The Technology Footprint of An Organization

By Lekhana Molleti (darivxe)

Contents

1 *Executive Summary*

This report presents a comprehensive OSINT investigation into the technology footprint of Cloudflare, Inc. The goal was to map Cloudflare's externally visible infrastructure, vendor ecosystem, security posture, employee presence, and public digital footprint using only publicly accessible sources. Through DNS analysis, network scanning, job listing review, patent research, community activity, social media analysis, leaked data checks, and source-code repository examination, the investigation builds a multi-layered view of Cloudflare's operational environment.

The findings confirm Cloudflare's reliance on a globally distributed Anycast network, extensive Zero Trust architecture, and a wide partner ecosystem across identity, analytics, incident response, and cloud infrastructures. Cloudflare maintains a strong and transparent online presence, with its staff actively contributing to open-source software and public events. Several third-party security incidents indirectly affected Cloudflare, revealing insights into its internal tooling and identity systems. Overall, the investigation demonstrates Cloudflare's mature, cloud-centric, and security-focused operational structure.

1.1 *Scope*

This investigation examines Cloudflare's publicly visible technology footprint, focusing on its internet-facing infrastructure, technology stack indicators, third-party integrations, and public digital presence. Using OSINT techniques, the study collects and verifies data from official sources, developer platforms, media posts, and leak-monitoring sites to map Cloudflare's external architecture and assess its publicly exposed technologies. No internal systems or non-public resources were accessed.

1.2 *Methodology*

The investigation followed a structured OSINT and analytical framework to ensure comprehensive coverage of Cloudflare's public technology footprint.

Data Collection

- Gathered open-source intelligence (OSINT) from official documentation, technical blogs, press releases, and Cloudflare's public website.
- Reviewed secondary sources including cybersecurity reports, breach analyses, and reputable industry publications.
- Examined publicly available government records, procurement notices, and patent filings to identify Cloudflare's technology use and service contracts.
- Collected social media data from platforms such as LinkedIn, X, Discord, YouTube, Instagram, and Facebook to understand Cloudflare's public communication and technical outreach.

Infrastructure and Technology Analysis

- Conducted DNS, hosting, and certificate enumeration using tools such as **dig**, **DNSDumpster**, **crt.sh**, and **Shodan** to map Cloudflare's internet-facing infrastructure.
- Reviewed Cloudflare's partner and vendor ecosystem to understand external service dependencies and integrations.

Security and Incident Investigation

- Examined publicly disclosed security incidents involving Cloudflare or its third-party vendors to infer internal systems, identity management tools, and operational workflows.
- Verified findings using public breach reports, blog disclosures, and threat intelligence writeups.

Social Media and Community Review

- Analyzed Cloudflare's presence across social platforms and developer communities to identify event activity, technical discussions, product announcements, and employee insights.
- Reviewed Discord developer conversations, YouTube engineering talks, and conference recordings for additional architectural clues.

Source Code and Employee Profiling

- Examined Cloudflare's official GitHub organization to identify open-source repositories and operational tooling.
- Cross-referenced GitHub profiles of Cloudflare employees to understand technical expertise, contribution patterns, and public-facing engineering culture.

Leaked Data Surface Checks

- Performed passive searches on GrayHatWarfare, Pastebin, and leak-monitoring platforms to identify exposed Cloudflare-related material.
- Confirmed that no internal Cloudflare assets were leaked, while noting third-party references and user-posted scripts.

Documentation and Presentation

- Findings were compiled into structured sections, supported by screenshots, diagrams, and evidence-based explanations.
- All sources were referenced to ensure credibility, traceability, and adherence to OSINT best practices.

---

2. Investigative Findings

Organization Overview: Cloudflare, Inc.

Cloudflare, Inc. is a global cloud-based security and performance company that provides services designed to protect and accelerate internet applications. **Founded in 2010 and headquartered in San Francisco**, Cloudflare operates one of the world's largest and most distributed edge networks. Its core mission is to help create a **faster, safer, and more reliable internet** for organizations and users across the globe.

