

はじめに

Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのプラットフォームで、Cisco のファイアウォールおよびデバイス全体でセキュリティポリシー管理を統合し、簡素化します。ポリシーの一貫性が合理化され、直感的で高度なインターフェイスが提供され、複数のデバイスマネージャ間での設定の変更が調整されます。

- Security Cloud Control を使用した Meraki の管理, on page 1
- Cisco Security Cloud Control の概要 （4 ページ）
- Security Cloud Control によってサポートされる製品およびソリューション （5 ページ）
- Security Cloud Control Firewall Management の概要 （6 ページ）
- ファイアウォール管理ダッシュボード （7 ページ）

Security Cloud Control を使用した Meraki の管理

Cisco Meraki デバイスを Security Cloud Control にオンボードすると、Security Cloud Control は Cisco Meraki ダッシュボードと通信してそのデバイスを管理します。Security Cloud Control は MX デバイスと直接通信しません。

Security Cloud Control は設定要求を Cisco Meraki ダッシュボードに安全に転送し、その後ダッシュボードが新しい設定をデバイスに適用します。詳細については、Security Cloud Control と Meraki の通信方法, on page 3を参照してください。

Security Cloud Control は、オブジェクトとポリシーの問題を特定し、考えられる修正や代替オプションを提案することで、Cisco Meraki 環境を最適化するツールを提供します。これは、デバイスとテンプレートの両方に関連付けられたポリシーに適用されます。Security Cloud Control を使用して次のことができます。

- 1 つ以上の Meraki デバイスでポリシーを同時に管理します。
- 包括的な環境で、FTD および Cisco ASA デバイスとともに Cisco Meraki ポリシーまたはテンプレートを監視および管理します。
- Meraki テンプレートを使用して複数のネットワークを管理します。
- FTD や Cisco ASA デバイスなど、サポートされている他のプラットフォームとの互換性のあるオブジェクトを使用してアクセスルールをカスタマイズします。

Meraki MX デバイスのオンボーディング

デバイスを Security Cloud Control にオンボードする前に、Cisco Meraki ダッシュボードでアカウントを作成し、デバイスまたはテンプレートをダッシュボードにオンボードする必要があります。API トークンを生成して Security Cloud Control と通信するためには、組織が Cisco Meraki ダッシュボードにアカウントを持っている必要があります。

Cisco Meraki MX デバイスまたは Cisco Meraki テンプレートを Security Cloud Control にオンボードできます。

Security Cloud Control コンソールを介して Cisco Meraki MX のログイン情報と権限を処理します。正しいログイン情報または権限がないと、Security Cloud Control は Meraki デバイスと通信できません。

詳細については、「Cisco Meraki MX ログイン情報の更新」および「Cisco Meraki API キーの生成と取得」を参照してください。

Meraki レイヤ 3 ルールと Security Cloud Control

現時点では、Security Cloud Control はレイヤ 3 ファイアウォールルールのみをサポートしています。レイヤ 3 ルールは、OSI モデルのネットワーク層でポリシーを管理することを可能にします。詳細については、「Using Layer 3 Firewall Rules」を参照してください。

Cisco Meraki ダッシュボードでレイヤ 3 アウトバウンドルールを作成できます。Security Cloud Control は、デバイスを Security Cloud Control にオンボーディングするときに、Cisco Meraki ダッシュボードで定義されたレイヤ 3 ルールを読み取ります。その後、Security Cloud Control で、FTD または ASA ルールを管理する場合と同じ方法でこれらのルールを管理できます。詳細については、「Cisco Meraki アクセス コントロール ポリシーの管理」を参照してください。

オブジェクト

オブジェクトを使用して、新しいアクセス コントロール ポリシーを最適化できます。Cisco Meraki ダッシュボードでは、プロトコルと IP アドレスのグループまたは IP アドレス範囲を使用します。対照的に、Security Cloud Control ではさまざまなオブジェクトを使用してルールを管理します。Security Cloud Control が Cisco Meraki プロトコルをオブジェクトに移行する方法を理解するには、「Cisco Meraki デバイスに関連付けられたオブジェクト」を参照してください。次のオブジェクトを Security Cloud Control で作成し、Cisco Meraki ダッシュボードの IP グループに変換できます。

