FORTINET

ハイブリッドワーカーに最適なSASEソリューションの選択

目 次

概要

従業員の勤務場所に関係なく、重要なアプリケーションやリソースに安全かつ認証に基づいてアクセスできる環境は、現代の組織で常に必要とされています。大半の組織は、信頼性と柔軟性に優れたセキュリティソリューションであるセキュアアクセスサービスエッジ（SASE）に移行し、ネットワーク、データ、ハイブリッドワーカーを保護しています。

強力な SASE ソリューションは、セキュアリモートアクセス、セッション / アプリケーションごとの高度な認証、エンタープライズクラスのセキュリティを、単一のクラウドベースソリューションに結合したものです。SASE は、どこからでも活用でき、従来の社内勤務で利用され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も提供します。

ただし、すべての SASE ソリューションが有効というわけではありません。アプリケーションごとのアクセス、セキュリティ機能、セキュリティの有効性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を使用する組織では、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。特に、問題の検知やユーザーエクスペリエンスの最適化のために、エンドツーエンドで環境を管理しようとすればなおさらです。IT のリーダーシップは、自社環境に適した SASE を評価する場合、複数のコアユースケースを調査し、さまざまな重要機能を慎重に検討する必要があります。

現代のハイブリッドな労働環境が与えるサイバーセキュリティへの影響

大多数のビジネスにとって、ハイブリッドワーカーは対処が必要な課題となっています。この課題に加えて、効率性、コスト削減、柔軟性を強化するため、アプリケーションやサービスのクラウド移行が着実に進行しています。

サイバーセキュリティチームにとっては、こうした事業運営の急激な変化によって新たな問題が生じています。最近の調査によると、セキュリティおよびビジネスリーダーの 73% が、リモートワークが原因で組織はより多くのリスクにさらされていると感じています[1]。

このように問題が増加している原因の多くは、現在の課題への対処がまったく考慮されていない旧式または不十分なセキュリティにあります。

たとえば、多くの企業は、新型コロナウイルスのパンデミックが発生してから数週間以内に、従来の VPN（仮想プライベートネットワーク）による接続ではリモートワーカーの増加に対応しきれないことに気づきました。VPN では規模に応じた運用が意図されておらず、結果的にセキュリティの問題が発生しました[2]。

急速に進化する今日のハイブリッドな職場環境を保護するには、SASE ソリューション戦略のように堅牢で目的に応じたセキュリティが求められます。

攻撃対象領域の拡大に伴い、社内外の環境で脅威への露出に優先度を付けて識別・支援する新しいテクノロジーへの需要が高まっています[3]。

シングルベンダーによる SASE アプローチ

あらゆる場所でユーザーに安定した接続とセキュリティを提供するには、ネットワークソリューションとセキュリティソリューションをエッジとクラウド内でコンバージする必要があります。最も基本的なレベルの SASE は、複数の NaaS（Networking-as-a-Service）機能と SaaS（Security-as-a-Service）機能を 1 つのソリューションに結合します。

異なるベンダーのソリューションを統合しようとしても、このような結合は上手くいかない場合があります。しかし、プラットフォーム中心のシングルベンダーの SASE ソリューションなら、テクノロジーを統合し、ネットワーク機能とセキュリティ機能をコンバージして運用効率を向上させることが可能です。ただし、SASE ソリューションは独立した存在ではありません。安全で信頼できる接続を確保し、場所を問わず必要に応じて優れたユーザーエクスペリエンスを提供するには、大規模なネットワーク / セキュリティアーキテクチャへのシームレスな統合が可能な SASE ソリューションを検討することも、組織にとっては重要です。

新たなチャンス到来のときには常にそうですが、緊急のニーズに応えて新市場の一角を占めようとするベンダーが必ず出現します。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、なかには未成熟なテクノロジーや不適切な機能に依存しているものもあります。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、既存のセキュリティテクノロジーや拡大を続けるハイブリッドネットワークと連携していません。組織がシームレスなソリューションを構築し、ソリューションを複雑化するのではなく合理化するのに役立つ製品はほとんどありません。

