proofpoint.

ソリューション概要

Proofpoint User Protection

メールの枠を超えてアカウント乗っ取りや
フィッシングに対する保護を拡大し
従業員をサポートする

主なメリット

- メールの枠を超えて**フィッシング保護を提供**
- プルーフポイントの**統合脅威インテリジェンス**により、保護を強化
- 脅威に直面した従業員が**安全な選択を行えるようにガイド**
- アカウント乗っ取りへの**対応を自動化**

サイバー犯罪者は変わらず、人を騙すソーシャル エンジニアリングに熱心です。ユーザーを騙したり脅したりすることにより、認証情報を窃取したり、悪意のあるコードを実行させたりします。メールは依然として、このような攻撃の主要経路となっています。しかし、攻撃者は他の多くのデジタルチャネルを悪用するようにもなっています。

Slack、Microsoft Teams、LinkedIn、Zoomなどのコラボレーションやコミュニケーションのツールです。こうした攻撃は、ユーザーアカウントを侵害し、乗っ取ることを目的としています。プルーフポイントが2024年に行った調査によると、組織の99%が、頻繁にアカウント乗っ取りの標的になっています。また、こうした攻撃の影響を受けた組織は62%近くにのぼります[1]。

このような所見から、組織は、従業員を保護し、アカウント侵害のリスクを低減するための包括的なアプローチを必要としていることがわかります。

Proofpoint User Protectionは、メールの枠を超えた追加の保護レイヤーをユーザーに提供します。リスクベースの学習を自動化し、最もクリック数の多いユーザーやVery Attacked People(VAP)を明らかにします。シームレスなユーザー エクスペリエンスを確保しながら、メッセージングやコラボレーションのアプリケーションにおいて配布される、悪意のあるURLリンクをブロックします。また、AIベースの検知を用いて修復を自動化し、アカウント乗っ取りから防御し、脅威への対応を迅速に行います。

1. プルーフポイント調べ、サンプルサイズn > 5000組織、2024年

可視性を向上させ保護を強化

Proofpoint User Protectionは、プルーフポイントのHuman-Centric セキュリティ プラットフォームの実力を解き放ちます。プルーフポイントの統合脅威インテリジェンスとリスクインサイトにより、保護を強化し、高リスクの個人や悪意のあるアクティビティを詳細に可視化できます。

Proofpoint User Protectionは、Proofpoint Nexus®を使用しています。Nexusは、AI、機械学習、リアルタイムの脅威インテリジェンスを活用した、包括的な脅威インテリジェンス プラットフォームです。Proofpoint User Protectionは、この業界有数の脅威検知スタックを提供し、配布された方法にかかわらずすべての悪意のあるURLリンクをブロックします。Microsoft 365、Google Workspace、Oktaなどのツールでアカウント乗っ取りを高精度で特定します。Proofpoint User Protectionは、高リスクのユーザーを明らかにすることもできます。ユーザーの行動のほか、セキュリティ トレーニングや脅威シミュレーションにおけるパフォーマンスを分析することで、明らかにします。このリスク分析により、現在進行しているアカウント侵害の痕跡を探すこともできます。

このように人的リスクの可視性が向上したことで、適応型セキュリティ制御を、さまざまなリスクプロファイルをもつユーザーに適用することができます。例えば、VAP (Very Attacked People: 要注意人物)、フィッシングメールのリンクをよくクリックしてしまうユーザー、攻撃者に特に狙われている人物をカスタマイズされたセキュリティ トレーニングに自動的に登録することができます。アカウントが乗っ取られた場合の自動修復アクションを適用することもできます。アクセスの無効化、パスワードのリセット、アカウントの隔離などの操作が可能です。サードパーティ アプリのアクセスを無効にしたり、メールボックス ルールへの悪意のある変更を元に戻したりすることもできます。

