SOLUTION BRIEF

フォーティネットのユニファイド SASE による ハイブリッドワーカーの保護

概要

攻撃対象領域は WFA（Work From Anywhere：場所に縛られない働き方）によって大幅に拡大し、ホームオフィスやモバイルワーカーも含まれるようになりました。このような複雑化はネットワーク、アプリケーション、リソースの保護を一層困難なものにしています。セキュアアクセスサービスエッジ（SASE）はこうした複雑さを解消し、IT チームがより適切に WFA ユーザーを保護できるようにします。

SASE ソリューションは、あらゆる規模の支社やリモート拠点で安全なアクセスと高パフォーマンスな接続を実現します。ただし、多くの SASE ソリューションは問題の一部しか解決できません。フォーティネットのユニファイド SASE は、包括的なシングルベンダー SASE ソリューションによって、WFA セキュリティのあらゆる課題に対処します。このソリューションは、必要とされるすべてのコンポーネントを提供し、複雑さを解消します。そのために、ソフトウェア定義型広域ネットワーク（SD-WAN）とクラウド提供型のセキュリティサービスエッジ（SSE）を統合し、ネットワーキングとセキュリティのコンバージェンスをネットワークエッジからリモートユーザーにまで拡張します。さらに、一元管理や統合エージェント、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（DEM）の機能も提供します。

84% の企業はハイブリット環境で働く WFA 従業員によるネットワークアクセスの保護を必要としています。多くの場合、WFA の従業員はさまざまな場所、例えばオンサイトや自宅、あるいは Wi-Fi 接続を利用できる場所であればどこからでもアクセスします [1]。

ハイブリッドワーカーの課題

ハイブリッドワーカーの保護には特有の課題が伴います。新たなネットワークエッジの急速な拡大や、WFA 従業員の増加によって、サイバー犯罪者がすぐにでも悪用できる脆弱性が生じているからです。一貫したセキュリティポリシーの適用と徹底、さらには全ユーザーのエクスペリエンスの最適化が必要とされています。

フォーティネットのユニファイド SASE は、Web、企業アプリケーション、Software-as-a-Service（SaaS）アプリケーションといったユーザーのアクセス先に関係なく、一貫性のあるセキュリティとユーザーエクスペリエンスを提供します。このソリューションは、世界中に 140 ヵ所以上の拠点がある高パフォーマンスで拡張可能なクラウドネットワークを備え、広範なカバレッジ、優れた拡張性、確かなセキュリティ制御を可能にします。

シンプル、シームレス、スケーラブルなセキュリティとネットワーキングをクラウドから提供

フォーティネットのユニファイド SASE は、他社ベンダーが提供する基本的な SASE コンポーネントはもちろんのこと、多種多様なセキュリティとネットワーキングの機能を提供します。ソリューションの内容は次の通りです。

エンドポイント保護、ゼロトラストネットワークアクセス（ZTNA）、DEM

エンドポイント保護、ZTNA、DEM には単一のエージェント「FortiClient」を使用します。

FortiClient は、ローカルとリモートの両方のエンドポイントを保護します。テレメトリによってエンドポイントを可視化し、すべてのフォーティネット セキュリティ ファブリック コンポーネントが統一ビューでエンドポイントを確認できるようにすることで、追跡、意識向上、コンプライアンスの徹底、レポート作成を支援します。

フォーティネットユニバーサル ZTNA は、ユーザーやアプリケーションの所在地に関係なく、柔軟なゼロトラストのアプリケーションアクセス制御を実行します。IT チームは ZTNA を使用して、ビジネスクリティカルなアプリケーションへのアクセスを、ユーザー単位およびセッション単位で認証、保護、監視することができます。ZTNA は、継続的かつほぼリアルタイムでデバイス態勢を評価し、コンプライアンス違反のデバイスやセッションを速やかに遮断します。

DEM によってトラブルシューティングが簡素化され、エンドツーエンドのユーザーエクスペリエンスを監視することができます。DEM はエンドユーザーエクスペリエンスを包括的なビューに表示し、それらのデータを測定可能なビジネス成果に変換する一方、平均修復時間（MTTR）を短縮します。フォーティネットは、エンドポイントデバイス、オンプレミスネットワーク、ユーザー、アプリケーションを包括的に監視するエンドツーエンドの DEM を提供します。ラストマイルの監視は、各クラウド拠点から最速の接続を実現します。ファーストマイルの監視は、ユーザーのローカルネットワークやエンドポイントデバイスに至るまで、問題点を容易に特定できます。