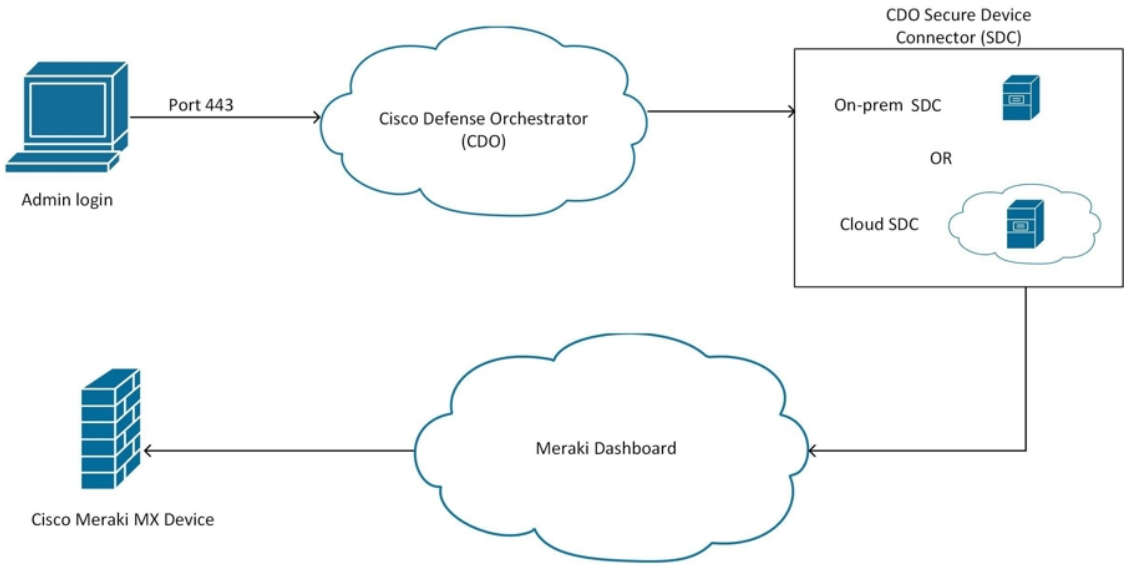
- ネットワークオブジェクトまたはオブジェクトグループ
- ネットワークサービス（ポート）オブジェクト

Cisco Meraki ダッシュボードでレイヤ 3 アウトバウンドルールを作成できます。Security Cloud Control は、デバイスを Security Cloud Control にオンボーディングするときに、Cisco Meraki ダッシュボードで定義したレイヤ 3 ルールを読み取ります。その後、Security Cloud Control で FTD または ASA ルールを管理する場合と同様に、これらのルールを管理できます。Cisco Meraki アクセス コントロール ポリシーの詳細については、「Cisco Meraki アクセス コントロール ポリシーの管理」を参照してください。

Security Cloud Control と Meraki の通信方法

Security Cloud Control から Meraki デバイスへの展開

Security Cloud Control は、設定の変更を Cisco Meraki MX デバイスに直接展開しません。展開は複数のステップからなるプロセスです。次の図は、デプロイメントプロセスを示しています。



Cisco Meraki MX デバイスの Security Cloud Control で行った設定の変更は、展開を決定するまで Security Cloud Control でステージングされます。設定の変更を展開すると、Security Cloud Control から Cisco Meraki ダッシュボードに転送され、Cisco Meraki MX デバイスに実装されます。Security Cloud Control はファイアウォールポリシーを管理し、Cisco Meraki ダッシュボードはポリシーが適用されるネットワークを管理します。どちらの操作も、Cisco Meraki MX デバイスがネットワークトラフィックを管理および処理する方法に影響を与えます。

古いテナントを持つ一部のお客様は、SDC を介して Meraki MX デバイスを Security Cloud Control に接続する場合があります。そのようなお客様は、この方法を引き続き使用できます。あるいは、Cisco Meraki MX を再オンボーディングするか、接続ログイン情報を更新して SDC を削除できます。Security Cloud Control を Meraki MX に接続するために SDC は必要ありません。

