MENLO SECURITY

世界中どこからでも業務が可能

ユーザーがどこに移動しても、SaaSプラットフォームへの高速で信頼性の高い、安全なアクセスを提供するために

Solution Brief

現代のユーザーは頻繁に移動し、互いにコラボレーションし、柔軟です。そして、これまで以上にセキュリティリスクに晒されています。

[1]Datto, "Global State of the Channel Ransomware Report"

Software as a Service（SaaS）は従業員の生産性を向上させましたが、企業の安全性を低下させもしました。かつて、企業の攻撃可能な領域はデータセンターを保護するゲートウェイに限定されていましたが、今では制限無く拡大しています。企業が使用しているツールが多いほど、セキュリティチームが追跡、監視、および保護しなければならない攻撃対象は大きくなることに、攻撃者は気づきました。企業を攻撃するために、SaaSサービスが狙われることが多くなっています。

2020年にはSaaSアプリケーションの25%がランサムウェアの標的になり、その内の3分の2近くがMicrosoft 365ソリューションを狙っていました。[1]

これらのサービスの多くは正規のサービスであり、セキュリティ対策製品のホワイトリストに登録されているため、悪意のある攻撃者が偽のアカウントを作成してしまえば、共有ファイルの通知やリンク、あるいはメールの添付ファイルを使ってマルウェアを送信することが簡単に行えます。これが意味することは、ユーザーがフィッシングリンクやマルウェアにアクセスすることをブロックするためのセキュリティが回避されてしまい、企業がこれらの高度な攻撃に対する防御策をほとんど、またはまったく失ってしまうということです。

従来型のサイバーセキュリティのアプローチでは不十分：不幸な結果につながります

従来からの検知と対応のアプローチは、カテゴリ分けと最新のリアルタイムな脅威インテリジェンスに依存しています。しかし残念ながら、SaaSプラットフォームにおいては、悪意のあるリクエストと正当なリクエストを識別する方法はありません。

企業は選択を迫られています。SaaSのすべてのトラフィックをブロックして生産性を大幅に制限し、クラウドトランスフォーメーションを停滞させるのか、それともすべてのトラフィックを妨げずにユーザーのデバイスに流しこむのかという選択です。後者を選ぶ場合、ユーザーをこれらのタイプの攻撃から保護することはできません。

より優れたアプローチは、ゼロトラスト戦略を採用し、SaaSサービスを介して送信されるメールリンクや添付ファイルを分離するセキュリティレイヤーを構築することです。

これは、悪意のある既知のサイトをブロックし、クラウド内の他のすべてを分離するグローバルクラウドプラットフォームを使用することで実現できます。分離に際して、既知または未知の脆弱性があるかどうかは関係ありません。悪意があるかどうかに関係なく、エンドポイントのブラウザーであらゆるコンテンツが実行されないようにすることで、重大な損害を被る可能性を排除できます。ユーザーは、メール、ドキュメント、またはSaaSプラットフォーム内のリンクを自由にクリックすることができ、その結果生じるトラフィックはクラウド側でリモートで実行されるため、ユーザーのデバイスにマルウェアは配信されません。

メリット

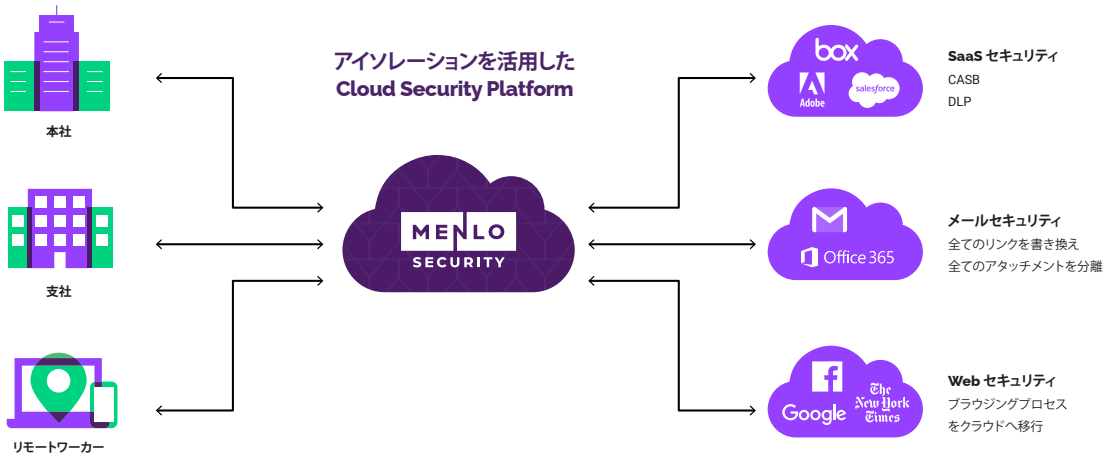
SaaSプラットフォームにアクセスするリモートユーザーに企業のセキュリティポリシーを適用します

