

# Private Access

**あらゆる企業のリソースに迅速かつシンプルで安全なゼロトラストネットワークアクセスを実現します。**

チームが必要とするアプリケーションに安全に接続することで、いつでも、どこからでも仕事ができる柔軟性を提供します。Private Accessは、ユーザーがアクセスできないはずのデータやアプリを全般的に見つけられないようにしアクセスされるのを防ぐ一方で、IDとアプリを中心としたポリシーを用いて生産性を向上させます。

## 強固なセキュリティ

Private Accessは、クラウドベースのSoftware-Defined Perimeter (SDP) を使用して設計されており、アプリケーションごとに安全で分離された接続を実現します。最小権限の適用とリアルタイムのDevice Postureのチェックにより、特定の許可されたユーザーにのみ各アプリケーションへのアクセスが許可されます。アプリケーションマイクロトンネルは、横方向移動を防ぐために、各アプリケーションセッションを分離して封じ込めます。

## 強化された管理機能

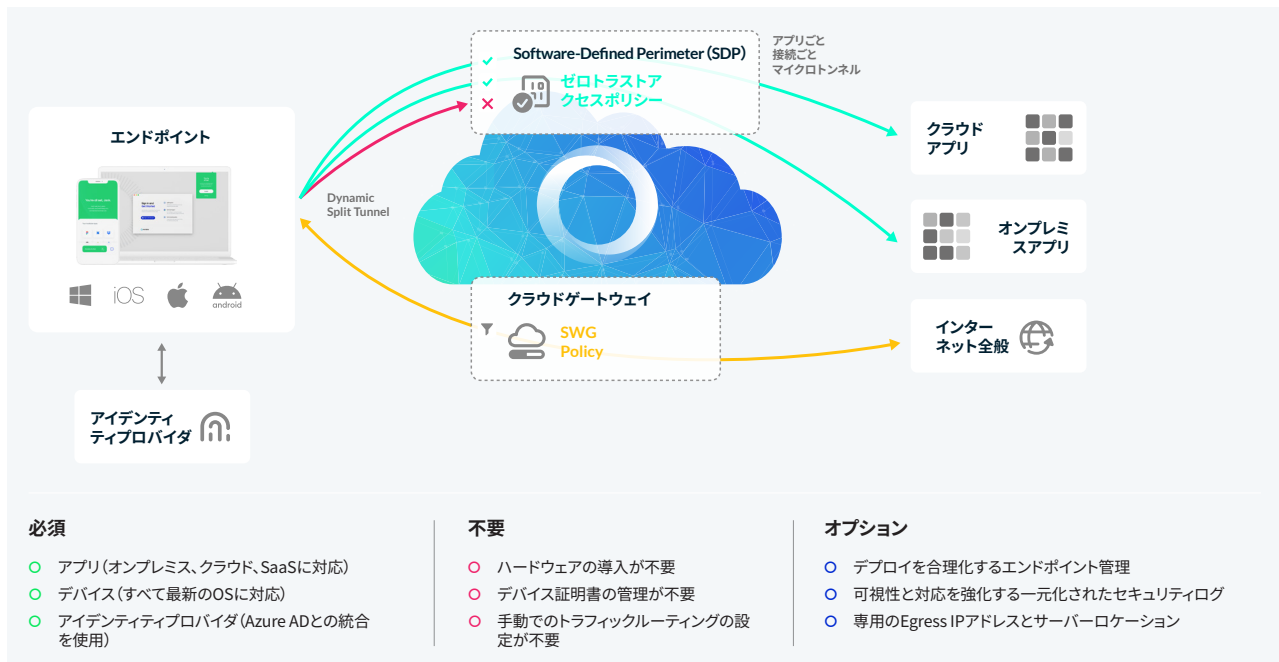
Private Accessは完全なクラウドベースのアーキテクチャを採用しているため、オンプレミスでの機器の管理や複雑なサイズの要件はありません。サービスエッジは、無制限のエンドポイント接続に対応できるようダイナミックにスケールします。Private Accessはより効率的で、アクセス内容の可視性と制御を失うことなく、不必要にコストのかかるすべてのトラフィックの完全なフルトンネル化を使う必要がなくなります。つまり、ルーティングなしのポリシーが適用できます。

