS）、Web アプリケーション ファイアウォール（WAF）、ウイルス対策フィルタリング、データ損失防止（DLP）、および FQDN /URL フィルタリング機能が含まれます。

重要 Multicloud Defense Gateway は、クラウドサービスプロバイダーのロードバランサの制限により、現在 IP フラグメンテーションをサポートしていません。フラグメンテーションが必要にならないように、最大伝送ユニット（MTU）サイズを調整してネットワーク全体で一貫性を保つことを**強く**お勧めします。

Multicloud Defense SaaS コントローラ

Multicloud Defense SaaS コントローラはゲートウェイスタックを管理します。コントローラにはさまざまなマイクロサービスが搭載されており、クラウドサービスプロバイダー LB とゲートウェイインスタンスのオーケストレーションを促進する API サーバーが含まれています。これにより、ロードバランサ自体がモニターする、ロードバランサの「ターゲットプール」からのインスタンスの追加と削除による動的スケーリングが可能になります。

設定

Multicloud Defense Gateway は、約 3 秒ごとに Multicloud Defense Controller と継続的な通信を行い、正常性ステータスとポリシーの更新情報を送信します。これにより、プロアクティブな正常性レポート、ゲートウェイの交換、および必要に応じた拡張性の調整が可能になります。

最適化されたゲートウェイインスタンス

Multicloud Defense Gateway インスタンスは高度に最適化されたソフトウェア上で動作し、効率的なトラフィック処理と高度なセキュリティの適用のための単一パスのデータパスパイプラインを組み込んでいます。各ゲートウェイインスタンスは、ポリシーの適用を担当する「ワーカー」プロセス、トラフィック分散とセッション管理を行う「ディストリビュータ」プロセス、コントローラと通信する「エージェント」プロセスの 3 つのコアプロセスで構成されます。ゲートウェイインスタンスは、「データパスの再起動」のために「サービス中」にシームレスに移行できるため、トラフィックフローを中断することなくスムーズな更新が可能になります。

