



# クラウドアプリケーションへの 高速で安全なアクセスを提供する

## 課題

### 戦略の実施

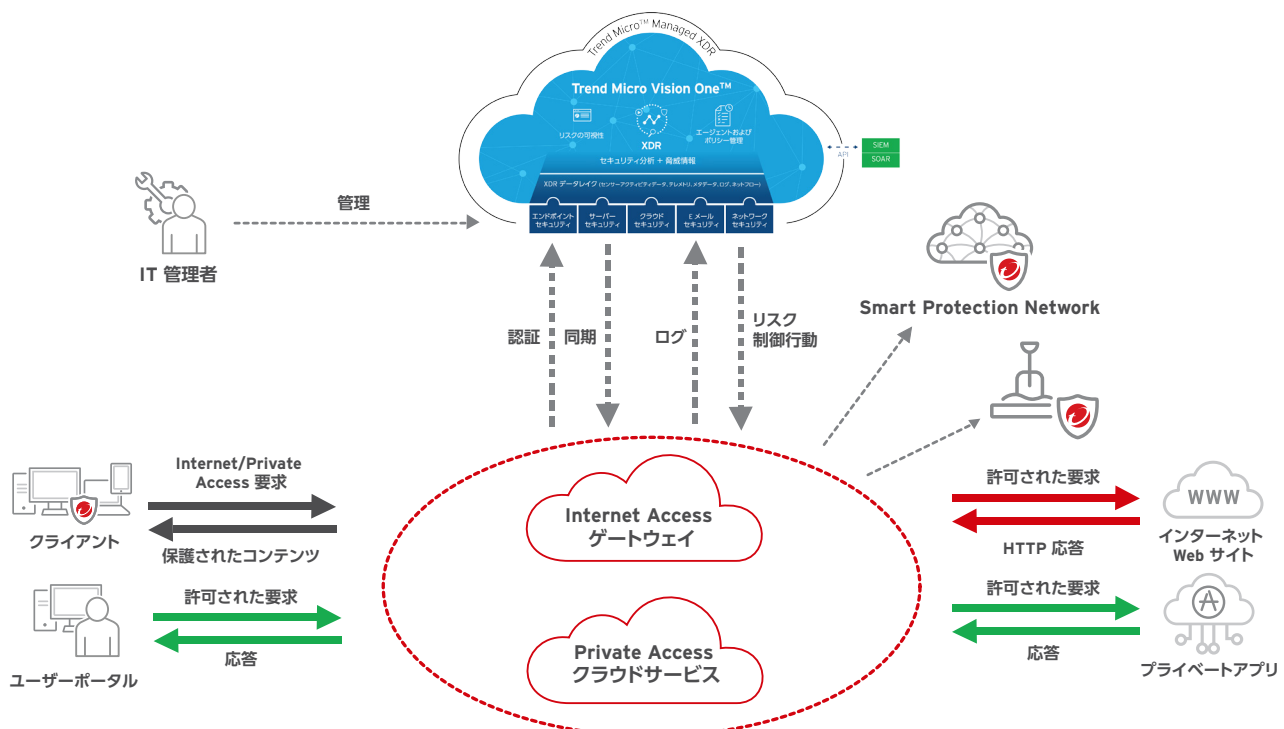
組織のサイバーセキュリティは、戦略レベルから見ると複雑なタスクです。同様に、戦略の日常的な管理と影響も重要です。組織がゼロ・トラストのようなセキュリティの新しいモデルに目を向けると、戦略担当者と戦術担当者の両方が最初のステップに圧倒されてしまいがちです。

組織のセキュリティ運用を大規模に変革することは、一朝一夕にできることではありません。トレンドマイクロの考え方は、**まず目の前にある実現可能な問題に対する解決策を提示することです**。これにより、運用チームは最初の問題を乗り越え、その後の問題を通じて、全体的な目標に向けてセキュリティを有意に向上させることができます。

