Proofpoint Adaptive Email DLPでMS Purviewを補完する

Microsoft PurviewとProofpoint Adaptive Email DLPを組み合わせて、メールによる情報漏えいに対する強力かつスマートな防御を実現

主なメリット

- メールによる偶発的および意図的な情報漏えいを防止
- 市場における評判の喪失や顧客離れのリスクを低減
- GDPR（EU一般データ保護規則）やCCPA（カリフォルニア州消費者プライバシー法）の侵害による罰金を抑制
- 組織におけるセキュリティ意識を向上させる

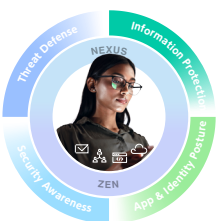
Microsoft Purview と Proofpoint Adaptive Email DLP は、どちらもメール上の情報漏えい対策（DLP）をサポートするものです。しかし、これらの製品のアプローチはそれぞれ異なり、低減できるリスクも異なります。そのため、Proofpoint Adaptive Email DLPのインテリジェンスを活用し、Purviewの足りない部分を補完すれば、メールにおいて最も包括的かつ堅牢な情報漏えい対策を構築することができます。

PurviewとProofpoint Adaptive Email DLPの違い

Purviewは、多くのセキュアメールゲートウェイが提供する機能である、ポリシーベースのアプローチを採用しています。コミュニケーションの暗号化や、データのガバナンスと維持にも対応しています。しかし、Purviewは、管理者の管理によるルールによって機能するため、実装するには時間がかかり、エラーが発生しやすく、維持も簡単ではなく、すべてのリスクを阻止するには不十分です。Purviewはまた、ユーザーの意図を学習するための振る舞い分析も備えていません。誤検知と実際のリスクを区別するには、ユーザーの意図を理解できることが重要です。

Proofpoint Adaptive Email DLPは、振る舞いAIを使用してメール上の偶発的および意図的な情報漏えいを防止します。メール誤送信、ファイルの添付間違い、情報の持ち出しを阻止することで、リスクと修復にかかるコストを削減します。また、セキュリティチームは、誤検知の調査にかかる時間を減らせるため、その時間を保護の微調整に割り当てることができます。

このソリューションは、人に起因するリスクの4つの主要エリアを低減する、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。



Purviewではメールの誤送信を阻止できない

Purviewのメールルールは、事前定義された特定の種類のコンテンツが組織から流出するのを防ぐには効果的です。しかし、メールの送り間違いを阻止することはできません。メールの誤送信を阻止するには、過去のメールパターンなどのコンテキスト（背景情報）やメール内容に基づいて、従業員の普段の行動を詳しく理解する必要があります。

Proofpoint Adaptive Email DLPは、12か月以上におよぶメールのヒストリカルデータを分析し、送信者と受信者の通常のコミュニケーション パターンを学習します。Proofpoint Adaptive Email DLPは、このインテリジェンスを使用し、メールの誤送信を未然に特定して阻止します。

Purviewはメールによるデータ持ち出しに対し効果的でない

メールによるデータ持ち出しの多くは、従業員が機密データを自分宛に送信するという形で発生します。これは、従業員がライバル企業に転職しようとする際によく見られます。

Purviewでは、GmailやYahooなどの無料メールサービスを一括でブロックできますが、そうすると業務関連のメールもブロックしてしまうため、有効ではありません。また、データが個人のメールドメインに送信されてしまうのを防ぐこともできません。無料メールサービスとのすべてのやり取りにフラグが付けられてしまえば、誤検知が増えすぎて、セキュリティチームによる分析の妨げとなってしまいます。

Proofpoint Adaptive Email DLPは、業界で最も豊富なデータでトレーニングされた高度なAIを用いています。従業員のメール上の行動を分析することで、不審なものと通常のコミュニケーションを区別するよう学習します。これにより、より正確で効果的なアラートが得られるため、調査を迅速化しながら、時間とリソースを節約することができます。

Proofpoint Adaptive Email DLPはリアルタイムでユーザーを指導

Purviewでは、メールポリシーに違反した従業員に、ポリシーのヒントを警告メッセージとして表示する設定が可能です。しかし、これらは、構成と調整に時間がかかります。また、警告があまりにも頻繁に表示されれば、ユーザーは、無視するようになるかもしれません。これは、「アラート疲れ」と呼ばれる現象です。

Proofpoint Adaptive Email DLPは、追加のセットアップ不要で、リスクのある行動について、コンテキストに基づくリアルタイムの警告を提供します。ユーザーは、メールの誤送信やファイルの添付間違いを送信前に修正することができます。従業員が機密データを自分や他の人に送信しようとした場合、Proofpoint Adaptive Email DLPは、その構成に基づいて、従業員の行動をブロックまたは追跡できます。

連携させればさらに効果的

メールによる情報漏えいが起これば重大な被害につながるおそれがあります。このようなインシデントにより、組織に課徴金、風評被害、ビジネスの損失が生じる可能性があります。調査、規制機関への報告、コンプライアンス関連の報告により、人件費がかさむ場合もあります。

機密性が最も高いデータを保護し、こうした被害を回避するには、静的なルールベースのアプローチではなく、柔軟かつインテリジェントなメールDLPソリューションが必要です。

Purviewと、Proofpoint Adaptive Email DLPのAIを活用したパワーを組み合わせれば、メールによる情報漏えいに対する、包括的かつ堅牢な保護を築くことができます。

詳細はこちら：http://proofpoint.com/jp