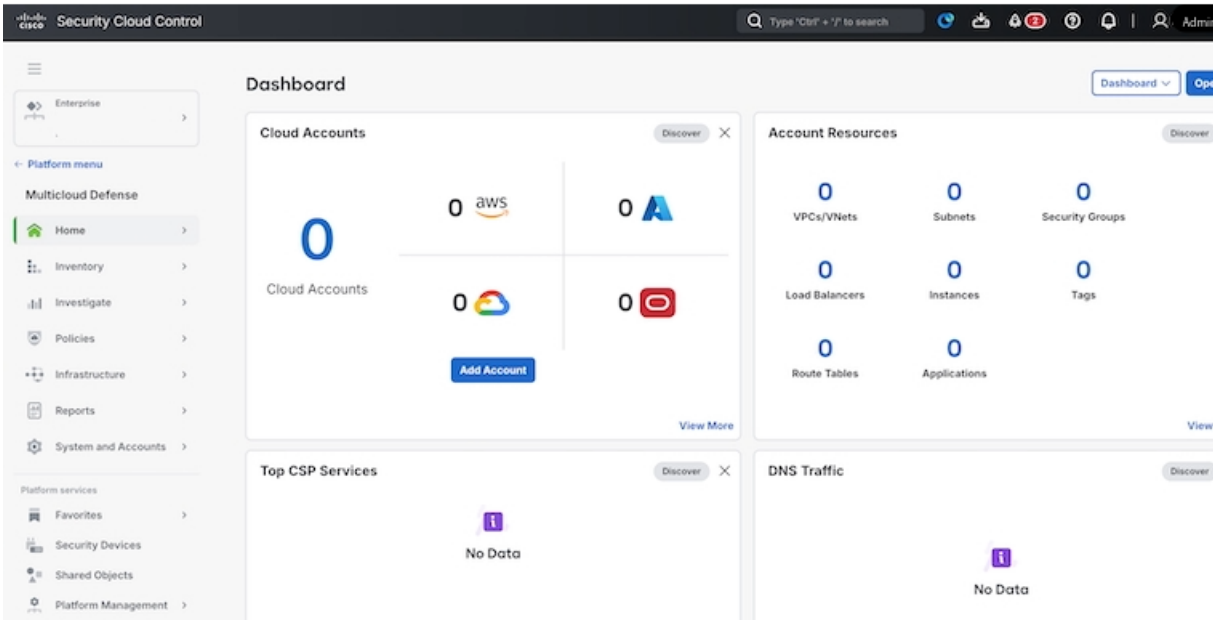
高度なセキュリティプロファイル

Multicloud Defense Gateway は、単一パスのデータパスパイプライン内にきめ細かいセキュリティプロファイルを実装し、進化するトラフィックのニーズに対応します。お客様は、必要に応じて柔軟に[高度なセキュリティプロファイル（Advanced Security Profiles）]を有効または無効にすることができます。パイプラインの単一パスアーキテクチャにより、サードパーティエンジンにトラフィックをオフロードする必要がなくなります。たとえば、完全な TLS 復号はパイプライン内で選択的にトリガーされるため、不要なデータ転送を行わずに効率的に処理できます。

本質的に、Multicloud Defense は高機能の合理化されたセキュリティフレームワークを提供し、コントローラのオーケストレーション、ゲートウェイ通信、および最適化されたデータパス処理を調和させ、堅牢で効率的なマルチクラウド保護メカニズムを実現します。

Multicloud Defense Controller ダッシュボード

Multicloud Defense Controller のダッシュボードには、アカウント、アカウントリソース、および上位のポリシーまたはプロファイルの現在の状態を一目で確認できる多数のウィジェットがあります。



次のウィジェットのいずれかをドラッグアンドドロップすると、ダッシュボードを必要に応じてカスタマイズして整理することができます。また、ウィジェットの [x] をクリックしてダッシュボードビューから削除したり、[詳細情報（View More）]をクリックして対象のウィジェットに関連付けられているページに直接移動したりすることもできます。各ウィジェットの上部には、ウィジェットが提供する Multicloud Defense の機能（検出、検知、展開、防御）が示されます。

デフォルトでは、次のウィジェットが生成されます。

クラウドアカウント

これは、Multicloud Defense Controller に接続しているクラウドアカウントの数と、クラウド サービス プロバイダーの種類と数を示す概要レベルのビューです。

このウィジェットから [アカウントの追加（Add Account）] をクリックすると、接続ウィザードが起動し、新しいクラウド サービス プロバイダーのオンボーディングをサポートします。

アカウントリソース

これは、接続されているすべてのクラウドアカウントに割り当てられているリソースの一般的なリストです。次のリソースのうち、現在使用されているリソースの数が表示されます。

- VPC/VNet。
- サブネット。
- セキュリティ グループ。
- ロードバランサ。
- インスタンス。
- タグ。
- ルートテーブル。
- [アプリケーション（Applications）]。

上位 CSP サービス（Top CSP Services）

クラウドサービスプロバイダーサービスをトップダウンで示すこの表示は、Multicloud Defense Controller にすでに接続しているクラウド サービス プロバイダーの DNS トラフィックを一般化するものです。

DNS トラフィック

「上位 CSP サービス」と同様に、この DNS トラフィックウィジェットは、トラフィックをアクティブに処理しているクラウド サービス プロバイダーの現在の DNS トラフィックを限定的に表示します。より多くのインサイトを得るために、ウィジェットを検出範囲全体に拡張することをお勧めします。

悪意のあるトラフィックが発生した VPC/VNet（VPCs/VNets with Malicious Traffic）

このウィジェットには、悪意のあるトラフィックが発生した最近の VPC または VNet が表示されます。イベントと攻撃の包括的なリストを確認するには、ウィジェットを拡張してトラフィックを表示します。

悪意のあるトラフィックが発生した上位ポート（Top Ports with Malicious Traffic）

この小さなスナップショットには、クラウドアカウントの中で、悪意のあるトラフィックが最もヒットしたポートが表示されます。

セキュリティに関する注意事項

[セキュリティに関する注意事項（Security Considerations）] ウィジェットは、Multicloud Defense が提供する手段では保護されないアプリケーション、VPC または VNet、および関連するゲートウェイを要約する提案型のウィジェットです。

システム ログ

[システムログ（System Logs）] ウィンドウには、アカウントが影響を与えるログ、関連付けられているゲートウェイ、イベントまたは攻撃の重大度などをカタログ化する、最近のログ履歴が表示されます。このウィジェット、そうでなければ [システムログ（System Log）] ページ全体を貴重なリソースとして利用することを強くお勧めします。

