FORTINET

ユニファイド SASE 検討ガイド

ハイブリッドワークに最適な
シングルベンダー SASE ソリューションを
選択するための考慮事項

課題

ハイブリッドワークの従業員の増加に伴い、企業ではオンサイトとオフサイトのロケーションからネットワークとアプリケーションにアクセスする従業員を保護する必要があります。この WFA（work from anywhere：場所に縛られない働き方）への移行により、攻撃対象領域が大幅に拡大してセキュリティの格差が広がり、ネットワークとアプリケーションの保護がより複雑になりました。

リモートアクセスを保護するための仮想プライベートネットワーク（VPN）は、ハイブリッドワークの従業員によるエンタープライズアプリケーションへのアクセスを効果的に保護するには十分ではなくなっています。多くの場合、組織のネットワークにアクセスするとき、VPN は必要以上のアクセスをユーザーに提供します。この結果、攻撃対象領域が拡大し、盗用したクレデンシャルを持つ攻撃者がクリティカルなリソースに容易にアクセスできてしまいます。VPN は接続を検査しないため、乗っ取り接続や侵害されたエンドポイントデバイスを介して攻撃対象領域を誤って拡大し、ラテラルムーブメントの脅威リスクが高くなります。VPN は通常、中央のロケーションに集約されているため、自宅やその他の遠隔ロケーションから作業するユーザーのレイテンシ問題も発生します。

ユーザーがクラウド内の SaaS や他の分散アプリケーションにアクセスすることが増えているだけでなく、シャドウ IT と呼ばれる、非承認アプリケーションの使用が大幅に増加しています。セキュリティチームは、使用されている SaaS アプリケーションについて把握し、このようなアプリケーションを介した保存またはアクセス対象のデータの種類を制御する必要があります。

さらに、現在のハイブリッドワーク環境の保護は、変更の多くが慎重に計画された戦略ではなく、有機的に発生したため、独自の課題にもなり得ます。多数のネットワークとセキュリティ製品を持つ新たなネットワークエッジが急速に普及し、WFA ユーザーを取り込んだものの、多くの場合は独立した各プロジェクトで導入したため、サイバー犯罪者がこれをチャンスと考えて悪用しかねない脆弱性が生じています。

図 1：SASE の傾向と促進要素

SASE による課題の対処

セキュアアクセスサービスエッジ（SASE）アーキテクチャは、ユーザーへのセキュアなアクセスと高パフォーマンスの接続を大小の規模の拠点やその他のオフサイトのロケーションで提供することで、WFA ユーザーのセキュリティを確保するという課題に対処します。

SASE アーキテクチャは、SD-WAN とクラウド提供のセキュリティサービスエッジ（SSE）機能を融合し、ユーザーはあらゆる場所からインターネット、SaaS、プライベートアプリケーションに安全かつ高速にアクセスできます。

ゼロトラストネットワークアクセス（ZTNA）、FWaaS（Firewall-as-a-Service）、セキュアウェブゲートウェイ（SWG）、クラウドアクセスセキュリティブローカー（CASB）などの SSE 機能はクラウドサービスとして提供され、デバイスまたはエンティティの ID ベースでのゼロトラストアクセスを実現します。リアルタイムのコンテキスト、セキュリティ、コンプライアンスポリシーにより、SSE 機能は一貫したモニタリングと適用を確実に実施するよう支援します。

ユニファイド SASE はシングルベンダーの SASE ソリューションであり、すべての SASE コンポーネントが、統一した管理とエージェントを備えた共通の OS エンジンをベースとして密接に統合されています。ユニファイド SASE は、セキュア SD-WAN、（無線 AP などの）シンエッジ、クライアントエージェント、（Chromebook などの）エージェントレスサポートを使用した拠点からのオンプレミス接続をサポートする統合ポリシーを使用して、柔軟なデプロイメントを可能にします。このような統合セキュリティの構成によって、総所有コスト（TCO）を削減でき、現行のオンプレミスインフラストラクチャを置換してあらゆる場所で一貫したセキュリティを提供するよりも、柔軟なデプロイメントを実現できます。