### 管理者が直面する問題

「クラウドアプリケーションへの高速で安全なアクセスを提供しつつ、可視性と制御性を確保するにはどうすればよいか?」

パブリッククラウドアプリケーション=SaaSに依存してビジネスを展開している企業は、もはや当たり前になってきています。Microsoft 365、Google Workspace、Salesforce、SAPなどがこれにあたります。より多くのビジネス機能がこれらのパブリックアプリケーションに移行するにつれ、可視性とアクセスの制御は「困難」から「存在しない」までになりました。これは、内部で処理されるデータに対するリスクを増大させます。



## 機能

### 異なるテクノロジーを橋渡しする

Trend Micro Zero Trust Secure Access は、これまで切り離されていた複数のテクノロジーに集中制御と統合的な可視性を提供することを目的としています。Trend Micro Zero Trust Secure Access - Internet Access Advancedは、強力なセキュア Web ゲートウェイ (SWG) とクラウドアプリケーションのアクティビティセンサの機能を統合しています。この実績ある技術を Trend Micro Vision One の新しい視点を通して活用することで、SWG と CASB (Cloud Access Security Broker) スタイルの機能だけでなく、より広いエコシステムからの追加データを提供します。これにより、シンプルで一貫性のあるポリシー制御とともに、自動化されたアクセスの意思決定、豊富なテレメトリ、可視化されたレポートが可能になります。

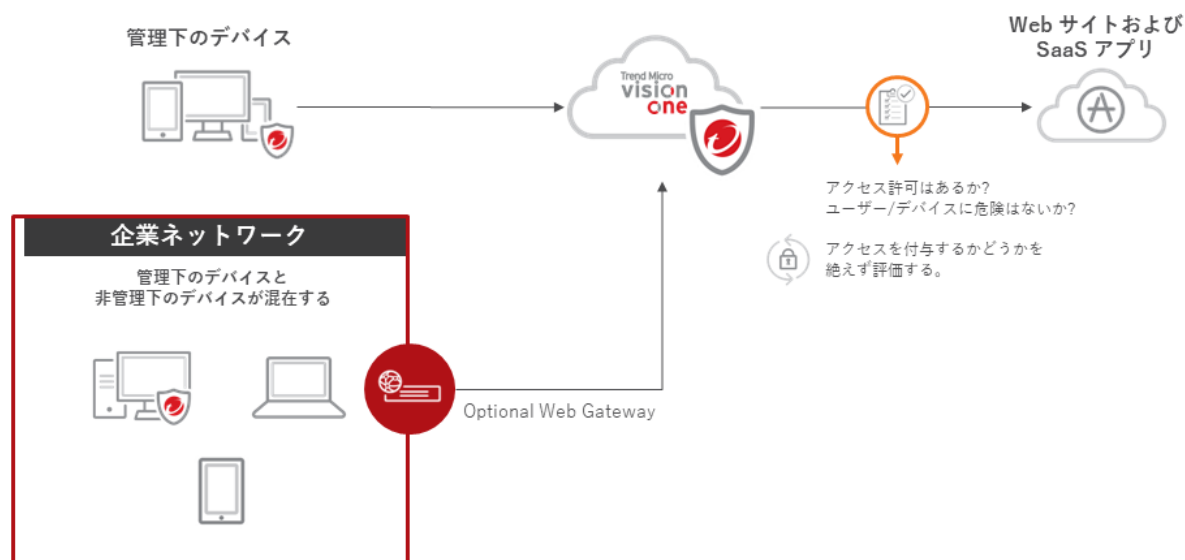
### 境界を越えて移動する

組織がデジタルトランスフォーメーションを進行させるにつれて、サービスとしてのソフトウェア (SaaS) アプリの可視性と制御性が置き去りにされる可能性があります。これが組織のサイバーリスクの対象範囲の拡大につながり、場合によっては不正アクセスやデータ損失などの問題を招くこととなります。また、セキュリティ強化の名の下でビジネスが遅延する可能性も高まるため、パフォーマンス上の懸念が発生します。

**データとアクセスコントロール:** Trend Micro Zero Trust Secure Access Internet Access は、SWG の技術により認可されている SaaS アプリケーションへのアクセスを管理します。これは、各接続に対して継続的なリスク評価を適用し、設定された動的なポリシーの範囲内で許可されたものだけにアクセスを許可するものです。また、クラウドアクセスセキュリティブローカ (CASB) の技術を適用し、データ損失の制御、プライバシーの確保、データアクセスポリシーの適合性を提供します。

