EBOOK

ゼロトラストによるトランスフォーメーションで鍵となる3つの要素

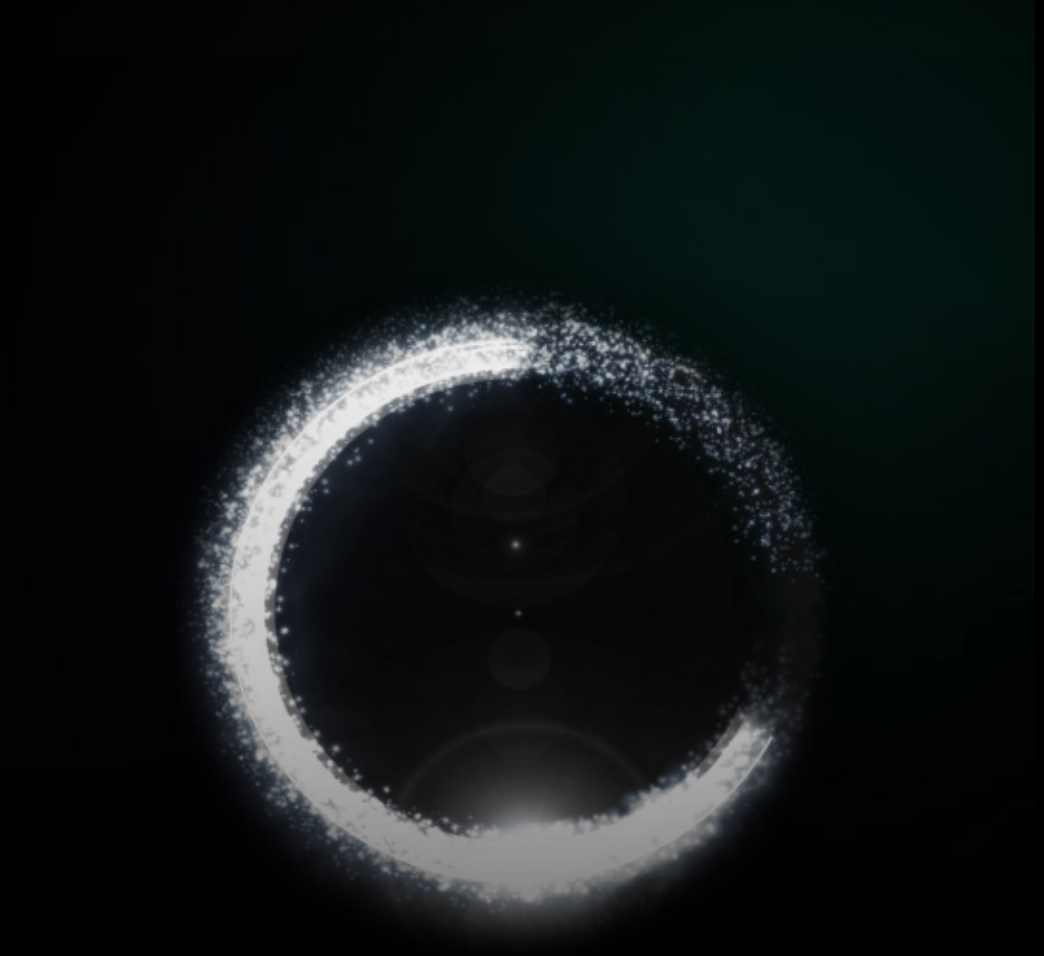
——プラットフォーム、人、プロセス

はじめに

ゼロトラストへの道

デジタルトランスフォーメーションは、今日のビジネスの進め方を根本的に変えました。**従業員が今では会社のネットワークよりインターネットを多く利用し、**あらゆる場所からアプリケーションやデータにアクセスするようになりました。機密度の高いビジネスデータが様々な場所に分散し、Microsoft 365などのSaaSアプリケーションやAWS、Azure、Google Cloud Platformのプライベートアプリケーションが企業の境界の外に存在するようになりました。

デジタルトランスフォーメーションのプロセスにより、ビジネスの俊敏性や情報フローは向上しますが、攻撃対象領域が大幅に拡大し、ビジネスが新たな脅威に直面することになります。ネットワークの保護に重点を置いていた従来のセキュリティアーキテクチャでは、このような新しい現実に対応できません。 ビジネスを保護し、デジタルトランスフォーメーションのメリットを手に入れるには**、ユーザとビジネス資産を中心とするクラウド提供型のゼロトラストセキュリティモデルへと移行する必要があります。**。



