MENLO SECURITY

世界有数の非営利医療機関における医療専門家と職員に対するWeb脅威のアイソレーション

Case Study

Overview

課題

急速に進化する脅威の状況、複雑なネットワーク、分散型の管理構造に直面して、数万人ものユーザーを抱えている世界有数の非営利医療機関では、医療専門家や職員を高まるWeb脅威から保護しなければならないという課題がありました。侵害されたWebサイトや悪意のあるWebサイトを1回クリックするだけでマルウェアに感染し、数百万件の電子医療記録が盗まれる恐れがありました。電子医療記録は、ダークウェブで社会保障番号やクレジットカード番号より高値で売買されるほどの価値があります。

解決策

この医療機関は、マルウェア感染を防ぐために、新たなアプローチとしてWebアイソレーションを採用しました。Webアイソレーションでは、ユーザーと潜在的な攻撃源との間に、安全で信頼できる実行環境、つまりアイソレーションプラットフォームが配置されます。アイソレーションプラットフォームは、ユーザーのエンドポイントから離れた場所でセッションを実行し、安全なレンダリング情報のみをユーザーのデバイスに送信することによって、ユーザーをWebマルウェアから保護します。

メリット

この医療機関は、優れたメールスパム、フィッシング、およびURLのフィルタリングソリューションによって保護されていましたが、Menlo Securityのアイソレーションプラットフォームにより、いかなるWebベースのサイバー攻撃によっても組織の多層セキュリティアプローチが突破されることはないと確信できるようになりました。この目標は、ユーザーの操作性に影響を与えることなく、また、ITチームに負担を強いることもなく達成されました。

多様なユーザーとロケーションの組み合わせを保護

この医療機関は、6つの州に50,000人以上の職員を擁しており、安全であるだけでなく、医師や派遣看護師などの医療専門家、ビジネスパートナー、ベンダー、施設職員、事務員に対応できる柔軟性と拡張性を備えたセキュリティソリューションを必要としていました。

彼らは、職務を遂行するためだけでなく、自分の生活を管理するためにもWebに頼っています。セキュリティという名のもとに彼らのWebアクセスを制限すれば、業界全体で医師や看護師が不足している中で、彼らのやる気をそぐことになりかねません。医療機関の間では頻繁に人材の争奪戦が起きており、医療専門家がどの医療機関で働くかを決める際には、Webやメールへのアクセスの容易さがその決定に影響を与える可能性があります。

この医療機関には非常に多くのユーザーがいるため、組織は、生産性に悪影響を及ぼす、ヘルプデスクへの問い合わせが増える、従業員向けの追加のトレーニングが必要になる、あるいは従業員にセキュリティ対策を逃れる口実を与えるような製品を導入することはできませんでした。また、導入展開は6つの州にまたがる必要があったため、アプライアンスの設置、構成、保守を行うのは現実的ではありませんでした。

「十分に安全」なセキュリティはもはや十分に安全ではない

今日、組織はマルウェア、フィッシング、ランサムウェア、およびその他のサイバー攻撃による日々の猛攻撃から身を守るために、数多くのアプローチを利用することができます。たとえば、ファイアウォールや次世代ファイアウォール（NGFW）など、ネットワーク境界の製品があります。また、セキュアWebゲートウェイやURLフィルタリング、統合脅威管理（UTM）製品など、Webベースのサイバー攻撃から組織を保護することを目的としたアプライアンスやソフトウェアもあります。さらには、アンチウイルス、アンチマルウェア、メールセキュリティゲートウェイ用のアプライアンスやソフトウェアなど、エンドポイント関連の特定の課題に対処する製品もあります。

これらの製品は、トラフィック、情報、メール、Webリンクなどが「安全」か「危険」かを判断する、単純なデシジョンツリーに基づいて機能します。「安全」か「危険」かの判断は、一般に、サイバー攻撃から保護するのに役立ってきましたが、確実なもの（フールプルーフ）ではありません。「安全」か「危険」かを判断するためのソースが最新である必要があります。サイバー攻撃がゼロデイ攻撃である場合には、「安全」か「危険」かというアプローチでは、攻撃を捕捉したり阻止したりすることができない可能性があります。また、誤ったアラートによってセキュリティオペレーションセンター（SOC）を消耗させる誤検知の問題もあります。もちろん、検知漏れについては言うまでもなく、これは攻撃が防御をすり抜けたことを表しているため、さらに深刻です。

