Proofpoint SER (Secure Email Relay)

アプリケーションや SaaS パートナーからのトランザクションメールを制御し、保護するための優れたソリューション

主なメリット

- 社内アプリケーションだけでなく、Salesforce、ServiceNow、Workday などの SaaS プロバイダーからのトランザクションメールも保護
- 送信前にすべての送信元からのメールの DKIM 署名を有効にすることで、DMARC の実装を促進
- 組織の SPF レコードに IP アドレスを登録している場合、不正アクセスされたサードパーティアプリや脆弱なメール サービスプロバイダーから信頼できるドメインを用いたメールが送信されないよう保護
- ペイロードの暗号化や情報漏えい対策 (DLP) により、個人識別情報 (PII) や個人健康情報 (PHI) など、アプリケーションメール内の機密データを保護
- オンプレミスのメールリレーを、安全なクラウドベースの代替ソリューションに置換え
- ユーザーメールをアプリケーションメールから分離することにより、ユーザーメールへの影響を防止

Proofpoint SER (Secure Email Relay) は、トランザクションメールを統合し、保護するソリューションです。不正アクセスされたサードパーティのアプリなどから組織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、DKIM 署名を有効にして DMARC コンプライアンスを満たすことを可能にします。Proofpoint SER は、ホストされたソリューションとして、クラウド移行の取り組みを実現できるよう支援します。

多くのアプリケーションは、オンプレミスのシステムからクラウドに移行しつつあります。しかしクラウド移行により、組織の攻撃対象領域が拡大しています。攻撃者は、クラウドのサードパーティアプリを使用して当該組織に「なりすまして」悪意のあるメールを送信するおそれがあり、送信者の詐称がおこなえないよう適切に制御しなければなりません。攻撃者が送信者のクラウド環境を悪用して、悪性メールを送信した場合、SPF/DKIM/DMARC をパスし、顧客、パートナー、従業員に直接送信される可能性があり、攻撃者が企業の情報を容易に盗むことができてしまいます。

Proofpoint SER は、個人情報を利用する、トランザクション目的のアプリケーションメールに対して、セキュリティ / コンプライアンス対策をおこないます。トランザクションメールは、社内アプリや Salesforce、ServiceNow、Workday といったサードパーティの SaaS パートナーから発信されます。メールには、請求書、認証コード、確認通知などが含まれます。Proofpoint SERを用いれば、ユーザーが作成したメールと同じレベルの保護をアプリから送信されたトランザクションメールにも提供します。

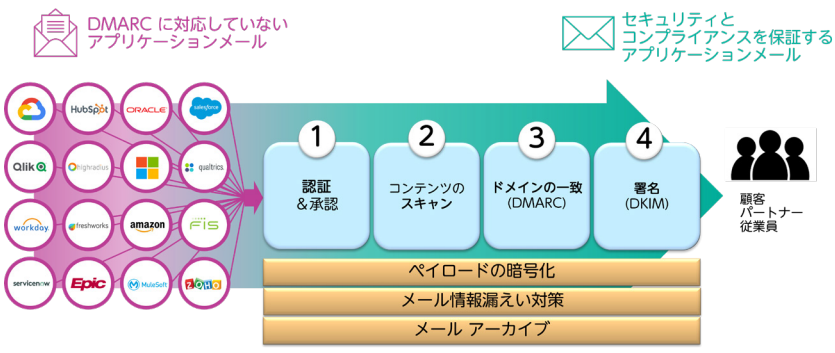

図 1: Proofpoint SER は、組織に代わってトランザクションメールを送信するクラウドアプリを保護し暗号化や情報漏えい対策 (DLP) などのセキュリティコントロールをアプリケーションメールに適用

トランザクションメールの例として、以下のようなものが含まれます。

- 報告・通知
- パッケージ配送通知
- 注文確認
- 電子レシート
- 保険の見積
- 満足度やフィードバックのリクエスト
- タスク通知
- IoT またはデバイスのアラーム通知
- アラート/危機管理

Proofpoint SER では、すべてのメールに DKIM 署名を使用することにより、DMARC 導入がより簡単になります。アンチスパム/アンチウイルス技術を利用して、メールを評価します。また、ペイロード暗号化やメール情報漏えい対策 (DLP) が利用できるため、機密データに関するリスクの低減につながります。Proofpoint SER により、メールアドレスを制御することができます。したがって、顧客、パートナー、従業員は、間違いなく当該組織からのメールのみを受信できるようになります。

脆弱な環境からメールを保護

アプリケーションメールやメール サービスのプロバイダーは、組織のドメインを使用したメールの送信が許可される可能性がありますが、セキュリティのベストプラクティスを遵守していない場合が多く、これが、アカウント侵害やプラットフォームの悪用につながるおそれもあります。どちらの場合でも、犯罪者は組織の信頼できる正規のドメインを使用し、メール認証をパスすることで、悪意のあるメールを送信する可能性があります。

Proofpoint SER では、検証済みの企業のみにメールリレーサービスの利用を許可するクローズドシステムが採用されています。任意のユーザーは、プルーフポイントのプラットフォーム上でフリーのアカウントを登録することはできません。これにより、脆弱なまたは不正アクセスされたメール サービスプロバイダーがもたらすリスクを大幅に低減できます。

また、SMTP 認証や TLS (STARTTLS) を使用して、承認済みのアプリケーションからメールを安全に受け取ることもできます。各メッセージには、プルーフポイントのアンチスパム/アンチウイルス対策が講じられます。本人になりすまして悪意のあるメールを送信しようとし、通信自体は認証を受けている場合であっても、Proofpoint SER は見逃さずにこれをブロックします。信頼できる IP の背後にあるアプリケーションメールを一元管理することもできます。これにより、組織に代わってメールを送信するアプリケーション送信者を犯罪者から分かりにくくすることができます。

DMARC 導入を促進

一部のアプリケーションまたは SaaS プロバイダーは、DKIM 署名に対応していません。SPF のみをベースとした DMARC 認証をクリアすることができますが、DKIM 認証がなければ、正規のメールに必要な認証の冗長性を欠くことになります。これにより、たとえばメールの転送が極めて困難になります。Proofpoint SER は、送信前にメッセージに DKIM 署名を行うことで、これらのトランザクションメールを DMARC コンプライアンスに完全に適合させることができます。これにより、組織のドメインに関する DMARC の Reject (受信拒否) ポリシーを迅速に適用できるため、犯罪者はもはやなりすましをおこなうことはできなくなります。

アプリケーションメールに関する規制コンプライアンスの遵守

アプリケーションはクラウドに移行しつつあります。移行するにつれ、各組織には、規制コンプライアンスの観点から、理想的とは言えないメールの選択肢しか残されていません。オンプレミスのシステムでアプリケーションメールを転送している組織もありますが、脆弱な外部環境にさらされることになります。また、クラウドベースのポイント ソリューションで何とか対応している組織もありますが、このようなソリューションは、アクティビティを一括表示できないことが多々あります。

Proofpoint SER では、アプリケーションメールに関する規制コンプライアンスの基準を満たすことができます。個人識別情報 (PII) や個人健康情報 (PHI) にアクセスできるアプリケーションからのメールでは、通信やペイロードを暗号化することができます。また Proofpoint SER では、アプリケーションメールに情報漏えい対策 (DLP) やアーカイブ ソリューションを使用することができるので、SEC (米国証券取引委員会) や FINRA (米国金融業規制機構) の規制にも対応しています。

詳細

詳細は proofpoint.com/jp でご確認ください。