まず定義を考える

ゼロトラストとは？

ゼロトラストの概念は10年以上前から存在するものですが、この用語が実際に何を意味するかについては、多くの混乱がありました。 ゼロトラストは、1つのテクノロジを指す言葉ではありません。

ゼロトラストは、最小限の特権アクセスとユーザやアプリケーションを基本的に信頼しないという原則に基づいて 今日の組織を保護するホリスティックアプローチです。 ゼロトラストは、すべてが敵対的という前提で始まり、**ユーザのアイデンティティとコンテキストに基づいてのみトラスト（信頼）を確立し、**すべての段階でポリシーがゲートキーパーとしての役割を果たします。

まず定義を考える

ゼロトラストの実践

ゼロトラストは、セキュリティ、ネットワーキング、最新のワークプレイスの実現などの今日の最も困難な課題の解決を支援します。

セキュリティ

サイバー脅威の防止：
ゼロトラストは、ユーザだけでなく、クラウドワークロード、サーバ、さらにはSaaSアプリケーションのサイバー脅威から保護を可能にします。

データ損失の防止：
ゼロトラストは、ホリスティックアプローチによって、偶発的あるいは意図的かに関係なく、クラウドワークロードも含むデータの流出や損失を防止できます。

ネットワーキング

ユーザとブランチの接続の簡素化：
ゼロトラストを採用することで、従来型のハブ &スポーク方式のネットワークのトランスフォーメーションが可能になり、ブランチオフィスやリモートユーザは、接続する場所に関係なく、インターネット経由で任意の宛先に安全に接続できるようになります。

安全なクラウド接続：
従来のサイト間 VPNをクラウドまで拡張すると、水平移動のリスクも拡大します。 ゼロトラストを代わりに採用することで、ワークロードを他のワークロードに安全に接続できます。

新しいワークプレイスの実現

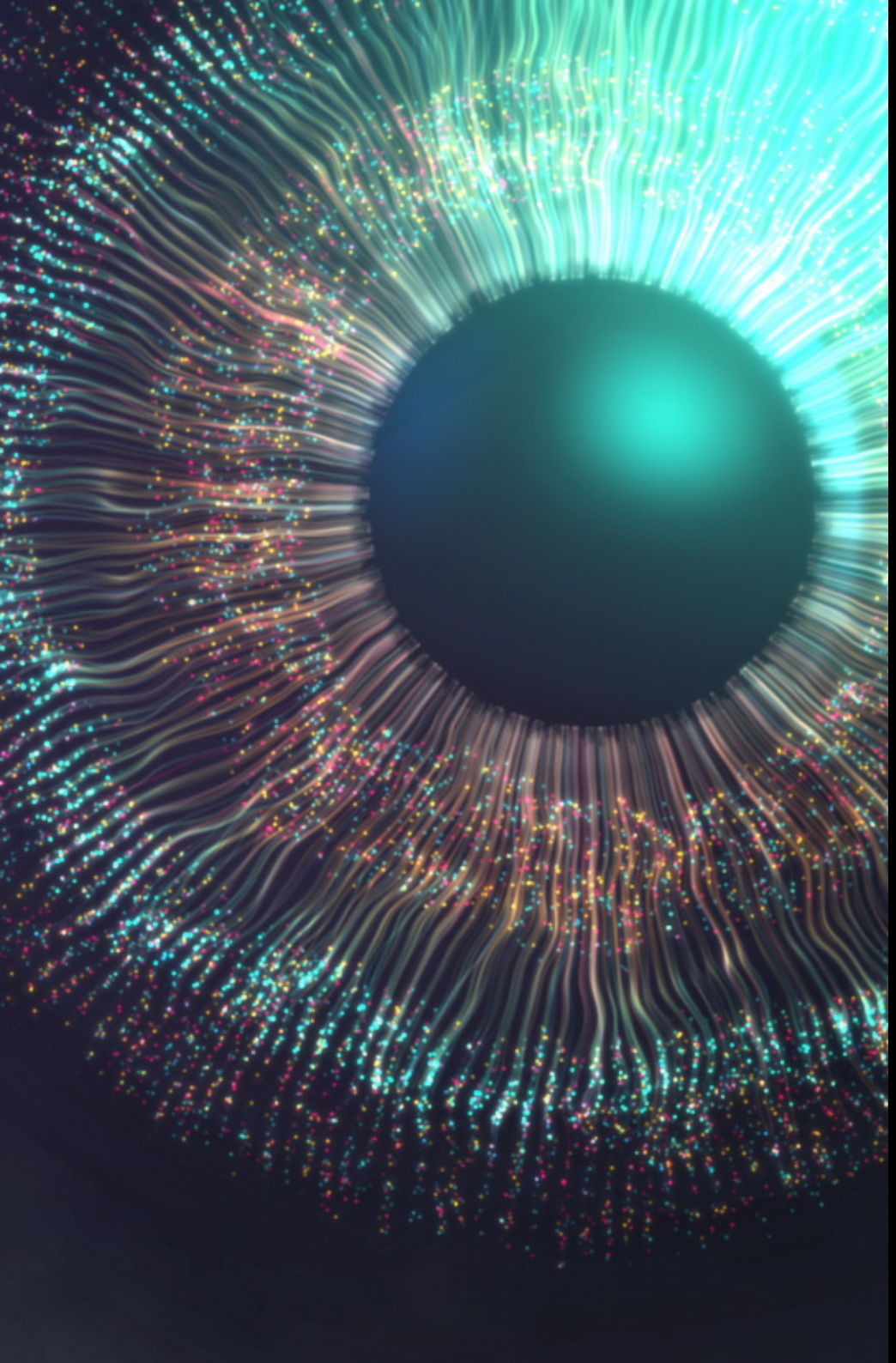
安全なWFA（Work From Anywhere）：
真のゼロトラストソリューションは、ネットワークやVPNをオンにする必要があるかどうかを心配することなく、あらゆる場所での安全かつシームレスな作業を可能にするものでなければなりません。

