PARTNER BRIEF

Unify risk posture with Cloudflare & CrowdStrike

Integrate to exchange risk indicators and enforce controls based on device posture.

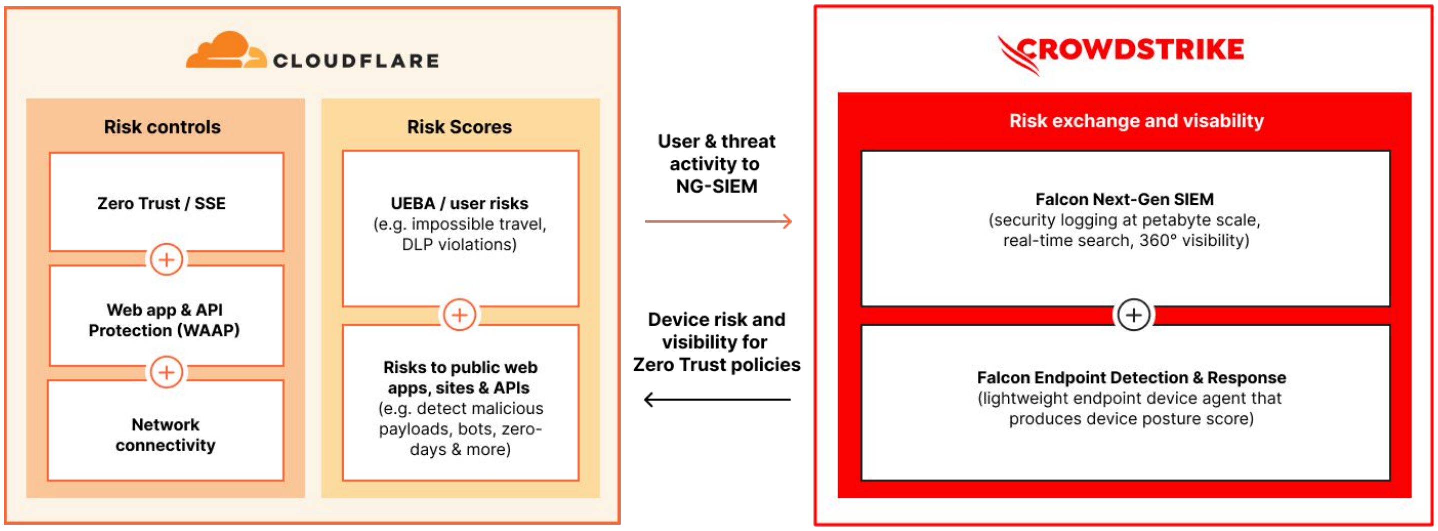
Challenge: Rising complexity to manage risks

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 & CrowdStrike

Cloudflare and CrowdStrike exchange risk signals and enforce security controls dynamically. Set up the integration only once and begin automating how you adapt to risks across users, devices, and applications:

- **Ingest** the CrowdStrike Falcon® Zero Trust Assessment (ZTA) score into Cloudflare to enforce device posture across all access requests
- **Share** Cloudflare logs with the Falcon® Next-Gen SIEM to enrich real-time visibility across Security Service Edge (SSE) and web application and API protection (WAAP) security domains


CLOUDFLARE
Risk controls
Zero Trust / SSE
Web app & API Protection (WAAP)
Network connectivity
Risk Scores
UEBA / user risks (e.g. impossible travel, DLP violations)
Risks to public web apps, sites & APIs (e.g. detect malicious payloads, bots, zero-days & more)
User & threat activity to NG-SIEM
Device risk and visibility for Zero Trust policies
CROWDSTRIKE
Risk exchange and visability
Falcon Next-Gen SIEM (security logging at petabyte scale, real-time search, 360° visibility)
Falcon Endpoint Detection & Response (lightweight endpoint device agent that produces device posture score)

Adopt Zero Trust

Default-deny, least privilege rules based on device posture for web, SaaS, and private app requests.