最上位アプリケーション（Top Applications）

このウィンドウは、使用されているすべてのクラウドサービスプロバイダーの上位アプリケーションを示します。

脅威

過去7日間のトラフィックと、脅威として分類された着信トラフィックの量を示すグラフを表示します。

脅威別の上位国（Top Countries by Threat）

この水平棒グラフは、期間全体で最も多くのイベントが作成された上位 10 か国のスナップショットを示し、さらにそのボリュームを期間中にイベントが発生した時間単位で分割して表示します。

データ漏えいの試み（Exfiltration Attempts）

現在 Multicloud Defense に接続しているクラウド サービス プロバイダーで発生した出力データ漏えいの一般的な表示を確認できます。

マイプロファイル情報（My Profile Information）

[ユーザープロファイル（User Profile）] ページは、ユーザー情報の詳細を表示するページです。このページにアクセスするには、Multicloud Defense ダッシュボードの右上隅にある [管理（Admin）] 矢印をクリックします。ユーザー名をクリックすると、次の情報が表示されます。

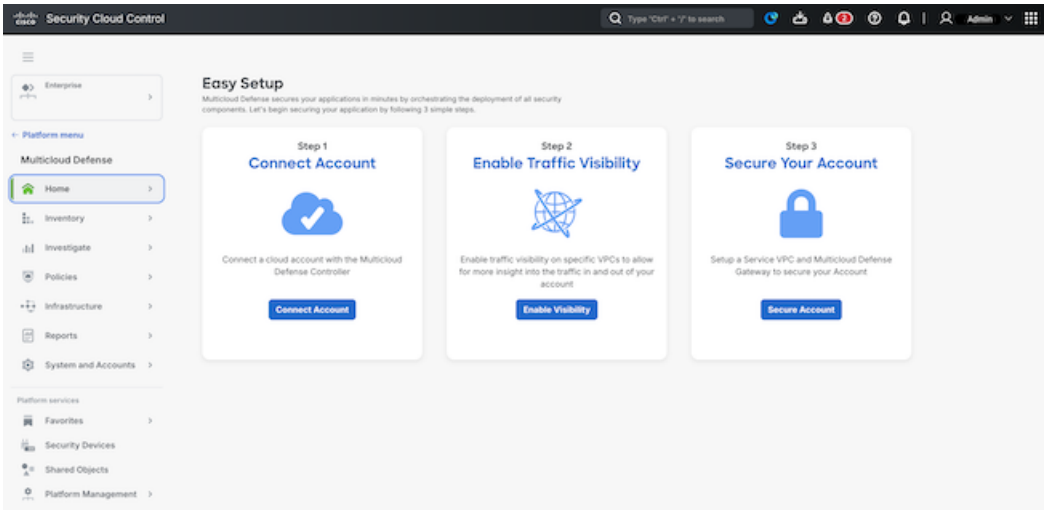
- 自分の名前。
- Multicloud Defense アカウントに関連付けられている電子メールアドレス。
- 現在のユーザーロール。
- 現在ログインしているテナントの名前。
- 割り当てられたすべてのアカウント。

このページは、一般的な知識を得る場合や、シスコサポートチームにサポートを求める場合に役立ちます。

Multicloud Defense 90 日間無料トライアル

CDO テナントにログすると、お使いのクラウドアカウントを Multicloud Defense に接続し、Multicloud Defense Controller の 90 日間無料トライアルを使用してクラウドアカウントを管理できるようにする手順を案内するウィザードが表示されます。90 日間のトライアルでは、Multicloud Defense Controller の有料サブスクリプションの全機能を利用できます。

図 *1 : Multicloud Defense* 簡単セットアップ



[始める（Get Started）] をクリックして、90 日間のトライアルを開始します。Multicloud Defense Controller のプロビジョニングプロセスが開始されます。

（注） 簡単セットアップは、次のクラウドプロバイダーをサポートしています。

- アカウントのオンボーディング：AWS、Azure、GCP、OCI
- トラフィックの可視性の有効化：AWS（フローログ、DNS クエリログ）、Azure（フローログ）、GCP（VPC フローログ、DNS クエリログ）
- サービス VPC/VNet の作成：AWS、Azure、GCP
- ゲートウェイの作成：AWS、Azure、GCP

サービス VCN のオーケストレーションは OCI ではサポートされていませんが（ユーザーがクラウドプロバイダーコンソールを使用してサービス VCN を作成する必要があります）、ゲートウェイのオーケストレーションは Multicloud Defense Controllerでサポートされています。Multicloud Defense Controller を開き、**[管理（Manage）] > [ゲートウェイ（Gateways）] > [ゲートウェイの追加（Add Gateway）]**に移動します。

