

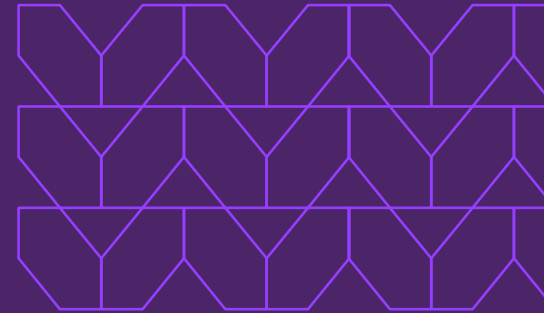


HEAT Shield

標的型ゼロアワーフィッシング攻撃 などの回避的な脅威からユーザーを 守り、企業を保護

ブラウザは、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ながら、インターネット由来の攻撃の主な侵入口にもなっています。ブラウザを狙った攻撃はデータの流出や認証情報の窃取、アカウントの乗っ取りにつながる可能性があります。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では、これらの攻撃を阻止することはできません。これらの攻撃では、シグネチャやデジタルパンくず (Digital Breadcrumbs) 』のような手掛かりが残されないことが多いためです。このような攻撃は検知回避型攻撃 (HEAT: Highly Evasive and Adaptive Threat) と呼ばれており、セキュリティをネットワークファイアウォールやエンドポイントセキュリティツールに依存している企業は、ブラウザベースの脅威やゼロアワーフィッシング攻撃にさらされることになります。

従来型のセキュリティインフラストラクチャは、既知の攻撃のシグネチャを使ったパターンマッチングによって脅威を検知してブロックしていますが、ブラウザからのシグナルを可視化することはできません。セキュリティチームは、エンドツーエンドの可視性を提供し、ユーザーを狙う脅威に対抗できる、動的なソリューションを必要としています。Menlo Security HEAT Shieldは、生産性に影響を与えることなく、ゼロアワー脅威からユーザーや組織をリアルタイムに保護します。

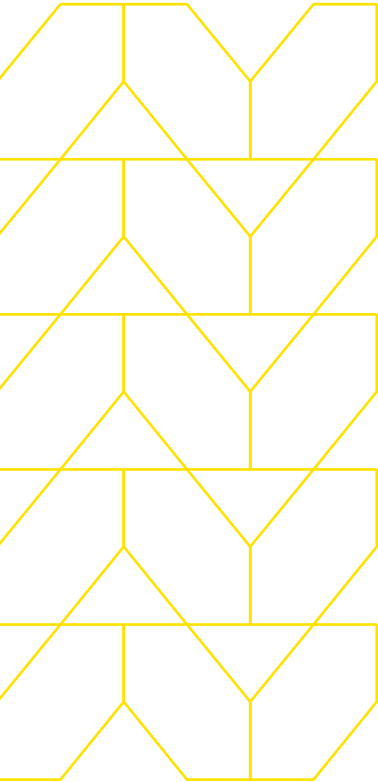


知っておくべき3つのこと:

ブラウザは、企業にとって最も重要な資産です。昨年、ブラウザベースのフィッシング攻撃は198%以上増加しましたが、そのうちの30%には、一般的なセキュリティツールを回避するためのテクニックが使われていました。

従来型の検知をベースとしたセキュリティアプローチでは、回避的なブラウザベースの脅威を含むゼロアワーフィッシング攻撃を防御することはできません。フィッシングリンクの75%は、カテゴリ分けされているか、信頼された既知のWebサイトから発信されているのです。

ゼロアワーフィッシング攻撃が最初に見つかってから従来型のセキュリティツールがそれを検知できるようになるまでには、平均で6日かかります。



製品概要

Menlo Security HEAT Shieldは、ブラウザ内部の活動と動的なWebコンテンツをAIで監視するため、ユーザーは脅威を気にせずに業務に集中することができます。HEAT Shieldは各々のWebセッションの全体像を把握して動的にポリシー制御を行い、ブラウザから攻撃可能な領域を排除します。そのため、業務を行っている場所に関係なく、すべてのユーザーに最新の保護を提供することができます。HEAT Shieldは、AIを駆使した解析とコンピュータビジョンを活用してフィッシング攻撃を防御し、ブラウザ内部からの回避的な脅威のシグナルを包括的に可視化します。このようなテレメトリデータは、従来型のネットワークセキュリティツールでは可視化できません。