Security Cloud Control と Cisco Meraki ダッシュボードの違いの 1 つは、オブジェクトの使用です。Cisco Meraki ダッシュボードで作成されたルールの場合、Security Cloud Control は Meraki の IP アドレスグループまたは IP アドレス範囲を取得し、それらをルールやデバイスポリシーに添付または関連付けできるオブジェクトに変換します。Security Cloud Control で作成されたオブジェクトを Meraki アプライアンスに展開すると、Cisco Meraki ダッシュボードはそれらのオブジェクトを IP アドレスグループまたは IP アドレス範囲に変換し直します。Security Cloud Control 内のオブジェクトは、他のデバイスプラットフォームと互換性があるため、固有かつ汎用性の高いオブジェクトです。Security Cloud Control でオンボードされた他のデバイスがある場合、すべてのデバイスに対して単一のオブジェクトを作成できる場合があります。Cisco Meraki デバイスに関連付けられているオブジェクトの詳細については、「Meraki デバイスに関連付けられるオブジェクト」を参照してください。

Cisco Security Cloud Control の概要

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セキュリティ プラットフォームです。

プラットフォームにセキュリティ製品を統合すると、エクスペリエンスが合理化になります。Cisco セキュリティ製品のサブスクリプションを購入すると、購入したすべてのサブスクリプションに関する単一の要求コードが記載された電子メールが 1 件届きます。新しい Security Cloud Control 組織に要求コードを入力すると、すべての製品が同時に Cisco Security Cloud Control にプロビジョニングされます。

Security Cloud Control では、ユーザーとグループの管理はプラットフォームレベルで行われます。これらのユーザーとグループにロールが割り当てられ、Security Cloud Control および統合製品を管理する権限が定義されます。

製品とツール間の移動は直感に行うことができ、すべての統合製品に共通のプラットフォームメニューとツールバーが標準化されています。

Security Cloud Control は、プラットフォーム上のすべての統合製品に次のコアサービスを提供します。

- **プラットフォーム管理**：ロールベースのアクセス制御の管理、サブスクリプションの要求、製品インスタンスの標準化された地域展開などの一般的なサービスは、Security Cloud Control によって提供されます。Security Cloud Control では、これらの機能を一元化することで、プラットフォームから管理されるすべての Cisco Security 製品間でのプロビジョニングおよびアクセス管理における一貫したユーザーエクスペリエンスが保証されます。管理者は、Security Cloud Control のメインナビゲーションバーにある プラットフォーム管理 メニューからこれらの共通サービスにアクセスします。
- **人工知能アシスタント**：Security Cloud Control の Cisco AI Assistant は、AI 中心のインサイト、自動化、およびコンテキストガイダンスを提供することにより、セキュリティ業務を合理化するように設計されています。管理者がセキュリティポリシーを管理し、問題をトラブルシュートし、Firewall、Duo、および Secure Access などの Cisco のセキュリティ製品全体で設定を最適化するのに役立ちます。Cisco Assistant は、自然言語処理とクロスプラットフォーム インテリジェンスを活用することで、効率を向上させ、インシデント対応を迅速化し、セキュリティワークフローを簡素化します。
- **Global Search**：プラットフォーム内の製品全体の値を検索する機能です。
- **Shared Objects**：デバイスやポリシー間で共有できるオブジェクトを作成および管理します。
- **Unified documentation portal**：すべてのドキュメントにアクセスできる、ドキュメントの「ヘルプ」エクスペリエンス。

Security Cloud Control と統合される製品：

Security Cloud Control からは、次のすべてのセキュリティ製品を管理できます。

- AI Defense
- Security Cloud Control Firewall Management
- Multicloud Defense
- セキュアなアクセス

Security Cloud Control から起動できる製品

Security Cloud Control から、これらのセキュリティ製品を起動できます。起動後、これらの製品はスタンドアロン製品として動作するため、Security Cloud Control を介して管理することはできません。このような製品のライセンスは Security Cloud Control からのみ要求または非アクティブ化できます。

[Cisco Security Cloud Control] ツールバーで、9 ドットメニュー をクリックすると、次の製品が起動します：

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco Duo
- Cisco XDR

Security Cloud Control によってサポートされる製品およびソリューション

現在、Security Cloud Control と統合できる製品は次のとおりです。

AI Defense：AI Defense はAIのユーザーとプロバイダーのリスクに対処します。Security Cloud Controlのネットワーク可視性と適用ポイントを使用して、AI Defense では、分散クラウド環境全体で承認済みおよび未承認の AI ワークロード、アプリケーション、モデル、データ、およびユーザーアクセスを検出するための検出と適用の手順が追加されます。AI を搭載したサービスを開発および提供する組織の場合、AI Defense は提供前に AI モデルの脆弱性を検出します。プロンプトインジェクション、サービス妨害（DoS）、データ漏洩といった急速に進化する脅威から AI アプリケーションを保護します。詳細については、「AI Defenseのドキュメント」を参照してください。

