

Zero Trust Security for Remote Workers

A technical sales strategy aligned to Cloudflare for Teams

FOR PARTNER USE ONLY

**NON CUSTOMER FACING
DOCUMENT**

Host:



Jean Ryu
Partner SE
APAC

Presenters:



Antonio Rancan
Cloudflare for Teams
SME



Chrisanthy Carlane
Partner Tech
Enablement

What we are going to cover today?

- Zero Trust Architecture and Cloudflare for Teams
- What we see in the field - Customer Use Cases
- Features and Integration
- Technical Qualification Questions
- Cloudflare for Teams showcase
- Product Packaging
- Partner Resources
- Q&A



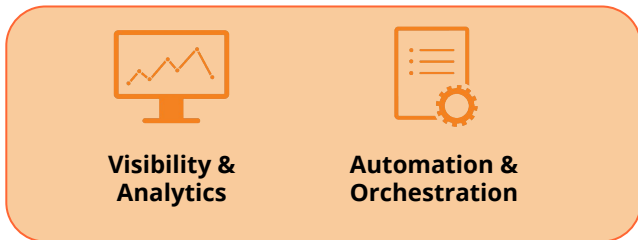
This training is aimed to provide Partners with a quick pointers on how to sell Cloudflare for Teams solution.

Documentations, online courses, technical resources is available at Partner Portal and Cloudflare University for deeper understanding.



Zero Trust is a security strategy that focuses on context-based authentication rather than network-and-location based trust

