Cisco Umbrella

eBook

脅威のリスクを低減し SASE への道をひらく クラウドセキュリティ

新しいビジネス手法を保護する最新のセキュリティ

クラウドによってすべてが変化した今、セキュリティにも変化が必要

クラウドへの移行は、今日のビジネスにとって革命的でした。ユーザーは新しい方法でツールやデータとつながり、生産性、コラボレーション、働き方の柔軟性が大幅に強化されました。対費用効果の高さ、拡張性、利用のしやすさを考えると、クラウドへの大規模な移行が迅速に進んだことも不思議ではありません。

2020 年の時点で、企業の 91% はパブリッククラウドを、72% はプライベートクラウドを使用しています。実際には、大半の企業が両方を使用し、69% がハイブリッドソリューションを選択しています。[1]

しかし、革命はそう簡単に実現するものではありません。クラウドは組織のセキュリティの維持に新しい課題をもたらしています。業務は一元的に管理されたオフィスからリモートに移行し、ユーザーはクラウドに直接アクセスするようになりました。つまり企業ネットワークの保護を離れて、脅威のリスクにさらされるようになったのです。さらに、インフラストラクチャ、アプリケーション、膨大な量の機密データがクラウドに保管されているため、侵害が発生すれば、企業は深刻な結果に直面します。

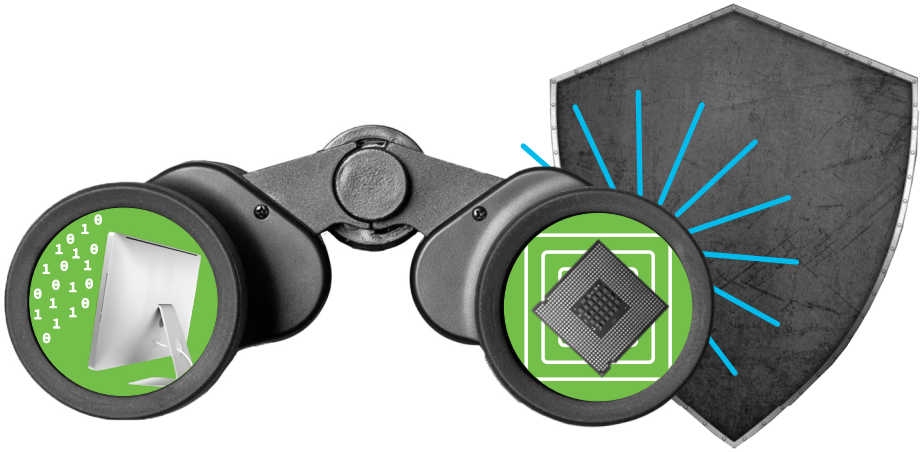
もはや従来のファイアウォールやセキュア Web ゲートウェイでは、組織が必要とするすべての保護を提供できなくなりました。クラウド独自のセキュリティの懸念に対応する新しいソリューションを導入するときがきています。

働き方の変化に伴い、脅威も変化

技術革新は絶え間なく進み、ますます加速しています。残念ながら、このことは脅威にも当てはまります。新しいテクノロジーによって私たちの働き方は進化していますが、攻撃者も増加し、その技法も高度化しています。独自の手法を使用し、特にクラウドを標的にして組織に侵入しています。

しかし、サイバー攻撃のスピード、性能、ステルス性が高まっているにもかかわらず、IT 担当者は依然として従来のネットワーク防御に依存しています。つまり組織の防御は時代遅れになるばかりで、高度なクラウドベースの脅威を効果的に防げなくなっています。

この新しい分野の攻撃に先手を打つために、最新のセキュリティソリューションは事後対応型でなく事前対応型であることが求められています。つまり、発生した脅威に対応するだけではなく、積極的にデータ、インサイト、インテリジェンスを活用して、ネットワークまたはユーザーに到達する前に脅威をブロックすることです。



