データシート

proofpoint.

PROOFPOINT クラウドアプリセキュリティブローカー

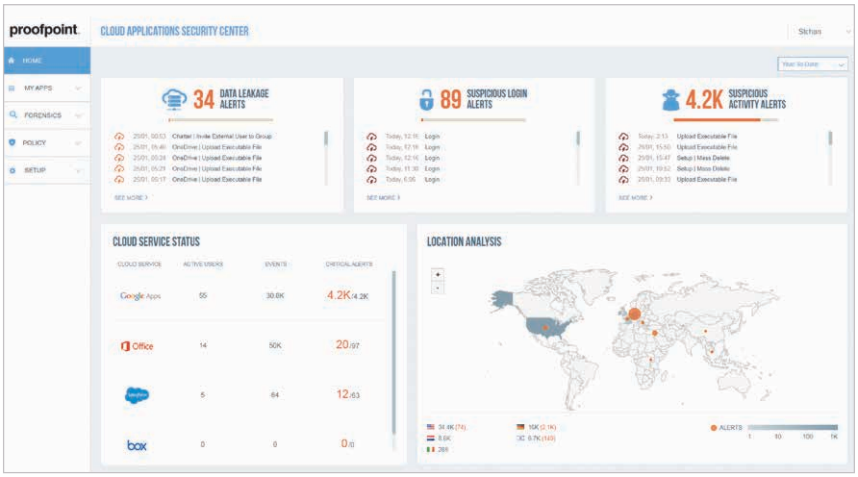
主な利点

- SaaS アプリに関して、独自の人を中心とした見方
- SaaS アプリにおいての最高の脅威検知、リスクベースのアクセスコントロール及び分析
- 脅威認知データセキュリティ
- サードパーティアプリコントロール
- 特定のベンダーを推進しない保護
- 自動ポリシーベース返答アクション
- 受賞歴のある顧客サポート

Proofpoint クラウドアプリセキュリティブローカー (PCASB) は人々とデータを高度な攻撃やクラウド内の事故的な情報共有、コンプライアンスリスクから守ります。PCASB は、クラウドアプリやサービスを自信を持ってご使用いただけるようにします。弊社の強力な分析は、重要なリスクファクターをもとに、お客様がユーザー及びサードパーティアプリに正しいレベルのアクセスを許可することができるようにします。

今日のサイバー攻撃は、人とその働き方を標的とします。多くの仕事はクラウドベースの E メールや Office365、G Suite や Box 等その他の SaaS アプリにて行われています。これらのアプリは重要なデータを含み、さらに幅広いサードパーティアプリに接続します。これにより、SaaS ホストデータのセキュリティ保護が今まで以上に難しくなっているのです。より良いクラウドアプリケーションセキュリティへの道は、E メールやその他のクラウドアプリケーションに関連した攻撃の発見に対する統合的アプローチにかかっています。弊社の統合化され、人を中心としたソリューションは、脅威を防ぎ、あなたの情報を守り、またコンプライアンスを維持するお手伝いをします。

ユーザーを中心とした可視性



クラウドにおけるセキュリティは、ユーザー及びデータの効果的な監視から始まります。PCASB は、クラウドアクセスとデータの取扱いについて、粒度の高い人を中心とした可視性を提供します。特権のあるアカウントを確認し、それが増え続けるのを防ぎます。SaaS アプリ内のどのファイルがデータ紛失防止 (DLP:Data Loss Prevention) ルールに違反しているか、その持ち主、またそれらをダウンロード及び共有している人物を知ることができます。重要な質問に対しての答えを手に入れることができ、すぐに行動に移すことができます。

PCASB はユーザーから文脈的データと行動分析を集め、疑わしい行動を見つけ出します。文脈的データにはユーザーの場所、端末、ネットワークやユーザーがアクセスしようとしている SaaS アプリが含まれます。例えば、一定の SaaS アプリには、あなたの設定した末端セキュリティ基準を満たす企業端末のみからのアクセスを許可することができます。読み取り専用アクセスのみ、またはユーザーのダウンロードできるデータに制限を設けることもできます。

高度な脅威からの保護

企業 SaaS アプリにアップロードされた悪意あるファイルは、あなたの環境全体に一瞬にして広がってしまう可能性があります。弊社のサンドボックス及び分析は、あなたの環境における可能性のあるリスクを検知します。そこから自動的にリアルタイムで検疫やその他の緩和措置を通して隔離することができます。

PCASB は弊社の豊富なクロスチャンネル（SaaS、E メール等）脅威インテリジェンスをユーザー特定のリスクインジケーターと組み合わせ、ユーザーの行動を分析、SaaS アプリ内での異常を検知します。これらの異常には過度のアクティビティ、通常とは違うアクセスの試み等があります。

