proofpoint.

ソリューション概要

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
- 正規のメールをブロックすることなく、組織のブランドがメール詐欺攻撃に悪用されるのを防止
- サプライヤー（取引先）に関するサイバーリスクを自動的に識別
- 信頼できるドメインを使用して送られたメールと類似ドメインから送られたメールをすべて表示
- プルーフポイントがホストする認証サービスにより、信頼性の高いSPF、DKIM、およびDMARCのレコードのホスティングを確保
- 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統合することにより、DMARCを確実かつ柔軟に運用
- Microsoft 365で管理されている企業所有のドメインについて、DMARC合格率を表示

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するとともに経験豊富なコンサルタントによるサポートを提供します。プルーフポイントの製品は、組織の評判をメール詐欺から守ります。組織ドメインを使用して送られたメールと類似ドメインから送られたメールの送信元を表示します。また、サプライヤーや、第三者が登録したサプライヤーの類似ドメインを識別することで、サプライヤー（取引先）に関するサイバーリスクを低減します。

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。Proofpoint EFDにより、メール詐欺攻撃においてブランドが使用されるのを防ぎ、インバウンドの詐欺リスクを低減します。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専門的ガイダンス

プルーフポイントでは、メール認証のセットアップをサポートするために、組織に合わせたプロジェクトプランを作成します。このプランにガイド付きワークフローが組み込まれており、セットアッププロセスを効率化します。プルーフポイントのコンサルタントがプランのあらゆる段階においてサポートします。送信者の識別を見直し、サードパーティやシャドーIT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個別ニーズに基づいてタスクを優先順位付けします。

このソリューションは、人に起因する4つの主要リスクを低減する、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。

ホスト型認証サービス

Proofpoint EFDには、プルーフポイントがホストする、SPF、DKIM、DMARCのサービスが含まれます。これらのホスティングサービスにより、Sender Policy Framework（SPF）、DomainKeys Identified Mail (DKIM)、そしてDomain-based Message Authentication, Reporting, and Conformance(DMARC)のポリシーをセットアップして管理することができます。これらはまた、地理的に分散したフォールト トレラントなサービスであり、信頼性を確保しています。

SPFホスティング

- SPFにおける従来のDNSルックアップの上限（10）を解消
- SPFレコード更新の作業を削減
- 適切な構文検証と共にレコードをリアルタイムで更新
- 送信インフラの難読化によりSPFセキュリティを向上
- 同じ送信インフラを使用する複数のドメインを容易に一括管理

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）
- DNS Security Extensions (DNSSEC)のサポート
- DKIMセレクタと公開キーを簡単にインポート

DMARCホスティング

- 組織ドメインのDMARCレコードの構成や管理を簡素化
- DNSSECのサポート
- 既存のDMARCレコード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、ブランドを保護します。

類似ドメインを特定

Proofpoint EFDは、Proofpoint Domain Discoverのドメイン登録情報を使用します。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ドメインを検知します。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、不審なドメインや、攻撃者が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、不審なドメインがアクティブになればアラートを提供します。

Proofpoint Takedownアドオンは、類似ドメインに、コンシューマー、パートナー、従業員が遭遇するリスクを低減します。レジストラやホスティング、コンテンツ デリバリ ネットワーク（CDN）、メールのプロバイダーを介して悪意のある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、組織の信頼できる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）を表示します。

プルーフポイントのダッシュボードは、攻撃者がどのドメインをハイジャックしようとしたかや、各ドメインの不正使用率を表示します。認証された送信者やDMARCレコードのほか、SPF、DKIM、DMARCのポリシーと合格率を表示します。

Proofpoint EFDは実用的な知見や推奨案を提供します。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、攻撃者も阻止できます。

サプライヤーリスクの可視化

Proofpoint EFDはDMARCのセットアップだけでなく、プルーフポイントのメールゲートウェイと連系することにより、サプライヤーリスクも表示します。Nexus Supplier Risk Explorerはサプライヤーを識別し、そのDMARCレコードを確認し、サプライヤーリスクを表示します。プルーフポイントの製品は、類似ドメインから送信されたメッセージを表示します。リスクレベルに基づいてアラート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

Proofpoint EFDは、プルーフポイントのメールゲートウェイと統合し、インバウンドトラフィックにおいてDMARCを適用します。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。

Microsoft 365のDMARC可視化

Microsoftのインバウンド サーバーに誘導されるMX (Mail Exchange)レコードを利用してMicrosoft 365を使用している場合でも、Proofpoint EFDは、組織ドメインのDMARCコンプライアンスを表示できます。このような可視性により、組織ドメインからのインバウンド トラフィックに対し、確実にDMARCを適用できます。

proofpoint.

プルーフポイント プラットフォームをご覧ください →