

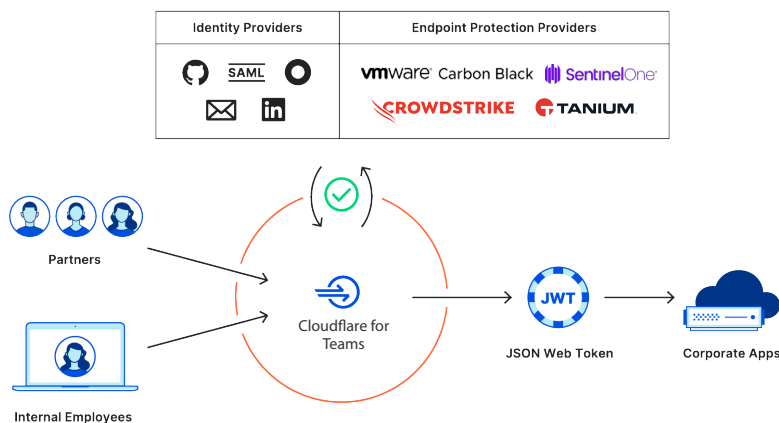
Cloudflare and Endpoint Security Providers

Cloudflare is partnering with leading endpoint protection providers — CrowdStrike, VMware Carbon Black, SentinelOne, and Tanium — to make Zero Trust security seamless for our customers.

As the global workforce becomes increasingly remote, employees, contractors, and vendors are constantly accessing sensitive corporate resources from a variety of devices. Securing sensitive resources means ensuring every connection originates from secured devices and verified users.

Our integrations with endpoint protection platforms enable Cloudflare customers to easily configure access rules using device posture signals from our partners.

Never trust, always verify identity and device posture



Identity and device verification

When a user logs in to an application protected by Cloudflare, we verify whether the device is protected by an endpoint security provider and also verify the user's identity with their identity provider.

How device verification works

Cloudflare checks if the endpoint security software is running on the device. Based on this status, access policies can be configured in the Cloudflare dashboard.

The Cloudflare Difference



Global reach

Bring enforcement decisions within 100ms of 99% of the world's Internet-connected population.



Integration with multiple providers

Mix and match across endpoint security and identity providers.



Easy setup

Just a few clicks in the Cloudflare dashboard to add device posture signals into Cloudflare for Teams policies.