Cloudflare Presales Engineer Training

22 Nov 2021

- Pradeep Mandloi, Siddhesh Chavan - Blazeclan
- Jean Ryu - Cloudflare

CLOUDFLARE

blazeclan

Core Use Cases

SECURITY

DDoS Attacks

Attack traffic degrades availability or performance and creates unpredictable surges in infrastructure costs

Malicious Bots

Malicious bots abuse customer applications through content scraping, account takeovers, credential stuffing, and fraudulent check outs

Data Theft

Attackers compromise customer data, such as user credentials, credit card information, and other PII

PERFORMANCE

Slow Internet Applications and APIs

Heavy pages and long distances from the origin slow down webpages, applications, and APIs

Slow Mobile Sites and Apps

Mobile clients introduce performance and content delivery constraints that hurt user experience

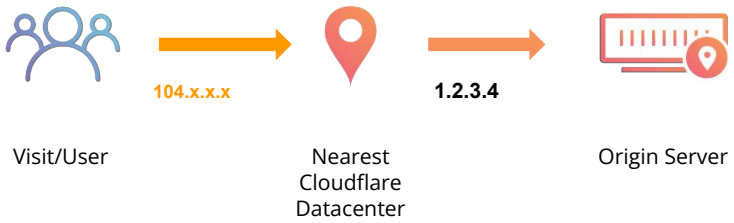
Unavailable Applications

Overloaded or unavailable infrastructure stops users from accessing applications

With a reverse proxy, setup is a 5-minutes DNS change.

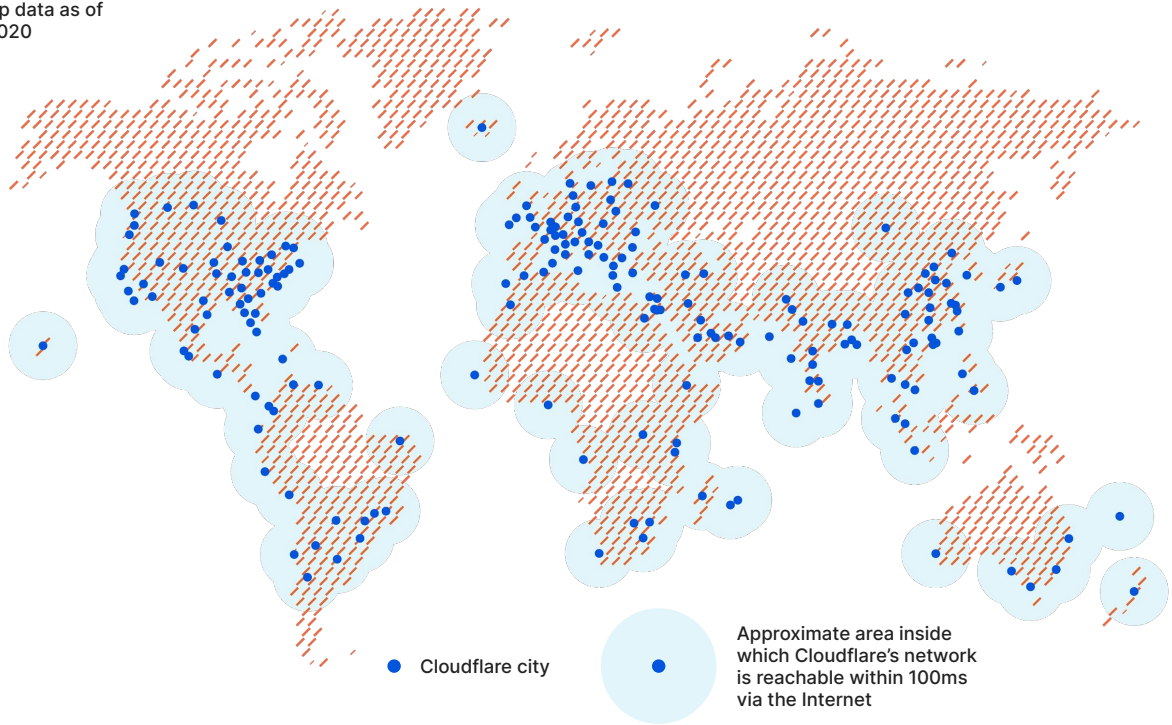
Before Cloudflare, an origin is exposed to visitors and attackers.

With Cloudflare, all requests route to the nearest data center via Anycast DNS and proxy to the origin.



Cloudflare edge network

Note: map data as of Jan 15, 2020



25M+
Internet properties

100 Tbps
of network capacity

250
cities in 100+ countries

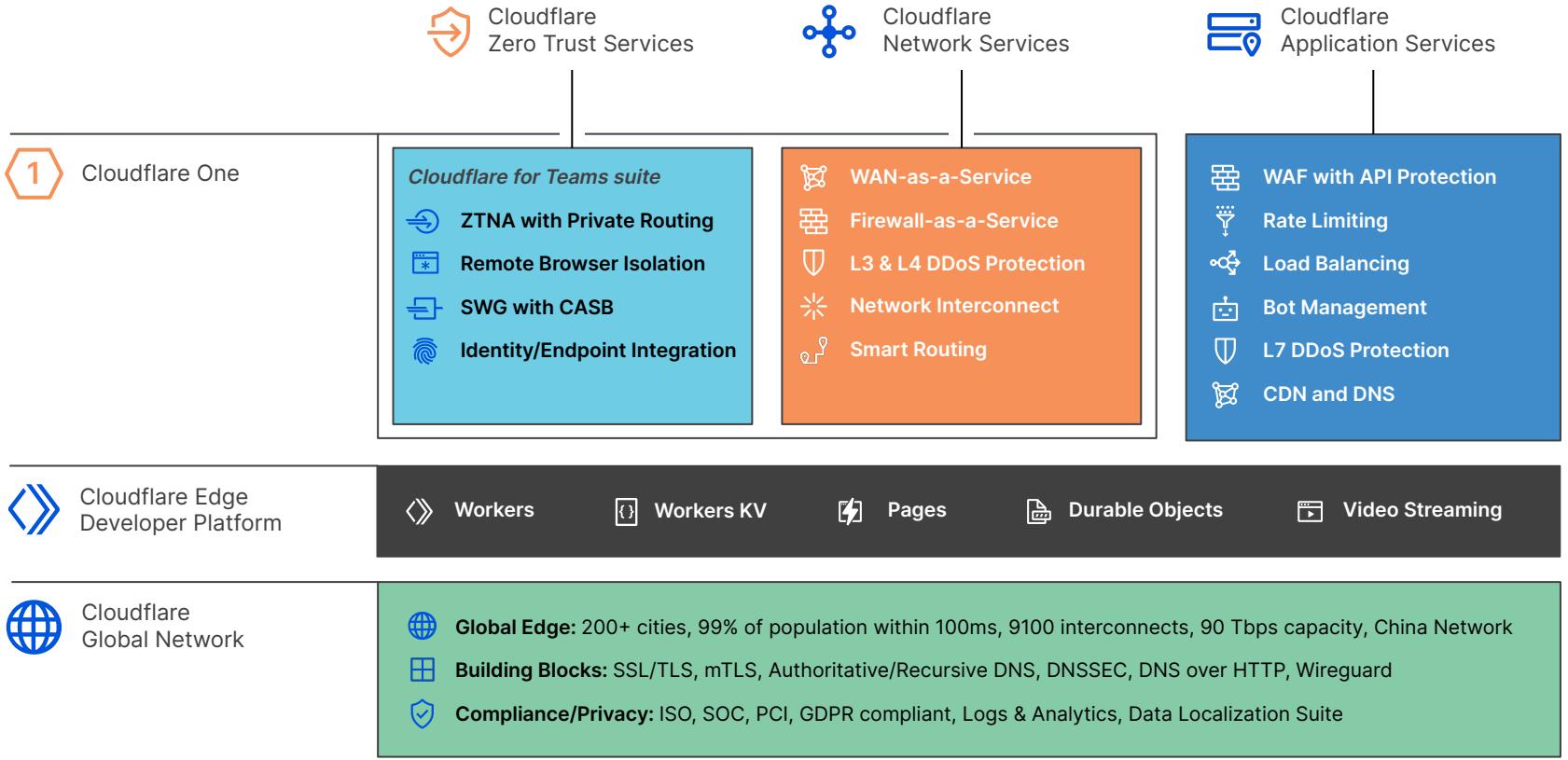
87B
cyber threats blocked each day in Q2'21

50ms
from 95% of the world's Internet-connected population

10,000
networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise (AS13335)

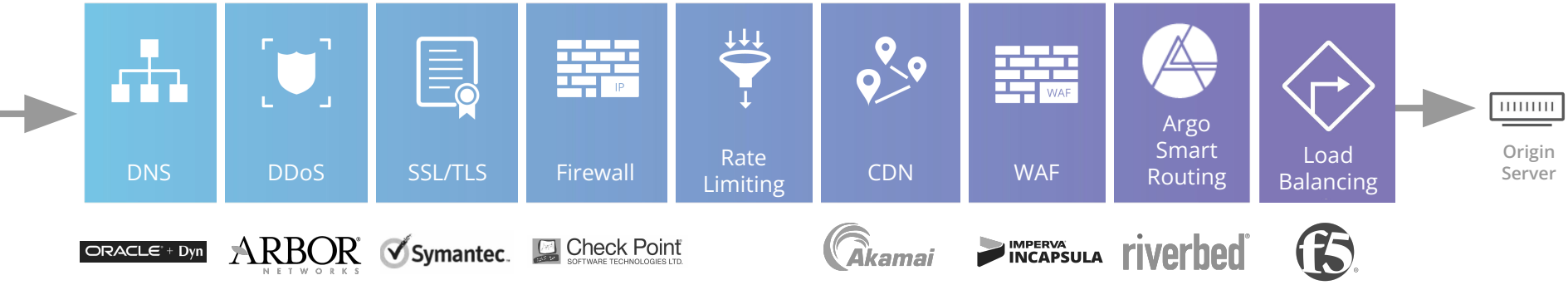
Cloudflare at a Glance

CLOUDFLARE



An integrated solution with lower TCO

Each Cloudflare Point of Presence runs an integrated stack of easy-to-use security, performance and reliability services



Why do enterprises choose Cloudflare?

INTEGRATED SOLUTION
NO TRADE OFFS

NETWORK SCALE

EASY, UNIFIED &
ADVANCED CONTROL

SHARED INTELLIGENCE

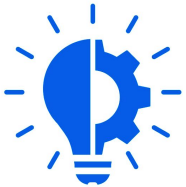
DEVELOPER FRIENDLY.
API FIRST.

MULTI-CLOUD SUPPORT

CLOUDFLARE

Differentiation (cont.)

EASE OF USE



SPEED OF INNOVATION

SUPPORT/OVERRELIANCE ON MANAGED SERVICES

MATURE SERVERLESS OFFERING

PERFORMANCE IN KEY AREAS (CHINA)

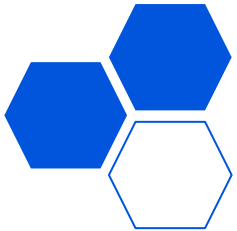
TOTAL COST OF OWNERSHIP (TCO)

Objection Handling for migrating customers

FEAR, UNCERTAINTY, AND DOUBT (FUD), LOWER ANALYST RANKINGS

MIGRATION PAINS/CONCERNS

NO MANAGED SERVICES



PERCEPTION ABOUT NO 1:1 OFFERING, FEATURE GAPS

PACKAGING + ADD-ON

CLOUDFLARE

Cloudflare - Defining the Edge

Products & Services

Application Services

- Web Application Firewall
- SSL/ TLS
- Bot Management
- Rate Limiting
- Layer 7 DDoS Protection CDN
- Load Balancing
- Stream Delivery
- DNS Services
- Logs and Analytics

Network Services

- WANaaS
- FWaaS
- L3 & L4 DDoS Protection
- *IDS/ IPS
- Smart Routing
- Network Interconnect

Zero Trust Services

- ZTNA
- SWG
- RBI
- *DLP

Cloudflare One

Cloudflare Platform

Serverless Developer Platform

Workers | Workers KV | Pages | Durable Objects | Video Streaming

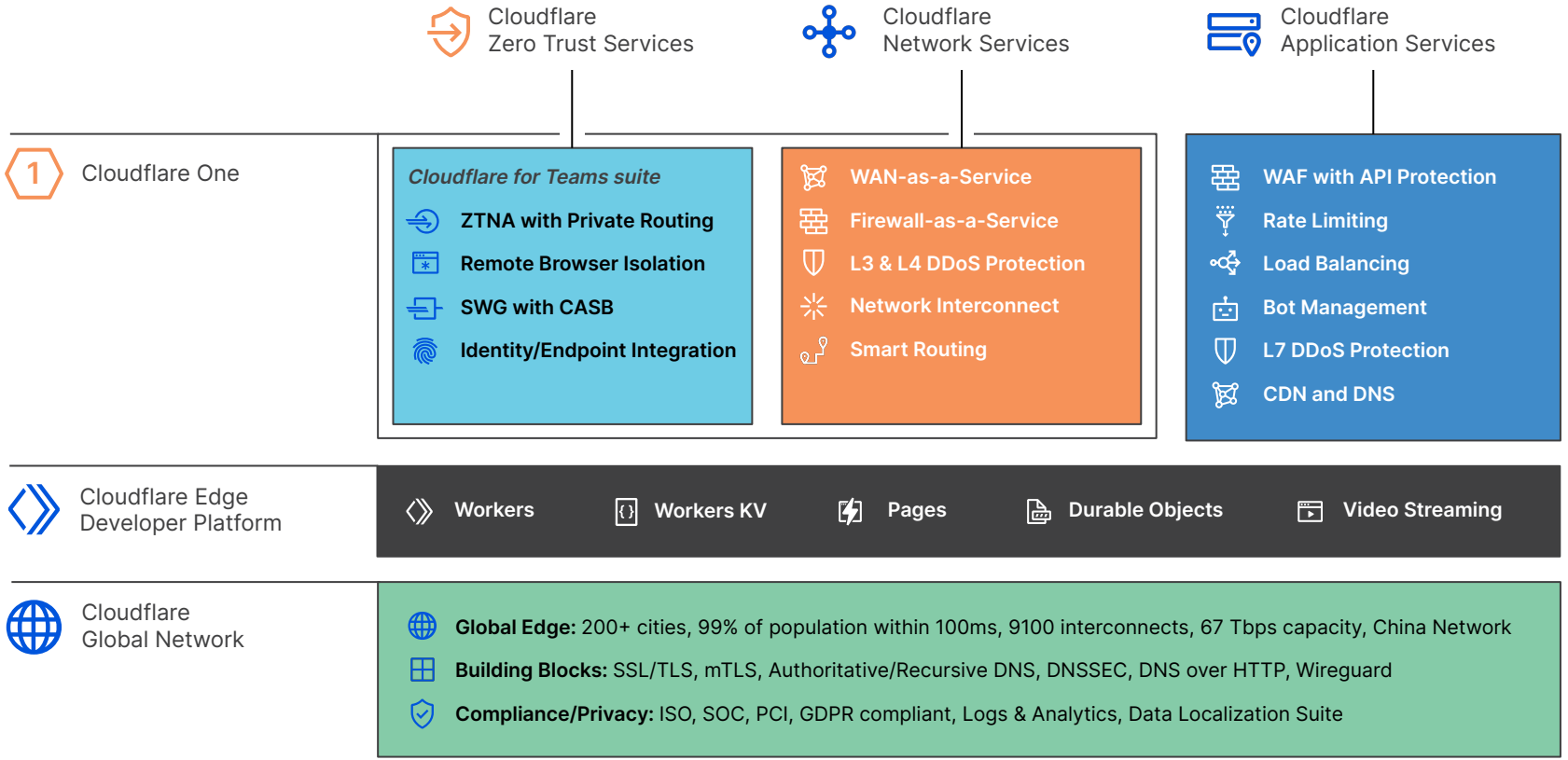
Cloudflare Network Infrastructure

~25 million Internet properties | 59 Tbps capacity | 200+ cities in 100 countries | 99% of population within 100ms
ISO/SOC/PCI/GDPR Compliance Certified | Support for latest web standards | China network