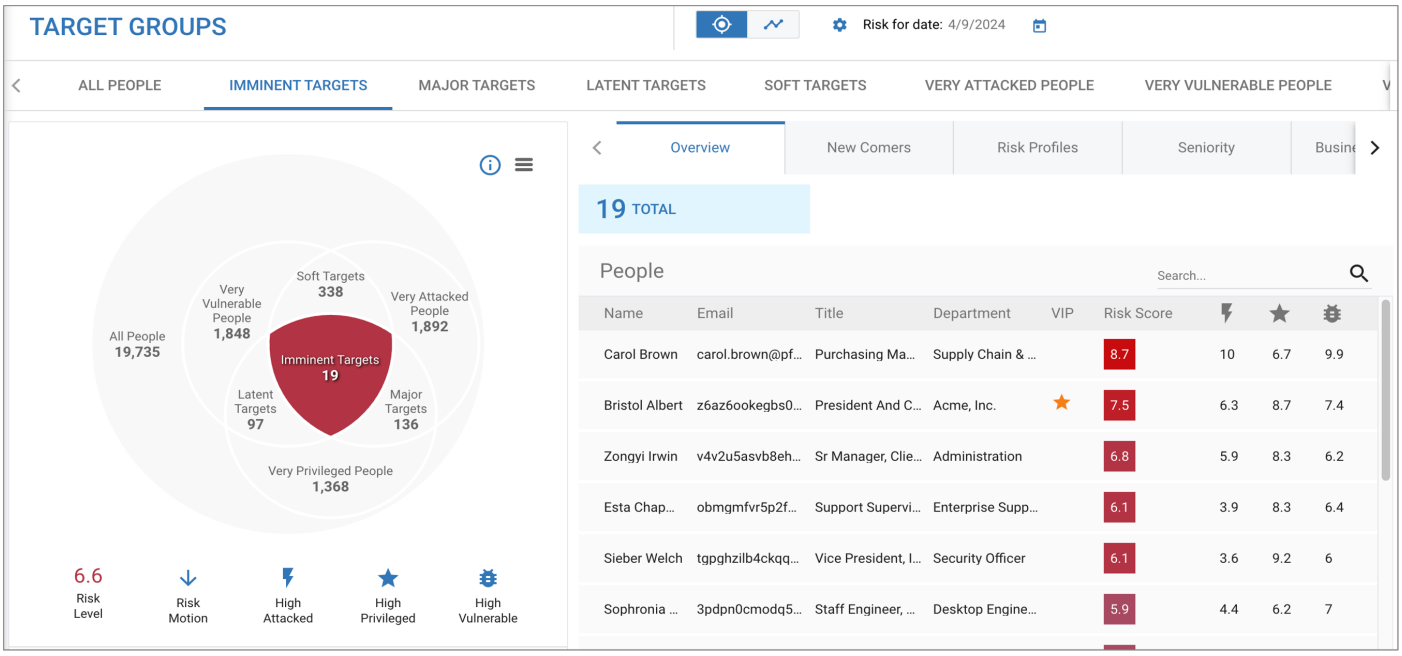

図1：Proofpoint User Protectionは、強化されたヒューマンリスクスコアにより、高リスクユーザーを特定します。こうした可視性の向上により、セキュリティの取り組みの優先順位付け、アダプティブ（適応型）セキュリティ制御の適用、最もリスクにさらされているユーザーへの追加教育の提供が可能になります。

ユーザーが新しい脅威に対するレジリエンスを築けるようサポートする

Proofpoint User Protectionは従業員に、進化するソーシャル エンジニアリング戦術に対するレジリエンスを高めるツール、知識、意欲を提供します。

プルーフポイントのグローバル脅威インテリジェンスから情報を取得するソリューションは、変化し続ける脅威状況に関する知見を即座に提供します。こうした知見を用いて、今まさに世に出回っている脅威や新しい脅威について、ユーザーを教育することができます。トレーニング、脅威シミュレーション、通知など、VAPが直面している特定の脅威について的を絞った教育を、VAPに提供できます。ユーザーの役割、行動、固有のリスクプロファイルに合わせてトレーニングを調整することもできます。

アダプティブ グループ機能およびパスウェイ機能により、高リスクユーザーを対象のキャンペーンに自動的に登録することができます。これにより、堅牢な行動変容プログラムの構築にかかる時間と労力を軽減できます。
また、ユーザーが脅威に直面した際に安全な選択を行えるようガイドすることもできます。