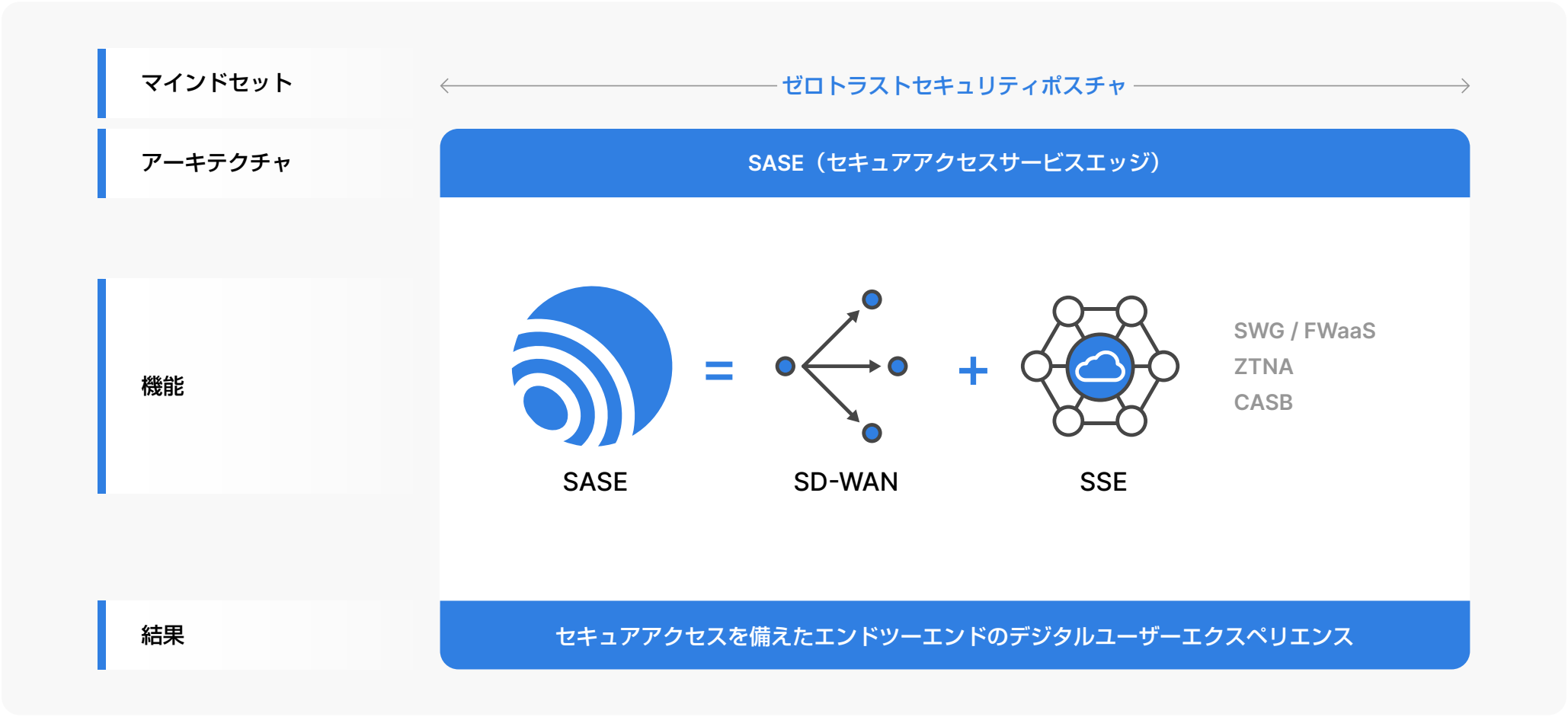

図 2：セキュアアクセスを実現する SASE フレームワーク

SASE ユースケース

ほとんどの組織にとって、SASE にはビジネス要件の進化に合わせて規模を調整し、適応を必要とする長期間の行程が伴います。適切なソリューションを確保するには、SASE ソリューションを評価する前に、組織での主要な促進要素とユースケースを特定する必要があります。

SASE にとって最も一般的なユースケースと推進要因は、以下の通りです。

- レガシー VPN からセキュアな ZTNA リモートアクセスへの入れ替え
- シャドウ IT の可視性と SaaS データ保護による SaaS アクセスの保護（CASB）
- ハイブリッドワークのための一貫したセキュアなインターネットアクセス（SWG と FWaaS）
- WAN エッジを実現するネットワークの最新化（SD-WAN）
- マルチネットワーク製品とセキュリティ製品を統合して複雑性とオーバーヘッドを軽減
- クラウド配信セキュリティ

クリティカルなビジネス上の推進要因とユースケースを特定すると、現在と将来のニーズに適した SASE ソリューションの選択に役立ちます。ユースケースを特定した後、機能上の要件を満たす全体的な要件を定義しながら、既存のネットワークとセキュリティインフラストラクチャのシームレスな統合を可能にする必要があります。SASE は、独立したソリューションではなく、統合ソリューションとしてデプロイする必要があります。自社のネットワークとセキュリティのインフラストラクチャを相互運用するように設計した SASE ソリューションを選択すると、デプロイメントや運用上のオーバーヘッドを簡素化し、予算の制約や実装のタイムラインに合わせることができます。

エンタープライズ SASE ソリューションを選択する際の主な考慮事項

多くの SASE ソリューションは、問題の一部しか解決しません。エンタープライズレベルの一貫したサイバーセキュリティを自社の WFA ユーザーに提供できない、またはネットワークエッジにデプロイされている物理 / 仮想ネットワークやセキュリティツールとシームレスに統合できないかのどちらかです。

この結果、一貫したサイバーセキュリティと最適なユーザーエクスペリエンスを提供できなくなります。さらに、拡張性、セキュリティ、オーケストレーションに関して、すべての SASE ソリューションが同等の機能を持っているわけではありません。最適な SASE ソリューションでは、実装が必要な技術について、または一貫した体制として機能するために必要な IT 人員についてのオーバーヘッドを増やさないようにする必要があります。