**パフォーマンス、アップタイム、および可用性:** Internet Accessでは、ゲートウェイの導入方法と導入場所の選択肢をお客様に提供しています。代表的な導入オプションは、パブリッククラウド内にトレンドマイクロがホストするゲートウェイを設置する方法です。アクセスはクラウドサービスプロバイダ (CSP) が管理し、お客様は最も近い接続拠点 (PoP) に接続されます。トレンドマイクロがホストするゲートウェイは柔軟性があり、トラフィックがどれだけ流れても、パフォーマンスと可用性が制限されることはありません。

**「エージェントあり」および「エージェントなし」の範囲:** エージェントを実行する環境が揃っていればベターですが、各デバイスにエージェントをインストールできない、あるいはサードパーティのエージェントがデプロイされているなど、例えエンドポイントがどのような状況にあっても「会社のセキュリティポリシーを適用する必要」があります。Internet Access は、エージェントの展開の如何に関わらず、インターネットアクセスのセキュリティを保護し、保護対象のギャップを悪用されることを防ぎます。



## 実装

### Internet Access による保護のしくみ

Internet Access はクラウドベースのセキュリティゲートウェイとして動作し、Web およびインターネットトラフィックをアプリケーションレベルでフィルタリングします。クラウドベースのソリューションによって、ネットワーク内外のユーザーすべてが高度に保護され、ポリシーが適用されます。サポート対象の最寄りのデータセンターに対しては、IPsec (Internet Protocol Security) トンネルによる接続の設定、軽量クライアントコネクタまたはプロキシ自動構成 (PAC) ファイル経由でのユーザートラフィックの転送が可能です。Internet Access はエンドユーザーとインターネットの間に位置し、TLS/SSL など複数のセキュリティテクノロジーの全体のトラフィックを検査します。

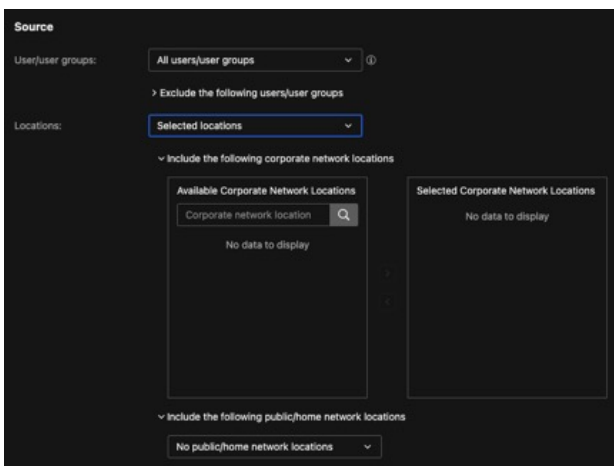
エンドユーザーは次のプロセスに従って Web サイトにアクセスします。

1. ユーザーが既存の SAML SSO 資格情報を使用して ID プロバイダ (IdP) に認証されます
2. ユーザーまたはユーザーグループ、ゲートウェイおよびロケーションが Access Gateway によって検証されます
3. 制御を許可または監視するようにルールが構成されている場合、アクセスが付与されます。URL またはクラウドアプリをブロックするようにルールが構成されている場合、アクションはブロックされます。Access Gateway で構成してあれば、トラフィックに対してさらに脅威保護ポリシーやデータ損失防止 (DLP) ポリシーが適用されます

