DataSheet

Menlo Security Browsing Forensics

ブラウザ内部のアクティビティに光をあてる

セキュリティおよびITの専門家が適切に組織を防御するためには、企業内のイベントを常に可視化しておく必要があります。この可視化の必要性が、さまざまなセキュリティツールやプラットフォームを生みだしました。これまで、ファイアウォールはペリメータレベルでのセキュリティを提供し、セキュアWebゲートウェイ（SWG）はポリシーに従ってネットワークセキュリティとフィルタリングを提供し、データ漏洩防止（DLP）ツールは知的財産を追跡してきました。

これらの技術が目指すゴールはそれぞれ異なりますが、すべてに共通することがあります。それは、企業のセキュリティチームがネットワークおよびエンドポイント、そしてアプリケーションをロックダウンするための重要なインテリジェンスを提供するということです。しかし、ネットワークとエンドポイントのセキュリティ制御が強化されたことは、別の問題を生み出しました。攻撃者は企業に侵入するための他の経路（安全性の低い資産）を探すことになり、彼らはそれを意外な場所、すなわちブラウザに見出したのです。

知っておくべき3つのこと：

近年、組織の攻撃対象は大幅に拡大しています。これはSaaSの急激な普及やデジタルサプライチェーンの拡大、ソーシャルメディアにおける企業のプレゼンス向上、カスタムアプリケーションの増加、リモートワークの普及、およびインターネット経由での顧客とのやり取りの増加などが原因です。[1]

Webブラウザは最も広く使われている企業向けアプリケーションですが、同時にエンタープライズセキュリティにおける大きな抜け穴にもなっています。

研究者は、2023年下半期にブラウザベースのフィッシング攻撃が上半期に比べて198%増加したことを発見しました。[2]

1 Gartner Top Trends in Cybersecurity for 2024

2 State of Browser Security: Defending browsers against zero-hour phishing attacks, Menlo Security

ブラウザが作り出した抜け穴により、新たな種類の脅威が生まれました。これらのエクスプロイトは検知回避型脅威（HEAT：Highly Evasive Adaptive Threats）と呼ばれ、「監視の目を避けて」企業に侵入するためにブラウザを利用します。組織がSaaSモデルの採用を進めた結果、ブラウザから多くの重要な企業アプリにアクセスできるようになりました。ブラウザを使えばあらゆるものにアクセスできるため、ユーザーが特定のアプリケーションを開く必要が無くなったのです。こうして、ブラウザはコンシューマーアプリケーションとエンタープライズアプリケーションの両方に対応できるユニバーサルクライアントになりましたが、同時にそれは、脆弱で十分に管理されていない新たな攻撃対象にもなったのです。この新たなリスクを緩和するためには、ブラウザの可視化と制御が不可欠です。Menlo Securityはブラウザアイソレーションに加え、CASBやDLP、RBI、プロキシ、FWaaS、プライベートアクセスなど、セキュアWebゲートウェイのすべての機能を単一のクラウドネイティブなプラットフォームに集約し、拡張可能なAPIとポリシー管理、レポート作成、脅威分析のための単一のインターフェースを提供します。

ネットワークやエンドポイントベースのセキュリティプラットフォームは多くの情報を提供してくれますが、最も高度なツールであっても、ユーザーのブラウザセッションを可視化することはできません。たとえばセキュリティおよびITチームは、DLPなどのイベントが発生した場合に、発生の事実を知ることはできるかもしれませんが、そのイベントがどのように発生したかを追跡することは簡単ではないのです。

インシデントレスポンスの場合、チームはアクションそのものを確認するのではなく、アクションが残した手がかりから断片的な情報をつなぎ合わせて悪意のあるアクションを追跡しなければなりません。状況を確認するために、チームはユーザーに対して数時間前（あるいは数週間前）に行った特定のアクションについて確認しなければならないことすらあります。

