DATA SHEET

FortiXDR

提供形態：

仮想マシン　ホスティング

インシデントの識別、調査、修復の完全な自動化

FortiXDR は、拡張検出および応答（XDR：Extended Detection and Response）により、フォーティネット セキュリティ ファブリックを強化します。具体的には、フォーティネット製品からのセキュリティや監査関連の情報フィードを分析し、潜在的なセキュリティインシデントを特定します。これらのクロスプラットフォームのフィードは、人工知能（AI）が調査したインシデントに関連付けられています。組織は、分類された結果に基づき、自動化されたクロスプラットフォームのレスポンスを事前に定義できます。FortiXDR をご利用のお客様は、より多くの脅威を特定し、迅速に封じ込め、セキュリティチームのアラートの負担を軽減できます。

検知能力の向上

セキュリティ ファブリック全体でネイティブに共有されている相関テレメトリにフォーティネットのキュレート分析を適用し、インシデントを高精度で特定します。

AI を活用した調査

フォーティネットがトレーニングしたディープラーニングエンジン、動的に選択されたエンリッチメント、およびマイクロサービスを活用し、通常はセキュリティ専門家が担当するようなセキュリティインシデントの調査を再現します。

レスポンス能力の向上

自動化が可能な、細分化されたフレームワークを使用して、複数のセキュリティインフラストラクチャコントロールにわたって修復アクションを事前に定義します。

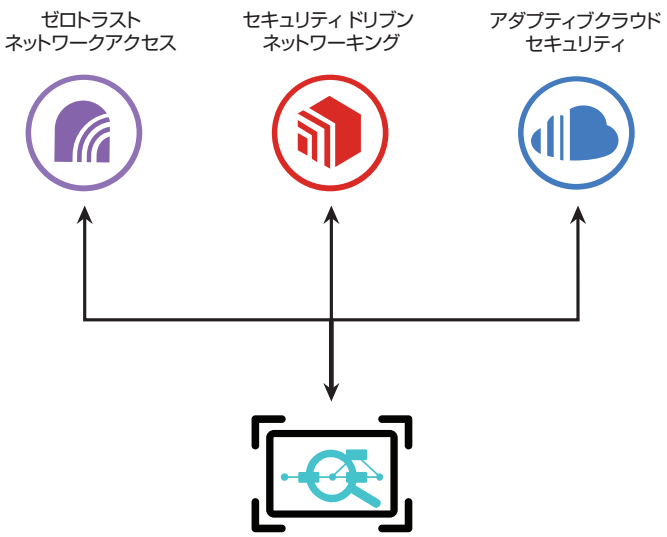
テレメトリ

- クラウドセキュリティ
- Web アプリケーション セキュリティ
- E メールセキュリティ
- ネットワークセキュリティ
- LAN / WAN / WLAN
- アイデンティティサービス
- エンドポイントセキュリティ
- IoT セキュリティ

ハイライト

完全に自動化することが可能な拡張検知と応答能力の向上（XDR）

FortiXDR は、フォーティネット セキュリティ ファブリックの拡張機能として、高機能の各コントロールを元に、業界で最も多くのサイバーキルチェーンステージをカバーする広範なテレメトリセットを活用しています。さらに、フォーティネット製品とサードパーティ製品の両方にわたり調整され、事前に設定された自動レスポンスをサポートしています。さらに重要な点として、FortiXDR は、インシデント調査を動的に実施するように訓練され、特許出願中の人工知能を搭載している唯一の XDR ソリューションであることが挙げられます。この AI は、プロセスのさまざまな側面をエミュレートするマイクロサービスを活用しており、セキュリティのプロフェッショナルのような役割を果たします。FortiEDR のクラウドネイティブの基盤の上に構築されているため、導入が容易で、フォーティネットのエキスパートたちが継続的にキュレーションを実施しています。



主な利点

アラート量の削減

FortiXDR は、セキュリティ ファブリックの相関テレメトリに分析を適用し、クロスプラットフォームのセキュリティ情報やアラート量を 75% 削減することで、高精度なインシデント検知を実現します。

