CLOUDFLARE

製品概要

Cloudflare Browser Isolation インターネット接続のためのビルトイン型Zero Trust

Zero Trustをインターネットへ拡張

広い攻撃対象領域、限られた制御

現在、Webブラウザは最も広く普及している企業アプリケーションで、攻撃対象領域も大きくなっています。

しかし、ブラウザベースの脅威に対するこれまでのユーザー保護は完璧とはいいがたく、ユーザーと機密情報のインタラクションの安全を確保する制御の適用はなおさら困難でした。

Zero Trustを完璧に

ブラウジングにZero Trustを適用するということは、デバイス上で実行されるコードや操作を信用しないのがデフォルトだということを意味します。

Cloudflare Browser Isolationはすべてのコードを当社のエッジで実行し、信頼できないWebコンテンツからユーザーを隔離し、信頼できないユーザーやデバイスのブラウザ操作からデータを保護します。

平均的なリモートブラウザとは違う

- 互換性があり、どのWebページでもどのブラウザでも動作可能です。
- パフォーマンスがよく、遅延の少ないWebページストリームを実現します。

使用中のデータを信頼されていないユーザーやデバイスから保護し、デバイスとユーザーをランサムウェアやフィッシングから保護 — ゼロディ攻撃に対しても万全。

今すぐお試しください
インストールは不要です

後付けではない内蔵型セキュリティ

Cloudflareで構築

当社のブラウザ分離は、ネットワーク上の他のZero Trustサービスと共にゼロから構築されており、275か所以上の拠点で実行できるように設計されています。

Webブラウジングのセッションは、可能な限りユーザーに近い場所で提供され、高速な体験を保証します。

ネイティブ統合

他のプロバイダーとは異なり、Cloudflareはすべてのzero Trustサービスにブラウザの分離をネイティブに組み込んでいます。

単一インターフェースで管理：

- セキュアWebゲートウェイ（SWG）
- Zero Trustネットワークアクセス（ZTNA）
- クラウドアクセスセキュリティブローカー（CASB）
- クラウドメールセキュリティ（ロードマップ上）
- など

攻撃領域を削減
Zero Trustブラウジングは、未カテゴリ、高リスク、さらには低リスクのサイトの悪意のあるコードが、ユーザーのデバイスに侵入するのを阻止します。

デプロイを簡略化
Zero Trustのブラウジングポリシーを、アプリケーションアクセスの管理と同じ場所で設定します。

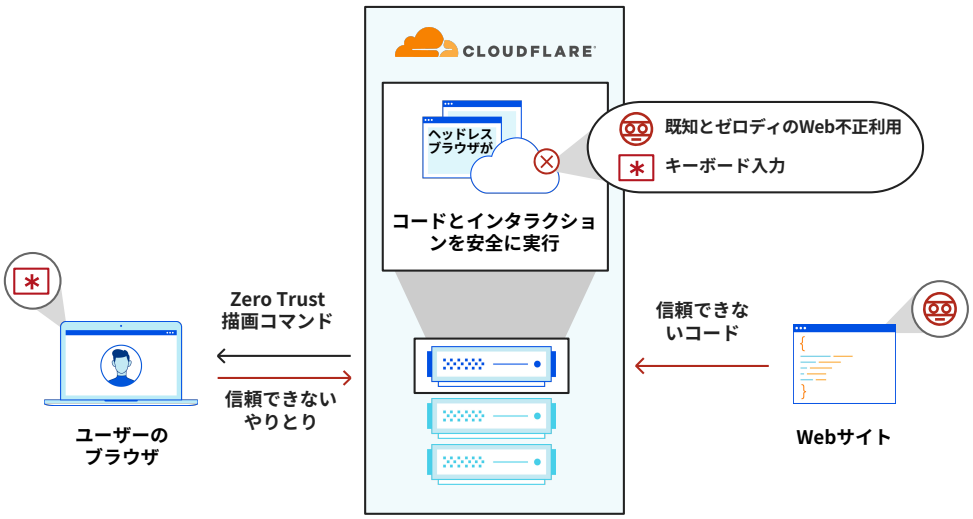
データを保護
アプリケーション内やリスクのあるサイト内でのユーザーアクション（キーボード入力、コピー、印刷、アップロード、ダウンロード）をコントロールすることで、データの損失とフィッシングの脅威を阻止します。

ユーザーエクスペリエンスを損なうことなく攻撃対象領域を最小化

課題：
既知の脆弱性に対して常に最新のパッチを全ブラウザに適用できているITチームはありません。しかも、たとえ最高のインテリジェンスがあっても、フィルターや検査で脅威を100パーセント防止、検出できることはまずないのが現実です。すべてのサイトをブロックしても解決にはなりません。過剰な制限はかえってユーザーの生産性を低下させかねません。

