MENLO SECURITY

White Paper

CISOのための エンタープライズ ブラウザガイド

ブラウザを守るための 適切なアプローチとは

デジタルトランスフォーメーション（DX）の発展は企業の働き方、サプライチェーンの再構築、カスタマーエクスペリエンスに大きな変革をもたらしています。このDXの変革を後押ししているのが皆様も利用されているSaaS（Software as a Servie）の出現です。SaaSの進化によりブラウザがOS（Operating System）のように複雑な業務を行う一つのプラットフォームに発展しました。攻撃者はこのブラウザを攻撃対象にしているためブラウザセキュリティが必要とされるようになりました。

Forresterによると、一般的な従業員は「デバイス使用時間」の75%をWebブラウザに費やしているということです。これには、ビジネスに不可欠なアプリケーションへのアクセスや仕事用のメールへのアクセス、ファイル共有などの様々なアクティビティが含まれます。

攻撃者はこの事実を決して見過ごしません。ブラウザは今や、ユーザーを侵害しようとする際の最初の標的とされています。Verizon 2022 Data Breach Investigation Report（DBIR）によると、Webブラウザを介してアクセスされるWebアプリケーションとメールはセキュリティ侵害の主要な攻撃ベクトルとなっており、インシデントの80%以上を占めています。Google Project Zero[1] の記録によると、2023年に悪用されたクライアント側のゼロデイの大半はブラウザの脆弱性でした。攻撃者はこのゼロデイを悪用して、被害者のエンドポイントにマルウェアやランサムウェアをインストールしたり、機密データを盗んだりします。

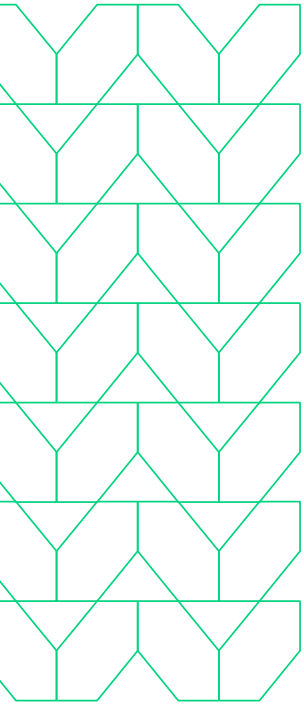
フィッシングやマルウェア、そしてランサムウェア攻撃が継続的に進化し成功を収め続けていることは、セキュアWebゲートウェイ（SWG：Secure Web Gateway）やEDR（Endpoint Detection and Response）ソリューション、あるいはファイアウォールなどの従来型のネットワークやエンドポイントセキュリティベースのソリューションでは、ブラウザベースのアクティビティを十分に可視化できないことを示しています。これら従来の検知方法は既知の悪質な脅威とのパターンマッチングや従来のネットワークシグナルを使うアプローチに依存しており、ブラウザの動作を完全に可視化できていないためです。たとえば、良性のカテゴリに分類されたサイトを悪用してURLレピュテーションエンジンを回避する攻撃は70%も増加しています[2]。攻撃者は、同じ攻撃でもソースと手法を変えることで、これらの従来型のソリューションの隙を突き検知回避型攻撃を仕掛けてきます。

[1] "0day "In the Wild"

[2] 出典: Menlo Labs

これらの脅威に対抗するために、セキュリティとITチームはネイティブのブラウザポリシーを使うべきではありません。既存のブラウザポリシーは、セキュリティチームがこれらの脅威から組織を保護するために達成しようとしていることと完全に一致しているわけではないからです。一般的に、ポリシーを強制することは簡単ではなく、どのポリシーが適切かを判断することが難しい状況となっています。

今日までのセキュリティ対策では、企業を保護できていません。組織はブラウザセキュリティのあらゆる側面に対応できる、包括的なブラウザセキュリティソリューションを必要としています。



ブラウザセキュリティとは

ブラウザセキュリティに特化した多くのソリューションは、3つの主要なカテゴリに分類できます。

ローカルブラウザ

- **メインストリームブラウザ**：これには、Google Chrome、Microsoft Edge、Apple Safariなどのブラウザが含まれます。各ブラウザベンダーは継続的にセキュリティ機能を追加しており、ブラウザが持つ機能を保護しています。
- **エンタープライズブラウザ**：これらのブラウザの多くはChromiumをベースにしており、エンタープライズユーザー向けに特別に設計されています。これらのブラウザは、主にユーザーのデバイスに一貫したエンタープライズポリシーを強制することに重点を置いています。
- **エンタープライズブラウザ拡張機能**：これらはメインストリームブラウザ用に設計されたもので、ブラウザ拡張機能の形でブラウザに機能を追加します。

従来型のリモートブラウザアイソレーション（RBI）：RBIは、ユーザーおよびそのデバイスと（通常はインターネットからの）信頼できないWebコンテンツを分離するために設計されたWebソリューションです。

クラウドベースのブラウザセキュリティ：エンタープライズブラウザとエンタープライズブラウザ拡張機能、リモートブラウザアイソレーションの機能を含む、ハイブリッドで柔軟なソリューションで、クラウドベースのサービスとして提供されます。

ブラウザセキュリティの主な機能

ブラウザセキュリティは、3つの主要な柱に分けることができ、それぞれについてユーザーの保護、企業の保護、管理者とエンドユーザーの両方への優れたユーザーエクスペリエンスの維持に不可欠な主要な機能とユースケースを備えています：

