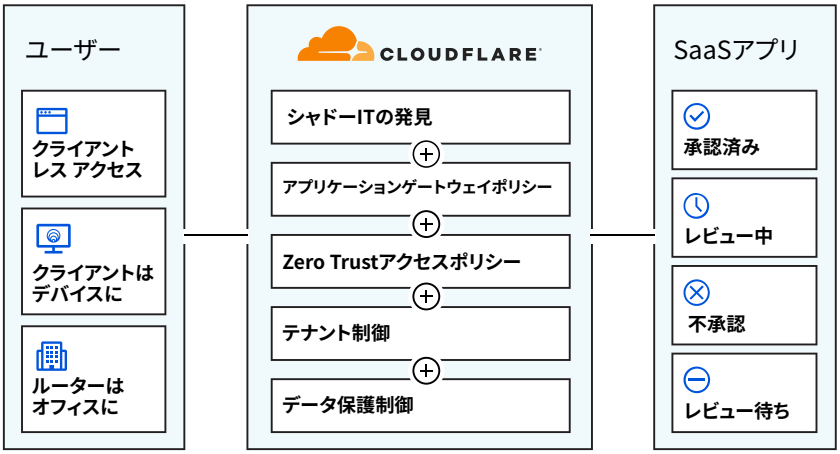
ソリューション概説

あらゆるSaaSアプリケーションで Zero Trustの可視性と制御を実現

SaaSアプリケーションを導入することで、チームはこれまでより多くの成果を上げられるようになりました。ただし、チームが柔軟性と自由度を手にする反面、組織はセキュリティリスクや可視性の課題、アクセス制御の問題などに直面することになりました。

Cloudflareは、お客様がデータと従業員を保護するのに不可欠な一方で、従業員が仕事を遂行するのに役立つツールを提供しています。



シャドーITの発見と管理

従業員の使用しているアプリケーションを可視化できなければ、機密データの格納、共有、第三者への漏えいを制御することはできません。Cloudflareは、貴社内での承認済み・未承認のアプリケーションをことごとく検出、分類、制御し、すべての接続とリクエストを一元化されたロケーションでログに記録します。

Zero Trustアクセスポリシーの適用

SaaSアプリケーションは企業ネットワークの外でホストされているため、貴社のセキュリティチームは、アプリケーションへのユーザーアクセスやデータの出入りに関して限定的な管理能力しか持ちません。Cloudflareは、Zero Trustセキュリティ対策のレイヤーをお客様のSaaSアプリケーションの前に置き、正当なユーザーを認証し、貴社のファイルやデータに許可のないユーザーや危険なデバイスがアクセスするのを阻止します。

テナント保護・データ保護の制御を適用

従業員がアプリケーションの間違ったインスタンスにアクセスすると、自社データを不適切な場所で共有・格納してしまう可能性があり、データ漏えいやその他のセキュリティリスクを招きかねません。Cloudflareは、当社ネットワーク上を転送中であろうと、当社のリモートブラウザ内で使用中であろうと、貴社のデータの共有と格納を制御しやすくします。お客様は、Zero Trustブラウジングポリシーを構築してデプロイし、従業員が間違ったアプリケーションや承認済みアプリケーションの間違ったテナントにアクセスするのを防ぎながら、あらゆるSaaSテナント内にあるデータを保護することができます。

