

observe IT | proofpoint.

攻撃者はシステムではなく「人」を狙う
だからセキュリティも「人」中心に

PEOPLE-CENTRIC アプローチを用いた 内部脅威対策

データ漏洩の 50% 以上は内部から

厳しい競争社会において、現代の労働環境はより国際化し、働く人々は短期間で会社を渡り歩き、また常にネットに繋がっています。従来のサイバーセキュリティは外部からの侵入に対抗することに焦点を当てていましたが、現代のセキュリティはそれに加え、内側からの脅威にも対応しなければなりません。

Proofpoint Insider Threat Management | ObserveIT は、インサイダー（内部関係者）の悪意、怠慢、または事故による情報漏えい、犯罪、およびブランド価値の毀損から企業を守ります。

組織における最大の脆弱性は「人」です。攻撃者が「人」から狙う中、セキュリティも「人」中心に組み立てる必要があります。PEOPLE-CENTRIC アプローチを用いた内部脅威対策の詳細をご覧ください。

100 か国以上で 1,200 社以上の 導入実績

AIRCATTLE

BainCapital

wering Forward

genpac

ptc

MS

TIAA



コンテキストの力 (インシデントの前後関係から全容をつかむ)

ObserveIT プラットフォームは、セキュリティチームがユーザーリスクを特定し、データの漏えいを防止し、インシデントレスポンスを迅速化できるように、ユーザーの行動とデータの動きの前後関係や相互関係を明らかにします。

ObserveIT は最新のアーキテクチャと軽量なエンドポイントエージェントを用いて内部脅威対策を効率化し、投資効果を迅速に具現化させます。

ユーザーリスクの特定

リスクの高いユーザーの行動やデータの動きを迅速に把握して、潜在的に内部不正をおこなう可能性がある人物を特定し、不正をおこなう前に対処します。

- 強力な分析力と脅威テンプレートのライブラリを活用して潜在的な脅威を検出し、対応します。
- 特権ユーザー、危険な状態にあるユーザー、業務委託先のコントラクターなどを監視します。
- エンドユーザーのプライバシーと匿名性を守ります。

インシデント対応の迅速化

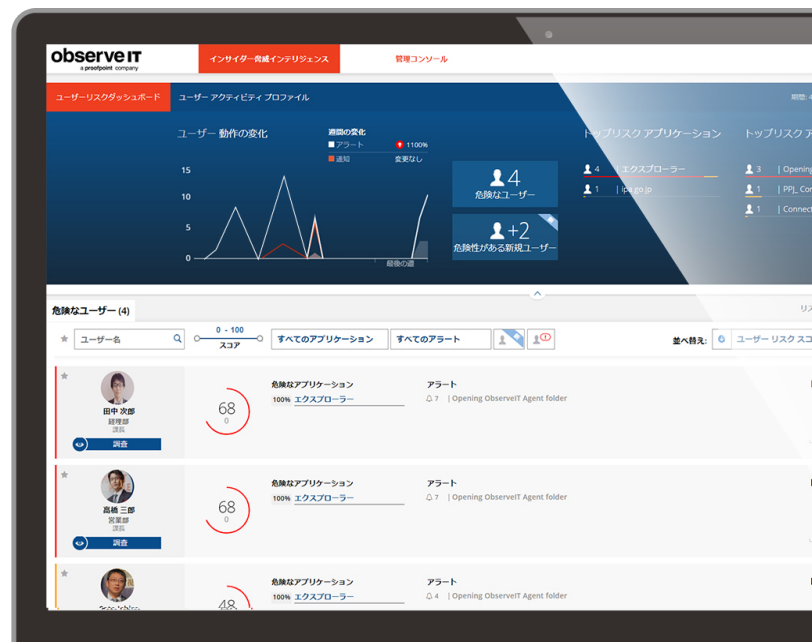
ObserveIT のアラートからコンテキストを把握し、誰が / どこで / いつ / なぜ / 何をおこなったかを特定できるようにします。

- セキュリティアラートに関するすべてのコンテキストを提供します。
- 数日あるいは数週間かかっていた調査を、分単位または時間単位に短縮します。
- エビデンスを迅速に整理し、意思決定や法的措置をサポートします。

OBSERVEIT について

ObserveIT プラットフォームは、企業のセキュリティチームがユーザーリスクを特定し、インサイダーによるデータ漏洩を検出し、セキュリティ インシデント レスポンスを迅速化できるように、ユーザー行動とデータの動きの相互関係を明らかにします。ObserveIT はパワフルなコンテキスト インテリジェンス エンジンと、顧客や主要なサイバーセキュリティ フレームワークから作成された 400 以上の脅威テンプレートを活用して、インサイダー脅威対策プログラムを効率化し、投資効果を迅速に具現化させます。

©ObserveIT, Inc.、ObserveIT は、米国およびその他の国にある Proofpoint, Inc. の登録商標です。本文書に含まれるその他のすべての商標はそれぞれの所有者に帰属します。



内部からの情報漏えい対策

エンドポイントからのデータ流出を可視化し、内部関係者 (インサイダー) による情報漏えいを検知して対応し、さらにユーザー行動のコンテキストを活用して意思決定をサポートします。

- USB、コピー & ペースト、印刷、コマンドライン、メール、Web アプリケーション、クラウドストレージなどからのデータ流出を可視化します。
- ユーザーの行動にリアルタイムに対応する、プロアクティブなユーザー教育やアプリケーションベースの防止策を導入します。これにより、犯行への抑止力を働かせることができます。

内部脅威対策プログラムの構築

世界有数のテクノロジーを活用した内部脅威への対策プログラムを構築し、脅威の検出や対応にかかる時間をシステムチェックに短縮します。

- セキュリティ運用部門、人事部門、法務、コンプライアンス部門、事業部門との円滑な情報共有を支援します。
- 内部脅威の評価、プレイブック、クラウドソーシングによる脅威テンプレートなどにより、ベストプラクティスを提供します。
- 内部脅威プロフェッショナルのコミュニティからの最新情報を検知ルールに反映しています。