MENLO SECURITY

DataSheet

Last-Mile Data Protection

重要なビジネス情報の意図的または偶発的な漏洩を阻止

ChatGPTのような人工知能（AI）ベースのツールを使用すると、悪意の有無に関係なく、ユーザーが入力した社会保障番号やクレジットカード番号などのPII（Personally Identifiable Information：個人を特定できる情報）をはじめとする機密データが公開されてしまう可能性があり、一人のミスによって生じた損害に対して企業が責任を負わなければならないこともあります。

ChatGPTなどの生成AIツールは、業務効率と生産性を高めるために必要不可欠な存在になりつつあります。これらの革新的なプラットフォームは、ユーザーのデータ入力に合わせた自然言語による応答を生成でき、高度にパーソナライズされた会話と独自のメッセージングを提供するように設計されています。

これらのツールは現代の企業に競争上の優位性をもたらすため、有効に使いこなさなければビジネスチャンスを逃すことにもなりかねません。その一方で、これらのツールは組織に重大なリスクをもたらす可能性があり、ユーザーとその機密データを保護するための対策が必要です。

知っておくべき3つのこと：

ユーザーが業務を行う場所は企業内から外部に移り、拡大を続けています。これに伴い、不正なデータ流出のリスクが飛躍的に増大しています。

従来型のセキュリティツールでは、企業のセキュリティチームが境界を越えて企業データを可視化したり制御したりできないため、コンプライアンスへの取り組みが阻害されることとなり、結果としてリスクが増大します。

Menlo Security Last-Mile Data Protectionは、アイソレーションを活用したアプローチで機密データを識別し、社外への流出を阻止します。

製品概要

Menlo Last-Mile Data Protectionは、すべてのトラフィックに含まれる機密データを識別して社外への流出を阻止します。ユーザーとインターネットの間にエアギャップを作成し、分離されたブラウジングセッションと分離されていないブラウジングセッションの両方について、すべてのファイルのアップロードとユーザー入力を100%確実に検査します。このアイソレーション技術によるアプローチは、ユーザーと分離されたブラウザの間のチャネルを制御し、システムがすべてを検査することを可能にします。Menlo Last-Mile Data Protectionの信頼性の高いデータ検査により、組織はエコシステム内のすべてのデバイスを監視することができます。

ChatGPTプライバシー

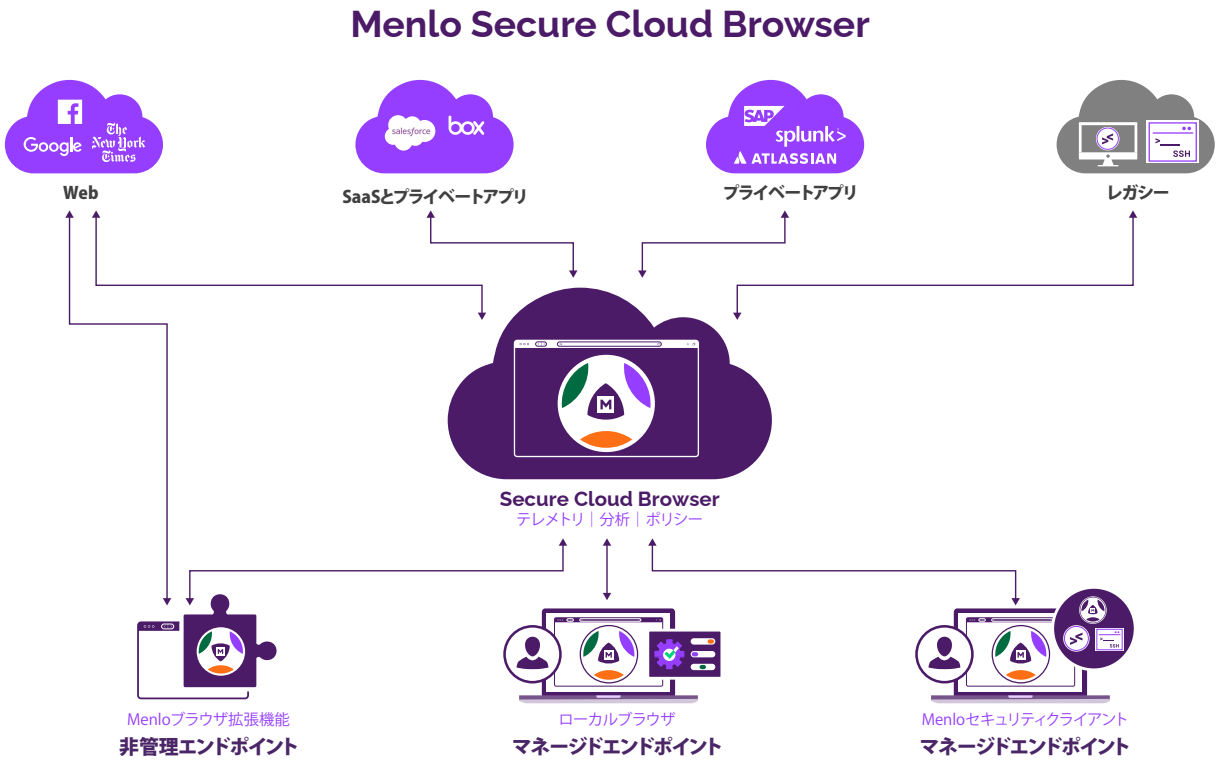
組織は、ChatGPTなどの新しい生成AIツールを活用して業務効率を高めようとしています。セキュリティリーダーは、ユーザーが誤って機密情報や顧客データを悪意のある人物の手に渡してしまうことがないようにしなければなりませんが、同時に生産性も維持する必要があります。知的財産やPIIなどの個人データを保護するためには、ポリシーと安全策を確実に適用してユーザーを保護し、機密情報がアップロードされてしまうのを阻止する必要があります。

