


TECH TALK

Andrey Moskvitin
Senior SE

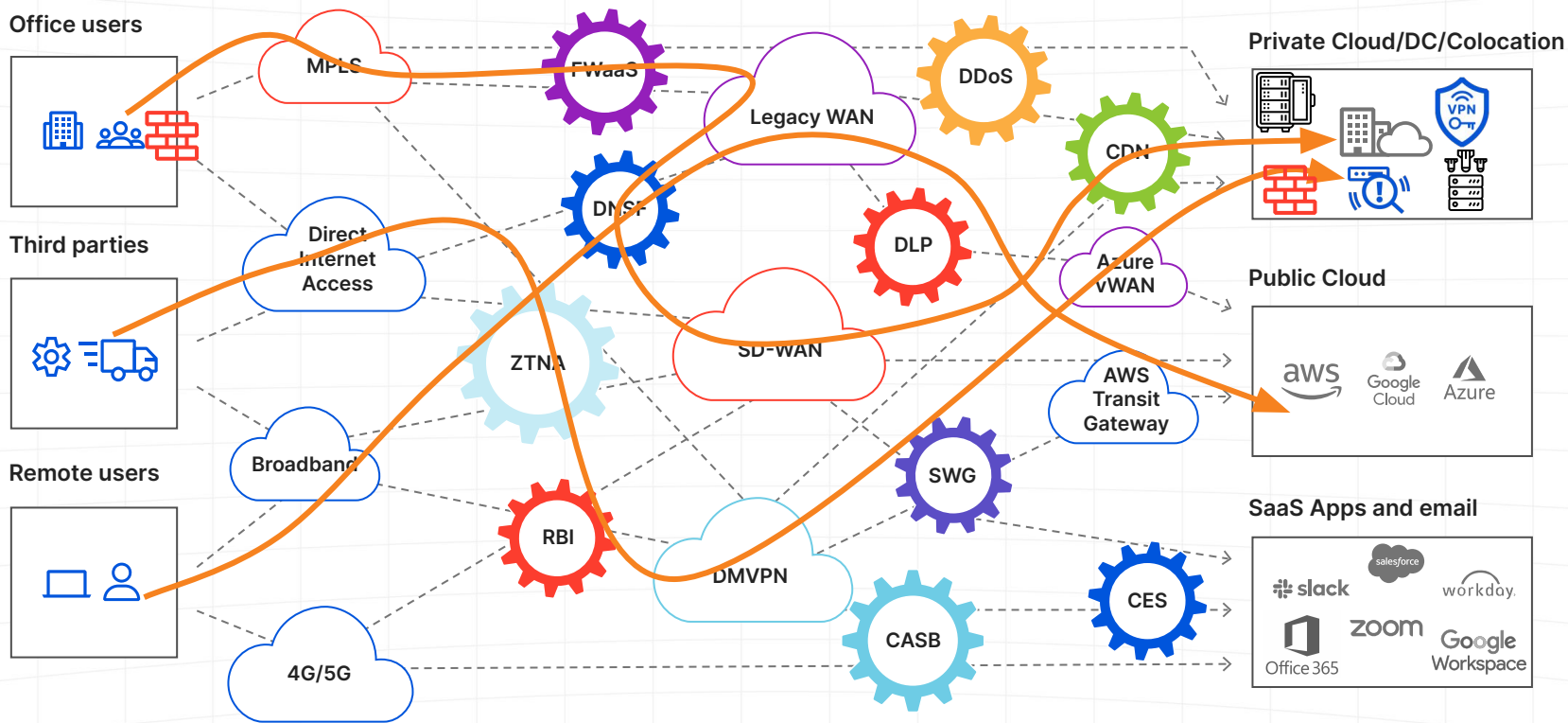
m@cloudflare.com



- 15+ years in cyber
- Alphabet soup of SABSA, CISSP, CISA, CISM, CCSP
- ex Cisco, Microsoft, McAfee
- Live on a small island of Madeira
- Worked in Australia, EU and CIS
- Have seen some things -
Big Banks to Fed Gov and
Commonwealth Games

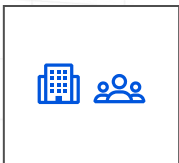
i am here
for you 

Today's Spaghetti Network



Simple Easy Future With Cloudflare

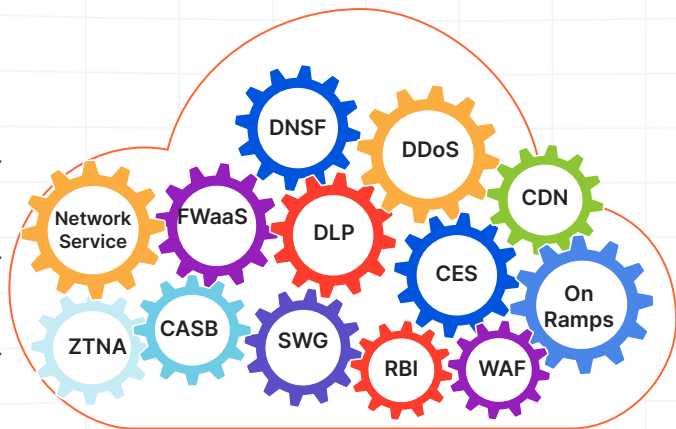
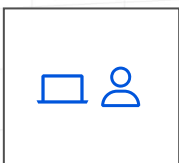
Office users



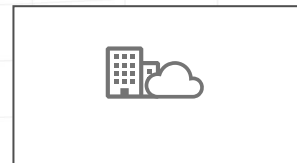
Third parties



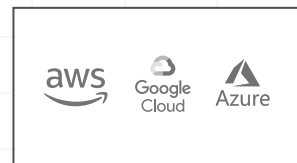
Remote users



Private Cloud/DC/Colocation



Public Cloud



SaaS Apps and email



Your business can be

Secure



Reliable



Private



Automated



4 times the return on investment (ROI) compared to on-premises deployments, up from 3.2X during the previous two-year period

2.5X faster recovery of initial investments, an increase that is expected to grow due to the acceleration of cloud adoption

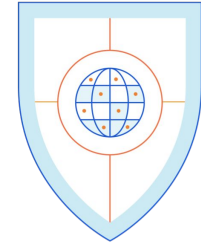
But clouds are not that secure...

Our certifications and memberships



and more
www.cloudflare.com/trust-hub

Compliant by Design



ISO 27001:2013

ISO/IEC 27001:2013 is an industry-wide accepted information security certification that focuses on the implementation of an Information Security Management System (ISMS) and security risk management processes. Cloudflare has been ISO 27001 certified since 2019.

ISO 27701:2019

ISO/IEC 27701:2019 is a new ISO privacy certification, implementing a comprehensive Privacy Information Management System (PIMS) aligned with various privacy regulations including the GDPR. Cloudflare has been ISO 27701 certified as a PII Processor and PII Controller since 2021.

SOC2 Type II

Cloudflare has undertaken the AICPA SOC 2 Type II certification to attest to Security, Confidentiality, and Availability controls in place in accordance to the AICPA Trust Service Criteria. Cloudflare's SOC 2 Type II report covers security, confidentiality, and availability controls to protect customer data.

BSI Qualification

Cloudflare has been recognized by the German government's Federal Office for Information Security as a qualified provider of DDoS mitigation services.

Compliant by Design



ISO 27018:2019

ISO/IEC 27018:2019 is an international privacy certification that extends an Information Security Management System (ISMS) to protect personal data when being processed in a public cloud. Cloudflare has been ISO 27018 certified since 2022 and the certificate is available upon request.

C5:2020

Cloud Computing Compliance Criteria Catalogue (C5:2020) is an auditing standard created by Germany's Federal Office for Information Security (BSI). The C5 standard ensures cloud service providers adhere to a baseline of information security criteria. The C5 report covers security controls to protect customer data and is available upon request.

PCI DSS 3.2.1

Cloudflare maintains PCI DSS Level 1 compliance and has been PCI compliant since 2014. Cloudflare is audited annually by a third-party Qualified Security Assessor QSA. Cloudflare's Attestation of Compliance is available upon request.

And more...

<https://www.cloudflare.com/trust-hub>

Keeping your data inside EU and private keys on-prem



Customer Metadata Boundary

Control over how metadata about your traffic is handled and stored.

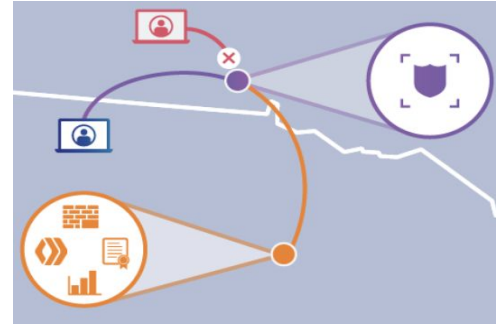
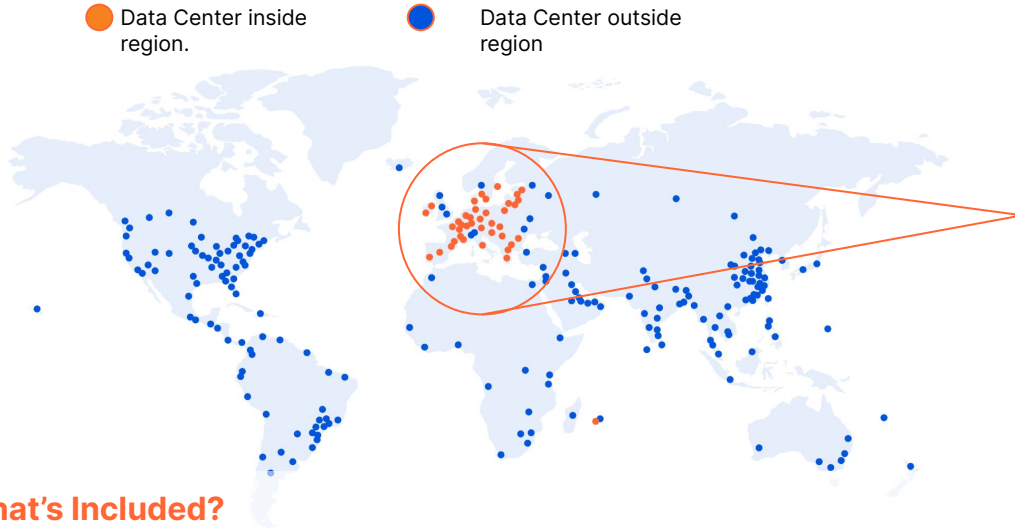
Payload Inspection Boundary

Control over where your traffic is decrypted and inspected.

Encryption Key Management

Control over where TLS encryption private keys are stored.

How Cloudflare's Data Localisation Works



What's Included?

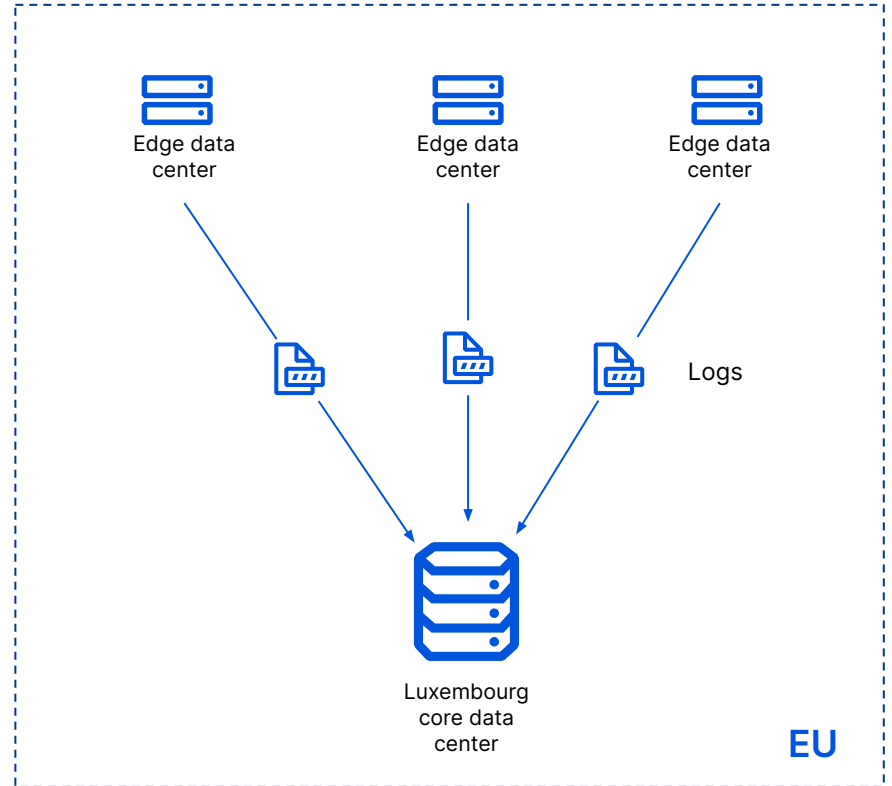
- **Payload Inspection Boundary (Regional Services)** ensure that *only* data centers in a preferred region decrypt TLS and apply HTTP services such as WAF, CDN and Workers
- **Customer Metadata Boundary** ensures that logs + analytics do not leave the region
- **Geo Key Manager + Keyless SSL** ensure that private SSL keys are only stored in specific regions

EU Customer Metadata Boundary

When enabled, it ensures that all customer-identifiable end user metadata that Cloudflare processes in our role as a Data Processor remains in the EU.

Any end user traffic log messages containing customers' account ID are not sent outside the EU. They are only sent to our core data center in Luxembourg.

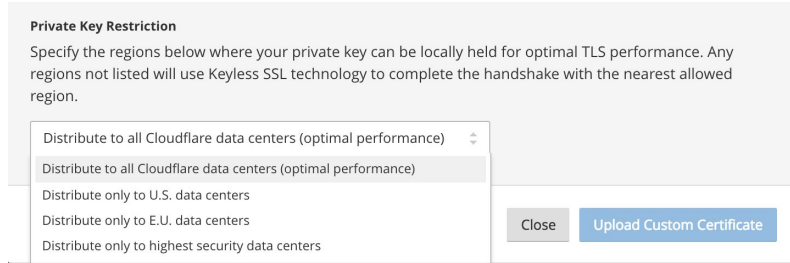
Logs & Analytics still available as before.



Encryption Key Management

Enable organizations to comply with regulatory and security policy requirements

Geo Key Manager

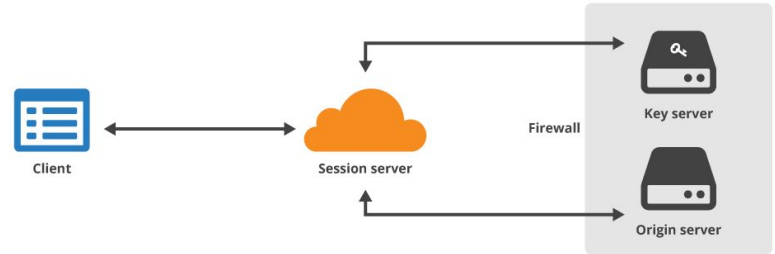


Keep your SSL/TLS private keys within a region (EU or US) when uploading to Cloudflare.

Prevent access to decryption keys outside in the intended region.

These encryption key management tools are also available to Customers outside the Data Localization Suite offering.

Keyless SSL



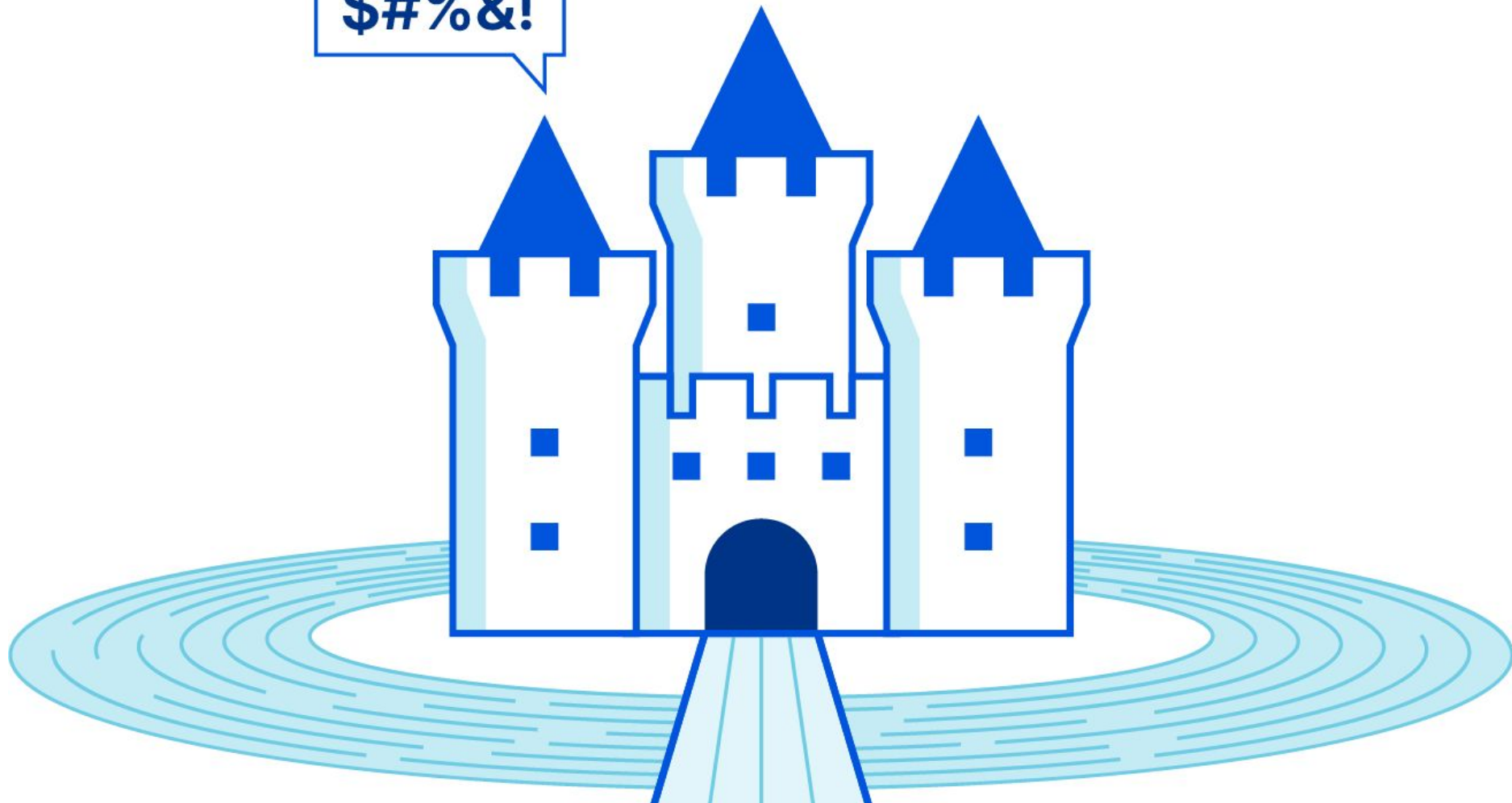
Keep your SSL/TLS private keys on your own servers or HSMs.

