CLOUDFLARE

SOLUTION BRIEF

Cloudflare for Unified Risk Posture

Automated and dynamic risk posture enforcement across more of your expanding attack surface.

Problem: Too much attack surface

Rising complexity to manage risks

It is becoming increasingly complex and inefficient for enterprises to keep track of and mitigate increasingly diverse risks across their expanding attack surface. Security teams today struggle with:

- **Too many siloed tools** with limited visibility and interoperability to assess risk holistically
- **Too many risk signals** leading to information overload, making it hard to prioritize risks
- **Too much manual effort** for risk analysis, demanding time, resources, and expertise

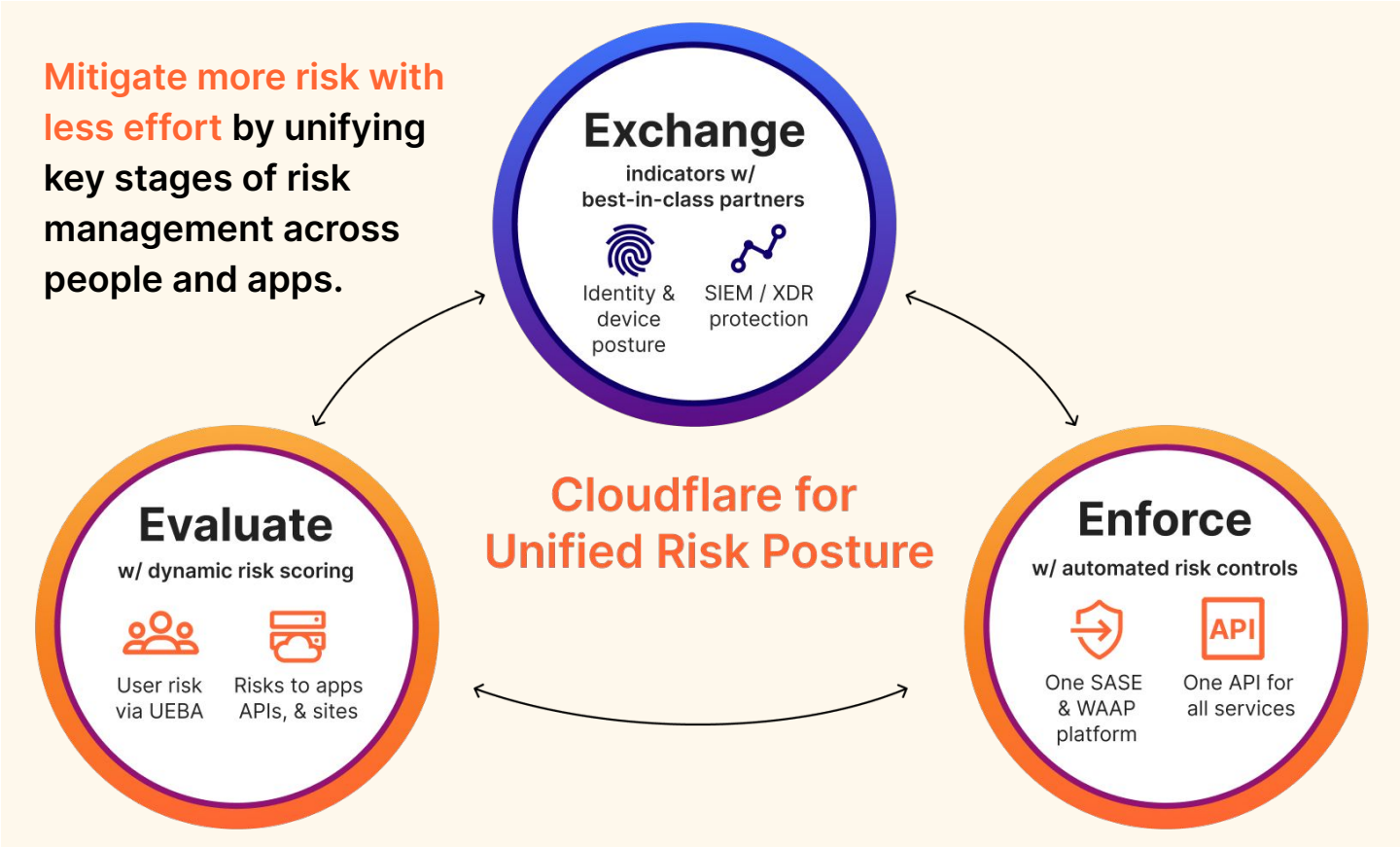
Solution: Unify risk posture controls

One platform to adapt to evolving risks

Converge SASE and WAAP security functionality onto Cloudflare's global network to manage risk across your people and apps. Simplify risk management by accomplishing three key jobs on one platform:

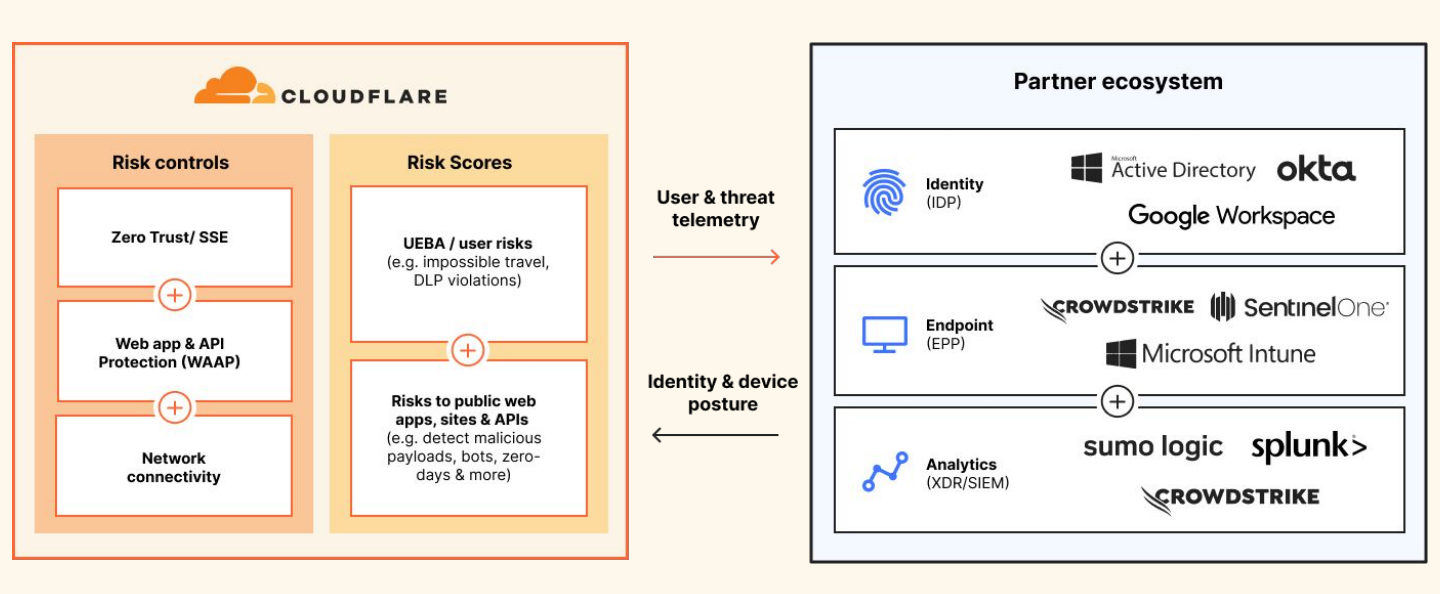
- **Evaluate risk across people and applications** with dynamic first-party risk scoring models
- **Exchange indicators with best-in-class tools** across EPP, IDP, XDR, and SIEM platforms
- **Enforce automated risk controls at scale** across any location and IT environment

Mitigate more risk with less effort by unifying key stages of risk management across people and apps.



Evaluate risk and exchange data with partners

Cloudflare assesses enterprise risk by leveraging dynamic first-party risk scoring models and by exchanging risk indicators with best-in-class technology partners.



Dynamic first-party risk scoring

Evaluate risk across people and apps with models backed by AI and machine learning.

User risk scoring (or UEBA)

Detect risk based on user behavior — an approach known as user entity and behavior analytics (UEBA). Cloudflare scores users as high / medium / low risk after observing suspicious or anomalous activity, such as impossible travel or DLP policy violations.

App risks

Build policies to protect apps, APIs, and sites based on models that identify malicious payloads, malicious browser scripts, bots, and zero-day threats.

