

Menlo Securityで ゼロトラストアクセスを容易に実現

ゼロトラストアクセスアーキテクチャを完成させ、
リモートユーザーの業務環境を整えます: ネットワークの
再構築やファイアウォールを更新する必要はありません

ゼロトラストの世界は複雑

ゼロトラストモデルは、認可されたユーザーのみがアプリケーションやシステム、そして情報にアクセスするという前提で設計されています。そこに「暗黙の信頼」という概念はありません。すべてのユーザーおよびデバイス、データ、ネットワーク接続を検証する必要があります。ゼロトラストにより、組織は静的な境界型のセキュリティから、利用ユーザー、資産、リソースに重点を置くフレームワークに移行することができます。従業員、パートナー、契約社員は、働く場所や使用するデバイスに関係なく、業務に必要なアプリケーションにアクセスする必要があるため、この変化はリモートワークにおいてこれまで以上に必要になっています。

組織は10年以上に渡って、どのようにゼロトラストを導入すれば良いかを考えてきました。しかし残念ながら、従来型のツールによるゼロトラストの導入は複雑性が高く、多くのケースで制限が発生します。これらの課題には以下が含まれます:

- **複雑な実装:** セキュリティチームとITチームは、ゼロトラストを導入する前に、組織内のどこにデータがあるのかを把握しておく必要があります。SaaSの爆発的な普及に伴い、データがプライベートデータセンターの外に移動しているため、このようなデータの棚卸しは特に困難になる場合があります。そして、BYODのユースケースが増加していることで、複雑さがさらに増します。
- **高コスト:** データの所在をマッピングし、従来型のゼロトラストプロジェクトを推進するためには、インフラストラクチャの再構築が必要になる場合があり、コストがかかる可能性があります。
- **生産性の低下:** 特定のポリシーやワークフローが、従業員の業務プロセスを阻害する可能性があります。従業員や契約社員は、日々の業務のために様々なアプリケーションにアクセスする必要がありますが、適切でない、あるいは誤ったアクセスポリシーは生産性を低下させるため、従業員が不満を感じる可能性があります。

ブラウザ経由でアクセス可能なアプリケーションが増えているため、組織はWebトラフィックとインタラクションにゼロトラスト原則を適用する必要があります。しかしゼロトラストアーキテクチャがブラウザにまで拡張されていなければ、真のゼロトラストを実現できたと言うことはできません。また、今日の働き手は契約社員やBYODユーザーで構成されることが多く、アプリケーションアクセスにゼロトラスト原則を適用することの重要性と必要性はさらに増えています。

アプリケーションアクセスにゼロトラストを実装するための鍵

組織は、回避的な脅威からブラウザベースのアプリケーションを保護しつつ、従来型の技術のコストと複雑さを緩和できるソリューションを必要としています。ソリューションには以下が求められます：

- ・ リモートアクセスのサポート
- ・ BYODおよびサードパーティアクセスの有効化
- ・ サイバー脅威のリスクを軽減
- ・ ユーザーアクションの可視性の向上
- ・ 容易な導入展開と管理

Menlo Securityによるゼロトラストアクセス

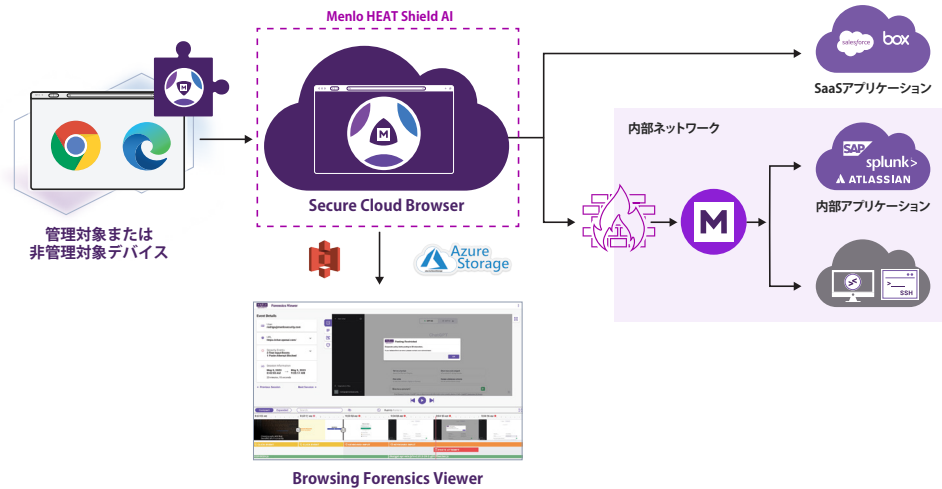
Menlo Secure Application Accessは、ゼロトラストアクセスを簡素化してITの複雑さを軽減し、プライベートアプリケーションやSaaSアプリケーションへのシームレスでセキュアなアクセスを可能にします。

さらに、アクセスはネットワーク全体にではなく、ユーザーの業務に必要な特定のアプリケーションに対してのみ許可されます。Menlo Secure Application Accessの基盤にはゼロトラスト原則が組み込まれており、広範囲に分散したユーザーやサードパーティに対しても、きめ細かく条件付きのアクセスポリシーを適用することができます。組織は、ユーザー、グループ、ソースIP、および地域ごとにアクセスを定義できます。

