DATA SHEET

FortiEDR

リアルタイムのエンドポイント保護、検知、自動レスポンスを実現

FortiEDR は、リアルタイムでのエンドポイントの自動保護、そしてオーケストレーションによるインシデントへのレスポンスを単一の統合プラットフォームで実現します。製造システムや OT システムだけでなく、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をはじめとするあらゆる通信デバイスを網羅し、柔軟な導入オプションを提供して運用コストの事前予測を可能にします。

リアルタイムでのプロアクティブなリスク減災と IoT セキュリティ

脆弱性評価やプロアクティブなリスク減災策に基づくポリシーなどを利用して、脆弱性が発見されたすべてのアプリケーションの通信を制御することにより、攻撃対象領域をプロアクティブに削減可能となります。

感染前の保護

機械学習に基づく、カスタマイズされたカーネルレベルの次世代アンチウイルス（NGAV）エンジンによって第一の保護レイヤーを提供し、ファイルベースのマルウェアによる感染を防ぎます。

感染後の保護

FortiEDR は、エンドポイントでセキュリティ侵害が発生している場合でも高度な攻撃をリアルタイムで検知してブロックするという他のソリューションにはない優れた特長を備えており、セキュリティ侵害やデータ漏えいを阻止し、問題を解決します。脅威の潜伏を防ぎ、インシデントの検知、無効化 / 阻止、調査、レスポンス、修復を実現する自動的な EDR（Endpoint Detection and Response：エンドポイントの脅威検知とレスポンス）の機能セットを提供します。

対応プラットフォーム

- Windows XP SP2 / SP3、Windows 7、8、10.x、Windows Server 2003 R2、2008 R1、2008 R2、2012、2012 R2、2016、2019
- macOS Yosemite (10.10)、
- El Capitan (10.11)、Sierra (10.12)、High Sierra (10.13)、Mojave (10.14)、Catalina (10.15)
- VDI環境：VMware Horizons 6および Citrix XenDesktop / XenApp
- Red Hat Enterprise Linux 6.8、6.9、6.10および7.x
- CentOS 6.8、6.9、6.10および7.x
- Ubuntu 16.04、18.04

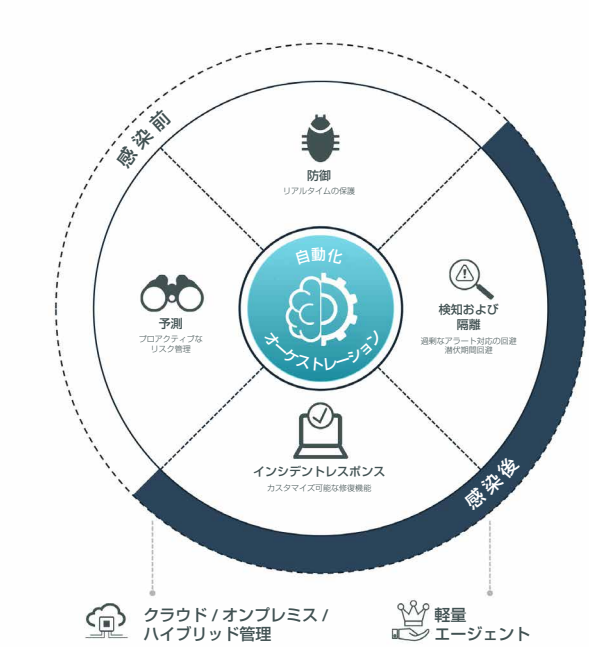
HIPAA COMPLIANT

PCI DSS COMPLIANT

ハイライト

包括的なエンドポイントセキュリティプラットフォーム

FortiEDR は、デバイスが既に侵害されている場合でも高度な脅威をリアルタイムで検知およびブロックし、セキュリティ侵害やランサムウェアによる被害を回避するために基礎から設計された唯一のエンドポイントソリューションです。インシデント発生時の自動レスポンスと修復を実現し、データの保護と同時にシステムのアップタイムやビジネス継続性を担保します。FortiEDR は、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 や製造制御システムに至るあらゆるエンドポイントを保護します。ネイティブのクラウドインフラストラクチャを使用して構築された FortiEDR は、クラウドはもちろん、ネットワークから隔離されている環境ではオンプレミスでの導入展開も可能で、ハイブリッドでの導入にも対応します。



