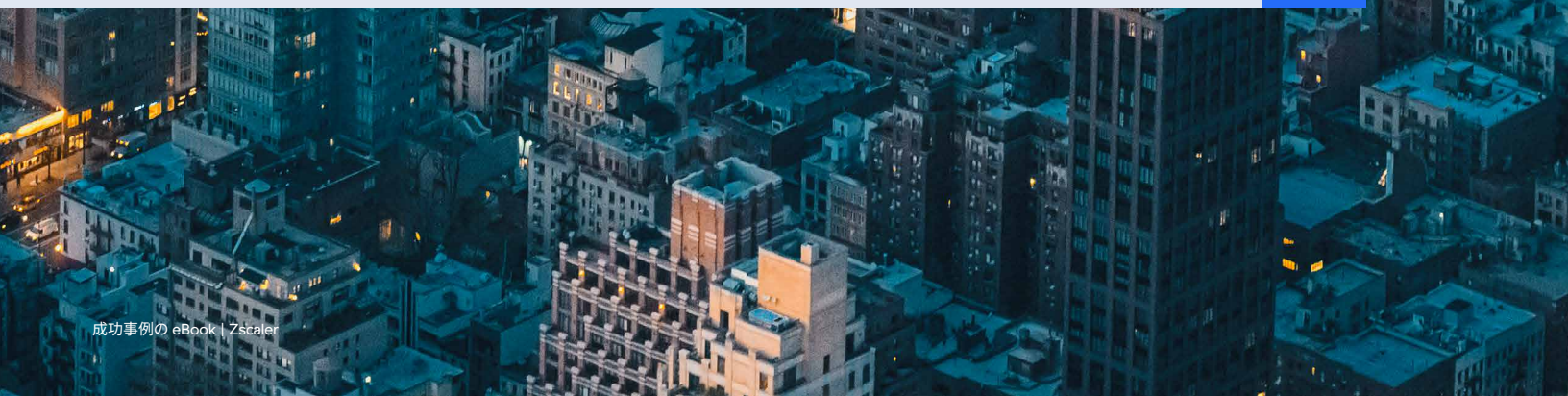
お客様の導入事例

Zscaler のゼロトラストと AI を活用した
トランスフォーメーションの事例

ゼロトラストと AI を活用する組織がどのようにセキュリティ態勢を改善し、優れたユーザー エクスペリエンスを促進しながら、M&A を簡素化したのかをご覧ください。

お客様第一主義は Zscaler のコア バリューの 1 つです。Zscaler は、最高のゼロトラスト イノベーションを提供することで、お客様が目標を達成できるようサポートします。世界中の 5,000 社以上のお客様が、AI を活用する Zero Trust Exchange プラットフォームの主な機能を活用して、コストと複雑さの軽減、ネットワーク アーキテクチャーの簡素化、ユーザーの保護、進化するサイバー脅威からの防御を実現してきました。この eBook では、世界で最も成功しているお客様の導入事例に焦点を当て、Zscaler のソリューションでネットワーク、セキュリティ、業務を変革する方法を詳しく解説します。



Zscaler は、15 年以上にわたってゼロトラストを牽引しており、現在もあらゆる規模や業界のお客様がゼロトラストの目標を達成し、それ以上の成果を出せるようにサポートしています。テクノロジーの世界においては常に「変化」が求められます。Zscaler の Zero Trust Exchange プラットフォームを導入すれば、IT インフラを継続的に改善し、イノベーションを推進しながら、あらゆる事態に対処できるようになります。

Mike Rich
CRO 兼グローバル セールス責任者

目次

業種ごとの
導入事例

AMS

地域ごとの導入事例

Zscaler Zero Trust Exchang で世界中のユーザーとデータを保護する AMN Healthcare

5,000 人以上のユーザーに安全なリモート ワーク エクスペリエンスを提供し、医療業界を狙うサイバー脅威の増加から患者データを保護

AMN Healthcare の概要

患者の転帰を改善する医療従事者向けソリューションを提供

医療 / 製薬

米国、テキサス州
ダラス

24 の拠点に
10,000 人以上の顧客

12 億

1 か月あたりに処理される Web トランザクションの数

700 万

3 か月でブロックされた脅威の数

数時間

あらゆる場所への安全なエッジの展開に要した時間

課題

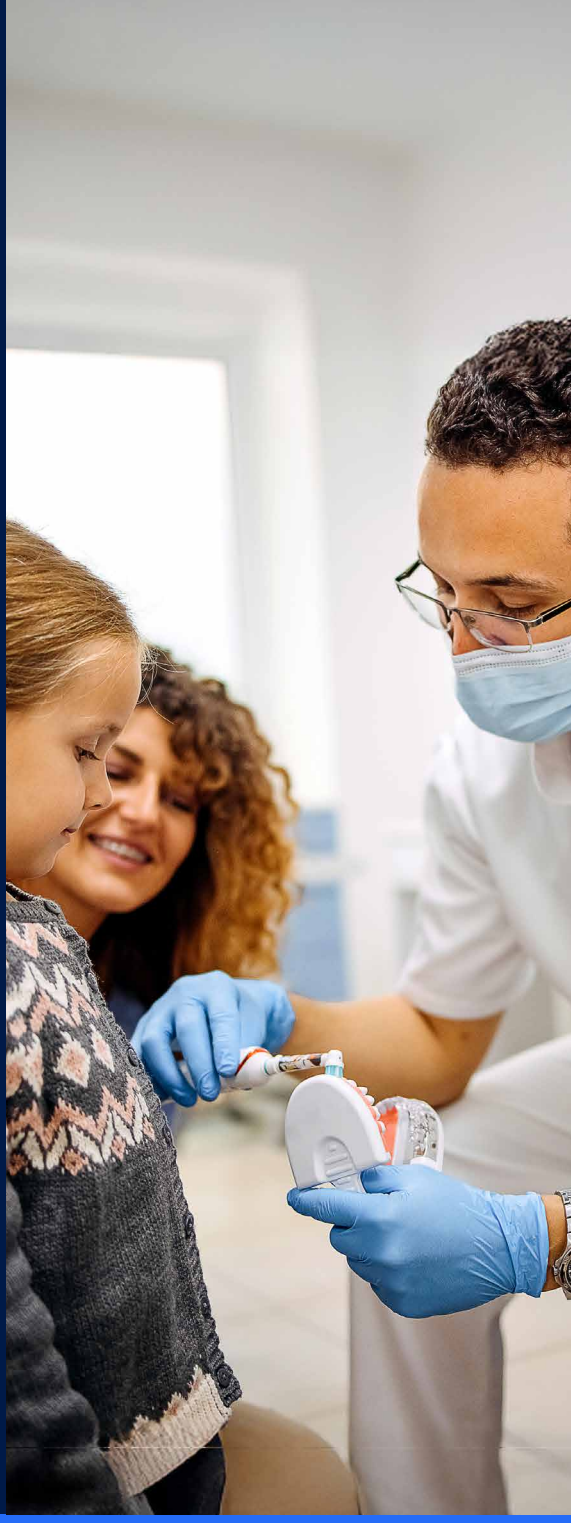
- 従来のセキュリティ インフラでは、進化を続けるクラウドファーストの運用エコシステムに対応不能
- 従来の VPN では、高まるリモート アクセスのニーズに対応できず、サイバー脅威に対するプライベート リソースの脆弱性が悪化
- 複数のポイント ソリューションを備えた複雑なセキュリティ アーキテクチャーでは、問題の可視化と解決の管理が困難

取り組みの各ステップ

1. **インターネットへの安全な直接接続のプロビジョニング：**世界中に分散した従業員が場所を問わず柔軟に作業できる環境を確立
2. **マイクロセグメント化されたプライベート アプリケーションへのゼロトラスト アクセスの展開：**従来の VPN に代わる安全なソリューションを提供
3. **モニタリング スタックの合理化およびエンドツーエンドの包括的な可視性の活用：**ユーザーの問題を早期に改善

成果

- **5,000 人以上のユーザーのアウトバウンドとインバウンド接続の保護：**世界中でリモート ワークの質と効率を向上
- **プライベート アプリケーションやデジタル製品へのゼロトラスト アクセス ポリシーの施行：**世界中の 10,000 人以上の顧客を保護
- **アーキテクチャーの簡素化および技術コストの削減：**管理負荷を抑えながら、セキュリティ態勢を強化



Zscaler のアプローチと当社のゼロトラストの理念は一致しており、Zero Trust Exchange プラットフォームは、AMN Healthcare が求めるゼロトラスト アーキテクチャーをまさに具現化したものでした。

Mani Masood 氏
AMN Healthcare、
情報セキュリティ責任者

成功事例を読む

Zscaler Zero Trust Exchange で業務の安全性と効率性を向上させた ATN International

2,500 人以上の従業員のリモート ワーク体制を強化し、VPN 関連のユーザーの問題を解消しながら、M&A に伴う統合とオンボーディングをより安全に促進

ATN International の概要

専門知識を活用し、遠隔地またはアクセスが困難な地域に通信インフラとサービスを提供

電気通信

米国、マサチューセッツ州ビバリー

世界中に 750,000 人の顧客

100%

VPN と VPN 関連のチケットの削減率

すべて

Zscaler で保護された従業員の数

数分

ユーザーの問題解決に要する時間 (以前は数時間)

