Cloudflareの Unified Risk Posture

拡大する攻撃対象領域のより広い範囲にリスクポスチャーを動的に自動適用

課題：広すぎる攻撃対象領域

さらに複雑化するリスク管理

拡大する攻撃対象領域全体について多様化するリスクを常に把握し軽減する業務は、ますます複雑化し、企業の効率も低下しています。セキュリティチームは次のような課題の解決に苦慮しています。

- **サイロ化されたツールが多すぎる：**リスクを総合的に評価するための可視性と相互運用性が制限されている
- **リスクのシグナルが多すぎる：**情報過多となり、リスクの優先順位付けが難しい
- **手作業のリスク分析が多すぎる：**時間、リソース、専門知識が必要

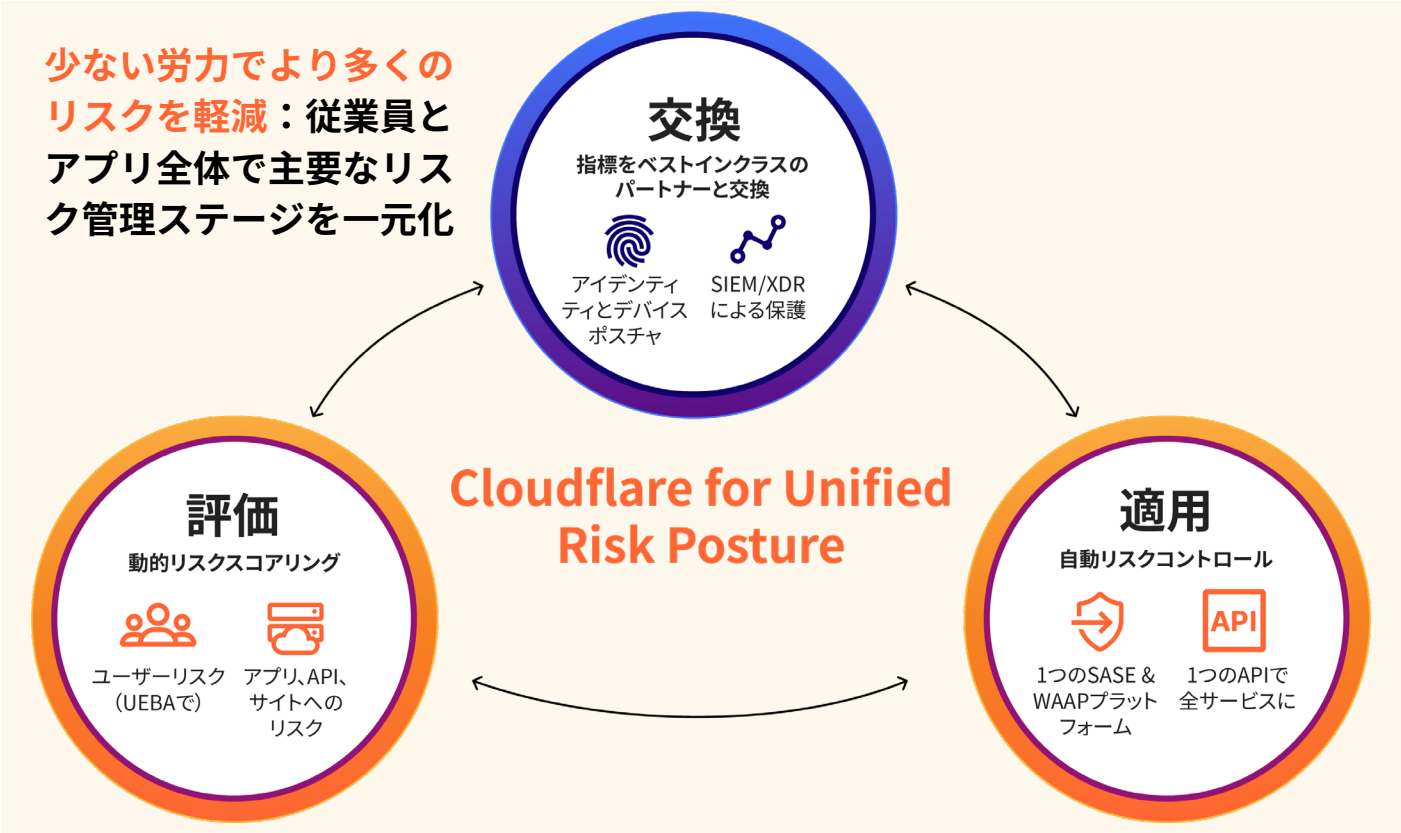
解決策：リスクポスチャーコントロールの統一

高度化するリスクに1つのプラットフォームで対応

SASEとWAAPのセキュリティ機能をCloudflareのグローバルネットワークに統合し、従業員とアプリ全体のリスクを管理します。3つの重要な作業を1つのプラットフォームで実現し、リスク管理をシンプルにします。

