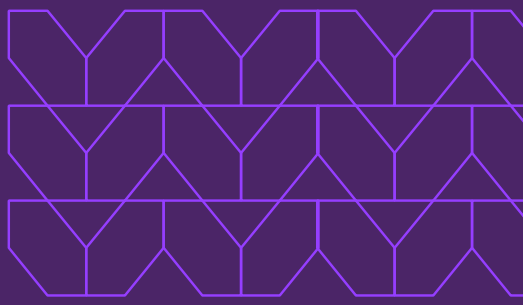
MENLO SECURITY

Data Sheet

Cloud Access Security Broker（CASB）

ユーザーに SaaS プラットフォームへの安全なアクセスを提供

現在、業務のほとんどはインターネットとブラウザーを使って行われています。高度に分散したモバイルユーザーは、動的で柔軟なSaaS（Software-as-a-Service）プラットフォームに接続することでコラボレーションし、どこに居ても高度な機能と性能を利用できます。その一方で、SaaSプラットフォームはユーザーとプラットフォームを直接的かつ持続的に接続するため、企業側からの可視性と制御性が失われ、悪意のある攻撃者がSaaSを攻撃経路として悪用するというリスクがあります。セキュリティチームは、現代の高度に分散したコラボレーション環境を維持しながら、ユーザーからSaaSへのアクセスを保護するための新しいアプローチを必要としています。



知っておくべき3つのこと：

最新のアプリケーションは、クラウドアプリケーションやサービスといった形で利用できるため、ユーザーはどこで仕事をしていても、重要なビジネス情報やツールにアクセスできるようになりました

これらのアプリケーションは、多くの場合ユーザーとプラットフォームとの間の直接的かつ安定した接続を必要としますが、企業のセキュリティチームはその経路に関与できません

メンロ・セキュリティのCASBにより、高度に分散したモバイルユーザーがSaaSプラットフォームに安全かつ確実に、安定してアクセスできるようになります

製品概要

Menlo Security Cloud Access Security Broker (CASB) は、ユーザーにSaaSプラットフォームへの安全なアクセスを提供すると同時に、セキュリティチームにはマルウェアを阻止するために必要な、深い可視性と制御性を提供します。メンロ・セキュリティはアイソレーションを使ったアプローチにより、インターネットトラフィックを中央のデータセンターにバックホールすることなく、ユーザーが最新のアプリケーションに安全にアクセスできるようにします。これにより、企業は分散したリモートユーザーに安全なローカルからのインターネットアクセスをクラウドスケールで提供することができます。

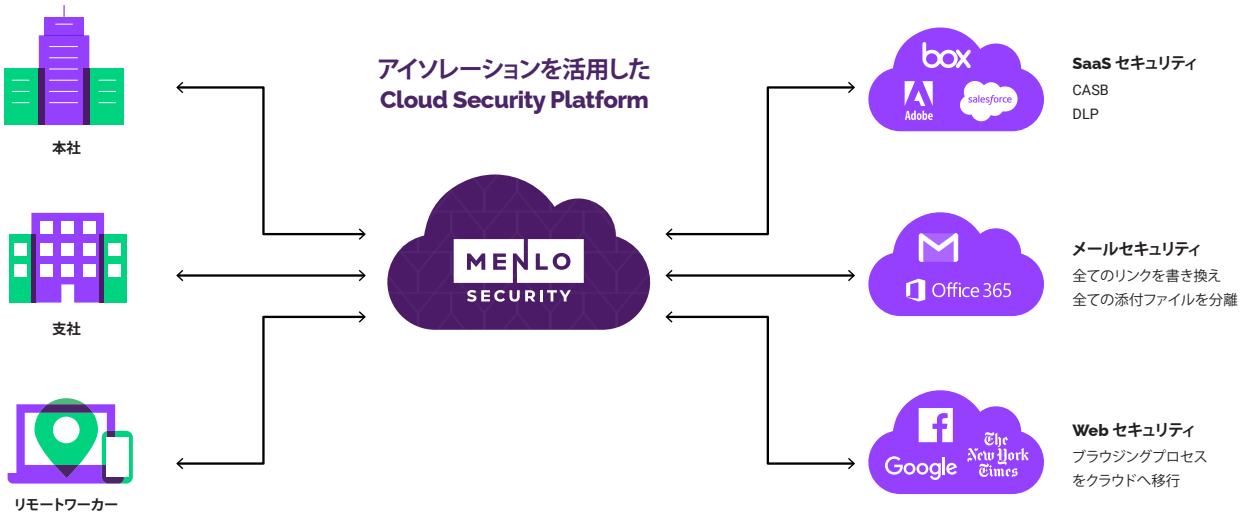
この柔軟でモバイルに対応したクラウド型のローカルインターネットブレイクアウトにより、ユーザーはデータセンターを保護するのと同じセキュリティ、可視性、制御性を備えたSaaSプラットフォームに安全に直接接続することができます