課題

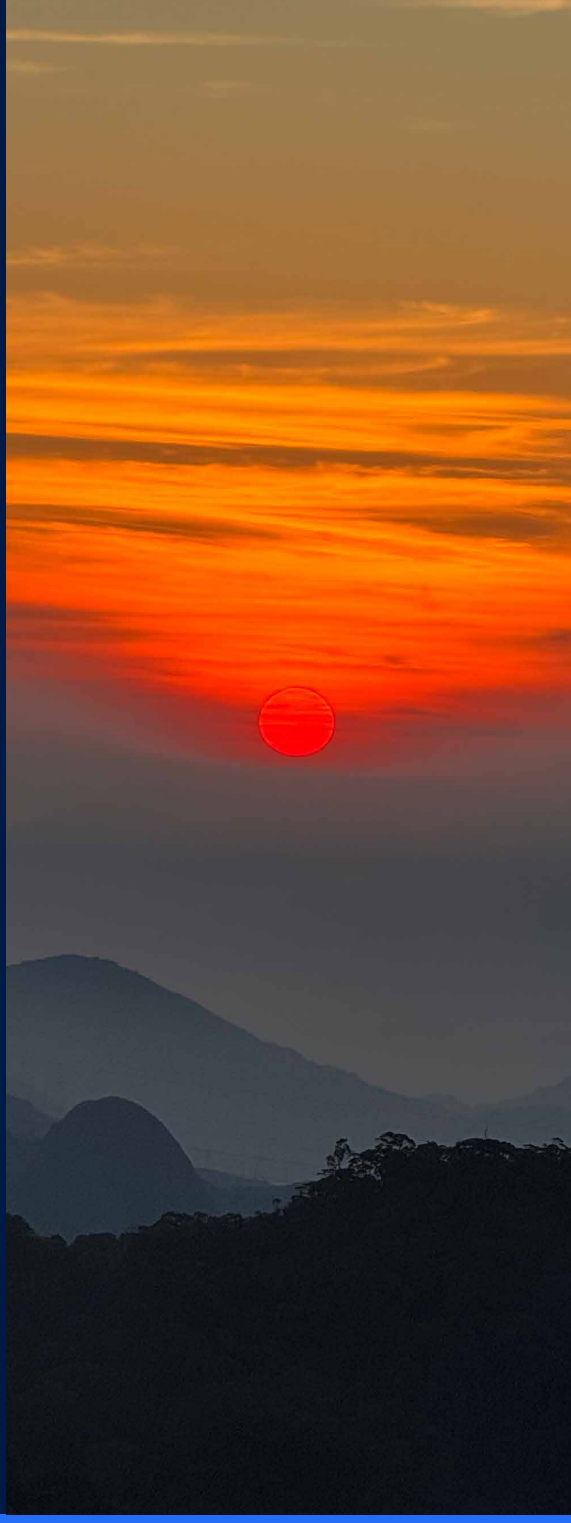
- オンプレミスのセキュリティ インフラでは、クラウドファーストの業務や将来の M&A の目標への効率的な対応が不可能
- 従来の VPN アプライアンスは拡張性に乏しいため、急増するリモート ワークに対処できず、ユーザー エクスペリエンスの低下やリスクの増加を誘発
- 従来のセキュリティ ソリューションでは、ユーザーの問題を事前予防的に軽減するための重要なクラウド統合が不可能

取り組みの各ステップ

1. **インターネットへの直接接続の提供：**トラフィック検査とログ機能を活用することで、ポリシー違反を防止
2. **VPN から最小特権のゼロトラスト アクセスへの移行：**プライベート アプリケーションやリソースへの接続に最小特権アクセスを適用
3. **AI を活用した Zscaler の機能と Microsoft との緊密な統合：**ユーザーの問題を迅速に特定して解決

成果

- **2,500 人以上のユーザーのリモート ワーク エクスペリエンスの改善：**VPN 関連のユーザーの問題を解消し、サービス チケットを 100% 削減
- **M&A にかかる期間の短縮および買収した組織のより安全なオンボーディング：**ゼロトラスト セキュリティ アーキテクチャーで可能に
- **問題の特定と解決に必要な時間をわずか数分にまで短縮：**レポートとモニタリングの堅牢な機能で達成



私がインフラ ツールとセキュリティ ツールの両方に求めていたのは、業務効率を高め、セキュリティを強化する機能です。Zscaler は、このどちらも満たしています。

Richard Casselberry 氏
ATN International、IT セキュリティ、アーキテクチャーおよびコンプライアンス担当 VP

成功事例を読む

Zscaler Zero Trust Exchange でゼロトラストを段階的に展開した Cox Automotive

セキュリティ アーキテクチャーを合理化し、5 大陸にわたるユーザーに安全な接続を提供しながら、オンラインで自動車を購入した何百万人もの顧客のデータを保護

Cox Automotive の概要

自動車サービスとテクノロジーの世界最大のプロバイダー

小売 / 卸売

米国、ジョージア州アトランタ

年間 23 億件のオンライン取引

3 万 +
保護された従業員の数

4 万
サポートされた自動車ディーラーの数

1
複雑さを軽減するプラットフォームの数

課題

- 包括的なゼロトラスト セキュリティ アーキテクチャーの基盤として機能する、クラウドに適したプラットフォームを導入
- 従来のファイアウォール アプライアンスでは、世界中に分散したユーザー グループのインターネット トラフィックを大規模に検査することが不可能
- 従来の VPN では、アイデンティティーベースのアクセス制御ポリシーに対応できないため、プライベート アプリケーションとデータのリスクが増加

取り組みの各ステップ

1. **クラウド ネイティブのマルチテナント ゼロトラスト プラットフォームの展開：**他のクラウド ソリューションとも簡単に統合可能
2. **インターネットと SaaS アプリへの安全な直接接続のプロビジョニング：**インライン トラフィック検査機能を活用
3. **VPN からゼロトラスト アクセスへの移行：**マイクロセグメント化された最小特権セキュリティ ポリシーをプライベート アプリへのアクセスに施行

成果

- **5 大陸にまたがる部門の保護：**場所を問わず働ける柔軟性を提供し、ユーザー エクスペリエンスを改善
- **重要なプライベート アプリとリソースの保護：**より費用対効果の高い方法で、数百万人の顧客に関するデータなどを保護
- **ファイアウォールや VPN など従来のセキュリティ ソリューションの廃止：**IT プロセスを合理化し、M&A のオンボーディングを加速

ユーザーのデバイスにエージェントをインストールすれば、Zscaler の他の機能を当社のアーキテクチャーに簡単に統合できるようになります。スイッチを「オン」にするだけで良いのです。

Jon Mahes 氏
Cox Automotive、サイバーセキュリティ担当シニア マネージャー

成功事例を読む

Zscaler Zero Trust Exchange でセキュリティを統合したコロンビア特別区政府

従来の VPN アプライアンスをリプレースすることで、セキュリティ アーキテクチャーを合理化し、リスクをリアルタイムで正確に把握しながら、15,000 人のユーザーを保護

ワシントン D.C. 政府の概要

コロンビア特別区の住民向けの重要なサービスの監督と管理を実施

公共機関

米国、
ワシントン D.C.

15,000 人以上
の職員

1.5 万
保護された
政府職員の数

～ 30 億
1 か月あたりに
処理される
トランザクションの数

20 万 +
1 か月あたりに
ブロックされる
セキュリティ脅威の数

課題

- 旧式のセキュリティ インフラではリモート ワークに対処できず、業務の非効率化が発生
- 従来の VPN アプライアンスは、組織のネットワークをエンド ユーザーのデバイスにまで拡張するため、機密データの侵害リスクが増大
- 従来のセキュリティ ポイント製品では脅威がすべて可視化されないため、リスクの評価と軽減が複雑化

取り組みの各ステップ

1. **インターネットと SaaS アプリケーションへの安全な直接接続の提供：**場所を問わず作業できる柔軟な環境を確保
2. **従来の VPN からマイクロセグメント化されたゼロトラスト アクセスへの移行：**プライベート リソースに一貫したセキュリティ ポリシーを施行
3. **AI を活用したデータとインサイトによるリスクの詳細な可視化：**潜在的な脅威をリアルタイムで大規模に軽減

成果

- **ゼロトラスト アーキテクチャーによるセキュリティ態勢の強化：**1 か月あたり最大 30 億件のトランザクションを処理し、20 万件以上の脅威をブロック
- **15,000 人のリモート ユーザー エクスペリエンスの改善：**既存のアイデンティティー ソリューションとシームレスに統合
- **リスク管理に対する取り組みの強化：**リスク要因とセキュリティ態勢に関するより詳細なインサイトを活用

Zscaler とのパートナーシップは当社にとって大変貴重なものであり、プラットフォームの迅速な導入、ユーザーの効率的なオンボーディング、従業員やユーザーの全体的なエクスペリエンスの向上をすべて実現できました。

Suneel Cherukuri 氏
ワシントン D.C. 政府、CISO

成功事例を読む

BYOD の大規模な実装、データ保護の改善、大幅なコスト削減を実現した DMI

全従業員にゼロトラスト接続を提供し、従業員が自分のデバイスからでも安全に作業できる環境を構築

DMI の概要

公共部門と民間部門の両方で事業を展開するデジタル サービスの世界的プロバイダー

ハイテク

米国、バージニア州マクリーン

80 か国に 2,100 人以上の従業員

70 万ドル +
年間のコスト削減額

2 未満
展開に要した週数

3%
展開後の SLA 解決の加速度

課題

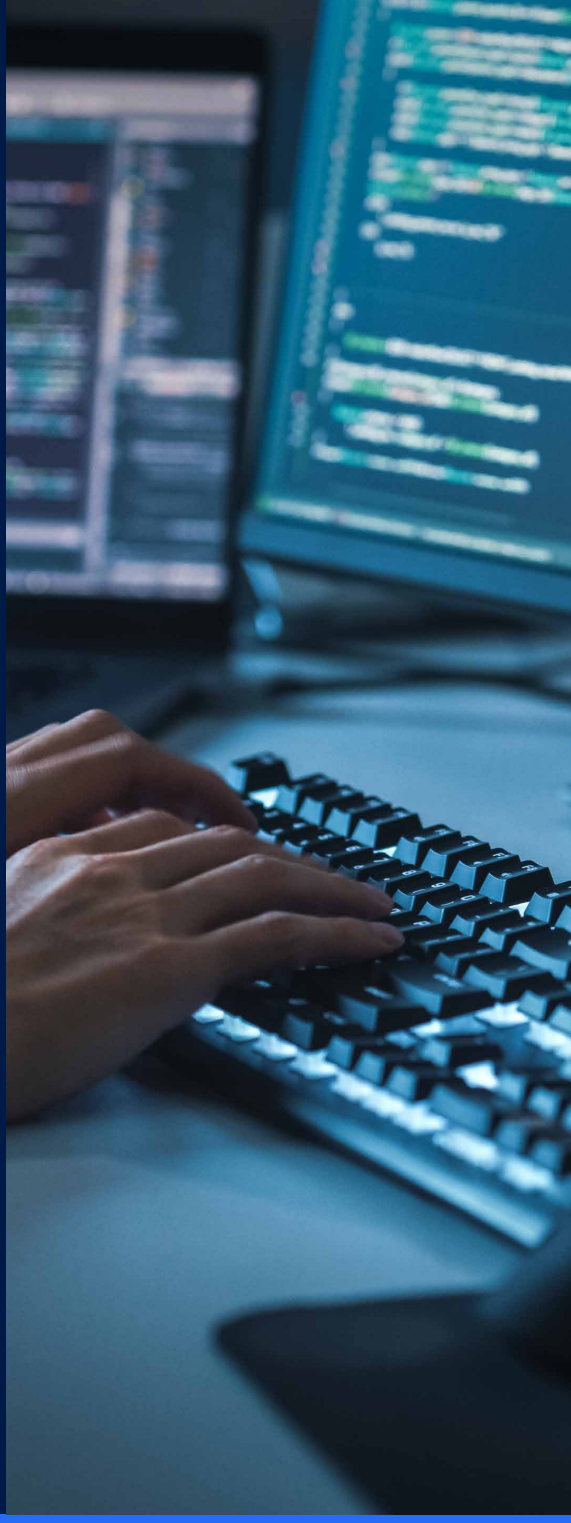
- 新しいハードウェアを従来の環境にインストールすると、ダウンタイムと停止期間が発生し、定期的な更新が必要に
- DMI のデバイスでの作業を義務付けると、従業員の生産性が低下し、二酸化炭素排出量へのグローバルな取り組みに悪影響が発生

