At-a-Glance

利点

- 一貫性のあるセキュリティ ポリシーを適用
- セキュリティ ポリシーの管理を簡素化
- 次世代ファイアウォール機能の活用
- セキュリティを維持するための財務面およびリソース面の負担を軽減

Cisco Defense Orchestrator

簡素化されたポリシー管理によるセキュリティ体制の強化

包括的な防御を実現するには複数階層のセキュリティが必要です。しかし、特に地理的に分散している組織の場合、セキュリティ ツールを利用すればセキュリティ ポリシーを管理・把握し続けることがより困難になります。

分散されているセキュリティ デバイスのすべてを対象にしたポリシーの管理は、複雑である上に時間がかかり、不整合やギャップが発生するのはほぼ確実です。こうした状況により、重大なリスクが発生します。セキュリティ デバイスの誤った構成は、セキュリティ侵害の最も一般的な原因です。

これこそが、Cisco® Defense Orchestrator を導入すべき理由です。この製品はクラウドベースの管理アプリケーションであり、シスコのセキュリティ デバイス全体のポリシーを管理する負担を軽減します。対象となる製品には、Cisco Adaptive Security Appliance (ASA)、Cisco Adaptive Security Virtual Appliance、Cisco ASA with FirePOWER™ Services、Cisco Web セキュリティ アプライアンス、および Cisco Umbrella があります。

ビジネスに不可欠な情報を守る簡単な方法

Cisco Defense Orchestrator を利用することで、ネットワーク運用スタッフは、シンプルかつ一貫性のある方法でセキュリティ ポリシーを作成・維持しながら、管理の複雑さとコストを軽減することもできます。セットアップは簡単で素早く実行でき、競合が発生することもありません。Defense Orchestrator はクラウド ソリューションであるため、新たな設備投資 (CapEx)、フロア スペース、アプリケーション管理は不要です。

Defense Orchestrator の導入により、以下の事柄を実現できます。

一貫性のあるセキュリティを適用

エンドツーエンドの分析によりポリシーの例外を検出します。複数デバイス全体を対象にしたポリシー監査により、問題を解決します。ポリシーをクリーンアップし、一貫したポリシーの適用を実現するテンプレートにより、新しいデバイスに対して適切なポリシーを簡単に導入します。アウトオブバンドの変更が発生した場合に自動通知を受け取ることにより、ポリシーの変更をモニタします。

セキュリティ ポリシーの管理を簡素化

分散したデバイスに対してルールを一元的に設定、適用、管理でき、計画された変更と計画外の変更の両方に対して継続的なポリシー変更管理を効率化します。ポリシーをさらに簡単に最適化します。脅威に対してさらに素早く対応し、変更の影響を導入前にモデル化することにより、リスクを低減します。セキュリティ ポリシーをクラウドに対して拡張し、高い信頼性を実現します。

アプリケーション層の機能の活用

FirePOWER Services の次世代ファイアウォール (NGFW) およびアプリケーション保護を使用して高度なセキュリティを実装します。管理対象の各製品に対する詳細な知識は必要ありません。オンプレミスとリモート両方の従業員を、さらに広範な攻撃から保護します。

Defense Orchestrator によって、以下の事柄を実現できます。

- **分析:** すべてのデバイスを対象として、エンドツーエンドのセキュリティ ポリシー設定を一元的に運用できます。セキュリティ設定を分析して誤った設定を検出し、セキュリティ ポリシーおよびオブジェクトにおける計画された変更および計画外の変更を管理できます。デバイスごとのセキュリティ設定で、エンドツーエンドのポリシー分析を利用できます。専門家の支援は必要ありません。
- **モデル:** 標準化されたポリシー テンプレートを作成できます。このテンプレートにより、ビジネスの成長に簡単に対応して、セキュリティ設定を一貫して適用できます。デバイスを導入する前に、変更の影響をモデル化できます。
- **修復:** デバイスに対して適切な変更が適用されていることを検証できます。変更管理プロセスごとに、適切な変更がリアルタイムで、またはオフラインで適用されていることを確認できます。Defense Orchestrator によって管理されているすべてのセキュリティ製品を対象に、一貫したセキュリティ体制を適用し、維持できます。
- **可視化:** 上位のアプリケーション、接続先、カテゴリ、攻撃、およびリスクに関する蓄積された情報を確認することで、Web ポリシーの適用の効果を確認します。

