SOLUTION BRIEF

FortiInsight による UEBA：ユーザー / エンティティ振る舞い分析

要約

内部関係者からもたらされる新たな脅威を特定して対処することは、過失あるいは故意のどちらであっても、組織にとって複雑な問題であることに変わりありません。しかしながら、これが無視できない問題であることは事実です。FortiInsight による UEBA（ユーザー / エンティティ振る舞い分析）をフォーティネット セキュリティ ファブリックに統合することで、フォレンジックの機械学習を使用して、内部関係者によってもたらされる脅威を最小限に抑えることができます。FortiInsight では、ユーザー、エンドポイント、アプリケーション、ピアグループ、ファイル、およびデータの移動をプロファイル化できるため、内部の脅威に対する保護が大幅に強化されます。

社内のユーザーによって発生するリスクは、その行動が過失あるいは故意のいずれであったとしても、サイバーセキュリティの観点から見れば、重大な盲点になる可能性があります。しかしながら、GDPR（General Data Protection Regulation：EU 一般データ保護規制）、HIPAA（Health Insurance Portability and Accountability Act：医療保険の携行性と責任に関する法律）、MiFID（Markets in Financial Instruments Directive：金融商品市場指令）、ISO（International Organization for Standardization：国際標準化機構）の規制をはじめとする現行の法規制によって、セキュリティイベントやデータ侵害につながる振る舞いに対応できることを文書化し実証できない企業に対し、厳しい罰則が課せられる恐れがあります。

フォーティネット セキュリティ ファブリックは、データセキュリティと脅威の検知に関連する独自の機能によって、高度な脅威からの強力な保護を可能にしています。エンドポイント監視と振る舞い分析の機能を装備することにより、ビジネスクリティカルなデータのリスクとなるユーザーの危険な振る舞いを検知し、対応と管理が可能になります。

FortiInsight によって、次のような脅威からの保護が強化されます。

- ポリシー違反
- 資産への不正アクセス
- データの外部への持ち出しと IP（知的財産）の盗難
- アカウントの侵害
- 内部関係者による不正行為

内部の脅威からデータを保護

FortiInsight は、ユーザーのミス、ポリシー違反、悪意のある内部関係者の行動、アカウントの侵害、外部からのアカウントの乗っ取りをはじめとする、既知および未知の脅威を検知します。

FortiInsight は、強力かつ柔軟な機械学習とユーザーの挙動に関する詳細なフォレンジックの両方を活用します。この組み合わせによって、ユーザーの振る舞いとデータの移動をネットワークの内部と外部の両方で監視し、組織のデータに関して、誰が、どこで、何を、いつ、といった振る舞いをあらゆる角度から可視化します。

FortiInsight は、データフローに関するユーザーの振る舞いを検証して、異常な振る舞い（一般的にはユーザーが検索することのないファイルへのアクセスなど）、作業パターンの変化、アカウントの侵害、ピアグループの異常な振る舞いを発見します。異常な振る舞いが特定された場合は、リアルタイムのアラートが関係者に送信されるため、ただちに調査を実施できます。

FortiInsight の主なメリット：

- システムリソースに影響を与えることなく、**データフローとユーザーの挙動に関するリアルタイムの実用的インテリジェンス**を提供
- ユーザーの挙動の分析をリアルタイムで処理することで、**迅速なインシデント対応**を実現
- コンプライアンスレポートと調査追跡によって、**一元化された重要なインテリジェンス**を提供
- **誤検知の排除**を可能にするため、ルールベースのエンジンが潜在的に危険なユーザーの挙動を高い精度で発見
- ユーザー、システム、ネットワークの各レイヤーでの通常の活動を学習することで、**包括的な保護と詳細なフォレンジック**を実現

