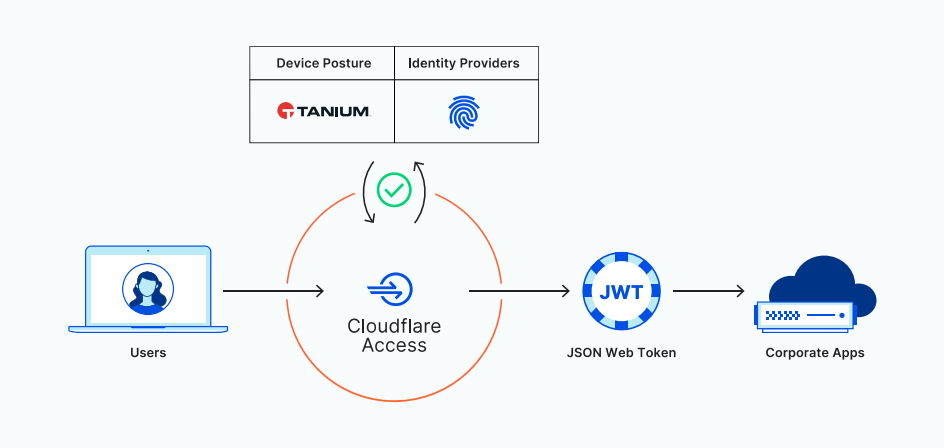
Tanium and Cloudflare

Zero Trust access to corporate apps. Now with device posture intelligence. Better together.

As your global workforce becomes increasingly remote, employees, contractors and vendors are constantly accessing your company's resources, and they're logging on from everywhere. Securing sensitive resources means ensuring every connection originates from trusted devices and verified users. Learn how Cloudflare and Tanium work together to provide defense-in-depth to internally-hosted applications.



Combine Tanium and Cloudflare for defense-in-depth to corporate apps

Add the Tanium device posture signal to a Cloudflare Access policy to make sure every connection to corporate apps is verified for user and device trust. When a user logs in to an application protected by Access, Access first verifies that the device is managed by Tanium, then checks policies from your corporate Identity Provider (IdP) to verify the user can access the corporate application. Every connection to your corporate application gets an additional layer of identity assurance, and users avoid having to fire up a VPN to get connected.

To see how it works in action, visit cfl.re/TaniumCloudflareTeams

Authenticate users on Cloudflare's global network

Cloudflare Access secures web apps, SSH connections, remote desktops and other protocols with Cloudflare's global network, where every request to the resource is evaluated for identity.

When corporate tools are protected with Access, they feel like SaaS apps, and employees can log in to them with a simple and consistent flow.

Protect corporate endpoints with Tanium

Tanium, a unified endpoint management and security platform, integrates with Cloudflare Access to ensure devices connecting to their cloud and Zero Trust networks are managed and secure; all without requiring another agent.

With Tanium, you can ensure your corporate endpoints are patched and protected, restricting access to only managed and secure devices.