Areas to secure
with Zero Trust

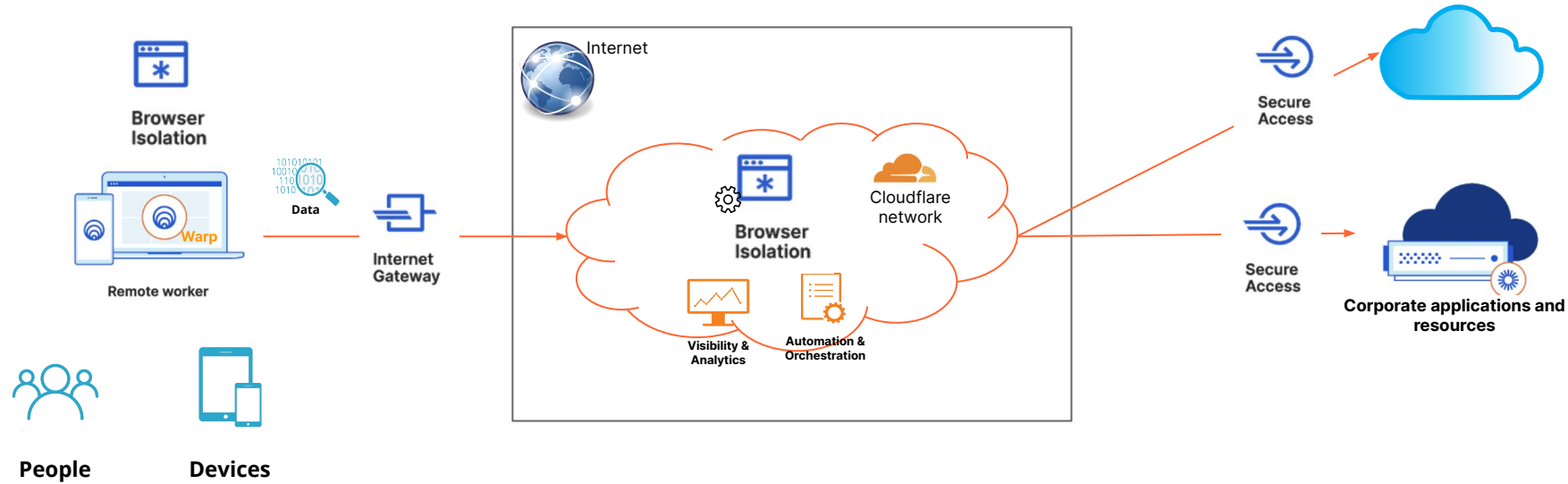


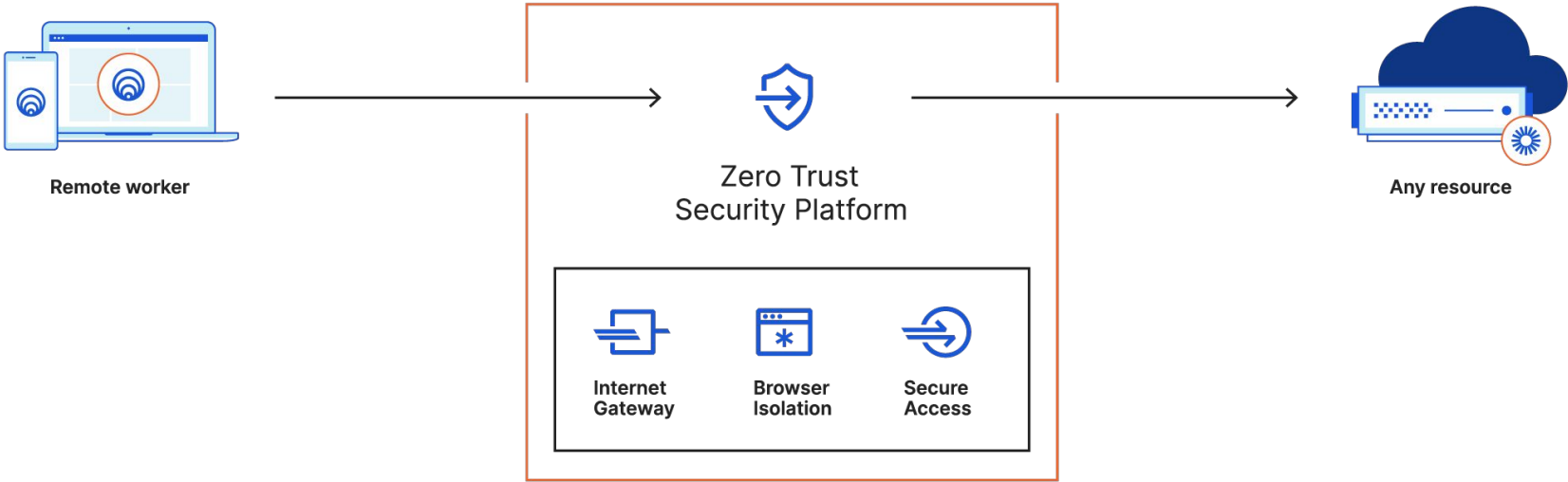
Zero trust is a strategic mindset based on core guiding principles:

- “Never trust, always verify”
- Access based on identity and context (not location on/off the network)
- Least privilege access by default

Key assumption: Your users and network are likely already compromised. Therefore, they should *not* be granted privileged access by default.

HOW IT APPLIES TO CUSTOMER ENVIRONMENT





- | | | | | | | | | |
|---|---|---|---|--|---|---|---|---|
|  |  |  |  |  |  |  |  |  |
| Intelligent routing | Global edge network | World's fastest resolver | Single-pass inspection | Single-pane management | Programmable interface | MDM • IdP • EPP integrations | Internet radar | Visionary innovations |

What is Zero Trust Security?

NEVER
TRUST
NON
EMPLOYEE

NO
TRUST,
EXCEPT
FROM
INTRANET

NEVER
TRUST,
ALWAYS
VERIFY

Zero Trust Solutions

What to look for:

1. The strength & distribution of the network
2. The cohesion and integration of the platform
3. The potential for future capabilities
4. The current features and capabilities
5. The cost & pricing model

What we see in the field?

Learn the examples of Zero Trust implementation, technical requirements and the challenges



How we deliver on remote work use cases

Use Case	How	In the real world....
Connect remote workers to corporate apps	Between devices and apps, route traffic (DNS, HTTP(S), RDP/SSH) through Cloudflare's network for better performance and reliability than your VPN*	ACME Corp. have less latency and better connections because their traffic is being sent to a nearby Cloudflare location, instead of being backhauled through a faraway data center via VPN.
Adopt Zero Trust security for apps access	Policy based on identity (verify via multi-factor authentication), posture (verify via endpoint protection/mgmt and gateway protection), and context (geo) instead of network location (IP)	In order to log in to Salesforce, John in Marketing at ACME Corp must have Tanium or Cloudflare's client installed, authenticate via a hard token, and be physically located in a designated country.
Adopt Zero Trust security for internet browsing	Isolate browser activity from gateway-protected devices to stop malware and phishing	John in Marketing browses social media during the work day. Corporate policy isolates John's session, so drive-by malware cannot reach his device.

