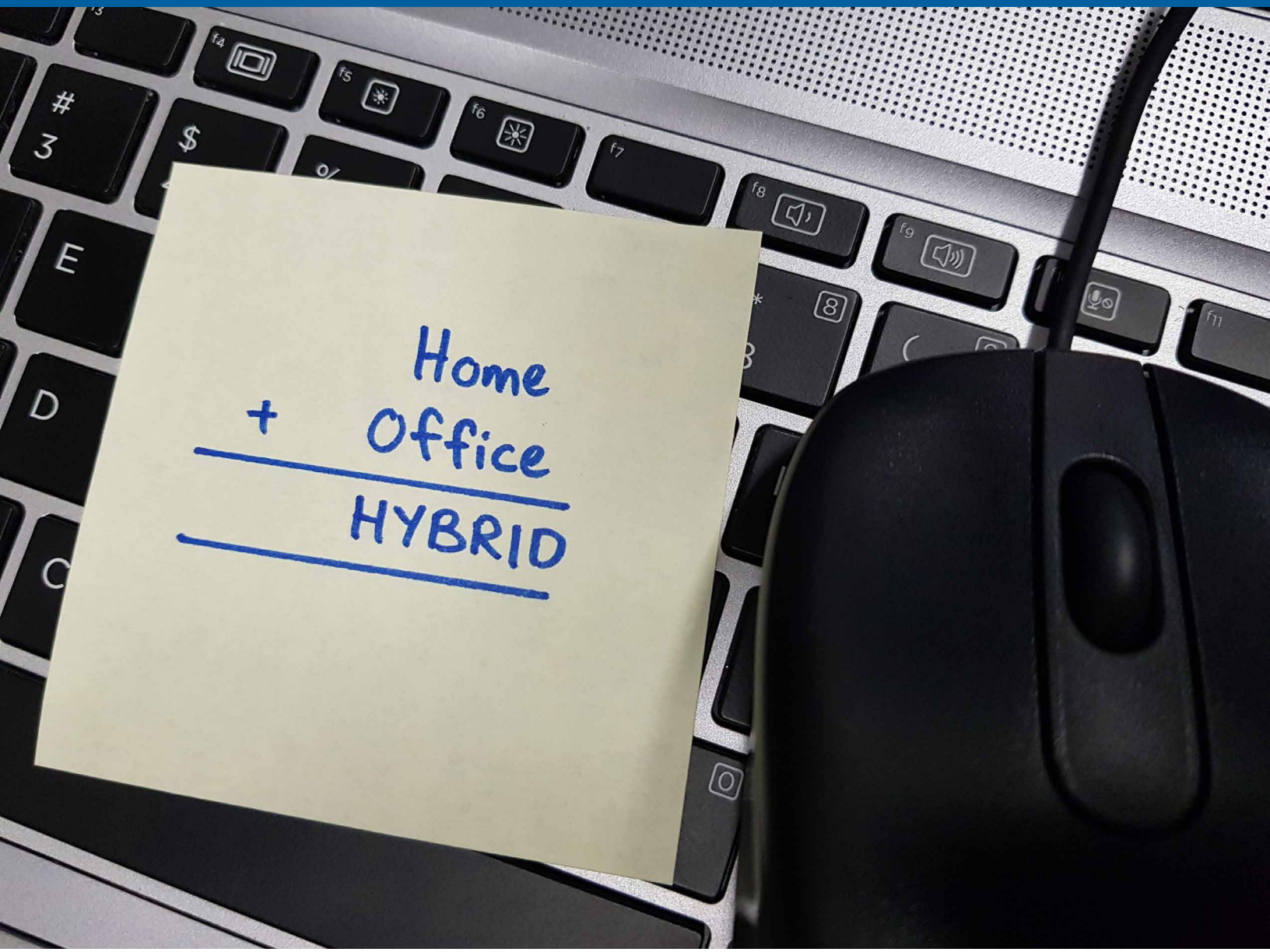
ゼロトラストで実現する安全な ハイブリッド ワーク

ハイブリッド ワークをより効果的に保護する ゼロトラスト アプローチとは



ZSCALER との協業による HMG STRATEGY 調査レポート

HMG STRATEGY　zscaler™

本書の要旨

世界が一変した 2020 年 3 月、CISO と情報セキュリティ部門は多くの新しい課題に直面しました。何百万人もの従業員が急きょ在宅勤務に切り替えられたことで、当時はまだ通用していた「組織には防護のための明確な境界線がある」という考え方が一掃されることになったのです。

