Proofpoint Isolation

企業や個人のメールにおいて高度なWeb脅威や悪意のあるURLからユーザーを保護

主なメリット

- すべてのWebコンテンツをリアルタイムで調査
- ランサムウェアやゼロデイURL攻撃から防御
- セキュリティで保護されたソーシャルメディアやコラボレーション アプリを含むすべてのアプリで、悪意のあるURLを分離
- 個人のWebメール、分類できないサイトや不審なサイトを分離
- 認証情報の窃取と正規アカウントの悪用を防止
- ファイルのアップロードやダウンロードにおけるインラインかつリアルタイムに動作する情報漏えい対策（DLP）を提供
- 地域のデータプライバシー規制への準拠を簡素化
- クラウドから迅速かつ簡単に展開 — 追加のハードウェアやエンドポイントエージェントのインストールは不要

Proofpoint Isolationは、ユーザーのWebブラウジングとメールアクティビティを保護します。クラウドベースのリモート分離機能を用いて、組織をマルウェアや情報漏えいの危険にさらすことなく、ユーザーはWebサイトや個人/企業のメールに自由にアクセスすることができます。

Proofpoint Isolationは、悪意のあるWebサイトの閲覧、標的型フィッシング攻撃、危険な個人Webメールの使用によって発生するセキュリティ/生産性/プライバシー問題を解決に導きます。さらにクラウドベースのソリューションのため、展開、管理、サポートは非常に簡単です。Proofpoint Isolationは、Information Protectionプラットフォームに搭載されています。

従業員がリスクのあるWebサイトを閲覧する、または企業メールまたはWebメールに記載されたURLをクリックすると、Proofpoint Isolationは、そのページを、ネットワーク外およびユーザーのデバイス外のセキュアなコンテナに返します。これにより、危険なコンテンツを環境外に締め出すことができます。ユーザーは、分離されたWebページを普段通りに表示・操作できますが、マルウェアやその他の有害コンテンツは画面から排除されます。データの盗難や損失防止のため、アップロード、ダウンロード、入力フォームを無効化することができます。また、プルーフポイント独自のリアルタイム コンテンツ調査は、フィッシングURLやランサムウェアといった、ゼロデイ脅威を検知します。このソリューションは、脅威が発見されると、そのページを今後使用できないようにブロックします。

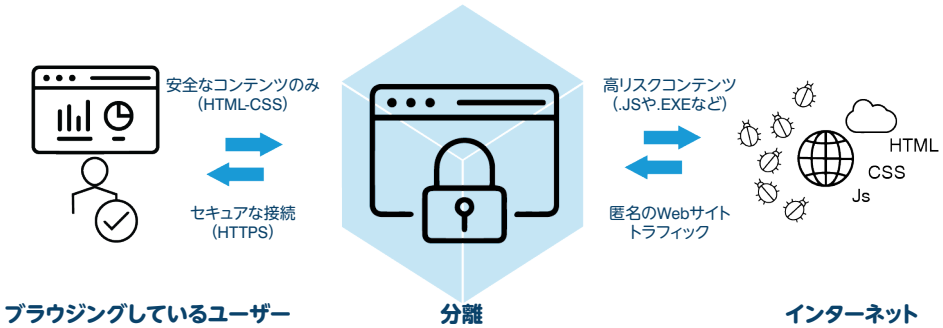

図1：Proofpoint IsolationはWebページから実行可能なコードを削除し、Proofpoint Isolationブラウザで安全なページをユーザーに返します。

リスクのあるURLと標的ユーザーに適応型セキュリティを活用

今日の攻撃者は、多くの場合、メールを攻撃経路として組織の従業員を標的にし、アカウントの侵害、認証情報の盗難、機密情報の漏えいを招いています。このように脅威が進化する中では、アダプティブ コントロールが高リスクユーザーの保護に役立ちます。ユーザーがメール内のURLをクリックしてWebサイトを訪問した場合、ポリシーに基づいてブラウジング セッションを自動的に分離します。Webメールも含む、高リスクのサイトや分類できないサイトはProofpoint Isolationに送信することができます。

