

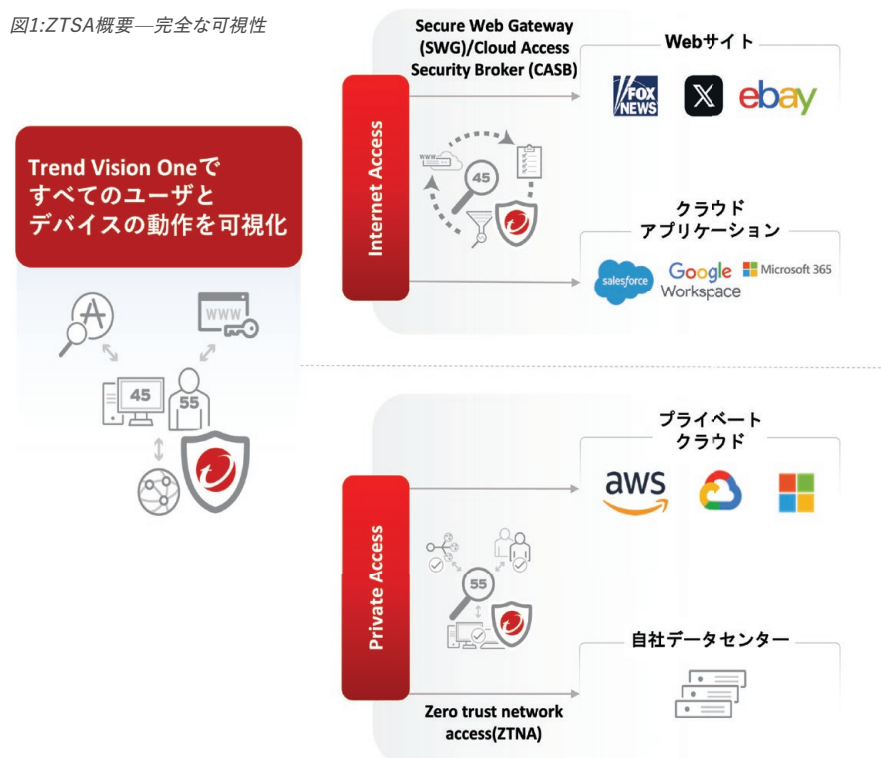
Trend Vision One™ – Zero Trust Secure Access (ZTSA)

ポリシーによる制御、リスク軽減、可視化でセキュリティ運用を一元化

今日では、多くの組織がハイブリッドまたはリモートワークが可能な働き方へ変化しています。アタックサーフェス（攻撃対象領域）が拡大するにつれてサイバーリスクが高まるため、もはや”Trust, but verify”（信頼せよ、しかし検証せよ）という考え方は通用しなくなっています。ひそかに巧妙なサイバー攻撃をしかける攻撃者や絶えず変化する脅威に直面した場合、従来までの暗黙の信頼に基づいたセキュリティ対策では十分に対峙することはできません。ゼロトラストの考え方に基づいた対策を優先することで、サイバーリスクを軽減できます。

Trend Vision One – Zero Trust Secure Access (ZTSA) を活用し、アクセス元のロケーションやアクセス先を問わず、ユーザ、デバイス、およびアプリケーションを、安全に接続します。ZTSAではセキュリティの状況をアクセス制御に迅速に反映する方法を採用し、きめ細かい可視化、強化されたセキュリティ、継続的なリスク評価によって、保護対策を強化します。また、生成AIサービス利用時のリスク対策機能の提供により、経営目標を支えるゼロトラストアーキテクチャの実現を推進します。

図1:ZTSA概要—完全な可視性



主な利点:

- ユーザとデバイスのネットワークアクセスを制御
- 厳格なアクセス制御によりデータやユーザを保護
- セキュリティチームとネットワークチームの運用を効率化しながら、リスクレジリエンスを強化
- 継続的なリスク評価により、可視性の拡大と対応時間の短縮を実現
- 生成AIサービスへのアクセスを保護し、生成AIのビジネス活用へ貢献

