2019 の機能概要

2019 年 11 月

2019 年 11 月

Firepower Threat Defense 6.5.0 を実行しているデバイスの CDO サポート

CDO は現在、FTD 6.5.0 デバイスを管理しています。CDO が提供するサポートの側面は次のとおりです。

- Firepower Threat Defense（FTD）6.5.0 を実行しているデバイスのオンボード。
- Firepower 4100 や Firepower 9300 などの追加の Firepower シリーズ デバイスのサポート。
- Microsoft Azure での仮想 FTD インスタンスのサポート。サポートされているデバイスの完全なリストについては、『Managing FTD with Cisco Defense Orchestrator』の「Firepower Threat Defense Support Specifics」を参照してください。
- デバイスは、個々の FTD または高可用性ペアで設定された FTD にすることができます。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Firepower Software Upgrade Path」を参照してください。次の注意事項は、アップグレードサポートに適用されます。

- デバイスが管理にデータインターフェイスを使用している場合、6.5.0 を実行している FTD では HA ペアのアップグレードはサポートされません。
- Firepower 4100 および Firepower 9300 デバイスのアップグレードは現在サポートされていません。
- 顧客は CDO のアップグレードページのドロップダウンを使用して、FTD 6.5.0 にアップグレードできます。6.5 イメージのダウンロードのためにデバイスに提供されるリンクは HTTP になります。これは、ダウンロードが HTTPS 経由で行われた場合よりも、イメージのダウンロード時間がわずかに長くなる可能性があることを意味する場合があります。さらに、FTD からのアウトバウンド HTTP トラフィックがブロックされている場合、イメージのダウンロードは失敗します。

- Firepower 1010 に FTD 6.5.0 がインストールされている場合、通常のファイアウォール インターフェイスとしてまたはレイヤ 2 ハードウェアスイッチポートとして実行するようにインターフェイスを設定できます。現時点では、CDO でのスイッチモードのサポートは読み取り専用です。スイッチポートモードのインターフェイスを作成または変更するには、FDM コンソールを使用します。CDO は、Firepower 1010s でのスイッチポートモードのサポートの開発を続けており、完全なサポートが利用可能になったら、新機能で発表します。
- 登録トークンを使用して FTD 6.5.0 デバイスをオンボードすると、セキュアイベントコネクタを使用せずに、接続イベント、ファイルイベントとマルウェアイベント、および侵入イベントを Cisco Cloud に直接送信できます。『Managing FTD with Cisco Defense Orchestrator』の「Implementing Cisco Security Analytics and Logging」を参照してください。
- FTD 6.4.x 機能の継続的なサポート。CDO は FTD 6.5 機能のサポートを継続的に開発しており、準備ができ次第サポートをリリースします。

CDO がサポートしている FTD 機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

IKEv1 によるサイト間 VPN 接続のサポート

CDO は、Internet Key Exchange バージョン 1（IKEv1）を使用したサイト間 VPN トンネルの作成をサポートするようになりました。Internet Key Exchange バージョン 2（IKEv2）をサポートしていないレガシーファイアウォールでサイト間 VPN を構成するのに役立ちます。Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Site-to-Site Virtual Private Network」を参照してください。

Firepower Threat Defense のテンプレートの改善

CDO では、FTD テンプレートのいくつかの側面をパラメータ化して、テンプレートをさらにカスタマイズできるようになりました。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Configure FTD Templates」を参照してください。

スマートライセンスの管理

CDO 内で Firepower Threat Defense デバイスのシスコ スマート ライセンスを管理できるようになりました。スマートライセンスはワークフローに組み込まれており、CDO インターフェイスから簡単にアクセスできます。CDO 内で次の Cisco Smart Licensing タスクを実行できるようになりました。

- 登録トークンを使用して FTD デバイスのオンボード中にスマートライセンスを適用する
- デバイスに適用されているライセンスを表示する
- Cisco Smart Software Manager へのライセンスを登録する
- デバイスのさまざまなライセンスタイプを有効または無効にする

