Proofpoint Email DLP および Proofpoint Email Encryption

ユーザーを騙してメールで機密情報を送らせようとする攻撃への対策

主なメリット

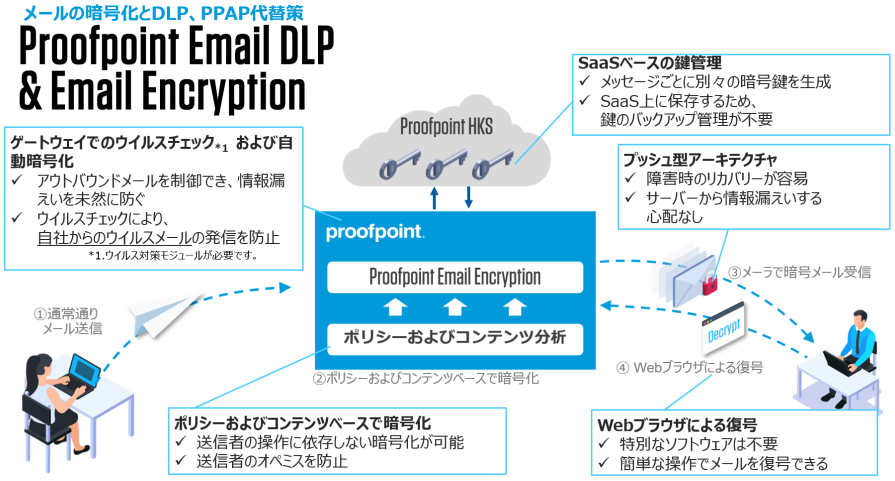
- 業界No.1のメールゲートウェイでメールDLPと暗号化を一元管理
- インフォメーション クラウド セキュリティプラットフォームと統合し、人に起因するあらゆるデータ損失に対応
- 構造化データおよび非構造化データ内の機密情報を分析し分類
- シームレスなユーザー エクスペリエンスとモバイル エクスペリエンスを提供

コンプライアンス

- 240を超える組み込みの分類子
- PCI、SOX、GLBA、SECインサイダー取引規制、およびその他の各国特有のテンプレートを用意
- GDPR、UK-DPA、EU-DPD、PIPEDA（カナダ）、英国国民保険番号、クレジットカード番号、マイナンバー（法人、個人）に対応
- PII、HIPAA、ICD-9、ICD-10、全米医薬品コード、その他の医療関連コードも対応

Proofpoint Email DLP（Data Loss Prevention）およびProofpoint Email Encryptionを使用すると、複数のソリューションを使用する煩雑さやコストに悩まされることなく、リスクを可視化し、対策を実行することができます。データは自動的に分類され、透過的暗号化が行われます。これらはすべてゲートウェイで一元管理されます。これにより、メール環境でのポリシーの定義や実行といった管理業務が改善されます。

Proofpoint Email DLPとProofpoint Email Encryptionを使用すると、機密データに対してきめ細かい制御を行うことができます。コンプライアンス対策を強化し、ユーザーを騙してメールで機密データを送信させようとする攻撃を阻止できます。メールは攻撃者が攻撃を仕掛ける際に一番よく利用する侵入ルートです。また、外部へのデータ漏えいのルートでもあります。



Proofpoint Email DLP — 潜在的なデータ侵害の阻止

Proofpoint Email DLPは、どれが機密データかを正確に分類し、データ漏えいの可能性がある送信メールを検知することで、外部への機密データの流出を防ぎます。

Exact Data Match (EDM: 正確なデータ照合)

Proofpoint Email DLP は、Exact Data Match (EDM: 正確なデータ照合)機能を提供します。この機能は、保護が必要な機密データを検出します。また、独自のカスタム ディクショナリや識別子を簡単にアップロードまたは作成できます。これにより、金融サービスの口座番号、現地形式の ID、医療記録番号などを基にして、組織にとって重要となるメールデータを分析できます。また、既存のディクショナリに組織固有の用語とコードを追加することもできます。ルートに基づく定義を用いて、受信および送信メール用のポリシーを作成できます。

メール詐欺対策

Proofpoint Email DLPには、きめ細かく調整された240以上の分類子が用意されています。これらの分類子により、ビジネスメール詐欺（BEC）攻撃でよく使用されるメッセージを自動的に発見、分類、ブロックします。これにより、ユーザーが騙されて従業員記録やW2（源泉徴収票）を送信したり、電信送金を行ってしまうなどのリスクを大幅に低減できます。

詳細分析とフィンガープリンティング

Proofpoint Email DLPは、構造化されていないコンテンツに含まれる機密データを正確に検知します。Proofpoint Email DLPでは以下が可能になります。

- 追加設定なしで、300以上のファイルタイプをスキャン可能
- 標準のOffice/PDF添付ファイル以外の形式の機密データも適切に処理
- ファイルタイプ プロファイラーを使用して、新規、カスタムまたは専用ファイルタイプにも対応。特許や覚書が含まれているファイルタイプにも対応できます
- 完全マッチングと部分マッチングで機密文書をフィンガープリンティング。データが異なるファイル形式で保存されている場合でもフィンガープリンティングが可能です

規制コンプライアンス対応の自動化

Proofpoint Email DLPは、シンプルなEDMよりも高度な機能を提供します。事前に作成されたディクショナリを使用して、機密データの漏えいを迅速に発見できます。Proofpoint Email DLPは次の機能を提供します。

