

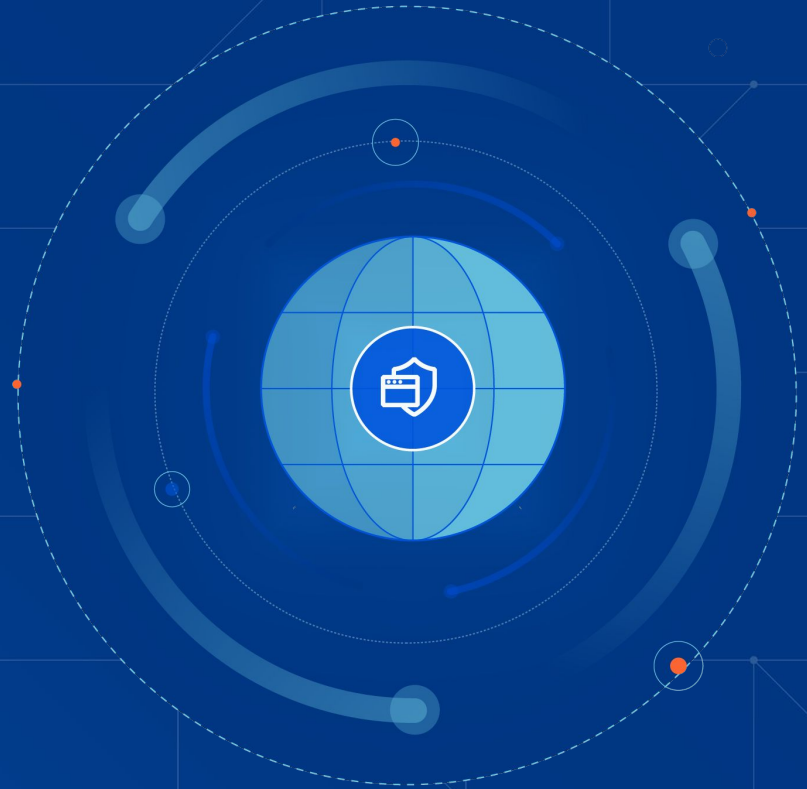
**We are helping build
a better Internet.**





Cloudflare on Tour

Houten – 8 Februari 2023



WIE ZIJN WIJ?



Jan van Leuken
Enterprise Account Manager
06-15835064
jvanleuken@cloudflare.com



Michiel Appelman
Sr. Solutions Engineer – Cloudflare
michiel.cloud/flare



Introduction



Trends (Jan)



Cloudflare Intro (Jan)



Zero Trust Deep-dive (Michiel)



Lunch 12:00 - 13:00 - all in restaurant.





Trends



Welcome to ChatGPT

in your OpenAI account



chat.openai.com



Hi



Hello! How can I help you today? Is there something you need help with or would like to learn more about? I'm here to assist you with any questions you may have.



chat.openai.com

Checking if the site connection is secure



Verify you are human







Forwarded messages

KillMilk 28/01/23

Мед учреждения Нидерланды :

<http://www.umcutrecht.nl/> -- Университетский медицинский центр
Утрехта

<https://www.lumc.nl/> -- Университетский медицинский центр
Лейда

<http://www.radboudumc.nl/> -- Медицинский центр университета
Радбуда

<https://www.mumc.nl/> -- Медицинский центр Маастрихтского
университета

<https://www.erasmusmc.nl/en/> -- Медицинский центр Университета
Эразмус

<https://www.catharinaziekenhuis.nl/> -- Катарина Зикенхейс

<https://www.jeroenboschziekenhuis.nl/> -- Больница Йеруна Боша

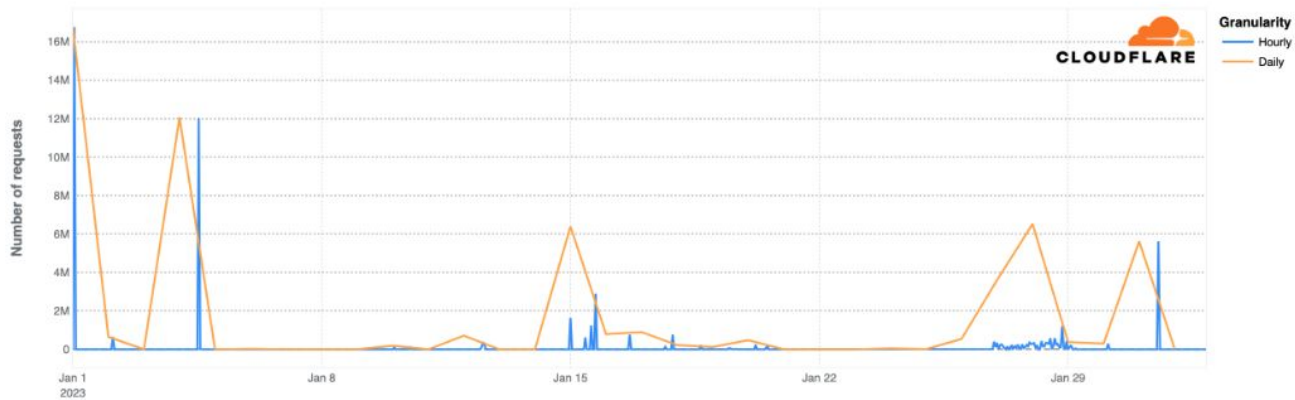
<https://www.mmc.nl/> -- Медицинский центр Максима

<https://www.mst.nl/> -- Medisch Spectrum Twente (MST)

<https://reinierdegraaf.nl/>

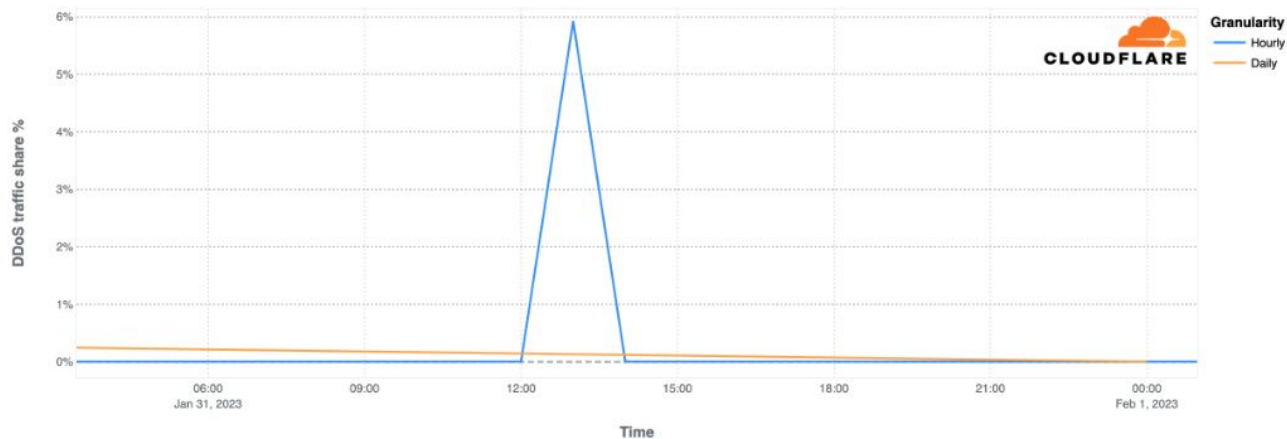
DDoS traffic to Health related industries over time

2023-01-01 00:00:00 - 2023-02-01 21:00:00



DDoS traffic shares to Health related industries over time

2023-01-01 00:00:00 - 2023-02-01 21:00:00





Cloudflare Intro

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

Security

Privacy

Performance

Resilience

Agility



275+

cities in 100+ countries,
including mainland China

30

Data centers in China

11,000+

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

172Tbps

of network edge capacity
and growing

To provide a private, secure, reliable, performant, agile enterprise-grade Internet experience, Cloudflare is everywhere

126B

Daily threats blocked

95%

of world's Internet users
within **50ms** of our network

100%

Uptime **SLA**

This is only possible because we see

~20%

of the Internet traffic







- Overview
- Traffic
- Security & Attacks
- Adoption & Usage
- My Connection
- Domain Rankings
- Outage Center
- Reports
- API

Domain information

TLS

WHOIS

Global

Domain categories

- Search Engines
- Technology

Domain Categorization Feedback

Visitor location

Tracking google.com popularity by location. Popularity & location insights are derived from Cloudflare 1.1.1.1 data



Ranking	Country	Percentage
1	United States of America	
2	Vietnam	
3	Canada	
4	Germany	
5	Brazil	
6	Russia	
7	United Kingdom	
8	Sweden	
9	South Africa	
10	Ukraine	

WHOIS

Registration Information for google.com

Name
MarkMonitor, Inc.

TLS Certificates

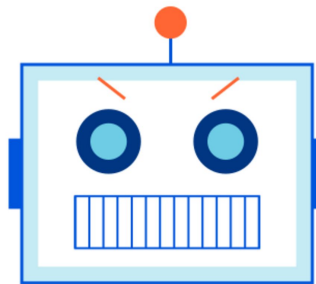
Certificates issued by a trusted Certificate Authority for google.com

Issuing Organizations (0)	Country (C)	Common Name (CN)	# of certificate
---------------------------	-------------	------------------	------------------

