MENLO SECURITY

ゼロトラストアクセス
BYODセキュリティ
VDIの削減
VPNの置き換え

Menlo Secure Application Access

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、ゼロトラストへの取り組みを加速

IT 環境の大きなトレンドが示している通り、従来型のネットワークベースのアプリケーションアクセステクノロジーは明らかに老朽化しており、多くの組織がその現実に直面しています：

- パンデミック後の業務環境の劇的な変化を踏まえ、ゼロトラストの必要性が高まっています。
- VPNやVDIのような従来型のテクノロジーはユーザーエクスペリエンスにおいて劣ることが多く、トラフィックに対するセキュリティ上の可視性が制限され、管理されていないデバイスへの導入展開が煩雑になります。
- アプリケーションがWebベースのアクセスに移行するペースが速く、Webブラウザが主要なアクセステクノロジーとなっています。
- Webベースの脅威はますます巧妙化しており、AIとDevOpsの手法を活用して急速に変化し拡散します。

Menlo Secure Application Accessは、管理対象および非管理対象デバイスに対して、社内およびWebベースのアプリケーションとデータへの、ポリシーに基づくアクセスを提供します。アクセスが許可されるアプリケーションやWebサイトは、Webポータルやブラウザ拡張機能を通じて、見やすいタイル形式またはリスト形式で表示されます。Webベースでない従来型のアプリケーションへは、クライアントを追加してアクセスとセキュリティ制御を提供します。Menlo Secure Cloud Browserにより、社内およびインターネット上のWebプロパティへの安全なアクセスが保証されます。ユーザーは、エンタープライズアプリケーションやSaaSアプリケーションに直接アクセスするのではなく、Secure Cloud Browserを経由して接続します。これにより、侵害されたエンドポイントがエンタープライズアプリケーションからデータを盗み出そうとするのを防ぎ、侵害されたサーバーからの悪意のあるコンテンツがエンドポイントを悪用するのを防ぎます。

SOLUTION BRIEF

ゼロトラストアクセス

課題

まず、ゼロトラストの基本原則について考えてみましょう：

- ユーザーとデバイスの検証と認証
- 最小権限アクセス
- 継続的なモニタリングと再検証

デジタルトランスフォーメーションが進むにつれ、より多くのアプリケーションがクラウドに移行し、ハイブリッドな業務形態が普及したことで、ゼロトラストネットワークアクセス（ZTNA）がセキュリティの標準となりました。しかし現代においては、ゼロトラスト原則が場所に関係なく「何も信頼しない」ことを義務付けており、ユーザーには必要なアプリケーションへのアクセスのみを許可することに重点が置かれるようになっています。ZTNAはゼロトラストアクセス（ZTA）へと進化したのです。

現在、ほとんどのユーザーが業務アプリケーションにアクセスするための主要なメカニズムとして使っているのは、Webブラウザです。しかしゼロトラストソリューションの中には、そのブラウザを完全に保護できないものがあります。

Menlo Securityのソリューション

現在市場に出回っている他のゼロトラストアクセスソリューションとは異なり、Menlo Secure Application Accessは導入展開も管理も簡単で、使いやすい管理コンソールを通じて提供されます。Menlo Secure Application Accessは、Menlo Secure Cloud Browserと組み合わせることで、以下の機能を備えた包括的なゼロトラストアクセスを実現します：

- 内部アプリケーションを非表示にし、最小権限ベースでアクセスを許可します。
- ユーザー、グループ、場所、アプリケーションごとに最小権限によるアクセスが許可され、アプリケーションごとに固有の管理が行われます。
- すべてのWebリクエストはSecure Cloud Browserで実行され、Webサーバーとブラウザを脅威からアイソレーション（分離）し、攻撃対象を最小化します。
- ラストマイルのデータ漏洩防止（DLP）は双方向に機能し、機密データを検知して社内アプリケーションからのダウンロードをブロックするとともに、インターネットへのアップロードもブロックすることができます。
- 管理されていないデバイスによる攻撃から社内アプリケーションを保護し、そのデバイスのユーザーが感染した可能性のあるファイルをアップロードするのを阻止できます。
- 直感的な集中管理により、管理負荷を軽減します。