取り組みの各ステップ

1. **インターネットへの安全なアクセスと真のゼロトラスト接続の確保：**時間のかかる手動でのデバイス設定を必要とすることなく、従業員、請負業者、サードパーティーに安全なアクセスと接続を提供
2. **ブラウザー分離を活用した BYOD プロジェクトの推進：**従業員が自分のデバイスで作業できる環境を確保

成果

- **ゼロトラストを 2 週間以内に展開：**ユーザーへの影響やダウンタイムはゼロ
- **年間 700,000 ドルの節約：**オンボーディングとオフボーディングのエクスペリエンスを向上させ、新しいオフィスとデバイスの設定時間を短縮



従業員全員にノートパソコンを購入する代わりに、従業員が個人のデバイスを仕事に使用できるようにする BYOD プロジェクトを安全に進められたことで、年間 700,000 ドル以上ものコストを削減できました。

Mauricio Mendoza 氏
DMI、グローバル IT およびセキュリティ担当バイス プレジデント

成功事例を読む

AI を活用したセグメンテーションで世界中の業務を保護した Eaton

高度な脅威対策、侵害リスクの軽減、パートナーとの統合による可視性の向上を可能にし、クラウド移行を実現

Eaton の概要

航空宇宙などの業界向けの世界的な電気機器メーカー

製造

米国、オハイオ
州クリーブランド

170 か国に 90,000 人以上の
従業員とユーザー

400 万

1 か月あたりに
ブロックされる脅威の数

9 万

ゼロトラストでインターネット
やプライベート アプリに接続
する世界中の従業員の数

多数

シームレスに統合した
戦略的アライアンス
パートナーの数

課題

- 従来の VPN とファイアウォールは組織の成長を妨げるほか、パンデミック中およびそれ以降に 30,000 人以上の工場従業員への対応が不可能
- 従来の境界型セキュリティ アーキテクチャーでは、クラウドファースト戦略やセグメンテーションのニーズに対応することが困難
- 不十分な可視性によって脅威検出が制限されるため、修復までの時間が長期化

取り組みの各ステップ

1. **セキュリティのリプレース:**セキュリティ ツールとアクセス ツールをリプレースし、インターネットとプライベート アプリへのゼロトラスト接続を確保
2. **AI イノベーションの採用：**AI を悪用する脅威を検出して対処すると同時に、製造拠点にセグメンテーションを実装
3. **攻撃に対する意識向上：**予防型かつ予測的な侵害の検知と対応を実施

成果

- **より安全で信頼性が高く、調整されたユーザー エクスペリエンスの確保：**従業員とサードパーティーの両方に提供
- **AI による効率的な脅威検出：**その他にも情報漏洩防止、修復、ChatGPT の使用状況の可視化、アプリケーション セグメンテーションにも AI を活用
- **アクセス制御の強化：**ゼロトラスト セグメンテーションおよび EDR、CDR、NDR のツールと統合

Zscaler は使いやすく、その機能は 1 つのエンドポイント エージェントに組み込まれています。Zscaler を世界中の環境にすばやく展開し、自社側のリソースをほとんど必要とすることなく、機能を拡張できました。

Jason Koler 氏
Eaton Corporation、CISO

成功事例を読む

何百万もの脅威をブロックしながら M&A に伴う統合を加速し、所要期間を数か月から数日にまで短縮した Guaranteed Rate

セキュリティ ハードウェアの廃止、優れたレジリエンスの確保、常時オンのセキュリティ、攻撃対象領域の削減を Zscaler で実現

Guaranteed Rate の概要

全米 50 州で 500 以上の支店を運営する、米国第 2 位の規模の小売住宅ローン融資企業

金融サービス / 保険

米国、イリノイ州シカゴ

6,000 人以上の従業員

97%
検査された暗号化トラフィックの数

250 万
3 か月でブロックされた脅威の数

2 ～ 3 倍
アプリへのアクセスの速度

課題

- VPN 経由でオンプレミスや AWS の多数のプライベート アプリに接続するため、攻撃対象領域が拡大
- 500 以上の支店からのトラフィックをデータ センターにバックホールする必要があるため、パフォーマンスと生産性が低下
- 従来のファイアウォールでは、インターネットからネットワークに侵入してラテラル ムーブメントを行うゼロデイ脅威の検出が不可能

取り組みの各ステップ

1. **インターネットと SaaS へのアクセスの保護：**クラウド経由のアクセスで、500 以上の支店からのトラフィックのバックホールを排除
2. **VPN のリプレース：**データ センターとクラウドの 500 以上のプライベート アプリへの高速かつ安全なアクセスを提供
3. **ユーザー エクスペリエンスの最適化：**パフォーマンスの問題をより迅速かつ効率的に特定して解決

成果

- **攻撃対象領域の最小化：**ユーザーが最小特権の原則に基づいて直接接続できるようにしながら、検知と対応を強化
- **不正侵入のリスクの軽減：**インラインの TLS/SSL トラフィック モニタリングと AI を活用した高度な脅威対策で実現
- **ラテラル ムーブメントの防止：**デセプション テクノロジーを活用して、攻撃者を機密性の高いリソースから遠ざけ、脅威をリアルタイムで封じ込めることで環境全体を保護

Risk360 でサイバー リスクの死角を可視化できるため、時間を割くべき課題により集中できます。そのため、最も差し迫ったサイバー リスクに対処し、軽減できるようになりました。

Darin Hurd 氏
Guaranteed Rate、CISO

成功事例を読む

クラウド ネイティブ ゼロトラスト アーキテクチャーで 自社の取り組みを強化する MGM Resorts International

ゼロトラスト セグメンテーション、情報漏洩防止、ビジネス全体にわたる実用的かつ高度なインサイトを活用しながら、短期間での価値実現を達成

MGM Resorts International の概要

31 のリゾート地に展開するゲーミング、エンターテイメント、宿泊業の大手

エンターテインメント / 宿泊および飲食サービス

米国、ネバダ州ラスベガス

世界 70,000 人の従業員

初日
プラットフォームの価値の発揮

27.5 万
1 か月あたりにブロックされる脅威の数

50%
従業員のデバイスの利用効率の向上

課題

- 城と堀のセキュリティ環境でユーザーにネットワークへの広範なアクセスを許可することでラテラル ムーブメントのリスクが増大
- 従来の VPN ゲートウェイによってトラフィックにボトルネックが発生し、ユーザー エクスペリエンスが低下
- ユーザー ベース全体のブラウジング アクティビティーについて、従来のセキュリティ ツールから得られるインサイトが限定的

取り組みの各ステップ

1. **VPN のリプレースとゼロトラスト セグメンテーションの実装：**全従業員の環境に適用
2. **プライベート アクセス ソリューションの迅速な展開：**さらにデジタル エクスペリエンス管理やデータ保護ソリューションも導入
3. **デセプション テクノロジーの採用：**活動中の攻撃者による不正侵入を防止

成果

- **従業員のエクスペリエンス向上：**環境全体でパフォーマンス強化や接続の高速化を実現
- **新たな脅威に対応：**包括的な DLP、プライベート アクセス、ゼロトラスト セグメンテーションで防御
- **全社的なセキュリティ態勢の強化：**クラウドファーストのアプローチによってビジネスの迅速化も支援

全社でのゼロトラスト セグメンテーションをごく短期間で実現できました。情報漏洩防止やアプリケーションに関するインサイトの管理など、日常的な作業も簡単に行えています。

Stephen Harrison 氏
MGM Resorts International、CISO

成功事例を読む

Zscaler Zero Trust Exchange でセキュリティと効率性を改善した Mercury Financial

Zscaler のシームレスな統合と AI 機能を活用して安全なリモート ワーク環境を確保し、機密性の高い財務データを脅威から保護

Mercury Financial の概要

金融上の信用の構築と管理を支援するノンバンクの金融サービス企業

- 金融サービス / 保険
- 米国、テキサス州オースティン
- 500 人以上の従業員

100%
シームレスなエクスペリエンスを得たリモート ワーカーの割合

76%
IT サポートチケットの減少率

ゼロ
マルウェアによるダウンタイム

課題

- 従来のセキュリティ ソリューションでは、完全なインライン トラフィック検査ができず、脅威の検知と防止が困難
- 従来の VPN は、分散した従業員が抱えるクラウドファーストのニーズを満たせず、ユーザー エクスペリエンスが低下
- ユーザーのアクティビティーとデバイス ポスチャーに関するデータが限られており、リモート ワーカーの問題の診断と解決が困難

取り組みの各ステップ

1. **インターネットへの安全な直接接続：**AI を活用した脅威の封じ込め機能でデータの侵害を阻止
2. **VPN からマイクロセグメント化されたゼロトラスト アクセスへの移行：**プライベート アプリへのリモート接続を制御し、安全性を確保
3. **主な統合とより堅牢なユーザーのインサイトの活用：**リスクを高めることなく、管理負荷を軽減

成果

- **攻撃対象領域の削減：**Zscaler の展開後は、マルウェアやランサムウェアによるダウンタイムがゼロに
- **ラテラル ムーブメントの制限と影響範囲の縮小：**脅威がセキュリティ スタックに侵入した場合、迅速に修復
- **AWS、CrowdStrike、Okta との統合によるセキュリティ インフラの合理化：**規制順守を強化

Zscaler はゼロトラストのあらゆる側面をカバーするため、この分野のリーダーといえるでしょう。Zscaler と同じ機能を他で利用しようとすると、複数のベンダー ソリューションが必要になります。

Arjun Thusu 氏
最高情報責任者
Mercury Financial

成功事例を読む

Zscaler Zero Trust Exchange で優れたユーザー エクスペリエンスを確保する Molson Coors

VPN アプライアンスの必要性を排除し、世界中の従業員の接続を保護しながら、問題解決を加速させるためのインサイトを入手

Molson Coors の概要

世界第 3 位の規模を誇るビール メーカーであり、飲料業界の世界的なイノベーター

食料品 / 飲料品 / たばこ

米国、イリノイ州シカゴ

17,000 人以上の従業員
42 以上の醸造所

1.7 万
ゼロトラストで保護されたユーザーの数

96%
ユーザーの問題解決までの時間の短縮率

数百万
1 日あたりにブロックされる脅威の数

課題

- ファイアウォール アプライアンスは、インターネットへのリモート アクセスの需要に合わせて拡張できず、インライン トラフィック検査が困難
- ユーザーのアクティビティーとデバイス ポスチャーを十分に可視化できないため、パフォーマンスの問題の特定と解決が困難
- VPN アプライアンスを利用する従来のセキュリティ アーキテクチャーでは、ネットワーク環境がフラットになり、攻撃対象領域が拡大

