MENLO SECURITY

セキュアなアプリケーションアクセスを実現する、VPN置き換えの現代的なアプローチ

仮想プライベートネットワーク（VPN）の限界を Menlo Secure Application Accessで克服

過去にセキュアなリモートアクセスを必要としていたのは、勤務時間外に業務を行うユーザーやモバイルユーザーだけでした。しかし今では、私たち全員がハイブリッドアクセスとゼロトラストアクセスを利用して業務を行っています。

リモートアクセスはかつて、メールクライアントが仮想プライベートネットワーク（VPN）ゲートウェイを介してサーバーに接続することに重点を置いていました。しかし多くのVPNゲートウェイは、その複雑さや高いコスト、そして克服できないセキュリティリスクが指摘されたために、取り残されてしまっています。また、今ではメールだけでなく、ユーザーが業務に使用するすべてのアプリケーションにアクセスできるようにしなければなりません。

この新しいハイブリッドな業務モデルが一般化したことでデジタルトランスフォーメーションが進展し、SaaS（Software as a Service）プラットフォームへの移行が加速しています。ユーザー、アプリケーション、データ、エンドポイントがインターネットを介して接続されるようになっており、プライベートネットワークインフラストラクチャ内にあるわけでは無いのです。このようなモデルでは、VPNゲートウェイはほとんど価値を提供できません。クラウドVPNと高価なクラウドネットワークサービスは、古い「ネットワーク接続」モデルを単に置き換えただけのものだからです。最新のアプローチを採用することで、アプリケーションへのセキュアなアクセスとゼロトラストポリシーの適用が大幅に向上します。

SOLUTION BRIEF

世界的なパンデミックによって、開発から数十年経ったVPNテクノロジーの限界が露呈し、それからすでに数年が経過しました。VPNの利用が急激に拡大した結果、処理が遅延したり操作にタイムラグが生じたりしてユーザーエクスペリエンスが低下したため、拡張性に関わる問題が指摘されました。また、ユーザーのリモートワークへの移行が急激だったため、外部からアクセスできるようにするために特定の重要なアプリケーションをインターネット上に置くことを余儀なくされた組織もありました。しかしDMZにアプリケーションを配置するのは危険な行為です。ユーザーは業務の遂行に必要なアプリケーションにアクセスできるようにはなりましたが、それと同時に攻撃対象も大幅に拡大することになりました。

VPNのもうひとつの問題は、その基本的な仕組みにあります。VPNは、ユーザーを特定のアプリケーションではなく、ネットワーク全体に接続してしまいます。多要素認証（MFA）が実装されていない場合（残念ながら多くの環境でこの機能が欠如しています）、攻撃者は巧妙に仕組まれたフィッシングキャンペーンによって窃取したユーザー認証情報を使ってVPNに侵入し、他の認証プロセスを経ることなく、あらゆるビジネスシステムにアクセスすることができます。Colonial Pipelineへのランサムウェア攻撃で起きたのは、まさにこれでした。2022年5月、ハッカー集団のDarkSideが、侵害されたVPNパスワードを使ってColonial Pipelineのネットワークにアクセスしました。このグループはそのアクセス権限を使ってネットワークのインフラストラクチャを横方向に移動し、データを盗み、ネットワークにランサムウェアを感染させました。

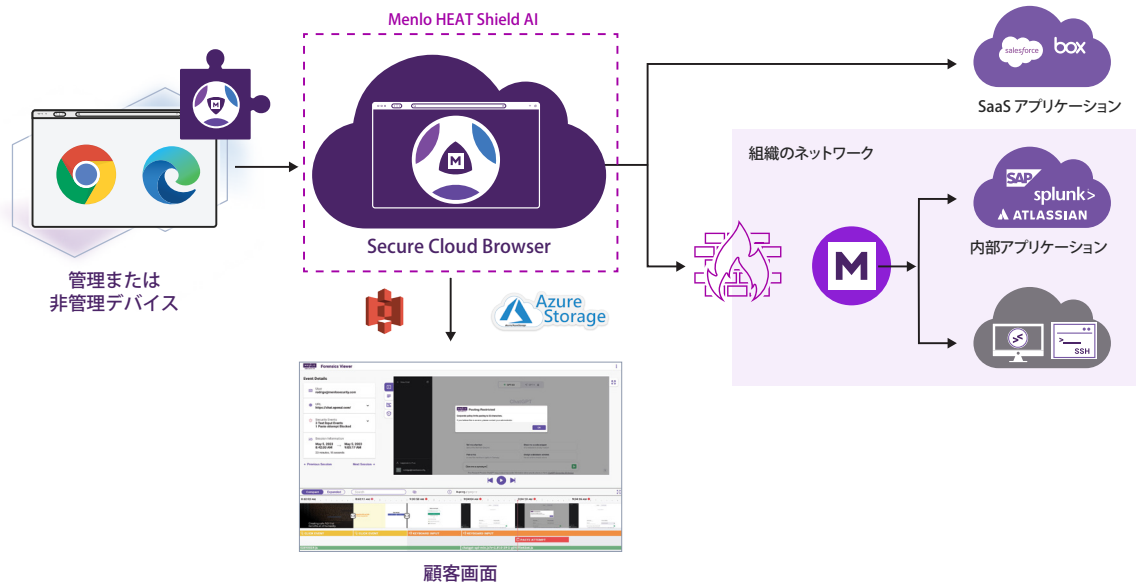
MFAが実装されていればこの攻撃を阻止できたかもしれませんが、最近のいくつかのMFAバイパス攻撃で見られるように、MFAでさえも回避される可能性があります。さらに、VPNはインターネットに直接接続されているため、常時主要な脅威の標的となります。