Security Cloud Control Firewall Management： Security Cloud Control Firewall Management（旧称 Cisco Defense Orchestrator）は、クラウドベースのセキュリティポリシーマネージャで、シスコのファイアウォールやその他のデバイス全体でポリシーを簡素化および統合します。詳細については、『Cisco Security Cloud Control ドキュメント』の「ファイアウォール」を参照してください。

Multicloud Defense：Multicloud Defense は、マルチクラウドセキュリティに対する簡素化および高度に自動化されたアプローチを提供します。このソリューションにより、組織は単一の

SaaS 提供コントロールプレーンと、一元化または分散された PaaS 提供データプレーンアーキテクチャを使用して、マルチクラウド環境を管理および保護できます。 Multicloud Defense では、すべての主要なクラウドプロバイダーで継続的な可視性、統合された保護、およびダイナミックなポリシー更新が提供されるため、各クラウドプロバイダーごとにソリューションごとに個別のポイントソリューションを用意する必要がなくなります。詳細については、「Multicloud Defenseのドキュメント」を参照してください。

セキュアなアクセス：Cisco セキュアなアクセス は、インターネットベースの脅威に対して複数のレベルの防御を提供するクラウドベースのプラットフォームです。組織のネットワークから接続する場合でも、ネットワークからローミングする場合でも、インターネット、SaaSアプリケーション、およびプライベート デジタル リソースに安全に接続できます。ポリシールールを使用して、リソース、ユーザー、デバイスのコレクションにセキュリティ管理を構成および適用します。 詳細については、「Secure Access Documentation」を参照してください。セキュアなアクセス サブスクリプションには、追加料金なしで Security Cloud Control を介した アイデンティティ インテリジェンス 統合も含まれます。これには、スタンドアロン アイデンティティインテリジェンス ダッシュボードへのアクセスは含まれません。詳細については、「Cisco Identity Intelligence と Cisco Secure Access の統合」を参照してください。

Cisco XDR (Extended Detection and Response)：Cisco XDR は、セキュリティ運用を簡素化し、インシデント対応を迅速化するように設計されたクラウドネイティブの拡張可能なセキュリティソリューションです。エンドポイント、ネットワーク、ファイアウォール、電子メール、アイデンティティ、およびDNSを含む複数のソースからテレメトリを収集および分析し、Cisco Talos から提供される強化されたコンテキストと脅威インテリジェンスを使用して高度な脅威を検出します。

Cisco XDR は潜在的なリスクと影響に基づいて脅威に優先順位を付け、誤検出を減らし、AI 中心のガイダンスと自動化を提供して調査と修復を合理化します。この統合アプローチにより、セキュリティ オペレーション センター（SOC）チームは、マルチベクトル、マルチベンダー環境でシスコおよびサードパーティのセキュリティツールの両方を統合することで、より迅速に行動でき、生産性を向上させ、サイバーレジリエンスを構築できます。詳細については、「Cisco XDR ヘルプセンター」を参照してください。

Security Cloud Control Firewall Management の概要

Security Cloud Control Firewall Management、旧 Cisco Defense Orchestrator は、分散環境でのセキュリティポリシー管理を簡素化します。これにより、管理対象のファイアウォールやデバイス間で一貫したポリシーを維持できます。Security Cloud Control では、**ファイアウォール**は**製品（Products）**に表示されます。

Security Cloud Control Firewall Management は、不整合を特定し、解決ツールを提供することにより、セキュリティポリシーを最適化します。また、オブジェクト共有、ポリシー共有、および設定テンプレートもサポートされているため、デバイス間で一貫した設定を適用できます。

Security Cloud Control Firewall Management は、Adaptive Security Device Manager（ASDM）などのローカルデバイスマネージャと共存できます。他のマネージャが行った設定変更を追跡し、必要に応じて違いを調整します。

このプラットフォームには、脅威防御 デバイスを オンプレミス Firewall Management Center または クラウド提供型 Firewall Management Center にオンボーディングするのに役立つガイド付き Day 0 エクスペリエンスが含まれています。主要な機能に焦点を当てており、それらの機能をアクティブ化および設定するのに役立ちます。