- ブラウザを管理する
- ユーザーを保護する
- アクセスとデータをセキュアにする

ブラウザの管理

ブラウザを管理することは、新しい概念ではありません。主要なブラウザ管理プラットフォームであるMicrosoft IntuneとGoogle Chrome Enterprise Managerは、一元的に管理できる数百もの管理パラメータを提供しています。ほとんどの企業はブラウザのバージョン管理と拡張機能の管理において最小限のパラメータにしか注意を払っておらず、ブラウザはほぼデフォルトの設定のまま利用されています。ブラウザ管理のベストプラクティスには、ブラウザを最適に保護するための最小限のパラメータセットの設定が含まれます。

ブラウザの管理には、企業の全体的なセキュリティポスチャに関連する次のポリシー要素が含まれます：

- バージョン管理
- 許可またはブロックされたブラウザ拡張機能の列挙
- 特定のブラウザ機能の無効化（USBインタラクションの禁止など）
- パワーユーザー機能へのアクセス制限（開発者ツールへのアクセスなど）

そしてこれらのポリシーは、企業全体に導入されているさまざまなブラウザに対して一貫性を持って展開し、適用する必要があります。

ユーザーを保護する

ユーザーを保護することは、ブラウザセキュリティの中核です。ソリューションは、一般的なものから高度なものまで、以下のようなあらゆる攻撃を防ぐ必要があります：

- ブラウザの脆弱性の悪用
- ランサムウェアを含むマルウェアのダウンロード
- フィッシング（ゼロアワーフィッシングを含む）

ブラウザが機能を追加するにつれ、悪意のある攻撃者が悪用する可能性のある潜在的な欠陥のリストが増えて行きます。2022年11月から2023年11月の間に、GoogleはChromeにおける深刻度「緊急」および「高」の問題を175件修正しました[3]。これらすべての脆弱性は、ブラウザエンジンとしてChromiumを採用しているMicrosoft Edgeやすべてのエンタープライズブラウザに影響を及ぼしました。これらの脆弱性の多くでは、悪意のあるWebサイトにアクセスするだけで任意のコードが実行される可能性があります。また、攻撃者はブラウザに昔から存在する攻撃対象を探し続けており、何年も眠っていた脆弱性を発見しています。ゼロデイ脆弱性などでは、多数のエンドユーザーデバイスのブラウザに短期間でパッチを適用する必要があるため、セキュリティとITチームは、増え続けるWeb脆弱性のリストを確認してそれらに対処するために、かなりの時間を費やす必要があります。これらの脆弱性をそのまま放置すると、攻撃者が標的のシステムでリモートコードを実行できる扉が開かれたままになり、ランサムウェアなどのマルウェアが被害者のシステムにインストールされてしまいます。このようなリスクにもかかわらず、エンタープライズユーザーが読み込んだページの25%以上が、Chromeの最新バージョンよりメジャーバージョンで2つ以上古い、深刻度の高い脆弱性を多数含むブラウザによるものであったことが確認されています[4]。

[3] 2022年11月1日から2023年11月1日の間にChromeのStableチャンネルで修正された問題のうち、重要度が「高」または「緊急」に設定された問題の総数。これらの問題の多くには、CVEが関連付けられています。

[4] 2023年11月15日の24時間にメンロセキュリティが収集した数億ページの読み込みにおける測定値に基づいています。

さらに、マルウェアやフィッシングの面でも、攻撃者はその手法とインフラを絶えず進化させています。そのため、防御側は検知ロジックとシグネチャのデータベースを常に更新し続ける必要があります。これらの先進的な攻撃は、侵入口として好んでWebブラウザを活用しています。

一部の企業では、管理されていないエンドポイントのサポートにおいて、特定のユースケースがみられます。たとえば、会社が所有していないパソコン機器から特定のアプリケーションにアクセスする必要がある、期間限定の契約社員などです。このように会社が所有していないパソコン機器のブラウザを管理を実現できます：

- 管理されていないデバイスに、エンタープライズブラウザの使用を義務付けます。ユーザーは、
  個人所有のデバイスにアプリケーションをインストールすることを強制されます。
- 管理されていないデバイスの、既存のブラウザにブラウザ拡張機能を追加するように義務付けられます。

どちらの場合もポリシーを強制でき、さまざまな働き方に合わせたポリシーにて管理をすることはできます。

アクセスとデータをセキュアにする

アクセスとデータをセキュアにすることは、ゼロトラストネットワークアクセスの戦略においても一般的です。リモートアクセスにおける戦略と実装を、従来のレイヤー3でのIPSec VPNから、最小権限でのアプリケーションアクセス（ネットワークではなくアプリケーションへのアクセス）のパラダイムに進化させた企業が、多く採用しています。アプリケーションごとのアクセス制御への移行は、企業に新たなビジネスチャンスをもたらします：

- アプリケーション（SaaSやプライベートクラウド）へのきめ細かな
  最小権限アクセス
- 管理者にとっての管理の容易さ
- エンドユーザーエクスペリエンスの向上
- インフラコストの削減

これらは通常、次のようなデータ漏洩防止と組み合わされます：

- ドキュメントとアーカイブファイルのアイソレーション
- データマスキング
- 電子透かし
- 一般的な共有プラットフォームへの読み取り専用アクセス

前述のように、エンタープライズアプリケーションの大部分は、従来のクライアント/サーバー型から最新のWebベースのアプリケーションに移行しています。企業はブラウザセキュリティを活用することで、シンプルかつ強力なアクセスポリシーとアプリケーション固有のポリシーを、グループ/ユーザーごとにきめ細かく作成できます。さらに、アプリケーション自体がそのようなポリシーをネイティブにサポートしていない状況でも、きめ細かいポリシーを作成できます。

