CLOUDFLARE

WHITEPAPER

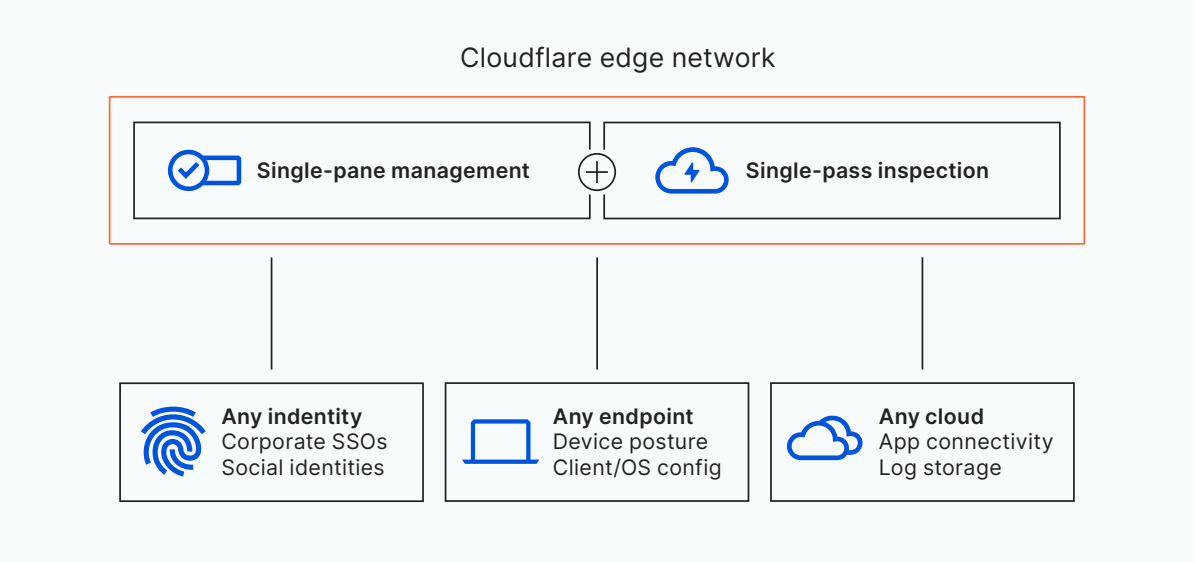
Cloudflare's Zero Trust Integrations

Build on the identity, endpoint, and cloud providers you already use

Juggling multiple identity, endpoint, and cloud providers within an organization is inevitable, but need not be burdensome. At Cloudflare, our goal is to empower your organization with the most robust security in the easiest-to-use way. Unlike other vendors, we do not have any vested interest in what specific providers in those categories you work with today or in the future.

We're agnostic. Therefore, our long-held strategy has been to design Cloudflare Zero Trust to integrate with as many other solutions as possible.

Through integrations, Cloudflare aggregates signals across multiple providers and serves as a single control pane to enforce context-rich, granular policies all across our global network. Moreover, these integrations do not require researching dense technical documentation; they are pre-built as workflows for more seamless, single-pane management.



Here, we highlight three principles we follow to meet customers where they are:

- **Identity agnostic:** Authenticate users across multiple identity provider types for frictionless access across all users without any configuration headaches.
- **Endpoint agnostic:** Enrich your device posture checks in more granular and adaptive ways with signals both from your favorite endpoint providers and our device client.
- **Cloud agnostic:** Secure applications on any public or private (on-prem) cloud to avoid long-term vendor lock-in.

