

Proofpoint Email Protection

既知及び未知のメール脅威を検出して阻止

主なメリット

- より多くの脅威をより早く検出し、より強固な保護を提供します
- 迅速なメールの追跡とメールハイジーン（衛生管理）で生産性を向上させます。
- 高い柔軟性で大規模な企業にも対応します
- セキュリティ オペレーションと脅威レスポンスを自動化して作業を効率化します
- 統合されたメール暗号化、メール DLP、Targeted Attack Protection などで保護を強化します
- 業界をリードするクラウド配備時の SLA：
 - 99.999%のサービス可用性
 - 100% のウイルス対策
 - 1分未満のメール遅延
 - 99%のスパムを 阻止またはリダイレクト

サイバー脅威の攻撃経路として最もよく使われるのはメールで、90% 以上のサイバー攻撃はメールがトリガーになっています。¹ フィッシングやマルウェアといった一般的なメール脅威に加え、ビジネスメール詐欺 (BEC) が急増して、新しい脅威となっています。Proofpoint Email Protection は、他のセキュリティソリューションでは見逃してしまうような既知及び未知の脅威を検出します。Proofpoint は毎日何十億通ものメールを処理しているため、より多くの脅威をより早く検出し、検出の難しい非マルウェア攻撃 (詐欺メールなど) からも組織を保護します。Email Protection を用いれば、大半の脅威をユーザーの受信箱に届く前に阻止できます。

Proofpoint Email Protection はメールの送受信の保護や管理を支援し、機械学習とマルチレイヤーの検出技術を用いて、悪意のあるメールを識別して阻止します。また最新の脅威や一般的な迷惑メールを動的に分類し、詐欺メール、フィッシング、マルウェア、スパム、バルクメールなどを含む様々なメールのきめ細かな管理を実現します。そして非常に柔軟性が高く、セキュリティ ポリシーやメール ルーティング ルールをカスタマイズすることができます。Fortune 1000 の企業に最も利用されているメール セキュリティですので、大規模な企業にも対応可能です。さらにクラウド、オンプレミス、ハイブリッドのいずれの環境でも利用できます。

¹ Data Breach Investigations Report, Verizon, 2019 (2019 年 Verizon データ漏洩調査レポート)

他のソリューションでは見逃してしまう新しい脅威を検出

フィッシング及び詐欺メールを検出

Proofpoint Email Protection は未知の脅威でも、ユーザーの受信箱に到達する前に検出します。独自技術である Stateful Composite Scoring Service (SCSS) は、高度な機械学習機能でメールを分類し、非マルウェア脅威 (クレデンシャルフィッシングや、ビジネスメール詐欺 (BEC) などの詐欺メールなど) も検出します。SCSS は数十億通のメール属性 (メールのヘッダー、コンテンツなど) の分析結果を用いて送信者のレピュテーションを評価します。この情報に加えて組織内の通常のフローを学習し、また他の Proofpoint 製品からの情報も集めてセキュリティのベースラインを形成します。このベースラインを基にすれば、基準から外れたメールを迅速に発見してブロックできるため、全体的な有効性が上がります。SCSS はアップデートに頼るのではなく、リアルタイムに学習することで、安全なメールと危険なメールを適切に分類し、変化する攻撃手法に対応します。

悪意のあるメールや不要なメールを阻止

Email Protection にはマルチレイヤーの検出技術が組み込まれており、進化を続ける脅威に対抗します。シグネチャを使った検出では、ウイルス、トロイの木馬、ランサムウェアなどの既知の脅威を阻止します。また、レピュテーションの動的な分析では、ローカル及びグローバル IP アドレスを継続的に評価して、メールを受け取るかどうかを決定します。さらに、独自のメール分類子で、詐欺メール、フィッシング、マルウェア、スパム、バルクメール、アダルト コンテンツ、信頼の輪などといった様々なメールを動的に分類し、タイプ別に隔離します。これらの機能を組み合わせることで、悪意のある活動の兆候を発見して対処することができます。

わずか数秒でメールを検索

Email Protection には、強力な検索機能が搭載されています。このスマートサーチ機能では、数十の検索条件に基づいて通常は発見が困難なログデータを簡単に検索でき、また、メールがどこから送られてきて、どこに送られようとしているのかも迅速に追跡できます。Email Protection は 100以上の属性のメタデータなどを含む詳細な検索を数分ではなくわずか数秒で完

了し、その検索結果を 100 万件までダウンロード/エクスポートできます。さらに複数のリアルタイム レポートによってメール フローと傾向を細部にわたって可視化できますから、問題へのプロアクティブな対応が可能になります。

高い柔軟性で大規模企業にも対応

他社のソリューションとは異なり、Email Protection は世界最大規模の企業のニーズにも対応します。グローバル、グループ、ユーザー レベルで、高度にカスタマイズしたメール ファイアウォール ルールを作成することができ、要件に沿ったセキュリティ ポリシーやメール ルーティング ルールを作成して、簡単に適用できます。Email Protection には複数の配備オプション (オンプレミス ハードウェア、仮想マシン、SaaS を含む) があるため柔軟性が高く、いずれにおいても同じ機能が活用できます。

エンドユーザーのセキュリティ意識を向上

メール警告タブ機能を用いれば、安全かどうかの判断が難しいグレーエリアのメールについて、エンドユーザーは十分な情報を得たうえで適切な意思決定をできるようになります。メールに付随するリスクを簡単に説明し、リスク レベルを色分けしてわかりやすく表示するため、危険なメールにエンドユーザーの注意を促して不正アクセスのリスクを低減させられます。

また、Email Protectionを使うとエンドユーザーがバルクメールのような危険度の低いメールの管理、隔離されたメールの確認、そして適切なアクションの実行などもできるようになり、メール管理者はこういった業務から解放されます。ユーザーからのフィードバックは Proofpoint に送信され、Proofpoint はこれをバルクメールの分類の正確性向上に役立てます。

メール暗号化及び DLP の集中管理

Proofpoint Targeted Attack Protection、Email Encryption、または Email Data Loss Prevention (DLP) でセキュリティを簡単に強化できます。Email Protection では基本的なメール暗号化と DLP 機能を提供していますが、同じ管理コンソールを使ってさらに強固なメール暗号化と DLP 機能を使用することもできます。これらは完全に統合されているため、メールで送信される機密データの管理が容易になり、メールによるデータ漏洩やデータ損失も防ぐことができます。また多くのコンプライアンス要件も満たすこともできます。

詳細は proofpoint.com/jp でご確認ください。

proofpointについて

Proofpoint, Inc. (NASDAQ:PFPT) は、サイバーセキュリティの主導的企業であり、組織の最大の資産であり同時に最大のリスクでもある「人」を守ります。Proofpointは、クラウドベースの統合ソリューションによって、世界中の企業が標的型脅威を阻止し、データを守り、ユーザーがサイバー攻撃に対してより大きな耐性を持てるように支援します。また、Fortune 1000の過半数を超える企業を含むあらゆる規模のトップ企業が、メールやクラウド、ソーシャルメディア、Web関連の最も重要なセキュリティリスクおよびコンプライアンスリスクを低減させるために、Proofpointを利用しています。詳細は www.proofpoint.com/jp でご確認ください。

©Proofpoint, Inc. Proofpointは、米国およびその他の国におけるProofpoint, Inc.の商標です。記載されているその他すべての商標は、それぞれの所有者に帰属します。