柔軟性の高いセキュアなブランチの変革

シスコは、ブランチ ユーザ、接続されたデバイス、およびアプリケーションの使用を、WAN 全体のすべてのダイレクト インターネット アクセス (DIA) ブレークアウトおよびすべてのトラフィックで保護します。

ブランチはビジネスの顔であり、収益の 90% を生み出します。成長を加速するために、ブランチをデジタル化し、ネットワークのアーキテクチャを再構築して、ブランチをインターネットやマルチクラウド アプリケーションに直接接続しようとしています。

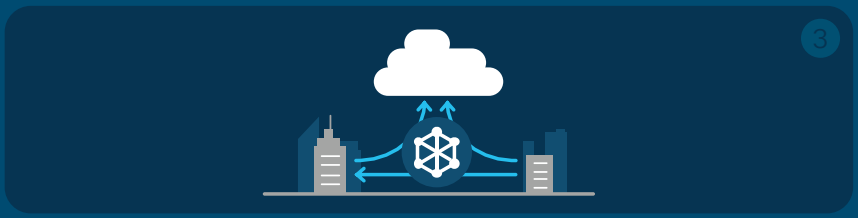
お客様がブランチを保護する戦略は 3 つあります。DIA を有効にしている場合 (#2)、または間もなくそうする場合 (#3) には、ブランチからクラウド エッジへのセキュリティ スタックが必要です。

バックホーリングを続行する

データセンター (DC) エッジにある既存のセキュリティ スタックは、すべてのブランチ ユーザ、接続されたデバイス、およびアプリケーションの使用に対応しています。

セキュリティの向上

一部のゲスト ユーザもしくはすべてのユーザ、O365 などの一部のアプリまたはすべてのアプリによる既存の DIA ブレークアウトを保護しているセキュリティ スタックを更新したり、レイヤを追加したりします。



SD-WAN およびセキュリティの導入

数十から数千箇所に及ぶ、新しい DIA ブレークアウトを備えたブランチに変革し、優れたセキュリティ、パフォーマンス、シンプル化、コスト削減を実現します。

すべてのセキュリティ リスクを軽減する

SD-WAN ベンダーの 90% 以上は、従来のセキュリティ ベンダーではありません

内部から外部
マルウェア感染
命令および制御
フィッシング攻撃
許容外の使用

内部
認証されていないアクセス
水平方向への 感染活動
コンプライアンス違反

外部から内部 *
不正アクセス
サービス拒否攻撃

* オンサイト サービスやデバイスにリモートからアクセス可能

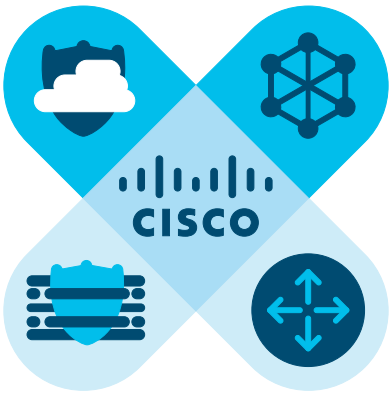
ブランチからクラウドへのシスコのオープンな統合型アーキテクチャは、エッジに配置されるセキュリティスタックとセキュアな SD-WAN ファブリックを備えており、ブランチを柔軟に変革します。