- コンプライアンスに違反している通信を確実に検知
- スマート識別子による詳細アルゴリズム チェック
- クレジットカード番号、ID 番号、その他様々な機密情報の誤検知を最小化
- 高度な近接分析と相関分析で複数の要素の検知精度を向上

ディクショナリの用語に加重して用語のマッチング率を調整したり、例外を許可することもできます。

運用効率の改善

インフォメーション クラウド セキュリティ プラットフォームとの統合

Proofpoint Email DLPは、プルーフポイントのインフォメーション クラウド セキュリティ プラットフォームと統合されています。これにより、市場をリードするメール、クラウド、Web、エンドポイント向けのソリューションや、オンプレミスのファイル リポジトリの連携が可能になります。プルーフポイントのプラットフォームはこれらの各チャネルのコンテンツ、行動、脅威テレメトリーの情報を統合し、統合アラート管理インターフェースを介して、人に起因するデータ損失にあらゆる側面から包括的に対応します。共通のデータ分類子を使用することで、チャンネル全体に一環したDLPポリシーを展開できます。これにより、時間が節約でき、管理の手間も省くことができます。

Smart Send

Smart Send機能を使用すれば、メール送信者がアウトバウンドポリシーに違反した場合、自分で違反を修正できます。これはパワフルかつ管理が簡単なツールで、IT部門の負担を軽減し、より戦略的な仕事に取り組むことが可能になります。また、ユーザーの教育にも役立ちます。このツールでは、ポリシーごとにルーティングを定義できます。機密資産をユーザー自身、人事部門、IT部門などにリルートすることもできます。

Proofpointリアルタイムレポート

Proofpoint Email DLPは、迅速な意思決定とアクションができるよう、可視性とワークフローを提供します。これにより、傾向や統計をリアルタイムに確認してインシデントを管理し、違反メールに適切な処置を行えるようになります。これらの作業は1つのダッシュボードから実行できます。インシデントはドリルダウンしてレビューできます。メールや添付ファイルの領域がハイライト表示され、これらに一致する内容がトレーニング文書やポリシーの横に表示されます。インシデントマネージャーでは違反についてコメント、追跡、検索が可能で、一致するメールはエクスポートできます。

グラフィカルレポートでは違反が経時的に表示されます。ポリシー別、ユーザー別に違反を表示し、またポリシーごとに頻繁に違反するトップユーザーを表示できます。傾向を確認することで、効果が出ている領域や改善機会のある領域を特定できます。レポートはスケジュールに基づいてメール送信するか、イントラネットサイトに公開して管理者の時間を節約できます。

Proofpoint Email Encryption - 確実な暗号化、可視化、制御

Proofpoint Email Encryption はポリシーベースのDLPエンジンを使用しています。この制御機能により、以下が可能になります。

- 暗号化ポリシーを定義
- LDAPまたはADに統合し、グローバル、グループ、ユーザーレベルで動的にポリシーを適用
- 宛先に基づいて暗号化を定義。たとえば、ビジネスパートナー、サプライヤー、送信者、添付ファイルタイプなどのメッセージ属性を追加できます

Proofpoint Email EncryptionはTLSフォールバックとしても機能し、フェイルセーフの暗号化を実現できます。

Proofpoint Email Encryptionにより、以下が可能になります。

- 中断のない、安全なビジネス コミュニケーション
- グループ間やユーザー間の通信を保護。社内の暗号化機能を提供します。メールを外部にルーティングしたり、労力をかけて他のソリューションを導入する必要がなくなります。
- 暗号化メールの取り消しを細かく設定可能。ユーザーは受信者の暗号化メールアクセス権限を取り消し、終了、復元できます。これにより他のユーザーや、この受信者が受け取った他のメールへ影響することはありません

鍵管理作業が不要

鍵管理のための作業が不要になるため、管理者は暗号化の対応に集中できるようになります。生成された鍵は安全に保存され管理され、クラウドベースのインフラストラクチャからいつでも利用可能です。鍵はメールコンテンツとは別に保存されるので、プライバシーとセキュリティを確保できます。

メール受信における ユーザーエクスペリエンスの向上

シームレスなユーザーエクスペリエンスを提供することで、Proofpoint Email Encryptionは、従業員がポリシーを回避することを防ぐことができます。プルーフポイントのソリューションを用いれば、複数の方法で暗号化メールにアクセスできます。デフォルトはSecure Readerです。ユーザーがメッセージに含まれているHTML形式の暗号化ファイルをクリックするとWebポータルに誘導され、そこから暗号化されたメッセージに簡単にアクセスできます。他にもDecrypt Assistという方法があります。これはモバイル向けの方法で、メッセージにはリンクが埋め込まれています。このリンクをクリックすると、モバイル用に最適化されたWebポータルに移動し、そこから暗号化されたメッセージにアクセスできます。
暗号化メールへのアクセスや管理は、Secure Readerの受信ボックスから実行できます。これにより、暗号化メール処理でシームレスなユーザーエクスペリエンスを提供できます。また、組織によるメール管理も簡単になります。Outlookアドイン機能を用いると、ユーザーはボタンをクリックするだけで暗号化メールを簡単に送受信できます。また社内メールの暗号化も可能なので、従業員間の機密性の高いやりとりも保護できるようになります。

詳細はこちら

詳細は**proofpoint.com/jp**でご確認ください。