ユーザエクスペリエンスの最適化：
ゼロトラストで、従業員ごと、アプリケーションごとのユーザエクスペリエンスを把握できるようにすることで、一貫性ある優れたユーザエクスペリエンスの提供が可能になります。

ゼロトラストを成功に導く計画

インターネットが新しい企業ネットワークとなりつつ今、**ゼロトラストによって、ビジネスエコシステム全体での高速かつシームレスで安全なアクセスへの移行が可能になります。**

しかしながら、ゼロトラストセキュリティモデルの実装は、単にITの1つの機能ではなく、組織の従来の範囲を超えて、ビジネスのあらゆる領域に影響します。ゼロトラストの実装を成功させるには、**人、プロセス、テクノロジプラットフォームの課題を解決し、機会を活用するための詳細な戦略が必要です。**



ゼロトラストの基盤を作る

プラットフォーム

ゼロトラストは、アイデンティティやアプリケーションのセグメンテーションのような単なる1つのテクノロジではありません。**ゼロトラストは戦略であり、セキュリティエコシステムを構築するための基盤です。**ビジネスポリシーを使用し、インターネット経由でユーザをアプリケーションに安全に接続します。そして、その中心にあるのが、以下の3つの重要な要素に支えられるゼロトラストテクノロジプラットフォームです。

1. アイデンティティと**ポリシーに基づいて接続する**
2. アプリケーションを**見えなくする**
3. **ポリシーベースのアーキテクチャで**アプリを接続し、トラフィックをインスペクションする

ゼロトラストの基盤を作る

プラットフォーム

1 アイデンティティとコンテキストに基づく接続

従来型のVPNとファイアウォールは、ユーザをオンネットワークにすることで、アプリケーションにアクセスできるようにします。オンネットワークになることでユーザにトラストが付与されるため、脅威や攻撃の水平移動のリスクが大きくなります。ゼロトラストでは、コンテキストに基づくアイデンティとポリシーを使用することで、きめ細かいアクセスポリシーとセキュリティポリシーに基づいて認証されたユーザを許可されたアプリケーションに安全に接続し、ユーザをオンネットワークにすることはありません。アクセスを制限することで、水平移動を防止し、ビジネスリスクを軽減します。さらには、ネットワークリソースをインターネットに公開する必要がないため、DDoS攻撃や標的型攻撃からの保護が可能になります。