主な利点

FortiEDR は、セキュリティプロセスを自動化するとともに過剰なアラート対応や脅威の潜伏を回避し、感染後であってもリアルタイムの保護を実現します。

保護

FortiEDR を利用することで、エンドポイントはリアルタイムで自動的に保護されると同時に、オーケストレーションによるインシデントレスポンスがプラットフォーム全体で実現します。感染後であってもリアルタイムで侵害を阻止し、データの流出やランサムウェアによる暗号化を防止します。

管理

FortiEDR は、直感的なインタフェースを備えた単一の統合コンソールを提供します。クラウド管理型のプラットフォームでは一元的な管理が可能で、エンドポイントに関する日常的なセキュリティ業務を自動化します。

拡張性

ネイティブのクラウドインフラストラクチャを採用しフットプリントも小さい FortiEDR は迅速な導入配備が可能で、多数のエンドポイント保護に対応する優れた拡張性も備えています。

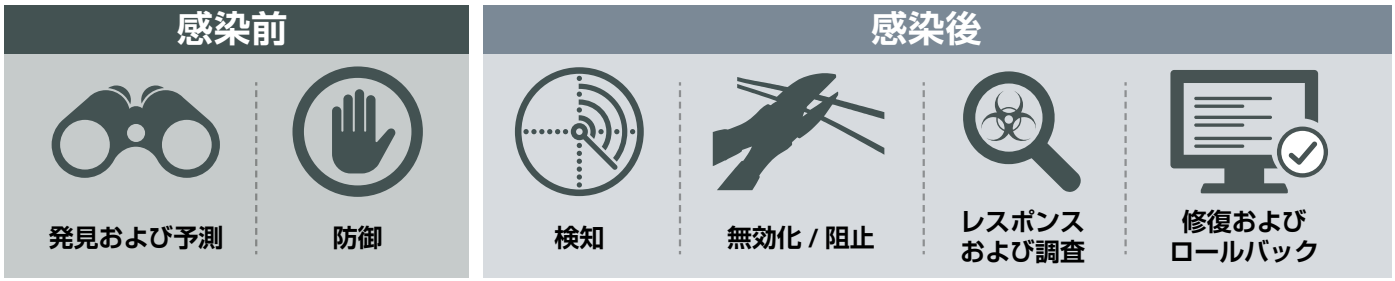
柔軟性

FortiEDR は、エンタープライズの多様なユースケースに対応することができます。クラウド型の管理プラットフォームは、ネットワークから隔離された環境ではオンプレミスへの導入展開が可能で、セキュアなクラウドインスタンスへの導入もサポートします。オンラインとオフラインのどちらでもエンドポイントは保護されます。

コスト

侵害発生後の対応費用や損害の発生を回避すると同時に、コストは低額の予測可能な金額に抑制され TCO も一定水準を超えることはありません。

主な機能と特長



発見および予測

FortiEDR は、脆弱性の評価と発見を通じて攻撃対象領域に対するポリシー制御の自動化を実現します。これにより、セキュリティチームは以下が可能になります。

- 不正なデバイス（保護 / 管理されていないデバイスなど）および IoT デバイスの発見と制御
- アプリケーションとレーティングの追跡
- システムやアプリケーションの脆弱性の発見と仮想パッチによる脆弱性の減災
- リスクベースのプロアクティブなポリシーによる攻撃対象領域の縮小

防御

FortiEDR は、機械学習に基づくアンチウイルスエンジンを活用してマルウェアを実行前に阻止します。複数の OS に対応するこの次世代アンチウイルス（NGAV）機能は構成のカスタマイズが可能で、単一の軽量エージェントに組み込まれて提供されます。このため、ユーザーは追加のインストールを実行することなくマルウェア対策を任意のエンドポイントに割り当てることができます。

- 機械学習型のカーネルベースの NGAV を実現
- 継続的に更新されるクラウド上のデータベースから提供されるリアルタイムの脅威インテリジェンスを活用し、脅威情報を補強
- オフライン保護機能を使用し、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
- USB デバイス制御

検知および無効化

FortiEDR は、ファイルレスマルウェアやその他の高度な脅威をリアルタイムで検知して無効化し、データの保護および侵害の防止を実現します。疑わしいプロセスフローや振る舞いを検知すると、アウトバウンド通信、および必要な場合はそれらのプロセスからのファイルシステムへのアクセスをブロックし、潜在的な脅威を即座に無効化します。このような手順により、データの流出、コマンド&コントロール（C&C）通信、ファイルの改ざん、ランサムウェアによる暗号化を防ぎます。

同時に、バックエンドで追加のエビデンスを継続的に収集してイベントデータを補強し、インシデントを分類します。これにより、潜在的に適用可能な自動インシデントレスポンスのプレイブックポリシーが作成されます。FortiEDR は、既に侵入を許しているデバイスであってもデータ侵害やランサムウェアによる損害をリアルタイムで外科的に防止し、ビジネスの継続性を担保します。