シャドーITの発見と管理

従業員が使用するアプリケーションの評価

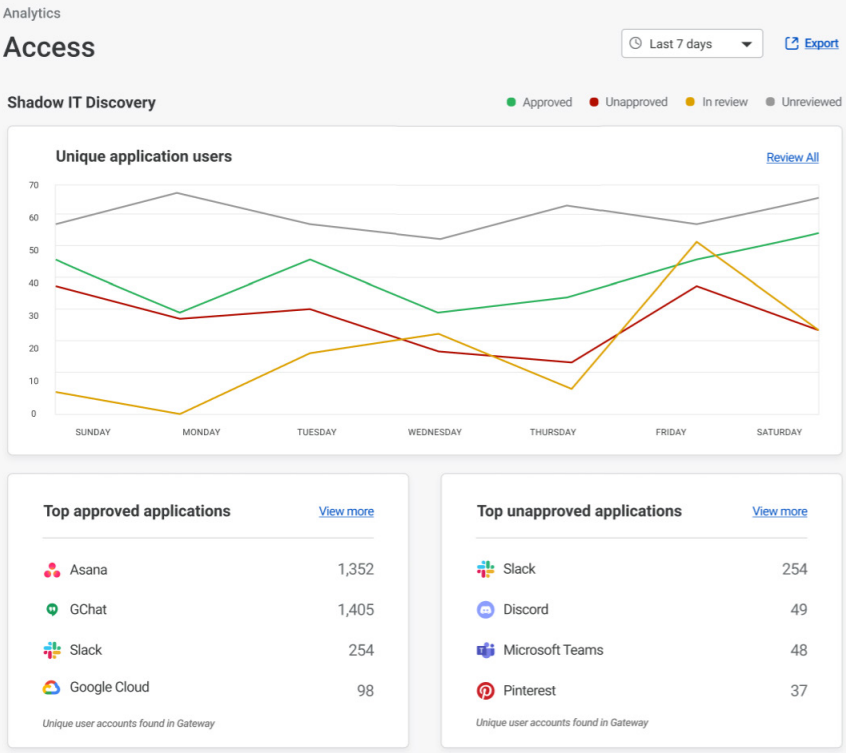
ITチームが従業員の使用しているアプリケーションを見られなければ、アプリケーション上でデータに起こっていることを制御することはできません。Cloudflareは、活動ログですべてのHTTPリクエストを集計し、自動的にアプリケーションタイプ別に分類します。それを基にステータスを設定し、会社全体で承認済みと未承認のアプリケーションを追跡できます。

すべての接続とリクエストをログに記録

従業員が正式に承認されていないアプリケーションにアクセスしたり管理対象外のデバイスで機密情報にアクセスしたりすると、組織にリスクをもたらします。Cloudflareはそうしたリスクの軽減に役立ちます。接続とリクエストはすべて一元化されたロケーションでログに記録され、どのアプリケーションが使用中で、ユーザーがそこでどのような活動をしているかを把握できます。管理者は、SaaSアプリケーションへのリクエストをブロックしたり許可したりする権限も持ち、ユーザーが重要なセキュリティ制御をかいくぐって組織内のアプリケーションやリソース、データに許可なくアクセスするのを阻止します。

主な特徴

- Cloudflareによって既に保護されているアプリケーションを自動追跡します。
- ログをCloudflareネットワークに最長6か月保持します。
- お客様のクラウドログストレージおよびSIEMサービス（1か所または複数）にログをプッシュします。



SaaSアプリケーションにZero Trustアクセスポリシーを適用

CloudflareのIDプロキシを介してSaaSへのアクセスを保護

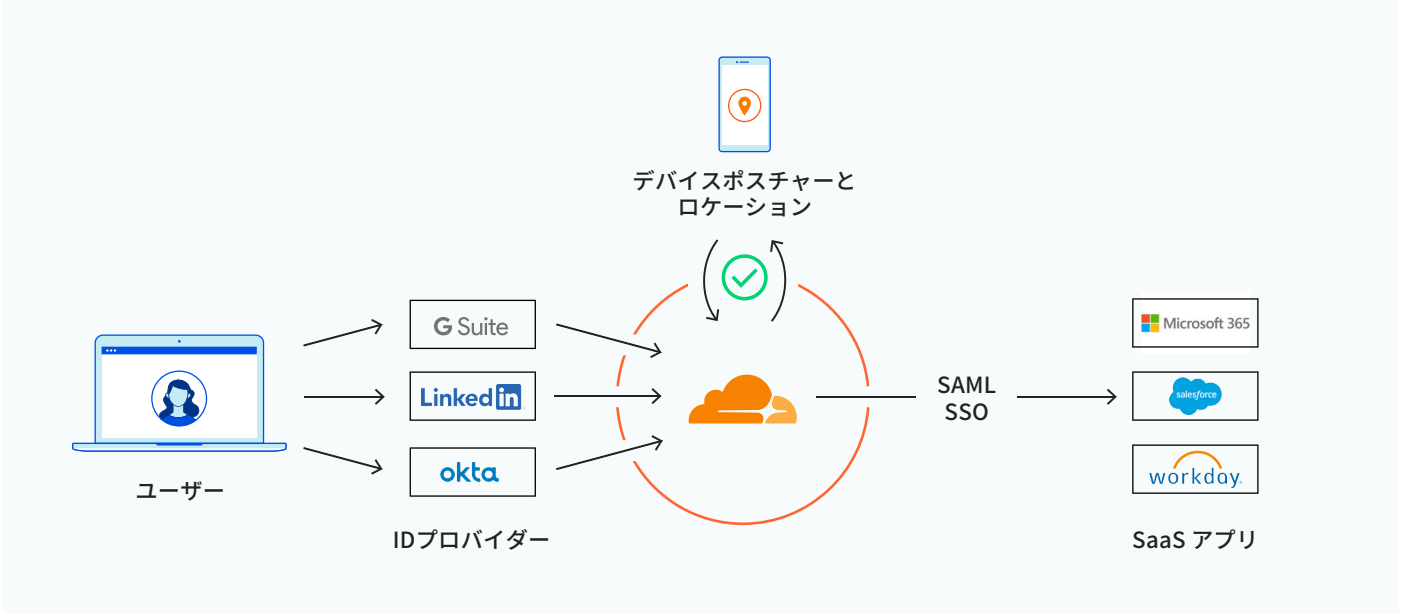
SaaSアプリケーションは第三者にホストされるか、ビジネスユニットに管理されることが多いため、ITチームはユーザーがアプリケーションにアクセスする方法についてほとんど発言権を持たないのが一般的です。Cloudflareはお客様のIDプロバイダーとSaaSアプリケーションの間にあって、お客様がID認識型、コンテキスト主導型のZero Trustルールを作成し、ログインのプロセスに適用できるようにします。この流れでエンドユーザーエクスペリエンスが損なわれることはありません。

