ホワイト ペーパー

ハイブリッド ワークの生産性向上にセキュリティとユーザー エクスペリエンスが重要な理由

はじめに

これからはハイブリッド スタイルで仕事をしていく時代です。この 3 年間、多くの組織がリモート ワークを導入するために急ピッチでテクノロジー トランスフォーメーションを進めましたが、リモートとオンサイトの双方にそれぞれのメリットがあることが明らかになってきています。在宅勤務への切り替えを急きょ余儀なくされたことで、これまで実際に顔を合わせながら、チームとしてのつながりを強めつつ企業文化を育んでいた日常がどれほど価値のあることか、企業は改めて実感することとなりました。しかし同時に、リモート ワークは従業員がプライベートと仕事のバランスをとりながら、高い生産性を確保できることもわかっています。

リモートとオンサイトの両方のメリットを活かすために、多くの企業が一定日数のオフィス勤務を呼びかけるようになっていますが、これまで以上に柔軟で適応性に優れた多様な働き方を推進しています。

企業の 77% が恒久的なハイブリッド ワーク ポリシーを採用しており、従業員がオフィスで働く日を選択できる自由度の高いハイブリッド モデルが最も一般的となっています。このモデルの最大のメリットは従業員の柔軟性を最大限に引き出せることで、仕事における満足度だけでなく、多くの場合、生産性の向上にもつながります。

生産性と仕事の満足度の向上は、高度なスキルや知識を持つ従業員の需要に供給が追い付いていない現在、特に重要です。先行き不透明な経済状況が続いているにもかかわらず、現在、労働市場は歴史的な人材不足にあり、全米商工会議所が収集したデータによると、米国には 1,000 万を超える求人が出ている一方、求職中の失業者は 600 万人にすぎず、結果的にあらゆる業界や規模の企業が現場スタッフから経営幹部に至るまで、ポジションを埋めるのに苦労していることがわかっています。

労働力不足が叫ばれる中、ユーザーがオフィスで作業するときも、自宅やそれ以外の場所で作業するときも、仕事の満足度や生産性に貢献するテクノロジーを活用したエクスペリエンスを提供することが、企業に強く求められています。

しかし、すべての組織が、従業員がどこにいても業務に必要なすべてのアプリケーションにアクセスできるようにするための長期的な戦略、つまりアプリケーションがクラウドまたはプライベート データ センターのどちらでホストされていても、シームレスで安全なアクセスと一貫したエクスペリエンスを提供できる戦略を持ち合わせているわけではありません。

ここで必要なのは、優れたユーザー エクスペリエンスを確保しつつサイバーセキュリティ リスクから組織を保護する新しいソリューションです。組織が長期的な働き方戦略を構築するうえで特に重要なのが、リモートとオフィスの双方の従業員に優れたエクスペリエンスと強力な保護を確実に提供すること、そして在宅と出社のハイブリッド スタイルにおいてもこれを実現することです。

ハイブリッド ワークの保護になにが必要なのか

これまで、堅牢なセキュリティとリソースへのアクセスのしやすさは、どちらも重要でありながら両立することはほぼ不可能と考えるテクノロジー関係者は少なからず存在しました。しかし現在は、最新のクラウドベースのソリューションにより、セキュリティを損なうことなく、高速でシームレスなアプリケーション アクセスをユーザーに提供できるようになっています。また IT リーダーは、従業員の場所に左右されることなく、脅威対策を常時有効に保ち、低レイテンシーでの接続を実現しています。

このようなソリューションは、**セキュリティ**と**質の高いユーザー エクスペリエンス**という 2 つの主な要件を満たすことで、ハイブリッド ワークの導入を成功に導いています。では、それぞれ具体的に詳しく見てみましょう。

ユーザー エクスペリエンス

従来のハブ&スポーク ネットワークは、ハイブリッド ワークのニーズを満たしたり、生産性を向上させたりする目的で構築されたものではありません。このモデルに沿って設計されたネットワークでは、セキュリティ ポリシーは、企業の中央データ センター内にあるセキュリティ アプライアンスとファイアウォールのスタックによって施行され、すべてのトラフィックはこのハブ経由でルーティングされる必要があります。この方法でトラフィックをバックホールすると、アプリケーションのパフォーマンスが低下し、特に現在主流となっているビデオ会議ソフトウェアなどの最新のコラボレーション ツールで問題が発生します。日常のワークフローにおいてますます中心的役割を担うようになったこれらのツールは、レイテンシーがあるとうまく機能しません。