Proofpoint Isolationは未知の脅威を解析するサンドボックスであるProofpoint TAP (Targeted Attack Protection)と統合して、高リスクユーザーに送られた企業メール内のURLを分離できます。Proofpoint TAPと統合することで、リアルタイムにフィッシングのスキャンと検知ができるようになります。ブラウザセッションが分離されるとProofpoint TAPダッシュボードに通知が送られ、新しい脅威を発見してリスクを低減します。

攻撃対象領域の縮小

多くの組織で、企業ネットワークへの接続時も個人Webメールやインターネットの使用を許可しています。これを把握している攻撃者は、個人のWebメールを使用している特定の従業員を標的にし、巧妙な攻撃を仕掛けます。こうした攻撃の半数以上は、会社支給デバイスでのインターネットや個人メールの使用がきっかけとなっています。

Proofpoint Isolationは、従業員が個人のWebメールを自由に使用し、インターネットを安全に利用できるようにしながら、リスクを低減します。組織側でアクセスをブロックしたり、ユーザーの行動を追跡したりする必要はありません。リスクのあるWebサイトやクラウドアプリへのトラフィックを分離されたセッションにリダイレクトするだけです。これは、企業の環境、クラウド、ユーザーのデバイスから隔離された環境内で安全に行われます。Proofpoint Isolationは、さまざまなブラウザベースの攻撃から防護します。水飲み場型攻撃や武器化されたクラウド アプリケーション（Microsoft SharePointやDropboxなど）へのリンクなどといったWebベースの攻撃を防げます。

分離セッションではペイロードや悪意のあるマクロのついた、ファイルのダウンロードを阻止します。Proofpoint Isolationは、ユーザーの入力を動的に制限することでブラウザを介した認証情報の窃取を防ぎ、ダウンロードの阻止でドライブバイマルウェア攻撃を防ぎます。さらに、悪意のあるWebコンテンツからエンドポイントを守ります。また信頼できるサイトでも、不正アクセスされたサイトであればコンテンツの分離をします。

ITチーム負荷の軽減

さまざまなユーザーがさまざまなリスクをもたらし、必要とするアクセスレベルもさまざまです。時に従業員は、不明なURLや個人のWebメールへのアクセスを必要とします。ほとんどのソリューションでは、リスクを承知でアクセスを許可するか、アクセスを却下してユーザーの生産性に影響を与えるか、ITチームはどちらかを選ばなければなりません。多くの場合、特例で今回だけアクセスを許可してほしい、という個人やグループからのリクエストでITチームはオーバーフローしてしまいます。こうした例外の管理は時間がかかったり、困難であったりします。

Proofpoint Isolationでは、管理者がユーザーグループやそのアクセスを制御するためのブラウジング ポリシーをいくつも作成できるため、こうした問題を回避できます。例えば、広範なアクセスが必要な調査者、経営幹部、その他のユーザーには、比較的制限の少ない、個別の制御を適用できます。このようなアダプティブ コントロールにより、ITチームの負荷を低減でき、ケースバイケースでアクティブに例外を管理する必要がなくなります。

Proofpoint Isolationは、Proofpoint Enterprise DLP (Data Loss Prevention)に統合されています。これは、機密データのアップロードやダウンロードにおけるインラインかつリアルタイムに動作する情報漏えい対策（DLP）を提供します。このソリューションは、データ分類を共有し、アラート管理と調査を単一のポータルから行うことができます。URL、URLカテゴリ、ファイルの種類、ファイルに機密データまたはマルウェアが含まれているかといった条件によってアップロードやダウンロードを制限できます。

分離されたブラウザセッションは攻撃者からは完全に見えないので、ユーザーを標的にすることは不可能です。また、このソリューションにより、現地のデータプライバシー規制に対応することもできます。従業員のプライバシー問題やコンプライアンス違反を回避できます。

Proofpoint Isolationは、展開が容易で、既存のWebフィルター、プロキシ、ゲートウェイ、ファイアウォール ツールとも連携します。

詳細はこちら

詳細は、**proofpoint.com/jp**でご確認ください。