これまで仮想デスクトップインフラストラクチャ（VDI：Virtual Desktop Infrastructure）に依存していた企業は、高額なインフラコストと劣悪なユーザーエクスペリエンスに辟易して廃止したいと考えています。そのため使い慣れたブラウザインターフェースに移行して最新のWebアプリケーションに高いパフォーマンスのユーザビリティを実現したいと考えています。それと同時に、移行先のソリューションは堅牢でなければならず、VDIが提供してきた強力な保護（機密データが画面に表示されない限りエンドポイントに届かず、バックエンドサーバーが潜在的に悪意のあるクライアントに直接公開されない）を維持する必要があります。

従来型のWebアプリケーションや未成熟なSaaSソリューションでは、ユーザーへの機密データの公開を制限するためのきめ細かな制御ができないことが多く、コンテンツフィルタリングのためのレイヤーを新たに追加する必要があります。きめ細かな制御ができる場合でも、アプリケーションごとに設定するのが困難であったり、アプリケーションの設定がセキュリティチームの管理下になかったりする場合があります。またユーザーはWebコンテンツを閲覧するだけでなく、ドキュメントをダウンロードして数ページだけ閲覧したり、ドキュメントを開かずに別のWebアプリケーションに転送したりする場合があります。さらに、ユーザーがWebコンテンツまたはドキュメントにアクセスできるようになると、意図的または偶発的（会社のポリシーに精通していないなど）に、認可されていないコンテンツをSaaSアプリケーションに貼り付けたりアップロードしたりする可能性があります。よくあるシナリオは、ChatGPTなどの生成AIサイトの利用です。ブラウザのセキュリティレイヤーはこれらすべてのシナリオにおいて、コンテンツフィルタリングポリシーを一貫して厳密に強制する必要があります。

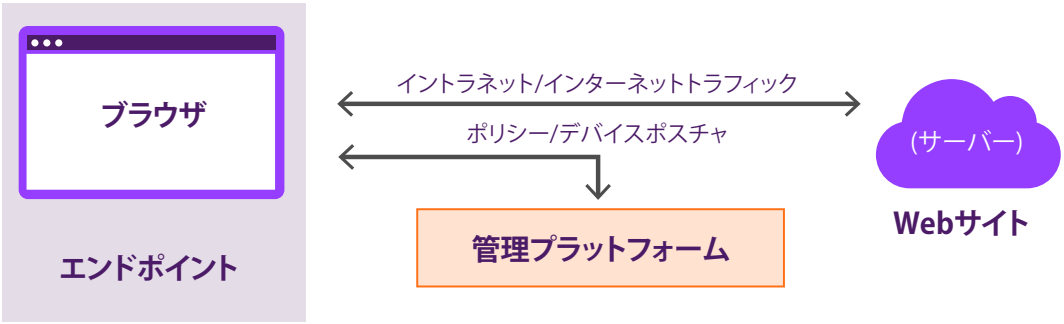
企業は、信頼できないエンドポイントや侵害されている可能性のあるエンドポイントへ機密データがさらされることを制限することに加えて、Webアプリケーションサーバーがこれらのクライアントにさらされることを減らしたいと考えています。悪意のあるクライアントが、脆弱なサーバーにエクスプロイトのためのペイロードを送信するかもしれないためです。

ローカルブラウザ（メインストリームおよびエンタープライズブラウザ）

ブラウザセキュリティの問題に対し、ローカルブラウザは2つのコンポーネントからなるソリューションで対応します。

- 一元化された（多くはクラウドベースの）管理プラットフォーム
- ブラウザ

多くのブラウザはChromiumをベースとして構築されており、ポリシーの強制やDLP機能、ローカルブラウザとファイルの間のアイソレーション機能などのエンタープライズ向けの機能を備えています。特にエンタープライズブラウザについては、エンタープライズファーストのブラウザを使用することで全体的な攻撃対象を縮小させ、セキュリティポリシーと基本的なセキュリティ機能によってセキュリティサービスエッジ（SSE：Security Service Edge）の機能を補完することで、企業とユーザーを適切に保護できるというのがソリューションの前提となっています。



ローカルブラウザを管理する方法

ローカルブラウザは、Microsoft IntuneやGoogle Chrome Enterprise Managerなどのオンプレミスまたはクラウドベースの管理プラットフォームを介して管理でき、セキュリティポリシーやその他の設定を定義してローカルブラウザにプッシュすることができます。

メインストリームブラウザの場合、追加機能を有効にするためのライセンスの問題があります。たとえばMicrosoft Intuneを使用して拡張機能を管理するためには、上位レベルのエンタープライズライセンス、Microsoft Defenderライセンス、そしてさらに追加のライセンスが必要です。

ローカルブラウザがユーザーを保護する方法

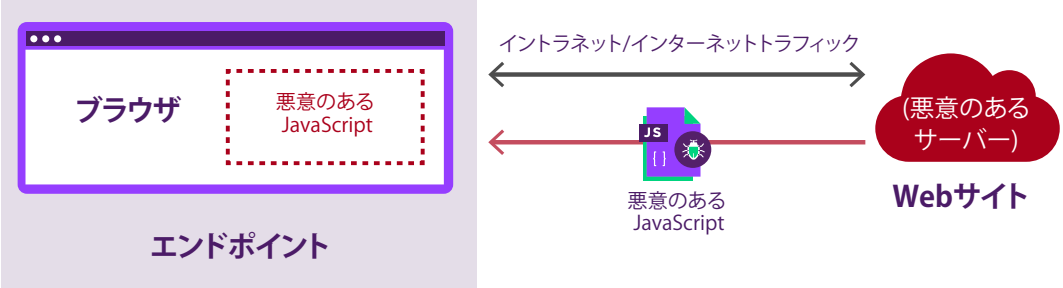
ソフトウェアの欠陥や防御メカニズムの脆弱性を攻撃者や特定の攻撃が利用できる場合、ブラウザ、デバイス、およびネットワークにリスクをもたらします。