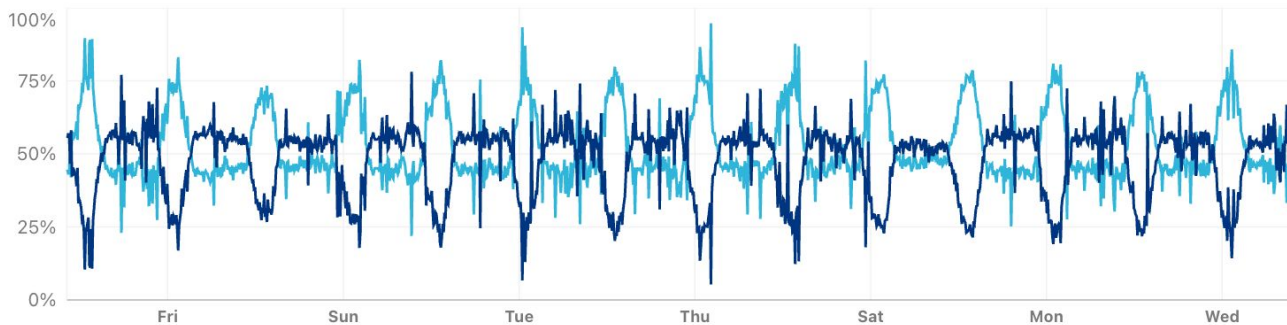
Bots: The good, the bad, and the ugly

● Bot
50%

● Human
50%

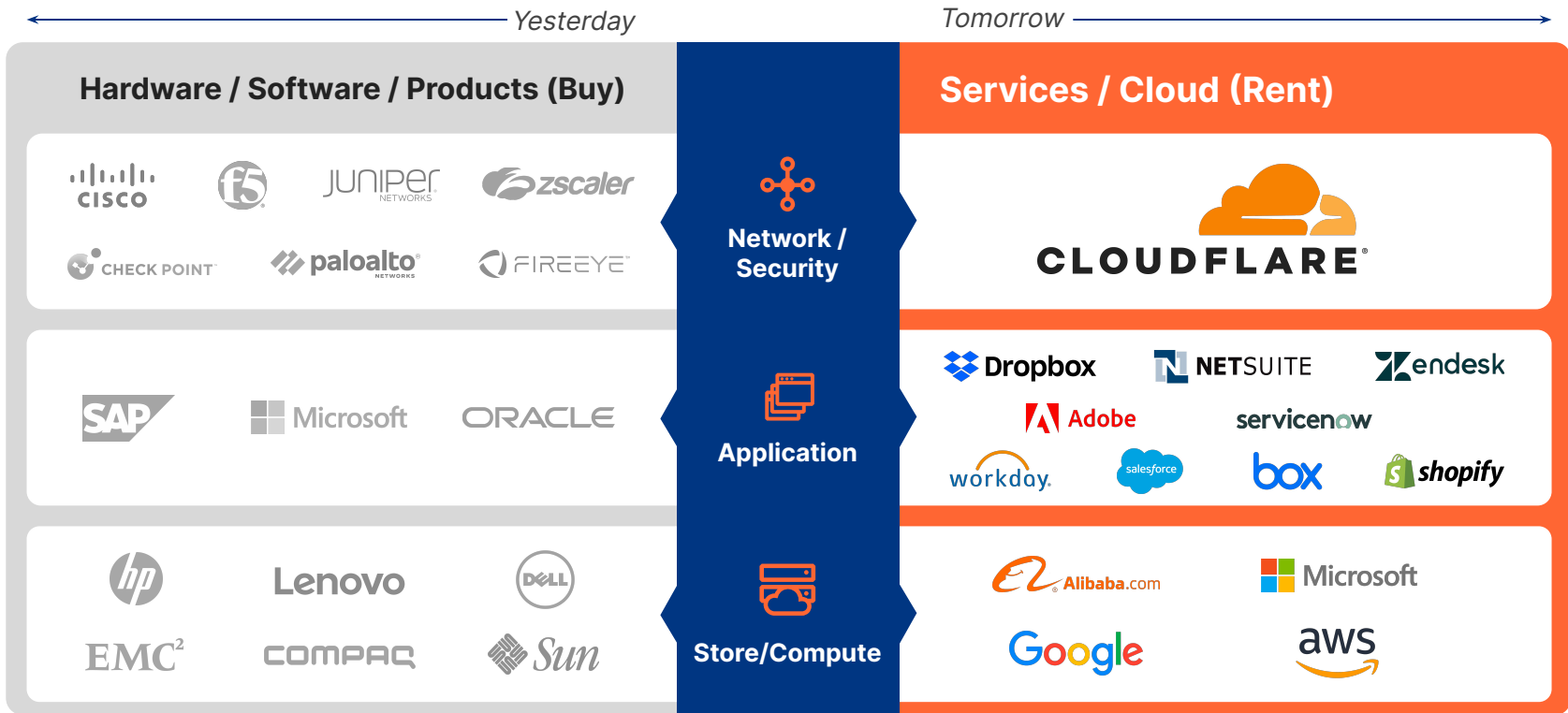


- Credential Stuffing
- Account Takeover
- Inventory Hoarding
- Content Scraping
- Credit Card Stuffing
- Content Spam
- API Abuse



...WON'T GET YOU THERE

Cloudflare was built for what's next



WHAT WE OFFER



Cloudflare Platform



Cloudflare
Zero Trust Services



Cloudflare
Network Services



Cloudflare
Application Services

1

Cloudflare One



Zero Trust Network Access



Secure Web Gateway



Cloud Access Security Broker



Cloud Email Security



Remote Browser Isolation



Data Loss Prevention



WAN-as-a-Service



Firewall-as-a-Service



L3 & L4 DDoS Protection



Network Interconnect



Smart Routing

IDS/IPS ¹



WAF with API Protection



Rate Limiting



Load Balancing



Bot Management



L7 DDoS Protection



CDN and DNS



Cloudflare Edge
Developer Platform



Workers



Pages



R2



Workers KV



Durable Objects



Images



Stream



Cloudflare
Global Network



Compliance/Privacy: FedRAMP, ISO, SOC, PCI, GDPR compliant, Logs & Analytics, Data Localization Suite

Cloudflare

Add site

Support

BurritoBot

Websites

Domain Registration

Analytics & Logs

Security Center

WAF

Turnstile

Magic Transit

Magic Firewall

L3/4 DDoS

Zero Trust

Magic WAN

Area 1

Workers

Workers for Platforms

Pages

R2

<<

Collapse sidebar

https://dash.cloudflare.com

Magic Firewall

Control unwanted traffic by monitoring risks and applying Firewall rules to your entire network on Cloudflare's edge.

Custom rules

IDS

New

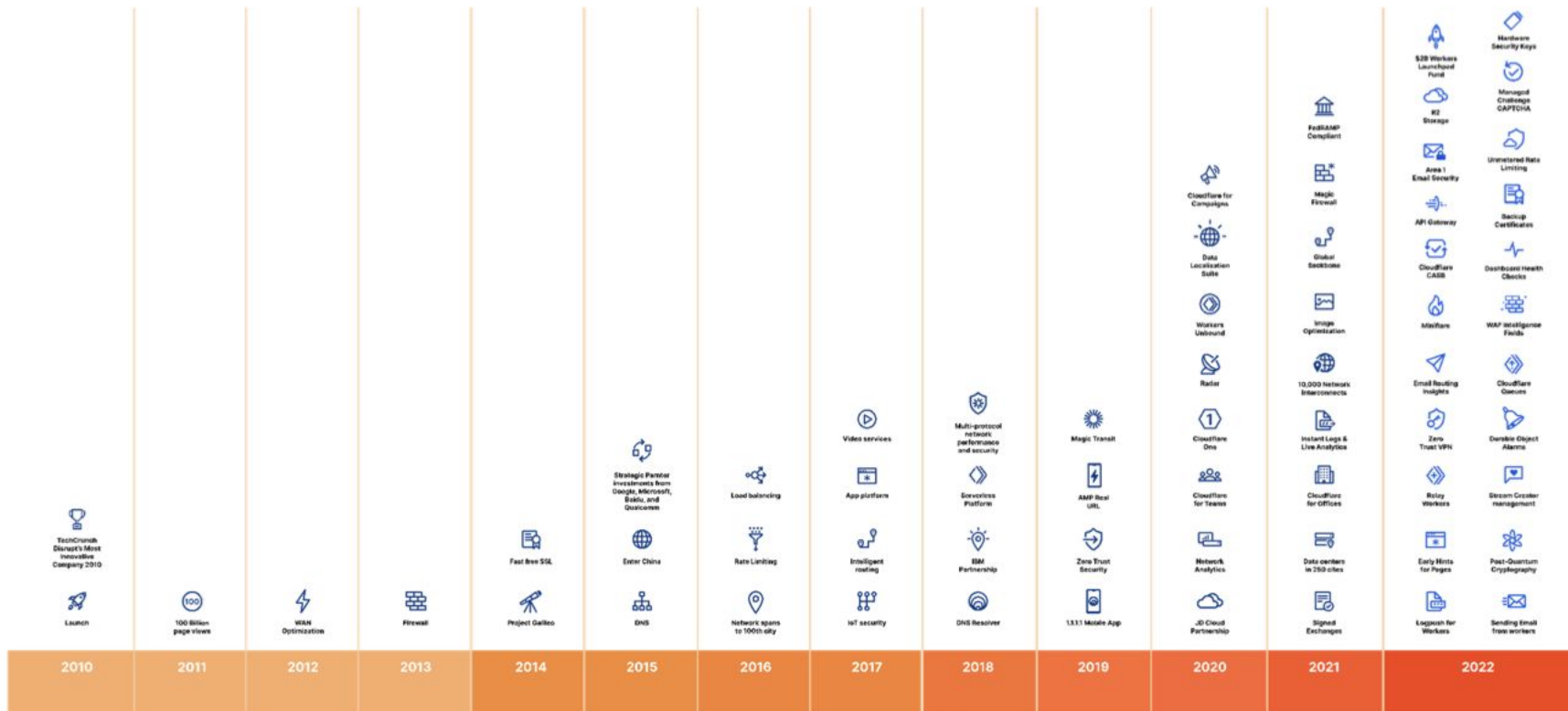
Custom rules

Create and manage security rules to filter the traffic that reaches your network. Traffic is matched in order of the configured rules. For additional information refer to the [developer documentation](#).

Add a rule

	Action	Description	Filter	Activity over the past hour	Enabled
⬆ ⬇ ⬆	Allow	lime Time to Live or; + 1 more ID a614288500...	equals 5 or; + 1 more	Not enough data	Edit Delete
⬆ ⬇ ⬆	Allow	test IP Source Address ID abd4d086d4...	equals 1.1.1.1	Not enough data	Edit Delete
⬆ ⬇ ⬆	Allow	Allow Web Traffic TCP Dst Port ID 26c3b99edd...	is in 80 ...	Not enough data	Edit Delete
⬆ ⬇ ⬆	Allow	some more rules IP Source Address ID e6cad7b220...	equals 1.23.4.5	Not enough data	Edit Delete
⬆ ⬇ ⬆	Block	IP Header Length ID 99a24c7f84...	equals 12	Not enough data	Edit Delete

