aruba
a Hewlett Packard Enterprise company

SASEを活用:

エッジからクラウドまでセキュアなネットワークを実現

在宅勤務の拡大に伴い、クラウドへの移行が加速しています。ネットワークパフォーマンスを向上し、セキュリティギャップを解消するために、どのような計画を立てていますか？ご利用のアーキテクチャーには、必要な変革とは?

新しく在宅勤務を始めた従業員の53%が今後も継続を希望

クラウド、エッジ、IoTによりデータやアプリケーションの配置が見直されている

セキュリティとネットワークを統合し、ビジネス保護を強化するSASEアーキテクチャーを実現

サイロ化されたネットワークやセキュリティインフラストラクチャの維持はもはや不可能

クラウド内で増え続けるアプリケーション

ユーザーとデバイスが従来の企業ネットワークの範囲外に存在する

従来型のセキュリティとネットワークのアプローチが機能しない理由

切り離されたセキュリティやネットワーキクのサイロ、
制限のあるハードウェア中心のアプローチにより、以下の問題が発生します。

- 複雑性が増し、柔軟性と効率性の低下
- 耐障害性とリカバリ機能が阻害される
- ビジネス機会を逃し、競合他社に遅れをとるリスク
- クラウド利用や在宅勤務者サポート対応が困難

なぜゼロトラストエッジが必要なのか

ゼロトラストエッジ ソリューションは、データセンターやクラウド、エッジにわたって強力な認証機能やアイデンティティとロールをベースとしたアクセス制御、ユーザーとデバイスの適切な区分けを実現します。

ゼロトラスト、アイデンティティ、ロールベースのポリシーフレームワークでSASEを補完し、エッジからクラウドにわたるユーザーや、デバイス、アプリケーション、データを保護します。

Forrester 2021

ゼロトラストエッジとSASEのメリットとは？

- セキュリティをネットワークの根幹に組み込む
- 企業のサービスとアプリケーションにセキュアなアクセスを提供し、在宅勤務者を保護
- ブランチWANで優先度の高いビジネスアプリケーションのトラフィックを優先
- ビジネス要件に基づくユーザーとIoTデバイスの保護と区分け
- WANファブリック経由で高リスク環境に接続する顧客、従業員、契約業者、デバイスなどから保護
- ゼロトラストエッジ ソリューションに組み込まれたセキュリティおよびネットワークサービスの一元管理、監視、分析が可能

ゼロトラストエッジの導入を判断するための3つの質問

1. クラウドのアプリケーションのセキュリティは万全か？
2. エッジにあるデバイスとユーザーの保護に苦労していないか？
3. 従業員の53%が在宅勤務を継続できるか?

セキュリティとネットワークサービスにゼロトラストエッジ モデルを導入:

セキュアアクセス サービスエッジ (SASE) はゼロトラストエッジである

Forresterレポートで以下の内容をご確認いただけます。

- サイロ化したネットワークおよびセキュリティ インフラとその運用が急速に消えつつある理由
- どのタイプのゼロトラストエッジ方式がビジネスに適しているのか
- マルチベンダーと単一ベンダーの選択を評価する方法

レポートはこちら

aruba
a Hewlett Packard Enterprise company