ゼロトラスト

ゼロトラストセキュリティモデルは、組織のネットワーク展開、管理方法に変化をもたらします。

特定のネットワークからリソースへアクセスする対象を暗黙的に信頼するのではなく、通常とは異なるアクセスを安全ではないアクセスと仮定します。その結果、対象者、デバイス、および各種資産間のすべてのアクセスを検証して、認証と認可を行います。

さらに、包括的なリスク評価を実施して、ネットワークとの接続が確立される前に、アクセス元のアカウントとデバイスのリスク状態を検証します。

AIを活用したTrend Vision Oneプラットフォームとの統合

統合サイバーセキュリティプラットフォームTrend Vision Oneは、ZTSAに加え、ASRM(Attack Surface Risk Management)機能とXDR(Extended Detection and Response)機能を提供しています。Trend Vision Oneにより、自組織におけるリスク状態及びセキュリティ対策状況を継続的に評価、セキュリティ戦略の拡充と最新情報の提供を可能にします。SSE(Security Service Edge)の観点では、ZTSAはSWG(Secure Web Gateway)、CASB(Cloud Access Security Broker)、ZTNA(Zero Trust Network Access)の機能を提供し、AIサービスに加えて、ネットワーク、Web、クラウド、およびプライベートアプリケーション全体へのユーザおよびデバイスからのアクセスを保護することができます。

強力なアクセス制御を組織に導入することで、一つのプラットフォームを通じてセキュリティ体制全体を強化します。

図2: ZTSA – AI Service Access概要



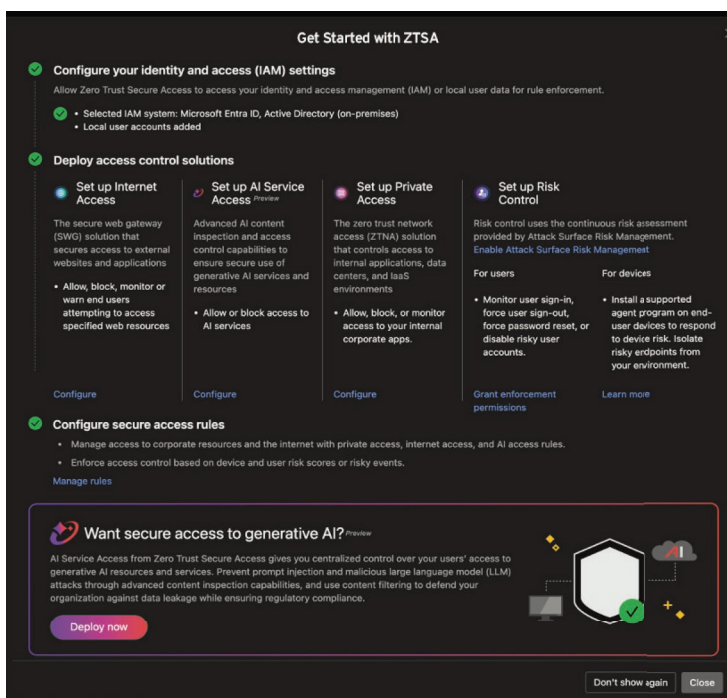
相反するAIサービス利用と安全なアクセスを両立

ZTSAを活用する組織では、敵対的な利用を防止しながら、生成AIをビジネスやセキュリティ運用に活用できます。パブリックまたはプライベート生成AIサービスへのアクセス時にゼロトラスト原則に基づいたアクセス制御をすることが、防御の強化へつながります。

ZTSA – AI Service Accessは、生成AIサービスへのアクセスを制御し、生成AIサービスのプロンプトおよびレスポンスのコンテンツを検査することができます。コンテンツの特定、フィルタリング、分析を行い、パブリックおよびプライベート生成AIサービスにおける機密情報の漏えいや、安全でないレスポンスを防止します。可視性を高めて組織の生成AIサービスの利用状況を監視および管理し、ユーザのアクセス時の情報漏えいの可能性やプロンプトインジェクションによる攻撃の防止をサポートします。これにより、攻撃者による生成AIサービスに対する操作リスクの可能性を軽減できます。

