MENLO SECURITY

White Paper

クラウドを分割する。アイソレーションによる強固なセキュリティ

新型コロナウイルスは、Webアイソレーション導入のチャンスをもたらしました

変化が起きています

パンデミックの前でさえ、世の中の変化の速度は速くなっていました。それが今では、ビジネス、技術、社会すべてがワープスピードで進化しているようです。

新型コロナウイルス感染拡大の下でデジタルトランスフォーメーションが加速し、CSOは大きな課題を突きつけられました。しかしその一方で、時代遅れのサイバーセキュリティのアプローチについて考え直すチャンスも与えられました。

現代の脆弱性は、リモートワークの急増、ユーザー行動の変化、およびクラウド環境の複雑さによって引き起こされます。今必要なのは、昔のアプローチに戻ったりこれ以上回避策を考えたりするのではなく、今後も従来型の「検知と防止」をベースとした技術に依存し続けるのかどうかについて今一度考えることです。

何らかの侵害を経験したと報告した企業が2020年に81%に達したとき、サイバーセキュリティは変曲点に達したのです

変化することができれば、パンデミックからの脱出はより安全なものとなるでしょう。しかしそれは、考え方を変えて、アイソレーションに対して新たな気持ちで取り組むことができればの話です。

以前にも同様な話がありませんでしたか?

アイソレーションは、コンセプトとしては新しいものではありません。しかし、現在のソリューションを支えている技術は最新のものです。アイソレーションによって、企業のIT部門は「侵害は、されるかどうかではなく、いつされるかという問題である」という時代遅れの決まり文句からようやく解放されることになります。

仮想デスクトップインフラ（VDI）やアプリケーション仮想化、クライアント仮想化などの従来からのアイソレーション技術は、アクティブなコンテンツがエンドポイントに配信されないようにすることで、ユーザーを保護しようとするものです。これらの技術は原理としては有効ですが、実際に提供されるユーザーエクスペリエンス（UX）は遅く、とても満足できるものではありません。

VDIとアプリケーションの仮想化では、コンテンツは別のコンピューティングインフラで実行され、エンドユーザーの画面にピクセル単位でレンダリングされます。Webページの読み込みは遅く、アクション（文字の入力やリンクのクリック）を実行してから画面上でそれを確認できるまでに、かなりの遅延があります。またユーザーは、ページの印刷やコンテンツのコピー/ペーストなどの標準的な機能を使えないことがあります。

クライアントの仮想化には、専用のエンドポイントソフトウェアの導入やOSの変更、そしてPCの再ビルドが必要になり、それによって動作が不安定になることもあります。期待どおりに動作したとしても、ユーザーのマシンから大量のリソースが要求されます。

メンロ・セキュリティは、クラウドベースのプラットフォームでWebコンテンツを分離する独自のIsolation Core™技術を提供しており、生産性やユーザーエクスペリエンスを低下させずに100%安全にWebおよびメールコンテンツを表示させることができます。

メンロ・セキュリティのプラットフォームは、フィッシング、ランサムウェア、マルバタイジングなどの主要な脅威に対応します。また、企業および個人のメールを保護し、機能制限やエンドユーザーエクスペリエンスの低下を招くことなく、企業がコンプライアンスを達成することをサポートします。

これが典型的な組織にとって何を意味するのかを考えてみましょう。

リモートワーカーの保護を強化

日常業務のほとんどをオンラインで行う分散した従業員のおかげで、最も混乱した時期でも運用を安定させることができましたが、リモートワーカーの存在はサイバーセキュリティの提供を困難にしている側面もあります。