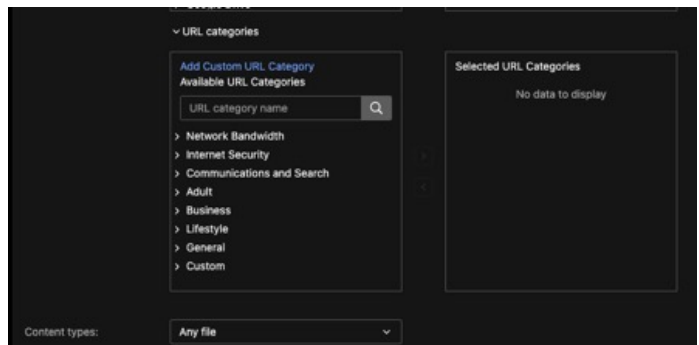
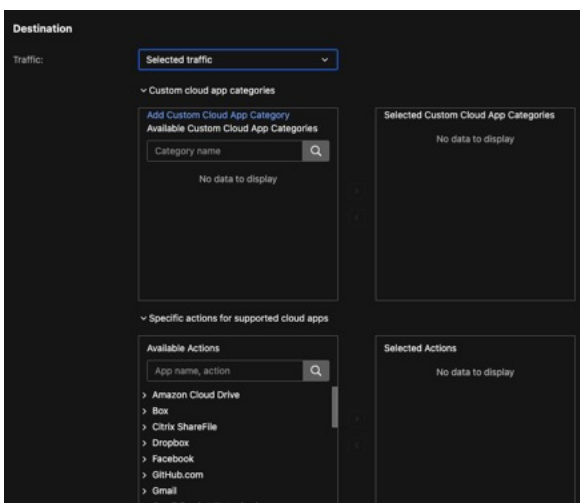
### 簡単なセットアップ

サイトを許可または制限する設定では、以下のようにわずか数ステップでアクセスを追加または削除できます。

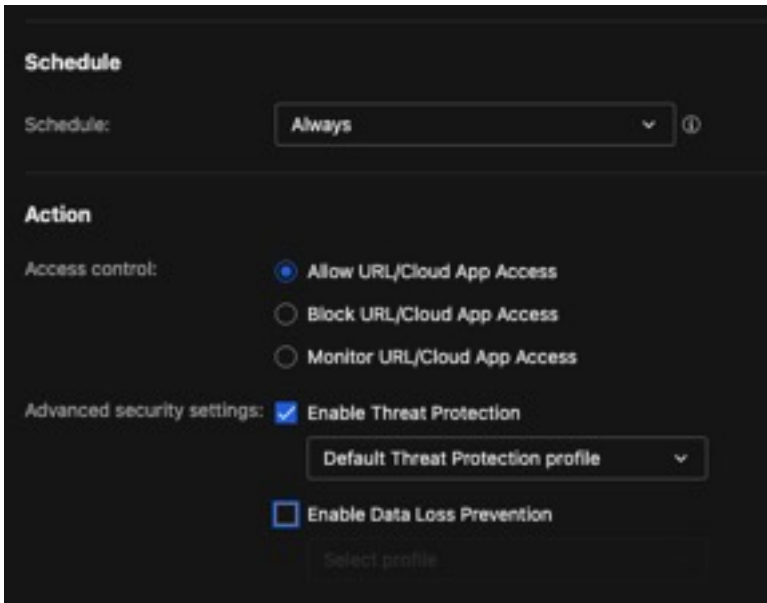
1. ユーザーグループまたはロケーション(あるいはその両方)を選択します



2. 「トラフィック」または「コンテンツ」の種類を選択します (トラフィックの宛先を識別するように設計されています)



### 3. 「スケジュール」および「アクション」を指定します



#### 次のステップ

Zero Trust Secure Access - Internet Access の無料試用版は Trend Micro Vision One を通じてご利用になれます。詳しくは、弊社の [Trend Micro Zero Trust Risk Insights](#) をご覧いただくか、アカウントチームにお問い合わせください。

[Trend Micro Vision One の 60 日間の無料試用版](#) にサインアップしてインターネットへの安全なアクセスを今すぐお試しください。



Securing Your Connected World

- ・ ©2022 by Trend Micro Incorporated. All rights reserved. Trend Micro,
- ・ Securing Your Connected World, および Trend Micro Smart Protection
- ・ Network は、トレンドマイクロ株式会社の商標または登録商標です。その
- ・ 他の各社の名前および製品名は、一般に各社の商標または登録商標です。
- ・ 本書に記載されている情報は、予告なしに変更される場合があります。
- ・
- ・
- ・ 収集される個人情報と理由については、当社の Web サイト
- ・ (<https://www.trendmicro.com/privacy>) のプライバシーに関する通知を
- ・ 参照してください
- ・
- ・ [SB00\_SaaS\_App\_Use\_Case\_220713US]