デバイスのオンボーディング要件

デバイスをオンボーディングする前に、次の前提条件を満たしてください。

- インストールウィザードを完了します。
- デバイスのライセンスを取得します。

これらの前提条件を満たした後、Security Cloud Control Firewall Management オンボーディングウィザードを使用してデバイスをオンボーディングします。

次の制約事項に注意してください。

- 組織に関連付けられている Security Cloud Control Firewall Management にデバイスをオンボーディングした後は、それらのデバイスを別の組織に移行できません。
- デバイスを新しい組織に移動するには、新しい組織にデバイスを再度オンボーディングする必要があります。

シスコ オンライン プライバシー ポリシー

Cisco Systems, Inc. およびその子会社（以下総称して「シスコ」といいます）は、皆様のプライバシーを保護し、シスコの Web サイト、ならびに製品およびサービス（以下「ソリューション」）を快適にお使いいただけるよう全力を尽くします。『シスコ オンライン プライバシー ポリシー』をよく読み、シスコがユーザーの個人情報を収集、使用、共有、保護する方法を明確に理解してください。

ファイアウォール管理ダッシュボード

ファイアウォールダッシュボードは、さまざまなカテゴリ全体でテナントレベルの詳細をモニタリングおよび管理するための中心ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

左側のペインで、[ダッシュボード（Dashboard）] をクリックします。

ダッシュボードのカスタマイズ

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードに表示するウィジェットを選択または選択解除します。

3. ウィジェットをドラッグアンドドロップして、希望に応じて配置できます。

ダッシュボードは、**[Top Insights & Alerts]**、**[Top Actions]**、および **[Top Information]**の 3 つの主要なセクションに分割されています。各セクションでは、最適なセキュリティおよび運用管理を維持するために役立つさまざまなカテゴリのインサイトが提供されます。

上位のインサイトとアラート

このセクションは、テナントに対して **Insights** が有効になっている場合にのみ表示されます。エレメントフロー、RA VPN 予測、アクセス制御ポリシーの異常、CPU およびメモリの使用率が高い、Snort CPU およびメモリの使用率が原因で発生する高トラフィックに関連するインサイトを表示できます。

上位アクション

このセクションは、テナントに対して **Insights** が有効になっている場合にのみ表示されます。有効にすると、次のウィジェットが表示できます。

- **[ポリシーアナライザおよびオプティマイザ（Policy Analyzer and Optimizer）]**：セキュリティポリシーを分析し、異常を検出し、ファイアウォールのパフォーマンスを向上させるための最適化推奨事項を提供します。

  詳細については、「ポリシーアナライザおよびオプティマイザ」を参照してください。

- **Insights**：設定、正常性と操作、トラフィックとキャパシティなどのカテゴリごとに、アクティブなインサイトと傾向を表示します。

  詳細については、「 Insights」を参照してください。

- **[機能の導入（Feature Adoption）]**：使用状況を評価して改善できる機能の導入率を示します。

  詳細については、「機能の導入状況の評価と改善」を参照してください。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。テナントに対して有効になっている機能に応じて、次のウィジェットを表示できます。

- **設定状態（Configuration States）**：デバイス設定を Security Cloud Control によって維持される設定と比較して、不整合や競合を特定できます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理（Change Log Management）**：完了した変更ログと保留中の変更ログを表示して、運用の変更を追跡できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「変更ログ」を参照してください。

- **RA VPN セッション（RA VPN Sessions）**：リモートアクセス VPN セッションのアクティビティを表示します。

詳細については、「RA VPN セッション」を参照してください。

- **インベントリ全体（Overall Inventory）**：デバイスの総数を表示し、問題、保留中のアクション、その他、およびオンラインに分けてデバイスをグループ化します。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN（Site-to-Site VPN）**：VPN トンネルの総数と、アクティブおよびアイドルのトンネルの割合が表示されます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