Menlo Last-Mile DLPにより、セキュリティチームはAIプラットフォームへのデータ入力を制御し、機密コンテンツがアップロードされるのを防ぐことができます。これにより、データ漏洩の潜在的なリスクは分離されたレイヤーの中で緩和されるため、AIツールの利用が拡大しても、組織はセキュリティについて心配せずに済みます。

Menlo Last-Mile Data Protectionは、ファイルタイプや正規表現、または設定済みのデータタイプライブラリを使って機密性が高いとみなされる特定のデータタイプを識別します。

機密情報や顧客データは、Excelスプレッドシートなどのファイルに含まれていたりユーザーがブラウザのWebフォームに入力したりすることで流出します。Menlo Cloud Security Platformはトラフィックを可視化して制御できるため、すべてのデータの出口を確実に監視できます。これによりMenlo Last-Mile Data Protectionは、ブラウザの送信フォームやブラウザ以外のトラフィックから発生する潜在的なデータ漏えいを監視し、阻止することができます。

ユーザートラフィックがMenlo Secure Cloud Browserを通過する際に、暗号化されたWebトラフィックとクラウドサービスが検査され、潜在的なデータ流出の可能性がないかが確認されます。ここで、DLPポリシーがすべてのユーザーとデバイスに対してグローバルかつ一律に適用されます。



Menlo Security Data Loss Prevention：主な機能とメリット

特徴	メリット
Menlo Secure Cloud Browser	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で実行することにより、Webサイトを安全に表示
	ネイティブのブラウジング体験に影響を与えることなく、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
Document Isolation	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
	ドキュメントのオリジナルバージョンをダウンロードするか、安全でクリーンなバージョンをダウンロードするかを選択可能
	サードパーティのCDRソリューションと統合し、ファイルをスキャン
	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
Global Cloud Proxy	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き、「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分析
	Palo Alto Networks WildfireやCisco Secure Malware Analyticsなど、既存のサードパーティ製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統合
	リスクのある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のある行動を検知

特徴	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大規模に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
Global Elastic Cloud	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り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	幅広いブラウザをサポートし、ネイティブのブラウザで動作するため、ユーザーはいつもの環境でWebにアクセス可能
	新しいブラウザのインストールや使用は不要
	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追加のセキュリティコントロールを適用
	Last-Mile Data Protection、FWaaS、Global Cloud Proxy

特徴	メリット
Menlo Last-Mile Data Protection	インターネットへのドキュメントのアップロードやフォームベースの投稿を制限
	サードパーティDLPとの統合（オンプレミスおよびクラウドベースのDLP）
	オンプレミスソリューションの可視性を強化
接続方法とエンドポイントサポート	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
	CDR、SSO
	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
	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

データを完全に検査するためには、アイソレーションが不可欠です。Webページは多くの場合アップロードプロセスをわかりにくくしてしまうため、従来型のDLPソリューションでは送信データの解読が困難です。レガシーなプロキシやネットワーク検査デバイスと比較した場合のアイソレーションの利点は、ブラウザのセッションを完全に可視化できることです。Menlo Security Last-Mile Data Protectionは、世界中の300を超えるデータカテゴリのライブラリを管理して、包括的に全世界をカバーしています。たとえば、米国のある地域では機密であったり規制要件に該当したりするデータが、シンガポールやブラジルのような他の地域ではほとんど問題が無い場合があることを認識しているのです。

ユーザーが社外で仕事をするようになり、組織がクラウド化を進めているため、データ漏洩防止（DLP）はますます重要になっています。従来型のDLPソリューションでは、企業のセキュリティチームは、境界を越えて企業データを可視化し管理することができません。

Menlo Last-Mile Data Protectionは、機密データを特定して社外に流出するのを防止し、コストがかかり企業評価にも直結するデータ漏洩インシデントのリスクを低減します。Secure Cloud Browserのアプローチにより、情報のネットワークへの出入りを独自に制御し、信頼性の高いデータ検査とユーザー入力を実現します。

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/をご覧いただくか、japan@menlosecurity.comまでご連絡下さい。

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

Menlo Securityについて

Menlo Securityは、Menlo Secure Cloud Browserによって高度に回避的な脅威を排除し、生産性を維持します。Menlo Securityは、クラウドベースのセキュリティが目指す、導入展開が容易なゼロトラストアクセスを実現します。Menlo Secure Cloud Browserは、エンドユーザーがオンラインで業務を行う間、ユーザーからは見えない形でサイバー攻撃から防御し、同時にセキュリティチームの運用負担を軽減します。

Menlo Securityは、ユーザーを保護してアプリケーションへのアクセスを確保し、完全なエンタープライズブラウザソリューションを提供します。Menlo Securityなら、ワンクリックでブラウザセキュリティポリシーを導入することができ、SaaSやプライベートアプリケーションへのアクセスを保護して、ラストワンマイルまで企業データを守ります。信頼と実績のあるサイバー防御により、あらゆるブラウザでデジタルトランスフォーメーションを保護します。Menlo Securityと共に、安心してビジネスを前進させましょう。