アドバンスド メール セキュリティ ソリューション

既知および未知のメール脅威を防ぎ、高度な攻撃と狙われるユーザーを可視化

メールは現代のビジネスの基盤となる不可欠な機能です。しかし同時に、サイバー攻撃の経路として最もよく使われるものでもあります。90% 以上の脅威はメールを介して届きます。[1] メール攻撃はフィッシングから新しいメール脅威まで、日々進化しています。メール攻撃にはビジネスメール詐欺 (BEC)、サプライチェーン攻撃、ランサムウェア、クラウドアカウント侵害なども含まれます。こうした高度なフィッシング脅威から人や重要なデータを守るには、プルーフポイントの統合ソリューションが最も効果的です。

プルーフポイントは完全かつ拡張可能なメールセキュリティプラットフォームで、高度な攻撃から人を守ります。メール脅威の検知と阻止、そして最大のリスクである Very Attacked People™ (VAP) の可視化を実現し、また実践的な知見を提供するため、リスクをより深く理解し、脅威により早く効果的に対応できるようになります。

既知および未知の脅威が受信箱に届く前に検知しブロック

堅牢な統合脅威対策プラットフォームで高度な脅威を阻止

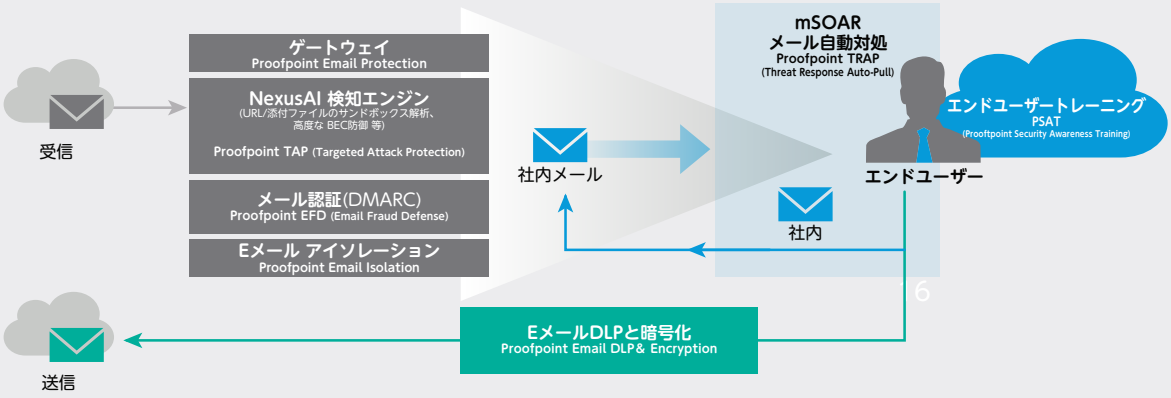
プルーフポイントは、より多くの脅威をより早く検知するため、より優れたプロテクションを提供します。悪意のある URL や添付ファイルのついたメールだけでなく、マルウェアを使用しない認証情報のフィッシングやビジネスメール詐欺 (BEC) などもブロックします。プルーフポイントは Impostor Classifier を用いて詐欺やフィッシング脅威を動的に分類します。また、高度な機械学習機能を提供する Proofpoint Advanced BEC Defense を使用して送信者のレピュテーションを確認します。この情報に加え、組織内の通常フローを学習し、また他のプルーフポイント製品からデータを収集して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識別できるため全体的な有効性が上がります。

プルーフポイントはマルチレイヤーのコンテンツ分析、レピュテーション分析、サンドボックスを用いてメールを分析します。これにより、ポリモーフィック型マルウェアやランサムウェアなどの高度なメール脅威がユーザーに届く前に効果的に阻止できます。そして、クリック時間帯に基づく予測型の URL サンドボックスで、悪意のある URL を検知してブロックします。URL を書き換えることでどのようなネットワークやデバイス上でもユーザーを保護し、さらに、受信して武器化してしまったメールも検知します。