市場に出回っている多くの製品では、何らかの形で重量級のクライアントおよび/または複雑なネットワーク変更が必要になるため、ZTNAの設計と導入が複雑になる場合があります。これに対しMenlo Secure Application Accessは、URL、ユーザー名、パスワードをユーザーに提供するだけで、ゼロタッチの導入展開が可能です。

BYODユーザー向けのセキュアなアクセス

課題

ゼロトラストでは、認証、検証、データ保護に必要なプロセスや手法の検証が必要です。そのような手法の多くは、エンドポイントにインストールして設定する必要がある、重量級のクライアントを必要とします。これは、以下のようなユーザーグループにおいては、困難または不可能な場合があります：

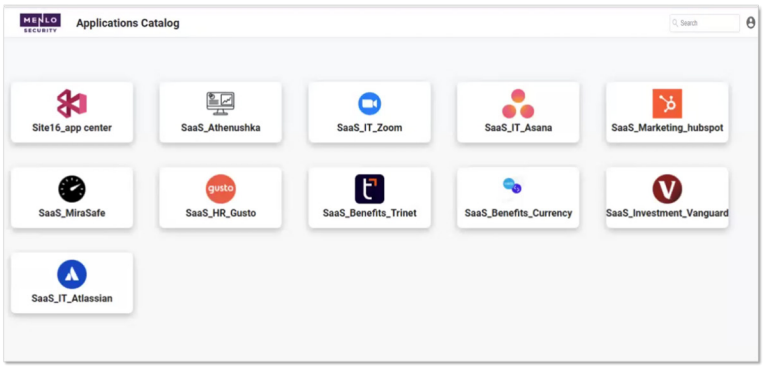
- 契約社員およびパートナー
- 合併や買収に関わるユーザー
- デバイスの持ち込みが許可されているユーザー（BYOD）

多くの場合ビジネス上の理由から、これらのグループのユーザーはSAP、Oracle、Confluenceなどの社内向けのWebベースのアプリケーションや、Salesforceなどの管理されセキュリティで保護されたパブリックのSaaSアプリケーションにアクセスする必要があります。データの流出を防ぐためには、これらのリソースへのアクセスを管理し、セキュリティで保護しなければなりません。

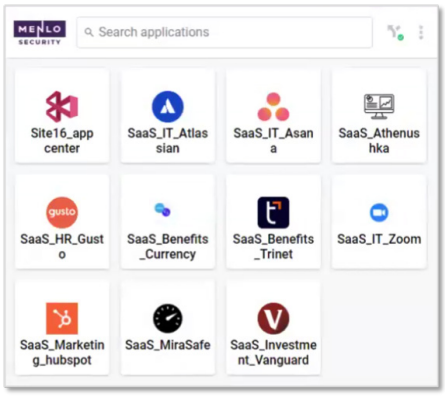
Menlo Securityのソリューション

Secure Application Accessは、ゼロトラストアクセスを管理されていないユーザーやデバイスへ迅速かつ容易に拡張し、指定されたアプリケーションのみにアクセスできるようにします。現在市場に出回っているほとんどの製品では、クライアントの導入展開、ネットワーク設定およびインフラの変更が必要ですが、Menlo Securityはそれらとは異なり、URL、ユーザー名、パスワードのみを使う、完全にゼロタッチの導入展開が可能です。

Secure Application Accessでは、WebトラフィックをMenlo Secure Cloud Browser経由で誘導します。管理されていないデバイスには組織的なデータ保護制御が適用されていないため、一般的にデータ流出のリスクが高くなります。Menlo Last-Mile DLPは、社内のWebアプリケーションからのデータ流出を阻止し、管理されていないデバイスからの漏洩リスクを緩和します。さらに、社内アプリケーションには管理されていないデバイスからの感染リスクがあります。管理されていないデバイスには、組織が義務付けているマルウェア防止策が適用されていない場合があり、そのような制御に対応できないことさえあります。ブラウザコンテキストを持たない製品とは異なり、Menlo Security Cloud Browserは、非管理対象のデバイスをWeb経由の脅威から保護しながら、ミッションクリティカルな社内アプリケーションとデータを非管理対象デバイスのリスクから保護します。