Aggregate multiple identities onto Cloudflare

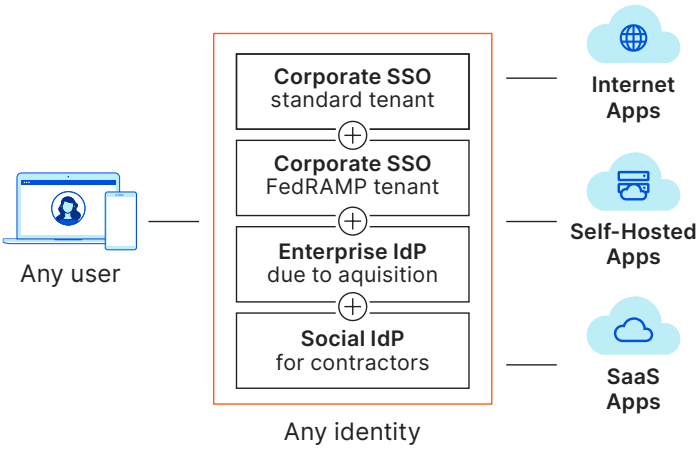
Multi-SSO

Cloudflare built one of the first Zero Trust access solutions to support multiple identity providers (IdPs) simultaneously. Today, we integrate with leading corporate IdPs (such as Okta or Azure AD), as well as social identities (like LinkedIn or Github) and open source standards (like SAML or OIDC). Moreover, we support multiple instances of the same IdP: for example, a FedRAMP and non-FedRamp use of Okta.

Federate multiple identities at once

Our ability to federate identity across many IdPs can jumpstart the process of building identity-aware policies. Organizations no longer need to build custom integrations between their IdPs.

Growth-stage organizations with more limited infosec personnel may find federation a particularly powerful tool to scale a Zero Trust approach without the hassle of consolidating a single centralized directory.



Key features

- Cloudflare integrates with multiple IdPs simultaneously, all best-in-class
- Federate multiple providers and multiple instances of each provider
- Faster onboarding for 3rd party users and M&A partners

Use Case:

Making 3rd party users feel like first class citizens

Cloudflare's identity-agnostic approach is particularly handy when collaborating with third parties outside your organization such contractors, acquired businesses, or partners. Least-privileged access rules can be set up in minutes based on the identities these users already bring to the table.

This no-fuss flexibility avoids the inefficiencies and security risks of provisioning SSO licences, deploying VPNs, or creating one-off permissions.

Best-in-class endpoint protection partners

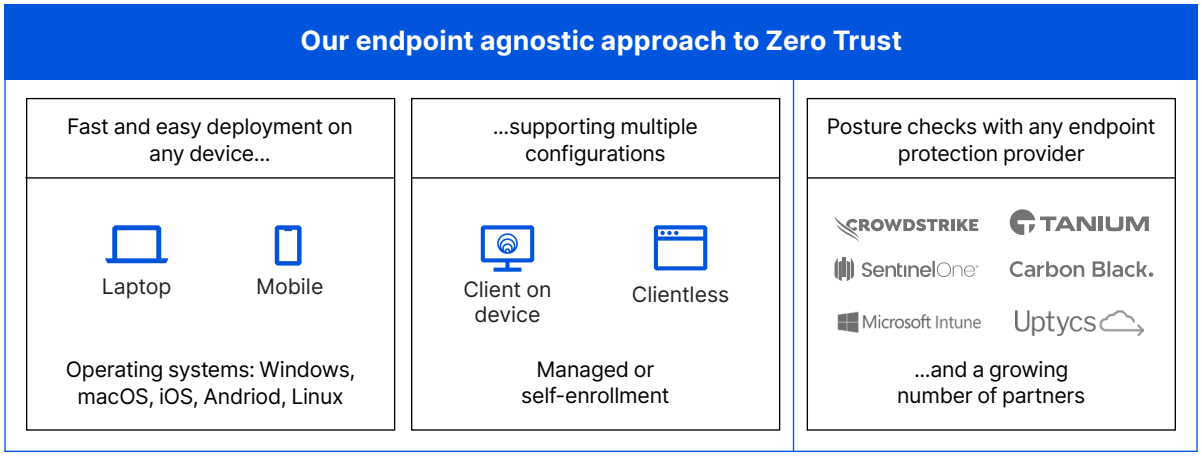
Partnerships

Cloudflare partners with CrowdStrike, SentinelOne, VMware Carbon Black, Tanium, Uptycs and Microsoft Intune.

Customers can onboard multiple endpoint protection providers at once and leverage security signals and risk assessment capabilities of those solutions.

Configuration

Configuring any of these providers is just a few clicks on the Cloudflare dashboard with prebuilt workflows. Once set up, Cloudflare can check that devices are running your preferred endpoint software to provide ongoing monitoring against malware and other threats before allowing or denying access to a protected application.



Integrations enhanced by ourdevice client (WARP)

Leveling up security often requires a device client, which can enrich device posture checks with additional attributes. We've deliberately optimized ours for flexible and effortless adoption.

