MENLO SECURITY

White Paper

Adaptive Clientless Rendering™

Menlo Security Isolation Core™ を強化する技術的革新

Webブラウザーはビジネスにおいて最も重要なアプリケーションの1つですが、攻撃に対して最も脆弱でもあります。

Webブラウザーはビジネスにおいて最も重要なアプリケーションの1つですが、攻撃に対して最も脆弱でもあります。悪意のあるWebページをロードするという単純な行為ですら、エンドポイントを危険に晒すには十分であり、それがマルウェアのインストール、データの流出あるいは企業ネットワークの侵害に繋がります。悪意のあるコンテンツのダウンロードは、ほとんどの人が考えるよりも簡単に起こります。電子メールは攻撃の媒体として使われ続けています。信頼できる個人やブランドから送信されたように見えるメールを攻撃者は簡単に送ることができるためです。リンクをクリックをすることでマルウェア感染するサイトへ誘導されたり、偽物のWebサイトにIDやパスワードを入力して漏洩してしまうことに多くのインターネット利用者は意識が足りていません。その一方で、ブラウザーが高機能化するに従って攻撃者が悪用できる脆弱性も無制限に増え、リンクはより本物らしくなります。

現代のブラウザーエクスプロイトにおいて重要な役割を担っているのは、アクティブコンテンツです。現代のWeb環境におけるアクティブコンテンツは、主にFlashとJavaScriptの形式で提供されます。どちらの形式でも、アクティブコンテンツは利用者のブラウザーで実行され、攻撃者にとって有用な制御とブラウザーの実行環境、そして脆弱性への可視性を与えてしまいます。より具体的には、アクティブコンテンツを通してメモリレイアウトの検出（アドレス空間ディスクロージャー）、データ空間への書き込み（ヒープスプレー）、生成したコードの書き込み（JITスプレー）、こういったエクスプロイトを成功させるためのキーテクニックを攻撃者が利用できるようにしてしまうのです。

最近のエンドポイントには、ブラウザーエクスプロイトに対する簡単な防御が組み込まれていますが、高度な攻撃者であれば、アクティブコンテンツを使った多段階攻撃でこれらの防御を回避することができます。たとえば、単純なコードインジェクションとReturn-Oriented Programming（ROP）のエクスプロイトであれば、データ実行防止（DEP/NX）とアドレス空間配置のランダム化（ASLR）の2つの防御策によって阻止することができます。しかしアクティブコンテンツを利用すると、エクスプロイトは二次的な脆弱性（たとえば、ネイティブコードのメモリ位置を暴露する脆弱性）をトリガーすることができ、DEPとASLRの両方を回避することができます。次にエクスプロイトはそのコードを使用して、攻撃者からの命令を実行するROPコードシーケンスを作成することができるのです。

25%

2022年までに、組織の25%がブラウザーアイソレーションを採用するでしょう。

Verizon, 2018 Data Breach Investigation Report

アイソレーションは未来の技術です

リモートブラウザーアイソレーションは、エンドポイントでアクティブコンテンツを実行することに起因するセキュリティ上の課題を解決するためのテクノロジーです。その中核にあるのは、分離ブラウザーという概念です。分離ブラウザーは、ブラウザーが侵害される可能性をエンドポイントから分離することを目的としたものです。クラウド上に隔離された環境を作って分離ブラウザーを稼働させ、そこにアクティブコンテンツを含むWebページを読み込んで実行させます。ほとんどの実装では、分離ブラウザーとエンドポイントは安全なチャネルによって分離され、最小限の非常に制限されたプロトコルを使用して通信が行われます。そのプロトコルは、ユーザーからの入力を分離ブラウザーに送り、レンダリングの更新をエンドポイントに送信します。このような「エアギャップ」を挟んでブラウザーを分離することで、今日の高度なゼロデイエクスプロイトを防ぐことができます。不審なアクティブコンテンツを分離ブラウザーで実行すれば、エンドポイントが探査されてデータが盗み出されることはありません。分離ブラウザーは二次的な脆弱性の悪用を防ぎ、標準のエンドポイント防御を回避させないようにします。