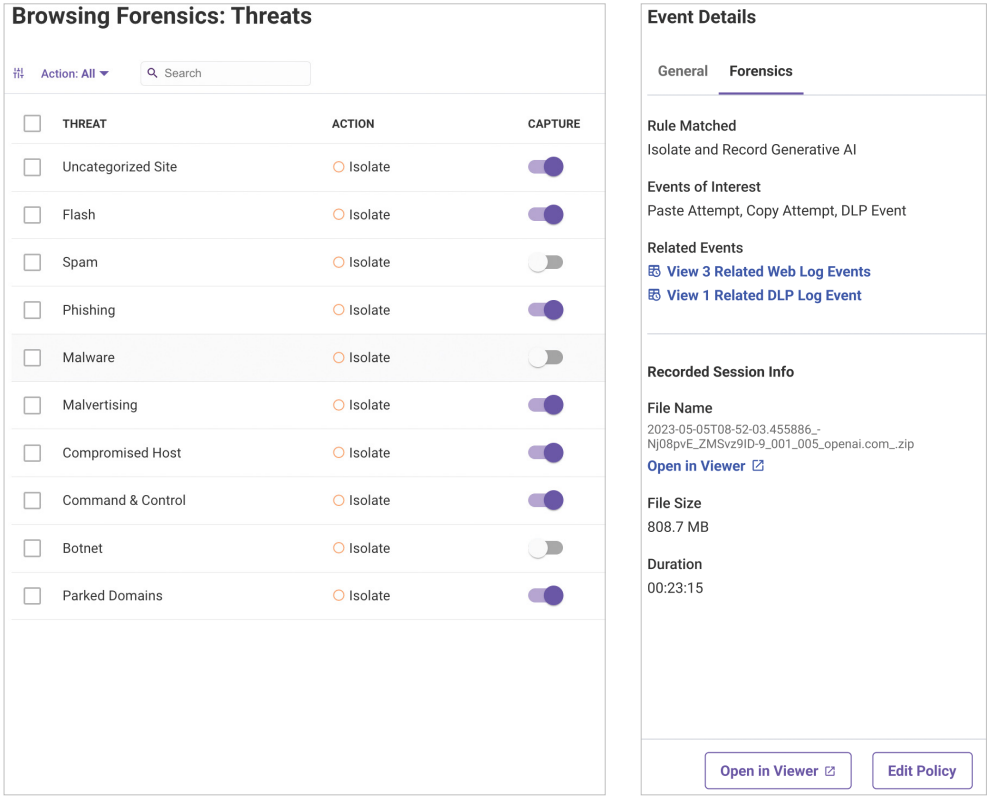
従来型のセキュリティ機能を使って侵害を解決しようとすることは、防犯カメラを確認する代わりに、足跡を辿って強盗事件を解決しようとするようなものです。

このようなインシデント対応の方法では、時間がかかる上に不明瞭な結果しか得られません。調査を行うために必要となる追加の時間とスタッフの集中力という2つの要素は、ほとんどの企業で不足しています。また、ブラウザセッションを可視化できないことは、専任の脅威ハンターにとっても足枷となります。他のセキュリティインシデントでも同様ですが、組織の脆弱性を詳細に特定するための時間がかかればかかるほど、最初の侵害がおよぼす影響が深刻化する恐れがあります。

製品概要

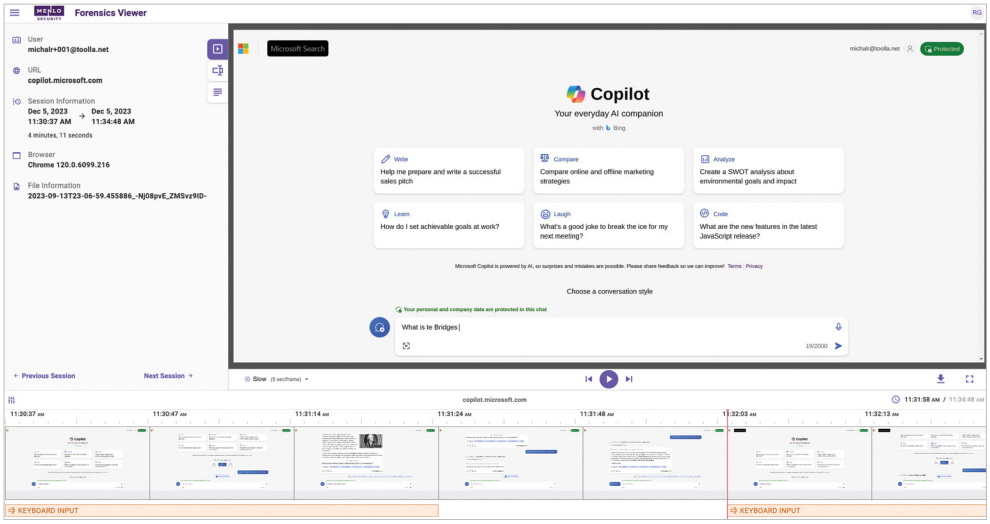
Menlo Security Browsing Forensicsは、ポリシーで定義されたブラウザセッションを記録し、セキュリティ、監査/コンプライアンス、人事その他の必要なイベントの調査において顧客チームをサポートします。これらの記録は、Heat Shieldでの検知やポリシー（プライベートまたは機密アプリケーションへのユーザーのアクセスなど）によって開始されます。

