MENLO SECURITY

Solution Brief

Microsoft 365 および Google Workspace での業務を保護

ユーザーがどこに移動し、どこで業務を行っても、
ビジネスを安全に守ります

私たちの働き方は変化し続けており、ユーザーはこれまで以上にクラウドベースのオフィスソフトに依存するようになっています

現在、ユーザーは自宅やリモートオフィス、あるいは顧客サイトなどで業務を行っており、クラウドベースのオフィスプラットフォーム上でメール、ファイル共有、メッセージング、オフィスアプリなどを使って世界中の同僚とコラボレーションを行っています。Google Workspace（旧 G Suite）はこの分野のパイオニアであり、世界中の数百万人ものユーザーが毎日Google Drive、Google Docs、Google Chatその他のビジネスアプリを使用しています。さらに、Microsoft 365（旧 Office 365）は現在、世界中の企業の従業員の5人に1人が使用しており、ユーザー数において最も広く使用されているクラウドサービスとなっています。

しかし、これらのプラットフォームを利用している何億人ものビジネスユーザーは、そのままフィッシングやランサムウェア攻撃の潜在的な標的でもあります。悪意のある攻撃者は、GoogleやMicrosoftの偽のロゴを使ってブランディングされた本物そっくりのメールを簡単に作成し、慎重に精査されたターゲットに送ることができます。これらのフィッシングメールの多くには、ダウンロード時にユーザーのデバイスに感染するコードを含む悪意のある添付ファイルが含まれています。さらにプラットフォーム自体も攻撃ベクトルとして使用されることがあります。悪意のあるファイルをホストして、それが未知のターゲットと共有される可能性があるのです。

従来型のサイバーセキュリティソリューションは、分散したユーザー毎のセキュリティ体制にギャップを生み出します

これらのソリューションは、カテゴリー分け、ホワイトリストとブラックリスト、およびリアルタイムの脅威インテリジェンスを使用して、クリックした時点でコンテンツを許可するかブロックするかを決定します。しかし残念ながら、信頼されているプラットフォームからのリクエストを悪意のあるものと正当なものに分類する方法はありません。そして、Webプロキシ経由ですべてのMicrosoft 365またはGoogle Workspaceトラフィックの検査とルーティングをすることは、ネットワークアーキテクチャと遅延の問題から難しいのが現状です。

問題を複雑にしているのは、今日のクラウドアプリケーションがユビキタスな接続を想定して構築されているため、通常のファイアウォールとプロキシ（セキュアWebゲートウェイなど）で構成される従来のセキュリティインフラに多大なストレスがかかることです。トラフィックの増加に応じて、企業はハードウェアを追加または強化して拡張する必要があります。そうしないと、ユーザーのパフォーマンスが大幅に低下してしまいます。

企業は選択を迫られています。Microsoft 365またはGoogle Workspace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込むのかという選択です。そして現状では多くの企業が、Microsoft 365またはGoogle Workspaceトラフィックがプロキシなどの従来のセキュリティレイヤーをバイパスしてユーザーと直接接続することを許しているのです。しかしこのアプローチでは、攻撃者にとって重大なセキュリティ上の障壁が排除されることになり、攻撃者がネットワークに侵入できるようになってしまいます。

セキュリティへの最新のアプローチ：ゼロトラスト

ゼロトラストアーキテクチャの中核となるのは、いかなるトラフィックも信頼しないという考え方です。すべてのブラウザーベースのインターネットトラフィックを悪意のあるものとして扱い、Webトラフィックをエンドポイントデバイスから分離する必要があります。このアプローチは包括的であり、検知をベースとしたセキュリティに由来する多くの問題を取り除きます。しかし、これまでの一般的なゼロトラストには、大きな管理上の負荷がかかっていました。組織は、ユーザーのデバイスがインターネットに接続するすべてのポイントで、複雑で高価なハードウェアまたはソフトウェアクライアントを導入展開して管理しなければならなかったのです。これでは、高度に分散した環境ではうまく拡張させることができません。

