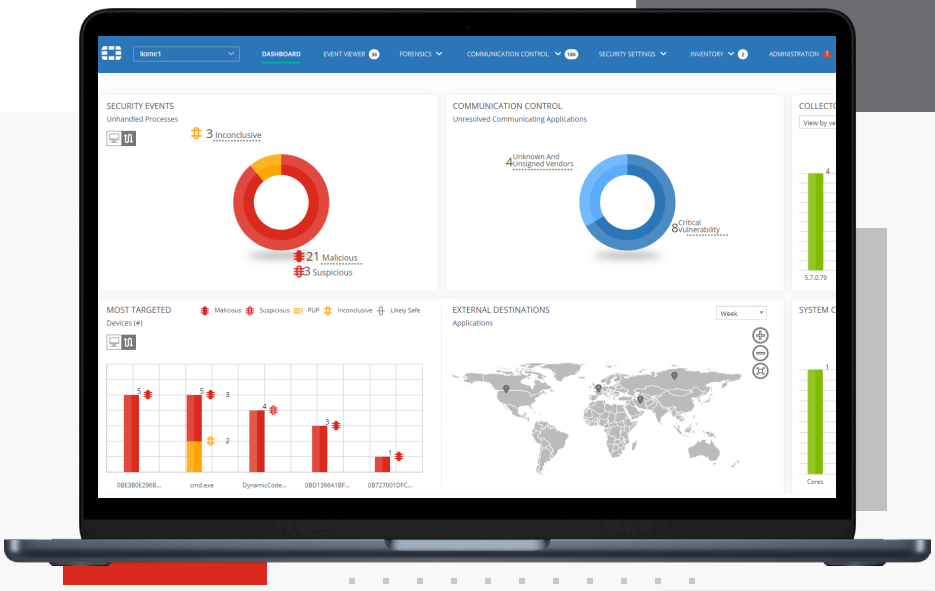
FortiEDR



ハイライト

- 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
- 感染前の保護
- 感染後の保護

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、あらゆる保護対象デバイスのインシデントレスポンスのオーケストレーションにより、リアルタイムでの自動化されたエンドポイント保護を可能にします。これには、現行や旧式のオペレーティングシステムを搭載するワークステーション、サーバー、クラウドのワークロードに加えて、製造業や OT のシステムも含まれます。FortiEDR は、多数のサードパーティソリューションとともに、フォーティネット セキュリティ ファブリックとのネイティブ統合を実現します。

提供形態

ソフトウェア

対応プラットフォーム

- Windows XP SP2、7、8、8.1、10、11（32 ビット / 64 ビット）
- Windows Server 2003 SP2、R2 SP2、2008 SP1、2008 R2 SP2、2012、2012 R2、2016、2019、2022
- MacOS バージョン：El Capitan（10.11）、Sierra（10.12）、High Sierra（10.13）、Mojave（10.14）、Catalina（10.15）、Big Sur（11）、Monterey（12）、Ventura（13）
- Linux バージョン：RedHat Enterprise Linux / CentOS 6.8+、7.2+、8+、9+
  Ubuntu LTS 16.04.5+、18.04 / 20.04 / 22.04 サーバー（64 ビット）
  Oracle Linux 6.10、7.7+、8.2+
  Amazon Linux AMI 2 2018
  Open SUSE Leap 15.2
  SUSE Linux Enterprise Server SLES v12 SP5、v15
  RedHat 9
- サポートする VDI 環境：VMware Horizons 6 および 7、Citrix XenDesktop 7
- 上記サポートする OS で Google Cloud Marketplace に対応

主な機能

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

脆弱性評価と、仮想パッチ / デバイス検出 / アプリケーション制御などのリスク減災策により、攻撃対象領域を大幅に削減します。

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）エンジンによって実証済みの第一の保護レイヤーを提供し、ランサムウェアのような高度な攻撃からの感染をリアルタイムで防止します。