ユーザーが実際に必要としているのは特定のアプリケーションへのアクセスですが、一部のVPNにはネットワークアクセスそのものを拡張してしまうという、一般的なリスクを超えた脆弱性を持つものがあります。Ivantiは2024年の最初の数カ月の間に、Connect Secure VPNデバイスに関わる5つの重大な脆弱性（CVE-2023-56805、CVE-2024-21887、CVE-2024-21893、CVE-2024-21888、CVE-2024-22024）を公開する必要がありました。

複数の脅威インテリジェンスによれば、これらの脆弱性のうち3つは現在も悪用されており、ひとたび侵入された場合、これらの脆弱性によって攻撃者は重要な財務、人事、エンジニアリングシステムを含む組織のネットワーク全体に自由にアクセスできるようになります。さらに、VPNは暗号化されているため、ユーザーの行動を可視化することができません。

今こそ、最新のソリューションが必要です

セキュリティチームとエンタープライズアーキテクトは、VPNに代わるソリューションを探していました。代替案の多くは複雑でコストがかかり、新たなリスクをもたらすことすらあります。認証や認可など、アクセスやセキュリティに特定の要素をプロビジョニングするアプローチもありますが、可視性に欠けています。Menlo Securityが提供するSecure Application Accessは、シンプルで効率的、かつコスト効率に優れたセキュアなアクセスを提供し、ゼロトラストポリシーを適用することができます。



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。

Menlo Secure Application Access と Browsing Forensics

Menlo Secure Application AccessとMenlo Browsing Forensicsを組み合わせることで、ユーザーセッションとトランザクションを完全に可視化したセキュアなリモートアクセスを実現できます。Menlo Secure Application Accessは、認可されたアプリケーションのダッシュボードを各ユーザーに提供します。Menlo Securityは、ネットワークをすべて開放するのではなく、代わりにアプリケーションごとのアクセスを提供することで、ネットワークの分離を維持します。Browsing Forensicsを使用すると、ネットワーク指向のアプローチの複雑さや転送時のセキュリティによるトレードオフなしに、TLSで暗号化されたWebアプリを可視化できます。

Secure Application AccessとBrowsing Forensicsを組み合わせることで、ユーザーはゼロトラストポリシーの範囲内で、どこからでも簡単に業務を行えるようになります。個々のユーザーセッションの記録は、インシデントの分析と対応、コンプライアンスの遵守、脅威の探索に必要な可視性を提供します。ユーザーは、ポータルまたはブラウザ拡張機能で表示されるダッシュボードからアプリケーションを起動するだけです。

Menlo Secure Application Accessは、Menlo Secure Cloud Browser経由でアプリケーションと通信することでアプリケーションを保護します。ユーザーは目的のサーバーに直接アクセスする代わりに、Menlo Securityのクラウドブラウザにアクセスします。クラウドブラウザがアプリケーションの画面をレンダリング（描画）して安全なコンテンツのみを配信するため、ユーザーのローカルブラウザは安全です。ローカルブラウザとクラウドブラウザの組み合わせは、ユーザーにアクセス手段だけでなく、コンテンツベースの攻撃からの保護も提供するのです。

また、Secure Cloud Browserはネットワークの分離を維持し、AIが主導する保護機能によってすべてのリクエストを検査します。このアーキテクチャにより、パラメータの改ざん、Webスクレイピング、APIの不正使用、およびその他多くの問題を含む可能性のある、ユーザー側からの悪意のあるリクエストからアプリケーションを保護します。エンドポイントを侵害できたとしても、攻撃者はサーバーに直接アクセスしてリクエストを送ることはできません。すべてのアプリケーションリクエストは、エンドポイントのブラウザではなく、Menlo Secure Cloud Browserから行われます。

