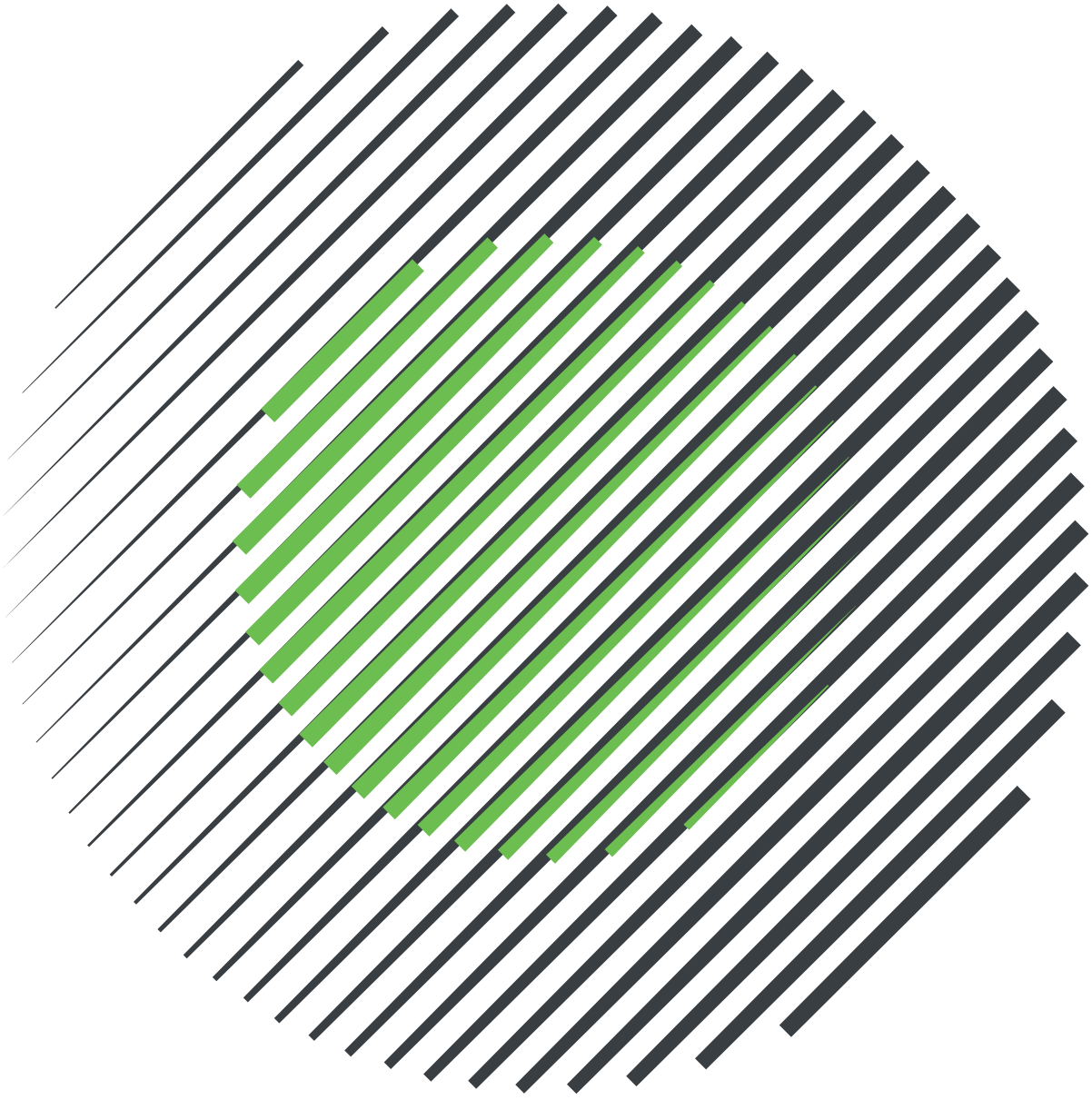
5 ステップで実現する

# 境界のないセキュリティ

Zero Trust モデルを採用してセキュアなアプリケーションアクセスを実現



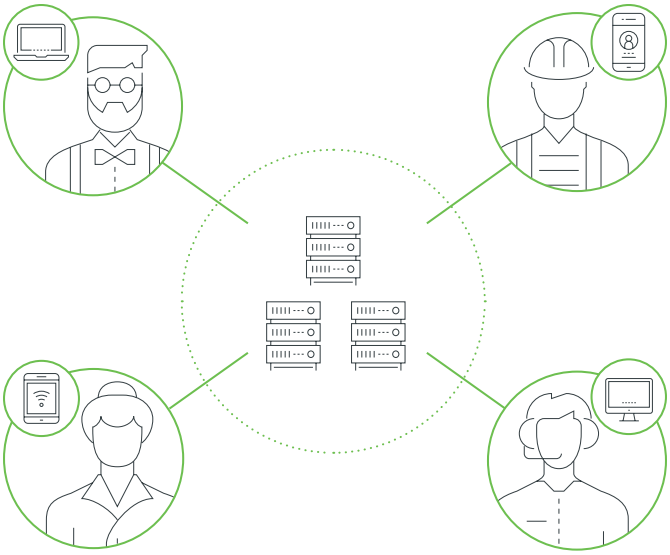
Duo Security はシスコの一員となりました。

セキュリティにおいては、往々にして理論と実際が一致しない場合があります。

従来の境界ベースのセキュリティモデルは、重要なデータとアプリケーションを一元的に扱い、仮想プライベートネットワーク (VPN)、ファイアウォール、モバイルデバイス管理 (MDM) ソリューションを利用してアクセスを管理するもので、理論上、ネットワークを効果的に保護できるはずです。

ただし実際には、この古いアプローチはあまり現状に適応できていません。特に、ユーザーが自分のデバイスを仕事に持ち込み、企業の機密データがサードパーティのクラウドサービスに保存されている状況には対応できていません。また、古いモデルの脆弱性を悪用する脅威が増しているため、境界セキュリティを超えて進化することは、将来にとって良いアイデアというだけでなく、競争力を維持したい組織にとっては不可欠なことです。

このような状況の変化により、新しいパラダイムの必要性が高まっています。新しいパラダイムとは、2010 年に元 Forrester Research 社のアナリストである John Kindervag 氏が最初に考案し、後に Google 社が「BeyondCorp」アーキテクチャに採用したもので、一般的に「Zero Trust」モデルと呼ばれています。このホワイトペーパーでは、Zero Trust の概要と、組織に Zero Trust モデルを導入するための 5 つの重要なステップについて説明します。