世界的なパンデミックが拡大し、大半の企業がリモートで作業を続ける中、既存のネットワーク アーキテクチャーでは広範囲に分散した従業員や組織を十分に保護できない事実が明らかになりました。一方、データ センターからクラウドや SaaSプラットフォームへとアプリケーションがこれまでにないスピードで移行し、その数は増加し続けています。O'Reilly Mediaが実施した調査によると、2022年にアプリケーションの50%以上をクラウドに移行する計画がある組織は48%にのぼることがわかっています[1]。

ハイブリッド ワークの課題として挙げられるもう1つの要素は、在宅勤務環境における管理対象外の個人用デバイスに関連するセキュリティ上の懸念の高まりです。仮想プライベート ネットワーク(VPN)へ継続的に依存してきた結果、多くの組織が危険にさらされています。

こういった点は、CISOや企業のセキュリティ リーダーの大半が、防御を強化して組織をエンド ツー エンドで保護するために、最新のゼロトラスト アーキテクチャーを採用している理由の一部に過ぎません。

Zscalerのアメリカ地域フィールドCTOである**Lisa Lorenzin**は次のように述べています。「ゼロトラストの主な強みの1つは、セキュリティ制御を特定のリスク レベルや各ユース ケースの優先度に合わせて調整できることです。最新のゼロトラスト ソリューションでは、適切な抽象化レイヤーでこれを実現できます。こういった制御は、ネットワークに接続するエンドポイント間ではなく、アプリケーションに接続するユーザーに対してインラインで配置できます」

企業がデジタル フットプリントを拡大し、デジタル製品とサービスのポートフォリオを構築し続ける今、組織のデジタル ビジネス モデルのすべての階層を保護するためにゼロトラスト アーキテクチャーが求められています。これは、HMG StrategyとZscalerが118人のセキュリティ リーダーを対象に共同実施した最近の調査で、**CISOや企業セキュリティの担当役員の61%がゼロトラスト セキュリティ モデルは組織のデジタル エコシステムを保護するための効果的なアプローチであると考えている**ことからもその必要性は明白です。

HMG StrategyはZscalerと提携して、重大な脆弱性が存在するハイブリッド ワークに移行してからの脅威の活動状況の変化やゼロトラスト アーキテクチャーを導入するメリットとそこから生じるさまざまな可能性を調査しました。この調査レポートでは、以下を詳細に解説しています。

- ハイブリッド ワーク環境の主なセキュリティ リスクと課題
- 現在のアーキテクチャーではビジネスの安全性を十分に確保できない理由とそこから生じる経済的損失
- 最近のランサムウェア攻撃やネットワーク セキュリティ侵害の事例
- ゼロトラスト アーキテクチャーの採用が緊急に求められる背景
- ゼロトラスト セキュリティ モデルの採用が企業にとってプラスとなった実例
- ハイブリッド ワークにゼロトラスト アーキテクチャーを実装するための推奨事項

[1] *O'Reilly Media*による2021年クラウド導入レポート

ゼロトラストとは何か

次のうち、ゼロトラストのセキュリティ モデルを正確に定義しているものはどれですか？

表1:

ゼロトラストは、クラウド環境やモバイル環境で組織を保護するためのフレームワークで、ネットワークの境界はデジタル環境にはもはや存在しないという信念に加えて、すべてのユーザーおよびアプリケーションは本質的に信頼されるべきではないという考え方である

ゼロトラストは、ネットワーク境界の内外を問わず、あらゆるものを信頼してはならず、アクセスを許可する前にシステムに接続しようとするすべてを検証する必要があるという信念に基づくセキュリティ概念である

誰も決して信用しない

いずれも該当しない

0.5%

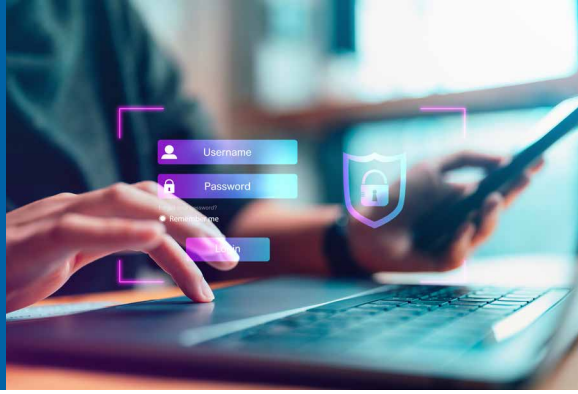
出典：ゼロトラストを理解する – ハイブリッド ワークの保護; HMG Strategy/Zscaler による調査; 118人のCISOとシニア セキュリティ リーダー