脅威は驚異的な速度で増加

56% 毎日 1,000 以上のセキュリティアラートに対処している大企業の割合

70% 過去 5 年間で取り扱うアラートが倍増したセキュリティ担当者の割合 [2]

クラウドセキュリティ導入に立ちはだかる障害

企業はクラウド向けにもっと効果的な新しい保護が必要であることを認識しています。しかし、その導入は必ずしも簡単ではありません。最近のレポートによると、クラウドセキュリティの 導入を阻んでいる 3 つの大きな原因は、人材およびトレーニングの不足(53%)、新しいソリューションと既存のテクノロジーを統合できないこと (37%)、そして予算上の制約 (36%) です。[3]

予算の制約は常にセキュリティチームについてまわる問題ですが、統合こそ最近の本当の問題です。相互に接続されていないシステム (新しいセキュリティソリューションが、組み込まれるのでなく後から「追加」されている) があると、特に IT リソースが不足している組織の場合は脅威に先手を打つことが一層難しくなります。さまざまなシステムから膨大な量のアラートが発せられるため、セキュリティ態勢を総合的に理解することや、優先して対応すべきアラートを把握したりするのは容易ではありません。

クラウドセキュリティが最も効果を発揮するのは、ソリューションが統合およびシンプル化され、IT チームが環境を完全に可視化して最新の状況を掌握できるときです。

クラウドセキュリティの導入を阻む 3 大原因

53% スタッフ、人材、トレーニング不足

37% 新しいソリューションと既存のテクノロジーを統合できない

36% 予算上の制約

72%

クラウドセキュリティ態勢に自信がない組織の割合[3]

クラウドベースのリスクを解決するクラウドベースのセキュリティ

クラウド内のユーザー、デバイス、データ、アプリケーションを確実に保護するためセキュリティチームに必要なのは、企業の境界を越えて拡張できる包括的な可視性です。

ユーザーがどこからインターネットにアクセスするかにかかわらず、潜在的な脅威を特定し、悪意のあるアクセス先や活動をブロックし、攻撃にいち早く対応できる必要があります。

また、1 か所から一貫性のあるセキュリティポリシーを簡単かつ効率的に適用できなければなりません。

つまりセキュリティチームに必要なのは、場所を問わずに可視性、コントロール、保護を提供できるクラウドベースのセキュリティソリューションです。そのソリューションを見つけるための明確な道すじがあります。

クラウドベースのセキュリティソリューションの重要コンポーネント

クラウドを想定して構築された保護機能

- 接続されたクラウドアプリケーションの包括的な可視性とコントロール
- パブリック クラウド インフラストラクチャで実行されているアプリケーションに拡張されたセキュリティとコントロール
- 自社開発またはサブスクライブしているクラウドアプリケーションの保護

プロアクティブなパフォーマンス

- オンネットワークとオフネットワーク両方の脅威をより簡単に特定し、すばやくブロックできるようにする信頼できるインテリジェンス
- 悪意のあるインフラストラクチャの特定と、クラウド内の機密データの修復

今日のニーズだけでなく、将来のニーズも想定して構築

- 環境全体に拡張可能で、既存のスタックとシームレスに統合できるセキュリティ

堅牢なセキュリティ

- 侵害を受けたアカウント、組織内に潜む脅威、クラウドマルウェア、データ侵害に対する防御

SASE：場所を問わずにユーザー、アプリケーション、デバイスを保護する新しいアプローチ

前述のとおり、クラウドセキュリティにとっての大きな障害の 1 つは、多くのソリューションがうまく連動せず、必要な追加作業や潜在的な保護のギャップが生じていることです。今日の脅威に対応するには、ネットワーク機能とセキュリティ機能をクラウドで統合する必要があることが明らかになっています。

