![CLOUDFLARE logo]

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 and inefficiency

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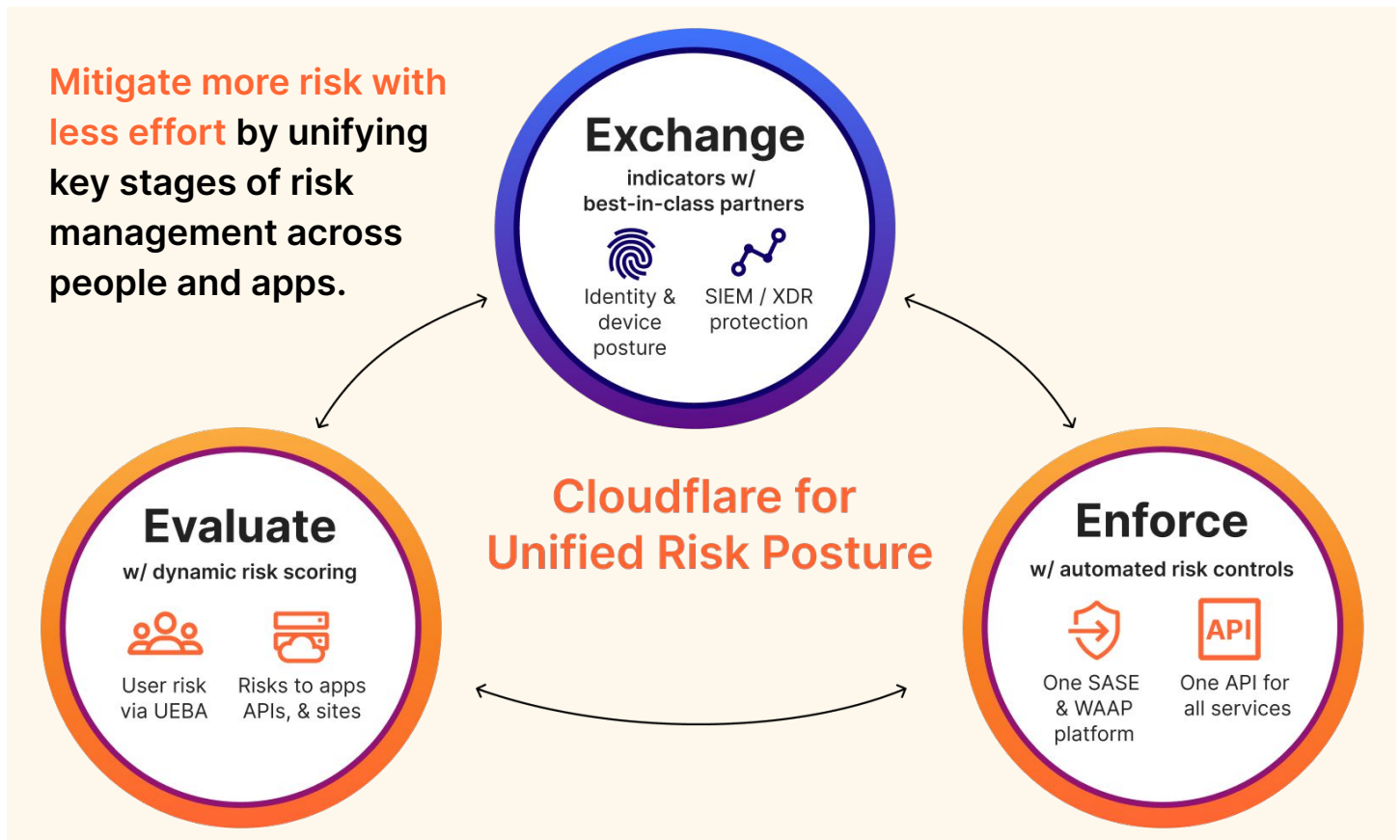
- **Too many siloed tools** with limited visibility and interoperability to assess risk holistically
- **Too many risk signals** leading to information overload, making it hard to prioritize risks
- **Too much manual effort** for risk analysis, demanding time, resources, and expertise

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 models
- **Exchange indicators with best-in-class tools** across EPP, IDP, XDR, and SIEM
- **Enforce automated risk controls at scale** across any location or IT environment

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

Exchange indicators w/ best-in-class partners
- Identity & device posture
- SIEM / XDR protection

Cloudflare for Unified Risk Posture

Evaluate w/ dynamic risk scoring
- User risk via UEBA
- Risks to apps APIs, & sites

Enforce w/ automated risk controls
- One SASE & WAAP platform
- One API for all services

Competitive comparison

Based on data as of 2024 May 07

Ready to discuss your risk management approach?
Request a consultation

	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