No need to upload private keys to Cloudflare.

Zero Trust



\$#%&!



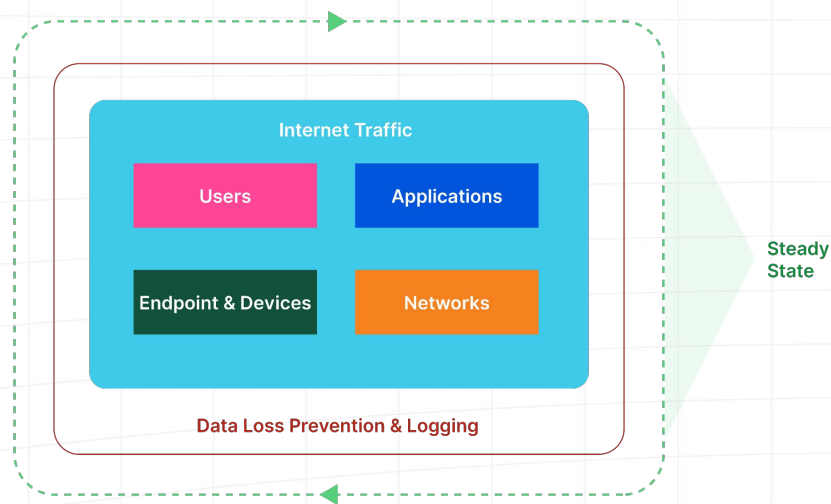


ATSTOK!!!

Roadmap to Zero Trust architecture

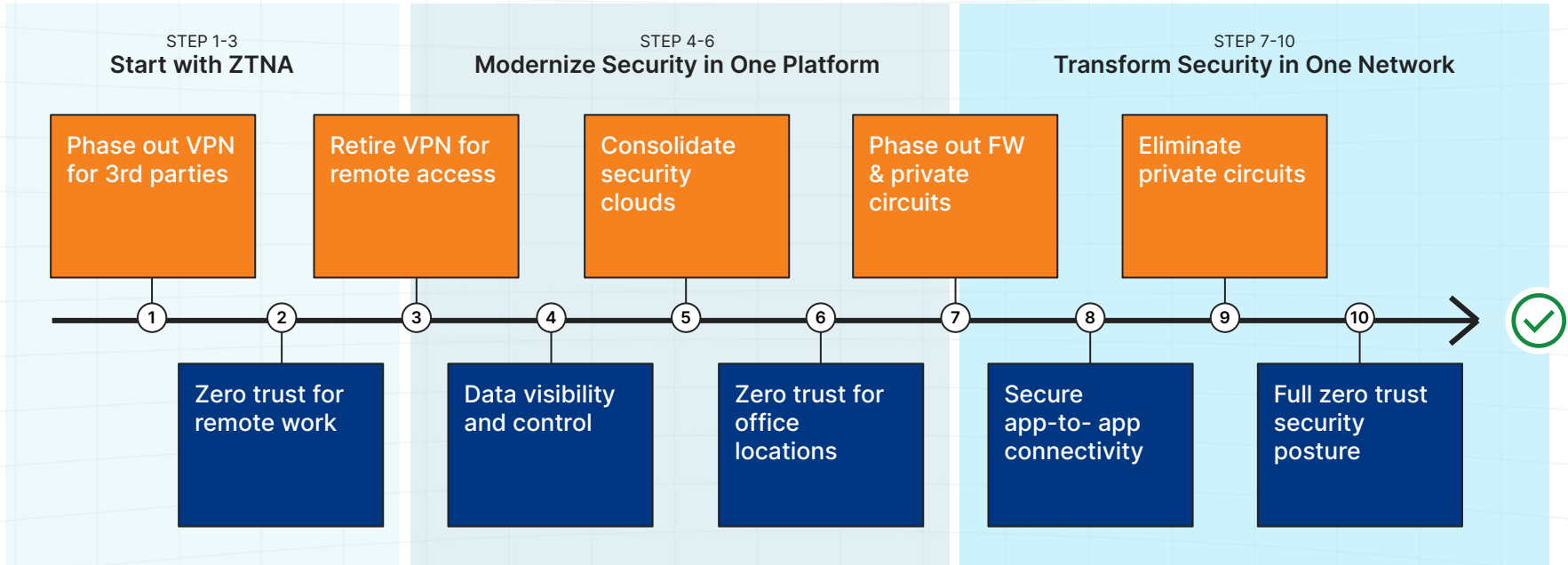
Details @ zerotrustroadmap.org

Below we visualized the relationship of seven major components to organizational security that needs to be considered when it comes to implementing a comprehensive architecture — the 28 steps on the right can be re-ordered.



	Component	Goal	Level of Effort
Phase 1	Internet traffic	Deploy global DNS filtering	1 bar
	Applications	Monitor inbound emails and filter out phishing attempts	1 bar
	DLP & logs	Identify misconfig and publicly shared data in SaaS tools	1 bar
Phase 2	Users	Establish corporate identity	2 bars
	Users	Enforce basic MFA for all applications	1 bar
	Applications	Enforce HTTPS and DNSsec	1 bar
	Internet traffic	Block or isolate threats behind SSL	2 bars
	Applications	ZT policy enforcement for publicly addressable apps	1 bar
	Applications	Protect applications from layer 7 attacks	1 bar
	Networks	Close all inbound ports open to the Internet for app delivery	1 bar
Phase 3	Applications	Inventory all corporate applications	2 bars
	Applications	ZT policy enforcement for SaaS applications	2 bars
	Networks	Segment user network access	3 bars
	Applications	ZTNA for critical privately addressable applications	1 bar
	Devices	Implement MDM/UEM to control corporate devices	2 bars
	DLP & logs	Define what data is sensitive and where it exists	2 bars
	Users	Send out hardware based authentication tokens	2 bars
	DLP & logs	Stay up to date on known threat actors	1 bar
Phase 4	Users	Enforce hardware token based MFA	2 bars
	Applications	ZT policy enforcement and network access for all applications	3 bars
	DLP & logs	Establish a SOC for log review, policy updates and mitigation	2 bars
	Devices	Implement endpoint protection	1 bar
	Devices	Inventory all corporate devices, APIs and services	1 bar
	Networks	Use broadband Internet for branch to branch connectivity	2 bars
	DLP & logs	Log and review employee activity on sensitive apps	2 bars
	DLP & logs	Stop sensitive data from leaving your applications	2 bars
	Steady state	DevOps approach for policy enforcement of new resources	2 bars
Steady state	Implement auto-scaling for on-ramp resources	2 bars	

A common journey to Zero Trust and SASE: **optimize your network at your own pace**



 Security Policy  Infrastructure Consolidation

Analyst Validation



Market-leading Zero Trust / SASE platform

Honorable mention in the *Gartner Magic Quadrant for Security Service Edge 2022*.

Representative vendor in the *Gartner Market Guide for Zero Trust Network Access 2022*.

Contender in the *Forrester New Wave Zero Trust Network Access Q3 2021*.

Leader in the *KuppingerCole Leadership Compass for Zero Trust Network Access 2022*.

Leading provider in the *Omdia Market Radar for Zero Trust Access*.

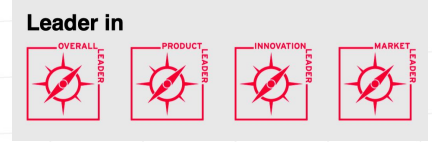
Representative vendor in the *EMA Availability & Buying Options in the Emerging SASE Market*.

Read Cloudflare One reviews in *Security Service Edge* from enterprise peers—verified by Gartner

Analyst Validation

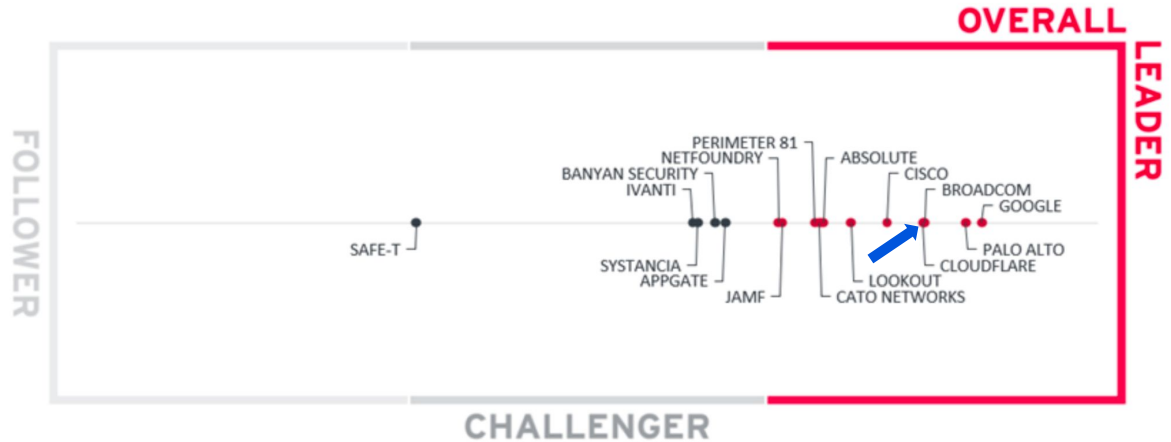


Cloudflare is a Leader in ZTNA 2022 KuppingerCole Leadership Compass



Cloudflare strengths

- Fully integrated organically developed security and access management platform
- Largest global cloud infrastructure with low-latency reach for 99% of the world population
- Integrates with all major identity providers and endpoint detection and response vendors
- Transparent clientless user experience
- Massive market presence and global brand recognition

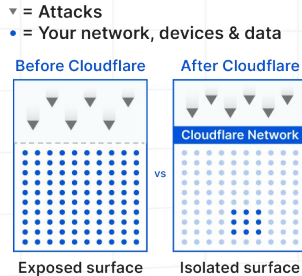


Cloudflare is an international company specializing in accelerating and protecting internet applications through an intelligent global security cloud without adding hardware or installing software. Cloudflare Access, part of the company's Cloudflare One platform for Zero Trust and SASE, connects any user to any application or network with fine-grained clientless or client-based access.

Saving time and €€€ with Zero Trust

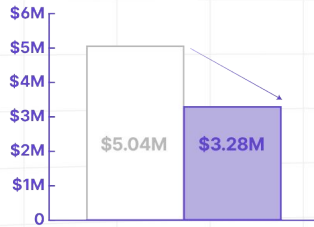
1. Reduce attack surface

91% ↓



2. Reduce breach costs

35% ↓



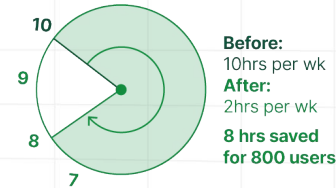
3. Accelerate onboarding

60% ↑



4. Reduce IT tickets

80% ↓



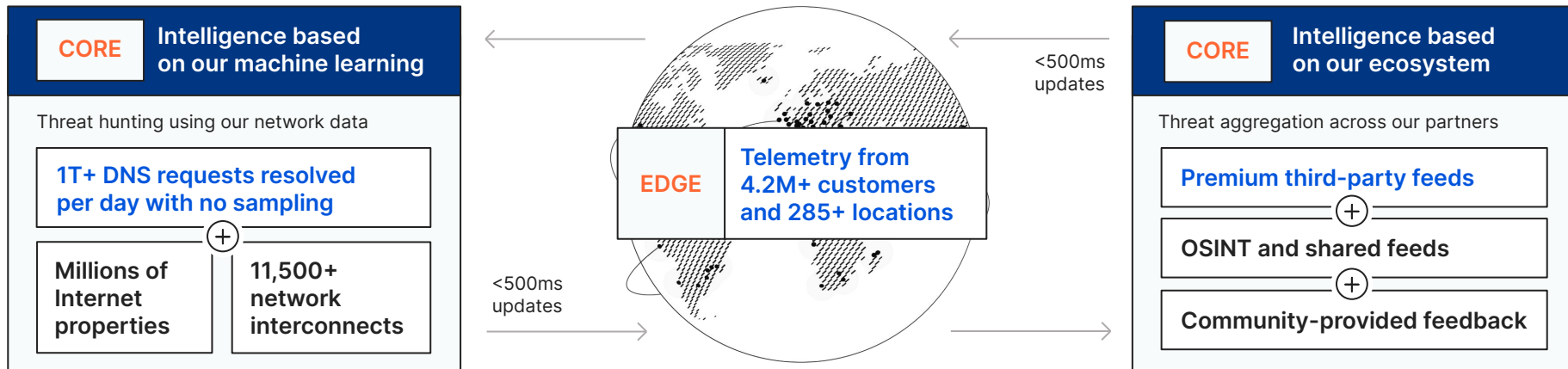
5. Reduce latency

39% ↓



Licensed per users!
Not devices, bwidth, apps, geos, offices or boxes

Comprehensive coverage against Internet-borne threats



Security risk categories to block, isolate or logpush to SIEM per policy rule

Malware
Phishing
Cryptomining

Newly seen domains
New domains
Unreachable domains

DGA domains
DNS tunneling
C2 & botnet

Spyware
Spam
Anonymizer

Cloudflare is the only composable, Internet-native platform that delivers local capabilities with global scale and with...

Security

Privacy

Performance

Resilience

Agility



285+

cities in 100+ countries,
including mainland China

30

Data centers in China

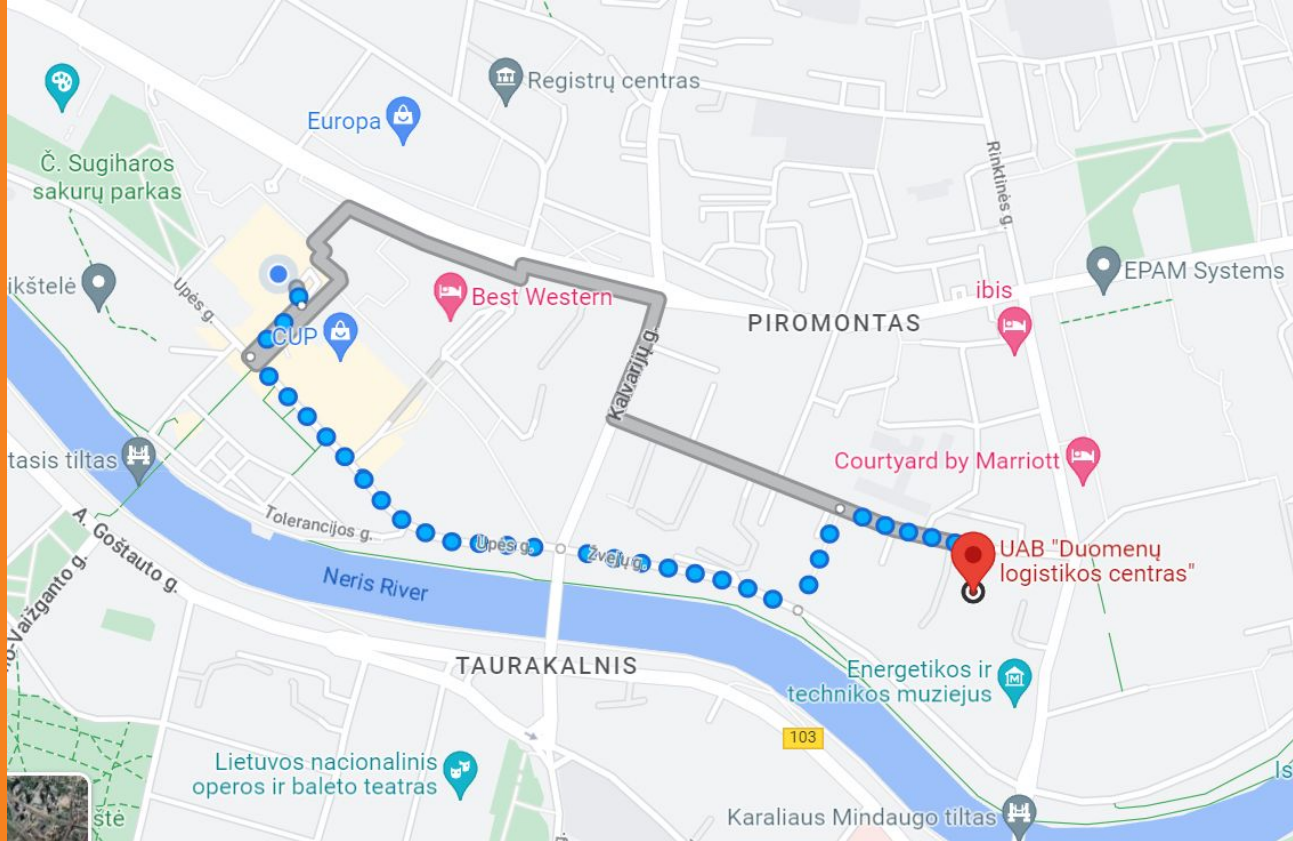
11,500+

networks directly connect to
Cloudflare, including ISPs,
cloud providers & large enterprises