ユーザーデバイスに対するアプリケーションのアクセス許可を判定

IT部門は、会社の管理するデバイスがSaaSアプリケーションにログインする方法について、きめ細かく制御する必要があります。Cloudflareは、SAML認証をサポートするすべてのアプリケーションについて、シングルサインオンプロセスに、Zero Trustルールを挿入します。まず、ユーザーはIDプロバイダーの認証を受け、次にCloudflareがデバイスポスチャーやロケーションに照らしてリクエストを検証し、SaaSアプリへのアクセスを許可します。その際、継続的な検証では柔軟なセッション管理が行われます。また、セキュリティ管理者はデバイスごとのポリシーを作成でき、ユーザーがmTLS証明書など事前に定められたセキュリティ要件に適合するデバイスを使っている場合に限って、アプリケーションへのアクセスを認めることもできます。

主な特徴

- 複数のIDプロバイダーや同一プロバイダーの複数インスタンスを統合します。
- アプリケーションごとのルール（例：MFAはハードキーが必要）に基づいてユーザーIDを検証します。
- アプリケーションごとのルール（例：SWGポリシー適用、EPPインストール済み、mTLS証明書取得済み、ディスク暗号化有効化済み）とロケーションに基づいてデバイスポスチャーを検証します。
- Cloudflareのアプリケーションランチャーポータルを使えば、ユーザーはすべての承認済みSaaSアプリを見て、アクセスすることができます。



