SOLUTION BRIEF

リアルタイムの自動インシデント レスポンスでエンドポイントのセキュリティを強化

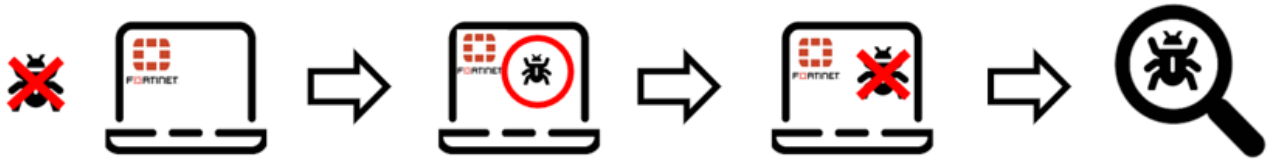
概要

高度な攻撃を受けた場合、エンドポイントはわずか数分で（時には数秒で）感染を許してしまう可能性があります。第一世代の EDR（Endpoint Detection and Response）ツールは、脅威の進化に後れを取っています。手作業によるトリアージとレスポンスを必要とするため、時間がかかり過ぎるだけでなく、アラートも大量に生成されます。そのようなソリューションは、セキュリティオペレーションのコストを上昇させると同時にインシデントレスポンスのプロセスを遅滞させて、本番環境の稼働停止やシステムユーザーの業務の中断を引き起こします。

2016 年 1 月 1 日以降、ランサムウェアによる攻撃は平均で 1 日 4,000 件以上も発生しています [1]。

FortiEDR は、エンドポイントの感染前と感染後にリアルタイムで高度な脅威保護を提供し、このような課題に対処します。FortiEDR は、プロアクティブに攻撃対象領域を減らして、マルウェアによる感染を防ぎ、潜在的な脅威をリアルタイムで検知して無効化します。セキュリティ侵害とマルウェアによる損害を自動的かつ効率的に防ぎ、セキュリティオペレーションを合理化すると同時にユーザーと本番環境の機器をオンライン状態に保ち、業務の継続を実現します。

エンドポイント感染後の FortiEDR による保護の仕組み



エンドポイントの FortiEDR エージェントがファイルベースのマルウェアの大半を実行前に阻止して感染を防ぎます。

感染した場合でも、リアルタイムで脅威を検知して無効化し、被害の発生を阻止します。

脅威を封じ込めた後には、プレイブックとクラウドベースのインテリジェンスに基づいてインシデントへのレスポンスのオーケストレーションが行われます。

FortiEDR は、メモリとスナップショットを保存してフォレンジック調査のガイドラインを提供します。

FortiEDR によるエンドポイントのセキュリティ強化の仕組み

FortiEDR は、脅威の防止、検知、そしてレスポンスの機能を軽量のフットプリントに集約した次世代エンドポイント保護ソリューションで、システムリソースに制約のあるデバイスでも簡単に導入することができます。FortiEDR は、脅威の発見とリスクの減災、次世代アンチウイルス（NGAV）、振る舞いベースの検知、リアルタイムのブロック、自動インシデントレスポンス、フォレンジック調査、脅威の追跡、仮想パッチなどの様々な機能を備えています（図 1 を参照）。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する FortiEDR は、FortiGate、FortiNAC、FortiSandbox、FortiSIEM などのセキュリティ 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。

プロアクティブなリスク減災

FortiEDR は、既存のエンドポイントにインストールされている FortiEDR コレクタを使用し、管理されていないデバイスやアプリケーションを継続的にスキャンしてセキュリティチームに完全な可視性を提供します。アナリストは、アプリケーションのレーティング、脆弱性、リアルタイムの脅威インテリジェンスに基づいて通信制御ポリシーを割り当てることができます。プロアクティブなリスク減災により、保護されていないエンドポイントの数を最小限に抑えて攻撃対象領域を減らします。

リアルタイムの脅威防止

FortiEDR には、ファイルベースのマルウェアからエンドポイントを保護する機械学習（ML）ベースの AV エンジンが組み込まれています。FortiEDR は、インターネットに接続されていないエンドポイントも保護することができます。フットプリントが小さく幅広いオペレーティングシステムをサポートする FortiEDR は、リアルタイムのオペレーションシステムを実行する POS（販売時点情報管理）端末や製造業務で使用されるプロセスコントローラなど、リソースに制約のあるデバイスにも導入することができます。