記録された各々のセッションはMenlo Forensics Logのエントリを持ち、これにはイベントのサポートデータが含まれ、記録にワンクリックでアクセスできます。Forensics Logのデータには関連する記録へのリンクが含まれており、ほぼリアルタイムに利用可能です。記録されたセッションはお客様が指定した場所に転送され、アクセス制御された環境でセキュアに保存されます。Browsing Forensicsは、AWSとAzureの両方のストレージオプションをサポートしています。



Menlo Security Browsing Forensics Viewerは記録されたさまざまなコンテンツを表示し、アナリストが迅速かつ簡単に実証された結論に到達できるようサポートします。

Menlo Browsing Forensics Logsは、DLPやコピー/ペーストなどのアクション、そしてウイルススキャンとサンドボックスの結果など、従来からあるユーザーセッションの詳細に加え、重要なイベントの概要およびそれに関連する注目すべきログを追加します。Browsing Forensics LogsにはDLP Logへのリンクが含まれるため、研究者が内部関係者の脅威を調査するような場合に、脅威の全体像とその作為性を把握することができます。



Browsing Forensicsのログには、記録へのリンクと共に記録の要約も含まれており、研究者はワンクリックでブラウジングセッションのデータを表示できます。これにより、調査のための時間を大幅に短縮することができます。

Browsing Forensicsのユースケースには、以下のようなものがあります：

- フィッシングインシデントへの対応
- データセキュリティ
- 脅威ハンティング
- 生成AIサイトとChatGPT
- コピー/ペースト
- セキュリティリサーチ
- 内部関係者の脅威
- 監査とコンプライアンス

メリット

解析の必要なデータではなく、すぐに利用できる情報を提供

Menlo Securityを使用することで、起点となるセキュリティイベントと結果としてのインシデントの詳細を、最終的に点と点で結ぶことができます。Menlo Browsing Forensicsは、Webセッションとユーザーインタラクションの包括的な記録を自動的に保存するため、あらゆるブラウザセッションの完全な履歴にアクセスできます。これらの記録はお客様が指定した場所に自動的に保存され、SIEMに送信できます。

セキュリティインシデントを迅速に解決

セキュリティインシデントがいつまでも解決されない場合、組織の潜在的なリスクが増大します。Menlo SecurityのBrowsing Forensicsはブラウザベースの情報を可視化するため、インシデントがどのように発生したかを正確に把握することができます。ユーザーのアクションを確認する機能により、ユーザーのアクションが不注意によるものであったのか、あるいは悪意のあるものであったのかを判断できます。

組織とユーザーのプライバシーを保護

Menlo Securityが可視化を行う際に、システムがユーザーのブラウジング記録を保持することはなく、Menlo Securityのスタッフがこれらのセッションを閲覧することもありません。コンテンツはお客様が指定するAWSまたはAzureのストレージに直接送信され、ログはお客様の指示によりSIEMに読み込むことができます。

Menlo Securityでブラウザを管理

Menlo Securityは、企業で使用されているすべてのブラウザおよびユーザー、そしてアプリケーションや関連する企業データへのアクセスを保護し、完全な企業向けブラウザセキュリティソリューションを提供します。ワンクリックでブラウザセキュリティポリシーを導入し、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、ラストワンマイルまで企業データを守ります。Menlo Securityなら、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安全に実現できます。

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。