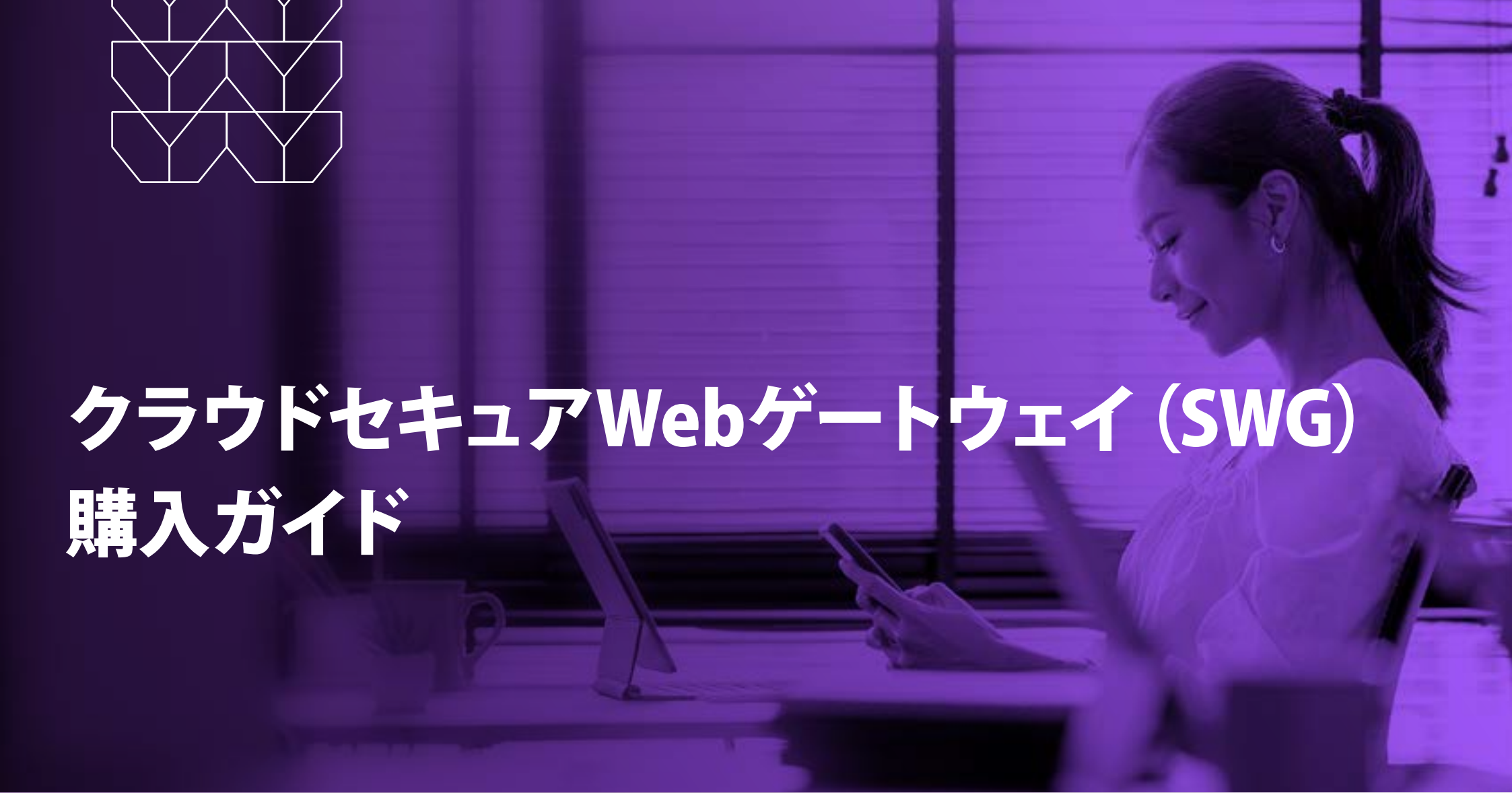

クラウドセキュアWebゲートウェイ（SWG）購入ガイド

eBook

MENLO SECURITY

目次

現代の働き方

これからの働き方はさらなる分散へ

ユーザーは今後も社内ネットワークだけでなく、安全性が低いWiFiを使う家庭やコーヒーショップなどの場所から、企業が提供した個人用デバイスを使用するでしょう。

9/10

の経営幹部が、今後もハイブリッドモデルが続くと考えています[1]

