

Menlo Secure Application Accessで Virtual Desktop Infrastructure (VDI) を刷新

コストを削減しながら従業員のアクセシビリティの
問題に対処

今日の働き手のニーズ

今日の世界では、さまざまな個人やリモートワーカー、短期契約の契約社員などがアプリケーションにアクセスして業務を行う必要があります。そしてこれらの従業員やサードパーティは、どこで仕事をするかに関係なく、アプリケーションへの安全で信頼できるアクセス手段を必要としています。それと同時にセキュリティチームとITチームは、これらのアプリケーションで使用される機密データが悪用されたり、信頼できないデバイスに流出したりしないように保護する必要があります。真に効果的であるためには、今日の働き手向けのセキュリティは次のようなものでなければなりません：

- **スケーラブル**：組織は、場所を問わず、ユーザートラフィックの急激な変化に対応できる必要があります。
- **ゼロトラスト**：従来型の検知と対応ツールの「死角」が攻撃の成功につながらないように、テクノロジーアーキテクチャを構築する必要があります。
- **コンバージド**：ソリューション機能は、メールやWebなど複数のセキュリティニーズをサポートし、ラストマイルのデータ漏洩防止 (DLP) 機能を提供する必要があります。
- **ハイパフォーマンス**：セキュリティチームとITチームは、アプリケーションアクセスソリューションがシームレスなユーザーエクスペリエンスを提供することを保証する必要があります。

今日の働き手にとってのVDIのデメリット

1990年代から2000年代にかけて組織の運営方法を変革したのは、リモートデスクトップやシンクライアントコンピューティング、そしてVDIといった技術でした。VDIは強固なセキュリティと柔軟性を低コストで提供し、多くの従業員が安価なマシンで業務を行えるようになりました。これが従来型のワークステーションやデスクトップ環境に対する優位性でした。VDIはリモートアクセス用のVPNを代替または補完して仮想化された業務環境を提供できるため、リモートワーカーのサポートにも役立ちました。

しかし、ブラウザベースのアプリケーションが普及するにつれ、VDIはもはやこのような優位性を提供できなくなり、その一方で課題が明らかになっています。それでも、多くの組織は依然としてVDIシステムを使用しているため、セキュリティチームとITチームは不満を感じており、より高度で柔軟性が高く、コスト効率に優れたアプローチへの移行を訴えています。

VDIのデメリット

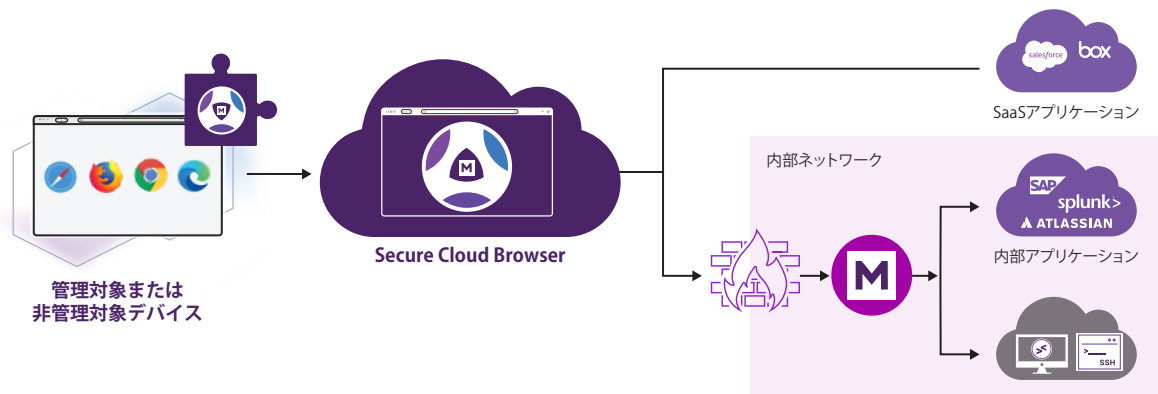
- **コストが高く、大量のリソースが必要:** VDIには多額の先行投資が必要で、導入後も継続的なコストが必要であり、それはユーザー1人あたり1,000~4,000ドルと報告されています。高額なライセンス費用に加え、ハードウェア、ソフトウェア、ストレージ、コンピューティングリソース、帯域幅、継続的なメンテナンスにかかる費用も発生します。
- **高い複雑性:** VDIの導入展開にはさまざまなコンポーネントが含まれるため、トラブルシューティングと保守が困難かつ複雑になります。
- **セキュリティ上の懸念:** VDIは公開されたサーバーで稼働するため、攻撃の標的となっており、攻撃者が組織内を横方向に移動するメカニズムを提供してきました。プロトコルは成熟しており、最新の認証とトランスポートセキュリティが適用されていますが、これらのサーバーもまた、脅威に対抗するためにパッチを適用し監視する必要があるシステムの1つです。高度に回避的な脅威は、VDIシステムを利用して永続的なプレゼンスを確立し、侵害を行います。
- **ユーザーエクスペリエンスの低下:** ロケーションやエンドポイントのリソース、あるいはネットワーク接続環境によっては、VDIを使う場合のユーザーエクスペリエンスは最適とは言えない場合があります。