アイソレーションの課題：実用に堪えるものにするために

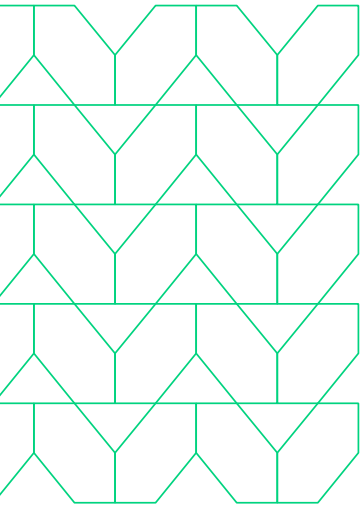
セキュリティ上の利点は明白ですが、リモートブラウザーアイソレーションがセキュリティテクノロジーとして広く採用されるためには、IT部門およびエンドユーザーのニーズを満たす必要があります。そこで、私たちはブラウザーアイソレーションを実用に堪えるものにするための5つの要件を特定しました。

最初の要件は**クライアントレスでの導入**を可能にすることです。エンドポイントにソフトウェアをインストールする必要が完全に無くなれば、IT部門の負担は軽減され、エンドポイントの動作を不安定にするリスクも減らすことができます。クライアントレスであれば、ネットワーク内のプロキシ設定によって簡単に企業全体にデプロイでき、企業ネットワーク内のすべてのデバイス（個人用デバイスを含む）のブラウジングポリシーとセキュリティアップデートを完全に集中管理することも可能になります。

それと同じくらい重要なのは、**ネイティブなユーザーエクスペリエンス**です。これはユーザーが通常のブラウジングとブラウザーアイソレーションによるブラウジングとの間に違いを感じないということであり、エンドユーザーの生産性を維持し、ブラウザーアイソレーション導入への理解を得るために重要です。ユーザーはブラウジングの方法を変える必要は無く、ブラウザーの挙動が変わることもありません。さらに、さまざまなメディアタイプ（テキストとビデオ）においてレンダリングの速度と品質がネイティブブラウザーと同じでなければならず、印刷やコピー&ペーストなどの日常使われる操作はいつもどおり機能する必要があります。地理的条件も、ユーザーエクスペリエンスに影響を与えるべきではありません。ユーザーは、どこからでもWebを閲覧し、Software-as-a-Service（SaaS）プラットフォームにアクセスできる必要があります。それが海の向こう側であろうと、道を挟んだ地元の喫茶店であろうと同じです。

スケーラビリティも重要です。企業がクラウドへの移行を進めるにつれ、Webリクエストの数も増えて行きます。このリクエストの増加に簡単に対応できるよう、時間のかかるキャパシティプランニングなどを必要とせずに拡張できるようにしておく必要があります。

すべてのセキュリティポリシーを確実に守れるように、ブラウザーアイソレーションも、その他のセキュリティスタックと**統合**される必要があります。これには、アイソレーションコアが持つ広範なアーキテクチャ上のロールを、CASB（Cloud Access Security Broker）やDLP（Data Loss Prevention）などの付加サービスに拡張することも含まれます。



そして最後に、リモートブラウザーアイソレーションによってマルウェアを効果的に封じ込め、誤検知を減らし、ヘルプデスクのコストを削減し、損傷したマシンイメージの再作成を減らして、運用コストを削減しなければなりません。なぜなら、今日の競争の激しいビジネス環境では、すべての支出がそれに見合うものでなければならないからです。

これらの要件を満たすためには、エンドポイントの変更（エージェントや特別なプラグインの導入）無しで、分離ブラウザーのレンダリング結果をエンドポイントのブラウザーに透過的にリモーティング（リモート処理）するという難しい問題を解決しなければなりません。

