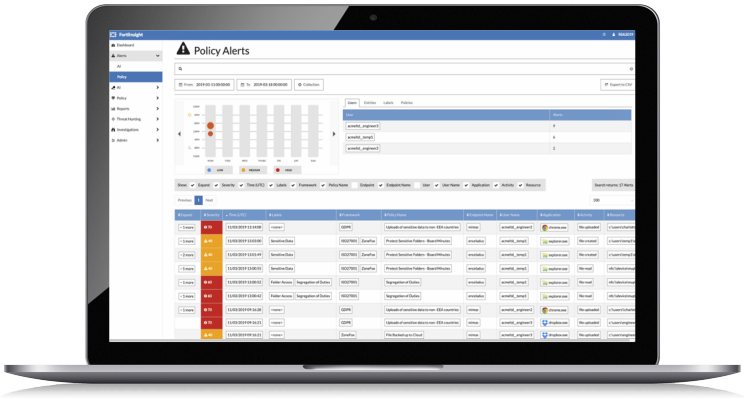
DATA SHEET

FortiInsight

ユーザーの振る舞いに基づく脅威検知ソリューション

FortiInsight は、高度な脅威を検知して、ビジネスにおけるクリティカルデータのリスクとなる振る舞いの特定、レスポンス、管理を可能にする、フォーティネット独自のデータセキュリティ / 脅威検知ソリューションです。強力かつ柔軟な機械学習とユーザーのアクションに関する詳細なフォレンジックを組み合わせることで、他のソリューションよりも迅速に事実を特定します。



拡張知能（AI）

機械学習と UEBA（ユーザー / エンティティ振る舞い分析）により、データの可視性が強化されます。機械学習によって調査プロセスの各段階が最適化され、侵害されたアカウントからデータの盗難にいたるまで、新たな脅威を特定します。

法規制のコンプライアンス支援

組織内におけるデータへのアクセス、使用、移動の詳細な可視化、コンプライアンスのフレームワークに特有のルール、レポートの作成、さらにコンプライアンスに反する振る舞いの特定と対処、そして管理のための分析が可能です。

監視とフォレンジックレベルのレポート機能

データの保存場所、あるいはユーザーがネットワークの内部 / 外部のどちらにいるかを問わず、データの移動やエンドポイントの活動を 24 時間監視します。ユーザーの振る舞いに対するフォレンジックの完全な履歴を蓄積し、詳細な調査とレポートを提供します。

ハイライト

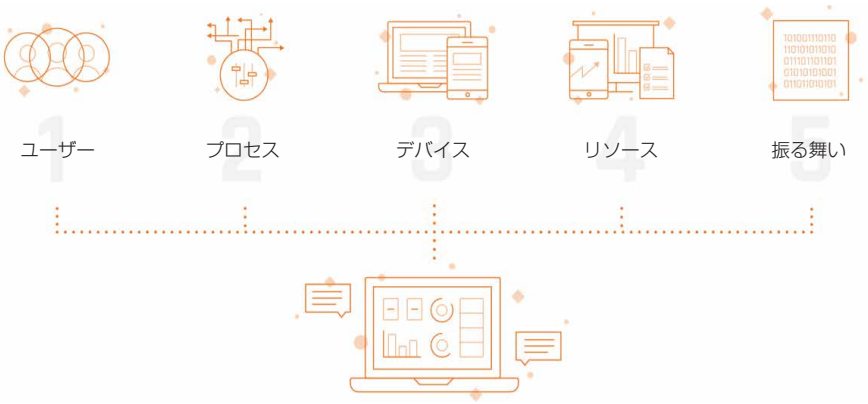
- エンドポイントエージェントは、収集されたエンドポイントのメタデータだけを使用するため、極めて少ないシステムリソースで動作します。
- エージェントがインストールされると即座にデータの収集が開始され、データの動きに関する実用的インテリジェンスが直ちに提供されます。
- リアルタイムのデータ処理とユーザーの振る舞いの分析によって、迅速なインシデント対応が可能になります。
- ユーザー、システム、そして各ネットワークレイヤーでの通常の行動を学習することで、環境の全体像を提示し詳細なフォレンジック機能を提供します。
- FortiInsightはFortiSIEMや任意のSIEMと統合でき、API経由でポリシーやAIのアラートを利用可能になります。これらの方法によって、境界からネットワークの中核までの相関付けが初めて実現しました。