*Previewed, but not available yet

Cloudflare at a Glance

CLOUDFLARE



Cloudflare products comes with ENT plan

Managed Authoritative DNS	Managed SSL	Unmetered DDoS	WAF	Firewall Rules	IP Reputation Intelligence	Optimization	CDN	Analytics & Logpush

https://www.cloudflare.com/en-gb/cloudflare-product-portfolio/

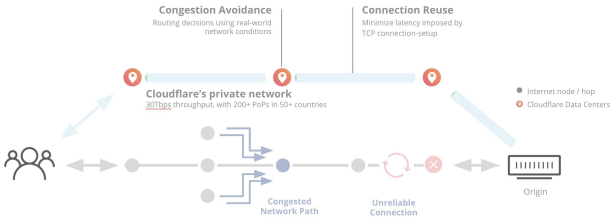
Products need additional packaging

Managed Authoritative DNS	Managed SSL	Unmetered DDoS	WAF	Firewall Rules	IP Reputation Intelligence	Optimization	CDN	Analytics & Logpush
Argo	Rate Limiting	Spectrum	Load Balancing	Bot Management	Stream Delivery	Payload Inspection	Image Resizing	API Shield
SSL for SaaS	Waiting Room	Mutual TLS	China Network	Stream			DNS Firewall	Secondary DNS
Access	Gateway (SWG, Warp) DNS Recursive	Remote Browser Isolation						Premium Success
Magic Transit	Magic WAN	Magic Firewall					Cloudflare Network Interconnect	Bandwidth Alliance
Workers	Workers KV							

Legend	ENT Application services	Application Services add-on	Cloudflare for Teams (ZTNA)	Network Services	Edge Computing	Protect authoritative DNS	Success Offering	Optional benefits (not CF product)

Argo: 3 Components

Smart Routing



Problem

- When edge to origin is cross continent, network congestion, timeout can happen.

Solution

- Argo Smart Routing will find optimal route from edge to the origin.

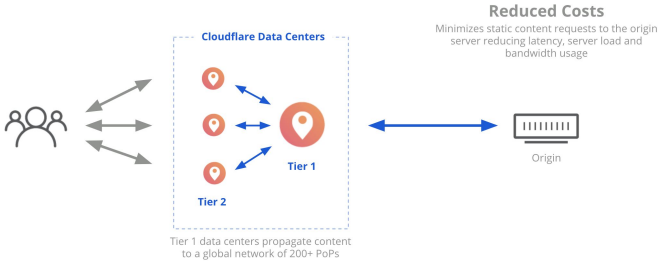
Qualification

- Edge <-> Origin is far
- Notable DYNAMIC contents
- Performance improvement is needed

Can a partner test?

- Yes

Tiered Caching



Problem

- When there's notable static contents and origin bandwidth is limited, customer doesn't want the origin to communicate to 200 data centers.

Solution

- Argo Tiered Caching will assign <40 PoPs or 1 PoP as Tier 1.

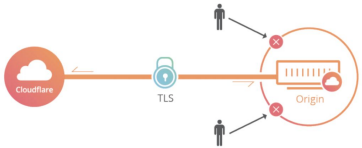
Qualification

- Edge <-> Origin is far
- Notable STATIC contents
- Performance improvement is needed
- Origin bandwidth pipeline is limited

Can a partner test?

- Yes

Tunnel



Problem

- Customer wants to put their private cloud, k8s instance, or RDP apps behind Cloudflare network.

Solution

- Argo Tunnel can help.

Qualification

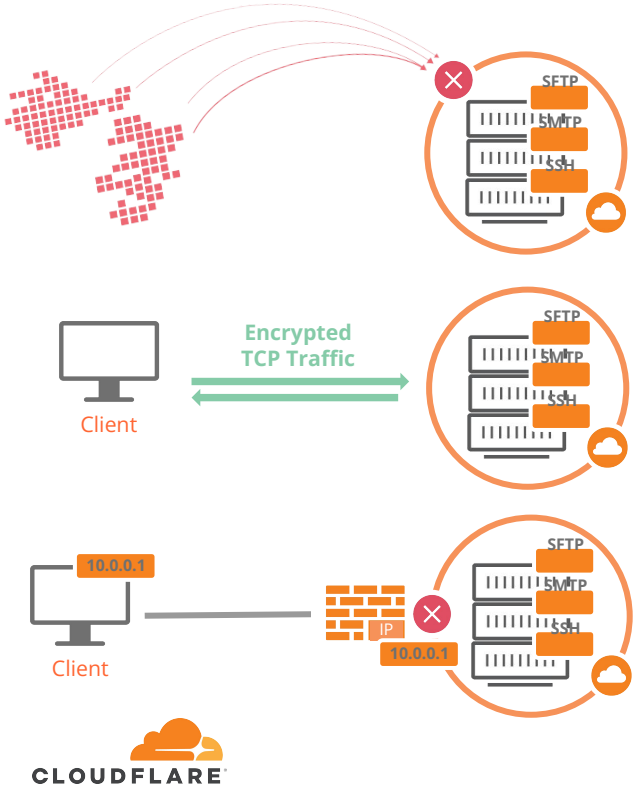
- Origin is private
- Origin needs to lock down
- SSH/RDP Integration with Access for authentication

Can a partner test?

- Yes

Cloudflare Spectrum

Proxy non-HTTP/S TCP traffic through Cloudflare



Problem

When the customer has

- TCP/ UDP applications
- Web applications using custom ports

that they want to protect, It is not proxyable with Cloudflare core product.

Solution

- TCP/UDP applications: Cloudflare Spectrum can **L4 proxy** it and provide DDoS protection without knowing the application protocol.
- Custom port web applications: Cloudflare Spectrum can **L7 proxy** it and provide DDoS/WAF/CDN and all application benefits.

Qualification

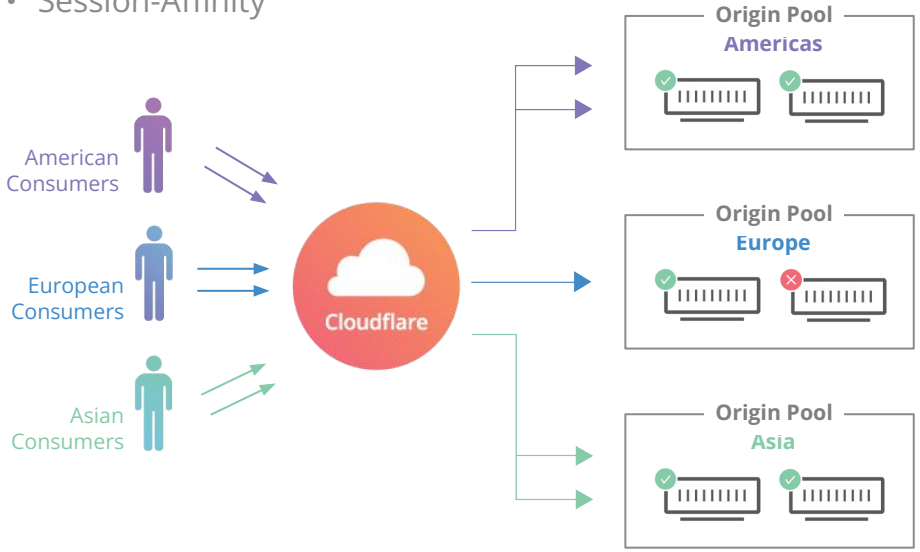
- Customers' non-standard applications and its port
- Domain name that connects to the application
- They want **DDoS protection** vs performance improvement
- Their additional technical requirements

Can a partner test?

- Yes

Cloudflare Load Balancing

- Health checks with fast failover
- Global and local load balancing
- Weight load balancing
- Session-Affinity



Problem

- Customer has multiple origin servers, overutilized or geographically distant servers, etc, with traffic steering requirements.

Solution

- Cloudflare's fully cloud based DNS Load Balancing can help to steer user traffic to available / nearest origin.

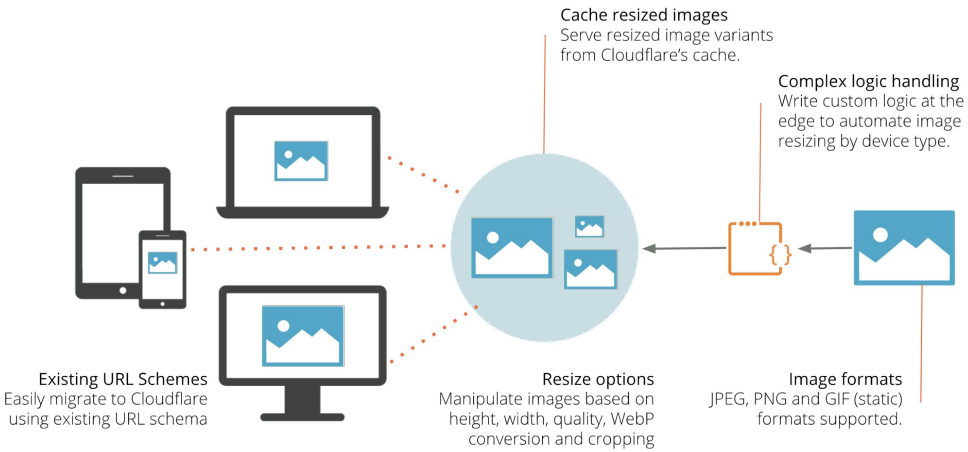
Qualification

- Customer has multiple origin servers
- They have HA requirement
- Number of origin servers and monthly DNS queries

Can a partner test?

- Yes

Image Resizing



Problem

- Resizing every image to handle every possible device geometry consumes valuable time, and it's exceptionally easy to forget to do this resizing altogether.

Solution

- Cloudflare's Image Resizing helps to resize, crop, compress, conversion of the images on the fly.

Qualification

- Lots of image requests
- Currently using resizing, or have resizing requirements per device type, user resolution, network, country etc.

Can a partner test?

- Yes

Payload Inspection

```
// any query string parameter contains "foo"
case-insensitive
any(lower(http.request.uri.args.values[*])[*]
contains "foo")

// any cookie contains "bar" case-insensitive
any(lower(http.request.headers["cookie"][*])[*]
contains "bar")

// check for a substring in the request body if the
request:
// 1) method is POST, PATCH, PUT or;
// 2) Content-Length header value is >0
(http.request.method in {"POST" "PATCH" "PUT"} or
any(http.request.headers["content-length"] ne "0"))
and http.request.body.raw contains "substring
```

Problem

- Customer wants to create custom firewall rules based on the request payload, such as form submission, deny admin login

Solution

- Payload Inspection will work at Firewall Rules engine and customers are able to create any custom rules that could inspect the request body

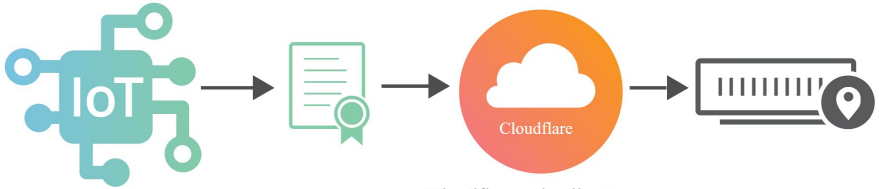
Qualification

- Customers who has related problems
- Customers with lots of security related rules (Firewall Rules) - Payload Inspection could be interesting for them

Can a partner test?

- Yes

Cloudflare Mutual TLS & API Shield



IoT Device uses client certificate to authenticate itself to Cloudflare

Cloudflare only allows devices with certificates signed by device manufacturers root CA

Problem

- Customer needs to authenticate human users, or IoT devices, or services accessing their endpoint using **client certificate**. (mutual TLS, 2-way-SSL)

Solution

- Cloudflare mTLS will provide a way for customers to upload their certificate chain and authenticate clients upon their access request.