すべてのSaaSアプリケーションにテナントとデータの保護制御を適用

アプリケーションの社外インスタンスへのアクセスを制限

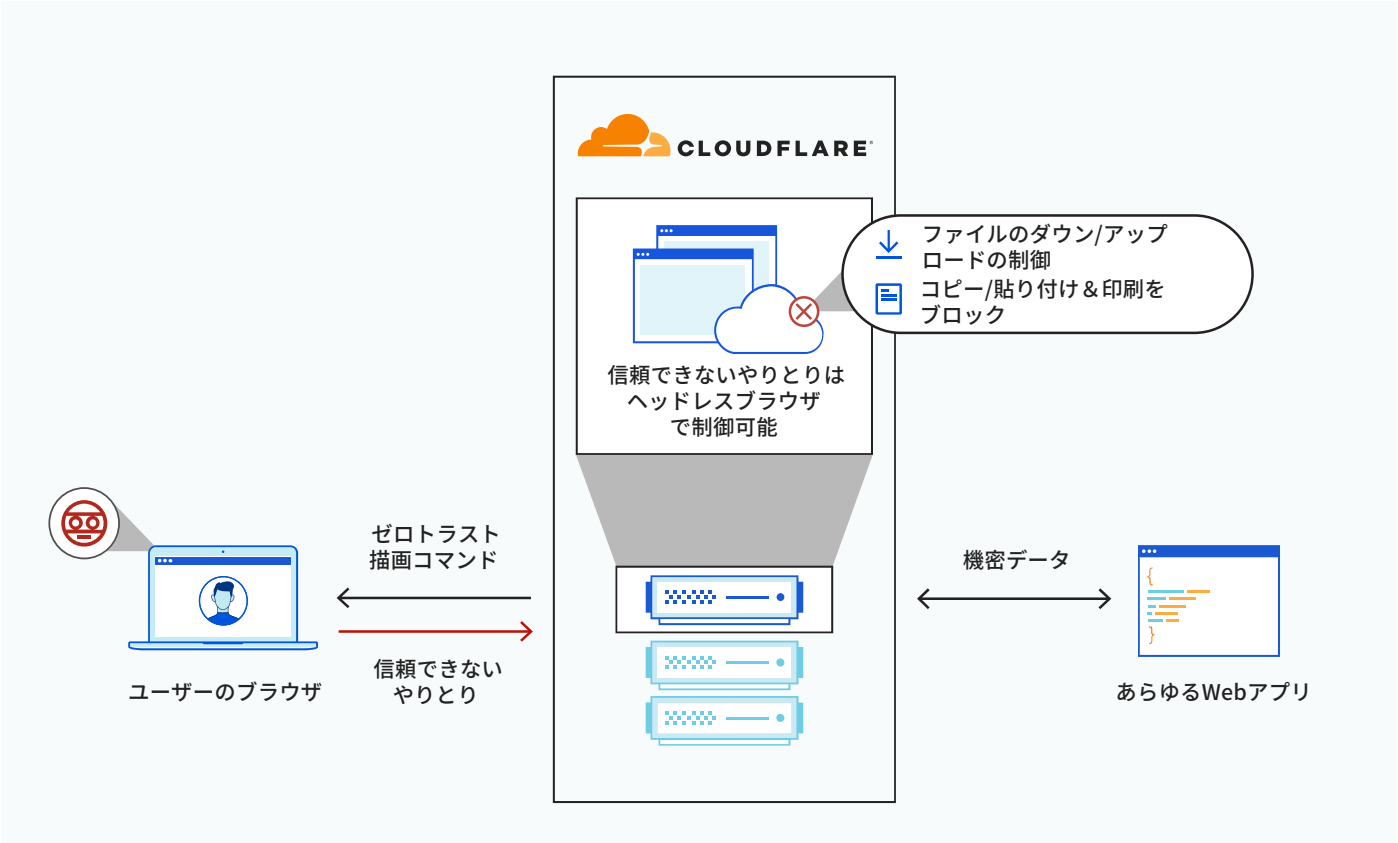
Cloudflareは、HTTPゲートウェイポリシーによってテナント制御を可能にします。このポリシーはアプリケーションのコンシューマーバージョンにユーザーがアクセスしないように設定することができます。企業VPN経由でオンプレミスのプロキシサーバーを使ってポリシーを適用する代わりに、Cloudflareは大規模なグローバルデータセンターネットワークを使ってすべてのトラフィックとリクエストをフィルタリングおよび検査します。そのため、ユーザーがさらなる遅延やパフォーマンスの低下を経験することはありません。

企業データのテナント経由の漏えいを阻止

Cloudflareは、Zero Trustのブラウジングポリシーの作成とデプロイを容易にし、お客様のWebベースアプリケーション内のデータ制御と保護を実現します。アプリケーションコードはすべて、エンドポイントデバイスではなく、当社の大規模グローバルネットワーク上でリモート稼働するセキュアなヘッドレスブラウザで実行されます。そのため、安全性が損なわれたデバイスや信用できないデバイスから機密データを守り、ゼロデー脅威から保護することができるのです。ユーザーがデータにどのようにアクセスし、それらをどう共有するかについては管理者が制御権限を保持しているため、偶発的なデータロスや重大なデータ漏えいのリスクを最小限に抑えられます。

主な特徴

- アプリケーション、アプリケーションタイプ、ホスト名、ユーザーID、セキュリティリスクなど複数の基準に基づいてブラウザの挙動を許可または阻止します。
- ブラウザ上でのユーザーの行動（ダウンロード、アップロード、コピーと貼り付け、キーボード入力、印刷などの機能を利用）を制御します。



Cloudflareの違い

プラットフォームの幅広さ

Cloudflareは、Zero Trustアクセス（ZTNA）、ゲートウェイ（SWG）、ブラウザ（RBI）の制御をお客様のSaaSアプリケーションの前面に配置しますので、お客様のITチームが専用のCASB製品を構成・運用する必要はありません。

ゼロから構築

CloudflareのCASBが提供する機能はすべてゼロから構築されているため、当社のZTNAサービス、SWGサービス、RBIサービスとシームレスに連携します。アプリケーションやチームを保護するために複数のポイント製品を操作する必要はなくなります。

単一画面で一括制御

Cloudflareを使えば、単一のダッシュボードで、組織でポリシーを設定し、アプリケーションへのアクセスや利用を管理することができ、すべてのリクエストや許可を一目で監視することができます。

Cloudflareは、ネイティブに統合したZero Trustセキュリティ機能スイートを提供し、チームでのSaaSアプリの監視、保護、制御に役立ちます。

詳細情報はこちら