Cloudflare sits in a unique position in the internet ecosystem. Instead of hosting websites or storing customer data like traditional cloud providers, Cloudflare functions as an **intermediary layer** between users and the servers that host online content. By routing traffic through its global Anycast edge network, Cloudflare is able to reduce latency, mitigate malicious activity, filter attacks, and optimize application delivery — all without requiring changes to a customer's existing infrastructure.

Cloudflare's Official Site

Global Infrastructure Footprint

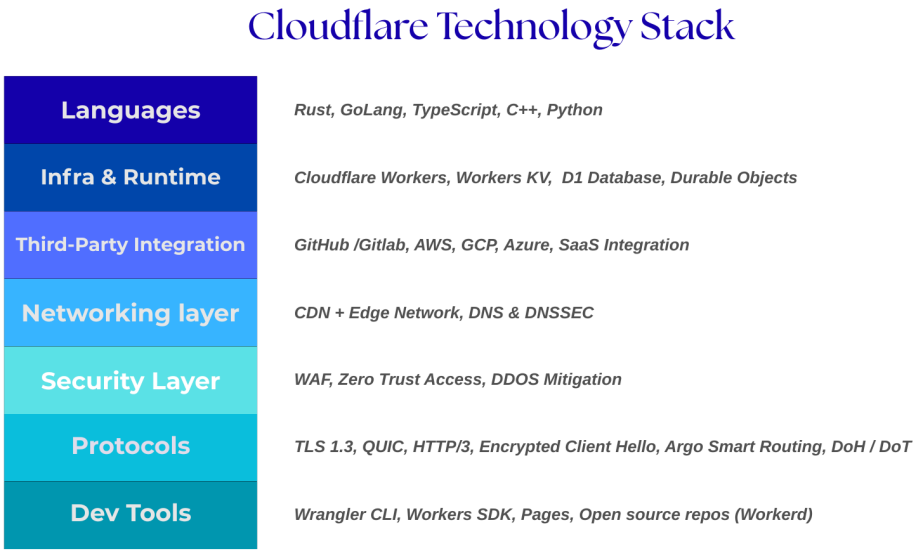
Cloudflare's infrastructure is distinguished by its **Anycast-based edge network**, which spans **over 300 data center locations worldwide**. Instead of routing traffic across centralized regional hubs, Cloudflare advertises the same IP addresses from many geographic points simultaneously. This means:

- Users are connected to the **nearest Cloudflare data center**
- Latency is reduced because traffic does not need to travel across continents
- The system is resilient - if one data center is unavailable, traffic is shifted automatically

This distributed model is central to how Cloudflare delivers **high availability, strong redundancy, and DDoS resistance at scale**.

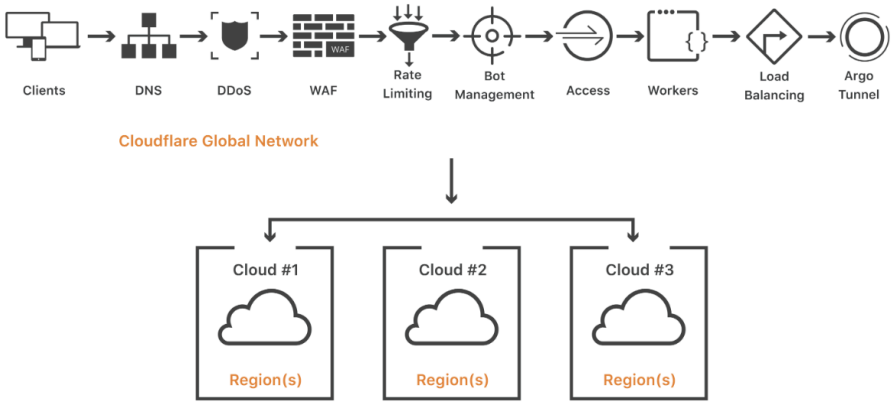
Technology Stack

Cloudflare's technology stack is built to support its global edge network, security services, and developer platform. The following graphic presents a simplified overview of the major components Cloudflare relies on to operate and deliver its services.