Move faster with a platform that constantly delivers innovation



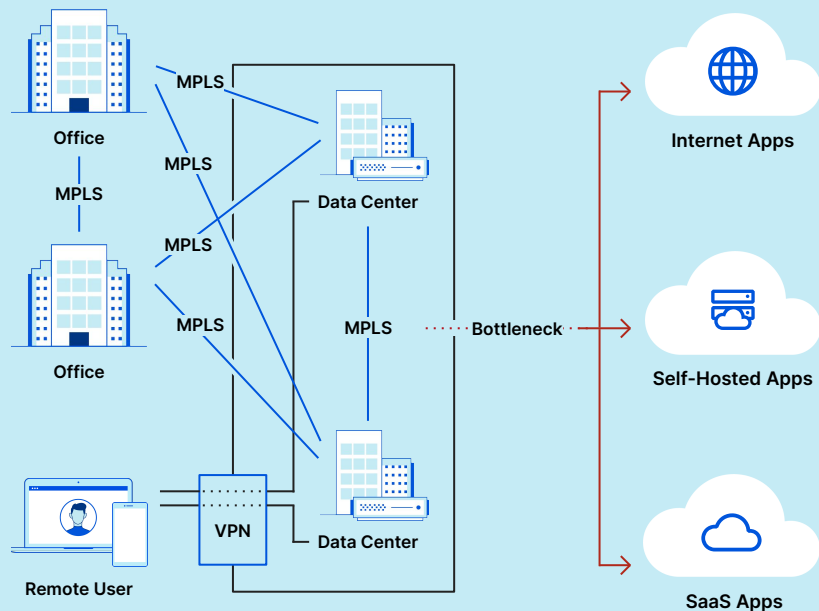




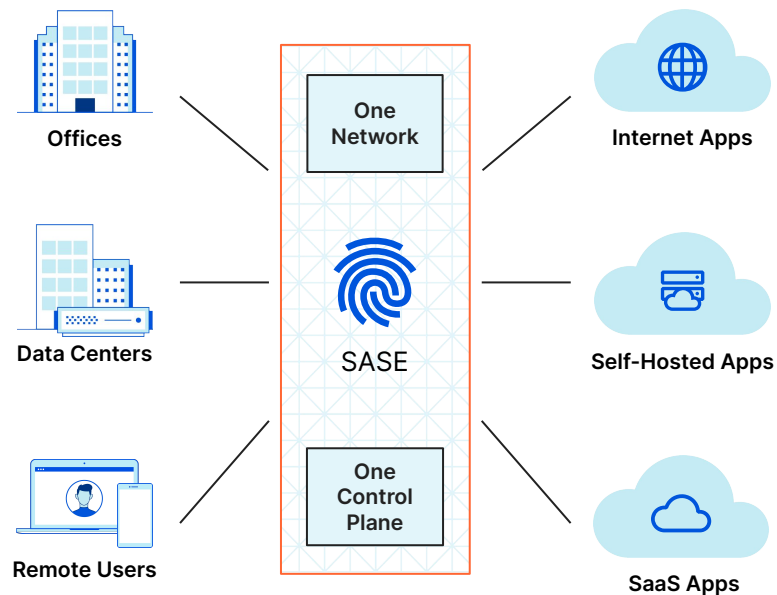
Cloudflare Zero Trust

SASE is an architecture design for Zero Trust

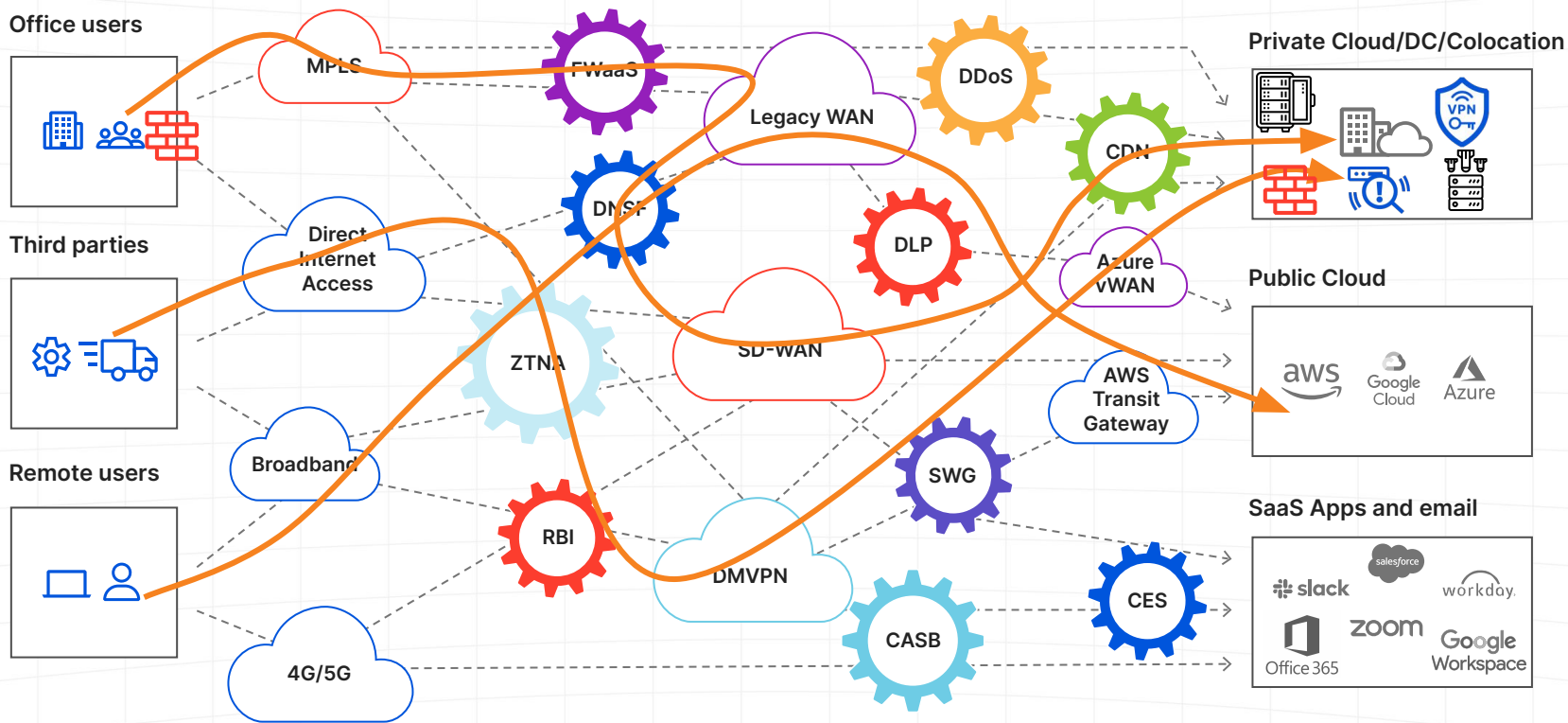
Today's corporate network



Internet-native connectivity with Zero Trust security built-in

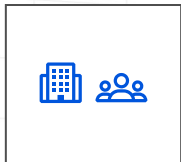


Today's fragmented corporate network



Any-to-any, end-to-end fabric

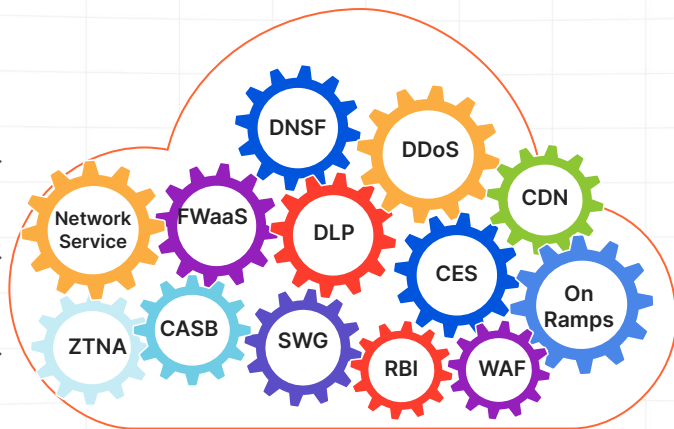
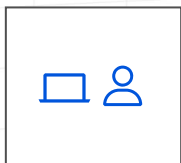
Office users