*Note: It's not about replacing the VPN, it's about reducing reliance on it

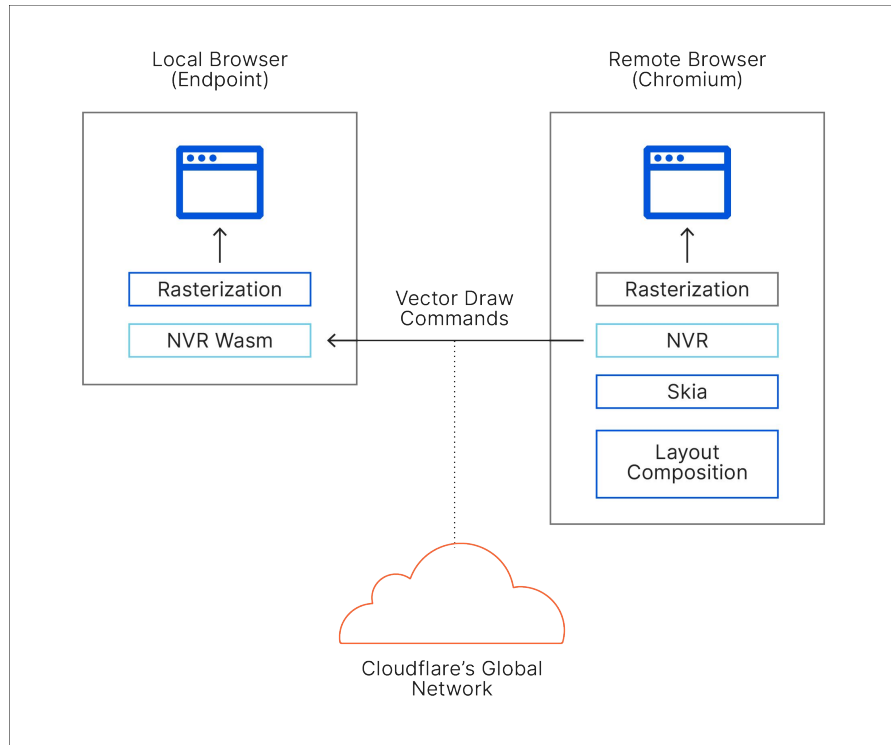
How we deliver on remote work use cases

Use Case	How	In the real world...
Protect data from unauthorized access and uploads	Fine grained control over user and device access rights; prevent file uploads/downloads	John in marketing can upload and download files in Google Drive, ACME Corp's approved/official file sharing platform. When he tries to upload a file to Dropbox, the action is blocked.
Protect devices from malicious content within a site	Any known or unknown malicious content is run remotely in safe containers across our network, isolating it from reaching the device's local browser	While reading the news, John inadvertently clicks on a banner ad. The website tries to download a plugin on his browser, but the action is blocked.
Protect users from phishing sites	Native and third-party threat intel blocks phishers before they strike	John receives a suspicious email from a vendor asking him to login to a streaming site. The site has been flagged as phishing, so it's blocked.

What's New









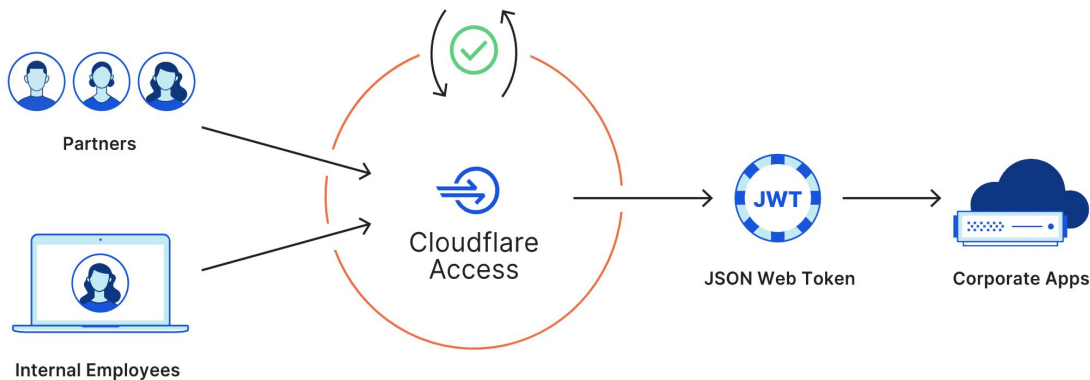
Cloudflare Browser: Next Generation Approach