ゼロタッチのアプリケーションアクセス
Menlo Web Portal



シングルタッチのアプリケーションアクセス
Menlo Enterprise Extension

VDIの削減

課題

仮想デスクトップインフラストラクチャ（VDI）は、仮想化を活用してデスクトップコストを削減するアプローチとして登場しました。VDIベンダーは、LAN経由でデスクトップセッションを配信するプロトコルを開発しました。VDIのプロトコルは暗号化をサポートしてはいますが、VDIツールは元々リモートワーク向けに設計されたものではありません。VDIソリューションは通常、セキュアなリモートアクセスのためのVPN機能を統合していないのです。そのため、ITチームがVDIアクセス時のセキュリティを保護するには追加でVPNが必要です。LANに適したVDIのプロトコルをWANに移動させ、VPN経由でプッシュすると、エンドユーザーエクスペリエンスが低下する傾向があります。

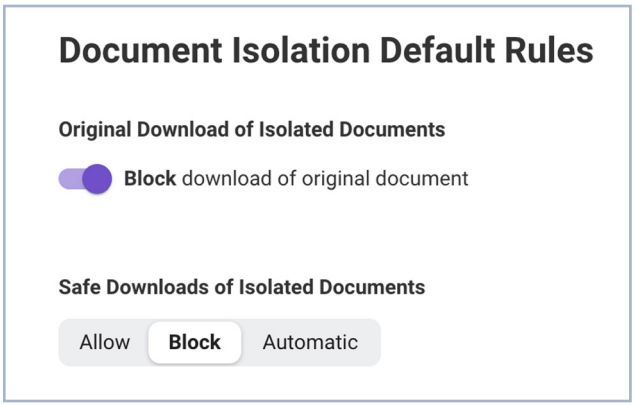
VDIの課題として、他に以下のものがあります：

- 導入展開のコストが高く、1ユーザーあたり1000ドルを超えると報告されています。
- VDIには多くのインフラストラクチャコンポーネントと関連ソフトウェアが必要なため、サポートやトラブルシューティングが複雑になります。
- Webページをピクセルに変換し、RDPやHDX、または独自のVDIプロトコル（ファイアウォールのポートを開放する必要がある）を使うVDIの手法は、HTTP/SやHTMLと比較すると、時代遅れで非効率的です。
- リモートワークでは大きい遅延が発生しがちですが、VDIプロトコルはそうした環境向けに設計されていないため、リモートユーザーのエクスペリエンスが悪化します。

Menlo Securityのソリューション

VDIで提供されるアプリケーションの多くは、Webベースでアクセスできるように進化しています。Menlo Secure Application AccessはVDIインスタンスを置き換え、管理対象デバイスと非管理対象デバイスがセキュアにWebを活用できるようにします。

VDIに対するブラウザセキュリティのメリットを示すリスクシナリオをご紹介します。



ファイルとアーカイブのセキュリティ
エンドポイントへのすべてのダウンロードを無効にできることに注意

最初のシナリオ：ユーザーがVDIセッションを開始します。パスワードで保護されたファイルへのリンクとそのパスワードが記載されたメールがメッセージとともに届きます。*この契約書には署名する必要があります。*ユーザーがリンクをクリックするとファイルがダウンロードされます（ユーザーにはわかりませんが、ファイルは感染しています）。ユーザーがファイルをダブルクリックしてパスワードを入力すると、ユーザーのVDIインスタンスが感染します。社内ネットワーク内のトラフィックは安全であると想定されているため、マルウェアは組織のネットワーク内を自由に移動することができます。

