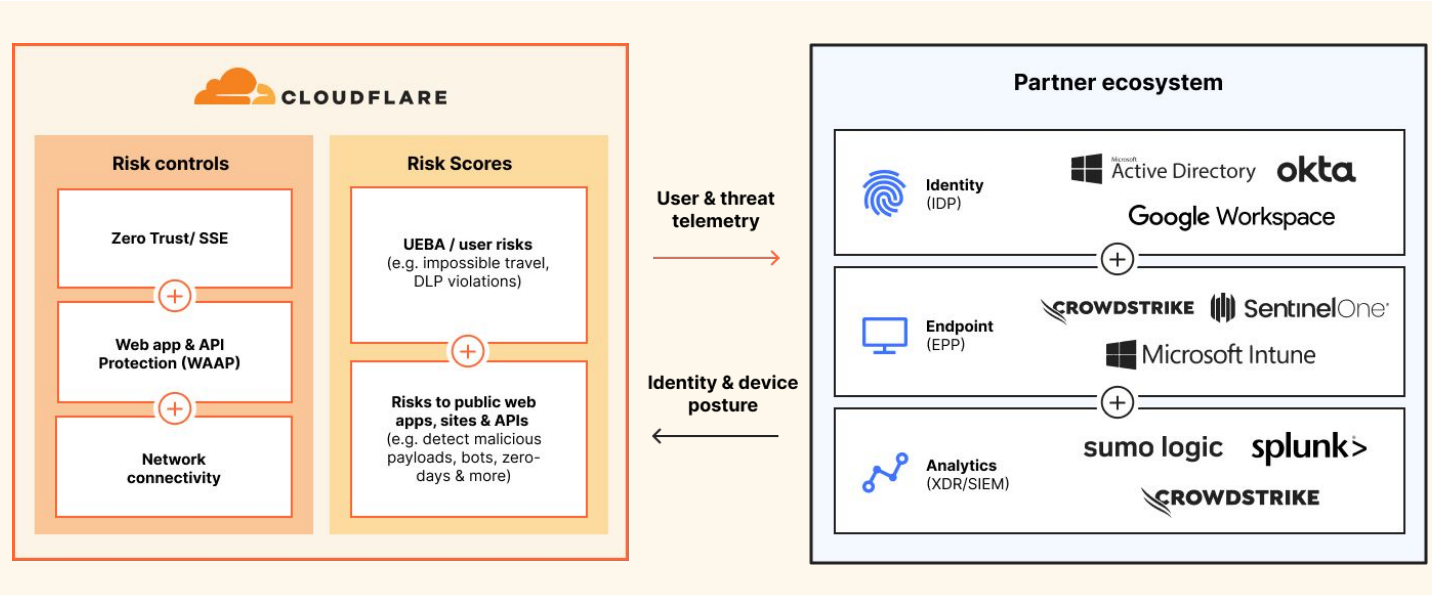
Integrated Cloudflare Zero Trust with Best-In-Class Partners

Achieve a more unified risk posture through one time integrations via a singular API.



Challenge

It's becoming too complex for enterprises to effectively and efficiently manage risk posture across their expanding attack surface. The combination of too many risk signals, too many siloed tools, and too much manual effort have long been a pain point for organizations seeking to control who has access to their internal network and applications.

The Solution

Cloudflare works with numerous partners to exchange information and enforce security controls, through one-time integrations with our SSE and SASE platform, Cloudflare One.