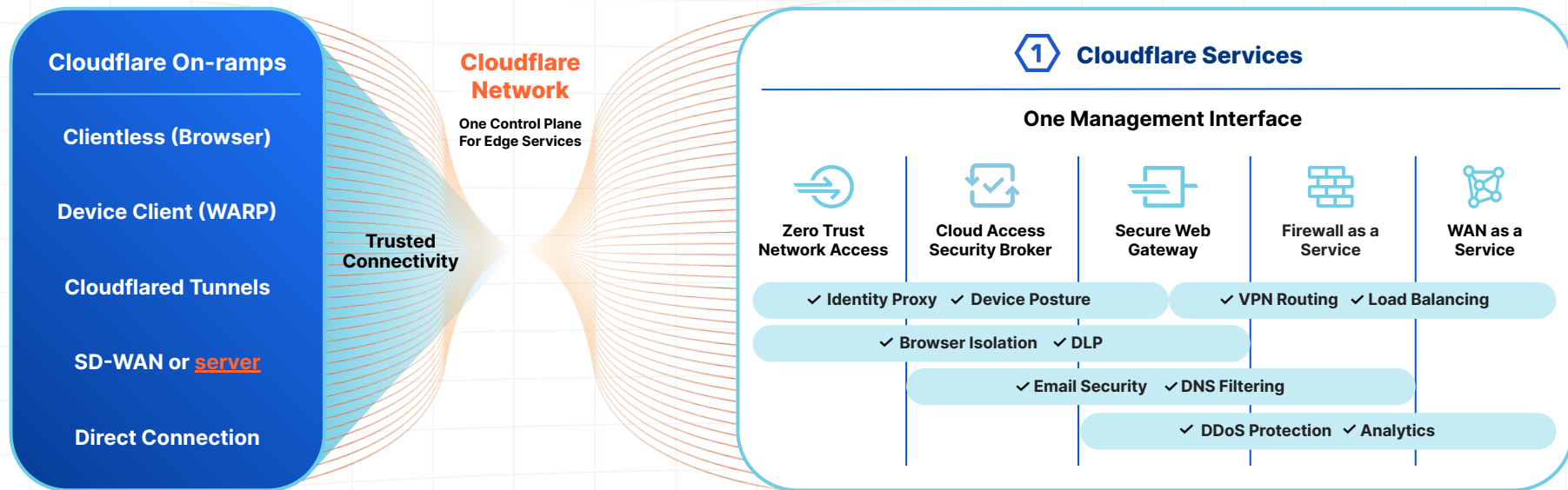
192 Tbps

of network edge capacity
and growing

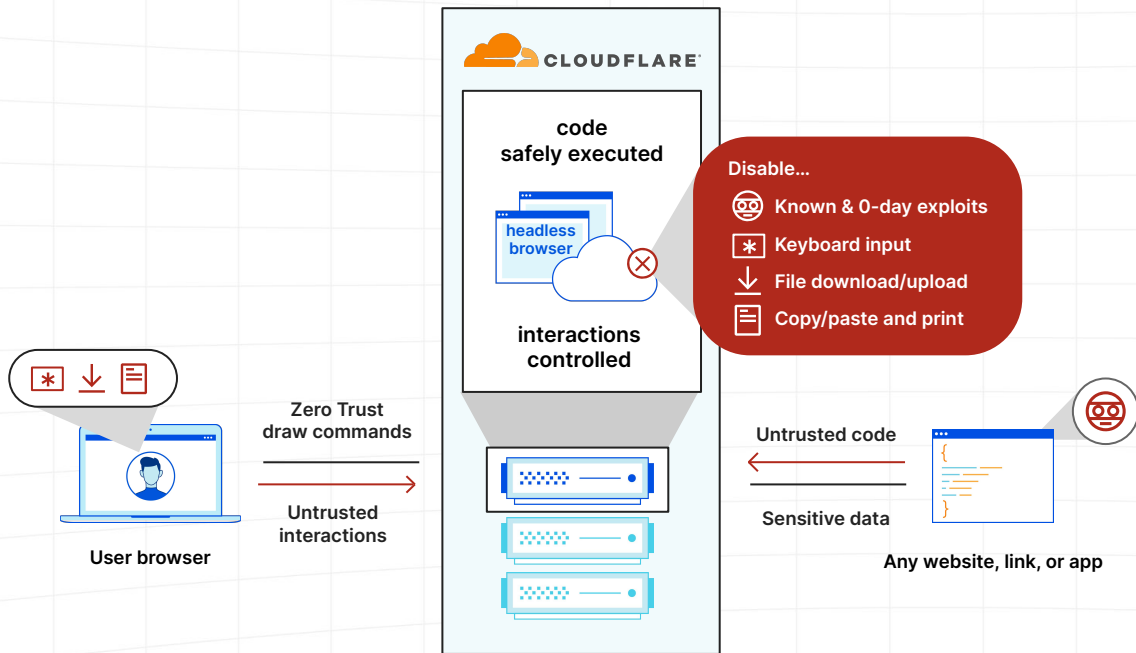
J13 / Data logistics - Juozapavičiaus Street 13



One network - everywhere



Remote Browser Isolation



Isolating inbound and outbound

Chromium containers w plugins

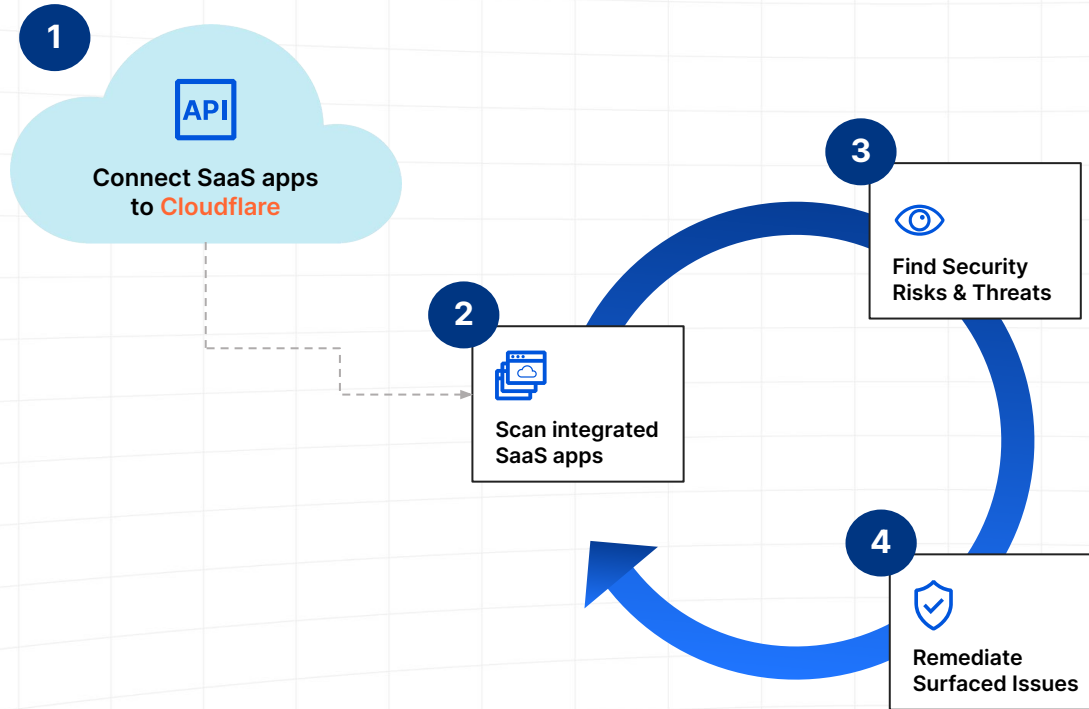
Safe sandbox for
email links and dodgy websites

Limit data exfiltration

Same or better speed

Compatibility w/all browsers

CASB through API and web proxy



Google Workspace

Microsoft 365

slack GitHub

salesforce box

Jira

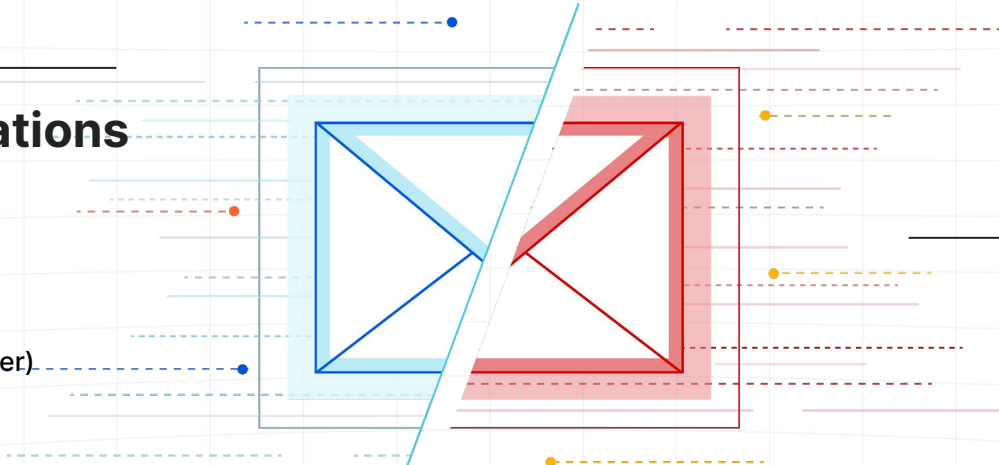
Confluence

Email is here to stay and the biggest risk

#1 way organizations communicate

70%

of organizations use cloud email solutions today. (Gartner)

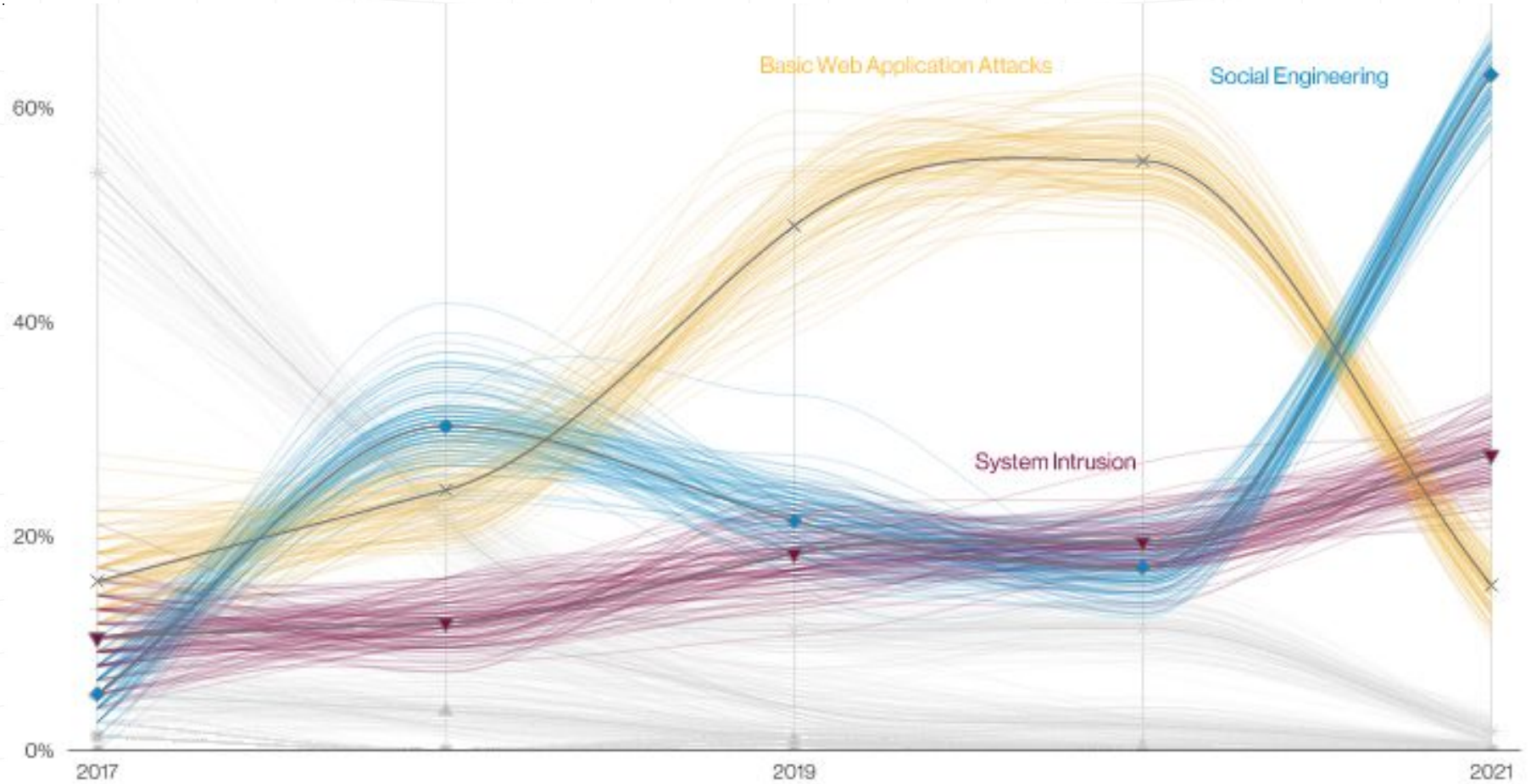


#1 threat attack vector

91%

of all cyber attacks begin with a phishing email. (Deloitte)

Verizon Databreach investigations report '22



Advanced email security



PREEMPTIVE

Early Discovery
Campaign Hunting
Actor Infrastructure
Monitoring

01



AREA 1
SECURITY

02



COMPREHENSIVE

Multi-Variety Attacks
Multi-Channel Attacks
Multi-Vector Attacks

04



ACCOUNTABLE

SLAs
Privacy
Biz Model

03



CONTEXTUAL

Natural Language
Understanding
Sentiment Analysis
Intent, Tone & Relationships

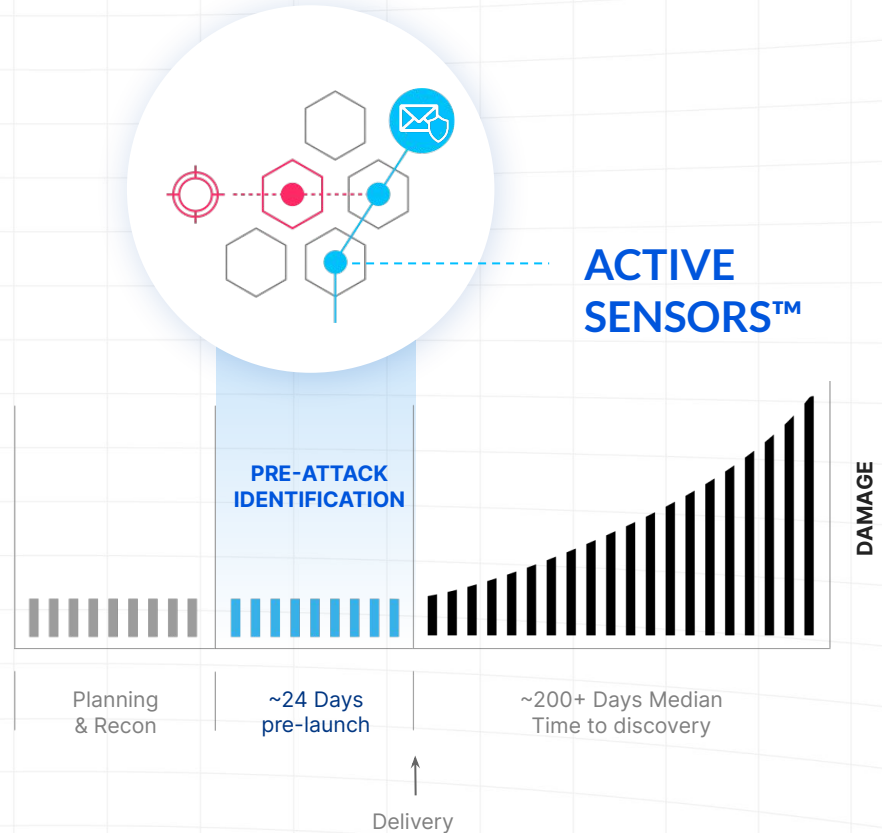


CONTINUOUS

Pre-Delivery
At-Delivery
Post-Delivery

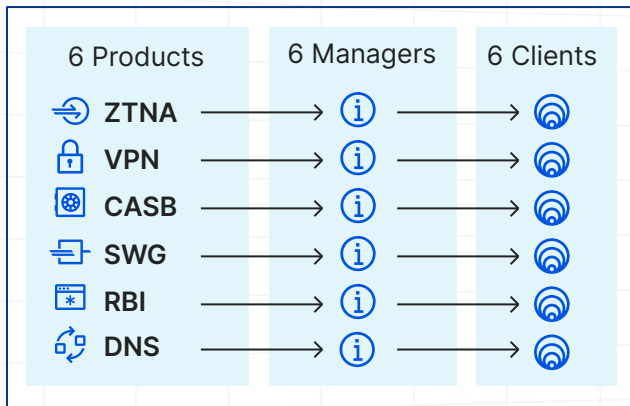
We have the only preemptive solution

- Massive-scale Phish Indexing, 8+ Billion pages
- Actor & campaign infrastructure hunting
- New Domains, Proximity Domains, Brand Domains
- User Impersonation, Browser Emulation
- In-the-wild Sandboxing



Terraform, API and IdP melts DevOps' hearts

Traditional Approach



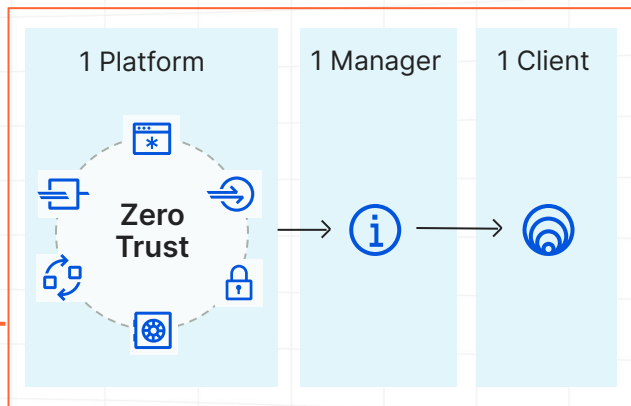
Problem #1:

Multiple point products require multiple policy managers, and multiple client deployments

Solution:

One seamless platform uses one policy manager, and one client deployment

With Cloudflare

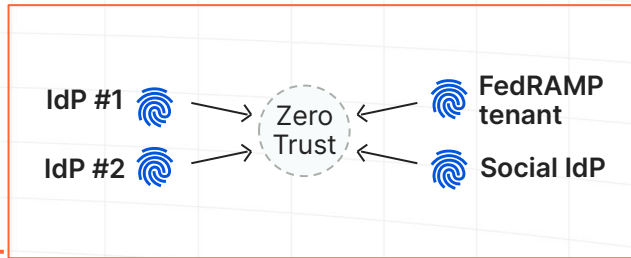


Problem #2:

Integrate only one identity provider (IdP) repeatedly and inconsistently

Solution:

