MENLO SECURITY

Menlo Protect with HEAT Shield AIと Browsing Forensics

ブラウザを狙う最も危険な脅威を可視化して徹底的に阻止

企業向けアプリケーションがクラウドに移行し、ハイブリッドワークが一般的になった結果、ユーザーは業務に必要なアプリケーションやデータにアクセスする主要な手段としてブラウザを活用するようになりました。

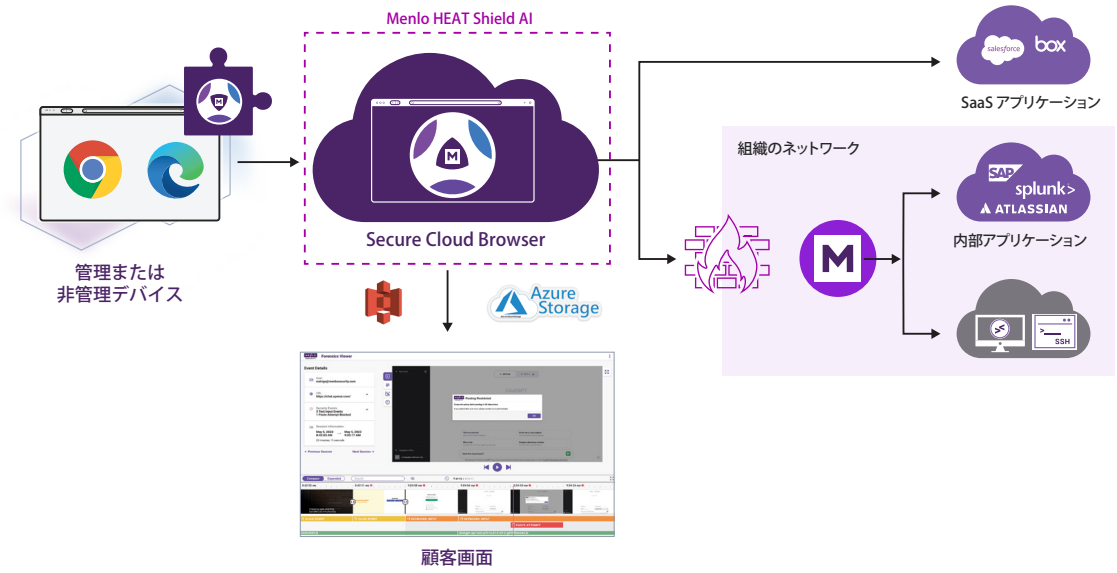
その結果、ブラウザは多くのデスクトップアプリに取って代わり、今では組織の主要な業務環境になっています。この変化は大きな可能性を生み出した一方で、以前からの課題である可視性を悪化させることにもなりました。

ブラウザのトラフィックはネットワークレベルの防御を通り抜けるように設計されているため、セキュリティチームやITチームがユーザーのブラウジングセッション内の行動を可視化することはできません。その結果、フィッシング攻撃やその他のブラウザベースの脅威も爆発的に増加しました。

組織はWebベースでアクセスするアプリケーションへの移行を急いでいますが、これらは主要なアクセス手段としてWebブラウザを使います。このような背景から、Webベースの脅威はますます高度化しており、AIサービスやDevOpsの手法を活用し、最新の脆弱性を探しながら急速に変化/拡散しています。

セキュリティおよびインシデント対応の専門家は、長年にわたりこれらのブラウザベースの攻撃の根本的な原因を調査することができませんでした。彼らは、ネットワークセキュリティツールやセキュアWebゲートウェイ、その他のクラウドセキュリティプラットフォーム、そしてエンドポイントでの検知と対応（EDR）ツールからの情報を苦労してつなぎ合わせていたのです。ユーザーのデバイス自体を検査することもありました。しかし残念ながら、最終的に決定的な証拠が得られないため、対応チームは結論を推測するしかありません。攻撃の起点となるサイトは長期間稼働しないよう設計されているため、脅威ハンターも同様の問題に悩まされています。

