proofpoint

Proofpoint による保護

最大の脅威経路を保護するために、人を中心としたメールセキュリティを採用する企業が増えている理由

ポイント

94% のデータ漏洩はメールを使った攻撃が発端 [2]

ビジネスメール詐欺 (BEC) とメールアカウント侵害 (EAC) の被害額は全世界で **262 億ドル** [3]

86% の組織が 2019 年に BEC 攻撃を受けている [4]

メールセキュリティが重要な理由

電子メールは、 現代のビジネスでは不可欠な中心的機能です。 しかし同時に、 マルウェア攻撃 [1] やフィッシング、 ビジネスメール詐欺 (BEC) などの脅威の 90% 以上が、 攻撃経路として電子メールを使っています。

Proofpoint は、 人そのもの、 人が使うデータやデジタルチャネル、 そして彼らのデジタルアクティビティを標的とする攻撃に対抗する、 最も効果的なソリューションを提供します。 Proofpoint の人中心のアプローチにより、 サイバーセキュリティのギャップを埋めることができます。

Proofpoint が最高の保護を提供できる理由

現在のサイバー攻撃は、 テクノロジーではなく人を標的にしています。 そのため Proofpoint のサイバーセキュリティは、 人を中心としたアプローチをとっています。 Proofpoint のソリューションを使うと、 人が生み出すリスクを理解し、 報告することができます。 そして人を標的とする脅威を阻止し、 安全を確保するために必要なツールを提供します。 これほど効果的に人やブランドを保護できるサイバーセキュリティ企業は他にはありません。

最も効果的な脅威対策

メールを使う脅威は、 進化を続けています。 それに常に先んじるためには、 以下のようなメール脅威を阻止する改革を続けなければなりません。

- クレデンシャル フィッシング
- BEC
- メールアカウント侵害 (EAC)
- 多段階マルウェア

Proofpoint は、 こういった脅威を阻止する新しい検出技術を提供しています。 Proofpoint の動的かつ多階層化された脅威検出機能は、 日々の脅威分析から学習し続けます。 この脅威分析は、 一日に数十億通のメールと数千のマルウェアサンプル、 そして数百万のクラウドアカウントについて行われています。

それだけではありません。 進化を続ける攻撃者に先んじるため、 Proofpoint では売上の 20% 以上を R&D に投資しています。 これほどの投資をしている企業は、 この業界でもわずかです。

例えば、あるお客様はデータ漏洩のリスクを半減でき、導入初年度だけで数十万ドル規模の価値が生まれました。[5]

Proofpoint は他のメールセキュリティツールよりも多くのマルウェア、 フィッシング、 BEC/EAC 攻撃を阻止します。

[1] *Verizon*。 「2019 Data Breach Investigations Report （2019 年データ漏洩調査レポート）」 2019 年 7 月。
[2] Ibid。
[3] 被害額。 *FBI*。 「Business Email Compromise: the $26 billion scam （ビジネス メール詐欺 : 被害額 260 億ドル）」 2019 年 9 月。
[4] *Proofpoint*。 「2020 年 State of the Phish」 2020 年 1 月。
[5] *Forrester*。 「The Total Economic Impact Of Proofpoint Advanced Email Protection （Proofpoint Advanced Email Protection から得られる経済効果）」 2019 年 10 月。

可視化

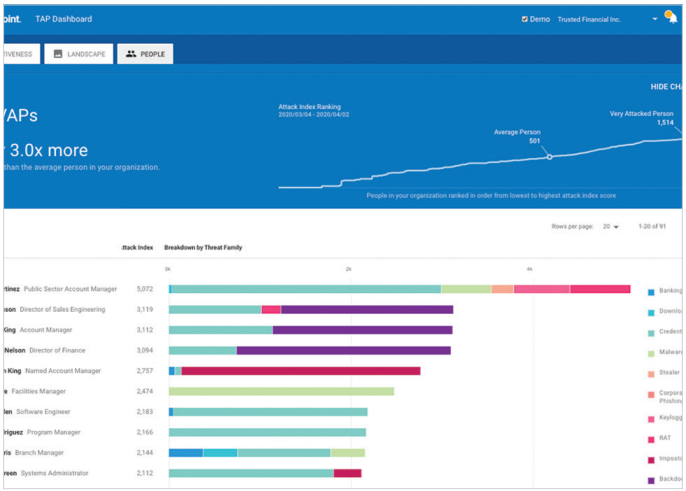
メールによる脅威は、人を攻撃します。 そのため、それらを阻止、検出し、 復旧するためには、 まず Very Attacked People ™ (VAP) を知ることが必要です。 VAP とは攻撃者が興味を持つ人物であり、そのため最もリスクの高い人物です。