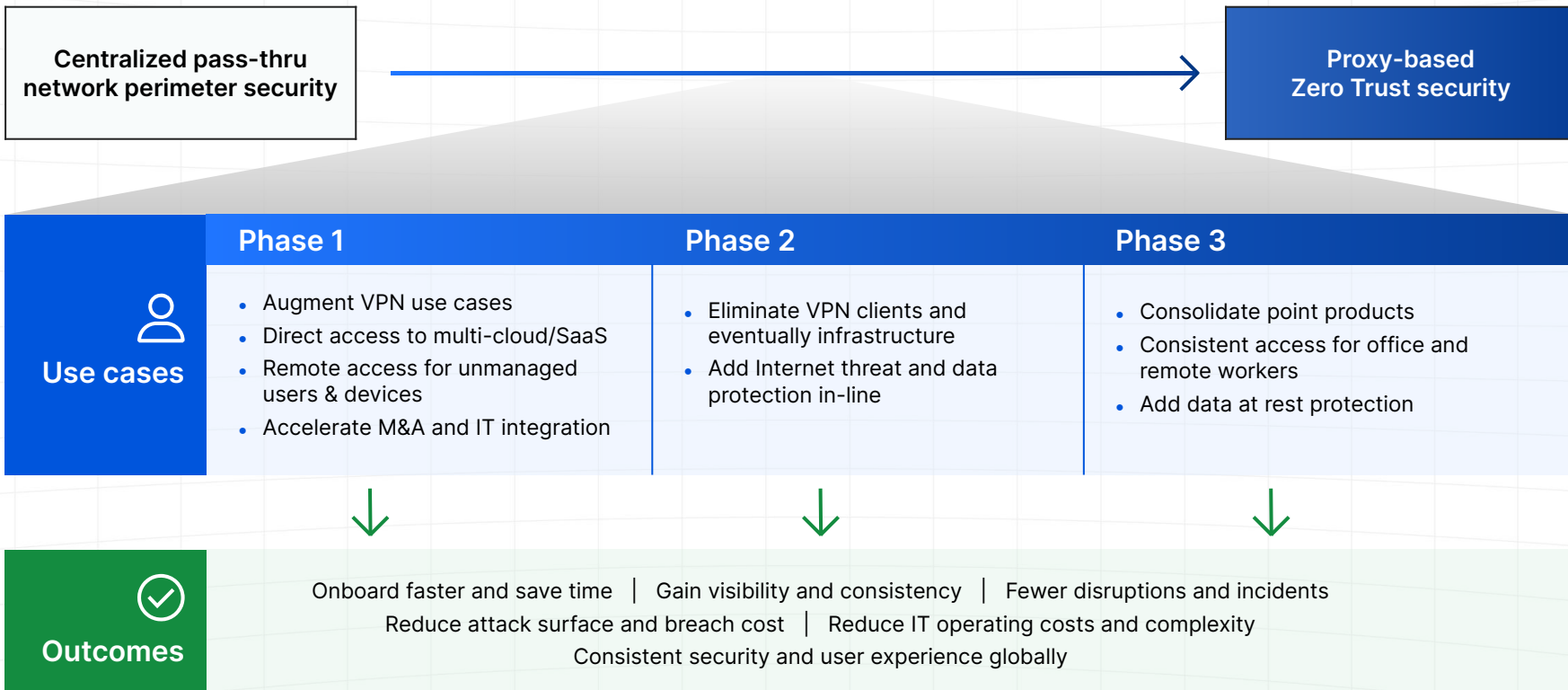
Integrate many IdPs and tenants of the same IdP just once



Give Zero Trust a try
Free up to 50 users

<https://dash.cloudflare.com/sign-up/teams>

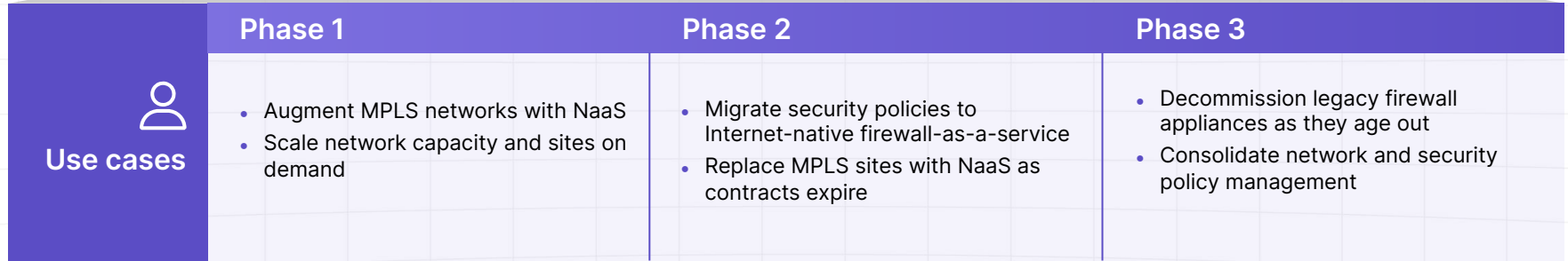
Security modernization



Network transformation

Expensive, rigid networks
via proprietary circuits
and appliances

Network as-a-service
with built-in security



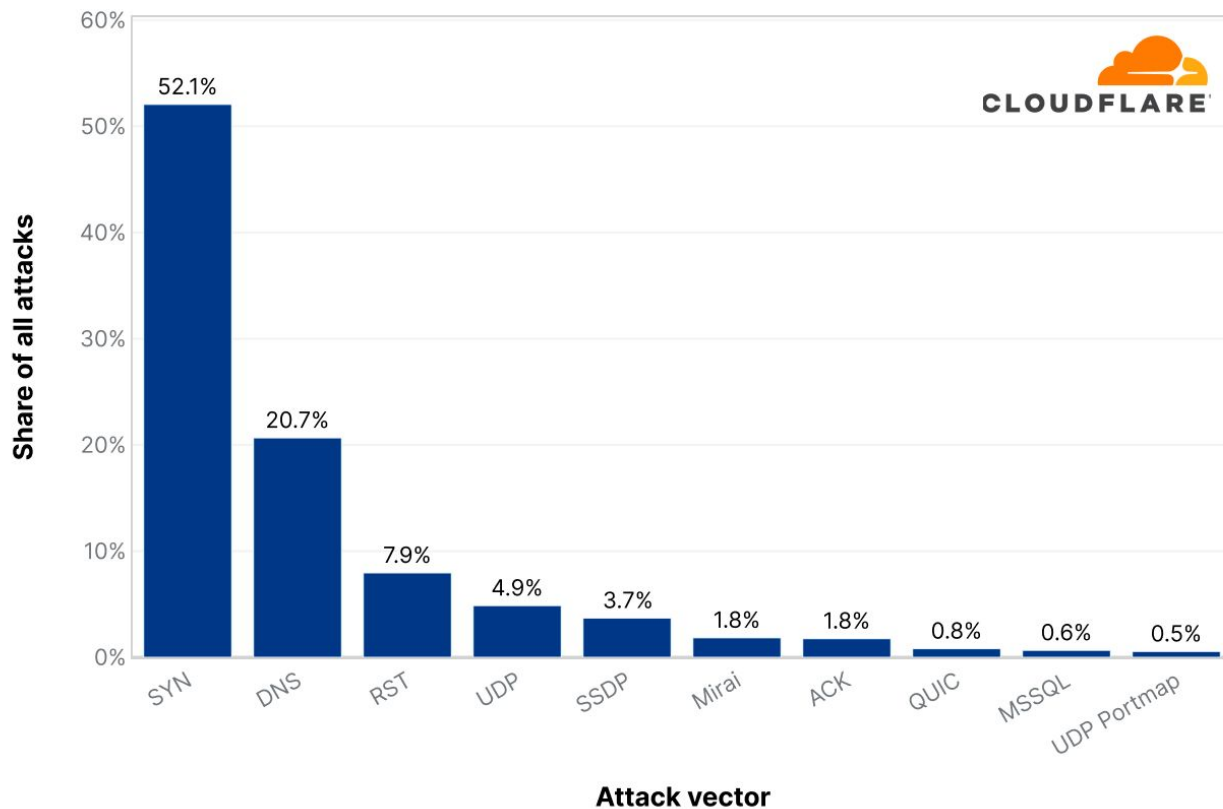
Outcomes

Predictable network performance and consistent security globally | Increased business agility — scale on-demand
Reduce IT operating costs and complexity — no appliances to manage

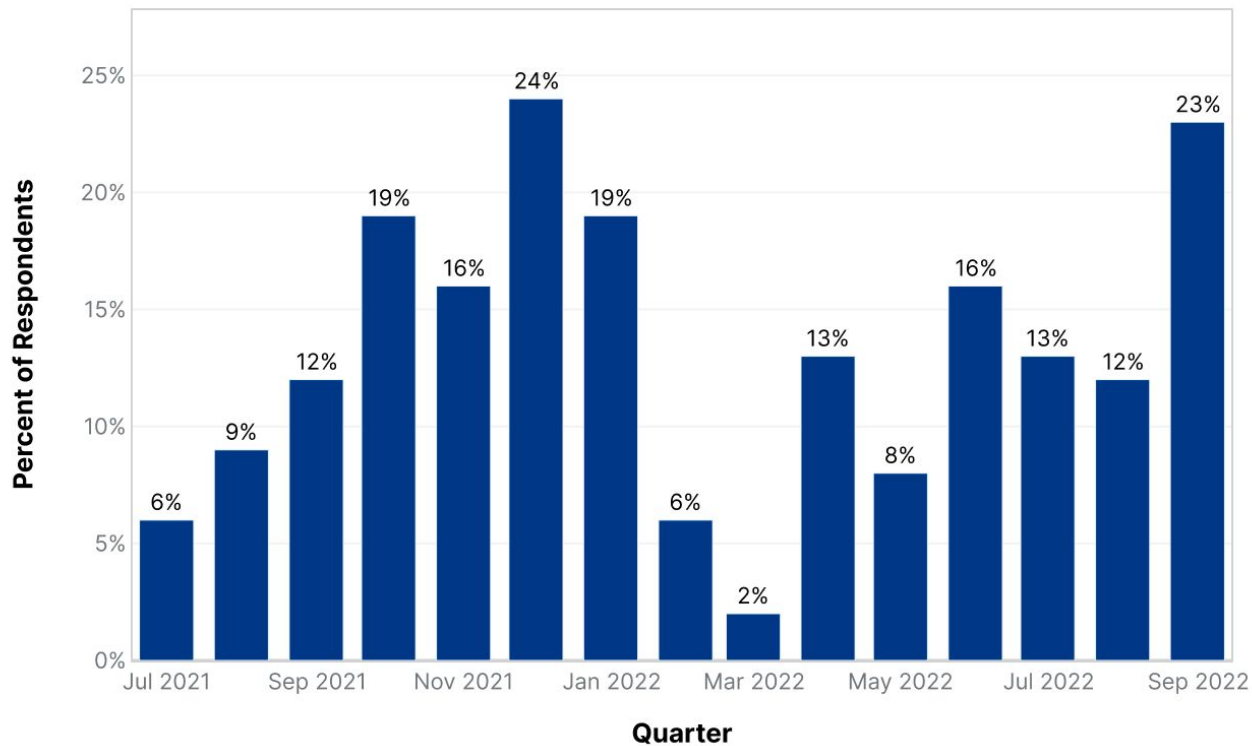
DDoS Trends 2022



Network-Layer DDoS Attacks - Distribution by top attack vectors



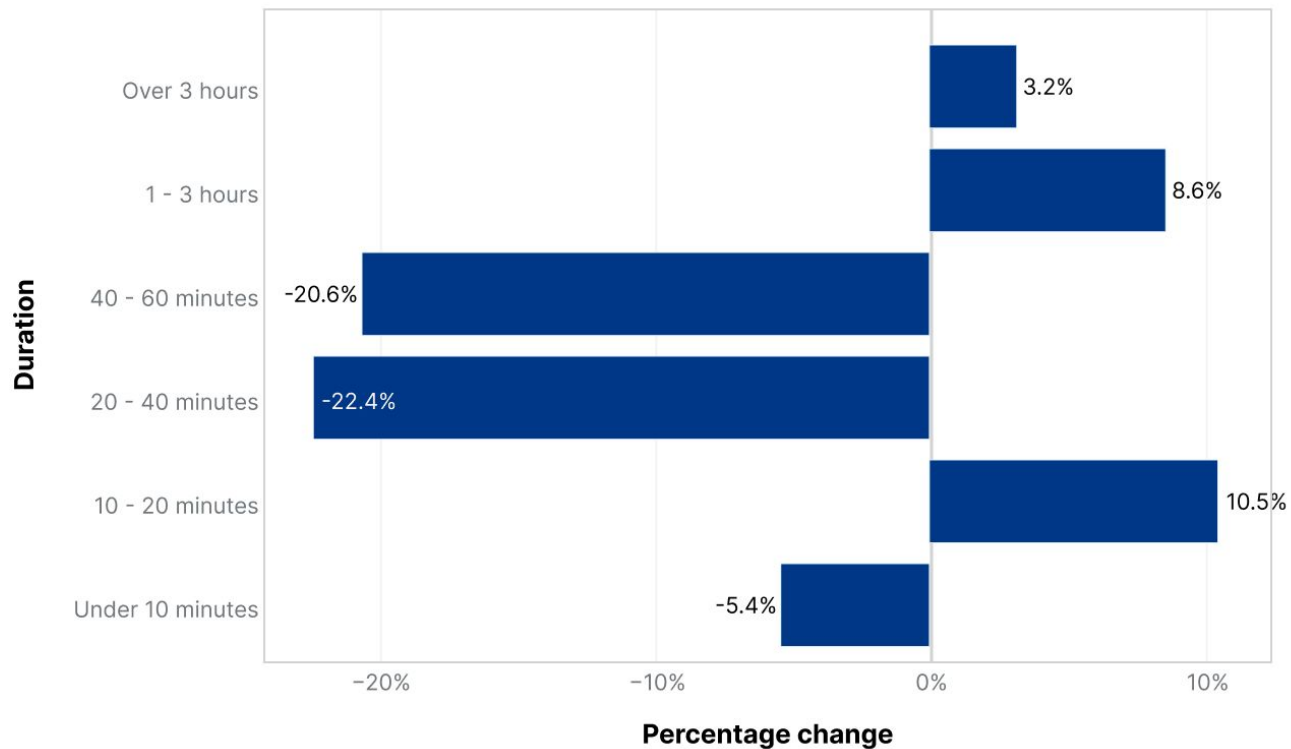
Ransom DDoS Attacks & Threats by Month

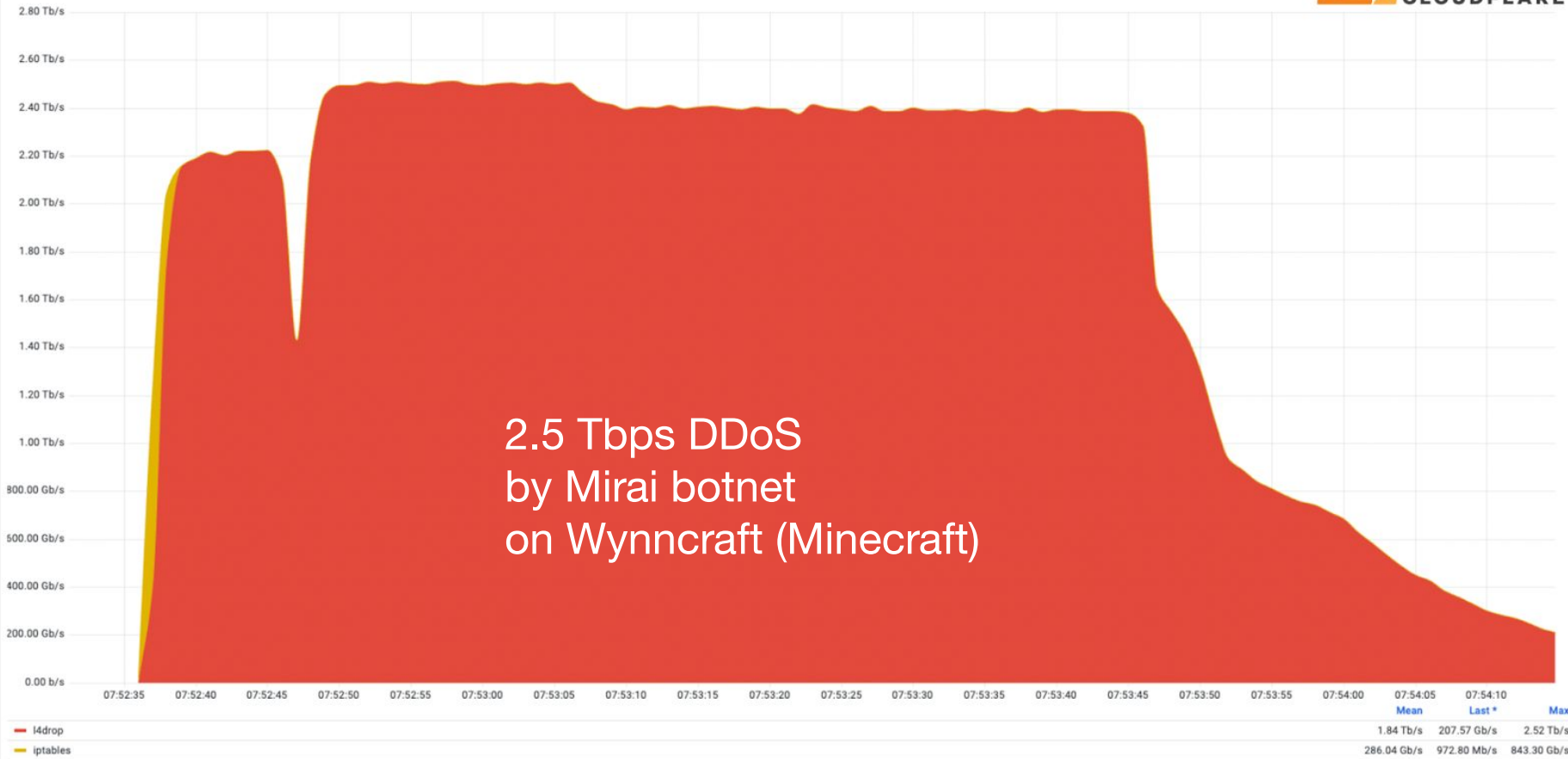


Network-Layer DDoS Attacks - QoQ change in duration



CLOUDFLARE

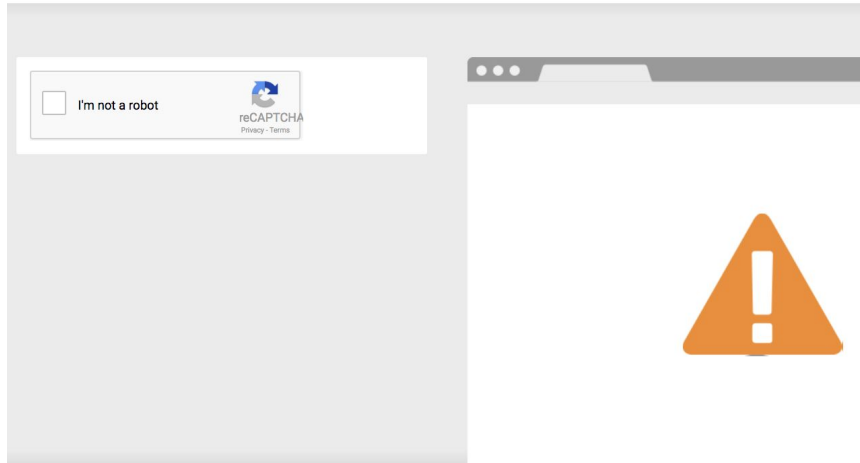




Seen This Before?

One more step

Please complete the security check to access www.jamesaskham.us



Why do I have to complete a CAPTCHA?

What can I do to prevent this in the future?



Checking your browser before accessing cloudflare.com.