ゼロトラストとは、「何も信頼しない」を前提に、最小特権アクセスによる制御と厳格なユーザー認証によって確立されたコンテキストに基づいて、セキュリティ ポリシーを適用するサイバーセキュリティ戦略です。適切に調整されたゼロトラスト アーキテクチャーを用いることで、ネットワーク インフラの簡素化、ユーザー エクスペリエンスの向上、そしてサイバー脅威に対する防御力の強化を実現できます。

「ゼロトラストの主な強みの1つは、セキュリティ制御を特定のリスク レベルや各ユース ケースの優先度に合わせて調整できることです」

LISA LORENZIN
南北アメリカ地域担当フィールドCTO
Zscaler

ハイブリッド ワーク環境が抱える主なセキュリティ課題への取り組み



リモート ワークには、安全性の低いホーム ネットワークや管理対象外となる個人デバイスに関連したセキュリティ上の課題が常に存在するものの、長い年月を経て普及してきました。2020年3月から多くの企業がリモート ワーク環境へと移行したことで、各組織のデジタル フットプリントが飛躍的に拡大し、それに伴い攻撃対象領域を含む脆弱性も高まっています。

従業員の大多数はネットワーク セキュリティの知識が乏しく、機密性の高い顧客データや専有データはもとより、自分自身の安全を守るために必要な手段も把握していません。企業ネットワークのファイアウォールとVPNを介してサービスに接続すれば安全だと考えられがちですが、境界ベースのネットワーク セキュリティではユーザーを危険にさらす可能性が残っているのです。

一部のセキュリティ部門は従業員がフィッシング攻撃の理解を深められるようにフィッシングのシミュレーションを実施していますが、それでも多くの組織が攻撃にさらされる一定の「脆弱性」は存在したままとなっています。これは、Zscalerの2021年版VPN リスク レポートで、VPNはIT環境の安全性を維持する際の足かせとなると72%の経営幹部が懸念していることからも明白です。

VPNの脆弱性

従業員や企業の機密データの保護にVPNを使用し続けることは、さまざまな面でリスクが発生します。

Lorenzinは、VPNの3つの基本的な欠点を指摘しています。

1. 各VPNゲートウェイにはインバウンド リスナーがあり、それ自体が攻撃対象領域になる。
2. 攻撃対象領域が拡大し、VPNゲートウェイは巧妙な攻撃を仕掛けるハッカーにとっての起点になる。
3. VPNは本質的にオープンな性質を持つため、セキュリティ部門は従業員がアクセス権を持たない、または持つべきではないアプリケーションやシステムから明示的に除外する必要がある。

壊滅的な被害を及ぼした2021年のColonial Pipelineへのサイバー攻撃は、ユーザーに多要素認証を求めない従来のVPNを介して始まりました。サイバー犯罪者が組織のネットワーク内で水平移動するという典型的な攻撃で、ユーザーのVPN資格情報を盗み出したあとでColonial Pipelineのネットワークへのアクセスを取得し、水平に移動して重要な財務アプリケーションにアクセスして機密データを盗み、身代金を要求しました。

この攻撃により、米国東海岸と南部のほとんどの燃料供給が一時的に停止し、ビットコインで440万ドル相当の身代金が支払われました。

ハイブリッド ワークでランサムウェアやその他のサイバー攻撃の被害に遭った他の企業として、ドイツの化学製品販売業者であるBrenntagが挙げられます。このケースでは、ランサムウェア集団であるDarksideがBrenntagの北米ネットワーク上のデバイスを暗号化し、暗号化されていないファイルを盗み出しました。その後、同様に身代金としてビットコインで440万ドル相当が支払われています。