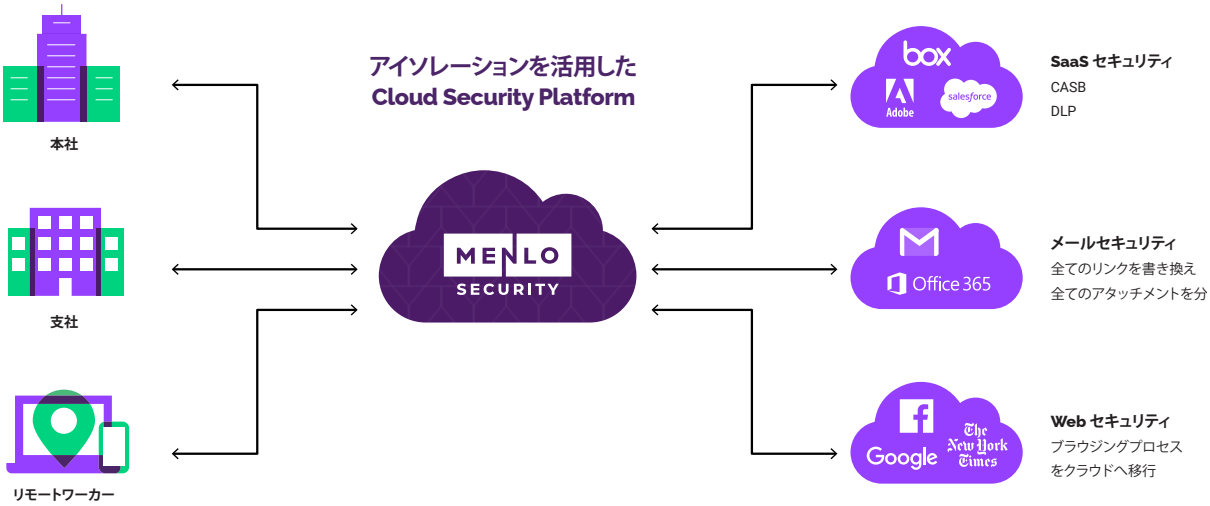
現在、従業員の少なくとも70%が、デバイスを企業ネットワークに接続するためにSaaSソリューションとリモートネットワークアクセスを使用しています

ブラウザーのエクスプロイトは脆弱性の原因となる可能性があるため、定期的に更新やパッチ適用を行い、メンテナンスする必要があります。ユーザー、デバイス、およびITチームが地理的に離れている場合、これを行うのは難しくなります。

多くのユーザーはルールを守り、常に侵害のリスクを意識しながらデバイスを扱っており、CSOはそれにある程度依存しています。しかし大企業に存在する数万のエンドポイントに渡ってその期待を拡大しようとすると、課題が明確になります。これらのさまざまなデバイスはいずれも、ネットワークをダウンさせる可能性があります。

メンロ・セキュリティのIsolation Core™は、自宅、オフィス、顧客サイト、公共のWi-Fiなど、ユーザーがどこからログインしても、サイバーセキュリティポリシーが適用されるようにすることで、安全なリモートワークを可能にします。

メンロ・セキュリティはIsolation Core™をCloud Security Platformに拡張し、クラウド上に独立したユビキタスなセキュリティ層を構築しており、すべてのWebおよびメールトラフィックはこのプラットフォームを通過します。悪意のあるトラフィックはブロックされ、それ以外のトラフィックはユーザーのエンドポイントから遠く離れた場所に隔離されます。セキュリティチームは、ひとつのプラットフォームからデータ保護とトラフィックフローの制御を行うことができます。



これは、ユーザーのデバイスに既知または未知の脆弱性があったとしても、マルウェアは侵入できないことを意味します。それが良いものであれ悪いものであれ、コンテンツはユーザーのブラウザー内では実行されないのです。

このプラットフォームのセキュアWebゲートウェイ（SWG）機能には、Cloud Access Security Broker（CASB）、データ漏洩防止（DLP）、Firewall as a Service（FWaaS）、およびPrivate Accessが含まれます。これらは一体となって、企業とユーザーがインターネットを安全でシームレスに使えるようにするというメンロ・セキュリティの目標を支えています。現在メンロ・セキュリティは、世界の10大銀行のうち8行、5大クレジットカード発行会社のうち4社、そして米国の大規模な政府機関のいくつかを保護しています。

クラウドとデジタルトランスフォーメーションに安全な場所を提供

ITインフラとサービスをクラウドに移行することは、デジタルトランスフォーメーションの重要なステップです。しかしこの移行は、すべてのインターネットトラフィックを中央のセキュリティ集約ポイントに送り込むという従来のハブ&スポーク型のネットワークモデルに過大な負荷をかけます。このような従来型のアーキテクチャの下では、エンドユーザーが世界中からSaaSプラットフォームやWebアプリにログインした場合に、この集約ポイントがボトルネックになり、遅延が発生する可能性があります。