These risk models apply to any public-facing or internal infrastructure protected by Cloudflare. This means that you can apply protections against app vulnerability exploits, DDoS, and bots in front of internal apps like self-hosted Jira and Confluence servers.

Exchange with partners

One-time integrations with Cloudflare's unified API help you to do more with your existing tools.

Ingest risk indicators

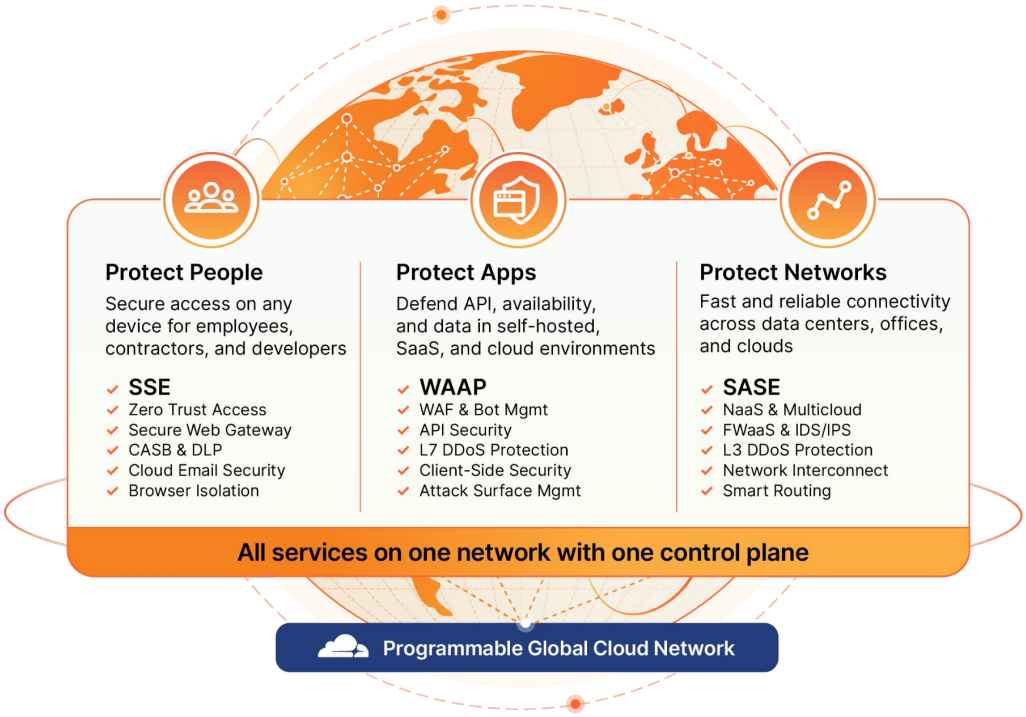
Cloudflare ingests risk scores from endpoint protection (EPP) and identity provider (IDP) partners. With these integrations, you can enforce identity and device posture checks for any access request to any destination in line with Zero Trust best practices. Onboard multiple providers at once to enforce different policies in different contexts.

Share telemetry

Send Cloudflare logs to extended detection and response (XDR) and security information and event management (SIEM) platforms for further analysis and additional risk mitigation steps.

Enforce automated risk controls at scale

One platform to apply protections based on first- and third-party risk scores, uniquely powered by an intelligent, programmable global cloud network.



Simplify risk management
Consolidate vendors to reduce complexity and enterprise risk.

See more, protect more
Get automated, dynamic risk & threat intelligence from our massive global network.

Scale everywhere
Resilient and consistent protections across any location around the world.

Sample use cases

Use case: Protect sensitive data

Problem: User mishandles regulated data (e.g. PII, health, financial) or proprietary information (e.g. developer code).

Solution: Prevent data leaks with data loss prevention (DLP) controls. Flag user as risky based on high number of DLP violations and investigate activity. Restrict or isolate that user's access to other environments with Zero Trust Network Access (ZTNA) or browser isolation policies.

