MENLO SECURITY

ブラウザーセキュリティの概要

ブラウザーを標的とした回避型の脅威を防止

毎年数十億ドルもの予算がサイバーセキュリティに費やされていますが、その中で最も保護されていないのがWebブラウザーです。しかしWebブラウザーは、今や最も広く使用されているエンタープライズアプリケーションであり、そのために攻撃者の主要な標的となっています。攻撃者はランサムウェアやフィッシング攻撃の主要な標的としてWebブラウザーを狙っており、検知を回避して攻撃の成功率を高めるために、回避性の高い脅威を使用します。

WebゲートウェイやEDR（Endpoint Detection and Response）、ファイアウォールなどの従来型のネットワーク/エンドポイントセキュリティをベースにしたソリューションは、既知の脅威を検知するためにパターンマッチングなどの技術に依存しています。しかしこれらはブラウザーの動作を完全には可視化できないため、ブラウザーベースの活動を検知できません。ブラウザーセキュリティは、ブラウザー内の活動について可視性と制御性を提供することでこの問題を解決し、ユーザーを狙うマルウェアやフィッシング攻撃を阻止することができます。この可視性により、既知のシグネチャやパターンが利用できるかどうかに関係なく、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、ブラウザーセキュリティが重要なのでしょうか

ブラウザーはデジタル経済において非常に大きな役割を果たしているため、高頻度で脅威に狙われます。ブラウザーセキュリティはエンタープライズセキュリティにおける重要な要素であり、様々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にとって一般的なツールとなっており、通常は偽のWebサイトやメールを使ってユーザーを騙して機密情報を開示させ、ユーザー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脆弱性は、Webフィルターによって悪意があるサイトに分類されていない、または開発者によってパッチが適用されていない、未知のフィッシング攻撃やセキュリティ上の欠陥を狙います。インラインのブラウザーセキュリティと動的なセキュリティ制御を適用することで、強力なブラウザーセキュリティを実現し、これらのゼロデイエクスプロイトを防ぐことができます。

回避型脅威の50%以上は、良性に分類されたWebサイトからのもので、ブラウザー内部で起きています

URLレピュテーションエンジンを回避するために評価の高いWebサイトを使用する**攻撃が70%増加**しました

Webマルウェア攻撃の20%は高度に回避的として分類されており、既存型のネットワークセキュリティ制御を回避します

有名企業になりすました**新しいフィッシングサイトが数分毎に作成**されています

マルウェアおよびウイルス：ブラウザーはマルウェアやウイルスの影響を受けやすい場合があり、それらがデバイスに感染し、データの窃取、システムの損傷、デバイスの制御の喪失などのさまざまな問題を引き起こす可能性があります。堅牢なブラウザーセキュリティは、これらのマルウェア攻撃を阻止し、より安全なブラウジング体験を提供します。

機密情報への安全なアクセス：ブラウザーは企業にとって重要なツールで、企業情報やSaaSアプリケーション、メール、ソーシャルメディア、バンキングなどのインターネットおよびオンラインサービスにアクセスするために使用されます。その中で、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情報を入力することがあります。これらの情報が攻撃者の手に渡らないように守るためには、ブラウザーセキュリティが不可欠です。

プライバシーの保護：ブラウザーはユーザーの行動を追跡し、Cookieを保存し、個人情報を収集する可能性があるため、プライバシーに関する懸念が生じます。効果的なブラウザーセキュリティソリューションは、ユーザーと組織がオンラインプライバシーを管理し、不要な追跡を阻止し、データが悪用されないようにするのに役立ちます。

Menlo Securityを選ぶ理由

Menlo Securityは、すべてのWebトラフィックに対して完全なエンドツーエンドの可視性を提供します。動的なポリシー制御によってブラウザーベースの脅威を特定し、それらがエンドユーザーに到達するのを防ぎます。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ソリューションは、既知の脅威のシグネチャに頼ったり、ネットワークベースのテレメトリーで訓練されたAI（未知のフィッシング脅威やその他の回避手法を検知することが困難）に依存したりしています。しかしMenlo Securityはそれらとは異なる方法で、導入が簡単で世界中のあらゆるブラウザーをサポートする、クラウドベースのブラウザーセキュリティサービスを提供します。

脅威が回避型に移行していることから、Menlo Securityは業界初の脅威防御機能スイートであるHEAT Shieldの提供を開始しました。これはブラウザーを狙う回避型脅威を検知して阻止するように設計されたものです。HEAT Shieldは、コンピュータービジョンやURLリスクスコアリング、Webページの要素分析などの複数のAIベースの技術を使用して、開かれているリンクがユーザーの認証情報を盗むよう設計されたフィッシングサイトであるかどうかを、リアルタイムにかつ正確に判断します。そして動的にポリシーを適用し、そのページを読み取り専用モードで表示するか、完全に阻止します。HEAT Shieldは、HEAT（検知回避型脅威）やゼロアワーフィッシング攻撃によるアクション指向の脅威インテリジェンスに晒されるブラウザーにリアルタイムの保護を提供し、エンドユーザーにシームレスなブラウジング体験を提供しながら、組織のセキュリティを強化します。

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

Menlo Securityについて

Menlo Security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。Menlo Security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。