SOLUTION BRIEF

FortiOS：フォーティネット セキュリティ ファブリックの基盤

概要

FortiOS は、フォーティネット セキュリティ ファブリックの核心となるフォーティネットのオペレーティングシステムです。フォーティネット セキュリティ ファブリックは、共通の管理 / セキュリティフレームワークに有機的に構築された、業界最高レベルの性能と拡張性を誇るサイバーセキュリティプラットフォームです。FortiOS がセキュリティ ファブリックのセキュリティとネットワーキングのすべてのコンポーネントを結び付けることで、シームレスな統合が実現します。これにより、ネットワーキングとセキュリティの機能のコンバージェンスが可能になり、あらゆる形態の環境で一貫したユーザーエクスペリエンスと強固なセキュリティ態勢が実現し、オンプレミス、クラウド、ハイブリッド、IT / OT / IoT インフラストラクチャのコンバージェンスが可能になります。

「FortiOS は、あらゆる場所に分散するユーザーやアプリケーションに対し、運用の効率化と一貫性あるセキュリティを提供します。」[1]

FortiOS 7.4 では、最も複雑なハイブリッド環境においても比類のない可視性と機能の適用を IT リーダーに提供する強力な新機能が追加され、次のような機能が強化されました。

- OT、IoT、IT のデバイスを保護する、業界初の統一されたネットワーキングとセキュリティのアーキテクチャ
- FortiAnalyzer が提供する、フォーティネットのセキュアネットワーキングポートフォリオ全体の業界初の統合管理と分析の機能
- 武器化された AI 攻撃、標的型ランサムウェア、犯罪者が支援する APT などの高度な攻撃から保護し、解決に要する時間を短縮する、SOC チーム向けの自動化とリアルタイムのレスポンス機能の強化
- FortiEDR、FortiXDR、FortiRecon、FortiDeceptor などの早期検知ソリューションにおける機能の強化による、アラートのトリアージとインシデントの調査の軽減
- リスクを低減し、OT / IT / IoT 環境のコンバージェンスを推進する新機能

FortiOS とフォーティネット セキュリティ ファブリックによる、幅広い適用領域で（Broad）システム連携し（Integrated）自動化された（Automated）セキュリティ

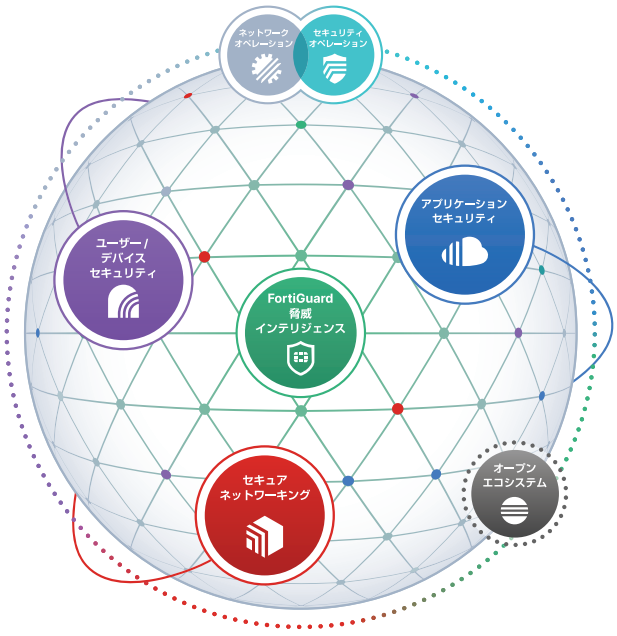

図 1：フォーティネット セキュリティ ファブリックの概略図

今日の分散したセキュリティ ファブリック全体でオペレーティングシステムが 1 つに統一されていることには、次のようなメリットがあります。

- セキュリティポリシーとコンフィグレーションの一元的で一貫性ある管理とオーケストレーション
- 攻撃対象領域の拡大と攻撃サイクルの各ステップに対応した広範な保護と制御
- コンテキスト対応セキュリティポリシーを高パフォーマンスで適用
- AI（人工知能）ベースの脅威の検知と提案
- AI ベースのデータ相関によるファブリックレベルの統一されたデータセットの分析とレポート
- 攻撃対象領域と攻撃サイクル全体のサイバー攻撃に対する自動的かつ多面的なリアルタイムのレスポンス
- SOAR（セキュリティオーケストレーション、自動化、レスポンス）の強化による脅威へのレスポンスの改善とリスクの低減