サイバー犯罪者はあらゆる業界や規模の企業を攻撃しますが、Accentureは「The Cost of Cybercrime (サイバー犯罪による損失)」レポートで、すべてのサイバー攻撃の57%がビジネスに対して実行されていると報告しています。また、Accentureの別のレポート「How Aligning Security and the Business Creates Cyber Resilience (セキュリティとビジネスの連携がサイバー耐性を生み出す方法)」では、1社あたりの平均攻撃回数が2021年には前年比で31%急増したことを明らかにしています。一方、データ侵害がもたらす1社あたりの平均被害額は、ビジネスのダウンタイム、ランサムウェアへの支払い、修復、法務関係、およびその他の費用を含めて386万ドルに達しています。

費用対効果の高いより優れたアプローチの採用

ゼロトラスト アーキテクチャーは損失の大きい侵害を防ぐだけでなく、攻撃対象領域を排除することもできます。また、複雑性の軽減やユーザー エクスペリエンスの向上、企業データの保護が可能になります。

Sanminaは、世界規模の電子機器製造サービス市場で急成長を遂げている分野にサービスを提供する、大手統合製造ソリューション プロバイダーですが、同社の例は代表的です。Sanminaはゼロトラストの原則を採用し、高度なインダストリー4.0をサポートするためにシステムの再構築に着手することでクラウド トランスフォーメーションを進めていましたが、ほどなくして、同社のセキュリティ部門は従来のVPN技術ではゼロトラストを実現できないことに気づきました。

「境界がなくなった現代の環境に適したアクセス ソリューションが必要でした」とSanminaの情報セキュリティ担当VPである**Matt Ramberg氏**は述べています。

35,000人を超える従業員を抱えるSanminaは、多くの企業と同様に、コロナ パンデミックをきっかけに以前に増してモバイルかつリモートで作業をする状況となり、ゼロトラストの実現が優先されるようになりました。

「毎日、数千人がリモートで働き、数万という数のアセットにアクセスする必要があります。VPNは時代遅れの手法で、実際に攻撃対象領域を生み出し、サイバーセキュリティ上のリスクを高めていました」とRamberg氏は続けます。

数々の選択肢を検討した結果、SanminaはZscaler Private Access™(ZPA)を導入することでZscaler Zero Trust Exchange™プラットフォーム機能を拡張する決断をしました。

Zero Trust Exchangeの基本的な構成要素であるZPAは、ユーザーやデバイスをネットワークではなく、アプリケーションに接続します。また、脅威の侵入経路となるバックドアを作成するファイアウォールやVPN[2]とは異なり、Zero Trust Exchangeはユーザーとアプリケーションを外部の脅威から見えないようにすると同時に、企業がユーザーのアクセスを制限し、企業ネットワークではなく必要なアプリケーションのみに接続することで、脅威の水平移動を防止します。

Zero Trust Exchangeを採用したSanminaのサイバーセキュリティ部門は、ユーザーとアプリケーション間のすべてのトラフィックをきめ細かく制御、保護しながら、内部アプリケーションをセキュリティ上の脆弱性から保護しています。これはVPNでは実現できません。

「境界がなくなった現代の環境に適したアクセス ソリューションが必要でした」

SANMINA
情報セキュリティ担当VP
Matt Ramberg氏

[2]境界防御型ファイアウォールの5大リスク＋それらを克服する1つの方法 - *Zscaler*

また、ファイアウォールやVPNを使用する場合と比べて、同社のユーザーがパブリック アプリケーションやプライベート アプリケーションにより高速かつシームレスにアクセスできるようになったことからも、Zero Trust Exchangeへの投資効果が大きいことがわかります。