ZTSA – AI Service Accessにより、セキュリティの強化、ユーザの生成AIサービスアクセスの保護、運用の効率化、コンプライアンスの維持を実現し、生成AIサービスの安全でシームレスな利用を可能にします。全体的なセキュリティ体制、ビジネス回復力、拡張性、運用の効果と効率、およびユーザーエクスペリエンスを向上させます。

図3: ZTSAを始めるためのガイド



Trend Vision OneとZTSAの主な機能

統合サイバーセキュリティプラットフォームTrend Vision Oneは、ASRM、XDR、ZTSA、多層なレイヤーにおけるセキュリティ機能へのアクセスを1つのコンソールで提供します。強化された可視性と拡大されたリスクへの気づきを実現することにより、複雑なインフラストラクチャの管理ではなく、戦略的なセキュリティ対策に集中できるよう、ネットワークチームとセキュリティチームの運用を強化します。

ZTSAでは、インターネット、SaaS (Software-as-a-Service) アプリケーション、および生成AIサービスへのアクセスを保護。XDRを活用した高度な相関分析とASRMを活用した継続的なリスク評価によって、ユーザのリスク状態の変化に応じてアクセスを自動的に許可または拒否することができます。



XDR、CASB、およびZTSAの単一エージェントを使用することで合理化された統合プラットフォームと、わかりやすい価格設定により、SASEの導入に伴う複雑さを軽減できます。



451 Research

S&P Global
Market Intelligence

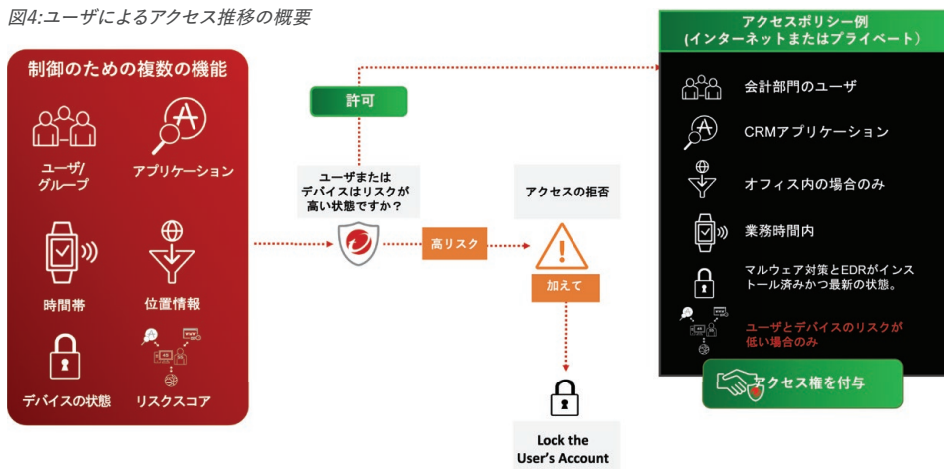
リスクインサイトの獲得、アクセス制御の向上、リスクの低減

継続的なリスク評価の活用

リスクは常に変化しており、セキュリティ体制を改善するためのメカニズムとして活用するためには、継続的に評価する必要があります。継続的なリスク評価の必要性から、Trend Vision One – Attack Surface Risk Management (ASRM) ソリューションは、ZTSAIに継続的なリスク評価を提供します。ASRMはテレメトリデータを収集し、エンドポイントエージェントとネットワークソリューションを活用してリスク低減のための意思決定を自動化します。

ASRMからのリスク評価データは、一定の間隔およびリアルタイムで動的に収集され、ユーザ、デバイスおよびアプリケーション間の通信の評価に利用されます。リスクスコアのしきい値を超過すると、接続通信がブロックされます。これにより、ネットワークが攻撃のリスクから保護される状態となります。リスクスコアがしきい値以下に戻ると、再接続が可能となり、安全に業務を継続できる状態となります。

