Fortinet Master Distributor

SCSK
夢ある未来を、共に創る。

ソリューション名 FortiEDR

SCSKと実現するマルウェア対策

誤検知が多い	隔離や駆除ができない	検知されたアラートへの対応方法がわからない
正規のファイルやアプリケーションを誤って検知・検出してしまい業務効率が低下	デバイスの隔離やマルウェアの駆除まではできず、人の手による分析や介入、MDRを同時に利用する必要がある	正規のファイルやアプリケーションを誤って検知・検出してしまい業務効率が低下

FortiEDR

エンドポイントの可視化、分析、保護、修復をリアルタイムで実行

FortiEDR 概要

準備 → 検知 → 分析 → 封込 → 根絶 → 復旧

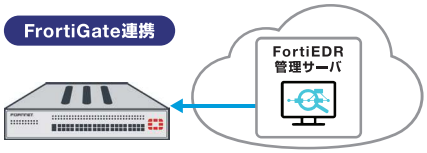
FortiEDRは検知だけでなく、準備から復旧まで対応

侵入前	**発見&予測**	アプリケーションの可視化やデバイスコントロール
侵入前	**予防**	カーネルベースでの保護と機械学習による次世代AV
侵入後	**検知と無効化**	**侵害をリアルタイムに停止**、不審な通信をブロック
侵入後	**対応と調査/修復**	プレイブックの実装、**自動的な対処と修復**

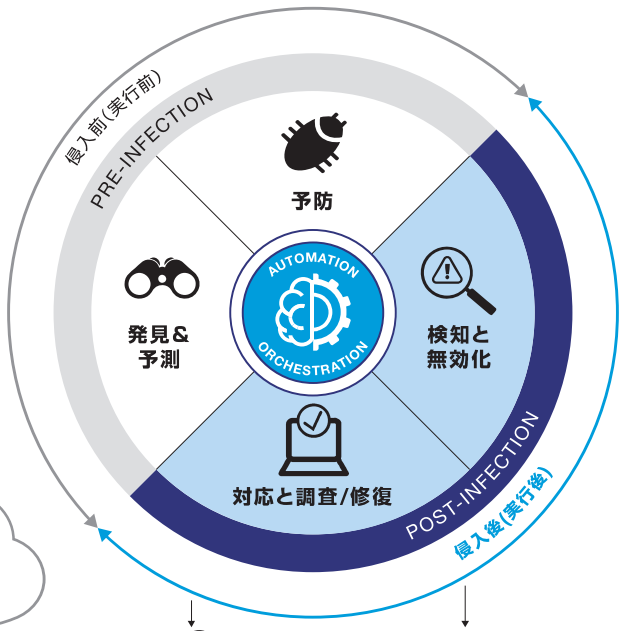
侵入前(実行時)フェーズ

発見 & 予測(Predict)
- アプリケーションの脆弱性を**自動で評価**
- リスクベースのプロアクティブポリシー/仮想パッチ
- 攻撃対象領域の削減に貢献

予防
- **機械学習/カーネルベース**のアンチウイルス
- 継続的に更新される**クラウドデータベース**



FortiEDRで検知された不審なIPアドレスの情報を
FortiGateに共有してFortiGateですぐにブロックできるようになります。



クラウド / オンプレミス / ハイブリッド管理

軽量 エージェント

侵入後(実行後)フェーズ

検知 & 無効化(DEFUSE)
- ふるまいベースの検知
- 悪意のある動きを自動/**リアルタイムでブロック**
- データの不正転送や感染の横展開、C&Cへの通信も見つけて**自動/リアルタイムで遮断**
- ファイルシステムへのアクセスを拒否 – ランサムウェアによる暗号化やレジストリの改ざんを**自動で修復**

対応と調査/修復
- イベントの**自動選別(Auto-Triage)**
- デバイスグループや脅威種別に基づいた**カスタマイズ可能なプレイブックを自動実行**
- **自動対処・修復**(ユーザ通知、プロセス切断、デバイス分離、ファイル削除、悪意のある変更の戻し、等々)