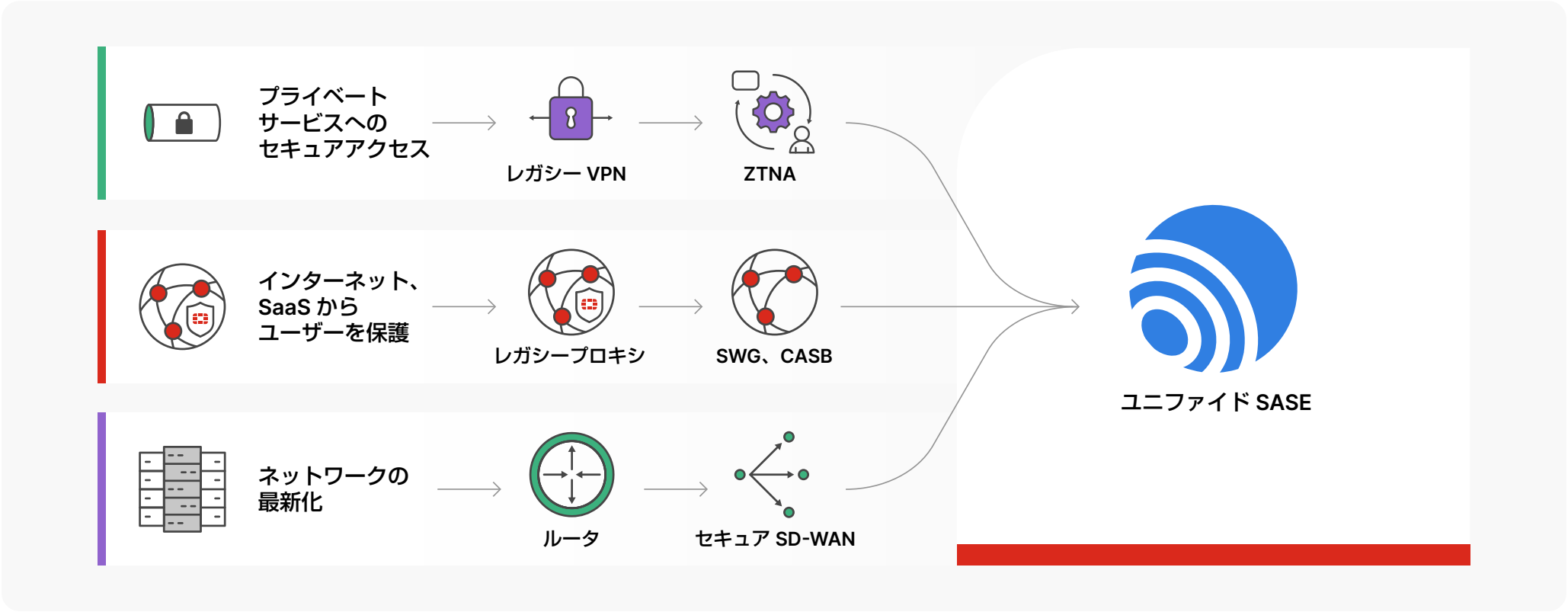

図 3：SASE を導入するエンタープライズの主要な取り組みとユースケース

SASE ユースケースのサポートについて 確認すべき SASE ベンダーへの主要な要件と質問

① 企業アプリケーションへのセキュアリモートアクセスと VPN の入れ替え

ゼロトラストでは、ネットワークまたは物理的なロケーションのみに基づいてユーザーアカウントまたはアセットに暗黙的な信頼を付与することはありません。セキュアなアプリケーションアクセスにゼロトラストセキュリティのモデルを適用すると、無制限のリモートアクセスを提供する従来の VPN トンネルを組織は必要としなくなります。

しかし、効果的な ZTNA ソリューションでは、ユーザー ID をベースにしてセッションごとに各アプリケーションへのアクセスを許可し、ほぼリアルタイムのデバイスポスチャを継続的に検証する必要があります。また、ZTNA ソリューションは、以下のコア要件にも対応する必要があります。

- ユーザー ID、およびほぼリアルタイムで継続的なデバイスポスチャ検証とモニタリングをベースにした、アプリケーションごとの明示的で詳細なアクセス制御
- 非準拠のデバイスとセッションをほぼリアルタイムでブロック
- デプロイメントと管理を簡素化するユニファイドエージェントの一部とした、エンドポイントセキュリティと脆弱性の管理
- アプリケーショントラフィックのセキュリティインスペクションと悪意のあるトラフィックのブロック
- Windows、Mac、Chromebook など、一般的なすべてのエンタープライズデバイスの種類に対応
- すべての企業アプリケーションへのセキュアなアクセスのサポート
- 企業ネットワーク上のユーザーにも、ユニファイド ZTNA ポリシーを適用