- OS 中心の検知を活用し、メモリベースの攻撃や「環境寄生型」攻撃など、ステルス性の高い侵入攻撃を高い精度で検知
- セキュリティ侵害をリアルタイムで阻止し、脅威の潜伏を回避
- ログ履歴全体の分析を実現
- ランサムウェアによる暗号化とファイル / レジストリの改ざんを防止
- 脅威の分類を継続的に検証
- 検知精度を強化して、過剰なアラート対応を回避

レスポンスおよび修復

各顧客向けにカスタマイズしたプレイブック、そしてすべての環境を網羅した実用的インテリジェンスを活用し、インシデントへのレスポンス業務のオーケストレーションを実現します。単一のデバイスあるいは環境全体に存在するデバイスに対して、インシデントレスポンスおよび修復のプロセスを合理化し、既に無効化済みの脅威によって加えられた不正な変更を手作業または自動でロールバックします。

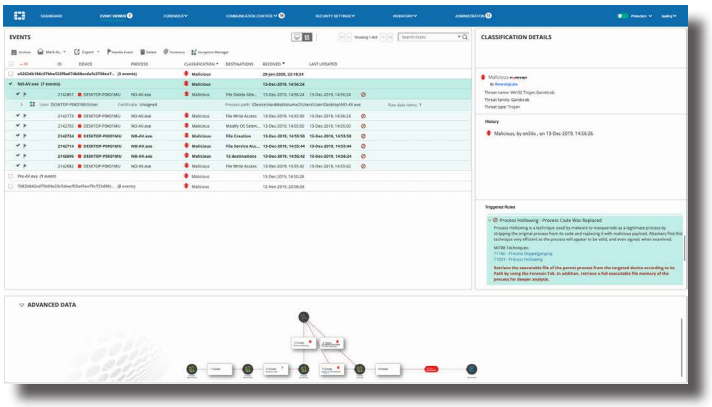
- インシデントの分類を自動化し、アラートの精度を改善
- プレイブックの自動化によって、インシデントレスポンスの手順を標準化
- ファイルの削除、不正なプロセスの停止、持続的な変更の取り消し、ユーザーへの通知、アプリケーションやデバイスの隔離、サポートチケットの発行など、インシデントへのレスポンスを自動化することでセキュリティのリソースを最適化
- インシデントの分類と攻撃の対象（エンドポイントグループなど）に関する情報を利用し、コンテキストベースのインシデントレスポンスを実現
- 特許取得済のコードトレース技術により、攻撃チェーンや不正な変更を完全に可視化
- システムのアップタイムを担保しながら、不正な変更のクリーンアップとロールバックを自動化
- 最適な MDR（Managed Detection and Response）サービスを提供

主な機能と特長

調査および追跡

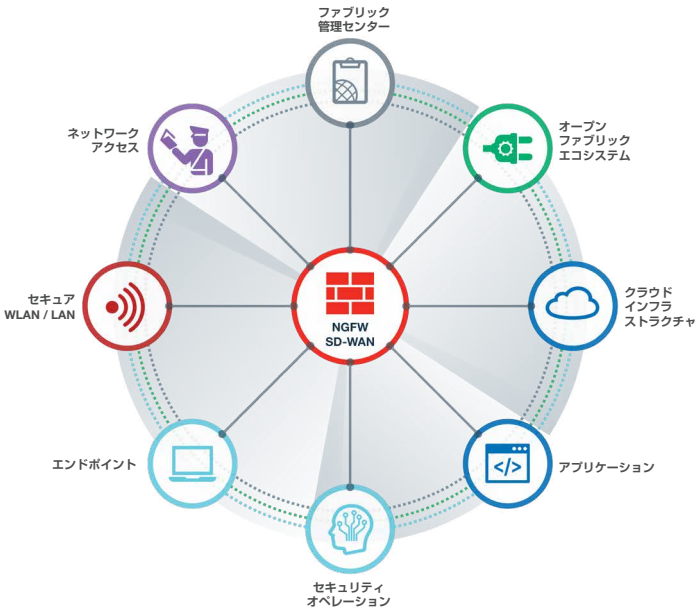
FortiEDR は、侵害されたエンドポイントに対するフォレンジック調査を行うため、感染前と後のマルウェアの詳細情報に基づいて脅威に関するデータが自動的に補強されます。独自のインタフェースでガイダンスやベストプラクティスを提示し、セキュリティアナリストに対して次に実行すべき論理的なステップを推奨します。