そこで有効なのが SASE です。

2019 年に Gartner によって紹介されたセキュア アクセス サービスエッジ(SASE) は、従来のサイロ化されたセキュリティサービスを統合し、エッジのユーザーとデバイスの近くでセキュリティを提供するモデルです。使用中のさまざまなソリューションを統合し、クラウドを通じてすべてのユーザー、場所、デバイスに提供する SASE なら、より強力なセキュリティ、効果的なコントロール、シンプルな管理を IT チームに提供できます。

SASE アーキテクチャには、以下のようなさまざまなセキュリティサービスが含まれています。

セキュア Web
ゲートウェイ

クラウド提供型
ファイアウォール

クラウド アクセス
セキュリティ ブローカ

DNS レイヤ
セキュリティ

SASE がお客様のセキュリティの課題を解決

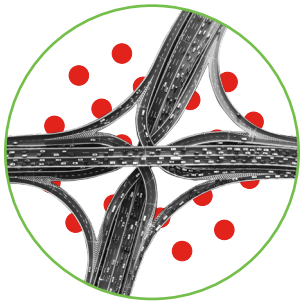
クラウドへの移行方法が組織によって異なるように、クラウドの保護方法も組織によって異なります。しかし、現在お客様が移行のどの段階にいるかにかかわらず、SASE アーキテクチャならお客様独自のニーズに対応できます。

予算上の制約

適切なプラットフォーム、つまりオープンで緊密に統合された単一のオファーとして販売されているプラットフォームは、SASE 標準に移行するために必要な構成要素を提供します。不必要なサービスに費用をかけずに最大限の保護を実現できます。また、IT とネットワークの進化のニーズに合わせて容易に拡張することもできます。

スタッフおよび人材不足

単一の統合セキュリティサービスを使用することで、脅威とアラートの監視 / 管理の複雑さが軽減されるため、チームは少ないリソースでより多くの作業を実行できるようになります。また、全体的な攻撃と感染が減少するため、修復に要する時間とダウンタイムが少なくなり、それぞれにかかるコストも削減できます。