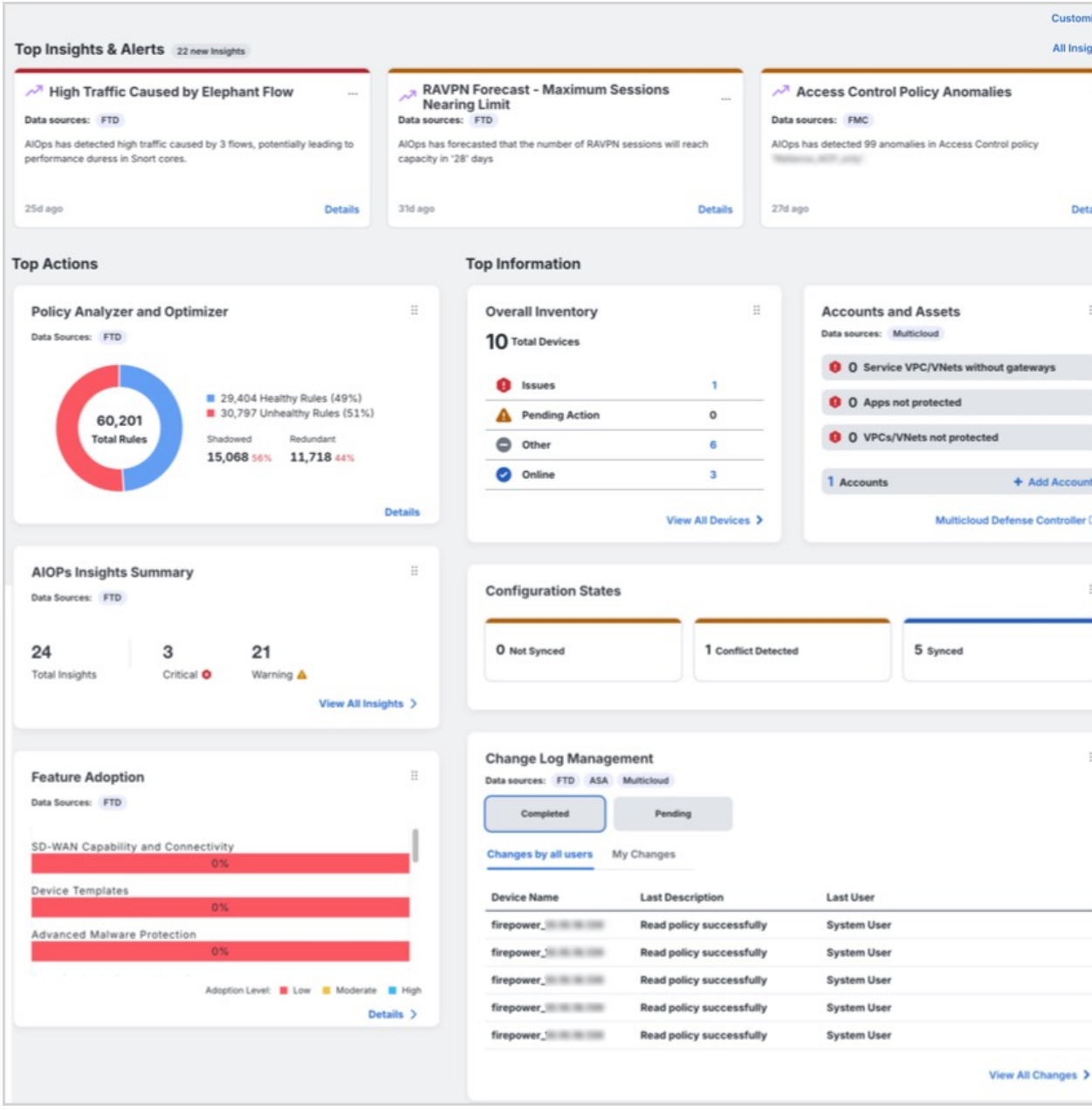
  詳細については、「サイト間 VPN」を参照してください。

- **アカウントとアセット**：
  - マルチクラウドのアカウントとリソースを効果的に追跡して管理するのに役立ちます。ここから Multicloud Defense Controller を起動できます。
  - **[+Add Account]** をクリックして、新しいアカウントを追加します。

  詳細については、「Multicloud Defense コントローラ」を参照してください。

- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。許可されたトラフィック（デフォルト）とブロックされたトラフィックの間でフィルタ処理できます。

- **トップ侵入およびマルウェアイベント**：上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。許可されたイベント（デフォルト）とブロックされたイベントの間でフィルタ処理できます。



アナウンスメント

[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目に関する詳細を知りたい場合は、関連するドキュメントへのリンクが提供されます。

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。