



働き方の変化に伴うリモートアクセスソリューションの変革

課題

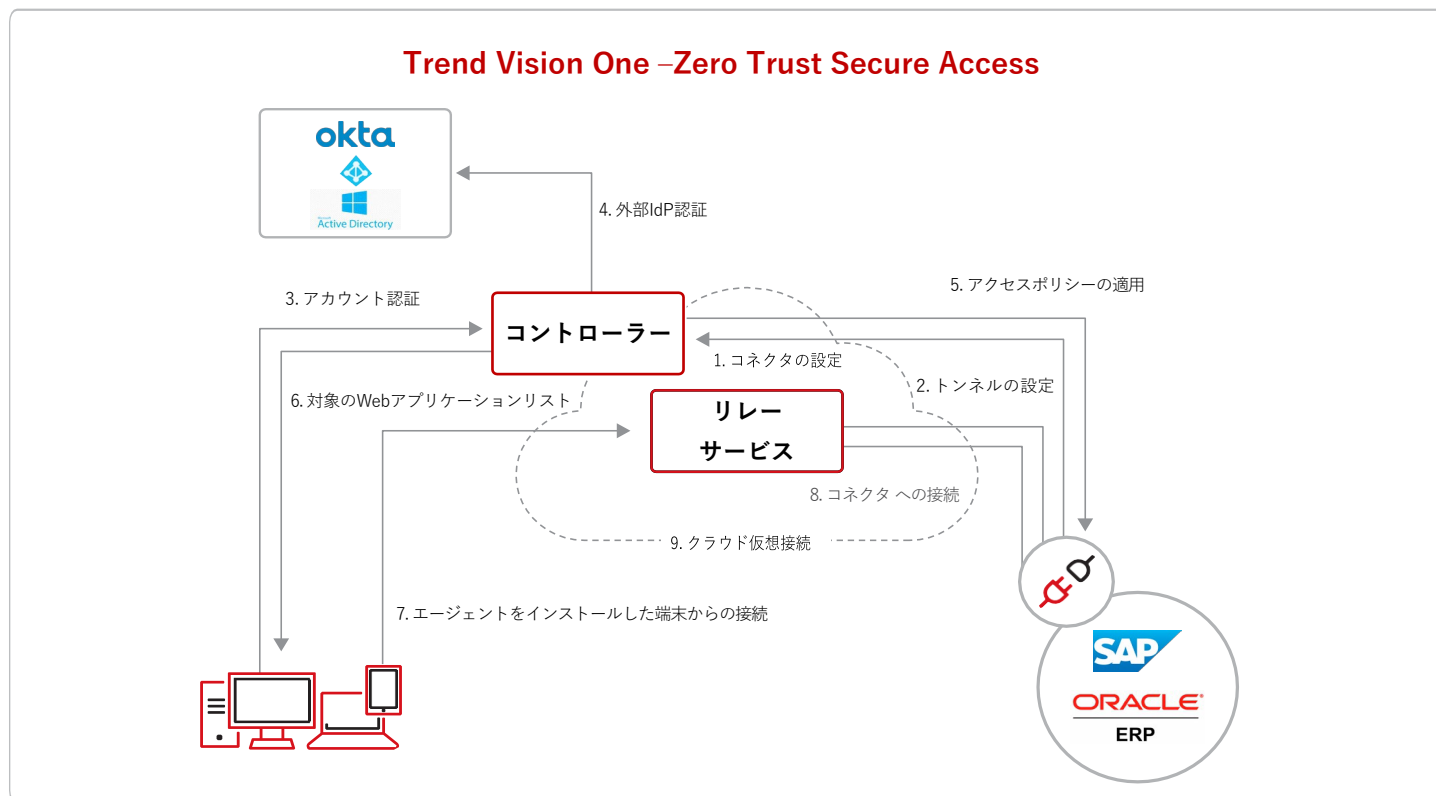
戦略策定への第一歩

組織のサイバーセキュリティは、戦略策定はもちろん、日々の運用も非常に複雑になっています。組織がゼロトラストなどの新しいセキュリティモデルを検討する場合、戦略的かつ戦術的なセキュリティ部門責任者であっても新しいセキュリティモデルへの第一歩は非常にハードルが高いのではないのでしょうか。組織のセキュリティ運用への大規模な変革を一朝一夕には実現することはできません。トレンドマイクロは、目の前の課題解決につながるソリューションの導入から着手することが新しいセキュリティモデルの実現への第一歩であると考えます。この一歩を踏み出すことにより、運用部門は組織全体のセキュリティ目標達成に向けて、段階的に課題を解決し、組織のセキュリティを向上させることができます。