しかし残念ながら、仮想デスクトップインフラ（VDI）ベースのビデオストリーミングとして知られ、現在最も普及しているリモート処理手法であるピクセルミラーリングでは、目標を達成できません。分離されたWebページをピクセルの塊としてしか扱っていないために、それをミラーリングされるクライアントも、それぞれのピクセルが何を表すかについてほとんど理解していないからです。その結果、何に対してもワンパターンのアプローチとなってしまい、表示されるコンテンツの種類（テキストかビデオか）に応じてリモート処理手法を対応させることができません。さらに、レンダリングのためにブラウザーのハードウェアアクセラレーション機能を使うことができないため、ページの読み込み時間と応答性が低下します。これは、印刷やコピー&ペーストなどの日常的に行う操作に影響を与えることになります。

いくつかのブラウザーアイソレーションのソリューションは、ピクセルミラーリングが持つ問題点を解決するために、クライアントレスという形態を変更し、特殊なエンドポイントブラウザーとプラグイン、そして仮想化との組み合わせを採用しました。しかしこういったトレードオフは、特定の環境では許容されるものの、トラブルチケットの増加とエンドポイントの混乱によってIT部門の負担が増大し、広範な導入は難しいことが証明されています。

Adaptive Clientless Rendering

Menlo Securityの特許技術であるAdaptive Clientless Rendering（ACR）アーキテクチャは、Menlo SecurityのIsolation-Powered Cloud Platformを支える中核技術です。ACRが従来のVDIベースのビデオストリーミングテクノロジーと明らかに異なっているのは、ACRは分離されたページの内容をより良く理解し、これにWebベースの配信手段を組み合わせることで、クライアントレスでのデプロイとネイティブなユーザーエクスペリエンスの維持を同時に実現している点です。

図1にあるように、ACRアーキテクチャには、セーフページと分離ブラウザーという2つの重要なコンポーネントが含まれています。

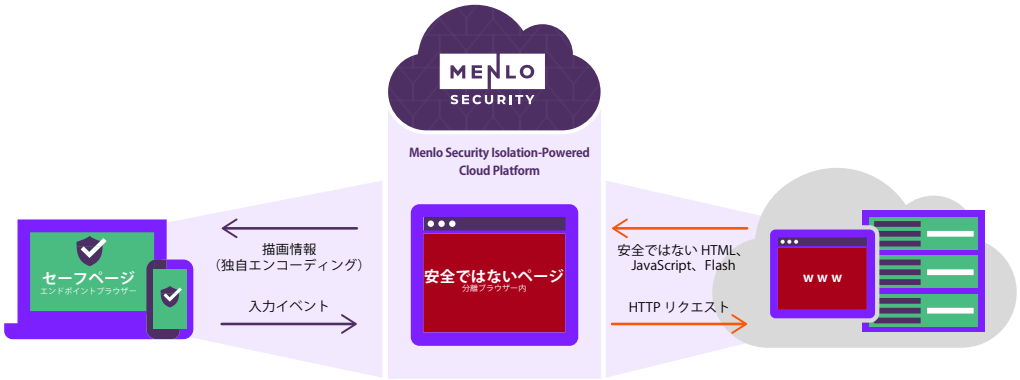


図1：ACRクライアントレスアーキテクチャ。分離ブラウザーによって解釈され、再生成された安全な描画情報(セーフページ)をエンドポイントのブラウザーが読み込み、反対に入力イベントを分離ブラウザーに中継します。通信は全てHTTPS上の安全な通信チャネル上で行われます。

セーフページは実際のWebページを安全な形に変換したもので、オリジナルページの代わりにエンドポイントのブラウザーに読み込まれます。セーフページはWebプロキシより提供され、ページを読み込んだ際、専用に作成された分離ブラウザーとの間にSSLで暗号化されたセキュアな通信チャネルを作り、その上で描画情報や入力イベントのやり取りを行います。セーフページは最新のWebの標準技術やブラウザーエンジンの進歩を素早く取り込み活用することで、エンドポイントのブラウザーやデバイスに依存することなく正確かつ効率良く動作しています。

