Proofpoint Insider Threat Management

People-Centricアプローチで組織の内部脅威を管理

主なメリット

- 内部関係者の危険なアクティビティを検知し、エンドポイントからのデータ損失を防止
- 内部脅威とデータ損失インシデントへの対応効率を向上
- 最新のクラウドネイティブ バックエンドを利用した拡張性の高いSaaSの導入で、早期に投資価値を実現
- 軽量のエンドポイント エージェントでユーザーの生産性を維持

主なユースケース

- それぞれのユーザーが持つリスクを特定
- エンドポイントからのデータ損失を防止
- ユーザー起因のインシデントにすばやく対応
- 内部脅威対策を強化

Proofpoint Insider Threat Management（以下、Proofpoint ITM、旧：ObserveIT）は、人を中心としたアプローチを採用し、内部関係者に起因するデータ損失、不正行為、ブランド価値の毀損から組織を守ります。権限のあるユーザーの悪意、怠慢、事故に起因する被害から組織を保護します。内部関係者によるデータ侵害から守るため、ユーザーのアクティビティとデータの移動を関連付けて分析します。また、危険な動作をリアルタイムで検知できるため、確固たる証拠を容易に集めることができます。

危険な動作をリアルタイムで検知し、阻止する

Proofpoint ITMを使用すると、危険なリスクが発生したときに、アプリケーション、ファイル、デスクトップ、サーバー、仮想化環境全体でリスクを相関分析できます。分析は、インシデントの発生直後におこなわれるのではなく、インシデントが発生する前の早い段階から始めることにより、リアルタイムに内部脅威を抑止することができます。リアルタイムの可視化機能により、内部脅威インシデントの検知、分析、防御、解決を効率的に行うことができます。

クラウドソーシングで実際の脅威に対応するシナリオ

次のような危険な動作をリアルタイムで検知できます。

- データ持ち出し
- 危険なラテラルムーブメント（ネットワーク内の展開）
- 権限の悪用
- アプリケーションの誤使用
- 不正アクセス
- 危険な可能性が高いアクション

Booleanロジック（ブール論理）ベースのルール ビルダーを用いると、ルールを簡単に作成し、環境に合わせて調整できます。提供される脅威シナリオをそのまま使用することも、変更して使用することもできます。また、一から作成することも可能です。プルーフポイントの広範な内部脅威ルールは、カーネギーメロン大学のCERT、NITTF、NIST、プルーフポイントのユーザーから収集した情報をベースに作成されています。

ポイント&クリックによる脅威ハンティング

脅威ハンティングは外部脅威のみを対象としたものではありません。Proofpoint ITMでは、ポイント＆クリック インターフェースを使用して、異常な行動をプロアクティブに探し、内部関係者による不要なリスクや不正行為を識別することができます。

効率の良いポイント＆クリック ハンティングで、次のことが可能になります。

- 実際の環境に合わせて危険な行動やアクティビティを評価する
- インテリジェントなグループ分けにより、無関係な大量のアクティビティを除外し、必要な情報のみに集中する
- タイムラインとスクリーンショットにより、異常な行動のコンテキスト情報を収集する

データ分類のサポート

Microsoft Information Protection (MIP) と連携し、ユーザーがファイルを操作すると、Proofpoint ITMエージェントがMIP秘密度ラベルをリアルタイムで読み取ります。ファイルのMIP秘密度ラベル、元の場所、種類、送信先に基づいて、検知と防御のルールを設定できます。

データ損失の予防

Proofpoint ITMは、共通のエンドポイント チャネルを使用して、機密データの流出を防ぎます。これには、USB接続のデバイス(ローカルの同期フォルダーなど)、ネットワークストレージ、フラッシュドライブ、マルチメディアデバイス、スマートフォンなども含まれ、ユーザーがオフラインの場合でも機能します。

次のように、USBに対するアクティビティをユーザー、グループ、ホスト別に管理できます。

- USBへのデータの書き込みをブロックする
- 特定のUSBデバイスをセーフリストに登録する
- ファイル名のパターンに一致するファイルをブロックする
- ファイルの種類でブロックする
- ファイルの送信元でブロックする
- グローバルな防止ルールを適用する

Proofpoint Enterprise DLP製品では、Eメールやクラウドアプリも保護の対象に追加できます。

インシデント対応の迅速化

多くの組織は、セキュリティイベントが発生した後に内部脅威の調査を行っています。その結果、既存のセキュリティツールの汎用的なワークフローでは内部脅威を阻止できないことに気付きます。内部データは機密性が高く、このようなデータを保護するには、サイバーセキュリティ以外のチームとも緊密に連携しなければなりません。

コンテキスト情報と確固たる証拠を迅速に収集

プルーフポイントのワークフローは、ユーザーが引き起こすイベントに合わせて調整されています。収集されたメタデータとスクリーンショットの中から、キーワードとフィルターを使用してセキュリティイベントを検索できます。新しいクエリー言語を習得する必要はありません。フィルターを保存して、脅威ハンティングや調査活動で使用することもできます。

調査で見つかった重大なイベントやアラートには、タグを付けて分類できます。証拠を共有するときに、このタグを使用して関連イベントとアラートを検索できます。これらの情報は、よく使うファイル形式 (PDFなど) でエクスポートできます。このレポートには、証拠となるスクリーンショットと、関連するコンテキスト情報 (誰が、何を、どこで、いつ) が含まれます。これにより、サイバーセキュリティの管理作業を効率的に実施できます。また、この情報は人事、法務、コンプライアンス、調査などの担当者にもわかりやすい形式で提供されます。

Proofpoint ITMアーキテクチャの利点

プルーフポイントのクラウドベースのアーキテクチャは、規模、使いやすさ、セキュリティ、拡張可能性を目的として構築されています。業界をリードする軽量のエンドポイントエージェントがアクティビティデータを収集するため、アプリに依存することなく、システムでのユーザーの行動を可視化できます。これにより、ユーザーの生産性が低下することはありません。

完全なSaaSデプロイ

Proofpoint Endpoint DLPは、スケーラビリティ、分析能力、セキュリティ、プライバシー、拡張性を重視した最新のSaaSプラットフォームです。セットアップも短時間で終わり、バックエンドのコストも抑えることができます。セキュリティ管理者は、組織全体の管理作業を効率的に行うことができます。これは、データ アクティビティが瞬時に可視化されることを意味します。

2つの問題を1つの軽量ソリューションで解決

Proofpoint Endpoint DLPと Proofpoint ITM は軽量な共通エージェントと最新のSaaSアーキテクチャを使用します。これにより、Proofpoint Endpoint DLPは日々のユーザーの操作によるデータ損失を防ぎます。Proofpoint ITMは、不正なユーザーやリスクの高いユーザーが行う危険な行動を防ぎます。

詳細

詳細は **proofpoint.com/jp** でご確認ください。