検知までの平均時間の短縮

FortiXDR はディープラーニングの人工知能を用いて調査プロセスを自動化し、セキュリティインシデントを 30 秒以内に分類します。

レスポンス時間の短縮

FortiXDR は、インシデントの種類、重大度、範囲、影響を受けるユーザーやグループに基づいてレスポンスフローを事前に定義し、調整されたレスポンスを自動化できます。

セキュリティチームの負荷を削減

アラート量の削減、AI による調査、応答アクションの自動化により、セキュリティの担当者は、サイバー脅威、組織のリスクの影響度、セキュリティ態勢を改善する機会の評価など、より戦略的な役割を担うことができます。

段階的な投資

FortiXDR は、ネットワークとエンドポイントのテレメトリの組み合わせにより優れた検出を可能にすることで、FortiGate のあらゆるお客様に付加価値を提供します。時間をかけて少しずつフォーティネット セキュリティ ファブリックを拡張し、E メール、Web アプリケーション、クラウドなどに範囲を拡大することで、フォーティネットへの投資効果をさらに高めることができます。

主な機能

検知機能の拡張

FortiXDR には、リスクの高いインシデントを正確に検知し、セキュリティ ファブリック全体でメタデータを確定するために精選され、拡張された一連の分析機能が搭載されています。

- ネットワーク / ポートスキャン / ARP スプーフィング
- ブルートフォース / C2C
- データ漏えい / ラテラルムーブメント（水平方向の移動）
- 認証情報 / アカウントの侵害
- フィッシング攻撃

AI を活用した調査

FortiXDR は、ディープラーニングエンジンを使用し、専門のアナリストの行動を再現するマイクロサービスによってさまざまな調査プロセスを動的に再現し、クロスプラットフォームの修復方法を返すことができます。

- テレメトリと脅威インテリジェンスを抽出
- 静的および動的ファイル分析を実行
- コミュニティやその他の評価を比較
- UEBA やその他のベースラインを構築 / 比較
- マイクロサービスの拡充

自動化が可能な検知能力の拡張

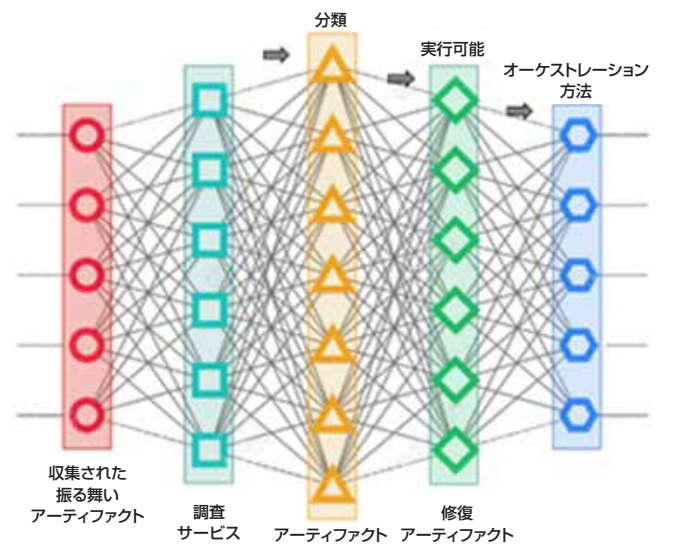
FortiXDR には、直感的なフレームワークが用意されており、お客様は以下の項目に基づいて、きめ細かなレスポンスアクションを事前に定義できます。