Deploy on most operating systems

- Our enterprise client - WARP - works across a growing list of the most popular operating systems (e.g. Windows, macOS, Linux, iOS, and Android).
- Our modern WireGuard architecture only ever requires minor OS-specific code tweaks.
- Our enterprise client has a consumer version used daily by millions worldwide. Testing for so many individual users means WARP comes more battle-ready than most clients used for Zero Trust.

Managed or self-enrollment options

- For managed devices, we document deployments with any script-based method across popular mobile device management (MDM) software.
- Self-enrollment of WARP can be useful for third party users and only takes a few minutes for any desktop or mobile phone.

Avoiding cloud provider lock-in

Problem

Some, more monolithic vendors are primarily interested in increasing your consumption of their cloud services, particularly at the storage and compute layers.

To nobody's surprise, their add-on security solutions don't integrate as smoothly as they should with other cloud providers. Little inconveniences like weaker documentation and bugs add up. That tech stack lock-in makes life more difficult for your infosec teams.

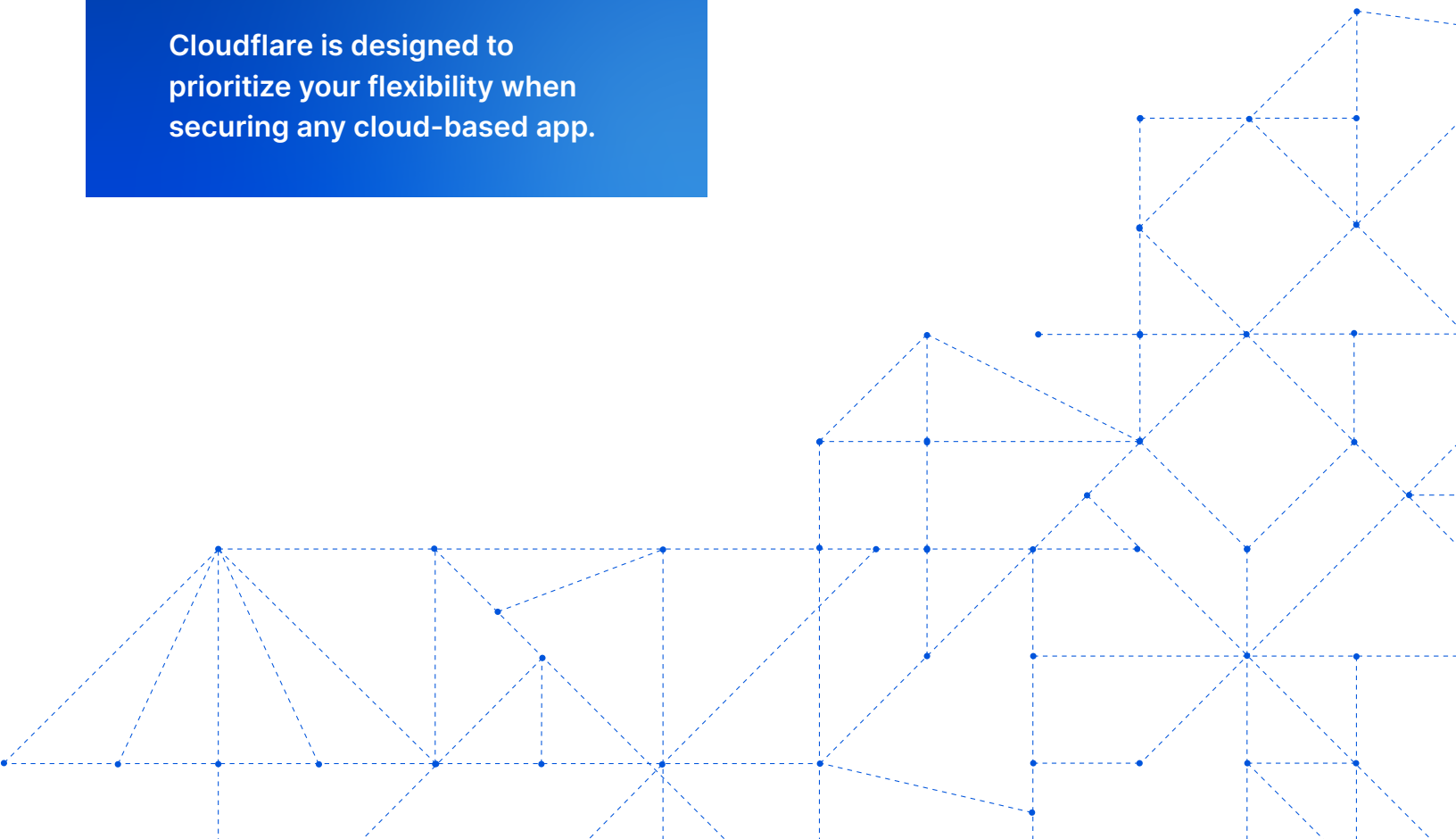
Solution

By contrast, our strategic focus is your security - not your cloud consumption. Cloudflare is cloud agnostic: We secure access to any resource in any public, private, or SaaS cloud environment.

Cloudflare is designed to prioritize your flexibility when securing any cloud-based app.

Key features

- Zero Trust access across public, private, and SaaS clouds environments
- No vendor lock-in to cloud compute or storage destinations
- App connectors, network on-ramp partners, and storage integrations that make it easy for you to interact with apps in any cloud



Cloudflare strengths

Extend connections to apps in any cloud

Our lightweight app connector works in every cloud

- Run command-line tool as a service on Linux and other OSes
- Pre-packaged as a Docker container
- Replica support for modern Kubernetes environments

Extensive interconnects with cloud providers

- Fast connections for users enabled by 11,000 interconnections between our network and other cloud providers, 50 of which are private interconnects with Microsoft, Amazon, and Google's data centers

