Kandji and Cloudflare: Improve Zero Trust Posture

Help teams enable device-aware ZTNA policies to protect their websites and applications with identity, context, and policy rules

Challenge

Today users, devices, and applications largely exist outside the traditional corporate perimeter. Traditional tools that connect employees to corporate applications (like VPNs and IP-based controls) grant excessive trust, exposing users to malicious threats like data loss, phishing, and malware. Moreover, they can increase an organization's attack surface, limit visibility, and frustrate end users.

Zero Trust Network Access (ZTNA) has recently emerged as a safer, faster, and easier way to enable access for increasingly distributed workforces. ZTNA protects specific resources, and users are granted access after verifying the identity, context, and policy adherence of each request. Adopting device posture in particular is a critical step and an important contextual signal for setting up effective Zero Trust policies.

Solution

Cloudflare and Kandji are working together to ensure a rapid, secure, and seamless setup of device-aware ZTNA policies. The integration works in two ways:

1. Device client deployment: Teams who need to implement a Zero Trust posture across their organization's Apple devices will need Cloudflare's device client running on every device. You can ensure not only that the device is trusted, but that it has the right security posture through the controls and settings enforced via Cloudflare's Zero Trust policies. This can be achieved by configuring Cloudflare WARP to make access to applications conditional to the Kandji software running on a device.

2. Custom access policy deployment: The WARP client can be deployed as a custom app. Through our integration, Kandji can install Cloudflare's device client and automatically reinstall if it is removed. Kandji can further improve device security posture through the enforcement of dozens of security settings across macOS computers. Deploying Cloudflare's client will enable admins to set Zero Trust policies that check for device posture before users access resources.

Benefits

Enable device-aware ZTNA policies: Enforce device posture policies at the endpoint through a diverse set of deployment approaches.

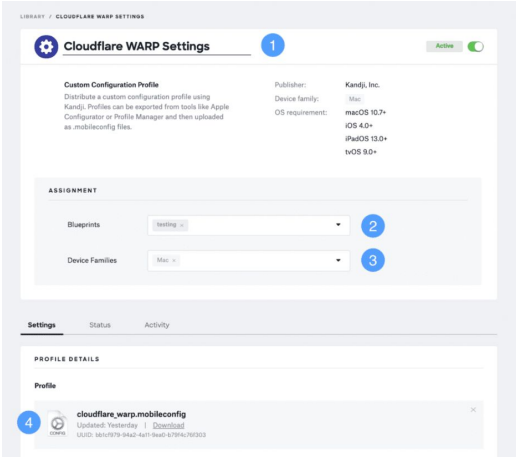
Ease of management: Configure policies for what users can do on a device with a set of parameters, offering admins a consistent experience.

Deploy updates with speed: Quickly and efficiently roll out new updates across a macOS fleet to ensure proper configuration.

Improved visibility: Obtain a unified view of device fleets across a dispersed user base to check that they are not compromised or lost.

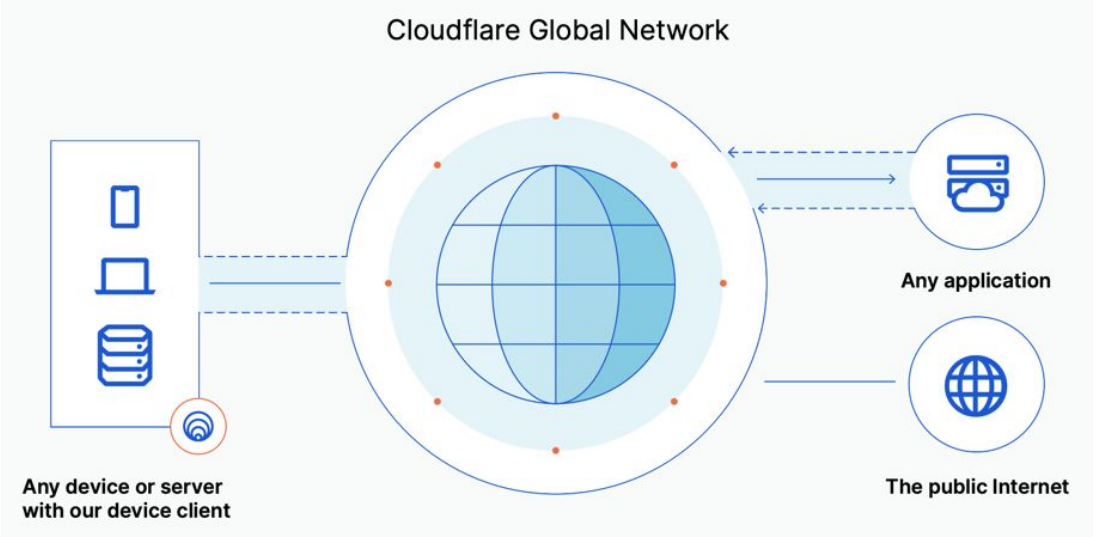
How to set up

Deploy Cloudflare's device client via Kandji following two steps: (1) setting up a custom profile and (2) deploying the client as a custom app. To learn more, follow instructions in our developer docs here.



How the Integration Works

With Kandji and Cloudflare, connecting to corporate resources is faster, safer, and more seamless for end users. Through this partnership with Kandji, Cloudflare can onboard user devices onto a Zero Trust architecture, allowing them to leverage both private routing and device posture. Moreover, admins can control how internal domains are resolved and IP traffic is routed or split tunneled, such that it will not affect any connectivity and even interoperate with existing VPN clients.



As requests are routed and accelerated through Cloudflare's edge, they are evaluated against Zero Trust rules to incorporate signals from your identity providers, device posture, and other contextual factors. Implementing a "never trust, always verify" posture can help you mitigate the most prevalent security vulnerabilities while leveraging Cloudflare's speed and scale.

About Kandji

Kandji is an Apple device management (MDM) and security solution built exclusively for IT teams at organizations that run on Apple. Kandji saves IT teams countless hours of manual, repetitive work with dozens of security controls organized into one-click compliance templates, pre-built automations, apps, and workflows. Learn more at kandji.io/product.

About Cloudflare

Cloudflare Zero Trust is a security platform that increases visibility, eliminates complexity, and reduces risks as remote and office users connect to applications and the Internet. In a single-pass architecture, user traffic is verified, filtered, inspected and isolated from Internet threats; and performance never suffers, as users connect through data centers near them in 250+ cities and 100+ countries around the world. Other Zero Trust providers offer multiple point products to protect from every threat vector, but leave customers to manage their own attack surface. Cloudflare's platform stops more attacks by isolating applications and endpoints from the attack surface by shifting it to our edge, and applies threat defenses to shield that edge. Learn more at cloudflare.com/products/zero-trust.