Cisco Umbrella

E-Book

ブランチ セキュリティに 対する先進的な アプローチ

クラウド エッジのセキュリティを確保して すべてのブランチ、リモート、およびローミング ユーザを保護。

cisco

方法を把握し、対応を開始。

ブランチ
ブランチ セキュリティの必然性を高めている要因

お客様の課題
ブランチで起きている変化

リスク
ブランチが直面しているリスク

クラウド エッジ
エッジ、そしてクラウド エッジとは

メリット:
セキュリティ + ネットワーキング:統合アプローチ

シスコのビジョン
ブランチとクラウド エッジを接続するセキュアなアーキテクチャ:シスコのビジョン

Umbrella
セキュアなクラウド エッジは DNS レイヤの適用から始まる

対応の開始
第一歩を踏み出すために

ブランチ セキュリティの必然性を高めている要因

ブランチは重要性が高まる中、変化しつつあります。

今日のビジネス環境では、これまで以上にブランチ オフィスの重要性が高まっています。平均的な企業では、ブランチで収益の大部分が創出され、80% のユーザ[1] がブランチを拠点としています。ただし大半の組織では、ブランチのセキュリティが限定的であるか、あるいはまったく確保されていないのが実情です。

企業はこれまで、ワイド エリア ネットワーク(WAN)を使用してブランチをデータセンターに接続し、すべてのトラフィックを中央の企業ネットワークにバックホールしていましたが、ビジネスと IT に対する新たなニーズがそうしたアーキテクチャに課題をもたらしています。事業運営では、複数のクラウドを介した Software as a Service(SaaS)および Infrastructure as a Service(IaaS)アプリケーションの利用が中心となり、従業員が使用するコネクテッド デバイスとそれらが使用される場所は、年々増加しています。生産性を最大限に高めるには、そうしたデバイスのすべてに高速かつ安定した接続を提供する必要があります。

ブランチの変革を迫っている 4 つの要因

複雑度
自動化されておらずエラーが発生しやすい運用と IT スキルの不足

コスト
使用率が低く柔軟性に欠ける WAN リンクと帯域幅の需要の増大

回避
新たな接続を確立するまでに時間がかかるうえ、アプリケーションのパフォーマンスに一貫性がない

中断
セキュリティとビジネスや IT に関する情報の欠如が原因で意思決定に時間がかかる

ブランチで起きている変化

WAN には複数の問題があります。

WAN は、プライベート データセンター内の IT リソースへのアクセスをブランチ オフィスとローミング ユーザに提供する目的で構築されました。しかし今日では、ネットワークの分散化が進み、多くのユーザが直接 SaaS アプリケーションに接続しているため、トラフィックをバックホールしてセキュリティ ポリシーを適用するのは効率的ではありません。しかし問題はそれだけではありません。インターネット トラフィックのバックホールはコストがかかるうえ、遅延を増大させます。そのためユーザは作業でフラストレーションを感じ、生産性が低下します。

このような理由から、多くのブランチ オフィスがダイレクト インターネット アクセス(DIA)に移行しています。実際に企業のデータ トラフィックの 40 ～ 60% がプライベート WAN からインターネットに移行しました。[2] その方法は、WAN をソフトウェア定義型(SD-WAN)に再設計することです。また、LAN をデジタルして、IoT、リッチ メディア コンテンツ、ゲスト Wi-Fi などに対応させる必要もあります。

WAN からの移行
企業のデータ トラフィックの 40 ～ 60% がプライベート WAN からインターネットに移行しています。

ブランチのデジタル化
多くの組織が、IoT、デジタル サイネージ、オムニチャネル エクスペリエンス、リッチ メディア コンテンツ、ゲスト Wi-Fi などの新たなデジタル ビジネス イニシアチブを導入しています。


30 %
エントリ ポイントとしてブランチを
標的にしている高度な脅威の割合。[3]

ブランチが直面しているリスク

アーキテクチャの変化とともにリスクが増大しています。

ブランチ オフィスや遠隔地の従業員にインターネットへの直接アクセスを許可することにより、成長を加速させ、通信コストを大幅に減らし、ネットワークのパフォーマンスを向上できます。こうしたメリットは IT 関連の意思決定者もはっきりと把握しています。ただし、全面的または部分的な DIA が増加するとリスクも増大します。主なリスク要因は攻撃対象領域の大幅な拡大ですが、それだけではありません。