検知とブロックの自動化

FortiEDR は、振る舞いベースの検知機能を活用して潜在的な脅威を自動的に特定し、無効化します。エンドポイントの内蔵ストレージに侵入することなくメモリ内に潜伏し、従来の AV による防御を容易に回避するファイルレスマルウェアに対して、このようなアプローチは特に有効です。ファイルレス攻撃は、「環境寄生型（LoTL：Living off the Land）」攻撃とも呼ばれ、正当なシステムリソースを悪用してすべての攻撃をメモリ内部のみで実行するほか、不正な目的を達成するためにランサムウェアなどの攻撃ベクトルを送り込みます。

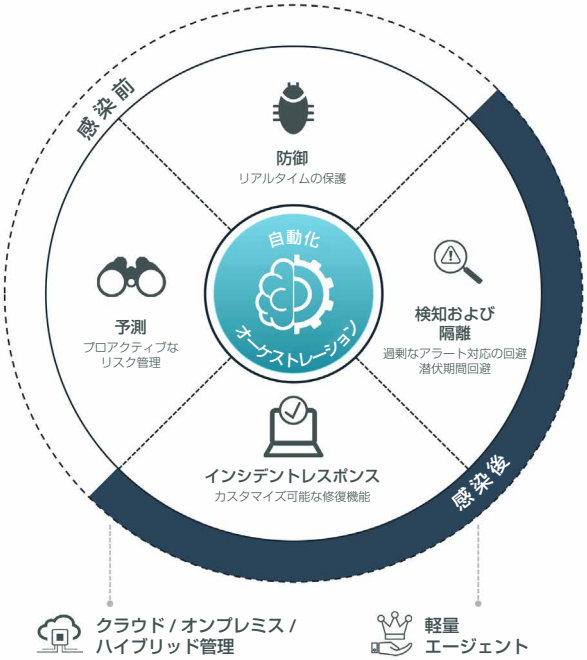


図 1：FortiEDR は、感染前・感染後それぞれで実施する機能を持ち、エンドポイントに対する脅威の検知とレスポンスを改善

不審な振る舞いが発生すると、FortiEDR は要求されるアウトバウンド通信とファイルシステムへのアクセスをすべてブロックし、攻撃を即座に阻止します。同時に、FortiEDR のクラウドベースのバックエンドで継続的に脅威が分類されて適切なレスポンスが可能となると同時に、ノイズが排除されてセキュリティ分析やオペレーションの効率化が実現します。

インシデントレスポンスのオーケストレーション

FortiEDR にはカスタマイズ可能なプレイブックが付属しており、インシデントへのレスポンスと修復のオーケストレーションおよび自動化が実現します。プレイブックによって呼び出される代表的な自動のアクションには、不正なプロセスの中止、ファイルの削除、持続的な脅威のクリーンアップ、不正な変更のロールバック、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オープンなどがあります。

すべてのエンドポイントが同等のリスク耐性を備えているわけではありません。たとえば、製造現場のコントローラシステムは高度な可用性が要求されるため、従業員のノート PC に比べてリスク耐性が低くなります。プレイブックを活用することで、セキュリティチームは脅威の分類とエンドポイントグループに基づいて適切なアクションを開始する、コンテキストベースのインシデントレスポンスを設計することができます。このアプローチによってインシデントレスポンスの一貫性が確保され、セキュリティチームが定型業務に費やす時間を減らすと同時に、リスク耐性に合わせてエンドポイントのセキュリティポリシーを調整することが可能になります。

フォレンジック調査

FortiEDR 独自のガイド機能付インタフェースでは、アラートに関する明確な説明や、フォレンジック調査の実行に必要な次の論理的なステップが表示されます。FortiEDR は、ATT&CK データベースなどの信頼できる情報源から提供される攻撃テクニックの詳細情報を活用し、自動的にデータを補強します。特許取得済のコードトレース技術により、サイバー攻撃チェーン全体の完全な可視性がセキュリティチームに提供されます。また、FortiEDR はメモリのスナップショットを保存して調査の実行を支援します。

ビジネスにおけるメリット

FortiEDR は、エンドポイント保護、インシデントへのレスポンス、セキュリティオペレーション、そして事業継続性といった各分野において、大きなビジネス価値を提供します。

リアルタイムの保護によるセキュリティの改善

リアルタイムで機能し機械学習（ML）を活用する FortiEDR は、セキュリティ侵害やデータ漏えい、そしてランサムウェアによる損害をリアルタイムで防止し、検知後即座にレスポンスを実行します。FortiEDR は、企業組織のエンドポイント保護を改善するだけでなく、防止スタックを回避する脅威の影響を最小限に抑えます。