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Onboard a Firepower Threat Defense Device with a Registration Token」および「Smart-licensing an Onboarded FTD」を参照してください。

2019 年 10 月

2019 年 10 月

アマゾンウェブサービスのサポート

CDO が AWS VPC を管理するようになりました。

アマゾンウェブサービス（AWS）仮想プライベートクラウド（VPC）は、AWS アカウントに関連付けられた仮想プライベートクラウドをユーザーに提供する商用クラウドコンピューティング サービスです。このネットワークは、AWS のスケーラブルなインフラストラクチャを使用する利点を備えた、独自のデータセンターで運用する従来のネットワークによく似ています。

CDO は、オブジェクトとルールの問題を特定し、それらを修正する方法を提供することにより、AWS VPC の最適化を支援します。CDO を使用して次のことを行います。

- FTD または ASA デバイスとともに AWS VPC 環境を管理します。
- AWS VPC に関連付けられたすべてのセキュリティグループルールを同時に管理します。
- FTD や 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間で互換性のあるオブジェクトを使用して、セキュリティグループルールを作成およびカスタマイズします。

- AWS VPC サイト間 VPN 接続を表示します。

詳細については、『Managing AWS with Cisco Defense Orchestrator』を参照してください。

CDO を使用して ASA を FTD デバイスに移行する

CDO は、適応型セキュリティアプライアンス（ASA）を Firepower Threat Defense（FTD）デバイスに移行するのに役立ちます。CDO には、ASA の実行構成の次の要素を FTD テンプレートに移行するためのウィザードが用意されています。

- インターフェイス
- ルート
- アクセス制御ルール（ACL）
- ネットワークアドレス変換（NAT）ルール
- ネットワークオブジェクトとネットワーク グループ オブジェクト
- サービスオブジェクトとサービス グループ オブジェクト

ASA 実行構成のこれらの要素を FTD テンプレートに移行したら、その FTD テンプレートを、CDO によって管理される新しい FTD デバイスに適用できます。FTD デバイスはテンプレートで定義された構成を採用するため、FTD は ASA の実行構成のいくつかの側面を使用して構成されるようになりました。

CDO を使用して ASA を FTD に移行するプロセスの詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Migrating ASA to FTD Workflow」を参照してください。

シスコが導入する Cisco Secure Sign-on と Duo Multi-Factor Authentication を使用した新しいシングル サインオン ソリューション

CDO はこの新しいソリューションを採用し、顧客のテナントを Cisco Secure Sign-on ID プロバイダー（IdP）および Duo Security 多要素オーセンティケータに変換します。

Cisco Secure Sign-On を使用すると、次のメリットが得られます。

- **強力で回復力のある ID**：AICPA SOC 2、CSA-Star、ISO 27001 などの最高の業界標準を満たすセキュリティ。また、顧客向けに分離された FedRAMP および HIPAA 環境もサポートします。
- **Duo 多要素認証（MFA）**：Cisco Secure Sign-On と統合された Duo MFA とは、適応型の階層化されたシンプルな認証を意味します。ワンプッシュ通知、ワンタップで簡単にアクセスできます。
- **シームレスなワークフローのためのシングルサインイン**：単一のユーザー名とパスワードを入力して、ワークフローを通じてコンテキストを維持しながら、場所やデバイスを問わずすべてのアプリケーションにアクセスします。
- **カスタマイズされたエクスペリエンス**：仕事用アプリを Cisco Secure Sign-On ダッシュボードに自由に配置できます。タブと検索バーで整理できます。

（注）
- 独自のシングルサインオン ID プロバイダーを使用して CDO にサインインする場合、この Cisco Secure Sign-On および Duo への移行は影響しません。独自のサインオンソリューションを引き続き使用します。
- CDO の無料試用期間中であれば、この移行は影響します。