分離ブラウザーはMenlo Security Cloud Platform上で実行され、エンドポイントに代わってWebページをロードします。そして動的なページ変更に対応して描画の更新情報をセーフページに送信し、セーフページからはユーザー入力を送信します。分離ブラウザーはChromiumブラウザーエンジンの最新バージョンをベースにしており、セキュリティ、安定性、および機能セットをChromiumと共有しています。しかし、感染と無縁でいられるブラウザーエンジンはありません。Menlo Security Cloud Platformは、分離ブラウザーにも感染のリスクがあることを想定して動作します。そのため、アイソレーションプラットフォームとエンドユーザーを保護するための重要な基礎として、Menlo Security Cloud Platformは分離ブラウザーの頻繁な廃棄、及び多層コンテナ分離を行っています。そのことで、永続的な感染や感染の広がりの両方を回避しているのです。

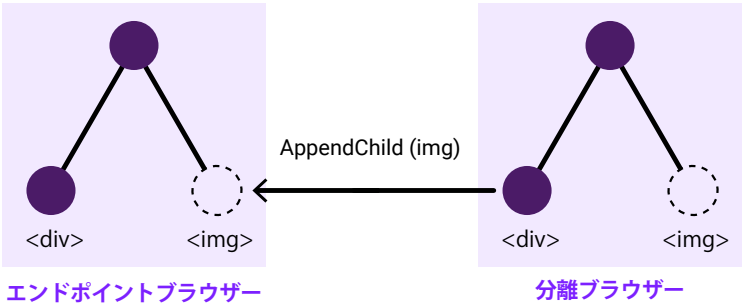
シームレスなユーザーエクスペリエンスを提供する複数のモード

ACRが透過的なユーザーエクスペリエンスを実現するための鍵となるのは、分離ブラウザー上のDOM（Document Object Model）の等価なバージョンをエンドポイントブラウザー側で再構築する機能です。DOMはブラウザー内部での動的な表現であり、ユーザーが見るのはそのレンダリング結果です。DOMをエンドポイントブラウザー側で再構築することで、スクロールなどのインタラクティブなアニメーションを含むほとんどのレンダリング作業を、GPUに最適化された仕組みを使って実行することができます。さらに、再構築されたDOMはレンダリングされたコンテンツのセマンティクスを開示するため、コピー&ペースト、ページ内検索、印刷、パスワードマネージャなどのブラウザーの全機能を引き続き利用できます。

ACRは、2つの異なる再構築モードを持っています。これらのモードのどちらが適用されるかは、使用されているエンドポイントデバイスやページコンテンツなど、さまざまな要因に基づいてページ単位で動的に選択されます。

モード1：DOM Mirroring

DOM Mirroringの目標は、DOMが持つ情報の無害な部分のみをエンドポイントのブラウザーにミラーリングすることです。クライアント側でのDOMの変更を反映するために、分離ブラウザーの各々のタブは、その時点でロードされているページのDOMツリーをアクティブに監視しています。これらの更新は、すべてのブラウザーが利用できる標準のDOM APIを使ってローカルのDOMに反映されます。



Adaptive Transcoding：DOM Mirroringは、DOM要素をクライアントに選択的に開示することで、VDIベースのビデオストリーミングアプローチに比べて明確な利点をもたらします。主な利点の一つに、DOM要素の粒度でリモート処理の方法を選択できることです。そのため、安全な静的要素はそのまま残され、アクティブで安全では無い要素は完全に削除されるか、要素のメディアタイプに合わせて変換された安全な代替コードに置き換えられます。

レンダリングとワークフローのオフロード：真に透過的なユーザーエクスペリエンスを提供するための中核となるDOM Mirroringは、エンドポイントブラウザーの機能を活用します。その結果、ページの高速読み込み、スムーズなスクロールとアニメーション、鮮明で高品質なHTML5ビデオ再生などのわかりやすいメリットが得られます。また、DOM Mirroringのセマンティックを理解するレンダリングにより、エンドポイントのブラウザーやプラットフォームが何であるかに関係なく、クライアントのブラウザーで真にネイティブなルックアンドフィールを再現することもできます。