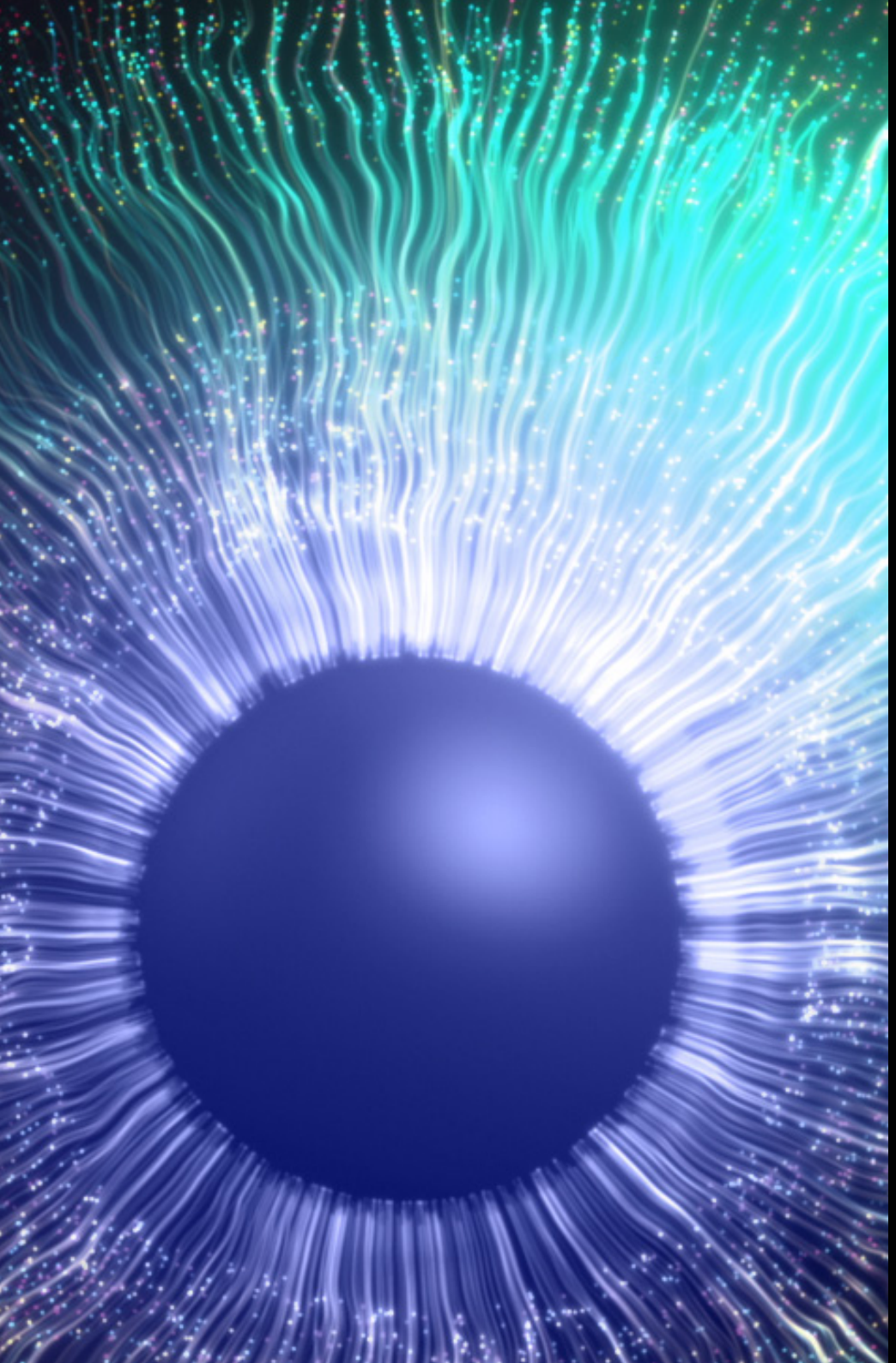
2 アプリケーションを見える場所に置かない

アプリケーションをクラウドに移行すると、攻撃対象領域が大幅に拡大します。従来型のファイアウォールでは、アプリがインターネットに公開されるため、ユーザだけでなく、ハッカーも簡単に見つけることができます。ゼロトラストアプローチでは、送信元のアイデンティティを隠し、IPアドレスを難読化することで、企業ネットワークをインターネットに公開しないようにします。アプリが攻撃者から見えなくなり、許可されたユーザのみがアクセスできるようにすることで、攻撃対象領域が縮小し、インターネット、SaaS、パブリッククラウド、プライベートクラウドのアプリケーションへの安全なアクセスが可能になります。

