

インターネットへの安全なアクセス



課題

戦略の実施

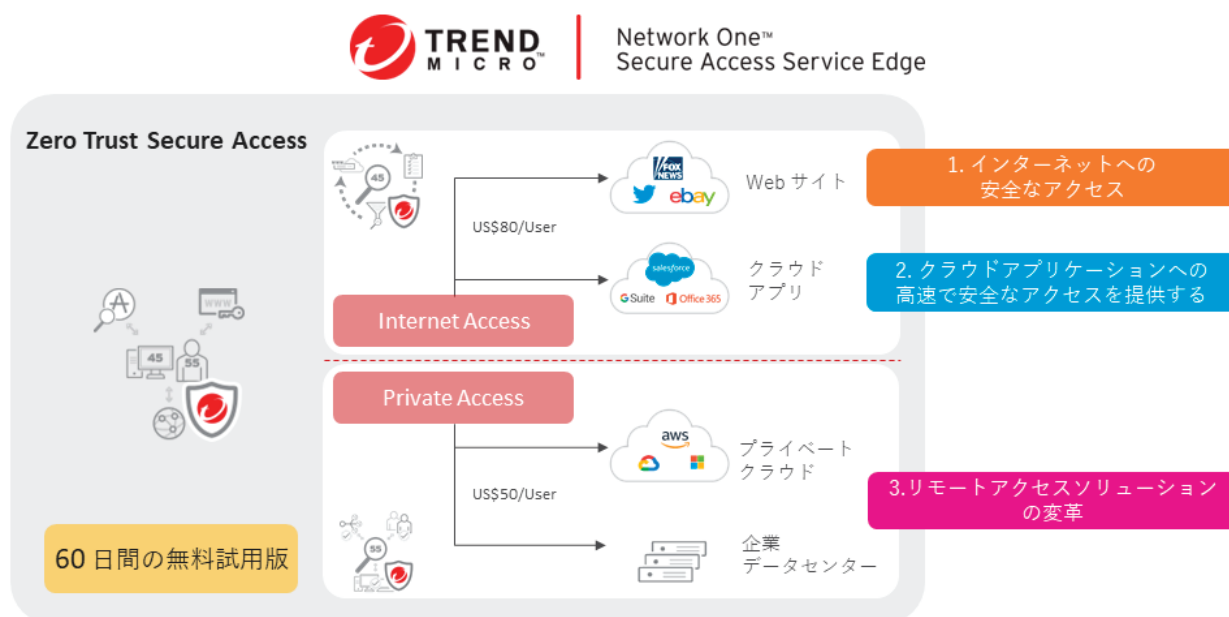
組織のサイバーセキュリティは、戦略レベルから見ると複雑なタスクです。同様に、戦略の日常的な管理と影響も重要です。組織がゼロ・トラストのようなセキュリティの新しいモデルに目を向けると、戦略担当者と戦術担当者の両方が最初のステップに圧倒されてしまいがちです。

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

「すべてのユーザーに企業ポリシーを適用し、インターネットへ安全にアクセスするにはどうすればよいか？」

ほとんどの組織は、企業ポリシーに沿ったガードレールの設定 (NSFW=Not Safe For Work 「職場で見ない方が良い」サイトの制限) と、デバイスのパフォーマンスや生産性に悪影響を与えずに脅威をブロックするセキュリティ保護の提供について共通の課題を抱えています。



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 は、強力なSWGの機能を備えており、この実績あるテクノロジーを Trend Micro Vision One の視点から活用し、その機能だけでなく、広範なエコシステムから追加の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。