ブラウザの脆弱性：

メインストリームおよびエンタープライズブラウザは、ローカルで実行される防御および保護の仕組みに依存しています。これは既知の脅威には有効かもしれませんが、ゼロデイ脅威には弱いという問題があります。これらのブラウザは、JavaScriptやWebGLの実行時コンパイラのような過去に脆弱性の原因となったブラウザ機能を無効にすることで、問題に対処しようとしています。しかし、機能を無効にすれば攻撃対象は縮小しますが、その機能に依存する正規のWebアプリケーションが動作しなくなり、ユーザーの作業効率が影響を受け、サポートコストが増加し、全体的なフラストレーションを高めてしまう恐れがあります。

さらにChromeのエンジニアリングチームは、ブラウザのセキュリティ問題について「これらのバグは、コードベース全体に均等に存在する[5]」と分析しています。その結果、過去12ヶ月間に修正された175件の脆弱性の多くは、ブラウザの機能に深刻な影響を与えたにもかかわらず、今でも侵害することができます。

[5] https://www.chromium.org/Home/chromium-security/memory-safety/



マルウェア（ランサムウェアを含む）：

メインストリームブラウザおよびエンタープライズブラウザは、ダウンロードされたファイルをスキャンして既知の不正なコンテンツを検知するための機能を提供します。これにはシグネチャのローカルデータベースを更新したり、検査のためにファイルをクラウドサービスに送信したりすることが含まれます。

フィッシング：

メインストリームブラウザとエンタープライズブラウザは、フィッシングの可能性があるコンテンツを検知するための機能を提供する場合があります。これらは既知のフィッシングドメインの最新のリストを使い、行動分析とコンテンツ分析によって、ページが悪意のあるものであるかどうかをリアルタイムに判断します。ポリシーベースのアクションによりページコンテンツへのアクセスをブロックしたり、ユーザー入力をブロックしたりできます。

ローカルブラウザがアクセスとデータをセキュアにする方法

アプリケーションアクセス：

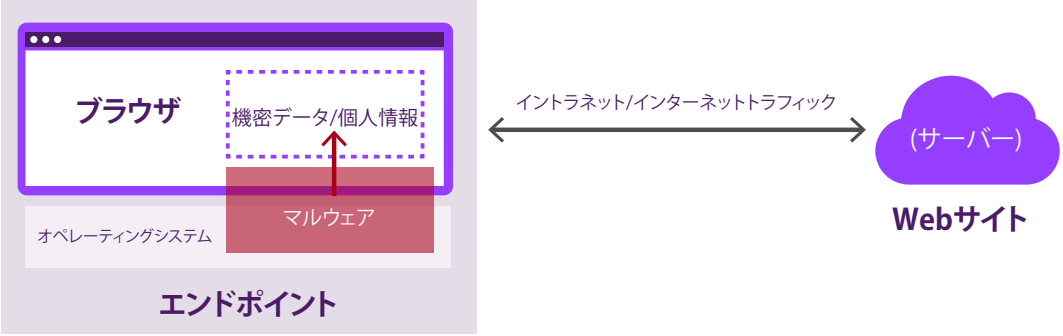
メインストリームブラウザとエンタープライズブラウザは、認可されたブラウザのみがアプリケーションサーバーにアクセスできるように制限しようとします。これは多くの場合、アプリケーション認証時にクライアントのセキュリティポスチャ（アクセスに使用されるブラウザを含む）を検証することで行われます。アプリケーションはOktaなどのIDプロバイダーを使用するように設定され、Oktaはメインストリームブラウザとエンタープライズブラウザのサードパーティコンポーネントに属するIPアドレスからの認証のみを許

可するように設定されます。認証されるとブラウザに認証トークンが発行され、ブラウザはそれをアプリケーションに提示します。これは、意欲的でない攻撃者を阻止するための小さな障害にはなりますが、Security-by-Obscurity（隠蔽/マスキングによるセキュリティ）のアプローチであり、回避することができます。攻撃者が完全にコントロールするブラウザなら、認可されたブラウザになりすますことができますし、攻撃者が認可されたブラウザのメモリから認証トークンを抽出して自身が完全にコントロールするブラウザに転送することもできます。

データ流出：

エンタープライズブラウザでは、機密データを「マスキング」することで、外部から見えないようにできます。マスキングされた情報はユーザーには表示されませんが、データのマスキングはサーバーではなくエンタープライズブラウザで行われるため、エンドポイントのメモリには存在することになります。OSまたはハイパーバイザーの制御権を持つ攻撃者はエンタープライズブラウザのメモリを読み取って情報を盗むことができますし、データの「マスキング解除」の機能を提供する場合もあります。ユーザーがマスキングされたデータを表示すると、監査ログのエントリが作成されることもあります。

ローカルにダウンロードされたファイル内の機密データを処理するために、エンタープライズブラウザが暗号化された領域にファイルを保持する場合があります。組み込みのビューアーを使用すれば、ユーザーはファイルの内容を見ることはできますが、エンタープライズブラウザが作った境界外に元のファイルをコピーすることはできません。