管理者が抱える課題

「リモートワークやハイブリッドワークの従業員に対して、プライベートアプリケーションとリソースへの安全なアクセスを提供するにはどうすればよいか？」

長年、組織はファイアウォールの一部またはスタンドアロンアプライアンスとして、オンプレミスリソースへのリモートアクセスをVPNに依存していました。働き方の変化に伴い、組織の攻撃サーフェスは拡大し、多くのリモートネットワークではオンプレミスと同等のセキュリティを担保することが難しくなりました。



主な特徴

複数テクノロジーの統合

Trend Vision One -Zero Trust Secure Access (ZTSA) は、これまで連携していなかった複数のテクノロジーを一元的に制御し、統合的に可視化することができます。ZTSA -Private Accessは、プライベートアプリケーションへのアクセスに対して、ゼロトラストネットワークアクセス (ZTNA)機能を提供します。VPNの代替となる信頼性の高い拡張機能を提供するだけでなく、リスクベースでの動的なアクセス制御、豊富なテレメトリデータ、レポートによる可視化、シンプルで一貫したポリシー設定が可能です。

社内ネットワークという境界を超えて

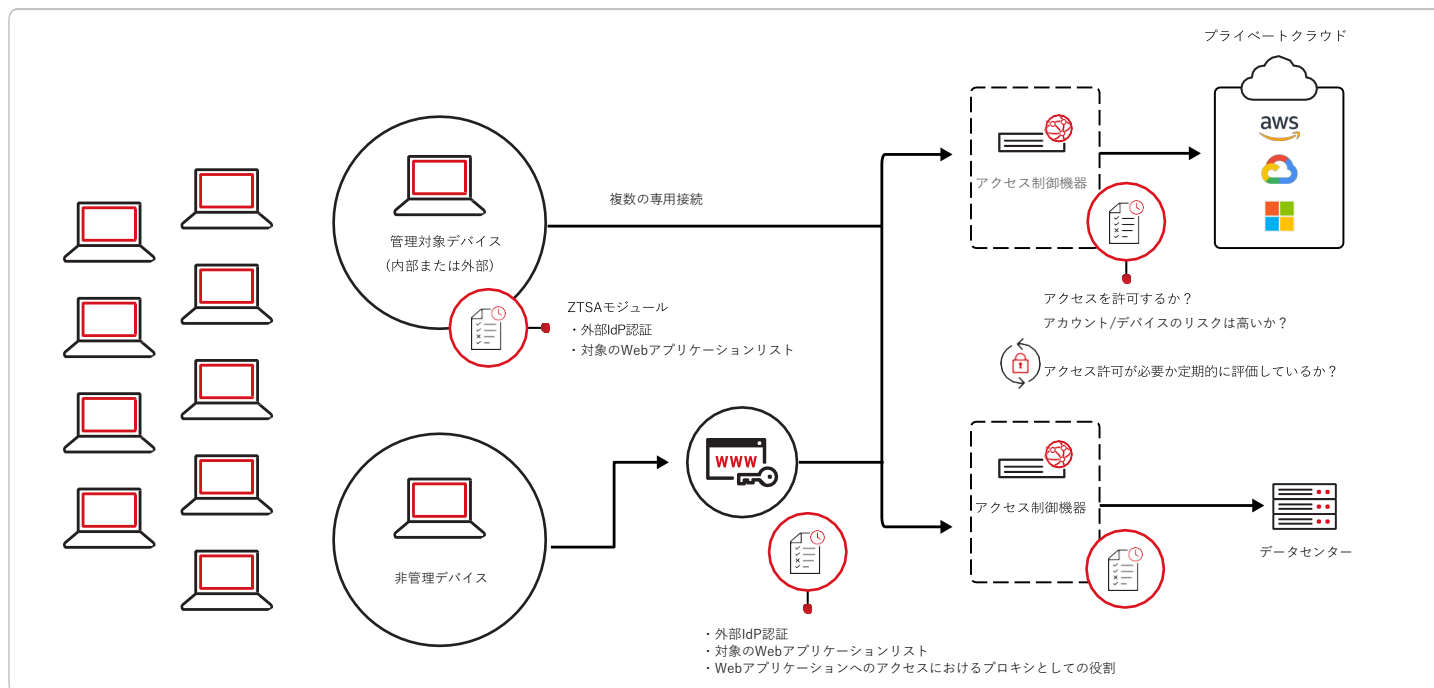
デジタルトランスフォーメーション (DX) を推進していくにつれて、多くの組織はオンプレミスのアプリケーションとリソースを保持する一方で、プライベートクラウドの利用を進めています。ハイブリッドおよびリモートワークを推進している組織にとって、迅速・スケーラブル・安全な方法でこれらのアプリケーションおよびリソースにアクセスすることが重要です。