Firewall-as-a-Service（FWaaS）とセキュア Web ゲートウェイ（SWG）

FWaaS では、クラウドのトラフィック、アプリケーション、およびサービスに対応した高パフォーマンスな SSL インスペクションと、AI を活用した高度な脅威検知が可能です。フォーティネットの FWaaS ソリューションは、リモートユーザー向けの安全な接続を確立して維持すると共に、ユーザーエクスペリエンスを低下させることなくトラフィックを分析します。

SWG は、暗号化トラフィックなどの Web トラフィックを保護するさまざまな機能によって、高度な Web の脅威に対する防御を強化します。Web フィルタリング、アンチウイルス、ファイルフィルタリング、データ漏洩防止、その他のセキュリティ制御が連携し、管理対象 / 対象外のデバイスで多層防御戦略を実現します。

クラウドアクセスセキュリティブローカー（CASB）とデータ漏洩防止（DLP）

FortiGuard CASB サービスは、SaaS アプリケーションの包括的な可視化、制御、セキュリティを実現します。悪意のあるアプリケーションはインライン CASB によってブロックされます。

FortiGuard データ漏洩防止サービスは、ハイブリッド環境全体の機密データを、セキュリティ侵害、内部関係者による脅威、データ漏洩から保護します。

SD-WAN

アプリケーションステアリングや動的ルーティングなど、**クラウドで提供される SD-WAN** 機能は、企業アプリケーションへの最短パスを識別します。そして、それらの接続の整合性が変化した場合には修正を行うことで、リモートワーカーに優れたユーザーエクスペリエンスを提供し、それを維持します。