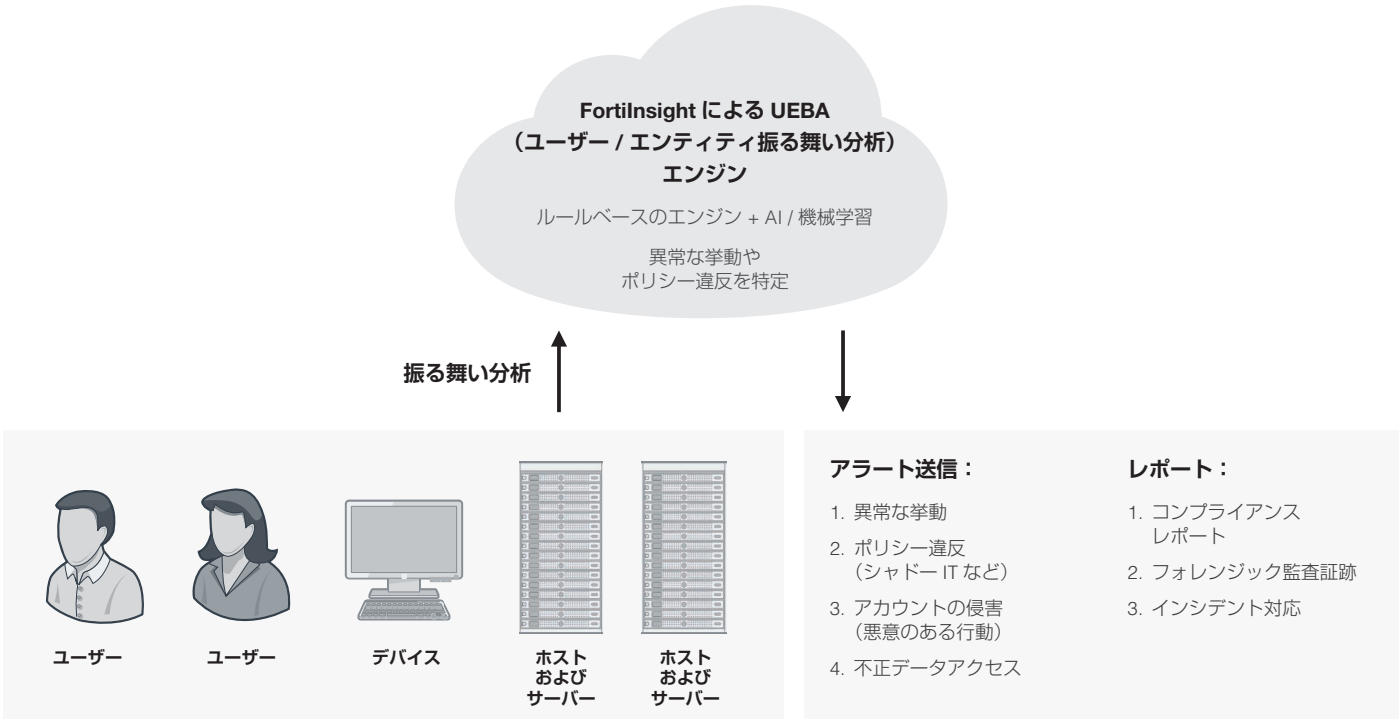

図 1：FortiInsight がエンドポイント監視と振る舞い分析機能をフォーティネット セキュリティ ファブリックに統合

FortiInsight ソリューションの主な機能と特長

FortiInsight をセキュリティ ファブリックに統合することで、ビジネスクリティカルなデータに対するユーザーの異常な挙動に関する実用的インテリジェンスがリアルタイムで提供されます。これにより、ユーザー、アプリケーション、ピアグループ、ファイル、エンドポイント、ネットワークの包括的プロファイルが構築されます。FortiInsight の中核機能には次のものがあります。

- **エンドポイントコネクタ / データベースコネクタ：**複数のプラットフォームやフォームファクターで発生する、ユーザーやエンドポイントの挙動の軽量のストリームから、（オン / オフ両方のネットワークの）データフローを完全に可視化できます。Microsoft SQL Server データベースから、ユーザーアクセス、データクエリ、およびデータベースの変更をリアルタイムで追跡します。
- **連携型のセキュリティ：**アラートやインシデント対応のタスクを実行するチームのメンバー毎に、異なるユーザー名とパスワードを割り当てることができます。
- **コンプライアンスレポート：**専用のレポート機能を利用することで、GDPR や HIPAA などの法規制のコンプライアンスが容易になります。
- **可視化とダッシュボード:**チャート、グラフ、ダッシュボードをゼロタッチで実装し、ユーザーの挙動を可視化できます。FortiInsight は、データを自動的に一元的なコンソールへ送信します。送信データには、ユーザー、プロセス、エンドポイント、リソースの種類（ファイル、データベース、アプリケーションなど）、挙動に関する重要な情報が含まれています。ログの収集や解析は必要なく、遅延なくすぐに分析が実行されます。
- **詳細なフォレンジック監査証跡：**すべてのユーザーとエンドポイントの振る舞いの完全なレコードを利用して、潜在的あるいは現実の侵害に迅速に対応できます。これは、効果的なインシデント対応、ケース（実例）の作成、コンプライアンスへの対応（GDPR の 72 時間以内の報告ルールなど）に不可欠な機能です。

ネットワーク内部 / 外部の保護

セキュリティ ファブリックへの統合によって、FortiInsight は自動検知とレスポンスの機能を活用したユーザーとエンドポイントの継続的な監視を通じて、内部の脅威からの保護が可能になります。コンプライアンス違反、不審あるいは異常な（オン / オフ両方のネットワークでの）振る舞いが特定され、ただちにアラートが送信されます。機械学習と高度な分析を活用する、フォーティネットの脅威検知のプロアクティブなアプローチが、エンタープライズネットワーク全体の保護と可視性のさらなる強化を可能にします。

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.co.jp/contact

お問い合わせ