セキュア インターネット ゲートウェイ

すべてのポートを脅威から保護し、インターネットやマルチクラウド アプリケーションへの安全なアクセスを実現します

エッジ ファイアウォールの柔軟性

次世代またはゾーン ベースのファイアウォール オプションでオンサイト サービスやデバイスを保護し、コンプライアンスを遵守します



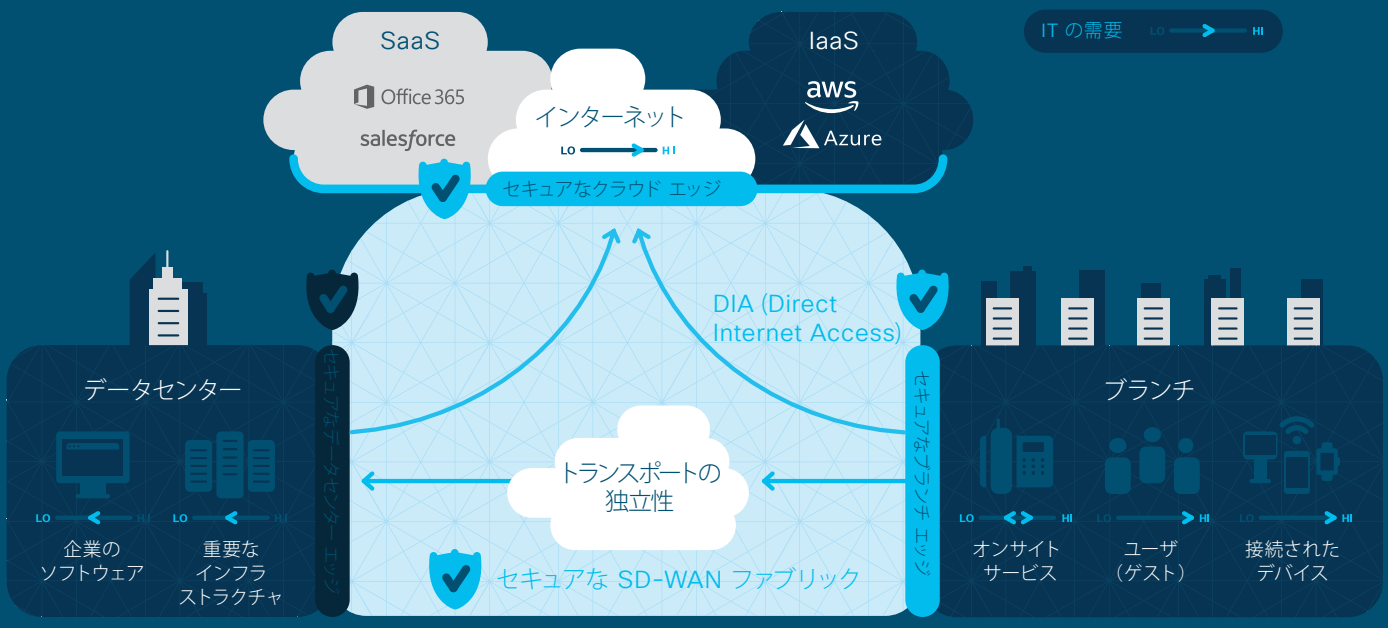
SD-WAN

クラウド向けの柔軟でセキュアな接続とクラウドによる俊敏な運用を実現しながら、アプリケーション パフォーマンスを保証します

エッジ ルータの柔軟性

音声、ビデオ、ワイヤレス、LTE、コンピューティング、コンテナなど、オンサイトの IT 需要に適合する、シン、リッチ、またはフル スタックのルータ オプション

シスコのソリューションによって、ブランチからクラウド エッジまで防御のすき間のない安全なブランチ変革を実現できます。



セキュリティの有効性とネットワークの対応力向上を同時に実現します。

マルチベンダー ソリューションとは異なり、Talos 脅威インテリジェンスを利用したシスコの脅威検知は、業界でトップクラスのスピードを誇ります。シスコの保護は、Umbrella の統計モデルおよび機械学習モデル、AMP のファイル レピュテーションおよび動的分析を活用して、常に学習および適応します。

ユーザ エクスペリエンスとビジネスの継続性を両立させます。

最適な導入事例が少ない新興企業とは異なり、シスコは、毎日 9000 万を超えるユーザが使用する、スピードと信頼性に優れたインフラストラクチャを構築しています。シスコの SIG (Secure Intenet Gateway) により、100% のビジネス稼働時間を保証します。シスコの SD-WAN により、アプリケーションの停止ゼロを保証します。

変革的

クラウド提供のセキュリティ
効果的に学習および適応し、攻撃される場所を保護

インテント ベース ネットワーキング
継続的に学習および適応し、アプリケーションのパフォーマンス問題に対応

高度な分析
アプリケーションの QoE モデルと脅威インテリジェンスによって、ビジネスや IT に関するインサイトを獲得

柔軟性

エッジ セキュリティ フルスタック
外部から内部、内部から外部、内部におけるレイヤ 3 ～ 7 のポリシーベースの保護

エッジ デバイスの柔軟性
ルータおよびファイアウォールには、シン、リッチ、フルスタック オプションが用意されており、オンサイトの IT 需要や既存の導入環境に柔軟に対応可能

オープン アーキテクチャ
プログラム可能な CLI に対する API でノースバウンドの自動化およびサウスバウンドの統合を実現

最もシンプル

クラウド管理
ブランチまたはクラウド エッジでネットワークを確立してセキュリティを適用することで運用コストを削減

ゼロ タッチのプロビジョニング
IaaS および SaaS アプリケーション用のクラウド導入を自動化

トランスポートの独立性
DIA またはセキュア VPN オーバーレイを使用するワークロードに対応したビジネス ポリシーを有効化

どうやって始めればよいですか。

1. どんな WAN トポロジや内部から外部のリスクでも、シスコの SIG、Umbrella によって、クラウド エッジのセキュリティが向上し、場所を問わずにユーザが保護されます。

   詳細：cisco.com/jp/go/umbrella
   トライアル：signup.umbrella.com

2. ブランチ エッジと SD-WAN ファブリックを保護するための単一のエッジ デバイスを求めている、予算が限られた IT チームには、Cisco Meraki MX が最もシンプルな方法です。

   詳細：cs.co/MX-fw-sdwan
   デモ / トライアル：cs.co/MX-demo

3. 複雑な WAN トポロジへの対応力を最大化したいネットワーク チームには、Cisco SD-WAN が最も柔軟性の高い方法です。

   詳細：cisco.com/jp/go/sdwan

4. リスクの高いロケーションの有効性を最大化したいセキュリティ チームにとって、シスコの NGFW は最も柔軟性があります。

   詳細：cs.co/FMC-demo