- Next generation RBI technology (not pixel; not DOM)
 - Eliminates tradeoffs inherent in existing RBI technologies
 - Security | Performance | User Experience
 - Lower bandwidth than local browsing
 - Typically faster than local browsing

Cloudflare + Endpoint Protection partners: End-to-end Zero Trust security solution

Identity Providers	Endpoint Protection Providers
 SAML   	vmWare [®] Carbon Black   

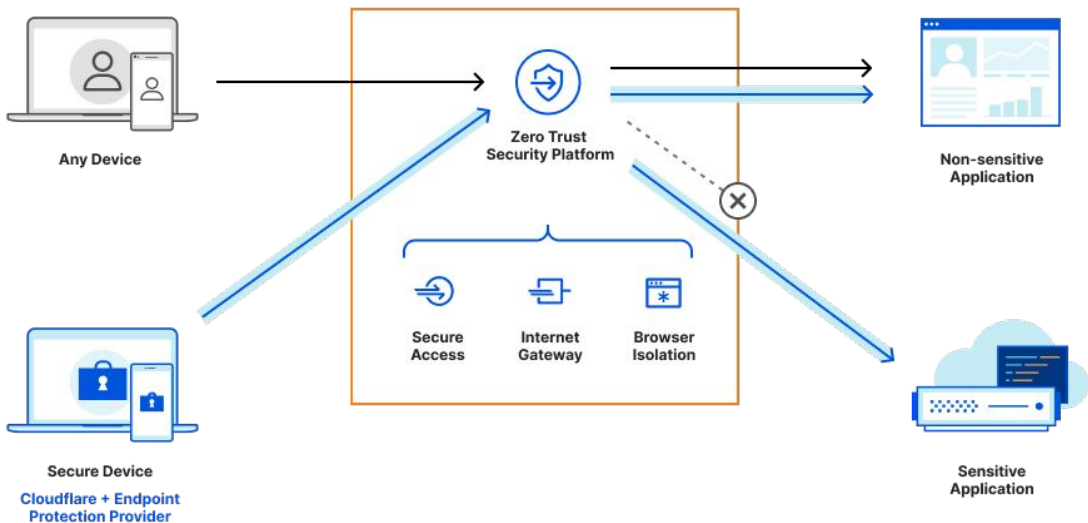


Add device posture signals to Cloudflare Access to make sure every connection to corporate apps is verified for **user** and **device** posture

