Multicloud Defense について

- Multicloud Defense （1 ページ）
- Multicloud Defense のコンポーネント （5 ページ）
- Multicloud Defense Controller ダッシュボード （8 ページ）
- Multicloud Defense 90 日間無料トライアル （11 ページ）
- Cloud Explorer （13 ページ）

Multicloud Defense

Multicloud Defense 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。

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を実現します。

Multicloud Defense の命名規則

Multicloud Defense は、さまざまなクラウド サービス プロバイダーと連携しています。普遍的なエクスペリエンスを提供するために、Multicloud Defense 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） リストされた値は、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

現在、AWS、Azure、GCP、および OCI の商用クラウド サービス プロバイダー地域のすべてのリージョンをサポートしています。詳細については、クラウド サービス プロバイダーのマニュアルを参照してください。

あるリージョンがサポートされていない場合、または新しいリージョンにサポートが必要な場合は、シスコサポートにお問い合わせください。

Multicloud Defense コンポーネントの推奨バージョン

すべての Multicloud Defense コンポーネントが最新バージョンで更新されていることを確認して、拡張機能、新機能、およびバグ修正を利用してください。利用可能な更新の詳細と、各リリースで対処される問題については、『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。最適な動作を確保するには、ここに記載されているバージョンを使用してください。

インターネットブラウザ

現在 Multicloud Defense では、**Chrome** ブラウザを使用してコントローラダッシュボードにアクセスすることを推奨しています。

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）を使用すると、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できます。Multicloud Defense Controller バージョン23.10の場合、IMDSv2 は、使用する Multicloud Defense Gateway バージョンに基づいて **[Required]** または **[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、**[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。

EC2インスタンスに設定されているIMDSバージョンを確認するには、表を参照してください。

表 *2:* ゲートウェイバージョンと *IMDS* バージョン

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のバージョンと移行手順の詳細については、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

表に、各ゲートウェイバージョンでサポートされているディスクサイズを示します。

表 *3:* 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	128 GB
23.10 まで	256 GB

クラウド サービス プロバイダー インスタンス タイプのサポート

サポートされているクラウド サービス プロバイダー（CSP）の推奨されるインスタンスタイプは次のとおりです。

表 *4:* クラウド サービス プロバイダー インスタンス タイプのサポート

CSP	インスタンス タイプ	最大メモリ使用量（KB）	最大帯域幅使用量（プロキシ）	最大帯域幅使用量（転送）
AWS	m5.2xlarge	32,000,000	4,400,000,000	9,000,000,000
	m5.xlarge	9,000,000	2,400,000,000	4,800,000,000
	m5.large	4,500,000	1,200,000,000	2,400,000,000
	m7i	4,500,000	1,200,000,000	2,400,000,000
Azure	Standard_D8s_v3 および Standard_D8s_v5	32,000,000	2,800,000,000	4,000,000,000
	Standard_D4s_v3 および Standard_D4s_v5	9,000,000	1,200,000,000	2,400,000,000
	Standard_D2s_v3 および Standard_D2s_v5	4,500,000	1,000,000,000	1,500,000,000
GCP	e2-standard-8	32,000,000	2,500,000,000	8,000,000,000
	e2-standard-4	9,000,000	1,600,000,000	4,000,000,000
	e2-standard-2	4,500,000	1,200,000,000	2,000,000,000
OCI	VM.Standard.E3.Flex	32,000,000	2,500,000,000	: 8,000,000,000

Cisco Security Cloud Control でのMulticloud Defense

Multicloud Defense は現在 Cisco Security Cloud Control にホストされています。Security Cloud Control は、単一の統合インターフェイスからセキュリティ製品を管理し、セキュリティの成果を達成できるようにするプラットフォームです。Security Cloud Control プラットフォームから、Multicloud Defense を他のセキュリティ製品とともに管理できます。

Multicloud Defense に登録すると、Security Cloud Control はデフォルトでテナントのアカウントを作成し、エンタープライズ全体をより適切に管理します。Cisco Security Cloud エンタープライズは、次のケースに対応します。

1. ライセンスを購入しており、すでに Multicloud Defense アカウントがある場合、
2. ライセンスを購入したが、Multicloud Defense アカウントが**ない**場合。