ブラウザの脆弱性を保護するために、Menlo Secure Application Accessは以下を行います：

- 組織は認可された正規のアクセスを提供すると同時に、インターネットからアプリケーションを隠すことができます。
- ネットワークではなく、特定のアプリケーションへのアクセスを提供します。この制御により、アプリケーションを保護するだけでなく、横方向の移動を阻止します。
- 不正アクセスによる攻撃を防止します。
- プロトコル操作、セッションハイジャック、クッキーの窃取による攻撃から防御します。

さらにMenlo Secure Application Accessは、ユーザーとアプリケーションの間で共有されるすべてのコンテンツに対して、サンドボックス化とアンチウイルススキャンを適用します。ユーザーが感染したファイルをアップロードした場合、Menlo Secure Application Accessはそのファイルがアプリケーションに感染したり、悪意のある活動を行ったりするのを阻止します。

これらのアプリケーションが保持する貴重なデータを包括的に保護するために、Menlo Secure Application Accessにはデータセキュリティ制御のレイヤーが追加されています。これらの制御は、コンプライアンスの遵守やデータ漏洩防止（DLP）に役立ちます：

- ダウンロード/アップロードの制御
- リードオンリー/リードライトポリシー
- アプリケーションおよび文書の電子透かし
- データの不明瞭化
- コピー/ペーストの制御

Secure Application Accessのシンプルなアーキテクチャとブラウザフォレンジックスの組み合わせにより、導入展開にかかる時間の短縮とセキュリティ強化を実現し、エンドユーザー、管理者、インフラストラクチャおよびネットワークチームのエクスペリエンスが向上します。

ブラウザ経由でアクセスできるアプリケーションの数は増え続けていますが、組織には直接アクセスする必要のあるレガシーアプリケーションがまだ残っているかもしれません。ブラウザベースと非ブラウザベースの両方のアプリケーションへの安全なアクセスを提供するために、Menlo Securityは柔軟な導入展開オプションを用意しています。Menlo Security Clientは、従来型のクライアントサーバーアプリケーションでも使用することができるため、すべてが最新のアプリケーションアーキテクチャに移行するまでの間も、エンドユーザーはアプリケーションにアクセスすることができます。

Menlo Browsing Forensicsは、スクリーンキャプチャ、ユーザー入力などを含んだ可視性という、もう1つの画期的な属性を提供します。この可視性は、パートナーやコントラクタ、合併/買収活動に関与するユーザーなどのサードパーティユーザーを考慮する場合に特に重要です。セキュリティチームは、Browsing Forensicsによって収集された情報を活用して、アクセス制御モデルが適用されていること、アプリケーションが適切に使用されていることを確認したり、監視リストに載っているユーザーなど、リスクの高いユーザーの活動を監視したりすることができます。Browsing Forensicsはまた、曖昧さを排除した深いレベルの洞察を効率的に提供します。

Secure Application AccessとBrowsing Forensicsを組み合わせることで、組織はVPNを置き換え、従業員とサードパーティに必要なコンテンツのみへのアクセスを提供し、セッション中のアクションを完全に可視化することができます。同時に、組織はセッション中のユーザーの行動を完全に可視化することができます。

メリット

ネットワークセグメントまたはネットワーク全体ではなく、特定のアプリケーションのみへのアクセスを提供します。

ダウンロード/アップロード、リードオンリー/リードライト、コピー/ペーストの制御を含むラストマイルのデータ保護に加え、電子透かしやデータの不明瞭化も可能です。

ユーザーセッションをキャプチャしてコンプライアンス要件が強制適用されていることを確認し、Webセッションとユーザー操作の記録を自動的に保存します。

ブラウザ上の操作を可視化することでセキュリティアナリストがその意図を読み取れるため、セキュリティインシデントを迅速に解決できます。

ネットワークトポロジやファイアウォールのルールを変更せずに、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。

ブラウザベースのアプリケーションにはゼロタッチかつエージェントレスで導入展開することができ、ブラウザベースのアプリケーション以外ではエージェントを利用できます。

組織がパンデミックの間も業務を継続することができたのは、従来型のVPNインフラストラクチャのおかげです。しかし、それと同時にこの数十年前のテクノロジーに関する新たなセキュリティ上の懸念やパフォーマンス問題も浮かび上がりました。組織には、よりシンプルでセキュアな代替手段が必要なのです。Menlo Secure Application AccessおよびBrowsing Forensicsは、現代の分散した労働力のための最適なソリューションを提供します。

人々の働き方を安全に守る方法について、詳しくはmenlosecurity.jpをご覧いただくか、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