そして最後に、DOM Mirroringはコピー&ペースト、検索、置換、印刷などのワークフローに関わる操作に影響を与えることはありません。たとえばコピー&ペーストについては、非同期なクリップボード操作に対するブラウザー側のセキュリティ制限があり、VDIベースのビデオストリーミングを使用した場合には、真にネイティブな方法でこれをエミュレートすることは困難です。印刷についても同様で、エンドポイントのブラウザーがページをピクセルの塊として表示しているため、任意の出力デバイスに対応するためにリフローできるドキュメントとは違い、一定の制約が生まれます。それとは対照的に、DOM Mirroringではエンドポイントブラウザーの既存のワークフローメカニズムに、ジョブを実行するために必要なすべての情報を提供するため、エミュレーションは必要ありません。

ドキュメントアイソレーションへの適用可能性：Webブラウザーと同様に、Microsoft OfficeやPDFビューアなども、Webからダウンロードされたり、メールの添付ファイルを介して送信されたりする悪意のあるコンテンツの影響を受けやすいアプリケーションです。ここでも、悪意のあるドキュメントに埋め込まれたアクティブコンテンツが、ホストアプリケーションの脆弱性を悪用する可能性があります。ACRを支える中核技術がドキュメントアイソレーション（ドキュメント分離）の問題にも有効に働くことは、別に驚きではありません。ブラウザー経由で悪意のあるドキュメントをダウンロードした場合、Menlo Security Cloud PlatformはACRを使用してそのドキュメントを元のレイアウトを保持したままHTML5のページにトランスコードします。DOM Mirroringにより、ドキュメントを安全かつ透過的に、クライアントレスでエンドポイントへミラーリングできるのです。

モード2：Smart DOM

ビジネスがクラウドに移行し、ユーザーはモバイルプラットフォームを使ってSaaSプラットフォームやWebアプリへミッションクリティカルなアクセスを行うようになっています。インターネット上のアイソレーションクラウドのレンダリングエンジンは、このトレンドに対応する必要があります。モバイルブラウザーのブラウジング機能は進化し、強力になっているため、新世代のアイソレーションエンジンの必要性がますます高まっています。モバイルデバイスが急増し、エンドポイントでコンテンツをリモート処理する上で、消費電力とネットワーク効率の両方に注意する必要が出てきました。Smart DOMと呼ばれるMenlo Securityの第2世代のオプションは、これらの新しい要件を考慮に入れたものです。

Smart DOMは分離ブラウザーのDOMツリーをミラーリングするのではなく、分離ブラウザーのコンポジターサブシステムが提供する低レベルのレンダリングデータ構造を用いて、エンドポイントブラウザー上に等価な別のDOMツリーを生成します。Smart DOMが採用している独自のDOM再構築アプローチには、いくつかのメリットがあります：

Smart DOM ACRは、さまざまなブラウザーでページを正確にレンダリングするため、新旧のブラウザー間、およびデスクトップデバイスとモバイルデバイス間で、より一貫性のあるユーザーエクスペリエンスを提供します。Smart DOMは、特許出願中の技術を用いてブラウザー間の非互換性を克服します。

Smart DOMは帯域幅を効率的に利用します。VDIベースのビデオストリーミングとは異なり、Smart DOMはデータ転送の重複を回避します。

DOMと同様に、**Smart DOMはネイティブのユーザーエクスペリエンスを保持します。**Smart DOMはブラウザーのGPUアクセラレーション機能を活用してエンドポイントで高速にレンダリングすることができ、デスクトップデバイスとモバイルデバイスで60FPSのスクロール、ピンチ/ズーム、アニメーションを可能にします。さらにSmart DOMは、コピー&ペースト、検索、置換、印刷、モバイルテキスト入力、エンドポイントのローカルフォント、ネイティブページウィジェットなどのネイティブサポート機能を正確にエミュレーションします。

Smart DOMはエンドポイント側でレンダリングを行います。Smart DOMはアクティブコンテンツをミラーリングしないため、攻撃対象領域が最小限に抑えられます。