メンロ・セキュリティのCASBはリアルタイムな可視性を提供し、許可されたアプリケーションと許可されていないアプリケーションの両方で、ユーザーのアクティビティを制御します。このサービスは完全に統合されており、ポリシーの作成と管理を簡素化し、既知の脅威や既存の脅威だけでなく、未知の脅威や将来の脅威にも打ち勝つことを可能にします。

Menlo Cloud Platformを通じてファイルやドキュメントなどのSaaSコンテンツが安全にアクセスされる際に、メンロー独自のIsolation Core™がユーザーを無許可のアプリケーションから保護します。メンロ・セキュリティは、安全かつ認可されたコンテンツのみをエンドユーザーのブラウザーに効率的に配信し、アプリケーションの操作性に影響を与えることはありません。

メンロ・セキュリティのCASBはまた、セキュリティチームがユーザーがアクセスしてくる地域や接続手段に関係なく、すべてのトラフィックに対して適切なセキュリティ制御を適用できるだけの可視性と、そのための機能を提供します。これには、OneDrive、Google Drive、Box、Dropboxなどのファイル共有サイトへの機密情報のアップロードを制御するデータ漏洩防止（DLP）機能や、ログイン、アップロード、ダウンロード、共有、作成、削除などのアプリケーション機能を制御する機能などが含まれます。管理者は、メンロのドキュメントアイソレーション、コンテンツスキャン、統合されたDLPによる脅威保護機能を維持したまま、許可されたアプリに対して許可されていないアプリよりも制限の少ないポリシーを適用することが可能です。

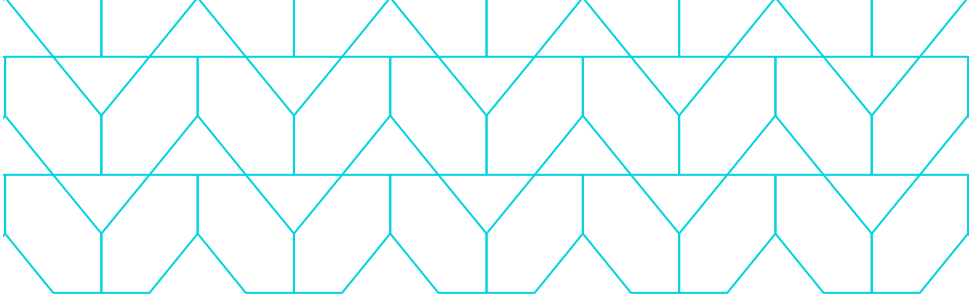
最も重要なことは、パフォーマンスに影響を与えIT部門のオーバーヘッドを増加させる、脆弱なVPNサービスや物理的なセキュリティアプライアンスに頼ることなく、最新のアプリケーションに対してこの可視性と制御性を提供できることです。



メンロ・セキュリティの Cloud Access Security Broker：主な機能とメリット

機能	メリット
Web アイソレーション	すべてのアクティブでリスクのあるWebコンテンツ（JavaScriptおよびFlash）をリモートのクラウドベースのブラウザーで実行することにより、Webサイトを安全に表示
	すべてのネイティブWebコンテンツを、ステートレスWebセッションを使用して破棄可能なコンテナで処理
ドキュメントアイソレーション	クラウド内のすべてのアクティブまたはリスクのあるコンテンツをエンドポイントから離れた場所で実行することにより、ドキュメントを安全に表示
	サニタイズされた安全なドキュメントやオリジナルバージョンのドキュメントをダウンロードするオプションを提供
	ファイルの種類とユーザーに基づいてドキュメントへのアクセスを制限するためのきめ細かいポリシー
クラウドセキュリティプラットフォーム	Webセキュリティおよびアクセスポリシーを集中管理し、あらゆる場所のあらゆるデバイス上のあらゆるユーザーに即座に適用
	一貫性のあるポリシーを使ったハイブリッドな導入展開をサポート
URL フィルタリングと利用規程（Acceptable Use Policies）	Webサイトの特定のカテゴリ（75以上のカテゴリ）のユーザーインタラクションを制限
	きめ細かいポリシー（ユーザー、グループ、IP）により、ユーザーのWebブラウジングを制御
	ファイルタイプに基づく「表示のみ、安全なダウンロード、またはオリジナルのダウンロード」を含むドキュメントのアクセス制御
帯域幅制御	ユーザー/グループポリシーを有効にして、低遅延/高帯域幅の環境（ビデオコンテンツなど）で帯域幅を予測に従って制御し、ユーザーエクスペリエンスを向上
コンテンツとマルウェアの解析	ファイルハッシュチェック、アンチウィルス、およびサンドボックスを使用した統合ファイル解析
	既存のサードパーティアンチウイルスおよびサンドボックスソリューションとの統合
	リスクの高いコンテンツを検査し、ダウンロードされたすべてのオリジナルドキュメントの悪意ある行動を検知