Proofpoint のソリューションは、 攻撃対象となる人について、実用的な可視化をし、 誰がどのような攻撃の対象になり、 また誰が攻撃されているのかを可視化します。

Proofpoint 独自の Attack Index は、 VAP が誰かを識別し、 リスクの評価と緩和の手助けをします。 Proofpoint Attack Index は脅威についての加重複合スコアで、 4 つの主な因子に基づいて計算されます ：

- ボリューム
- タイプ
- 標的の絞り込みの度合い
- 攻撃者の洗練度

この知見を活用してリスクを報告し、 また緩和策の優先順位付けができます。



Proofpoint Targeted Attack Protection ダッシュボードでVAPを可視化できます。

効果的かつ効率的なセキュリティオペレーション

多くの組織ではセキュリティスキルの不足や、インシデントの調査・復旧にかかる膨大な手作業に悩まされています。セキュリティチームは限界まで働いているものの、脅威は増加し続けています。世界のサイバーセキュリティの人手不足は400万人以上です。[6]

そのため、 負担を管理し軽減するセキュリティソリューションが必要とされています。 Proofpoint はほとんどの脅威を、 受信箱に届く前、 そしてインシデントになる前に阻止します。 また、主要なインシデント調査と対応を自動化し、 侵入した脅威の迅速な封じ込めや修正に必要となるコンテキストを提供します。

手作業や推測による対応に頼るのではなく、 ユーザーの受信箱から危険なメールを自動的に除去します。

自動的に除去されるメールは、 例えば危険な URL を含むメールや、 ユーザーが不審であると報告したメールなどです。 どのようなケースでも、 メールインスタンスはすべて自動的に検出され除去されます。 他のユーザー、 部門、 メーリングリストに転送済みのメールも対象です。

Proofpointのソリューションにより、あるお客様は運用コストを30万ドル削減でき、今まで2-3人必要だった作業に1人のセキュリティスタッフで対応できるようになりました。[7]

Proofpoint を使えば、 セキュリティチームは人でなければできない作業に集中できるようになり、 限られたセキュリティリソースでも対応できるようになります。

今すぐご検討ください

Proofpoint の顧客満足度は **95%** 以上、 またリニューアル率は **90%** 以上です。

以下のようなお客様にご利用いただいています。

- Fortune 100 企業の半数以上
- 大手国際銀行
- 大手国際小売業
- 著名な研究系大学
- 大手製薬会社

Proofpoint のクラウドベースのメールセキュリティソリューションは、 世界有数の高度な脅威インテリジェンスプラットフォーム上に構築されており、 最新の脅威の防止、 防御、 対処を効率的に実行します。

どのようなオプションがあるか、 詳しくお知りになりたい場合は、 現在のセキュリティ環境について簡単な無償アセスメントを提供しておりますので、 是非ご連絡ください。 24 時間以内に、 最小限の構成でセットアップできます。

こちらでお申し込みください。
proofpoint.com/jp/free-trial-request

[6] *(ISC)²*。 「2019 (ISC)² Cybersecurity Workforce Study. （2019 年 (ISC)² サイバーセキュリティ要員についての調査）」 2019 年 11 月。
[7] *Forrester*。「The Total Economic Impact Of Proofpoint Advanced Email Protection （Proofpoint Advanced Email Protectionから得られる経済効果）」 2019年10月。

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.