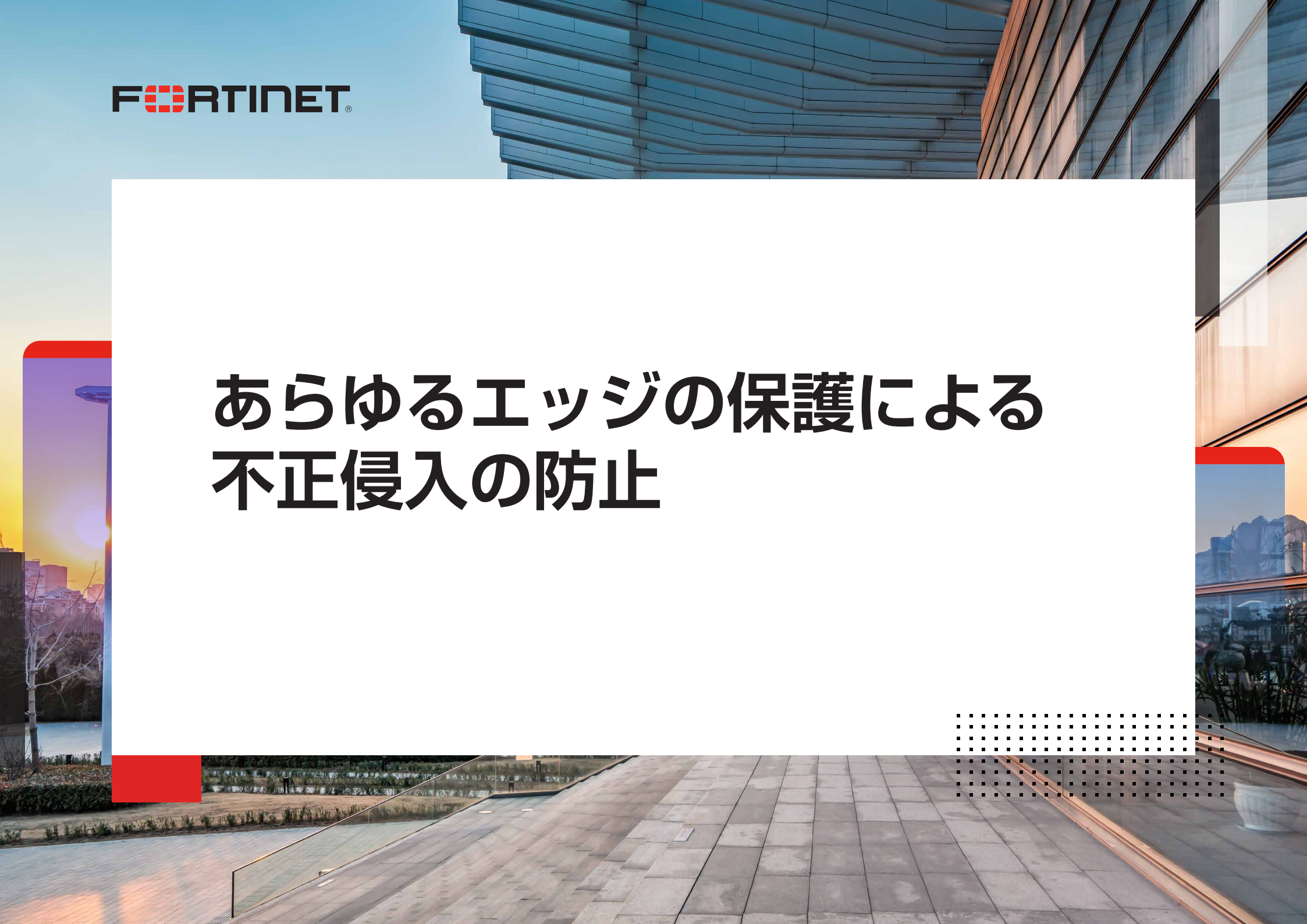


あらゆるエッジの保護による不正侵入の防止

目次

概要

今日のユーザーは、あらゆる場所であらゆるデバイスを利用し、あらゆるリソースに接続できるネットワークを必要としています。それと同時に、データセンターやキャンパスのネットワークを、次世代ブランチオフィス、プライベートやパブリックのマルチクラウドネットワーク、リモートワーカー、クラウドベースの SaaS サービスなどと連携したハイブリッド IT アーキテクチャで運用する必要があります。このような現状から、企業のセキュリティは、データ、アプリケーション、ワークロードにアクセスするすべてのユーザーとデバイスを保護し、追跡するため、移動し分散するネットワーク環境の完全な可視性を提供するという大きなプレッシャーに直面しています。