ユーザーが世界のどこからログインしているのかに関係なく、高速で信頼性が高く、一貫性のある接続を確保します

IT運用の複雑さを軽減し、セキュリティチームが戦略的脅威に集中する時間を確保します

メンロ・セキュリティのアイソレーションを活用したクラウドプラットフォームが課題を解決します

Isolation Core™を活用するMenlo Security Cloud Platformは、世界中に分散した従業員からSaaSへのアクセスを保護するために必要なセキュリティフレームワークを組織に提供します。ネイティブのWebブラウジングエクスペリエンスやパフォーマンスには影響を与えません。Menlo Security Cloud Platformは、サイバーセキュリティを検知と対応によるアプローチではなく、SaaSを含むクラウド内のすべてのアプリケーショントラフィックを分離するアプローチで実現します。マルウェアは取り除かれ、安全なコンテンツのみが配信されます。その結果、エンドユーザーエクスペリエンスに影響を与えない、100%マルウェアのないメールとWebのセキュリティが実現します。



メンロ・セキュリティのアイソレーション機能は、拡張性のあるグローバルクラウド上に構築されており、ユーザーは適切なロケーションに動的にルーティングされ、適切なセキュリティポリシーとプロトコルが一貫して適用されます。これらのロケーションでは、ユーザーエクスペリエンスを損なうことなく、トラフィックの予期しない急増に対応するために、容量と処理能力を動的に調整します。

このアプローチにより、本社と同じユーザーエクスペリエンスとセキュリティポリシーがリモートワーカーにも適用されます。

たとえばカリフォルニア州サンノゼにいるユーザーは、セキュリティのために通常は西海岸のデータセンターに誘導されます。同じユーザーが飛行機で日本に移動した場合、東京でのインターネットアクセスには、サンノゼにいる場合と同じセキュリティポリシーが適用されます。しかしインターネットへのアクセスは東京のデータセンターを経由してルーティングされるため、高速で信頼性が高く、安全な接続が提供されます。

ユーザーにSaaSへの安全なアクセスを提供することで業務を保護

現代においては、すべての業務はインターネットを介して行われています。そしてその多くが、ユーザーがさまざまな場所からSaaSプラットフォームにログインして行なわれる業務です。最近の調査によると、大規模な組織は平均1,000個近くのクラウドアプリを使用しています。[2] しかし多くのCIOは、組織が使用するクラウドアプリは30〜40個程度であると考えており、認識と現実の間に大きなギャップがあることを示しています。

メンロ・セキュリティは、高速で信頼性が高く安全なSaaS接続を提供するため、企業はリスクを心配せずにビジネスを円滑に運営し続けることができます。ユーザーがオンラインで行う必要があるすべての業務について、中断することなく、安全に、そして自信を持って行うことができ、業務に集中することができます。

メンロ・セキュリティがどのようにサイバー攻撃に対抗し、インターネットへのアクセスを保護し、組織にセキュリティを提供するのかについては、menlosecurity.com/ja-jp/にアクセスするか、ask@menlosecurity.comまでお問い合わせください。

[2] Truist Securities, "2021: A Cyberspace Odyssey; Defending Against a New Age of Cyberthreats"

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。