FortiOS 7.4 の新機能

FortiOS 独自の機能が、パフォーマンスや保護を低下させたり、イノベーションを減速させたりすることなく、ビジネスの遂行を可能にします。FortiOS 7.4 とセキュリティ ファブリックで強化された、今日の環境に固有の課題の解決を支援する主な機能の一部を以下に紹介します。

セキュアネットワーキングと管理

フォーティネットのセキュアネットワーキングポートフォリオと FortiOS 7.4 の新しいイノベーションが、FortiManager、ハイブリッドメッシュファイアウォール、セキュア SD-WAN、シングルベンダー SASE、ユニバーサル ZTNA（ゼロトラストネットワークアクセス）、セキュア WLAN / LAN を始めとする広範囲のソリューションに組み込まれています。

ハイブリッドネットワークの管理と分析を統一

FortiManager は、ハイブリッドメッシュファイアウォール、シングルベンダー SASE、ユニバーサル ZTNA、セキュア SD-WAN、セキュア WLAN / LAN などのセキュアネットワーキングのすべての要素で、かつてないレベルの可視性と機能の適用を IT リーダーに提供します。

ハイブリッドメッシュファイアウォールでデータセンターとクラウドの両方をサポート

FortiGate 7080F は、ポイント製品の排除、複雑さの低減、専用設計の ASIC テクノロジーと AI / ML を活用した高度なセキュリティによってパフォーマンスの向上を実現する、次世代ファイアウォール（NGFW）の新シリーズです。

FortiFlex は、ハイブリッドメッシュファイアウォールの導入のサポートや仮想マシン、FortiGate アプライアンス、SaaS ベースのサービスなどのさまざまな製品をポイント制で利用できるプログラムです。

支社（拠点）向けのセキュア SD-WAN

フォーティネットのセキュア SD-WAN は、クラウドまたはオンプレミスのどちらであっても、ビジネスクリティカルなアプリケーションの一貫性のあるセキュリティと優れたユーザーエクスペリエンスを可能にし、シングルベンダー SASE へのシームレスな移行を支援します。オーバーレイオーケストレーションの自動化によるサイト展開の加速やグローバルの WAN ステータスを確認するための監視マップビューの再設計などの機能が新たに追加されました。

リモートユーザーや支社（拠点）向けのシングルベンダー SASE

FortiSASE は、クラウドから提供するセキュリティとネットワーキングのコンバージェンスにより、ハイブリッドネットワークにおける運用を簡素化します。FortiSASE と FortiManager が統合されたことで、オンプレミスとリモートのユーザーの比類ない可視性と管理が実現しました。

リモートユーザーやキャンパス向けのユニバーサル ZTNA

フォーティネットのユニバーサル ZTNA は、業界で最も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あらゆる場所のユーザーやアプリケーションに提供します。ユニバーサル ZTNA から、ユーザーベースのリスクスコアが進行中のアプリケーションアクセスの継続的チェックの一部として提供されるようになりました。

支社（拠点）やキャンパス向けの WLAN / LAN

FortiAP セキュア無線 LAN アクセスポイントと FortiSASE の統合により、アクセスポイントと SASE との統合が業界で初めて実現しました。これにより、マイクロブランチにアクセスポイントを展開して、FortiSASE ソリューションにトラフィックを送信することでマイクロブランチを保護し、そのサイトのすべてのデバイスに包括的セキュリティを保証することができます。

