データシート

Menlo SecurityのWebセキュリティ—Isolation Core™を備えたセキュアWebゲートウェイ

Webトラフィックのセキュリティ保護とマルウェアの排除

業務システムはクラウドへの移行が進んでいるものの、従来のサイバーセキュリティソリューションは、クラウド向けに設計されておらず、最新のWebマルウェア攻撃からユーザーを保護できていません。解決策となるのは、Isolation Core™を備えたMenlo SecurityのセキュアWebゲートウェイ（SWG）によるセキュアなクラウドアクセスです。

クラウドトランスフォーメーションに伴う大きな課題

ユーザーが企業ネットワークから離れた場所で行っている作業の量が、企業ネットワークで行っている作業の量を初めて上回ったとき、クラウドトランスフォーメーションが達成されたことになります。この大きな転換によって、セキュリティポイントが中央だけにある従来のハブアンドスポークのネットワークアーキテクチャモデルを見直す必要性が発生します。これは、SaaSプラットフォームやWebアプリケーションによって生じるトラフィックパターンの変化（具体的には、全体的なネットワーク使用パターンと永続的な接続）によるものです。

残念ながら、既存のネットワークスタック（ファイアウォールやセキュアWebゲートウェイなど）では、このようなトラフィックパターンの変化には対応できないため、企業のセキュリティ体制に大きな死角が残ります。セキュリティチームは、組織に流入および組織から流出するWebトラフィックに対する可視性と制御を失い、さらにユーザーの操作性が根本的に変わることで、IT関連の予算に多大な影響をもたらします。

こうしたアーキテクチャ上の課題があることとは別に、インターネットは西部開拓時代のような状態にあります。というのも、今日でも事実上あらゆるWebサイト、リンク、Web広告が、マルウェアの配信に使われるからです。Web上のすべてのものにアクセスできるようにすることも、逆にインターネットへのアクセスを制限することも、非生産的であり、既に大きな負担のかかっているITサポートチームに、さらに無理を強いることにもなります。セキュリティの専門家が安全なコンテンツと悪意のあるコンテンツを簡単に区別できる方法はないため、組織はリスクにさらされ、ユーザーの生産性が妨げられているのです。

今日のサイバーセキュリティ環境：

- クラウドトランスフォーメーションによって、クラウドの業務システムに対するユーザーのアクセス方法が変わります。
- 従来のネットワークおよびセキュリティのアーキテクチャはクラウド向けに設計されておらず、Webユーザーを保護するのは困難です。
- ユーザーは、フィッシングやソーシャルメディア攻撃、認証情報窃取、その他最新のWebマルウェア攻撃の犠牲になっており、ユーザーや組織は危険にさらされています。

業務システムはクラウドへの移行が進んでいるものの、従来のサイバーセキュリティソリューションは、クラウド向けに設計されておらず、最新のWebマルウェア攻撃からユーザーを保護できていません。

解決策となるのは、Isolation Core™を備えたMenlo SecurityのセキュアWebゲートウェイ（SWG）によるセキュアなクラウドアクセスです。

脅威はクラウドアクセスに対応して進化を継続

従来のセキュアWebゲートウェイ（SWG）ソリューションでも、企業がインターネットのコンテンツをポリシーに基づいて許可またはブロックすることはできますが、どれをブロックしてどれを許可すればよいのかを、いったいどうやって判断すればよいのでしょうか。また、レガシなSWGは、検知／対応型のセキュリティアプローチに基づいていますが、既知の脅威しか特定できず、ますます高度化しているサイバー攻撃に対応していくことは事実上不可能です。さらに、レガシなSWGでは、異常を検知するために、脅威インテリジェンスデータベースからの不確かなリスクデータやシグネチャに依存したり、挙動監視機能が使用されたりしているため、誤検知や検知漏れ、検知できるようになるまでの遅延が生じます。動的コンテンツは、現在一般にアクセスされているサイトの大半で使用されていますが、そのことがセキュリティ対策の追従を困難にしているのです。

