Proofpoint Targeted Attack Protection™

クラウド型サンドボックスで標的型攻撃に対抗

ランサムウエア・バンキング型トロイの木馬を防御するメールセキュリティ

ウイルススパムーフィッシングースピアフィッシングと進化してきたメールの脅威は、現在 APT/ 標的型サイバー攻撃としてさらに脅威の度を増しています。APT/ 標的型サイバー攻撃は、特定のターゲットに向けた少量の攻撃であることから、従来のシグネチャやレピュテーションによる検知が有効に働かないという問題があります。

Proofpoint Targeted Attack Protection™ (以下「Proofpoint TAP」) は、この問題を全く新しいアプローチで解決します。それは、「継続的に異常を監視し、後から判明した脅威からもユーザーを守る」というものです。

クラウド型添付ファイルのサンドボックス

Proofpoint がサンドボックスを使って添付ファイルを実行し、危険性を検証ます。クラウド型ですから、お客様のリソースは必要ありませんし、お客様は安全に保護されます。

クラウド型 URL のサンドボックス

Proofpoint がお客様に代わってリンク先の Web サーバーにアクセスし、事前に危険性をチェックします。事後のチェックも行いますから、時間差攻撃にも対抗できます。

社内でも社外でも保護

社外からネットワークに接続する社員を、社内同様不正な Web サイトから保護します。

脅威の可視化

攻撃の事実や攻撃対象者など、脅威を可視化します。攻撃されたとき、対処に必要な情報を提供します。

Proofpoint TAP はビッグデータ技術を使ったアノマリティクス解析、URL を書き換えて危険なサイトへのアクセスを防ぐ Click-Time Defense、サンドボックス機能などを組合せ、ダッシュボードによって常に脅威を監視することにより、潜在的な脅威を監視し、脅威を見つけ次第それを無効化することができるのです。

Proofpoint TAP のアプローチはシグネチャやレピュテーションに頼らないため、将来 APT/ 標的型以外の脅威が現れても有効に機能します。コンピュータセキュリティはこれまで、新しい脅威が現れるとそれに対抗する、といった後手に回る対応しか取れませんでした。Prootpoint TAP は、新しいアプローチでこれを逆転し、初めてメールセキュリティに先手を打つことができるのです。

■ ビッグデータによる潜在的脅威の検知

Proofpoint による脅威検知はビッグデータ技術を元にしており、ネットワーク上のトラフィックを数百もの要素についてリアルタイムに分析します。これらの分析と過去のメールトラフィックパターンの分析から、メール送信元の普段の行動パターンを割り出し、過去と異なる挙動を示した場合に、疑わしい攻撃と判断します。

proofpoint™

■ Click-Time Defense により、危険な URL へのアクセスからユーザーを継続的に保護

最近の APT/ 標的型サイバー攻撃では、セキュリティソリューションに検知されないよう、メッセージ自身にはマルウェアを含まず、外部の (マルウェアに感染した、あるいは乗っ取られた) URL に誘導する手法が多くとられます。セキュリティソリューションの中にはメッセージ中の URL を検査してマルウェア判定を行う高度なものもありますが、攻撃はさらに高度化しています。メール配信の時点では正常なままにしておき、後からそのサイトにマルウェアを仕込むという攻撃では、メールゲートウェイを通過した後ですから、従来型のセキュリティシステムでは対抗できません。

Proofpoint TAP の「URL click-time defense」は、受信したメッセージに含まれる URL を書き換え、その URL をクリックしたユーザーはいったん Proofpoint に接続するようにします。ユーザーにより URL がクリックされるたびに、Proofpoint TAP がその URL が危険なもので無いかどうかを検証し、安全であればその URL へリダイレクトし、脅威であることがわかれば、アクセスをブロックします。

いったん URL を書き換えてしまえば、そのメッセージが外部に転送された後でも、ユーザーが社内ネットワークでなく社外のネットワークやモバイルデバイスからアクセスした場合でも保護は有効で、長期にわたって継続的にユーザーを守ることができます。

■ TAP ダッシュボードにより脅威を即座に可視化、迅速な対応と復旧が可能

Proofpoint TAP の Threat Insight Service は、Web ベースのダッシュボードとカスタマイズ可能な警告システムにより、攻撃状況をリアルタイムに可視化し、素早い対応と復旧を可能にします。

- 標的型サイバー攻撃の検知 (攻撃されているのか)
- 攻撃の規模
- 攻撃対象 (自社のみか、業界全体かなど)
- 攻撃手法 (マルウェア、フィッシングなど)
- 組織内の誰が狙われているのか
- クリックしてしまったユーザーはいるか
- 復旧作業が必要かどうか

上は TAP ダッシュボードの画面例です。特定の URL について、画面上部左にその URL がマルウェアを含んでいることが判明したことが表示されており、その右にこの URL を含むメールの受信数、受信時点でブロックした数、URL を書き換えた上で配信した数が表示されています。さらにその右に、配信されたメールを受け取った受信者が実際にクリックされた数が 1 であったことが表示され、そのクリックは許可されたこと (脅威を含む URL にアクセスしてしまったこと) がわかります。管理者は受信者をすぐに特定できますから、必要な措置を講じることができます。

■ 容易な導入

Proofpoint TAP はクラウドベースのソリューションですから、導入や設置作業が必要ありません。メールストリームを Proofpoint TAP にリダイレクトして頂くだけで、すぐにでも使い始めることができます。

Proofpoint について

Proofpoint Inc. (NASDAQ:PFPT) は、クラウドベースの包括的脅威保護、インシデント対応、セキュアなコミュニケーション、ソーシャルメディア及びモバイルセキュリティ、コンプライアンス、アーカイブ / ガバナンスを提供する、次世代の主導的セキュリティ / コンプライアンス企業です。世界中の組織が Proofpoint の専門知識、パテント取得済みの技術およびオンデマンドのデリバリーシステムを使ってフィッシング、マルウェアやスパムメールからシステムを守り、暗号化された機密情報や個人情報を守り、重要な情報や電子メールをアーカイブし管理します。

proofpoint™

お問合せ

日本プルーフポイント株式会社
〒103-0027 東京都中央区日本橋2-2-6 日本橋通り二丁目ビル 9F
TEL : 03-3510-7981 FAX : 03-5299-0232
Email : sales-japan@proofpoint.com
URL : http://www.proofpoint.co.jp/