SOLUTION BRIEF

リアルタイムかつ自動化されたエンドポイントセキュリティによるOT インフラストラクチャの保護

概要

OT（オペレーショナルテクノロジー）と IT（情報テクノロジー）のインフラストラクチャを統合する組織が増え、サイバーセキュリティはますます重要になっています。最近の調査によると、回答者の 70% が OT / IT の統合を歓迎しています[1]。また、回答者の 65% がインフラストラクチャの安全な統合に対して最も重要な役割を担う役職として CISO と回答し、統合における CISO に対する期待の大きさがうかがえます[2]。

CISO はこうした期待に応えるために OT のエンドポイント保護など、多くの課題を解決する必要があります。FortiEDR の堅牢なソリューションを導入することで、感染前の予防から感染後の対処まで、OT エンドポイントセキュリティによって脅威からリアルタイムでの保護が可能になります。また、脅威への迅速な対応、アクションの自動化が実現し、業務の中断を回避できます。

脆弱な OT エンドポイント

製造、輸送、公益事業、石油、ガスなどの業界の OT インフラストラクチャを標的とする高度なサイバー攻撃が増加しています。攻撃にはランサムウェアの一種であるクリプトウェアが使用され、重要な制御に関する情報をわずか数秒で暗号化し、生産ラインや安全システムを中断や停止に追い込みます。攻撃の動機はさまざまであり、金銭的利益のために身代金を要求する場合もあれば、重要なインフラストラクチャを停止させて、コミュニティの内外で大混乱を引き起こすことを目的とする場合もあります。

これまで、OT インフラストラクチャは自己完結型でエアギャップが存在したため、通常はインターネット経由の脅威から隔離されていました。しかし、現在では OT システムと IT システムの統合が一般化したため、パッチを適用していない旧式の OT エンドポイントはサイバー攻撃者の格好の侵入口になっています。また、OT デバイスはシステムリソースが制限されたレガシーのオペレーティングシステムを使用することが多いため、従来のエンドポイントセキュリティソリューションでは十分保護することはできません。

このようなセキュリティの課題を解決するために、多くの組織は新しいリスクを発見するたびにセキュリティのポイント製品を追加しています。しかし、このアプローチではセキュリティが複雑になり、セキュリティギャップは解消されません。最近の調査で OT のセキュリティ管理における重要な課題を尋ねたところ、回答者の 55% が「システムの分離と断片化」を挙げています[4]。

OT 環境に最適な FortiEDR

FortiEDR では、感染前の防止と感染後の対処の両方の機能によって、OT のすべてのエンドポイントにリアルタイムの高度な脅威保護が提供されるため、これらの問題を含め、さまざまな問題を解決できます。次世代エンドポイントセキュリティソリューションの FortiEDR には、EDR の多様な機能が集約され、軽量化されているため、システムリソースに制約のある OT デバイスでも簡単に導入することができます。

FortiEDR では、以下の機能によって生産環境のエンドポイントを強力に保護できます。

- リアルタイムの脅威検知
- 侵入後の保護
- 業務を中断しない修復
- 仮想パッチ
- エアギャップのシステムとレガシー Windows システムのサポート
- オンプレミスの導入オプション

重要なインフラストラクチャに対するサイバー攻撃が増加しています。最近の調査によると、回答者の 54% が今後 12 ヵ月以内に重要なインフラストラクチャが攻撃される可能性があると回答しています[3]。

FortiEDR の主な機能には次世代アンチウイルス（NGAV）、アプリケーション通信制御、エンドポイントの検知とレスポンス（EDR）の自動化、リアルタイムのブロック、脅威ハンティング、インシデントレスポンス、仮想パッチなどがあります（図 1）。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採用しているため、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できます。