## 直感的なユーザー体験

Private Accessは、高速で安全なリモートワークのために設計されたプロトコルを使用します。クラウドの拡張性と、不要なトラフィックのバックホールを回避する機能を組み合わせると、ユーザーは遅延の問題が解消されたシームレスなアクセスを享受することができます。このサービスは効率的であり、ネットワークの移行に適切に対応しているため、ユーザーはセルラーからWi-Fiへ、そしてまたWi-Fiからセルラーへと、中断することなく移行できます。

# アーキテクチャ

クラウドに組み込まれた最先端のアーキテクチャは、オンプレミスだけでなく、クラウドでホストされているあらゆるアプリケーションへのアクセスを提供できるよ  
うスケールします。



## 機能

### クラウドSDP

Private Accessは、クラウドベースのSDPを用いて構築されており、アプリケーションごとに安全で分離された接続を実現します。最小権限の適用とリアルタイムのDevice Postureのチェックにより、特定の許可されたユーザーにのみ各アプリケーションへのアクセスが許可されます。

### アプリのマイクロトンネル

Private Accessはゼロトラストネットワークアクセスソリューションで、デバイスとその上で実行されているアプリはネットワークインフラストラクチャに影響されません。Private Accessは、インフラストラクチャを経由するアプリレベルのマイクロトンネルを使用して、接続の確立時とアクティブなセッション全体の両方できめ細かい制御を可能にします。

### セッションレポート

詳細なセッションレポートにより、アクティブユーザーとそのユーザーが使用しているアプリケーションを監視できます。リアルタイム統計により、異常なアクティビティ、セッション時間や帯域幅の要求を把握できます。包括的な可視性により、管理者は不適切なコンテンツの監視、マルウェアの検出、データ漏洩の特定のための監査証跡を可能にします。

### 次世代プロトコル

エンドポイントの大半はWi-Fiやセルラー接続を利用していますが、ユーザーやアプリケーションは有線接続に求められるパフォーマンスを必要としています。Private Accessは、ユーザーが移動中に作業をしている場合でも、静かでシームレスなサービスを提供することで、高速、汎用、軽量で安全な接続を実現します。

### IDベースのソリューション

Private Accessでは、IDベースのポリシーを使用して、ユーザーとアプリケーションの権限を割り当てます。既存のディレクトリサービスとの統合により、ポリシーの迅速な展開と管理が可能です。トンネルを確立するためには、ユーザーが指定されたアプリケーションに対して適切な権限を持っている必要があります。

### ダイナミックスプリットトンネル

Private Accessは、許可されたユーザーのデバイス上のアプリケーションから、クラウドSDPの反対側にある関連アプリケーションへのトラフィックのみをルーティングするインテリジェントなトンネリングプロトコルを使用しています。これにより、セキュリティで保護されたアプリケーショントンネルを介してトラフィックが不必要に流れることがないため、アプリのマイクロトンネルポリシーが適切に適用されると同時に、エンドユーザーに最適な体験を提供することができます。

### シングルパケット認証

認証されていない第三者によるアプリケーションを見つけれないようにします。シングルパケット認証では、アクセスを仲介する前に、ユーザーとデバイスのIDを確認する必要があります。これは、許可されたユーザーからの接続試行のみが認識され、インターネット上の他のすべてのユーザーにサービスが「ダーク」に見えるようにすることを意味します。

### アダプティブアクセス

Private Accessでは、ユーザーやデバイスのリスクをリアルタイムに評価し、ルートに影響を与えたり、サードパーティとの統合によりシグナルとして使用することができます。デバイスのリスク状態が変化した場合、Private Accessは、ポリシーに基づいてセッションの終了やルートの変更をリアルタイムで行うことができます。