デジタル ビジネス プロジェクトの結果として、2022 年までに企業で生成されるデータの 75% が従来の中央のデータセンターやクラウド以外で作成および処理されるようになります。[4]

脅威が進化しつつある今日では、セキュリティに対する先進的なアプローチが必要です。

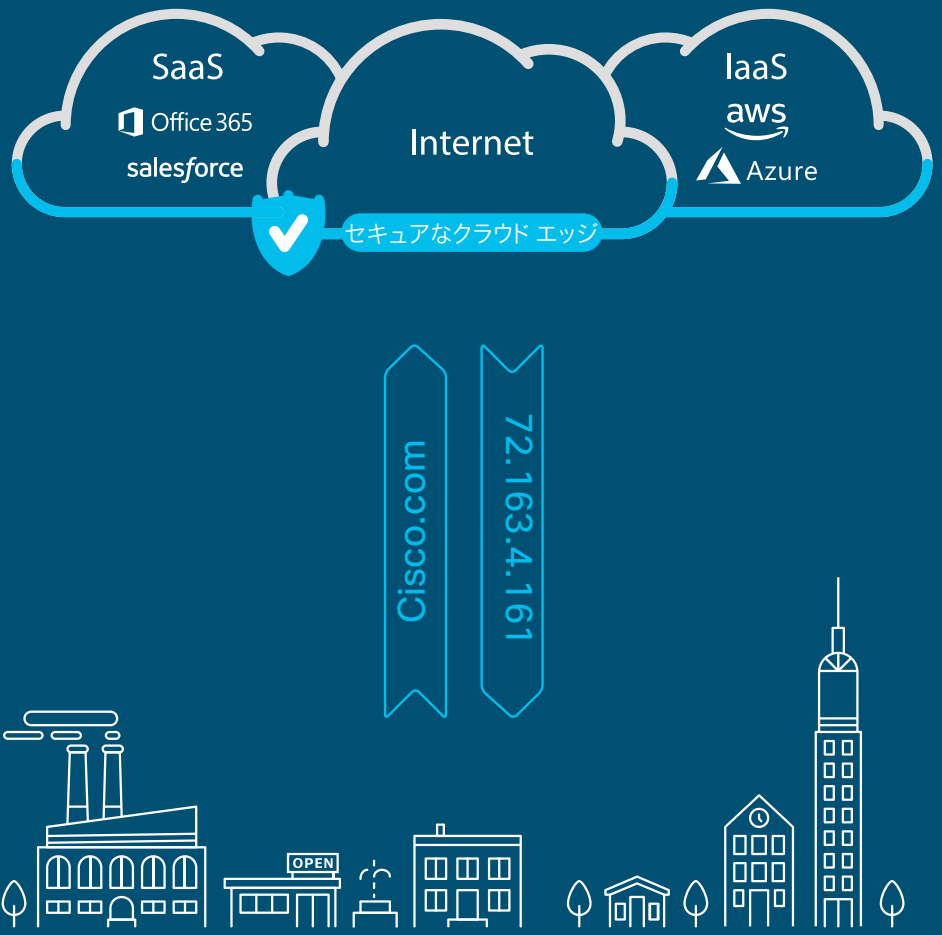
今日では、IT アーキテクチャだけでなく脅威も進化を遂げており、これまで以上に高度化しています。今日の組織は、マルウェア感染、コマンド & コントロール コールバック、フィッシング攻撃、サービス拒否攻撃、不正アクセス、許容できない利用といった多くの脅威からブランチを守る必要があります。

内部のセキュリティ リスク
従来とは異なるユーザやデバイスの接続が増加し、重要なビジネス リソースがリスクにさらされる

外部のセキュリティ リスク
DIA によってユーザ、接続デバイス、および使用中のアプリケーションがリスクにさらされる

エッジ、そしてクラウド エッジとは

今では最前線でセキュリティを確保してインターネット、SaaS アプリケーション、および IaaS を保護することが不可欠です。



以前の重点保護対象は、従来のセキュリティ スタックが構築されていたデータセンター エッジでした。しかし今日では、エッジは 1 つだけではなく、データセンター、クラウド、ブランチという 3 つの種類が存在します。それらすべてを統合できるのが WAN ファブリックです。

