proofpoint

ソリューション概要

Proofpoint Supplier Threat Protection (Proofpoint STP)

侵害されたサプライヤーのアカウントからの脅威を、被害が発生する前に検知・阻止

主なハイライト

- サプライヤーとのコミュニケーションの検出と監視を自動化
- 侵害されたサプライヤーのアカウントからの脅威をプロアクティブに検知して阻止
- アダプティブ コントロールを通じて、ユーザーがより安全な選択を行えるよう導く
- サプライヤーの侵害をさまざまなチャネルにおける攻撃経路にマッピングすることで、リスク対応を迅速化

概要

組織がエージェント型ワークスペースを導入するにつれ、サプライヤーとの関係は、メールにとどまらず、コラボレーションツールなどへと広がりつつあります。この拡大したエコシステムにより、攻撃者が乗っ取られたサードパーティやサプライヤーのアカウントを悪用する新たな機会が生まれています。こうした攻撃において、攻撃者は人の信頼を悪用し、サプライチェーンを悪用した多角的な詐欺を実行したり、認証情報を盗んだり、データを外部へ流出させたりしています。メッセージは正規のアカウントから送信されるため、こうした脅威は多くの場合、ドメインや認証に基づく防御をすり抜けます。

Proofpoint Collaboration Security Prime に含まれる Proofpoint Supplier Threat Protection (Proofpoint STP) は、サプライヤーアカウント侵害の継続的な可視性を提供し、サプライチェーン攻撃から積極的に防御します。Proofpoint Nexus™ AI とプルーフポイントのグローバルな脅威インテリジェンスを基盤として、サプライヤーとの通常のコミュニケーションパターンを学習します。これにより、メッセージが正当な認証済みドメインから送信された場合でも、ユーザーの行動におけるわずかな変化を検知することができます。

セキュリティチームは、さまざまなチャネルや攻撃段階において、サプライヤー侵害を追跡し、最も緊急性の高い脅威を迅速に特定して封じ込めることも可能です。これにより、サプライチェーンにおけるセキュリティ侵害のリスクを低減できるだけでなく、信頼できるパートナーとの関係を維持することにもつながります。