スクリーンショットとコピー&ペースト

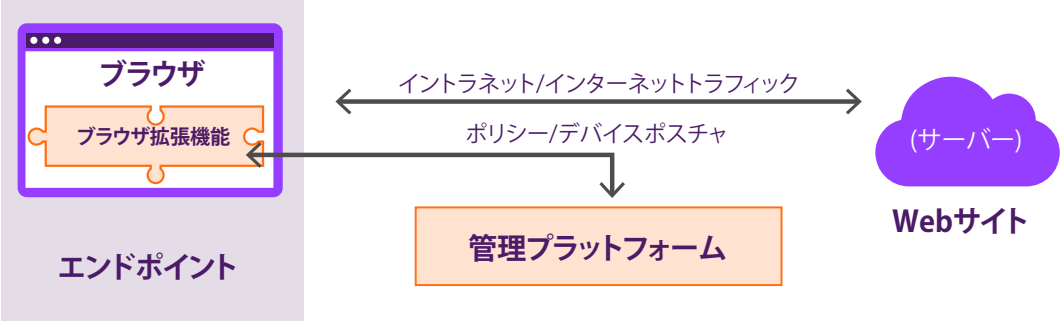
エンタープライズブラウザは、クライアントOSが提供するAPIを使用してスクリーンショットの作成やクリップボードへのデータのコピーを無効にすることができ、これは大変有効な機能です。しかしデータはエンドポイントのローカルに存在するため、エンドポイントを侵害した攻撃者はドキュメントがエンタープライズブラウザによって保護される前に、ネットワークバッファ内のドキュメントを「盗む」ことができます。スクリーンショットについては、エンタープライズブラウザは技術的に未熟な攻撃者への対抗策を提供します。技術的に未熟な攻撃者がスマートフォンなどで画面の写真を撮ることは依然としてできますが、それはさらなる制限を必要とする他の手段によって防ぐことができます。OSやハイパーバイザーを制御できる技術的に高度な攻撃者は、画面に送られたコンテンツを簡単にキャプチャし、エンタープライズブラウザが提供する保護を回避します。

ブラウザ拡張機能

ブラウザ拡張機能は、既存のメインストリームブラウザにインストールしてブラウザのセキュリティ機能の代替実装を提供します。市場には、さまざまな機能を持つブラウザ拡張機能があります。ブラウザ拡張機能およびそれに関連する機能は、ブラウザベンダーが提供するAPIのポリシー変更による影響を受けます。ブラウザのセキュリティ拡張機能が利用する機能やAPIは、悪意のある第三者がマルウェアを作成する際に使用される可能性があるため、ブラウザベンダーはブラウザ拡張機能の機能を制限し始めています。これは、ブラウザのベンダーによって異なります。

ブラウザ拡張機能を管理する方法

ブラウザ拡張機能は、ユーザーが利用しているほぼすべてのブラウザに対応しており、エンドユーザーの操作をほとんど必要とせずにインストールできます。その後、拡張機能は中央の管理プラットフォームと対話を始めます。



ブラウザ拡張機能がユーザーを保護する方法

ブラウザの脆弱性：

拡張機能を導入展開すると、Webの脅威に対する可視性と基本的な保護機能が提供されます。これらの拡張機能は、他のブラウザセキュリティソリューションが提供する機能のサブセットを提供します。既知の不正なURLからのコンテンツをブロックすることはできますが、攻撃対象を縮小させるためにブラウザの動作を大幅に変更することはできません。

マルウェア（ランサムウェアを含む）：

ユーザーによりダウンロードされた悪意のあるコンテンツを閲覧したりスキャンすることができず、マルウェアに対する保護はほとんどありません。

フィッシング

ブラウザ拡張機能は、フィッシング対策においてエンタープライズブラウザと同様のアプローチを取ります。

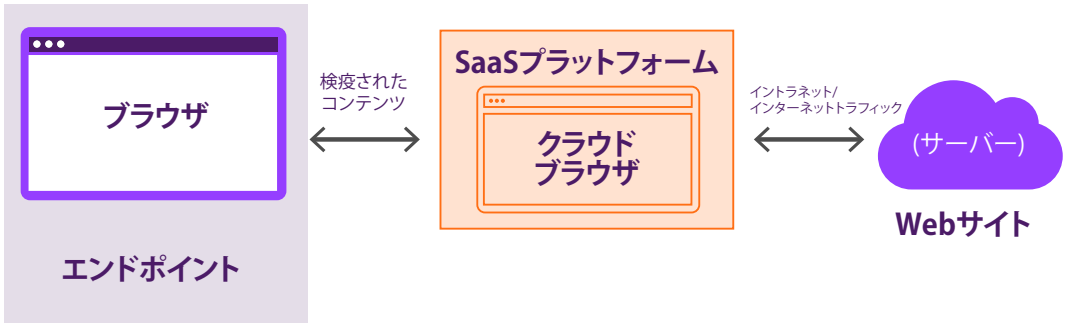
ブラウザ拡張機能がアクセスとデータをセキュアにする方法

アプリケーションアクセス：

ブラウザ拡張機能は、組織にアプリケーションの可視性を提供します。これらの拡張機能をインストールすると、機密性の高いユーザーや機密性の高いアプリケーションを識別するのに役立つ情報が提供されます。適切な情報があれば、組織はアプリケーションへの安全なアクセスを提供するためにどのようなアクションを取る必要があるかを理解できます。ただし、拡張機能はアンインストールが比較的簡単であるため、管理されていないデバイスには推奨されません。

