2024 の新機能

この章では、2024 年に Cisco Defense Orchestrator に追加された機能の一部について説明します。

- 2024 年 11 月 （1 ページ）
- 2024 年 10 月 （3 ページ）
- 2024 年 9 月 （3 ページ）
- 2024 年 8 月 （4 ページ）
- 2024 年 6 月 （6 ページ）
- 2024 年 5 月 （8 ページ）
- 2024 年 4 月 （10 ページ）
- 2024 年 3 月 （10 ページ）
- 2024 年 2 月 （11 ページ）
- 2024 年 1 月 （11 ページ）

2024 年 11 月

Security Cloud Control の概要

Cisco Defense Orchestrator は「Cisco Security Cloud Control」になりました。

Security Cloud Control は、ネットワークセキュリティから始めて、Cisco Security Cloud を統合するように設計された新しい人工知能組み込みの管理機能ソリューションであり、更新されたユーザーインターフェイス、共通サービス、およびセキュリティクラウド全体の設定、ログやアラートを接続するサービスメッシュを備えた最新のマイクロアプリ アーキテクチャです。

Cisco Secure Firewall Threat Defense と ASA ファイアウォール、Multicloud Defense、および Hypershield を管理し、それらの管理機能を追加のセキュリティ製品に拡張します。さらに、Cisco AI Assistant はポリシーと設定をプロアクティブに最適化し、問題を検出してトラブルシューティングします。

次の Security Cloud Control の新機能を確認してください。

- ネットワーク セキュリティ ソリューションの一元管理エクスペリエンス

- 脅威に対する防御のデバイスを迅速にオンボーディングし、新機能を発見するのに役立つガイド付きの「Day 0」エクスペリエンス
- すべての管理対象デバイスをエンドツーエンドで可視性化する統合ダッシュボード
- アップグレードされたメニューナビゲーションと簡単なネットワークおよびセキュリティアプリケーションへのアクセスにより、合理化されたソリューションのユーザビリティ
- ファイアウォールルールの作成と管理を容易にする 人工知能アシスタント
- AIOps Insights による運用のシンプル化と強化されたセキュリティ
- セキュリティ態勢を改善し、不良構成を排除し、ルールを最適化するためのポリシー分析。
- 一貫したポリシーの適用とオブジェクト共有により強化されたハイブリッド環境での保護
- リモートアクセスおよびサイト間 VPN 接続のモニタリングの改善
- 1 つのテナントで最大 1,000 ファイアウォールをサポートするための拡張性の向上

詳細については、Security Cloud Control の製品ページ、Security Cloud Control のドキュメント、および『Cisco Security Cloud Control のよくある質問（FAQ）』を参照してください。

2024 年 11 月 7 日

Firewall 移行ツールの更新

Cisco Security Cloud Control（旧 Cisco Defense Orchestrator）は、Firewall 移行ツールの更新バージョンをリリースしました。サイト間 VPN 設定の事前共有キーの一括更新を実行し、移行対象の設定にエラーを含むパラメータがある場合に移行を続行するか中止するかを選択し、ターゲット Threat Defense デバイスをスポークとして既存のハブやスポーク VPN 設定などに追加できるようになりました。リリースに含まれる機能のリストについては、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。

クラウド提供型 Firewall Management Centerに対する更新

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。詳細については、クラウド提供型 Firewall Management Center のリリースノート [英語] を参照してください。

2024 年 10 月

2024 年 10 月 17 日

マルチテナントポータルでのテナントの作成

テナントを作成し、ユーザーを追加して、プロビジョニングされたテナントでクラウド提供型 Firewall Management Center と Multicloud Defense を有効にできるようになりました。

詳細については、「Manage Multi-Tenant Portal」[英語] を参照してください。

2024 年 9 月

2024 年 9 月 13 日

ポリシーアナライザとオプティマイザを使用したセキュリティポリシーの分析と最適化

新しいポリシーアナライザとオプティマイザを使用して、ポリシーを分析し、異常を検出し、キュレーションされた修復の推奨事項を受信できるようになりました。推奨事項を適用すると、ポリシーが常に最適な状態になり、ファイアウォールのパフォーマンスが向上します。このツールは、クラウド提供型 Firewall Management Center と CDO 管理対象のオンプレミス Firewall Management Center バージョン 7.2 以降の両方のポリシーを分析できます。左側のペインで、**[インサイト（Insights）] > [ポリシーアナライザとオプティマイザ（Policy Analyzer and Optimizer）]** を選択します。