3 ポリシーベースでアプリを接続、トラフィックをインスペクションする

次世代ファイアウォールでの暗号化されたトラフィックのインスペクションは、容易なことではありません。多くの組織が暗号化されたトラフィックのインスペクションを回避し、結果、サイバー脅威とデータ損失のリスクが高くなっています。さらに、ファイアウォールは「パススルー」アプローチを採用しているため、分析が完了する前に未知のコンテンツが送信先に到達します。脅威が検知されるとアラートが送信されますが、間に合わない可能性があります。効果的な脅威保護と包括的なデータ損失防止を実現するには、送信先に到着する前にSSLセッションをインスペクションし、トランザクションのコンテンツを分析し、リアルタイムのポリシーとセキュリティを判断するプロキシアーキテクチャが必要です。さらには、パフォーマンスを低下させることなく、あらゆる場所から接続するユーザを保護する、スケーラブルな機能が必要です。

推奨されるアクション：Zscaler Zero Trust Exchange™のようなゼロトラストプラットフォームを評価する



カルチャーの転換を促す

人の力

ゼロトラストの採用を成功させるには、適切なプラットフォームが大前提ではありますが、新しいスキルを開発し、新しい文化の考え方を採用する必要もあります。迅速かつ安全にトランスフォーメーションを進める必要があるITリーダーから、ゼロトラストを導入するIT担当者、経営陣、エンドユーザ、広範なエコシステムまでの全員の協力がなければ、成し遂げられません。

カルチャーの転換を促す

人の力

ITリーダー

ITリーダーには、イノベーターであり、ストラテジストでもあることが求められます。 ゼロトラストを進める過程で、ビジネスとITの優先順位を調整し、サイロを解消し、適切なテクノロジとアーキテクチャを適用することで、トランスフォーメーションを推進し、ビジネスに必要な成果を達成する必要があります。 ゼロトラストを進めるにあたっては、以下が必要になります。

- **トランスフォーメーションに対する同業他社のベストプラクティス**や戦略を理解し、社内を組織してそれらの変更を実装する
- **IT担当者が ネットワーク中心アーキテクチャからゼロトラストアーキテクチャへの移行を成功させるために**必要なスキルや知識の育成を支援する
- ゼロトラストをエンドユーザに**見えない ようにする**

推奨されるアクション:
Zero Trust REvolutionariesなどのフォーラムに参加し、ゼロトラストやデジタルトランスフォーメーションのベストプラクティスに関する意見を交換する

カルチャーの転換を促す

人の力

IT担当者

企業のITチームは、ネットワークとセキュリティのエキスパートであり、ハードウェアに関する知識があり、30年以上にわたってITネットワークとセキュリティの原則に基づいてポリシーを設定してきました。IT担当者は、ゼロトラストへの移行の**影響を直接受けることになります。**これまでのスキルの多くを刷新し、デジタルトランスフォーメーションに必要な新しいスキルを習得する必要がありますが、組織はさらに多くの影響を受けることになり、将来に向けての価値ある知識の習得を継続していくことになります。

成功の鍵となるのは、ゼロトラストへと移行するための**高度なトレーニングをIT担当者に提供し、**新しいビジネスプロセス、ゼロトラストサービスを使用するためのベストプラクティスや手順を理解してもらうことです。同時に、ゼロトラストがいかに**時間の節約**につながり、組織により大きな**価値をもたらすか**を説明することもできるでしょう。

推奨されるアクション：
Zscaler Zero Trust Academyの認定トレーニングプログラムを活用して、ゼロトラストへの移行を加速させる方法をIT担当者が習得するよう支援する

カルチャーの転換を促す

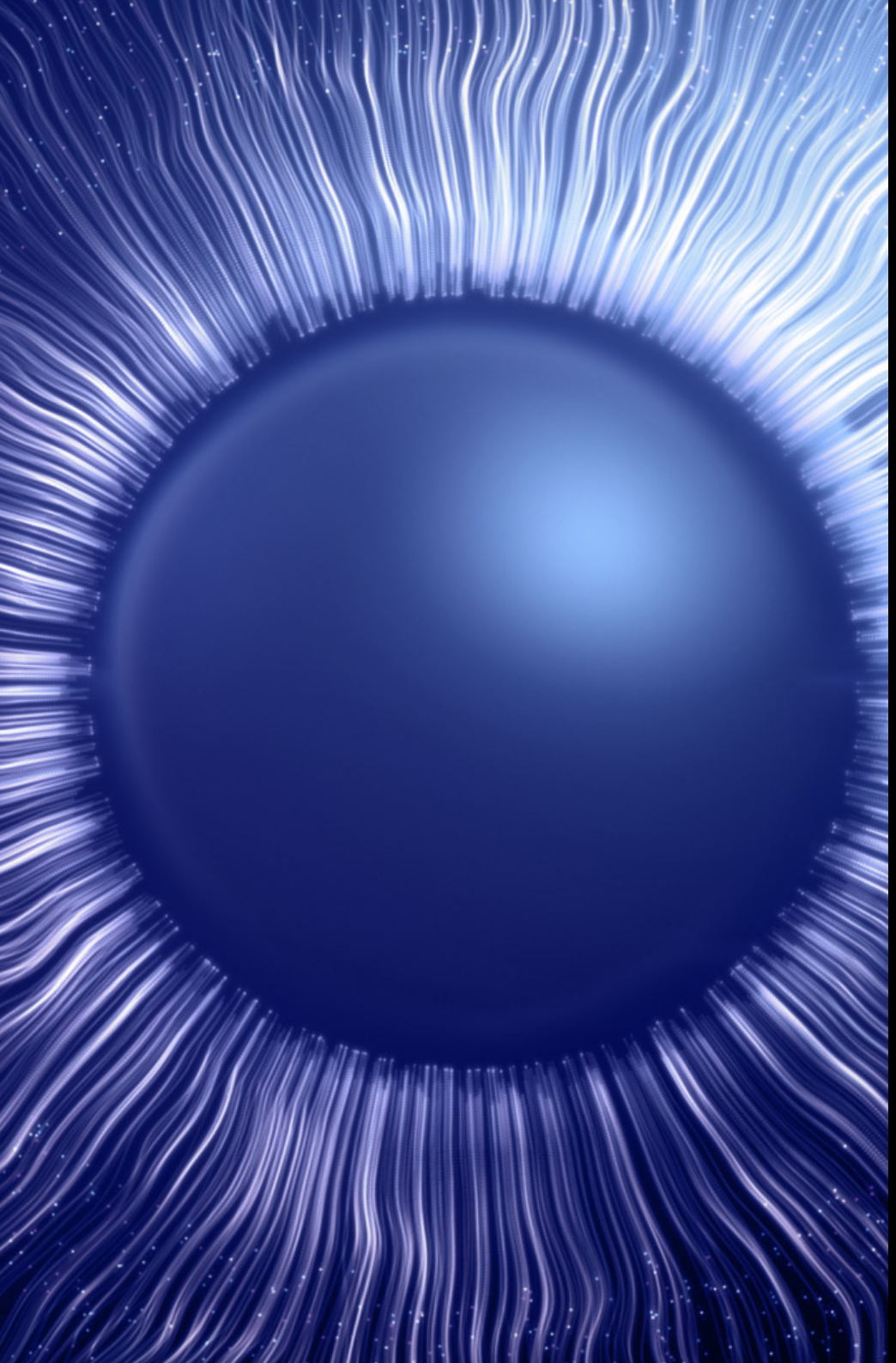
人の力

ユーザ

ゼロトラストは、正しく導入できれば、エンドユーザにとって目に見えないイネーブラとなり、場所やデバイスの制限なく、従業員が働けるようになります。ゼロトラストアクセスは常にアイデンティティとビジネスポリシーが基づいて提供され、クラウドサービスは最速のアクセスパス経由でユーザをアプリケーションに自動的に接続するため、ユーザの物理的な場所は関係なくなります。オフィス、自宅、あるいはそれ以外の場所で働く場合も、**一貫性ある高速のユーザエクスペリエンス**が実現します。

また、堅牢なゼロトラストソリューションにより、**ユーザのアプリケーションアクセスをブロックすることなく、リスクを大幅に軽減**できます。例えば、クラウドブラウザ分離テクノロジは、Webページを分離された環境でレンダリングされたピクセルとして配信することで、ユーザエクスペリエンスに影響を与えることなく、アクティブコンテンツへの安全なアクセスを可能にし、データのコピー&ペーストを制限する、ファイルのダウンロードを防止する、ダウンロード先を隔離されたコンテナ内に限定するといった方法により、ランサムウェアなどの巧妙な脅威からのエンドポイントデバイスの保護を可能にします。ゼロトラストはこれらの方法でテクノロジを活用することで状況に応じてリスクを軽減します。