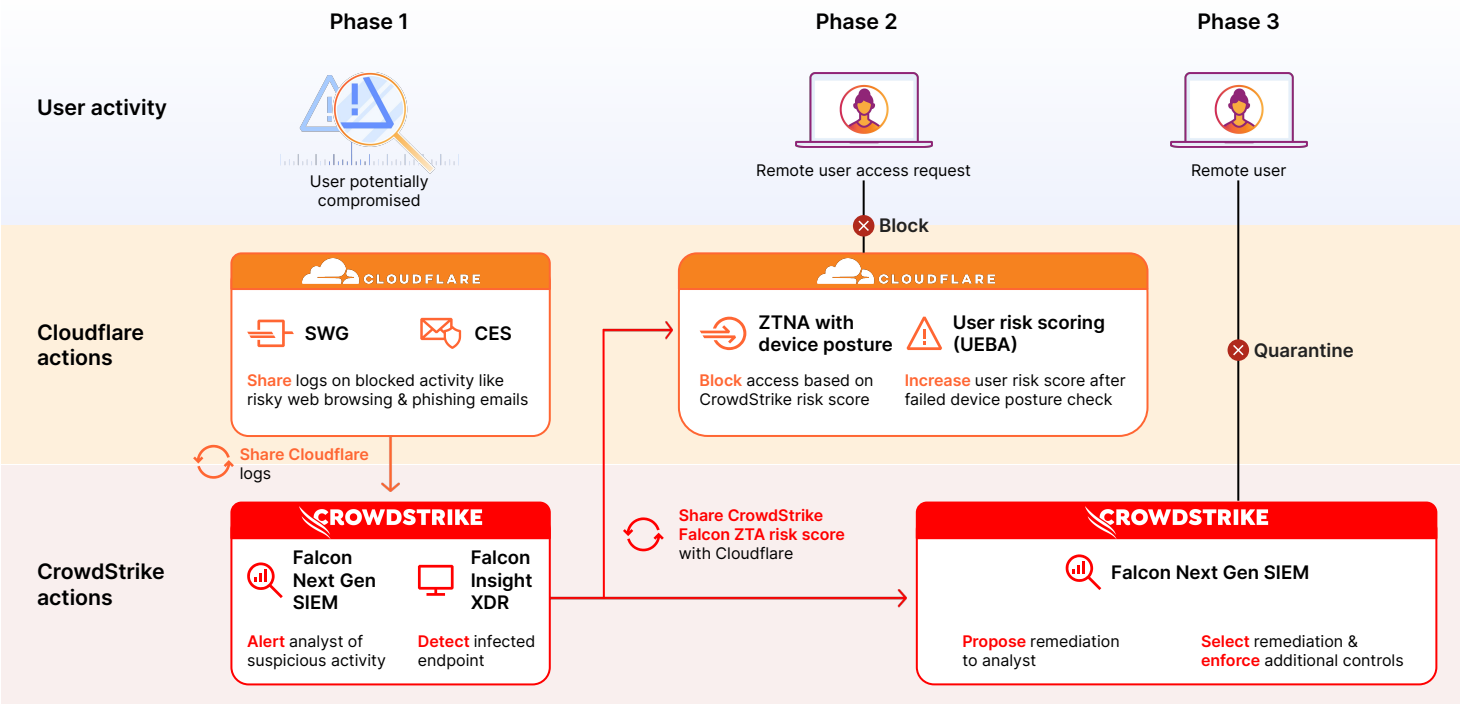
Use case: Protect applications, APIs, and websites

Problem: Threat actors and bots target public-facing apps, APIs, and sites.

Solution: Detect and mitigate malicious payloads, bots, and zero-days using ML-backed risk models like our WAF attack score or bot score. Review potential misconfigurations, data leakage risks, and vulnerabilities that impact your infrastructure.

Use case: Enforce Zero Trust with Cloudflare & CrowdStrike

Below is a sample workflow of how Cloudflare and CrowdStrike work together to enforce Zero Trust policies and mitigate emerging risks. Together, Cloudflare and CrowdStrike complement each other by exchanging activity and risk data and enforcing risk-based policies and remediation steps.



Phase 1: Automated investigation

Cloudflare and CrowdStrike help an organization detect that a user is compromised.

In this example, Cloudflare has recently blocked web browsing to risky websites and phishing emails, serving as the first line of defense. Those logs are then sent to CrowdStrike Falcon Next-Gen SIEM, which alerts your organization's analyst about suspicious activity.

At the same time, CrowdStrike Falcon Insight XDR automatically scans that user's device and detects that it is infected. As a result, the Falcon ZTA score reflecting the device's health is lowered.

Phase 2: Zero Trust enforcement

This org has set up device posture checks via Cloudflare's Zero Trust Network Access (ZTNA), only allowing access when the Falcon ZTA risk score is above a specific threshold they have defined.