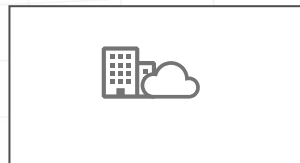
Third parties



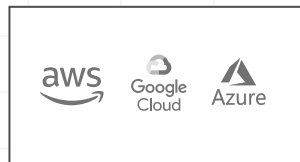
Remote users



Private Cloud/DC/Colocation



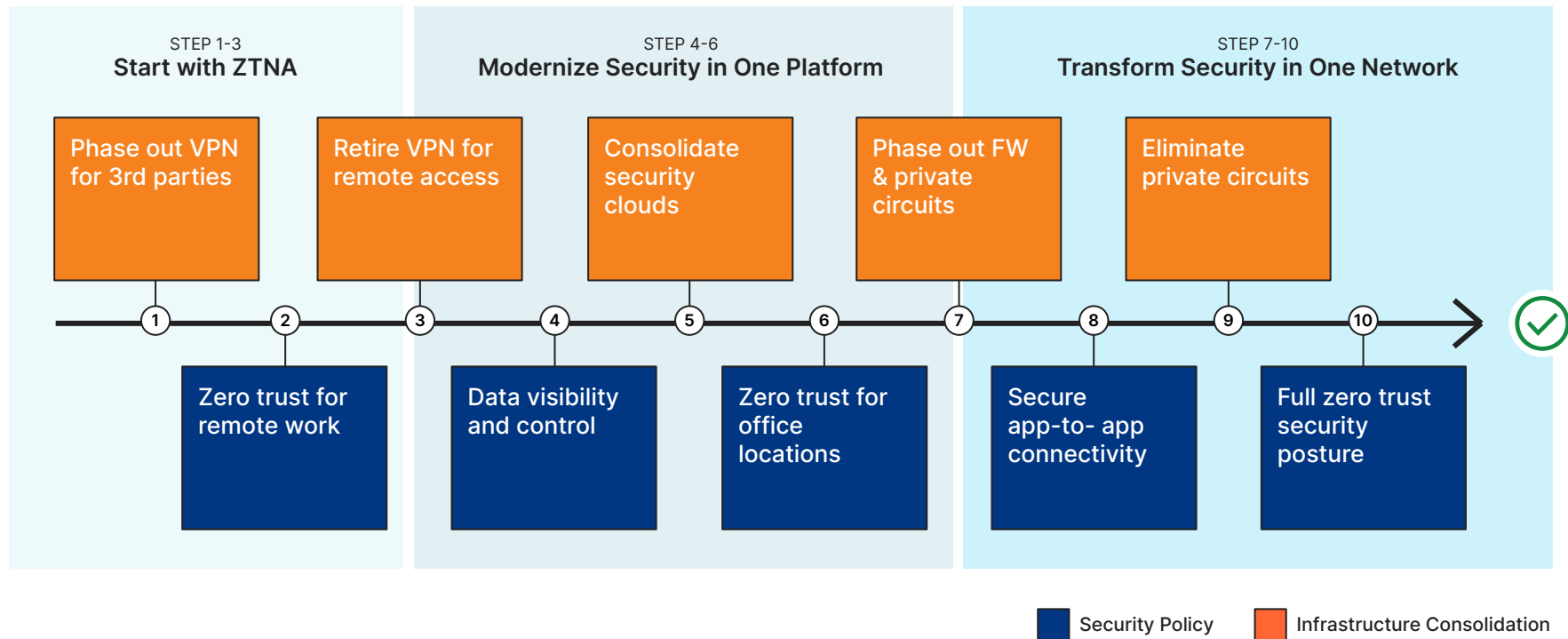
Public Cloud



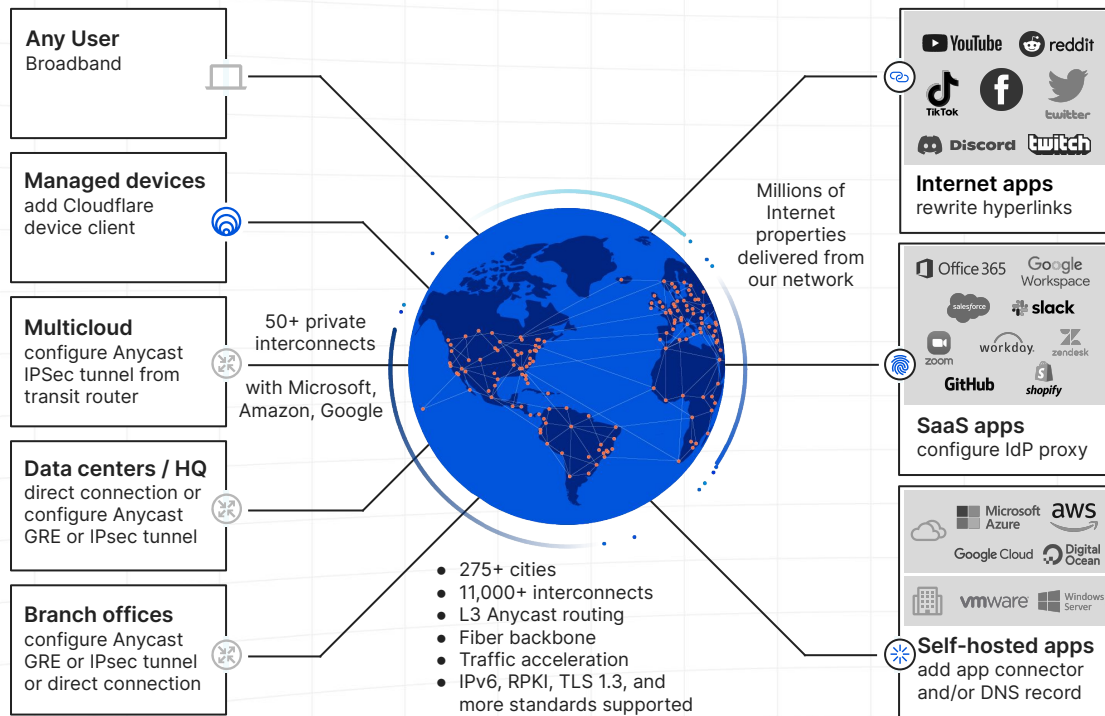
SaaS Apps and email



A common roadmap to Zero Trust and single-vendor SASE



Simple deployments, flexible architecture



Composable on-ramps

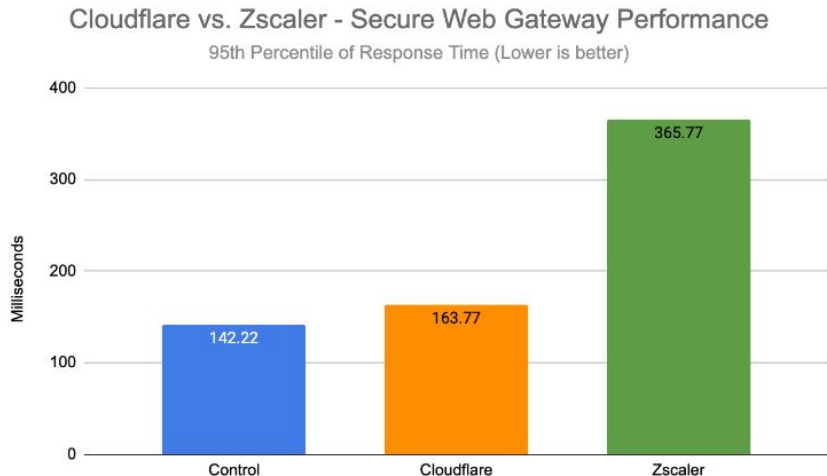
Clientless access
to rapidly adopt Zero Trust

Device clients
to fully replace your VPN

IP tunnels
over GRE/IPsec to phase out
legacy MPLS networks

Direct connections
bring SASE to your doorstep at
1600+ colos and up to 1000 offices

The Cloudflare difference



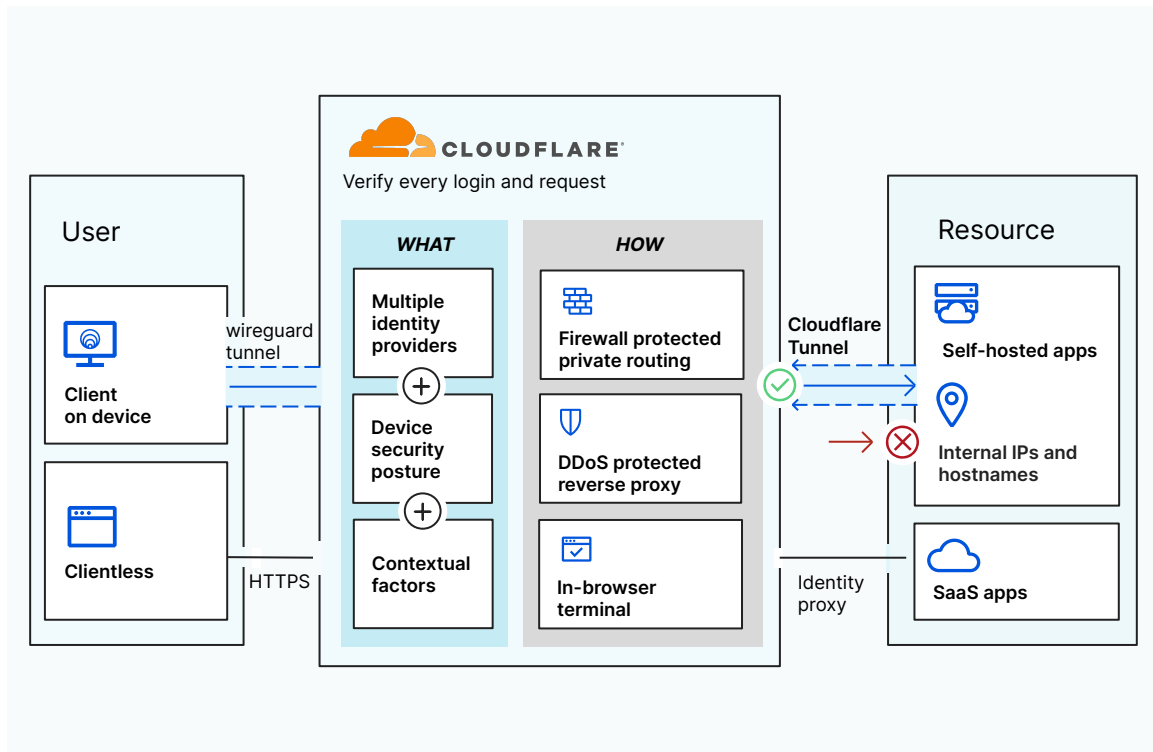
- Cloudflare's anycast network delivers security without the performance hit
- Close to *Control* group, i.e. without using a proxy at all

Secure Web Gateway - Response Time	
95th percentile (ms)	
Control	142.22
Cloudflare	163.77
Zscaler	365.77

<https://sasecloudmap.com/>

<https://blog.cloudflare.com/network-performance-update-cio-edition/>

VPN replacement or augmentation using Zero Trust Network Access



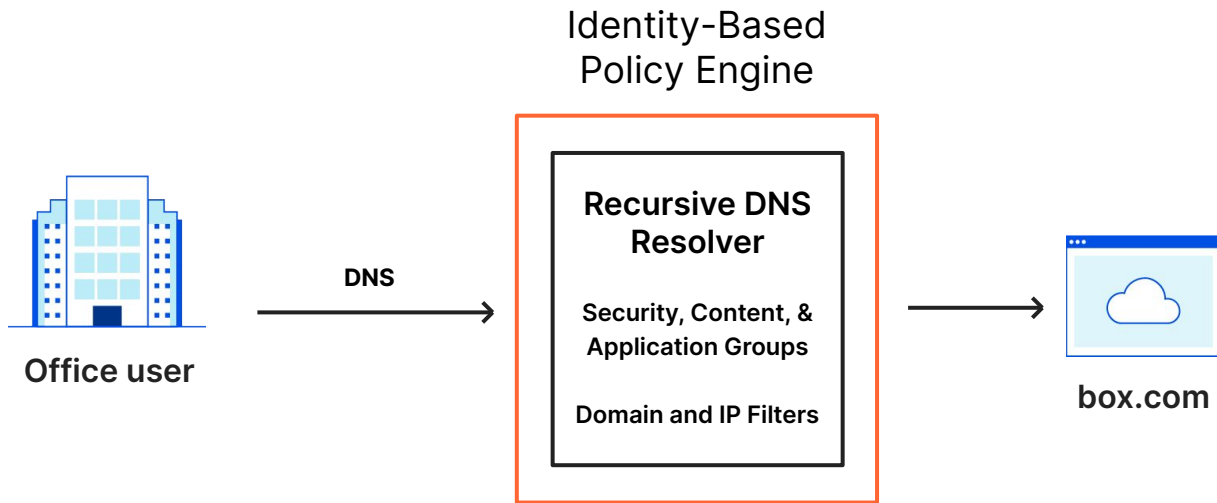
Same security and experience
accessing legacy non-HTTP
apps as modern apps

Built-in, industry-leading
DDoS & FW protections to
ensure that your resources are
always available