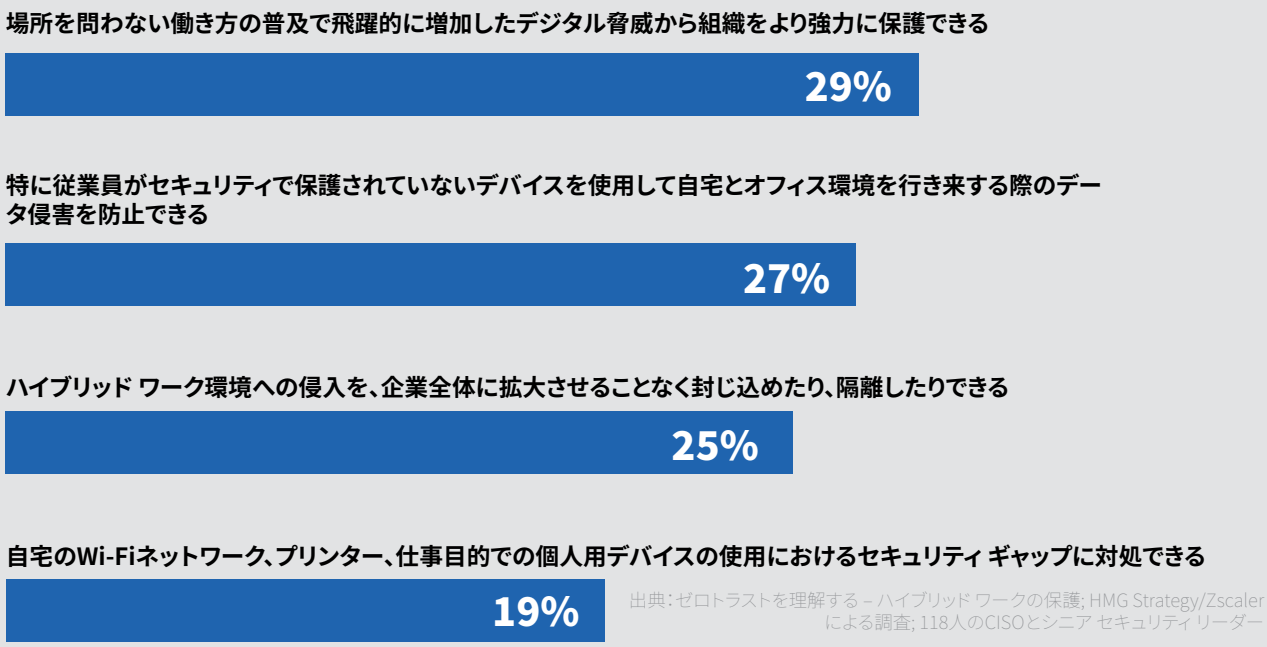
さらに、従来のファイアウォール、VPN、Webゲートウェイを取得、構成、管理、更新する場合と比べてIT管理にかかる費用が削減されます。「世界各地に複数の物理アプライアンスがあり、それぞれに独自の構成、ルール、パッチ、アップデート、メンテナンス契約が必要でした」とRamberg氏は話します。

ゼロトラスト アーキテクチャーを採用したSanminaは、インダストリー4.0技術の安全な利用拡大、IT管理コストの削減、敏捷性を高める吸収合併プロセスのスピードアップを実現し、同時にユーザー エクスペリエンスも改善しました。次のセクションでは、このセキュリティ手法の採用が急がれている背景と、実際に採用したことでメリットを享受した他の一流企業の例を紹介します。

ゼロトラストによるセキュリティの強化

ハイブリッド ワークの環境にゼロトラストのセキュリティ モデルを適用した場合の主なセキュリティ上のメリットは何ですか?

表2:



出典:ゼロトラストを理解する – ハイブリッド ワークの保護; HMG Strategy/Zscalerによる調査; 118人のCISOとシニア セキュリティ リーダー

CISOやセキュリティ リーダーが挙げているように、ハイブリッド ワーク環境にゼロトラストのセキュリティ モデルを適用するセキュリティ上の最大のメリットは、場所を問わない働き方の普及で飛躍的に増加したデジタル脅威から組織をより強力に保護できるという点です。

ゼロトラスト モデル採用の背景にある緊急性

オフィス勤務を再開したり、オフィス環境とリモート環境を使い分けたりする従業員が増加したことで、攻撃対象領域が拡大し、各企業のデジタル フットプリント全体に新たな脆弱性が生まれています。こういった課題はCISOやセキュリティ部門にとって大きな懸念材料となりつつあります。

従業員は、セキュリティで保護されていないデバイスを使用してオフィス環境とリモートワーク環境を絶え間なく行き来するため、サイバー犯罪者や国家レベルの攻撃者からデータ侵害やその他のサイバー攻撃を受ける可能性が高くなっています。HMG StrategyとZscalerの調査対象となった各セキュリティ リーダーが、ゼロトラスト アーキテクチャーを採用していると答えた主な理由はここにあります。

Lorenzinは次のように述べています。「ホーム オフィスであっても、カフェや会社のオフィスであっても、また、ラップトップを使用していても、クラウドベースのDesktop as a Service経由で接続していても、リソースへの同じアクセスが必要で、さらにアウトバウンド トラフィックに対しても同じ保護が間違いなく必要です。ゼロトラストは、一元化されたポリシーと可視性を実現する最適なアプローチです。まとまりがなく、十分な可視化と制御を提供できない複数の異なるソリューションに依存し続ける必要はないのです」