Multicloud Defense の新規顧客またはユーザーは、Security Cloud Control でこれらの手順を完了できます。

1. 組織を作成します。詳細については、『Getting Started Guide for New Customers of Security Cloud Control』の「**組織と地域**」セクションの「**組織の作成**」トピックをで参照してください。

2. 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。

3. サブスクリプションを要求します。Security Cloud Control アプリケーションの **Claim Subscription** セクションに要求コードを入力し、製品を要求します。Multicloud Defense が Cisco Security Cloud Control でアクティブ化されていることを確認する電子メールが届きます。詳細については、『Getting Started Guide for New Customers of Security Cloud Control』の「**Claim Your Product Subscriptions**」セクションを参照してください。

Multicloud Defense はプロビジョニングされ、Security Cloud Control のデフォルトのランディングページで使用できます。Security Cloud Control のナビゲーションペインには、組織の詳細とメニュー要素が含まれ、中央のエリアにはダッシュボードウィジェットが含まれます。

（注） 2025 年 8 月 6 日以降に Multicloud Defense をプロビジョニングし、**オブジェクト共有**を使用する場合は、Cisco Technical Assistance Center（Cisco TAC）にお問い合わせの上、この機能を有効化してください。

Multicloud Defense の既存ユーザーが Security Cloud Control に移行する場合は、『Getting Started Guide for Existing Customers of Security Cloud Control』を参照してください。

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、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 Gateway

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。Webポータルにアクセスして Multicloud Defense Controller を利用できます。または、Multicloud DefenseTerraform Provider 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、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。

自動スケーリングを容易にするために、Multicloud Defense Gatewayは次の機能を提供します：

- **自動スケーリングと自己修復（Autoscaling and Self-healing）**：自動スケーリングで自己修復を行うPlatform-as-a-Service（PaaS）として機能し、インラインネットワークベースのセキュリティ施行ノードとして機能します。自動スケーリングおよびゲートウェイの構造内でどのように動作するかの詳細については、以下を参照してください。
- **簡素化された管理（Simplified Management）**：仮想ファイアウォールの構築、高可用性セットアップの設定、またはソフトウェアインストールの管理を行う必要がありません。
- **高度なセキュリティプロファイル（Advanced Security Profiles）**：シングルパス データパスパイプライン内に詳細なセキュリティプロファイルを導入することで、サードパーティの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。

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。このソリューションは、組織がクラウドワークロードとアプリケーションをサイバー脅威から保護すると同時に、クラウド環境の柔軟性と拡張性を維持するのに役立ちます。

- **SaaS ベースの管理（SaaS-Based Management）**：Software-as-a-Service（SaaS）コントローラは、ゲートウェイスタックを管理します。また、CSP ロードバランサ（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用の API サーバーが含まれています。
- **動的スケーリング（Dynamic Scaling）**：高可用性用に監視され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および削除により、動的な水平スケーリングが容易になります。
- **継続的な通信（Continuous Communication）**：クラウド サービス プロバイダー（CSP）アカウントとの継続的な通信で、セキュリティポリシーを最新の状態に保つことができます。

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。

ゲートウェイの自動スケーリング

Multicloud Defense での自動スケーリングは、次の使用量しきい値に基づいてトリガーされます。

- **CPU Usage**
  - スケールアウト：CPU 使用率が 95% を超えるとトリガーされます。
  - スケールイン：CPU 使用率が 40% 未満になると発生します。
- **メモリ使用率**
  - スケールアウト：メモリ使用率が 85% を超えるとトリガーされます。
  - スケールイン：メモリ使用率が 40% 未満になると発生します。
- **Bandwidth Usage**
  - スケールアウト：帯域幅使用率が 75% を超えるとトリガーされます。
  - スケールイン：帯域幅使用率が 40% 未満になると発生します。
- **接続使用率**
  - スケールアウト：接続使用率が 75% を超えるとトリガーされます。
  - スケールイン：接続使用率が 40% 未満になると発生します。
- **負荷持続期間**：負荷条件が 120 秒間持続すると、自動スケーリングアクションがトリガーされます。
- **スケールインおよびスケールアウト期間**：スケールインおよびスケールアウトのアクションの両方に、一貫した負荷条件を確保するための 120 秒のアセスメント期間があります。