この、ユーザー側のブラウザーにコンテンツを安全にミラーリングするという新しい方法によってMenlo SecurityのACRテクノロジーの適合性は向上し、ブラウザーやWeb開発ツールの進化に合わせて新しいモードを追加できます。**どちらのモードを使うかはインテリジェントに最適化されますが、モバイルのデフォルトとしてはSmart DOMオブジェクトが設定されています。**これら2つのレンダリングモードは共にクラウドサービスとして提供されるため、サービスを止めずに継続的に進化させることができます。

これにより、Menlo Security Cloud Platformは、Webコンテンツをユーザーのデバイスにシームレスかつ安全にレンダリングできると同時に、ネイティブなブラウザーエクスペリエンスの精度を高め、さまざまなメディアに拡張し、Internet Isolation Cloudが必要とする帯域を減らすことができます。そして最も重要なことは、ユーザーのブラウジング体験がまったく変わらないことです。ユーザーはこれまでどおりWebを閲覧したり、Webアプリにアクセスしたり、オンラインで作業したりできます。パフォーマンスに影響を与えることはありません。

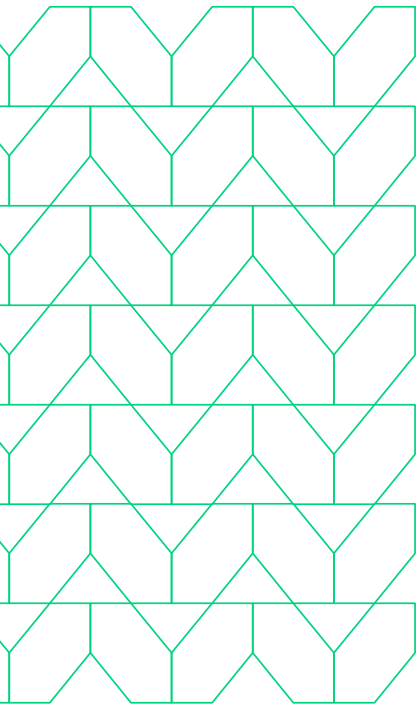
セキュリティ

ACRのセキュリティモデルの基本は、エンドポイントの防御が回避されないようにするための鍵はアクティブなコンテンツを実行させないことである、という原則です。コンテンツが実行されなければ、感染した分離ブラウザーがクライアントに何を送信したとしても、エクスプロイトが既存の防御機構を回避することはほとんどできません。この原則を念頭に置いて、ACRでは2つのセキュリティメカニズムを採用しており、これらを組み合わせることで、最も強力な敵に対しても強固な防御を提供します。

最初のメカニズムは**アクティブコンテンツのブロックとトランスコーディング**で、アクティブコンテンツがエンドポイントに送信されないようにします。DOM Mirroringモードでは、受信したすべてのDOM要素、属性、およびCSSを、ホワイトリストを使ってフィルタリングします。例えば、<script>要素とonclick属性は削除され、<object>要素は安全なリモート処理ウィジェットに置き換えられ、分離ブラウザー上でレンダリングされたプラグインウィンドウをトランスコードしてリアルタイムに表示します。

Smart DOMは、コンポジターレベルの構造（DOMやCSSの状態を含まないことが設計上保証されています）のみを送信するため、特別なフィルタリングメカニズムを必要としません。さらにMenlo Securityでは、エンドポイントブラウザーが確実にすべてのアクティブなコンテンツの実行をブロックするよう、最も厳しい設定（インラインスクリプトなし、プラグインなし）でのコンテンツセキュリティポリシーを採用しています。

