CLOUDFLARE

PARTNER BRIEF

Unify risk posture with Cloudflare and partners

Exchange risk indicators and automated risk posture enforcement with one time integrations.

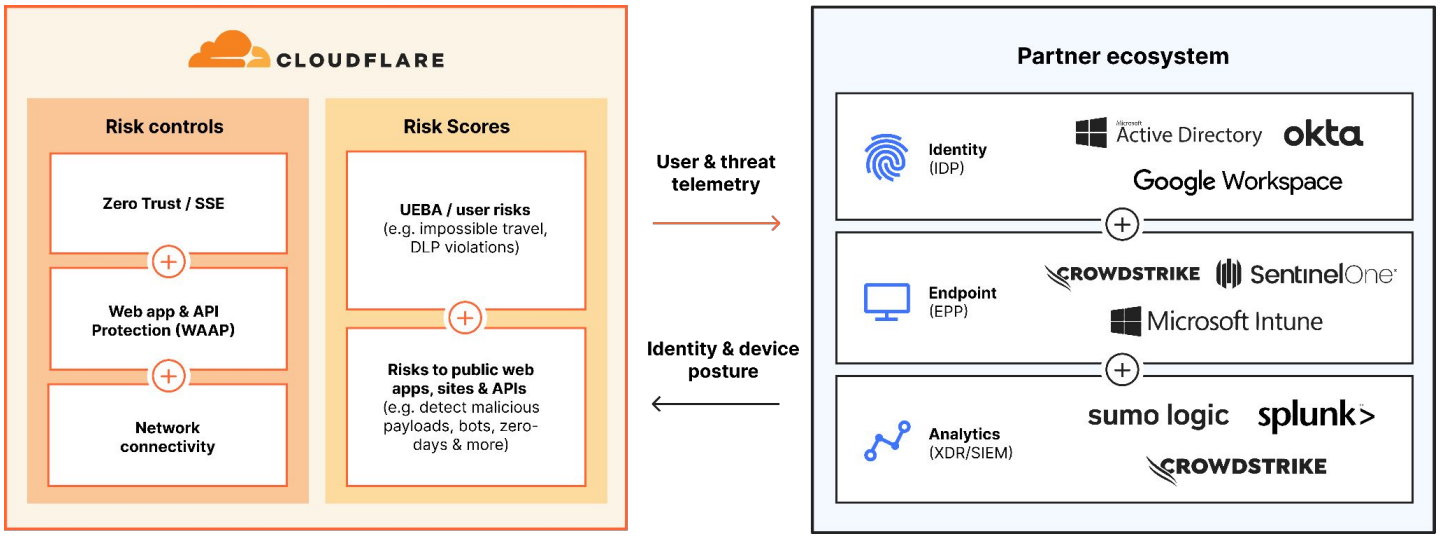
Challenge: Rising complexity to manage risks

Managing risk effectively and efficiently is becoming exceedingly complex as attack surfaces expand. Security teams today struggle with siloed tools with limited interoperability that require too much manual effort and expertise to assess, prioritize, and mitigate evolving risks within a business.

Joint solution with Cloudflare partners

Cloudflare exchanges risk signals with best-in-class technology partners to enforce security controls dynamically. One-time integrations with Cloudflare's unified API help you to do more with your existing tools:

- **Ingest** device posture, identity, and other risk scores from endpoint protection (EPP) and identity provider (IDP) partners to enforce posture checks for all access requests.
- **Share** Cloudflare logs to extended detection and response (XDR) and security information and event management (SIEM) platforms for further analysis and additional risk mitigation steps.



Adopt Zero Trust

Default-deny, least privilege rules based on identity, device posture and dynamic user risk scoring.