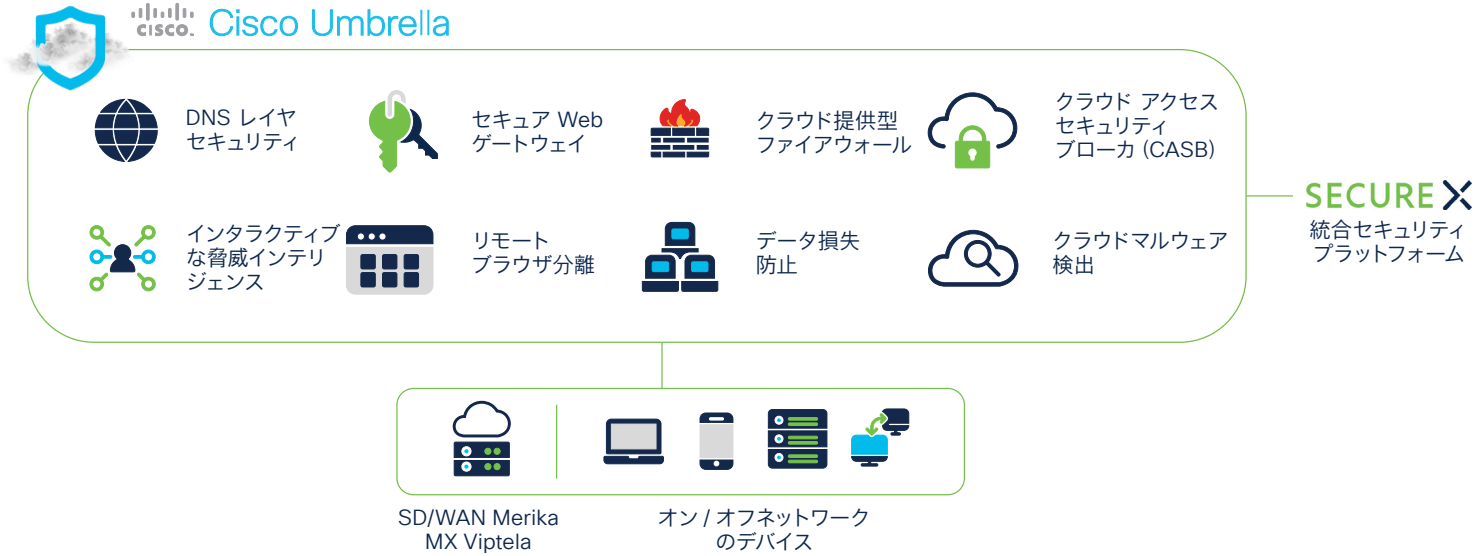


統合と互換性の問題

増加の一途をたどるニーズに対応するために、多くの組織は保護レイヤを増やすべく、断片的なセキュリティソリューションを数多く利用しています。しかし、そうしたソリューションの多くは連動しないため、管理が非常に難しくなります。ソリューションを 1 つに緊密に統合することで、チームは一貫性のあるよりシンプルな方法で管理することができます。

Cisco Umbrella のご紹介

シスコは SASE への移行を推奨しています。そのアプローチの基盤となる Cisco Umbrella は、複数のセキュリティ機能を単一のクラウド提供型ソリューションに統合し、すべてのデバイス、リモートユーザー、分散したロケーションに保護を拡大します。すばやく導入して簡単に使用でき、拡張性にも優れた Cisco Umbrella は、現在も将来もお客様独自のニーズと課題に対応できるクラウドセキュリティです。



脅威に先手を打つ。

- ワールドクラスのインテリジェンスを活用して現在の脅威と最新の脅威を発見できます。
- ネットワークやエンドポイントに到達する前にマルウェアを特定して阻止できるため、より早い段階で脅威をブロックできます。

保護を強化。

- 保護を拡張し、死角を排除します。
- エンドユーザーの生産性を低下させることなく、セキュリティを改善できます。
- コンプライアンスを確保します。

シンプルな管理。

- 感染の修復にかかる時間を短縮できます。
- Cisco Secure ポートフォリオとお客様のインフラストラクチャを連携させる、クラウドネイティブの組み込みプラットフォームである Cisco SecureX を使用して、一元的な可視性と修復手順の自動化を実現できます。

Cisco Umbrella

シスコ：SASE に向けた次のステップ

仕事の種類によって必要な保護の種類は異なります。シスコは、SASE のアプローチこそ未来のクラウドセキュリティであると確信しており、お客様の SASE 導入を支援する体制を整えています。

Cisco Umbrella とシスコのその他のセキュリティソリューションは、シスコの実績と安定した強力な機能に支えられています。30 年以上にわたって世界のネットワークを構築、保護して経験を培ってきたシスコは、Fortune 100 社のすべての企業の保護に貢献しています。

SASE はかつてないほど身近になっています。合理化され、シンプルでスケーラブルなクラウドベースのセキュリティが社内でどのように機能するのか確認したいお客様は、今すぐ Cisco Umbrella の無料トライアルを開始してください。

無料トライアルを開始

出典：

1. Hosting Tribunal、『Cloud Adoption Statistics for 2021』、2021 年 8 月
2. Dark Reading、『56% of Large Companies Handle 1,000+ Security Alerts Each Day』、2020 年 7 月
3. Cybersecurity Insiders、『2021 Cloud Security Report』、2021 年

Cisco Umbrella：

6,200 億
1 日あたりのインターネットリクエスト処理数

50 億
1 日あたりの Web レピュテーションリクエスト処理数

1 億 7,000 万以上
1 日あたりの悪意のある DNS クエリブロック数

20 億
1 日あたりのマルウェアサンプル処理数

1,000 以上
活用するピアリングパートナーシップとシスコ マネージドデータセンターのグローバルネットワーク

200 以上
年間の新たな脆弱性発見数