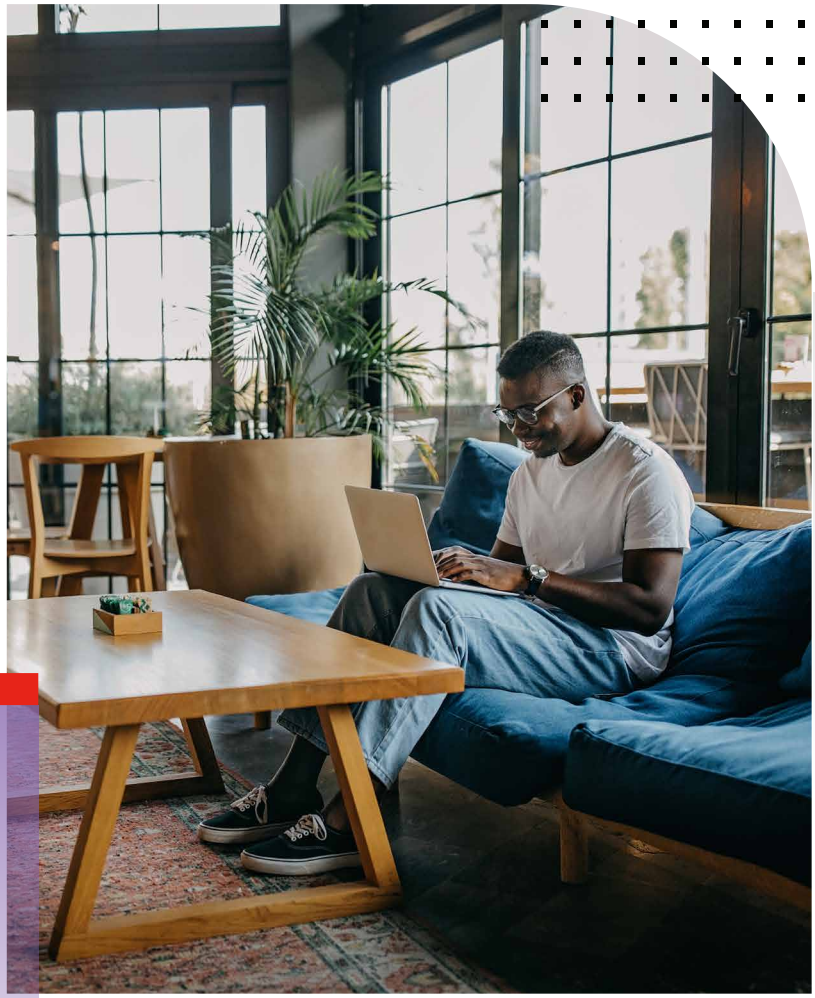
WHITE PAPER

どんな場所からでも働ける環境のシンプルな実現方法とは？

ユーザーの場所を問わず、一貫したセキュリティを提供



概要

この約 10 年間でテクノロジーは着実に進化し、従業員が使用するデバイス、働く場所、アクセスできるリソースにおいて柔軟性が向上しています。BYOD（私用デバイスの活用）とクラウドアプリケーションアクセスは、柔軟な仕事環境を実現するための最初のステップでした。

場所に縛られない働き方（WFA：Work-from-Anywhere）戦略が数年後、本格的に採用されるものになっていた矢先、COVID-19 の世界的パンデミック（大流行）により、その必要性を加速させました。そして現在、多くの従業員が WFA による選択の自由を会社に求めています。問題は、従業員の生産性と安全性を維持するハイブリッドな仕事環境を実現する方法です。

「フォーティネットグローバル脅威レポート」によると、ランサムウェアのインシデントは 2020 年 6 月から 2021 年 6 月までに約 1,100% 増加しました [1]。

ハイブリッドな労働力の確保

パンデミックが発生したとき、テレワークをサポートできる企業や組織はわずかでした。急遽、従業員はセキュリティの低いホームネットワークから会社のネットワークへ接続することになったのです。アクセス制御が不十分で、エンドポイントデバイスに脆弱性がありました。当然のことながら、サイバー犯罪者もたちまちその脆弱性を悪用するようになりました。Forrester によると、組織の 67% が、テレワークの脆弱性を狙ったサイバー攻撃により、ビジネスに影響を及んだことがあると言われています [2]。