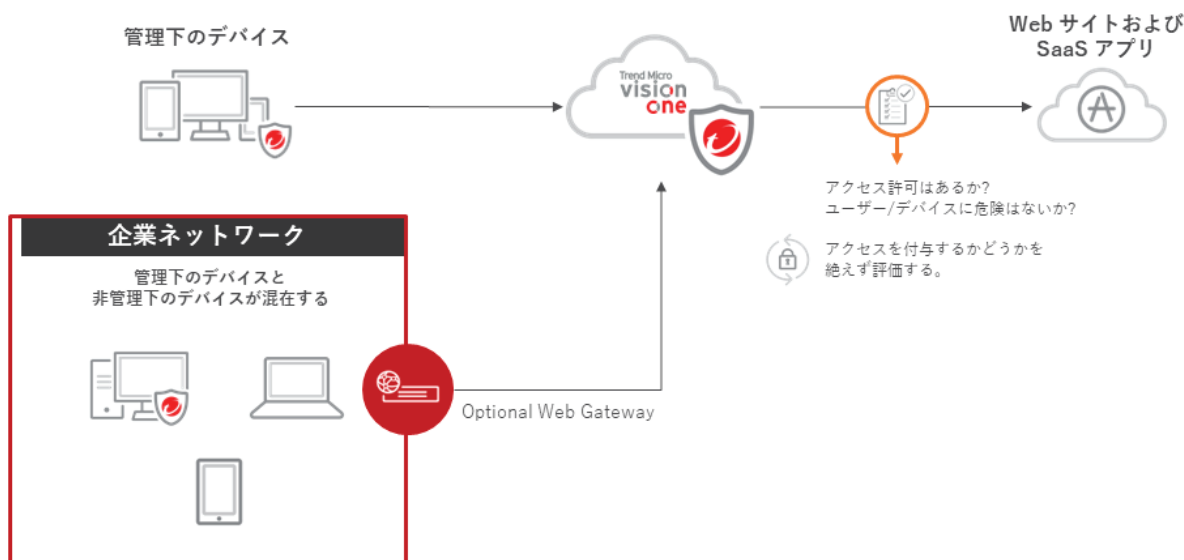
境界防御を超えて移動する

インターネットのアクセス制御の問題に対する既存の解決策にはたいいてい、いくつかの制約がありその制約が解決を損なうことがあります。それにはパフォーマンスの問題、誤検知、アップタイム、「エージェントあり」および「エージェントなし」の保護対象の可用性などがあります。Internet Access ではこのような課題に狙いを定め、これまでセキュア Web ゲートウェイの効果を低下させてきた障壁を取り払います。

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。

セキュリティの正確さ:トレンドマイクロでは社内調査チームを活用して、グローバルな脅威に関する情報を提供しています。これはいくつかのシステムで実装されており、その中には Web サイトのカテゴリとリスクに関する最新データを提供する Web レピュテーションサービス(WRS)も含まれています。このサービスでは世界中にデプロイされた数十億ものエンドポイントからデータを収集し、通常の Web アクティビティを妨げることなく、危険な Web サイトへのアクセスによる潜在的な影響を最小限に抑えます。

「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、例えば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。

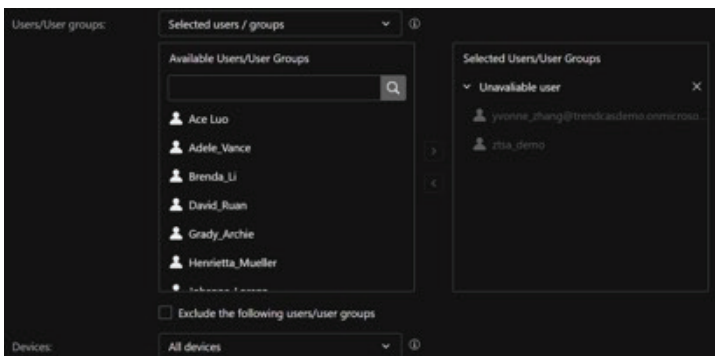
エンドユーザーは次のプロセスに従って Web サイトにアクセスします。

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

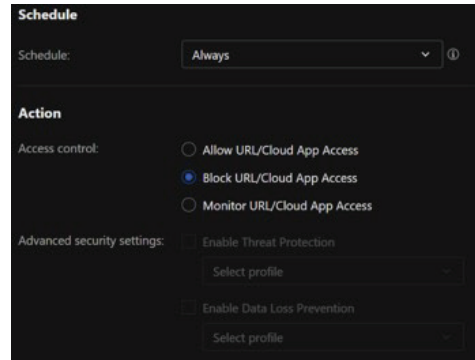
簡単なセットアップ

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。

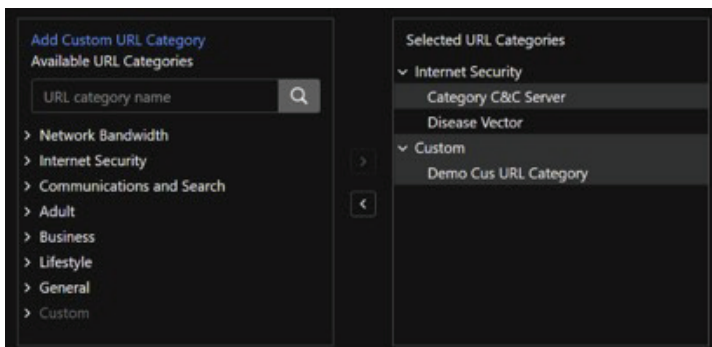
1. ユーザーまたはグループを選択します



3. 「スケジュール」および「アクション」を指定します



2. URL またはカテゴリを選択します



次のステップ

Zero Trust Secure Access - Internet Access の無料試用版は Trend Micro Vision One ソリューションを通じてご利用いただけます。詳しくは、弊社の [Trend Micro Zero Trust Secure Access](#) 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, および Securing Your Connected World 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

[SB01_Secure_Internet_Use_Case_221003US]