詳細については、『Managing AWS with Cisco Defense Orchestrator』の「Migrating to Cisco Secure Sign-On Identity Provider」を参照してください。

Secure Cloud Analytics との統合を含む Cisco Security Analytics and Logging

Cisco Security Analytics and Logging によりネットワークの可視性が向上するため、脅威をリアルタイムで迅速に検出し、インシデントを確実かつ大規模に修正できます。

Cisco Security Analytics and Logging を使用すると、すべての Firepower Threat Defense（FTD）デバイスからの接続、侵入、ファイル、マルウェア、セキュリティインテリジェンスのイベントをキャプチャし、CDO の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging）] ページから表示できます。イベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。Logging and Troubleshooting パッケージは、これらの機能を提供します。

Firewall Analytics and Monitoring パッケージを使用すると、システムは Secure Cloud Analytics 動的エンティティモデリングを FTD イベントに適用し、動作モデリング分析を使用して Secure Cloud Analytics の観測値とアラートを生成できます。Total Network Analytics and Monitoring パッケージを使用すると、システムは FTD イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、プロビジョニングされた Cisco Secure Cloud Analytics ポータルを CDO からクロス起動できます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Cisco Security Analytics and Logging」を参照してください。

2019 年 9 月

2019 年 9 月

登録トークンを使用した Firepower Threat Defense デバイスのオンボーディング

IP アドレス、ユーザー名、およびパスワードを使用する代わりに、登録トークンを使用して FTD デバイスをオンボードできるようになりました。これは、FTD に DHCP を使用して IP アドレスが割り当てられている場合に特に役立ちます。その IP アドレスが何らかの理由で変更されても、FTD は CDO に接続されたままになります。さらに、FTD はローカルエリアネット

ワーク上のアドレスを持つことができ、外部ネットワークにアクセスできる限り、この方法で CDO にオンボードできます。

このオンボーディング方法は、現在、FTD 6.4 リリースで、defenseorchestrator.cisco.com に接続しているお客様が利用できます。defenseorchestrator.cisco.eu に接続しているお客様はまだ利用できません。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Onboarding an FTD with a Registration Key」を参照してください。

2019 年 8 月

2019 年 8 月

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging によりネットワークの可視性が向上するため、脅威をリアルタイムで迅速に検出し、インシデントを確実かつ大規模に修正できます。

Firepower Threat Defense のリモートアクセス VPN のサポート

リモートアクセス（RA）VPN を使用すると、サポートされているラップトップ、デスクトップ、およびモバイルデバイスを使用して、個人がネットワークへの安全な接続を確立できます。CDO は、オンボーディングした Firepower Threat Defense（FTD）デバイスで RA VPN をセットアップするための直感的なユーザーインターフェイスを提供します。

AnyConnect はエンドポイントデバイスでサポートされている唯一のクライアントで、RA VPN 接続が可能です。

CDO は、FTD デバイスでの RA VPN 機能の次の側面をサポートします。

- プライバシー、認証、およびデータ整合性のための Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）
- SSL クライアントベースのリモートアクセス
- IPv4 および IPv6 のアドレッシング
- 複数の FTD デバイス間での共有 RA VPN 設定

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Remote Access Virtual Private Network」を参照してください。

Firepower Threat Defense のハイ アベイラビリティ イメージ アップグレードのサポート

CDO で FTD HA ペアをアップグレードできるようになりました。フェールオーバーペアをアップグレードすると、CDO は必要なアップグレードイメージを両方のデバイスにコピーします。CDO は、プライマリデバイスがアクティブモードになっていない場合は、それを一時的にア

クティブモードに移行してから、セカンダリデバイスをアップグレードします。セカンダリデバイスが正常にアップグレードされると、プライマリデバイスがアップグレードされます。フェールオーバーペアは、デバイスを一度に1つずつアップグレードして、ネットワークの中断を最小限に抑えます。

フェールオーバーペアをアップグレードするには、『Managing FTD with Cisco Defense Orchestrator』の「Upgrade an FTD High Availability Pair」を参照してください。

Firepower Threat Defense デバイスのサイト間 VPN

Firepower Threat Defense デバイス用のサイト間 VPN の一般提供が開始されました。

CDO を使用すると、地理的に異なる 2 つのサイト間で安全な接続を確立できます。これらのピアは、IPv4 アドレスと IPv6 アドレスの内部と外部の任意の組み合わせを持つことができます。サイト間トンネルは、Internet Protocol Security（IPsec）プロトコルスイートとインターネット キー エクスチェンジ バージョン 2（IKEv2）を使用して構築されます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。CDO にオンボードされているデバイスの次のシナリオで、サイト間 IPsec 接続を作成できます。

- 2 つの管理対象デバイス間
- 管理対象デバイスとその他のシスコのピア間
- 管理対象デバイスとサードパーティのピア間

Firepower Threat Defense のハイアベイラビリティのサポート

CDO は、Firepower Threat Defense ファイアウォールのハイアベイラビリティ（HA）のサポートを一般提供します。既存の HA ペアをオンボードするか、CDO で HA ペアを作成できるようになりました。HA 構成により、アップグレード期間中や予期しないデバイス障害など、デバイスが使用できないシナリオでも安全なネットワークを維持することができます。フェールオーバーモードでは、スタンバイデバイスはすでにアクティブになるように構成されています。つまり、HA デバイスの 1 つが使用できなくなっても、もう一方のデバイスはトラフィックの処理を続行します。

スタンドアロン FTD デバイスでサポートされる機能のほとんどは、HA 用に設定されたデバイスもサポートします。詳細については、『Managing FTD with Cisco Defense Orchestrator』の「FTD High Availability」を参照してください。

近日公開... FTD HA アップグレードのサポート。現在、HA ペアをアップグレードする必要がある場合は、アクティブなデバイスの FDM コンソールからアップグレードを実行する必要があります。

2019 年 7 月

2019 年 7 月

ASA デバイスの時間範囲オブジェクト

時間範囲オブジェクトを使用して、ネットワークポリシーのルールをカスタマイズできるようになりました。これらのオブジェクトを使用すると、1 回限りのルールまたは繰り返しルールを実行し、ネットワークがトラフィックを処理する方法をカスタマイズできます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「ASA Time Range Objects」を参照してください。

Firepower Threat Defense のサポート

CDO は、Firepower Threat Defense ファイアウォールのサポートを一般提供します。

CDO は、Firepower Threat Defense デバイスへのシンプルな管理インターフェイスとクラウドアクセスを必要とするファイアウォール管理者向けに設計されています。Firepower Device Manager（FDM）管理者は、FDM インターフェイスと CDO インターフェイスの間に多くの類似点があることに気付くでしょう。私たちは、マネージャ間で可能な限り一貫性を保つという考えで CDO を構築しました。

CDO は、ASA 5508-x、ASA 5515-x、ASA 5516-x、ASA 5525-x、ASA 5545-x、ASA 5555-x、FTD 2100 シリーズ デバイス、FTD 1000 シリーズ デバイス、または仮想 FTD デバイスにインストールされている場合、FTD バージョン 6.4.0 以降を実行している Firepower Threat Defense（FTD）デバイスを管理できるようになりました。

CDO を使用して、物理または仮想 Firepower Threat Defense（FTD）デバイスの次の側面を管理します。

- デバイス管理
- デバイスのアップグレード
- インターフェイス管理
- ルーティング
- セキュリティ ポリシー
- ポリシーと構成の一貫性を促進する
- 変更のトラッキング
- ネットワークのモニタリング

Firepower 1000 シリーズおよび仮想 FTD を含むすべての CDO FTD PID は、CCW で注文できます。PID はプラットフォーム固有ですが、ASA と FTD に共通です。詳細については、Salesconnect の注文ガイドを参照してください。

サポートしている機能の詳細については、『Managing FTD with Cisco Defense Orchestrator』を参照してください。

Meraki MX のサポート

CDO は、Meraki MX ファイアウォールポリシーを管理するようになりました。

Meraki MX は、分散展開用に設計されたエンタープライズセキュリティおよびソフトウェア定義ワイドエリアネットワーク（SD-WAN）の次世代ファイアウォール アプライアンスです。Cisco Defense Orchestrator を使用して、Meraki MX デバイスのレイヤ 3 ネットワークルールを管理できるようになりました。

CDO は、オブジェクトとポリシーの問題を特定し、それらを修正する方法を提供することにより、Meraki 環境を最適化するのに役立ちます。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。

CDO を使用して次のことを行います。

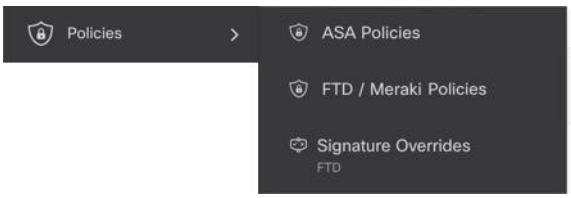
- 1 つ以上の Meraki デバイスでポリシーを同時に管理します。
- 包括的な環境で、FTD および ASA デバイスとともに Meraki ポリシーまたはテンプレートを監視および管理します。
- Meraki テンプレートを使用して複数のネットワークを管理します。
- FTD や ASA デバイスなど、サポートされている他のプラットフォーム間で互換性のあるオブジェクトを使用してアクセスルールをカスタマイズします。

詳細については、『Managing Meraki with Cisco Defense Orchestrator』を参照してください。

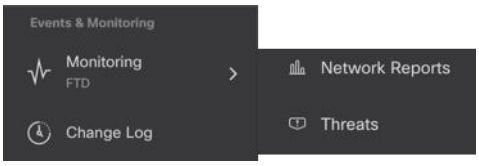
最新の GUI ナビゲーション

CDO の UI の操作がさらに簡単になりました。

ナビゲーションバーのポリシーメニューに、デバイスまたは機能別にグループ化されたポリシーが表示されるようになりました。テナントに現在存在するポリシーに到達するために必要なメニューパスのみを公開します。



FTD のすべての監視機能は、ナビゲーションバーの [イベントと監視（Events & Monitoring）] エリアにグループ化されています。[監視（Monitoring）] メニューには、[ネットワーク レポート（Network Reports）] と [脅威（Threats）] が表示されます。



2019 年 5 月

2019 年 5 月

デバイス接続のトラブルシューティング

このツールを使用すると、セキュアデバイスコネクタ（SDC）と任意のデバイス間の接続の問題をテストまたはトラブルシューティングできます。デバイスがオンボーディングに失敗した場合、またはオンボーディングの前に CDO がデバイスに到達できるかどうかを判断する場合は、この接続をテストすることができます。

詳細については、『Managing FTD with Cisco Defense Orchestrator』の「Troubleshoot a Secure Device Connector with the SDC」を参照してください。

2019 年 4 月

2019 年 4 月

CDO ユーザーエクスペリエンスの向上にご協力ください

CDO のユーザーエクスペリエンスについてお聞かせいただきたく、簡単にできる方法をご用意しました。CDO ポータルを離れることなくフィードバックを送信できるように、[ヘルプ（Help）] メニューに [フィードバックの提供（Provide Feedback）] ボタンを追加しました。気に入った点と改善点を教えてください。

フィードバックを送信する際は、会社でのあなたの役割を教えてください。あなたは、ネットワーク オペレーション センター、セキュリティ オペレーション センターにいますか。それとも IT 関連全般を扱うセンターにいますか。完了しようとしているタスクを教えてください。セキュリティポリシーを編集しようとしていますか、または変更ログで何かを見つけようとしていますか。

フィードバックを残す方法は次のとおりです。

ステップ 1 CDO にログインします。

ステップ 2 テナント名とアカウント名の横にある [ヘルプ（help）] ボタンをクリックし、[フィードバックの提供（Provide Feedback）] を選択します。

ステップ 3 フィードバックを入力して [電子メールの送信（Send Email）] をクリックします。これにより、ローカルメールサーバーに電子メールが生成されます。 これは手動で送信する必要があります。

サポートスタッフができるだけ早く対応します。

2019 年 2 月

2019 年 2 月

セキュアデバイスコネクタに影響を与えるコンテナ権限昇格の脆弱性への解決策：cisco-sa-20190215-runc

Cisco Product Security Incident Response Team（PSIRT）は、Docker の重大度の高い脆弱性について説明するセキュリティアドバイザリ cisco-sa-20190215-runc を公開しました。脆弱性の完全な説明については、PSIRT チームのアドバイザリ全体をお読みください。

この脆弱性は、すべての CDO ユーザーに影響します。

- CDO のクラウド展開された Secure Device Connector（SDC）を使用しているお客様は、修復手順が CDO 運用チームによってすでに実行されているため、何もする必要はありません。
- オンプレミスで展開された SDC を使用しているお客様は、最新の Docker バージョンを使用するように SDC ホストをアップグレードする必要があります。

CDO 標準の SDC ホストとカスタム SDC ホストを更新する方法の手順については、「Container Privilege Escalation Vulnerability Affecting Secure Device Connector」（cisco-sa-20190215-runc）を参照してください。

ASA デバイスの一括オンボーディング時にラベルを追加する

ASA デバイスを一括でオンボーディングするときに、カスタムデバイスラベルを指定できるようになりました。詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Onboard ASAs in Bulk」を参照してください。

Cisco IOS デバイスのサポート

Cisco Defense Orchestrator（CDO）を使用すると、Cisco IOS デバイスを管理できます。これらのデバイスでサポートされている機能は次のとおりです。

- Cisco IOS デバイスのオンボーディング
- デバイス構成の表示
- デバイスからのポリシーと構成の変更の終了

- アウトオブバンド変更の検出
- コマンド ライン インターフェイスのサポート
- 個々の CLI コマンドおよびコマンドのグループを、編集および再利用可能なマクロに変換可能
- SSH フィンガープリントの変更の検出と管理
- 変更ログに IOS デバイスへの変更を表示

自動展開のスケジュール

CDO を使用して 1 つ以上のデバイスの構成変更を行った後、都合のよい日時にそれらのデバイスへの変更の展開をスケジュールできるようになりました。たとえば、メンテナンスの時間帯やネットワークトラフィックが少ない時間帯に展開を実行するようにスケジュールできます。

詳細については、『Managing ASA with Cisco Defense Orchestrator』の「Enable the Option to Schedule Automatic Deployments」および「Schedule Automatic Deployments」を参照してください。

用語の変更：CDO が管理するデバイスへの変更を「展開」する

デバイスの構成の CDO のローカルコピーに加えた変更をデバイス自体に転送することを説明するために使用する用語を更新しました。以前はその転送を説明するために「書き込み」という言葉を使用していましたが、現在はその転送を説明するために「展開」という言葉を使用しています。

CDO を使用してデバイスの構成を管理および変更すると、CDO は構成ファイルの独自のコピーに加えた変更を保存します。これらの変更は、デバイスに「展開」されるまで、CDO で「ステージング」されたと見なされます。ステージングされた構成変更は、デバイスを通過するネットワークトラフィックには影響しません。CDO がデバイスに変更を「展開」した後にのみ、デバイスを通過するトラフィックに影響を与えます。CDO がデバイスの設定に変更を展開すると、変更された設定の要素のみが上書きされます。デバイスに保存されている構成ファイル全体を上書きすることはありません。

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。