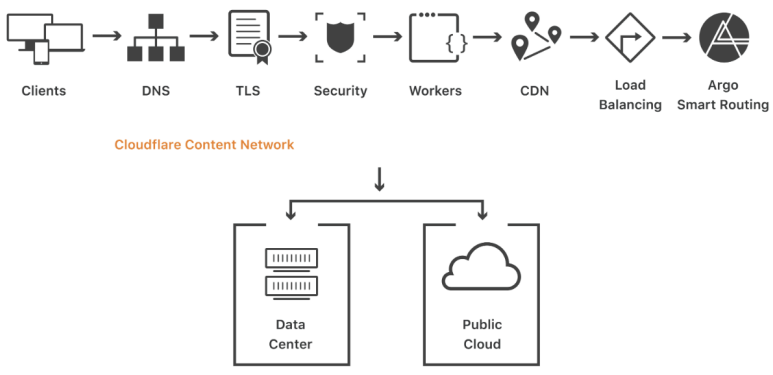
Cloudflare and Cloud Infrastructures

Cloudflare can work with any type of cloud setup, whether an organization uses a public cloud service, a private data center, a hybrid environment, or several cloud providers at the same time. Cloudflare sits in front of the existing infrastructure and acts as a protective and performance-enhancing layer. When a user sends a request, the request is routed through Cloudflare's global network. At the edge, Cloudflare filters attacks, improves speed, and applies security controls before the request reaches the original server.



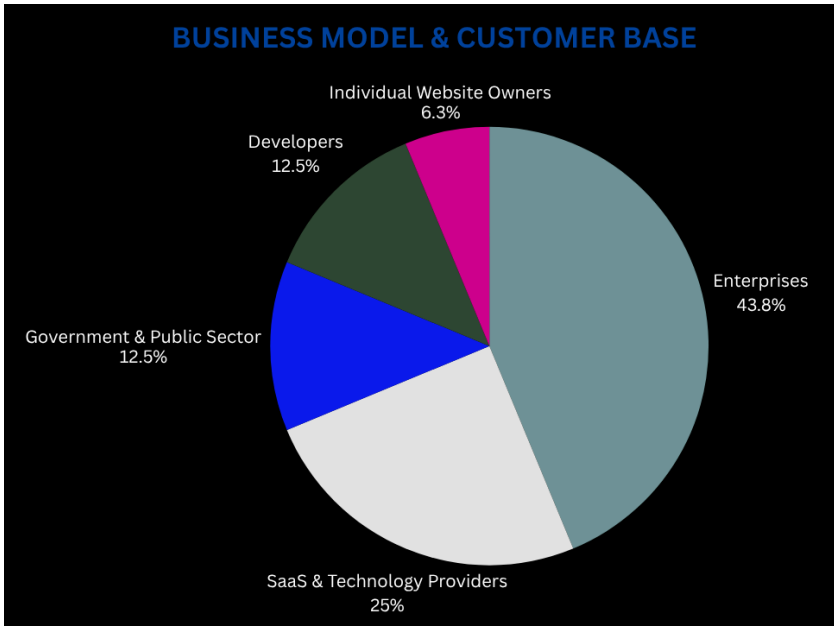
Cloudflare and multi-cloud

This approach does not require the organization to change where or how their applications are hosted. Cloudflare can be added without redesigning backend systems. Because of this, Cloudflare helps organizations improve reliability, performance, and security while keeping full control over their own cloud environment.