Menlo Securityは、このテレメトリに基づいて、最も高度なフィッシング攻撃でも緩和することができ、IOC (Indicators of Compromise) やその他のアプローチに基づく従来型のフィードよりも、はるかに早く攻撃を検知できます。HEAT Shieldのリアルタイムな動的制御により、攻撃にさらされる期間を最大で6日間も短縮できるため、保護バファが飛躍的に拡大します。

ゼロアワーフィッシングの「保護バファ」

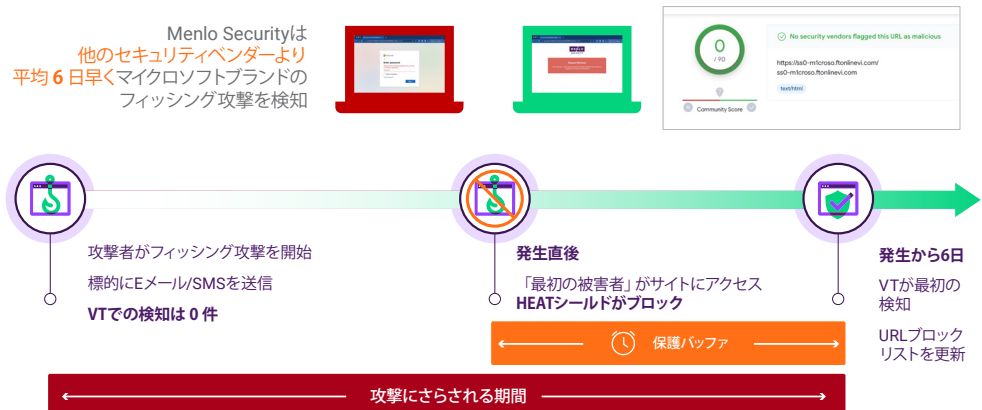
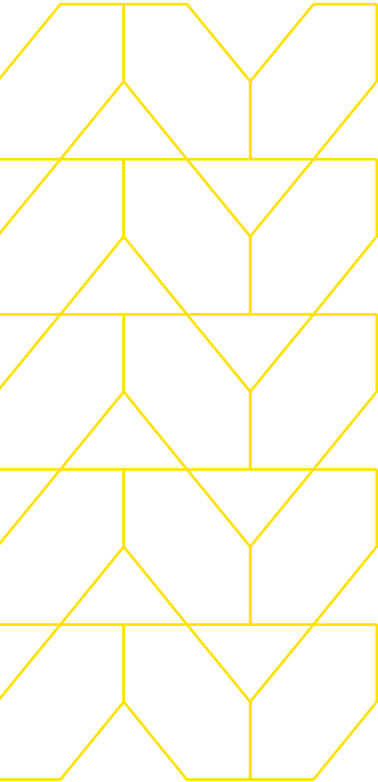


図1: Menlo Securityの保護バファがゼロアワーフィッシング攻撃から防御



Menlo Securityは、ブラウザを管理してユーザーを保護し、アプリケーションと企業データへのアクセスをセキュアに保ちながら、あらゆるブラウザとあらゆるデバイスに透過的なブラウザセキュリティエクスペリエンスを提供します。

HEAT Shieldのインテリジェンスは年間4,000億件を超えるセッションの分析を基に生成されるもので、全体的なセキュリティを向上させ、ブラウザベースの脅威からリアルタイムに保護します。HEAT Shieldを有効にすれば、企業はゼロアワーフィッシング攻撃から確実に保護されます。きめ細かなアクセスおよびセキュリティポリシーが適用され、Webセッションが監視されて保護されるため、ユーザーにリスクのないインターネットエクスペリエンスを提供できます。HEAT ShieldはMenlo Secure Cloud Browserを活用して回避的な脅威を防御するため、すべてのデバイスと場所においてポリシーを遵守できます。

