記事

SASEの評価: 保護、セキュリティ確保、最新化のための5つのユースケース

アプリケーション、ユーザー、データが従来のネットワークの境界を超えて移動し続ける中、多くの組織は環境の接続と保護の方法を評価しています。クラウドの導入、SaaSの利用、ハイブリッドワークによってトラフィックパターンとアクセス要件が変化し、固定拠点、バックホールトラフィック、連携が取れていないツールを中心に構築されたアーキテクチャーの限界が露呈することが多くなっています。

SASEは、そうした評価の重要な要素になりつつあります。SASEは、ネットワーキングとセキュリティを別々の分野として扱うのではなく、現代のアクセスパターンとセキュリティのニーズをサポートするように設計されたクラウド配信型のアプローチで両者を統合します。

SASEは全か無かの極端な選択ではありません。多くの組織はSASEをジャーニーと捉え、優先順位、既存のインフラストラクチャ、リスク態勢に基づいて、時間をかけて段階的に機能を導入しています。以下のユースケースは、このジャーニーでよく見られるポイントを反映しています。これらのユースケースは、組織が差し迫った課題に対処しながら、時間をかけてネットワーキングおよびセキュリティモデルの統合を進めることにより、実用的な観点からSASEを評価する方法を示しています。

1. クラウドファーストの世界に対応するためのブランチ接続の最新化

ブランチネットワークは本来、ほとんどのアプリケーションがデータセンターに存在し、トラフィックが予測可能な経路をたどっていた時代のために設計されたものです。今日では、クラウドアプリケーションとSaaSアプリケーションがトラフィックパターンを支配しており、特に分散したブランチ拠点では、集中型インフラストラクチャを介してデータをバックホールすると、レイテンシ、複雑さ、不必要なコストが生じる可能性があります。

セキュアSD-WANでブランチ接続を最新化することにより、組織はこのようなクラウドファーストの現実に適応できるようになります。ブランチのネットワーキング機能とセキュリティ機能を統合してアプリケーション対応型の一元化されたポリシーを適用することにより、組織は全拠点で一貫した制御を維持しながら、クラウドおよびSaaSトラフィックのパフォーマンスを最適化できます。このアプローチによって従来のブランチアーキテクチャーへの依存が低減され、時間をかけて広範なSASEの機能を統合するためのより柔軟な基盤が提供されます。

これによって可能になること

- ブランチ拠点からクラウドアプリケーションとSaaSアプリケーションへの最適化された直接アクセス
- ルーティング、セキュリティ、接続機能の統合による、よりシンプルなブランチ設計
- アプリケーション対応型トラフィックステアリングによるアプリケーションパフォーマンスの向上
- 分散したブランチ環境を管理する際の運用効率の向上

2. VPNからZTNAまでのハイブリッドワークのアクセスのセキュリティ確保

ハイブリッドワークが一般的になる中、多くの組織がリモートユーザーによるプライベートリソースへのアクセスの方法を評価しています。従来のVPNベースのアクセスモデルは、アプリケーションがデータセンターに存在し、ユーザーが予測可能な場所から作業をしていた環境のために設計されたものです。今日のクラウドファースト環境では、こうしたモデルはパフォーマンスボトルネックを引き起こしたり、ほとんどのユーザーが必要とする以上の広範なネットワークアクセスを付与したりする可能性があります。

ZTNAは、アクセスの決定をネットワークからアイデンティティへと移行させます。ZTNAは、ユーザーをネットワークに配置するのではなく、アプリケーションレベルでアイデンティティおよびポリシーベースのアクセスを適用し、従業員、請負業者、サードパーティユーザーにわたる最小権限の原則をサポートします。このアプローチにより、組織は基盤となるネットワークを公開したり、異なる時代のために設計されたVPNトンネルに依存したりすることなく、プライベートアプリケーションへのセキュアなアクセスを提供できるようになります。

これによって可能になること

- 広範なネットワーク接続ではなく、アプリケーションレベルのアクセス
- ユーザーのアイデンティティとコンテキストに基づく最小権限ポリシー
- リモート、オンプレミス、サードパーティユーザーに対する一貫したアクセス制御
- クラウドファースト環境でのセキュアなアクセスを再考する組織にとっての実践的な開始点

3. ユーザー、Web、SaaS全体にわたる一貫したセキュリティの適用

プライベートアプリケーションへのアクセスのセキュリティ確保は、課題の一部にすぎません。クラウドサービスやSaaSアプリケーションへの依存度が高まる中、プライベートアプリケーションへのアクセスだけにとどまらない、より広範なセキュリティ制御が必要とされています。ユーザーはさまざまな場所やデバイスからインターネットやSaaSプラットフォームとやり取りするため、従来の境界ベースのツールを使用して一貫した可視性とポリシーの適用を維持するのは困難です。