Never trust, always verify device posture



With Device Posture Rules

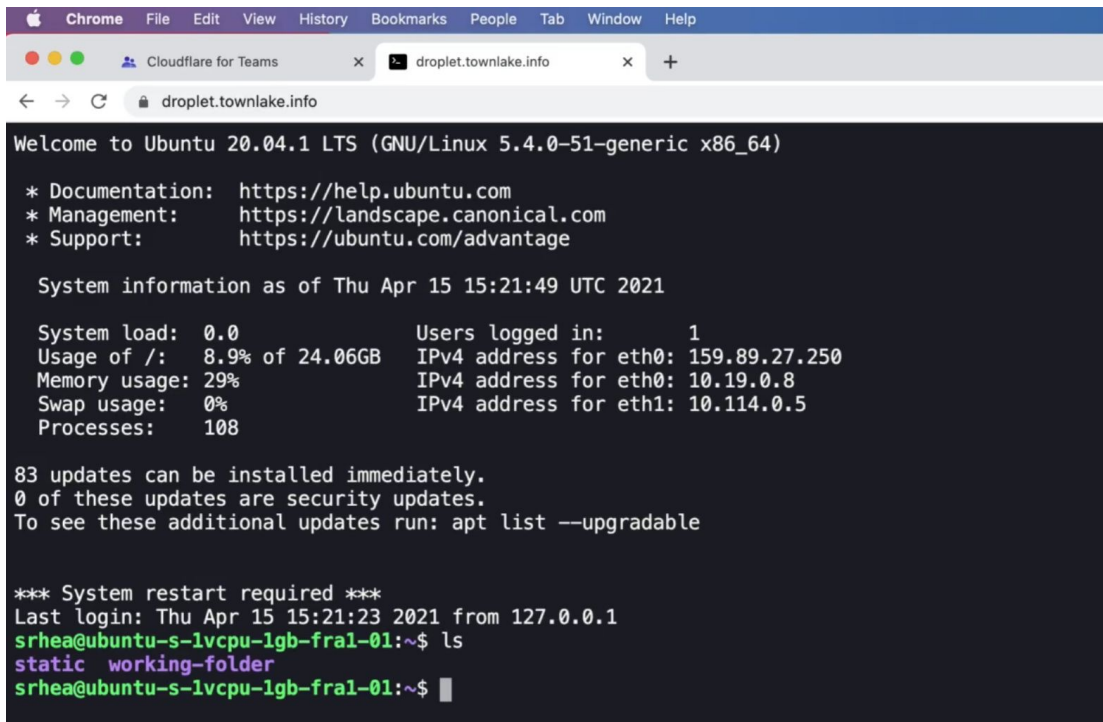


Our WARP client (installed on the device) checks if the endpoint security software is running on the device and communicates the status to Cloudflare, based on which users will be allowed or denied access.

Result — every connection to your corporate application gets an additional layer of identity and device assurance

A Zero Trust terminal in your web browser

Cloudflare's browser-based terminal renders a fully functional console that a user can launch with a single click.



The screenshot shows a Google Chrome browser window with the address bar displaying 'droplet.townlake.info'. The terminal content is as follows:

```
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-51-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Thu Apr 15 15:21:49 UTC 2021

System load:  0.0                Users logged in:      1
Usage of /:   8.9% of 24.06GB    IPv4 address for eth0: 159.89.27.250
Memory usage: 29%               IPv4 address for eth0: 10.19.0.8
Swap usage:   0%                IPv4 address for eth1: 10.114.0.5
Processes:   108

83 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

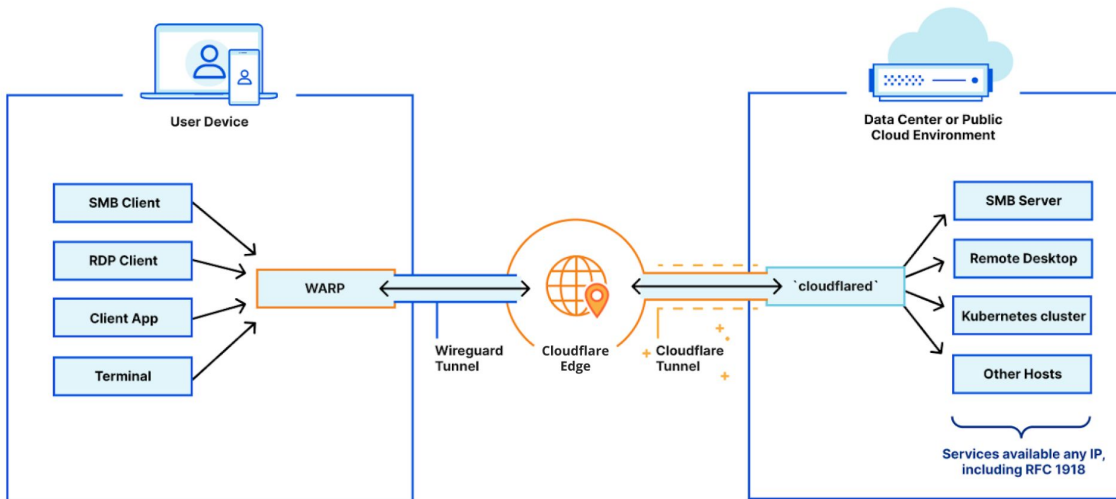
*** System restart required ***
Last login: Thu Apr 15 15:21:23 2021 from 127.0.0.1
srhea@ubuntu-s-lvcpu-1gb-fral-01:~$ ls
static  working-folder
srhea@ubuntu-s-lvcpu-1gb-fral-01:~$
```

<https://blog.cloudflare.com/build-your-own-private-network-on-cloudflare/>

Route Private IP Networks through Cloudflare

Combines the usability of VPN with performance and security of Cloudflare's network

1. Run cloudflared in data centre/cloud
2. Create Tunnel and route IP range
3. Run the tunnel
4. Connect using Warp client



<https://blog.cloudflare.com/build-your-own-private-network-on-cloudflare/>

Cloudflare for Teams: Access and Gateway integrated



Access

Zero Trust security for
all applications

- Unified access policies to internal applications and SaaS applications
- Apply additional device posture without expensive IDP upgrades
- Log and review every event and request
- Aggregate identity from multiple sources to simplify access control for mergers and acquisitions, contractors, partners and more
- Improve application delivery speed with Cloudflare's network scale and intelligent routing