また、急速に拡大し変化し続けるハイブリッドネットワークを管理する組織では、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。多数の 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 のジャーニーを開始する理由にかかわりなく、セキュリティの効果的な実装とパフォーマンスの向上により、組織は最終的に多くのメリットを享受できます [4]。

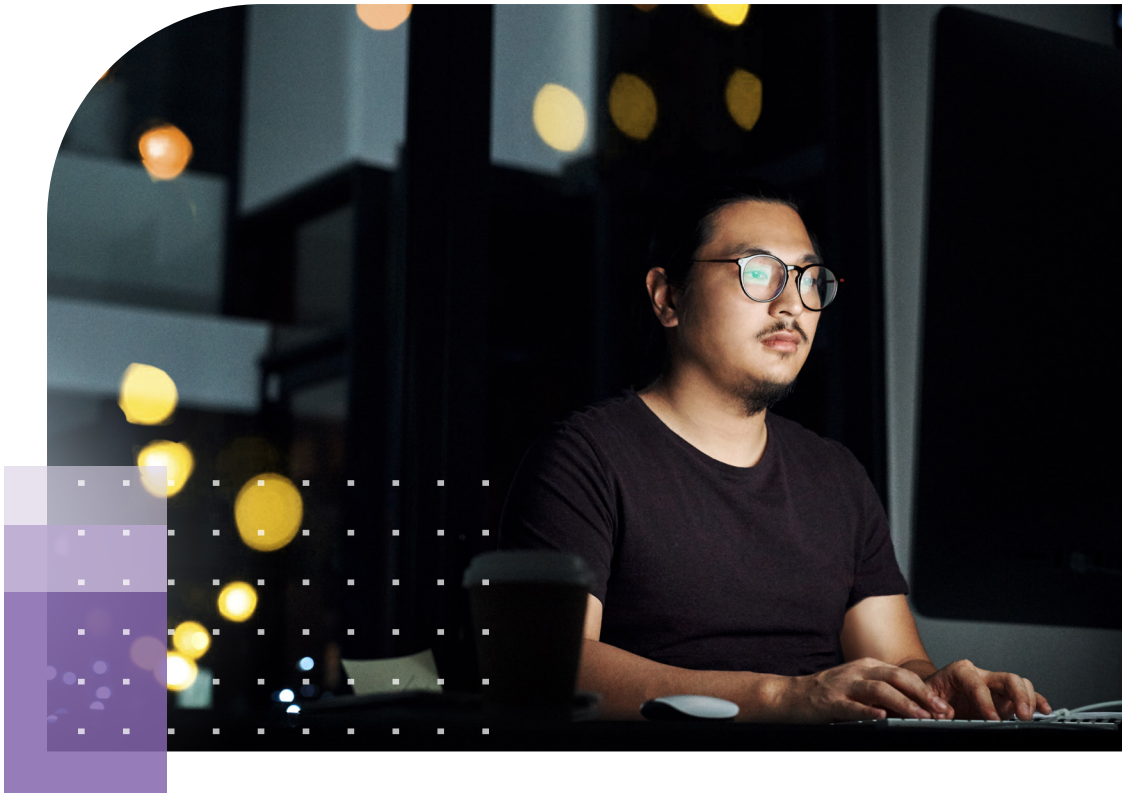
ソリューションの選択

重要な機能を評価し、リモートワーカーの保護に最適な SASE ソリューションを選択する場合、8 つの重要な検討事項があります。

1. シングルベンダーの SASE アプローチ

異なるベンダーのソリューションを統合型 SASE アーキテクチャとして連携させようすると、構築が難しいうえに、保守やトラブルシューティングで多大な時間を要します。シングルベンダーの SASE アプローチでは、ネットワーキングとセキュリティをコンバージし、管理、最適化、およびポリシー適用のすべてを 1 つのインタフェースで制御することができます。