今日では、かつて組織で管理されていたユーザと接続デバイスが企業の管理の枠外にあり、それが可視化とセキュリティ保護の空白地帯を生み出しています。インターネットに直接接続するブランチ オフィスの増加に伴って、データセンター エッジだけでなくクラウド エッジも保護することが重要となっています。

今や、インターネット、SaaS アプリケーション、および IaaS を最前線で保護することが不可欠なのです。セキュアなクラウド エッジを実現すれば、データ漏洩のリスクを軽減し、遅延を増大させることなく、すべてのポートとプロトコルでマルウェアを阻止できます。

セキュリティ + ネットワー キング: 統合型のアプローチ

シスコでは、ブランチとクラウド エッジを接続するアーキテクチャを統合することでセキュリティとネットワーキングを強化できる(すべき)と考えています。

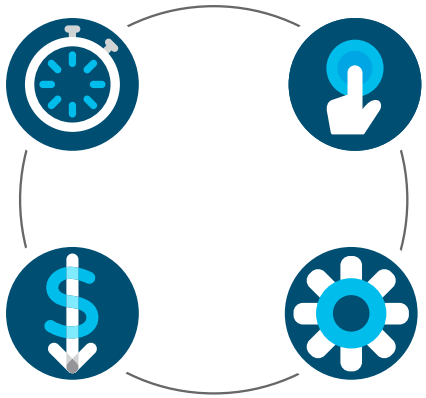
統合アプローチのメリット:

セキュリティの簡素化と高速化

検出時間を最短にして脅威の阻止を簡素化できます。

ユーザ エクスペリエンスの向上

非常に安定した高速のインターネットおよびマルチクラウド アクセスを実現できます。



ネットワーキングのコストの削減と俊敏性の向上

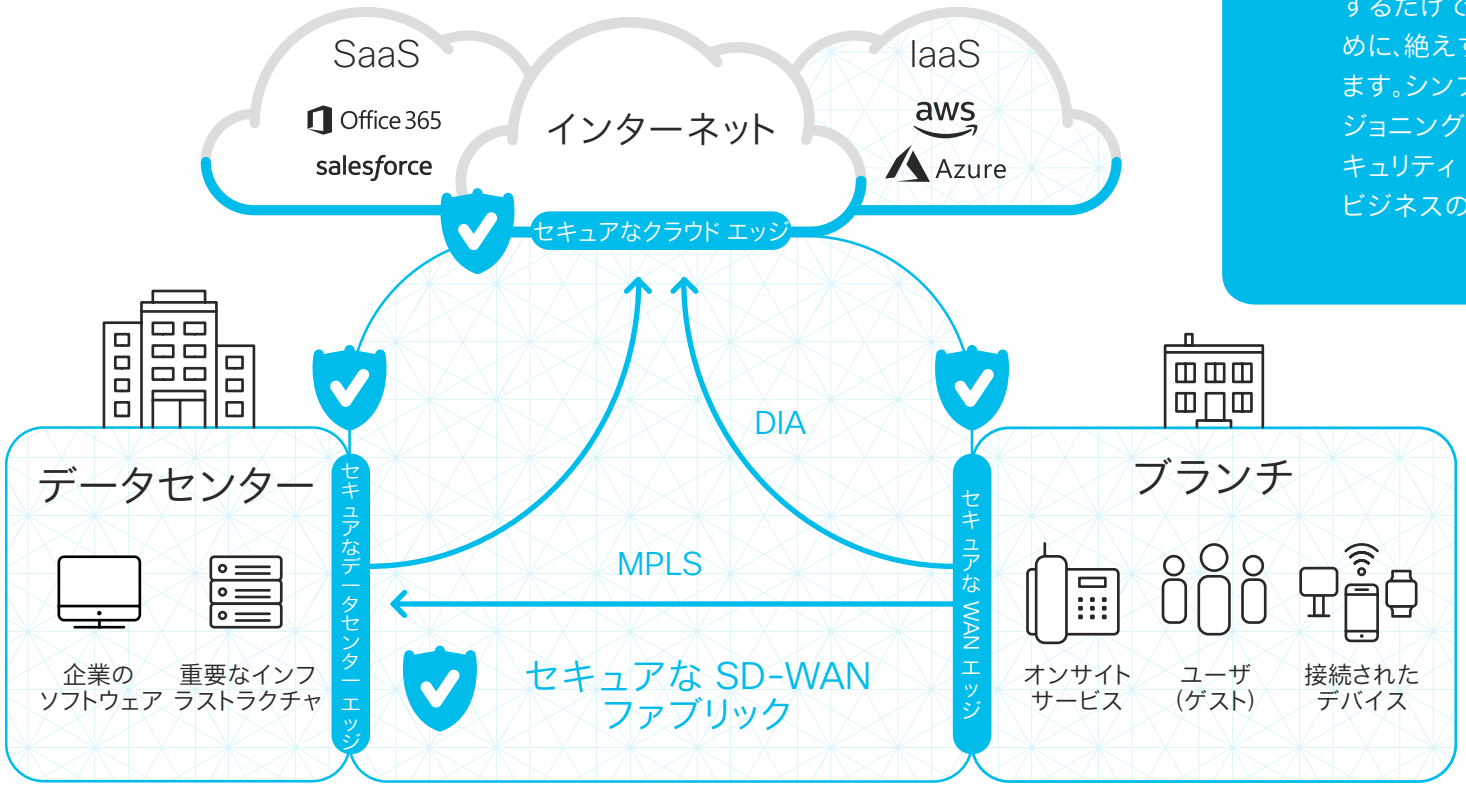
WAN に場所、デバイス、およびアプリケーションを簡単に追加すると同時に、運用コストと資本支出を最小限に抑えられます。