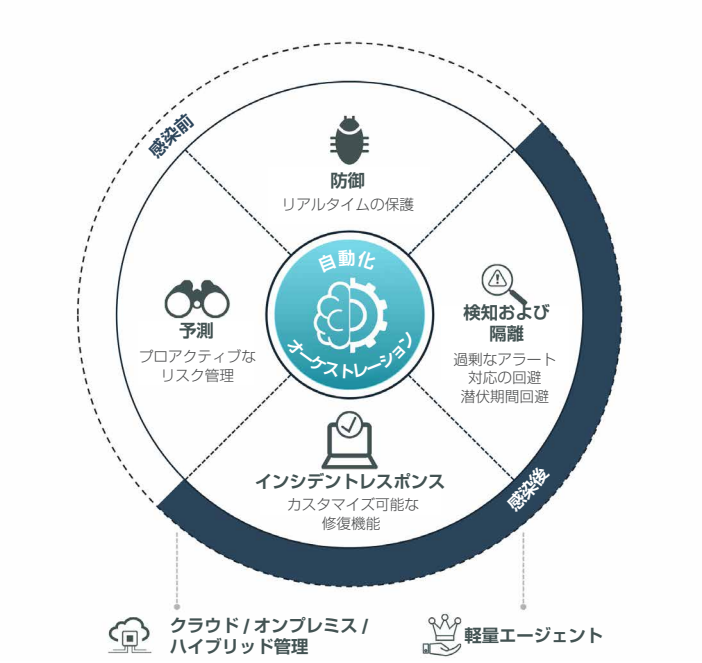


図 1：FortiEDR の機能

FortiEDR の主な利点

FortiEDR ではリアルタイムの自動レスポンス、生産の継続、中断不要のリスクの減災など、明確なビジネス価値を OT 環境に提供します。

リアルタイムの自動レスポンス

FortiEDR では不審なプロセスが検知されると、自動ブロックによってリアルタイムでプロセスが停止されます。また、フォーティネット クラウドサービスによって証拠が収集され、イベントの検証と分類が行われます。セキュリティチームはプレイブックをカスタマイズして、エンドポイントのグループ、ミッションに対する重要度、脅威の分類に基づいて対応を自動化できます。自動レスポンスと修復の機能にはプロセスの終了、不正なファイルや感染したファイルの削除、完全なクリーンアップ、ユーザーへの通知、そしてチケットの処理が含まれます。

また、感染前の予防と感染後の対処の両方が可能な包括的な保護がエンドポイントにリアルタイムで提供されるため、侵害に対する不安が軽減されます。さらに、大量のアラートの処理が不要になり、インシデントレスポンスの手順を標準化してセキュリティと運用のリソースを最適化できます。

生産の継続

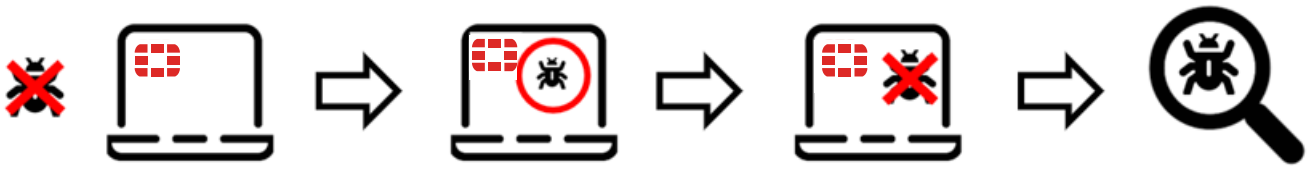
リアルタイムの自動レスポンスには、セキュリティ担当者が注意すべき落とし穴があります。たとえば、正規ユーザーがアプリケーションを操作しているときに検知システムが作動し、誤ってアラームが生成されることがあります。また、不適切なレスポンスがアプリケーションに悪影響を及ぼしたり、最悪の場合、ミッションクリティカルな生産システムがクラッシュしてブルースクリーンが表示されたりすることもあります。