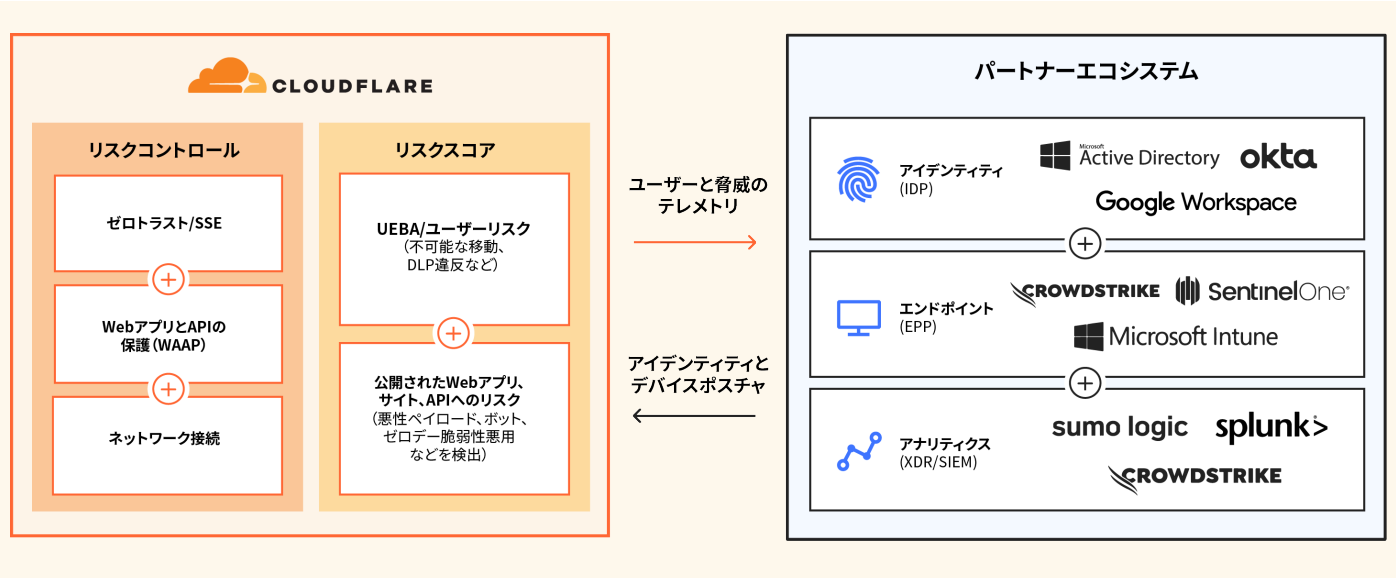
- **従業員とアプリ全体でリスク評価：**動的なファーストパーティリスクスコアリングモデル
- **クラス最高水準のツールで指標を交換：**EPP（エンドポイント保護プラットフォーム）、IDP（IDプロバイダ）、XDR（拡張検出・応答）、SIEM（セキュリティ情報およびイベント管理）の全プラットフォームに対応
- **リスクコントロールを自動かつ大規模に適用：**あらゆるロケーション、IT環境

少ない労力でより多くのリスクを軽減：従業員とアプリ全体で主要なリスク管理ステージを一元化



リスクを評価し、パートナーとデータを交換

Cloudflareは、動的なファーストパーティリスクスコアリングモデルを活用し、クラス最高水準のテクノロジーパートナーとリスク指標を交換して、企業のリスクを評価します。



動的なファーストパーティリスクスコアリング

AIと機械学習に基づいたモデルで、従業員とアプリ全体でリスクを評価します。

ユーザーリスクスコアリング（UEBA）

ユーザーの行動に基づいてリスクを検出：UEBA（ユーザーおよびエンティティの行動分析）と呼ばれるアプローチです。あり得ない移動やDLPポリシー違反などの疑わしい行動や異常な行動が観察されると、Cloudflareはユーザーに高リスク/中リスク/低リスクのスコアをつけます。