機能	メリット
分析とレポート	詳細なイベントログとあらかじめ用意されたトラフィック分析による組み込みおよびカスタムのレポートとアラート
	データの柔軟な調査と分析のための組み込みおよびカスタムのクエリ
	APIを使用してログデータをサードパーティのSIEMおよびBIツールにエクスポート
暗号化トラフィックの管理	TLS/SSLで暗号化されたWebブラウジングトラフィックをインターセプトして検査
	SSL検査の除外をプロビジョニング可能で、特定のカテゴリのWebサイトのプライバシーを確保
	暗号化されたセッションに隠された脅威を提示
グローバルエラスティック クラウド	世界中のリモートサイトやモバイルユーザー向けの安全で最適化されたWebアクセス
	自動スケーリングと最小遅延ベースのルーティングによって任意の場所からの接続が可能になり、1か月あたり数十億のセッションまで拡張可能
	ユーザーの迅速なプロビジョニング
	ISO27001およびSOC2認定のデータセンター
ネイティブなユーザー エクスペリエンス	さまざまなブラウザーのネイティブな状態で動作するため、ユーザーはこれまでと同じ環境でWebにアクセス可能
	新しいブラウザーをインストールしたり使用したりする必要は無し
	ピクセル化無しのスムーズなスクロール
ユーザー/グループポリシー および認証	特定のユーザー、ユーザーグループ、またはコンテンツタイプ（すべてのコンテンツ、リスクのあるコンテンツ、未分類）向けにポリシーを設定して微調整可能
	特定のユーザー、ユーザータイプ、またはコンテンツタイプの例外を作成
	ユーザー認証のためのSAMLサポートを備えたSSOおよびIAMソリューションと統合
Web ゲートウェイ	アイソレーションサービスに加え、追加のセキュリティ制御を適用
	メールアイソレーション、DLP、CASB、FWaaS、グローバルクラウドプロキシ



機能	メリット
データ漏洩防止（DLP）	インターネットへのドキュメントのアップロードを制限
	オンプレミスソリューションの可視性を強化
Cloud Access Security Broker（CASB）	確実なコンプライアンスのためにSaaSアプリケーションの可視性を強化
	サードパーティCASBソリューションとの統合
	SaaSアプリケーションのためのきめ細かいポリシー制御と、ログイン、アップロード、ダウンロード、共有、作成、削除などのアプリケーション機能の制御が可能
接続方法とエンドポイントサポート	WindowsおよびmacOSのためのエンドポイントエージェントオプションを含む、プロキシ自動設定 (PAC)/エージェントベースのトラフィックリダイレクション
	IPSEC/GREネットワークトラフィックリダイレクションをサポート
	主要なSD-WANプロバイダーとのシームレスな統合
API 統合	安全なWebセッションのためのシームレスなSaaS統合
	拡張性の高い標準規格とAPI、およびサードパーティとの統合をサポート
	コンテンツ API
	ポリシー API
	Splunk、IBM QRadar、Menlo iSOCなどのSIEMやログ分析ツールのためのログAPI
	SSO、SIEM、MDM、ファイアウォール、プロキシ、アンチウイルス、サンドボックス、CDRおよびSOARにおけるサードパーティとの検証済みの統合
	SD-WANおよびSASEとの統合

企業にとって最も重要なのは最先端のセキュリティ脅威から身を守ることですが、これまでのソリューションには限界があり、かつ脅威に対して遅れをとっています。一般的なSaaSアプリケーションはユーザーとプラットフォームの間の直接的かつ持続的な接続を必要とするため、悪意のある攻撃者はこれを攻撃のベクトルとして悪用しようとします。
メンロ・セキュリティのCASBは、SaaSプラットフォームから配信されるマルウェアやその他の悪意のあるコンテンツがエンドポイントに到達するのを防ぐことで、サイバーセキュリティに対するゼロトラストかつアイソレーションによるアプローチを可能にし、クラウドプラットフォームへのファイルアップロードによるデータ漏洩も防止します。
最も重要なのは、メンロ・セキュリティの保護はエンドユーザーにまったく気づかれないという点です。そして、セキュリティチームはすべてのユーザーのために安全でシームレス、かつ効果的な環境を維持するための運用負担を軽減できます。

ユーザーの働き方を保護する方法の詳細については、menlosecurity.com/ja-jp/ にアクセスするか、japan@menlosecurity.com までお問い合わせください。

お問い合わせ：
www.menlosecurity.jp
japan@menlosecurity.com

Menlo Securityについて

メンロ・セキュリティは、他に類を見ないアイソレーションを活用したクラウドセキュリティプラットフォームにより、企業が脅威を排除し、生産性を完全に維持することを可能にします。メンロ・セキュリティは、悪意のある攻撃を防ぐために最も安全なゼロトラストアプローチを提供し、エンドユーザーはセキュリティの存在を気にせずにオンラインで仕事をすることができ、さらにセキュリティチームの運用負担を軽減することで、クラウドセキュリティの目標を実現できる唯一のソリューションとなっています。これにより企業は安全なオンライン体験を提供することができ、ユーザーは安心して業務を行いビジネスを進めることができます。