詳細については、「Analyzing, Detecting, and Fixing Policy Anomalies Using Policy Analyzer and Optimizer」[英語] を参照してください。

2024 年 9 月 5 日

Firewall 移行ツールの更新

Cisco Secure Firewall ASA HA ペアから Threat Defense デバイスに設定を移行するときに、移行ツールで Threat Defense の高可用性（HA）ペアを設定できるようになりました。さらに、Cisco Cisco Secure Firewall ASA からサイト間 VPN 設定を移行するときに、サイト間ハブアンドスポーク VPN トポロジを設定できます。

詳細については、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。

Cisco Defense Orchestrator を使用した Cisco Secure Firewall Threat Defense 3100、4100、4200、または 9300 シャーシのオンボード

Firepower 3100、4100、4200、または 9300 シャーシを Cisco Defense Orchestrator を介してクラウド提供型 Firewall Management Center に追加できるようになりました。

管理センターとシャーシは、シャーシ MGMT インターフェイスを使用して個々の管理接続を共有します。Management Center は、シャーシレベルの正常性アラートを提供します。4100 または 9300 を設定する場合は、引き続き Cisco Secure Firewall Chassis Manager または FXOS CLI を使用する必要があります。3100 または 4200 の場合は、クラウド提供型 Firewall Management Center 内のシャーシ管理インターフェイスを使用できます。詳細については、「Onboard a Chassis」[英語] を参照してください。

2024 年 8 月

2024 年 8 月 23 日

クラウド提供型 Firewall Management Centerに対する更新

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。次に、更新の主要部分を示します。詳細については、クラウド提供型 Firewall Management Center のリリースノート [英語] を参照してください。

プラットフォーム

- Threat Defense バージョン 7.6.0 のサポート

高可用性/拡張性

- Cisco Secure Firewall 3100 のマルチインスタンスモード

アクセス制御：脅威の検出とアプリケーションの識別

- 機密性の高い、復号できないトラフィックの復号のバイパス

アクセス制御：アイデンティティ

- ユーザー アイデンティティ ソースとしての Microsoft Azure AD

ヘルス モニタリング

- 正常性データの収集（アラートなし）
- Firepower 4100/9300 のシャーシレベルの正常性アラート

管理

- Threat Defense の高可用性は、バックアップから復元した後に自動的に再開されます。

- 変更管理チケットの引き継ぎ、承認ワークフローのその他の機能。

トラブルシューティング

- CPU とルールプロファイラを使用して Snort 3 のパフォーマンスの問題をトラブルシュートします。

Management Center REST API

- Management Center REST API の更新。

2024 年 8 月 8 日

汎用テキスト Dynamic Attributes コネクタのサポート

汎用テキスト Dynamic Attributes コネクタを使用すると、IP アドレスのリストをテキストファイルで維持し、そのリストを使用してアクセス コントロール ポリシーを適用できます。たとえば、アクセス制御ルールの「許可リスト」または「ブロックリスト」の IP アドレスのリストを使用できます。IP アドレスを含むテキストファイルが更新されると、Cisco Secure Dynamic Attributes コネクタは、その IP アドレスリストを使用するアクセス制御ルールを定期的に更新します。テキストファイルごとに最大 10,000 個の IP アドレスを指定できます。詳細については、「Creating a Generic Text」[英語] を参照してください。

Multicloud Defense の VPN トンネルサポート

Multicloud Defense に VPN トンネルを作成し、Multicloud Defense Gateway を 1 つのエンドポイントとし、管理対象デバイスまたは GCP などのクラウド サービス プロバイダーをもう 1 つのエンドポイントとして作成できるようになりました。詳細については、Multicloud Defense ユーザーガイド [英語] を参照してください。

CDO の拡張監査ログ

監査ログに、ユーザーログイン、テナントの関連付けと関連付け解除、ユーザーロールの変更、Active Directory グループの変更など、ユーザー関連およびシステムレベルのアクションが表示されるようになりました。