Qualification

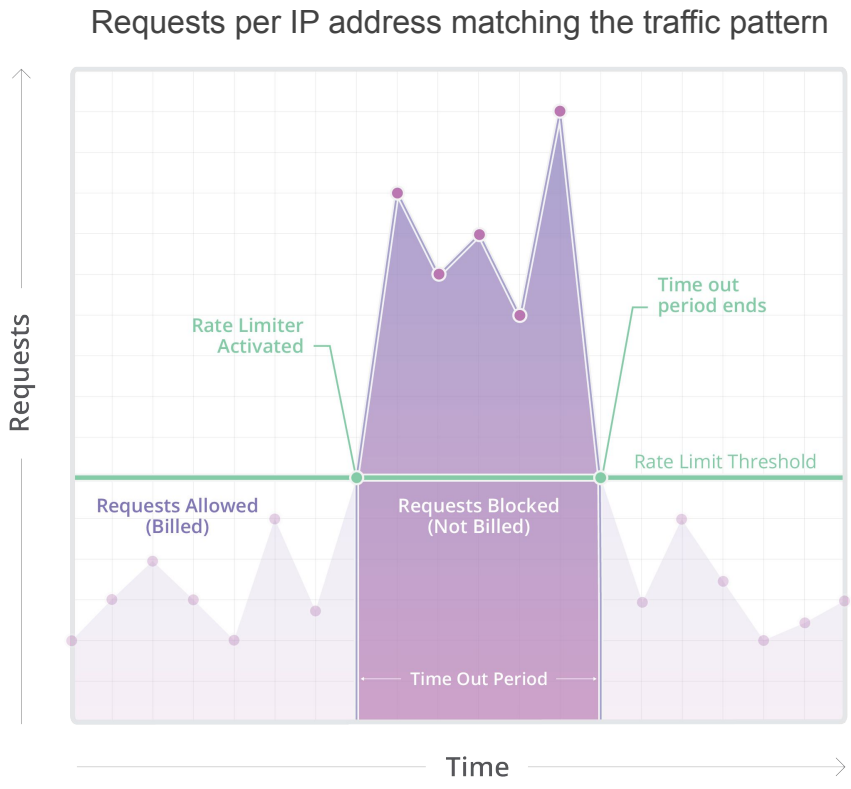
- Customers have endpoints that needs strong authentication (financial, government etc)
- Customers have mTLS in place now, want to have DDoS, WAF, and advanced security benefits to the endpoint

Can a partner test?

- Yes

“API Schema Validation” also there!

Cloudflare Rate Limiting



Problem

- Customers endpoint may overload with too many application requests.
  They need to have a robust way to protect the endpoint and keep the number of request per user to a reasonable level.

Solution

- Cloudflare's Rate Limiting offers a solution for them to limit the number of requests per user (IP, cookies), country, request headers.

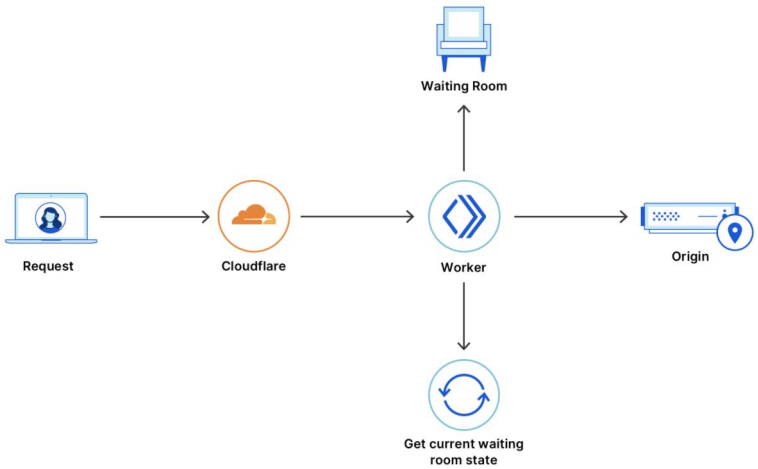
Qualification

- Customer has application DDoS concerns?
- Customer has the sensitive endpoint they need to ensure the availability?

Can a partner test?

- Yes

Cloudflare Waiting Room (Beta)



Problem

- When there are too many visitors, and origin overloads, the customers don't want to lose legit visitors. Instead of **Rate Limiting**, they want **virtual queue** so the visitors wait until the origin is able to serve them.
    - Popular concert ticketing
    - COVID-19 panic buying
    - Limited products, events that everyone loves

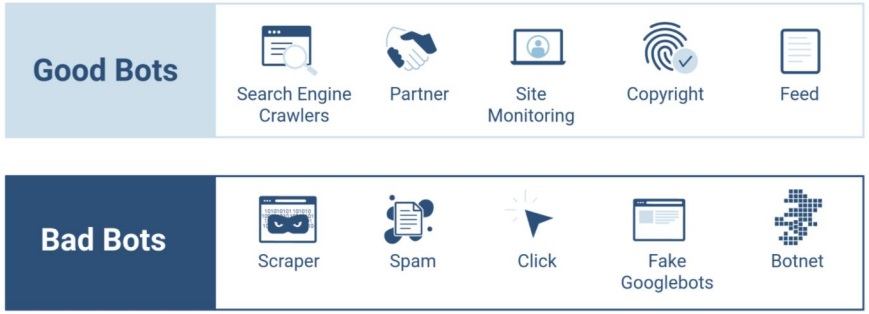
Solution

- Cloudflare Waiting Room will help to limit requests inbound to an application, and places these requests into a virtual queue. Users will know their estimated wait time.

Can a partner test?

- Yes

Bot Management



Problem

- Contents scraping, spamming, fake googlebots, checkout fraud… those bad bot activities are automated, but not necessarily always “malicious” from WAF perspective.

Solution

- Cloudflare Bot Management provides a way to see automated requests to the customer application, then allow good bots, and stop bad bots.

Qualification

- Customers who have described bot problems
  - What problem?
- Customers who have lots of automated traffic
- What endpoint to protect? Web application? Mobile application? Public API endpoint?

Can a partner test?

- Yes

Cloudflare Stream vs Stream Delivery

What is it?

- All in one video solution.
- Customer has a video to serve. Cloudflare takes care of storage; encoding; distribution; player; analytics.

Qualification

- Number of videos & size?
- Average number of views?
- Live streaming is not supported.

Can a partner test?

- Yes

What is it?

- Video CDN solution.
- Customer takes care of storage, encoding, player, DRM. They use Cloudflare CDN to effectively distribute the video.

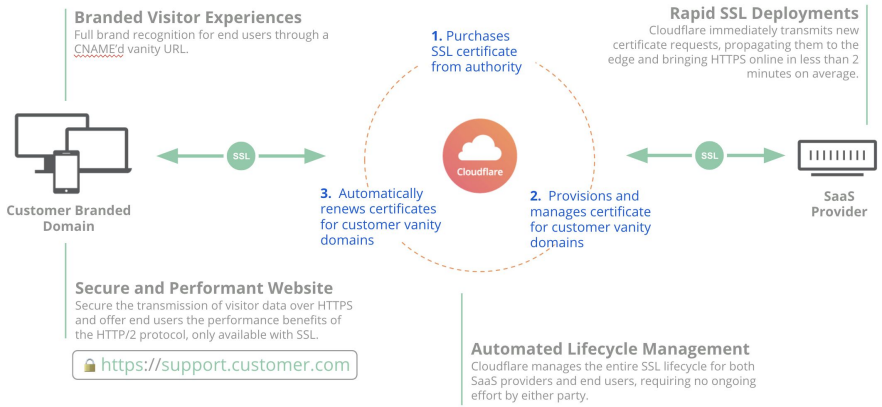
Qualification

- Data transfer?
- Live streaming or on-demand?
- Viewers and origin country?

Can a partner test?

- Yes

Cloudflare SSL for SaaS



CLOUDFLARE Burrito Bot theburritobot.com

Custom Hostname	SSL/TLS certificate status	Expires on	Hostname status	Origin server
s4s.simonwijckmans.com	Active	2021-08-05	Provisioned	Default
s4s.sslworld.cf	Active	2021-06-22	Provisioned	Default
saas.gauravm.cf	Active	2021-09-22	Provisioned	Default
saas.taskstar.org	Active	2021-06-30	Provisioned	Default

CLOUDFLARE

Problem

- SaaS or hosting providers who serve their end customers, they needed to have in-house way to provision HTTPS, security and performance for their customers' domains.

Solution

- Cloudflare SSL for SaaS makes life easier in managing SSL lifecycle
- End customers domains also get Cloudflare security, performance benefit

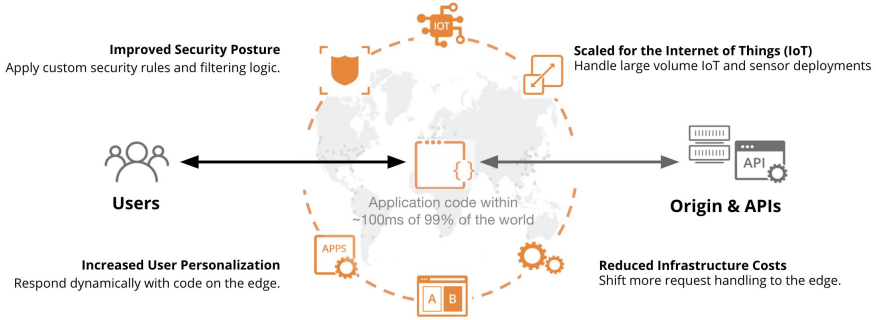
Qualification

- SaaS/hosting providers with "vanity" domains?
- What is their SSL/security/performance challenges today?

Can a partner test?

- Yes

Cloudflare Workers



What is it?

- Customers and partners can write their code at 200+ Cloudflare edge data center to deliver whatever they want.

Use Cases

- Great for granular control of Cloudflare products.
- Great to deploy custom logic, reduce the work at the origin
- Great for migration projects from incumbent provider.

Qualification

- See if the technical requirements is suitable for Workers
- See if the customer org is suitable for Workers
  - Lean, strong developers, who can DIY with Workers?
  - Traditional and large, who need **services partner**?

Can a partner test?

- Yes

Cloudflare Secure Registrar

Problem

- If a current registrar doesn't provide completely secure way to make changes to the upper registries, the customer can be vulnerable to domain hijacking.

Solution

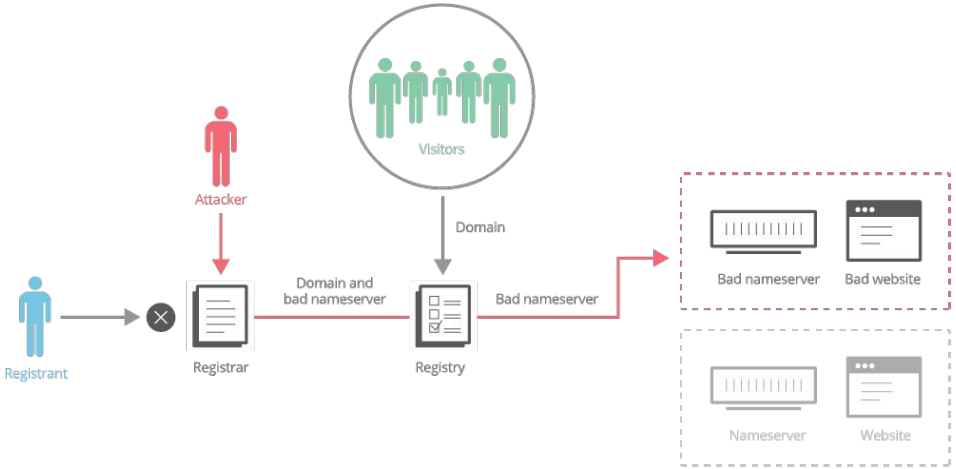
- Cloudflare "Secure Registrar" offers custom domain protection, the highest level of registrar security. Any changes to the domain information should go through customer-defined offline verification.

Qualification

- Is a customer particularly concerned with domain hijacking?
- Customer's trust to their current registrar is low?
- Is a customer premium?

Can a partner test?

- No



DNS Firewall

Cloudflare DNS Firewall

Problem

- Customer has their **authoritative DNS** they are reluctant to change to cloud based Cloudflare DNS, but it is vulnerable to DDoS attack and often slow in region the current infra cannot cover.

Solution

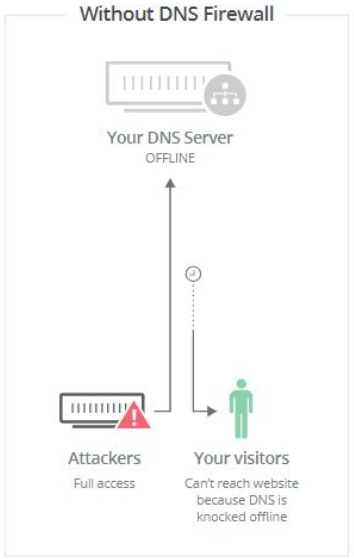
- Cloudflare DNS Firewall will be a CDN for customers DNS.
  - DDoS Protection for DNS
  - Performance Improvement
  - DNSSEC supported

Qualification

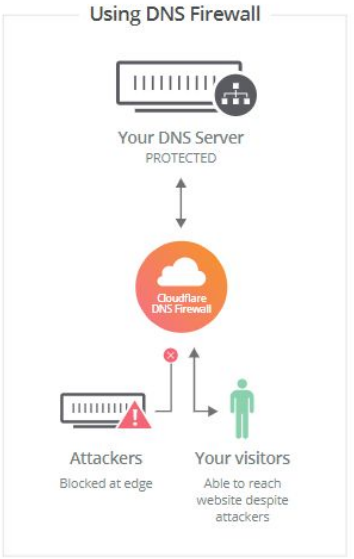
- What is their current DNS and how it is implemented?
- What is the major pain points and technical requirements?

Can a partner test?

- Yes



WITHOUT CLOUDFLARE DNS FIREWALL
The Attacker is able to directly attack your origin DNS server, preventing the visitors from completing DNS lookups.



WITH CLOUDFLARE DNS FIREWALL
Cloudflare DNS Firewall stops the attacker at the edge and keeps your DNS server protected.

Cloudflare Secondary DNS

Problem

- Customer has their **authoritative DNS** they are reluctant to change to cloud based Cloudflare DNS, but it is vulnerable to DDoS attack and often slow in region the current infra cannot cover.

Solution

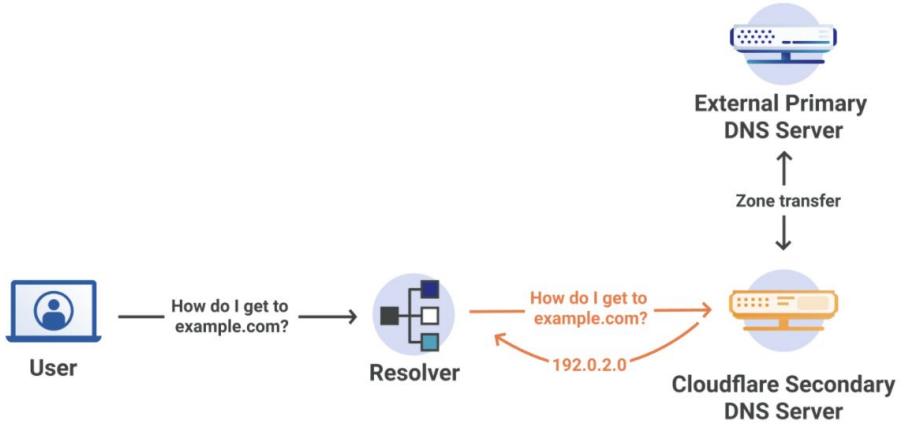
- Cloudflare Secondary DNS in 200+ data centers will be exposed to the internet instead of customers DNS.
    - Zone Transfer from hidden primary DNS
    - Push the record change

Qualification

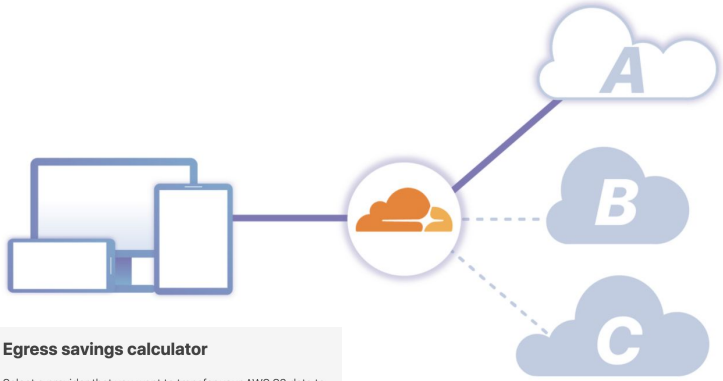
- What is their current DNS and how it is implemented?
- What is the major pain points and technical requirements?