多くの企業が将来を見据えて、大多数の従業員を対象に、最低でも一部の労働時間において継続的にテレワークを計画しています。従業員の生産性を維持するためにすでにツールやソリューションに投資しているため、従業員が引き続きテレワークを望めば、会社としてもそれを否定する理由はありません。

ハイブリッド勤務形態の場合、1 週間のうち数日だけ出社し、残りを自宅やリモートで勤務することが考えられます。こうした従業員や使用デバイスは、各環境間をシームレスに移動する必要性が生まれます。これに伴い、どこにいてもクラウドやデータセンターのアプリケーションやリソースに安全にアクセスできる必要があります。

場所に縛られない働き方をサポートするために、企業はセキュリティを考慮し、ユーザーがどこにいても追跡、有効化、保護できるソリューションを導入する必要があります。こうした企業では、ゼロトラストアクセス（ZTA）とゼロトラストネットワークアクセス（ZTNA）を組み合わせたエンドポイントのセキュリティが必要になります。また、安全な接続性のために、セキュア SD-WAN（ソフトウェアによって定義された広域ネットワーク）と SASE（セキュアアクセスサービスエッジ）も必要になります。アクセスポリシーエンジンは、ユーザーおよびデバイスの ID、場所、デバイスタイプ、態勢に基づいて適切なアクセスを提供し、安全なアクセスを確立する必要があります。

多くの企業が直面している問題は、多数の独立系ベンダー製品を使用して WFA をサポートしようとしていることです。エンドポイント保護（EPP）を提供するベンダーがいれば、エンドポイントの脅威検知とレスポンス（EDR）を提供するベンダーや、認証基盤などを提供するベンダーもいます。また、データセンター、拠点、使用するさまざまなクラウドプラットフォームに異なるベンダーのファイアウォールを配備している場合もあります。多数のベンダーを利用することで、緊密で信頼性の高いソリューションを構築することはほぼ不可能です。最終的には一時的に導入した製品・ソリューションにより状況を複雑化してしまうことで全体的な IT コストが増えてしまいます。

これらに代わる解決策として、より良い方法は完全統合型サイバーセキュリティ・メッシュ・プラットフォーム・アーキテクチャの一部としてソリューションを導入することです。この方法は、個別に運用される製品・ソリューションに比べ、セキュリティが強化され、管理や連携が簡素化され、TCO（総所有コスト）が向上します。

あらゆる場所で保護

WFA をサポートするには、ユーザーが会社、自宅、または会社や自宅以外の出張先で働くときに機能するセキュリティが必要になります。それぞれの場所で課題がありますが、信頼できるセキュリティテクノロジーで完全な保護を実現する必要があります。

フォーティネットの「ランサムウェア調査レポート」によると、67% の組織がランサムウェアの標的になったことがあると回答しています [3]。

オフィス勤務

企業はビジネスを行う上でアプリケーションに依存しているため、従業員がオフィスで働く場合でも、アプリケーションへのアクセス、アプリケーションに接続するネットワーク、アプリケーションを実行するデバイスを保護することは、多層防御において最も重要な要素となります。ほとんどの職場では、ハッカーがアクセスしたいと考える顧客データ、サーバー、アプリケーション、ID 情報、ユーザー資格情報、ソースコードがあります。職場でユーザー、デバイス、サーバーを保護するには、次世代ファイアウォール（NGFW）が、重要な情報リポジトリに対するさまざまな防御の中で最初の手段となります。組織は、エンドポイントセキュリティ、ゼロトラスト、ID 管理を一体化して、NGFW を補完する必要があります。

- NGFW は、キャンパス、データセンター、拠点、クラウド環境において高度で一貫性のあるセキュリティを確保することで、外部からのアクセスを保護します。
- ZTNA エージェントと ID サービスは、アプリケーションや他のリソースへのアクセスを制御して、セキュリティを確保します。ZTNA は、アプリケーションへのアクセス、オフィスでの暗号化トンネル、ユーザー検証を制御する内部制御を提供します。
- ユーザーおよびデバイスセキュリティ用の EDR などのエンドポイントセキュリティ。EDR はユーザーデバイスを保護する手段を提供し、重要なデータと相互作用します。

また、オフィス環境には、セキュア SD-WAN などのネットワーキングおよびセキュリティソリューションも必要になります。このソリューションは、アプリケーション対応のインテリジェンスを備えたデータセンター、クラウド、拠点、キャンパスのロケーション間の WAN 接続を最適化する統合型セキュリティプラットフォームにより、高度なネットワーキングツールを提供します。