取り組みの各ステップ

1. **高度な脅威検出機能を備えたインターネットへの直接接続のプロビジョニング：**リモート ユーザーとサードパーティー ユーザーを保護
2. **ユーザーとデバイスのエンドツーエンドの可視性の活用：**セキュリティ管理を簡素化しながら、ユーザーの問題解決を加速
3. **プライベート アプリケーションへのアクセスを従来の VPN からゼロトラストにリプレース：**リソースを保護し、ユーザー エクスペリエンスを改善

成果

- **優れたユーザー エクスペリエンスの確保：**世界中の 42 の醸造所で働く従業員とサードパーティー パートナーに提供
- **ユーザーの問題解決にかかる平均時間の短縮：**根本原因を特定し、軽減アクションを自動化することで、解決までの時間を数時間から数分にまで短縮
- **高度な脅威のブロック：**ラテラル ムーブメントを排除することで、プライベート アプリケーションと機密性の高いデータのセキュリティを改善

Zscaler がブロックする脅威は日によって異なりますが、常に数十万から数百万に上ります。シンプルで使いやすく、すぐに習得できます。制限はありません。

Jeremy Bauer 氏
Molson Coors Beverage Company、情報セキュリティ担当シニア ディレクター (CISO)

成功事例を読む

Department of Education

VPN からゼロトラストに移行したニューヨーク市教育局

100 万人以上のユーザーと 200 万台以上のデバイスのインターネットとプライベート アプリケーションへのアクセスを保護

ニューヨーク市教育局の概要

米国最大規模で、世界でも最大級の学校システムであるニューヨーク市教育局 (NYC DOE)。ニューヨークの 5 つの行政区全体の幼稚園から 12 年生までの 100 万人以上の学生と、150,000 人以上の教師と管理スタッフにサービスを提供

教育

米国
ニューヨーク州
ニューヨーク市

100 万人以上のユーザー
と 200 万台以上のデバイス

200 万 +
保護された学生と
従業員のデバイスの数

15%
攻撃の減少率

40%
ブロックされた
脅威の増加率

課題

- 従来のインフラでは、100 万人以上のユーザーに安全で一貫性のあるエクスペリエンスを提供するように拡張することは不可能
- 従来の VPN とファイアウォールのアプローチでは、高度なサイバー脅威のブロックにおいて無力
- エンドポイントの可視性が不十分なため、同局のリモート学習デバイスの保守とモニタリングが困難

取り組みの各ステップ

1. **インターネットと SaaS への安全なアクセスの提供：**ゼロトラスト プロキシ アーキテクチャーですべての TLS/SSL トラフィックを大規模に検査
2. **VPN からゼロトラスト ネットワーク アクセス (ZTNA) への移行：**高速でシームレスなユーザー接続を提供
3. **可視性の改善：**エンドツーエンドのデジタル エクスペリエンス モニタリングでネットワークとデバイス全体を詳細に可視化

成果

- **高速かつ信頼性の高い安全なアクセスの拡張：**場所やデバイスによらず、学生や職員が安全に学習アプリケーションにアクセス可能
- **コンテンツに基づいたトラフィックのフィルタリング:**単純な URL のブロックにとどまらず、学習デバイスでの CIPA 順守にも対応
- **ネットワーク パフォーマンスの向上：**環境内のネットワークと DNS の問題を検出して解決

Zscaler によって、AI が社内の環境でどのように機能しているのかを把握できるため、インシデントにより早く対応できるようになります。Zscaler は、膨大なデータの中から重大なセキュリティ脅威をいち早く特定する手助けとなると確信しています。

Demond Waters 氏
ニューヨーク市教育局、
CISO

成功事例を読む

Zscaler Zero Trust Exchange を活用して安全なユーザーエクスペリエンスを最適化した Southwest Gas

従来のセキュリティ ソリューションから脱却し、2,300 人のハイブリッド勤務の従業員と 50 の営業拠点により迅速で信頼性の高い接続を提供

Southwest Gas の概要

アリゾナ州、ネバダ州、カリフォルニア州で天然ガス サービスを提供するエネルギー会社

エネルギー / 石油 / ガス / 鉱業

米国、ネバダ州 ラスベガス

200 万人以上の顧客

4 ～ 6
包括的なゼロトラストの展開にかかった週数

95%
ユース ケースの達成率

1
簡素化を実現する単一ベンダーのプラットフォームの数

課題

- 従来のセキュリティ インフラでは、クラウド トランスフォーメーションやハイブリッド ワークへの移行に対応するための拡張性が不十分
- 遠隔地の営業拠点や従業員に高速で信頼性の高いインターネット接続を提供することが困難
- 従来の VPN では、アイデンティティーベースのアクセス ポリシーを適用できないため、脅威に対するプライベート アプリとデータの脆弱性が悪化

取り組みの各ステップ

1. **マルチテナント ゼロトラスト プラットフォームの展開：**セキュリティ スタックを合理化し、リモート ワーク環境を最適化
2. **インターネットと SaaS アプリへの直接接続のプロビジョニング：**場所を問わず脅威から一貫して保護
3. **VPN からゼロトラスト アクセスへの移行：**プライベート アプリケーションへのアクセスを保護することで攻撃対象領域を縮小し、情報漏洩を阻止

成果

- **場所に左右されない安全な作業環境の構築：**2,300 人のハイブリッド勤務の従業員に安全で柔軟な作業環境を提供し、50 か所の営業拠点のユーザーとデータのセキュリティを確保
- **マイクロセグメント化された最小特権のアクセス制御ポリシーの提供：**プライベート アプリケーションへのアクセスを制御し、重要なデータを保護
- **ゼロトラストの採用の加速：**セキュリティ管理の複雑さを排除し、テクニカル サポートへのリクエストを削減

価値実証 (PoV) を実施したうえで、最新のアーキテクチャーを備えた Zscaler を選択しました。このアーキテクチャーによって、セキュリティ スタックをクラウドに置き、リモート ワーク環境を最適化できました

David Petroski 氏
Southwest Gas、シニア インフラストラクチャー アーキテクト

成功事例を読む

進化する脅威を Zscaler Zero Trust Exchange で検出してブロックする United Airlines

従来のソリューションよりも 40% 多くの脅威を排除し、世界中の 80,000 人のユーザーを保護しながら、1 億 4,300 万人の乗客により安全な空の旅を提供

United Airlines の概要

48 か国で事業を展開する世界第 3 位のアメリカの航空会社

輸送サービス

米国、イリノイ州
シカゴ

350 以上の拠点に
80,000 人以上の従業員

6

ゼロトラスト トランスフォーメーションに要した月数

1PB

検査される TLS トラフィック

300 万ドル +

従来のソリューションからのコスト削減額

課題

- データ センターを利用する従来の境界型アーキテクチャーでは、デジタル トランスフォーメーションの加速が不可能
- 従来のファイアウォールと VPN には十分なアジリティーが備わっていないため、リモート ワークの増加に合わせて拡張できず、ユーザーとデータのリスクが増大
- 以前のセキュリティ ポイント製品には高度な脅威検出機能がなく、攻撃対象領域が拡大

取り組みの各ステップ

1. **インターネットと SaaS アプリへの安全な直接接続の提供：**場所を問わず一貫してユーザーを保護
2. **VPN からゼロトラストの最小特権アクセス ポリシーへの移行：**プライベート アプリとデータを侵害から保護
3. **クラウド統合とエクスペリエンス モニタリング機能の活用：**脅威に関するリアルタイムの可視性を改善

成果

- **80,000 人の従業員がどこからでも安全に働ける環境の構築：**2,000 以上の重要なプライベート アプリへのセキュア リモート アクセスを確保
- **アーキテクチャーの複雑さとコストの削減：**6 つのセキュリティ ポイント製品と空港で使用していたファイアウォールを排除
- **セキュリティ エコシステムの統合とポリシーの動的な施行：**脅威を 40% 以上ブロックし、セキュリティ態勢を改善

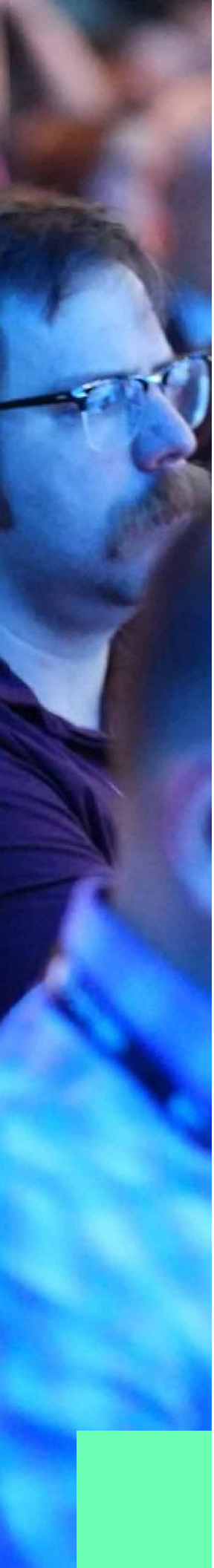
Zscaler を導入したことで、従業員、お客様、パートナーがどのネットワークを使用していても、トラフィックの安全性が確保されていると実感できます。