さらに、そのシングルベンダーソリューションが分散ネットワークでの相互運用も可能で、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ことができれば理想的です。これにより、ネットワークのいずれか一方のエッジで接続や制御を終了する代わりに、アクセスおよびセキュリティポリシーによってユーザーとアプリケーションをエンドツーエンドで追跡することが可能になります。



ビジネス環境全体でネットワークとセキュリティを正しく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し、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場所を問わずに提供することができます。

2. 複数のユースケースに対応する統一したエージェント

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。効果的な SASE ソリューションは、ZTNA、CASB（クラウドアクセスセキュリティブローカー）、エンドポイント保護など複数のユースケースを単一のエージェントでサポートします。さらには、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。

3. セキュアインターネットアクセス

リモートワークが新たな日常となる中、インターネットに直接アクセスするユーザーによって、組織の攻撃対象領域は大幅に拡大しています。有効なソリューションは、ユーザー（またはアプリケーション）をその所在にかかわらず追跡し、適切な機能を提供して保護できなければなりません。

クラウドベースのセキュリティソリューションには、暗号化トンネル（従来の VPN など）を上回る機能が求められます。また、トラフィックを検査し、既知および未知の攻撃を検知して対応するように設計された、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を提供する必要があります。つまり、優秀な SASE ソリューションは、SWG（セキュア Web ゲートウェイ）機能が組み込まれており、データと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ほか、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、ディープ SSL インスペクションなどの機能も備えています。

4. 柔軟でセキュアなプライベートアクセス

柔軟な SASE ソリューションは、企業アプリケーションの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、それらのアプリケーションへの安全なアクセスを提供します。

統合型 ZTNA 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。ZTNA は ID とコンテキストに基づいてアクセスを許可し、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します。

望ましい SASE ソリューションは、SD-WAN および次世代ファイアウォール（NGFW）ソリューションとシームレスに統合され、SASE PoP を通じてインテリジェントなステアリングや動的ルーティング機能を提供します。また、企業アプリケーションへの最短パスを自動的に検出して保護することで、優れたユーザーエクスペリエンスを実現します。理想的には、これらすべての機能が単一のエージェントによって提供され、ZTNA、トラフィックリダイレクト、CASB、エンドポイント保護などに対応している必要があります。

5. セキュア SaaS アクセス

効果的な 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、安全なアクセスを提供する必要があります。これは、キャンパス、拠点、自宅、モバイル環境の間を定期的に移動するハイブリッドワーカーにとって不可欠な機能です。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も保護し、ユーザーがオンプレミスかオフプレミスかに関係なく、エンタープライズクラスのセキュリティで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。さらには、インラインと API ベースの両方の機能をサポートして、デュアルモードの CASB にも対応する必要があります。これにより、クリティカルデータを保護すると同時に、シャドー IT の課題を特定して解決します。

要約すると、以下の機能を提供する SASE ソリューションが組織には必要となります。

- 主要 SaaS アプリケーションの可視化
- リスクの高いアプリケーションに関するレポート
- 機密データを保護するアプリケーションのきめ細かな制御
- 管理 / 非管理デバイス両方のアプリケーションでのマルウェアの検出と修復

6. オンボーディングの簡素化による柔軟な消費モデル

SASE ソリューションを選択する際の検討事項として、テクノロジーだけではなく支出負担の方法も考慮する必要があります。適切な SASE を活用すれば、投資支出ベースではなく運用支出ベースでの組織の事業の消費モデルに役立てることが可能です。この変化を効果的に実現するには、組織が余分なハードウェアを固定するのではなく、コスト対事業の成長に合わせたセキュリティの使用を予測できるようにする、簡素化した階層別ライセンスを提供する必要があります。

継続的なコスト管理は、オンボーディングの簡素化と統合されたエンドポイント管理システムの統合に関連付けることもできます。また、集中管理では、効率的な運用と詳細な分析を組み合わせ、ユーザー、エンドポイント、VPN イベント全体のログ記録やイベントなど、事前生成レポートやオンデマンドのレポートを含めて効率的なトラブルシューティングを行う必要があります。