特定のクラウド サービス プロバイダーとそのインスタンスタイプのサポートについては、クラウド サービス プロバイダー インスタンス タイプのサポート （3 ページ） を参照してください。

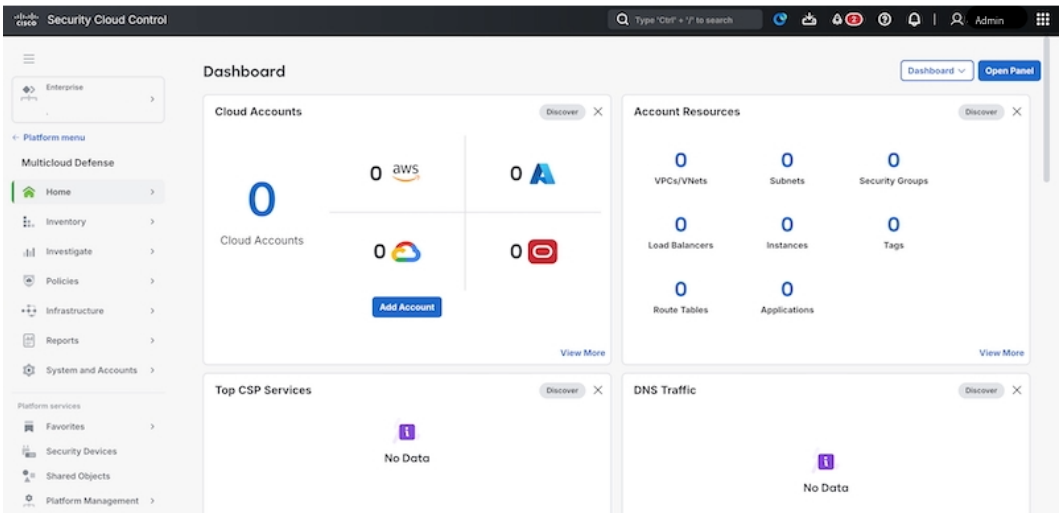
高度なセキュリティプロファイル

Multicloud Defense Controller 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。ウィジェットから削除するには、ウィジェットの右上隅にある「x」をクリックします。ウィジェット内にある **[View More]** をクリックすると、関連するページに直接移動してアカウントを追加できます。各ウィジェットの上部には、ウィジェットが提供する機能（検出、検知、展開、防御）が示されます。

ダッシュボードは、デフォルトでこれらのウィジェットを生成します。

クラウドアカウント

これにより、Multicloud Defense Controller に接続したすべてのクラウドアカウントの概要レベルのビューと、特定されたクラウド サービス プロバイダーごとのアカウント数が表示されます。

[Add Account] をクリックすると、新しいクラウド サービス プロバイダーをオンボーディングするための接続ウィザードが開きます。

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。これらのリソースのうち、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
- Instances
- タグ（Tags）
- 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）

Multicloud Defense Controller はクラウド サービス プロバイダーに接続し、ドメイン名システム（DNS）トラフィックを一般化したトップダウンビューを表示します。

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

[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

[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。このウィジェットまたは [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）

このウィジェットには、すべてのクラウド サービス プロバイダーで使用されている上位のアプリケーションが表示されます。

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）

この横棒グラフでは、イベントが最も多い上位 10 か国を示し、時間の増分ごとにボリュームを分類します。

データ漏えいの試み（Exfiltration Attempts）

このビューでは、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）

[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 **[Admin]** ドロップダウンリストからユーザー名を選択して、情報を表示します。