SOLUTION BRIEF



Browsing Forensicsが必要な答えを提供

Menlo Securityが提供するBrowsing Forensicsが、可視性の問題を解決します。トラフィックがMenlo Secure Cloud Browserを通過する際に、Webサイトのカテゴリ分け、脅威、ユーザーまたはグループによって指定されたセッションをキャプチャすることができます。記録されたパッケージは、お客様が指定したストレージに直ちに送られます。

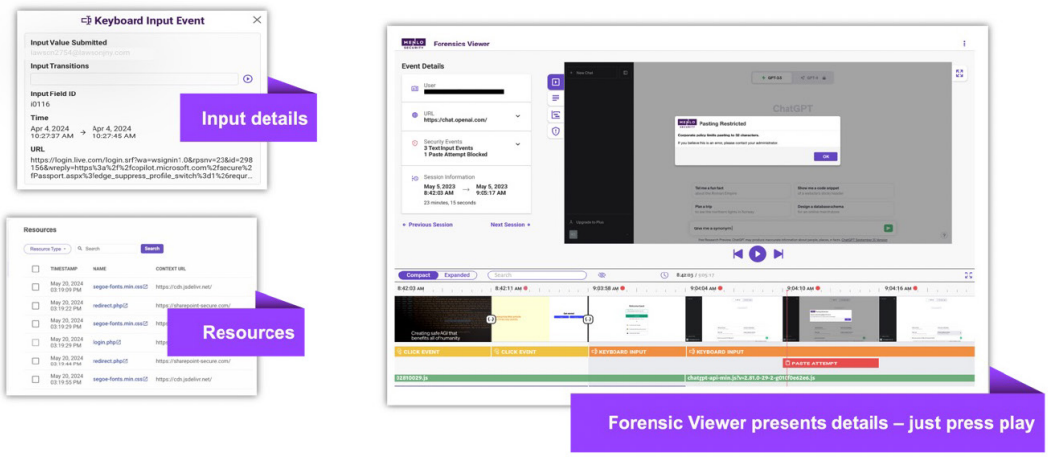
推測ではなく、詳細な情報で調査を完了

Browsing Forensicsでは、数回クリックするだけで豊富な詳細情報が表示されます。ファイルを再構成したり、ユーザーに直接インタビューしたり、エンドポイントを検査したりしてイベントを再構築する必要はありません。Browsing Forensicsなら、「再生」ボタンを押すだけで、ユーザーがどこに移動したか、そこで何をしたかを示すスクリーンキャプチャが表示されます。

ユーザーが操作した画面を見ることができるだけでなく、ユーザーが入力した記録も残るため、たとえばフィッシングサイトの場合、認証情報が入力されたかどうかを確認できます。また、Browsing Forensicsはページリソースもキャプチャするため、悪意のあるサイト自体がなくなっても、脅威ハンターは攻撃者の手法を知ることができます。

SOLUTION BRIEF

Menlo Protect with HEAT Shield AI と Browsing Forensics



Menlo Protect with HEAT Shield AIが回避的な脅威を阻止

Menlo Browsing Forensicsの手法は、検知回避型脅威（HEAT）に関連するものとして特に重要です。HEAT攻撃は組織内に足掛かりを築くために使用されることが多く、将来的にランサムウェアや恐喝攻撃に繋がります。Menlo Protect with HEAT Shield AIはHEAT攻撃に重点を置いており、これらの回避的な攻撃を捕捉して未然に防ぎます。Browsing Forensicsにより、セキュリティチームはユーザーに警告したり、同様の手法を警戒したりするために必要な詳細を得ることもできます。Menlo Securityのラストマイル DLP制御は、機密情報の流出を阻止します。最後に、インシデントが発生した場合、Browsing Forensicsは規制に準拠するために必要な、貴重なデータを提供します。

Browsing Forensicsは、Menlo Secure Application Accessにも対応しています。VDIの導入展開を最適化したい場合でも、VPNを置き換えたい場合でも、Secure Application Accessがプロセスを簡素化し、Browsing Forensicsは必要とされるユーザーセッションの詳細を提供します。

Menlo Protect with HEAT Shield AIの詳細

Browsing Forensicsの詳細

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