Gateway

Secure users, devices and networks
on the open Internet

- Catching threats at our network edge
- Enforce URL filtering with WARP Client
- Secure branch office traffic without hardware or centralized backhauling
- Inspect SaaS application traffic for Data Loss Prevention and compliance auditing
- Cloudflare Browser integration
- Eliminate expensive MPLS fees



WARP Client



Browser Isolation

Technical Qualification Questions

Use Cases and Discovery Questions

Use Cases	Questions
Connect remote workers to corporate apps	<ul style="list-style-type: none">• How are you handling remote user traffic?• Are you routing some or all of your traffic over a VPN?• Do you have any filtering policies in place?
Adopt Zero Trust security for application access	<ul style="list-style-type: none">• How granular is your access control today?• Using multifactor authentication? Are hardkeys required?
Adopt Zero Trust security for Internet browsing	<ul style="list-style-type: none">• How do you keep browsers or plugins always up to date?• Can you trust users to know that a site is phishing them?
Protect data from uploads and unauthorized access	<ul style="list-style-type: none">• Do you need to control the movement of data in/out of SaaS apps? Or apps you built in the public cloud?
Protect devices from malicious code in a site	<ul style="list-style-type: none">• Confident in your endpoint security stopping all threats?• What's your policy for users visiting a newly seen site?
Protect users from phishing sites	<ul style="list-style-type: none">• If a new phishing site were discovered, how would you go about blocking it today?

Cloudflare's Key Value Proposition

Reduce Risks

- ❑ Mitigate all known and unknown web-based malware and phishing on any site with no perceptible change to browsing performance
- ❑ Enforce least-privilege application access based on authorized users and devices after verifying identity and posture.
- ❑ Eliminate software conflicts or hardware failures from disrupting remote access.



Increase Visibility

- ❑ Mitigate risks by monitoring how sanctioned and unsanctioned apps are used by remote workers
- ❑ Investigate security or compliance incidents for up to 6 months (or extend via cloud storage integrations)



Eliminate Complexity

- ❑ Manage policies with simple rules based on identities, posture & context, not IPs, in one place across one dashboard
- ❑ Ultra-low latency by reducing reliance on VPN across a distributed remote workforce with single-pass inspection on the world's fastest edge network



Cloudflare for Teams

Product Packaging

<https://www.cloudflare.com/teams-pricing/>

Questions for Pricing

1. Number of Users
2. Access OR Gateway or Access+Gateway (Teams)
3. Browser Isolation (addon to Gateway)

Why Cloudflare for Zero Trust Solution?

Integrated security

DDOS protection, WAF and other Cloudflare Security offerings

Performance

Cloudflare's larger global network deliver better, more consistent performance.

Shared Threat Intelligence

Shared intelligence gathered servicing >25M websites and >3M customers

Cost Effective

Per user pricing with no unexpected charges for bandwidth and for application connectors(for protecting internal/SaaS apps). Economies of scale through building a global network

Browser Isolation

Cloudflare patented network vector rendering technology offers improved security and faster web browsing experience.

Roadmap

Cloudflare offer full SASE product roadmap that includes solutions to protect branch office networks and on-premise data centers.

Partner Resources



- **PartnerPortal Asset Library: Slides, SalesPlay, Battlecard**
- **Cloudflare University: Cloudflare for Teams Online Courses**
- **Try out Cloudflare for Teams!**
 - *Step by step Tutorials available*
 - *Reach out to your region Cloudflare Partner SE for access*
- **Cloudflare for Teams Main Documentation**
(<https://developers.cloudflare.com/cloudflare-one/>)

Tutorials

Name	Updated	Category	Length
● Filter DNS based on users and groups	4 days ago	 Web Gateway	<div><div></div></div>
Render an SSH client in a browser	2 weeks ago	 Zero Trust	<div><div></div></div>
Require corporate devices	1 month ago	 Zero Trust	<div><div></div></div>
SMB file shares	1 month ago	 Zero Trust	<div><div></div></div>
Connect through Cloudflare Access using a CLI	1 month ago	 Zero Trust	<div><div></div></div>

Thank you

FOR PARTNER USE ONLY

**NON CUSTOMER FACING
DOCUMENT**