MENLO SECURITY

ビジネスメールを保護

最も重要なビジネスツールであるメールを、フィッシングやランサムウェア、認証情報の盗難から保護します

Solution Brief

メールは現代の企業において最も重要なビジネスツールであり、だからこそ悪意のある攻撃者はそれを狙っています

1. Verizon Data Breach Investigations Report
2. Ponemon Institute, "Cost of a Data Breach 2020."

メールや侵害されたドキュメントに悪意のあるリンクを埋め込み、それをエンドユーザーにクリックさせるという戦術は、サイバー犯罪者が重要なビジネスシステムにアクセスしようとする際には非常に有効で、効果も実証されています。Verizon Data Breach Investigations Reportの中で分析されているほとんどすべてのマルウェアがメールにより配信されており、報告されたインシデントの80%以上がフィッシング攻撃で占められているのは、そのためです。[1] エンドユーザーは企業のセキュリティ戦略の中で最も脆弱な部分であり、彼らが頻繁に使うメールは最も簡単に侵害できるポイントですから、攻撃者がそこを狙うのは理にかなっています。

攻撃に使われるリンクは巧妙になりすまされていたり、信頼されている正規のサイトにそっくりだったりするため、訓練を受けていない善意のユーザーがそれらの違いに気づくことはほぼ不可能です。一度エンドユーザーのデバイスに感染すると、攻撃者はその先の企業ネットワークや重要なビジネスシステムにアクセスして大きな損害を与える可能性があります。

検知と対応によるメールセキュリティソリューションは、もはや有効ではありません

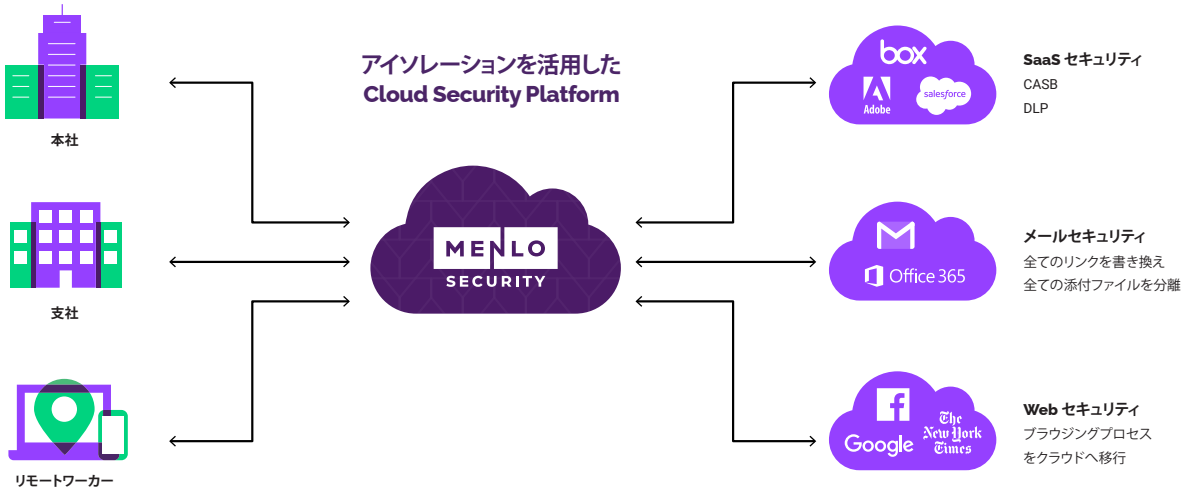
検知と対応という戦術のみに依存しているレガシーなセキュリティソリューションは、常に進化を続ける高度なメール攻撃について行くことができていません。これらのソリューションは、メール内のWebリンクと添付ファイルを分析して「良い」か「悪い」かを判断しています。しかし、最新の攻撃は組織内の特定の個人を標的にしており、ドキュメントまたはメールに含まれるリンクは通常、標的とするユーザー毎に異なります。そのためサードパーティのレピュテーションデータは存在せず、内部で分析するために必要なデータも十分ではありません。「良い」か「悪い」かの判断が正しく行われない場合、狙われて感染した「最初の被害者」は、認証情報が盗まれたりマルウェアをダウンロードさせられたりする可能性のあるサイトに直接アクセスすることになります。たったひとつのエラーが、大きな損害を与え復旧のコストがかかるサイバー攻撃を呼び込んでしまう可能性があるのです。