防止、早期の検知、リアルタイムのレスポンス

SOC チームによる、武器化された AI による攻撃、標的型ランサムウェア、犯罪者が支援する APT などの高度な攻撃からの保護と解決に要する時間の短縮を支援する、リアルタムのレスポンスと自動化の機能が新たに追加されました。5 つの主要分野に新しいソリューションが追加され、機能が強化されました。

エンドポイントセキュリティと早期のレスポンス

FortiEDR と **FortiXDR** は、複数の脅威インテリジェンスフィードを使用し、コンテキストが付加されたインシデントデータによるインタラクティブなインシデントの可視性を新たに追加することで、調査の簡素化と迅速化を支援します。

「FortiGate は、FortiOS オペレーティングシステムの優れた機能を活用することで、トップクラスのセキュア SD-WAN ソリューションを提供し、強力な LAN エッジコントローラーを搭載し、業界唯一のユニバーサル ZTNA アプリケーションゲートウェイを実現し、NOC と SOC のコンバージェンスを推進します。」[2]

FortiNDR Cloud は、実用的な分析で補完した堅牢な人工知能と侵害防止テクノロジーを組み合わせて利用します。このソリューションは、ネットワークデータの 365 日の保存と可視化、内蔵のプレイブック、ネットワークにおける異常や悪意のある振る舞いを検知する脅威ハンティングの機能を提供します。自己完結型のオンプレミス展開、または FortiGuard Labs の経験豊富な脅威エキスパートがメンテナンスする新しいガイド付き SaaS のいずれかを選択できます。

FortiRecon の FortiGuard Labs の脅威エキスパートのサポートにより、外部に公開されている資産、漏洩データ、ランサムウェア攻撃のインテリジェンスなど、サプライチェーンのベンダーやパートナーに関連する重要なリスクに対するプロアクティブな脅威インテリジェンスが強化されました。

FortiDeceptor による脆弱性アウトブレイク防御が可能になりました。FortiGuard Labs から報告された脆弱性をアウトブレイクデコイへのフィードとして自動的にプッシュ配信することで、攻撃者を偽の資産にリダイレクトし、キルチェーンの初期段階で攻撃を隔離します。SOAR プレイブックは、ディセプション資産の作成と戦略的な配置を自動的に開始することで、詳細なインテリジェンスも収集し、不審な活動を阻止することもできます。FortiDeceptor の新しい攻撃交換プログラムにより、FortiDeceptor のユーザーが匿名で最新の攻撃に関する価値あるインテリジェンスを交換し、侵害を回避するためのプロアクティブな手順を実行できるようになりました。

SOC の自動化と拡張

FortiAnalyzer に新たに追加された直感的なルールエディターを使用することで、異なるタイプのログソースの高度なイベント相関付けが可能になり、MITRE ATT&CK のユースケースにマッピングできるようになりました。

FortiSOAR に、ターンキー SaaS サブスクリプションオプション、機械学習を活用したインラインプレイブックの推奨、広範な OT セキュリティ機能とプレイブック、独自のノーコード / ローコードのプレイブック作成などの機能が追加されました。

FortiSIEM にリンクグラフテクノロジーが新たに追加され、ユーザー、デバイス、インシデントの関係を簡単に可視化できるようになりました。さらには、高度な機械学習フレームワークで従来の方法では見逃されてしまう可能性のある異常や異常値を検知することで、さらなる保護の強化が実現しました。

FortiGuard SOCaaS（SOC-as-a-Service）に、AI によるインシデントトリアージの支援に加えて、FortiGuard Labs の SOC 運用上の即応性と侵害評価のサービスが新たに追加されました。

AI を活用した脅威インテリジェンス

FortiGuard 産業用セキュリティサービスは、グローバルの脅威インテリジェンス、ゼロデイリサーチ、CVE（Common Vulnerabilities and Exposures）クエリサービスに基づき、OT と IT の両方のデバイスへの自動仮想パッチを強化することで、保護までの時間を大幅に短縮します。

FortiGuard IoT サービスは、IIoT（産業用 IoT）と IoMT（Internet-of-Medical-Things：医療用 IoT）デバイスのコンバージェンスにより、この業種に求められるきめ細かいレベルの OT セキュリティを実現します。