ビジネスの継続性の向上

インテントベース ネットワーキングを使用すればアプリケーションの保護を自動化でき、データからより有益な分析情報を得られます。

ブランチとクラウド エッジを接続するセキュアなアーキテクチャ:シスコのビジョン

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。



ブランチ オフィスの最大限の保護は、ネットワークとセキュリティが統合されたアーキテクチャによって実現します。こうしたアーキテクチャは迅速に展開でき、セキュリティの有効性やユーザ エクスペリエンス、ネットワークの俊敏性、ビジネスの継続性を向上させます。

シスコの統合アプローチは、ブランチのユーザ、接続デバイス、および使用中のアプリケーションが生み出す数万の DIA ブレイクアウトを保護します。シスコのインテントベース ソリューションは Cisco Talos のセキュリティ インテリジェンスに支えられ、クラウドで提供されます。攻撃を受けた場所を把握するだけでなく、業界最短の検出時間を実現するために、絶えず学習して状況に適応し、環境を保護します。シンプルなクラウド管理とゼロ タッチ プロビジョニングにより、ブランチに対する内外両方のセキュリティ リスクを軽減し、ネットワークの俊敏性とビジネスの継続性を向上させます。

セキュアなクラウド エッジは DNS レイヤの適用から始まる

Cisco Umbrella は、ユーザの場所を問わずインターネット上の脅威を最前線で防御できるセキュア インターネット ゲートウェイ(SIG)です。クラウド ソリューションとしての Umbrella はコストを削減するだけでなく、マルウェアやフィッシング、コマンド & コントロール コールバック、許容できない要求に対して防御を強化します。以下にその方法について説明します。

DNS および IP レイヤの適用

Umbrella は、DNS を使用してすべてのポートとプロトコル、さらには 直接 IP 接続の脅威を阻止します。マルウェアがエンドポイントやネットワークに到達する前に阻止します。

インテリジェント プロキシ

Umbrella は、Web トラフィック全体ではなく、高リスク ドメインに対する要求のみをルーティングさせることで、URL とファイルを詳細に調べます。遅延を生じさせたりパフォーマンスに影響を与えたりすることなく、効果的に環境を保護できます。