Deneen DeFiore 氏
United Airlines、バイス プレジデント兼最高情報セキュリティ責任者

成功事例を読む

EMEA

地域ごとの導入事例



Raiffeisen Bank International

Zscaler Zero Trust Exchange でセキュリティを変革する Raiffeisen Bank International

従来のアプライアンスをリプレースすることで、包括的な脅威対策とどこからでも働ける柔軟性を確保し、セキュリティ コストを削減

Raiffeisen Bank International の概要

オーストリアの大手投資銀行

金融サービス / 保険

オーストリア、ウィーン

12 の市場に数百万人の顧客

4.4 万
ゼロトラストで保護された従業員の数

1,860 万
銀行サービスを安全に利用する顧客の数

1
完全なゼロトラストを提供するプラットフォームの数

課題

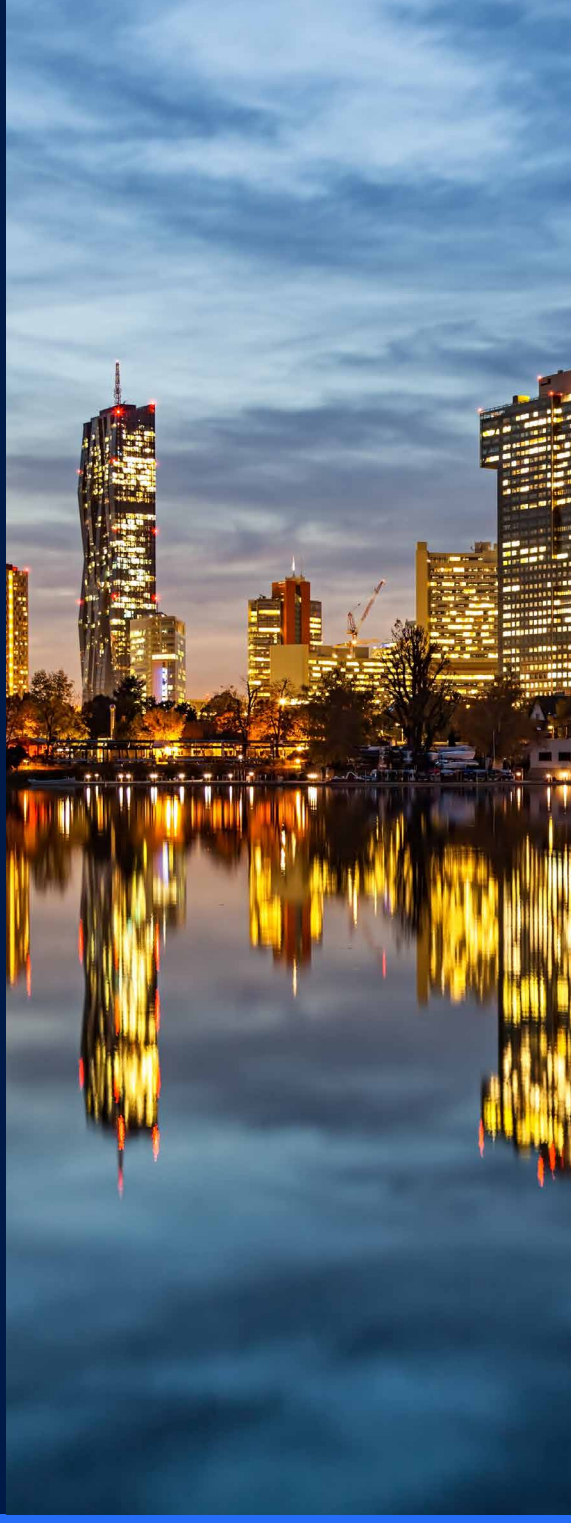
- 従来のセキュリティ インフラでは、クラウドファーストのアプローチに対応できず、ユーザーとワークロードにリスクが発生
- 従来のセキュリティ アプライアンスではさまざまな場所で働く柔軟性を確保できず、遅延やパフォーマンスの問題が発生
- VPN では、プライベート アプリへのアイデンティティーベースのアクセスを提供できないため、ポリシーに一貫性がなく、攻撃対象領域が拡大

取り組みの各ステップ

1. **包括的なゼロトラスト プラットフォームの展開：**Plivate Service Edge と Public Service Edge を活用してあらゆる場所のユーザーを保護
2. **バックホールが発生しないインターネットへの安全な直接接続：**ハイブリッド ワーカーに一貫したユーザー エクスペリエンスを提供
3. **VPN の廃止とプライベート アプリケーションへのゼロトラスト アクセスの導入：**同時にアイデンティティーベースのアクセス ポリシーを改良

成果

- **ハイブリッド ワークのアウトバウンド接続とインバウンド接続の保護：**あらゆる場所で一貫した保護を提供
- **遅延の削減と SaaS とプライベート アプリケーションのパフォーマンスの改善：**オフィス内とリモートのユーザー エクスペリエンスを強化
- **セキュリティ アーキテクチャーの合理化および脅威に対する包括的な保護の提供：**同時にセキュリティにかかる費用も削減



Zscaler とのパートナーシップにより、ゼロトラストの原則を適用し、セキュリティの強化、コストの削減、ユーザー エクスペリエンスの向上を実現できました。

Peter Gerdenitsch
Raiffeisen Bank International、グループ CISO

成功事例を読む

Zscaler Zero Trust Exchange でデジタル トランスフォーメーションを保護するマクデブルク市

Zscaler を活用して VPN をリプレースし、ハイブリッド ワークを強化しながら、進化し続けるデジタル基盤を構築するドイツの州都

州都マクデブルク市の概要

ザクセン アンハルト州の州都の住民に行政サービスを提供

公共機関

ドイツ、マクデブルク

2,500 人の職員

2,500
保護されたハイブリッド勤務の職員の数

23 万
サポートされる住民の数

1
セキュリティを簡素化する単一ベンダーのソリューションの数

課題

- 従来のハードウェアベースのセキュリティ アーキテクチャーでは、デジタル トランスフォーメーションの目標に対応するための十分なアジリティーが不足
- 従来のプロキシとファイアウォール ソリューションでは、増え続けるハイブリッド ワークに対応してインターネット接続を保護するための拡張が不可能
- VPN ではきめ細かなアクセス制御ができないため、プライベート アプリのリスクが高まり、リモート ワーク機能が限定的に

取り組みの各ステップ

1. **クラウド ネイティブ ゼロトラスト プラットフォームの展開：**セキュリティ アーキテクチャーを近代化し、デジタル トランスフォーメーションを加速
2. **インターネットへの安全な直接接続の展開：**組み込み済みのトラフィック検査機能を活用することで脅威を管理
3. **アイデンティティーベースのゼロトラスト制御による、プライベート アプリへのアクセスの保護：**重要なデータを一貫して保護

成果

- **ハイブリッド ワークのユーザー エクスペリエンスの改善：**1 か月あたり最大 1,500 人のユーザーの安全なリモート ワークを実現
- **セキュリティ コストと管理の複雑さの軽減：**従来のセキュリティ ポイント製品の廃止と革新的なアーキテクチャーの導入によって達成
- **将来のデジタル トランスフォーメーションの加速：**包括的でスケーラブルなゼロトラスト セキュリティ アーキテクチャーが後押し

他の自治体の先駆けとなるとともに、当市がクラウドベースのセキュリティ ソリューションを導入したように、優れたソリューションの評価と導入を他の自治体にも促したいと考えていました。

Tim Hoppe 氏
マクデブルク市、統計 / 選挙 / デジタル化担当局

成功事例を読む

3 か月未満で Zscaler を展開することでセキュリティ態勢を強化した Cisalfa Sport

ゼロトラスト プラットフォームで攻撃対象領域を削減し、従業員とサードパーティー ユーザーにシームレスなユーザー エクスペリエンスを提供

Cisalfa Sport の概要

イタリアを代表するオムニチャネルのスポーツ小売事業者

小売 / 卸売

イタリア、クルノ（ベルガモ県）

3,600 人以上の従業員

2.5

全社への Zscaler の展開に要した月数

130+

プライベート アプリとオンプレミスのインフラに安全にアクセスするサードパーティー パートナーと請負業者の数

70%

展開から 2 週間以内にオンボーディングされたユーザーの割合

課題

- VPN では、すべての従業員とサードパーティーが組織のネットワーク全体にセグメント化されずにアクセスできるため、潜在的な攻撃のリスクと影響範囲が拡大
- 従来の 2 つの VPN ソリューションではポリシーと構成が競合するため、一貫したセキュリティと管理が困難
- VPN 経由でアプリにアクセスすると、パフォーマンスが低下し、内部および外部のユーザーから大量のヘルプデスク チケットが発生

取り組みの各ステップ

1. **攻撃対象領域の削減：**脆弱な VPN をユーザーとプライベート アプリ間の直接接続にリプレース
2. **脅威のラテラル ムーブメントの阻止：**すべてのユーザーに最小特権アクセス ポリシーを施行
3. **ユーザー エクスペリエンスの強化：**アプリのパフォーマンスと信頼性が向上することで、リソースへのアクセスの中断がなくなり、複数の VPN へのログインも不要に

成果

- **全体的なセキュリティ態勢の強化：**すべてのユーザーにユーザーとアプリ間の直接接続と一貫したポリシー施行を提供
- **シームレスで透明性の高いクライアントレス アクセスの実現：**パートナーや請負業者を安全にプライベート アプリとデータに接続
- **遅延に関連するヘルプデスク チケットの削減：**最も近いポイント オブ プレゼンスから超高速接続を提供

Zscaler Zero Trust Exchange は、VPN を必要としないアプリへのより高速で安全なアクセス、環境全体のリスク軽減、ゼロトラストの拡張に向けた明確な道筋など、すべての基本条件を満たしています。

Fabio Freti 氏
Cisalfa Sport IT 運用とインフラ担当マネージャー

成功事例を読む

Zscaler Zero Trust Exchange でセキュリティ態勢と持続可能性を強化する Hydro

攻撃対象領域と二酸化炭素排出量を削減し、従来のハードウェアの廃止と 100% クラウドファーストという自社の目標を促進

Hydro の概要

40 か国に展開する世界最大級の再生可能エネルギー企業

製造

ノルウェー、オスロ

31,000 人の従業員

3.3 万
ゼロトラストで保護された従業員の数

1
コストと複雑さを軽減するために採用したベンダーの数

100%
クラウド運用の目標達成率

課題

- 従来のセキュリティ インフラとハードウェアでは、エネルギーを大量に消費し、組織の持続可能性目標と不一致
- 低帯域幅の MPLS ネットワークでは、クラウドに向かうデータ トラフィックの急増に対応するように拡張できず、パフォーマンスが低下
- 従来の VPN は「すべてかゼロか」のアクセス ポリシーを採用しているため、ネットワークが危険にさらされ、甚大な被害を招くランサムウェア攻撃が発生

取り組みの各ステップ

1. **インターネットへの安全な直接接続のプロビジョニング：**トラフィックのバックホールを排除し、アクセスの信頼性を改善
2. **従来の VPN からポリシーベースのゼロトラスト アクセスへのリプレース：**プライベート アプリケーションのデータをサイバー攻撃から保護
3. **クラウド トラフィック専用のエクスペリエンス モニタリング ソリューションの展開：**ユーザーの問題解決を加速

成果

- **従来のポイント製品の排除：**クラウド ネイティブのマルチテナント セキュリティ プラットフォームで二酸化炭素排出量を削減
- **SaaS アプリケーションのパフォーマンス向上：**140 拠点の 33,000 人の従業員のユーザー エクスペリエンスを改善
- **コストと管理の複雑さの軽減およびセキュリティ態勢の改善：**単一プロバイダーが提供するゼロトラスト ソリューションで達成

Zscaler Private Access を導入したことで、プライベート アプリケーションを使用するためにユーザーがネットワークに接続する必要がなくなりました。現在、新しい働き方をさらに改革するために、VPN の廃止に向けて取り組んでいます。

Armin Auth 氏
I&T 戦略プログラム責任者

成功事例を読む

Zscaler でデジタル トランスフォーメーションを加速させ、財務データを保護する Capitec

ゼロトラスト セキュリティを 3 か月で展開し、Zero Trust Exchange を活用して 17,000 人のユーザーを保護しながら、745,000 件の脅威をブロックする南アフリカ最大の銀行