従来型のリモートブラウザアイソレーション

従来型のリモートブラウザアイソレーション（RBI：Remote Browser Isolation）は、ゼロトラストアプローチによってWebおよびメールベースのマルウェアから組織を保護するものでした。RBIでは、すべてのWebトラフィックをクラウドベースのリモートブラウザ経由でルーティングします。コンテンツの善悪や、カテゴライズされているかされていないかに関係なく、すべてを潜在的に悪意のある可能性のあるものとして扱い、安全で検疫されたコンテンツのみをエンドユーザーに届けます。このアプローチでは、リモートのディスプレイでレンダリングされたピクセルをキャプチャし、必要に応じてビデオ圧縮を行った後にクライアントに送信します。このアプローチではユーザーとクラウドプラットフォームの間に広帯域幅の接続が必要となり、多くの場合ユーザーエクスペリエンスは従来とは異なるものになります。



RBIがブラウザを管理する方法

RBIの提供範囲には入りません。

RBI がユーザーを保護する方法

ブラウザの脆弱性、マルウェアおよびフィッシング：

通常、Webトラフィックはカテゴライズされずに、仮想化されたクラウド環境で強制的に実行されます。悪意を持っているかもしれないWebコンテンツはユーザーから離れた場所で実行されるため、エンドポイントに届くことはありません。ユーザーは悪意のあるサイトや添付ファイルの代わりに、クラウドでレンダリングされた安全なコンテンツを確認し、それを操作します。

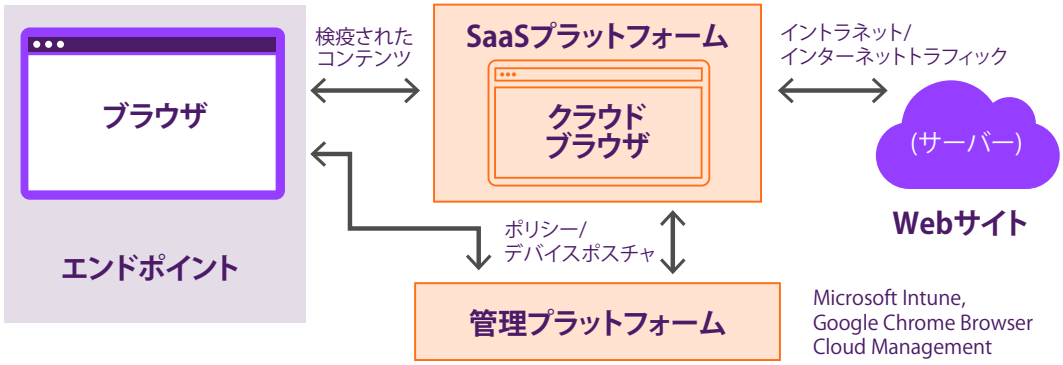
RBIがアクセスとデータをセキュアにする方法

RBIの提供範囲には入りません。

クラウドベースのブラウザセキュリティ

クラウドベースのブラウザセキュリティは、エンタープライズブラウザとブラウザ拡張機能、そしてリモートブラウザアイソレーションのハイブリッドを提供します。ブラウザはすべてのWebトラフィックをクラウドベースのブラウザセキュリティプラットフォームにルーティングするように設計され、これにより悪意を持つ可能性のあるアクティブコンテンツをブロックし、必要に応じて機密データを削除することができます。このアプローチにより、組織は任意のデバイスの任意のブラウザに対してブラウザセキュリティを有効にできます。クラウドベースのブラウザセキュリティは従来型のRBIとは異なり、より効率的なコンテンツベースのRBIを採用しています。これにより、ネイティブに近いユーザーエクスペリエンスを実現し、従来型のRBIで課題であった高帯域幅の接続を必要とする要件が緩和されます。その結果このアプローチでは、多くの場合「リスクがある」Webサイトのごく一部でしか使えなかった従来のRBIとは異なり、ユーザーが行うすべてのブラウジングを保護することができます。

たとえばメンロセキュリティのプラットフォームは、毎日数百万というユーザーのWebアクティビティの大部分を保護すると同時に、数千ものWebアプリケーションのデータアクセスも制御しています。セキュリティはクラウドを通じて提供されるため、ユーザーがオフィスや外出先、会議、顧客先など、どこにいても保護することができます。
さらに、ユーザーのエンドポイント側のセキュリティポスチャに関係なく、保護されたWebアプリケーションにアクセスするすべてのユーザーを保護します。これにより、アクセスされるデータについても、VDIのような非常に高価で手間のかかるアプローチと同等のセキュリティが保証されます。



クラウドベースのブラウザセキュリティがブラウザを管理する方法

管理機能：

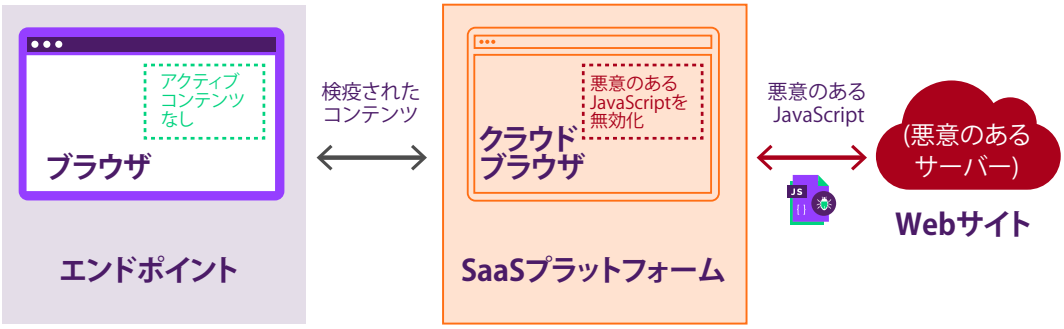
クラウドベースのブラウザセキュリティは、ブラウザに依存しないアプローチを採用しており、ブラウザ管理においてセキュリティを重視しています。クラウドベースのブラウザセキュリティは、GoogleやMicrosoftなどのメインストリームブラウザベンダーの管理機能をベースにしており、その上に構築されています。