20%

の従業員が完全にリモートです[2]

仕事のあるところに脅威もついてくる

80% **従業員の80%が、業務のためにインターネットを使っています[3]**

90% **侵害の90%はインターネットが原因です[4]**

75% **従業員は業務時間の75%をブラウザーで行っています[5]**

Webアプリへの依存が増えています

box Office 365 salesforce

Webの脅威は高度化・有効化へ

ITの意思決定者によると、攻撃者は攻撃の成果を高めるために、事前に標的について調査を行うようになっています。[6]

66%

が、セキュリティにおける最大の懸念事項としてランサムウェアを挙げています

57%

は、フィッシングを最大の脅威と考えています

52%

の回答者が、マルウェアを最も懸念しています

1 https://www.mckinsey.com/business-functions/organization/our-insights/what-executives-are-saying-about-the-future-of-hybrid-work
2 https://www.weforum.org/agenda/2021/07/work-form-home-hybrid-working-covid-pandemic-us-office/
3 https://www.statista.com/statistics/1114434/worldwide-adults-with-internet-access-employment/
4 https://info.menlosecurity.com/Solving-Your-Trust-Issues-with-SASE_webinar.html
5 https://cloud.google.com/blog/products/chrome-enterprise/chrome-is-helping-it-teams-support-cloud-first-workforce
6 Enterprise Cybersecurity Plans in a Post-Pandemic World

働き方の変化

そしてそれは、従来型のセキュリティ境界を押し広げます

モバイルユーザーやあちこちに分散したユーザーが企業のセキュリティ境界外からデータセンターアプリケーション、Webアプリ、Software-as-a-Service（SaaS）プラットフォームやWebサイトにアクセスすることは、今では珍しいことでは無く、あたりまえのことになっています。これらの新しい働き方は可能性に満ちており、エンドユーザーに多大なメリットをもたらし、ビジネスの継続性も高めます。しかし、従来型のオンプレミスのセキュリティソリューションをそのまま使用しながら生産性とセキュリティのバランスをとろうとすると、最終的には過去の環境と新しい状況が不整合を起こし、セキュリティ上の問題が発生することになります。

在宅勤務ブームが到来した当初、企業は社内システムへの安全なアクセスを提供するために、VPNを使ってインターネットトラフィックを本社や集中データセンターにバックホールしていました。しかしこの方法では遅延が発生したり帯域幅が不足したりするため、いつでもログインできる高速でシームレスな業務環境を期待していた従業員にとって大きな問題になったのです。大量のトラフィックのためにVPN機器がうまく機能しなくなると、企業は攻撃対象の拡大に対処するために従来型のセキュアWebゲートウェイ（SWG）を使用するようになりました。

しかしこれは戦略的に間違っており、従来型のSWGは急増するインターネットトラフィックのボリュームとリモートワークを保護することができず、その代わりに非効率性を生み出してしまい、企業は構成と管理の手間がかかる追加のハードウェアを導入する必要に迫られました。

クラウドデータセンターは助けにならない

スケーラビリティや可用性の課題が明らかになっており、セキュリティおよびネットワークベンダーは迅速に対応しようとしています。クラウドへの移行にあたって、多くの企業はそれまで使っていたシステム（仮想化されたリモートアクセス、セキュリティ、ネットワーキングアプライアンス）を、統合されたクラウドネイティブなプラットフォームに作り変えるのではなく、そのままパブリッククラウドに押し込むことを選択しました。しかし計算集約的な機能の場合には、クラウド事業者のコンテンツ配信ネットワークが大量に持つエッジロケーションで実行することができません。そのため、ただでさえ分散が進んでいるユーザーから、さらに遠い場所からセキュリティを提供することになります。