ユーザーのロケーションに関係なく、同じゼロトラストモデルを提供すると、組織内のあらゆる場所へのリモートアクセスを超えて ZTNA を拡張することができます。

セキュアなプライベート接続と ZTNA のユースケースについて 確認すべき SASE ベンダーへの質問：

- ベンダーの ZTNA ソリューションでデバイスのポスチャを継続的に確認する頻度を確認します。ZTNA ソリューションでは、10 ～ 15 分ごとではなく、ほぼリアルタイムでデバイスポスチャを確認し、侵害された、または悪意のあるユーザーやデバイスからの暴露リスクの回避が重要です。

- ユーザーが企業アプリケーションにアクセスしようとする際に、デバイスポスチャの確認に失敗したユーザーのセッションを、ベンダーの ZTNA ソリューションがどのように処理するか確認します。その ZTNA ソリューションでは、デバイスポスチャの確認に失敗して準拠から外れた場合、ユーザーのセッションをリアルタイムでブロックするか確認します。
- ベンダーの ZTNA クライアントにエンドポイントの保護と脆弱性管理が含まれているか確認します。このような機能のために複数のエージェントをインストールする必要があるか、それともユニファイドエージェント経由でサポートされているかどうか確認します。
- ベンダーの ZTNA ソリューションでは、認証済みのユーザーセッションにインラインセキュリティインスペクションを提供し、マルウェアの伝播をブロックするかを確認します。
- ベンダーの ZTNA ソリューションでサポートされているアプリケーションプロトコルを確認します。

2 セキュアインターネットアクセス

企業の周辺環境で保護対象外のリモートユーザーや拠点のロケーションでは、インターネットへの直接のアクセスによって攻撃対象領域が拡大し、これに関連したリスクが高くなります。このリスクに対処するため、SASE ソリューションには、IPS および Web フィルタリング機能、SWG 機能、およびディープ SSL インスペクション機能を備えたエンタープライズレベルの FWaaS が含まれている必要があります。また、SSE クラウド配信サービスの一環として、インラインのアンチウイルスやサンドボックス機能などの高度な脅威保護機能を備え、あらゆる場所から一貫したセキュアなインターネットアクセスを提供する必要があります。

IPS と Web フィルタリング機能を備えた FWaaS

FWaaS は、サービスとしてクラウドで提供する NGFW（次世代ファイアウォール）機能に対応する必要があります。ユーザーエクスペリエンスに影響を与えることなく、すべての接続を保護し、インバウンドとアウトバウンドのトラフィックを分析する必要があります。また、FWaaS は、L7 アプリケーションの可視性と制御、Web フィルタリング、SSL インスペクション、DNS セキュリティ、侵入防止システム（IPS）、高度な脅威防御（ATP）にも対応する必要があります。

高パフォーマンスの SSL インスペクションを備えた SWG

SWG は、インターネットユーザーとデバイスを最先端の Web 脅威から保護する必要があります。パフォーマンスを大幅に低下させることなく、SSL で暗号化した Web トラフィックなど、Web トラフィックを保護するための幅広い機能設定を備えている必要があります。

SWG は、エージェントモードまたはエージェントレスモードを使用する管理対象デバイスと非管理対象デバイスに対して、Web フィルタリング、アンチウイルス、ファイルフィルタリングなどのディープセキュリティインスペクション機能をサポートする必要があります。この Web フィルタリング機能では、URL と Web コンテンツに対して事前定義された共通 Web カテゴリに対応し、マルウェア、フィッシングサイト、不適切なコンテンツへのアクセスをブロックする必要があります。

インラインのアンチウイルスとリアルタイムのサンドボックス機能を備えた ATP

アンチウイルスのエンジンは、既知および未知の変異型ウイルスを検知して防止する必要があります。インラインのアンチウイルスには、最新のウイルス、スパイウェア、その他のコンテンツレベルの脅威から保護する自動アップデートを含める必要があります。

サンドボックス機能は、人工知能（AI）と機械学習（ML）テクノロジーを利用した高性能のセキュリティソリューションを提供し、高度な脅威をリアルタイムで特定し、隔離する必要があります。また、ゼロデイの脅威など悪意のある活動についてファイル、Web サイト、URL、ネットワークトラフィックを検査し、サンドボックス技術を使用してセキュアな仮想環境で疑わしいファイルを分析する必要があります。

AI を活用したセキュリティサービス

FWaaS、Web フィルタリング、DNS セキュリティ、アンチウイルス、アンチマルウェア、サンドボックス、IPS のための AI を活用したセキュリティサービスにもソリューションで対応する必要があります。これにより、最新の既知の脅威とゼロデイの脅威から包括的かつ最新の防御を確保できます。業界の代表的なセキュリティ認定をベースとして、IPS などの SWG と FWaaS コンポーネントの有効性を検証することが重要です。

