POINT OF VIEW

SASE ソリューションの評価における重要な指針

概要

現代のハイブリッド環境で、企業の資産やアプリケーションへの安全で信頼できる一貫したアクセスを提供することは、IT チームが直面している最大の課題です。今日の市場では、従業員が社内、自宅、あるいはその中間地点のどこにいようと、重要なアプリケーションやリソースに安全で認証に基づいたアクセスができるとともに、一貫性のあるエンタープライズクラスの保護が確立されていることが非常に重要です。

現在のハイブリッドネットワークの安全性は、最も脆弱なリンクに左右されます。従業員の自宅勤務への移行が急速に進んだ結果、マルウェア、なかでもランサムウェアによる組織への攻撃が急増しました。サイバー犯罪者は、企業ネットワークからセキュリティが不十分なホームオフィスへと、攻撃の標的を素早く切り替えました。そして、暗号化された VPN トンネルを乗っ取ることで、ネットワークに侵入することができました。

組織はより高度なソリューションを必要としています。SASE（セキュアアクセスサービスエッジ）は、ネットワーキングとセキュリティをコンバージする、つまり、クラウドベースのセキュリティと SD-WAN を統合するアーキテクチャです。これを使用して、リモートワーカーは重要なリソースにいつでも安全にアクセスできます。効果的な SASE ソリューションは、エンタープライズクラスのセキュリティ要素、たとえば SWG（セキュア Web ゲートウェイ）、ZTNA（ゼロトラストネットワークアクセス）、次世代型デュアルモード CASB（クラウドアクセスセキュリティブローカー）などを組み込み、Web、クラウド、およびプライベートアプリケーションへの一貫した安全なアクセスを保証します。SASE に統合された SD-WAN は、ビジネスクリティカルなアプリケーションへのアクセスを一元管理します。SASE を適切に実装すれば、従来の社内勤務で利用している保護機能やパフォーマンスを、リモートワーカーにまで拡張することができます。

ハイブリッド WFA（Work-From-Anywhere：場所に縛られない働き方）モデルが常時利用されるようになり、より信頼性の高いソリューションを必要としている IT チームの装備において、SASE は早くも欠かすことのできないツールとなっています。ただし、SASE ソリューションはどれも同じではありません。アプリケーションのパフォーマンス、アクセス、セキュリティなどはソリューションによって大きく異なります。また、動的で進化し続けるハイブリッドネットワークを使用している組織では、管理すべきテクノロジーがさらに追加されることで、人員が不足している IT 担当者の負担が増える可能性があります。

投資の前に検討すべき点

パンデミックの収束が近づいた頃、SASE の導入が急速に進みましたが、その理由の多くは切迫感でした。組織は、大量のリソースを必要とする一時的な WFA ソリューションを、もっと信頼性の高いものに変えたいと考えていました。しかしながら、新しい市場トレンドの勢いに流され、十分な情報がないまま購入に走ると失敗することになります。

多くの新規市場と同様に、SASE 市場でもシェアを獲得しようとするベンダーが出現しています。しかし、そうしたソリューションの多くは期待どおりの効果を上げておらず、セキュリティテクノロジーも未成熟または不適切なものです。その多くは独立したスタンドアロンソリューションとして動作し、組織内の他のテクノロジーと連携していません。特に、ハイブリッドネットワークとの統合が不十分です。また、対応が可能なユースケースの数も限られています。その結果、大抵はベンダーとソリューションの数を減らすどころか無秩序な拡大を助長し、すでに過度の負担を強いられている IT チームの管理業務を増やしています。

組織はやみくもに SASE の時流に乗ろうとするのではなく、資金を投じる前に以下の点を慎重に検討することが求められます。

SASE ソリューションはどれも同じではありません。アプリケーションのパフォーマンス、アクセス、セキュリティなどはソリューションによって大きく異なります。また、ハイブリッドネットワーク戦略を実践する組織では、管理すべきテクノロジーがさらに追加されることで、人員が不足している IT 担当者の負担が増える可能性があります。

大半の SASE ベンダーで使用されている手作業による制御やスクリプト、そして不十分な脅威インテリジェンスは、変化の激しい今日の脅威についていくことができないため、組織は脆弱な状態に置かれることになります。