クラウドアカウントの接続

Multicloud Defense Controller がプロビジョニングされると、[クラウドアカウントの接続（Connect a Cloud Account）] ページが開き、表示されている任意のタイプのクラウドアカウントを Multicloud Defense Controller に接続できます。

最初のステップは、1つ以上のクラウドアカウントのセットをオンボーディングすることです。これにより、Multicloud Defense Controller は、インベントリとトラフィックの検出、セキュリティ展開のオーケストレーション、ポリシーの作成と管理を行うことで、各アカウントと対話できるようになります。

クラウドアカウントを接続するには、次の手順に従います。

- AWS
- Azure
- GCP
- OCI

可視性の有効化

クラウドアカウントをオンボーディングしたら、そのクラウドアカウントのトラフィックの可視性を有効にします。CDO の Multicloud Defense で、[可視性の有効化（Enable Visibility）] をクリックします。

トラフィックの可視性を有効にすると、VPC/VNet フローログと DNS クエリログを収集することで、クラウドアカウント内のトラフィックフローに関する認識が深まります。Multicloud Defense はフローログと DNS クエリログを使用してトラフィックフローを理解し、脅威インテリジェンスのフィードと関連付け、Multicloud Defense を使用して保護できる既存の脅威に関するインサイトを提供します。

トラフィックの可視性を有効にするプロセスは、クラウドアカウントのタイプごとに異なりますが、一般的に、クラウドアカウントのリージョン、モニターする VPC/Vnet、ネットワークセキュリティ グループ、ログ用のクラウド ストレージ アカウントなど、アカウントの特徴を特定する必要があります。

クラウドアカウントのトラフィックの表示

トラフィックの可視性を有効にしたら、クラウドアカウントを通過するトラフィックを確認し、保護対策が必要な悪意のあるトラフィックを探します。

1. CDO にログインします。
2. 左側のペインで Multicloud Defense をクリックします。
3. 右上隅の Multicloud Defense Controller を選択して、新しいブラウザタブでコントローラを開きます。
4. Multicloud Defense ポータルで、**[検出（Discover）] > [トラフィック（Traffic）] > [トポロジ（Topology）]**に移動します。

5. [フィルタと検索（Filters and Search）] バーを使用して、モニターするクラウドアカウントを検索します。
6. [グローバルビュー（Global View）] のビューで、[悪意のあるトラフィック（Malicious Traffic）] をフィルタリングに追加します。
7. 悪意のあるトラフィックのバブルをクリックして、送信元の国、IP アドレス、FQDN、影響を受けるサービスおよびポートに関する情報を [リージョンビュー（Region View）] で確認します。

クラウドアカウントの保護

既知のセキュリティニーズに基づいて、トラフィックをモニタリングした後で、集中型ハブアンドスポークモデルまたは分散モデルを使用してアカウントを保護できます。

[アカウントの保護（Secure Your Account）] ウィザードを使用して、サービス VPC と Multicloud Defense Gateway を設定してアカウントを保護します。

1. CDO にログインします。
2. 左側のペインで Multicloud Defense をクリックします。
3. 右上隅の Multicloud Defense Controller を選択して、新しいブラウザタブでコントローラを開きます。
4. Multicloud Defense Controller ダッシュボードで、ナビゲーションパネルの [設定（Setup）] をクリックします。
5. [設定（Setup）] ページで、[アカウントの保護（Secure Account）] ボタンをクリックします。
6. [集中型（Centralized）] または [分散（Distributed）] をクリックし、[次へ（Next）] をクリックしてウィザードのセットアップを続行します。

   詳細については、Multicloud Defense Gateway の概要を参照してください。

簡単セットアップの再起動

CDO ダッシュボードの簡単セットアップのワークフローを完了し、90 日間の無料トライアルを開始した後で、簡単セットアップを再び起動させることはできません。ただし、簡単セットアップウィザードは Multicloud Defense Controller 内に存在するため、後で他のクラウドアカウントを接続したり設定したりすることができます。

1. CDO ダッシュボードの左側のペインで、Multicloud Defense をクリックします。
2. 右上隅で、Multicloud Defense Controller をクリックします。
3. Multicloud Defense ダッシュボードで、Multicloud Defense メニューバーの [設定（Setup）] をクリックします。

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。