世界的に拡大するリモート ファーストの働き方を保護するCareem

ゼロトラストのセキュリティ モデルは、中東地域で屈指の配車サービスを手掛ける**Careem**にとっては当然の選択肢でした。

Careemが設立された2012年当時、ITセキュリティには昔ながらの城と堀のアプローチが使用されていました。しかし、ドバイを拠点とする同社が近年リモートをメインとした働き方で、中東と北アフリカ全体で飛躍的に成長を遂げるにつれて、経営陣は従来型のセキュリティ モデルが急速な成長の妨げとなっていることを認識するに至りました。

CareemのCIOおよびCISOであるPeeyush Pate氏は次のように述べています。「当社の業務規模が4倍になると予想される中、従来型のセキュリティ インフラストラクチャーがリソースを大幅に浪費しており、従業員を効果的に採用できず、ビジネス目標の達成を妨げていることに気付きました。我々は、セキュリティのアプローチ全体を最新にする必要があったのです」

クラウドを活用したアプリ開発モデル、リモート中心の働き方、ビジネスの成長をサポートすることを目的として、Careemは50を超えるファイアウォールと数十種類の仮想プライベート ネットワーク(VPN)アプライアンスを含む従来のセキュリティ インフラストラクチャーに代わり、Zscaler Zero Trust Exchangeプラットフォームを搭載したゼロトラスト アプローチの導入を決断しました。

「データ、従業員、お客様を保護するゼロトラストのセキュリティ サービス エッジ(SSE)モデルを構築する際、Zero Trust Exchangeプラットフォーム以外に選択肢はありませんでした」とPatel氏は続けます。

Careemは、セキュリティ インフラストラクチャーを合理化および簡素化するために、Zero Trust Exchange内で複数のサービスを採用しました。その基盤として、SaaSアプリケーションとインターネットへのアクセスを保護するZscaler Internet Access™ (ZIA)、パブリック クラウド インフラストラクチャーやデータ センター内で実行されているCareemのプライベート アプリケーションへのアクセスを保護するZscaler Private Access (ZPA)、そしてユーザーに影響が出る前にアクセスの問題をプロアクティブに検出して対処するZscaler Digital Experience (ZDX)を導入しました。

また、プラットフォーム内においては、SaaSアプリケーションとIaaS環境の内部を調査して保存データを保護するクラウド アクセス セキュリティ ブローカー(CASB)や、クラウド内で機密性の高い個人データを取り扱う際の法規制の順守をサポートするクラウド情報漏洩防止(DLP)も導入しています。

Zero Trust Exchangeを導入したCareemは、ネットワーク セキュリティのストレスやコストの問題を解消しただけでなく、社内全体で敏捷性、生産性、リソースの強化を実現しました。

*Patel*氏は次のように述べています。「従業員からは、VPNアクセスに対する不満の声が非常に多く寄せられていました。ZPAを含むプラットフォームを採用したことで、こういった不満が解消されただけでなく、全体的なユーザー エクスペリエンスが大幅に改善しています。これに伴い、社員やCSRのネット プロモーター スコア(NPS)が70%増加しました」と続けます。

さらに、Careemは大幅なリソース削減に成功し、その分を開発エリアに再投資しています。「エンジニアリング アプリケーションへのアクセスを簡素化することで、年間約20,000時間を開発に充てられるようになりました。リソースを取り戻した当社は、ビジネス価値の創造に向かって再び歩みを進めています」と*Patel*氏は話します。

Careemが実際に経験したように、ゼロトラスト アプローチは、ハイブリッド ワークの環境でより強力な制御と保護を提供するだけでなく、敏捷性、生産性、コスト削減においても優れた効果を発揮しました。最後のセクションでは、ゼロトラスト アーキテクチャーの導入に関する推奨事項を紹介します。この推奨事項は、企業のハイブリッド ワークをより安全に保護することを目的としています。