さらに、このアプローチによってチーム間の委任関係を合理化できます。すべてのポリシー管理を1つのチームに一元化するのではなく、デスクトップチームがポリシーのサブセットの制御をセキュリティチームに委任するといったことができます。またクラウドベースのブラウザセキュリティは、ブラウザに依存しない方法でポリシーの作成を集約して簡素化します。各ポリシーを個々に操作するのではなく、ポリシーはグループ化され、ボタンをクリックするだけで複数のブラウザに対して有効にすることができます。

クラウドベースのブラウザセキュリティがユーザーを保護する方法

ブラウザの脆弱性：

クラウドベースのブラウザセキュリティは、攻撃対象を大幅に縮小することができます。ブラウザでどの機能を無効にするかをいちいち決めるのではなく、すべての機能はデフォルトでクラウドで実行され、エンドポイントまでは届きません。クライアントがその機能を必要とする場合でも、悪意を持つWebサイトにAPIが直接さらされることはありません。このようなアプローチにより、顧客が機能をサポートするかしないかを選択する必要はなく、セキュリティリスクを生み出す恐れはなくなります。その代わりに、この機能はクラウドで安全に実行されます。攻撃者はユーザーのブラウザでコードを実行できないため、前述のChromeの脆弱性を悪用してエンドポイントを侵害することもできません。

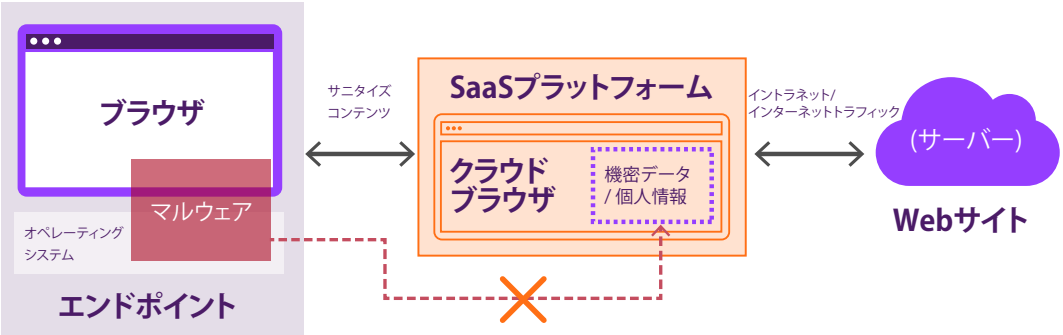


たとえば、インタラクティブな2Dおよび3Dグラフィックスをレンダリングするための JavaScript APIであるWebGLがサポートされているため、WebGLのセキュリティ問題を気にする必要はありません。これは、WebGLによるクライアント側のコンテンツ作成が、すべてクラウドブラウザで行われるためです。同様に実行時コンパイラも無効にする必要はありません。ページのJavaScriptは実行時コンパイラを安全に活用できるクラウドで実行されます。その際、ユーザーエクスペリエンスは影響を受けません（実行時コンパイラを無効にすると、重いJavaScriptページがさらに遅くなる可能性があります）。

ユーザーを保護するための重要なポイントは、常にブラウザを最新に保つことです。このアプローチでは、クラウドブラウザは自動的に更新されます。ユーザーデバイスの電源がオフになっていたり、回線が低速なために大規模な更新をプッシュすることが難しい場合でも、ブラウザを更新することができます。繰り返しになりますが、安全でない決断（古いクライアントからも閲覧できるようにする）とユーザーに不親切な決断（接続が遅い場合でも、閲覧前に強制的に更新プログラムをダウンロードさせる）の間にトレードオフは無く、どちらも避けなければなりません。

マルウェア（ランサムウェアを含む）：

クラウドベースのブラウザは、エンドユーザーがダウンロードしようとしたすべてのファイルを完全に可視化するため、ファイルがクライアントに送信される前にこれらのファイルを分析できます。メインストリームブラウザやエンタープライズブラウザと同様に、ファイルの内容はAVおよびサンドボックスタイプのアプローチでスキャンできます。その一方で、メインストリームブラウザやエンタープライズブラウザとは異なり、スキャンエンジンとシグネチャデータベースは、SaaSプラットフォームで常に最新の状態に保たれます。また、悪意があると判断されたペイロードがエンドポイントまで届くこともありません。



フィッシング：

クラウドベースのブラウザは、ユーザーに向けて送信されたすべてのコンテンツをレンダリングし、ユーザーからのすべての入力を監視するため、既知の不正な行動とコンテンツをベースとしたエンタープライズブラウザと同じタイプのアプローチを実装できます。エンドポイントに足場がなくともこれを行うことができるため、すべてのエンタープライズユーザーに一貫した保護を提供できます。検知のためのすべてのロジックとシグネチャはクラウドで実行されるため、最新の検知機能をすべてのブラウザに即座に適用できます。このような「遅延時間ゼロ」の保護機能は、進化し続けるフィッシングコンテンツと戦うために重要です。