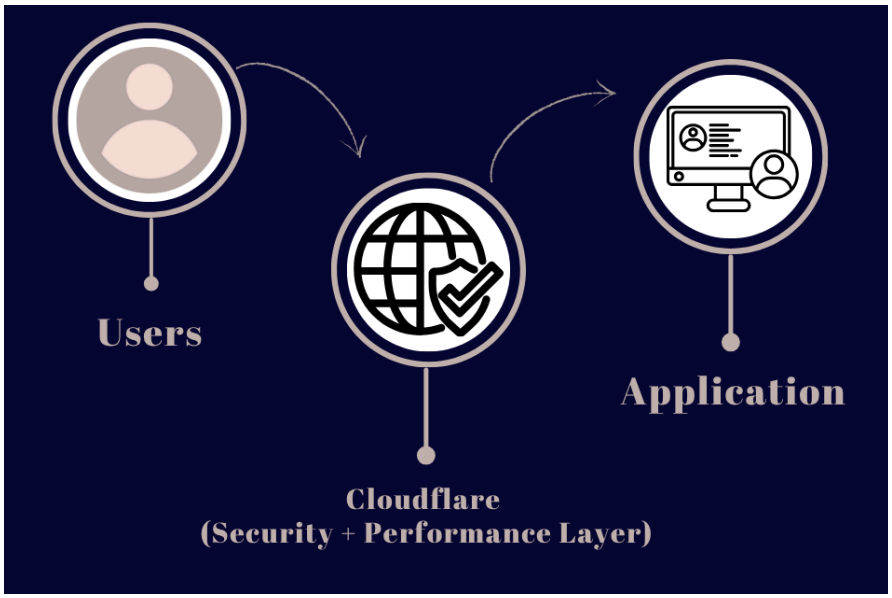


Cloudflare and hybrid cloud

Cloudflare serves a wide range of internet users, and the chart reflects how broadly its services are adopted. Enterprises make up the largest share, showing Cloudflare's importance in securing large-scale infrastructure. SaaS providers and government clients also represent major portions, while developers and individual site owners round out the rest through Cloudflare's accessible platform and free tier. Overall, the distribution shows how deeply Cloudflare is embedded across the entire internet ecosystem.



Strategic Position in the Internet Ecosystem



darivxe - Cloudflare footprint

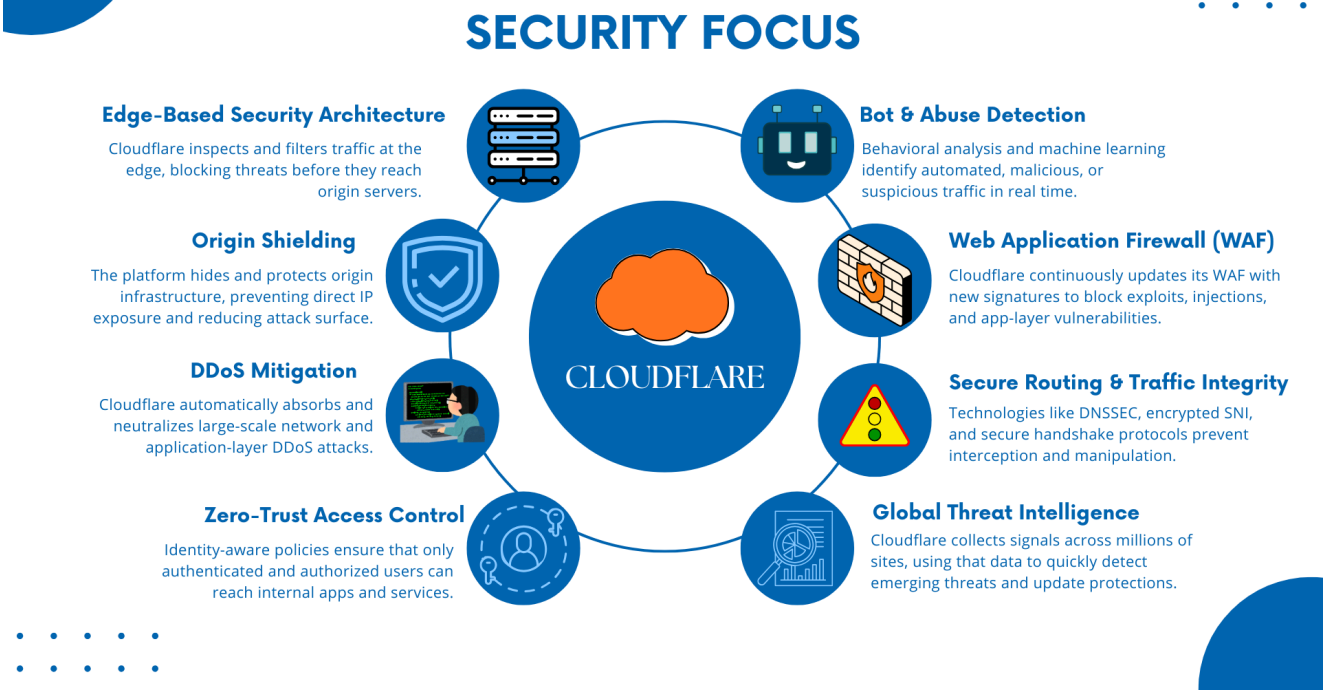
Cloudflare is positioned as a **critical infrastructure facilitator**. It does not replace cloud providers such as AWS, Azure, or GCP, instead it **sits between the public internet and those providers**, functioning as:

