データシート

proofpoint.

PROOFPOINT BROWSER ISOLATION

企業と個人を標的にした高度な攻撃からユーザーを保護

主な利点

- リスクベースのアダプティブコントロールで企業メール内の悪意あるURLを分離
- 未知や新規のドメインなどのハイリスクなWeb利用ではブラウザを分離（Isoration）
- クレデンシャルの盗難と悪用を防止
- 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
- シームレスなブラウジング
- GDPRへのコンプライアンスを簡素化

標的型フィッシング攻撃やクレデンシャル盗難からのユーザーの保護は依然として難しい問題です。さらに悪いことに、攻撃者は大規模な攻撃キャンペーンで悪意のあるURLを用いて瞬く間に被害を拡大させます。このように増え続ける脅威に対して、私たちはどのような対策をすべきでしょうか。Proofpoint Browser Isolationでマルウェアやデータ流出を防げば、ユーザーはインターネットを安全に使用できるようになります。

製品説明

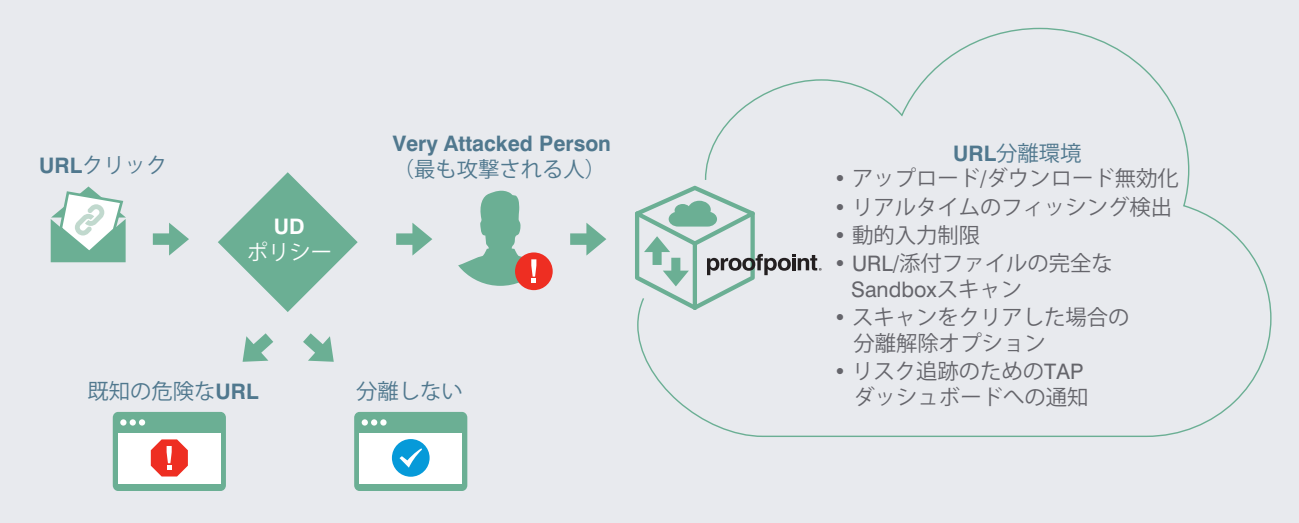
ブラウザ分離（Isolation）は、ブラウザセッションを安全なコンテナに分離するため、ユーザーはWebサイト、個人メール、企業メールに安全にアクセスできるようになります。セキュリティで保護されたコンテナ内でブラウザセッションを分離することにより、これを行います。これは、マルウェアや悪意のあるコンテンツからユーザーを守る独自のソリューションです。アップロードやダウンロードは無効化され、機密データの盗難や流出を防ぎます。これらによって、標的型フィッシング攻撃や危険なWeb利用によって発生するセキュリティ/生産性/プライバシー問題を解決できます。さらに、この製品は簡単に展開、管理、サポートできます。

機能と利点

危険なURLと狙われているユーザーのセキュリティ対策

攻撃者はフィッシングメールで組織内の特定の個人を狙っています。攻撃されやすいユーザーを守るためには、アダプティブコントロールが必要になります。Proofpoint Browser Isolationは、企業メールに含まれる悪意のあるWebベースのコンテンツからユーザーを守る機能です。ブラウザの分離により、ブラウザセッションは、ユーザを危険度の高いURLから保護するためのポリシーに基づき分離されます。未知のURL、ソーシャルネットワーク、オンラインクラウドアプリなどからユーザーを守ります。

Proofpoint Targeted Attack Protection （TAP）と統合されているため、TAPを使用していれば企業メールでのBrowser Isolationの利用が可能です。人を中心とした管理、そしてTAPで、リスクを効果的に低減します。管理者は企業メール内のリスク要因をベースにして、分離環境を使うユーザーを選択することができます。TAPとの統合により、リアルタイムにフィッシングのスキャンと検出が可能になります。分離されたブラウザセッションはTAPダッシュボードから確認することができ、リスクをトラッキングできます。



攻撃対象領域の縮小

多くの組織では、職場での個人Webメールやインターネットの使用を許可しています。攻撃者はそれを知っており、そこを狙って高度な攻撃を仕掛けてきます。調査によると60%近くの攻撃が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から起こっています。インターネットや個人メールの利用を許可しながらリスクを減らすにはどうしたらよいでしょうか。

Proofpoint Browser Isolationを使うと特定のWebサイトやクラウドアプリケーションを分離することができるので、インターネットや個人メールの安全な使用と組織のセキュリティ向上の両方を実現できます。これによって会社の資産にリスクが生じることはありません。ファイルの中身やユーザーの行動の監視も必要ありません。ペイロードのついたファイルやメール添付ファイル、悪意あるマクロのダウンロードを阻止し、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を分離します。これにより、水飲み場型攻撃や、武器化されたMicrosoft SharePointやDropboxなどのクラウドアプリケーションへのリンクからユーザーを保護することが可能になります。ブラウザを使ったクレデンシャルの盗難は、動的な入力制限で防ぐことができます。Browser Isolationはドライブバイダウンロードも阻止し、また、その他の悪意あるWebコンテンツからエンドポイントを守ります。

IT部門の負荷の軽減

未分類／未知のURLや個人Webメールへのアクセスをユーザーに許可するのは非常にリスクが高いですが、業務上そういったサイトを使わなければならないこともよくあります。ほとんどのソリューションでは、どのサイトを許可しどれをブロックするかは、ITチームが決定しなければなりません。こういったドメインすべてをブロックしてしまうと、特例で今回だけアクセスを許可してほしい、というリクエストでIT部門はオーバーフローしてしまいます。

そのためBrowser Isolationが役立つのです。ユーザーのインターネットの利用によって発生するセキュリティ上、生産性上、そしてプライバシー上の問題をProofpoint Browser Isolationが解決します。ブラウジングセッションをコンテナ内に安全に分離すれば、ユーザーは個人Webメールやその他のサイトに自由にアクセスできるようになり、そしてIT部門はケースバイケースで特例許可を出す作業から解放されます。さらに、この製品の展開、管理、サポートは非常に簡単なので、IT部門の生産性向上によりコスト削減効果がすぐに現れます。また、ユーザーを信用することでユーザーのモラルを高めることができ、さらに個人Webメールのプライバシーを尊重することでコンプライアンス上の問題を回避できます。Proofpoint Browser Isolationは100%クラウドベースなので、展開は簡単です。またWebフィルター、プロキシ、ゲートウェイ、ファイアウォールとの統合も可能です。

詳細は www.proofpoint.com/jp でご確認ください。