感染後の保護

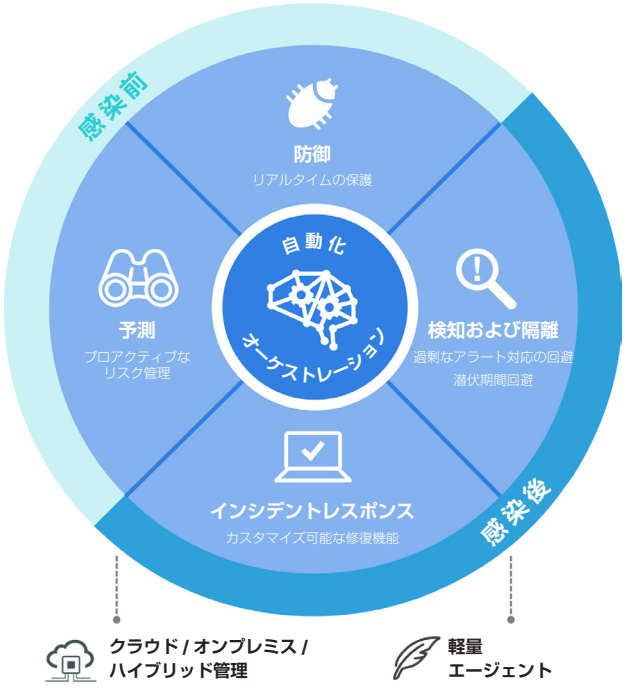
FortiEDR は、エンドポイントでセキュリティ侵害が発生している場合でも高度な攻撃をリアルタイムで検知してブロックするという他のソリューションにはない優れた特長を備えており、セキュリティ侵害やデータ漏えいを阻止し、問題を解決します。脅威の潜伏を防ぎ、インシデントの検知、無効化 / 阻止、調査、レスポンス、修復を実現する自動的な EDR（Endpoint Detection and Response：エンドポイントの脅威検知とレスポンス）の機能セットを提供します。

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稼働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、オンプレミス、ハイブリッドでの導入展開も可能です。



主な利点

FortiEDR は、従来のソリューションや方法と比較すると、イベントの検知と修復にかかる時間を大幅に短縮します。

保護

MITRE ATT&CK Enterprise Evaluation の結果および SE Labs Endpoint Security Enterprise 2022 Q4 テストで証明されているように、FortiEDR は、プラットフォーム間でオーケストレーショ ン化されたインシデントレスポンスによるプロアクティブなリアルタイム自動エンドポイント保護を可能にします。FortiEDR は、AI と機械学習をカーネルレベルで使用し、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、統一された直感的なクラウド管理型プラットフォームを提供します。エンドポイントセキュリティの定型業務を自動化することで、担当者の負担を軽減し、セキュリティギャップを解消します。RBAC やセキュアリモートシェルもサポートしています。

統合

フォーティネットのソリューションと、NGFW、NAC、SIEM、ZTNA、NDR、SOAR などのサードパーティのソリューションと統合することで、セキュリティと自動オーケストレーションを向上させます。

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。

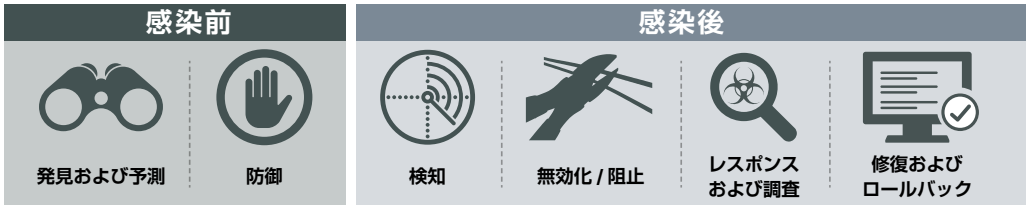
柔軟性

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、オンプレミス、またはセキュアなクラウドインスタンスへの導入が可能です。オンラインとオフラインのどちらのエンドポイントも、ポリシー違反がないかシステム動作を継続的に監視するオンボード AI により保護されます。

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 CVE ステータスの追跡
- 仮想パッチ適用とリスクベースのプロアクティブポリシーにより、システムおよびアプリケーションの脆弱性の発見と減災

防止

FortiEDR は、機械学習に基づくアンチマルウェアエンジンを活用して攻撃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
- FortiGuard 脅威インテリジェンスを通じて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
- アプリケーション制御を活用して、許可またはブロックされたアプリケーションを事前定義リストに簡単に追加が可能で、この機能は、POS デバイスなどの機密度の高いシステムのロックに有効
- 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（C2）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、FortiEDR のバックエンドである FCS（Fortinet Cloud Services）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、有効化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。

主な機能と特長（続き）

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
- フォーティネットクラウドサービス（FCS：Fortinet Cloud Services）内の FortiGuard 脅威インテリジェンスとマルチエンジンサンドボックスにより、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。インシデントレスポンスと修復のプロセスを合理化し、Windows、macOS、Linux 上の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、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。