図4: ユーザによるアクセス推移の概要



“

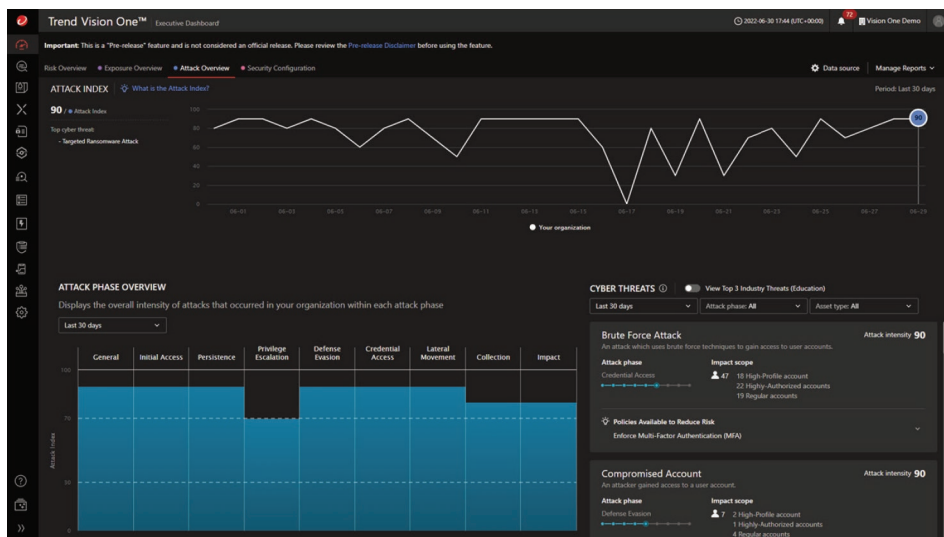
組織には「継承される信頼」が存在するが、ゼロトラストでは攻撃者がその信頼に便乗することを防止することができます。

”



トレンドマイクロ株式会社
市場戦略担当バイスプレジデント
Eric Skinner 氏