セキュアなインターネットアクセスのユースケースについて確認すべき SASE ベンダーへの質問：

- ベンダーのソリューションは、暗号化された Web トラフィックのディープ SSL インスペクションに対応しているか、SSL インスペクションを有効にすると、パフォーマンスに大きな影響があるか
- ベンダーのソリューションのセキュリティ有効性は、FWaaS、IPS、アンチウイルス、アンチマルウェア、Web フィルタリングなどの機能について認定されているか
- ベンダーのソリューションでは、SWG や FWaaS などコアテクノロジーのコンポーネントが OEM で構成されているか
- 内部脅威研究の専門知識を有しているか、またはサードパーティの OEM に脅威インテリジェンスを依存しているだけか
- ゼロデイの脅威を検知し対応するために、AI を活用したセキュリティインテリジェンスを提供しているか
- 既知および未知の脅威からの高度な脅威保護を提供するために、インラインのアンチウイルスとサンドボックスのサポートを提供しているか

3 セキュア SaaS アクセス

SaaS 導入が急速に拡大するにつれて、企業はシャドウ IT とデータ流出の阻止に苦労しています。セキュア SaaS アクセスをユーザーに提供するには、SSE には次のようなコア機能が必要です。

次世代デュアルモード CASB

インラインと帯域外サポートの両方を使用する次世代のデュアルモード CASB では、主要な SaaS アプリケーションを特定し、危険性の高い未許可のアプリケーションを報告してシャドウ IT 課題を克服することで、包括的な可視性を提供する必要があります。また、次世代 CASB では、アプリケーションのきめ細かな制御を提供する必要があります。これによって、管理対象デバイスと非管理対象デバイスの両方のアプリケーションで機密データを保護し、マルウェアを検出および修復することができます。

データ保護と拡張 DLP サポート

SASE ソリューションは、きめ細かいデータ保護ポリシーエンジンを提供することで、データ関連の違反や侵害から保護するのに役立つ、高度にカスタマイズ可能なデータ保護機能のスイートに対応する必要があります。DLP シグネチャの幅広い設定、カスタマイズ可能なパターンとポリシーエンジン、高度で正確な DLP コンテンツ分析エンジンを提供し、可能な限り最善のデータセキュリティポスチャの実現に役立てる必要があります。また、SOX、GDPR、PCI、HIPAA、NIST、ISO 27001 など、DLP 活動とコンプライアンス標準に関する内容の豊富な定義済みレポートを提供する必要があります。

セキュアな SaaS アクセスのユースケースについて確認すべき SASE ベンダーへの質問：

- ベンダーのソリューションはインラインの CASB と API ベースの CASB の両方をサポートしているか
- ベンダーのソリューションは、すべての SaaS アプリケーションの可視性に対応しているか（認可済み / 未認可の SaaS アプリケーションを把握しシャドウ IT に対応）
- ベンダーのソリューションは、SOX、GDPR、PCI、HIPAA、NIST などのコンプライアンス標準の定義済みレポートをサポートしているか
- ベンダーのソリューションは SaaS アプリケーションの DLP 機能を提供しているか
- ベンダーの DLP ソリューションは、偶発的なデータ侵害を防ぐための高度なデータ照合技術をサポートしているか

4 拠点接続のためのセキュア SD-WAN

多くの SASE ソリューションは、SSE 機能を提供するか、SSE クラウドに拠点トラフィックを転送する軽量な SD-WAN 機能を提供する程度です。この結果、拠点のロケーションから高速で安全なアクセスを提供する際に格差が生じます。最適な SD-WAN ソリューションでは、1 つの集中管理システムで管理するネットワークとセキュリティを融合し、ネットワークやセキュリティのエキスパートがインストールのために現場に行かなくても、サイトを迅速に立ち上げることが可能です。効果的で拡張性のある SASE ソリューションでは、拠点のロケーションでセキュアな

SD-WAN デバイスを提供する必要があります。このようなロケーションでは、コアの WAN エッジネットワークと拠点セキュリティ機能を統合し、拠点のロケーションからインターネット、SaaS、プライベートアプリケーションへの高速かつセキュアなアクセスを提供します。

セキュア SD-WAN は、以下のコア機能に対応する必要があります。

- **トランスポートの独立性：**セキュア SD-WAN は、インターネット、MPLS、4G、LTE、5G など、複数の種類のアップリンクをサポートします。
- **パス制御：**SD-WAN は、帯域幅効率、フェイルオーバーとレジリエンスを可能にするアクティブパスを利用できるようにする必要があります。
- **セキュリティ：**SD-WAN は、アンチウイルス、アンチマルウェア、データ損失防御、IPS、IDS、サンドボックス、URL およびコンテンツフィルタリングを提供する、統合された次世代ファイアウォールなど、拠点ロケーションごとに統合 NGFW を含むセキュリティを確保する必要があります。
- **アプリケーションの最適化：**SD-WAN ソリューションは、動画や音声トラフィックと SaaS アプリケーションなどのアプリケーションを最適化する必要があります。また、数千ものアプリケーションをインテリジェントに識別し、適切なリンク上で動的に制御する必要があります。
- **暗号化：**SD-WAN は、本社と拠点ロケーションの間のブロードバンドを介したエンドツーエンドの暗号化トンネルの作成に対応する必要があります。企業は SD-WAN を使用して WAN トラフィックを暗号化し、効果的な暗号化を確保する必要があります。
- **ゼロタッチのプロビジョニング：**ソリューションは拠点の SD-WAN デバイスのオンボードを最適化する必要があります。
- **自動化とオーケストレーション：**集中型の一元管理ですべての機能をサポートする必要があります。