2番目のセキュリティメカニズムは**プロトコルチェックとその適用**で、感染した分離ブラウザーからの不正な形式の更新によってアイソレーションプラットフォームが騙されてアクティブコンテンツを実行してしまうことを阻止し、感染した分離ブラウザーが侵害を支援する情報を誤って送信させないようにします。特に、分離ブラウザーからのすべてのレンダリング更新は正規の形式である必要があります。たとえばDOM Mirroringモードでは、DIV要素には「div」タグが必要です。エンドポイントはそれ以外の文字列を受け付けません。エンドポイントのブラウザーが予期せずに解釈してしまうような奇妙な文字コードを含む文字列も受け付けません。次にエンドポイントは、送信するメッセージが単純なユーザー入力プロトコルに準拠していることを確認します：例としては、「ボタン1をクリック」、「キーコード45」、「45までスクロール」などです。その結果、感染した分離ブラウザーがエンドポイントの脆弱性を調査したり、標準のエンドポイント防御の回避に役立つ情報を盗み出すためのチャネルが封じられます。



これまで：
ブラウザーアイソレーションは、アクティブコンテンツをエンドポイントから切り離すことで、未来のゼロデイ脅威からもユーザーを保護することを約束します。

これから：
アイソレーションは、エンドユーザーがオンラインで仕事をしている間にマルウェアがエンドユーザーに到達するのを防ぎ、セキュリティチームの運用負荷を軽減することで、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可能にします。

ドキュメントアイソレーションへの適用可能性

Webブラウザーと同様に、Microsoft OfficeやPDFビューアなども、Webからダウンロードされたり、メールの添付ファイルを介して送信されたりする悪意のあるコンテンツの影響を受けやすいアプリケーションです。ここでも、悪意のあるドキュメントに埋め込まれたアクティブコンテンツが、ホストアプリケーションの脆弱性を悪用する可能性があります。ACRを支える中核技術がドキュメントアイソレーション（ドキュメント分離）の課題にも有効に働くことは、別に驚きではありません。

ブラウザー経由で悪意のあるドキュメントをダウンロードした場合、Menlo Security Cloud PlatformはACRを使用してそのドキュメントを元のレイアウトを保持したままHTML5のページに変換します。そして、変換されたコンテンツを分離ブラウザーに読み込み、ドキュメントをミラーリングしてエンドポイントに提供します。

結論

ブラウザーの機能は、JavaScriptからアクセス可能な新しいAPIと共に拡張を続けています。今後はこの新しい攻撃対象領域に対する新たなエクスプロイトが予想され、アクティブコンテンツは引き続きエクスプロイトの主要な経路となるでしょう。ブラウザーのアイソレーションは、アクティブコンテンツの実行をエンドポイントから分離することにより、これらの未来の脅威からユーザーを保護することをお約束します。しかし、その目的を達成するためには、ブラウザーアイソレーションはクライアントレスでのデプロイと完全に透過的なユーザーエクスペリエンスの両方を実現しなければなりません。Menlo Security Isolation-Powered Cloud Platformの中核にある新しいリモート処理テクノロジーであるAdaptive Clientless Rendering™（ACR）は、エンドポイントのブラウザー上で本格的なDOMをアダプティブかつ安全に再構築することで、ネイティブでのレンダリングを可能にし、ネイティブブラウザーの機能をフルに活用することで、この課題を解決します。

ACRは、アクティブコンテンツがエンドポイントのブラウザーで実行されないようにするメカニズムであり、クライアントレスでネイティブなブラウジングエクスペリエンスを提供しながら、同時にゼロデイ脅威からの防御も実現します。

ユーザーの働き方を守るための詳細については、www.menlosecurity.jpをご覧頂くか、japan@menlosecurity.comまでご連絡下さい。

Menlo Securityについて

Menlo Securityは、Web、ドキュメント、メールからマルウェアの脅威を排除することによって、組織をサイバー攻撃から保護します。Menlo Securityは、グローバル2000に名を連ねる何百社もの企業と主要な政府機関におけるセキュアクラウドトランスフォーメーションの達成を支援してきました。Menlo SecurityのCloud Security Platformは、拡張性に優れており、あらゆる規模の企業に包括的な保護を実現します。エンドポイントソフトウェアは不要で、エンドユーザーの操作性にも影響しません。Menlo Securityは、ガートナーセキュアWebゲートウェイ（SWG）についてのマジック・クアドラントでビジョナリーに選出されています。

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