

Menlo Security Secure Application Access

Secure Cloud Browsing と
Global Private Access アーキテクチャによる
ゼロトラストアクセス



ゼロトラストアクセスへの
最短ルート

ミッションクリティカルな
アプリケーションとデータを
保護

どこからでも、中断無く
業務を行うことが可能

従来型のネットワークアクセスの課題

企業は、従来型のネットワークアクセスがもたらすコストや複雑性、そしてリスクに対応する必要があります。また、ゼロトラストアプローチにはネットワークインフラストラクチャの管理が必要となりますし、複雑なセキュリティサービスエッジ (SSE) の導入展開も行う必要があります。VPNやVDIなどの従来型のアプローチでは、その複雑なアーキテクチャやスケーラビリティ (拡張性) 上の制約により、ユーザーエクスペリエンスが劣悪になりがちです。また、ユーザーの行動に対する可視性が制限され、管理されていないデバイスへの過剰なアクセスをプロバイダーが提供してしまう可能性もあります。

Menlo Secure Application Access (SAA) : 企業アプリケーションとSaaSへの シンプルでセキュアなアクセス

ゼロトラストアクセスへの最短経路: セキュリティおよびITチームは、複雑でコストのかかるアーキテクチャ変更を行うことなく、数回クリックするだけで企業アプリケーションへの管理されたアクセスを提供できます。

ミッションクリティカルなアプリケーションとデータを保護: Menlo Secure Cloud Browser上に構築されたSAAは、ネットワークを分割し、感染したエンドポイント、脆弱なブラウザ、インターネットトラフィックなどからアプリケーションを常時保護します。Menlo Secure Cloud Browserではポリシーベースのデータ管理が適用されるため、機密データがエンドポイントに到達することはありません。

どこからでも、中断なく業務を行えます: ユーザーは、ポータルやブラウザの拡張機能を経由して、使い慣れたブラウザを使ってアプリケーションにアクセスできます。アプリケーションへは、任意のデバイスや場所から、ソフトウェアをインストールすることなくアクセスできます。

主なメリット

数分で設定できるカスタマイズ可能な制御で、Webアプリケーションのセキュリティを確保します。

従業員やコントラクターがデバイスにソフトウェアをインストールする必要は無く、ブラウザポータルや拡張機能を通じてアプリケーションにアクセスできます。

感染したデバイスや、データを流出させようとするユーザーなどから、アプリケーションとデータを保護します。

Menlo Securityは、アプリケーションへの最短ルートをユーザーに提供することで、遅延を削減し、生産性を向上させます。

アプリケーションへのルートがシンプルで効率的になることで、従来型の技術と比較して5倍から10倍のコスト削減を実現します。



主な機能

Webアプリケーションへのセキュアなアクセスを数分で設定

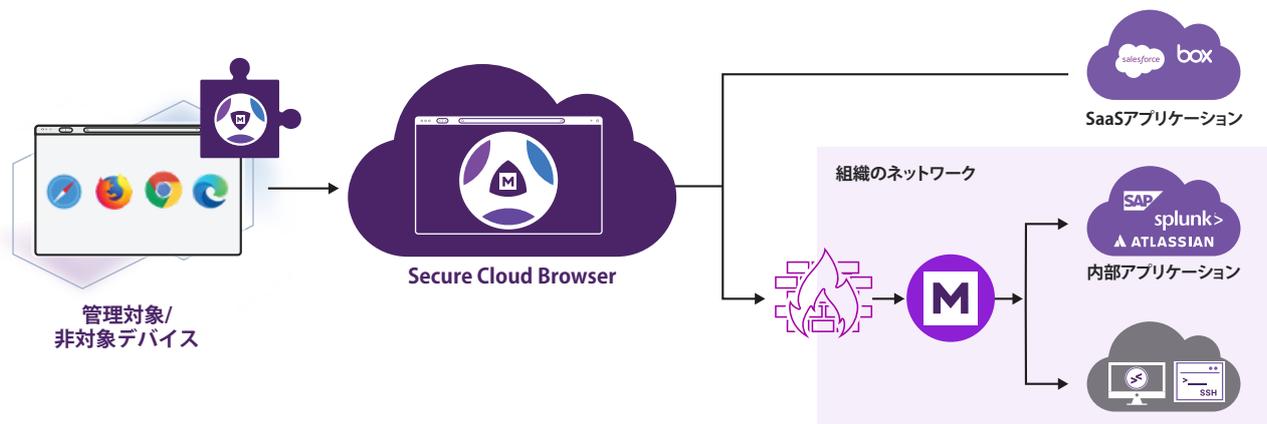
Menlo SAAは、インフラストラクチャを変更する必要が無く、エージェントも不要です。エージェントが不要な導入展開によって複雑さが軽減され、企業はアプリケーションへのセキュアなアクセスを迅速に提供できます。

- ネットワークの再構築やファイアウォールの更新の必要はありません
- DNSレコードを変更する必要はありません
- 証明書のインポートは不要です

脅威からアプリケーションとユーザーを保護

Menlo Secure Application Accessは、Menlo Secure Cloud Browserにより、クロスサイトスクリプティング、Cookieの盗用、セッションハイジャック、感染したファイルのアップロードなどのデスクトップの脅威から、ミッションクリティカルなアプリケーションとデータを保護します。

