CrowdStrike + Cloudflare

Bring integrated Zero Trust security to devices, applications, and corporate networks

An evolving corporate perimeter

Traditional network security models are no longer fit for purpose

Today users, devices, and applications exist outside the traditional corporate perimeter. Applications live in the cloud, teams work remotely, and cyber threats exploit our lack of visibility plus the excessive trust built into perimeter-based approaches. Budgets are falling and scarce, so costly hardware and complex multi-vendor solutions are less attractive as an IT investment.

All CISOs and CIOs want to ensure their employees and contractors are able to securely and efficiently access critical resources at all times, with no additional burden to their existing infrastructure or their security and IT teams. They are looking for safer, faster, easier ways to secure devices and enable access for hybrid or increasingly distributed workforces — without increasing an organization's attack surface and frustrating end users.

Today's corporate network

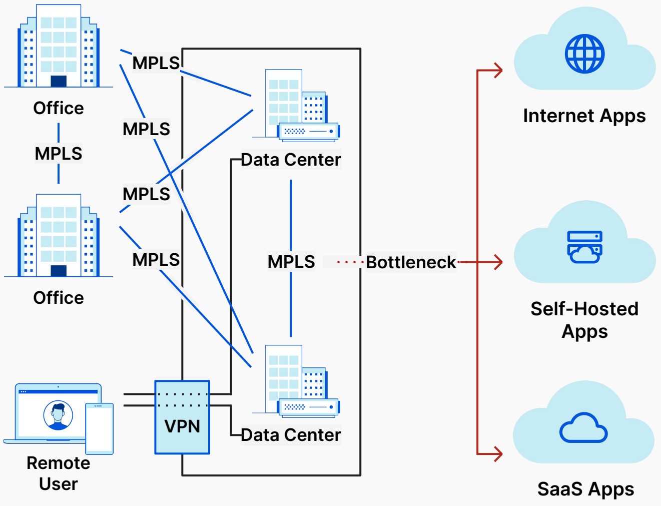


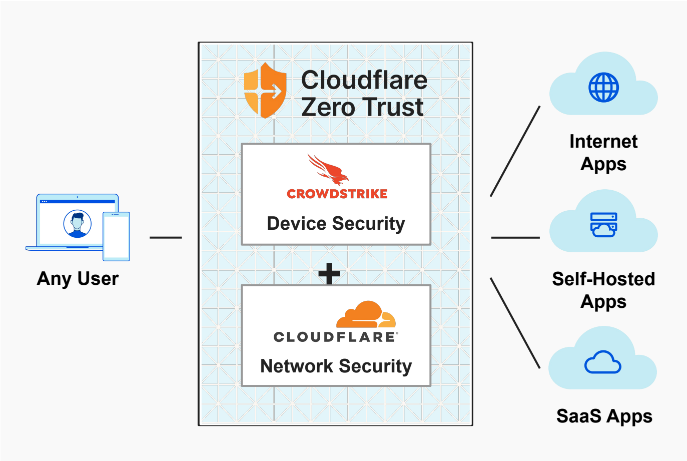
Figure 1: Traditional network and application security can no longer stretch to cover rapidly expanding risks, coupled with an ever more permanent hybrid workforce that are slowed down by antiquated connectivity methods.

> **"The CrowdStrike Falcon platform secures customers through verified access controls, helping customers reduce their attack surface and simplify, empower, and accelerate their Zero Trust journey. By expanding our partnership with Cloudflare, we are making it easier for joint customers to strengthen their Zero Trust security posture across all their endpoints and their entire corporate network."[1]**
>
> Michael Sentonas, Chief Technology Officer at CROWDSTRIKE

Integrated Zero Trust security with Cloudflare + CrowdStrike

A simpler, more cost-effective solution

With Cloudflare and CrowdStrike's integrated Zero Trust security solution, customers achieve security across devices and corporate networks, all while significantly reducing the IT and operational work involved in the configuration of traditionally complex solutions.



Our roadmap to Zero Trust

Combine device + network security and enable conditional access to applications from any endpoint, regardless of the users or location. CrowdStrike customers can create device posture-based Network Access (ZTNA) and Secure Web Gateway (SWG) policies with Cloudflare to strengthen their Zero Trust posture.

Identify and mitigate threats with threat intelligence: CrowdXDR alliance allows joint customers to combine insights from Cloudflare's global network, spanning more than 275 cities in over 100 countries, with CrowdStrike's endpoint data to identify and stop cyber attacks.

Rapid collaboration in under attack situations: CrowdStrike is an incident response partner of Cloudflare, allowing CrowdStrike customers to get prioritized onboarding and support from Cloudflare in an under Attack scenario.

Simple, flexible architecture

A valuable integration that is easy to setup and maintain, not involving a time-consuming, error-prone experience that other legacy providers offer.

Stop breaches before they occur

Identify and isolate threats by preventing infected or vulnerable devices from accessing sensitive data (e.g. account credentials).

Faster, future-proof innovation

Cloudflare and CrowdStrike are building integrations across their product suite to allow customers to evolve fast, without adding to the agent fatigue.

Accelerate your Zero Trust roadmap

Request an architecture workshop

Not ready for your assessment?

Request a free trial.

1. Cloudflare blog post, March 17, 2022, "Cloudflare and CrowdStrike partner to give CISOs secure control across devices, applications, and corporate networks", https://blog.cloudflare.com/cloudflare-crowdstrike-partnership/