

Menlo Secure Cloud Browser の概要

ブラウザベースの攻撃からユーザーを保護し、最も重要な企業資産を守り、ゼロトラストアクセスを簡素化します

クラウドベースのアプリケーションの増加は、ハイブリッドな業務環境への移行と共に、私たちの仕事の進め方を根本的に変えました。メールに代表されるこれらのアプリケーションの多くは専用のクライアントアプリからブラウザベースのアクセスに移行しており、様々なデバイスを横断して利便性を高めることができます。しかし、企業環境においてブラウザの重要性が増しているにもかかわらず、従来型のネットワークやエンドポイントのセキュリティ制御では、ブラウザベースの脅威を検知できないことが少なくありません。攻撃者は、高度なフィッシングキットやHTMLスマグリングのようなコード難読化技術などを使ったHEAT (Highly Evasive and Adaptive Threats) 攻撃を使ってこの脆弱性を悪用し、ファイアウォールやサンドボックス解析のような従来型のセキュリティツールを回避します。これは、ランサムウェアへの感染やアカウントの乗っ取り、機密データ流出などの深刻な事態に繋がります。

Secure Cloud Browserとは

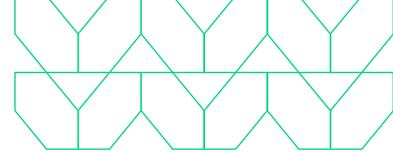
Menlo Secure Cloud Browserは、あらゆるブラウザをセキュアなエンタープライズブラウザに変えます。Menlo Secure Cloud Browserは、柔軟で統合管理されたクラウドネイティブなプラットフォームで稼働しており、ローカルデスクトップのデジタルツインをリアルタイムに作成し、エンドポイントから離れた場所でコンテンツを実行し、再構成された安全なコンテンツのみをユーザーのローカルブラウザに配信します。これにより帯域幅の消費を抑え、遅延をゼロにすることができるため、ユーザーは安心して自由にネットを利用することができます。Menlo Secure Cloud Browserは、コンテンツの善悪やWebサイトがカテゴリ分けされているか否かに関係なく、すべてのコンテンツを悪意のある可能性があるものとして扱い、処理します。



ブラウザは、企業において最も狙われている攻撃対象の1つです。Googleによると、**インターネット攻撃の80%以上がエンドユーザーのブラウザを標的としています。**

ネットワークセキュリティもエンドポイントセキュリティも、ブラウザ内部での包括的な保護を提供することができないため、**昨年**はブラウザベースの攻撃が急増しました。**フィッシングリンクの75%、回避型マルウェアの70%以上**が、既知やカテゴリ分け済み、または信頼できるWebサイトから発信されていることが確認されています。

現在一般に広く導入されているセキュリティツールは、ブラウザ内部の可視性を欠いています。ゼロアワー攻撃が最初に出現してから最終的にセキュリティツールの検知メカニズムに追加されるまでに、**平均で6日間**かかっています。



Menlo Securityは、Secure Cloud Browserでデータと情報を分析して、ゼロデイ攻撃やHEAT攻撃を阻止します。高度なAI技術やクラウドコンテンツ検査機能、セキュアなドキュメントおよびアーカイブビューアを使用することで、シグネチャやデジタルパンクズによる検知ができない未知の脅威や回避型マルウェアを特定して阻止します。Menlo Securityは、WebページをSecure Cloud Browserでレンダリングすることで、Webページで何が起きているかを正確に把握し、JavaScriptやスマグリングされたコードなどの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防ぎます。ランサムウェアや攻撃者のグループの多くは、従来のセキュリティ制御を回避するためにこれらの手法を使用することで知られています。Menlo Securityは、実際に攻撃者グループ「Evil Proxy」を最初に発見して、これを阻止しました。この攻撃は侵害されたWebページでリバースプロキシの手法を使用してユーザーのログイン認証情報を盗み、システムへのアクセスを取得しようとしています。