セキュア SD-WAN サポートについて確認すべき SASE ベンダーへの質問：

- ベンダーの SD-WAN ソリューションがアプリケーショントラフィックの制御でサポートするアプリケーションシグネチャの数
- ベンダーの SD-WAN ソリューションでサポートされているアプリケーションの最適化機能
- 悪意のある通信が企業ネットワークに伝播するのを検査し遮断する、ベンダーの SD-WAN に含まれるセキュリティ機能の種類
- ベンダーの SD-WAN 機能は、MEF などの業界認定を受けているか
- ベンダーの SD-WAN ソリューションは、リンクに障害がある場合に接続を最適化するか、FEC とパケット複製技術を使用して接続の修復が可能か

5 クラウドベースの SSE によるシンエッジの保護

SASE ソリューションは、リモートユーザーのデバイスや拠点の範囲を越えてロケーションやエンドポイントへの柔軟な接続を提供する必要があります。クラウド配信の SSE 機能は、シンエッジを保護するコスト効率の高い選択肢です。このような機能では、完全な次世代ファイアウォールをオンプレミスで展開したり、エンドポイントにクライアントをインストールしたりできない場合がある LAN、ワイヤレス LAN、OT 環境を保護します。

多くの企業では、無線 AP を導入して、（小売店舗など）リモートロケーションでの接続を提供しています。このような AP では、シンエッジ内からインターネット、SaaS、プライベートアプリケーションとの通信を保護するために、大規模な拠点サイトと同水準のセキュリティが必要です。エンドポイントごとに NGFW やクライアントをデプロイすることなく、無線 AP と直接統合することで、クラウド配信型の SSE 機能を提供可能な 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を提供し、複雑性とコストを削減します。さらに、SASE ソリューションは、拠点の SD-WAN デバイスを超えて、ゼロタッチのプロビジョニングを拡張することができ、シンエッジの無線 AP にも同様の機能を提供します。

無線 LAN とシンエッジのサポートについて確認すべき SASE ベンダーへの質問：

- ベンダーの SASE ソリューションは、シンエッジの無線 AP から SSE POP へのセキュアな直接接続を提供しているか
- ベンダーの SASE ソリューションは、シンエッジで無線 AP からインターネット、SaaS、プライベートアプリケーションへの安全なアクセスを実現する SSE 機能を提供しているか
- ベンダーの SASE ソリューションは、シンエッジから接続する無線 AP にクラウドベースのオンボーディングを提供するか

6 地理的な SASE POP のカバレッジとレイテンシ

組織では、ユーザーの作業場所と、アプリケーションのアクセスおよび存在箇所を特定する必要があります。これにより、低レイテンシでユーザーの配置場所に近いポイントオブプレゼンス（POP）を提供する SASE ベンダーを選択できるようになります。

さらに、すべての SASE ベンダーが各 POP で SSE セキュリティ機能をフルスタックで提供しているわけではありません。以下の理解が重要となります。

- 各 SASE POP で可能な機能
- クラウドネットワークを介してトラフィックを最適に制御するために、SASE ベンダーが POP で持つあらゆる仕組み
- ベンダーが主張する POP の総数だけではなく、ベンダーが提供する SSE インスペクションのサービス品質保証

地理的な POP カバレッジとレイテンシについて確認すべき SASE ベンダーへの質問：

- ベンダーの SASE POP のすべてのリストを確認可能か
- 各 POP で SSE 機能のフルスタックを提供しているか
- 各 SSE POP のレイテンシに対して、セキュリティインスペクションのどのようなサービス品質保証があるか
- ベンダーの SASE POP には、SD-WAN ベースのインテリジェントなアプリケーション制御が含まれており、アプリケーションで低レイテンシパスを迅速に選択できるか
- POP のディザスタリカバリのための仕組み
- 複数の顧客の間のデータは POP で分離されているか

7 ユニファイド SASE

市場では多くの SASE アプローチがあり、SASE デプロイメントに必要な機能や統合のレベルが異なります。企業は、ニーズに合った適切な SASE ソリューションを特定するために、このようなレベルの違いを認識する必要があります。

デュアルベンダーの SASE

デュアルベンダーの SASE ソリューションは、通常、2 つの異なるベンダーの SD-WAN 機能と SSE 機能（ZTNA、SWG、FWaaS、CASB、DLP）を備えています。通常では、エンタープライズのネットワークチームは SD-WAN テクノロジーの選択をリードし、エンタープライズのセキュリティチームは通常、SSE 機能の選択をリードします。デュアルベンダーの SASE は、ネットワークとセキュリティをサービスとして提供するさまざまなベンダーを選択する柔軟性を提供しますが、複雑性とコストの増大につながります。導入や運用は簡単ではありません。