詳細

シスコには、セキュリティ テクノロジーに関する 10 年以上の経験と、業界最大規模のセキュリティ データベースがあります。このソリューションは、Cisco ASA、ASA with FirePOWER Services、Cisco Web セキュリティ アプライアンス、WSA、および Cisco Umbrella など、複数のプラットフォームのポートフォリオを統合するための、当社のコミットメントを表すものです。

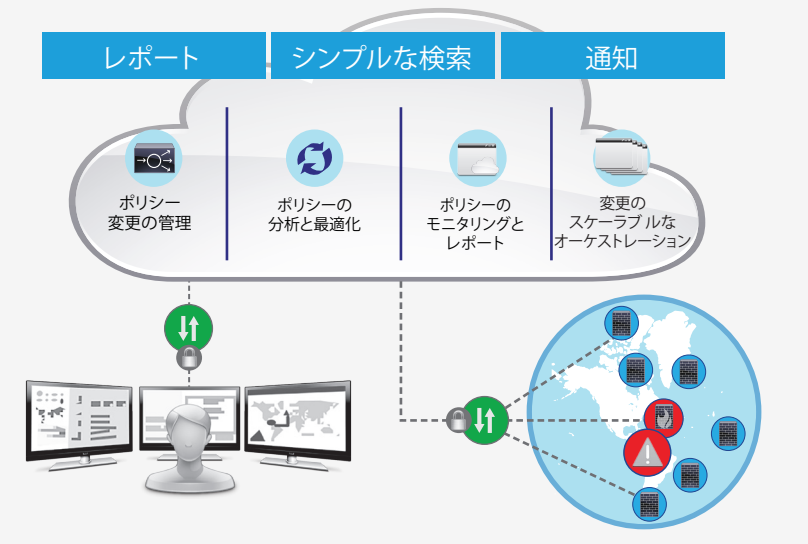
Cisco Defense Orchestrator について詳しくは、cisco.com/go/cdo を参照してください。

Defense Orchestrator が貴社をどのように支援するのか直接体験するには、まず cdosales@cisco.com までご連絡ください。

セキュリティを維持するための財務面およびリソース面の負担を軽減

高い安全性と信頼性を備え、常時利用可能で、スケーラブルなマルチテナント クラウド ソリューションを使用して、どこからでも管理できます。セキュリティ体制の強化と維持にかける時間とリソースを減らし、他の優先事項に当てることができます。

図 1. Cisco Defense Orchestrator の主な機能



機能	期待できる成果
デバイスのオンボーディング	複数の安全性の高い手法により、オンラインかオフラインを問わずに管理対象デバイスに接続する
オブジェクトおよびポリシーの分析	デバイス全体を対象に、重複したポリシーや未使用のポリシー、一貫性のないルール、または一貫性のないネットワーク オブジェクトなどの問題をポリシーやオブジェクト レベルで検出し、修正する
アプリケーション、URL、マルウェア、脅威のポリシー分析	アプリケーションまたは接続先のホスト名によるトラフィックのブロックにより、レイヤ 7 の保護を管理する
セキュリティ テンプレート	テンプレートを設計・管理して、新しいデバイスの簡単な導入を実現する
シンプルな検索	任意のオブジェクト名、ACL 名、ネットワーク、またはアプリケーション ポリシー エレメントで検索することで、デバイス タイプ全体に対してポリシーがどのように適用されているかを確認する
変更の影響のモデル化	非実動環境に変更を適用することにより、ポリシー変更の影響を導入前に判断する
アウトオブバンドの通知	ポリシー変更時に自動的な通知を受け取る
レポート	上位のアプリケーション、宛先、カテゴリ、攻撃、リスクに関するレポートを利用して、ポリシーの効果を追跡する

Cisco Defense Orchestrator の利用事例

ある国際的な小売企業では、全国にわたる数千の小売支店に対して、会社運営でバックホーリングを発生させることなくポリシー構造を適用できる方法を探していました。

同社は、エンドツーエンドの可視性および制御を向上させるために、次世代の機能へと移行することを希望していました。そこで、シンプルな管理プロセスにより、ネットワーク全体のポートとアプリケーションを対象にしたテンプレートを作成しました。

C45-736943-02 07/17