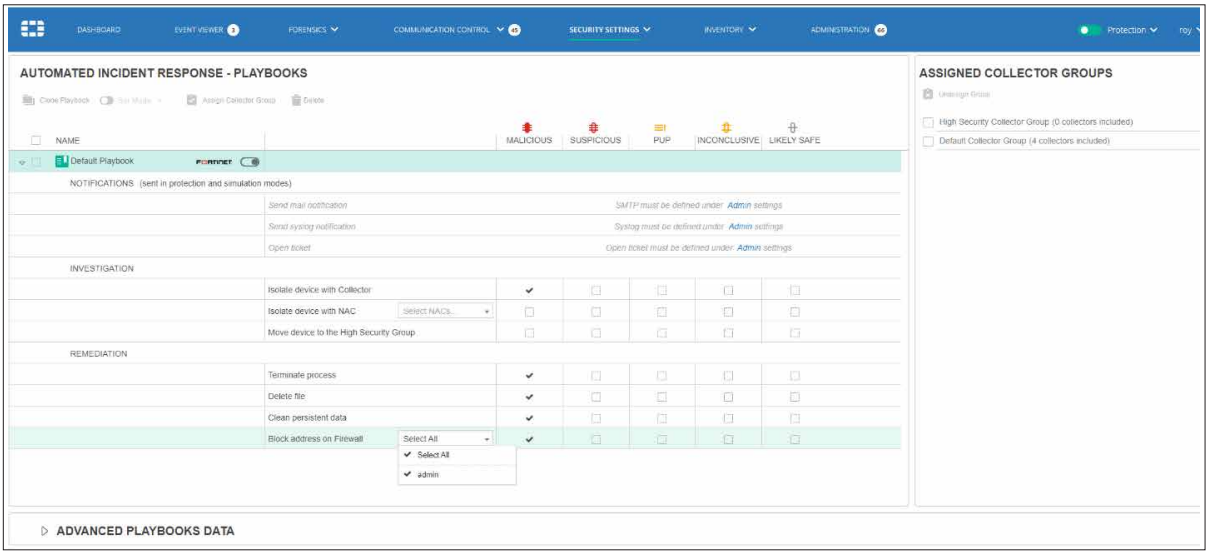
- ユーザーとグループ
- インシデントのタイプ、重大度、範囲
- デバイスの隔離と修復
- 認証情報の有効期限
- 新しい脅威インテリジェンス

サードパーティのサポート

FortXDR は、FortiGate、FortiNAC、FortiSandbox、FortiEDR などのさまざまなフォーティネット製品との統合に加えて、コネクターを介した以下のようなフォーティネット以外の API がサポートする製品との統合も可能です。

- ファイアウォール
- アイデンティティサービス
- チケットプラットフォーム
- クラウドアクセスセキュリティブローカー
- クラウドワークロード保護プラットフォーム



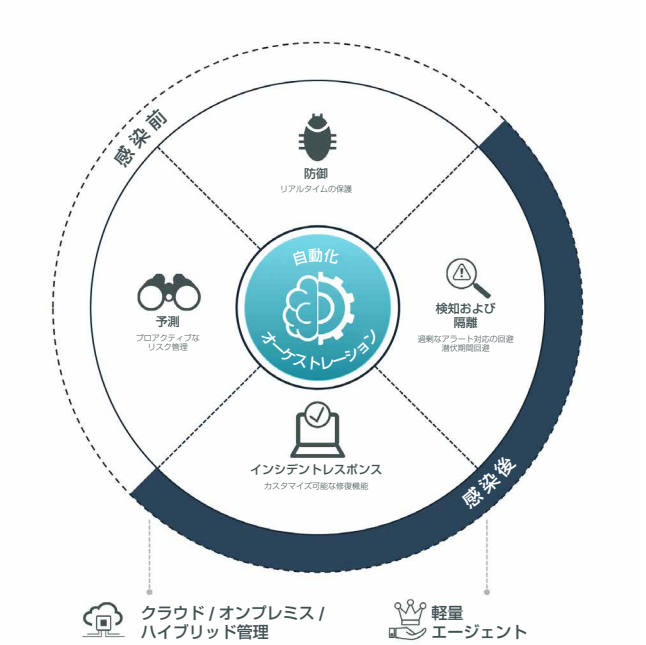


主な機能

実行前と実行後の保護

FortiXDR は、FortiEDR のクラウドネイティブの基盤の上に構築されており、以下のように侵入やランサムウェアの被害をリアルタイムで阻止する機能を備えています。

- 実行前および実行後の振る舞いベースの保護
- システムの稼働を停止することなく、攻撃を検知して防御する独自機能
- 特許取得済みのランサムウェア保護機能により、ファイルの書き込みアクティビティをリアルタイムで傍受し、コマンドを評価して暗号化を防止
- 最新 / レガシー OS を実行するワークステーションやサーバーから、POS や OT 制御システムに至るあらゆるエンドポイントを保護
- クラウド、オンプレミス、エアギャップ環境、ハイブリッドに導入可能