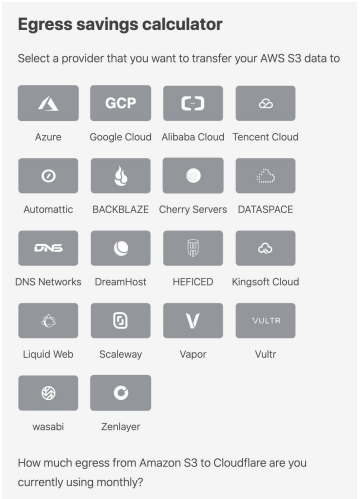
Can a partner test?

- Yes



Bandwidth Alliance





Problem

- Customer's current origin egress bandwidth (i.e. AWS) cost is too high even with Cloudflare fronting the end user traffic.

Solution

- Cloudflare has Bandwidth Alliance program with lots of providers that can **waive** or **discount** the egress fee **to Cloudflare** depending on the current provider.
- Waive/discount is provided by the corresponding partner.

Qualification

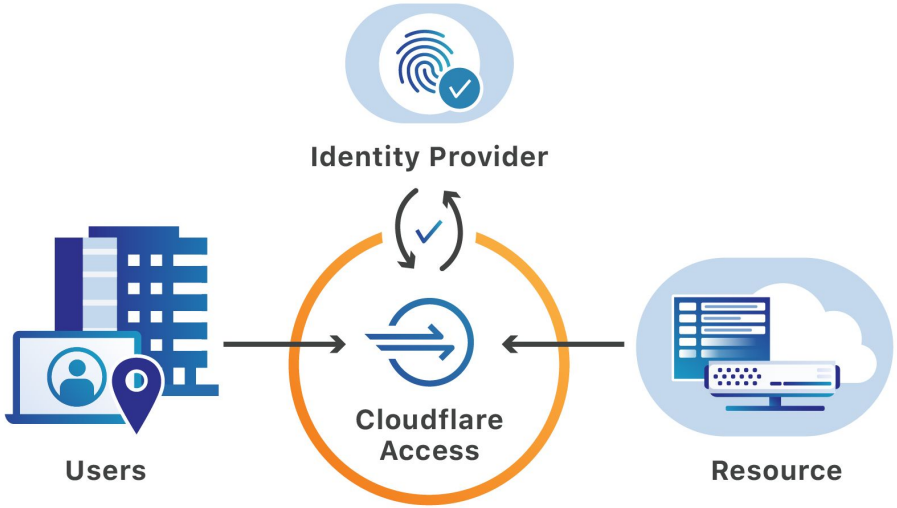
- Current origin provider?
- Current monthly data transfer (GB, TB, PB)?
- Which to-be provider they're interested in?

Can a partner test?

- No

Cloudflare Access

Zero Trust Security Solution



Problem

- Everyone's working remotely in 2021.
- VPN is slow. It has poor user experience. It drills a hole at the corp network. It becomes vulnerability itself. It doesn't help with digital transformation, etc.
- Customers need **zero trust network access** solution with great visibility.

Solution

- Cloudflare Access provides zero trust solution and it helps to consolidate user experience and admin complexity.

Qualification

- What corp application - web, rdp, ssh? Where are they located?
- What IdP customer is using, can it be integrated?
- How many users? Where are they located?
- The other technical/policy requirements?

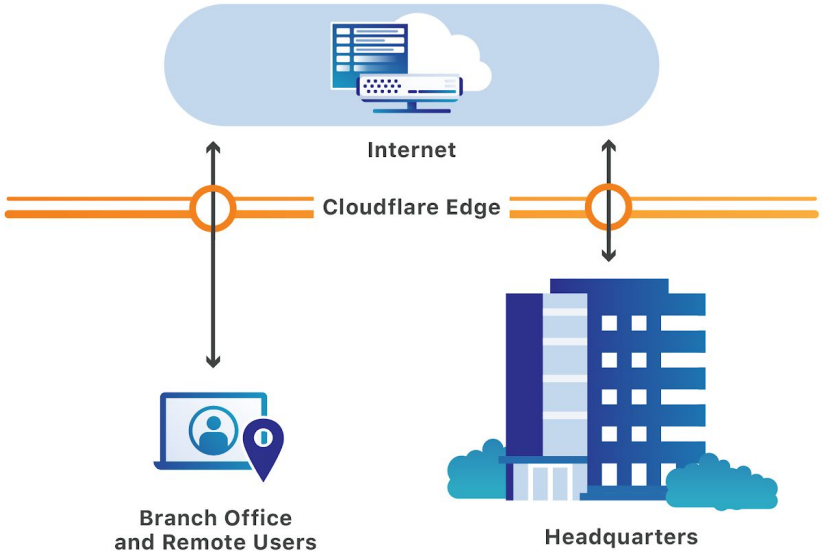
Can a partner test?

- Yes

CLOUDFLARE

Cloudflare Gateway

Secure Web Gateway Solution



Problem

- Everyone's working remotely in 2021.
- Devices can be compromised. Employees may access undesired websites and attacked by ransomwares.
- Customers need **secure web gateway** solution that can log, inspect, secure traffic from remote corporate devices.

Solution

- Cloudflare Gateway provides secure web gateway with DNS/HTTP filtering, and great visibility.

Qualification

- How many users? Where are they located?
- Users OS? (Mac OS, Windows, iOS, Android, Linux supported)
- The other technical/policy requirements?

Can a partner test?

- Yes

CLOUDFLARE

Cloudflare Remote Browser Isolation

The fastest and safest browsing experience is the Cloudflare Browser running in the cloud on our network.

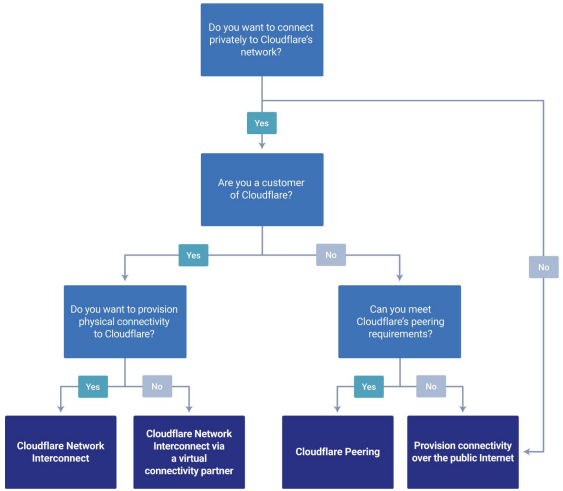
WHAT Release globally to all PoPs; sandbox browsing experience

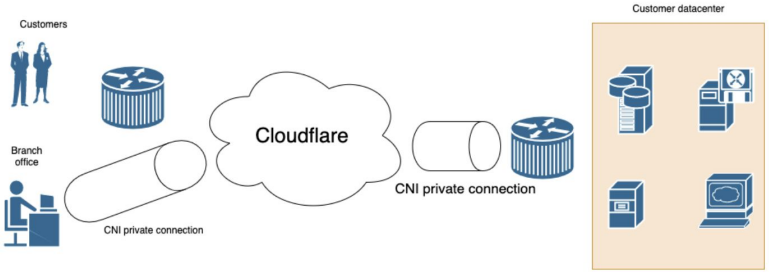
WHY Stop zero-day threats on the Internet without slowing down users.

HOW https://developers.cloudflare.com/browser-isolation/

TEST? Yes!

Cloudflare Network Interconnect





What is it?

- Physically connect customer data center directly to nearest Cloudflare data center for a more reliable and secure experience than connecting over the public Internet

Qualification

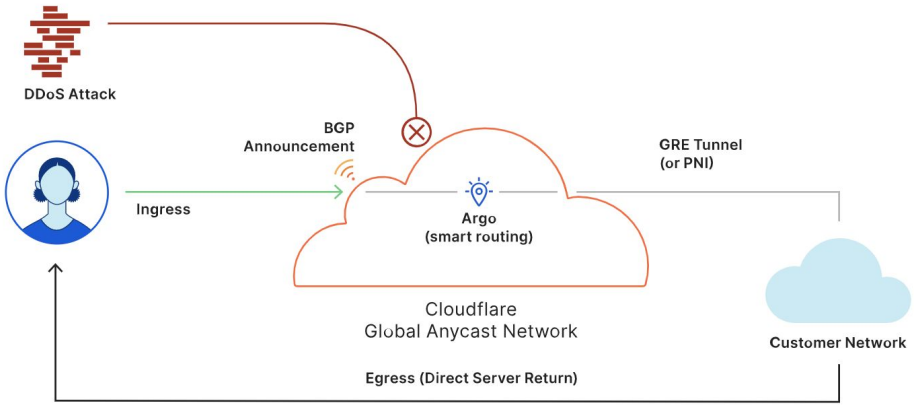
- Have an on-prem network? (/24 IP prefix and ASN)
- Is a Cloudflare Enterprise customer?
- Where are they located today?

Can a partner test?

- No

DIGITAL REALTY
CORESITE
EQUINIX
BBIX
consoleconnect
edgeconnex
Megaport
Netrality Data Centers
packetfabric
TERACO
zayo
365 DataCenters

Magic Transit



Problem

- In 2021, customer's on-prem networks is moving to hybrid architecture. They need **better cloud-based protection** that serves them the best, versus the legacy appliances, or point cloud solutions.

Solution

- Cloudflare Magic Transit supports your digital transformation perfectly, with great cost efficiency.

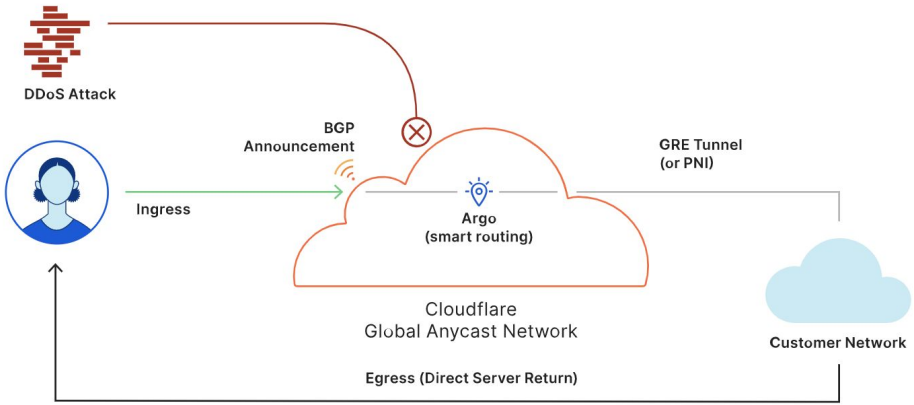
Qualification

- Customer has on-prem network?
  - IP prefix bigger than /24
  - ASN
- On-demand or always-on?
- How many prefixes, how many physical locations?
- Current bandwidth (circuit size) at each of the locations?
- What is current MTU? What is current routing hardware?
- The other technical requirements

Can a partner test?

- No

Magic Firewall



What is it?

- L4 Firewall-as-a-service.
- Your on-prem L4 Firewall can be removed now.
- Cloudflare Magic Firewall allows you to control inbound traffic/port and rate limit as you like.

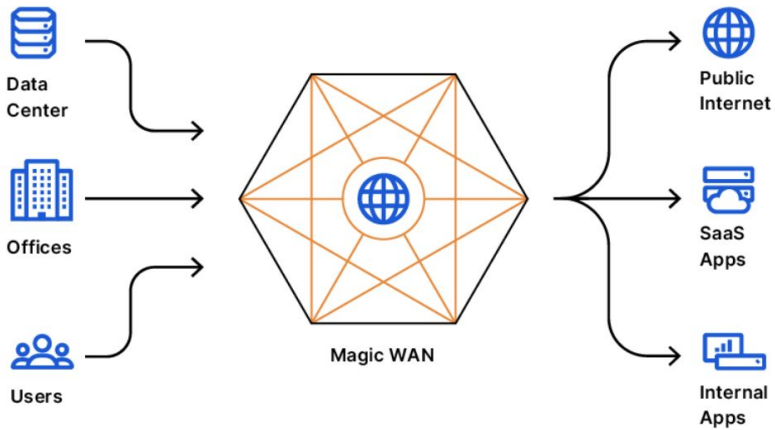
Qualification

- Magic Transit

Can a partner test?

- No

Magic WAN



What is it?

- MPLS-as-a-service.
- Your on-prem L4 Load Balancer can be removed now.
- Connect your branch offices, remote users, data centers to the edge and control traffic steering.

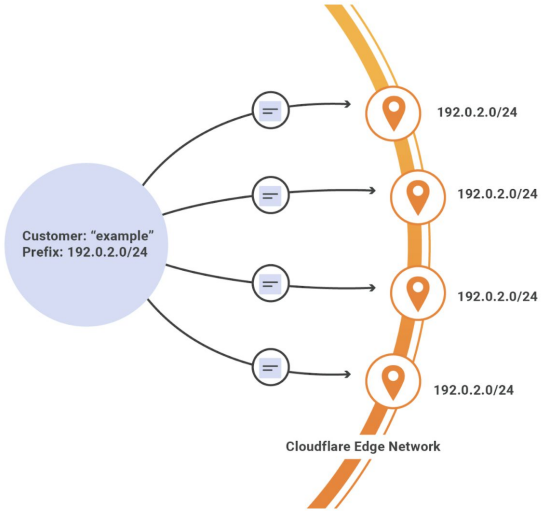
Qualification

- Magic Transit

Can a partner test?