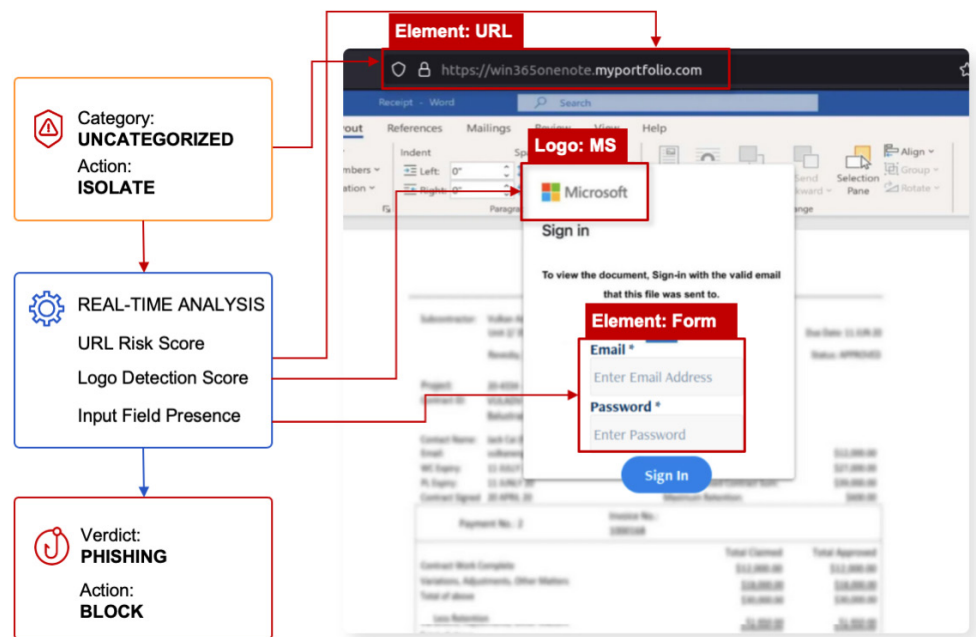


図2: カテゴリ分けされていないWebサイトに対するHEAT Shieldの動作

HEAT Shieldの主な機能：

ゼロデイエクスプロイトからの保護：

ユーザーのローカルブラウザからWebサイトに直接アクセスするのではなく、ユーザーからのリクエストをMenlo Secure Cloud Browserで実行するため、ローカルブラウザには安全でクリーンなコンテンツのみが配信されます。このアプローチにより、悪意のある活動がエンドポイントに到達することを防ぎます。

AIによるクリック時検査：

WebリクエストはSecure Cloud Browserで実行されるため、各ページのJavaScriptやDOM要素、ロゴ、入力フィールド、URLパスなどについて、AIベースの実行時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を入力させないようにすることができます。

リアルタイムにロゴを検知：

HEAT Shieldは、既知のブランドやサービスになりすましたWebサイトを、コンピュータビジョンを使って識別します。コンピュータビジョンによる識別は、偽の画像でユーザーを騙そうとする動的な攻撃に対して、迅速かつ正確な保護を広範囲に提供することが可能です。カスタムロゴにも対応しており、組織を標的にした攻撃からユーザーを守ります。

ゼロアワーフィッシングからの保護バッファ：

Menlo Securityは、リアルタイムの動的ポリシー制御を使用して、他のセキュリティベンダーや脅威インテリジェンスフィードよりも（場合によっては最大6日間も）先行して攻撃を検知できるため、ゼロアワーフィッシング攻撃の脅威を緩和することができます。

ブラウザをエンドツーエンドで可視化：

回避的な脅威に関するインテリジェンスとアラートを提供し、リアルタイムに可視化してインシデントレスポンスを改善します。詳細な脅威インテリジェンスとアラートはMenlo Securityの管理者ポータル内の専用ダッシュボードで表示できるほか、API経由でお客様のSIEM/SOCツールと連携させ、パフォーマンスを向上させることも可能です。

簡単な導入と管理：

Menlo HEAT Shieldは導入展開と管理が簡単です。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、ユーザーが使い慣れたブラウザで業務を続けることができ、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もありません。有効化した後、すぐに管理ポータル内で強制アクションを定義して、監視を始めることができます。

グローバルに利用可能：

HEAT Shieldは、世界中に配置された50ヶ所を超えるPoP (Point of Presence) でシームレスに動作し、145の国と地域をカバーします。

Menlo Securityでブラウザを保護

Menlo Securityは、ブラウザのセキュリティ機能をHEAT Shieldと共にSecure Cloud Browserに統合しています。既存のブラウザを効果的に管理してユーザーを保護し、アプリケーションアクセスと企業データをセキュアに維持します。これらはすべて単一のインターフェースから行うことができ、ポリシー管理やレポート作成、行動のための脅威分析などを簡単に行えます。

企業にとっては、最新のセキュリティ脅威から保護することこそが最優先事項です。しかし、既存のソリューションは機能が制限されており、脅威に対して受動的です。Menlo Securityは、他社とは根本的に異なるアプローチを採用してブラウザの攻撃対象を排除し、クラウドセキュリティの目標を達成できる唯一のソリューションです。導入が簡単なゼロトラストアプローチによって攻撃を阻止し、エンドユーザーがオンラインで業務を行う間はユーザーから見えない形でサイバー攻撃を防御し、同時にセキュリティチームの運用負担を軽減します。

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/をご覧ください。また、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。

©2024 Menlo Security, All Rights Reserved.