Unify network and cloud
access in minutes

DNS filtering for office locations

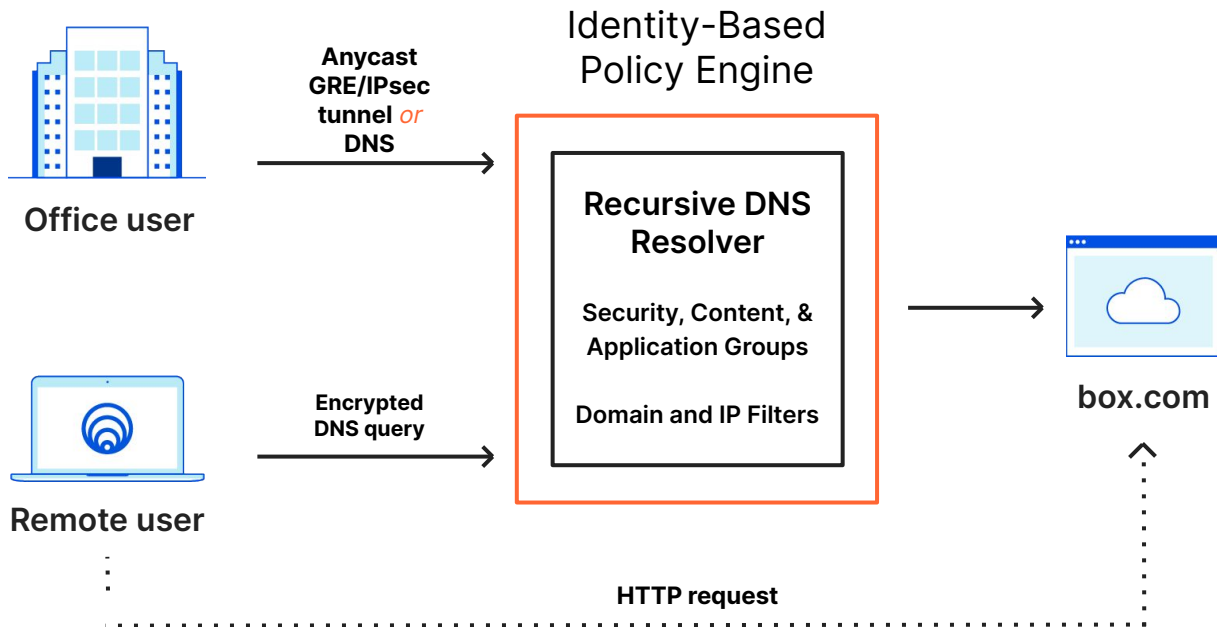
Level 1: Protect office locations with DNS filtering



1. Source IPv4 or IPv6 address checked for location
2. Query checked for policy adherence
3. Query blocked, allowed, or overridden
4. Allowed domain resolves
5. Site loads for user

DNS filtering for remote workers

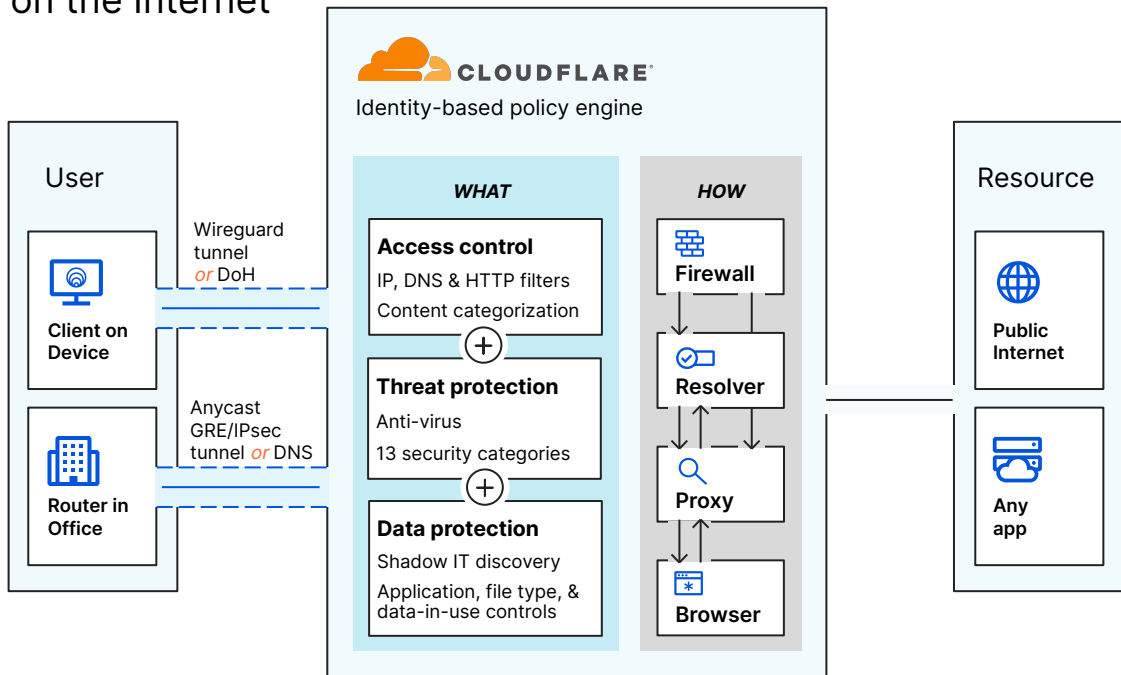
Level 2: Protect remote workers and office locations with encrypted DNS filtering



1. DNS query encrypted over DoH or DoT
2. Encrypted query sent to Gateway
3. Query decrypted
4. Query checked against policy
5. Query blocked, allowed, or overridden
6. Allowed domain resolves
7. Site loads for user

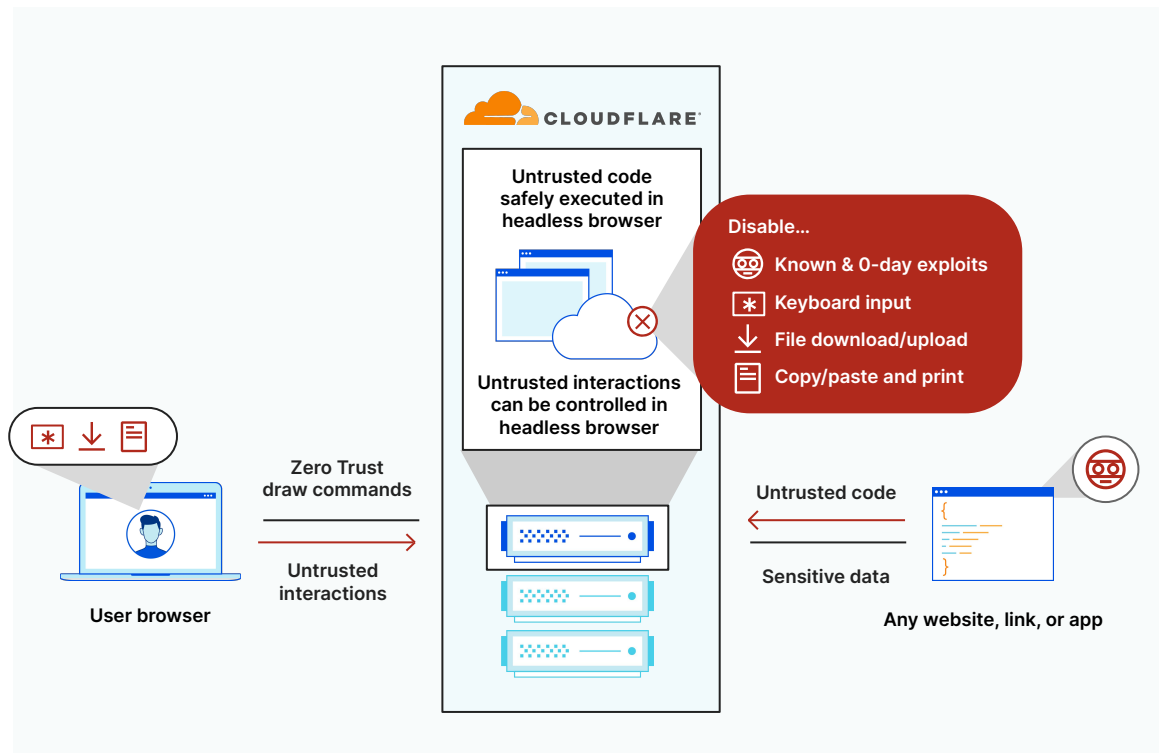
Secure Web Gateway for Work from Anywhere

Level 3: Protect office locations, remote users, and corporate data from threats on the Internet



1. WARP encrypts all Internet-bound traffic
2. Sends HTTP and DNS requests to Gateway
3. Query decrypted
4. Query checked against policy
5. Query blocked, allowed, or overridden
6. Allowed domain resolves
7. Gateway intercepts traffic over port 80 and 443
8. Request checked against policy based on configured enforcement order
9. Request blocked or allowed
10. Site loads for user

Perfected Internet protection via Zero Trust web browsing and email links



Reduce attack surface

Safely visit uncategorized or risky sites without overblocking users

Stop data loss

Enable contractors or BYOD to access apps with sensitive data

Compatibility with all browsers

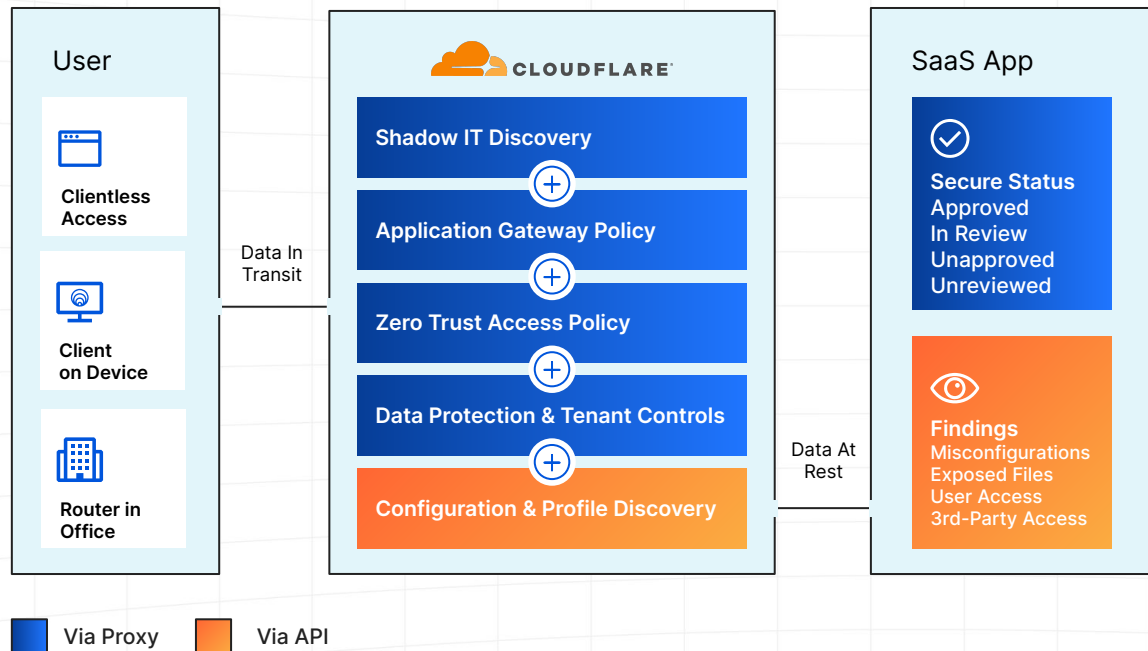
No page scrubbing, so it works natively with any site or app