Menlo Secure Application Accessは、リモートアクセスとBYODユーザーを簡単にサポートするために、ブラウザベースのアプリケーションをゼロタッチかつエージェントレスで導入展開します。エージェントレスで簡単に導入できることで、組織には以下のようなメリットがあります：

- ・ さまざまなアプリケーションへのアクセスを、迅速にプロビジョニングおよびデプロビジョニングできます。これはユーザーにとって非常にセキュアな方法で行うことができ、ネットワークポロジやファイアウォールのルールを変更する必要はありません。
- ・ ハードウェアを追加する必要が無いため、低いコストと少ないメンテナンス作業でセキュアなアクセスを提供できます。
- ・ セキュアなアクセス手段を数分で導入展開できるため、組織のニーズに合わせて迅速に拡張することができます。

ブラウザベースでないアプリケーションを利用する場合には、Menlo Security Clientをインストールします。クライアントはクラウド版と同じインターフェースでアクセスを管理および監視し、同じアプリケーションへのアクセスをユーザーやグループごとに区別して提供できます。



ユーザーはアプリケーションに直接アクセスするのではなく、レンダリングされたアプリケーション画面に、ポータル内で、あるいはブラウザの拡張機能を通じて、安全にアクセスできます。

Secure Application Accessは、Menlo Secure Cloud Browserを基盤として構築されており、ユーザーのローカルブラウザの堅牢化されたデジタルツインをクラウド上に作成します。ユーザーがアプリケーションへのアクセスをリクエストすると、そのリクエストはSecure Cloud Browserに複製されて実行されるため、ユーザーのエンドポイントに存在するかもしれないあらゆる脅威からサーバーとデータが保護されます。またこれにより、パラメータの改ざんやWebスクレイピング、APIの不正使用などの潜在的な脅威からアプリケーションを守ります。

Secure Cloud Browserは、さらなる保護のためにサンドボックス化とAVスキャンも提供します。ユーザーが感染したファイルをアップロードした場合、Secure Cloud Browserは、そのファイルがアプリケーションに感染したり、その他の悪意のある活動を行ったりするのを阻止します。その後で、「クリーン」なリクエストがアプリケーションに送られます。サーバーから返されるコンテンツも同じ方法で処理され、すべてのアクティブコンテンツはユーザーのローカルブラウザではなく、Secure Cloud Browserでレンダリングされます。サーバーが侵害されるような稀な場合であっても、その脅威がユーザーに広がることはありません。

さらに強固に保護するために、アクセス前とアクセス中の両方でポスチャチェックを有効にして、ファイアウォールの状態、OSのバージョン、ディスク暗号化などの重要なデバイス基準を検証することができます。これらのチェックはCrowdStrikeと統合され、CrowdStrike Zero Trust Assessment (ZTA)スコアの有無などの追加要素を評価するエンドポイントポスチャチェックを可能にします。

Menlo Securityなら、組織はポスチャチェックのためにクライアントの導入を強制されることはありません。その代わりに、Managed Chromeを活用してクライアントレスでポスチャチェックを行うことができ、IT部門がChromeの設定を管理し、ブラウザのポスチャに基づいて権限を付与することができます。

組織は可視性を高めることで、ゼロトラストが正しく実装されているかどうかを確認することができます。しかし、ブラウジングセッションは長い間セキュリティチームやITチームにとって「死角」であったため、可視性を高めることができませんでした。Menlo SecurityのBrowsing Forensicsが、この問題を解決します。Browsing Forensicsを有効にすると、ブラウジングセッションがSecure Cloud Browserを通過する際にポリシーに基づいてセッションを記録することができます。ポリシーには特定のアプリケーションやユーザー、グループを含めることができるため、セキュリティおよびIT、コンプライアンス、監査の各チームは、ユーザーがどこにアクセスし、何をしたのかを最終的に確認することができます。



リードオンリー/リード・ライト、アップロード/ダウンロードなどのきめ細かな条件付きアクセスポリシー



ブラウザベースのアプリケーションをエージェントレスで簡単に導入展開



悪意のあるユーザーや感染したエンドポイントからアプリケーションを保護しながら、クリーンで安全なコンテンツのみをエンドポイントに配信



アプリケーション内のエンドユーザー行動の可視性を向上

ゼロトラストアクセスを容易に実現

Menlo Securityは、導入展開が容易でユーザーにも優しいソリューションでゼロトラストアクセスを実現します。パートナーや契約社員、BYOD社員などが業務を行えるようにすると同時に、ゼロトラストアクセスポリシーを強制適用し、Web脅威からの防御、ラストワンマイルまでのデータ保護を継続的に実現します。

人々の働き方を安全に守る方法について、詳しくはmenlosecurity.jpをご覧ください。また、japan@menlosecurity.comまでメールでお問い合わせください。



メンロ・セキュリティ・ジャパン株式会社

住所：〒100-0004 東京都千代田区大手町 1-6-1 大手町ビル 4F FINOLAB
Webサイト： <https://www.menlosecurity.jp>
お問い合わせ先： japan@menlosecurity.com