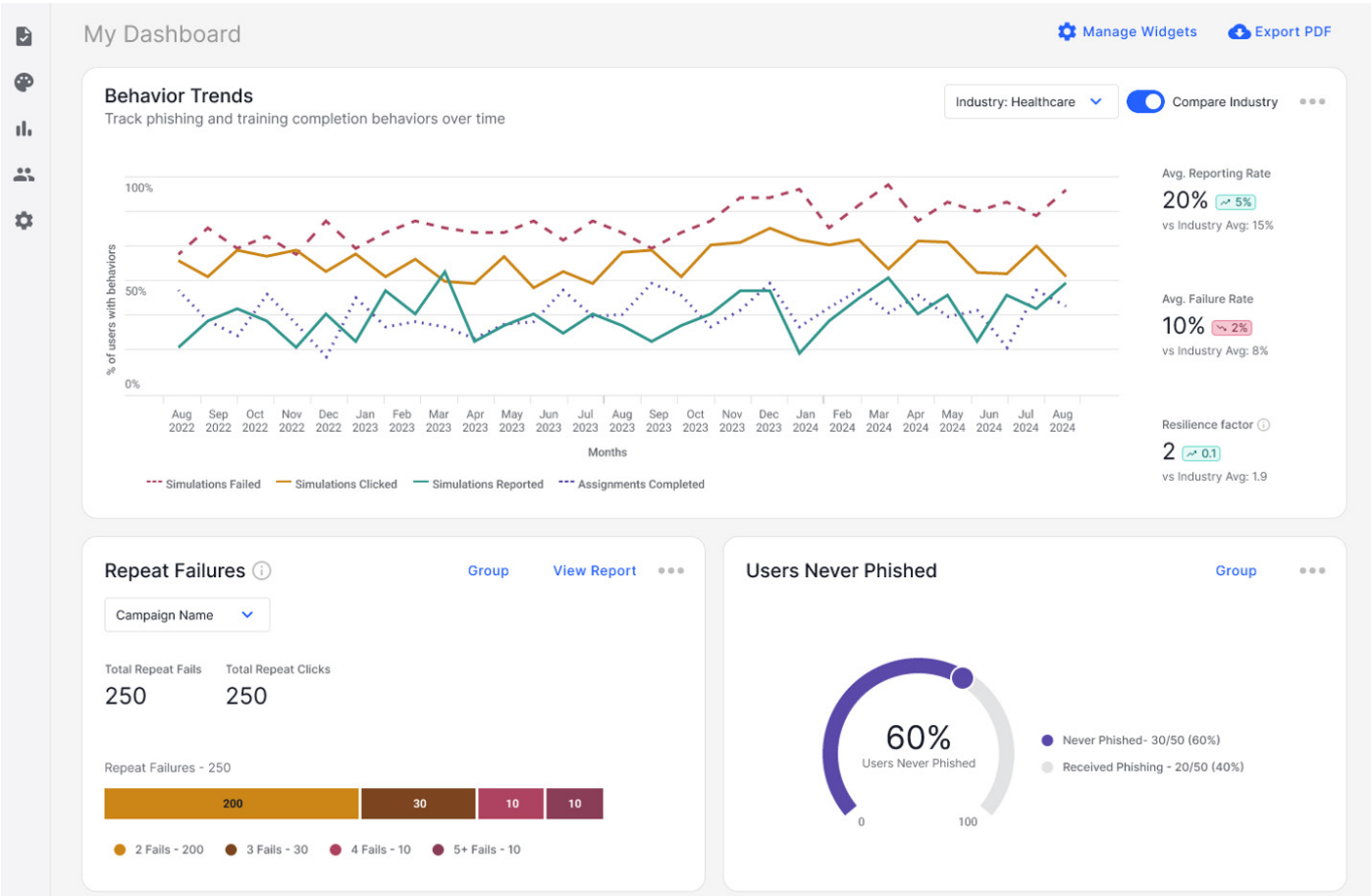

図2：Proofpoint User Protectionはプルーフポイントのグローバル脅威インテリジェンスから情報を得ています。これは、進化し続ける脅威状況に関する知見を提供します。時間の経過と共に行動の傾向を把握しながら、新しい脅威についてユーザーを教育できます。

さまざまなプラットフォームにおいて悪意のあるリンクをブロックする

サイバー犯罪者は、メール以外のデジタルチャネルも悪用するようになっています。

Microsoft Teams、Zoom、Slack、LinkedInや、その他のソーシャルメディアプラットフォームといったチャネルです。

Proofpoint User Protectionは、これらすべてのチャネルにおいて悪意のあるURLをブロックする、広範な保護を提供します。

Proofpoint User Protectionは、21兆以上のURLを分析している、Proofpoint Nexusを使用しています。このインテリジェンスに基づいて、Proofpoint User Protectionは、URLのレピュテーション調査とブラウザ内のURLを分析します。