受け身では無く、ラジカルに

従来型のサイバーセキュリティソリューションは、Webサイトが安全かどうかを判断するために、決定論的なロジックを使用しています。この「○か×か」の二元的なアプローチは信頼性に欠け、脅威をどのように分類するかによってセキュリティ上の問題を生じる可能性があります。Webサイトやマルウェアが急増し高度化していることを考えると、この受動的なアプローチはもう限界です。ベンダーはサンドボックスや新しい人工知能（AI）や機械学習（ML）の技術が問題を自動で解決すると主張していますが、基本的には人間の介入と大量の脅威データを必要とするため、これらの手法も本質的には受動的いうことができます。

クラウドベースのセキュアWebゲートウェイ：

ユーザーを守る最新のアプローチ

どのSWGが最適なのかを見極める

現代の高度に分散した、どこからでも業務ができる環境で、すべてのSWGソリューションがうまく機能するわけではありません。新規にSWGの導入を検討する場合、最新の配信モデルをサポートするだけでは変革は望めません。そうではなく、攻撃者が検知を回避して認証情報を盗んだり、エンドポイントを侵害したり、ネットワーク内で横展開したりする結果を引き起こす「検知と対処」のアプローチから抜け出す必要があります。

セキュリティは業務を邪魔するのでは無く、効率を上げるためのもの

従業員は、FacebookやYouTubeなどのサイトを個人的に利用するなど、ブラウジングに際して自由度を求めています。しかし従来型のSWGは、ユーザーがアクセスしたいサイトの利用を禁止するような包括的な「許可かブロックか」のポリシーを使用する傾向があります。さらに混乱を招くのは、このような時代遅れの方法では、ビジネスに不可欠ではあるものの、悪意を持つ可能性もある「未分類」のWebサイトにもアクセスできなくなってしまうことです。このような事態が発生すると、多くの場合ITチケットが発行され、対応コストが増加し、すべての関係者が不満を感じます。またユーザーは禁止を回避することができるため、結局のところ、このセキュリティ対策は安全を保証するものではありません。例えばあるWebサイトへのアクセスが禁止された場合、ユーザーは別のデバイスからアクセスしようとするかもしれず、そこで悪意のあるコンテンツにアクセスして認証情報が盗まれるかも知れません。

デジタルトランスフォーメーションへの取り組みを加速させるために、既知および未知、そして未来の脅威に打ち勝ち、生産性を守ることができる、以下の6つの機能と利点を備えたクラウド専用のSWGを検討してください：

1. クラウドスケーラブルなアイソレーション
2. Secure Access Service Edge (SASE) との互換性
3. ゼロトラスト
4. 未来への対応
5. 見えないセキュリティ
6. グローバルでスケーラブルなセキュリティ

1 クラウドスケーラブルなアイソレーションを備えたSWG

クラウド上でスケール可能なアイソレーションを備えたSWGは、これまでとは根本的に異なるアプローチにより、企業が安全にクラウドへ移行するために必要な機能を提供します。それは、業務が行われている場所すべてにセキュリティを提供し、マルウェアが侵入する前に無力化することです。

SWGは、すべてのWebコンテンツにリスクがあり、組織に危険をもたらす可能性を持つと想定しているため、これまでのように分類やフィルタリング、メンテナンスが大変なポリシーを使って「許可かブロックか」の判断を行う必要がありません。また、クラウドベースのプラットフォームのため、IT管理者やセキュリティ管理者は、すべてのユーザーに対してセキュリティやアクセスのポリシーを簡単かつ集中的に設定することができ、きめ細かい制御が可能になります。組織の規模やニーズが変化しても、アイソレーションは企業やユーザーのニーズに合わせて自動的にスケールします。