解決策：
当社のBrowser IsolationはChromiumブラウザのヘッドレスバージョンを実行します。これにより、すべてのブラウザコードをお客様のエンドポイントではなく当社のエッジでレンダリングし、マルウェアなどの既知および未知の脅威を軽減します。低遅延のためエンドユーザーには気付かれず、まるでローカルブラウザのように感じられるのです。

仕組み



デバイスクライアントと共にデプロイ
ユーザートラフィックをデバイスからCloudflareのグローバルネットワークに送り、L4-7の十分なフィルタリングと検査を行います。

クライアントレスのデプロイメント
ユーザーのパブリックIPやデバイスを、サイト上で悪性かもしれないコードに露出することなく、ユーザーを分離されたハイパーリングへ送ります。

主なユースケース

ランサムウェア

分離することでランサムウェアの感染を効果的に防ぎます。しかし、分離されていないサイトでも、危険なサイトやドメインをブロックするSWGや、脅威のラテラルムーブメントを抑えるZTNAなどのサービスとネイティブに統合することで、防御力を強化することができます。

フィッシングとメールセキュリティ

分離は、フィッシングリンクに含まれる有害なコードがローカルで実行されるのを阻止するだけでなく、機密性の高い個人情報のキーボード入力も阻止します。さらに近日中に、管理者がArea 1を使ってワンクリックでメールフィルタリングを有効化できるようになります。

ゼロデイ攻撃

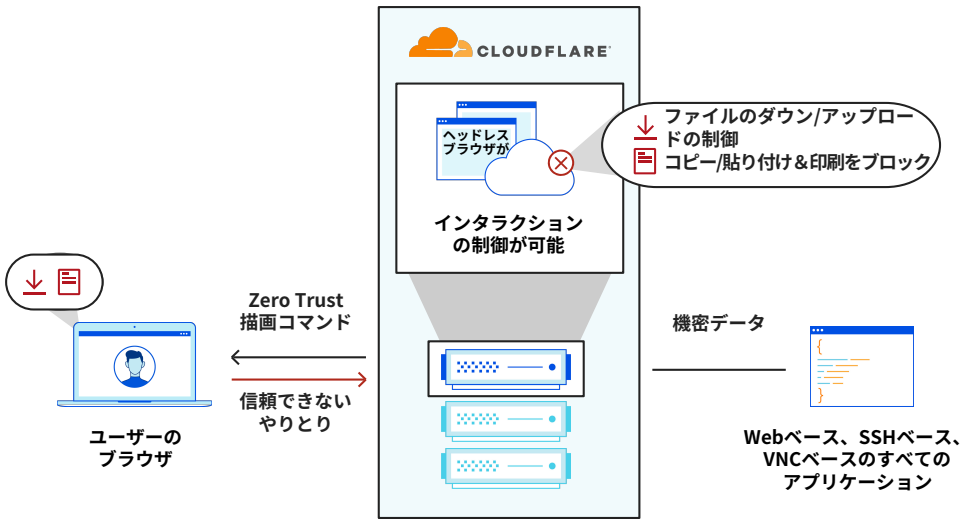
ゼロデイ脆弱性に対するパッチが提供された場合、Cloudflareはネットワーク上のすべてのリモートブラウザに自動的にパッチを展開します。このため、管理者は、強制的なアップデートのためにユーザーの作業を中断させることなくデバイスを保護することができます。

Webブラウザ内のデータを保護

課題：
SaaSソフトウェアが普及し、Webブラウザはユーザーがデータにアクセスする主要手段となりました。しかし、従来、いったんブラウザへ送られたデータについては管理者は限定的な制御しかできませんでした。ユーザーは、機密データや個人識別可能情報をコピーして、他のWebサイトやアプリ、ロケーションへ張り付けたり印刷したりできるのが通常です。そうした行動は珍しくなく、データ漏洩のリスクを増大させます。

解決策：
分離されたブラウザを起動すると、あらゆるWebサイトやSaaSアプリケーションの機密データを保護するための制御が管理者に戻ります。管理者は、数回のクリックで、ブラウザ内でリスクのあるユーザーの行動を防止するきめ細かいルールを作成することができます。これには、ダウンロード、アップロード、コピーペースト、キーボード入力、印刷機能の制限が含まれます。

仕組み



デバイスクライアントと共にデプロイ
ユーザーがマネージドデバイス上でどのようにデータとインタラクションを行っているかを完全に可視化し、デバイスポスチャに応じたポリシーを作成します。