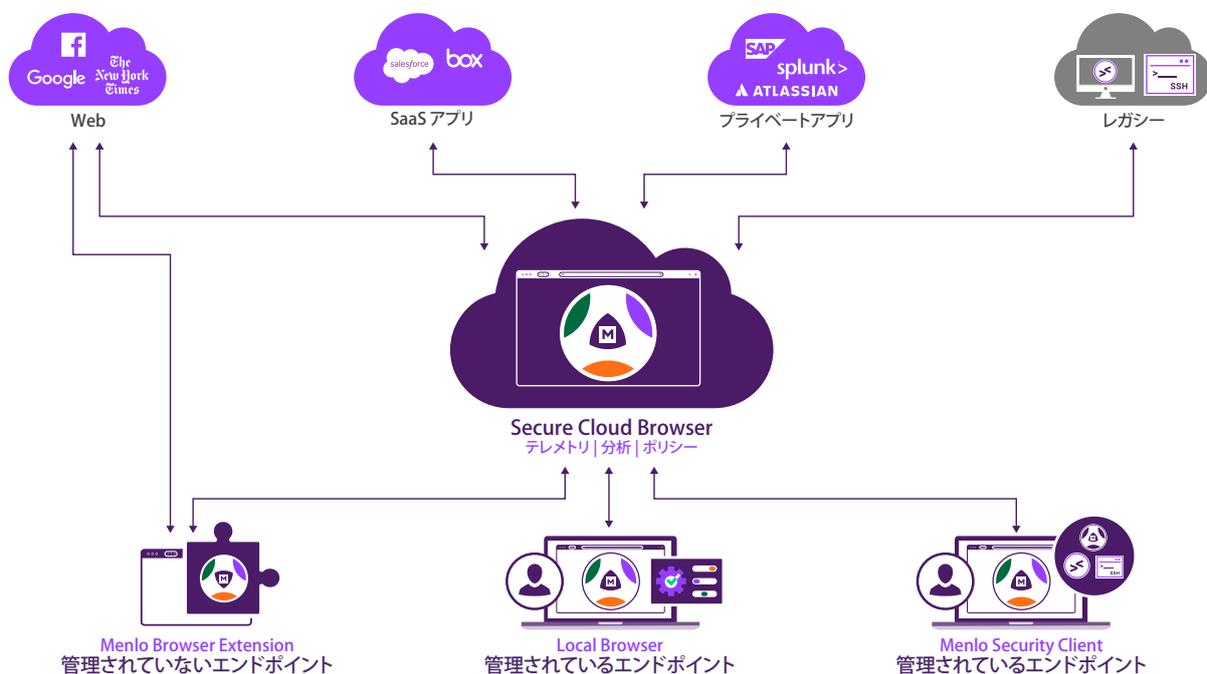
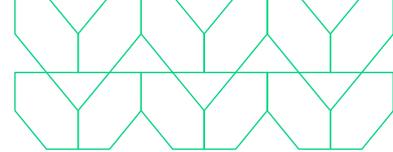


図1: Menlo Secure Cloud Browserは、脅威をエンドポイントに到達させません

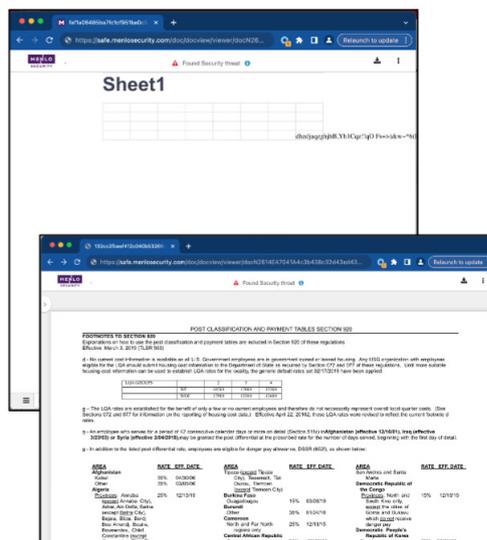
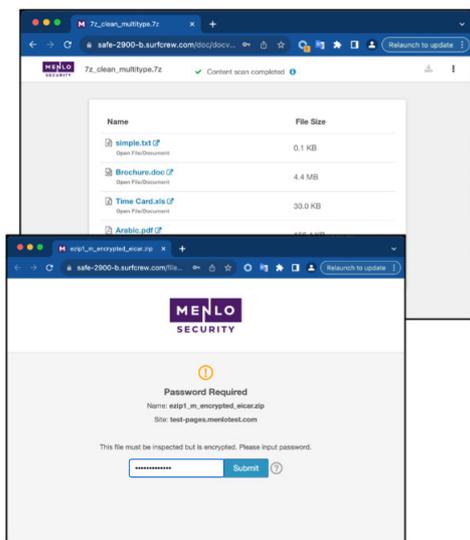
Menlo Secure Cloud Browserは、AIとWebページの個々の要素についての高度なURLランタイム分析を組み合わせることで、回避的な手法を特定します。Menlo Secure Cloud Browserは、最先端のオブジェクト検出モデルであるMenlo Computer Visionを使用して、Webコンテンツ内の画像とその位置を特定してロゴを識別します。Menlo Computer Visionの革新性は、高精度かつリアルタイムにロゴを検出し、階層化モデルによる分類を大規模プラットフォームで処理して、ユーザーをどのように保護するかを決定する能力にあります。また、Menlo Securityのセキュアなクラウドドキュメントとアーカイブのビューアは、パスワードで保護されたファイルをエンドポイントにダウンロードすることなく、安全に閲覧することを可能にします。これによりセキュリティチームは、従来のコンテンツ検査を回避するために使用される回避手法を無効化し、ゼロデイ攻撃による危険にさらされる可能性を低くすることができます。



Secure Archive
Viewer

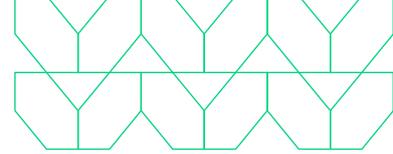


Secure Document
Viewer



脅威がエンドポイントに到達する前に阻止します Menlo Secure Cloud Browserは、ブラウザの攻撃対象 を排除し、業務を行う場所に関係なく、すべてのユーザー に最新の保護を提供します

