MENLO SECURITY

Secure Enterprise Browser 概要

ブラウザを狙う回避的な脅威から防御

Webブラウザは組織で最も広く使われるアプリケーションになり、攻撃者はブラウザを狙っています。しかし、サイバーセキュリティに毎年数十億ドルが費やされているにもかかわらず、ブラウザの保護は遅れています。一般的に使われているネットワークセキュリティツールがブラウザのトラフィックを可視化できないため、今だに組織内で最も保護されていない攻撃対象のままとなっているのです。攻撃者はランサムウェアやフィッシング攻撃の標的としてWebブラウザを狙っており、検知を回避して成功率を最大化するために、高度に回避的な脅威を使用しています。

WebゲートウェイやEndpoint Detection and Response（EDR）、ファイアウォールなどの従来型のネットワークおよびエンドポイントセキュリティツールは、既知の脅威とのパターンマッチングなどの検知機能に依存しており、ブラウザの動作を完全には可視化できません。そのため、ブラウザ内の活動を捕捉することができないのです。Menlo SecurityのSecure Enterprise Browserソリューションはこの課題を解決し、ブラウザ内の活動を可視化することで、マルウェアやフィッシングを阻止します。この可視性により、既知のシグネチャやパターンを使った検知に頼らずに悪意のあるWebサイトを特定してブロックすることができます。

なぜブラウザセキュリティが必要なのか

ブラウザはデジタル経済圏において非常に大きな役割を果たすようになり、脅威の標的にされることが急増しています。このようなビジネスで利用されるブラウザは組織のセキュリティにおける重要なコンポーネントとなっており、さまざまな方法でユーザーを保護します：

フィッシング攻撃：フィッシングは攻撃者がよく使用するツールで、偽のWebサイトやメールなどでユーザーを騙し、機密情報を漏洩させることでユーザーのシステムを侵害したり、データを盗んだり、不正にアクセスしたりします。

ゼロデイエクスプロイト：ゼロデイフィッシング攻撃やその他のゼロデイ脆弱性は、悪意のある攻撃としてカテゴリー分けさていない未知の攻撃や、誰も見たことがないフィッシング攻撃です。また、これには開発者による修正が行われていないセキュリティ上の欠陥も含まれます。ブラウザセキュリティを導入し、ユーザーに対して動的にセキュリティを適用することで、これらのゼロデイエクスプロイトから防御することができます。

マルウェアとウイルス：ブラウザはマルウェアやウイルスに対して脆弱で、デバイスが感染すると、データの窃取、システムの損傷、ユーザーデバイスの制御不能など、さまざまな問題を引き起こす可能性があります。Menlo SecurityのSecure Enterprise Browserの堅牢なセキュリティ機能は、このようなマルウェア攻撃を防御し、より安全なブラウジングエクスペリエンスを可能にします。

機密情報への安全なアクセス:ブラウザは、インターネットやオンラインサービスへのアクセスに使用される主要なツールであり、組織の情報やSaaSアプリケーション、メール、ソーシャルメディア、バンキングなどでも利用されています。エンドユーザーはパスワードやクレジットカード情報、個人データなどの機密性の高い情報を入力しがちなため、これらの情報が悪意のある第三者の手に渡らないようにするには、ブラウザセキュリティが不可欠です。

プライバシーの保護:ブラウザはユーザーの活動を追跡し、クッキーを保存し、個人情報を収集するため、プライバシーに関する懸念が生じます。Menlo SecurityのSecure Enterprise Browserソリューションは、ユーザーや組織がオンラインプライバシーを管理し、不要な追跡をブロックし、データを悪用から保護するのに役立ちます。

Menlo Securityを選ぶ理由

Menlo SecurityはすべてのWebトラフィックをエンドツーエンドで可視化し、動的なポリシー管理を可能にするため、ブラウザベースの脅威を特定してエンドユーザーへの感染を防ぐことが可能です。Menlo Securityは、既知の脅威のシグネチャに頼るオンプレミスおよびクラウドベースのネットワークセキュリティツールや、未知のフィッシング脅威や回避的なテクニックを検知できない、ネットワークベースのテレメトリのみに依存するシステムとは異なります。その代わりにMenlo Securityは、世界中のあらゆるブラウザをサポートし、導入展開が容易なクラウドベースのブラウザセキュリティサービスを提供します。

回避的な脅威が増加しているため、Menlo SecurityはMenlo Protect with HEAT Shield AIを提供しています。これはブラウザを狙う検知回避型脅威（HEAT）を検知してブロックするために設計された、業界初の脅威防御機能スイートです。HEAT Shield AIは、コンピュータビジョンやURLリスクスコアリング、Webページ要素の分析など、複数のAIベースのテクニックを使用することで、開こうとしているリンクが認証情報を盗むために設計されたフィッシングサイトかどうかをリアルタイムかつ正確に判断することができます。もしそれがフィッシングサイトであれば、HEAT Shield AIは動的にポリシーを適用し、ページをリードオンリーモードで表示するか、完全にブロックします。HEAT Shield AIは、高度に回避的な脅威やゼロアワーフィッシング攻撃に関するアクション指向の脅威インテリジェンスを提供してブラウザをリアルタイムに保護し、エンド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しつつ、セキュリティを向上させます。Menlo Security Application Accessは、あらゆるユーザーに対して、必要とするアプリケーションへ最小権限でアクセスできるようにする保護機能を追加で提供します。これらのセキュリティ制御には、ネットワークアクセスに代わるアプリケーションアクセス、リード/ライト、アップロード/ダウンロード、コピー/ペースト、電子透かしなどが含まれます。

人々の働き方を安全に守る方法について、詳しくはmenlosecurity.jpをご覧いただくか、japan@menlosecurity.comまでメールでお問い合わせください。

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