アプリのリスク

アプリ、API、サイトを保護するポリシーを構築：悪意のあるペイロード、悪意のあるブラウザスクリプト、ボット、ゼロデー脅威を識別するモデルに基づいてポリシーを構築します。

これらのリスクモデルは、Cloudflareによって保護されたあらゆる外部/内部インフラに適用されます。つまり、セルフホスティングのJiraやConfluenceサーバーのような内部アプリの手前で、アプリの脆弱性の悪用、DDoS攻撃、ボットに対する保護を適用することができます。

パートナーとのデータの交換

CloudflareのAPIを使用した統合により、既存のツールでより多くのことができるようになります。統合は一度で済みます。

リスク指標の取り込み

Cloudflareはエンドポイント保護プラットフォーム（EPP）やIDプロバイダ（IDP）などのパートナーからリスクスコアを取り込みます。これらの統合により、ゼロトラストのベストプラクティスに沿って、あらゆる送信先へのあらゆるアクセスリクエストに対してIDおよびデバイスポスチャーのチェックを実施できます。複数プロバイダを一度にオンボードして、さまざまなコンテキストで異なるポリシーを適用可能です。

テレメトリーの共有

Cloudflareのログを拡張検出・応答（XDR）およびセキュリティ情報・イベント管理（SIEM）プラットフォームに送信して、ステップを追加してさらなる分析とリスク軽減を行います。

自動リスクコントロールを大規模に実施

インテリジェントでプログラマブルなグローバルクラウドネットワークにより、ファーストパーティとサードパーティのリスクスコアに基づいて単一のプラットフォームで保護を適用します。

シンプルなリスク管理
ベンダーを統合し、複雑さと企業リスクを軽減します。

可視性を高めて保護を強化
Cloudflareの巨大なグローバルネットワークから、リスクと脅威に関する自動かつ動的なインテリジェンスを入手します。

あらゆるロケーションでスケーリング可能
世界中のあらゆる場所で、復元力の高い一貫した保護を実現します。

サンプルユースケース

ユースケース：機密データの保護

課題：ユーザーが誤って規制対象データ（PII、健康、金融など）や専有情報（開発者コードなど）を操作する

解決策：データ損失防止（DLP）制御でデータ漏えいを防ぐ。高リスクのフラグをDLP違反が多いユーザーに立て、アクティビティを調査します。ゼロトラストネットワークアクセス（ZTNA）またはブラウザ分離ポリシーにより、該当ユーザーによる他の環境へのアクセスを制限・分離します。