Capitec の概要

2,100 万人にサービスを提供し、顧客満足度 1 位を獲得する南アフリカ最大の銀行

金融サービス / 保険

南アフリカ、ケープタウン

860 支店に 15,450 人の行員

3
プライベート アプリを AWS に移行するのに要した秒数

1.25 億
1 年間に防止されたポリシー違反の数

3
包括的なゼロトラストの実装に要した月数

課題

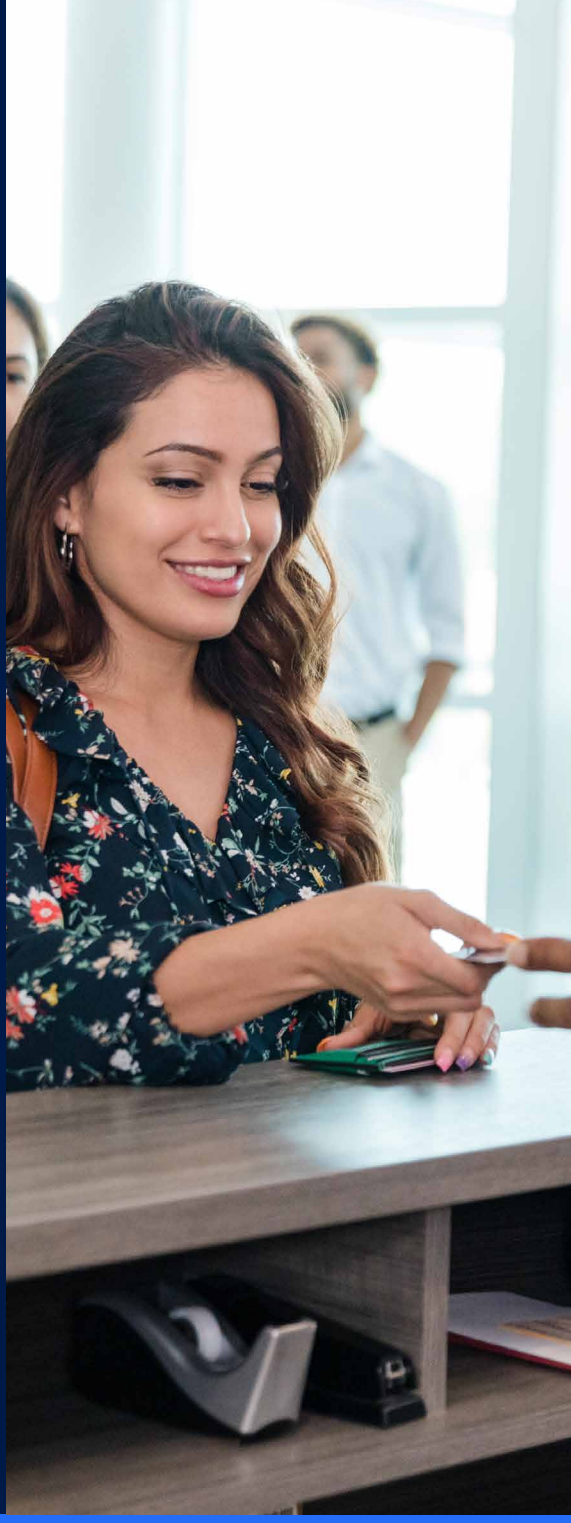
- 境界ベースのセキュリティ アーキテクチャーでは、価値の高い財務データを侵害や漏洩から効果的に保護することが不可能
- ファイアウォールや VPN などの従来のセキュリティ アプライアンスでは、管理が複雑でユーザーの生産性が低下
- ユーザー エクスペリエンスに関する可視性が限られており、問題の特定と解決に対する事前予防的な対策の策定が不可能

取り組みの各ステップ

1. **インターネットと SaaS アプリへの安全な直接接続：**トラフィックを検査することで、データ侵害を防止
2. **従来の VPN アプライアンスからゼロトラスト アクセスへの移行：**プライベート アプリケーションや機密性の高い財務データが対象
3. **高度なデジタル エクスペリエンス機能と実用的なインサイトの活用：**長年にわたるユーザー エクスペリエンスの問題を解決

成果

- **17,000 人のユーザーのインターネットとクラウド アプリケーションへのアクセスの保護：**1 年あたり 1 億 2,500 万件のポリシー違反を防止
- **1,100 万人以上の顧客がアクセスするプライベート バンキング アプリケーションの保護：**ポリシーベースのゼロトラスト アクセスを活用
- **デジタル トランスフォーメーションの加速：**ダウンタイムやセキュリティ障害を発生させることなく、わずか数秒でアプリを AWS に移行



Zero Trust Exchange を自社の環境に導入したところ、3 か月未満でゼロトラストのセキュリティ ソフトウェア エージェントがすべてのユーザーに展開されました。

Andrew Baker 氏
Capitec、CTO

成功事例を読む

Zscaler の技術を実装し、さまざまなユース ケースに対応する Noatum

インターネットや SaaS、プライベート アプリへの安全なアクセス、強固なサイバー脅威検出、最適化されたユーザー エクスペリエンスなどを実装

Noatum の概要

輸送と物流サービスにおける代表的な多国籍企業グループ

輸送サービス

スペイン、バルセロナ

4,300 人以上の従業員

初日
プラットフォームの価値の発揮

ゼロ
VPN とファイアウォールの利用

360 度
リスクを定量化する角度

課題

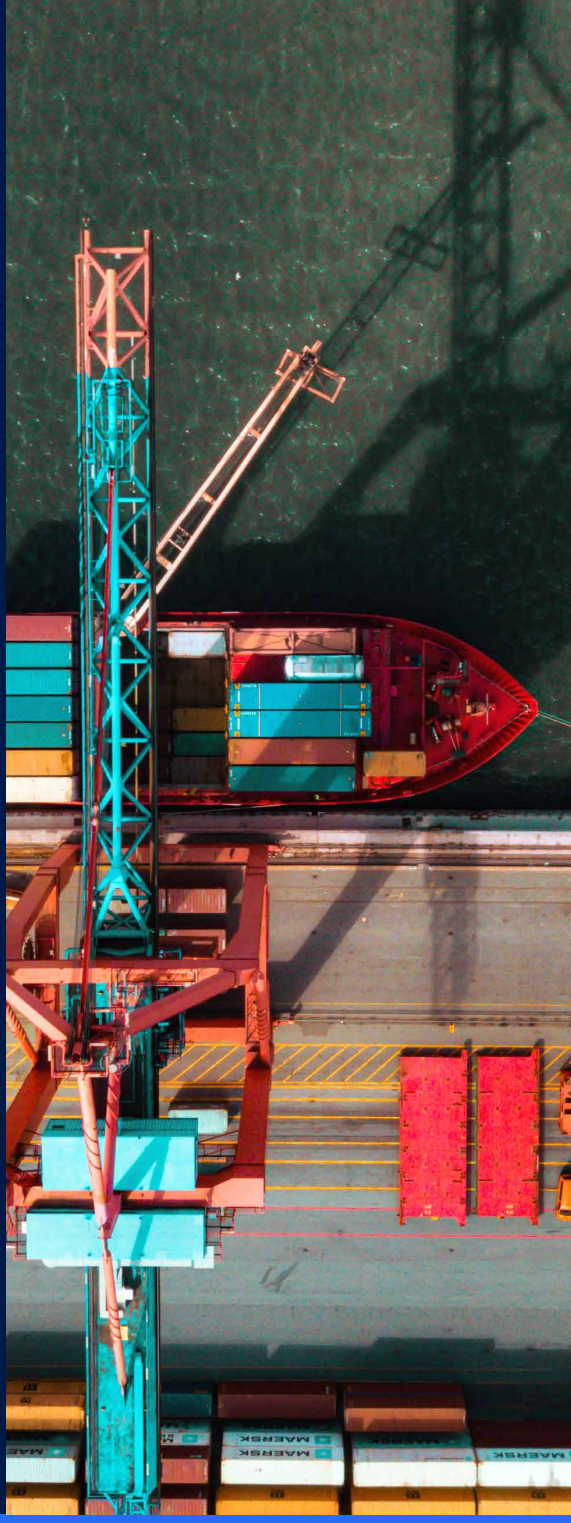
- 従来の VPN では、ユーザーがインターネットにアクセスする際に生じるサイバー攻撃のリスクが増大
- ファイアウォールなどの従来のセキュリティでは、暗号化されたトラフィックの検査が不可能
- 境界ベースのアーキテクチャーでは、M&A に伴うオンボーディングが過剰に長期化

取り組みの各ステップ

1. **VPN のリプレース：**クラウド プラットフォームに移行し、インターネットとプライベート アプリへの安全なアクセスを確保
2. **クラウドベースの単一のエクスペリエンス モニタリング ハブの作成：**ZDX で提供
3. **ビジネス リスクの評価：**Zscaler Risk360 で総合的に評価

成果

- **場所を問わずに働ける環境の提供：**安全でシームレスなユーザー アクセスにより、どこからでも安心して働くことが可能に
- **ユーザー インシデントの最小化：**根本原因分析を改善し、知識とアジリティーを提供
- **リスク評価の改善：**インターネットからシステムやアプリを見えなくすることで、脅威対策も改善



従来の VPN では、インターネットに接続されたサービスを保護できないため、常に攻撃を受けるリスクがありました。これが、Zscaler のようなソリューションを探すようになった理由です。

Josep Pou 氏
Noatum、CISO

成功事例を読む

Zscaler Internet Access で安全かつシームレスな接続を提供する Sanitas

さまざまな場所で作業する 12,000 人以上のユーザーがインターネット、SaaS、プライベート アプリケーションに安全にアクセスできる環境を構築

Sanitas の概要

急成長を遂げている大手医療保険会社

医療 / 製薬

スペイン、マドリード

スペインなどの欧州と南米に 11,700 人以上の従業員

2.5
すべてのユーザーへの展開に要した月数

1.2 万～1.5 万
Zscaler で保護されたユーザーの数

ゼロ
データ センターへの接続の必要性

課題

- クラウドベースのモデルがなく、それぞれの事業部門が個別のセキュリティ手段を利用
- VPN はセキュリティが不十分で、ユーザー認証という煩雑なプロセスが必要
- パートナーのオフィスからはデータ センターに接続できず、アプリケーションへのアクセスが不可能

取り組みの各ステップ

1. 統一されたクラウドベースのゼロトラストの展開：組織全体を大規模に保護
2. VPN からゼロトラスト モデルへの移行：場所を問わず、すべてのユーザーの接続を改善
3. アプリケーションへの安全でシームレスなアクセスの確保：パートナーを含むすべてのユーザーに提供

成果

- 2 か月半で 12,000 ～ 15,000 人のユーザーの保護：Zscaler Internet Access によって実現
- 場所を問わずに働ける環境の確保：オフィスのようなエクスペリエンスで柔軟かつ俊敏なビジネスが可能に
- 安全なアクセスの提供：ワークロードとアプリケーションを保護

従業員は現在、透明性が高く柔軟性があり、アジリティーに非常に優れた方法で、オフィスと同じように自宅で作業できています。他のソリューションで見られた障壁はありません。

Antonio Cerezo 氏
欧州および南米担当サイバーセキュリティ責任者

成功事例を読む

Zero Trust Exchange で セキュリティとデジタル エクスペリエンスを 向上させた Colt Technology Services

Zscaler とのパートナーシップによりゼロトラスト アーキテクチャーを 3 か月で展開し、他社のセキュリティ トランスフォーメーションの達成を支援

Colt Technology Services の概要

世界中の 25,000 以上の組織にネットワーク、音声、データ センター サービスを提供

電気通信

英国、ロンドン

世界中の 60 拠点に 5,000 人以上の従業員

5,000
保護されたハイブリッド勤務の従業員の数

83%
展開速度の向上率 (従来のソリューションとの比較)

1 億
1 四半期に防止されたポリシー違反の数

課題

- ハイブリッド ワーク環境に対応するためにクラウド移行を加速させると、攻撃対象領域と侵害のリスクが増加
- 古いプロキシ ソリューションでは、暗号化されたトラフィックのインライン検査を管理できず、マルウェアの死角が発生
- 従来の VPN アプライアンスでは、プライベート アプリケーションへの動的なアクセス ポリシーが有効になっていないため、リモート ワークの維持が困難

取り組みの各ステップ

1. **クラウド ネイティブのゼロトラスト セキュリティ アーキテクチャーの展開：**クラウドファーストの業務とハイブリッド ワークに対応
2. **インターネットへの安全な直接接続のプロビジョニング：**暗号化されたすべてのトラフィックを検査することで、脅威と情報漏洩を阻止
3. **従来の VPN の廃止とゼロトラスト アクセスの導入：**プライベート アプリケーションに安全に接続できるようにすることで、リモート ワークを簡素化し、安全性を向上

成果

- **5,000 人以上のハイブリッド勤務の従業員への優れたデジタル エクスペリエンスの提供：**同時にアウトバウンドとインバウンドのトラフィックを保護
- **インターネット トラフィックの大規模な検査：**1 四半期あたり 67 億件のトランザクションを処理し、476,000 件のセキュリティ脅威をブロック
- **マイクロセグメンテーションとプライベート アプリケーションへのポリシーベースのアクセス：**従来の VPN では不可能

優れたユーザー エクスペリエンスと高度なセキュリティを同時に実現できているのは、Zscaler の成果と言えるでしょう。クラウド ネイティブの Zscaler プラットフォームは、従業員がどこで働いていても、またどんなデバイスを使用していても、安全な環境を確保します。

Ash Surti 氏
Colt Technology Services、
最高デジタル情報責任者

成功事例を読む

Zscaler Zero Trust Exchange で安全なハイブリッド ワーク環境を実現した Primetals Technologies

データ センターの廃止、従来のセキュリティ スタックの統合、デジタル トランスフォーメーションの加速をすべて Zscaler で実現した金属生産のグローバル リーダー

Primetals Technologies の概要

鉄鋼生産を専門とする冶金プラント ソリューションのグローバル リーダー

ハイテク

英国、ロンドン

7,500 人以上の従業員

7,500
ゼロトラストで保護されたユーザーの数

最大 35%
インフラ コストの削減率

4.53/5
従業員の満足度

課題

- データ センターを中心に構築された従来のセキュリティ スタックでは、クラウドファーストのデジタル トランスフォーメーションに対応するための拡張が不可能
- ファイアウォールや VPN などの従来のセキュリティ アプライアンスでは、新しい SD-WAN ネットワークの再設計に対応するための十分なアジリティーが不足
- 古い VPN アプライアンスでは、世界中に分散したハイブリッド ワーカーのリモート接続の効果的な保護が困難

取り組みの各ステップ

1. **SD-WAN に対応する、インターネットへの直接接続の展開：**インフラを合理化し、パフォーマンスを改善
2. **VPN からゼロトラスト アクセスへの移行：**世界中のユーザーが安全にプライベート アプリケーションにアクセスできるようにすることで、あらゆる場所で作業できる環境を構築
3. **高度なユーザー エクスペリエンス モニタリング機能の活用：**従業員とのコラボレーション ツールの機能を最適化

成果

- **セキュリティ スタックの簡素化：**データ センターの利用を減らし、インフラ全体にかかる費用を削減
- **シームレスなアウトバウンドとインバウンド接続の確保：**ハイブリッド勤務のユーザー グループが対象 (そのうち 25% はフル リモート勤務)
- **ヘルプデスクのチケットの削減および問題解決の加速：**エンドユーザーのエクスペリエンスを向上させて、管理負荷を軽減

クラウドへの移行過程で、セキュリティ スタックを近代化する必要がありました。これを達成するうえで、Zscaler Zero Trust Exchange (ZTE) は非常に重要な役割を果たしました。

Ralph Deleja-Hotko 氏
Primetals Technologies、バックエンドおよびクラウド ソリューション責任者

成功事例を読む

ゼロトラストでセキュリティをグローバルに強化し、アプリへの「必要最低限」のアクセスを 実現した Unilever

Zscaler によって VPN を排除して、ユーザーにアプリやインターネットへの安全な直接接続を提供し、190 か国で業務を合理化

Unilever の概要

34 億人が日々使用する製品を提供する世界的な消費財企業

製造　英国、ロンドン　190 か国で販売

30 億 +
1 週間あたりに保護されるトランザクションの数

99.9%
2 か月で 220TB のデータを処理しながら維持された稼働率

1,500+
「必要最低限」のゼロトラスト アクセスで管理されるアプリケーションの数

課題

- 従来の VPN の柔軟性の不足とグローバル クラウド戦略に対応するための拡張性の欠如
- 従来のセキュリティ モデルのアクセス制御と可視性の不足によるリスクの増大
- リモート アクセスの需要の拡大による VPN インフラへの負担とユーザー エクスペリエンスへの悪影響

取り組みの各ステップ

1. **インターネットと SaaS へのアクセスの保護：**TLS/SSL トラフィックの完全な検査と高度な脅威対策によって実現
2. **VPN のリプレース：**プライベート アプリケーションへのゼロトラスト アクセスを導入
3. **ユーザー エクスペリエンスの改善：**デジタル エクスペリエンスを監視してパフォーマンスの問題を迅速に特定し、解決

成果

- **リスクの軽減：**アプリケーションへの安全な直接接続により、VPN の制約や脆弱性を排除
- **運用効率の向上：**99.99% の稼働時間で大規模にデータ トラフィックを処理
- **グローバル クラウド戦略のサポート：**190 か国にわたり安全なリモート アクセスを提供し、従業員の柔軟性を維持

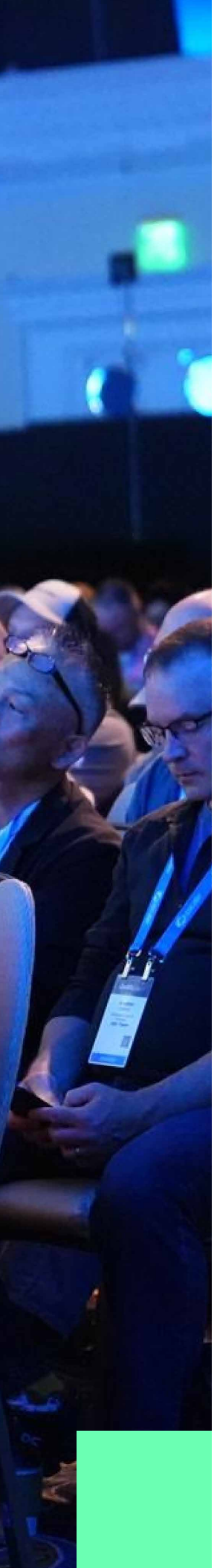
Zscaler のゼロトラスト アプローチにより、Unilever のセキュリティは大きく変化しました。VPN のボトルネックを排除することで、世界中の従業員がアプリケーションに安全にアクセスできるようになり、パフォーマンス、柔軟性、レジリエンスが強化されました。

Richard Mardling 氏
Unilever、アクセス / 接続担当ディレクター

成功事例を読む

APJ

地域ごとの導入事例



JOHN HOLLAND

Zscaler Zero Trust Exchange でネットワーク コストを 50% 削減した John Holland

Zscaler によって、SD-WAN への移行を円滑化するとともに、多数のファイアウォールを置き換え、運用効率とセキュリティ態勢を改善

John Holland の概要

総合インフラ、建物、鉄道、複合一貫輸送の分野をリードするオーストラリア企業

建設

オーストラリア、ビクトリア州メルボルン

従業員 5000 人以上
拠点数 120 以上

1 週間
ゼロトラストの展開に要した期間

6,000
保護されたスタッフと請負業者の数

12.2 万
3 か月でブロックされた脅威の数

課題

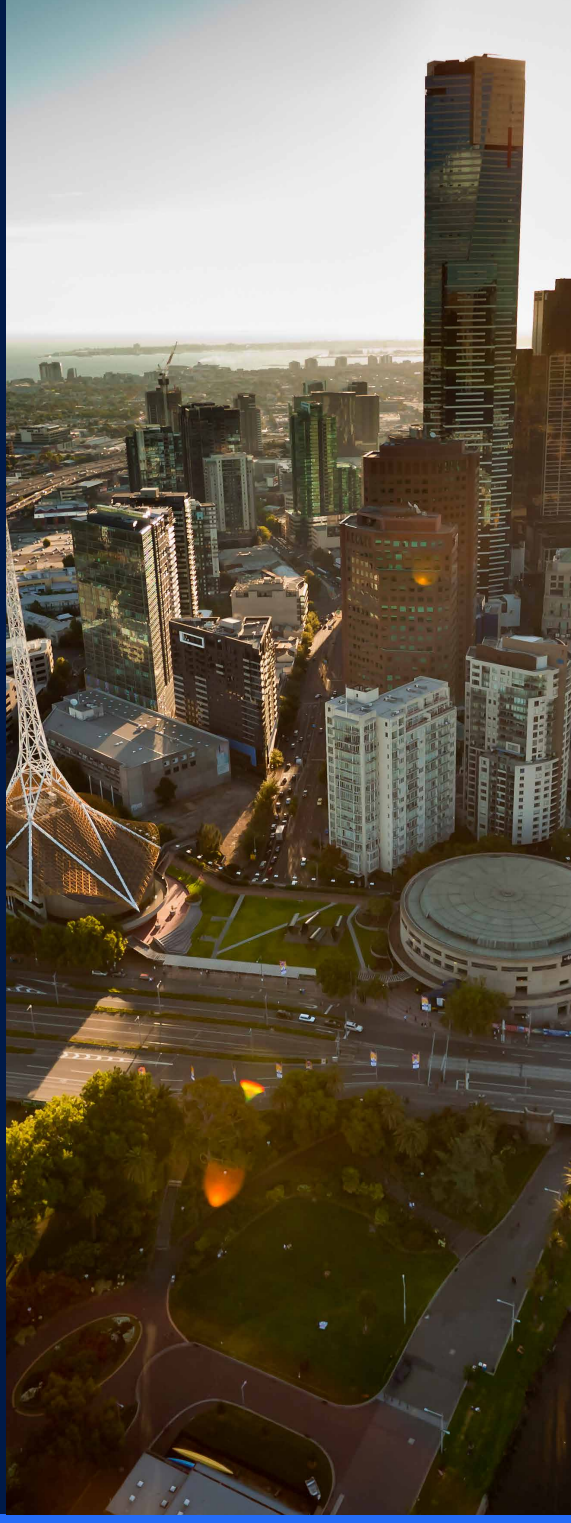
- 従来の境界型セキュリティ アーキテクチャーは、クラウドファーストのビジネス運用に対応するための拡張性が不十分
- 旧式の MPLS ネットワークでは、大量のトラフィックのバックホールが必要になるため、IT サービスの速度低下やコストの増大が発生
- 従来のファイアウォール アプライアンスでは、暗号化されたトラフィックをインラインで検査できず、脅威に対する脆弱性が増大