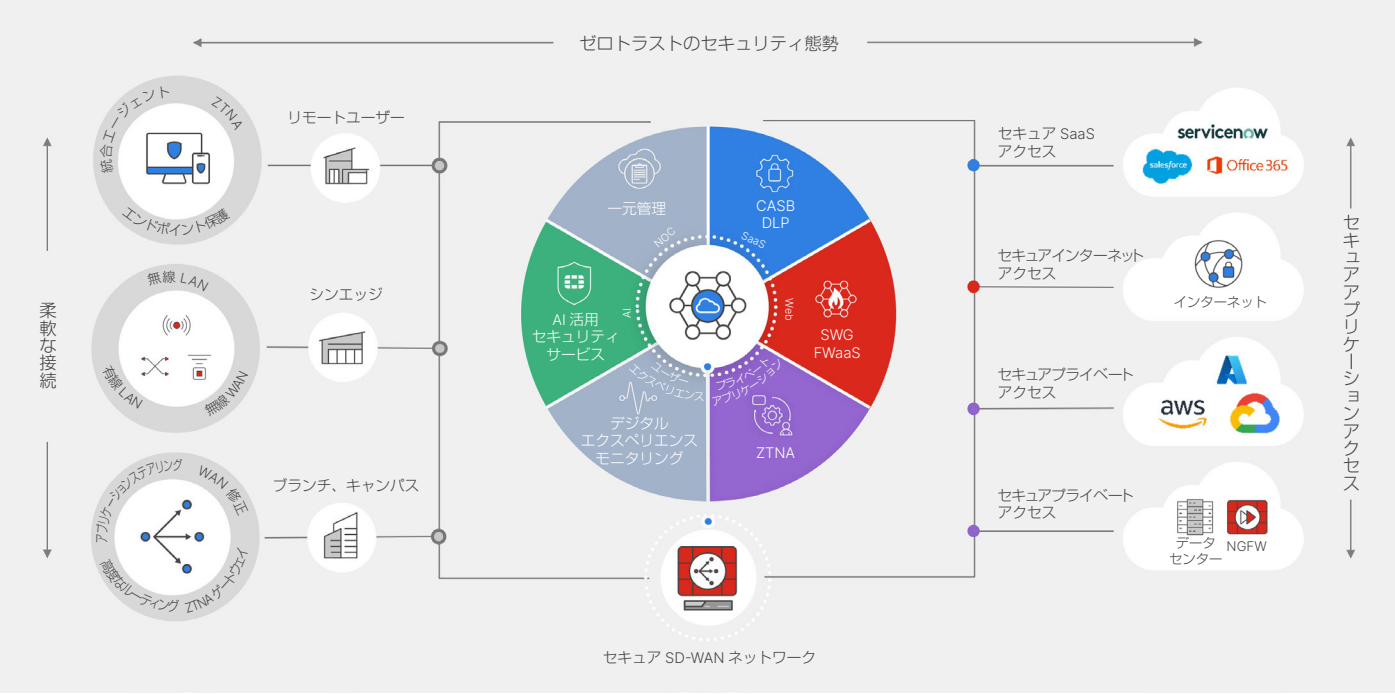


図 1：フォーティネットのユニファイド SASE と AI 活用セキュリティサービス

主要なユースケース

セキュアインターネットアクセス（SIA）

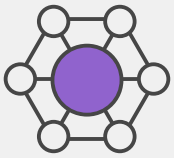
FWaaS と SWG の包括的な機能は、エージェントとエージェントレスの両方のアプローチをサポートすることで、管理対象と管理対象外のデバイスをどちらも保護します。ネイティブに統合された FortiGuard AI 活用セキュリティサービスは、ランサムウェアやその他の高度な攻撃からコンテンツとユーザーを保護します。

セキュアプライベートアクセス（SPA）

企業アプリケーションへのゼロトラスト接続と、独自の方法で統合された SD-WAN は、低遅延のアクセスを実現します。ZTNA は、ネットワークアクセスを制限することで脆弱性を排除します。フォーティネットのユニバーサル ZTNA では、きめ細かいアプリケーションアクセスを実装することで、明示的なアプリケーション単位のアクセスを実現できます。また、暗黙的信頼モデルのセキュリティ戦略を、より安全性の高い明示的信頼戦略に転換することもできます。フォーティネットのユニバーサル ZTNA は、継続的かつほぼリアルタイムでデバイス態勢を検証し、コンプライアンス違反のデバイスやセッションを遮断します。

セキュア SaaS アクセス

インラインとアウトオブバンドの両方をサポートする次世代デュアルモード CASB は、重要な SaaS アプリケーションを識別し、危険なアプリケーションを通知することで、アプリケーションを包括的に可視化し、シャドー IT の問題を解決します。CASB と DLP は、きめ細かいアプリケーション制御によって機密データを保護するほか、管理対象と管理対象外の両方のデバイスで、アプリケーションに潜むマルウェアの検知と修復を行います。



「SASE 市場は成長しているだけでなく、ネットワークおよびセキュリティアーキテクチャに対する企業のアプローチに変化をもたらしています。企業がハイブリッドワークや分散アプリケーションといった新常識への適応を進める中、ネットワーキングとセキュリティを統合し、一貫性のあるクラウドネイティブなソリューションを構築することがきわめて重要になっています」[2]

シンエッジロケーションからのセキュアアクセス

フォーティネットのユニファイド SASE は、AI を活用したクラウドベースのセキュリティによって、シンエッジからインターネットおよび企業アプリケーションへのアクセスを保護します。これにより、エンドポイントエージェントがなくても、マルウェア、ランサムウェア、ゼロデイなどのサイバー脅威に対する防御が可能になります。

FortiAP 無線アクセスポイントはインテリジェント機能を使用して、シンエッジロケーションから SASE POP（Point of Presence）へのトラフィックをオフロードします。これにより、すべてのデバイスで規模に応じた包括的セキュリティインスペクションを実行できます。こうした統合によって、SASE と同じ管理コンソールを使用して、フォーティネットの WLAN ポートフォリオを管理することもできます。フォーティネットのソリューションは、ゼロタッチプロビジョニングによって FortiAP デバイスもクラウドから管理できるため、現場スタッフによるオンサイト管理は必要なくなり、管理コストも削減できます。