Simplify threat defense

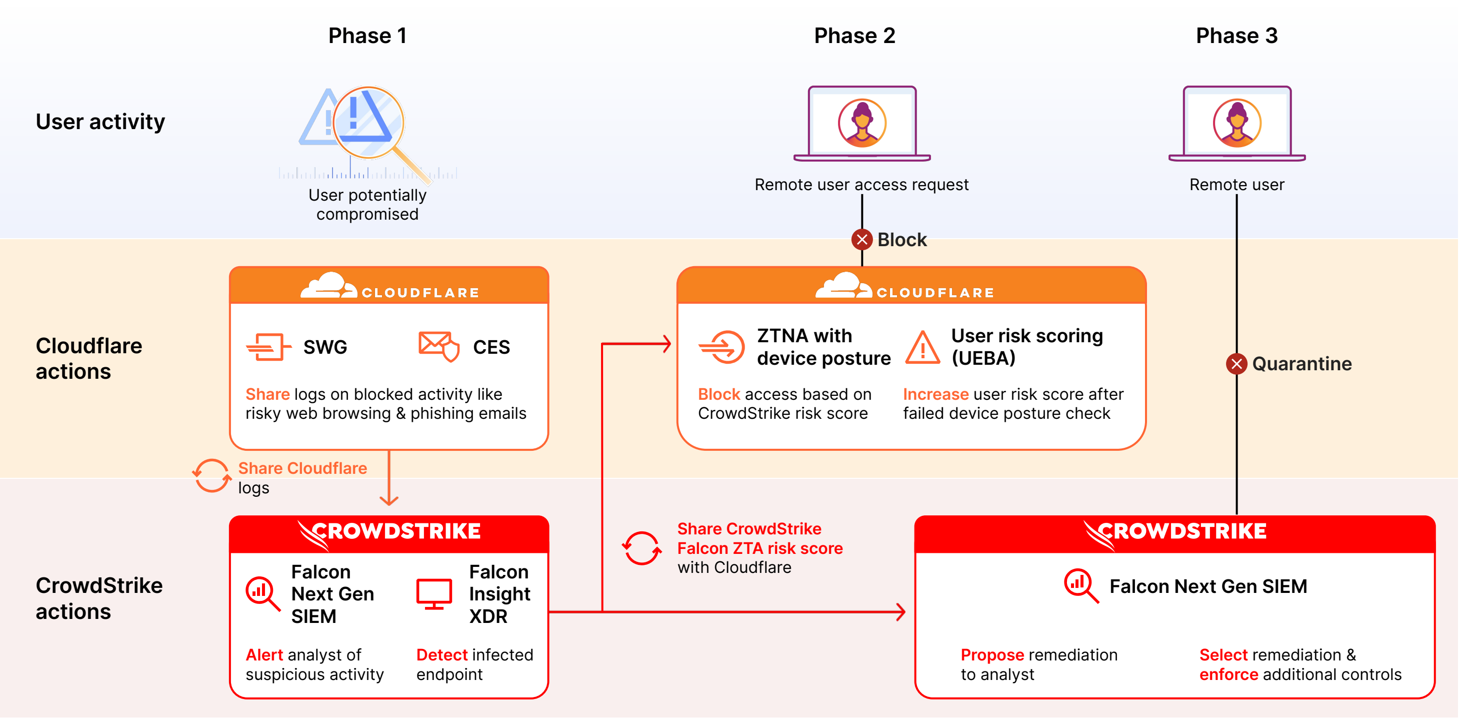
Layer policies to guard users and devices from multi-channel phishing, ransomware, and more.

Automate SOC response

Build mitigation workflows within your CrowdStrike NG-SIEM enriched by Cloudflare telemetry.

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

Phase 2

Phase 3

User activity

User potentially compromised

Remote user access request

Block

Remote user

Cloudflare actions

CLOUDFLARE

SWG

CES

Share logs on blocked activity like risky web browsing & phishing emails

Share Cloudflare logs

CLOUDFLARE

ZTNA with device posture

Block access based on CrowdStrike risk score

User risk scoring (UEBA)

Increase user risk score after failed device posture check

Quarantine

CrowdStrike actions

CROWDSTRIKE

Falcon Next Gen SIEM

Alert analyst of suspicious activity

Falcon Insight XDR

Detect infected endpoint

Share CrowdStrike Falcon ZTA risk score with Cloudflare

CROWDSTRIKE

Falcon Next Gen SIEM

Propose remediation to analyst

Select remediation & enforce additional controls

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.

Impacts

Flo Health uses Cloudflare & CrowdStrike to enforce device posture for all employees access requests to sensitive apps.

Case study on the world's most popular female health app

"The Cloudflare integration with Crowdstrike strengthens our overall security posture."

Troy Ridgewell
Head of Security, Stax
Case study on this AWS management platform

"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

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