ソリューション概要

Taniumで実現するゼロトラスト

IDだけでなくデバイスの状態も検証が必要な理由とは

ゼロトラストとは

ゼロトラストのコンセプトはシンプルで「あらゆるユーザやデバイスを信用せず、常に検証する」ことです。ゼロトラストを実現するためには、次の3つのポイントを確認しましょう。

- ユーザの資格情報
- ユーザがアクセスしようとしているデータ
- ユーザが使用するデバイス（エンドポイント）

状況に応じたアクセス管理、多要素認証（MFA）、ネットワークアクセスに関する最新のアプローチと最小権限の原則とを組み合わせることで、クラウドファースト、そしてモバイルファーストの時代にも対応できるアジャイルなセキュリティモデルを維持できます。

これにより攻撃対象領域を縮小し、検証済みの承認した環境下で、必要なユーザのみに機密データのアクセス権を付与することでリスクを低減できます。

デバイスの検証がゼロトラスト成功の鍵に

従来のゼロトラストでは、ネットワークアクセスとシングルサインオンによるIDとアクセス管理（IAM）を重視してきました。しかし、リモートワークの増加に伴って、境界の概念は次第にあいまいになっており、デバイスが新たな境界となることでデバイスの状態の重要性が高まっています。

そこでデバイスの検証という第3の柱を用意することで、資格情報の盗難や、さらにはデバイスそのものが盗難に遭うことでMFAを突破しネットワークにアクセスされることからも保護することができます。ネットワーク内に侵入された場合も、環境内のコンプライアンス違反や重大な脆弱性を監視しておけば、デバイスの保護が機密情報の流出やそれ以上の損失を防ぐための最後の砦となります。

だからこそ、ゼロトラストへのアプローチの3つ目の要素として、コンバージド・エンドポイント管理が重要になるのです。

デバイスの状態をシームレスに大規模検証

Taniumを使えば、この新たな境界となるエンドポイントをリアルタイムに可視化して制御することができます。リアルタイムで正確なエンドポイントのデータが手に入らなければ、コンプライアンスを徹底することはできず、アクセスの前提となるデバイスの状態も検証できません。認証だけでは、デバイスが確実に保護されているかどうかを見極めることはできません。システムにアクセスするにはデバイスが必須であるため、セキュリティはシステムとアクセスという両輪で考える必要があります。

アイデンティティやアクセスのポリシーを導入した後も、Taniumでデバイスがポリシーを順守しているかを継続的にチェックし、どのユーザも信用しないというゼロトラストのアプローチを徹底できます。

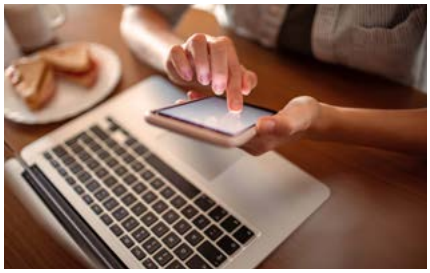
また、Tanium Platformの機能を使えば、すでに導入済みのゼロトラスト用のツールと連携することも可能です。

ゼロトラスト用のコンポーネント

デバイスのコンプライアンス状態の監視と対応
デバイスのセキュリティ状態を確認し、異常がある場合にはITチームがアクションできる状態に

IDとアクセス管理（IAM）
認証時に各ユーザの情報を確認し、アクセス権をロールベースのルールと照らし合わせて比較

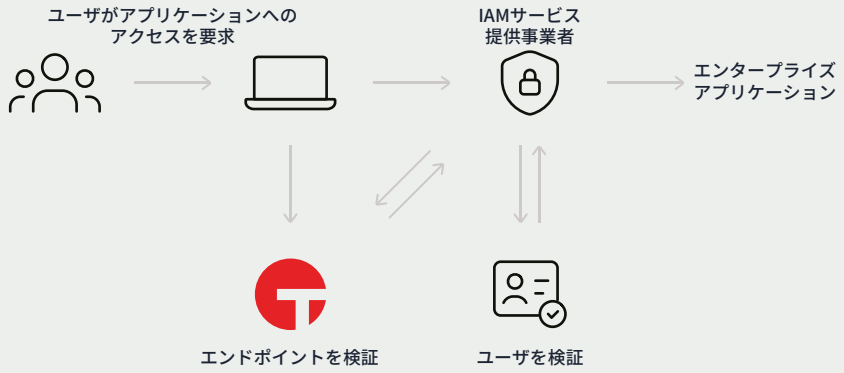
ネットワークアクセス
ユーザのペルソナや使用するデバイスに基づいて、リソースやネットワークセグメントへのアクセスを制御



ゼロトラストを実践するためにタニウムがデバイスの検証をサポートします。詳細はお問合せください。

Taniumを活用したゼロトラストの実践によるメリット

- **すべてのエンドポイントを可視化**し、環境内に接続されている端末を常に把握
- エンドポイントデータを即座に大規模に把握し、**情報を一元管理**
- 重要なデータが保存されたシステムへのエントリーポイントを閉鎖することで、**攻撃対象領域を縮小**
- アクセスの前提条件となる**デバイスの状態を検証**
- ポリシーを確実に実践することで**常にコンプライアンスを守り**、問題が発生した場合もすばやく診断や修正を実施
- **機密データを特定**し、漏洩を防止
- 問題が発生した場合にも状況を**コントロールして迅速に対応**
- TaniumのAPIを使って、既にゼロトラストのために**導入済みのツールと連携**
- ユーザが使用したり、データのやり取りが発生しているシステムのリスクスコアを表示するダッシュボード機能で、**リスクプロファイルをリアルタイムに把握**
- **IT資産の利用状態の基準値を作成**することで、従業員のニーズに合わせたゼロトラストアプローチの設計をサポート



ゼロトラストのアプローチを進める中でデバイスの状態を考慮しない企業では、リスクを完全に管理することはできません

さまざまな場所で業務が発生する現代の企業には、セキュリティを維持するために、ユーザとエンドポイントの両面から環境全体のすべてのアクティビティを簡単に監視し、制御することが求められています。そのためには、リモートワークやクラウドサービス、モバイル通信が普及した今の時代に、シームレスなセキュリティモデルで対応しなくてはなりません。ゼロトラストは、この新しい時代に対応するために誕生しました。そして、大規模な環境でゼロトラストセキュリティを実現するための鍵となるのが、エンドポイントの可視化です。

Taniumのコンバージド・エンドポイント管理プラットフォームを使った堅固なゼロトラストの実践について、詳細はぜひお問合せください。
https://www.tanium.jp/contact-us/

業界唯一の統合型エンドポイント管理（XEM）プロバイダであるタニウムは、複雑なセキュリティとテクノロジー環境を管理するための従来のアプローチにおけるパラダイムシフトをリードしています。デバイス間の包括的な可視性、統一されたコントロールセット、そして「機密情報と大規模インフラの保護」という単一の共有目的に向けた共通のタクソノミを提供する単一のプラットフォーム内にIT、コンプライアンス、セキュリティ、リスクを統合することで、タニウムは、すべてのチーム、エンドポイント、ワークフローをサイバー脅威から保護します。タニウムは、「Fortune 100 Best Companies to Work For」に含まれ、6年連続で「Forbes Cloud 100」に選ばれています。実際、Fortune 100の半数以上と米軍は、タニウムが人々を保護し、データを守り、システムを保護し、あらゆる場所のあらゆるエンドポイントを監視して制御することを信頼しています。これが“The Power of Certainty”です。

www.tanium.jpをご覧いただき、FacebookとTwitterでフォローしてください。