2つ目のシナリオ：ブラウザセッションを保護できるMenlo Securityで、VDIを置き換えます。パスワードで保護されたファイルへのリンクとそのパスワードが記載されたメールがメッセージとともに届きます。*この契約書には署名する必要があります。*再び、ユーザーがそのリンクをクリックします。すると、Menlo Securityは次のいずれかの方法でユーザーと組織を保護します：

- ダウンロードは行わず、悪意のあるファイルをホストしている疑わしいWebサイトをブロックします。
- Webサイトが許可されたサイトの場合、ファイルはローカルブラウザでは無く、Menlo Secure Cloud Browserにダウンロードされます。ユーザーがパスワードを入力するとファイル内のマルウェアが識別され、ダウンロードがブロックされます。

WebアプリケーションをVDIからMenlo Secure Application Accessに移行することで、特にリモートユーザーにおいて、安全で堅牢なユーザーエクスペリエンスを実現し、大幅なコスト削減を可能にします。

VPNの置き換えとゼロトラストアクセスへの進化

課題

VPNは通常、多くのアプリケーションを含む広範なネットワークセグメントへのアクセスをユーザーに許可するため、最小権限を前提とするゼロトラストを実現することはできません。

- VPNはネットワークレベルのアクセスを提供してしまい、さらにはインターネットに露出しているため、脆弱性という観点からは許容できないリスクを引き起こす可能性があります。
- VPNの通信は暗号化されているため、報告、監査、侵害調査、フォレンジックに必要なセッションの可視性を確保できません。
- MFAが必要な場合などは特に、コントラクタや買収した組織のチームメンバーなどのゲストを追加するのは非常に困難です。VPNクライアントは、相互運用性の問題から管理されていないデバイスへのインストールが困難な場合があります。また、最近MFAはハードウェアトークンではなくモバイルアプリへと進化していますが、多くの組織では依然としてハードウェアトークンが一般的であり、依然として配布に関する課題もあります。

Menlo Securityのソリューション

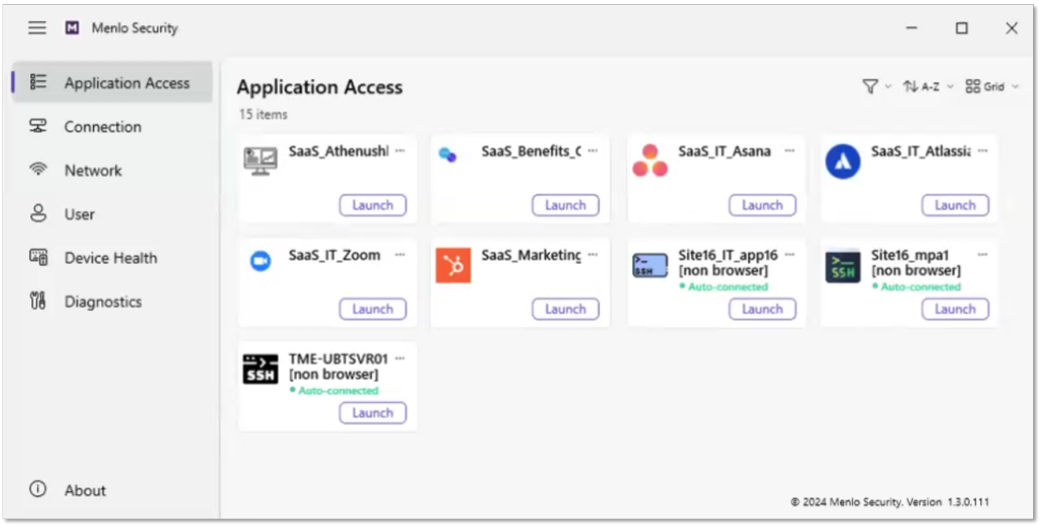
- Secure Application Accessは、ネットワーク全体やネットワークセグメント全体を開放するのではなく、組織のWebサーバーをDMZから排除し、独自のネットワークマイクロセグメントに組み込むことができます。
- ブラウザコンテキストを持たないVPNとは対照的に、Secure Application Accessには、コピー/ペーストの制限などのWeb利用時の制御や、電子透かしやデータ不明瞭化などのラストマイルのDLP機能が含まれています。
- VPNは通信を暗号化しますが、それとは異なりMenlo Browsing ForensicsはSecure Application Accessのすべてのユーザートラフィックをログに記録します。VPNからブラウザコンテキストを提供するソリューションに移行することで、より迅速なインシデント分析と対応が可能になります。
- VPNクライアントと同様に、Menlo Security Clientはデバイスのポスチャチェックを行います。
- VPNクライアントとは異なり、Menlo Security Clientでは許可されたアプリケーションのみが表示されます。