さらに、今日のサイバーセキュリティの脅威から企業を保護するには、Webとメールに関するユーザーの行動についてはもちろん、脅威と脆弱性についての深い洞察とコンテキストも必要です。セキュリティアナリストや脅威の検知／対応チームは、攻撃発生時にユーザーがどのような行動をとっていたかを正確に知る必要があります。しかし、ユーザーの行動に対する可視性の確保は、仮に方法が存在したとしても、困難なものです。

Webセキュリティやマルウェア対策に対する既存のアプローチは、無計画なツールの導入、セキュリティチームの過剰な負担を生じさせ、非効果的で費用もかかります。Webベースの攻撃は非常に頻繁に発生しており、成功もしています。今日の脅威およびクラウドトランスフォーメーションの課題には、ネットワークアーキテクチャに対する根本的な再検討、つまりクラウド向けに設計されSaaSアプリケーションをサポートするアーキテクチャへの置き替えが必要なことは明白です。

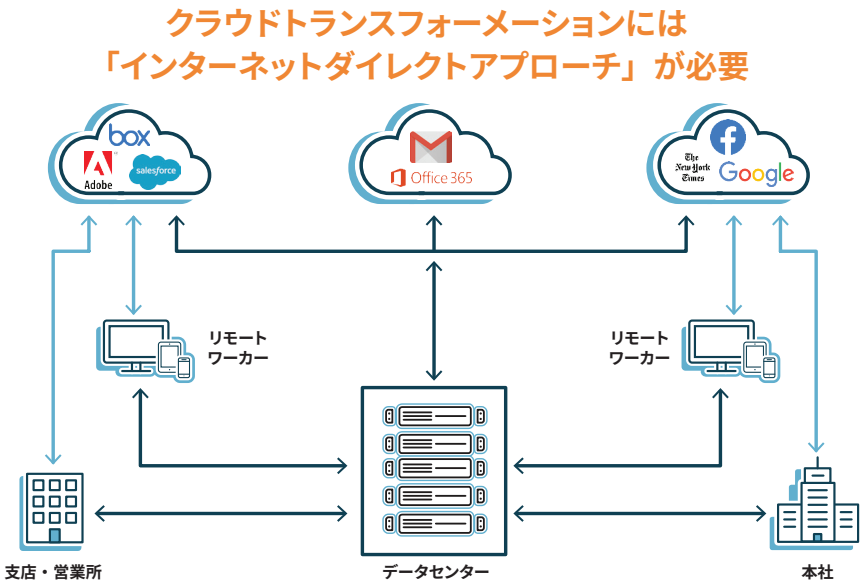


図1：クラウドトランスフォーメーションでは、従来のトラフィックパターンに対処して、企業がユーザーにセキュアなインターネットアクセスを提供する方法を再検討することが必要になります。

アイソレーションコアを備えたMenlo SecurityのSWG

アイソレーションコアを備えたMenlo SecurityのセキュアWebゲートウェイは、セキュアなクラウドトランスフォーメーションを実現するために企業が必要とする機能を提供します。グローバルエラスティッククラウドからサービスとして提供されるMenlo SecurityのSWGによって、ユーザーはどこで業務を行っていたとしてもインターネットに安全に接続できるようになります。企業では、Webベースのサイバー脅威からの保護、きめ細かなアクセスポリシーとセキュリティポリシーの適用、Webトラフィックの制御、監視および保護、データ漏洩と認証情報窃取の防止、クラウドアプリケーションの安全性、すべての機器と場所にわたるコンプライアンスの徹底、これらが保証されるようになります。Menlo SecurityのSWGは、比類のないパフォーマンスとスケールでこれらを実現します。

Menlo Securityのアイソレーションコアは、すべてのWebコンテンツにはリスクがあり、潜在的に悪意のあるコンテンツをホストしている、ということを前提にして動作します。これにより、許可するかブロックするかを粗っぽい分類や詳細な分析によって判断する必要がなくなります。その代わりに、アイソレーションするかブロックするかのポリシーを使用します。許可されたコンテンツに対し、Menlo SecurityのAdaptive Clientless Rendering™（ACR）が、ユーザーの操作性や生産性に影響を与えることなく、また特別なクライアントソフトウェア／プラグインを必要とすることもなく、許可されたコンテンツをエンドユーザーのブラウザーに効率的に配信します。これによって、エンドユーザーが生産性を損なうことなく安心してクリック、ダウンロード、ブラウジングといった操作を行えるだけでなく、セキュリティチームがセキュリティ体制における100パーセントの信頼度を回復することができます。