シングルベンダー SASE

シングルベンダー SASE ソリューションは、SWG、CASB、ネットワークファイアウォール、ZTNA などの SD-WAN 機能と SSE 機能を提供します。このような機能は、クラウド中心のアーキテクチャを使用し、共通の管理コンソールでシングルベンダーによって提供されます。シングルベンダー SASE ソリューションは、デュアルベンダーの SASE ソリューションで 2 つの異なるベンダーの SD-WAN 機能と SSE 機能を組み合わせようとするよりも管理が簡単で、コスト効率が高く、デプロイが容易です。

ユニファイド SASE

すべてのシングルベンダーの SASE ソリューションが共通のプラットフォームまたはオペレーティングシステム（OS）を使用しているわけではありません。これは、複数の製品を統合したシングルベンダー SASE を提供したり、複数の SASE コンポーネントにサードパーティの OEM テクノロジーを使用したシングルベンダー SASE を提供したりするように選択したベンダーも存在するためです。また、多くの場合、多数のクライアントエージェントをデプロイする必要があり、複雑性とコストが増大します。

SASE のアプローチとデプロイメントについて確認すべき SASE ベンダーへの質問：

- エンタープライズクラスの SD-WAN と SSE のクラウド配信セキュリティを備えたシングルベンダー SASE ソリューションを提供しているか
- 共通のコンソールで SSE 機能を集中管理できるか
- ベンダーの SASE ソリューションは、異なるオペレーティングシステムで統合した複数の製品を使用しているか、または共通の OS プラットフォームを使用しているか
- ベンダーの SASE ソリューションは、既存のオンプレミスでのネットワークセキュリティインフラストラクチャと統合し、オンプレミスと SSE で一貫したポリシーを適用するのに十分な柔軟性を備えているか

図 4：ユニファイド SASE

8 エンドツーエンドのデジタルエクスペリエンスモニタリング

SASE ソリューションは、エンドツーエンドの可視性を提供するデジタルエクスペリエンスモニタリング（DEM）に対応する必要があります。これにより、解決時間を短縮し、最適なユーザーエクスペリエンスを確保して維持するために必要なデータが IT チームに提供されます。

DEM は、ユーザーとグローバル SASE POP でインサイトを提供し、レイテンシ、ジッタ、パケットロス、平均オピニオンスコアなどの一般的な指標に基づいて、共通の SaaS アプリケーションのパフォーマンスに関する包括的な可視性を提供する必要があります。また、DEM は、問題のトラブルシューティングを支援し、解決までの平均時間を短縮するために、ユーザーから共通の SaaS アプリケーションへのアクセスのパフォーマンス測定基準のモニタリングと、各 SASE POP から SaaS アプリケーションへのアクセスのパフォーマンスのエンドツーエンドのモニタリングも提供する必要があります。

DEM に関する SASE ベンダーへの質問：

- ベンダーの SASE ソリューションは DEM を提供しているか
- ベンダーの DEM 機能でサポートしている SaaS アプリケーションとパフォーマンス指標の種類
- ベンダーの DEM 機能は、ユーザーからのパフォーマンスに関するインサイトを提供するか

図 5：SaaS アプリケーションのデジタルエクスペリエンスモニタリングレポート

9 AI を活用したセキュリティと SOC-as-a-Service

企業には、最新のゼロデイ脅威に対抗し、24 × 7 モニタリングのセキュリティ脅威をサポートするために高セキュリティの有効性を提供する SASE ソリューションが必要です。しかし、多くの SASE ソリューションは、シグネチャベースの IPS に基づく既知の脅威の防御と検知にとどまります。継続的なセキュリティモニタリングを維持するためには、社内セキュリティ、SOC 要員、テクノロジーへの追加投資が必要です。

AI を活用したセキュリティは、ゼロデイ脅威に対する防止、検知、自動レスポンスを可能にします。ただし、すべての SASE ベンダーが幅広いデプロイメントに対応しているわけではなく、ゼロデイ脅威を検出する AI や ML の効果的な支援に必要な大量のセキュリティデータの収集機能を備えているわけではありません。企業は、SWG、FWaaS、ZTNA、CASB、DLP などの不可欠な SSE 機能を補強し、広範囲のセキュリティ脅威からの防御を維持するために、AI を活用した機能を補強する十分に広範囲で大量のテレメトリデータを収集可能な SASE ソリューションを探求する必要があります。

さらに、SASE ソリューションは、既存のシステムと統合する必要があります。この統合によって、SOC テクノロジーと人員への投資を最小限に抑え、セキュリティの脅威へのほぼリアルタイムでのモニタリングとレスポンスを実施します。

AI を活用したセキュリティと SOC-as-a-Service について確認すべき SASE ベンダーへの質問：

- AI と ML に使用するデータセットの範囲と量
- エンドポイント、ネットワーク、およびアプリケーションから収集するデータの量と、そのデータを収集する頻度
- SOC-as-a-Service の一部として、ベンダーのサービス品質保証では、セキュリティイベントの発生時に、企業への迅速な通知が可能か
- 機密情報を ChatGPT に入力するユーザーから組織を保護する方法