従来のセキュリティ アーキテクチャーでは、リソースへのスムーズなリモート アクセスをサポートできないため、煩雑なログイン操作が必要な仮想プライベート ネットワーク (VPN) などの複雑なソリューションを実装する必要があります。この場合、リモート ワーカーは、オフィスで作業するときとは大きく異なる方法で、業務に不可欠なアプリケーションなどのリソースにアクセスしなければなりません。

また、従業員の分散化が進むにつれ、IT 部門がエンド ユーザーに影響を与える問題を追跡して解決することもますます難しくなっています。デバイス、ネットワーク、アプリケーションの監視に使われる既存のツールは、アプリケーション配信チェーンを断片的にしか表示できません。そのため、ユーザーのデバイスとアプリの間には死角が生まれてしまい、IT 運用部門とサービス デスクは、可視性を得るために複数のツールからデータを手動でエクスポートして関連付ける必要があります。デジタル エクスペリエンスをエンドツーエンドで可視化できないと、IT 部門は「消火活動」ばかりをすることになります。ユーザーが影響を受けないうちに問題を積極的に特定して解決することができず、常に、問題が報告されてから解決に奔走しているのが実情です。

そこで必要となるのが、インターネットやプライベート アプリケーション、Software as a Service (SaaS) アプリケーションにどこからでも高速かつシームレスにアクセスでき、すべての従業員に常に最高のユーザー エクスペリエンスを提供できるソリューションです。技術的な観点からいうと、これは、ユーザーと接続先のアプリケーションとの間の最短パスを確保するダイレクト ピアリングによって実現できます。ダイレクト ピアリングは、VPN やファイアウォールの必要性を排除することで、レイテンシーを大幅に削減します。

また、IT 部門がデジタル エクスペリエンスをリアルタイムで監視して、エンド ユーザーが経験している状況をすぐに確認できるようなソリューションも必要です。こういったソリューションを採用することで、ユーザーが問題に気付く前の段階で、パフォーマンスを最適化できます。

セキュリティ

リモート ワークが大規模に導入されたことで、多くの新しいデバイスが企業ネットワークに接続してリソースにアクセスしようとするため、攻撃対象領域が劇的に増加しています。脅威アクターは現在、過剰に利用されている VPN やファイアウォールに狙いを定め、ここで提供される限られた保護をすり抜ける手段を模索しています。ネットワークとその中にあるすべてのリソースに完全にアクセスできるようになると、組織にとって最も価値のあるデータ資産が流出する可能性が生じてしまいます。

現代の複雑なコンピューティング エコシステムで効果的に侵害を防止するためにも、ネットワーク全体へのアクセスという概念を捨て、代わりに、アクセスは個々のアプリケーションにのみ、必要に応じてその都度許可されることが重要になってきます。これは、ゼロトラスト セキュリティ アプローチの中核となる概念、「マイクロセグメンテーションの原則」と一致し、この原則を順守することで、脅威アクターが侵害された 1 つのアカウントを出発点に他のリソースにアクセスする水平移動の可能性を排除できるだけでなく、アプリ

ケーションがインターネット上で検出されないようにすることもできます。基本的には、これで攻撃対象領域全体が排除されます。

現在、ほとんどの攻撃トラフィックは暗号化されていますが、レガシー ファイアウォールは暗号化されたトラフィックに潜む脅威を検出できません。そのため、効果的なデータ保護には、トラフィックがどこから来て、どこに向かうのか、デバイスの所有者が従業員なのか企業なのかなどの条件に左右されることなく、すべてのトラフィックを検査できる新しいアプローチが非常に重要となります。

また、複雑な分散環境においても、セキュリティ部門が一貫したデータ保護ポリシーをシームレスに適用できる新しいソリューションも必要です。

アプリケーションとユーザーの強力なゼロトラスト ネットワーク アクセスを、場所を問わずに実現する Zscaler Zero Trust Exchange

新しいハイブリッド ワークを保護するために、ゼロトラストを採用する企業は増えています。Zscaler は、こうした組織がコストと複雑さを最小限に抑えながら、生産性の維持に必要なアプリケーションに従業員が安全にアクセスできるように、Zero Trust Exchange を構築しました。企業規模でゼロトラスト セキュリティを提供するように設計された Zero Trust Exchange では、最小特権アクセスの原則が適用され、すべてのユーザーやアプリケーションは本質的に信頼されないものとみなされます。これを、あらゆるネットワークや場所で、ユーザー、ワークロード、デバイスのすべての通信を保護する単一のプラットフォームから実現します。