- No

BYOIP



What is it?

- The Cloudflare edge will announce a customer's own IP prefixes and the prefixes can be used with our Layer 7 services, Spectrum, or Magic Transit.

Qualification

- Customer has on-prem network?
  - IP prefix bigger than /24
- What Cloudflare services the customer wants to use with BYOIP?
- The other technical requirements

Can a partner test?

- No

Cloudflare Premium Success

Success Offering Features

Premium Offering available for annual contract value below $100,000.

	Standard	Premium
Onboarding		
Access To Enterprise Customer Portal	✓	✓
Customer Success Led Onboarding Assistance	✓	✓
Designated Customer Success Manager	✓	✓
Guided Onboarding Experience		✓
Expert Tuning Workshop		✓
Optimized Experience		
Annual Health Check	✓	✓
Monthly Operational Review [email]	✓	✓
Periodic Executive Business Review		✓
Technical Support		
Access To Support Community	✓	✓
24/7 Email And Chat Support	✓	✓
Emergency Phone Support Hotline	✓	✓
Under Attack Support Engineer For Magic Transit		✓
Prioritized Case Handling		✓
Availability SLA Credit	10x Credit	25x Credit
Technical Support Response SLA		
P1 - Urgent	<2 Hr	<1 Hr
P2 - High	<4 Hr	<2 Hr
P3 - Normal	<48 Hr	<24 Hr
P4 - Low	<48 Hr	<24 Hr
Training/Education		
Access To Online Documentation	✓	✓
Access To Online Training Workshops	✓	✓
Use Case Optimization Workshops		✓
Customized Training Workshops		✓
Reporting		
Cache Analytics Insights	✓	✓
Health Check Analytics Insights	✓	✓

What is it?

- Customer Success Offering that tells the Cloudflare team's engagement level with the customer.
    - Key difference: Standard Success does not include **Onboarding**. Partners have to take care of customer onboarding without CF team.
    - Cost difference: approximately 20%

Simple Thinking Suggestion

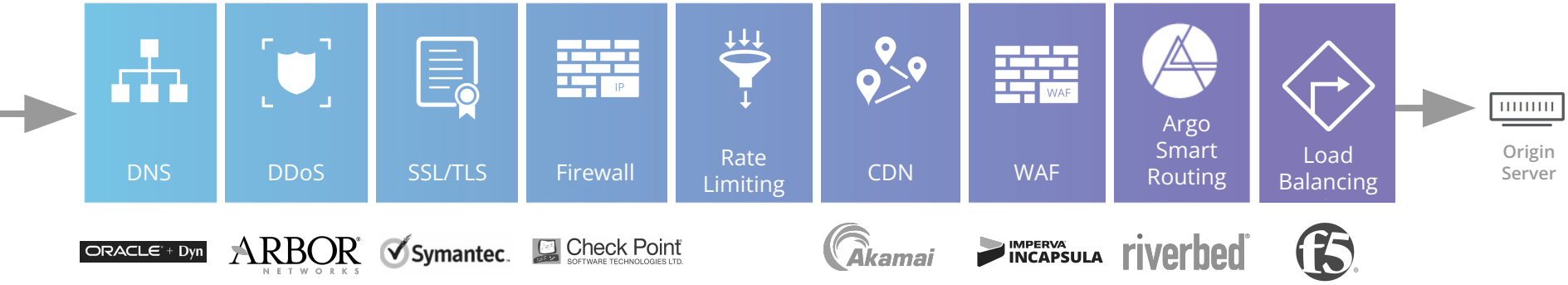
- High-touch customer? -> Premium Success
- Non-testable product? -> Premium Success
- You (as a partner) are confident? -> Standard Success

What sets Cloudflare One apart?

Capability	Cloudflare	Legacy appliances	Point cloud security solutions
Performance			
Global network spanning 200 cities and 100+ countries w/ DDoS mitigation capacity of 59 Tbps	✓	✗	✗
World's fastest public DNS resolver	✓	✗	✗
Ease of use			
Single pass traffic inspection with one code base	✓	✗	✗
Self-service dashboard	✓	✗	✗
One powerful management plane for network and security services	✓	✗	✗
Security			
Threat intelligence harnessed from over 25M Internet properties	✓	✗	✗
Comprehensive firewall-as-a-service across L3/4/7	✓	✗	✗

An integrated solution with lower TCO

Each Cloudflare Point of Presence runs an integrated stack of easy-to-use security, performance and reliability services



CUSTOMER STORIES

Customers benefit from integrated security, performance, and reliability

HubSpot

35% performance improvement

SoFi

60% reduction in malicious traffic

LogMeIn

41k WAF blocks per month

AutoTrader

50% acceleration in DNS performance

leCab

900k login attempts blocked in 2 hours

ypo

50% decrease in page load times

Customers realized lower TCO with Cloudflare

AutoTrader

75% savings in Egress costs

Quizlet

50% savings in GCP & Network Egress bill

DISCORD

$200k in annual savings from hardware & bandwidth costs

buzzlie

96% savings in AWS bandwidth bill

CLOUDFLARE

Customer use case #1

Pain point: DDoS attack for websites & DNS (Industry: Government)

Key Win

- Strong cloud network
- Self-serviceability
- Partner's MSSP

Solution Design:

Managed Authoritative DNS ✓	Managed SSL ✓	Unmetered DDoS ✓	WAF ✓	Firewall Rules ✓	IP Reputation Intelligence ✓	Optimization ✓	CDN ✓	Analytics & Logpush ✓
Argo ✓	Rate Limiting ✓	Spectrum ✓	Load Balancing ✓	Bot Management	Stream Delivery	Payload Inspection	Image Resizing	API Shield
SSL for SaaS ✓	Waiting Room	Mutual TLS	China Network	Stream			DNS Firewall ✓	Secondary DNS
Access	Gateway (SWG, Warp) DNS Recursive	Remote Browser Isolation						Premium Success ✓
Magic Transit	Magic WAN	Magic Firewall					Cloudflare Network Interconnect	Bandwidth Alliance
Workers	Workers KV							

CLOUDFLARE

Customer use case #2

Pain point: Contents distribution, bot attack
(Industry: SaaS e-commerce business)

Solution Design:

Managed Authoritative DNS ✓	Managed SSL ✓	Unmetered DDoS ✓	WAF ✓	Firewall Rules ✓	IP Reputation Intelligence ✓	Optimization ✓	CDN ✓	Analytics & Logpush ✓
Argo ✓	Rate Limiting ✓	Spectrum	Load Balancing	Bot Management ✓	Stream Delivery	Payload Inspection	Image Resizing	API Shield
SSL for SaaS	Waiting Room	Mutual TLS	China Network	Stream			DNS Firewall	Secondary DNS
Access	Gateway (SWG, Warp) DNS Recursive	Remote Browser Isolation						Premium Success ✓
Magic Transit	Magic WAN	Magic Firewall					Cloudflare Network Interconnect	Bandwidth Alliance
Workers	Workers KV							

Key Win

- Intuitive solution
- Real-time propagation
- Competitive global performance & SEO

CLOUDFLARE

Customer use case #3

Pain point: DDoS / Comprehensive security (Industry: Banking)

Solution Design:

Managed Authoritative DNS ✓	Managed SSL ✓	Unmetered DDoS ✓	WAF ✓	Firewall Rules ✓	IP Reputation Intelligence ✓	Optimization ✓	CDN ✓	Analytics & Logpush ✓
Argo ✓	Rate Limiting ✓	Spectrum	Load Balancing ✓	Bot Management	Stream Delivery	Payload Inspection ✓	Image Resizing	API Shield
SSL for SaaS ✓	Waiting Room	Mutual TLS	China Network ✓	Stream			DNS Firewall	Secondary DNS
Access	Gateway (SWG, Warp) DNS Recursive	Remote Browser Isolation						Premium Success ✓
Magic Transit ✓	Magic WAN	Magic Firewall ✓					Cloudflare Network Interconnect	Bandwidth Alliance
Workers ✓	Workers KV ✓							

Key Win

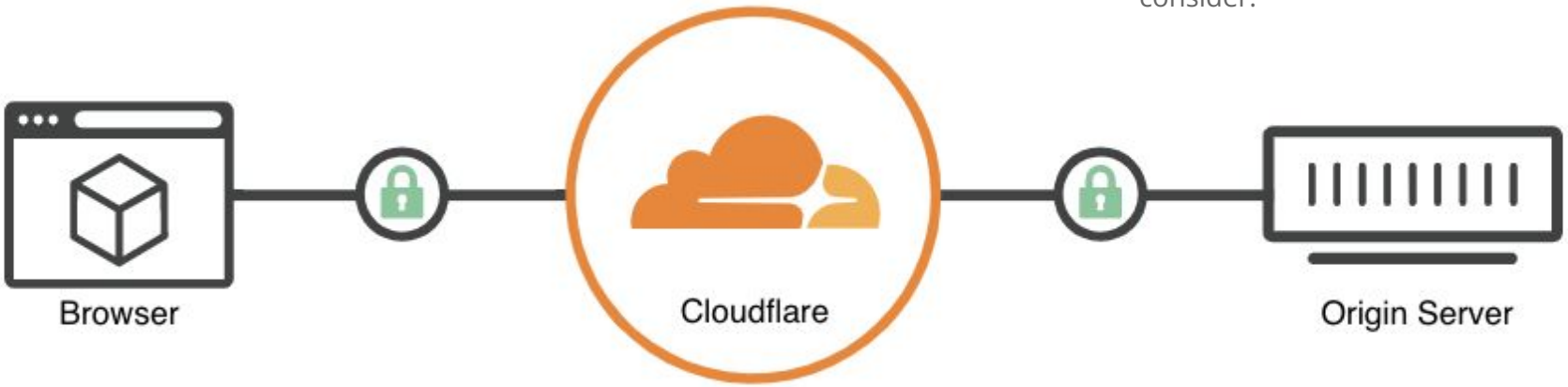
- Continuous Innovation
- Partner's MSSP/PS/Workers
- Lower total TCO

CLOUDFLARE

CUSTOMER ONBOARDING STEPS

Anycast & Reverse Proxy

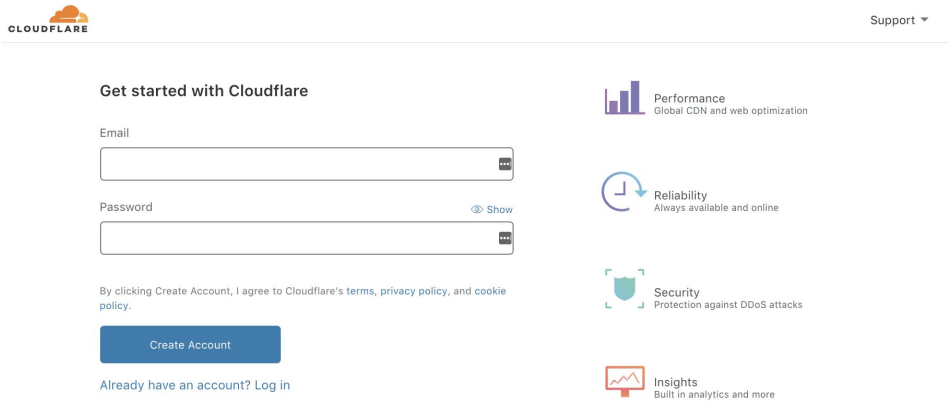
1. DNS change to initiate reverse proxy
2. The closest POP from the visitor responds to the request based on anycast
3. Full stack implementation on all POPs.
4. Origin talks to Cloudflare POPs, not directly to clients
5. There're 2 HTTPS connections to consider.



Step 1: Account creation

Creating an account with Cloudflare is easy. To get started, just fill out your email address and create a password.

For additional assistance, see our step by step guide.

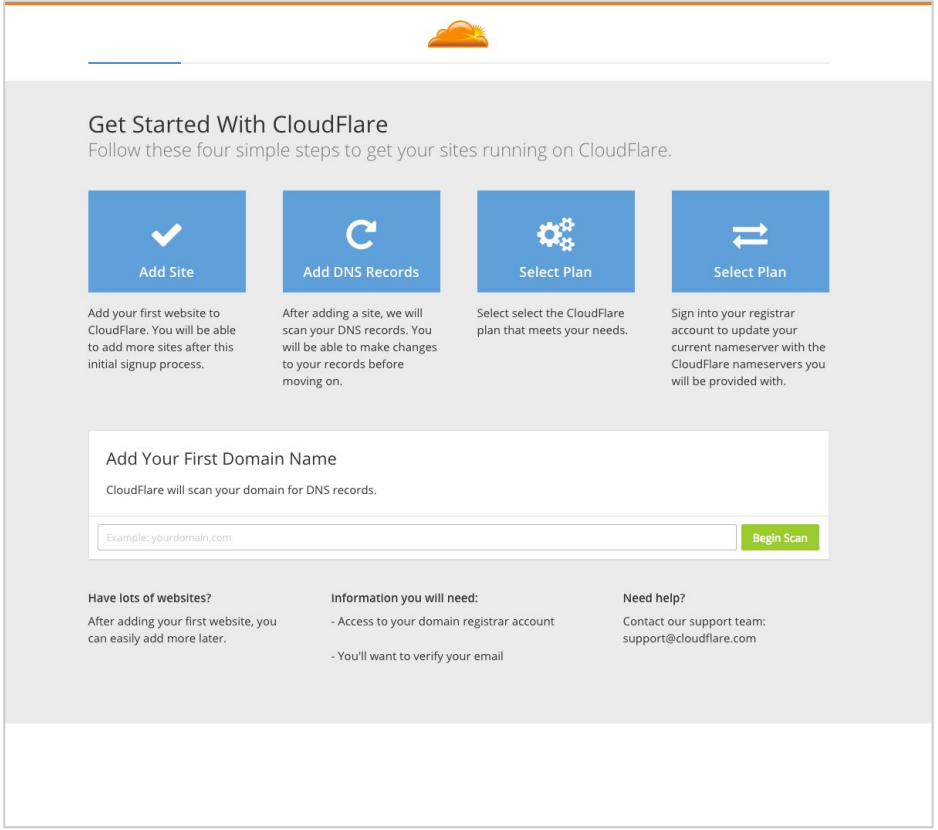


Step 2: Add your first website

After adding your first website, we then scan your DNS records.

You may still need to add additional records or we recommend uploading a zone file.

Cloudflare will accept zone files in BIND format for ease of domain transfer.



CLOUDFLARE

Step 3: Configuring DNS

There are two ways to connect to Cloudflare:

Full (How-To Full)

Cloudflare's robust, global and fast DNS becomes your authoritative DNS provider.

Pros:

- Cloudflare protects the apex domain.
- Leverages Cloudflare's network for DNS which is very fast, highly available, and resilient to DNS based attacks.

Cons:

- Changing the authoritative provider is not always possible for organizations.

CNAME (How-To CNAME)

You keep your primary DNS provider and link individual subdomains to Cloudflare.

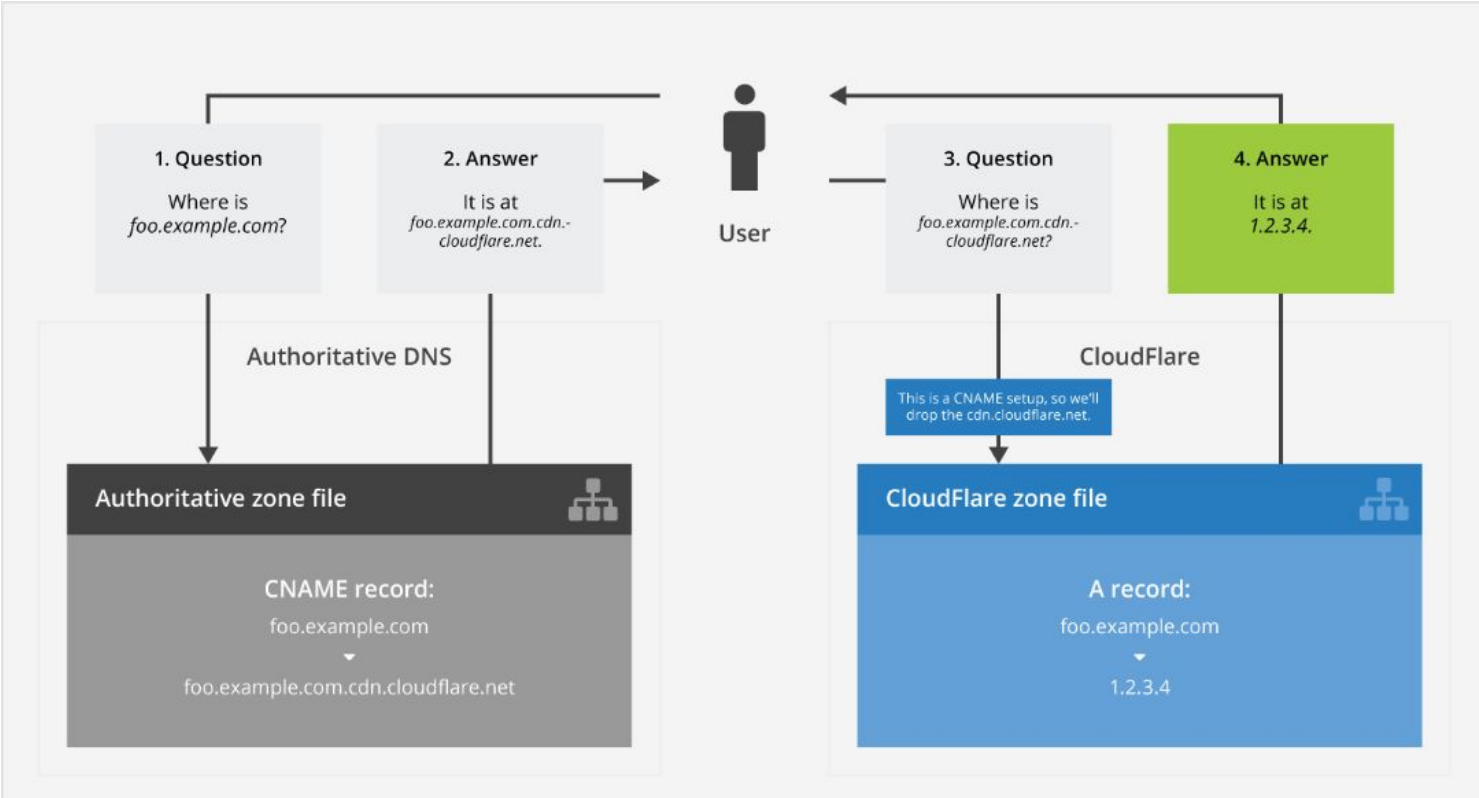
Pros:

- Requires limited change and allows only a single subdomain to be sent through Cloudflare.

Cons:

- We cannot protect your apex domain
- An attacker may overwhelm your authoritative DNS provider which will cause all DNS functions to fail including the CNAME to Cloudflare.

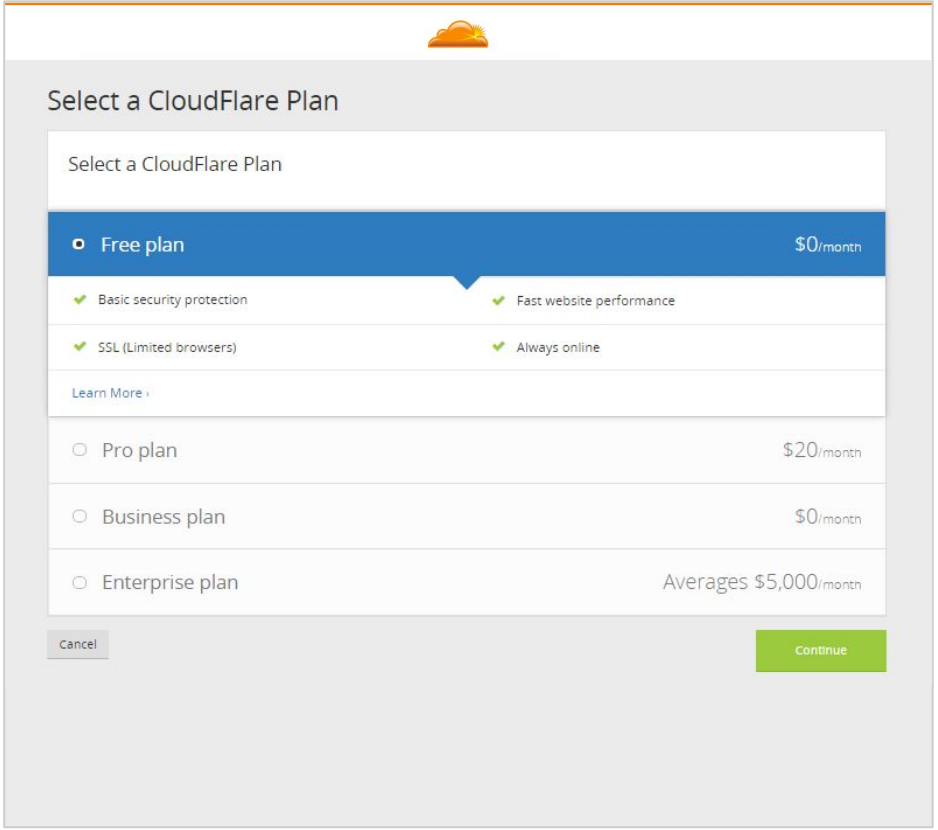
Understanding CNAME Setup



Step 4: Select Cloudflare Plan

Choose the free plan for now, and you will be upgraded to Enterprise by your dedicated team.

Or, if you were given an Enterprise license, you can use that now.

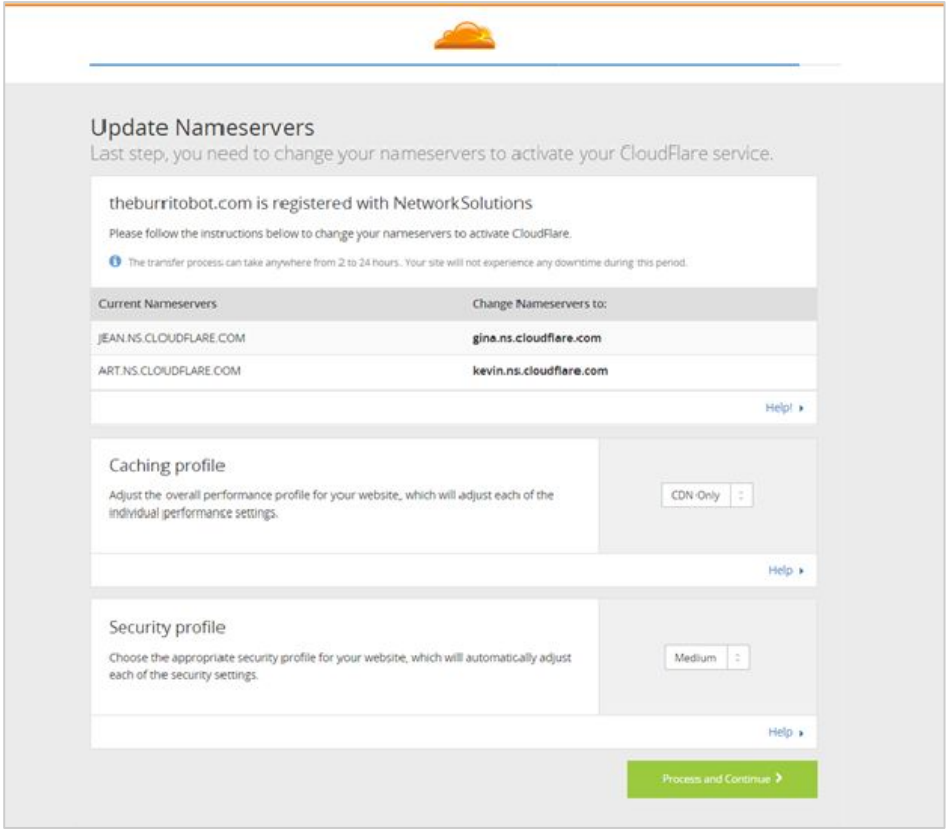


CLOUDFLARE

Step 4: Initial Settings

You'll be asked to either update your nameservers or add a TXT record depending on your DNS decision.

Next, you can leave your settings as the default. Your dedicated team can tune your website to fit your performance and security needs.



CLOUDFLARE

Step 4 : Cloudflare Account Activation

Once you choose how to setup your account, you can follow below steps:

Full Setup

1. Make sure you have all DNS records uploaded at Cloudflare DNS.
2. Put all records as Grey-cloud.
3. At your registrar, change your nameservers pair to Cloudflare nameservers. Find step-by-step guide here.
4. Check if new NS records are well propagated, e.g. http://dnschecker.org
5. After we detect new NS records being set to CF nameservers, your Cloudflare account will be activated.

Grey-cloud — Inactive Proxy

Record resolves to the configured IP address. Non-HTTP(s) traffic should be grey-clouded.

CNAME Setup

1. Don't change nameservers.
2. After your account team changes account setting to CNAME setup, you can find TXT record in the dashboard. (e.g. 856172357-3825555).
3. Add the TXT record in the authoritative DNS. Cloudflare-verify.*example.com* (replace example.com).
4. Once Cloudflare detects the TXT record well set, your Cloudflare account will be activated. (it may take few hours.)
5. At Cloudflare dashboard DNS app, you can add hosts and origin addresses which you would like to delegate to Cloudflare.

Step 5: Configuring SSL

Select how your traffic is encrypted.

Upload custom SSL certificates

You can upload a custom SSL certificate to Cloudflare

- Fastest and most common
- Cloudflare presents your existing certificate to your users
- Keys are never stored on-disc, only decrypted on demand
- Using your own certificate can allow you to go live immediately (You can always migrate later).

Cloudflare issued SSL certificate

Cloudflare will provide a certificate from our our CA partners.

- Valid for *.example.com and the root (example.com)
- *.*.example.com (subdomain of subdomain) **not** supported
- Ownership of your domain must be verified by our CA Partner. How to verify manually

Step 6: Prepare your origin network

Preparing your network

- Configure firewalls to prevent access to your servers, load balancers, and other infrastructure from non-Cloudflare IP addresses
    - This means allowlisting Cloudflare IPs in your Access Control List to prevent rate-limiting or false positives from any intrusion detection systems.
- Prevents attackers from recording/recognizing the “fingerprints” of your hardware when probing your IPs

Set up Cloudflare Standalone Health Checks

- At Cloudflare dashboard, set up Cloudflare standalone health checks to verify the origin server responds to Cloudflare data center’s HTTP(S)/TCP requests.
- You can find it at Traffic/Health Checks. Select the relevant region as per the business requirement.
- Proceed to the next step only after the health checks are marked as Healthy .

Step 6: Prepare your origin network

Review HTTP headers and cookies added by Cloudflare

- Cloudflare passes all HTTP headers as-is from the client to the origin and adds additional headers as specified here. Review the headers and make sure the origin server will work as expected.
- Cloudflare uses HTTP cookies to maximize network resources, manage traffic, and protect our Customers' sites from malicious traffic and the details are described here. Review the cookies and make sure the origin server will work as expected.
- Whenever in doubt, run a local/staging test at the step 7 and verify there's no problem.

Restoring original user IP addresses (optional)

- HTTP requests will be coming from Cloudflare, instead of the actual users. Cloudflare adds "CF-Connecting-IP" and standard "X-Forwarded-For" headers to all request
- Nginx, Apache, and IIS configs to switch the logged IP are available.
- You can find out how to easily restore the originating IP address here!

Step 7: Staging

Local testing

HTTP(s) and Websocket traffic can be pushed through Cloudflare from your local machine by altering your host file with a valid Cloudflare IP. (How to alter your host file).

Development domain testing

A stand-alone development domain is recommended to allow testing before moving production traffic through Cloudflare.

Subdomain Testing

A development subdomain works as well. It is also possible to CNAME a subdomain to your production traffic if your server is configured to properly handle a different host header.

Orange-cloud — Active proxy

Record resolves to Cloudflare IP address for HTTP(s) and Websocket traffic.

Grey-cloud — Inactive Proxy

Record resolves to the configured IP address. Non-HTTP(s) traffic should be grey-clouded

How to test locally with a Hosts file

1. Open your Host File
   a. Windows (As Admin): C:\Windows\System32\Drivers\etc\hosts
   b. OSX: /private/etc/hosts

2. Put in a Valid Cloudflare IP Address for your domain or subdomain

3. You may need to flush the OS DNS Cache
   a. Windows: ipconfig /flushdns
   b. OSX: How to Flush OSX DNS
4. You may need to flush the browser DNS Cache:
   a. Chrome: In Chrome URL bar type:
      chrome://net-internals/#dns
   b. Safari: From Safari Menu Select: Safari > Empty Cache.
5. Use curl to confirm Cloudflare headers and traversal
   a. curl -s -D - www.example.com -o /dev/null

6. Visit your website to confirm using your browser.

Cloudflare IP addresses:
The Cloudflare IP address must be valid for the domain/zone being tested. They can be found by testing the DNS resolution for any orange-clouded DNS record in the domain, or by a Cloudflare employee.

```
##
# Host Database
##
127.0.0.1       localhost
...
198.41.209.86         example.com
198.41.209.86         www.example.com
198.41.209.86         secure.example.com
```

CLOUDFLARE

Step 8 : Push traffic - Full Setup

Once you've finished til step 7, we can push traffic via Cloudflare proxy.

Full Setup Onboarding

1. At Cloudflare DNS, change the host to orange-cloud.
2. Once changed to orange-cloud, the host is accelerated and protected by Cloudflare.

Orange-cloud — Active proxy

Record resolves to Cloudflare IP address for HTTP(s) and Websocket traffic.

Step 8 : Push traffic - CNAME Setup

Host delegation, CNAME Setup Onboarding

1. At Cloudflare DNS, configure the origin address and turn on orange-cloud.

   www.example.com A 1.2.3.4 (origin) 

2. At your authoritative DNS, add a CNAME record as following.

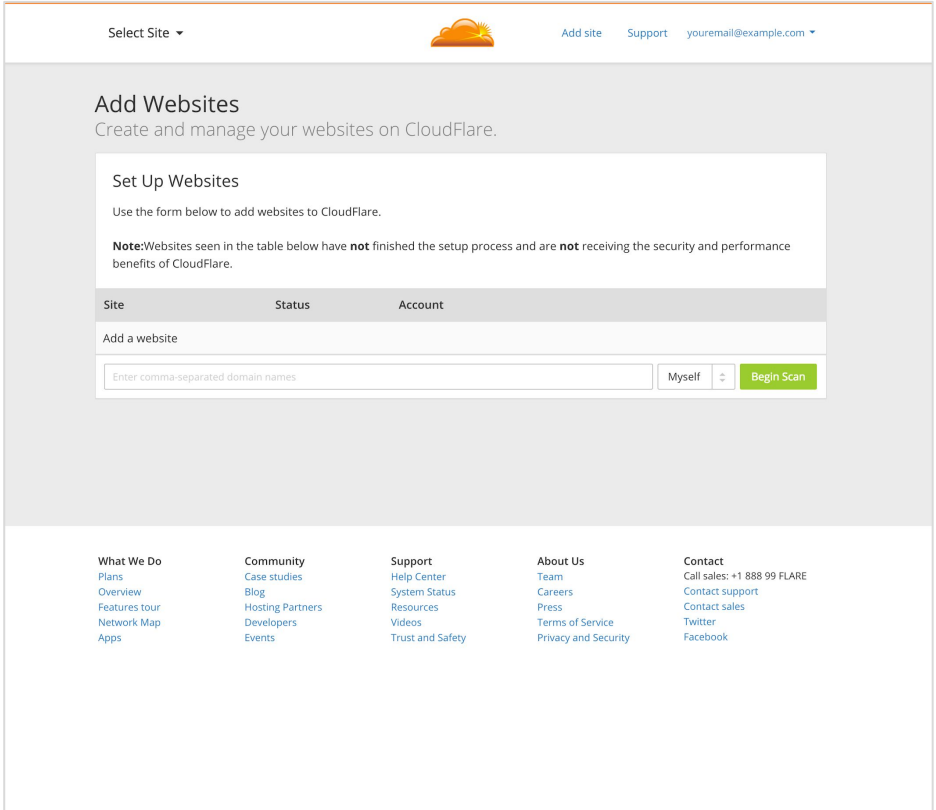
   www.example.com CNAME www.example.com.cdn.cloudflare.net

3. Once new DNS record is propagated, the host is accelerated and protected by Cloudflare.

Setup complete!

At this point you should have your account and website up and running. You should be aware of how to test it effectively and safely.

If you have more domains, they can be added easily by following the steps again for each zone. You can also add multiple zones into Cloudflare at the same time by separating them with a comma on the add a site page or using our API.



CLOUDFLARE

SIZING + DISCOVERY

Product Sizing - Application Services

1. Number of requests /month
2. Data transfer (egress) /month
3. Number of domains (TLD only)

- Add-on products have additional criteria

CLOUDFLARE

DNS (Authoritative DNS, DNS Firewall, Secondary DNS)

- Who is your current DNS provider? (*SE can look up with domain)
- What is your current registrar with which you have registered your domain?
- What would be the primary pain with your existing provider?
    - Have you ever experienced availability problem with your DNS?
    - How satisfied are you with your current DNS resolution speed? Would you be interested in accelerating it further from any location of the world?
    - Do you have DNSSEC implemented today? If it's going to be easy to deploy, would you be interested in having additional DNS security?
- (If their existing DNS is on-prem) Is it possible to consider moving your DNS to fully cloud based managed DNS?
- (If the answer is no) Do you have enough DDoS protection and DNS security for your on-prem DNS?

CLOUDFLARE

SSL/TLS

- How many domains do you manage the SSL certificates?
- How does your current SSL management cycle look like today?
    - Would you be interested in easing the SSL management with managed SSL?
- Do you have any specific requirements for your SSL certificates, or are you ok with a recommended most secure way? (i.e. specific CA, specific cipher suites, cryptography algorithm, "EV")
- Do you have any 3rd party customer domains that you need to secure/proxy traffic through your site? ⇒ SSL for SaaS
- Is server side certificate sufficient? Does your application require client certificates to be presented? ⇒ API Shield/Mutual TLS
- (Don't ask first, but if the customer asks) Do you have a data sovereignty concern about having out-of-country data centers being able to inspect your application traffic with the private key? ⇒ Regional Services, Spectrum, or Keyless SSL

CLOUDFLARE

DDoS / Rate Limiting

- Have you ever experienced DDoS attack? Do you have concerns about DDoS?
- Are your concerned applications web-based? Or are they non-web-based, web with non-standard ports, or a whole IP network? How do you currently protect them?
  ⇒ Possibly Spectrum
  ⇒ Possibly Magic Transit
- Have you ever experienced an escalated bandwidth bill after a DDoS attack and your traffic usage went above your agreed bandwidth cap?
- Do you have particular peak time at your application? How often your origin server's CPU goes busy at the peak time?
- If your origin server gets overwhelmed, what would happen? Would the origin server just go unavailable? Or do you have an auto-scaling backend? If auto-scaling, how do you control and limit the cost that could be caused by non-legitimate increased requests?
- How do you get visibility into the normal user vs heavy actors with a lot of requests which could potentially be abusing your application
- If you don't have visibility, would your security team be benefited by getting real-time visibility?
- How do you penalize the heavy actors while not disrupting the normal users experience?
- Would you like to have a way to protect the origin server from being overloaded by too many visitors?
  ⇒ Possibly Bot M
  ⇒ Possibly Waiting Room

CLOUDFLARE

WAF

- Are you running any hardware for web application firewall, or DDoS mitigation?
- Has your site ever being compromised?
- Do you ever worry about site security or hackers compromising your site?
- Do you currently have/worry about bots attacking your site?
- Do you currently have detailed real-time visibility to the security events?
- How does the process look like in your organization when you need to provision a new security rule? Does your team own that, or is there a separate security team?
    - How often do you update your WAF? Do you need an update to be protected against a newly discovered attack vector?
    - How easy is it to create new security rules to address the threat that are unique to your business?
    - How important is it for your team to spend less time in managing the WAF/business specific security rules?

Caching

- How do you distribute the contents today?
- Do you have any concern about the current way?
    - Is performance good enough? Any cost concern? Lack of security?
- Do you only need a pure caching service? How do you secure the contents of the website? How does your current CDN provider provide security capabilities? Are you using a separate 3-party vendor for the security portion?
- Where are your clients/users mainly located?
- Where is your origin server located?
    - On-prem:
        Where is it physical located?
        Who is your ISP?
        How are you being charged by the ISP?
        Does your ISP charge overage for international bandwidth?
        ⇒ Possibly Argo Tiered Caching - Custom topology
        ⇒ Check the direct peering
    - Cloud:
        Who's the provider?
        Where's the location?
        How does the monthly bandwidth bill look like?
        ⇒ Possibly Bandwidth Alliance
- Do you have any peak times that the content is being accessed?
- what type of content mix (static/dynamic) do you have on your website?
  ⇒ If video included, Stream Delivery
- How do you control the caching behaviour today? Do you do it at the origin, or at your CDN provider?

CLOUDFLARE

Optimization/Speed

- Are there any current performance bottlenecks that you've identified with your site/application?
- What types of clients/devices mostly access your content?
- Would you need any image resizing to be done for any mobile users that currently access your site?
- Do you have a team who works purely on the contents optimization and compression?

CLOUDFLARE

Argo Smart Routing

- How many % of your traffic should stay dynamic?
- Where are your clients/users mainly located? Where is your origin server located?
- L4 or L7?

Argo Tiered Caching (Smart Tiered Caching, Custom Tiered Caching)

- Are we proposing Stream Delivery?
- Is the customer concerned about high cache hit rate?
- How is the customer's origin ISP/cloud provider charging the customer?
- Do they have concerns about the origin bandwidth fee or the origin international bandwidth fee?

Argo Tunnel

- Do you worry about hackers getting access to your Origin IP and sending direct attacks over?
- (Do they worry about attackers spoof Cloudflare IP as their source IP to DDoS the origin server?)
- Is it possible to consider installing a third party deamon on your application gateway or an origin server?

CLOUDFLARE

Load Balancing

- Do you have multiple origins?
- Is your customer base spread out geographically?
- Do you have or would you need HA configuration?
- Could you tell us your desired traffic steering set up?
- How fast would you want the switchover to happen?

CLOUDFLARE

Spectrum

- Have you ever experienced DDoS attack? Do you have concerns about DDoS?
- Do you have any TCP/UDP applications, web applications with non-standard ports that you currently host on your origin servers?
    - What applications/ports you need to securely proxy ?
- How do you currently protect them?
- How do you find the current protection? Do you have any challenges you could share?
- Where is the origin server and the users located? Do you currently have any performance concerns?
  ⇒ Possibly TCP Argo Smart Routing

Bot Management

- You have indicated you have one of the following concerns (need to be figured out by BDR/AE discovery). Could you tell us more about what has happened?
  - credential stuffing,
  - content scraping,
  - content spam,
  - inventory hoarding,
  - credit card stuffing
- ⇒ find out if the target application/endpoint has any of the below that comes with known limitation
  - Endpoints which receive API traffic from automated processes ⇒ Possibly API shield
  - Endpoints which receive API traffic from a Mobile Application
  - Endpoints which return a JSON response
- How do you current protect these endpoints against bot attacks? Do you have any challenges you could share?
  - How do you measure the false positives / false negatives of the current protection?
  - How do you ensure the good bots, crawlers are not affected by your current protection?

CLOUDFLARE

Workers

- Are you considering going serverless or implementing a serverless architecture?
- Do you need to offload any work off of your origins?
    - Do you get customer feedback that the responsiveness of your site is too slow? Have you thought about executing requests closer to the eyeball as a solution?
- Are there any application use cases that would benefit from logic being executed at the network edge vs at your origin server?
- Do you have developers resources to develop and maintain Workers code or would you need to outsource?

CLOUDFLARE

API Shield (API Schema Validation, Mutual TLS)

- Do you have an API endpoint?
  - What is the schema of the API?
  - Is it a public API endpoint, or a private API endpoint that needs strict client verification?
- How do you currently protect the API endpoint against DDoS attack, bots and abusers?
  - Have you ever experienced false negatives, like the DDoS attackers slowly drain the resource of your API endpoints by keeping the rate below the protection threshold?
- How do you ensure private API endpoint is only being used by the approved clients?
  - weak & easy way like token-based — Have you ever been compromised, or do you have any concerns about being compromised with the current security?
  - has mTLS now — How do your WAF and application security work together with the mTLS? Are they compatible?

CLOUDFLARE

Image Resizing

- How are you currently supporting Image Resizing (in-house solution or 3rd party solution)?
- What are some of the main image manipulation controls you are using? (Width, height, quality etc)
- If you are not using an image resizing solution how labor intensive is it doing this manually?
- How many unique image variants do you support for every image instance?
- Are you caching these variants with a CDN?
- How many monthly image requests do you have and what is the cache hit ratio of those requests?
- What is the average size of your Original/master images (in Megapixels)?

(Polish and Image Resizing doesn't work well together)

CLOUDFLARE

Stream, Stream Delivery

- Are you doing VOD, live or a combination of both?
- What kind of video files are you trying to deliver?
- What is the geographic distribution of your user traffic?
- Where are your origins located?
- What does your current video architecture look like (Storage, encoding, CDN and player)?
- What are you using currently to protect your videos? What do you need for protection of your videos? (token authentication, DRM)
- What is the primary pain with your existing provider and what are your priorities in evaluating a new provider?
- What clients will be used to play video content (web browser, Roku, Fire Stick, Apple TV etc.)
- How many concurrent viewers do you have at peak times?
- How long are your video chunks or segments?
- Do you know your Mbps at the 5th, 50th, and 95th percentiles?
- Are you considering us as a primary CDN or secondary? (for larger clients, >1PB per month)
- What are the key metrics you're using to evaluate new vendors in testing?

CLOUDFLARE

Waiting Room

- Do you have particular peak time at your application? How often your origin server's CPU goes busy at the peak time?
- Do you have a way not to lose the visitors when origin server is overloaded by too many visitors?
- How much accuracy would you need when providing the estimated wait time to the queued visitors?

CLOUDFLARE

SSL for SaaS

- Do you provide SaaS, or hosting business? Do your customers (external domains) need to CNAME to your service to get your service?
- Would you like to extend your Cloudflare benefit (security, performance, reliability) to your customers' external domains?
- What exactly are the Cloudflare benefits you would like to extend to the custom hostnames? (for compatibility check)
- Are your customers domains on host level or do they need their apex domain to be proxied too?

CLOUDFLARE

China Network

- Do you have Origin Servers in China or outside or both?
- Are you currently hosting with any other CDN within China?
- Do you have an ICP License already?
- Do you have users within China accessing applications hosted outside of China?
- Do you have users outside China accessing applications hosted inside China?
- Do you have a custom cert for securing your China hosted applications?