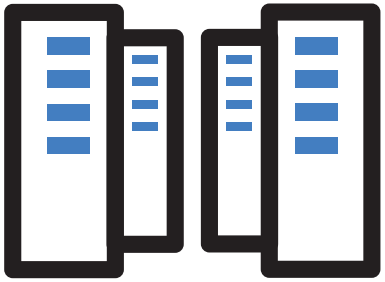
残念ながら、従来型のファイアウォールなどのセキュリティツールの多くは、このような課題を解決するように設計されておらず、ワークフローやデータが高度に予測可能な静的なネットワークチェックポイントを前提に設計されたものです。しかしながら、時代は変化しました。

新たな問題

データセンターは必要不可欠ではあるものの、もはや企業アプリケーションが置かれる主要な場所ではなくなり、あらゆる場所にアプリケーションを展開できるようになりました。トランザクションやワークフローに複数の環境やアプリケーションが関係するため、送信元、送信先、データパスが何度も変わる可能性があり、トランザクションをエンドツーエンドで追跡して保護するのは不可能です。

5G が普及し、特にトラフィック全体の 95% が暗号化されるようになったことで、従来型のファイアウォールが処理に追いつくのが困難になっています。暗号化されたトラフィック、特に SSL/TLS（セキュアソケットレイヤー / トランスポートレイヤーセキュリティ）トンネルが、リモートアクセスやトランザクションを保護する目的で広く使用されるようになりましたが、サイバー犯罪者も暗号化を利用して、企業のデータや機密情報を盗んだり、ランサムウェア攻撃を仕掛けたりします。ほとんどのファイアウォールは、パフォーマンスやユーザーエクスペリエンスに大きく影響することなく、暗号化されたトラフィックを復号してインスペクションすることはできません。そのため、暗号化されたトラフィック、特に超高速で移動するデータのほとんどがインスペクションされないのが現状です。

マルチクラウド環境とハイブリッドワーカーも、セキュリティ要件を大きく変える要因となっています。アジャイルアプリケーション開発やスケールアウト / スケールアップ機能がクラウドにより可能になったことで、リモートワーカーによって増加するアプリケーションアクセスへの対応も可能になりました。しかしながら、コンプライアンス、プライバシー、知的財産の保護などの理由から、多くのビジネスクリティカルアプリケーションをオンプレミスのデータセンターに置く必要があります。ところが、従来のファイアウォールの多くは、ユーザーからデータセンター、データセンターからクラウド、ユーザーからクラウド、データセンターからデータセンターへの相互接続モデルなどのハイブリッドデータセンターのユースケースをサポートできません。



データセンターは必要不可欠ではあるものの、もはや企業アプリケーションが置かれる主要な場所ではなくなり、あらゆる場所にアプリケーションを展開できるようになった

新たなソリューション

ハイブリッドアーキテクチャのサポートと保護には、分散ネットワーク全体の一元的な可視化が必要であり、これには、ネットワークのすべてのユーザーとデバイスに加えて、それらがアクセスするアプリケーションとリソースについての知識、さらには、あらゆる場所での異常な振る舞いや不正活動の特定が含まれます。必要なセキュリティリソースをすべて集結し、タイムリーな協調型のレスポンスを可能にする必要もあります。今日の拡大するネットワークとそこに存在する多数のエッジをサポートするため、多くの企業が、SASE（セキュアアクセスサービスエッジ）、SD-WAN（ソフトウェア定義型広域ネットワーク）、ZTNA（ゼロトラストネットワークアクセス）といった異種ソリューションを採用するようになったことで複雑化が進み、可視性やユーザーエクスペリエンスが低下し、攻撃への効果的なレスポンスが困難になっています。

これらの機能をネットワーク全体のセキュリティをコンテキストに応じて調整する統一されたプラットフォームに統合する、新しいNGFW（次世代ファイアウォール）アプローチが必要です。

キャンパスやデータセンター、マルチクラウド、支社、ホームオフィスなどと、セキュリティが必要とされる場所はさまざまですが、ユースケースは非常に似ています。そのためには、セキュリティを 3 つの主要機能、すなわち、「保護」、「統合」、「拡張」に分解する必要があり、この 3 つの概念を理解することで、シームレスなユーザーエクスペリエンスとビジネス目標に沿った保護を実現するセキュリティ戦略の実装が可能になります。

保護

アプリケーションのアクセスと利用を高速化するツールとの相互運用を含め、NGFW は、アプリケーションライフサイクル全体を認識する必要があり、これには、高度な画像認識やビデオコンテンツのフィルタリングに加えて、必要不可欠である Web フィルタリングを提供し、適切な使用とコンプライアンスが保証されるようにすることが含まれます。