ZTNAにSWG (セキュアWebゲートウェイ) とCASB (クラウドアクセスセキュリティブローカー) の機能を追加するUnified SSE (セキュリティサービスエッジ) のアプローチは、ユーザーアクセス、Webトラフィック、SaaSの使用に一貫してセキュリティポリシーを適用します。これらの制御機能を個別のツールとしてではなく、まとめて管理することにより、組織は、環境の分散化が進む中でポリシーのギャップを縮小してユーザーアクティビティに対する可視性を向上させ、より均一に保護を適用できます。このモデルは、セキュリティチームがWebベースの脅威に対処したり、シャドーITやデータロスなどのSaaSのリスクを管理したり、不必要な運用の複雑化を伴うことなく最小権限の原則を適用したりするのに役立ちます。

これによって可能になること

- ユーザー、Webトラフィック、SaaSアプリケーションにわたる一貫したポリシー適用
- WebアクティビティとSaaSの使用状況に対する可視性の向上
- より安全なインターネットの閲覧とWebベースの脅威からの保護
- クラウドファースト環境向けのスケーラブルなセキュリティ基盤

4. ユニバーサルZTNAによるIoTと管理対象外のデバイスの保護

IoTとエッジデバイスは、依然として現代の環境で最も根強いセキュリティギャップの1つです。多くは管理対象外で、パッチの適用が難しく、エンドポイントエージェントを実行できないため、従来のゼロトラスト制御を一貫して適用するのは困難です。このようなデバイスがエンタープライズネットワークやクラウドサービスに接続されることが増えるのに伴って、ユーザー中心のセキュリティモデルや境界ベースのセキュリティモデルが対処できるように設計されていなかった方法で攻撃対象領域が拡大されています。ユニバーサルZTNAは、ユーザーだけでなくIoTやその他の管理対象外のデバイスにもアイデンティティ主導のアクセス制御を拡張し、プロファイリング、セグメンテーション、グローバルポリシーを使用して各デバイスがアクセスできるものを制限します。

AIを活用したNACは、このようなアプローチを強化するとともに、環境全体のデバイスの可視性、動作分析、継続的な信頼性検証を向上させることにより、管理対象外のデバイスやIoTの保護をサポートします。認証が完了すると、IoTトラフィックをセグメント化し、ミッションクリティカルなアプリケーションのトラフィックから分離できます。また、多くのIoTデバイスは、アップデートやテレメトリなどのアクティビティのためにインターネットトラフィックやクラウドトラフィックを生成するため、SWGの機能とセキュアSD-WANを統合することにより、組織は各デバイスにSSEエージェントをインストールすることなく、これらのデバイスを保護できるようになります。このアプローチでは、すべてのデバイスにWebセキュリティが拡張され、URLフィルタリングなどの機能を通じて有害なWebサイトに対する保護が提供されます。これらの機能を組み合わせることで、組織はIoTセキュリティのギャップを解消すると同時に、ユーザー、デバイス、トラフィックにわたる一貫したゼロトラスト保護を適用することが可能になります。

これによって可能になること

- プロファイリングと行動分析によるIoTと管理対象外のデバイスの可視化
- デバイスのアクセスの到達範囲を制限し、横方向のリスクを軽減するセグメント化されたアクセスポリシー
- エージェントを実行できないデバイスに対する一貫したゼロトラストの適用
- エンドポイントを複雑化させることのない、IoTトラフィックに対するWeb脅威保護