エンドユーザーに気づかれないセキュリティ

エージェントやプラグインのインストールが不要で、スクロールや操作も遅延無くスムーズなため、アイソレーションレイヤー内で操作しているユーザーは、SWGに守られていることに気づきません。

アイソレーションにより、すべてのユーザーが安全かつシームレス、そして実用的にインターネットを利用できます。セキュリティのために生産性を犠牲にするのではなく、アイソレーションを使うべきです。

2 SASEとの互換性を備え、将来のアーキテクチャにも対応

Gartner®によると「2025年までに、企業の少なくとも60%は、ユーザー、ブランチ、エッジ・アクセスを対象としたSASE採用に向けた明示的な戦略とタイムラインを作成する（2020年は10%）」ということです[7]

SASEとは何か？そして、それはどのようにセキュリティを強化するのか？

SASEは、Software-Defined Wide Area Network（SD-WAN）の機能と、セキュアWebゲートウェイ（SWG）、Cloud Access Security Broker（CASB）、Firewall-as-a-Service（FWaaS）、Zero Trust Network Access（ZTNA）などのネットワークセキュリティの機能を緊密に統合しています。またSASEは5Gなどの接続性とも統合されており、現代において業務を安全に行うことを目指す企業のダイナミックでセキュアなアクセスへのニーズをサポートするフレームワークを提供します。

SASEへの集約が成熟し進化し続ける中で、企業は、将来のアーキテクチャを決定する上で、接続性よりもセキュリティが重要な設計ポイントになるという認識を持つようになっています。

SASEのセキュリティモデルは、いくつかの点で有用です。

1. クラウドベースのインフラを利用して、セキュリティサービスを容易に導入し、提供できる
2. セキュリティスタックを統合することで、IT部門が管理、更新、維持しなければならないセキュリティ製品の数を最小限に抑えることができる
3. 信頼を前提とせず、完全なセッション保護を実現する
4. 機密データへの不正アクセスや不正使用を防止する

SASE導入の旅は、クラウドベースのSWGと共に始める

Gartnerによると、多くの企業のSASE導入には数年かかるということです。しかし、私たちの働き方の変化は、すでにコンピューティング環境やエンドユーザーに影響を与え始めています。つまりほとんどの企業は、SASEフレームワークの完全な導入を待っている余裕はないということです。SASEの一時的な代替として、クラウド型のSWGは管理しやすい出発点となり、SASEと同じメリットを多く提供し、将来のSASE導入へ向けての準備とすることができます。このため、SWGの導入を検討する際には、それがSASEアーキテクチャの導入とアップグレードの計画に合っているかどうかを確認してください。

クラウドベースのSWGのフレームワークがSASEスタックの他のコンポーネントと連携しているかどうかを確認し、アプローチを統一することを検討してください。これには、以下と統合できるかどうかも含まれます：

- Zero Trust Network Access（ZTNA）
- Cloud Access Security Broker（CASB）
- Remote Browser Isolation（RBI）
- Cloud DLP
- クラウドファイアウォールの機能

これらを緊密に統合することにより、ユーザーは、必要なツールや情報に安全かつシームレスにアクセスできるかどうかを心配することなく、生産性の高い仕事をすることができます。その一方でITチームは、SASEのセキュリティコンポーネント全体の集中管理やポリシー作成が可能になり、より良い可視性を得ることができます。

7 Source:Gartner, "2021 Strategic Roadmap for SASE Convergence", Neil MacDonald, Nat Smith, Lawrence Orans, Joe Skorupa, 25 March 2021.
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission

3 ゼロトラストは必須の要件

SASEとは何か？そして、それはどのようにセキュリティを強化するのか？

ゼロトラストは、Gartnerが提唱するSASEの基本要素の一つです。そして、クラウド型SWGの差別化要素でもあります。ホワイトハウスがゼロトラストアプローチへの移行を指示したため、サイバーセキュリティの未来におけるゼロトラストの重要性がかつてなく高まっています。今後、政府機関がクラウドを使う際には、サイバーインシデントの予防、検知、評価、修復ができるような方法で行う必要があります。