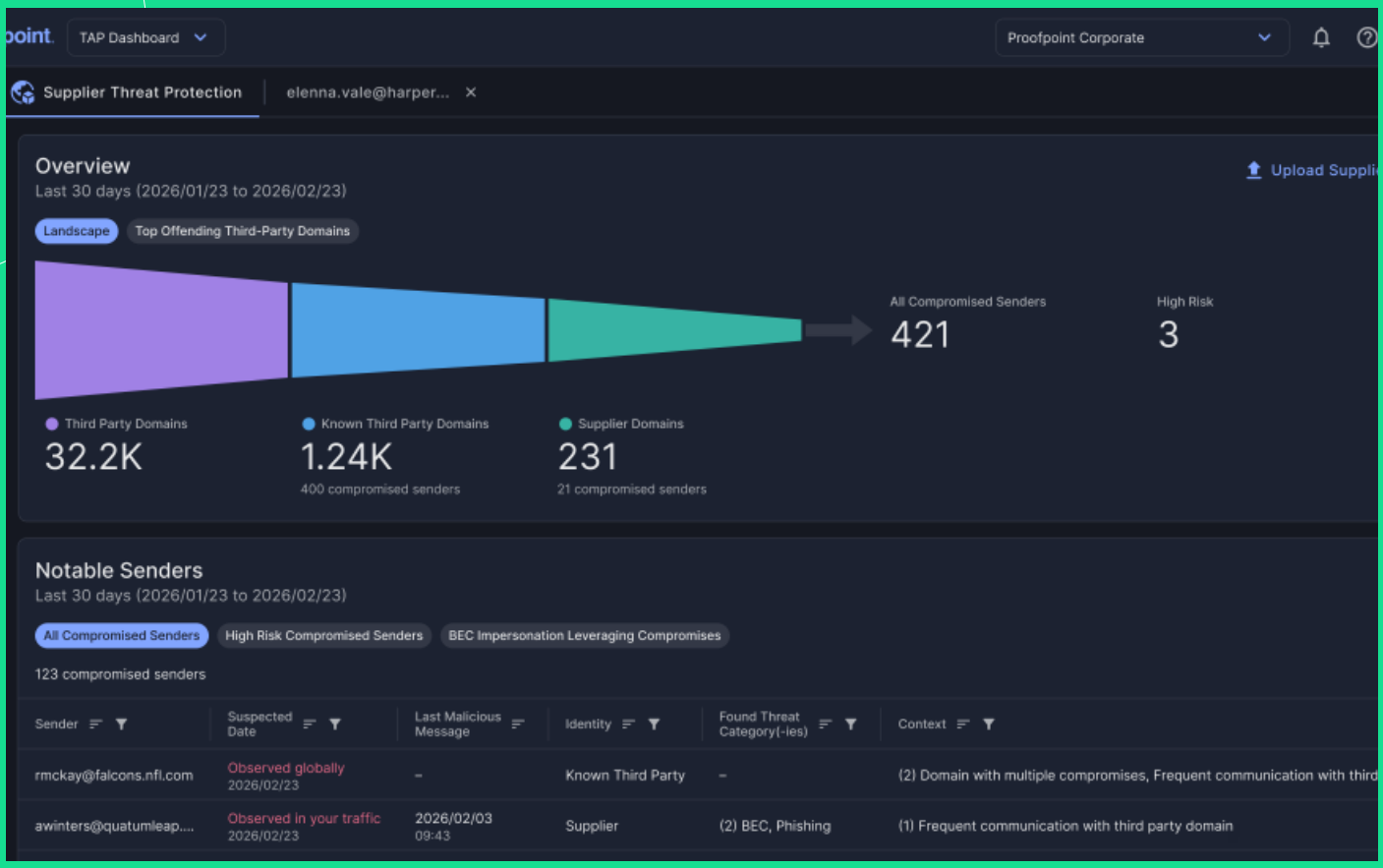

図1:プルーフポイントは、不正アクセスを受けたと思われるサプライヤーのアカウントを検知し、関連するコンテキスト情報およびメッセージ保護を提供します。

サプライヤーを起点とした攻撃に対する包括的な防御

プルーフポイントは、AIを活用した多層的な防御により、サプライヤーを起点とした攻撃から組織を守ります。サプライヤー関連の悪意あるメールは、ユーザーに届く前にブロックされ、検知の正確性は99.999%です。同時に、行動分析型AIは、信頼できるサプライヤーとの関係を監視し、正当で認証済みのドメインからであっても、侵害の兆候を微細なレベルで検知します。つまり、攻撃者は信頼されたアカウントを隠れ蓑にして、防御を突破することはできないということです。

メッセージにリスクがあるものの、明らかに悪意のあるものではない場合、プルーフポイントは警告タグやブラウザ分離といった応適型防御を追加します。これにより、ユーザーは業務に関する正当なメッセージの配信を妨げることなく、より安全な選択を行うことができます。不審なリンクは、クリックされた場合でも自動的に分離またはブロックされます。プルーフポイントは、配信前のブロック機能と、その場でのインテリジェントなユーザー保護機能を組み合わせることで、サプライヤー経由の攻撃ライフサイクル全体において、真の多層防御を実現します。

サプライヤーエコシステムへの詳細な可視性

プルーフポイントは、セキュリティチームに対し、サードパーティのエコシステム全体におけるサプライヤーリスクについて、詳細かつ継続的な可視性を提供します。これにより、問題が発生してから対処するのではなく、サプライチェーンのリスクをプロアクティブに管理することができます。組織とコミュニケーションを取るすべてのサプライヤーのドメインを明確に把握できます。これには、現在取引中のベンダー、新たに確認されたサードパーティ、過去に侵害と関連付けられたドメインが含まれます。これにより、サプライヤーのリスク状況を動的に示すマップが得られます。

プルーフポイントは、悪意のあるメールを検知するだけにとどまりません。サプライヤーが組織とどのように関わっているかを理解するための重要なコンテキストも得られます。請求書などの財務上のやり取り、通常とは異なる受取人、コミュニケーションパターンの変化、不審な内容を確認することができます。

Proofpoint Nexusは、280万以上の顧客から収集された2.1兆件以上のメールを分析し、エコシステム内の任意の場所で発見された侵害済みサプライヤーアカウントを、多くの場合、これらのアカウントが組織を標的にする前に特定します。このレベルの可視性があれば、先進的なエージェント型ワークスペースにおいて、自信を持ってサプライヤーネットワークを拡大することができます。

簡素化された調査により効率を最大化

Proofpoint Supplier Threat Protection は、Proofpoint Collaboration Security Prime 内で、サプライヤーアカウント侵害の検知と対応を一元化します。これにより、セキュリティチームはインシデントの発生件数と調査にかかる時間を削減することができます。サプライヤー関連の悪意あるメールは配信前にブロックされ、リスクの高いメッセージには警告タグが付与され、ブラウザ分離が適用されます。これにより、アナリストによる確認が必要なインシデントの数は減り、手動での確認を必要とする、サプライヤーに起因するイベントも減らすことができます。日常的な優先順位付けの作業が減ることで、セキュリティチームは最も重要なリスクに注力できるようになります。

万が一インシデントが発生した場合でも、調査に必要なすべての情報が1か所にまとめられています。サプライヤーの行動は、関連メール、クラウド、アカウント乗っ取りの兆候と自動的に関連付けられます。チームは、その問題が単独のものか、それともより大規模な多段階攻撃の一部であるかを即座に把握できます。Proofpoint Prime Threat Protection Workbenchは、攻撃がさまざまなチャネルにおいてどのように移動しているかを視覚的にマッピングします。これにより、影響を把握し、対応の優先順位を一目で判断しやすくなります。セキュリティチームは、1つのコンソールから、コミュニケーションの詳細な履歴や行動のコンテキストを確認できるほか、必要な措置を講じることができます。その結果、複数のツールを切り替える必要がなくなります。これにより、迅速に封じ込めを行うことができます。また、影響を受けたサプライヤーと明確な証拠を共有でき、是正措置の調整、再発防止、ビジネス関係の強化が可能になります。

詳細はこちら

proofpoint.