Menlo Secure Cloud Browserは、使いやすく導入も簡単です。管理者は、悪意のある行動を阻止するための利用規程 (Acceptable Use Policies) を設定することができます。ユーザー、グループ、ファイルの種類、Webサイトのカテゴリ、またはクラウドアプリケーション毎にポリシーを適用し、コンテンツを阻止するタイミング、読み取り専用モードでレンダリングするか、またはオリジナルの形式のままでアクセスできるようにするかを決定できます。Secure Cloud Browserは、変化する従業員のニーズやトラフィック量に対応するために世界規模でスケールし、ユーザーが使うブラウザに関係なく、すべてのユーザー、すべてのタブ、すべてのWebセッションにリスクのないローカルブラウジングエクスペリエンスを提供します。ユーザーは使い慣れたブラウザで業務を続けることができ、Menlo Securityは回避的な脅威からブラウザを保護し、アプリケーションとデータへのアクセスをラストマイルまで保護します。



Secure Cloud Browserの主な機能：

ゼロデイブラウザエクスプロイトに対するプロアクティブな保護：

ユーザーのブラウザからWebサイトに直接アクセスするのではなく、各WebリクエストはMenlo Secure Cloud Browserで送信および実行され、安全でクリーンなバージョンのみがユーザーのブラウザに配信されます。これにより、すべてのブラウザとエンドポイントでゼロデイブラウザエクスプロイトによるリスクが排除され、パッチがリリースまたは展開される前でもユーザーを完全に保護することができます。

ゼロタッチのコード保護：

Menlo Secure Cloud Browserは、JavaScriptやスマグリングされたコードなどの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上でローカルに実行されるのを防ぎ、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。

エンドツーエンドでブラウザを完全に可視化：

回避的な脅威に関するインテリジェンスと実用的なアラートがSOCチームに配信され、リアルタイムの可視性を提供し、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集約、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、パフォーマンスを最適化できます。

インラインAIによる保護：

Menlo Securityでは、各WebリクエストはSecure Cloud Browserで実行され、DOM要素、ロゴ、URLパスを含む各ページのAIベースのリアルタイム分析が可能になります。フィッシングやマルウェアの脅威が検知された場合、動的なポリシー制御によってサイトを完全にブロックしたり、ページを読み取り専用モードにしてデータ入力をさせないようにすることができます。

多層的なコンテンツ検査：

Menlo Secure Cloud Browserは、パスワードで保護されたファイルを検査し、ドキュメントのマルウェア分析を行い、アンチウィルス、ファイルハッシュルックアップ、クラウドサンドボックス、ファイル処理ポリシーを適用してファイルを安全なPDFに変換します。

セキュアなクラウドドキュメントとアーカイブの表示：

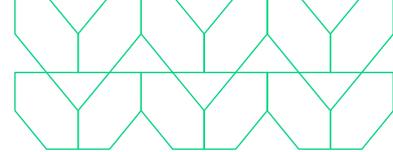
エンドポイントにファイルをダウンロードする必要はなく、セキュアなドキュメントおよびアーカイブビューアーを使って、あらゆるドキュメントを安全に開いて表示することができます。これにより、ネストされたアーカイブやパスワードで保護されたアーカイブを含むドキュメントやアーカイブのコンテンツを、エンドポイントを関与させずに安全に表示できます。

ユーザー/グループポリシーと認証制御：

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、危険なコンテンツ、未分類）に対するポリシーと例外要求を設定し、細かく調整します。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、ブラウザセッションを忠実に記録するブラウザフォレンジックツールを使用して、スクリーンショット、ユーザー入力、ページリソースを含むユーザーの閲覧セッションのタイムラインを完全に可視化できます。



柔軟な導入と簡便な管理：

導入展開と管理を簡単に行えます。デスクトップ/モバイルを問わず、あらゆるデバイスのあらゆるブラウザをサポートしているため、ユーザーは使い慣れたブラウザで業務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。一度有効化すれば、管理ポータル内で適用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：

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、SASE向けの、拡張性の高い標準サポート、API、サードパーティ統合のセットです。

Menlo Securityは、通常のブラウザをセキュアなエンタープライズブラウザに変えます

Secure Cloud Browserは脅威を完全に阻止し、従来型のセキュリティツールでは阻止できない手法を使うゼロデイWebエクспロイトやブラウザベースの攻撃からユーザーを保護します。Menlo Securityは他社とは根本的に異なるアプローチを採用して既存のリスクギャップを縮小し、業務を行う場所に関係なく、すべてのユーザーに最新の保護を提供します。

Menlo Secure Cloud Browserは、悪意のある攻撃を防ぐために最もセキュアなゼロトラストアプローチを採用しており、エンドユーザーにはセキュリティの存在に気づかせず、セキュリティチームの運用負担を軽減して、クラウドセキュリティの目標を達成します。

人々の働き方を安全に守る方法について、詳しくはmenlosecurity.comをご覧くださいか、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

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。

©2024 Menlo Security, All Rights Reserved.