2021年5月12日のブリーフィングでは、ゼロトラストアプローチは暗黙の信頼を排除することで従来のネットワーク境界の内外を問わず脅威から保護することができ、アクセスやその他のシステム対応の可否を判断するために、複数のソースからの継続的な検証を必要とすることを明確にしています。[8] そうした条件の下でユーザーにアクセス権が与えられますが、その範囲は業務を遂行するのに必要な最低限の範囲に限られます。

ハイブリッドユーザーのためのセキュリティ

ゼロトラストのアプローチは広範囲に影響するため、ハイブリッドユーザーのパズルを解くためには欠かせない要素となります。ゼロトラストでは、ユーザー、デバイス、ネットワーク接続、データなど、すべてのものを信頼できないと考えるため、ユーザーが移動する際には、一貫したセキュリティ体制も一緒に動かす必要があります。

アイソレーションを活用したクラウドベースのSWGは、ユーザーのネイティブなブラウジング体験を維持するゼロトラストアプローチを実現します。

「悪いものを見つける」必要を無くす

多くのベンダーがゼロトラストアプローチを採用していると主張していますが、すべてが同じ機能を持つわけではありません。そのベンダーがどのようにアーキテクチャを適用しているかを検証し、以下の点を確認するようにしてください：

- 脅威を防止するために受動的に「悪いものを見つける」必要がないこと
- ユーザーを、マルウェアが侵入する可能性のある場所から離れた、安全な場所に保つことができること
- データだけで無く、ユーザーとデバイスの両方が信頼されていないとみなされるよう、双方向で動作すること

より緊密な統合により、ユーザーは必要なツールや情報に安全かつシームレスにアクセスできるかどうかを心配することなく、生産性の高い作業を行うことができます。その一方でITチームは、SASEのセキュリティコンポーネントを一元的に管理し、ポリシーを作成し、全体を可視化することができます。

8 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

4 未来への対応

グローバルな業務環境は今後も分散したままであることが予想されるため、ベンダーは新しい環境をサポートするためにSWGを適切に近代化する必要があります。
現在のニーズを満たし、将来の課題も克服できる、十分な柔軟性を備えたSWGを選択するためには、いくつかの重要な要素に注目しておく必要があります：

将来の変化に対応できること

ゼロトラストのアプローチは広範囲に影響するため、ハイブリッドユーザーのパズルを解くためには欠かせない要素となります。ゼロトラストでは、ユーザー、デバイス、ネットワーク接続、データなど、すべてのものを信頼できないと考えるため、ユーザーが移動する際には、一貫したセキュリティ体制も一緒に移動させる必要があります。

一部改修や置き換えの必要が無いこと

クラウドへの全面的な移行は、一夜にしてできるものではありません。ほとんどの場合、移行には数年を要します。SWGが既存のセキュリティインフラで動作し、将来的に状況が変化した場合でも追加機能を購入する必要がないことを確認してください。

何があってもすべてのユーザーを保護すること

何年経っても、高速で安全、かつ信頼性の高いアクセスが必要であることに変わりはありません。しかし、接続する人、アクセスする場所やネットワーク、デバイスは変わる可能性があります。SWGは、ハードウェアを新たに導入することなく、スイッチを切り替えるだけで迅速に拡大・縮小できる必要があります。これにより、企業はWebベースのサイバー脅威から保護され、きめ細かなアクセス制御とコンプライアンスの遵守がすべてのデバイスと場所に一貫して適用されることになります。