- A global **traffic manager**
- A **security enforcement checkpoint**
- A **performance optimization layer**

Because of this role, Cloudflare influences how information moves, how digital identity is verified, and how applications interact with users on a global scale.

Organisational Focus On Security

Cloudflare's security model is built directly into its global edge network, allowing threats to be detected and stopped before they reach an application's origin. The company blends traffic filtering, identity controls, threat intelligence, and automated mitigation to reduce exposure across millions of internet properties. This graphic highlights the core components of Cloudflare's security architecture and how each layer contributes to a unified, edge-first defense model.



2.1 *Public Records*

Analysis of DNS Records

DNS (Domain Name System) records serve as a foundational layer of an organization's internet presence. By examining Cloudflare's DNS configuration, it is possible to infer **network architecture**, **service distribution model**, **security posture**, and **third-party vendor dependencies**. The DNS records retrieved for **www.cloudflare.com** and associated subdomains provide clear evidence of a **globally distributed edge computing strategy**, enabled through Cloudflare's Anycast network.

Using dig

```
; <<>> DiG 9.20.11 <<>> www.cloudflare.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26631
;; flags: qr rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cloudflare.com.            IN      A

;; ANSWER SECTION:
www.cloudflare.com.     114     IN      A       104.16.124.96
www.cloudflare.com.     114     IN      A       104.16.123.96

;; Query time: 77 msec
;; SERVER: 2401:4900:50:9::7b7#53(2401:4900:50:9::7b7) (UDP)
;; WHEN: Thu Nov 06 18:35:54 IST 2025
;; MSG SIZE  rcvd: 79
```

When querying the domain www.cloudflare.com, the response returned two IPv4 addresses:

104.16.124.96

104.16.123.96

Both of these IP addresses belong to Cloudflare's network under **ASN AS13335 (CLOUDFLARENET)**. These IPs are part of Cloudflare's **Anycast routing system**, meaning the same IP address is served from many data centers worldwide. Instead of directing requests to a single fixed server, Cloudflare routes traffic to the **closest and most available edge location**.

This confirms that Cloudflare uses a **distributed edge architecture**, where website and application traffic is processed at the nearest point-of-presence. This approach reduces latency, improves performance, and ensures continuity even if one data center is unavailable.

