Proofpoint EFD vs Stand Alone DMARC

EFDがDMARC専用ソリューションより優れている理由

製品

- Proofpoint EFD (Email Fraud Defense)
- Proofpoint TAP (Targeted Attack Protection)
- Proofpoint Email Protection
- Proofpoint Domain Discover
- Proofpoint SER (Secure Email Relay)

主なメリット

- 脅威状況に対する広く深い知見を得られる
- 機械学習アルゴリズムの活用によりインテリジェントな識別分類を行う
- 他の Proofpoint 製品やサービスとの強力な統合により、セキュリティへのプラットフォームベースでのアプローチを実現する

不審なソーシャルインタラクションの 96% はメールによるものであり[1]、企業はこれまで以上にメールユーザーを保護する必要があります。ここ何年もの間に、Sender Policy Framework (SPF)、DomainKeys Identified Mail (DKIM)、Domain-based Message Authentication, Reporting, and Conformance (DMARC) などのメール認証の標準が、メールでのスプーフィングや詐欺による攻撃からの防御を目的として登場してきました。

DMARC は、SPF と DKIM の能力を組み合わせたものです。これは、ビジネスメール詐欺 (BEC)、フィッシング、スプーフィングなどの攻撃を減らすのに非常に効果的であることが実証されてきました。しかしDMARCの問題点として、他のSPFとDKIMの 2 つの標準をベースにしているため、理解するのに時間がかかることがあります。また、DMARC 戦略の導入は複雑になりがちです。さらに、DMARC のレポートはたいてい解析が困難です。

DMARC 戦略のセットアップと管理を支援する数多くのソリューションが登場しています。それら多くのソリューションと同様、Proofpoint EFD (Email Fraud Defense) は、DMARC の実装を効率的に展開するのに役立ちます。しかし、Proofpoint EFD が実現するのはそれよりはるかに多くの事柄です。脅威状況についての比類のない知見を提示します。また、機械学習を活用し、インテリジェントかつ徹底的にユーザーを保護します。さらに、セキュリティへのプラットフォームベースでのアプローチにより、他の Proofpoint ソリューションとシームレスに統合し、包括的で柔軟な保護を実現します。

1 Verizon「Data Breach Investigations Report (データ侵害調査レポート)」2020 年

包括的な脅威インサイト

Proofpoint EFD により、脅威状況について広く深い知見を得ることができます。120 以上の消費者向けメッセージングプロバイダーから、テレメトリーデータと DMARC フォレンジックデータを収集しています。Proofpoint EFD はこの豊富なデータを使って、ブランドやドメインのなりすましの脅威について詳細に示すことができます。

機械学習による防衛

Proofpoint EFD は、機械学習アルゴリズムを採用しています。これらは、Proofpoint メールゲートウェイを介したインバウンドの請求(インボイス)詐欺検知機能により、サプライヤーを特定してスコアリングできます。これにより、依存関係にあるサードパーティを簡単に追跡できます。また、サプライヤーに関連している可能性がある、標的とされている脅威をスクリーニングします。

サプライヤーのリスクからの保護

Proofpoint EFD には、Nexus Supplier Risk Explorer が含まれています。このツールは、サプライヤーと、サプライヤーがユーザーへの送信に使用しているドメインを自動的に識別します。そして、各サプライヤーのリスクをダッシュボードビューに提示し、優先順位を付け、DMARC レコードを検証します。

ドメイン悪用についての知見の取得

Proofpoint EFD の標準機能である Proofpoint Domain Discover は、ブランドを装ったドメインを検出する機能です。これらのドメインは多くの場合、従業員、顧客、パートナーを標的にしています。Proofpoint Domain Discover は、機械学習と人工知能を用いて膨大なドメインデータを分析し、ドメイン詐欺や侵害ドメインを発見します。

緊密なエコシステムと統合

Proofpoint EFD は、フォーチュン 1000 に取り上げられている中で最も広く展開されているソリューションです。プラットフォームベースのアプローチにより、サービスの多くはシームレスに活用できます。また、Proofpoint の検知システムと Proofpoint EFD の DMARC レポートとの間の緊密なエコシステムの統合を活かすこともできます。

Proofpoint EFD の統合には、次の機能が組み込まれています。

- **Proofpoint TAP (Targeted Attack Protection):** Proofpoint TAP は、8,000 社以上の Proofpoint 顧客のメールゲートウェイで監視されている脅威メトリックを提供します。このため、EFD レポートには、実世界における企業の脅威検知データが表示されます。多くの業種や地域にわたってこれほど幅広く脅威の可視性を提供しているソリューションは他にありません。Proofpoint EFD から、Proofpoint TAP ダッシュボード内に表示されるスピーフィング攻撃情報へリンクさせることができます。
- **Proofpoint Email Protection:** Proofpoint EFD は、Proofpoint Email Protection における悪意のあるドメインベースのブロッキング情報への連携をサポートしています。
- **Proofpoint Virtual Takedown:** Proofpoint Domain Discover から収集した情報を使用して、悪意のあるドメインや犯罪者のドメインを提出することで、Virtual Takedown を開始できます。これらのドメインには、フィッシングや、犯罪活動に関係する悪意のあるコンテンツの配送などに関与しているものが含まれている可能性があります。また、ISP、デバイス、Web サービス、セキュリティ製品など幅広い分野で利用されているブロックリストに記載されているドメインも含まれている可能性があります。
- **Proofpoint Secure Email Relay (SER):** Proofpoint SER は、不正アクセスされたサードパーティの送信者（購入確認メールの配信サービスなど）がユーザーのドメインを使用して悪意のあるメールを送信するのを防ぎます。認証情報アクセスを認められた送信者のみにこのサービスの利用を許可することで、脅威リスクを低減します。

詳細はこちら

詳細は proofpoint.com/jp でご確認ください。