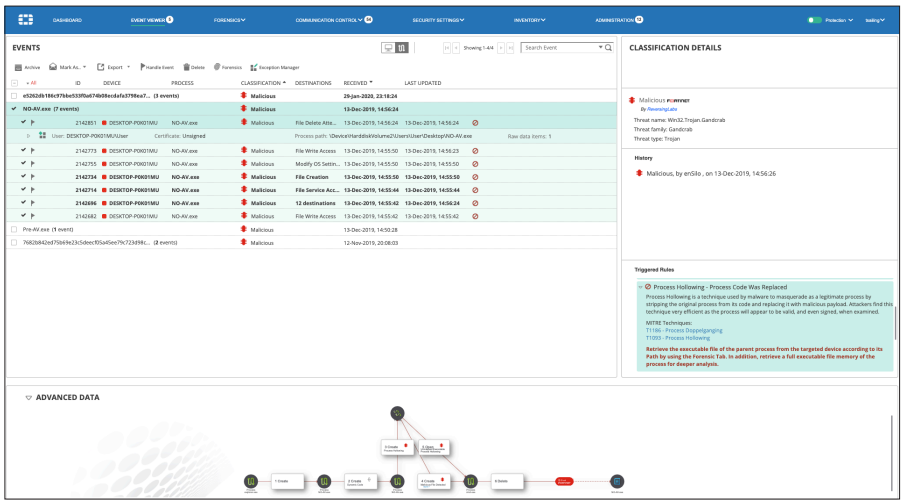
- インシデントの分類を自動化することで、インシデントレスポンスを改善し、容易な解決を実現
- セキュリティアナリストにレスポンスアクションを推奨
- プレイブックの自動化により、フォーティネット セキュリティ ファブリックとサードパーティのセキュリティおよび IT ツール全体において、インシデントレスポンスの手順を標準化
- ファイルの削除、不正なプロセスの停止、持続的な変更の取り消し、ユーザーへの通知、アプリケーションやデバイスの隔離、サポートチケットの発行など、インシデントへのレスポンスを自動化することでセキュリティのリソースを最適化
- インシデントの分類と攻撃の対象（エンドポイントグループなど）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
- システムの稼働を担保しながら、不正な変更のクリーンアップとロールバックを自動化
- オプションの MDR（Managed Detection and Response）サービスにより、さらなる支援の利用が可能

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。TAXII などの一般的な IoC 構文を FortiEDR の Lucene 構文に変換することで、サードパーティのクエリを利用した脅威ハンティングが容易になります。

機能

- 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



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修復用 VLAN へ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、すぐに利用できる FortiEDR 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。

FortiClient EMS

FortiEDR からエンドポイントのステータスを取り込んで、ゼロトラストネットワークアクセス（ZTNA）のポスチャーチェックを実行します。

FortiNDR

リアルタイムの AI ベースのネットワーク脅威検知をエンドポイントデータと組み合わせることで、早期に高度な脅威情報を提供し、インシデントの分析と対応時間を短縮します。これにより、SOC アナリストは、あらゆる環境（オンプレミス、ハイブリッド、マルチクラウド）において、既知および未知の脅威をより効率的に検知し、迅速なレスポンスが可能になります。

サービス

FortiEDR 導入ベストプラクティスサービス（BPS）

導入サービスは、エキスパートによる支援を提供することで、導入を確実に成功させます。これらのサービスには、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、環境のチューニング、トレーニングが含まれます。

