



個人所有デバイス 持ち込み (BYOD)

Duo は1万を超える組織に採用され、3億を超えるエンドポイントに関するインサイトを提供することで、重要なビジネスアプリケーションへのセキュアなアクセスの実現に貢献しています。

課題：

可視性の欠如

BYOD (個人所有デバイス持ち込み) を導入した企業では、従業員の生産性が向上する一方で、個人のデバイスでセキュリティの正常性が可視化されないという重大なセキュリティ問題も発生しています。

従来のモバイルデバイス管理 (MDM) ソリューションでは、この可視化を実現するためにエンドポイントにエージェントを導入する必要があ

ります。しかし、プライバシーの侵害を懸念して、自分のデバイスでこのソリューションを使用しないユーザーが多くなります。その結果、網羅性と可視性が著しく損なわれることになります。

企業と個人のすべてのデバイスを可視化し、企業ネットワークと重要なアプリケーションを脆弱なエンドポイントや潜在的なデータ漏洩から保護する新しい方法があります。



Duo は、最も広く使われている次のようなアプリケーションと連携します。



ソリューション:

Duo のエンドポイント可視性

Duo の Unified Access Security (UAS) ソリューションには、次の3つの主要なメリットがあります。

01

BYOD に関するセキュリティポリシーの適用

すべてのデバイスを対象にセキュリティの正常性を可視化し、企業に脆弱性リスクをもたらす恐れのある古いオペレーティングシステム、ブラウザ、プラグインを監視できます。

画面ロックやパスワードなどのセキュリティ機能を持たないモバイルデバイスや、ジェイルブレイクやルート化が施されたモバイルデバイスを特定できます。

さらに、このデータを使用してセキュリティポリシーを適用し、古いデバイスによる企業アプリケーションへのアクセスをブロックします。これによって、セキュリティの脆弱性やマルウェア感染のリスクが軽減されます。

02

完全なデバイスインベントリ

Duo は、アプリケーションにアクセスするすべてのユーザーデバイスを可視化します。これには、ラップトップ、デスクトップ、モバイルデバイスが含まれます。デバイスは、ユーザーが所有するものでも、企業が所有するものでもかまいません。

環境にアクセスしているデバイスを可視化すると、これまで見えなかったデバイスや未知のデバイスに起因する全体的なリスクが判断でき、アプリケーションのリスクに基づいてセキュリティポリシーを適用できます。

03

デバイスの態勢に関するインサイト

Duo を使用すると、アプリケーションにアクセスするすべてのデバイスのセキュリティ態勢について、管理者が深いインサイトを得ることができます。デバイス上で動作している OS、ブラウザ、Flash、Java などのソフトウェアが最新かどうか判断できます。モバイルデバイスの場合、パスワードロックが有効になっているか、暗号化が有効になっているか、ジェイルブレイクされているかどうかを知ることができます。

これらのインサイトに基づいてポリシーを設定することで、セキュアで信頼できるデバイスのみアプリケーションへのアクセスを許可できます。

「
Duo から得られる認証ソースに関するデータは貴重です。
これまでほとんど不明瞭だったユーザーデバイスの情報が
得られるようになったことにも価値を実感しています」

Thomas Siu 氏

Case Western Reserve 大学
最高情報セキュリティ責任者