Menlo Security Cloud Platform：

- SaaS用に設計された安全なインターネットダイレクトアーキテクチャを提供します。
- ユーザー数、デバイス数、アプリケーション数の増加に合わせてセキュリティと帯域幅を自動スケーリングします。
- データ保護のためにセキュリティの制御機能と可視性を集約します。

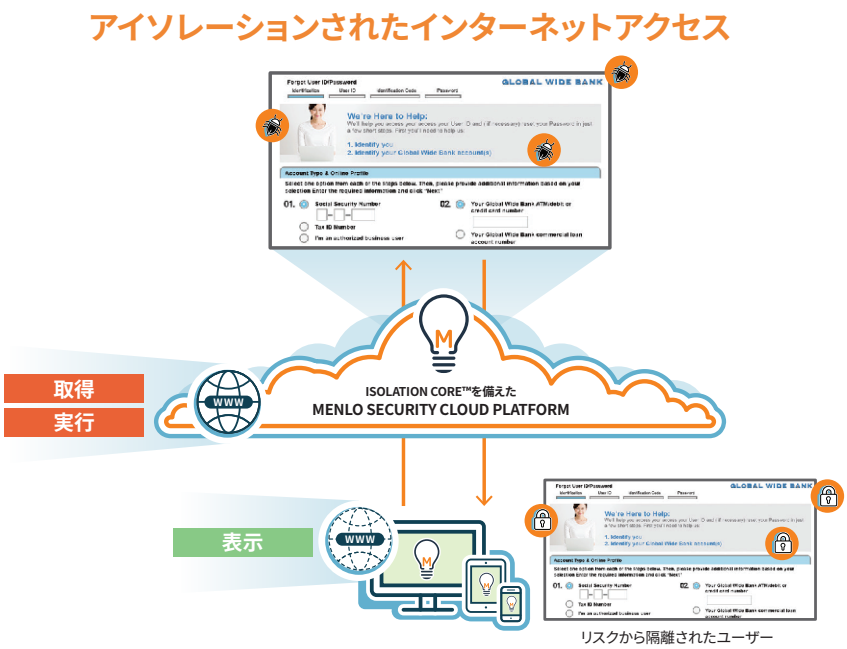


図2：Menlo Security Cloud Platform

アイソレーションを備えたMenlo Security Cloud Platform

メールセキュリティ

- リンクと添付ファイルを自動でアイソレーション
- 未知のフィッシングサイトやランサムウェア攻撃からユーザーを保護
- リスクのあるWebフォームの読み取り専用バージョンを用いて認証情報窃取を防止
- クリック時に、フィッシング攻撃についてユーザーに警告

Webセキュリティ

- 水飲み場型攻撃を始めとするWebベースの脅威を排除
- 攻撃を気にすることなく、インターネット全体へ自由なアクセスを確保
- プロキシベースのソリューションが有する従来のWebアクセス制御を継続使用
- ハードウェアベースのアプライアンスを使用することなくスケーラブルなHTTPSインスペクションを実行

脅威防御

- すべてのWebコンテンツに悪意があることを前提として、あらゆる脅威をアイソレーション
- 既知の脅威をネットワークに侵入してくる前にクラウドベースのサンドボックスで実行および分析
- ドキュメントやファイルを読み取り専用モードでレンダリング
- 既知の脅威を防ぐために既存の検知／対応技術を活用