Our ZTNA denies the user's next request to access an application because the Falcon ZTA score falls below that threshold.

Because of this failed device posture check, Cloudflare increases the risk score for that user, which places them in a group with more restrictive controls.

Phase 3: Remediation

In parallel, CrowdStrike's Next-Gen SIEM has continued to analyze the specific user's activity and broader risks throughout the organization's environment. Using machine learning models, CrowdStrike surfaces top risks and proposes solutions for each risk to your analyst.

The analyst can then review and select remediation tactics — for example, quarantining the user's device — to further reduce risk throughout the organization.

Customer impacts

Benefits	Sample metrics
Reduce effort in SecOps with less manual policy building & greater agility in responding to incidents	• Increase # of automated workflows • Reduce # of clicks to build policies • Reduce mean time to detect (MTTD) • Reduce mean time to respond (MTTR)
Reduce cyber risk with automated and dynamic risk posture enforcement across your attack surface	• Reduce # of critical incidents • Increase # of threats blocked automatically

What they are saying

"Cloudflare is helping us mitigate risk more effectively with less effort and simplifies how we deliver Zero Trust across my organization."

Anthony Moisant
SVP, Chief Information Officer
and Chief Security Officer, Indeed

#1 job site in the world
with over 350M unique visitors per month

"Having a single Cloudflare solution in place to help us manage complexity across our global operations has made our lives so much easier."

Wilson Tang
Director of Engineering, Platform Core Services, Delivery Hero

German online food ordering and delivery company operating in over 70 countries

Read the case study

Competitive comparison

Based on data as of 2024 May 07

	Cloudflare	Zscaler	Netskope	Palo Alto Networks (Prisma Access)
Evaluate risk with first-party risk scoring models				
Real-time User and Entity Behavior Analytics (UEBA) models / user risk scoring	✅	✅	✅	✅
Access to 1st party email / phishing risk data	✅	❌	❌	❌
Malicious payload and zero-day detection via WAF	✅	❌	❌	❌
Single dashboard view for all risks posed by users and apps	Work in progress within Cloudflare Security Center	✅	Advanced posture visibility via Netskope Cloud Exchange must be managed on customer infrastructure	Available only for app and app usage risks
Exchange risk signals with third-party tools				
Integrations with leading Endpoint Protection Platform (EPP) & Extended Detection & Response (XDR) providers (e.g. CrowdStrike, SentinelOne, Microsoft)	✅	✅	✅	✅
Partnerships with leading Identity Providers (IDPs) & Single SIgn Ons (SSOs) (e.g. Okta, Ping Identity, Microsoft)	✅	✅	✅	✅
One API for all services	✅	❌	Full Netskope API capabilities only available with customer support intervention	❌
One-time setup for 3rd party integrations across all services	✅	❌	❌	❌
Enforce risk controls				
Build policies based on user risk	✅	✅	✅	✅
One management interface to build all Security Service Edge (SSE) policies	✅	❌	✅	✅
Every service runs in every data center	✅	❌	✅	✅
Network scale	>320 locations >13,000 peering points	70 locations 116 peering points	>70 regions 183 peering points	119 on-ramps 47 compute centers
Terraform automation	Single repository for entire Cloudflare platform	19 repositories	No policy creation via Terraform	Requires multiple Terraform providers and modules

The Cloudflare difference

Simplicity of our unified platform

Unify risk posture management on one platform that converges secure access service edge (SASE) and web app & API protection (WAAP) controls.

Limitless interoperability between services, so you can get started faster and simplify ongoing risk management.

Orchestrate all Cloudflare services with our single API for customization and automation with infrastructure as code tools like Terraform.

Flexibility of our integrations

Exchange risk data with the EPP, IDP, XDR, and SIEM tools you already use to adapt to changes in risk throughout your organization.

Unlike with other vendors, set up integrations only once and leverage those capabilities across Cloudflare's entire platform, so you can extend controls across your IT environments with agility.

Unmatched scale of our global cloud network

Every security service is available for customers to run across each of our 320+ network locations.

Single-pass inspection and policy enforcement are always fast, consistent and resilient.

Plus, unique visibility from our network (which proxies 20% of the web and sees 3T DNS queries per day) powers AI/ML-backed models to defend against emerging risks.

Ready to discuss your risk management approach?
Request a consultation

Want to keep learning more?
Read our announcement blog or visit our website