

# Cloudflare and CrowdStrike

Easily deploy seamless Zero Trust protection from the network to the device, then stop breaches with an AI-native SOC platform



## Key Highlights

- **Strengthen Zero Trust:** Integrate device posture assessments from Falcon's ZTA with Cloudflare's Secure Access Service Edge (SASE) platform for secure, conditional access across enterprise network applications.
- **Enhance Threat Defense:** Combine Cloudflare policies with CrowdStrike telemetry to defend against phishing, ransomware, and multi-channel attacks.
- **Automate SOC Workflows:** Leverage AI-driven CrowdStrike Falcon Next-Gen SIEM enriched by Cloudflare data to streamline threat detection and speed up remediation.

## The Challenge

Enterprises are struggling to effectively and efficiently keep the expanding attack surface secure. The combination of siloed tools and distributed users means significant manual effort is required to accurately assess who and what can access the enterprise network and applications. Security teams and Zero Trust solutions need a comprehensive view of device and user risk to inform decisions.

## Enhance and Speed Up Remediation Through Collaboration

The integration of Cloudflare and CrowdStrike provides Zero Trust capabilities across devices and the corporate network. CrowdStrike Falcon Zero Trust Assessment (ZTA) performs continuous security and compliance checks on endpoints to generate an assessment score. This score is used by Cloudflare's Zero Trust platform to help determine whether the device is authorized to connect to the enterprise network or applications. Cloudflare can also enforce conditional policies based on the ZTA score to limit access and reduce risk.

Logs from Cloudflare's platform are shared with the AI-driven CrowdStrike Falcon Next-Gen SIEM to drive threat identification and remediation. Shared data improves context while automation reduces time to remediation. Customers benefit from an integrated offering that reduces IT complexity and improves security posture.



### Expand Zero Trust

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



### Simplify threat defense

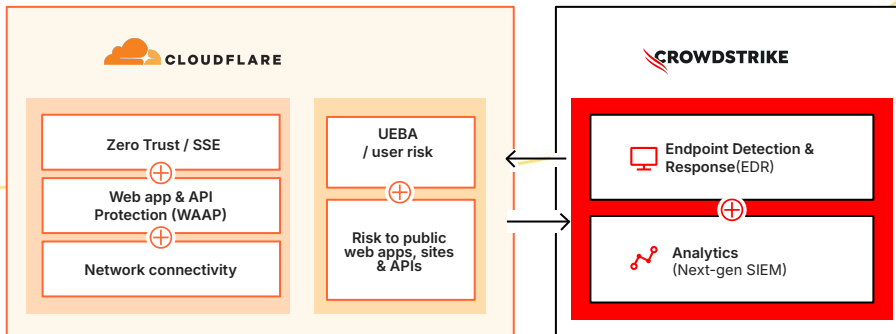
Layer Cloudflare policies to guard users and devices from multi-channel phishing, ransomware, and more.



### Automate SOC response

Build AI-assisted mitigation workflows in Falcon Next-Gen SIEM enriched by Cloudflare telemetry.

## Our Joint Solution At-A-Glance



**Figure 1: Cloudflare / CrowdStrike Integration**

Users connect to Cloudflare, which references the CrowdStrike ZTA score to determine access.

## 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?

[Visit our tech partner directory](#)