図5: Trend Vision One -Executive Dashboard: 攻撃段階の概要



組織における信頼の再考

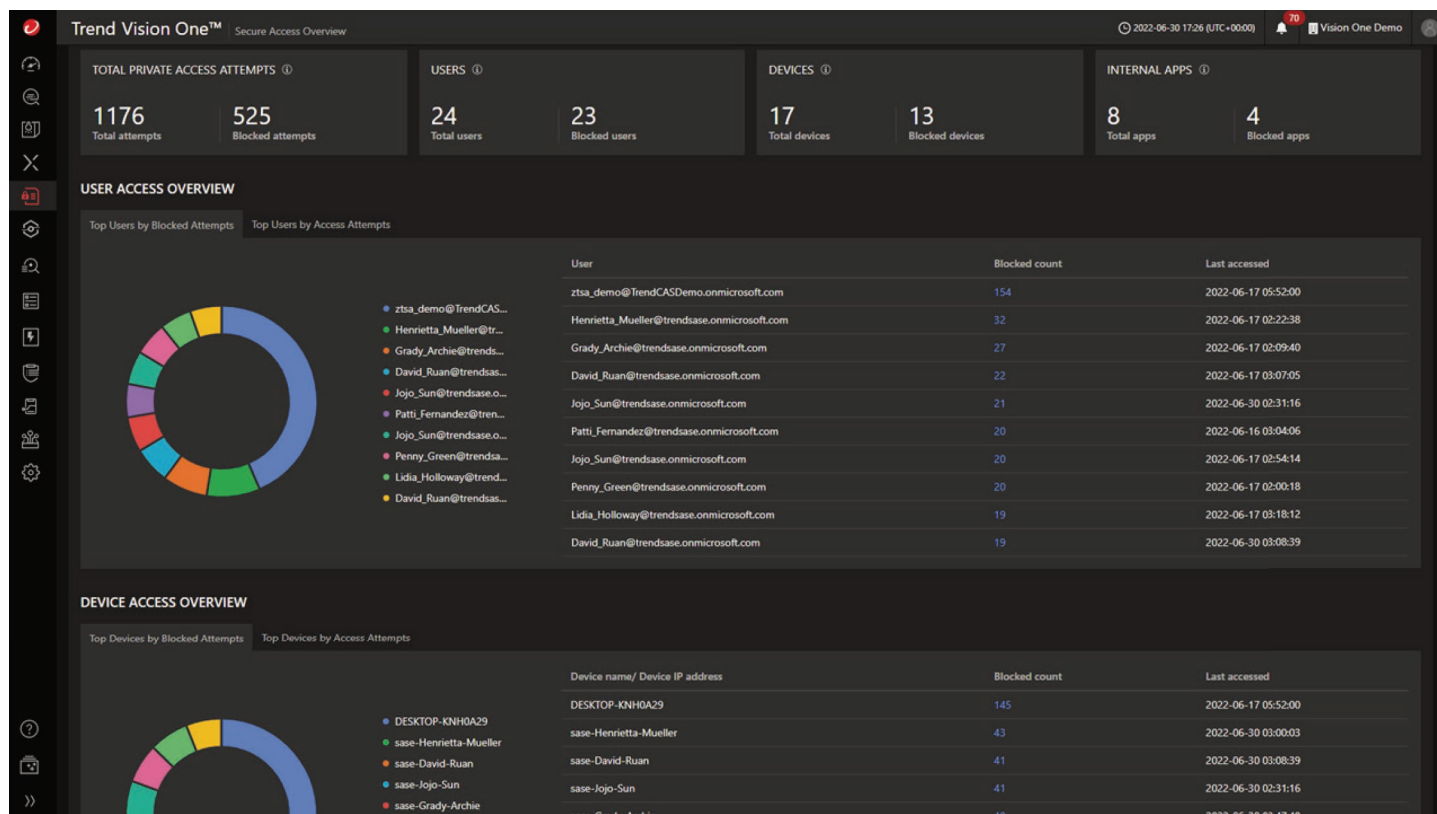
多くの組織では、暗黙の信頼が標準となっています。しかし、これがお客様組織を非常に大きなリスクに晒してしまいます。1件のアイデンティティ侵害がお客様環境で大混乱を引き起こし、ネットワーク全体に広がる可能性があります。

デジタルトランスフォーメーションと同様に、ゼロトラストへの道は、ソリューションを導入することがゴールではなく継続的な改善が必要です。組織の最も優先度の高いリスクと現在のセキュリティ体制に応じて実行可能な4つの重要なステップがあります。多くのユースケースが存在し、組織がゼロトラストアーキテクチャに向けて長期的に実装できるものもありますが、短期的には以下のステップを踏むと良いでしょう。

1.SWG (Secure Web Gateway):インターネットへのアクセス保護とリアルタイムの可視化

- 安全なWeb閲覧、シャドールITへのアクセス制御のためのエージェント及び、エージェントレスによる保護を提供
- 高度なコンテキスト化されたデータをTrend Vision Oneに提供し、可視性を向上
- インターネットアクセス状況を可視化し、セキュリティとポリシーコントロールを実現
- 組織管理のデバイスと持ち込みデバイス(BYOD)の両方を保護
- ASRMを活用した継続的なリスク評価を提供
- Trend Vision Oneの単一のコンソールでの運用を実現

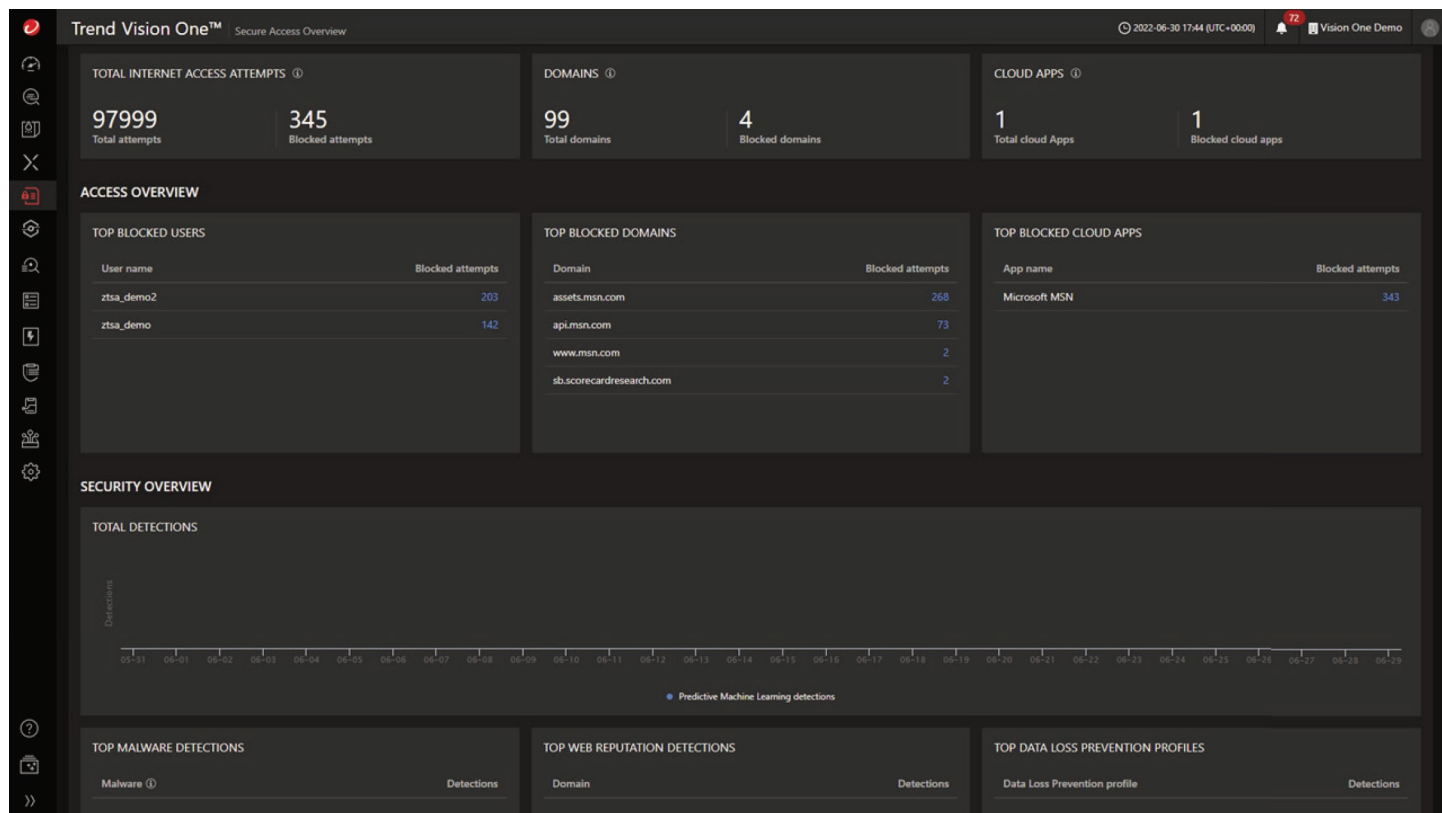
図6:Trend Vision One-ZTSA概要



2.CASB (Cloud Access Security Broker):クラウドアプリケーションの安全なアクセスと制御

- サクシオンITへのアクセスのためのエージェントとエージェントレスによる保護を提供
- クラウドアプリケーションへの安全なアクセスを提供し、ポリシー違反とセキュリティリスクを可視化
- データや重要な情報への不正アクセスのリスクを軽減
- きめ細かいクラウドアプリケーションのアクション制御によりアプリケーションのアクティビティを監視
- ASRMを活用した継続的なリスク評価を提供
- Trend Vision Oneの単一のコンソールでの運用を実現

図7:Trend Vision One-ZTSA インターネットアクセスの概要

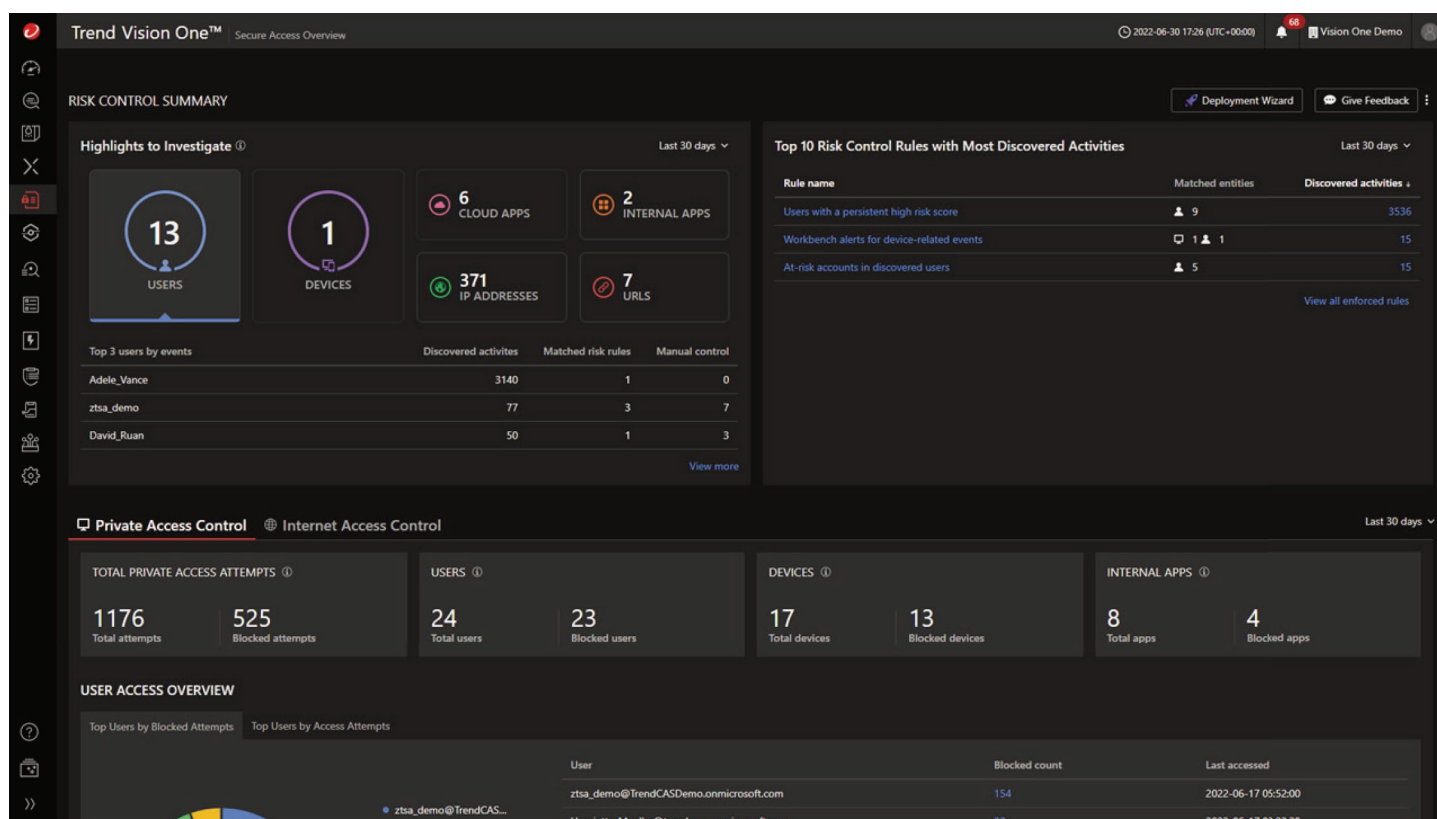


3.ZTNA (Zero Trust Network Access):最新のアプローチでビジネスに不可欠なリソースへの安全なアクセスを実現

- エンドユーザが組織のアプリケーションやリソースに簡単にアクセスする制御オプションを備えたエージェント及び、エージェントレスによる保護を提供
- 仮想プライベートネットワーク (VPN)による暗黙の信頼を削減、リスク評価を強化
- アプリケーションとリソースへの認証された安全なジャストインタイムアクセスを提供し、保護を強化
- ネットワークの特定の部分のみにアクセスを制限することで、侵害に遭った場合の影響を最小限に
- ASRMを活用した継続的なリスク評価を提供
- Trend Vision Oneの単一のコンソールでの運用を実現
- 継続的なリスク評価によるアプリケーションとリソースへのアクセス制御、リスク状態の変化に応じた動的なアクセス制御を実現

ZTSAは特定のアプリケーションとリソースへのゲートウェイを提供し、その他のネットワークへのアクセスを制限します。これにより、有効なユーザ認証情報が漏えいした場合でも、組織に付与されるアクセスレベルの制限を通じ、サイバー攻撃の影響範囲を最小限に留めます。