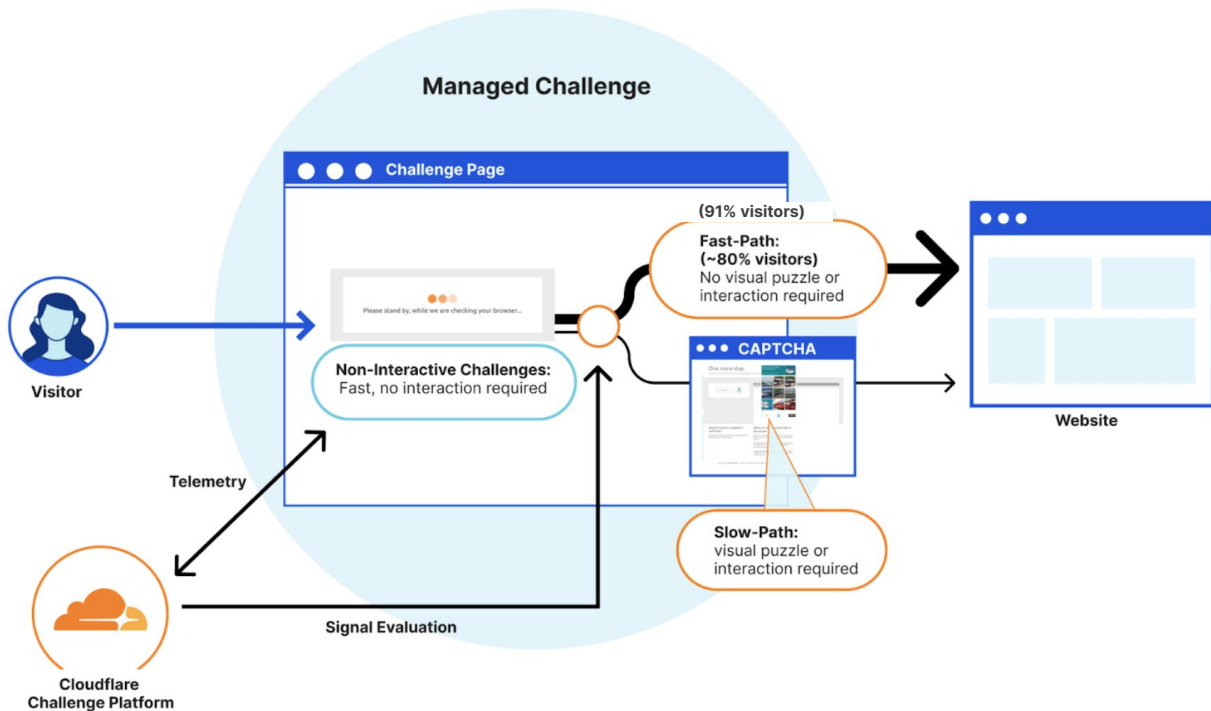
This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...

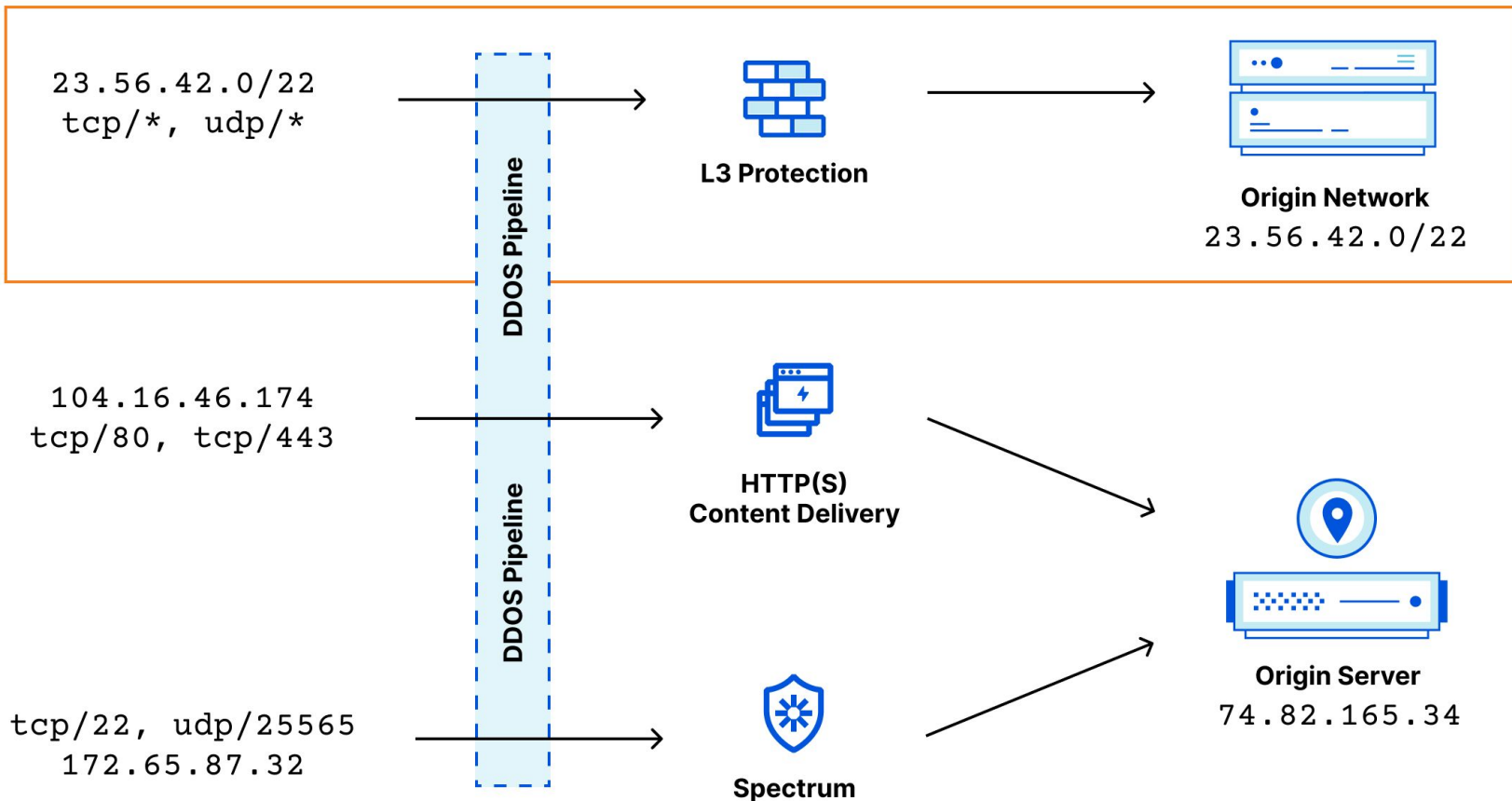
[DDoS protection by Cloudflare](#)

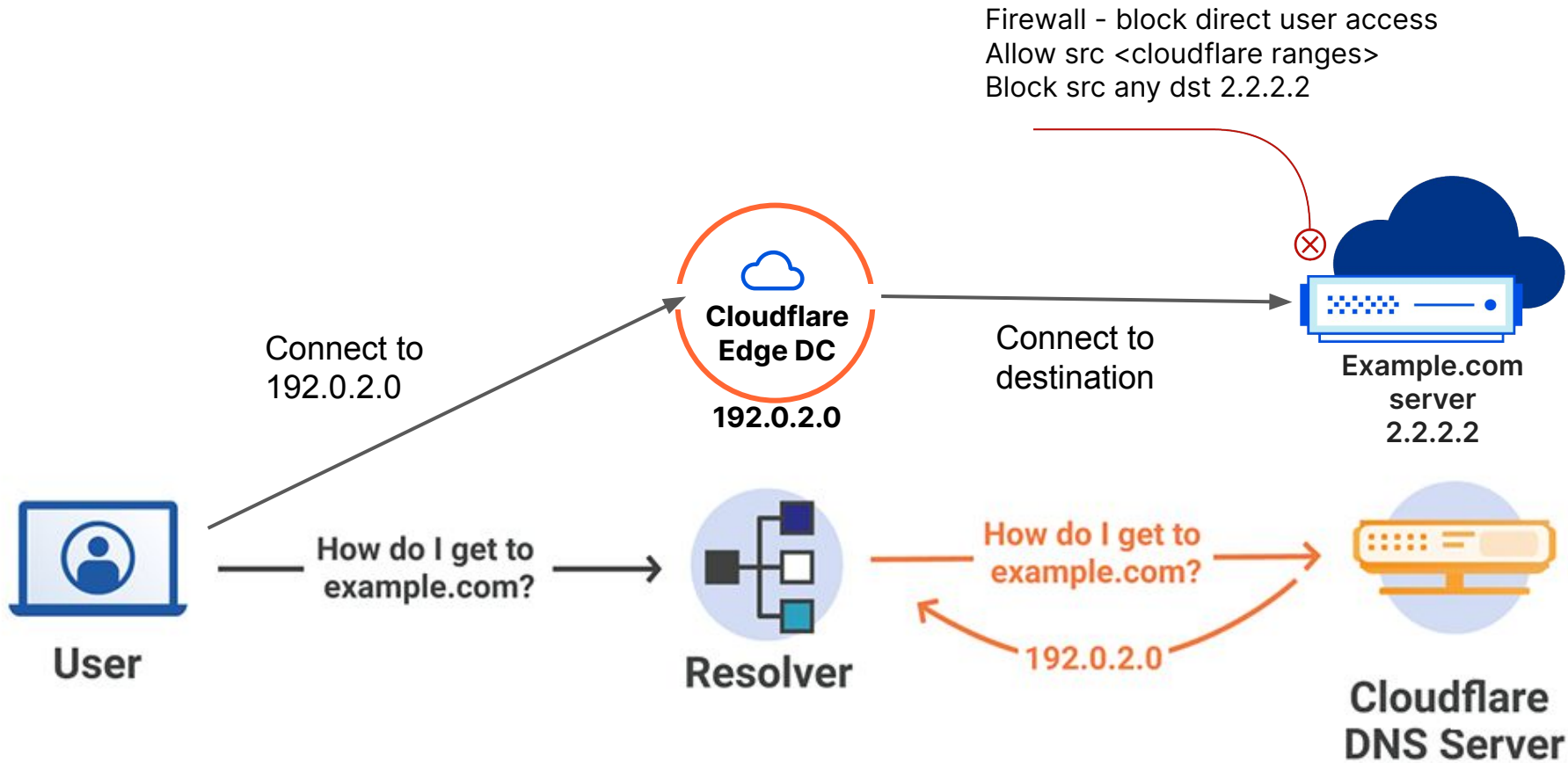
Ray ID: 418704044bc4818a

Managed Challenge to replace CAPTCHAs

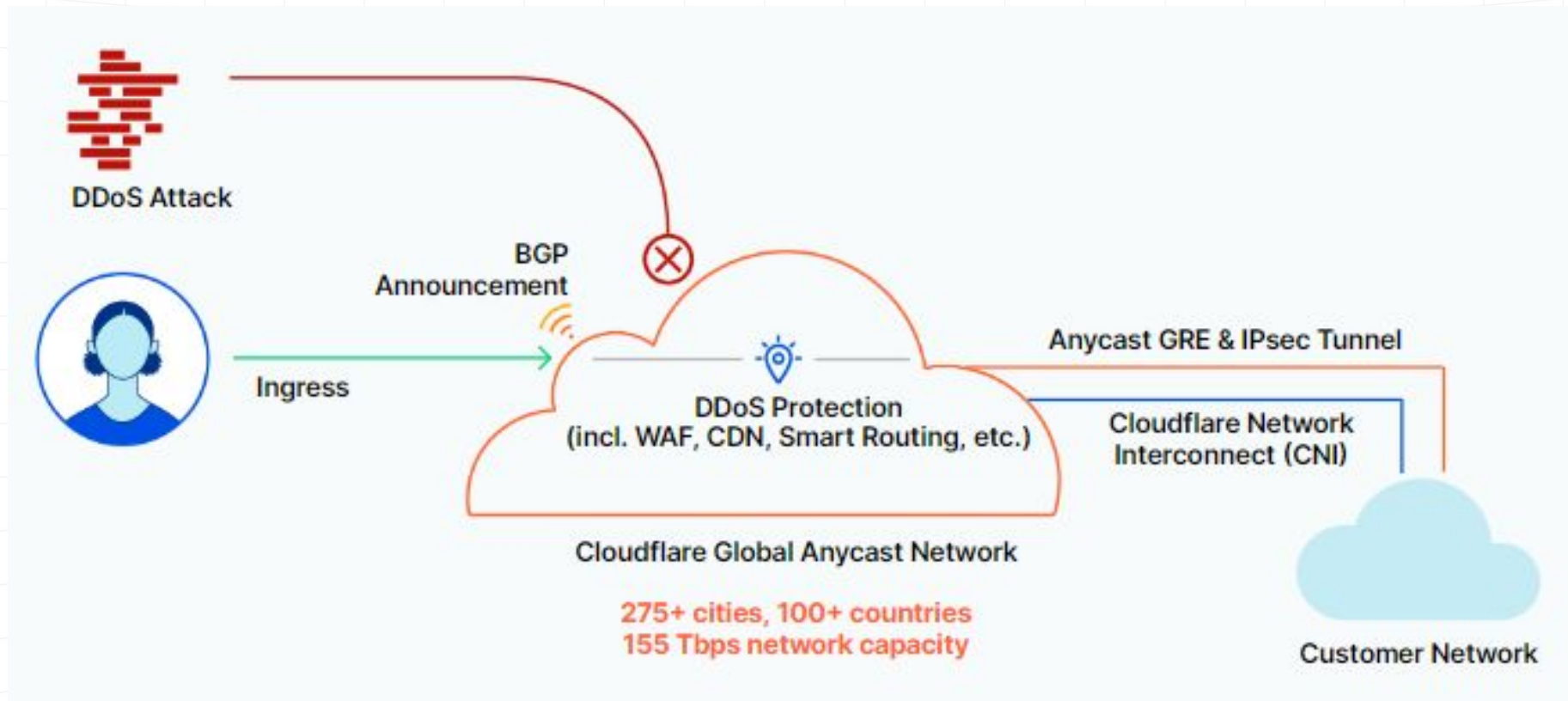


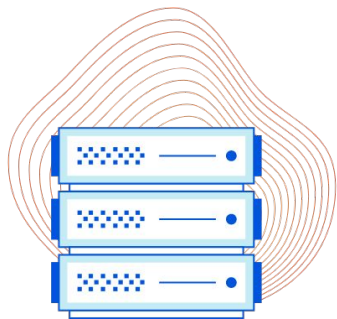
How exactly do we integrate?





Network with built-in DDoS Protection

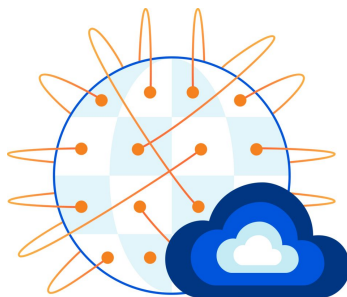




Magic Transit

Network-layer DDoS Protection as-a-service

DDoS protection for entire IP subnets across on-premise, cloud-hosted, and hybrid networks. The Cloudflare network advertises your IP address space via BGP to accept, process and accelerate traffic destined for your network



Magic WAN

WAN-as-a-service

Replace legacy WAN architectures such as MPLS. Securely connect any traffic source - data centers, offices, devices, cloud properties - to Cloudflare's network and configure routing policies to get the bits where they need to go



Magic Firewall

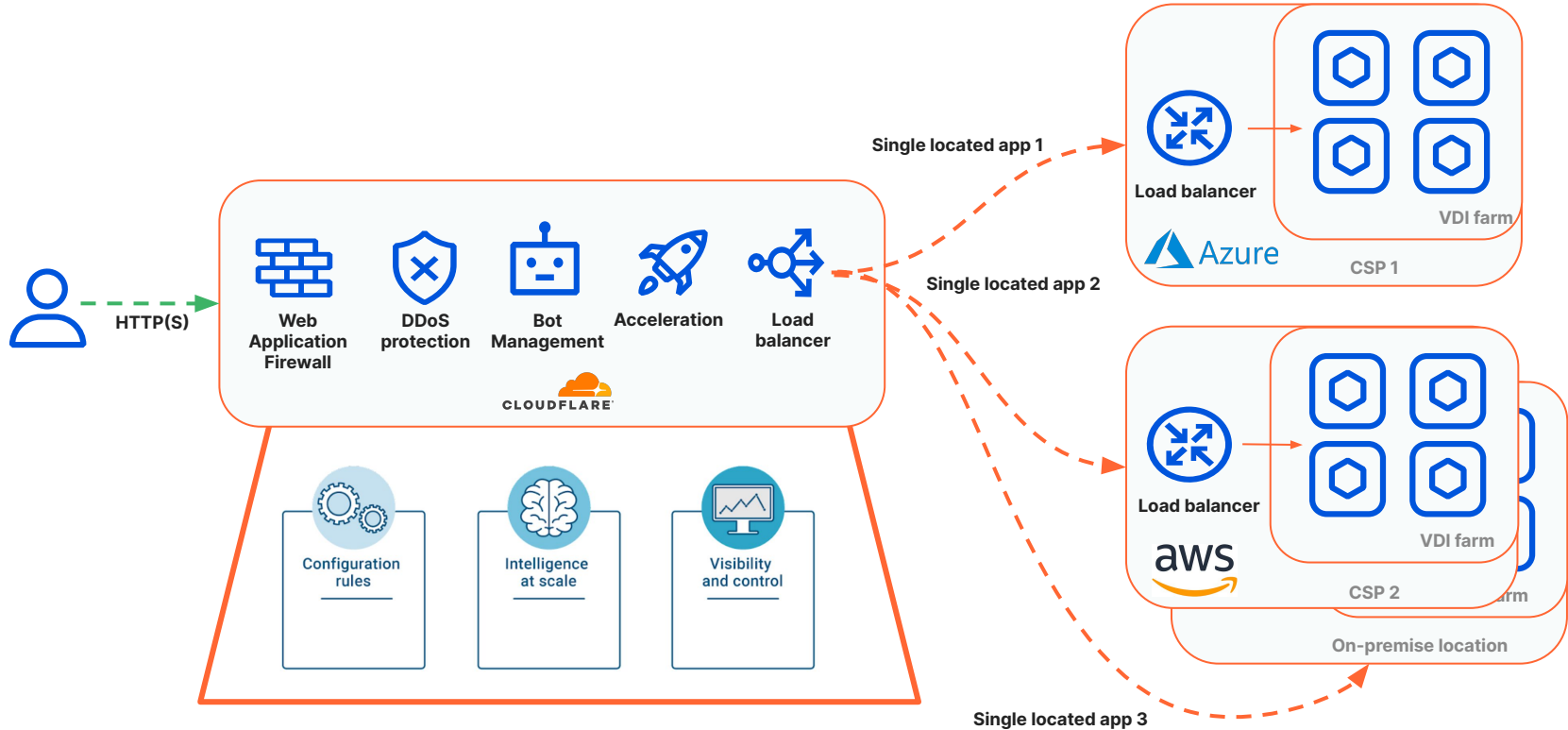
Network Firewall-as-a-service

Enforce centrally-managed firewall policies at the edge, across traffic to/from any entity within your network. Integrates seamlessly with Magic Transit and Magic WAN