データ侵害による組織の平均コストは386万ドルに上っています[2]

メンロ・セキュリティのアイソレーションを活用したCloud Platform がメールを保護

Menlo Security Cloud Platformは、メール攻撃によって引き起こされるマルウェアへの感染、認証情報の盗難、およびドライブバイエクスプロイトを排除します。アイソレーションを活用したMenlo Security Cloud Platformを既存のメールサーバーインフラ（Microsoft ExchangeやOffice 365、Google Gmail、その他のWebメールなど）と統合することで、すべてのメールリンクと添付ファイルはアイソレーションプラットフォームを通過するように変換されます。別途アプライアンスを導入したり、エンドポイントへクライアントやエージェント、プラグインなどをインストールする必要はありません。ユーザーがメール内のリンクをクリックすると、メンロ・セキュリティがサインインページを読み取り、専用モードでレンダリングし、ポリシーを適用してユーザーが悪意のあるWebフォームに機密情報を入力するのを防ぎます。

その際最も重要なことは、ユーザーエクスペリエンスやワークフローには一切影響がなく、すべてがユーザーに対して透過的でシームレスであることです。実際、ほとんどのユーザーは、自分のWebコンテンツが自分のデバイスではなくクラウド上で処理されていることにすら気づきません。



メンロ・セキュリティのメールアイソレーションソリューションは、導入展開された瞬間にすべての企業とすべてのメールユーザーを保護することができる、唯一のメールセキュリティソリューションです

メンロ・セキュリティにより、管理者はグループまたは個々のユーザーのワークフローポリシーを定義することも可能です。リスクの高いユーザーは読み取り専用ページにリダイレクトして認証情報を入力させないようにしたり、その他のユーザーには特定のセキュリティ対策を回避させたりすることができます。またユーザーを安全に分離すると同時にユーザーの行動統計も監視することができ、クリック時メッセージ（カスタマイズ可能）を表示させて、フィッシングに対する意識を向上させるトレーニングを強化することができます。

メリット

既存のメールインフラと簡単に統合

メールで配信されるマルウェア、ドライブバイエクスプロイト、フィッシング攻撃を排除

メールクライアントやクラウドサービスでネイティブのユーザーエクスペリエンスを維持

アイソレーションベースのメールセキュリティによって業務を保護します

メールは、企業にとって最も重要なビジネスツールです。人は生来、他人を信頼してしまいがちであるという特質を持っており、それにつけ込もうとする攻撃からエンドユーザーを保護する必要があります。メンロ・セキュリティは、セキュリティの責任をユーザーに負わせず、メールに関連したすべての添付ファイルとトラフィックを悪意のあるものとして扱います。すべてのトラフィックはクラウド上のアイソレーションレイヤーで実行されるため、悪意のあるコンテンツはユーザーのデバイスにアクセスできません。その結果ユーザーは、基盤となるインフラのどのデバイスで業務を行う場合でも、いつでもメールにアクセスできると共に常に保護されます。

世界各地のユーザーに安全なインターネットアクセスを提供しながら組織をサイバー攻撃から守る方法については、menlosecurity.com/ja-jp/ にアクセスするか、japan@menlosecurity.com までお問い合わせください。

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

Menlo Securityについて

メンロ・セキュリティは、他に類を見ないアイソレーションを活用したクラウドセキュリティプラットフォームにより、企業が脅威を排除し、生産性を完全に維持することを可能にします。メンロ・セキュリティは、悪意のある攻撃を防ぐために最も安全なゼロトラストアプローチを提供し、エンドユーザーはセキュリティの存在を気にせずにオンラインで仕事をすることができ、さらにセキュリティチームの運用負担を軽減することで、クラウドセキュリティの目標を実現できる唯一のソリューションとなっています。これにより企業は安全なオンライン体験を提供することができ、ユーザーは安心して業務を行いビジネスを進めることができます。