詳細については、「Audit Logs」[英語] を参照してください。

2024 年 6 月

2024 年 6 月 27 日

アップグレードされた Cisco ASA アクセス コントロール ポリシー インターフェイス

CDO に、強化された共有アクセスリスト、簡素化されたルール管理、および強化された検索結果ナビゲーションを備えた、アップグレードされた Cisco ASA アクセス コントロール ポリシー インターフェイスが導入されました。

詳細については、「Manage ASA Network Security Policy」[英語] を参照してください。

2024 年 6 月 20 日

CDO の [イベントロギング（Event Logging）] ページに UTC とローカルタイムゾーンのトグルボタンが追加されました。この更新により、デバイスによって生成されたイベントは、ユーザーの選択に応じて、ローカルタイムゾーンまたは UTC のタイムスタンプで表示されるようになりました。デフォルトでは、イベントタイムスタンプはローカルタイムゾーンで表示されます。

詳細については、「Change the Time Zone for the Event Timestamps」[英語] を参照してください。

2024 年 6 月 13 日

アプリケーションモニタリング用の新しい 脅威防御 ダッシュボードウィジェット

CDO には、[上位のWebアプリケーション（Top Web Applications）]、[上位のクライアントアプリケーション（Top Client Applications）]、[上位のブロックされたWebアプリケーション（Top Blocked Web Applications）]、[ブロックされた接続別の上位のユーザー（Top Users by Blocked Connections）] の 4 つの新しいダッシュボードウィジェットが追加されました。これらの新しいウィジェットでは、最も使用されている Web アプリケーションとクライアントアプリケーション、および最もブロックされた接続を持つユーザを一目で確認できます。脅威に対する防御 ダッシュボードに表示される情報はシステムのライセンス方法、設定方法、デバイスの展開方法によって異なります。**[分析（Analytics）] > [FTDダッシュボード（FTD Dashboard）]** をクリックして、新しいダッシュボードウィジェットを表示します。

詳細については、「About the FTD Dashboard」[英語] を参照してください。

脅威防御 から クラウド提供型 Firewall Management Center への移行を一時停止して、インポートされた共有ポリシーを確認する

脅威に対する防御 から クラウド提供型 Firewall Management Center への移行プロセスを一時停止して、インポートされた共有ポリシー設定を確認できるようになりました。この段階では、評価期間は開始されず、脅威に対する防御 のマネージャも変更されないため、設定を確認する

時間ができます。設定を確認後、移行プロセスを再開して、スケジュールされた移行期間中にクラウド提供型 Firewall Management Center にデバイス固有の設定をインポートできます。[ツールとサービス（Tools & Services）] > [cdFMCへのFTDの移行（Migrate FTD to cdFMC）] の順にクリックします。

詳細については、「脅威防御 から クラウド提供型 Firewall Management Center への移行」を参照してください。

2024 年 6 月 6 日

Cisco AI Assistant を使用したファイアウォール管理

CDO 管理者は、Cisco Defense Orchestrator（CDO）の Cisco AI Assistant とクラウド提供型 Firewall Management Center の統合により、Cisco Secure Firewall Threat Defense ポリシーをより効率的に管理し、ドキュメントにアクセスできるようになりました。Cisco AI Assistant には、いくつかの主要な機能があります。

- [事前有効化アシスタント（Pre-Enabled Assistant）]：Cisco AI Assistant は、すべての CDO テナントでデフォルトで有効になっています。必要に応じて、テナントの[一般設定（General Settings）] ページで無効化できます。
- [容易なアクセス（Easy Access）]：CDO のネットワーク管理者と管理者は、ロギング後にテナントのダッシュボードの上部にあるメニューバーから Cisco AI Assistant に直接アクセスできます。

- [ユーザーオリエンテーション（User Orientation）]：Cisco AI Assistant ウィジェットを初めて開くとカルーセルウィンドウが表示され、Cisco AI Assistant の紹介、データプライバシー保護に関する説明、効果的な使用に関するヒントが提供されます。
- [ポリシールールアシスタンス（Policy Rule Assistance）]：Cisco AI Assistant は、Cisco Secure Firewall Threat Defense デバイスでポリシールールの作成プロセスを簡素化します。管理者は、簡単なプロンプトを使用してアクセス制御ルールを迅速に作成できます。
- [製品ナレッジリソース（Product Knowledge Resource）]：Cisco AI Assistant には、CDO とクラウド提供型のファイアウォール管理のドキュメントが取り込まれており、サポートが必要な場合は、質問できます。
- **ユーザーフレンドリーなインターフェイス**：
  - [シンプルテキスト入力ボックス（Simple Text Input Box）]：ウィンドウの下部にあり、Cisco AI Assistant を簡単に操作できます。
  - [スレッド履歴（Thread History）]：Cisco AI Assistant に尋ねる質問や一連の質問は、スレッドと呼ばれます。Cisco AI Assistant にはスレッド履歴が保持されるため、自分の過去の質問を参照できます。