Static IP/BYOIP

- Check if the customer has one of the following use cases
  Apex proxying: Customer needs an IP address to use for their apex 'A' record
  Zero rating: Work with deals with mobile phone providers to "zero rate" traffic sent to their IPs
  Egress filtering: Allow traffic from customer infrastructure through a firewall to reach domain, but is unable or unwilling to permit access to the entire IP network
  (Sub)domains with MX record: CNAMEs are incompatible with MX records, so some DNS providers prohibit you from adding a CNAME
  Latency reduction: Ad networks have expressed desire to avoid CNAME lookup time
- Are these IPs at risk of being blocked or filtered? If yes, why?

O2O (Not customer-facing product)

- Does the customer use **Cloudflare-enabled service** as their origin server?
  - Example: Salesforce, Shopify, Marketo....
- What are the Cloudflare products the customer needs? (Not all products interoperatible)

Premium Success vs Partner Referral

Premium success should be positioned as

- an elevated success experience for customers that require a more high touch experience
- enhanced Support SLAs
- customized workshops with their account team (does not mean weekly check in calls)

Consider partner referral from the early stage of the deal if we anticipate the customer would:

- need intensive handholding technical support
- need consistent, non-stop technical consultancy, guided or managed troubleshooting
- need production cutover standby at non working hours
- need 24/7 SOC services
- need managed services, professional services
- need regular (weekly, monthly) customised reporting
- need development and maintenance of Workers script

NEXT TOPIC & ASSIGNMENTS

Fictional Customer Scenario

Based on the given customer's response, please prepare Blazeclan's own further discovery questions needed, and complete solution design.

https://docs.google.com/spreadsheets/d/1GnL1I2rUcWFJKWQi9YP3aKR7BsRam9ad/edit#gid=1097359140

Managed Authoritative DNS	Managed SSL	Unmetered DDoS	WAF	Firewall Rules	IP Reputation Intelligence	Optimization	CDN	Analytics & Logpush
Argo	Rate Limiting	Spectrum	Load Balancing	Bot Management	Stream Delivery	Payload Inspection	Image Resizing	API Shield
SSL for SaaS	Waiting Room	Mutual TLS	China Network	Stream			DNS Firewall	Secondary DNS
Access	Gateway (SWG, Warp) DNS Recursive	Remote Browser Isolation						Premium Success
Magic Transit	Magic WAN	Magic Firewall					Cloudflare Network Interconnect	Bandwidth Alliance
Workers	Workers KV							

CLOUDFLARE

Fictional Customer Scenario (cont)

Please prepare customer-facing presentation focusing on the strength, based on the discovery:

- **High level solution overview**
- **Dashboard demo**

Slide reference (Cloudflare standard deck)

- https://docs.google.com/presentation/d/1QglFG7c4rhKwfcii6aErLCx5k5ssw0ps/edit
- https://docs.google.com/presentation/d/1uSF-1xy8Akto_Bo8qNSNVvreA7C-bGfEEBFCbx_0mc0/edit

Dashboard demo reference

- https://drive.google.com/file/d/1Hcxs9dlS9L6XKJ7lENZap0FF8DWMo7FA/view?usp=sharing

Next topic

Pitch-off together!

- **Cloudflare presentation - by Jean**
- **Cloudflare presentation - by Blazeclan (Own branding)**
- **Cloudflare dashboard demo & QNA - by Blazeclan**

Solution design exercise

- **Solution design practice based on actual past customer scenario**
- **(implementation exercise to come - next training)**

Schedule

- **WEDNESDAY**

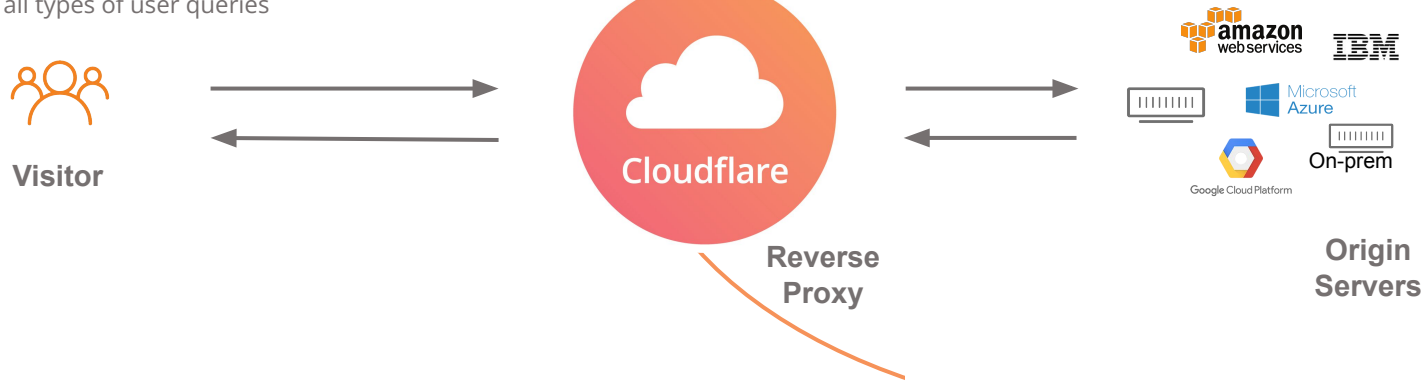
// Appendix

High Level Overview

Anycast Network
Connects each consumer to the nearest data center
Distributes attack traffic across data centers
Additional Cloudflare PoPs added for customer automatically as network grows

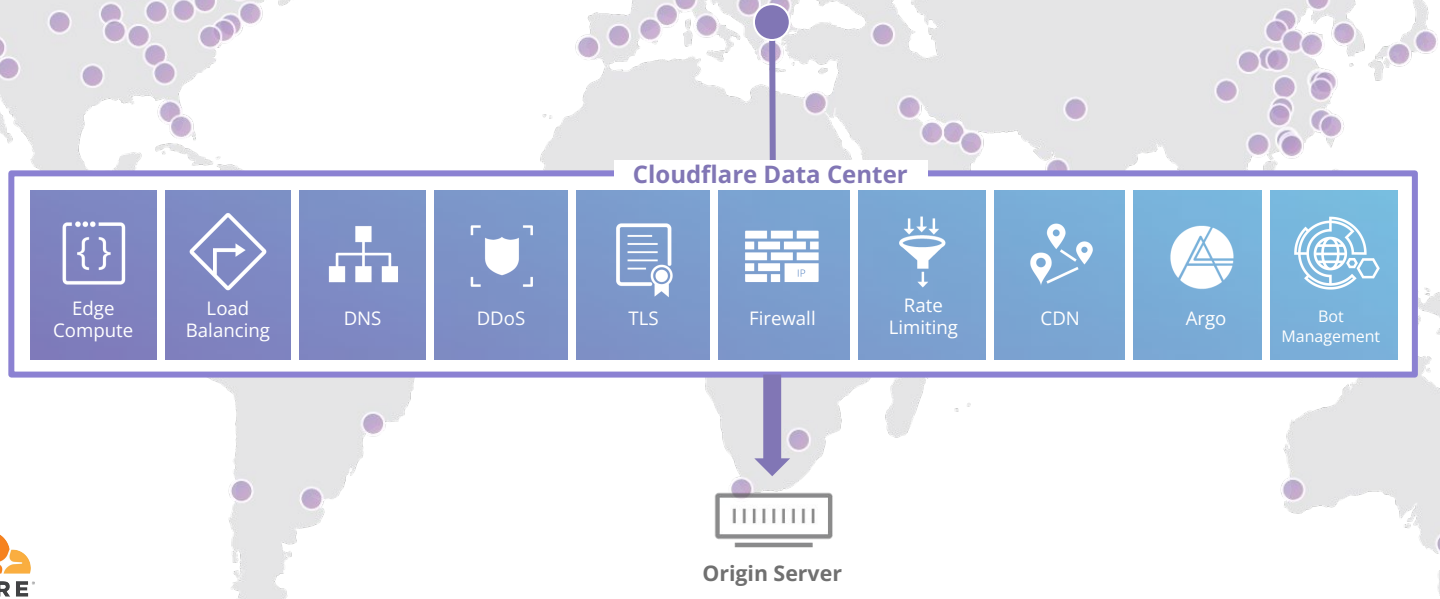
Modern, Unified Architecture
Integrated stack, where each server reliably runs all types of user queries

Scalable, Global Network
Elastic horizontal scaling with redundancy across all servers. All data centers utilize commodity hardware so that the network can be expanded at low cost



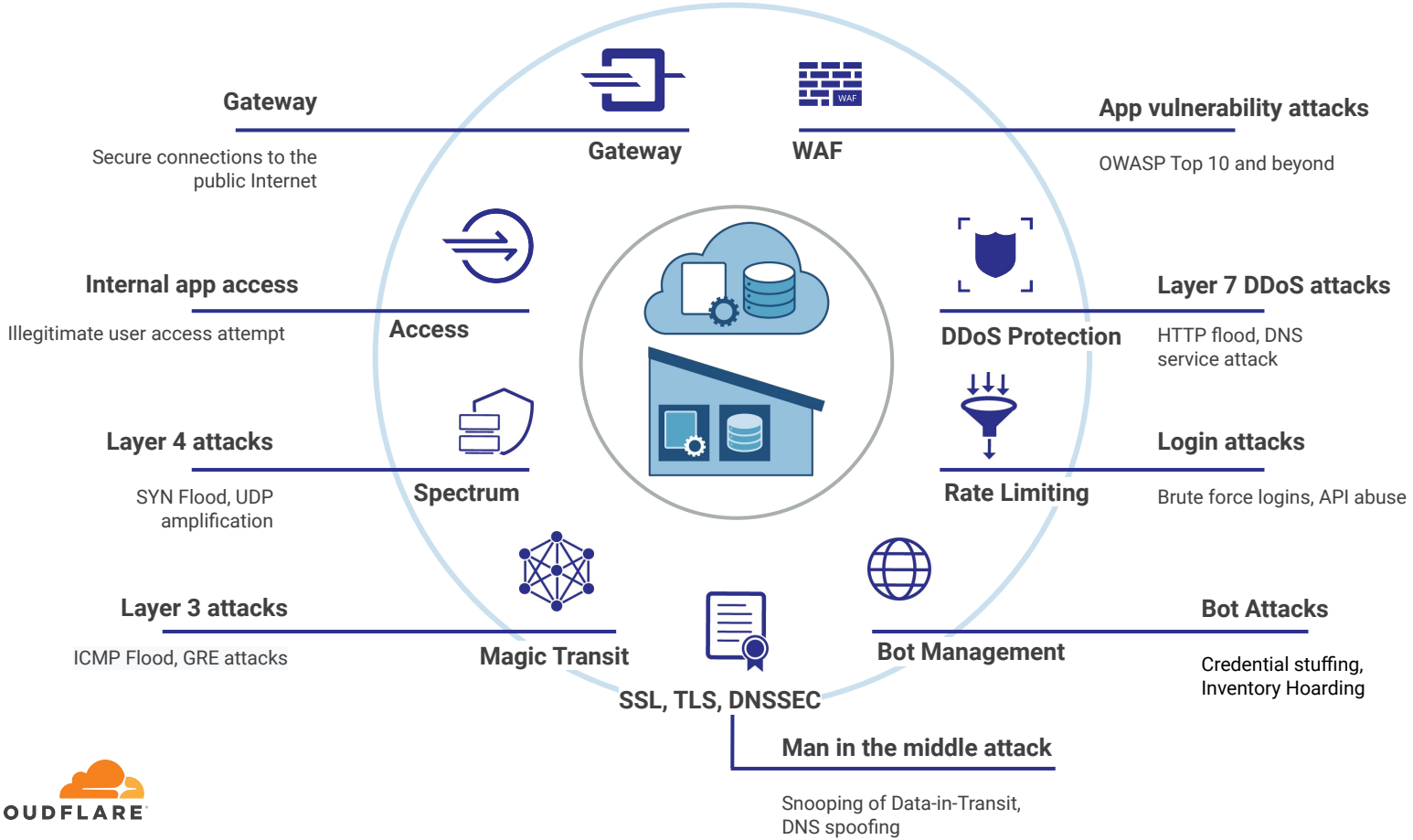
Every Data Center Performs Every Task

It's not just about the ***# of data centers, it's about capabilities***. Each data center is identically designed with the same software stack and runs on our own hardware stack.



CLOUDFLARE

Simple, Integrated, Intelligent Protection for Your Apps and Data



CLOUDFLARE

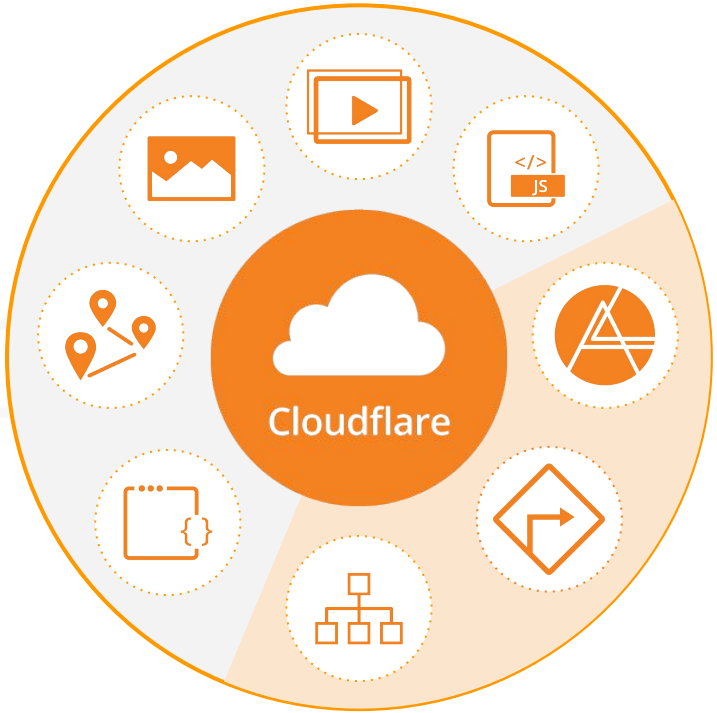
Cloudflare Performance Services

Stream
Reduce technical debt and overhead of building video streaming infrastructure

Image Optimization
Optimize image file delivery with resizing, compression and parallel streaming of progressive JPEGs

CDN
Easily integrate and customize caching and serverless functions with an API first architecture

Workers
Reduce origin dependencies and server overhead with advanced serverless edge functionality



HTTP/2 Prioritization
Prioritize web resource loading and minimize the impact of render blocking JavaScript

Argo Smart Routing
Employ intelligent routing for content requests from the origin

Global Load Balancing
Source content from the origin closest to the user

Modern Protocols
Easily leverage modern protocols for improved performance like TLS 1.3, AMP, HTTP/2 and HTTP/3