単一ベンダーの SASE アプローチ

大多数の組織は、従来型のインフラストラクチャとクラウドベースのシステムを組み合わせた、ハイブリッドネットワークの運用を今後も続けていくでしょう。問題は、こうした環境でベンダーが乱立することで、可視性や制御が低下することです。サイロの中で動作するセキュリティ / ネットワークコンポーネントは自動化できません。SASE ソリューションがネットワークの他の部分と連携していなければ、IT チームがエンドツーエンドのトラフィックを追跡し保護することは不可能です。マルチベンダーの SASE ソリューションを構成し、それに付随する実装や管理の課題を抱えるよりも、単一ベンダーの SASE ソリューションを採用してネットワーキングとセキュリティをコンバージし、すぐに利用できる統合型ソリューションを構築すべきです。SASE ソリューションは、クラウドとオンプレミスのデバイス間でシームレスに接続を切り替える必要があります。これにより、ネットワークのエッジで終了するのではなく、アクセスおよびセキュリティポリシーによるユーザーの追跡が可能になります。ネットワーキングとセキュリティをエンドツーエンドでコンバージすることによってのみ、組織は包括的なゼロトラストアーキテクチャを実装することができます。セキュリティ ドリブン ネットワーキングのユニークなアプローチをクラウドエッジまで拡張すれば、あらゆる場所で一貫したセキュリティと優れたユーザーエクスペリエンスを維持できます。

企業アプリケーションへの柔軟なセキュアプライベートアクセス

現代の組織は急速に進化しています。これらの組織には、自社固有のビジネス環境に対応し適応できる、柔軟な SASE ソリューションが必要です。今日のように動的な組織の要求に応えるには、適応力のある SASE ソリューション、つまり、プライベートデータセンターであろうとパブリッククラウドであろうと、企業アプリケーションへの安全な接続を確保できるソリューションが必要不可欠です。SASE ソリューションは、きめ細かい制御ができる ZTNA を使用して企業アプリケーションへの安全なアクセスを維持するほか、SD-WAN および NGFW ソリューションともシームレスに連携し、企業アプリケーションにアクセスするユーザーに最適なエクスペリエンスを提供します。さらには、クラウドベースの PoP によるインテリジェントなステアリングと動的ルーティング機能を利用して、重要なリソースへの最短パスを自動的に検出し維持します。これにより、現代のハイブリッドワーカーに対応できる、一貫したユーザーエクスペリエンスを実現します。

複数のユースケースに対応する統合型エージェント

ユースケースごとに異なるエージェントをオンボーディングしていると、保守業務は瞬く間に複雑かつ高額になってしまいます。SASE ソリューションは、ZTNA、CASB、エンドポイント保護など、複数のユースケースに使用できる単一のエージェントを提供するとともに、トラフィックを自動的にリダイレクトし、クラウドベースのセキュリティによってアセットとアプリケーションを保護します。

ユーザーアクセス制御

ZTNA は、現在のように分散したリソースとハイブリッドワーカーを保護するために不可欠なツールとして登場しました。汎用の ZTNA ソリューションは、あらゆる場所のユーザーを認証し、個々のアプリケーションへの明示的なアクセスを許可し、一貫した監視を行います。また、不測の事態が起こった場合には対応策を実施します。

一貫したポリシーの適用と優れたユーザーエクスペリエンス

SASE テクノロジーは単発のソリューションとして動作するのではなく、組織の大規模ネットワークやセキュリティアーキテクチャと容易に統合できる必要があります。SASE ソリューションのセキュリティプロトコルとポリシーが、ネットワークの他の場所で使用されているものと同じであれば理想的です。さらに、システム管理者は SASE ソリューションと既存のテクノロジーを統合し、シームレスな連携を通じてセキュリティとネットワークの運用を最適化できなければなりません。一貫したネットワーク運用によって、ネットワークの内外を問わず、従業員の優れたユーザーエクスペリエンスが実現されます。

AI を活用した脅威インテリジェンス

ユーザーとアプリケーションの安全性を維持するには、最新の脅威に合わせて SASE ソリューションのセキュリティコンポーネントを継続的に調整する必要があります。しかし、大半の SASE ベンダーで使用されている手作業による制御やスクリプト、そして不十分な脅威インテリジェンスは、変化の激しい今日の脅威についていくことができないため、組織は脆弱な状態に置かれることになります。SASE ソリューションは、エンタープライズクラスのセキュリティコンポーネントに加えて、AI を搭載した脅威インテリジェンス機能も活用する必要があります。この機能は、教師あり / 教師なし学習モデルを使用して構築され、今日の巧妙で捕捉しにくいセロデイ攻撃を防止するために、膨大な数のサイバーイベントで訓練されています。

SASE ソリューションが対応すべき基本ユースケース

SASE の導入は、一見すると簡単に思えます。SASE ソリューションを購入してユーザーに配布したら、あとは忘れてしまって構いません。多くの SASE 営業担当者はそのように説明するでしょう。しかし、IT の知識がある方はご承知のように、何事も思ったほど簡単にはいきません。たとえ最も単純なソリューションであっても、細かいところを間違えると失敗することがよくあります。