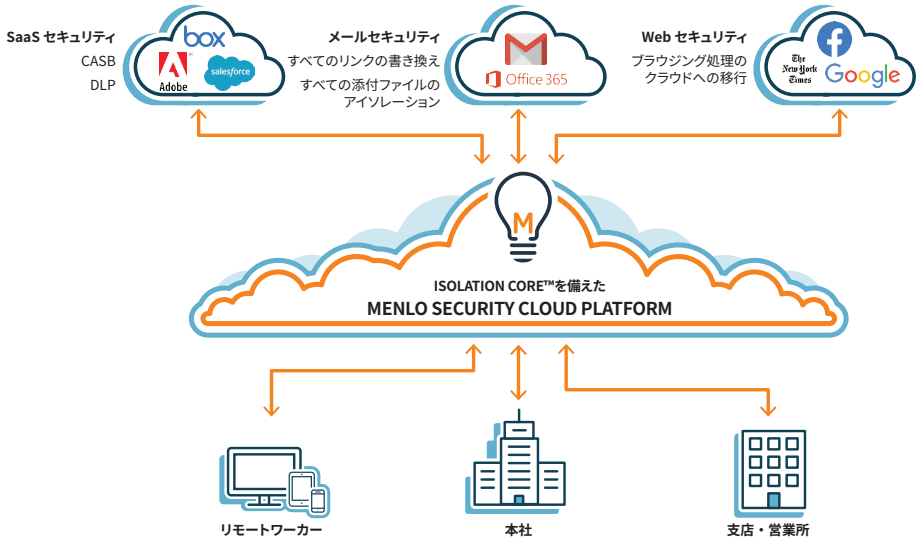
データ保護

- データ漏洩から組織を保護
- クラウドベースのDLPを通じ、企業に流入するデータと企業から流出するデータに対する可視性を確保
- ワンクリックでCloud Access Security Broker（CASB）機能を提供
- 既知および未知のクラウドアプリケーションに対してユーザーアクセスを検出および制御

グローバルエラスティッククラウド

- ユーザーがどこで業務を行っていても、セキュアなインターネットアクセスを確保
- 本来のブラウジングの操作性を変えることなく、一貫したパフォーマンスを確保
- 増加するグローバルユーザーベースをサポート
- 複数の地域にわたり、一貫してインターネットへのアクセス制御とポリシーを適用

Menlo Securityはセキュアクラウドトランスフォーメーションを提供



結論

クラウドトランスフォーメーションの時代が到来した今、ユーザーはどこで業務を行っていても、SaaSプラットフォーム、Webアプリケーション、リッチメディアのWebサイトに、安全かつ確実にアクセスできる必要があります。アイソレーションコアを備えたMenlo SecurityのセキュアWebゲートウェイは、セキュアなWebアクセスを提供します。パフォーマンスに影響を与えることも、本来のWebブラウジングの操作性を変えることもありません。それと同時に、IT部門は運用コストを抑えながら、現時点での実際の需要の減少や流れに応じてクラウドのセキュリティサービスを調整することができます。Menlo Securityは、組織に流入するトラフィックや組織から流出するトラフィックを保護しながらクラウドトランスフォーメーションを実現し、組織が迅速な革新と、絶えず変化する顧客の要求への対応を継続的に実現できるようにします。

詳細については、www.menlosecurity.jpをご覧になるかjapan@menlosecurity.comにメールでお問い合わせください。

アイソレーションコアを備えたMenlo SecurityのセキュアWebゲートウェイは、パフォーマンスに影響を与えることも、本来のWebブラウジングの操作性を変えることもなくセキュアなWebアクセスを提供します。

Menlo Securityについて

Menlo Securityは、Web、ドキュメント、メールからマルウェアの脅威を排除することによって、組織をサイバー攻撃から保護します。Menlo Securityは、グローバル2000に名を連ねる何百社もの企業と主要な政府機関におけるセキュアクラウドトランスフォーメーションの達成を支援してきました。Menlo SecurityのCloud Security Platformは、拡張性に優れており、あらゆる規模の企業に包括的な保護を実現します。エンドポイントソフトウェアは不要で、エンドユーザーの操作性にも影響しません。Menlo Securityは、ガートナーセキュアWebゲートウェイ（SWG）についてのマジック・クアドラントでビジョナリーに選出されています。

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