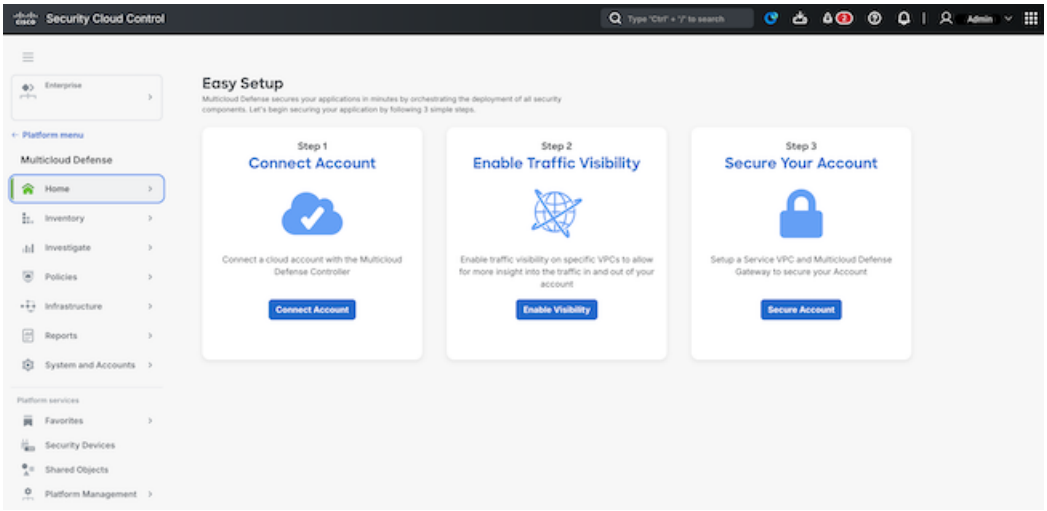
- 自分の名前。
- Multicloud Defense アカウントに関連付けられている電子メールアドレス。
- 現在のユーザーロール。
- 現在ログインしているテナントの名前。
- 割り当てられたアカウント

一般的な情報を知りたい場合、またはシスコサポートに支援を依頼する際には、このページをご利用ください。

Multicloud Defense 90 日間無料トライアル

Security Cloud Control テナントにログインすると、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



[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 DefenseMulticloud Defenseでサポートされています。Multicloud Defense を開き、 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

オンボーディング後、クラウドアカウントのトラフィックの可視性を有効にするには、Multicloud Defense の Security Cloud Control で **[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タイプごとに異なりますが、通常は、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 アカウントといったアカウント特性を識別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. Security Cloud Control 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. 右上隅にある **[Multicloud Defense Controller]** をクリックして、コントローラを新しいブラウザタブで開きます。
4. Multicloud Defense ポータルで、 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. **[Global View]** のビューで、**[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、**[Region View]** で影響を受けた国、IP アドレス、FQDN、サービス、およびポートに関する情報を確認します。

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。

[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. Security Cloud Control 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. 右上隅にある **[Multicloud Defense Controller]** をクリックして、コントローラを新しいブラウザタブで開きます。
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. **[Setup]** ページで、**[Secure Account]** をクリックします。
6. **[Centralized]** または **[Distributed]** をクリックします。
7. **[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。

簡単セットアップの再起動

Security Cloud Control 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は、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. Security Cloud Control 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. 右上隅にある **[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。

Cloud Explorer

Cloud Explorer は、クラウドアセットとその関係をグラフィカルに可視化できるように設計されています。サービス VPC、VPC/VNet、サブネット、インスタンスなどのコンポーネントを含むネットワークトポロジの包括的なビューを提供します。この可視化により、ユーザーは単

一のインターフェイス内のリソースの構造と相互接続を管理できます。Explorer は、クラウドインフラストラクチャを可視化し、これらのアセットとその相互接続を管理し、保護することを望むユーザーにとって役立ちます。大量のクラウドインフラストラクチャと接続を管理するには、それらを手動で作成するか、Terraform を使用します。

Cloud Explorer の主な機能は次のとおりです。

- グラフィカル表示：クラウドリソースの明確な視覚的なトポロジを表示することで、アセット間の関係を把握しやすくなります。
- インタラクティブな資産管理：ユーザーはグラフィカルインターフェイスを操作して、リソースを効果的に管理および保護できます。
- 統合されたセキュリティ態勢：Cloud Explorer インターフェイス内のアセットを直接保護することにより、ユーザーは自分のセキュリティポスチャを構築し、強化できます。