セキュリティ ファブリック統合

FortiXDR はフォーティネット セキュリティ ファブリックアーキテクチャを活用して、次のような多くのセキュリティ ファブリックコンポーネントと統合しています。

- FortiGate：侵入攻撃後の IP アドレスの一時停止またはブロックなどの高度なレスポンスアクションを指示
- FortiNAC：デバイスの隔離など高度なレスポンスアクションを指示
- FortiSandbox：リアルタイムのイベント分析と分類、脅威インテリジェンスを共有
- FortiSIEM：イベントとアラートを送信し、監視とレポートを統合
- FortiGuard Labs：インシデントを補強して調査を支援

サードパーティのサポート

FortXDR は、さまざまなフォーティネット製品との統合に加えて、コネクターを介した以下のようなフォーティネット以外の API がサポートする製品との統合も可能です。

- ファイアウォール
- アイデンティティサービス
- ネットワークサンドボックス
- データレイク

フォーティネットのサービス

FortiGuard のエキスパートは、アーキテクチャとプランニング、構成、インストール、プレイブックのセットアップ、環境チューニング、トレーニングなど、導入を成功させるための先行導入サービスと専門家によるサポートを提供します。また、継続的な MxDR（Managed eXtended Detection and Response）サービスを提供し、24 時間 365 日、専門家による継続監視を可能にします。

主な機能

管理アーキテクチャ

単一の統合管理コンソールでは、防止、検知、インシデントレスポンスのすべての機能が提供されます。拡張REST APIを使用して、コンソールアクションなどに対応することも可能です。

ネイティブのクラウドインフラストラクチャ

FortiXDR は、マルチテナント管理機能をクラウドで提供します。このソリューションは、クラウドネイティブ、ハイブリッド、オンプレミスのいずれかで導入できます。また、エアギャップ環境にも対応しています。

軽量なエンドポイントエージェント

FortiEDR は、CPU 使用率 1% 未満、最大 RAM サイズ 120 MB、ディスクスペース 20 MB で稼働し、生成するネットワークトラフィックも最小限に抑えます。

オフライン保護

エンドポイントで保護と検知を実行して、ネットワークに接続されていないエンドポイントを保護します。

サポートされるプラットフォーム

FortiEDR は Windows、macOS、Linux オペレーティングシステムをサポートし、オフライン保護を提供します。

- Windows（32 ビット / 64 ビット）XP SP2 / SP3、7、8、8.1、10
- Windows Server 2003 R2 SP2、2008 R1 SP2、2008 R2、2012、2012 R2、2016、2019
- macOS のバージョン：Yosemite（10.10）、El Capitan（10.11）、Sierra（10.12）、High Sierra（10.13）、Mojave（10.14）、Catalina（10.15）、Big Sur（11.0）
- Linux のバージョン：RedHat Enterprise Linux および CentOS 6.8-10、7.2-9、8.0-3、Ubuntu LTS 16.04.5-7、18.04.1-5、20.04.1 サーバー、64 ビット、Oracle Linux 8.2-3（サポート）、SuSE SLES 11.1-4、12.1-12.5、15.01-1（6/30）、Amazon Linux AMI 1-2（6/30）
- VMware および Citrix の Virtual Desktop Infrastructure（VDI）環境。サポートする VDI 環境：VMware Horizons 6 および 7、Citrix XenDesktop 7

オーダー情報

Product	Description
Option 1	FortiEDR Protect & Respond and XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.
Option 2	FortiEDR Protect & Respond and Managed XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.
Option 3	FortiEDR Discover, Protect & Respond and XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.
Option 4	FortiEDR Discover, Protect & Respond and Managed XDR Subscription and 24×7 FortiCare, plus FortiCare Best Practice Service.

* それぞれ、25、500、2,000、10,000 シート単位のライセンスが用意されています（最低発注単位は 500 シート）。

フォーティネットジャパン株式会社

〒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

Copyright© 2021 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。