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

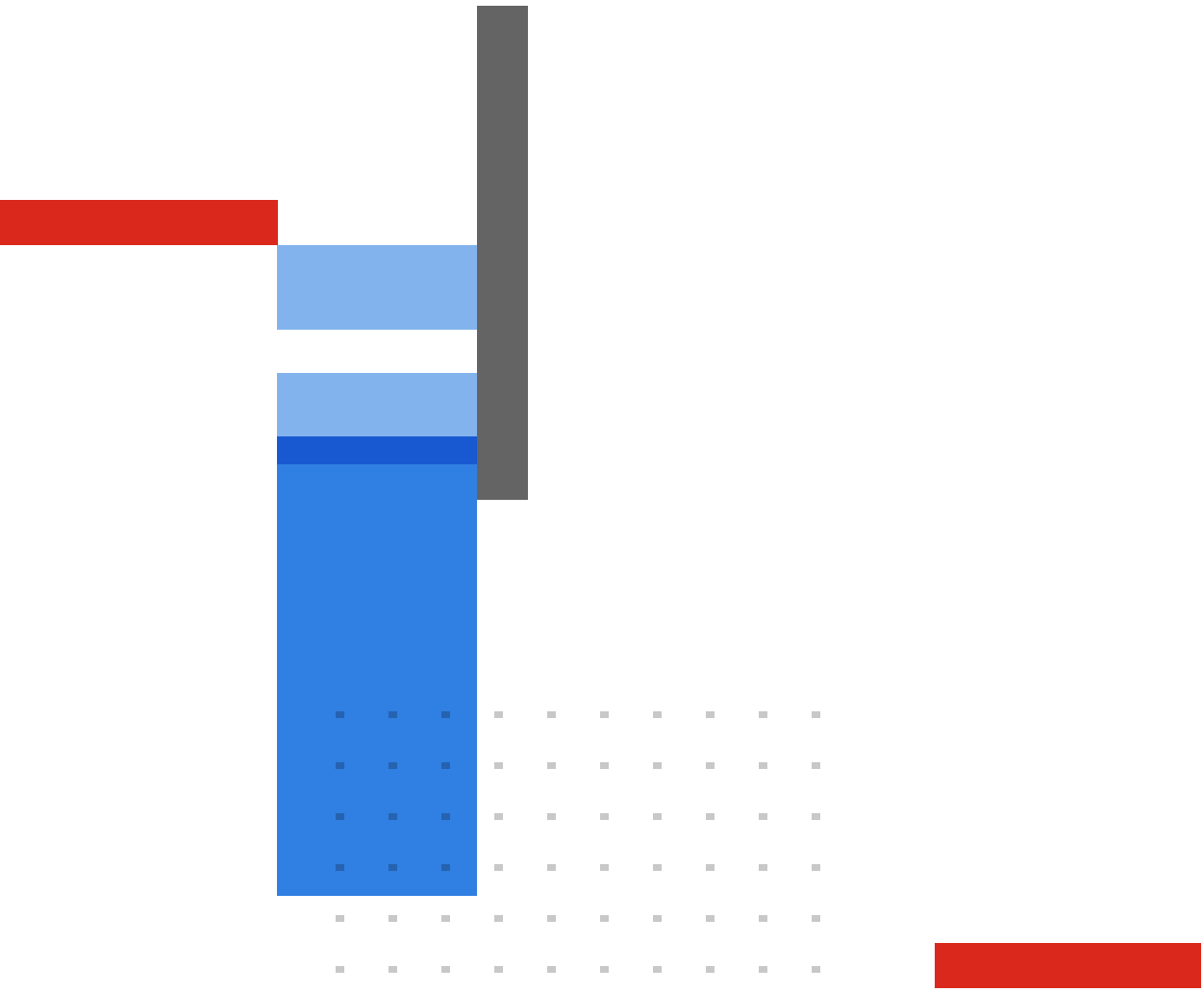
管理およびアーキテクチャ

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英語と日本語で提供されます。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。管理者や管理コンソールのユーザーに対するきめ細かい RBAC（ロールベースのアクセス制御）により、リスクの高いセキュリティ設定の構成ミスを回避できます。セキュアリモートシェルは、時間制限付き証明書を含む豊富なセキュリティユーティリティにより、管理者によるあらゆる場所で働く従業員のリモートでのトラブルシューティングを可能にすることで、エクスプロイトの減災を実現します。

- **オフライン保護：**エンドポイントで保護と検知を実行し、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展開することが可能です。
- **軽量エンドポイントエージェント：**FortiEDR ソリューションは、CPU 使用率 1 ～ 2% 未満、メモリ使用量 200 MB ～ 350 MB、ディスク容量 750 MB ～ 1 GB 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。（メモリ使用量とディスク容量の上限は、脅威ハンティング [レスポンスライセンス] 機能に関連します。
- **クラウドからの導入が可能：**Google Compute Engine の自動導入オーケストレーションにより、Google Cloud Marketplace からの導入が可能です。

フォーティネット CSR ポリシー

フォーティネットは、サイバーセキュリティを通じてあらゆるお客様の進歩と持続可能性を推進し、人権を尊重する倫理的な方法でビジネスを遂行し、常に信頼できるデジタル世界を実現することをお約束します。お客様には、フォーティネットの製品およびサービスを使用して、違法な検閲、監視、拘留、または過剰な武力行使などの人権の侵害または乱用に関与したり、何らかの形で支援したりしないことをフォーティネットに表明し、保証していただくことになります。フォーティネット製品の利用にあたっては、フォーティネットの EULA（エンドユーザー使用許諾契約）を遵守し、EULA に違反すると疑われる場合は、フォーティネット不正告発規定に概要が記載されている手順で報告する必要があります。



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

販売代理店
図研ネットウエイブ株式会社
本社 〒222-8505 神奈川県横浜市港北区新横浜3-1-1
TEL : 045-470-5303 FAX : 045-473-1782
中日本営業所 〒460-0003　愛知県名古屋市中区錦2-4-15 ORE錦二丁目ビル6F
TEL : 052-218-5415
西日本支店　〒530-0002 大阪市北区曽根崎新地1-4-20 桜橋IMビル8F
TEL : 06-6450-0860
MAIL : ft-info@znw.co.jp　URL : https://www.znw.co.jp

DS-FEDR-R16-202402-R1