従業員がメッセージングまたはコラボレーションのツール内のリンクにアクセスしようとすれば、Proofpoint User ProtectionはURLをリアルタイムで分析します。URLが悪意のあるものであるとわかれば、これをブロックします。このようにしてユーザーは、悪意のあるWebサイトやコンテンツから常に保護されます。

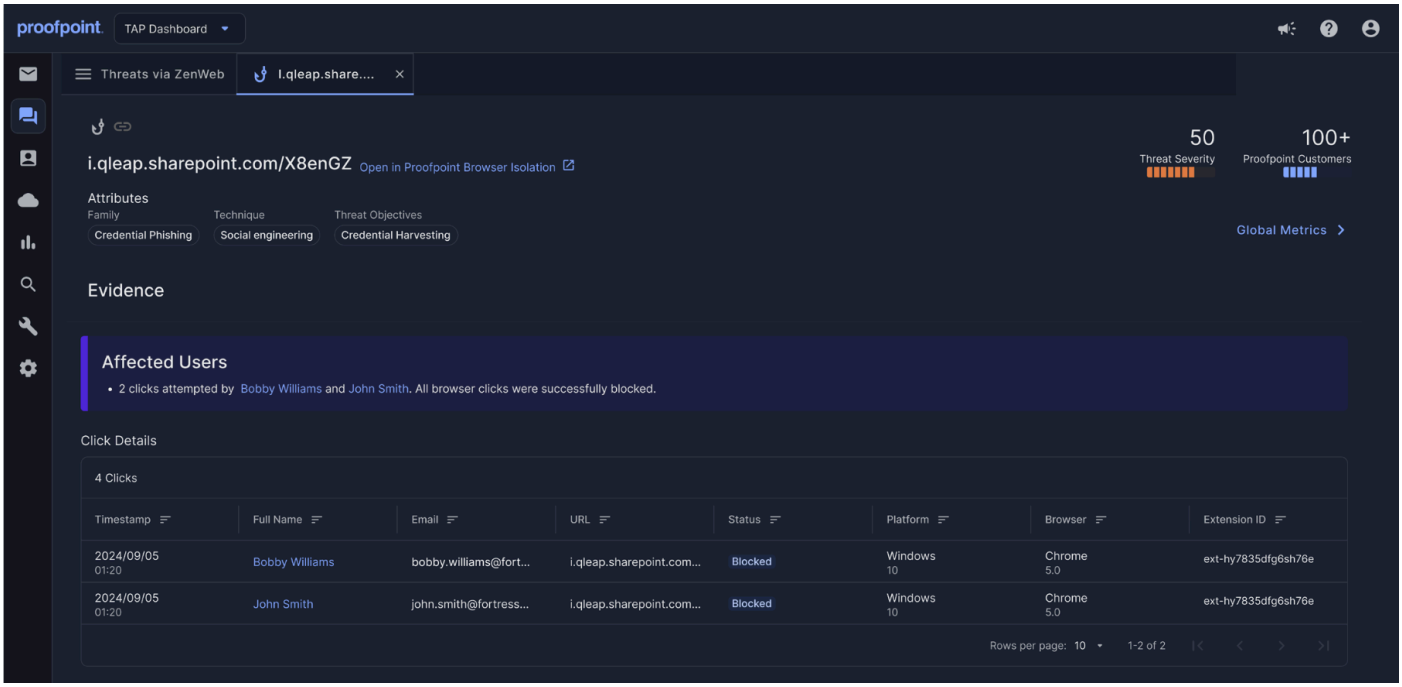

図3：プルーフポイントはメールの枠を超えてフィッシング保護を提供します。メッセージング、コラボレーション、コミュニケーションのプラットフォームにおいて共有された悪意のあるURLもブロックします。

侵害されたアカウントを迅速に検知して対応

従業員のアカウントがMicrosoft 365、Google Workspace、Oktaなどのツールで侵害されても、Proofpoint User Protectionが安心感を与えてくれます。損害が発生する前にインシデントを検知して対応します。Proofpoint User Protectionは、AI、機械学習、行動分析、Nexusの脅威インテリジェンスを用いて、不審なクラウドアカウントのアクティビティを検知します。そして、これらをメールの脅威と関連付けて、より高精度でアカウント乗っ取りを特定し、元に戻します。