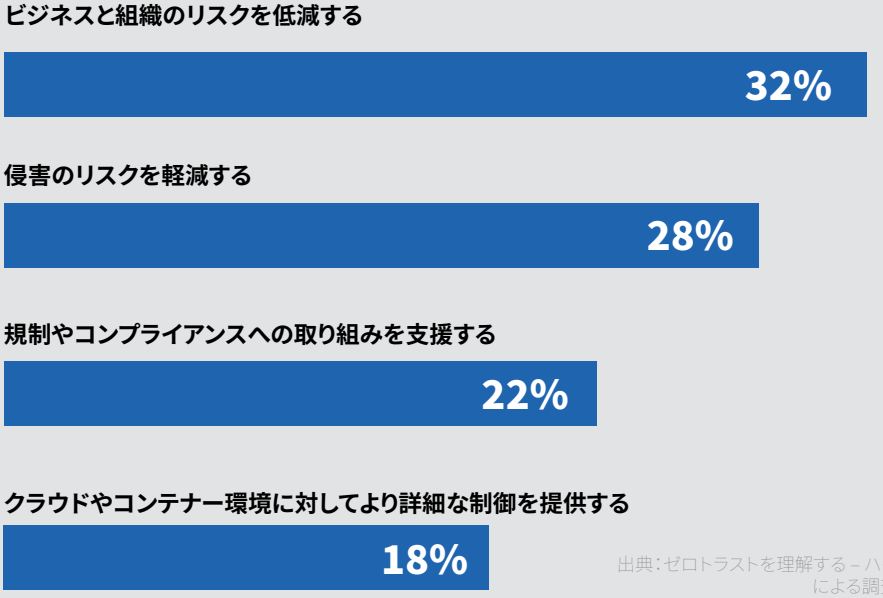
「データ、従業員、お客様を保護するゼロトラストのセキュリティ サービス エッジ(SSE)モデルを構築する際、Zero Trust Exchangeプラットフォーム以外に選択肢はありませんでした」

PEEYUSH PATEL氏
CIO兼CISO
Careem

ゼロトラストのメリット：リスクの軽減、制御の強化

ゼロトラストのセキュリティ モデルを採用した場合の主なビジネス上および運用上のメリットは何ですか？

表3:



出典：ゼロトラストを理解する – ハイブリッド ワークの保護; HMG Strategy/Zscaler による調査; 118人のCISOとシニア セキュリティ リーダー

ゼロトラスト モデルが生み出すビジネスと運用のメリット

Sanmina や Careem、そしてその他の企業がゼロトラスト アプローチの採用を通じて得たビジネスや運用上のメリットは、Lorenzin が目にした Zscaler の他の顧客のケースでも強みとなっています。

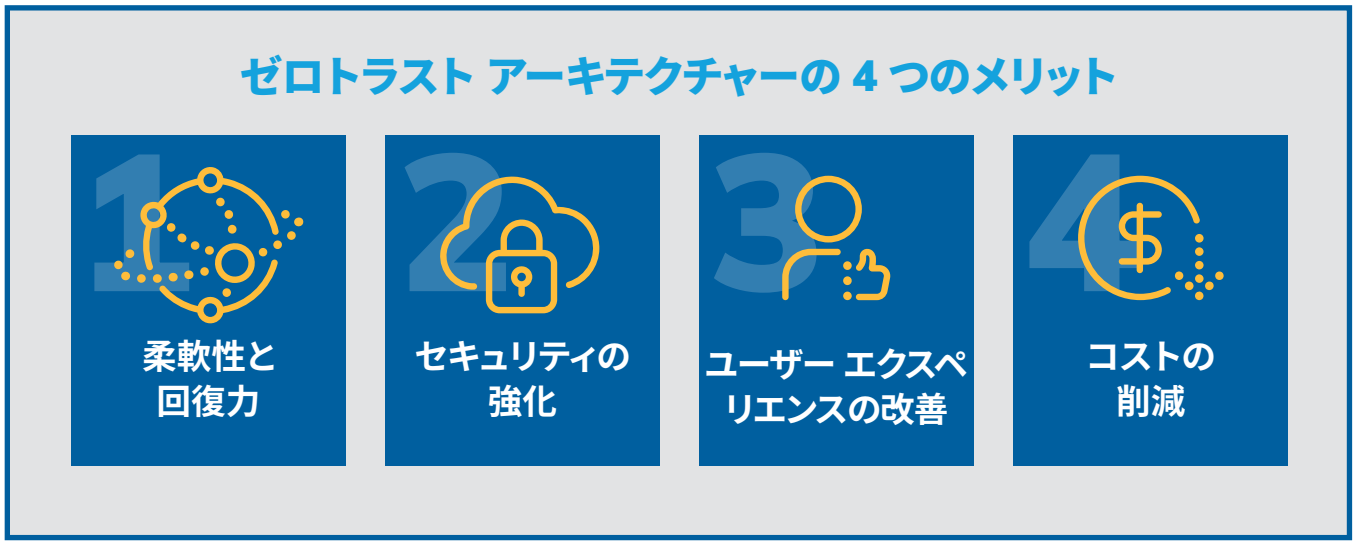
Lorenzin は次のように述べています。「ゼロトラスト モデルには主に 4 つのメリットがあります。**1 つ目は柔軟性と回復力です。**これには迅速な導入と、組織の進化にスピーディーに適応する能力が含まれます。