コマンド & コントロール コールバックのブロック

その他の方法でデバイスが感染した場合でも、攻撃者のサーバへの接続を Umbrella がブロックします。データ漏洩や、ランサムウェアによる暗号化を阻止します。

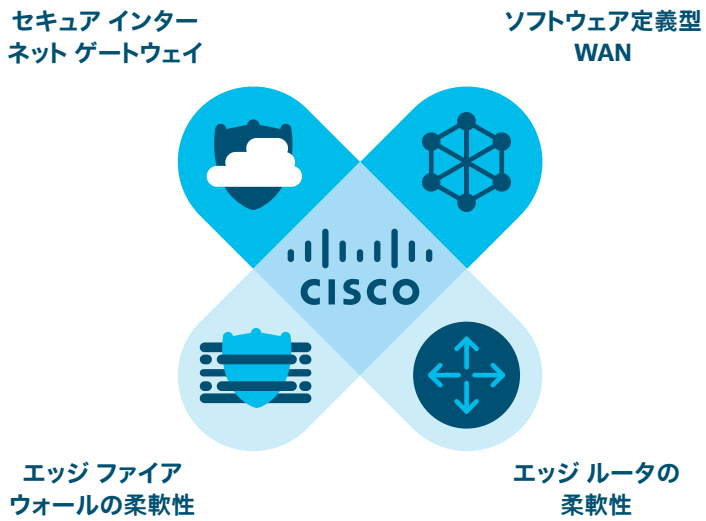
Umbrella は、インターネット アクティビティから学習して、現行の脅威や新たな脅威で構築された攻撃インフラを自動的に特定します。インターネット全体のマルウェア、ドメイン、IP、およびネットワークの関係を把握します。

Umbrella を活用すれば、修復のコストと侵害による損害を減らし、脅威を検出して封じ込めるまでの時間を短縮できます。また、あらゆる場所やユーザのインターネット アクティビティとクラウド アプリケーションに対する可視性を向上させます。Umbrella は、展開するだけでブランチ オフィスを保護できる最もシンプルなセキュリティ ソリューションです。ハードウェアをインストールしたり、ソフトウェアを手動で更新したりする必要がありません。ブラウザベースのインターフェイスにより、迅速な設定と継続的な管理が可能です。

他社のセキュリティ ソリューションに欠落している保護能力

シスコは 1 日あたり 1,750 億件を超えるインターネット要求を分析することで、比肩することのない分析情報を活用しています。ブランチ ネットワークに SD-WAN を導入する際や、顧客にゲスト Wi-Fi を提供する際、Umbrella はインターネットに直接接続するユーザをシンプルかつ効果的な方法で保護します。

また、Cisco SD-WAN と Umbrella の統合によって、ネットワーク全体から数百のデバイスに数分で Umbrella を展開し、マルウェア、ランサムウェア、C2 コールバックなどの脅威から Web/DNS レイヤを即座に保護できます。



1,750 億件

インターネット要求

9000 万人

1 日のアクティブ ユーザ数

1.6 万社

企業顧客

160 カ国

導入先の地域

Cisco Umbrella

対応の開始
クラウド エッジを保護することから開始

ネットワーク内外の
可視化と保護

脅威に対する防御の
最前線

アプリケーションの検出とブロック
によるシャドー IT の可視化と制御

脅威を早期に検出できる
インテリジェンス

悪意のある接続先や
ファイルを広範にカバー

インターネットに直接アクセスする
ユーザに対する Web/DNS レイヤ
の保護

最もオープンでシンプル
なクラウド セキュリティ
プラットフォーム

数分で世界中の脅威を防ぐことが
できます。14 日間無料でお試しく
ださい。

Umbrella の無料トライアルを開始

出典:

1. 「It's not your dad's branch office」、Nojitter.com、2016 年
2. 「Network Evolution and Market Outlook」、IDC 社、2017 年
3. Gartner 社、「Bring Branch Office Network Security Up to the Enterprise Standard」、Jeremy D'Hoinne 著、2013 年
4. Gartner 社、「Start Moving Data Management Capabilities Toward the Edge」、Ted Friedman 著、2017 年