クラウドベースのブラウザセキュリティがアクセスとデータをセキュアにする方法

アプリケーションアクセス：

ユーザーはクラウドブラウザを介してのみ、保護されたサーバーにアクセスできます。攻撃者はクラウドブラウザを改ざんする能力を持っていないため、ソフトウェアスタックの特権的なレイヤーを制御することはできません。また攻撃者は、クラウドベースのブラウザのメモリを調べたりセッショントークンを盗んだりして脆弱なアプリケーションと直接やり取りすることもできません。これは安全なネットワークパスが設定されているためで、ブラウザセキュリティプラットフォームを通過するすべてのトラフィックはそれを通らなければならないのです。

このアプローチは、攻撃者から離れたクラウドでソフトウェアが安全に実行されるVDIベースのアプローチに似ています。しかし、ユーザーがソフトウェアをインストールしたり、リモートOSを狙うことができるVDIとは異なり、ブラウザセキュリティへのクラウドベースのアプローチでは、ブラウザを実行しているオペレーティングシステムがさらさ

れることはありません。この環境では、攻撃者はクラウドブラウザを標的にして、ページ内をクリックしたりフォームにキーボード入力したりすることしかできません。また、強制的に読み取り専用モードにすることもでき、入力がオフにされるとユーザーはデータを入力できなくなり、マウス操作のみで目的のサイトと対話することになります。

データ流出：

クラウドベースのブラウザセキュリティにおいては、機密データをエンドポイントにまったくダウンロードしません。このアプローチでは、マスキングされたデータを確実に保護するだけでなく、改ざんできない監査ログも提供します。つまり、ユーザーが機密性の高いフィールドのマスキング解除を行った場合、攻撃者が改ざんできない方法でその行動をログに記録できるのです。ユーザーが悪意を持っていることが判明した場合、盗まれた個人情報（PII：Personary Indentifiable Information）の「影響範囲」について、正確な全体像を把握することができます。

これはファイルにも適用されます。これらはユーザーから離れたクラウドにある真に保護された領域に保管でき、ユーザーはクラウドビューアーによってファイルの一部のみを表示したり（プラットフォームはファイルのどの部分が表示されたかを正確に追跡できます）、エンドポイントに触れることなくWebアプリケーション間でファイルをコピーしたり（Gmailの添付ファイルを取得してBoxフォルダに入れるなど）できます。

まとめ

世の中にはブラウザを保護するためのさまざまなソリューションがありますが、まずビジネスニーズを特定し、ブラウザセキュリティの主要な機能を理解して、組織に適したソリューションを見つけることが重要です。企業は長年にわたりブラウザセキュリティに取り組み、セキュリティツールをパッチワークのように導入してきましたが、業界はクラウドベースのソリューションに移行しつつあります。最終的にブラウザとユーザー、そしてアプリケーションを標的とする脅威に大規模かつ最適に対処できるのは、クラウドベースのブラウザセキュリティなのです。

ブラウザセキュリティについての詳細については、menlosecurity.com/ja-jp/をご覧いただくか、japan@menlosecurity.comまでお問い合わせください。

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

Menlo Securityについて

Menlo Securityは、他に類を見ないアイソレーションを活用したクラウドセキュリティプラットフォームにより、企業が脅威を排除し、生産性を完全に維持することを可能にします。Menlo Securityは、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提供し、エンドユーザーはセキュリティの存在を気にせずにオンラインで仕事をすることができ、さらにセキュリティチームの運用負担を軽減することで、クラウドセキュリティの目標を実現できる唯一のソリューションとなっています。これにより企業は安全なオンライン体験を提供することができ、ユーザーは安心して業務を行いビジネスを進めることができます。

ブラウザセキュリティの機能比較

この表は、前掲の各テクノロジーがどのようにブラウザセキュリティの重要な機能をサポートしているかを示しています。これらの機能は、ユーザーを保護し、企業を保護し、管理者とエンドユーザーの双方にとって優れたユーザーエクスペリエンスを維持するために重要です。

		メインストリーム/エンタープライズブラウザ	ブラウザ拡張機能	従来型のRBI	クラウドベースのブラウザセキュリティ
管理ブラウザ	ブラウザ設定	●	● 制限あり	●	● エンタープライズブラウザマネージャが提供するAPIを介したクロスプラットフォーム
	スクリーンショット機能	● 回避可能	●	●	●
	デバイスポスチャチェック	●	●	●	● エージェントが必要な場合あり
	拡張機能	●	●	●	● エンタープライズブラウザマネージャが提供するAPIを介したクロスプラットフォーム
保護ユーザー	ブラウザ脆弱性からの保護（ゼロデイを含む）	●	●	● クラウド内のすべてのアクティブコンテンツ	● クラウド内のすべてのアクティブコンテンツ
	マルウェアからの保護	●	● ダウンロードファイルの可視性に制限あり	● エンジン/シグネチャのアップデートが容易；クロスデバイス	● エンジン/シグネチャのアップデートが容易；クロスデバイス
	フィッシングからの保護	●	●	● エンジン/シグネチャのアップデートが容易；クロスデバイス	● エンジン/シグネチャのアップデートが容易；クロスデバイス
セキュアアクセスとデータ	データ流出防止	● 高度な攻撃者によって回避可能	●	● 範囲外	● 保護されたデータはエンドポイントに届かない
	データ削除	● 高度な攻撃者によって回避可能	●	● 範囲外	●
	電子透かし	●	●	● 範囲外	●
	アプリケーションアクセス	● 高度な攻撃者によって回避可能	●	● 範囲外	● クラウドブラウザのみからアクセス可能
	コピー&ペースト	● 高度な攻撃者によって回避可能	●	● 範囲外	●
	拡張機能の露出	●	●	● 範囲外	● クライアント拡張機能への露出は無し
	ログと監査	● 改ざん防止性なし	●	● 範囲外	●