ハイブリッド ワークのための ZTNA

多くの組織がハイブリッド ワーカーやリモート ワーカーをサポートしながらセキュリティ リスクを軽減しようしているため、ゼロトラスト ネットワーク アクセス (ZTNA) の概念は、急速に浸透しています。ZTNA は、企業のアプリケーションやリソースの周囲にアイデンティティーやコンテキストに基づいた論理的なアクセス境界を作成するという、アナリスト企業の Gartner が最初に提唱した考え方です。この境界を適用するために、ZTNA サービスは、許可されたユーザーとアプリケーション間の接続を仲介し、ゼロトラストベースのセキュリティ ポリシーに従ってのみアクセスを許可します。

しかし、ZTNA のメリットは単に VPN の代わりとなる機能を持つという域を超えて、オフィスから接続しているユーザーやリモートで接続しているユーザーにまで及びます。強力な ZTNA では、ユーザーはオンサイト勤務、自宅勤務を問わず、同じレベルでのゼロトラストベースのセキュリティを利用できます。

強力な ZTNA を実現するには、ZTNA 機能を拡張してオンサイトとリモートの両方のユーザーで同じように機能させ、ユーザー エクスペリエンスやセキュリティに違いが出ないように徹底する必要があります。これを実現するには、ローカル ユーザーが企業のデータ センター内でホストされるアプリケーションへアクセスする場合でも、クラウド内の場合と同様に、ユーザーとアプリケーション間の安全な直接アクセスを提供できるソリューションが必要です。

クラウドネイティブ プラットフォームである Zero Trust Exchange は、ユーザーと管理者の両方に可能な限り最高のエクスペリエンスを提供しながら、オンサイトやリモートからインターネット、プライベート アプリケーション、SaaS アプリケーションへの高速で安全な接続を仲介します。Zero Trust Exchange は、以下の 3 つを提供することでユーザー エクスペリエンスとセキュリティの両立を実現します。

- どこからでも高速でシームレスなアクセス：SaaS アプリケーションとのダイレクト ピアリングや、ユーザーに最も近いブローカーを介するアクセスを利用することで、トラフィックが常にユーザーと宛先の間の最短パスを通るようにします。同時に、VPN やファイアウォールの必要性を排除します。
- ビジネス リスクの軽減：アプリケーションへの直接アクセスを提供することで、マイクロセグメンテーションを実施し、ユーザーとアプリケーションの間に 1 対 1 の接続を作成して攻撃対象領域を減らします。ユーザーのアカウントが侵害された場合でも、脅威がネットワーク上で移動することを防ぎます。
- 隙のないデジタル エクスペリエンス：Zero Trust Exchange を使用すると、IT 部門はデジタル エクスペリエンスを監視してパフォーマンスを最適化でき、エンド ユーザー エクスペリエンスの低下を未然に防げます。これにより、生産性に影響が出る前に、アプリケーション、ネットワーク、デバイスの問題を速やかに修正できます。

Zscaler Zero Trust Exchange は、特に Zscaler Private Access (ZPA) Private Service Edge が導入された今、強力な ZTNA を達成するための完璧なソリューションです。ZPA Private Service Edge は、Zscaler Zero Trust Exchange のすべてのメリットを、企業のデータ センターでホストされているプライベート アプリケーションに拡張します。ZPA Private Service Edge が Zero Trust Exchange のすべての機能をプライベート データ センターまたはパブリック クラウド エッジに拡張することで、オフィス内で働くユーザーのレイテンシーが削減され、アプリケーション パフォーマンスも向上します。同時に、ゼロトラストのセキュリティ ポリシーも施行されます。ZPA Private Service Edge では、このようなポリシーが可能な限りエッジの近くで施行されるため、ローカル ユーザーもリモート ユーザーも、データ センターまたはクラウドのどちらのアプリケーションにアクセスする場合でも、同じエクスペリエンスを得られます。

Zscaler Zero Trust Exchange を採用することで、組織は真のゼロトラスト セキュリティ態勢を実現できます。費用対効果と効率性に優れた方法で、今日のハイブリッド ワークが求めるあらゆるセキュリティとパフォーマンスのニーズを満たすことができます。

zscaler™ | Experience your world, secured.™

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 SSE 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。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp