DATA SHEET

Menlo Protect with HEAT Shield AI

動的なポリシー管理とAIを活用した脅威防御

AIによるクリック時検査

ブランド偽装をリアルタイムに検知

ゼロアワーフィッシングからの保護

攻撃者の先を行くために

現代の高度なブラウザベースの脅威との戦いは、終わりの無いいたちごっこです。攻撃者は常に攻撃手法を進化させており、AIを活用したフィッシングキットやゼロデイURL、さらには最も警戒心の強いユーザーをも欺く巧妙なソーシャルエンジニアリングなどの手法を駆使しています。IPやドメインのような既存のIOCに基づく防御や、ドメインエイジやレピュテーションのような簡単に偽装できるヒューリスティックに依存する従来型の防御は、ますます効果がなくなっています。脅威ランドスケープは絶えず変化しており、重要な防御戦略としてブラウザセキュリティに重点を置く、新しいアプローチが求められています。

現代の最も回避的なフィッシング脅威にも対抗できる、AIを活用した脅威防御

Menlo Protect with HEAT Shield AIは、AIを活用したクリック時検査と最先端のコンピュータビジョン技術を駆使してWebコンテンツを動的に分析し、プロアクティブな防御を提供します。これにより、簡単に回避できる従来型の指標に頼ることなく、新しいURLや高度ななりすましテクニックを使用したフィッシングも、リアルタイムに検知して阻止することができます。Menlo Protect with HEAT Shield AIは、静的な指標の活用から動的なコンテンツ分析に重点を移すことで、回避的な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対して、より堅牢な保護を可能にします。

Menlo Protect with HEAT Shield AIは、ブラウザ内部でのAIによる解析とコンピュータビジョン技術により、ゼロアワーフィッシング攻撃を阻止し、従来のネットワークセキュリティツールでは見ることのできなかったテレメトリソースである、高度に回避的な脅威のシグナルを包括的に可視化します。このテレメトリによって、Menlo Securityは最も巧妙なフィッシング攻撃でさえも緩和することができ、ユーザーが脅威に露出される期間を最大6日間短縮して保護バッファを拡大します。

主なメリット

ブラウザは、組織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。

従来型の検知ベースの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、カテゴリ分け済みか信頼できるとされた既知の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発見され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、平均で6日間かかります。

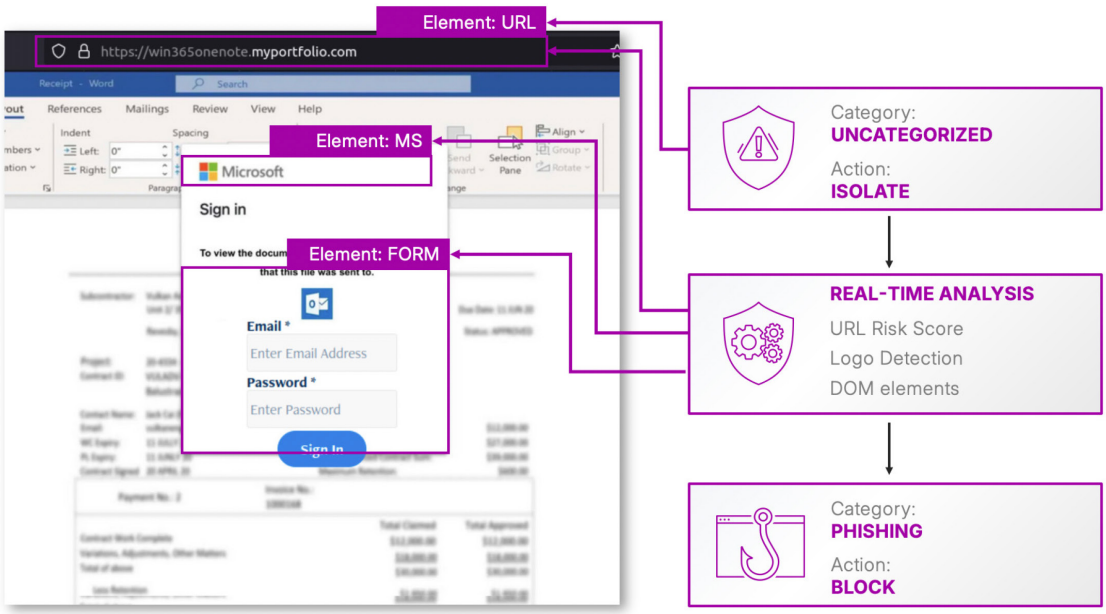
Menlo Protect with HEAT Shield AIのインテリジェンスは年間4,000億を超えるセッションの分析から生成されており、ユーザーをブラウザベースの脅威からリアルタイムに保護し、全体的なセキュリティを強化します。HEAT Shieldを有効にすれば、組織はゼロアワーフィッシング攻撃から確実に保護されます。アクセスコントロールとセキュリティポリシーを正確に適用し、Webセッションを監視して保護するため、ユーザーにリスクのないインターネットエクスペリエンスを提供できます。Menlo Protect with HEAT Shield AIは、回避的な脅威からの防御にMenlo Secure Cloud Browserを活用しているため、すべてのデバイスと場所でポリシーを遵守することができます。

主な機能

ゼロアワーフィッシングからの保護：ローカルブラウザが直接Webサイトにアクセスするのではなく、ユーザーからのWebリクエストはMenlo Secure Cloud Browser内で実行され、ユーザーの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、ゼロアワーフィッシング攻撃をリアルタイムに検知して保護することができ、脅威を緩和します。

AIによるクリック時検査：WebリクエストはSecure Cloud Browser内で実行されるため、各ページのJavaScript、DOM要素、ロゴ、入力フィールド、URLパスなどについて、AIによるラン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、正確に定義されたポリシー管理により、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防止したりすることができます。

リアルタイムのロゴ検知：Menlo Protect with HEAT Shield AIは、コンピュータビジョンを使用して、有名なブランドやサービスを偽装したWebサイトを識別します。コンピュータビジョンによる識別は、画像を使って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大規模に提供します。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。



Menlo Protect with HEAT Shield AIは、カテゴリ分けされていないWebサイトをリアルタイムに分析し、
正規のものか悪意のあるものかを識別します

リアルタイムな脅威アラートによる包括的なブラウザの可視化：回避的な脅威に関するインテリジェンスとアラートにより、リアルタイムな可視化とインシデントレスポンスの向上を実現します。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ツールから直接利用してパフォーマンスを向上させることができます。

簡便な導入展開と容易な管理：Menlo Protect with HEAT Shield AIの導入と管理は簡単で、任意のデバイス上のあらゆるブラウザを保護することができます。ユーザーは好みのブラウザで業務を行うことができ、IT部門は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。機能を有効化した後、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。

世界中から利用可能：Menlo Protect with HEAT Shield AIは、どこからでも利用可能なクラウドネイティブアーキテクチャを採用しており、組織の内外を問わず、すべてのユーザー、すべてのタブ、すべてのWebセッションに対して、リスクの無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。

Menlo Protect with HEAT Shield AIがブラウザベースのフィッシング攻撃を阻止

Menlo Protect with HEAT Shield AIとMenlo Secure Cloud Browserを組み合わせることで、組織は既存のブラウザを効果的に管理してユーザーを保護し、アプリケーションへのアクセスと組織のデータを守ることができます。

最新のセキュリティ脅威からユーザーを保護することは組織にとって最優先事項ですが、既存の製品は対症療法的であり、機能には限界があります。Menlo Securityは、他社と根本的に異なるアプローチを使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。Menlo Securityは、攻撃を阻止してセキュリティチームの運用負担を軽減するゼロトラストアプローチをシンプルに導入します。オンラインで業務を行う際に、ユーザーがセキュリティを意識する必要はありません。

回避的な脅威からユーザーと組織を保護

Menlo Protect with HEAT Shield AIは、ゼロアワーフィッシング攻撃や、回避的なテクニックを使用するその他のマルウェアを動的に識別して阻止します。従来型のセキュリティツールでは阻止できなかった、高度な脅威からユーザーと組織を保護します。

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