Lightning-fast user experience

No pixel pushing, so it feels no different than local browsing



Secure your SaaS applications



Current API Integrations

 **Google** Workspace

 **Microsoft 365**

 **slack**

GitHub

 **salesforce**

box

Reduce burden on tech and operations

Traditional Approach

6 Products 6 Managers 6 Clients



Problem #1:

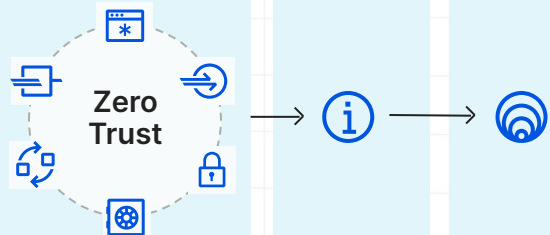
Multiple point products require multiple policy managers, and multiple client deployments

Solution:

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

Cloudflare

1 Platform 1 Manager 1 Client

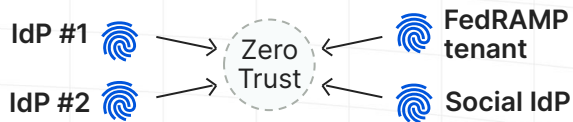


Problem #2:

Integrate only one identity provider (IdP) repeatedly and inconsistently

Solution:

Integrate many IdPs and tenants of the same IdP just once



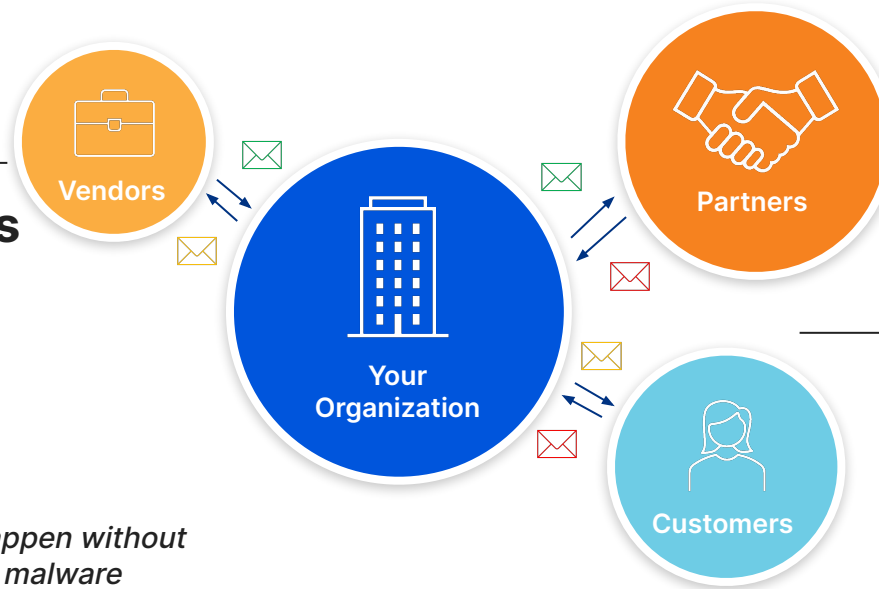
Email is the ...

#1 way organizations communicate

70%

of organizations use cloud email solutions today. (Gartner)

- *Email attacks can happen without network intrusion or malware*
- *Extends beyond direct employee access decisions*



#1 threat attack vector

91%

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

AREA 1 OVERVIEW



PREEMPTIVE

Campaign Hunting

Preemptive
Crawling

Frontier
Management
- Static & Dynamic

User
Impersonation
& Browser
Emulation

Dual Sandboxing
(In-the-wild &
Delivery)

CONTEXTUAL & COMPREHENSIVE

Type 2/3/4 BECs

Sentiment
Analysis

Conversation /
Thread
Analysis

Partner
Social Graph

Active Fraud
Verdict
Escalations

URLs & Payloads

Deep Link
Traversals &
Instant Crawls

Deep Payload
URL
Assessment

Blind URL
Assessment

New Domain
Assessments

Encrypted
Attachment
Scanning

Image Analysis
& Vector
Mapping



Area 1 Email Security

CONTINUOUS & ACCOUNTABLE

Integrated Prevention,
Detection & Response

Integrated API
& Orchestrations

Rapid Scale Indexing,
Retrieval & Search

Single Pane With Zero
Touch Service

Cloud Native
With Adaptive Scaling

Multi-mode Protection
MX / API / CONNECTOR / JOURNALING / BCC / DNS

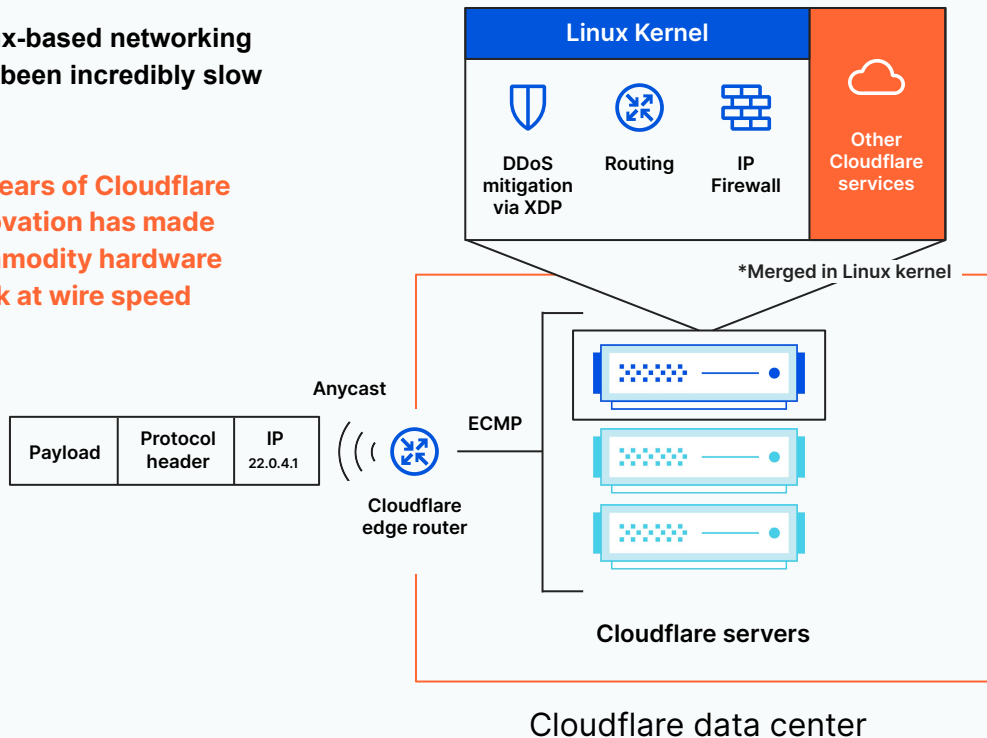


Cloudflare Network Services

Linux-based networking
had been incredibly slow



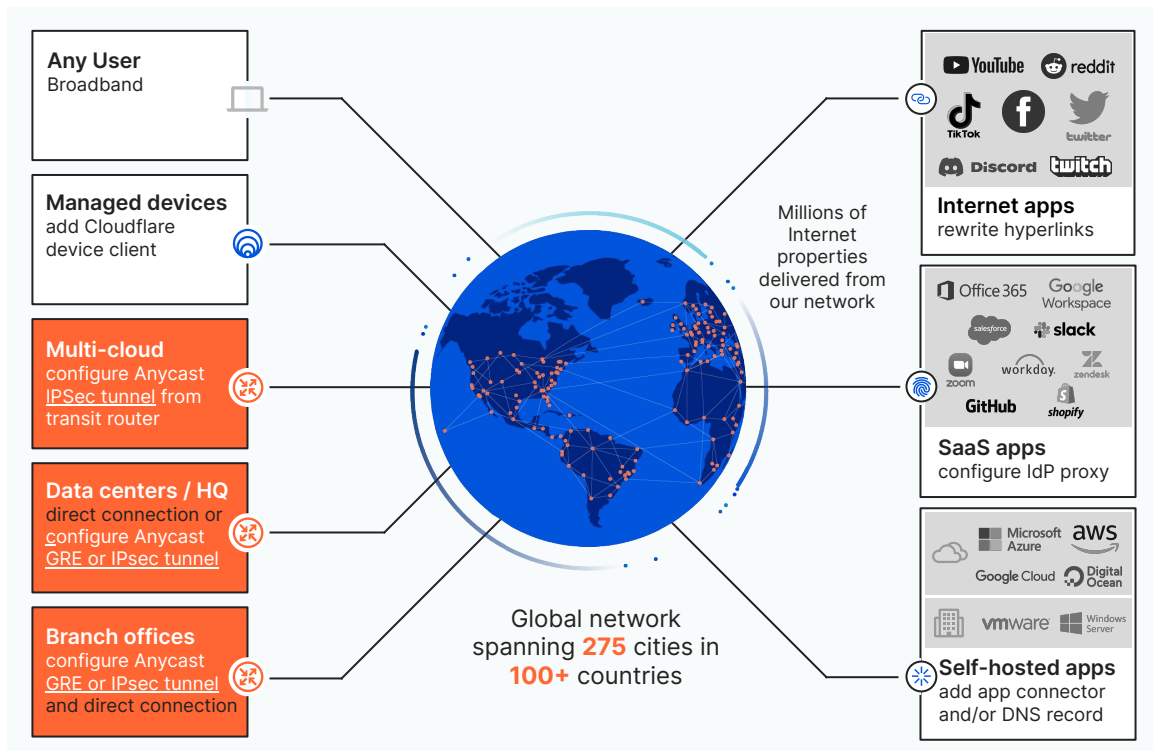
10 years of Cloudflare
innovation has made
commodity hardware
work at wire speed



*Merged in Linux kernel...

