Proofpoint EFD (Email Fraud Defense)

主なメリット

- 導入プロセスをガイドすることにより DMARC の実装を容易に
- 誤って正規のメールをブロックすることなく、メール詐欺攻撃から組織のブランドを保護
- サプライヤーと、サプライヤーがもたらすリスクを自動的に識別
- 信頼できるドメインから送られたメールと類似ドメインを可視化
- 業界をリードするプルーフポイントのゲートウェイと統合することにより、DMARC を確実かつ柔軟に運用

Proofpoint Email Fraud Defense（以下、Proofpoint EFD）は、ガイド付きワークフローで DMARC の効率的な実装を可能にし、また専任コンサルタントのサポートを提供します。あなたの組織になりすまして顧客や取引先企業を狙うメール詐欺攻撃を阻止して、あなたの組織のブランドを守ります。また、あなたの組織のドメインを使って送信されるメールや類似の偽ドメインを完全に可視化できます。また、サプライヤーを自動で識別してサプライヤーがもたらすリスクを緩和し、また第三者が登録したサプライヤーの類似ドメインも自動で識別します。

Proofpoint EFD は、DMARC プロセス全体においてガイドします。また、顧客、ビジネスパートナー、従業員をビジネスメール詐欺 (BEC) から守ります。メール詐欺攻撃からブランドを保護し、インバウンドの詐欺リスクを軽減します。また、組織間で送受信されるすべてのメールを認証します。正規のメールをブロックしてしまうことはありません。

使いやすさ

専任コンサルタントとガイド付きのワークフロー

コンサルタントがプロジェクトを作成し、ガイド付きワークフローも提供されます。プルーフポイントのプランにより、メール認証を完全に効率的に導入できます。プルーフポイントのコンサルタントがお客様の導入プロセスをサポートします。委託先のサードパーティを含むすべての正当な送信者が適切に認証されるように、送信者の識別をサポートします。コンサルタントはメール環境を分析して、多くのメールを送る送信者やメールボリュームなどといったクライテリアと個別ニーズに基づいてタスクを優先順位付けします。

ホスト型認証サービス

Proofpoint EFD には SPF ホスティングと DKIM ホスティングが含まれます。これらは、セキュリティを向上させながら簡素化された構成と管理を提供します。

SPF ホスティング

- 従来の DNS ルックアップの上限 (10) を解消
- SPF レコード更新のオーバーヘッドを削減
- レコードをリアルタイムに更新
- 過剰な許可レコードの防止により SPF セキュリティを向上

DKIM ホスティング

- DKIM セレクタとキーの構成や管理をシンプルに
- 柔軟な DKIM セレクタ ホスティング オプションの提供（委託または非委託）
- DNSSEC のサポート
- 地理的に分散したフォールト トレラントなサービスを作成
- DKIM セレクタと公開キーを簡単にインポート

包括的なブランド プロテクション

Proofpoint EFD は信頼されたドメインを悪用して詐欺メールを送信できないよう阻止します。そして、あなたの組織になりすますメール詐欺攻撃からブランドと評判を守ります。

類似ドメインを特定

Proofpoint EFD は Proofpoint Domain Discover の情報を活用します。自動的に類似ドメインを特定します。メール攻撃やフィッシング サイトで、ブランドを偽装した新規登録ドメインを動的に検知します。プルーフポイントでは何百万ものドメインを分析し、ドメインの登録データを（メールアクティビティとアクティブな攻撃に関する）プルーフポイント独自のデータに関連付けて、不審なドメインの全貌を明らかにします。どのようにブランドになりすましているかという情報も提供します。また、不審なドメインが活動を始めて武器化した場合、ただちにアラートを送ります。

Proofpoint Virtual Takedown アドオンを使用すると、消費者、ビジネスパートナー、従業員が、悪意のある類似ドメインを使った攻撃にさらされないように対処でき、そしてレジストラやホスティング プロバイダーを介してドメインを削除するよう働きかけることができます。またプルーフポイントのメールゲートウェイでブロックできるよう、ドメイン情報をエクスポートすることも可能です。

メールエコシステムに対する 360 度の可視性

Proofpoint EFD は、あなたの組織のドメインを使用して送信されたメール（コンシューマーの受信箱、ビジネス ゲートウェイ、組織のゲートウェイに送られたメール等）を可視化します。

包括的ダッシュボードでは、以下の情報を提供します。

- 攻撃者がどのドメインをハイジャックしようとしたか
- 各ドメインの不正使用率
- DMARC、SPF、DKIM の通過率とポリシー
- 認定送信者とその DMARC レコード

Proofpoint EFD は実用的な知見や推奨案を提供します。対処が必要なタスクを追跡し、管理するため、アクションの実行漏れを防げます。Proofpoint EFD では DMARC の失敗や正規メールがブロックされてしまうことを心配する必要がなく、またドメインのスプーフィング（なりすまし）も阻止できます。

サプライヤーリスクの可視化

Proofpoint EFD は DMARC の実装だけでなく、サプライヤーリスクの可視化も可能にします。Nexus Supplier Risk Explorer 機能はサプライヤーを自動的に識別し、その DMARC レコードを検証し、サプライヤーがもたらすリスク（なりすまし、フィッシング、マルウェア、スパムなど）を明らかにします。またメール数と、サプライヤーの類似ドメインから送られたメールについても明らかにするため、潜在的な脅威をさらに詳しく調査することもできます。また各サプライヤーのドメインのリスクを優先順位付けすることにより、最もリスクの高いインシデントに集中できるようになります。

プルーフポイントのメールゲートウェイとの統合

メール認証とセキュア メール ゲートウェイの完全な統合を提供します。業界をリードするプルーフポイントのメールゲートウェイと Proofpoint EFD を組み合わせることで、DMARC をインバウンド トラフィックに適用し、詐欺攻撃のリスクを低減できます。特定ドメインの DMARC レピュテーションを確認するため、正規メールが何かの理由で DMARC 認証に失敗してしまった場合でもゲートウェイでブロックされることはありません。また正規メールについて、セキュリティ体制に影響を与えることなくオーバーライドポリシーを作成することも可能です。

詳細

詳細は **proofpoint.com/jp** でご確認ください。