メリット

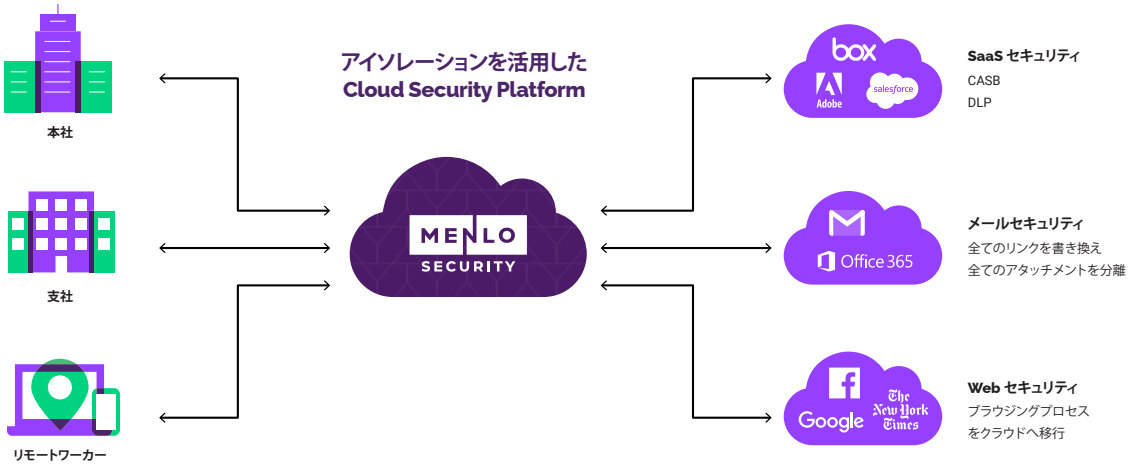
ユーザーへの脅威となるマルウェアを排除します

ユーザーとオフィススイートの間の直接の接続を有効にします

安全で低遅延の接続をグローバルに提供して、ユーザーエクスペリエンスを最適化します

メンロ・セキュリティが起こした革新：アイソレーションを活用したプラットフォーム

メンロ・セキュリティはゼロトラストアプローチを採用しており、Menlo Security Cloud Platformを通じてスケーラブルで簡単に実装できるソリューションとして提供します。Isolation Core™を活用するMenlo Security Platformは、クリックした時点で許可かブロックかを決定するのではなく、クラウド上に構築した独立したセキュリティレイヤーを使ってすべてのトラフィックをエンドユーザーのデバイスから遠く離れた場所に分離し、悪意のあるトラフィックをブロックします。Webコンテンツが良いものか悪いものか、カテゴリ分けできるかどうかは関係ありません。アイソレーションを活用したプラットフォームは、すべてのトラフィックに悪意があると仮定し、その前提で適切に取り扱います。また、このプラットフォームはクラウド上にあるため、非常に柔軟で迅速です。組織のクラウドと同じ規模にスケーリングし、ユーザー数やビジネスサイクル、そしてトラフィック量の変化に迅速に対応します。



Menlo Security Platformを使用すれば、ユーザーはWebメールやGoogle Workspace、またはMicrosoft 365ドキュメント内の任意のリンクを自由にクリックすることができ、それによるパフォーマンスへの影響や感染のリスクはありません

プラットフォームを通過したトラフィックには、ユーザーのデバイスにマルウェアを配信する手段は残されていません。アイソレーションレイヤーはクラウド上のサービスとして提供されるため、オフィスプラットフォームにアクセスする場所や方法に関係なく、世界中のユーザーを等しく保護します。

Solution Brief

クラウドトランスフォーメーションを推進します

企業がGoogle WorkspaceまたはMicrosoft 365のどちらを利用しているとしても、ユーザーはこれらのオフィススイートに確実かつ安全にアクセスできる必要があり、それはどこから業務を行っていようが関係ありません。しかし残念ながら、サイバーセキュリティにおける従来型の検知ベースのアプローチには、これらのほぼユビキタスなプラットフォームを使用してシステムを侵害する攻撃者を阻止するための手段が用意されていません。それらの代わりに、企業は業務を保護するための現代的なアプローチを採用しなければなりません。Isolation Core™を活用するMenlo Security Platformは、マルウェアやその他のWebベースの攻撃がGoogle WorkspaceやMicrosoft 365を経由してエンドポイントに到達するのを防ぎ、業務を保護するためのゼロトラストアプローチを可能にします。そしてそれを、ユーザーがアプリケーションを利用する際のエクスペリエンスに影響を与えずに行います。

メンロ・セキュリティがどのように業務を保護するのかをご確認ください。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。

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。