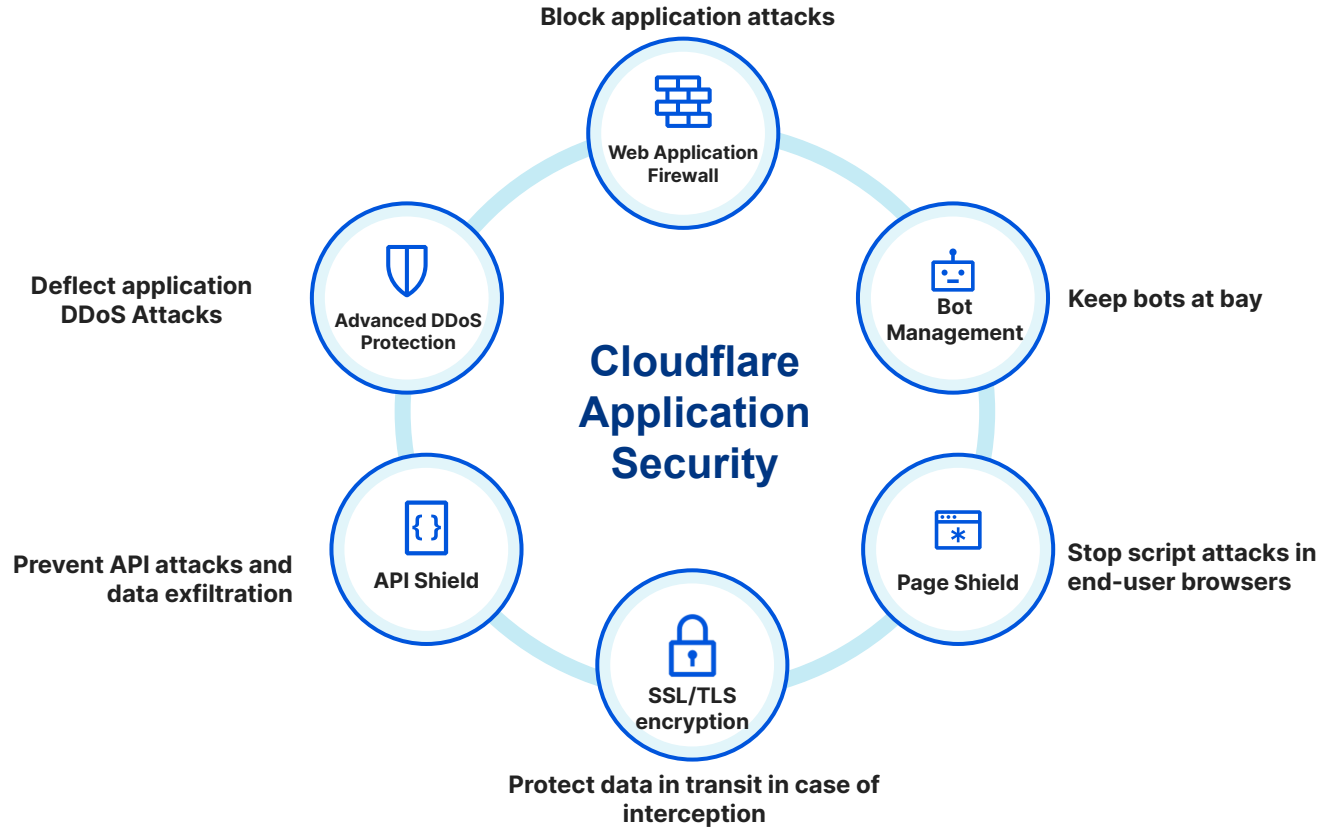
Securing Your Web Business



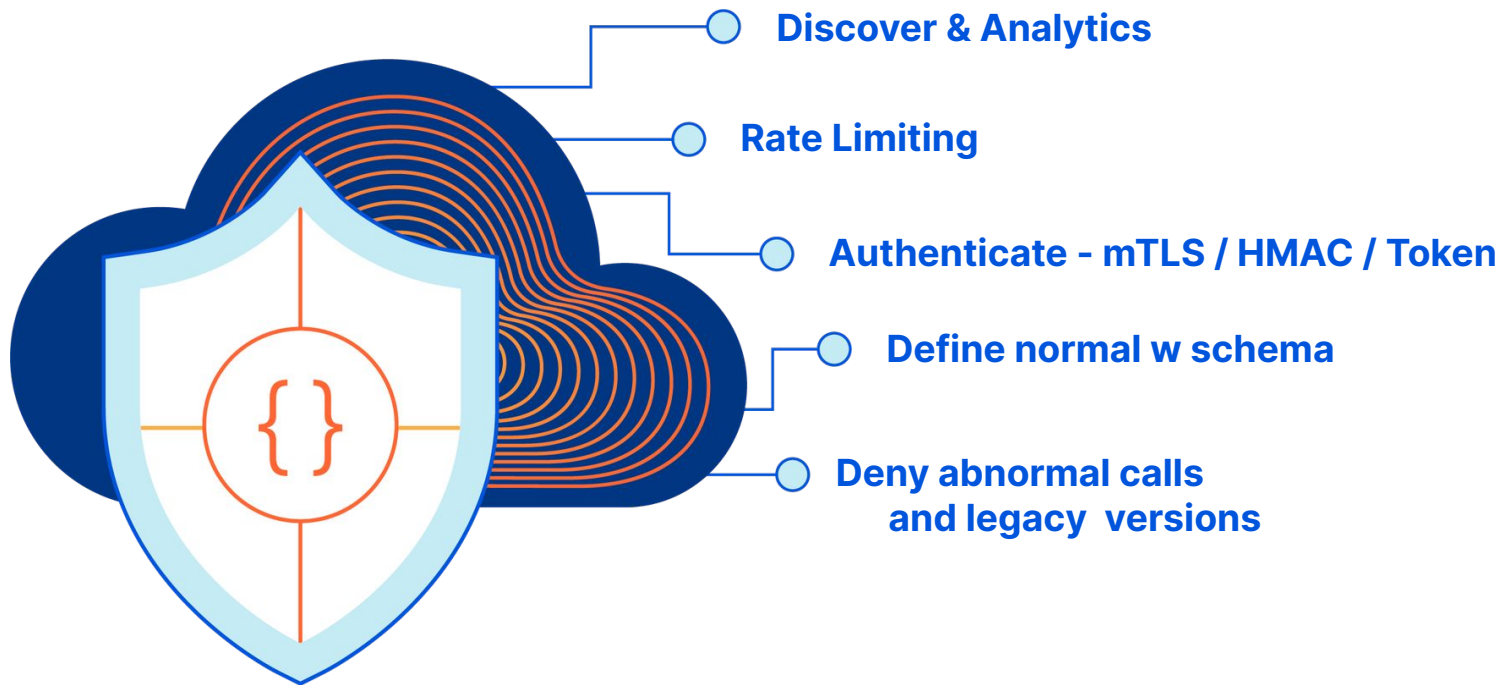
Gentleman Package aka CORE



Application Security

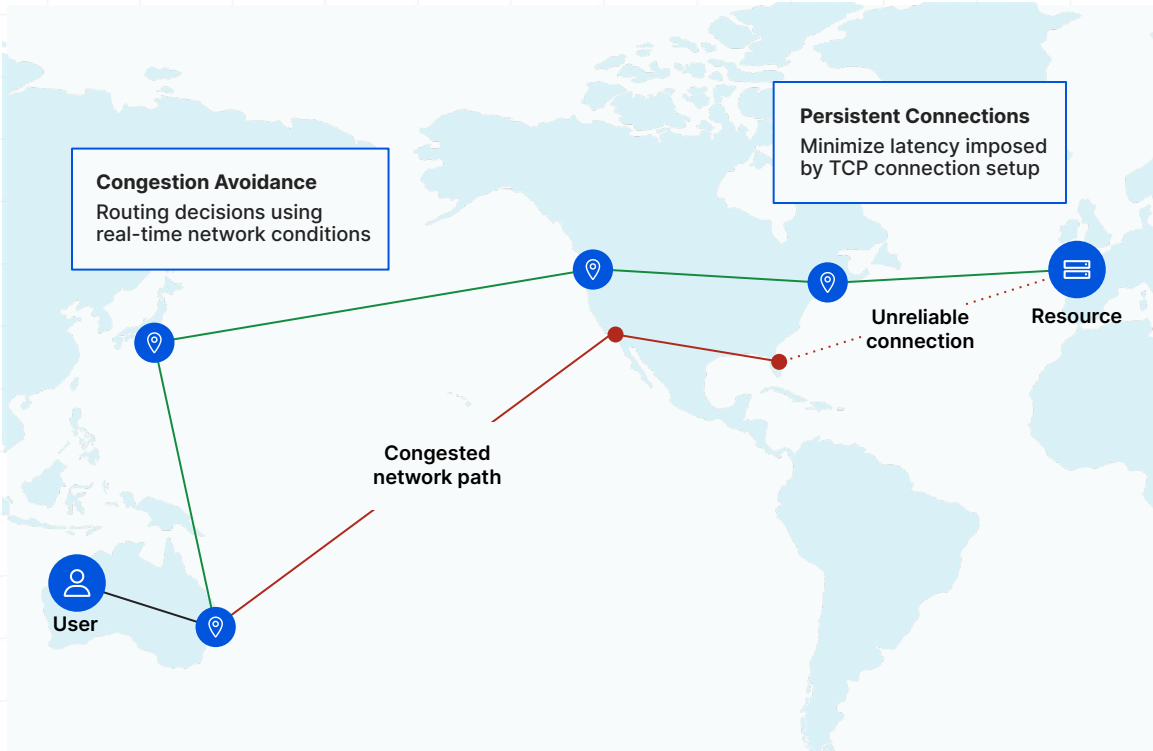


Protect your APIs



Argo Smart Routing

Faster and more reliable Internet



[network speed & scale]

39%

faster web app performance¹
using intelligence from
36M+ HTTP requests/s

[cost-efficient innovation]

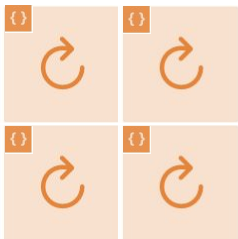
17%

shorter RTT for TCP traffic¹
using intelligence from
39K+ new connections/s

[1] on average

Workers - Serverless workloads

Closer to users without egress fees

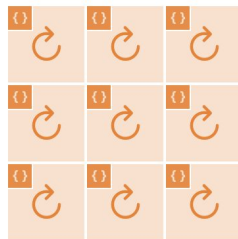


Generation One

No metal box;
Virtual machines

Hours to deploy

OS, runtime, libraries
and application

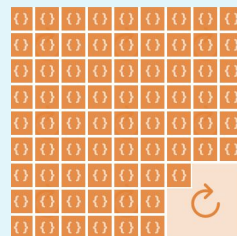


Generation Two

No virtual machine;
Containers/Kubernetes

Minutes to deploy

Runtime, all libraries,
and applications



Generation Three

No containers;
Serverless V8 isolates

Seconds to deploy

Uncommon libraries
and applications

5.4x

Faster product dev time
than older generations

10x

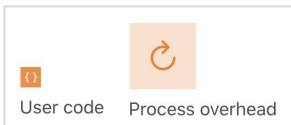
More cost-efficient than
similar serverless platforms

0ms

Cold starts (no container
runtime) for auto-scaling

<500ms

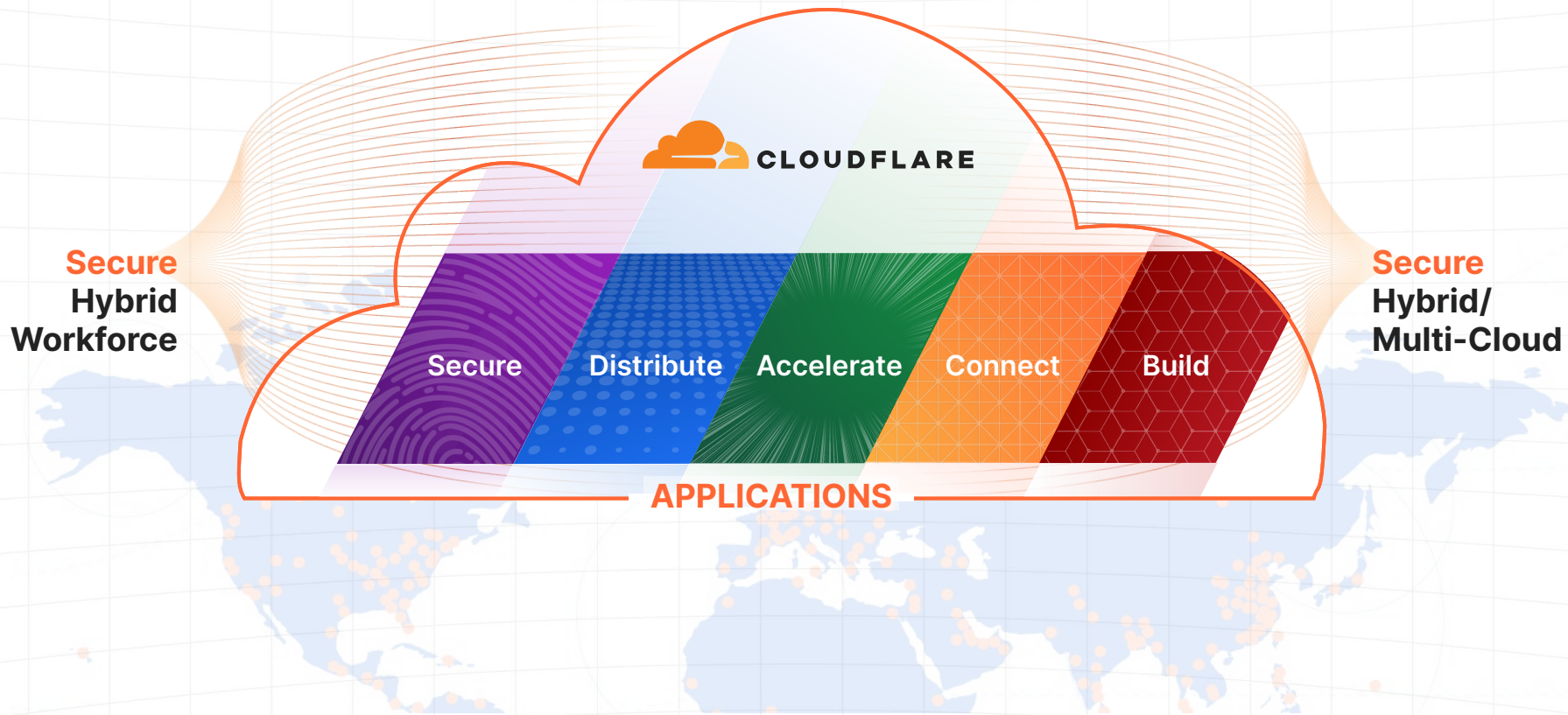
Global policy change
and threat intel updates



What else?

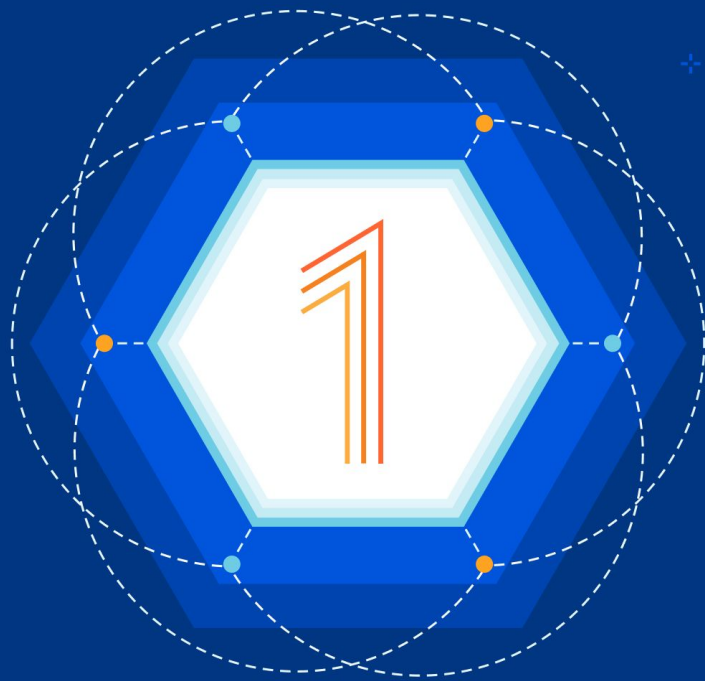


- CACHE** - downsize servers and uplink up to 3X
- ZARAZ** - improve SEO and latency
- BOTS** - serve only humans and trick competitors
- R2** - replace S3 quickly when sick of egress fees
- STORAGE** - KV pairs or D2 database
- STREAM** - we host video on-demand and LIVE
- IMAGES** - launch another “Instagram” in days
- WAITING ROOM** - ready for any seasonal spikes



Thanks Heaps

m@cloudflare.com

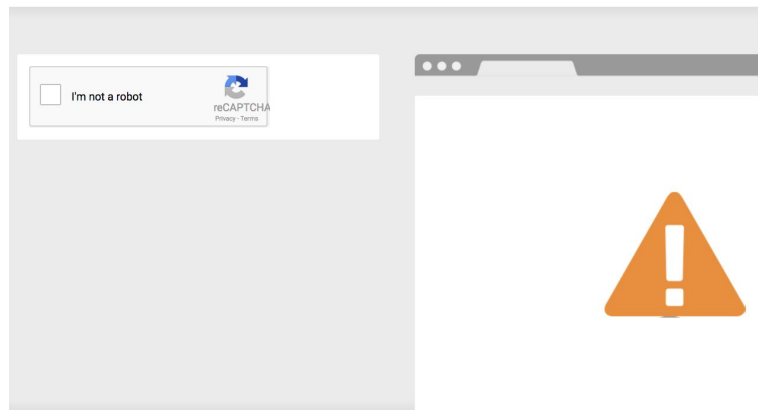


Captcha Challenge

- IP Firewall CAPTCHA same presentation as IP Reputation, WAF and Country challenge pages.
- Ensures visitor is not a bot.
- First CAPTCHA presents picture challenge.
- Page is logged as a 403 in Status Codes.
- Counts as 'Cached Bandwidth' and a 'Cached Request'
- Can generate a CAPTCHA with 'cf-setopt-chl' header value of '1'.

One more step

Please complete the security check to access www.jamesaskham.us



Why do I have to complete a CAPTCHA?

What can I do to prevent this in the future?

