DATA SHEET

Menlo Remote Browser Isolation

ブラウザを狙うマルウェアやフィッシングの脅威を排除して業務を保護

回避的な脅威をエンドポイントから排除

ユーザーデータを保護

ユーザーにシームレスなブラウジングエクスペリエンスを提供

組織にとって最も重要なアプリケーションであるブラウザを保護

今日の組織においてインターネットは欠くことのできないビジネスツールであり、これを使わずに業務を行うことは不可能です。ユーザーは広い範囲に分散しており、日常の業務を滞りなく行うために、Webサイトやクラウドアプリケーション、そしてSaaS（Software-as-a-Service）プラットフォームへの高速で信頼性の高いアクセス手段を必要としています。

しかし、インターネットには悪意のある脅威や検知回避型脅威（HEAT）が蔓延しており、これらが組織にとっての大きなリスクとなっています。セキュリティチームは、ユーザーの業務効率に影響を与えることなく、Webブラウジングを保護するための新しいアプローチを必要としているのです。

ユーザーがどこにいても、回避的なフィッシングやマルウェアから保護

Menlo Security Remote Browser Isolationは、セキュリティチームがマルウェアに対抗するためのゼロトラストアプローチに必要な可視性と管理性を提供します。脅威ランドスケープが拡大する中、攻撃者は検知回避型攻撃（HEAT）によってWebブラウザを狙っています。この攻撃は従来型のセキュリティ防御を回避し、最新のブラウザの標準機能を悪用してランサムウェアを配信したり、認証情報を盗んだり、マルウェアを導入展開したりします。

Remote Browser Isolationは、脅威を事後的に特定するのではなく、Menlo Secure Cloud Browserと連携して、脅威が標的に到達することを阻止します。クラウドにローカルブラウザのデジタルツインを構築してすべてのWebトラフィックを通過させ、エンドポイントには安全なコンテンツのみを配信します。Webコンテンツが良質か悪質か、あるいはカテゴリー分け済みか否かは関係ありません。Menlo Securityはゼロトラスト原則を採用しているため、すべてのコンテンツが悪意のあるものであると仮定し、それに従って処理を行います。

主なメリット

生産性を高めるために、ユーザーはWebベースの情報、SaaSアプリケーション、オンラインドキュメント、コラボレーションツール、その他のビジネスリソースに、安全かつ確実にアクセスできる必要があります。

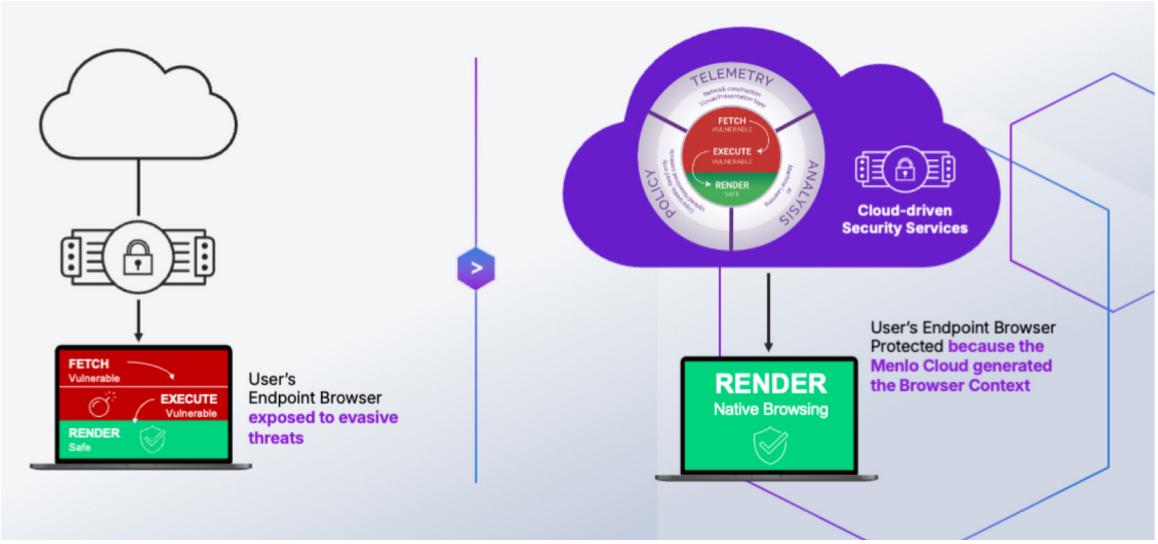
従来型の検知ベースのセキュリティアプローチでは、検知回避型攻撃（HEAT）やランサムウェア、ゼロデイ、クレデンシャル窃取などの最新の脅威から保護することはできません。

Menlo Remote Browser IsolationとMenlo Secure Cloud Browserを組み合わせ、これまでとは根本的に異なるアプローチを採用することで、脅威の一歩先を行き、ブラウザベースの脅威を完全に排除することができます。