SASE ソリューションが対応すべき主なユースケースを理解することが、適切な評価につながります。考慮すべき 5 つの基本的なユースケースを以下に紹介します。

1. **セキュアインターネットアクセス：**リモートワークやハイブリッドワークが一般化するにつれて、組織が対処しなければならない攻撃対象領域は、インターネットに直接アクセスすることによって拡大しています。サイバー犯罪者は、このように拡大する攻撃対象領域を今後も標的とするでしょう。したがって組織には、ユーザー（またはユーザーが使用するアプリケーション）の所在地に関係なく、ユーザーを追跡して適切な機能を提供し、保護することができるソリューションが必要です。

   SASE セキュリティは、暗号化トンネルを上回る機能を提供し、今日の高度な脅威に対処する必要があります。また、トラフィックを検査し、既知および未知の脅威を検知して対応するよう設計された、エンタープライズクラスのセキュリティソリューションのポートフォリオも備えていなければなりません。必要な機能には、データやアプリケーションを監視して Web ベースの攻撃から保護する SWG ソリューションのほか、ZTNA、URL フィルタリング、DNS セキュリティ、フィッシング対策、アンチウイルス、アンチマルウェア、サンドボックスなども含まれます。

2. **セキュアプライベートアクセス：**現在のように動的な組織の要求に応えるには、柔軟な SASE ソリューション、つまり、配置場所がプライベートデータセンターであろうとパブリッククラウドであろうと、企業アプリケーションへの高速で安全な接続を確保できるソリューションが必要不可欠です。ZTNA が組み込まれた SASE ソリューションでは、認証されたユーザーに対して、アプリケーションごとに明示的なアクセスが許可され、永続的なトンネルは不要です。ID とコンテキストに基づいてアクセスを許可するとともに、継続的な検証を行うことで、ネットワーク上で誰が何を使用するかを効果的に制御できます。さらに SASE ソリューションは、SD-WAN および NGFW ソリューションとシームレスに統合することができます。これにより、SASE PoP でのインテリジェントなステアリングと動的ルーティング機能を利用してリソースへの最短パスを自動的に検出し、企業アプリケーションに適した高度なユーザーエクスペリエンスを実現します。使用するエージェントを 1 つに限定し、トラフィックリダイレクト、ZTNA、CASB、エンドポイント保護を 1 つのツールにまとめるのが理想的です。

3. **セキュア SaaS アクセス：**SASE ソリューションは、アプリケーション、デバイス、ユーザー、ワークロードの配置場所に関係なく、重要なリソースへの安全なアクセスを提供する必要があります。SaaS アプリケーションに対する企業の依存度が高まっていることから、クラウドベースの効果的なセキュリティソリューションによってミッションクリティカルなデータを保護し、クラウドベースの情報を安全に保管しなければなりません。効果的なソリューションは、インラインと API ベースの両方の機能をサポートして、次世代型デュアルモード CASB に対応することで、シャドー IT の課題を解決するとともに、クリティカルデータを保護します。
4. **クラウドベースの管理：**クラウドベースの SASE 管理システムには、包括的な可視性、レポート作成、ロギング、および分析機能が必要です。これにより、Web セキュリティの運用が効率化され、検知とレスポンスに要する平均時間（MTTD と MTTR）を短縮することができます。ただし、監視用の管理コンソールを追加することで、IT チームに余計な負担をかける場合があります。特に、SASE セキュリティ要素が、サイロ化したポイントソリューションとして動作している場合はなおさらです。ハイブリッド環境を管理している組織の場合、SASE の管理とオンプレミスの管理との連携が求められます。SASE クラウドに配置されたコンポーネントとオンプレミスのソリューションが連携できれば、統合機能が一層強化され、一貫したポリシーをオーケストレーションして適用することができます。
5. **簡素化されたオンボーディングと柔軟な利用体系：**SASE の検討事項には、利用方法だけでなく料金の支払い方法も含まれます。シンプルなライセンス体系により、組織は過剰なハードウェアに資本を投下することなく、ビジネスの成長に応じたコストや、セキュリティの利用状況を予測することができます。簡素化されたオンボーディングとエンドポイント管理によって、効率的な運用ときめ細かい分析が可能になり、事前生成されたオンデマンドレポートも利用できます。たとえば、ユーザー、エンドポイント、および VPN のイベントについて詳細なログを作成し、効率的なトラブルシューティングを実行できます。

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