- エンドユーザーの作業の中断を最小限に抑えながら調査を自動化
- 脅威が自動的に無効化およびブロックされるようになり、セキュリティアナリストは自身の都合に合わせて追跡が可能
- 特許取得済のコードトレース技術により、デバイスがオフラインの場合でも攻撃チェーンやスタックを完全に可視化して決定的な証拠を特定
- メモリベースの脅威を追跡するため、インメモリ攻撃のメモリスナップショットを保存
- ガイド機能を備えたインタフェースは、疑わしいまたは不正なイベントとしてフラグが付けられた理由の明確な説明や類似する MITRE 攻撃フレームワークのリストを表示すると同時に、フォレンジック調査に必要な次の手順を提示



ガイド機能を備えたインタフェースは、疑わしいまたは不正なイベントとしてフラグが付けられた明確な理由や類似する MITRE 攻撃フレームワークのリストを表示すると同時に、フォレンジック調査に必要な次の手順を提示

セキュリティ ファブリック統合



FortiEDR は、フォーティネット セキュリティ ファブリックのアーキテクチャを活用し、FortiGate、FortiNAC、FortiSandbox、FortiSIEM をはじめとする多数のセキュリティ ファブリック コンポーネントと統合することができます。

FortiGate

FortiEDR コネクタを使用することで、エンドポイントの脅威インテリジェンスやアプリケーション情報を FortiGate と共有可能になります。FortiEDR の管理者は、感染後の IP アドレスの使用中断やブロックなど、より強力なレスポンスを FortiGate に指示することができます。

FortiNAC

FortiEDR は、エンドポイントの脅威インテリジェンスや発見された情報資産を FortiNAC と共有します。Syslog を共有することにより、FortiEDR 管理者はデバイスの隔離をはじめとする強力なレスポンスを FortiNAC に指示することができます。

FortiSandbox

FortiEDR と FortiSandbox をネイティブ統合することによってファイルがクラウド内のサンドボックスに自動送信され、リアルタイムのイベント分析や分類が実現します。さらに、脅威インテリジェンスが FortiSandbox と共有されます。

FortiSIEM

FortiEDR は、脅威分析とフォレンジック調査を目的としたイベント情報やアラートを FortiSIEM に送信します。FortiSIEM は FortiEDR OOTB の指定のパーサーを備えているほか、JSON や REST API を利用した FortiEDR との緊密な統合も可能です。

FortiGuard Labs

FortiEDR は、FortiGuard Labs とのネイティブ統合によって脅威インテリジェンスを更新することが可能で、リアルタイムのインシデント分類に対応し精度の高いインシデントレスポンスのプレイブックを有効化できます。

サービス

FortiEDR 導入サービス

円滑な導入を支援するこのサービスは、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、トレーニングをはじめとする専門的なサポートを提供します。

FortiResponder MDR（Managed Detection and Response）サービス

FortiResponder MDR（Managed Detection and Response）サービスは、経験豊富なアナリストと実績あるプラットフォームによる 24 時間 365 日の継続的な脅威の監視、アラートのトリアージ、インシデント分析を提供します。高度なトレーニングを受けたエキスパートがすべてのアラートのレビューと分析を実行するほか、継続的なセキュリティを確保するための対策の実施、さらにはインシデントレスポンス担当者と IT 管理者がとるべき次のステップや減災に関する詳細な推奨事項の提供を通じて、顧客企業は安心してビジネスに注力できるようになります。FortiResponder MDR サービスは、既存のオペレーションを拡大すると同時に、SOC のさらなる発展を支援します。

技術仕様

管理およびアーキテクチャ

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。

- **オフライン保護：**エンドポイントで保護と検知を実行し、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。
- **ネイティブのクラウドインフラストラクチャ：**FortiEDR は、クラウドでマルチテナント管理機能を提供します。クラウドネイティブ、ハイブリッド、またはオンプレミスのソリューションとして導入展開することが可能で、ネットワークから隔離されている環境もサポートします。
- **軽量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 のわずかなリソースで稼働することが可能で、生成するネットワークトラフィックも最小限に抑えられています。

サポートす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 SP2、2012、2012 R2、2016、2019
- macOS 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)
- Linux バージョン：RedHat Enterprise Linux、CentOS 6.8、6.9、6.10、7.2、7.3、7.4、7.5、7.6、7.7、Ubuntu LTS 16.04.5、16.04.6、18.04.1、18.04.2 サーバー（64 ビット）
- 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

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