頑強なポリシーテンプレートがリアルタイムであなたに問題を警告し、リスクベースの認証及び必要な際には権限を減らすこともできます。そうすることであなたのデータの暴露、誤使用または削除を防ぐことができます。また、既存のアイデンティティ管理ソリューションを SAML 認証を通して統合することもできます。弊社のマルチモード建築で、API や転送・リバースプロキシから保護を行うこともできます。

リスク認知データセキュリティ

あなたの組織データのさらに多くが、繊細な内容のものも含めクラウドに保管されています。PCASB は DLP クラシファイアを共有しますーこれには内蔵のスマートアイデンティティ感知、辞書、ルールやテンプレート等が含まれます。これらのポリシーの統一により、あなたは繊細なデータをより早く見つけ、守ることができます。

内蔵のクラシファイアは PCI、PII、PHI 及び GDPR 規則をカバーしています。そしてフレキシブルなカスタムルールでご自分の DLP ポリシーを構築し、データの共有やダウンローについてコントロールできます。暗号化、データのマスキング、検疫やコンプライアンス遵守のための文脈のレバレッジ等が行えます。

PCASB は、広すぎる許可や、許可なく行われるデータ共有によって危険にさらされているデータを見つけ、保護することを可能にします。例えば従業員は個人アカウントとデータ共有を行っている可能性もあり、大量のデータをエクスポートしている可能性もあります。ユーザーを中心とした可視性と行動モニタリングは放置及び乗っ取りの可能性のあるアカウントを素早く検知することができます。さらに重要な点は、PCASB はユーザーレベルのリスクインジケーターと DLP 検知を関連付けることです。この洞察により、より有効な DLP アラートとアクセスコントロールの変更が可能となります。

サードパーティアプリがコントロール及びシャド―イングする

アプリ市場では、Office 365、G Suite、Box やその他のプラットフォーム用に何百というサードパーティアプリを提供しています。弊社はベンダーを公平に見た深い評価を提供し、サードパーティアプリやアドオンから守ります。リスクがある可能性がある場合、弊社は完全な透明性、客観的識別とタイムリーな返答を提供します。正しいレベルの可視性とコントロールにより、弊社はユーザーの生産性を維持し、そのリスクを制限するお手伝いをします。深さのある分析があなたのリスクとアプリごと、またユーザーごとの内容を確認することもできます。

コントロールでは、分析結果をもとにアクションをご自分で決める、または自動化することができます。特権のあるユーザーへのポリシーは、読み書き可能または読み取り専用等のアクセストークンの授与許可等を決定するのに役立ちます。また、アプリからの決められた限度を超えるリクエストを拒否することも可能です。いつでもあなたがコントロールできます。

PCASB はあなたの機関全体においての IT をシャドーイングする可視性を提供します。ネットワークトラフィックログの監査や、リスクスコアを使用してクラウドアプリをグループ分けするお手伝いもします。このスコアは、データ紛失やコンプライアンス不遵守についての決定のお手伝いをします。

ホリスティックな保護

Proofpoint 標的攻撃保護と PCASB を E メールに併用することで、クロスチャネル洞察の脅威検知を改善することができます。共働することで、このソリューションは E メールベースの攻撃と、権限のないアクセスおよびデータ漏洩を関連付けます。

PCASB と、Proofpoint のその他の情報保護を併用することで、クラウドアプリ、メール、社内ファイル共有や SharePoint 内のデータ保護を単純化します。共有データクラシファイアとテンプレートは、デジタル企業内全体で一定化されたセキュリティとコンプライアンスポリシーを強化させるお手伝いをします。

詳細

Proofpoint クラウドアプリセキュリティブローカーは、SaaS アプリケーションを自信をもってご使用いただくことができるようにします。弊社の受賞歴のあるグローバルサポート機関を背後に、フォーチュン 100 企業の半数に、その従業員、データ及びブランドの保護において弊社をご使用いただいています。proofpoint.com/us/products/cloud-app-security-broker より、無料のリスク評価について、またのそのお試し方法についてご覧ください。

PROOFPOINT について

Proofpoint Inc.（NASDAQ:PFPT）は次世代のサイバーセキュリティ企業です。組織が高度な脅威とコンプライアンスのリスクから今日の業務のあり方を保護できるようサポートしています。Proofpoint は、サイバーセキュリティに従事する人々が、彼らのユーザーを標的にした高度な攻撃（電子メール、モバイルアプリ、ソーシャルメディア経由）からユーザーを守り、社内の重要な文書や情報を保護し、万一の場合には社内のチームが、素早く対応するために必要な知識とツールを活用できるようにしておく支援をさせていただきます。現在のモバイルおよびソーシャルメディアに対応した IT 環境向けに構築され、クラウドの力とビッグデータを生かした分析プラットフォームを活用して、今日のより高度な脅威に対抗することができる Proofpoint ソリューションを、フォーチュン 100 企業の半数以上を含む様々な規模の一流企業にご利用いただいています。