- [フィードバック（Feedback）]：Cisco AI Assistant の応答に対する高評価または低評価のフィードバックを提供します。

詳細については、『Cisco AI Assistant ユーザーガイド』を参照してください。

2024 年 5 月

2024 年 5 月 30 日

インドの CDO

CDO は現在、インドの https://in.cdo.cisco.com で入手できます。https://www.getcdo.com にアクセスして、インドでテナントを作成できます。

クラウド提供型 Firewall Management Center の更新

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。この更新に含まれる多くの新機能については、クラウド提供型 Firewall Management Center のリリースノート [英語] を参照してください。

2024 年 5 月 23 日

オーストラリアの CDO

CDO は現在、オーストラリアの https://aus.cdo.cisco.comで入手できます。https://www.getcdo.com にアクセスして、オーストラリアでテナントを作成できます。

CDO API

CDO は、プログラムで CDO と対話できる RESTful API を提供するようになりました。API は、デバイス管理と展開、オブジェクト管理、検索、変更ログのモニタリング、ユーザー管理など、広範な CDO 機能へのアクセスを提供します。詳細については、Cisco Defense Orchestrator API Documentation [英語] を参照してください。また、CDO テナントの右上隅にあるユーザーメニューから移動して、CDO API ドキュメントにアクセスできます。

（注） CDO GraphQL API はサポート対象外、または使用不可となりました。

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストするようになりました。Secure Firewall ASA デバイスから 脅威に対する防御 デバイスに移行する前に、ネットワークおよびポートオ

ブジェクトを最適化でき、さらに、FDM による管理デバイスから 脅威に対する防御 デバイスに DHCP、DDNS、および SNMPv3 の設定を移行できます。

その他の新機能の詳細については、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。

CDO テナント通知とユーザー通知設定の再配置

通知とユーザー設定のタブが移動しました。[通知（Notifications）] は、**[設定（Settings）]** > **[通知設定（Notification Settings）]** の左側にあるナビゲーションバーに配置されており、電子メールサブスクリプションとサードパーティサービスの統合を管理できます。[ユーザー設定（User Preferences）] は、**[ユーザー名ID（Username ID）]** > **[設定（Preferences）]** > **[通知設定（Notification Preferences）]** に配置されており、テナントに関連付けられているデバイスで特定のアクションが発生したとき、デバイス証明書の期限が近いときや期限切れになったとき、またはバックグラウンドログ検索が開始、終了、または失敗したときにトリガーできます。[ユーザー通知設定（User Notification Preferences）] は個人ユーザーに固有の設定ですが、[テナント通知（Tenant Notifications）] はテナントに関係しているすべてのユーザーに適用されます。詳細については、「Tenant Management」[英語] を参照してください。

デバイス証明書の有効期限通知

CDO は、Cisco Secure Client（旧 AnyConnect）証明書の有効期限ステータスと、Cisco ASA、FDM による管理、および FTD デバイスの管理証明書を監視するようになりました。CDO は、各証明書の期限日が近づくか、期限切れになるとユーザーに通知します。

「Device Certificate Expiry Notification」[英語] を参照してください。

2024 年 5 月 16 日

Multicloud Defense の Cisco Security Cloud Control のサポート

Cisco Security Cloud Control Enterprise は、既存の Multicloud Defense アカウントの追加をサポートするようになりました。 Multicloud Defense タイルを Cisco Security Cloud Enterprise ダッシュボードに追加して、他のシスコ製品インスタンス、ユーザーアイデンティティの管理、および Cisco Security Cloud ポートフォリオ全体のユーザーアクセス管理を監視して一元化できます。詳細については、Multicloud Defense ユーザーガイド [英語] の「Multicloud Defense in Cisco Security Cloud Control」を参照してください。