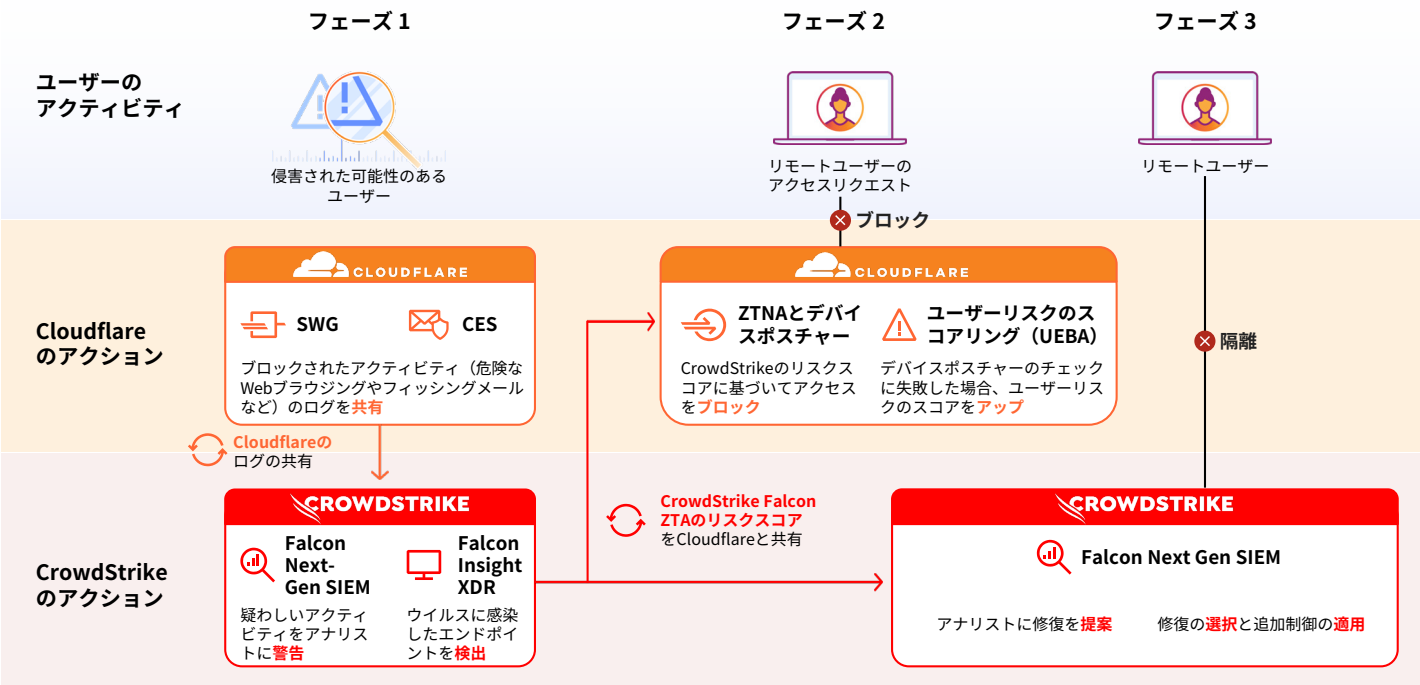
ユースケース：アプリ、API、Webサイトの保護

課題：攻撃者やボットが、公開アプリ、API、サイトを標的にしている

解決策：WAF Attack Scoreやポッドスコアのような機械学習ベースのリスクモデルを使用して、悪意のあるペイロード、ボット、ゼロデー脅威を検出し、軽減します。潜在的な設定ミスやデータ漏えいのリスク、インフラに影響を与える脆弱性をチェックします。

ユースケース：CloudflareとCrowdStrikeによるゼロトラストの適用

以下は、CloudflareとCrowdStrikeが連携してゼロトラストポリシーを適用し、新たなリスクを軽減するワークフロー例です。CloudflareとCrowdStrikeはアクティビティとリスクのデータを交換し、リスクベースのポリシーと修復ステップを適用することで相互に補完しています。



フェーズ1：自動化された調査

CloudflareとCrowdStrikeは、ユーザーが侵害されていることを組織が検知できるよう支援します。

この例では、Cloudflareが最近、防衛の最前線として危険なWebサイトのブラウジングやフィッシングメールをブロックしました。それらのログがCrowdStrike Falcon次世代SIEMに送信され、この組織のアナリストに疑わしい活動について警告します。

同時に、CrowdStrike Falcon Insight XDRがそのユーザーのデバイスを自動的にスキャンし、感染を検出します。その結果、デバイスの健全性を反映するFalcon ZTAスコアが低下します。

フェーズ2：Zero Trustの適用

この組織ではCloudflareのゼロトラストネットワークアクセス（ZTNA）を介してデバイスポスチャーチェックを設定し、Falcon ZTAのリスクスコアが定義した特定のしきい値を超えた場合のみ、アクセスを許可しました。

ここでは、Falcon ZTAスコアが閾値を下回っているため、CloudflareのZTNAはこのユーザーの次のアプリケーションアクセスリクエストを拒否します。

デバイスポスチャーチェックで不合格となったため、Cloudflareはこのユーザーのリスクスコアを上げ、制限の厳しい制御の対象グループに入れます。

フェーズ3：改善

同時に、CrowdStrikeの次世代SIEMは、組織の環境全体におけるこのユーザーのアクティビティとより広範なリスクを分析し続けます。CrowdStrikeが機械学習モデルを使用して主要なリスクを表面化し、各リスクに対応するソリューションをアナリストに提案します。

続いて、アナリストが修復方法（ユーザーのデバイスを隔離するなど）を検討して選択し、組織全体のリスクをさらに軽減することができます。

組織にとってのインパクト

メリット	サンプルメトリックス
SecOpsの業務負担を軽減 手作業のポリシー作成が減り、より俊敏なインシデント対応が可能になります	• 自動ワークフローの増加 • ポリシー作成のクリック数減少 • 平均検出時間（MTTD）の短縮 • 平均応答時間（MTTR）の短縮
サイバーリスクを低減 攻撃対象領域全体に、リスクポスチャを動的に自動適用します	• 重大インシデントの減少 • 脅威の自動ブロック件数増加