JavaScript Challenge

- Same in presentation as the I'm Under Attack Mode (IUAM).
- Prevents bots from accessing a webpage.
- Validates real browser user without human interaction.
- Counts as a 503 response, cached bandwidth, cached request
Browser Challenged in Analytics.
- Also referred to as an **Interstitial Page**
- Rate Limiting product is becoming a more popular alternative but requires more configuration.
- Can be forced with 'cf-setopt-chljs' header with a value of '1'.



Checking your browser before accessing cloudflare.com.

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...

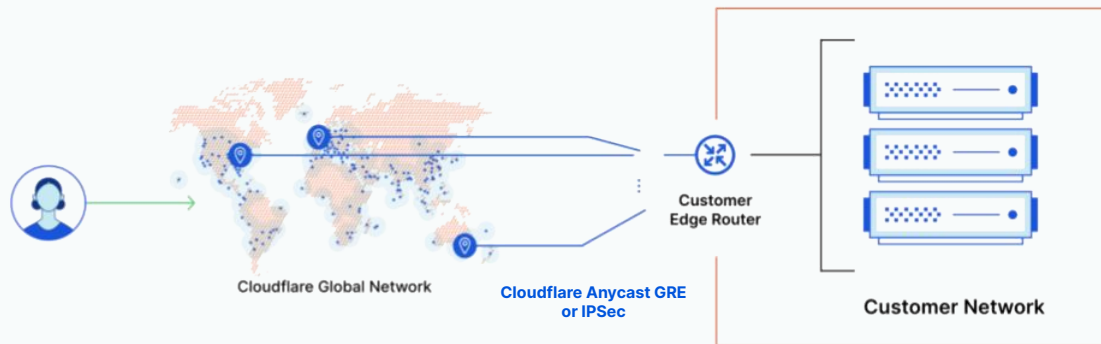
[DDoS protection by Cloudflare](#)
Ray ID: 418704044bc4818a

Why Zero Trust at all?

Problem	Band-aids	Cloudflare One
Teams lack visibility into how users access their data	→ Backhaul all traffic through centralized hardware	→ Log and audit every request and connection close to the user on Cloudflare's network
Every user of a SaaS application becomes a vector for data loss	→ Build different rules in each app or deal with apps that lack controls	→ Apply granular RBAC control for any application in one place
Applications that are Internet-facing can leak data	→ Point solutions that require constant configuration	→ Scan all responses leaving your apps without slowing down*
Every server and device can potentially leak sensitive data	→ Backhaul all traffic through centralized hardware	→ Scan all traffic close to the user or server and control rules in a single location*

* Launching soon

Anycast Routing for L3/L4/L7 Traffic



Connect via GRE or IPsec

- The tunnel is bound to an IP address, not a specific device or data center location
- GRE provides easy connectivity from any network device
- IPsec provides privacy and easy integration with public cloud VPCs

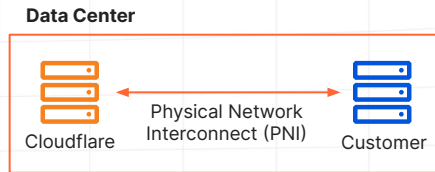
Set it & forget it

- Health checks from all Cloudflare data centers used to route traffic over healthy tunnels
- ECMP-based load balancing (set weights & priorities for tunnels)

Customers have multiple options to connect to the Cloudflare network

- **Layer 1 - Physical Network Interconnect (PNI)**

- Direct connection to Cloudflare routers
- Available in over 250+ Cloudflare cities



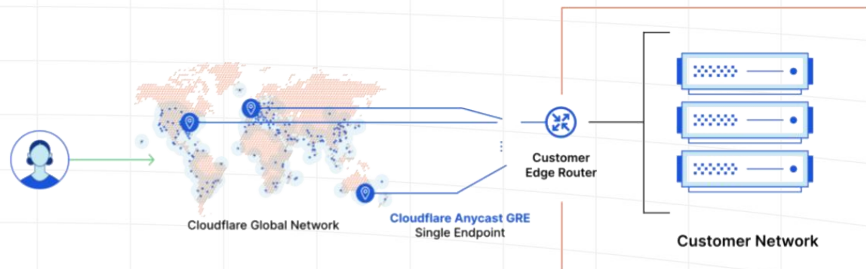
- **Layer 2 — Cloudflare Network Interconnect (CNI)**

- Use an intermediary *network fabric* partner in between your network and Cloudflare
- Available in over +1,600 data centers: [Equinix, Megaport, PacketFabric, Console Connect, Coresite and Epsilon]



- **Internet (Anycast GRE or IPsec Tunnel)**

- Available in any location with an Internet connection
- Fast setup and no single point of failure with redundant Anycast GRE or IPsec tunnels



The Cloudflare application security portfolio

Cloudflare keeps applications and APIs secure and productive, thwarts DDoS attacks, keeps bots at bay, detects anomalies and malicious payloads, encrypts data in motion, all while monitoring for browser supply chain attacks.



Integrated Management & Analytics



Application DDoS

Block L7 DDoS attacks



WAF w/ advanced rate limiting

Stop attacks, abuse and exploits



Bot Management

Stop bot traffic



API Gateway

API security and management



Page Shield

Stop client-side attacks



TLS/SSL

Data security

Cloudflare Security Center

Attack surface management

The Cloudflare Bot Difference



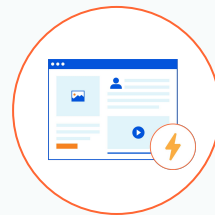
No tradeoffs

- No code required
- One integrated security suite
- Latency < **0.3 milliseconds**
- No SDK required



More data & smarter models

- Over 1 trillion bot requests every day
- We learn from roughly **500,000 self-serve** bot customers
- 5 advanced detection engines



Immediately actionable

- **Onboard in minutes**; block while under attack
- Retroactive analytics
- Automatically integrated into WAF
- Intuitive reporting in the Cloudflare Dashboard.

Key detections

Machine Learning

Machine Learning

Trained on all:

- False positives
- False negatives

New model inputs & features

Anomaly Detection

Site-Specific Anomaly Detection

Better:

- Request clustering
- Baseline of traffic

“Booster pack” for Bot Management

JavaScript Detections

JavaScript Detections

Improved:

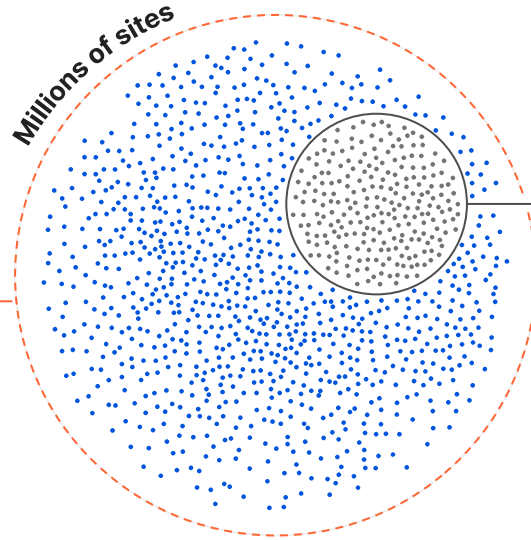
- Speed
- Headless browser detection

Feedback into ML engine



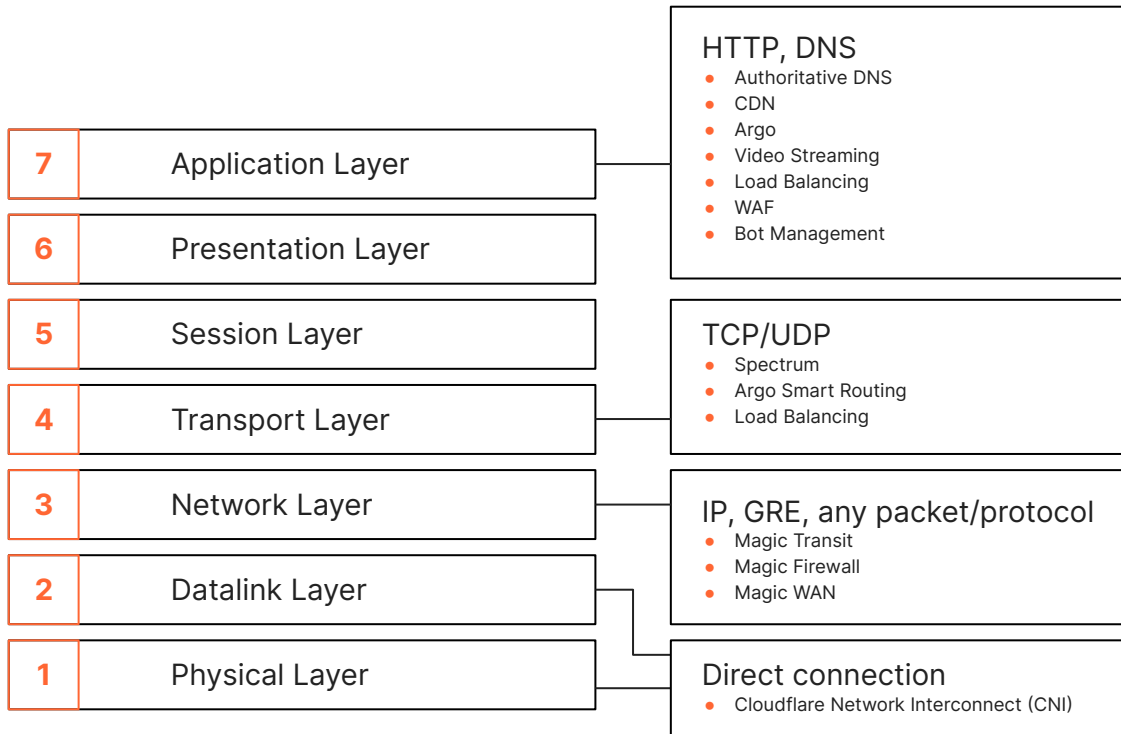
The Cloudflare Difference

Unlike our competitors, we train detections on all data— **for our entire customer base**



Bot Management customers

Cloudflare services across the OSI stack



Cloudflare WAF

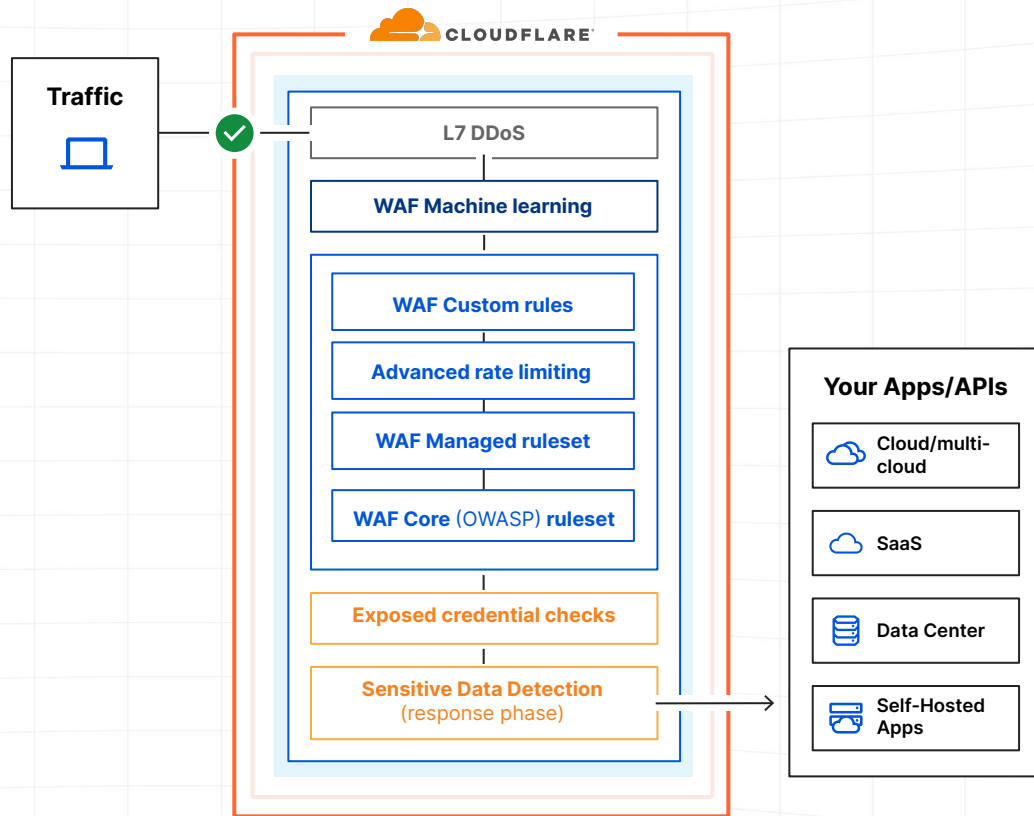
World-class protection for every request

Faster protection with new managed rules to block emerging exploits.

Layered rulesets to stop attacks along with machine learning models to stop bypasses.

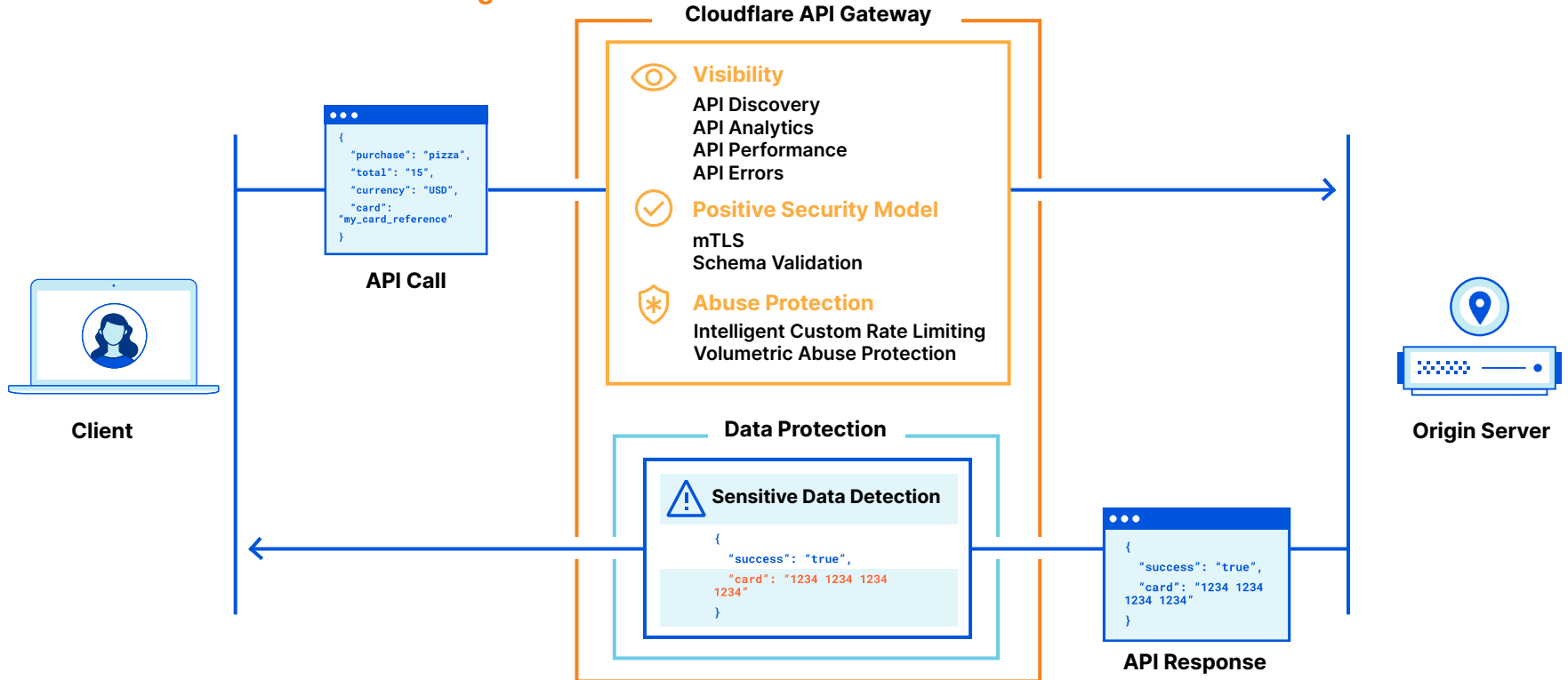
Powerfully simple detections for stolen credentials and data exfiltration.

API-first advanced rate limiting

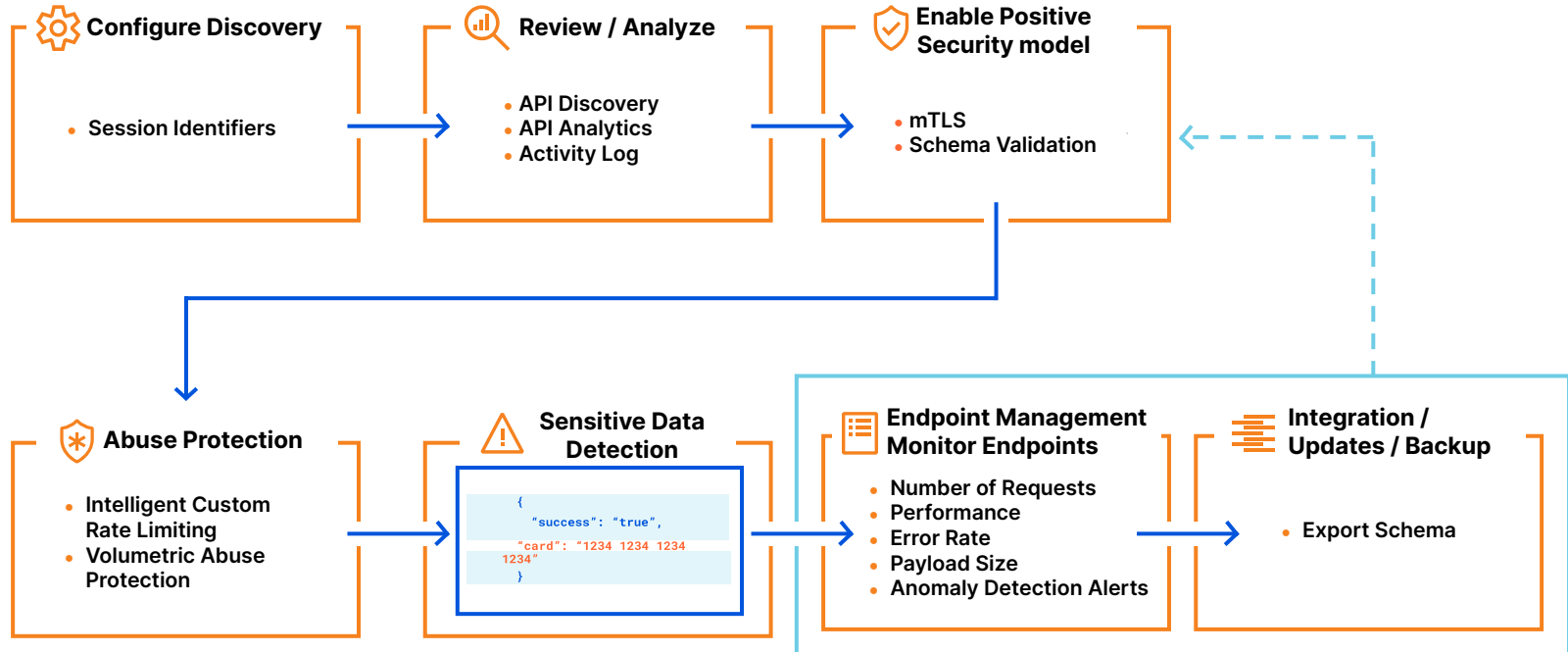


Cloudflare API Gateway Capabilities and Traffic Flow

All API traffic is secured at the edge!