またSecure Cloud Browserは、HTMLスマグリングなどのコンテンツベースの攻撃とともに、信頼性に基づいてドメインをカテゴリ分けするWebフィルタを回避するLURE (レガシURLレピュテーション回避) 攻撃など、Webを介した脅威からもユーザーを保護します。エンドポイントが侵害された場合でも、攻撃者はデータに直接アクセスしたり、サーバーにリクエストを発行したりすることはできません。



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、ポータル内から、あるいはブラウザの拡張機能を通じて、レンダリングされたアプリケーション画面に安全にアクセスします



機密データをラストワンマイルまで保護

Secure Cloud Browserに実装されたラストマイルのデータ漏洩防止(DLP)機能により、機密データは組織の管理下に留まり、侵害されたエンドポイントや未認可のユーザーから保護されます。DLP機能には以下が含まれます:

- コピー/ペーストの制御
- リードオンリー/リードライトでWebサイトを制御
- Webアプリとファイルダウンロードのための電子透かし
- アップロードとダウンロードの制御
- データの不明瞭化
- 許可されたアップロードとダウンロードのためのDLP

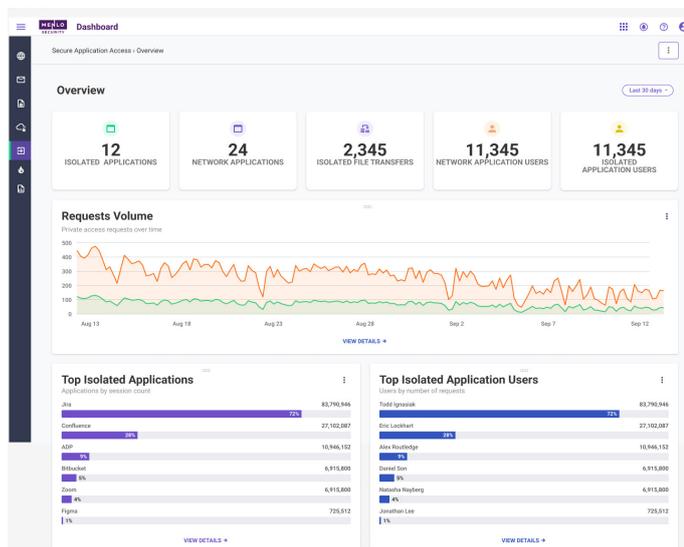
Menlo Secure Application Accessはクラウドベースのため、エンドポイントベースのアプリケーションアクセス技術とは異なり、デバイスに機密情報をダウンロードすることはありません。この機能により、攻撃者がデバイスのメモリに保存されたデータにアクセスすることを阻止します。

最小権限アクセスの適用

Menlo Secure Application Accessは、ユーザー、グループ、ソースIP、および地理的な場所によって定義された最小権限アクセスを適用します。Menlo SecurityのSAAは、ネットワークベースのサービスのようにネットワーク全体またはセグメント単位で制限するのではなく、利用するユーザーが必要とする特定のアプリケーションへのアクセスのみに制限します。従業員、パートナー、コントラクターには、明示的に認可されたアプリケーションのみが表示され、それらにしかアクセスすることはできません。

アプリケーションへのアクセスとユーザーアクションの可視化

Menlo SAAは、ブラウジング活動、ユーザー名、ソースロケーションなど、すべてのアプリケーションアクセスの詳細なログを記録し、セキュリティ監視を強化します。Menlo SAAは、SIEMやEDR/XDRなどの既存のセキュリティツールと統合できます。Menlo Browsing ForensicsはユーザーのWeb活動を完全に可視化し、より深い洞察を得ます。



Menlo SAAダッシュボードでは、最も頻繁にアクセスされるアプリケーションやDLP違反など、アプリケーションの使用状況の概要と傾向を表示します



従来型アプリケーションのサポート

Menlo SAAのMenlo Security Clientは、Web以外の従来型アプリケーションへもセキュアなアクセスを提供します。リモートアクセスのユースケースでは、Menlo Cloudを介したセキュアなトンネリングが可能です。

デバイスのポスチャチェック

Menlo Secure Application Accessは、アクセス前とアクセス中に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確認するポスチャチェックを行ってセキュリティを強化します。これらのチェックはCrowdStrikeと統合されており、CrowdStrikeの有無やZTAスコアなどの追加的な要素を評価するエンドポイントポスチャチェックを行えます。

Menlo Securityなら、企業はポスチャチェック用のクライアントを導入展開する必要はありません。その代わりに、Managed Chromeを使っ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部門はChromeの設定を管理し、デバイスのポスチャに基づいて権限を付与することができます。

包括的なデバイスサポート

ユーザーは管理対象か否かに関わらず、モバイルを含む任意のデバイスの既存のブラウザから、アプリケーションにアクセスすることができます。

ゼロトラストをトランスフォーム：リスクを低減しながらアクセスを簡素化

Menlo Secure Application Accessは、ブラウザセキュリティとグローバルなプライベートアクセスクラウドをベースにしたユーザー中心のゼロトラストアーキテクチャにより、アプリケーションのセキュリティに革命をもたらします。



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