推奨されるアクション：
優れたユーザエクスペリエンスを
可能にするツールを提供する、
Zscaler Digital Experienceのような
ゼロトラストアーキテクチャを活用する



プログラムによるパス

プロセス

ゼロトラストを実現し、ビジネストランスフォーメーションを加速させるための手順とは、どのようなものなのでしょうか。何から始めるべきかの判断は、最も難しいことのように思えるかもしれませんが、ゼロトラストをプラットフォームから始め、**データ、人、デバイス、ワークロードへと拡張していくことが重要です。**

そのためには、アイデンティティプロバイダ、エンドポイントセキュリティソリューション、SIEMソリューションと製品の強力な統合が、ゼロトラストにおいてコンテキストを追加し、採用を簡素化する上での不可欠な要素となります。

プログラムによるパス

プロセス

統合の必要性を考慮し、**以下のツールを提供するゼロトラストプラットフォームとテクノロジパートナーエコシステムを選定することで、**設計を明確にし、ゼロトラストの採用を推進することができます。

- **ソリューションブループリント - ユースケースの**リファレンスアーキテクチャの提供
- **設計ガイドライン - 設計原則と**統合のベストプラクティスの共有
- **導入ガイド** - PoV（価値実証）と本番環境の導入に向けて統合を進める際の構成ガイダンスの提供

適切なブループリントによって、ホリスティックゼロトラストソリューションの実装がはるかに容易になります。特定のユースケースを想定して設計された共同検証済みのリファレンスアーキテクチャと、ベストプラクティスに基づいてそれらのプラットフォームを併せて使用するためのセキュリティアーキテクト向けの規範的設計ガイダンスを提供してくれるベンダを選択します。

このようなガイダンスによって、導入が簡素化され、効率的な運用と最高のユーザエクスペリエンスが保証され、最適なセキュリティの適用を可能にする、構造化されたフレームワークが提供されます。これらすべてによって、組織におけるゼロトラストの採用が加速します。

推奨されるアクション：パートナーとの密接な統合を可能にするソリューションを活用し、ゼットスケーラーのエコシステムのような、検証済みの設計やブループリントを提供するソリューションを選択する

ゼロトラストのメリットを手に入れる

デジタルトランスフォーメーションは、企業の俊敏性と効率性の向上を可能にしますが、そのためには、ネットワークとセキュリティのアーキテクチャの見直しが必要です。ゼロトラストは、**クラウドファーストの企業のデジタルトランスフォーメーションを加速させ、従業員がどこでも生産的かつ安全に働けるようにするための基盤**となりますが、そのためには、何よりも先に、適切なプラットフォーム、人、プロセスが組み込まれた戦略を策定することが重要です。

アイデンティとビジネスポリシーを使用してトラストを確立し、ユーザをオンネットワークにすることなくリソースに接続するプラットフォームを選択します。アプリケーションを攻撃者から見えないようにし、許可されたユーザのみがアクセスできるようにすることで、アプリケーションを保護します。さらには、パススルーファイアウォールではなくプロキシアーキテクチャを採用して、データを保護し、サイバー脅威からの効果的な保護が保証されるようにします。

同業他社から、トランスフォーメーションのベストプラクティスと戦略を学び、新しい文化を育成し、ゼロトラストアーキテクチャの実装と管理に必要なスキルを習得し、エンドユーザに見えない、シームレスなゼロトラストの実現を目指します。正しいブループリントがあれば、これらはすべてが容易になります。**パートナーとの堅牢な統合が可能なゼロトラストプラットフォームを活用することで、共同で検証されたリファレンスアーキテクチャやこれらのプラットフォームを**併せて利用する際の規範となる設計ガイダンスも提供されます。

これらの要素を考慮することで、**ゼロトラストのメリットを手に入れてデジタルトランスフォーメーションを加速させ、ITを真のビジネスイネーブラにすることができます。**

真のゼロトラストプラットフォームの無限に広がるメリットをぜひ体感してください。

ゼロトラストへの取り組みを開始する

zscaler™