リモートワーカーが使用するSaaSアプリケーションは時間とともに変化し、トラフィックパターンも変化します。Office 365だけでも、ユーザーごとに20を超える永続的な接続を作成し、ネットワークハードウェアに過負荷をかけることがあります。トラフィックが急激に落ち込んだり急上昇したりすると、予測できないパターンを生成してネットワークセキュリティスタックの基本要素に過負荷をかける可能性もあります。これらの問題は、単独で、または複数が組み合わさり、アプリケーションパフォーマンスの問題を引き起こし、ユーザーエクスペリエンスを低下させる恐れがあります。

アイソレーションは、エンドユーザーを保護する方法を根本から変えることにより、これらの問題を解決します。アイソレーションは、エンドポイントから離れた場所でWebセッションを実行し、ライブコンテンツのレンダリングされたバージョンのみをデバイスに配信するため、トラフィックのボトルネックを発生させません。

このアプローチは、ダウンロードされたドキュメントやクリックされたリンクに関係なく、サイバー犯罪者をユーザーのデバイスから分離します。これにより、マルウェアや横方向への侵害などの他のリスクを阻止することができます。従業員は安心してインターネットを使用することができ、ビジネスに内部的な脅威を与えることなく、クラウドのすべてのメリットを享受できます。

このように、アイソレーションはクラウドへの移行とデジタルトランスフォーメーションを成功させる鍵になります。トラフィックの可視性とセキュリティ制御の適用を強化することにより、SaaSアプリケーションの真の価値を解き放ちます。すべてのWebトラフィックが、高度な保護を保証するメンロ・セキュリティのアイソレーションプラットフォームに送信されるため、従業員は安心してクラウドアプリケーションを使用することができます。

顧客事例

世界中の大企業350社以上が、メンロ・セキュリティのアイソレーションプラットフォームを使ってエンドユーザーを保護し、マルウェアを阻止しています。

グローバルな金融サービスブランドは、10万人以上のユーザーのためにメンロ・セキュリティのIsolation Core™を導入しました。180日間で2,000個近くのフィッシングリンクがクリックされ、8,500個の悪意のあるWebサイトにアクセスがあり、それらのサイトでのクリックで安全と判定されたのは30%のみでした。

マルウェアの感染またはその他のネットワーク侵害：

ゼロ

従業員数2,000人、年間売上高10億ドルの米国の地方銀行が、Webやメールの脅威に対する100%の保護を実現するためにネットワークアイソレーションを導入しました。この銀行は3年間でアプライアンスを廃止し、セキュリティをクラウドに移行しました。また、VPNの帯域幅を削減することでネットワークパフォーマンスを向上させました。

投資収益率：

261パーセント

8万人のユーザーを抱える米国の連邦政府機関では、メンロ・セキュリティのCloud Security Platformの使用を開始後わずか30日で大幅な改善が見られました。エンドユーザー端末へのファイルダウンロードが70%減少し、VPNの帯域幅が50%削減されました。

8,000以上の

悪意のあるWebサイトへのアクセスがありましたが、マルウェアの感染や侵害はありませんでした

アイソレーションによって自由を獲得

新型コロナウイルスがもたらした変化、すなわち新しい顧客行動やデジタルタッチポイントへの移行、リモートワークの急増などにより、業界ごとにデジタルへの移行が急速に進んでいます。

パンデミックは私たちの仕事や生活のあり方を変え、それは今も続いていますが、サイバーセキュリティはそれに追いついていません。従来からの検知と対応の戦略に頼ることにはリスクが伴い、重要なシステムやアプリケーションの多くをクラウドに移行しつつある企業には適していません。

今、私たちはセキュリティの転換期を迎えており、これは拡大するサイバー脅威からネットワークやIP資産、そしてエンドユーザーをどのように保護するかを再考する、またとないチャンスです。ここで正しい道を選択した企業は、これまで以上に安全な環境を手に入れることができるでしょう。

CSOにとっては、これまで足かせとなっていたものに挑戦する千載一遇のチャンスでもあります。

デジタルトランスフォーメーションが進む中、メンロ・セキュリティのアイソレーション技術は、ユーザーのWebブラウジングやメール習慣を保護することができます。その結果、従業員は会社のネットワークが侵害されることを心配することなく、どのエンドポイントからでも、どの場所からでもWebアプリケーションやSaaSサービスにアクセスすることができます。

Isolation Core™を活用したMenlo Security Cloud Platformの詳細については、menlosecurity.com/ja-jpをご覧いただくか、ask@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。