未来の脅威に備えること

私たち自身、業務環境、そして未来の攻撃を取り巻く世界は、常に変化しています。クラウドベースのSWGは、検知と対処のアプローチから脱却し、次に何が起こるかわからない状況でも、確実な保護を提供できるように取り組むべきです。アイソレーションとゼロトラストにより、脅威がさらに高度化しても、今と同様にプロアクティブに保護することができます。特定の脅威情報やシグネチャの更新に頼る必要はありません。

5 ユーザーを取り囲む「見えないセキュリティ」

最新のクラウドベースのSWGを導入することで、セキュリティを強化するだけでなく生産性を向上させることができます

最新のSWGを導入することで、完全なセキュリティとポジティブなエンドユーザー体験を実現します：

ユーザーにネイティブで安全なブラウジング体験を提供：アクセスを単純に拒否するのではなく、アイソレーションによってネイティブなブラウジング体験を維持できるSWGを検討してください。Webブラウザーは、特別なクライアントソフトウェアのインストールや追加のハードウェアを必要とせず、遅延もなく、意図された通りに動作しなければなりません。そしてユーザーは、フォームへの入力、ドキュメントの安全な表示/ダウンロード、カット、コピー、ペースト、印刷などの標準的な機能をいつもどおりに利用できなければなりません。

ユーザーを取り囲む保護層：検知と対処のアプローチでは、攻撃や脅威、または攻撃の兆候を確認したときには、攻撃者がすでにエンドポイントを侵害していたり、横方向に拡散し始めている可能性があります。クラウドSWGでは、攻撃に事後的に対応するのではなく、そもそもユーザーに攻撃が届かないようにする必要があります。アイソレーションにより、ユーザーはWebを閲覧する際に目に見えない保護層に囲まれて操作することになり、既知で既存の脅威や未知で高度な未来の脅威を阻止することができます。

Webやドキュメントのアイソレーション機能には以下のようなものがあります：

- ユーザーの一部ではなく、すべてのユーザーを対象にできるスケーラビリティ
- JavaScriptやFlashなどの危険なコンテンツを安全に表示することができる、クラウドベースのリモートブラウザー
- CPUパワーを消費しない電力効率の高いレンダリング
- ステートレスWebセッションを使用して、ネイティブWebコンテンツを破棄可能なコンテナで処理
- ファイルタイプやユーザーに応じてWeb操作やドキュメントへのアクセスを制限する、きめ細かいポリシー設定
- エンドポイントから離れたクラウド上でドキュメントを安全に表示
- 安全でサニタイズされた再現性の高いオリジナルファイルを提供することで、デスクトップおよびモバイルデバイスでの印刷、検索、コピー/ペースト、共有が可能

すべての人にポジティブな体験を

SWGの管理体験も、ユーザー体験と同じくらい重要です。ITチームは以下のことをできる必要があります：

すべての Web トラフィックを監視：暗号化された Web トラフィックと暗号化されていない Web トラフィックを完全に検査することで、セキュリティチームはユーザーと彼らが使用する Web ベースのツールとの間のコミュニケーションを可視化し、組織を標的とする脅威の詳細を知ることができます。

帯域幅をインテリジェントに制限： ユーザー/グループポリシーにより、ブラウザーセッション内の帯域幅をインテリジェントに制御することができます（例：ビデオ再生解像度の制限など）。しかし、サイトの他の側面に制限をかけてユーザー体験を低下させるようなことはありません。

6 グローバルでスケーラブルなセキュリティ

完全なSASEソフトウェアスタックであっても、スケーラビリティは保証されていません。
SWGを検討する際には、オプションが統一されたSASEソフトウェアスタックで構築されているかを確認してください。そうすることで、セキュリティとネットワーク機能がコンテキストを共有することができます。

ユーザーが新しい場所で業務を行う場合にセキュリティの適用範囲を拡大することは、長い間、時間と手間のかかるプロセスでした。ベンダーを選定し、契約を締結し、ハードウェアを設置し、設定を完了するまでに数ヶ月を要することもあります。その間、業務は悪意のある攻撃にさらされる可能性があります。