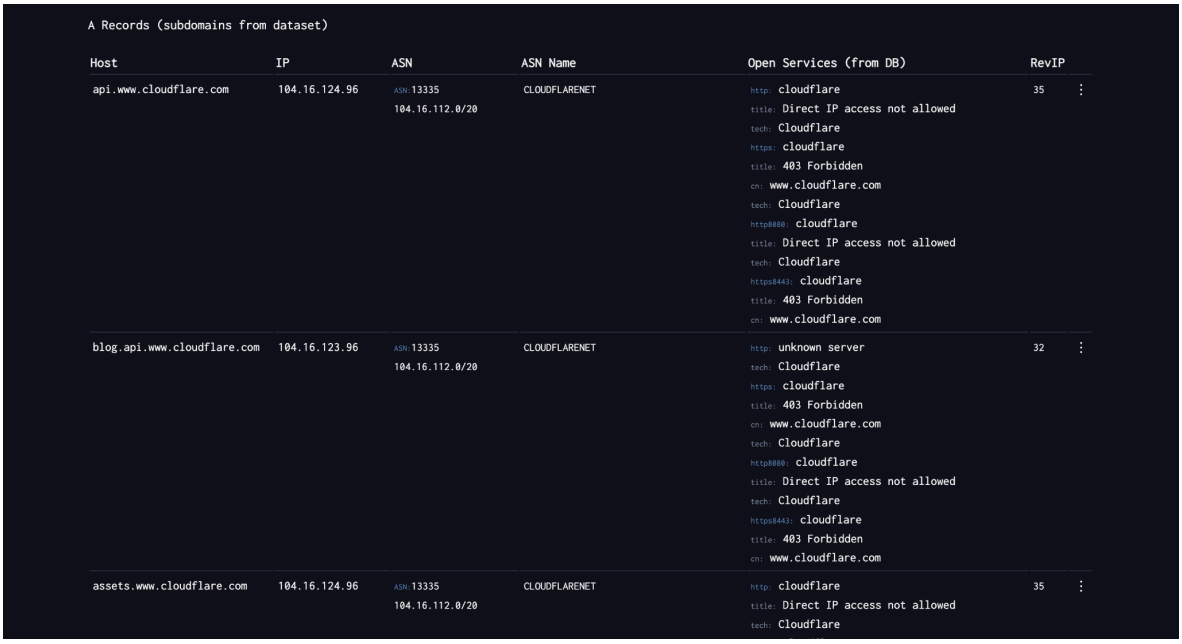
What this indicates

Cloudflare prioritizes **global availability**, **low-latency delivery**, and **resilience**, all achieved through its Anycast-based infrastructure.

Using DNSDumpster

The DNSDumpster output provided a visual overview of Cloudflare's publicly observable infrastructure. The map and hosting information indicate that Cloudflare operates across a globally distributed network. The highlighted regions show that Cloudflare has system presence across multiple continents, which aligns with its Anycast edge delivery model.

The IP range shown, **104.16.112.0/20**, further reinforces that Cloudflare uses a shared Anycast block to distribute traffic across many data centers around the world.



A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
api.www.cloudflare.com	104.16.124.96	ASN:13335 104.16.112.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare https: cloudflare title: 403 Forbidden cn: www.cloudflare.com tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare https8443: cloudflare title: 403 Forbidden cn: www.cloudflare.com	35
blog.api.www.cloudflare.com	104.16.123.96	ASN:13335 104.16.112.0/20	CLOUDFLARENET	http: unknown server tech: Cloudflare https: cloudflare title: 403 Forbidden cn: www.cloudflare.com tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare https8443: cloudflare title: 403 Forbidden cn: www.cloudflare.com	32
assets.www.cloudflare.com	104.16.124.96	ASN:13335 104.16.112.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare	35

The **Open Services** portion of the output shows responses such as **"Direct IP access not allowed"** and **403 Forbidden**. This indicates that Cloudflare does not allow users to access the service directly via the raw IP address. Requests must pass through Cloudflare's routing and security layers before reaching the application. This is intentional. It prevents attackers from bypassing inspection controls and reaching origin servers directly.