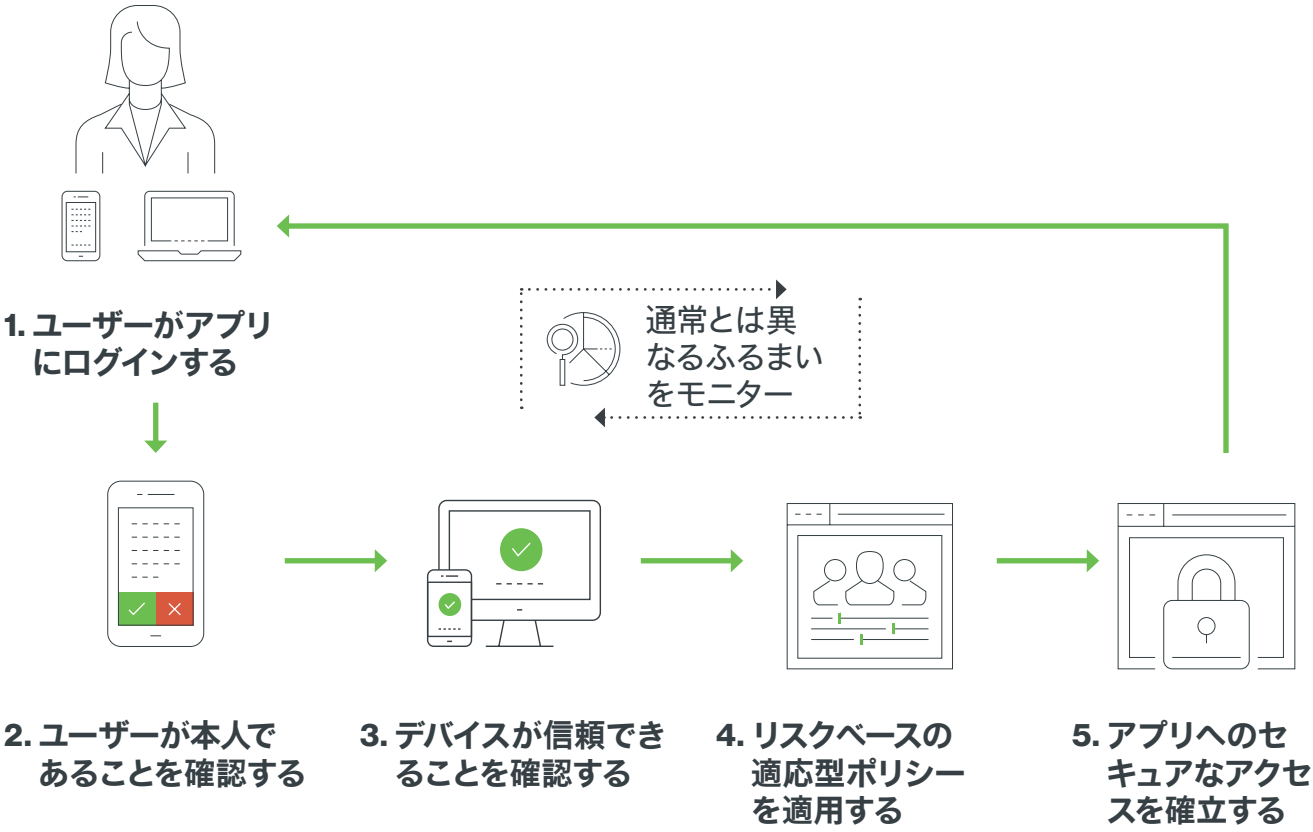
従来のアプローチ

最新のアプローチ

# 新しい「Zero Trust」パラダイム

一元的な Web セキュリティアプローチが最初に確立されたとき、すべてのビジネスネットワークには、定義された明確なセキュリティ境界があったため、このアプローチは理にかなっていました。しかし、もう当てはまりません。今やユーザーとそのデバイスは至る所に存在し、セキュリティ境界は、それぞれの場所にあるからです。

# Zero Trust モデルのワークフロー




かつては、どのユーザーからのアクセスは信頼でき、どのユーザーはそうではないかを判断するのに時間を費やしていましたが、Zero Trust パラダイムは、そうではありません。ユーザーが任意のデバイスから円滑にアクセスできる必要があるという現実を受け入れ、すべてのアクセスが信頼できないネットワークから行われているものとして扱っています。Zero Trust モデルを導入すると、企業が管理しているデバイスと管理していないデバイスを把握し、デバイスの信頼性に基づいてアクセスを許可できるようになります。

Zero Trust モデルに移行することは、多くのオフィスが、受付で建物への出入りを管理していたことから、セキュリティバッジで管理するようになったことと似ています。通常、古いモデルでは、受付の管理者が誰を入れて誰を入れないかを決定します。一方セキュリティバッジを使用すると、適切な資格のある人だけが入れます (受付を否定しているわけではありません。セキュリティバッジを使用すると、セキュリティが向上し、入退室の管理がしやすくなると言っているだけです)。

Zero Trust は、「正しいパスワードを持っているか」といった 1 つの基準に基づいて検証するのではなく、複数のデータポイントを考慮して、ユーザー中心のセキュリティを確立します。セキュリティは複数の要素に基づいて、たとえば、「多要素認証 (MFA) のアクセス要件を満たしているか、かつ、最新のモバイル オペレーティング システムを導入しているか、かつ、各ビジネス固有のセキュリティポリシーに準拠しているか」といったことを効果的に検証します。すべてのセキュリティ対策を調整しながら組み合わせてアクセスポリシーを適用することで、アクセスデバイスや時間を問わずに効果的なセキュリティを確立できます。

理論はここまでにして、境界のない Zero Trust セキュリティパラダイムを導入するための 5 つのステップを詳しく見ていきましょう。

# 1

# ユーザーが本人であることを確認する

ユーザー名とパスワードだけではもはや不十分です。Verizon 社の「*2017 年度データ漏洩 / 侵害調査報告書*」によると、報告された Web セキュリティ侵害の 81% もで、盗まれたパスワードや脆弱なパスワードが利用されていました。[1] ユーザーが本人であることを適切に確認するには、MFA などの強力な認証ポリシーが必要です。

最初のステップは、すべてのユーザーとアプリケーションに MFA を導入することです。これは思ったより簡単です。また、すべてのユーザーとデバイスのインベントリが作成され、今後のステップに活用できるというメリットも得られます。