Our Partners

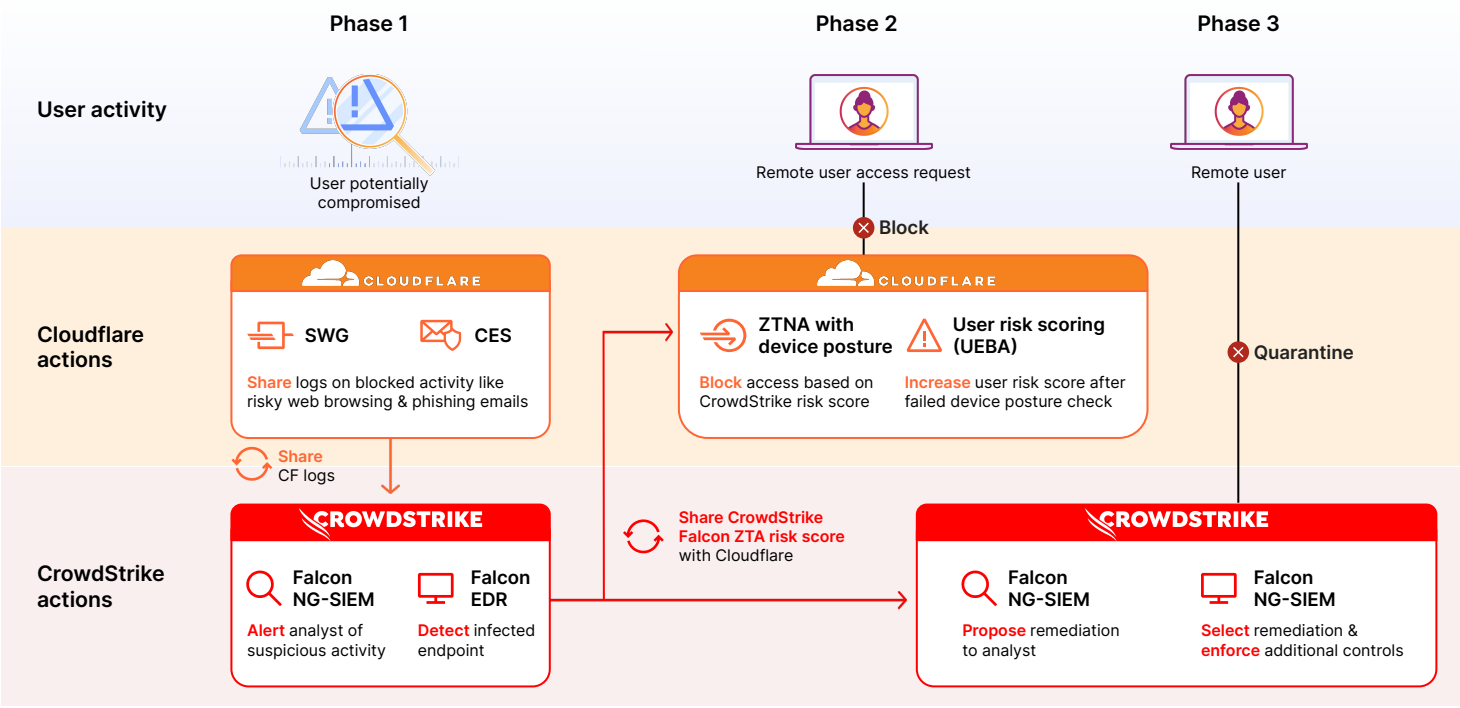
Endpoint Protection Providers (EPPs): When a user logs in to an application protected by Cloudflare, we verify whether the device is protected by an EPP, who can check if the device has been infected with malware or has any other active security threats present. In some cases, Cloudflare ingests risk scores from EPP partners to further verify if a device is deemed too risky to access internal apps or network capabilities. This instantaneous exchange of information shuts down threats automatically.

Identity Providers (IdPs): Meanwhile, identity providers verify that employees accessing the network are who they say they are. Cloudflare works with leading IdPs to thwart fraudulent access attempts, including incidents of impossible travel.

SIEM / XDR Providers: Our collaboration also extends to SIEM and XDR partners, who ingest comprehensive data from Cloudflare into a centralized dashboard. This empowers security analysts to swiftly detect and respond to security threats.

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-GenSIEM 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.

What customers and partners 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

indeed®

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

"By expanding our partnership with Cloudflare, we are making it easier for joint customers to strengthen their Zero Trust security posture across all endpoints and their entire corporate network."

Michael Sentonas
President, CrowdStrike

CROWDSTRIKE

Global cybersecurity leader and Cloudflare technology partner

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