⑩ 統合クライアントエージェント

多くの SASE ソリューションでは、エンドポイント保護、脆弱性管理、DEM、ZTNA、SSE の接続用にサードパーティクライアントの追加が必要です。これにより、TCO だけでなく、デプロイメントと運用の複雑性が増大します。

ユニファイド SASE ソリューションは、クラウドとエンドポイントでセキュリティ機能を統合し、複雑性とコストを削減します。

統一クライアントサポートについて確認すべき SASE ベンダーへの質問：

- ベンダーの SASE クライアントは脆弱性管理とエンドポイント保護に対応しているか、またはエンドポイントセキュリティのサードパーティベンダーに依存しているか
- ベンダーの SASE クライアントには、DEM サポートが含まれているか、別のサードパーティクライアントに依存しているか
- ベンダーの SASE ライセンスに含まれるクライアント機能

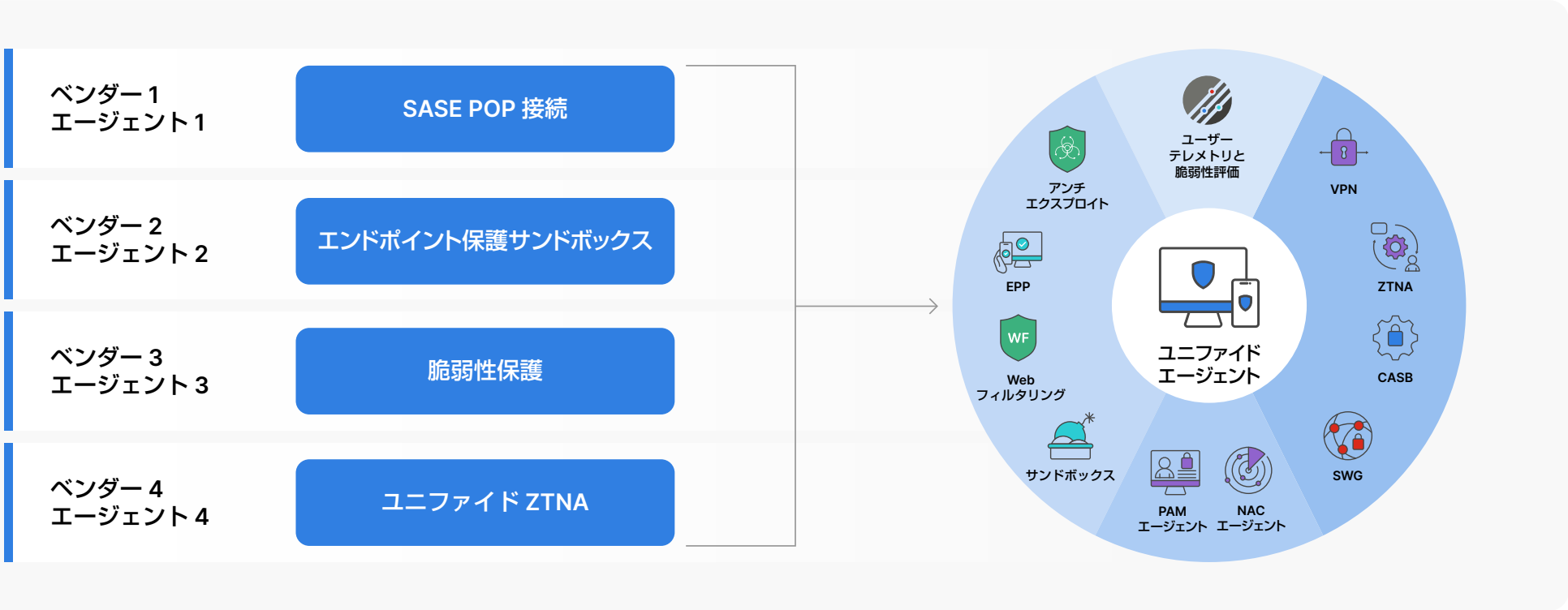

図 6：統合クライアントエージェント

結論

市場には多数の SASE ベンダーが存在します。堅牢な SASE ソリューションでは、完全な機能を提供するために複数の製品が必要です。これらのコンポーネントが 1 つのシステムとして動作するように設計されていなければ、統合と運用が複雑になり、コストが高くなる可能性があります。これでは、SASE で見込まれるネットワークとセキュリティの統合効果がなくなってしまいます。

SASE は長期間の取り組みが必要な行程であり、1 つの段階で完結するソリューションではありません。ビジネスニーズとユースケースを評価して、要件に合った SASE ベンダーを特定する必要があります。ほとんどの場合、これは、現在と将来のニーズに対応するために必要な幅広い機能を提供する、シングルベンダーのユニファイド SASE ソリューションを探求することになります。柔軟性を提供し、企業の SASE 実装の段階に合わせて対応し、長期間の行程全体で企業をサポートする SASE ベンダーなら、後悔せずに提携を進められます。

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

EB-Buyers-Guide-SASE-202405-R1