他社のソリューションでは、アカウント乗っ取り後のアクティビティに対応する能力が限られています。これに対し、プルーフポイントなら、アカウント乗っ取りの検知後、脅威対応を迅速に行うことができます。攻撃者による変更を特定し、攻撃者のアクセス権を削除します。パスワードのリセット、メールボックスのルールやマルチファクタ認証（MFA）設定への変更の修復、悪意のあるサードパーティ アプリケーションへの接続の遮断を行います。また、攻撃者によってアップロードされたファイルを隔離し、削除します。

Proofpoint User Protectionにより、これらすべての操作を自動化できます。これにより、アカウント乗っ取りの調査や対応にかかる時間を短縮し、組織に危害がもたらされる可能性を最小限に抑えることができます。

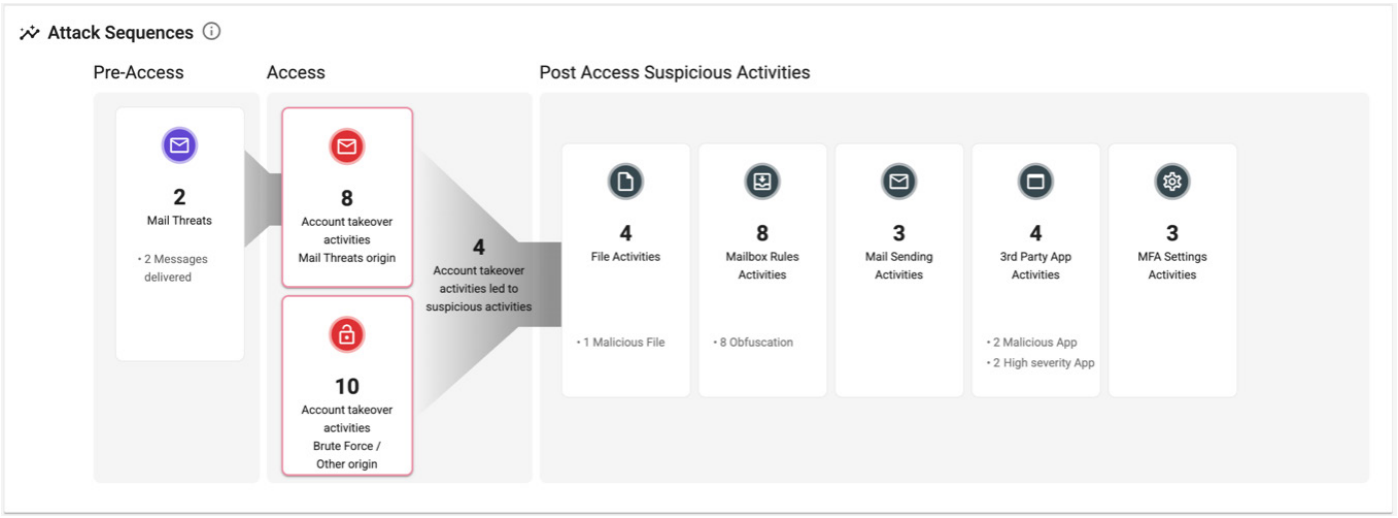

図4：Proofpoint User Protectionは、侵害されたアカウントに関するアクセス前後の悪意のあるアクティビティを表示します。

プルーフポイントの専門知識を活用しセキュリティ プログラムを最適化する

テクノロジーは脅威対策に重要ですが、先進的なアプローチは、人とプロセスにも対応している必要があります。適切なスキルセット、最適なソリューション、強力なセキュリティ文化があれば、組織は進化する脅威状況に適応できます。プルーフポイントのプレミアムサービスとプルーフポイントのソリューションを組み合わせることで、「人」を中心とした、包括的な脅威対策戦略の導入と管理をサポートするエキスパートチームが利用できます。ガイダンスから実践的なシステムのプログラムの管理にいたるまで、プルーフポイントのプレミアムサービスのチームが、セキュリティにおいて真の成果を達成し、価値創出までの時間を短縮できるようサポートします。

proofpoint.

プルーフポイント プラットフォームをご覧ください →