SSN	GENDER	BIRTH DATE
172-32-1176	M	1958/04/21
514-14-8905	F	1944/12/22
213-46-8915	F	1958/04/21
524-02-7657	M	1962/03/25
489-36-8350	M	1964/09/06
514-30-2668	F	1986/05/27
505-88-5714	F	1963/09/23
690-05-5315	M	1969/10/02

可視化された社会保障番号

SSN	GENDER	BIRTH DATE	MAIDE
XXX-XX-XXXX	M	1958/04/21	Sr
XXX-XX-XXXX	F	1944/12/22	Am
XXX-XX-XXXX	F	1958/04/21	Pir
XXX-XX-XXXX	M	1962/03/25	H
XXX-XX-XXXX	M	1964/09/06	Po
XXX-XX-XXXX	F	1986/05/27	Nich

不明瞭化された社会保障番号

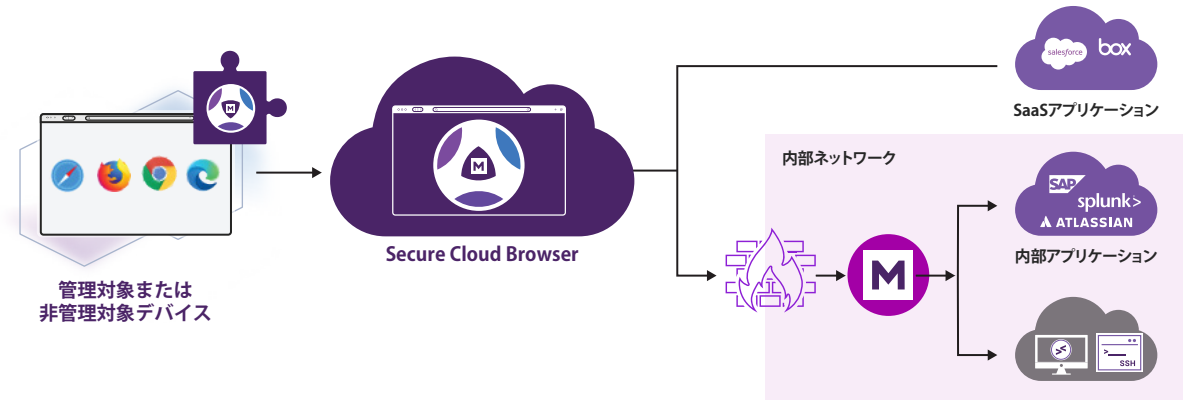


許可されたアプリケーションを表示するMenlo Security Client

ゼロトラストアクセスの簡素化と高速化

ユーザーは一日の大半をWebブラウザと共に過ごすため、組織には管理対象デバイスと非管理対象デバイス、そしてあらゆるWebブラウザで動作する、セキュアなアクセスソリューションが必要です。Menlo Secure Application Accessは、煩雑で時代遅れのVDIおよびVPNインフラストラクチャを置き換えることができる最新のソリューションです。Secure Application Accessは、管理されていないデバイスを使用するユーザーにセキュリティを提供しながら、ゼロトラストの展開を加速します。

詳細については[menlosecurity.com/ja-jp/product/secure](menlosecurity.com/ja-jp/product/secure)をご覧ください。



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