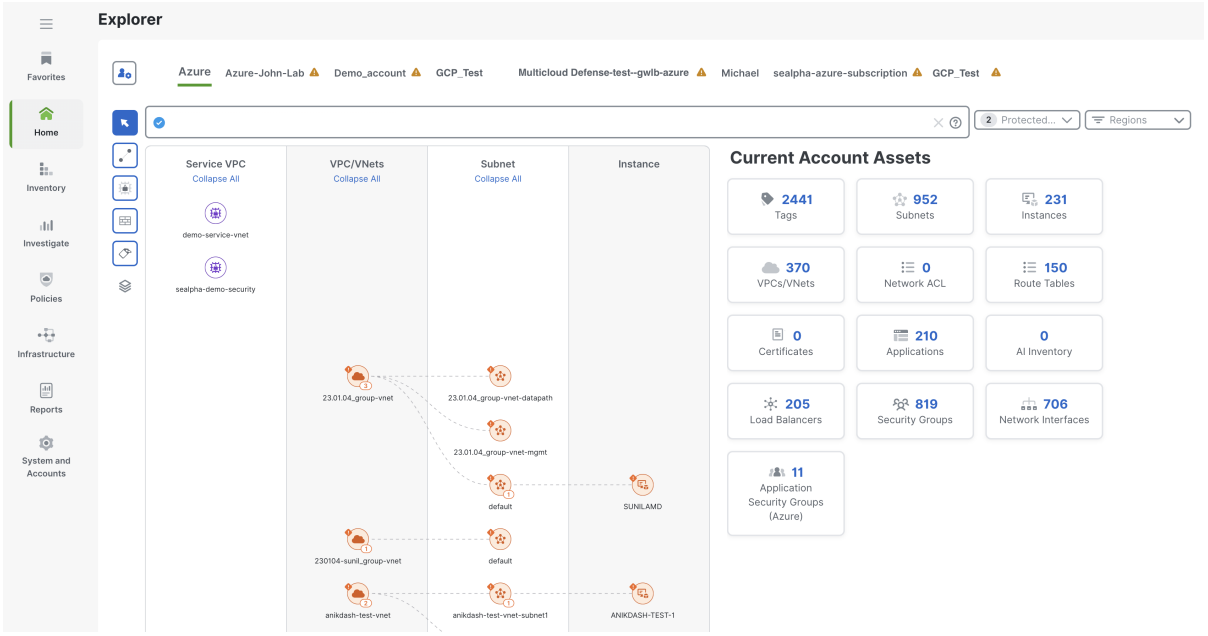
Cloud Explorer の利点は次のとおりです。

- 可視性の強化：すべてのクラウドアセットとその相互接続の統合ビューを提供することで、リソース管理が簡素化されます。
- セキュリティの向上：ユーザーは、サービス VPC とゲートウェイを作成し、簡単なドラッグアンドドロップ操作でリソースを保護し、アセットを接続する線を引くことで、アセットを保護できます。
- 使いやすさ：直感的なインターフェイスで複雑な設定を簡素化し、ユーザーはアセットに対してすぐにアクションを実行できます。
- シナリオベースの有用性：ユーザーがリソースの関係を理解したり、セキュリティ態勢を動的に強化したりする必要があるシナリオで特に役立ちます。

Cloud Explorer にアクセスするには、**[Home]** > **[Explorer]** の順に選択します。

アカウントを作成するか、アカウントを選択してビューアに追加するには、アイコン（ ）をクリックします。

図 *2 : Cloud Explorer*



左側のペインにあるアイコンを使用して、次のアクションを実行します。

- 移動（）：ドラッグアンドドロップアクションで、アセットをプールレーン間で移動します。
- セキュア（）：アセット間の接続を確立し、関連する画面で設定することにより、アセットを保護します。たとえば、サービス VPC アイコンをクリックしてドラッグして線を形成し、次のレーンの VPC に接続します。表示される関連画面で、VPC を設定して保護します。
- SVPC の追加（）：アイコンをクリックし、サービス VPC を [**Service VPC**] プールレーンにドロップします。これにより、詳細を入力できる [**Create Service VPC**] のドロワが開きます。
- ゲートウェイの追加（）：アイコンをクリックし、ゲートウェイをレーンにドロップします。これにより、詳細を入力できる **[Create Gateway]** のドロワが開きます。
- タグの追加（）：選択したオブジェクトにタグを追加します。 をクリックして、ディスプレイに表示するタグを 3 つまで選択します。

中央のエリアまたはキャンバスには、サービス VPC、VPC/VNet、サブネット、およびインスタンスのプールレーンが含まれます。含めるアセットは、レーンに表示されます。アセットをクリックし、ゲートウェイの追加、アセットの保護、アセットのポリシーの作成などのアクションを実行します。 アセットをクリックして、すべてのアセットの接続のビューを展開または折りたたむこともできます。

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。