メールベースのサイバー攻撃を防御する Menlo Securityのメールアイソレーション

メールは最も多用される攻撃手法、かつ企業環境で最も脆弱なリンク

利点：

- Webフォームへの重要なユーザー認証情報の入力を阻止
- リスクが疑われるリンクのクリックにより、組織に甚大なリスクを引き起こす可能性があるユーザーを特定
- 設定可能な警告メッセージをリアルタイムで表示して、フィッシング認識向上トレーニングを追加で実施
- 安全なバージョンまたはオリジナルの添付ドキュメントのダウンロードを許可するポリシーを設定
- クラウドベースのアンチウイルスおよびサンドボックス環境でオリジナルのドキュメントを自動スキャンし、許可を判定（パスワード付きのZIPファイルにも対応）
- ユーザー操作性や既存のワークフローに影響を与えることなく、既存のメールサーバーインフラストラクチャと統合

従来のセキュリティソリューションによる保護の弱点

今もなお、メールはマルウェアの拡散を企てるサイバー犯罪者にとって、最も一般的で最も成功している攻撃手法です。従来のメールセキュリティソリューションは、サンドボックスを用いて、組織内とサードパーティの脅威インテリジェンスフィードに基づいて「良い」か「悪い」かを判定しますが、現在のメール攻撃で最も多いのは、小規模なグループや特定の個人など、標的を極端に絞り込むタイプの攻撃であり、現在利用されているようなレピュテーション情報は今後ますます意味をなさなくなっていきます。

つまり、こうした攻撃を前にして、検知だけに頼るアプローチではユーザーや組織を保護することはできません。

Menlo Securityメールアイソレーション

Menlo Securityは、攻撃者が悪意のあるリンクやメール添付ファイルを使ってユーザーのエンドポイントへマルウェアを配信することを防御するために、アイソレーションを活用します。Menlo Securityメールアイソレーションは、Menlo Securityクラウドアイソレーションゲートウェイとの緊密な統合に基づいて、ブロックあるいはアイソレーションのアプローチによって、悪意のある既知のリンクや添付ファイルを自動的にブロックすると同時に、安全と見なされたリンクや添付ファイルを含むそれ以外のすべてをアイソレーションします。このゼロトラスト戦略により、メールをきっかけとして悪意のあるコンテンツがユーザーのエンドポイントにアクセスすることを一切なくすことができます。

このソリューションは、既存のメールサーバーインフラストラクチャとシームレスかつネイティブに統合されるため、メールにおけるユーザー操作性に違和感が生まれることはなく、新しいメールシステムについて学び直したり、ソフトウェアを新たにインストールしたりする必要もありません。すべてのWebコンテンツとメール添付ファイルはMenlo Securityクラウドアイソレーションゲートウェイ（MSIG）を経由するため、マルウェアがユーザーのデバイスへ到達できる可能性があるすべての経路を遮断します。これはその他のどのメール保護サービスも提供していない、業界初のソリューションです。

メールリンク

メール内のリンクが本物かどうかをひとつひとつ判定する方法を採用していないため、許可するかブロックするかを粒度の低い分類に基づいて判断する必要がありません。Menlo Securityでは、アイソレーションゲートウェイを介してすべてのWebコンテンツをアイソレーションします。つまり、取得と実行の命令は、ユーザーのブラウザーから遠く離れたクラウドで行われます。

管理者は、Webページやフォームを読み取り専用で表示するカスタムポリシーを設定できるため、ユーザーが誤って認証情報を入力してしまうことを阻止できます。さらに、最もフィッシング攻撃の犠牲になりやすいユーザーに関する有用な情報を分析したり、設定可能な警告メッセージをリアルタイムに表示して、最も気付きを得やすいタイミングでフィッシング対策トレーニングを実施したりすることができます。

96%

メール経由で実行されるソーシャルエンジニアリング攻撃の割合

—ベライゾン2018年度
データ漏洩/侵害調査報告書

メール添付ファイル

受信したメールをユーザーが開き、添付ファイルをクリックすると、瞬時にアイソレーションされた100%安全な状態でドキュメントが表示されます。Menlo Securityによるこのアイソレーションは、既存のワークフローを崩壊させたり、ユーザー操作性を低下させたりすることはありません。さらに、管理者は、マクロが除去された安全なPDFバージョンで添付ドキュメントをダウンロードできるオプションを提供できます。場合によっては、高度なアンチウイルスとサンドボックスでスキャンした後に、オリジナルの添付ドキュメントのダウンロードを、一部のユーザーに限り許可することもできます。パスワード付きの添付ファイルにも対応しています。

Menlo Securityのゼロトラストアプローチ

多くの組織が、アンチスパム、アンチウイルス、データセキュリティ、暗号化などあらゆる種類のメールセキュリティソリューションを運用しているにもかかわらず、メールベースのサイバー攻撃の毒牙から逃れることができていません。この状況から抜け出すには、検知だけに頼るアプローチから脱却し、セキュアWebゲートウェイソリューションとメールアイソレーションを統合すべきです。そうすれば、リスクがあるかどうかに関係なく、メール経由でもたらされるすべてのWebコンテンツとドキュメントをユーザーのエンドポイントデバイスから常に切り離しておくことができます。このゼロトラスト戦略こそ、ブラウジングやメールの操作性を犠牲にすることなく、メールベースの攻撃からユーザーと組織を守る唯一の手段です。

Menlo Securityのソリューションを活用して組織を保護する方法について詳しくは、japan@menlosecurity.com までお問い合わせください。

Menlo Securityについて

Menlo Securityは、Web、ドキュメント、メールからマルウェアの脅威を排除することによって、組織をサイバー攻撃から保護します。Menlo Securityは、グローバル2000に名を連ねる何百社もの企業と主要な政府機関におけるセキュアクラウドトランスフォーメーションの達成を支援してきました。Menlo SecurityのCloud Security Platformは、拡張性に優れており、あらゆる規模の企業に包括的な保護を実現します。エンドポイントソフトウェアは不要で、エンドユーザーの操作性にも影響しません。Menlo Securityは、ガートナーセキュアWebゲートウェイ（SWG）についてのマジック・クアドラントでビジョナリーに選出されています。

お問い合わせ：
www.menlosecurity.jp
japan@menlosecurity.com