メールとブラウザの分離でクリックしても安全

攻撃者が組織への侵入を試みる方法はひとつだけではありません。彼らはさまざまな手法や攻撃経路を用います。例えば、会社のメールや個人の Web メールに攻撃をしかけてきたり、またはユーザーが会社のデバイスで私用のインターネット閲覧をしているときを狙ったりします。Proofpoint Email Isolation と Proofpoint Browser Isolation を用いれば、ユーザーは Web サイト、個人 Web メール、コーポレートメールに安全にアクセスできるため、安心して Web サイトを利用できるようになります。また Web サイトが分析されるまで、アップロード / ダウンロードを無効化し、データ入力を制限することもできます。ページが開かれると同時にリアルタイム フィッシング対策スキャンが実行されます。これにより、そのページがフィッシングサイトの可能性があるかどうか、わずか数秒で確認することができます。この技術により認証情報の盗難対策が強化されます。配信後に害を及ぼすような URL のついたフィッシングメールには特に効果を発揮します。

1 2020 年 Verizon データ漏洩調査レポート
(Data Breach Investigations Report, Verizon, 2020)



プルーフポイントのアドバンスド メール セキュリティ ソリューション

メール認証でメール詐欺を防止

DMARC (Domain-based Message Authentication, Reporting and Conformance) はなりすましドメインを阻止する最も効果的な対策です。また、あなたのドメインを使ったなりすましメールも防止します。プルーフポイントは DMARC を迅速にデプロイし、正規のメールを誤ってブロックするリスクを最小限に抑えるため、従業員、パートナー、顧客を確実にサイバー脅威から守ることができます。また、プルーフポイントが提供する可視性、ツール、サービスを活用すれば、正規のメールの認証や、詐欺メールのブロックを簡単に行えるようになります。また、DMARC 認証を迅速かつ安全に実行して、信頼できるドメインを悪用した詐欺メールをプルーフポイント ゲートウェイでブロックします。さらに、どのような手法が使われていても、また誰を標的にしたものであっても、あらゆるなりすまし脅威を単一のポータルから確認できます。また、第三者が登録した類似の偽ドメインにフラグを立てます。これにより、詐欺的な類似ドメインを使用したメール攻撃を、攻撃が行われる前に阻止することができます。プルーフポイントのマネージドサービスには、経験豊富なコンサルタントによるデプロイサポートが含まれています。また、信頼できる送信者（第三者を含む）は適切に認証されるように、送信者の識別もプルーフポイントがサポートします。

内部メールを保護し脅威を迅速に封じ込める

内部メールの保護は受信メール対策と同様に重要です。攻撃者は侵害したアカウントを使ってフィッシング攻撃、ビジネスメール詐欺 (BEC)、マルウェアなどを送付します。プルーフポイントは URL や添付ファイルに悪意のあるコンテンツが含まれていないかをスキャンします。悪意のある内部メールが検知された場合は、既に内部で転送または受信されていた場合でも、メッセージを自動的に取り除いて隔離できます。また、どのアカウントが侵害された可能性があるかをレポーティングするため、管理者はそういったアカウントに迅速な対処ができます。

攻撃と攻撃対象となった人を可視化

現在のサイバー脅威は人を狙って攻撃をおこなうため、ユーザーは組織の最大の資産でありながら最大のリスクでもあります。リスクを緩和し、幹部や役員にリスクを報告するためには以下のような情報が必要です。

- 誰が最も注意すべき人物である VAP™ か
- どのように狙われているか
- 誰がそういった攻撃に騙されやすいか

プルーフポイントは標的型攻撃と攻撃対象となった人を可視化するため、誰が組織にとってリスクとなっているかを判断できます。こういった知見があれば、高リスクユーザーに適したセキュリティ制御をおこなうアダプティブ コントロールを実施し、リスクを優先順位付けし緩和することができます。

さらに、脅威とキャンペーンに関する詳細なフォレンジック情報をリアルタイムで提供します。この脅威分析を用いれば、攻撃の対象となっているユーザー、攻撃の発信源、攻撃の様相（メールサンプルやスクリーンショットを含む）まで、詳細に確認することができます。さらに、メール攻撃と不審なログインとを結びつけ、アカウント侵害をより的確に発見し阻止します。

また、Nexus Supplier Risk Explorer はサプライヤーのなりすましや、侵害されたサプライヤーやドメインを自動的に識別し、それらを使って送られてきたメールも識別します。どのサプライヤーが高リスクかを可視化することで、複雑な攻撃にも包括的に対応できるようになります。

運営効率の改善

ほとんどの組織ではセキュリティ要員が不足しています。さらに、ほとんどのセキュリティチームはいくつものセキュリティベンダーや製品の管理に時間を割かれ、加えてこれらは連携されていないことも多々あります。プルーフポイントの統合ソリューションを用いれば、重要な脅威にフォーカスし、脅威検知や修復を自動化することができるため、貴重な時間と費用を節減することができます。