FortiEDR ではプロセスを終了してエンドポイントを隔離する代わりに、アウトバウンド通信とファイルシステムへのアクセスがブロックされ、脅威が排除されます。不審なプロセスが無害であると判断された場合、FortiEDR では生産システムに影響せずにブロックを解除できます。また、セキュリティインシデントの場合もマシンをオフラインにせずに修復できます。生産工場のシステムの接続が維持されるため、ユーザーにも影響しません。IT / OT インフラストラクチャを統合する場合、この機能は特に重要であり、セキュリティチームは IT に悪影響を及ぼさずに OT デバイスを迅速かつ効果的に保護できます。

中断不要のリスクの減災

OT システムへのパッチ適用には注意が必要です。生産を中断させないために、運用チームは予定されたメンテナンススケジュールに従った変更しか許可されないことがあります。しかし、その間、システムは攻撃に対して脆弱になります。

FortiEDR ではアプリケーションと脆弱性が継続的に評価され、セキュリティチームは仮想パッチを適用してリスクをプロアクティブに軽減できるため、このような問題は起こりません。このプロアクティブなアプローチによってリスクが緩和されるため、予定されたメンテナンス以外でマシンをオフラインにする必要はありません。



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を実行前に阻止して感染を防止します。

感染した場合でも、FortiEDR が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。

発見および予測

FortiEDR ではエンドポイントの攻撃対象領域をプロアクティブに検知できます。また、不正なデバイスやアプリケーションが可視化されるため、システムやアプリケーションの脆弱性を特定し、仮想パッチを適用してプロアクティブにリスクを緩和できます。

防御

カーネルベースの NGAV では、ファイルベースのマルウェアを自動で防止できます。FortiEDR に継続的に更新されるクラウドベースの脅威インテリジェンスと機械学習を組み合わせることで、時間の経過とともに知識が蓄積され、脅威をより効果的に特定できるようになります。

検知および無効化

FortiEDR は振る舞いベースの検知によって感染後の保護にも対応し、侵害やランサムウェアによる被害をリアルタイムで阻止できる業界唯一のソリューションです。

レスポンスおよび修復

カスタマイズ可能なプレイブックを使用することにより、セキュリティチームはインシデントレスポンスの調整、対応と修復のプロセスの効率化と自動化、およびオンラインでの修復が可能になります。このアプローチでは、ユーザーの作業や業務の中断を回避しながらネットワークを保護できます。

調査および追跡

FortiEDR ではフォレンジック調査に必要な脅威に関する詳細情報が提供されます。その独自のインタフェースにはガイダンスとベストプラクティスのほか、推奨される手順も表示されます。

世界の公益事業の意思決定者の 64% が高度なサイバー攻撃が最大の課題であると回答しています [5]。

フォーティネットの導入支援と 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が導入、構成、プレイブックの設定とカスタマイズなどの専門的なサポートを提供
- フォーティネットの MDR サービスである FortiResponder が 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提供
- フォーティネット認定 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

終わりに

高度な脅威、特にランサムウェアは日々増加し、巧妙化しているため、組織は OT のエンドポイントをはじめ、セキュリティ対策全体を強化する必要があります。FortiEDR は、リソースが制限された OT デバイスにも簡単に導入できる軽量な次世代エンドポイント保護ソリューションです。FortiEDR を導入することで、エンドポイントのセキュリティが強化され、セキュリティチームは迅速なインシデントレスポンスと効率的なセキュリティ管理が可能になり、生産ラインの停止やユーザーの生産性の低下など、コストの増加につながる影響を回避できます。

[1]「Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT」、Ponemon Institute、2019 年 2 月（英語）：
https://www.tuvopensky.com/wp-content/uploads/2019/02/TUV-Rheinland-OpenSky-2019-Research-Report-on-Safety-Security-and-Privacy-in-the-Interconnected-World-of-IT-OT-_-IIoT.pdf

[2] 同上

[3] 同上

[4]「Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?」、Siemens and Ponemon Institute、2019 年

[5] 同上

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-Protecting-OT-Infrastructures-202109-R1