7. クラウドベースのシンプルな管理と可視化

クラウドベースの SASE 管理システムでは、可視化、レポート、ログ、分析を総合的に提供する必要があります。このようなシステムでは、効率的なセキュリティ運用を確保しながら、検知と修復の平均時間を短縮できます。ただし、SASE の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と、セキュリティチームに不要な負担を強いる場合があります。特に、限られた IT 担当者でハイブリッド環境を管理している組織では、その可能性が高くなります。

クラウドに配置した SASE コンポーネントとオンプレミスのセキュリティソリューションをシームレスに連携すれば、統合機能をさらに強化し、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。

予防的なトラブルシューティングとエンドツーエンドの可視化のためのデジタルエクスペリエンスモニタリング（DEM）も、あらゆる SASE ソリューションの鍵となります。組織で DEM を活用すれば、アプリケーションとデバイスの相互作用により、ユーザーエクスペリエンスを統一して可視化できます。DEM は、エンドポイントデバイス、オンプレミスネットワーク、ユーザー、アプリケーションに対応します。これにより、エンドユーザーのエクスペリエンスを包括的に把握し、測定可能な事業成果に結びつけることが可能です。

8. あらゆる構成に対応する柔軟な導入機能

SASE ソリューションは、組織のアーキテクチャに適応し、WLAN / LAN エクステンダーへの拡張統合を含めて組織でマイクロブランチと関連デバイスをセキュリティ保護する必要があります。その結果、サンドボックス化、侵入防止システム、URL フィルタリングなどのエンタープライズクラスの保護を、セキュリティアプライアンスやサービスを追加することなくマイクロブランチに拡張するという、クラウドベースのセキュリティを提供する新しい手法が組織で可能になります。

信頼できる Work From Anywhere（場所に縛られない働き方）

推定では、米国の労働人口の約 66% がリモート勤務を継続していることを受けて[5]、ハイブリッドワーカーの保護という課題は近いうちに、セキュリティチームが常に向き合わなければならない現実となりそうです。コアユースケースの解決に必要な機能を適切な SASE ソリューションに正しく実装すれば、分散した従業員に安全で信頼できるアクセスを提供するとともに、エンタープライズクラスのクラウドベースセキュリティでリモート接続を強化できます。

厳選したソリューションの採用によって、組織は重要な業務に専念すると同時に、複雑な統合を手作業で管理する必要性を排除し、進化し続けるエンドツーエンドのハイブリッド IT 環境で一貫したセキュリティ態勢を構築することが可能です。

[1] 「Zero Trust Security in the Age of Remote Work」、i4DM、LinkedIn、2023 年 9 月 6 日（英語）：https://www.linkedin.com/pulse/zero-trust-security-age-remote-work-i4dm/

[2] 「Hybrid workforce model needs long-term security roadmap」、Andrew Froehlich 著、West Gate Network、2021 年 6 月 25 日（英語）：
https://www.techtarget.com/searchsecurity/opinion/Hybrid-workforce-model-needs-long-term-security-roadmap

[3] 「Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management」、Ruggero Contu、Elizabeth Kim、Jonathan Nunez 著、Gartner、2023 年 4 月 19 日（英語）：
https://www.gartner.com/en/documents/4283299

[4] 「As SASE Evolves, Organizations Can Choose the Best Model to Meet Their Needs」、Dave Abbott 著、CDW、2023 年 4 月 24 日（英語）：
https://www.cdw.com/content/cdw/en/articles/security/as-sase-evolves-organizations-can-choose-the-best-model-to-meet-their-needs.html

[5] 「25 Trending Remote Work Statistics [2023]: Facts, Trends, and Projections」、Jack Flynn 著、Zippia、2023 年 6 月 13 日（英語）：
https://www.zippia.com/advice/remote-work-statistics/

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

EB-SASE-WFH-era-202401-R1