NGFW ソリューションは、高度なセキュリティソリューションを提供し、IPS（侵入防止システム）やアンチマルウェアを統合することで、既知、ゼロデイ、未知の攻撃を防止する必要もあります。さらには、E メールセキュリティやサンドボックスなどの補完的な製品から常に共有される脅威インテリジェンスフィードをサポートすることで、最新の脅威の検知と防御を可能にするものである必要があります。

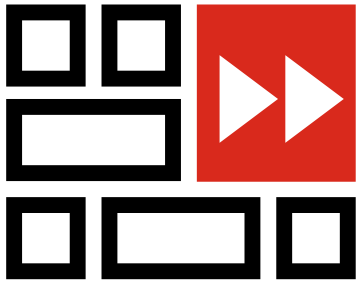
EDR（エンドポイントの脅威検知とレスポンス）や WAF（Web アプリケーションファイアウォール）を始めとするセキュリティシステムなどの他のソリューションとの相互運用が可能である必要もあります。ネイティブの脅威保護との組み合わせや他のテクノロジーとの統合により、現在および将来のあらゆる脅威からのネットワークの効果的な保護が可能になります。

統合

NGFW は、HTTPS セキュアチャネルに隠れてデータを盗んだりランサムウェアをロードしたりする高度な攻撃を完全に可視化できるものでなければなりません。オンプレミスの NGFW からの直接の提供あるいはクラウドベースの SASE による提供のいずれであっても、ネットワークとセキュリティの必要不可欠な機能を統一された 1 つのソリューションにシームレスに統合し、ルーティングと接続の高度な機能に動的セキュリティソリューションを組み合わせる必要があります。

アクセスを要求するユーザー、デバイス、アプリケーションを識別し、適切なネットワークセグメントに自動的に割り当てる必要もあります。これには、ネイティブに統合されたプロキシサービスが必要です。デバイスからの最初のアクセス要求で、ファイアウォールは、エンドポイントクライアント（ユーザーやサーバーの場合）やネットワークアクセス制御（IoT [モノのインターネット] / IIoT [産業用 IoT] デバイスの場合）ソリューションと連携する必要があります。そのため、多要素認証をサポートしてユーザーやデバイスの役割を判断し、関連するポリシーとリンクさせて、業務に必要なアプリケーションやネットワークのセグメントへのアクセスのみを許可する必要があります。

アプリケーションやワークフローがある環境から別の環境へ移動する場合も、NGFW があらゆる場所で同じポリシーを理解して実装し、適用する必要があります。この一貫性あるオーケストレーションと適用のアプローチと一元管理により、アプリケーション、ワークフロー、その他のトランザクションをエンドツーエンドでセキュリティが追跡できるようになります。



アプリケーションやワークフローがある環境から別の環境へ移動する場合も、NGFW があらゆる場所で同じポリシーを理解して実装し、適用する必要がある

拡張

ファイアウォールをどこに導入する場合であっても、確実に言えるのは速さが必要であり、将来的にはさらに加速させる必要があるということです。今日のデータセンターは、ビッグデータを活用した高度モデリング、低遅延の高速金融トランザクション、ハイパーパフォーマンスの大規模マルチユーザー環境のいずれであっても、大量のデータをトランザクション速度で生成し、処理します。

速さとは、ファイアウォールがいかに速くデータをインスペクションできるか、自動化をサポートできるかということです。NGFW は、高度で協調型のセキュリティを提供し、時間のかかる手動のプロビジョニングを不要にすることで、高速の攻撃からネットワークを効果的に保護する必要があります。手動の操作は、処理を遅らせ、構成エラーによってランサムウェアなどに攻撃されてしまう恐れもあります。

ところが、従来型のファイアウォールのほとんどがすでにほぼ限界の状態で動作しているため、成長するビジネスニーズに合わせて拡張することはできません。それは、ハイパーパフォーマンスを考慮して設計されていないためです。最大の問題は、グラフィックスカード、スマートフォン、クラウドサーバーなどのあらゆるものがカスタムチップで動作する時代に汎用プロセッサを採用していることです。セキュリティはプロセッサ負荷の高い活動であり、今日のパフォーマンス要件に対応するには、パフォーマンスを低下させたり、IT やセキュリティの限られた予算を圧迫したりすることなく、ファイアウォールのすべての機能を提供するスケーラビリティが必要です。

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

EB-Protecting-Every-Edge-202211-R1