最初の取り組みとして MFA を導入することは、ユーザーを Zero Trust モデルに簡単に移行させる良い方法です。管理者が境界のないセキュリティという考えに適応するには、時間がかかる場合がありますが、ユーザーも同様に、Zero Trust モデルの一環として、ログインするたびに追加のセキュリティ対策が求められることに慣れる時間が必要です。

[1] Verizon 社 2017 年度データ漏洩 / 侵害調査報告書 (DBIR)、**http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017**

# 2

# ユーザーのデバイスとアクティビティを詳細に可視化する

ユーザーが本人かどうかを判断するための仕組みが整ったので、次は、ユーザーがアプリケーションにアクセスする際に使用しているデバイスを可視化します。

このステップで重要なことは、個人および企業が管理するすべてのユーザーデバイスのインベントリを作成して維持することです。そうすることで、デバイス自体の存在を可視化し、それらのデバイスのセキュリティ態勢に関する重要な情報も取得できます。これは、組織が所有 / 管理するデバイスと、ユーザーが所有 / 管理するデバイスを区別するために重要です。なぜなら、アプリにアクセスしようとしているデバイスの種類を正確に把握することで、ユーザーとデバイスに関連するセキュリティリスクを確認できるからです。

3

# ユーザーデバイスの信頼性を確認する

Zero Trust モデルにおいて、複数の調整されたデータポイントに基づいてセキュリティを管理する方法について説明しました。この新しいパラダイムでは、これら多くの重要なデータポイントから、アクセスを要求しているエンドポイントデバイスについてより多くの情報が得られます。3 番目のステップでは、エンドポイントデバイスの特性を定義して確認します。この特性は、ログインのたびに相互参照されます。

たとえば、多くの企業は、Zero Trust パラダイムを採用して、主に次の 2 つの方法でデバイスの信頼を確立します。1 つは、デバイスにこれまでアクセス権が付与されたことがあるかを確認することで、2 つ目は、デバイスに必ず自社のセキュリティ要件（デバイスのオペレーティングシステムの最小バージョンや暗号化など）を遵守させることです。

デバイスが企業で管理されているものかどうかを把握することも重要です。

ユーザーとデバイス両方の「信頼性の判断」は、アプリへのアクセスをユーザーに許可する前に行われることに注意してください。たとえば、ユーザーが適切なログイン情報を持っていても、何らかの点で企業の最低基準を満たしていないデバイスから仕事用電子メールシステムにログインしようとすれば、アクセスは拒否されます。

# 4

# リスクベースの適応型アクセスポリシーを適用する

次に、ユーザーとデバイスの両方を考慮したセキュリティポリシーを作成します。たとえば、「企業の電子メールシステムにログインするには、ユーザー名、パスワード、および MFA の認証が必要」とポリシーを定義するのではなく、デバイスとユーザーのポリシーを調整して、「企業の電子メールシステムにログインするには、ユーザー名、パスワード、MFA の認証が必要で、かつ、デバイスはセキュリティの最低基準を満たすもののみ」と定義します。

例を挙げると、リモートユーザーが午前 9 時に自宅からログインして電子メールをチェックする場合、これは通常のふるまいとみなされ、ポリシーの範囲内です。しかし、同じユーザーが週末にログインし、過去にアクセスしたことのない Salesforce の顧客データをチェックするとしたら、これは通常とは異なるふるまいとみなされ、リスクベースモデルではチェックされます。

また、ユーザーとそのデバイスに関連するリスクは、アクセスごとに変わる可能性があるため (ユーザーのデバイスソフトウェアが古くなった場合など)、許容可能なレベルにリスクを抑えるために、アクセスポリシーも状況の変化に適応できる必要があります。

# 5

# すべてのアプリケーションに対してセキュアな接続を確立する

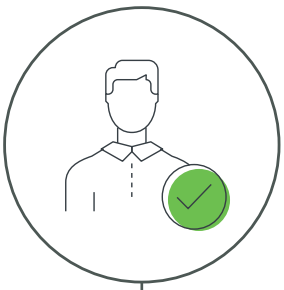
ユーザーのアイデンティティとデバイスの信頼性の両方が検証されて、ユーザー / デバイスポリシーが適用されると、ユーザーのデバイスとアプリケーション間でセキュアな接続が確立されます。