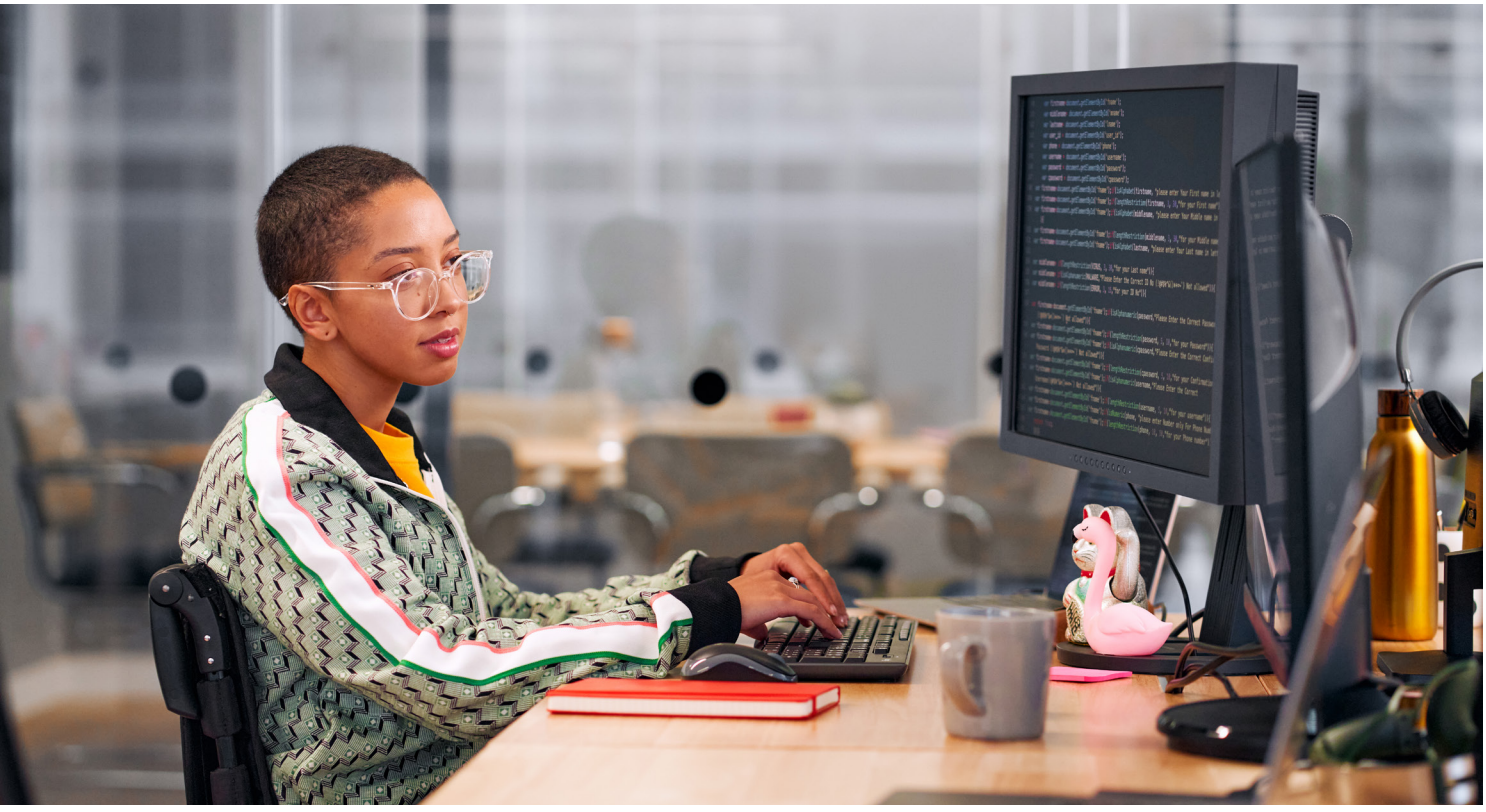
5. Unified SASEによるアクセス、セキュリティ、接続の統合

アクセス、セキュリティ、接続を別のイニシアチブとして管理すると、不必要な複雑さが生じる可能性があります。分断されたツール、ポリシーの重複、手作業による統合作業は、展開を遅延させ、環境拡大に伴って一貫性の維持をより困難にします。このような断片化は、時間とともに運用のオーバーヘッドを増大させ、組織が新たな要件に適応する能力を制限する可能性があります。

Unified SASEアーキテクチャーは、これらの機能を単一のクラウド配信型モデルに統合します。セキュアなアクセス、WebとSaaSの保護、最新のブランチ接続を連携させることにより、組織はユーザー、アプリケーション、拠点全体にわたる変更の導入と管理の方法を簡素化できます。このような統合アプローチは、導入の迅速化をサポートして統合の手間を減らし、環境が進化し続ける中でチームがより自信を持って運用を行えるよう支援します。

これによって可能になること

- 複数のプラットフォームをつなぎ合わせる必要のない、よりシンプルなSASEの機能の導入
- 管理モデルとポリシーモデルの一元化による運用のオーバーヘッドの削減
- 複数のユーザー、アプリケーション、拠点にわたるより迅速な変更の展開
- 不必要な複雑化を伴うことなく拡張できる一貫性のあるアーキテクチャー



Unified SASEへの移行のサポート

SASEを評価する組織は多くの場合、それを一度にすべてを行うイニシアチブとしてではなくジャーニーとして捉えます。最初にアクセス、セキュリティ、ブランチのモダナイゼーションに取り組んでから、Unified SASEアーキテクチャーを通じてそれらの機能を統合することにより、組織は、要件が変化し続ける中で柔軟性、一貫性、長期的なスケーラビリティをサポートする基盤を構築できます。

HPEは、このようなジャーニーのあらゆる段階でお客様をサポートできる位置付けにあります。HPEのAIネイティブのUnified SASEプラットフォームは、SD-WAN、SSE、NACを単一のアイデンティティ主導のアーキテクチャーに統合します。さらに、このプラットフォームはAIOpsを活用して高度な可観測性と認証を実現し、組織がサードパーティの環境でもユーザー、デバイス、アプリケーションをリアルタイムで可視化し、それらの信頼性検証を継続的に行えるようにします。

SASEへの移行に向けた第一歩を踏み出す場合でも、導入済みの機能を統合しようとする場合でも、組織は自信を持って前進できます。

詳細情報

HPE.com/networking

HPE.comにアクセス

今すぐチャット

a00158357JPN

HEWLETT PACKARD ENTERPRISE

hpe.com