取り組みの各ステップ

1. **クラウドネイティブで包括的なゼロトラスト セキュリティ プラットフォームの展開：**俊敏性と拡張性により優れた IT 環境を構築
2. **ファイアウォール アプライアンスへの依存とネットワーク コストの低減：**インターネットと SaaS アプリへの安全な直接アクセスで実現
3. **高度な脅威検知機能によるセキュリティ エコシステムの合理化：**データ侵害のリスクを排除

成果

- **すべてのユーザーを 1 週間でゼロトラストに移行：**120 以上のプロジェクト サイトでのネットワーク アクセス プロビジョニングを高速化
- **ゼロトラスト接続の採用により数百のレガシー ファイアウォール アプライアンスを廃止**し、ネットワーク コストを 50% 削減
- **ユーザーの接続の保護：**400 TB のトラフィックを処理し、四半期あたり 9,800 万件のポリシー違反を防止



Zscaler によってセキュリティが補強されて、自社のプロセスがシンプルになりました。そのおかげでセキュリティが大幅に向上しました。

Kier Morrison 氏
John Holland、IT テクノロジー運用担当ゼネラル マネージャー

成功事例を読む

Zscaler Zero Trust Exchange で VPN を段階的に廃止し、従業員と重要なアプリを保護する Probe CX

セキュリティ スタックの合理化、ポリシー管理の簡素化、技術コストの削減を実現しながら、強固なセキュリティを確保

Probe CX の概要

カスタマー エクスペリエンスとビジネス プロセスを専門とする、オーストラリア最大のアウトソーシング業者

サービス

オーストラリア、ビクトリア州メルボルン

32 のサービス拠点に 19,000 人の従業員

100%
VPN の削減率

81 億
1 四半期に処理されるトランザクションの数

310 万
3 か月でブロックされた脅威の数

課題

- 従来のセキュリティ アーキテクチャーでは、従業員の急増やクラウドファーストのアプローチの進化に合わせた拡張が不可能
- 従来の VPN では、マイクロセグメント化されたアクセス制御ポリシーに対応できないため、プライベート アプリケーションのリスクが増加
- ユーザー エクスペリエンスとアプリケーションのパフォーマンスを十分に可視化できないため、問題を軽減する作業が複雑化し、時間も消費

取り組みの各ステップ

1. **インターネットと SaaS アプリケーションへの安全な直接接続：**バックホールの必要がないインライン トラフィック検査を実施
2. **VPN からゼロトラスト アクセスへの移行：**プライベート アプリケーションへのアクセスを保護することで、知的財産と重要なデータの安全性を強化
3. **高度なユーザー エクスペリエンス機能の活用：**問題解決を加速させて、シームレスなリモート ワーク エクスペリエンスを実現

成果

- **ゼロトラストの原則に基づいた場所を選ばない柔軟な働き方の確保：**5 か国の 7,600 人のユーザーに提供
- **1 四半期に約 285TB のトラフィック処理：**一貫したセキュリティ ポリシーを施行し、攻撃対象領域を最小化
- **マルチテナント プラットフォームによるセキュリティ管理の簡素化：**低い TCO でゼロトラスト セキュリティを提供

このテクノロジーを導入したことでさまざまなメリットが得られましたが、中でも環境内の VPN を完全撤廃できたことは特に大きな成果です。

Rohan Khanna 氏
Probe CX、最高技術責任者

成功事例を読む

Persistent

セキュリティを強化し、設備投資 / 運用コストを前年比で 200 万ドル節約した Persistent

機密性の高い顧客データや IP データの保護、イノベーションの加速、複雑さの軽減、環境、社会、ガバナンス (ESG) の目標の推進をすべてゼロトラストで実現

Persistent の概要

企業の近代化と高度なテクノロジーを活用したイノベーションの推進をサポートする世界的なモダナイゼーション パートナー

ハイテク

インド、プネー

21 か国に
23,000 人の従業員

85%
VPN の排除による
セキュリティ態勢の
改善率

80+
デセプションによって
90 日間でブロックされた
優先度の高い攻撃件数

4 倍
VPN と比較したプライベート アプリへの
アクセス速度

課題

- 21 か国のリモート ワーカーへの高速接続とより生産的なユーザー エクスペリエンスの提供
- クラウド環境全体での知的財産と機密性の高いクライアント データの保護
- 複雑なインフラの簡素化
- 環境全体でのハードウェアと運用コストの削減
- 組織の急激な成長にも対応できるスケーラブルなソリューションを備えた、長期的なゼロトラスト パートナーの選定
- 二酸化炭素排出量の削減による環境への影響の最小化

取り組みの各ステップ

1. **セキュリティ態勢の向上：**インターネット、SaaS、プライベート アプリへの安全な直接接続を提供
2. **遅延の短縮、コストの削減、ユーザー エクスペリエンスの向上：**信頼性と安全性が低い VPN やファイアウォールを排除
3. **貴重な知的財産と顧客データの保護：**高度な情報漏洩防止 (DLP) とデセプション テクノロジーを活用

成果

- **リモート アクセスの改善と高速化：**世界中に分散した 23,000 人の従業員のリモート アクセスを 4 倍高速化
- **複雑さの排除：**セキュリティの有効性と効率性を向上
- **検知と対応の強化：**CrowdStrike、Microsoft Entra ID、Securonix との統合によって加速
- **自社の製品やサービスの拡大：**Zscaler を中心とするセキュリティ プラクティスを備えた製品を自社の顧客に提供

セキュリティ部門は、Zscaler DLP によってシャドー生成 AI アプリの使用状況を詳しく把握できます。入力されたプロンプトなどが可視化され、リアルタイムで DLP のブロックとアプリケーションの分離を実行できます。

Debashis Singh 氏
Persistent、最高情報責任者

成功事例を読む

Zscaler Zero Trust Exchange でハイブリッド ワーカーを保護する Cebu Pacific Air

3,900 人の従業員のリモート ワーク エクスペリエンスを向上させ、アジア全域の 7 か所の戦略的ハブで重要な業務を保護

Cebu Pacific Air の概要

60 以上の都市にフライトを運航するフィリピンの大手航空会社

輸送サービス

フィリピン、マニラ首都圏

7 か所の戦略的ハブに 3,900 人の従業員

2.34 億
1 四半期に防止されたポリシー違反の数

90%
ユーザー満足度の向上率

2
ゼロトラストベースのリモート アプリ アクセスの展開にかかった週数

課題

- 従来のセキュリティ インフラでは、デジタル トランスフォーメーションの取り組みが遅れ、侵害や脅威のリスクが増加
- 従来のセキュリティ アプライアンスでは、業務に不可欠なプライベート リソースの適切な保護が不可能
- VPN アプライアンスにはパフォーマンスと接続の問題があるため、リモート ワークが困難になり、安全性が低下

取り組みの各ステップ

1. **旧式のセキュリティ アーキテクチャーの廃止：**代わりに包括的なクラウドネイティブのゼロトラスト プラットフォームを展開
2. **高度な脅威対策機能を備えたインターネットへの安全な直接接続の提供：**ハイブリッド ワーカーをより適切にサポート
3. **従来の VPN アプライアンスからゼロトラスト アクセスへの移行：**プライベート アプリケーションへのきめ細かなアクセス制御を実施

成果

- **場所に左右されない安全な作業環境の構築：**VPN の代替ソリューションを通じて安全で柔軟な作業環境を 3,900 人のユーザーに提供することで、ユーザーの満足度が 90% 向上
- **セキュリティ スタックの合理化および堅牢な保護の提供：**1 年あたり 7 億 3,300 万件のトランザクションを処理
- **セキュリティ態勢の強化：**1 四半期あたり 2 億 3,400 万件のポリシー違反を防止し、45,000 件のセキュリティ脅威をブロック

当社のような動的な業務環境においても、Zscaler を利用することで従業員は常に生産性を維持できています。必要なリソースへのアクセスの妨げになることも、セキュリティを犠牲にすることもありません。

Laureen Cansana 氏
Cebu Pacific Air、CIO

成功事例を読む

maxeon

事業分離後に Zscaler で デジタル トランスフォーメーションを 実現した Maxeon Solar Technologies

Zero Trust Exchange を導入することで、データ センターの廃止、セキュリティ態勢の強化、世界中の 5,000 人のユーザーのリモート ワーク エクスペリエンスの改善を可能にした太陽エネルギー業界のリーダー企業

Maxeon の概要

100 か国以上で営業展開する世界有数のソーラー パネル メーカー

エネルギー / 石油 / ガス / 鉱業

シンガポール

40 拠点に 5,000 人の従業員

134%
1 四半期に処理された トラフィックの増加率

3,100 万
1 四半期に防止された ポリシー違反の数

290 万
3 か月でブロックされた 脅威の数

課題

- データ センターを中心に構築された従来の境界セキュリティでは、進化するクラウドファーストのインフラへの対応が不可能
- 従来のファイアウォールでは、リモート アクセスのニーズの高まりに合わせて拡張できないため、パフォーマンスが低下し、リスクが増加
- 従来の DLP ソリューションは管理が難しく、重要な知的財産や資産の侵害リスクが発生

取り組みの各ステップ

1. **インライン トラフィック検査によるインターネットへの直接接続の保護：**ユーザーがどこにいても安全なインターネット接続を提供
2. **ゼロトラストに特化したエクスペリエンス モニタリング ソリューションの展開：**オンボーディングとライセンスのプロセスを合理化
3. **統合型 DLP ソリューションの導入：**重要な情報の保護、規制順守、データ侵害の防止を実現

成果

- **デジタル トランスフォーメーションの加速：**すべてのデータ センターが廃止され、ワークロードの 70% がクラウドに移行
- **場所を問わずに安全に働く柔軟性の確保：**16 か国に分散して働くユーザーグループに提供
- **1,400 件以上の特許を含むミッションクリティカルな IP データの保護：**セキュリティ態勢を改善し、事業継続性を確保

私たちは有名なベンダーをいくつも評価しましたが、Zscaler は Gartner Magic Quadrant でリーダーの一社と評価されており、その機能が実証済みであることから、最も優れた選択肢であることは明らかでした。

Stephen Gani 氏
Maxeon Solar Technologies、CISO

成功事例を読む