FortiSIEM 統合セキュリティ分析ダッシュボードに、産業用デバイスと通信パスのパデューモデル階層へのマッピング、脅威の修復に役立つ OT に特化した新しいプレイブック、OT 脅威分析を支援する ICS MITRE ATT&CK マトリクスの利用などの機能が追加されました。

アイデンティティとアクセス

FortiPAM 特権付きアカウント管理は、IT / OT ネットワークにリモートアクセスを提供します。ユーザーが重要な資産にアクセスしようとした場合の ZTNA 制御も可能になりました。ZTNA タグを適用することで、脆弱性、アンチウイルスシグネチャの更新、場所、マシングループのデバイス態勢を継続的にチェックできます。

アプリケーションセキュリティ

FortiDevSec は、アプリケーションコードとランタイムアプリケーションに包括的アプリケーションセキュリティテストを提供します。このソリューションには、SAST、DAST、SCA が組み込まれているため、脆弱性や構成ミスを早期に検知し、秘密の検出などの保護が可能になります。

サイバー物理システムと産業制御システムのリスクの軽減

フォーティネットのソリューションポートフォリオと OT 向けセキュリティ ファブリックは、サイバー物理セキュリティ専用に設計されています。以下の点が強化されました。

FortiGate 70F Rugged 次世代ファイアウォール（NGFW）は、過酷な環境を前提に設計されたフォーティネットの Rugged ポートフォリオに追加された最新の製品です。新しいコンパクトな設計により、ネットワーキングとセキュリティの機能の単一プロセッサへのコンバージェンスが実現しました。

FortiDeceptor Rugged 100G は、過酷な産業用環境に最適な、Rugged 仕様の新しい産業用アプライアンスです。

FortiPAM は、エンタープライズグレードの特権付きアクセス管理を IT と OT の両方のエコシステムに提供します。

FortiSIEM 統合型セキュリティ分析ダッシュボードに、イベント相関付けとセキュリティイベントのパデューモデルへのマッピングの機能が追加されました。

FortiSOAR には、過剰なアラート対応を軽減し、IT / OT 環境におけるセキュリティの自動化とオーケストレーションを可能にする機能が追加されました。

FortiGuard 産業用セキュリティサービスでは、2,000 以上のアプリケーション制御シグネチャを活用することで、OT アプリケーションやディープパケットインスペクションをサポートするプロトコルへの対応が可能になりました。

フォーティネットの OT 向けサイバーセキュリティ診断プログラム（CTAP）は、OT ネットワークセキュリティの効果やアプリケーションフローを検証し、エキスパートによるガイダンスも提供します。

OT セキュリティチーム向けの **OT 机上演習**を、脅威分析、緩和、インシデント対応に精通した FortiGuard インシデントレスポンスチームのファシリテーターが指導して実施します。

FortiOS とフォーティネット セキュリティ ファブリックが現在と将来のセキュリティの課題を解決

FortiOS 7.4 は、今日の急速に変化するネットワーキングとセキュリティのハイブリッド環境のニーズをサポートする強力な機能を提供します。今日の進化し続ける脅威からの保護を可能にするため、FortiOS は継続的にアップデートされています。フォーティネット セキュリティ ファブリック ソリューションの導入により、ユーザーやネットワークが広範囲に分散する環境であっても、あらゆる規模の組織がセキュリティやネットワーキングの現在および将来のあらゆる課題の解決に必要なツールを手に入れることができます。

1「Ken Xie（ケン・ジー）への Q&A：成長、差別化ポイント、FortiSP5」、フォーティネット、2023 年 2 月 13 日：
https://www.fortinet.com/jp/blog/business-and-technology/ken-xie-growth-differentiators-fortisp5

2「Setting the Record Straight on Competitor Misinformation」、John Maddison、フォーティネット、2022 年 11 月 11 日（英語）：
https://www.fortinet.com/blog/business-and-technology/setting-the-record-straight-on-competitor-misinformation

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

SB-FortiOS7.4-Security-Fabric-202305-R1