Cloudflare API Gateway provides visibility via API discovery and analytics, provides capabilities to manage API endpoints, implements a positive security model, and prevents API abuse.



API Shield defense-in-depth



L3 & L7 DDoS

Stop all volumetric DDoS attacks at network and application layers.



API Discovery and Visibility

Ongoing visibility into API endpoint estate.



Strong Authentication

Authenticate mobile and IoT with mTLS while confirming credentials are not compromised.



Positive API security model

Positive security via schema validation to block everything except traffic that conforms to schema.



Anomaly Detection

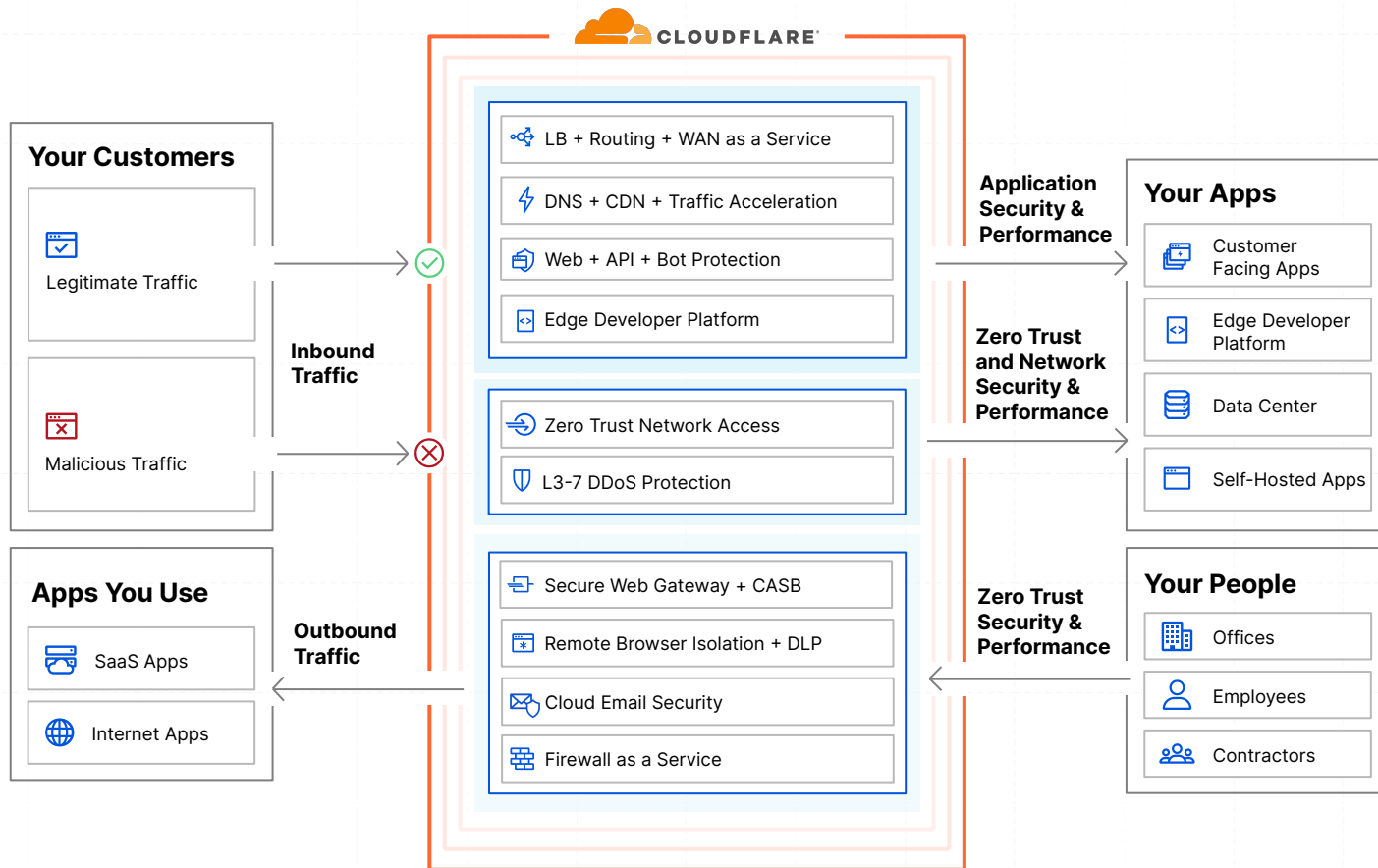
Stop API abuse with advanced rate limiting and blocking of volumetric anomalies including for bots and mobile API traffic



Sensitive Data Detection

Prevent sensitive data from leaking via APIs

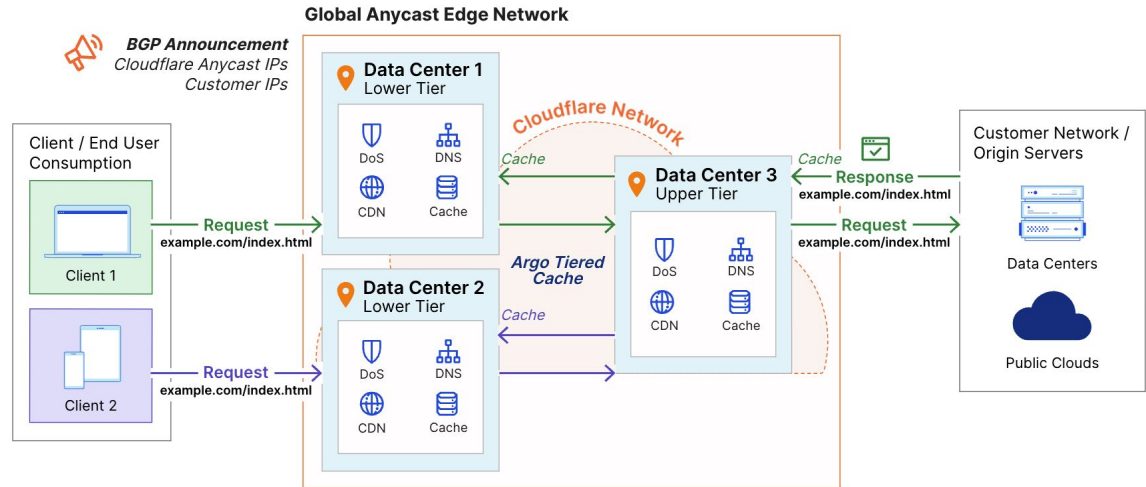
Visualizing ingress and egress traffic with Cloudflare



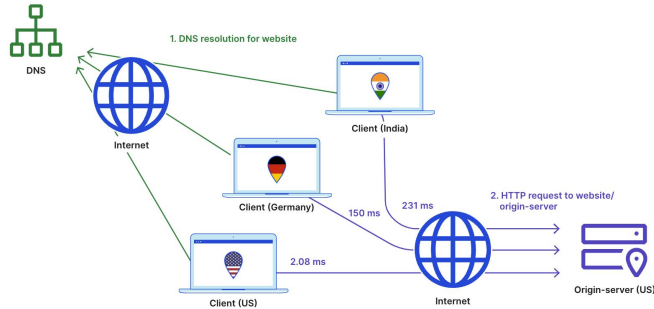
Cloudflare CDN Reference Architecture

[Download](https://www.cloudflare.com/resource-hub/) from <https://www.cloudflare.com/resource-hub/>

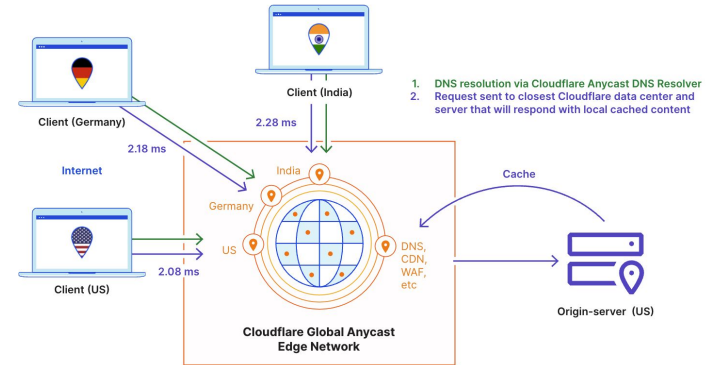
- Cloudflare CDN Benefits and Advantages
- Enhancements with Argo Features
- Architecture/Design and Traffic Flows
- Tiered Cache Topologies and Recommendations



Before Cloudflare CDN



After Cloudflare CDN



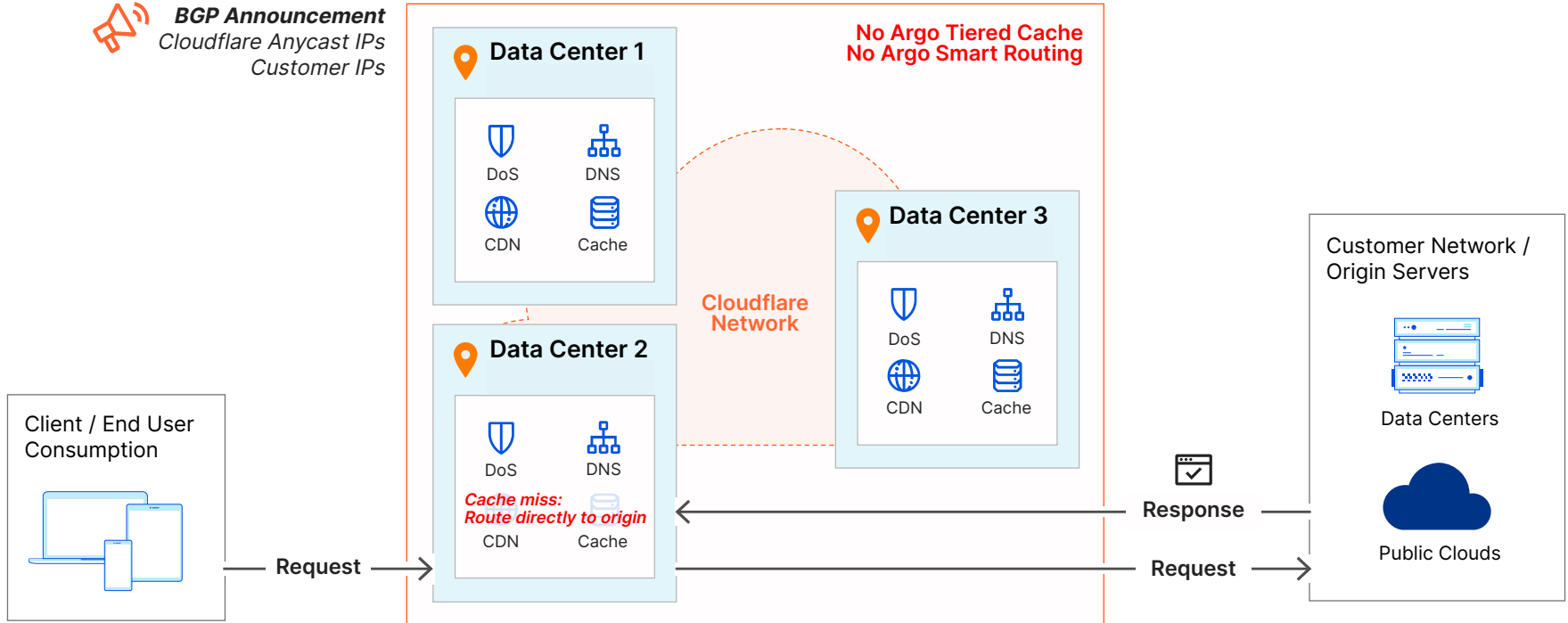
- **Scale, resiliency, and performance** - one global network with every service running on every server in every Cloudflare data center; Edge nodes able to respond with cached content quickly
- **Hardened Anycast network** - decreased latency while improving network resiliency, higher availability, and increased security due to larger surface area for absorbing both legitimate traffic loads and DDoS attacks
- **Enhanced CDN Solution with Argo Smart Routing and Tiered Cache**
- **Easily enable additional services** - Cloudflare provides a host of performance, security, and reliability services including DNS, DDoS protection, and WAF, which can be easily enabled and uses the same edge architecture

No Argo Tiered Cache Enabled and No Smart Routing Enabled

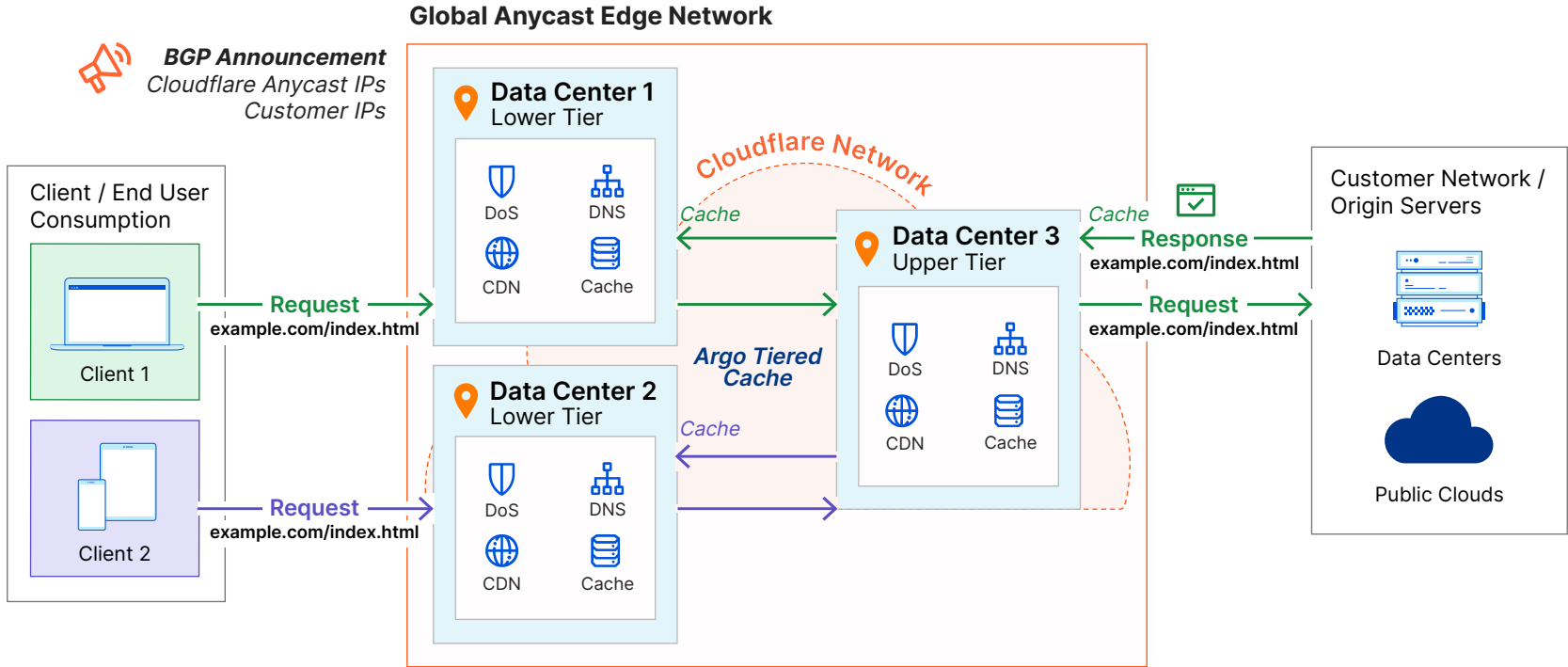
Global Anycast Edge Network



BGP Announcement
Cloudflare Anycast IPs
Customer IPs



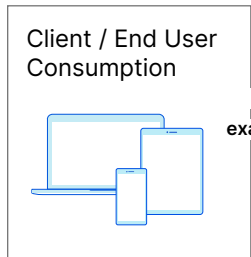
Argo Tiered Cache Enabled with Smart Tiered Cache Topology



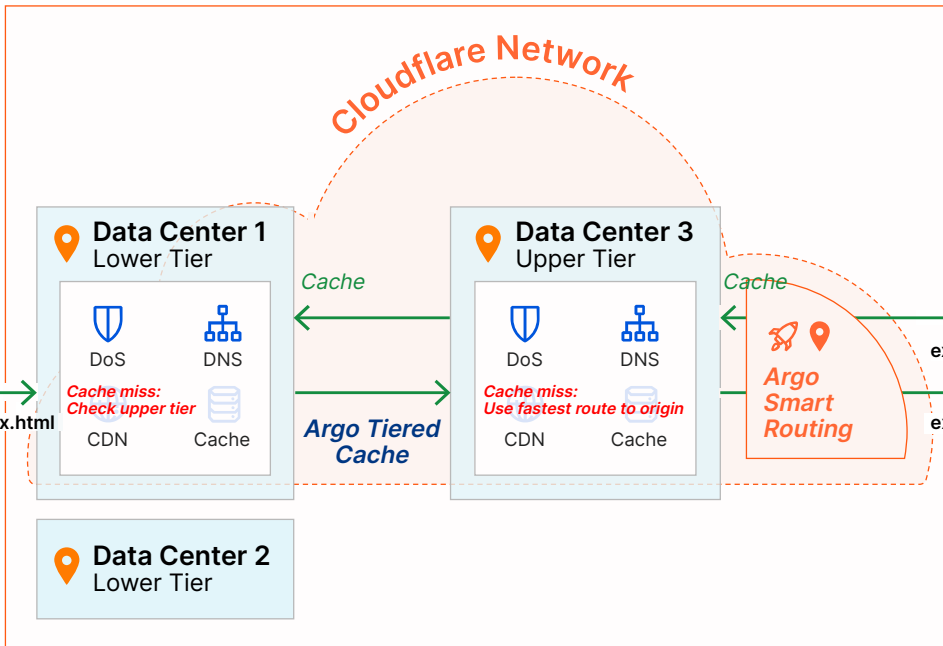
Global Anycast Edge Network



BGP Announcement
Cloudflare Anycast IPs
Customer IPs



Request
example.com/index.html



Response
example.com/index.html

Request
example.com/index.html