ワンクリックで悪意のあるメールを自動対処

送信後に害を及ぼすような URL を含むフィッシングメールを取り除きます。また侵害された内部アカウントからの望ましくないメールもワンクリックまたは自動で隔離します。転送されてしまったメールも隔離できます。また、Nexus Threat Graph は豊富なアラートを提供し、自動的にフォレンジック データの収集と比較を行います。これにより脅威を可視化して実際の運用に活用できます。手作業や推測でのインシデント対応をなくし、脅威に迅速かつ効率的に対処できるようになります。

Abuse(不正報告) メールボックス運用の効率化

なりすましやフィッシング攻撃のユーザー報告と、セキュリティチームの対応を効率化します。これにより IT 部門の負荷を大幅に低減できます。Abuse(不正報告) メールボックスの対処を自動化すると、ユーザーは PhishAlarm® メール報告アドインからワンクリックで、または E メール警告タグから直接、不審なメッセージを報告できます。報告されたメールは複数の脅威インテリジェンスとレピュテーション システムを用いて自動的に分析され、メールが悪意のあるものであると分かれば、そのメールやその他のコピー（転送されたものも含む）は自動的に隔離されます。手動でインシデントを管理したり調査したりする必要はありません。そしてユーザーにはカスタマイズされたメールが送られ、メールが悪意のあるものであったことが通知されます。こういった通知で、将来、類似のメールをまた報告するようユーザーを奨励できます。

フィッシングやなりすましの脅威をユーザーが識別できるようトレーニング

最新のメール脅威の多くは、人がアクションを取らなければ発動しません。セキュリティ意識の高いユーザーは、サイバー攻撃に対する最後の砦になることができます。これはフィッシングやビジネスメール詐欺（BEC）が防衛線をすり抜けてしまった場合は特に重要になります。プルーフポイントの VAP™ レポート、フィッシングシミュレーション、ナレッジアセスメントを活用すれば、攻撃を受けているユーザーを識別し、またユーザーの自己防御能力を評価できます。プルーフポイントはカスタマイズ可能なターゲットを絞った教育を提供し、ユーザーが脅威から組織を守るために必要な知識とスキルを身に着けられるようにします。ユーザーへの攻撃シミュレーションでは実際のフィッシングと同じものを使い、実際に脅威に直面したときにどうすべきかをユーザーが学べるようにしています。攻撃シミュレーションに騙されたユーザーにはその場で学ぶことができるジャストインタイムのガイダンスを自動的に提示し、今後は脅威を回避できるようにします。また E メール警告タグも提供します。これは特定のメールに付随するリスクを簡単に説明し、メールを報告すべきかの判断に役立つ情報を提供します。

メールを介したデータ損失への対策

メールは最大の攻撃経路であり、最大のデータ損失経路でもあります。そのためメールを介したデータ損失の予防と機密データの保護が重要になっています。プルーフポイントのソリューションはメールコミュニケーションを可視化し、メールを介した意図的または事故によるデータ損失を防ぎます。難しい設定は不要です。これには E メール情報漏えい対策 (DLP) と暗号化が統合されており、集中管理が可能です。プルーフポイントは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ます。また、きめ細かく調整されたポリシーと事前に作成されたディクショナリを提供します。これらは規制やデータプライバシー法で保護されるデータを自動的に発見して分類します。これにより、様々な業界におけるデータ保護ルール (PCI DSS、SOX、HIPAA、GDPR 等) の順守が容易になり、また手作業も軽減されます。暗号化と組み合わせると、ポリシーを自由に定義しカスタマイズしてメール内の機密データを自動的に暗号化できるので、機密データのやり取りの管理や保護が簡単になります。

サマリー

プルーフポイントのアドバンスド メールセキュリティ製品群は最大の脅威経路であるメールを効果的に保護し、また攻撃や、攻撃されやすい人を可視化します。
プルーフポイントのソリューション:

- 既知および未知のメール脅威を組織に侵入する前に阻止
  Proofpoint Email Protection
- ユーザーを狙う脅威を可視化
  Proofpoint TAP (Targeted Attack Protection)
- 自動脅威対応で運用を効率化
  Proofpoint TRAP (Threat Response Auto-Pull)
- エンドユーザーが防御壁となれるようトレーニング
  PSAT (Proofpoint Security Awareness Training)
- メールを介したデータ損失を阻止
  Proofpoint Email DLP & Encryption

詳細

詳細は proofpoint.com/jp でご確認ください。