Zero Trust モデルの導入は、まずリスクが最も高いアプリケーションから始めます。最終的にはすべてのアプリを保護する必要があるため、最も重要なアプリから始め、重要度に応じて順番に導入していきます。状況によっては、「スイッチを切り替える」だけでセキュアな接続を確立できる場合もありますが、特定のアプリケーションが正しく機能するようにするには、アクセスプロキシが必要になる場合もあります (アクセスプロキシは、エンドユーザー、使用中の Zero Trust プラットフォーム、ネットワーク間の接続を管理するものです)。

アプリへの接続は、アクセス元のネットワークに基づいて信頼を「推測」して行うのではなく、ユーザーとデバイスの信頼を「検証」して行うものであることを認識しておいてください。

アプリケーションへのセキュアな接続と適応型ポリシーが組み合わされ、ユーザーアイデンティティとデバイスの信頼性が検証されると、アクセス判断がネットワークからアプリケーションに移ります。これが Zero Trust セキュリティモデルの中核となるコンポーネントです。

# Zero Trust 成熟度モデル

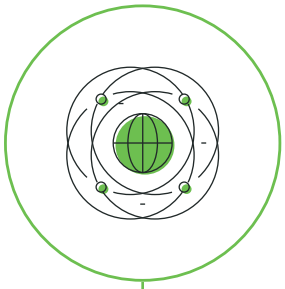


1 ユーザーが本人であることを確認する

2 ユーザーのデバイスとアクティビティを詳細に可視化する

3 ユーザーデバイスの信頼性を確認する

4 リスクベースの適応型アクセスポリシーを適用する



5 すべてのアプリケーションに対してセキュアな接続を確立する

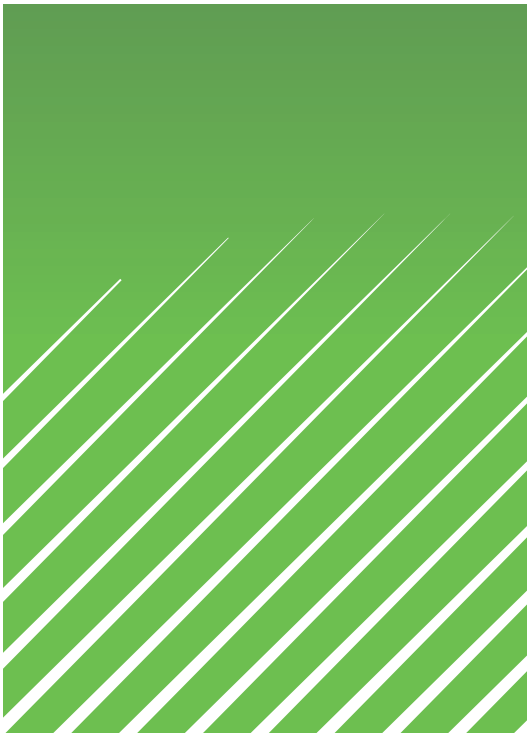
Zero Trust

# このモデルで不要になるもの

Zero Trust モデルに移行する時期や方法を検討するにあたり、最後に、新しいモデルでは何が不要になるかを考えます。VPN、ネットワーク アクセス コントロール (NAC)、MDM ソリューションは必要ありません。つまり、これらの製品の導入や管理によるオーバーヘッドもすべてなくなるということです。独自の次のステップを検討する際は、従来のモデルから移行することで削減できる時間、コスト、労力を必ず考慮してください。