ブランチおよびキャンパス向けセキュア SD-WAN

フォーティネットのユニファイド SASE には、業界で唯一有機的に開発されたソフトウェアが含まれています。このソフトウェアは ASIC 搭載の高速プラットフォームで補完され、ブランチとキャンパスに最も包括的なセキュア SD-WAN ソリューションを提供します。ユニファイド SASE はアプリケーションをリアルタイムで最適化し、一貫性のあるレジリエントなアプリケーションエクスペリエンスや、高度な次世代ファイアウォール保護を実現します。MPLS を SD-WAN 経由のブロードバンドに切り替えることでコストが削減され、アプリケーションのパフォーマンスが向上します。こうした切り替えによって、ユーザーエクスペリエンスを最適化し、ダイレクトインターネットアクセスを保護することができます。

フォーティネットの優位性

フォーティネットのユニファイド SASE は、独立したクラウド専用アプローチを提供するのではなく、フォーティネット セキュリティ ファブリック プラットフォームに統合されています。フォーティネット セキュリティ ファブリックは、セキュリティ全体を単一のオペレーティングシステム「FortiOS」で管理し、広範な可視性、きめ細かい制御、一貫性のあるプロアクティブな保護をあらゆる場所に提供します。フォーティネットのユニファイド SASE には、他にも以下のような利点があります。

複雑さの軽減と完全な可視性

一元的な管理によって、可視性、保護、エンドユーザーエクスペリエンスの最適化など、ハイブリッドワークに関連する課題の解決を可能にします。フォーティネットのユニファイド SASE は、FWaaS、SWG、ZTNA、CASB、DLP、DEM などあらゆる SSE 機能を単一のコンソールで管理します。

優れたユーザーエクスペリエンス

インテリジェントなアプリケーションステアリングや動的ルーティングなど、クラウドで提供される SD-WAN 機能によって、リモートワーカーの生産性と優れたエクスペリエンスを保証します。

エージェントレス接続

BYOD デバイスや、エージェントをダウンロードできないデバイス（Chromebook など）では、プロキシ自動構成ファイルとシンエッジデバイスを用いたエージェントレスセキュリティを利用できます。

シンエッジのセキュリティ

FortiAP ならびに FortiExtender で展開されるシンエッジには、フォーティネットのシンエッジ SASE ソリューションが包括的でエージェントレスな保護機能を提供し、管理を簡素化します。これにより、OT / IoT デバイスのアクセスは保護され、Wi-Fi を使用するホームオフィスや小規模オフィスでのアクセスが簡素化されます。フォーティネット独自のこの機能を使用すれば、アプライアンス、エージェント、サービスなどを追加しなくても、エンタープライズクラスの保護をシンエッジロケーションにまで拡張できます。

終わりに

単一のオペレーティングシステムで動作するフォーティネットのユニファイド SASE は、クラウドから提供される統合型ソリューションであり、分散ネットワークの他のコンポーネントとシームレスに連携しながら、ユーザー、アプリケーション、エンドポイントデバイスを保護します。フォーティネットのユニークなソリューションは、ネットワークとセキュリティを一元的に可視化でき、クラウドでホストされる直感的なユーザーインタフェースを使って容易に構成することができます。単一の管理コンソールで SSE の全機能と DEM を管理することで、オペレーションが簡素化され、ROI が増大すると共に、ハイブリッドワークセキュリティへの移行が促進されます。

複雑さを解消し柔軟なソリューションを提供するというフォーティネットのコミットメントは、従来型のリモートアクセス、マイクロブランチの展開、SD-WAN の統合などさまざまなユースケースで証明されています。このような優れた適応性によってゼロトラストが強化され、たとえソフトウェアエージェントを配置できない場所であっても、継続的な検証によってすべての接続で堅固なセキュリティ態勢を維持することができます。

今日の WFA の課題をフォーティネットのユニファイド SASE で解決する方法については、こちらをご覧ください。

[1]「How To Balance Employee Trust, Empowerment And Compliance In A Remote-Work World」、E Shawn Farshchi、Forbes、2023 年 1 月 31 日（英語）：
https://www.forbes.com/sites/forbeshumanresourcescouncil/2023/01/31/how-to-balance-employee-trust-empowerment-and-compliance-in-a-remote-work-world/

[2]「Single-vendor SASE to Dominate Market Growth as Enterprises Favor One-Stop Solutions」、Dell'Oro Group、2024 年 1 月 24 日（英語）：
https://www.delloro.com/news/sase-market-to-skyrocket-to-over-16-billion-by-2028/

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