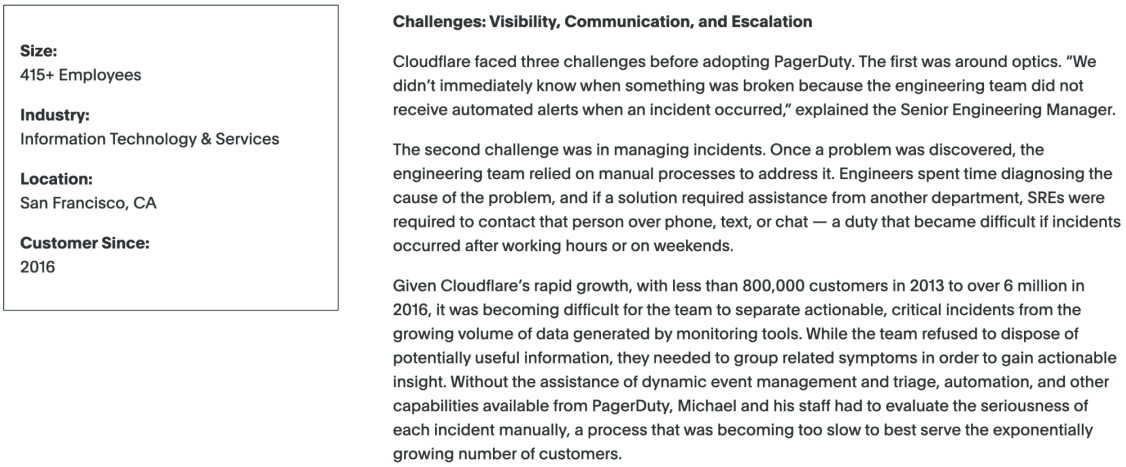
The results also display multiple language and region variations of Cloudflare-hosted domains. Together, these patterns demonstrate that Cloudflare uses its edge network to handle API calls, deliver static assets, and serve localized versions of content, all while maintaining control of security and traffic filtering at the entry point.

Cloudflare listed as a customer

Public vendor listings and third-party service disclosures provide insight into the external platforms and technologies that an organization relies on to support its operations. In Cloudflare's case, several vendors openly identify Cloudflare as one of their customers. This allows us to understand part of Cloudflare's internal tooling and operational ecosystem.

PagerDuty

PagerDuty, a leading incident response and on-call workflow platform, lists Cloudflare as a customer in its public customer case studies. This suggests that Cloudflare relies on PagerDuty for coordinating operational alerts, responding to service incidents, and maintaining high availability across its globally distributed network. The use of PagerDuty demonstrates that Cloudflare prioritizes structured incident management and real-time operational monitoring. *pagerduty*



Size:
415+ Employees

Industry:
Information Technology & Services

Location:
San Francisco, CA

Customer Since:
2016

Challenges: Visibility, Communication, and Escalation

Cloudflare faced three challenges before adopting PagerDuty. The first was around optics. "We didn't immediately know when something was broken because the engineering team did not receive automated alerts when an incident occurred," explained the Senior Engineering Manager.

The second challenge was in managing incidents. Once a problem was discovered, the engineering team relied on manual processes to address it. Engineers spent time diagnosing the cause of the problem, and if a solution required assistance from another department, SREs were required to contact that person over phone, text, or chat — a duty that became difficult if incidents occurred after working hours or on weekends.

Given Cloudflare's rapid growth, with less than 800,000 customers in 2013 to over 6 million in 2016, it was becoming difficult for the team to separate actionable, critical incidents from the growing volume of data generated by monitoring tools. While the team refused to dispose of potentially useful information, they needed to group related symptoms in order to gain actionable insight. Without the assistance of dynamic event management and triage, automation, and other capabilities available from PagerDuty, Michael and his staff had to evaluate the seriousness of each incident manually, a process that was becoming too slow to best serve the exponentially growing number of customers.