Menlo Securityは、Remote Browser Isolationと共に、CASB、DLP、RBI、プロキシ、FWaaS、プライベートアクセスなどを含むセキュアWebゲートウェイ（SWG）の機能を単一のクラウドネイティブなプラットフォームに統合しています。Menlo Cloudは、ポリシー管理、レポート、脅威分析のための拡張可能なAPIと単一のインターフェースを提供します。また、従業員のニーズやトラフィック量の変動に対応するため、処理能力の計画やエンドポイントに導入展開するクライアントの設定を必要としません。このスケーラビリティにより、きめ細かなアクセスとセキュリティポリシーの適用、データ流出の防止、クラウドアプリケーションの安全性確保、あらゆるデバイスとロケーションでのコンプライアンスの維持が保証されます。

Menlo Remote Browser IsolationとMenlo Secure Cloud Browserを併用することで、ユーザーの働き方を完全にサポートできるだけでなく、管理者は利用ポリシーを設定して、侵害されたWebサイト、サイバースクワッティング、ファイルのアップロードとダウンロード、不適切な共有、その他の未知の脅威などの悪意のある活動を阻止することができます。ユーザー、グループ、ファイルタイプ、Webサイトのカテゴリ、またはクラウドアプリケーションに基づいてポリシーを適用し、どの時点でコンテンツを阻止するか、読み取り専用モードでレンダリングするか、あるいはオリジナルのコンテンツにアクセスできるようにするかを決めることができます。

Menlo Securityは、比類のないパフォーマンスと規模でこれを実現します。中核となるプロキシ機能を提供しながら、クラウドへの直接のインターネットアクセス（direct-to-cloud）を可能にし、URLフィルタリング、サンドボックス化されたデータ流出防止、アンチウイルススキャン、CASB、およびその他の統合技術を含むセキュリティチェックにより、トラフィックを処理します。



Menlo Secure Cloud Browser Isolationは、回避的な脅威をエンドポイントに侵入させません

主な機能

ブラウザベースの脅威に対するプロアクティブな保護：クラウドベースのセキュアな環境ですべてのWebコンテンツを実行することで、既存のブラウザリスクの課題を縮小します。Menlo Securityは、JavaScriptやスマグリングコードに隠されているような悪意のある動的コンテンツやペイロードがエンドポイントでローカルに実行されるのを阻止し、従来型のセキュリティツールを回避する高度なマルウェアから保護します。

クラウドドキュメントとアーカイブを安全に表示：エンドポイントにファイルをダウンロードする必要はありません。Menlo SecurityのSecure Domument and Archive Viewerは、あらゆるドキュメントを安全に開いて表示することができます。印刷、検索、コピー/ペースト、共有をサポートし、デスクトップとモバイルデバイスの両方でアクセス可能な、精度の高いセキュアなバージョンのファイルを提供します。

エンドツーエンドでブラウザを完全に可視化：回避的脅威に関するインテリジェンスと実用的なアラートをSOCチームに提供してリアルタイムに可視化することで、インシデント対応能力が向上します。詳細な脅威インテリジェンスとブラウザフォレンジックを既存のログ収集、自動化、セキュリティオーケストレーションツールに統合して、最適なパフォーマンスを実現します。

ブラウザフォレンジックを統合：インシデント対応チームは、Menlo Browser Forensicsを使用してブラウザセッションを高精度に記録し、スクリーンショット、ユーザー入力、ページリソースなど、ユーザーの閲覧セッションの完全な視覚的タイムラインを表示できます。

柔軟な導入展開と容易な管理：Menlo Securityは、さまざまなデスクトップおよびモバイルデバイス上のあらゆるブラウザをサポートしているため、ユーザーは好みのブラウザで作業を続けることができます。IT部門が新たにエンドポイントソフトウェアを管理する必要はありません。一度機能を有効化すれば、管理ポータル内で強制アクションを簡単に定義し、監視することができます。

シームレスなAPI統合：Menlo Securityは幅広い標準規格やAPIをサポートしており、SSO、SIEM、MDM、ファイアウォール、プロキシ、AV、サンドボックス、CDR、SOAR、SD-WAN、およびSASEなどにおいて、サードパーティとの統合が可能です。

回避的な脅威から保護し、ブラウザ内部での危険なユーザー活動を防止

Menlo SecurityのRemote Browser Isolation技術は、Menlo Secure Enterprise Browsingソリューションの中核であり、インターネットでのブラウジングすべてをクラウドベースのリモート環境に分離して実行することで、ユーザーをブラウザベースの脅威から保護します。Remote Browser Isolationは、Webコンテンツをユーザーのデバイスで直接実行するのではなく、安全な仮想コンテナ内で処理します。このアプローチにより、回避的なマルウェアや高度なフィッシング攻撃などの脅威がエンドポイントに到達するのを防止し、ユーザーはWebサイトやアプリケーションをシームレスに利用できます。Menlo Securityは潜在的に有害なコンテンツをユーザーのデバイスから排除することにより、ブラウジングパフォーマンスに影響を与えることなく、強力な保護を提供します。

MENLO SECURITY

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