お客様の声

「Cloudflareのおかげで少ない手間でリスクを効果的に低減でき、組織全体に渡るゼロトラスト導入が簡単になりました。」

Anthony Moisant氏
SVP、最高情報責任者
兼最高セキュリティ責任者、Indeed

世界No.1の求人サイト
ユニーク訪問者数は月間350M以上

「Cloudflareのソリューションを1つ導入しただけで、複雑なグローバルオペレーションを管理しやすくなり、業務が楽になりました」

Wilson Tang氏
エンジニアリングおよびプラットフォームコアサービスディレクター、Delivery Hero

70か国以上で事業を展開するドイツのオンライン食品注文＆配送企業

導入事例を読む

競合他社との比較

2024年5月7日時点

	Cloudflare	Zscaler	Netskope	Palo Alto Networks（Prisma Access）
ファーストパーティリスクスコアリングモデルでリスクを評価				
リアルタイムのユーザーとエンティティの行動分析（UEBA）モデル/ユーザーリスクスコアリング	✅	✅	✅	✅
ファーストパーティのメール/フィッシングリスクデータへのアクセス	✅	❌	❌	❌
WAFでの悪意のあるペイロードとゼロデー脅威検出	✅	❌	❌	❌
ユーザーとアプリによるすべてのリスクを1つのダッシュボードで表示	Cloudflare Security Center内で進行中の業務	✅	Netskope Cloud Exchangeでのポスチャーの高度な可視化は、顧客のインフラ上で管理する必要がある	アプリとその使用リスクにのみ対応
サードパーティツールとリスクシグナルを交換				
主要なエンドポイント保護プラットフォーム（EPP）および拡張検知・応答（XDR）プロバイダとの統合（例：CrowdStrike、SentinelOne、Microsoft）	✅	✅	✅	✅
主要なIDプロバイダ（IDP）およびシングルサインオン（SSO）との連携（例：Okta、Ping Identity、Microsoft）	✅	✅	✅	✅
1つのAPIで全サービス	✅	❌	Netskope APIの全機能を利用するには、カスタマーサポートの介入が必要	❌
すべてのサービスで、一度でサードパーティとの統合を設定可能	✅	❌	❌	❌
リスク制御の適用				
ユーザーリスクに基づくポリシーの構築	✅	✅	✅	✅
1つの管理インターフェースですべてのセキュリティサービスエッジ（SSE）ポリシーを構築	✅	❌	✅	✅
それぞれのサービスをすべてのデータセンターで実行	✅	❌	✅	✅
ネットワークのスケール	320以上のロケーション 13,000以上のピアリングポイント	70のロケーション 116のピアリングポイント	70以上の地域 183のピアリングポイント	119のオンランプ 47のコンピュートセンター
Terraformによる自動化	Cloudflareプラットフォーム全体の単一リポジトリ	19のリポジトリ	Terraform経由でのポリシー構築は不可	複数のTerraformプロバイダとモジュールが必要

Cloudflareと他社の違い

シンプルなCloudflareの統合プラットフォーム

セキュアアクセスサービスエッジ（SASE）とWebアプリ＆API保護（WAAP）の制御を統合した1つのプラットフォームでリスクポスチャーを一元化します。

サービス間の無制限の相互運用性により、迅速な運用開始と継続的でシンプルなリスク管理を実現します。

Infrastructure-as-Codeツール（Terraformなど）によるカスタマイズや自動化のために、Cloudflareの単一APIで、すべてのCloudflareサービスをオーケストレーションできます。

統合の柔軟性

使用しているEPP（エンドポイント保護プラットフォーム）、IDP（IDプロバイダ）、XDR（拡張検出・応答）、SIEM（セキュリティ情報およびイベント管理）ツールとリスクデータを交換し、組織全体のリスクの変化に対応します。

他のベンダーのソリューションとは異なり、一度統合をセットアップするだけで、Cloudflareのプラットフォーム全体でその機能を活用できます。そのため、IT環境全体にすばやく制御を拡張することができます。

比類ないのスケールを誇るCloudflareのグローバルクラウドネットワーク

Cloudflareの320以上のネットワーク拠点で、すべてのセキュリティサービスを利用できます。

シングルパス検査とポリシー適用は迅速で、一貫性と復元力があります。

さらに、Cloudflareのネットワーク（全世界のWebの20%をプロキシし、1日あたり3兆件のDNSクエリを受信）から得られる独自の可視性によって、AI・機械学習活用モデルが強化され、新たなリスクから防御します。

リスク管理の方法についてのご相談：
ご相談のお申し込みはこちら

詳細を学ぶ：
Cloudflareの発表に関するブログやCloudflareのWebサイトをご確認ください