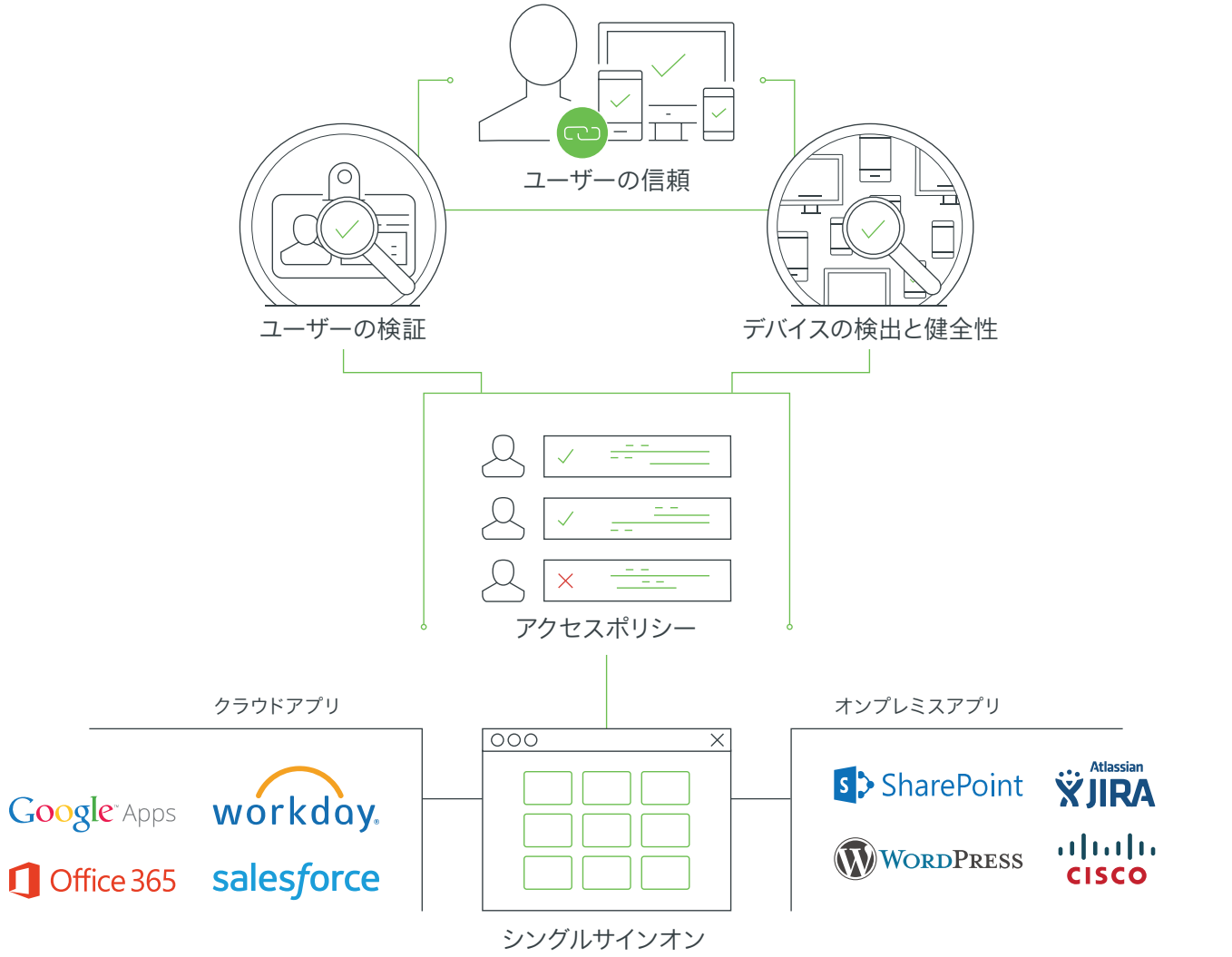
# まとめ

Zero Trust モデルは先に進む大きな一歩です。ユーザー名やパスワードなどのほとんど静的な基準から、ユーザーとデバイスの信頼性に基づいた動的なセキュリティに移行します。ユーザーが本人で、適切な環境において正しいデバイスを使用していることを確認できれば、企業はより安全になります。またユーザーは、自分の責任で自分のデバイスを正常な状態に保たなければならないことを理解しているので、さらに安全になります。



# Duo Beyond

## 信頼できるユーザーと信頼できるデバイスだけをアプリケーションに接続




**Duo Beyond** は、デバイスや場所に関わらず、すべてのユーザーに対して、あらゆるアプリケーションへのアクセスを保護します。すでにクラウド主体の組織や、クラウドへのセキュアで迅速な移行を求めている組織は、Duo Beyond を利用してオンプレミスとホスト型のアプリケーションを保護すると同時に、モバイルワーカーとモバイルワーカーが選んだデバイスも保護してください。

Duo Beyond は、Zero Trust セキュリティ プラットフォームを提供します。これにより、組織は、アクセス元のネットワークではなく、ユーザーのアイデンティティとデバイスの信頼性に基づいて、アプリケーションへのアクセスの可否を判断することができます。Duo は、この機能をクラウドから提供します。面倒でコストのかかる時代遅れのテクノロジーには依存しません。

## duo.com/beyond にアクセスして Duo Beyond の詳細を確認し、30 日間の無料トライアルをご利用ください。