Proofpoint ATO Protection (Account Takeover Protection)

クラウドアカウントの乗っ取りを検知して対応

主なメリット

- Microsoft 365、Google Workbench、Oktaのアカウント侵害を検知
- MFAを回避するアカウント乗っ取り攻撃から防御
- アカウント乗っ取り後のアクティビティに関する一元化されたビューで調査を迅速化
- アカウントを停止し、強制的にパスワードリセットを実行することで攻撃者の滞在時間を短縮
- メールボックスのルールやMFA設定への悪意のある変更を修復
- 不審なサードパーティ アプリケーションを削除

Proofpoint Account Takeover Protection (ATO Protection)は、Proofpoint TAP (Targeted Attack Protection)の拡張機能です。侵害されたクラウドアカウントを検知し、クラウド環境を保護します。

Proofpoint ATO Protectionは、Proofpoint TAP (Targeted Attack Protection)の拡張機能です。侵害されたクラウドアカウントを検知し、保護します。Proofpoint ATO Protectionは、人工知能（AI）、相関する脅威インテリジェンス、振る舞い分析を用いて攻撃チェーンにおける不審なアクティビティを検知します。攻撃者による侵害後の変更を検知し、攻撃者のアクセス権を削除します。メールボックスのルールやマルチファクタ認証（MFA）設定への悪意のある変更を修復します。また、不審なサードパーティ アプリケーションを削除し、不審なファイルの隔離や削除も行います。

Proofpoint ATO Protectionは、不審なログイン、攻撃されたユーザー、影響を受けたシステムや設定を確認できる、詳細なレポートを提供します。Proofpoint ITD (Identity Threat Defense)との統合により、アカウント乗っ取りによる、その他のアカウントやホストへの潜在的な影響をワンクリックで確認できます。これらの知見により、企業に被害をもたらす重大な侵害となる前に、攻撃を阻止することができます。

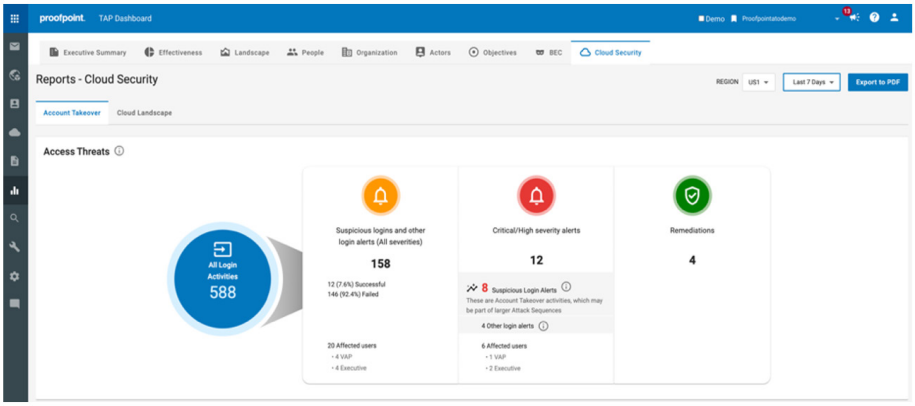
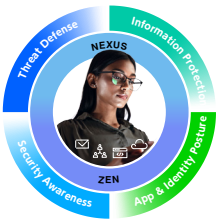


図1：Proofpoint ATO Protectionは不審なログインを検知し、脅威の調査や悪意のある変更の修復に役立つ詳細な知見を提供

このソリューションは、人に起因するリスクの4つの主要エリアを低減する、プルーフポイントのHuman-Centric Security統合型プラットフォームの一機能です。