在宅勤務

リモートやハイブリッド型の従業員は、ノート PC、モニター、外部 Web カメラを使用して自宅環境からログインするのが一般的です。しかし、ホームネットワークの場合、市販のワイヤレスルーターを使用するため、セキュリティが不十分であることが多く、IoT（モノのインターネット）デバイスが脆弱である可能性があり、ハッカーのアクセス経路になってしまうおそれがあります。また、ホームネットワークを使用する従業員は、ビデオ会議や大きな帯域幅を要するアクティビティなどに関しても問題に直面します。家族や同居人など、家の人がビデオストリーミングやオンラインゲームで帯域幅を消費している場合、従業員の生産性にも影響を及ぼす可能性があります。在宅勤務のユーザーには、下記が必要です。

- 従業員とデバイスを保護する EDR などのエンドポイントセキュリティ。
- アプリケーションや他のリソースへのアクセスを制御してセキュリティを確保する ZTNA エージェントと ID サービス。
- 企業ネットワークをはじめ、クラウドやデータセンターのアプリケーションへの安全なアクセスを確保するホームネットワーク向けの企業クラスのセキュリティ。これには、ビデオストリーミングやゲームよりもビジネストラフィックを優先するトラフィック管理が含まれます。

ホームオフィスソリューションでは、企業のファイアウォール保護をホームネットワーク全体に拡張する必要があります。また、ホームネットワークをセグメント化して業務トラフィックを可視化し、ビジネスアプリケーションの帯域幅を最適化する一方、業務外のネットワークに対しては従業員のプライバシーを確保する必要があります。

出張先 / 外出先からの勤務

ユーザーが出張に行ったり、社外や主なリモートスペースで仕事をしたりする場合、特有の脅威環境にさらされることも少なくありません。モバイルユーザーが業務に必要なアプリケーションやリソースに接続するとき、使用するネットワークやアクセスポイントが不明な場合や、セキュリティ保護されていない場合があり、そこからネットワークが侵害されるおそれがあります。モバイルユーザーには、下記が必要です。

- 従業員やデバイスを保護する EDR などのエンドポイントセキュリティ。
- アプリケーションや他のリソースへのアクセスを制御してセキュリティを確保する ZTNA エージェントと ID サービス。
- 会社や自宅のネットワーク外にいる従業員を保護するクラウドベースのファイアウォール機能に対応した、リモートネットワークセキュリティ SASE ソリューション。

モバイルネットワークソリューションには、多要素認証、クラウドベースの SWG（セキュア Web ゲートウェイ）、CASB（クラウドアクセスセキュリティブローカー）が含まれます。

脅威インテリジェンスにより強化された統合型 WFA セキュリティ

WFA をサポートするために、企業はサイバーセキュリティメッシュプラットフォームを実用的な脅威インテリジェンスを備えた統合型システムとして構築し、あらゆる場所での脅威の識別や保護情報により、セキュリティ製品が通知されたり機能できるようにしたりする必要があります。このようなプラットフォームでのアプローチでは、ゼロトラスト、エンドポイント、ネットワークセキュリティを、共通の API（アプリケーションプログラミングインタフェース）とインテグレーションポイントのセットで統合できるため、一貫性のある安全な環境を維持しながら、ユーザーが 1 つの場所から別の場所にシームレスに移動できるようになります。IT の面では、サイバーセキュリティメッシュによりポリシーの作成や適用が簡素化され、設定の統一化、管理の一元化、およびユーザー、デバイス、データ、アプリケーション、ワークフローの監視や制御が可能になります。

場所に縛られない働き方は昨今のパンデミックにより重要性が高まりましたが、この傾向自体は既に進められていたことであり、パンデミックはそれを加速させたに過ぎません。ハイブリッド型の仕事環境が普及していますが、企業としてはこうした働き方モデルの安全性を確認する必要があります。

[1]「フォーティネットグローバル脅威レポート 2021 年上半期版」、FortiGuard Labs、フォーティネット、2021 年 8 月：
https://www.fortinet.com/jp/demand/gated/TR-21H1

[2]「Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work」、Forrester、2021 年 9 月（英語）：
https://www.tenable.com/analyst-research/forrester-cyber-risk-report-2021

[3]「2021 年ランサムウェア調査レポート」、フォーティネット、2021 年 11 月：
https://www.fortinet.com/jp/demand/gated/ransom-survey-2021

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

WP-Work-From-Anywhere-202203-R1