2024 年 4 月

2024 年 4 月 25 日

CDO のダークテーマ

CDOは、よりカスタマイズ可能なユーザーインターフェイスの外観用にダークテーマオプションを提供するようになりました。右上隅にある[管理（admin）]ドロップダウンをクリックし、**[設定（Preferences）]**>**[一般設定（General Preferences）]**に移動し、[テーマ（Theme）]フィールドで[ダーク（Dark）]をクリックします。デフォルトのテーマは、[ライト（Light）]テーマです。

詳細については、「User Settings」[英語] を参照してください。

2024 年 4 月 18 日

オンプレミスの Cisco Secure Firewall Management Center へのネットワークオブジェクトの自動同期

CDO 内のネットワークオブジェクトを、CDO によって管理されるオンプレミス FMC に自動的かつ継続的に同期できるようになりました。この機能はデフォルトで無効になっています。この機能を有効にするには、[ツールとサービス（Tools & Services）] > [Firewall Management Center] に移動し、オンプレミス FMC を選択し、[アクション（Actions）] ペインで [設定（Settings）] を選択します。続いて、[ネットワークオブジェクトの検出と管理（Discover and Manage Network Objects）]をクリックし、[ネットワークオブジェクトの自動同期を有効にする（Enable automatic sync of network objects）] をクリックします。[ネットワークオブジェクトの検出と管理（Discover and Manage Network Objects）] トグルが有効になっていることを確認します。

詳細については、「Discover and Manage On-Prem Firewall Management Center Network Objects」[英語] を参照してください。

2024 年 3 月

2024 年 3 月 7 日

CDO テナントプロビジョニングの改善

強化された高速なプロビジョニングプロセスを使用して CDO テナントを作成できるようになりました。すでにテナントがある場合でも、新しい CDO テナントを作成できます。さらに、SecureX に対応していない オンプレミス Firewall Management Center がある場合、CDO を介し

て Cisco Security Cloud に登録できるようになりました。CDO アカウントがない場合は、登録プロセス時に作成できます。詳細については、「CDO テナントの作成」を参照してください。

個々の 脅威防御 デバイスによる Cisco Cloud へのイベントログの送信の無効化

個々の クラウド提供型 Firewall Management Center管理対象 脅威に対する防御 デバイス（バージョン 7.4.1 以降）で Cisco Cloud へのイベントログの送信を無効化できるようになりました。このデバイスレベルの制御を使用すると、必要に応じて、脅威に対する防御デバイスから Cisco Cloud に送信されるイベントログを一時的に停止できます。Cisco Cloud へのイベントログの送信を無効にする 脅威に対する防御 デバイスを指定するには、[インベントリ（Inventory）] をクリックし、対応する 脅威に対する防御 デバイスを選択して、[デバイス管理（Device Management）] ペインで [クラウドイベント（Cloud Events）] をクリックします。

Ubuntu での Secure Device Connector および Secure Event Connector のインストールの簡素化

Cisco DevNet サイトで利用可能な GitHub プロジェクト を使用して、Secure Device Connector と Secure Event Connector を Ubuntu サーバーに簡単に展開できるようになりました。詳細については、ドキュメントを参照するか、YouTube でビデオをご覧ください。

2024 年 2 月

2024 年 2 月 13 日

クラウド提供型 Firewall Management Center の更新

Cisco Defense Orchestrator は、クラウド提供型 Firewall Management Center の更新をリリースしました。この更新に含まれる多くの新機能については、クラウド提供型 Firewall Management Center のリリースノート [英語] を参照してください。

2024 年 1 月

2024 年 1 月 25 日

Firewall 移行ツールの更新

CDO は、Firewall 移行ツールの更新バージョンをホストするようになりました。Cisco Secure Firewall ASA の WebVPN 設定を、クラウド提供型 Firewall Management Center によって管理される Threat Defense デバイスの Zero Trust Access Policy 設定に移行できるようになりました。また、マルチコンテキスト Cisco ASA デバイスからシングルインスタンスの Threat Defense デバイスに移行する場合は、SNMP、DHCP、DVTI 設定を Cisco ASA から Threat Defense デバイスに移行して、ECMP ルーティング設定を移行できます。リリースに含まれるその他の新機能については、『Cisco Secure Firewall 移行ツール リリースノート』を参照してください。

2024 年 1 月 25 日

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。