クライアントレスのデプロイメント
アンマネージドデバイスでユーザーが日常的にアクセスする可能性が高い機密データ（顧客データなど）を扱うアプリを分離します。

主なユースケース

請負業者のアクセスを保護

ユーザーの端末にソフトウェアをインストールすることなく、特定のハイパーリンクへの接続を分離することができます。

このクライアントレスモデルを使用すれば、アンマネージドデバイス上で請負業者がインタラクションするデータを保護できます。追加設定コストは発生しません。

不審サイトでの入力を制御

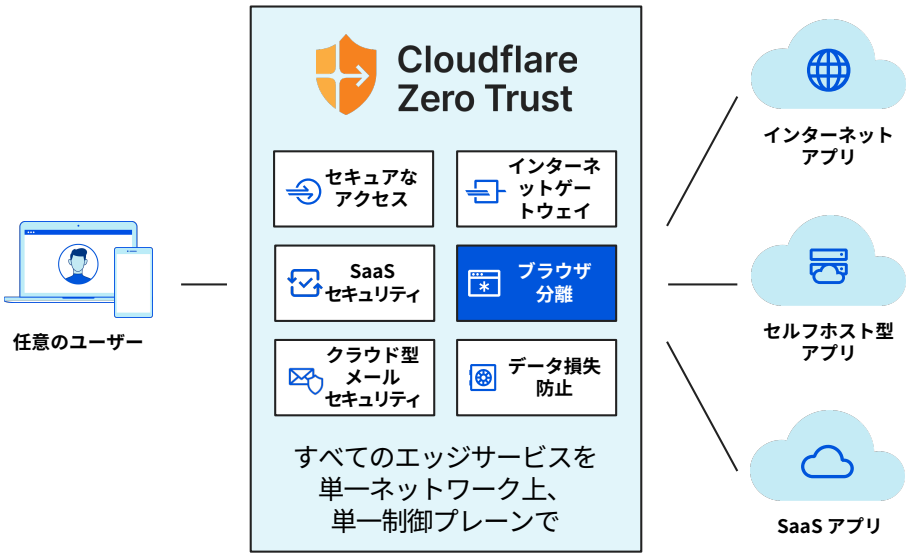
管理者は、「タイポスクワッティング」や「ドメイン」などのフィッシングによく使われるリスクの高いWebサイトを隔離することで、チームを保護することができます。Cloudflareは、サイトを読み取り専用モードで提供し、ファイルのアップロード、ダウンロード、キーボード入力を無効にしています。

サードパーティソリューションとの統合

クライアントレスな展開ができることで、管理者はCloudflareを既存のWebゲートウェイやメールゲートウェイと統合して、従来のサービスから段階的に移行することができます。リスクの高いクリックをリモートブラウザに送信し、カスタムブロックページなどの防御を適用します。

ブラウザ分離：Zero Trustの基本

分離はZero Trust原則の中核です。CloudflareのZero Trustプラットフォームで数クリックするだけで、可視性と制御をブラウザにも広げることができます。



分離が容易に
ブラウザ分離は以前は高価で複雑だったため、大企業だけが買えるスタンドアロン型のソリューションとして存在していました。

Cloudflareは、ZTNA、SWG、その他のSSEサービスとのネイティブ統合により、ブラウザ分離でZero Trustをさらに進める前に妥当なところからセキュリティ最新化を始めやすくなっています。

ローカル vs. リモートブラウジング

ローカルブラウジング
信頼できないWebページのコードとフィッシングサイトが、エンドポイントデバイスのローカルで実行されます。ユーザーはフィッシングWebサイトやデバイスへ無意識に機密データを入力でき、データはパッチ未適用の脅威やゼロデイの脅威に直接晒されてしまいます。

リモートブラウジング
フィルタリングされていないコードやサイトが、常時パッチが適用されるリモートブラウザで実行されます。ユーザーのインタラクションを制御してマルウェアやフィッシング攻撃を防止し、ゼロデイ攻撃をエンドユーザーのデバイスから遮断します。

Cloudflareのアプローチ

ネットワークベクトルレンダリング（NVR）
帯域幅に負担のかかるピクセルプッシュや脆弱なコンテンツの無害化と再構築技法とは異なり、NVRは悪意のあるWebページのコードを転送したり、エンドユーザーの使用感に影響を及ぼすことなく、安全な描画コマンドをデバイスにストリーミングします。

当社のグローバルネットワーク
他のプロバイダーは、パブリッククラウドプロバイダーでリモートブラウザをホストしています。Cloudflareではユーザーがどこからでもローカルで操作しているときと変わらない操作感を得られるよう、ブラウザをユーザーの近くに配置しています。

主な機能

- すべてのブラウザコードをユーザーから遠く離れたクラウドで実行
- ピクセルプッシングなし
- 超高速ネットワーク（世界のインターネットユーザーの95%から50ミリ秒以内）
- すべての最新ブラウザとの互換性
- デバイスクライアントの有無にかかわらずデプロイ可能
- 企業アプリケーションからのデータ漏えいを阻止し、シャドーITの可視性を確保
- ネットワークファイアウォールからのインテリジェンスとZero Trustルールによって、脅威をブロック
- 稼働率100%を保証するSLA

より高速で安全なブラウジング体験を今すぐ

Browser Isolationを試す