2 つ目はセキュリティの強化で、外部の攻撃対象領域をなくす能力が含まれます。これは、不正な水平移動を適宜抑制し、排除する手段になります。

3 つ目はユーザー エクスペリエンスの改善で、アプリケーションへのアクセスが今まで以上に高速で簡単、そして一貫性があることが含まれます。

そして、**最後のメリットはコストの削減**です。

世界中に展開されている複数の VPN ゲートウェイだけでなく、それらに付随したアプライアンスや機能 (ロード バランシング、DMZ ファイアウォール、DDoS 保護) のスタックへの設備投資を排除できます」



ゼロトラストの実現に向けて一歩踏み出す

ゼロトラストへの歩みを始めたばかりのCISOやセキュリティ リーダーであれば、簡単でシンプルなユース ケースの特定から始めることをお勧めします。そして、ゼロトラストの原則を適用し、組織がすでに実施している制御を決定したら、実際にそのユース ケースを実行してメリットを実証します。

「新しいことへのチャレンジを恐れる必要はありません。最初から難しい問題に挑戦するのではなく、効果的かつ難易度の低いユース ケースから始めることが重要です」と*Lorenzin*はアドバイスしています。

その後で、セキュリティ リーダーはCEOや取締役員に「ゼロトラスト アーキテクチャーとは何か、それがどのようにリスクを軽減し、ビジネスの可能性を広げ、従来のネットワーク中心のセキュリティ アプローチよりも優れた柔軟性と敏捷性を組織に提供できるのか」を説明します。その際、技術に明るくない取締役員がゼロトラスト アプローチの概念を理解できるように、例え話を交えてわかりやすく説明することがポイントです。

また、パイロット プロジェクトの成功体験を共有して、ゼロトラスト アプローチの価値を実証しながら、より広範囲にわたるゼロトラスト戦略への投資支援を得るようにします。

ゼロトラストを実際に導入した際の知見や経験談を、他の実践者から聞くことも有益です。こういったつながりを作る場として知名度が高いCXO REvolutionaries Forumは、戦略的なゼロトラストの達成を後押しすると同時に、優先順位の高いユース ケースに対処できる最適なプラットフォームを持つ、実績あるゼロトラスト パートナーとの提携も推奨します。

「すでにこの分野で実績があり、知識を豊富に備えているひとから吸収してください」とLorenzinは話します。

以上で解説してきたように、ゼロトラスト アーキテクチャーの採用は今が最適なタイミングであるだけでなく、ハイブリッド ワークとデジタル ビジネスを保護するためには不可欠な存在です。実践する価値は大いにあると言えるのではないでしょうか。

HMG Strategy について

HMG Strategyは、テクノロジー業界のエグゼクティブをつなぐ世界有数のデジタル プラットフォームであり、企業のありかたを再考してビジネスの世界を再形成することを目的としています。当社の地域およびバーチャルCIOならびにCISO Executive Leadership Series、書籍、Digital Resource Centerは、リーダーシップ、イノベーション、トランスフォメーション、キャリア アップに関するCIO、CISO、CTO、テクノロジー業界のエグゼクティブによる独自の調査を提供します。

HMG Strategyのグローバル ネットワークは、40万人を超えるシニアITエグゼクティブ、業界エキスパート、世界規模のソート リーダーで構成されています。

HMG Strategy独自のビジネス モデルを支える7つの信頼の柱については、こちらで詳細をご確認いただけます。

HMG Strategy:テクノロジー業界のエグゼクティブをつなぎ、企業のありかたを再考してビジネスの世界を再形成する最も信頼できるデジタル プラットフォーム。

Zscalerについて

Zscaler (NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchangeは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータ センターに分散されたSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、zscaler.jpをご覧いただくか、Twitterで@zscalerをフォローしてください。