パフォーマンス： ZTSA -Private Accessは、トレンドマイクロが提供するクラウド環境上で稼働するSaaS型またはオンプレミス型などの形式からプライベートアプリケーションやリソースにアクセスする方法を選択できます。クラウドベースのアプリケーションは、オンプレミスでルーティングすることなく接続できるため、従業員は過負荷なVPNに起因するパフォーマンスの問題に悩まされる必要はありません。

スケーラビリティとアクセシビリティ： ZTSA -Private Accessはプライベートクラウドとオンプレミスデータセンター全体で安定したアクセスを提供します。クラウドでは、安定したアクセスを提供するために、新しいゲートウェイが自動的にスケールされ、必要に応じて負荷のバランスを整えます。オンプレミスアクセスでは、負荷状況を考慮して展開可能なセルフホスト型ゲートウェイによってサポートされます。ZTSAは、デプロイされたゲートウェイ間で負荷バランスを保つクラウドステッチ型の専用接続を提供します。

安全なアクセス： VPNの導入は、組織のエンドポイントのネットワーク範囲に限定されます。一方で、組織のネットワークは、信頼されていない脆弱なホームネットワークにまで広がっています。ZTSA -Private Access は、ゲートウェイを介して特定のアプリケーションやリソースへのアクセスのみを提供することで、信頼されていないネットワークからのアクセスによるリスクを軽減します。これにより、社内外という境界を問わず、アカウントやデバイスなどのアクセス元の状態がポリシーを満たしている場合にのみトラフィックが通過できるようになります。さらに、継続的なリスク評価によりリアルタイムでアクセスを拒否することで、ネットワークへの脅威の侵入を阻止します。

エージェントレス・エンドポイントへの対応： 各エンドポイントの状態に関係なく、安全なアクセスを実現するためにセキュリティポリシーを適用する必要があります。ZTSA -Private Access は、エージェントレス・エンドポイントからのアクセスリクエストを目的とした認証ポータルを提供します。これにより、エンドポイントの状態にかかわらず、ポリシーによるアクセス制御と継続的なリスク評価を実現することができます。



実装

プライベートアプリケーションへのアクセス保護

ZTSA -Private Accessは、既存のアイデンティティプロバイダ (IdP) と連携し、IdPによる静的な多要素認証と組み合わせることで動的な検証を行い、アクセス制御を行います。具体的には、エンドポイントやアプリケーションのハードウェア、OS識別子、ファイルシステム情報、証明書情報、ロケーション情報といった複数の要素を組み合わせたコンテキストによってセッションごとに検証及び制御を行います。また、ゼロトラストネットワークアクセス (ZTNA) ゲートウェイを使用することで、AWSやMicrosoft Azureなどのクラウドプロバイダー上でホストされているアプリケーションへのアクセスが可能です。インサイドアウト (内側から外側へ) 接続によりプライベートアプリケーションをインターネット上から見えないようにすることで、組織は正当な利用を制限することなく攻撃リスクを軽減することができます。

ZTSA -Private Accessは、アクセス元のロケーションやデバイスを問わず、アイデンティティやデバイス、リスク状態、ロケーションといったコンテキストを基にした動的なプライベートアプリケーションへのアクセス制御を可能にします。最小権限の法則に基づいた、ソリューションによるユーザの制限ときめ細やかなアクセス制御を実装することによって、機密情報の漏えいの対策につながります。

エンドユーザによるオンプレミスまたはプライベートアプリケーションへのアクセスの流れ：

1. エンドユーザが既存の SAML SSO 認証情報を使用して IdP で認証する。
2. ZTSA -Private Accessがアクセス元の状態を検証し、サインインセッション中に継続的にチェックする。
3. コントローラーがアクセスを許可されたアプリケーションリストを ZTSA -Private Accessのエンドポイントモジュールに渡す。
4. ZTSA -Private Accessのエンドポイントモジュールからリレーサービスへのアウトバウンド接続が確立される。
5. ゲートウェイコネクタからリレーサービスへのアウトバウンド接続がさらに確立され、エンドユーザのデバイスとコネクタ間のセキュアな接続が確立される。

次のステップ

ZTSAは、統合サイバーセキュリティプラットフォームTrend Vision One上で提供されるソリューションです。ZTSAは、Trend Vision Oneの体験版をお申込みいただくと無料で30日間ご利用いただけます。ZTSAおよびTrend Vision Oneの詳細については、弊社担当営業へお問い合わせください。[Trend Vision Oneの30日間無料体験版で、プライベートアプリケーションへのアクセス及びインターネットアクセスへの動的なアクセス制御をぜひお試しください。](#)