Simplify defense in depth

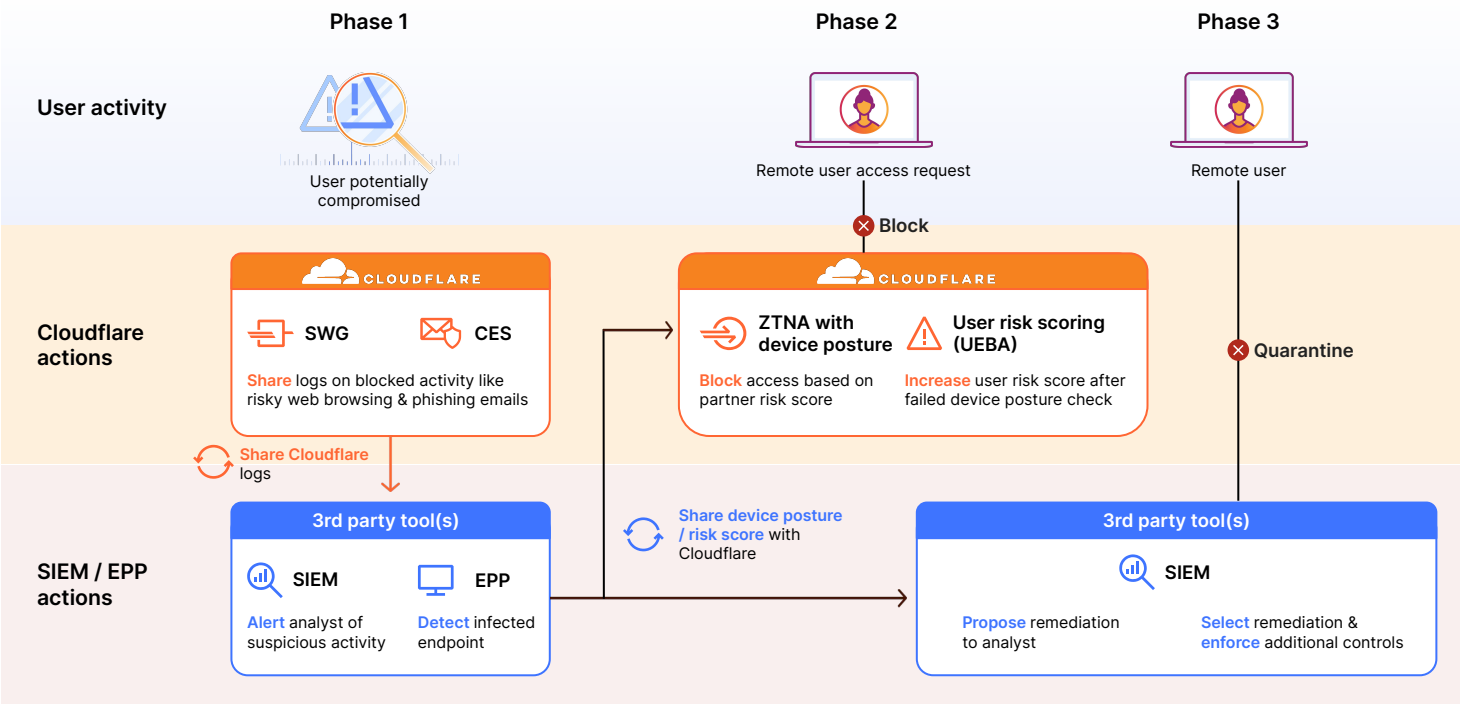
Layer policies to guard users and devices from multi-channel phishing, ransomware, and more.

Automate SOC response

Build mitigation workflows within your SIEM / XDR enriched by Cloudflare telemetry.

Use case: Enforce Zero Trust with Cloudflare and Partners

Below is a sample workflow of how Cloudflare and our technology partners work together to enforce Zero Trust policies and mitigate emerging risks. Here, Cloudflare exchanges activity and risk data with SIEM and EPP platforms to enforcing risk-based policies and take additional remediation steps.



Phase 1: Automated investigation

Cloudflare and EPP & SIEM partners 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 a SIEM partner, which alerts your organization's analyst about suspicious activity.

At the same time, the EPP partner automatically scans that user's device and detects that it is infected. As a result, EPP partner reflects a lower / unhealthier device posture score.

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 EPP partner's device posture score is deemed healthy.

Our ZTNA denies the user's next request to access an application because device posture from the EPP partner is deemed unsafe.

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, the SIEM partner has continued to analyze the specific user's activity and broader risks throughout the organization's environment. Using machine learning models, the SIEM partner 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.

What customers 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

Ready to discuss your risk management approach?
Request a consultation

Want to keep learning more?
Read our announcement blog or visit our tech partner directory