- **Express data path (XDP)**
In 60 μ s or less, analyze, move or drop raw link-layer packets with secret sauce being the logic and filters to automatically mitigate attacks
- **Inter-DC load balancing**
Anycast routing ensures no single DC gets overloaded
- **Intra-DC load balancing**
ECMP routing ensures no single server gets overloaded

Magic WAN



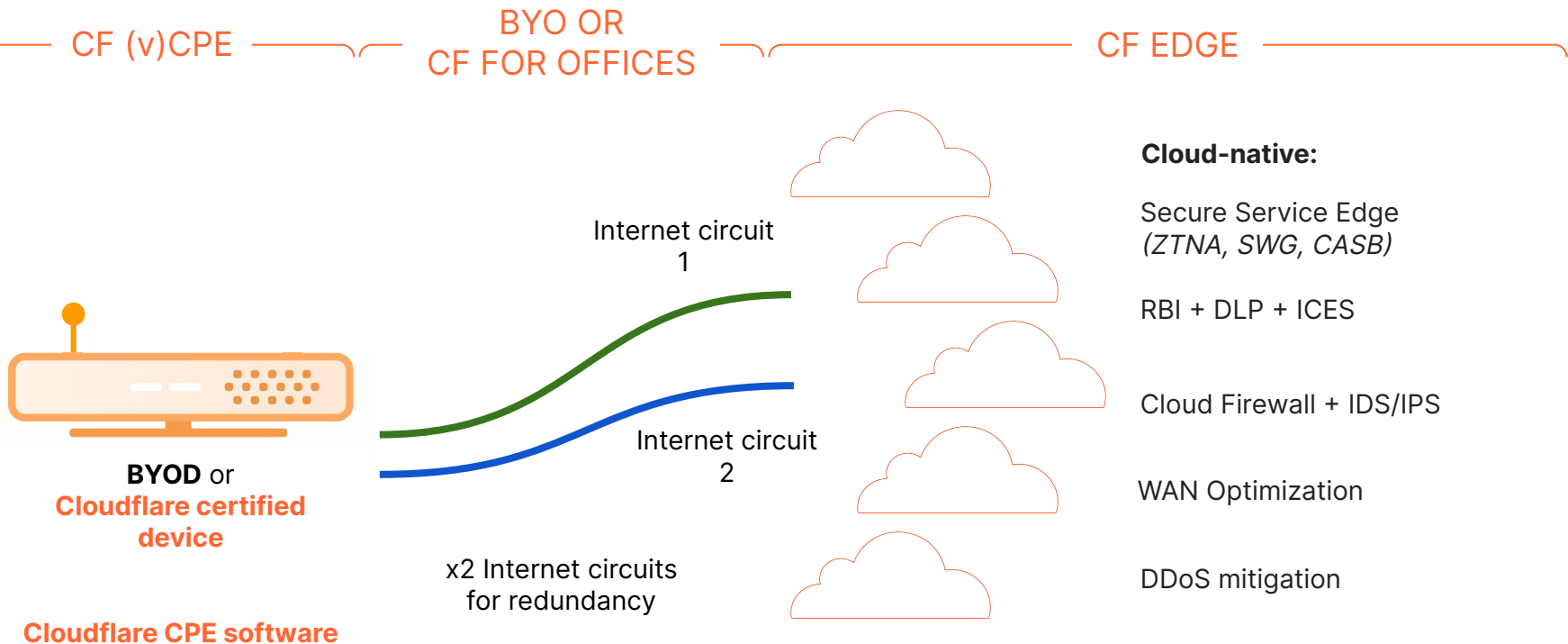
Cloudflare Magic WAN

GRE or IPsec tunnels use existing CPE, cloud transit gateways, or using pre-built SD-WAN integrations

Benefits

- Retire expensive MPLS services
- Retire legacy security appliances — firewall-as-a-service and SWG built natively into the network
- Avoid traffic backhaul to hub sites and improve app performance
- Simplify site-to-site connectivity with Anycast IPsec
- Performance advantages of full-mesh, with the simplicity of classic hub-and-spoke

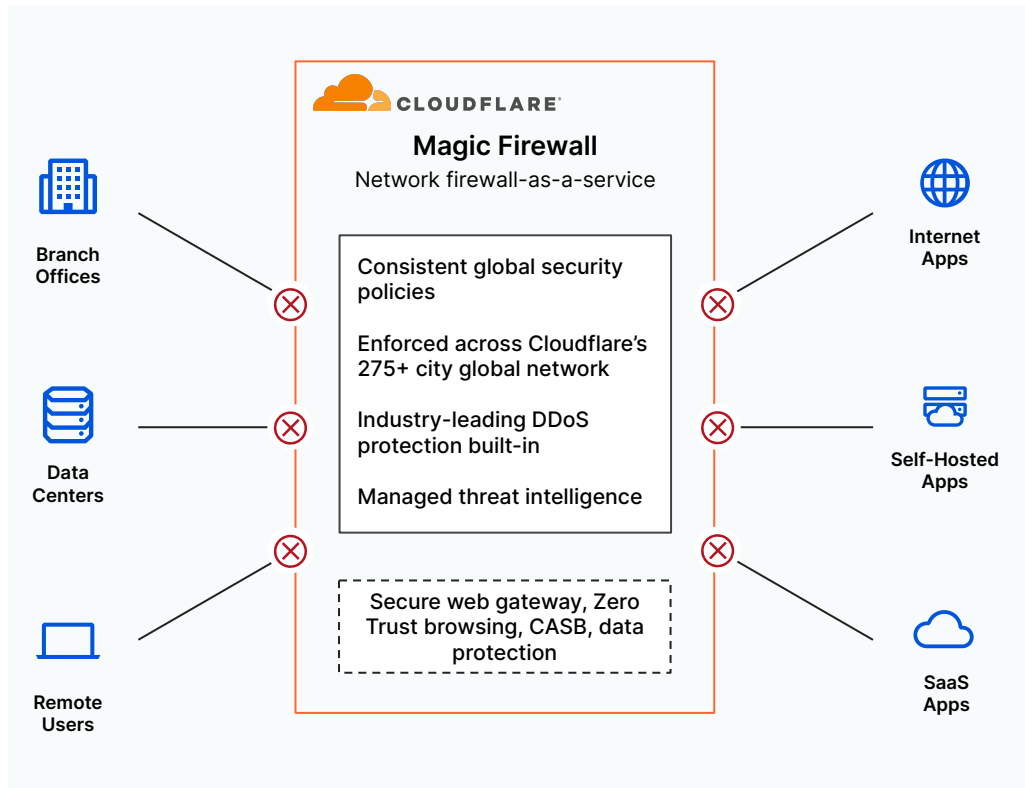
Magic WAN Connector



Magic Firewall: cloud-native security for your entire network

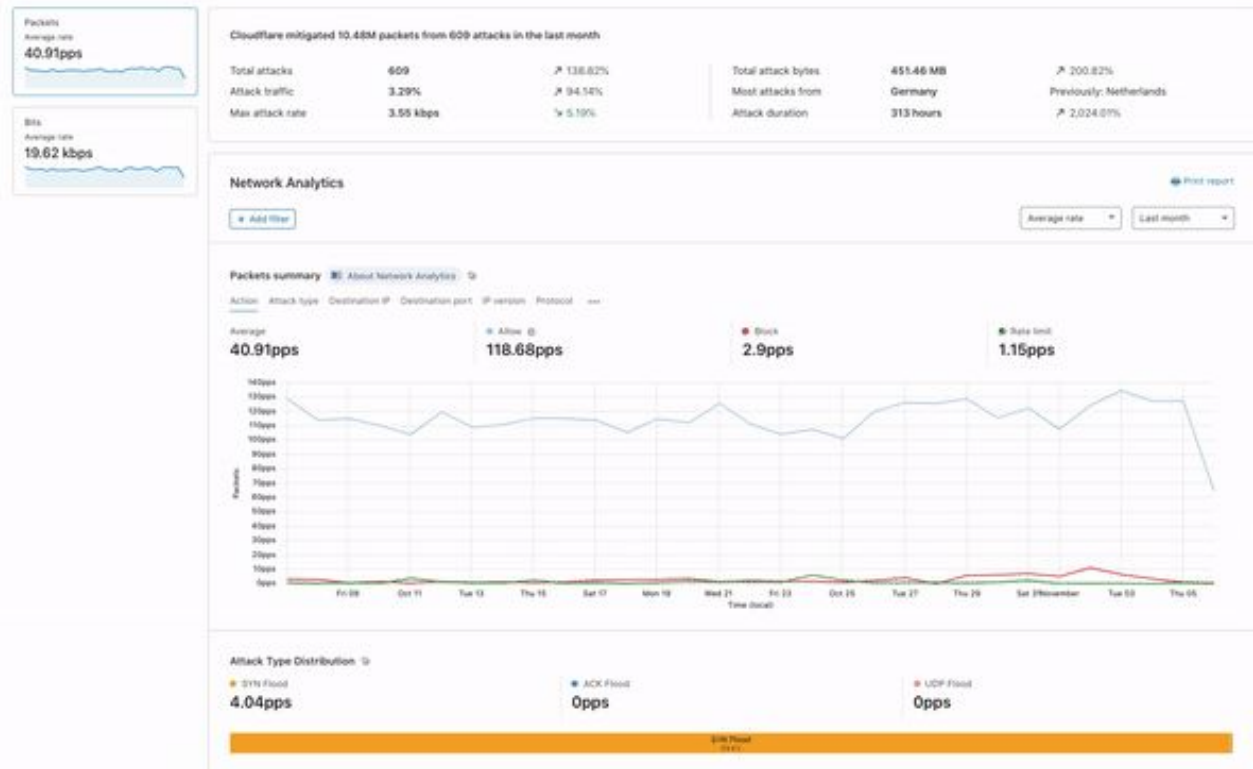
Magic Firewall — enforce consistent security policies across your branch offices, data centers, cloud properties and end-user devices.