図8:Trend Vision One-ZTSA プライベートアクセスの概要



4.ZTSA – AI Service Access:生成AIサービスへのアクセスを保護

- きめ細かい可視化を通じた、継続的なリスク評価に基づくアクセスポリシーの適用により、生成AIサービスへのアクセスを動的に制御
- 生成AIサービスの検査によって、潜在的な情報漏えいおよび想定外のレスポンスを回避
- プロンプトインジェクションを検出し、生成AIサービスの操作リスクの可能性を軽減
- プライベート生成AIサービスに対するDoS攻撃リスクを回避
- 生成AIサービスへの安全なアクセスを提供し、ポリシー違反とセキュリティリスクを可視化
- 個人情報や機密情報への不正アクセスのリスクを軽減

図9:Trend Vision One-ZTSA -AI Service Access

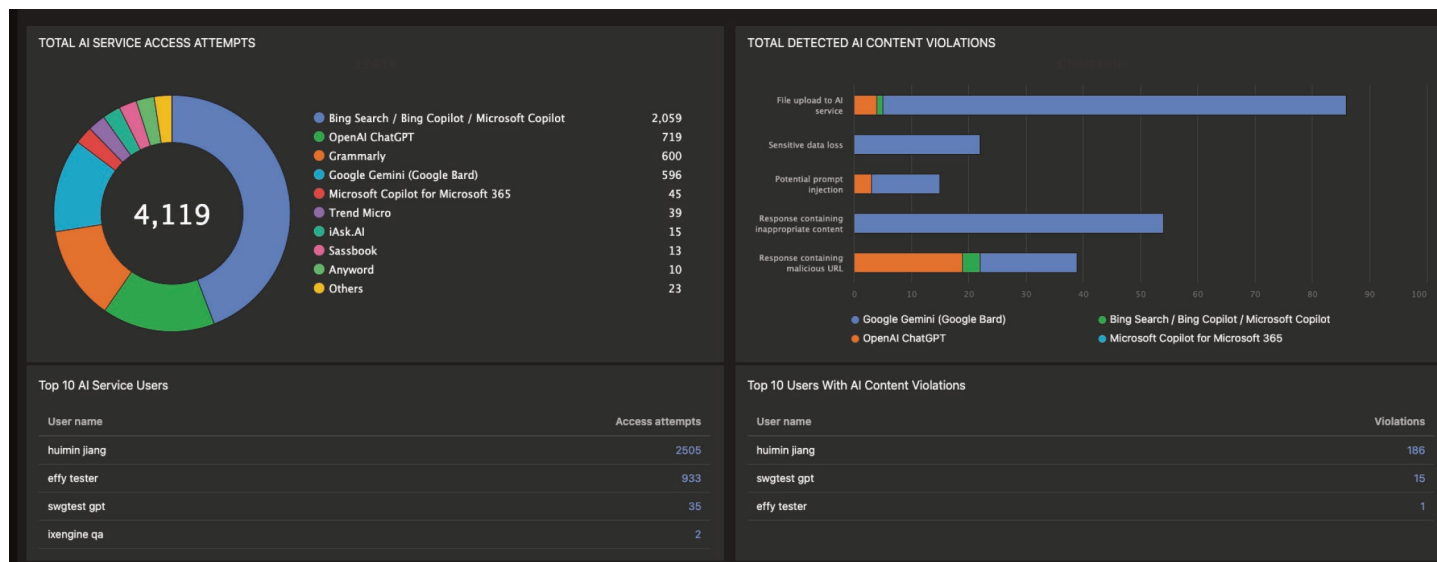


図10:ZTSAとXDREの関係性



> [無料体験版へアクセス](#)

Copyright ©2024 Trend Micro Incorporated. All rights reserved. Trend Micro, Trend Vision One, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. Trend Micro, the Trend Micro logo, and the t-ball logo Reg. U.S. Pat. & Tm. Off. (DS03_ZTSA_Datasheet_240731US)

[TrendMicro.com](https://www.trendmicro.com)

For details about what personal information we collect and why, please see our Privacy Notice on our website at: [trendmicro.com/privacy](https://www.trendmicro.com/privacy)