セキュリティオペレーションの最適化

FortiEDR は、標準化されカスタマイズも可能なインシデントレスポンスのプロセスによって、セキュリティワークフローを最適化します。反復的なタスクを自動化し、誤検知を最小限に抑えることでスタッフの負荷を削減すると同時に、過剰なアラート対応を回避します。自動的なアラートの統合やイベントの関連付け、わかりやすい攻撃グラフの表示により、インシデントレスポンスとフォレンジック調査を効率化します。

ビジネスの継続性の確保

FortiEDR は、稼働状態のシステムに対するレスポンスと修復が可能で、サービスの中断を回避してユーザーの生産性を維持します。また、システムリソースに制約のあるレガシー機器をサポートするため、そのような機器を長期に渡って活用可能になります。セキュリティチームは、FortiEDR を利用して悪意のある被害からシステムをロールバックすることが可能で、コストのかかるシステムの再イメージ化を回避できます。

FortiEDR の主な機能と特長

感染前		感染後			
発見および予測	防御	検知	無効化	レスポンスおよび調査	修復およびロールバック
プロアクティブなリスク減災	**マルウェア動作前の保護**	**リアルタイムの脅威検知**	**セキュリティ侵害とデータ漏えいの阻止**	**攻撃の完全な可視化**	**修復**
• 不正なデバイスや IoT 機器の発見 • アプリケーションおよびレピュテーション • 脆弱性 • リスクベースのポリシーによる攻撃対象領域の削減 • 仮想パッチ	• カーネルレベル • 機械学習の活用、シグネチャレス • アプリケーション	• 過剰なアラート対応の回避 • マルウェアの分類 • IOC の表示 • 攻撃チェーンの完全な可視化	• 業界初の感染後のリアルタイムブロック機能 • アウトバウンド通信のブロック • データ流出の防止 • データ改ざんとランサムウェアによる暗号化の防止	• カスタマイズ可能なインシデントレスポンスプレイブック • 脅威の潜伏期間回避 • フォレンジックデータの取得 • ファイルレス攻撃のメモリスナップショット • 空き時間での脅威追跡の実行	• 不正な変更のロールバック • 不正ファイルの削除 • 持続的な脅威のクリーンアップ • システムの再イメージ化 / 再構築回避 • 事業継続性の確保 • 外部修復ツール用の REST API 出力

フォーティネットの導入支援および MDR サービス

- フォーティネットのプロフェッショナルサービスは、アーキテクチャプランニング、構成、プレイブックのセットアップとカスタマイズ、トレーニングに関する専門的なサポートを提供します。
- フォーティネットの MDR サービスである FortiResponder が提供する 24 時間 365 日体制の脅威の監視、アラートのトリアージ、リモート修復サービスを活用することで、安心してビジネスに注力できるようになります。
- フォーティネットの認定 MSSP パートナーが、完全なマネージド SOC をはじめとする MDR サービスを提供します。

終わりに

高度な脅威やランサムウェアの数が増加し、巧妙化も進む現在、企業組織はエンドポイントをはじめとする全般的なセキュリティ対策を強化する必要に迫られています。FortiEDR は、軽量で導入しやすい次世代のエンドポイント保護、検知、そしてレスポンスの機能を提供します。FortiEDR を導入することで、セキュリティチームはエンドポイントのセキュリティ強化、さらにインシデントレスポンスの迅速化、セキュリティオペレーションの効率化が可能になると同時に、生産ラインの停止や専門知識を有する従業員の作業中断など、コストの増加に繋がる影響を回避できるようになります。

FortiEDR の代表的なユースケース

OT セキュリティ

FortiEDR は、マシンをオンライン状態に維持して保護の中断を回避しながら、運用テクノロジー（OT）環境で脅威を検知して無効化します。脆弱性を発見し、次回のメンテナンス時期までの間エクスプロイトからシステムを保護する仮想パッチなどを提供し、減災を制御します。極めて小さなフットプリントで機能する FortiEDR は、デバイスのパフォーマンスを損なうことなくレガシー機器やネットワークから隔離されているシステムをサポートします。

POS セキュリティ

FortiEDR は、POS（販売時点管理）システムでクレジットカード情報を保護し、攻撃を発生源で阻止します。PCI-DSS（Payment Card Industry Data Security Standard）認定済の FortiEDR は、システムが侵害された場合でもデータの流出を防止します。また、仮想パッチを提供して脆弱性から POS システムを保護します。小さなフットプリントで機能する FortiEDR は組込み型の OS をサポートし、レガシーの POS システムに最適なソリューションを提供します。

[1]「How To Protect Your Networks from Ransomware」、米国連邦捜査局、2020 年 2 月 3 日時点の情報（英語）：https://www.justice.gov/criminal-ccips/file/872771/download

FORTINET
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

SB-Boosting-Endpoint-Security-202004-R1