- Consistent security policies — deployed globally in under 500ms
- No appliances to manage — automatically scale with your business needs
- Eliminate unwanted traffic before it reaches your network
- Managed threat intelligence gleaned from the Cloudflare global network
- Optional upgrade to Secure Web Gateway, CASB, Zero Trust browsing

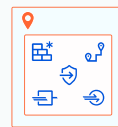
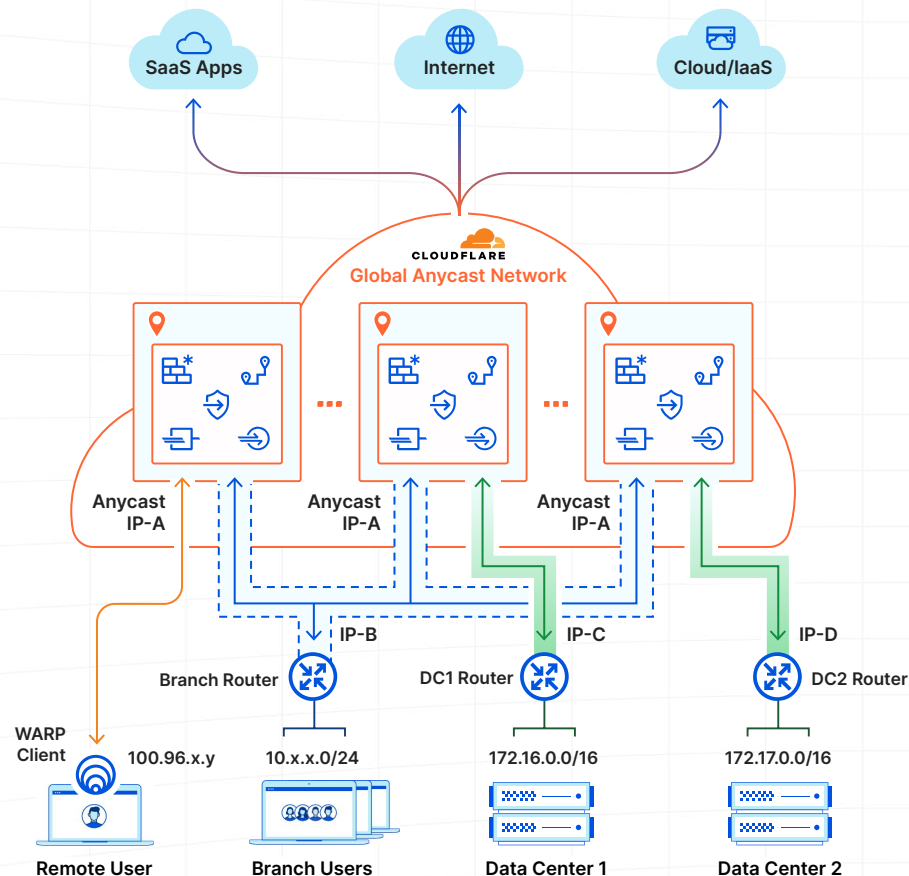


Troubleshooting made easy

- Quickly identify traffic anomalies
- View changes in traffic based on criteria such as, IP protocols, TCP flags, source country
- Take necessary remedial action to fine-tune your configuration



Magic WAN: data center on-ramp with CNI



Each data center in Cloudflare's global anycast network delivers all Cloudflare services, including Magic WAN, Magic Firewall, Zero Trust and DDoS services



Anycast IPsec/GRE Tunnels between customer site routers and Cloudflare global anycast network



CNI (direct connect) between customer data center site routers and nearest Cloudflare data center



WARP connections between remote users and Cloudflare global anycast network



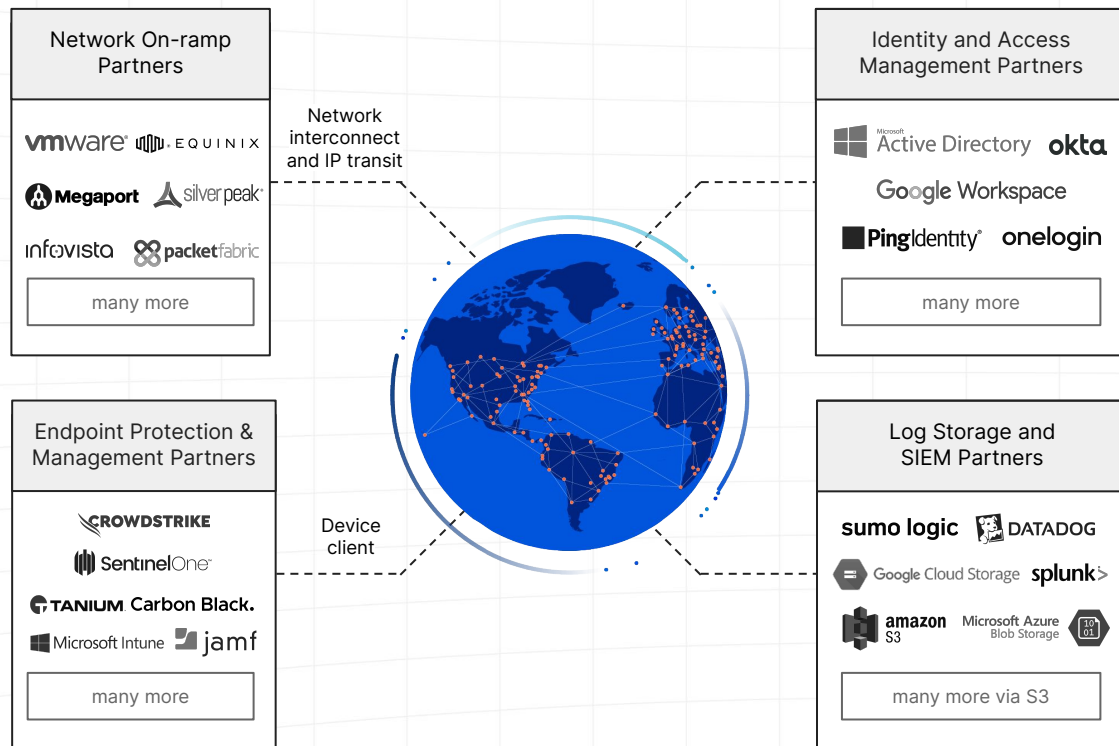
Higher cost MPLS or dedicated L2 circuits offering lowest latency between Data Centers

- **On-ramp to Cloudflare Magic WAN**
 - Customer branch sites with IPsec/GRE tunnel-capable routers on-ramp to Cloudflare Magic WAN via Anycast IPsec/GRE tunnels
 - Customer data center sites with close proximity to Cloudflare CNI data centers on-ramp to Cloudflare Magic WAN via CNI
 - Remote users on-ramp to Cloudflare Magic WAN via WARP client on their devices
- **Full-mesh Magic WAN** network connectivity (RFC 1918 address space) between all sites and users over Magic WAN
- **Web access** with Zero Trust control from all sites and users via Magic WAN + Cloudflare Zero Trust services
- **Fine-grain security and control**
 - Magic Firewall
 - Cloudflare Zero Trust



Cloudflare Platform

Make it fit in the bigger picture



We fit into your world

Identity, endpoint,
and cloud agnostic

Concurrently use
multiple providers

Programmable interface
with Terraform automation



Azure Routing Preference

Enable customers to be more multi-cloud and use industry-leading products



Azure Sentinel

Help customers analyze logs and drive insights for their web applications

Cloudflare recognized by Microsoft as a Security Software Innovator

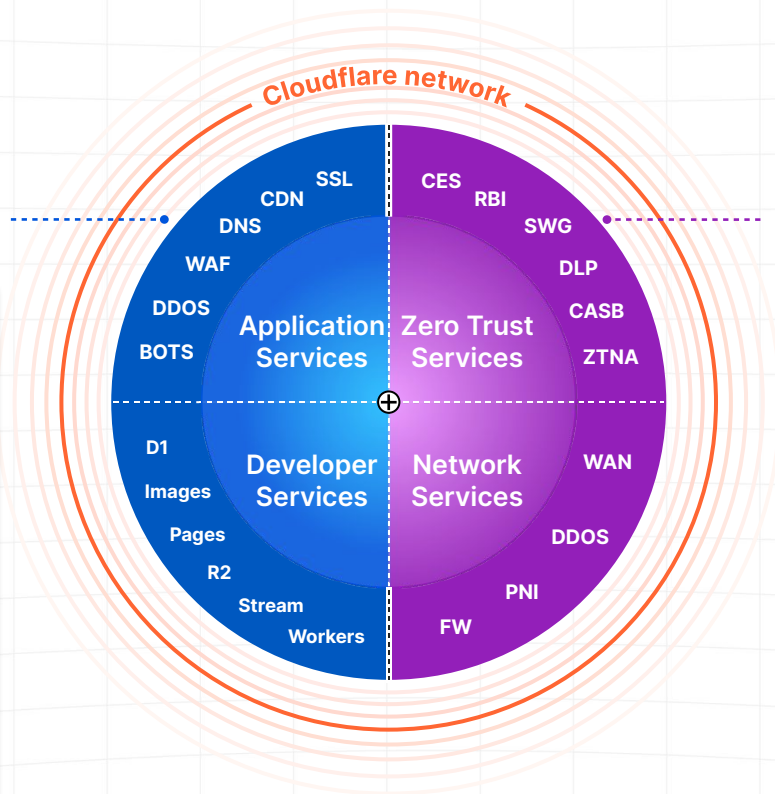
22/06/2022



Abhi Das



Kenny Johnson



Azure Active Directory

Enable secure authentication to customers' employees



Microsoft 365

Improve protection with a preemptive, comprehensive, accountable defense from socially engineered phish



Zero Trust for Azure Apps

Enable secure access to customers' on-premise applications or Azure-hosted apps without needing a VPN



Microsoft Intune

Identify, investigate, and remediate threats faster, and securely manage customers' devices from a single platform



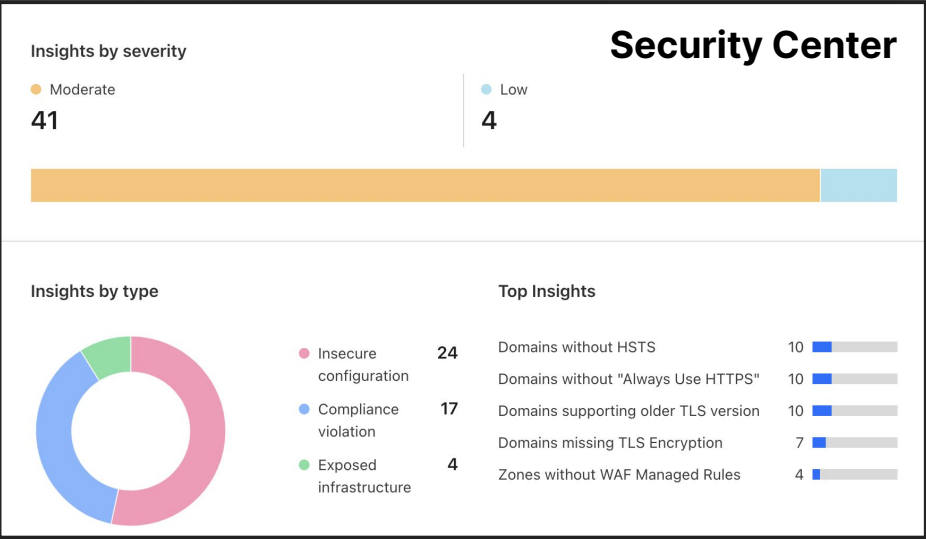
Microsoft NPP

Deliver a fast, secure Office 365 experience to customers' employees



Cloud App Defender

Detect a variety of security, data loss prevention, and misconfiguration risks



Cloudflare dashboard

6 months retention

Analytic summaries

Workplace records

Cloud storage platforms

amazon web services S3

Microsoft Azure Blob Storage

Google Cloud Storage

SIEM platforms

splunk

sumo logic

DATADOG

REST API and Terraform – for SOAR and Audits



Meer informatie?

- **Blijf hangen voor de lunch**
- 0800 - BEL JAN
- Start een gratis Phishing Risk Assessment

zerotrustroadmap.org

www.cloudflare.com

michiel.cloud/flare



Thank You