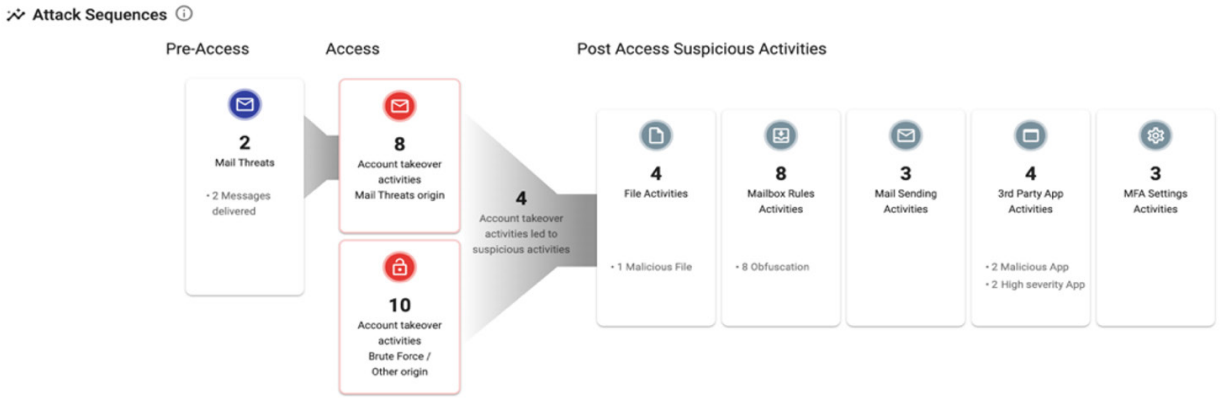


図2：Attack Sequence（攻撃シーケンス）レポートでは、侵害されたアカウントに関するアクセス前後の脅威アクティビティが確認可能

検知と可視性が向上

Proofpoint ATO Protectionは、クラウド環境における侵害されたアカウントや不審なメール、その他のアクティビティを検知します。数千の組織において監視された4,000万以上のユーザーから収集された脅威インテリジェンスを使用します。こうした情報を、AIや振る舞い分析と組み合わせて、組織環境内で発生した、通常とは異なるアクティビティを検知します。こうした手法の組み合わせにより、誤検知アラートを削減します。高精度の検知と、攻撃されたアカウントのすべてのアクティビティを明確に把握することができ、安心です。

アカウントが乗っ取られると、Proofpoint ATO ProtectionはアラートをTAPダッシュボードに追加します。アカウント乗っ取りのアクティビティ、ファイルやメールのアクティビティ、メールボックス ルールやMFA設定への変更、サードパーティアプリの追加が、攻撃タイムラインから確認できます。

迅速な調査

Proofpoint ATO Protectionは、セキュリティ アナリストに、アカウント乗っ取りの原因や、さらなるリスクを低減するための方法を提供します。この情報は、TAP調査システムとプロセスに統合されています。そのため、TAPが提供するデータを補完する知見を得ることができます。乗っ取られたアカウントは、攻撃タイムラインで確認できます。タイムラインで各イベントをクリックし、調べることができます。

アカウントがどのように攻撃されたか、また攻撃者の場所を確認することもできます。また同様の脅威の被害を受けたユーザーについても知ることができます。高度な分析により、ユーザー、IPアドレス、ドメイン、その他の属性の詳細なアクティビティ タイムラインが利用できます。こうした豊富な知見は、組織へのさらなるリスクを評価する上で役立ちます。

自動対応

Proofpoint ATO Protectionは、メールボックスのルールやMFA設定への悪意のある変更を検知し、修復します。攻撃者は多くの場合、メールボックスのルールを変更してシステム内に侵入し、監視を経て、最初の内部フィッシングやその他の攻撃手順を仕掛けます。Proofpoint ATO Protectionはまた、悪意のあるサードパーティ アプリを削除します。これらのアクションのすべてを駆使して、組織への損害を抑え、脅威の調査と対応にかかる時間を短縮します。他の悪意のあるアクティビティが調査によって明らかになれば、乗っ取られたアカウントを修復することができます。また、攻撃者がユーザーのアカウントに追加したファイルを削除することもできます。

「Proofpoint TAP Account Takeover」の名称は、
「Proofpoint Account Takeover Protection」へと変更されました。

詳細はこちら

詳細は **proofpoint.com/jp** でご確認ください。