Menlo Secure Application Access

Menlo Secure Application Accessは、ゼロトラストアクセスを簡単に実現し、コスト効率が高くセキュアなアプリケーションへの経路を提供します。

Menlo Secure Application Accessは、従業員と契約社員にWebアプリケーションと従来型のアプリケーションの両方を含むプライベートアプリケーションへのセキュアな接続を提供します。Secure Application Accessの中核は、ユーザーのエンドポイントと内部のアプリケーションおよびデータの間に位置するMenlo Secure Cloud Browserです。ここに配置することで、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VDIでは対処できないその他の多くの問題からアプリケーションを保護することができます。

SOLUTION BRIEF Menlo Secure Application AccessでVirtual Desktop Infrastructure (VDI) を刷新



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を使用すると、組織はアプリケーションアクセスに次のようなゼロトラスト原則を適用できます：

- ・ 悪意のあるユーザーからの保護
- ・ 利用ユーザー数、利用グループ数、ソースIP数、ロケーションに基づくアクセス
- ・ ポスチャチェック
- ・ アップロードの検査とブロック

Secure Application Accessにより、組織はきめ細かなラストマイルのDLP制御によってデータを保護できます。これらの制御により、セキュリティチームとITチームは、データ漏洩を心配することなく、パートナー、契約社員、リモートワーカーにアプリケーションへのアクセスを提供できます。これらの制御には以下が含まれます：

- ・ 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、コピー/ペーストの制御
- ・ アップロードとダウンロードに対するDLP制限
- ・ 電子透かし
- ・ データの不明瞭化

Secure Application Accessにより、組織は柔軟で簡単な導入オプションを使用してコストを削減できます。VDIに多額なコストをかける代わりに、組織は次の機能により、あらゆるデバイスのあらゆるブラウザから安全なアクセスを実現できます：

- ・ ブラウザベースのアプリケーション向けには、クライアントレスかつゼロタッチで導入展開
- ・ すべてのアプリケーションを設定してモニタリングする、使いやすい管理コンソール
- ・ レイテンシとコストを削減する、シンプルでありながらセキュアなアーキテクチャ

メリット



堅牢なセキュリティにより、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ます。



導入展開、監視、設定が容易です。



5-10倍のコスト削減が可能です。

ゼロトラストアクセスを簡単に実現

変化するVDI環境に組織が追従していく中で、従来型のアプローチが今日の働き手のニーズに適合しなくなっていることは明らかです。Menlo Securityは、コストを削減しながら、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アクセスを保護するためにゼロトラストアプローチを採用しており、組織がユーザーとデータを保護しながらシームレスなユーザーエクスペリエンスを提供できるよう支援します。

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