ハイライト

主な機能と運用に関する情報

豊富な実績を誇る優れたテクノロジーが、ネットワークの内部と外部の両方でデータに関する行動を監視することで、誰が、いつ、どこでアクセスしたか、といった、データに関するアクティビティを完全に可視化し、異常な行動を直ちに通知します。セキュリティ対策の強化、機密情報の保護、法規制におけるコンプライアンス支援を可能にします。

- FortiInsight は、ホスティング型ソリューションです。
- Endpoint Agent テクノロジーによって、クラウドストレージアプリケーション、Skype、Instant Messenger などとの間を移動するファイルが可視化されるため、暗号化されて移動するファイル名が追跡されます。
- ルールセットを採用し AI によって拡張された UEBA が、悪意のある内部関係者によるアクティビティから侵害されたアカウントにいたるまで、既知および未知の脅威を検知します。
- ユーザー、マシン、アプリケーション、ファイル、振る舞い、ネットワークの送信先 / 送信元のアクティビティが記録され、フォレンジックレベルの詳細情報を調査やコンプライアンスの目的で利用できるようになります。
- エンドポイントメタデータのビッグデータストレージアーキテクチャによって、遡及的ルールと「時間を遡る」機能が提供されるため、過去のイベントを現在のコンテキストで確認できます。
- エンドポイントの「ストアアンドフォワード」機能によって、オフラインでの不審な活動が報告されるため、ネットワークの死角が解消されます。
- FortiInsight は、最新のビッグデータテクノロジーを利用して数十億のイベントを収集、分析します。セキュリティチームは、収集された情報にほぼ瞬時にアクセスし、誰が給与データベースをダウンロードしたのか、誰かが顧客リストをその IP アドレスにアップロードしているのはなぜか、未承認のクラウドストレージアプリケーションを何人が使用しているのか、といった情報をすぐに確認できます。
- エンドポイントエージェントは、Windows で利用できます。



FortiInsight の仕組み

各システムにインストールされる、構成不要の軽量エージェントは、エンドポイントに対するいかなる分析や予防アクションも実行することなく、警告や調査に必要なデータの収集と送信だけを実行します。この「エンドポイントエージェント」アプローチには、高度な攻撃者が標的とする攻撃対象領域の縮小、エンドポイントのパフォーマンス低下の抑制、データの保存、分析、セキュリティチームへの提示を実行するクラウドベースのサービスへのテレメトリ送信といった、大きなメリットがあります。FortiInsight は、データの一元管理を通じて環境全体の相関付けと機械学習を可能にし、ユーザーとデータの振る舞いに対する比類ない実用的インテリジェンスを提供します。

FortiInsight では、高性能の機械学習を採用した高度なルールベースエンジンによって、ネットワークの内部と外部ですべてのアクティビティが確実に監視されます。許容可能なユーザーのアクティビティを特定するためのルールが作成され、そのルールが適用された後、ルールに違反するアクティビティが発生すると、アラートが管理者に送信されます。さらに、この機能セットは各種コンプライアンス（GDPR や HIPAA など）の潜在的な違反の解消に有効な実用的インテリジェンスの提供にも広く利用されます。

FortiInsight ソリューションは、機械学習を活用してデータに関する振る舞いやデータフローを検証することで、通常は検索されることのないファイルの検索、作業パターンの不自然な変化、アカウントの侵害、ピアグループのアクティビティの変化など、さまざまなユーザーの異常な行動を特定します。

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

DS-FUEBA-R1-201908-R1