Diverse network onramp partners that are not cloud-specific

- Easily connect any public and private cloud environment to our network using your existing SD-WAN routing method (e.g. VMware) or privately interconnect at over 1600 colo provider locations (e.g. Equinix)

Push log data to any cloud

Log data can be stored across clouds or sent directly to analytics providers

- Built-in support for one or more storage destinations concurrently including AWS, Azure, Google Cloud, and any S3-compatible API (e.g. Digital Ocean Spaces)
- Built-in integrations with analytics and SIEM tools like Sumo Logic, Splunk, and Datadog

Security across any public or private cloud

Roster of Zero Trust integration partners

Over time, Cloudflare will aggregate signals from an even wider roster of your preferred providers, all bolstered by the intelligence of our Zero Trust platform and global network.

Identity Providers

Corporate SSOs

- Centrify
- Citrix ADC
- Google Workspace
- JumpCloud
- Microsoft Azure Active Directory (AD)
- Okta
- OneLogin
- PingIdentity

Social identities

- Facebook
- GitHub
- Google
- LinkedIn
- Yandex

Open Source

- OIDC
- SAML 2.0

Endpoint Providers

Endpoint Protection Providers

(for device security posture)

- CrowdStrike
- Microsoft Endpoint Manager
- SentinelOne
- Tanium
- Uptycs
- VMware Carbon Black

Endpoint Management Providers

(for client deployment)

- Hexnode
- Ivanti
- Jamf
- JumpCloud
- Kandji
- Microsoft Intune

Network Onramp Partners

Physical Interconnect Partners

- 365 Data Centers
- BBIX
- CoreSite
- Cyxtera
- Databank
- Digital Realty
- EdgeConneX
- Equinix
- Netrality Data Centers
- Teraco
- Zayo

Fabric Interconnect Partners

- Console Connect / PCCW
- CoreSite
- Epsilon Infiny
- Equinix Fabric
- Megaport
- PacketFabric

SD-WAN

- Aruba (Silverpeak)
- Cisco
- VMware (Velocloud)

Cloud Providers

Cloud Storage Destinations

- AWS S3
- Google Cloud Storage
- Microsoft Azure Blob Storage
- Other vendors with an S3-compatible API

Cloud Analytics & SIEM Partners

- Azure Sentinel
- Datadog
- Elastic
- Google Cloud
- Graylog
- IBM QRadar
- Looker
- New Relic
- Splunk
- Sumo Logic

To learn more about Cloudflare Zero Trust and request a demo or POC from a sales representative, please visit: https://www.cloudflare.com/products/zero-trust.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3795.2022SEP22