企業のデータセンターの外でも、セキュリティ上の問題は付いて回ります。企業はネットワークベンダーやセキュリティベンダー同様、業務が行われているあらゆる場所にセキュリティを提供するためには、多くの場合、莫大な計算量を必要とすることに気付いています。また業務やリソースが分散しているため、常に遅延の問題に悩まされ、セキュリティ目標を達成できないこともあります。

パフォーマンスを低下させずに真のグローバル化とスケーラビリティを実現するためには、今のSWGを、すべてが統一されたクラウドネイティブなプラットフォームに作り変えなければなりません。そして、すべてのユーザーがどこからでも、どのようなデバイスからでも接続できるように、最小の遅延でルーティングし、自動的にスケーリングできる必要があります。

ワンタッチで、ユーザーのいる場所にセキュリティを提供

ユーザーはもはやデータセンター内には居ないのですから、セキュリティもデータセンターの壁の中にとどまるべきではありません。SWGを選択する際には、セキュリティをユーザーのいるエッジに近づけることができるかどうかが重要です。エンドユーザーこそが新たな境界であり、ワークロードとユーザーが常に変化していることを考えると、セキュリティチームがこれまで経験してきたような時間のかかるプロセスを必要とせず、グローバルにスケールできる柔軟性を備えたカバレッジが必要です。

クラウド経由でグローバルにスケール

- 新しいハードウェアや仮想マシンを導入展開する必要はありません
- 追加の設定も必要ありません
- 新たなベンダーも必要ありません
- 新しい契約書も必要ありません

生産性を守り、脅威に打ち勝つための **シンプルな選択**

ユーザー、働く場所、そして脅威が変化し続ける中で、組織に適したクラウドSWGを選択することは、ビジネス上の重要な決断です。メンロ・セキュリティはそれをシンプルにします。

Elastic Isolation Core™を活用したメンロ・セキュリティのSWGは、SWGのすべての機能をひとつのクラウドネイティブなプラットフォーム（CASB、DLP、RBI、FWaaS、Private Accessを含む）に集約し、拡張可能なAPIとポリシー管理、レポート作成、脅威分析のための単一のインターフェイスを提供します。

メンロ・セキュリティは、SASEセキュリティの約束を実現する唯一のソリューションとして、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ます。エンドユーザーがオンラインで仕事をしている間、セキュリティは見えず、セキュリティチームの運用負担を軽減します。

「許可かブロックか」のアプローチと決別

メンロ・セキュリティのSWGは、企業がすべてのユーザーに対して常にアイソレートまたはアイソレート/読み取り専用のポリシーを適用することを可能にし、これまでの検知と対処に頼る受動的なアプローチとは対照的に、セキュリティに対する真のプロアクティブなアプローチを可能にします。許可されたコンテンツについては、メンロ・セキュリティのAdaptive Clientless Rendering™ （ACR）技術により、ユーザー体験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やプラグインを必要とすることなく、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。その結果、セキュリティチームはセキュリティ体制を100%信頼することができ、エンドユーザーは安心してクリック、ダウンロード、ブラウジングを行うことができ、生産性を向上させます。

柔軟な導入展開オプション

メンロ・セキュリティは自社のCloud Security Platform上で数百万人のユーザーを保護しています。メンロ・セキュリティのSWGは、すべての組織のニーズを満たすために、オンプレミスでのホスティングやクラウドサービスとしての提供など、柔軟な導入展開オプションを提供しています。そして既存のネットワークインフラと統合し、あらゆるデバイスをサポートすることで、お客様のアーキテクチャやエンドユーザーにシームレスに適応するセキュリティを実現します。

メンロ・セキュリティで脅威を完全に排除

クラウドネイティブでスケーラブル、そして拡張可能な、他に類を見ないアイソレーションを活用したセキュリティプラットフォームで、生産性と安全性を守ります。

https://www.menlosecurity.com/ja-jp/

www.menlosecurity.com/ja-jp/

MENLO SECURITY