ほとんどのサイバーセキュリティプロバイダーは、自社のソリューションが組織とそのユーザー、エンドポイント、および顧客情報を99.9%の時間、保護すると断言しています。しかし残念なことに、すべての攻撃者が成功するために必要とするのはその残りの0.1%であり、組織のネットワーク、ユーザー、エンドポイント、そして何よりも重要である顧客情報が、暗号化されて身代金を要求されたり、盗まれて販売されたり、あるいは単に削除されたりするリスクにさらされています。この点を考慮した上で、この導入事例の医療機関は、基本的なアプローチでも多くの攻撃の阻止に役立つものの、すべての脅威には対処できないという結論に達しました。新たなアプローチが必要でした。

解決策：アイソレーション

この医療機関が最終的に導入展開するソリューションは、それが何であっても、次の3つの条件を満たす必要がありました。

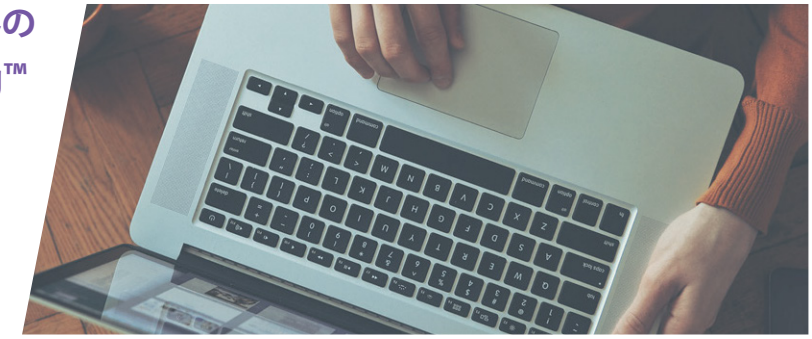
- **組織にとって必要なものか？**
- **組織の環境で機能するか？**
- **妥当な価格か？**

クラウドベースのMenlo Security Isolation Platform（MSIP）は、これらの条件を満たすだけでなく、侵害されたWebサイトや悪意のあるWebサイトを介してマルウェアがユーザーのデバイスに到達するのを阻止することにより、新たなレベルのセキュリティを提供します。このプラットフォームは、すべてのWebコンテンツをパブリックまたはプライベートクラウドの破棄可能な仮想コンテナーで開いてアイソレーションすることにより、セキュリティを損なうことなく、ユーザーがWebサイトやリンク、ドキュメントをオンラインで安全に操作できるようにします。従来から、マルウェア防御のためにアイソレーション技術を使用しようとする試みは、エンドポイントソフトウェアの導入展開や管理が必要だったり、ユーザーの操作性が低下または変化したりするなど、いくつかの主要な制限に悩まされてきました。Menlo Securityのクラウドベースのアイソレーションプラットフォームが選ばれた理由は、この製品が100%効果的であり、クライアントソフトウェアが不要であり、数分で導入展開でき、ユーザー操作性に影響を与えることなく世界中のあらゆる規模の組織を包括的に保護するよう簡単に拡張できるからです。

ユーザーが満足すればIT部門も満足

比較的短期間でのロールアウト中に、この医療機関のIT担当者は、ユーザーから好意的なフィードバックを受け取り、苦情は受けませんでした。製品を使用しているIT管理者でさえも、Webセッションがアイソレーションされていることを忘れてしまうことが多いと言っていました。これは、Menlo Securityの特許取得済みのAdaptive Clientless Rendering™（ACR）によって、完全にネイティブなユーザー操作性が保たれているためです。スクロール、コピーアンドペースト、右クリックメニュー、動画ストリーミング、印刷などの機能はすべて、これまでと同じ方法でアクセスでき、本来の機能を果たします。

Menlo Securityの特許取得済みのAdaptive Clientless Rendering™（ACR）は完全にネイティブなユーザー操作性を保ちます。



問題の解決

Menlo Security Isolation Platformソリューションは、未分類のWebサイトからのマルウェア感染を排除し、情報漏洩によって組織の電子医療記録が侵害される可能性を大幅に低減しました。

この医療機関は、このソリューションが安心感をもたらすだけでなく、感染したエンドポイントの修復やサイト分類要求の処理にかかる費用と人件費の両方で大幅な節約につながると推定しています。

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。