SendGrid

Additionally, the **DNSDumpster scan** displays **SendGrid** within the hosting and network association results. This implies that Cloudflare integrates with SendGrid's cloud email delivery infrastructure for system-generated or communication-related email processes. While Cloudflare operates the majority of its infrastructure internally, these findings demonstrate that the organization strategically utilizes external specialized platforms to support reliability, communication workflows, and operational responsiveness.

Okta for Identity and Access Management

Cloudflare uses **Okta** as its internal Identity and Access Management (IAM) provider. This means that when Cloudflare employees access internal tools, administrative dashboards, cloud consoles, or development systems, their identity is verified and authenticated through Okta before access is granted. Okta acts as the **central gatekeeper** for employee login sessions.

In an official post addressing a security incident involving Okta, Cloudflare directly confirmed that Okta is used as its identity provider. This statement is publicly verifiable and therefore provides reliable evidence of the relationship. *okta*

How Cloudflare uses Okta

Cloudflare uses Okta internally as our identity provider, integrated with Cloudflare Access to guarantee that our users can safely access internal resources. In previous blog posts, we described how we use Access to protect internal resources and how we integrated hardware tokens to make our user authentication process more resilient and prevent account takeovers.

In the case of the Okta compromise, it would not suffice to just change a user's password. The attacker would also need to change the hardware (FIDO) token configured for the same user. As a result it would be easy to spot compromised accounts based on the associated hardware keys.

Even though logs are available in the Okta console, we also store them in our own systems. This adds an extra layer of security as we are able to store logs longer than what is available in the Okta console. That also ensures that a compromise in the Okta platform cannot alter evidence we have already collected and stored.

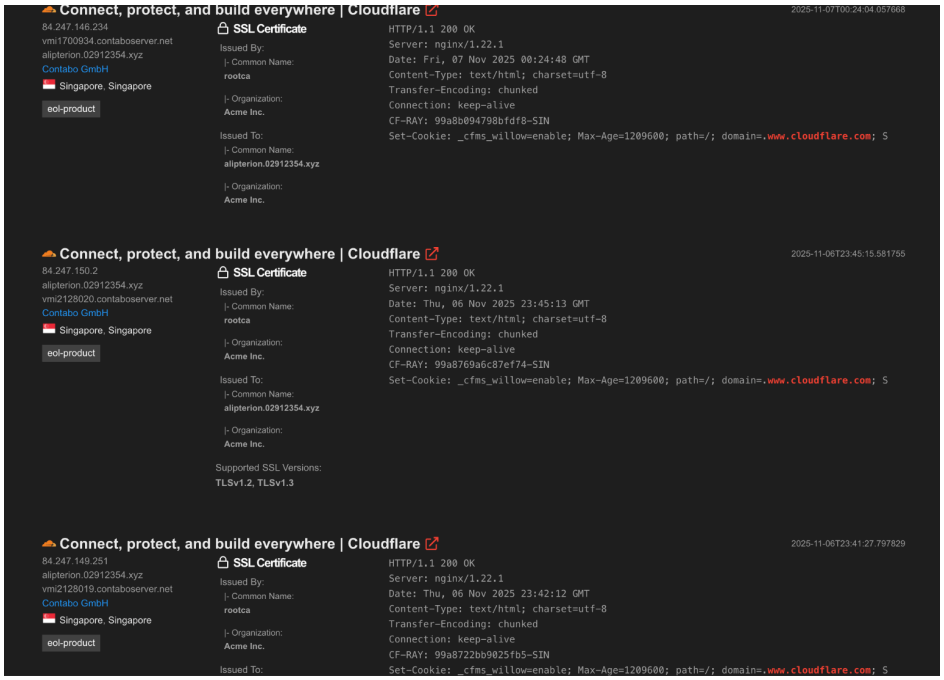
Okta is not used for customer authentication on our systems, and we do not store any customer data in Okta. It is only used for managing the accounts of our employees.

2.2 *Network and Hosting Footprinting*

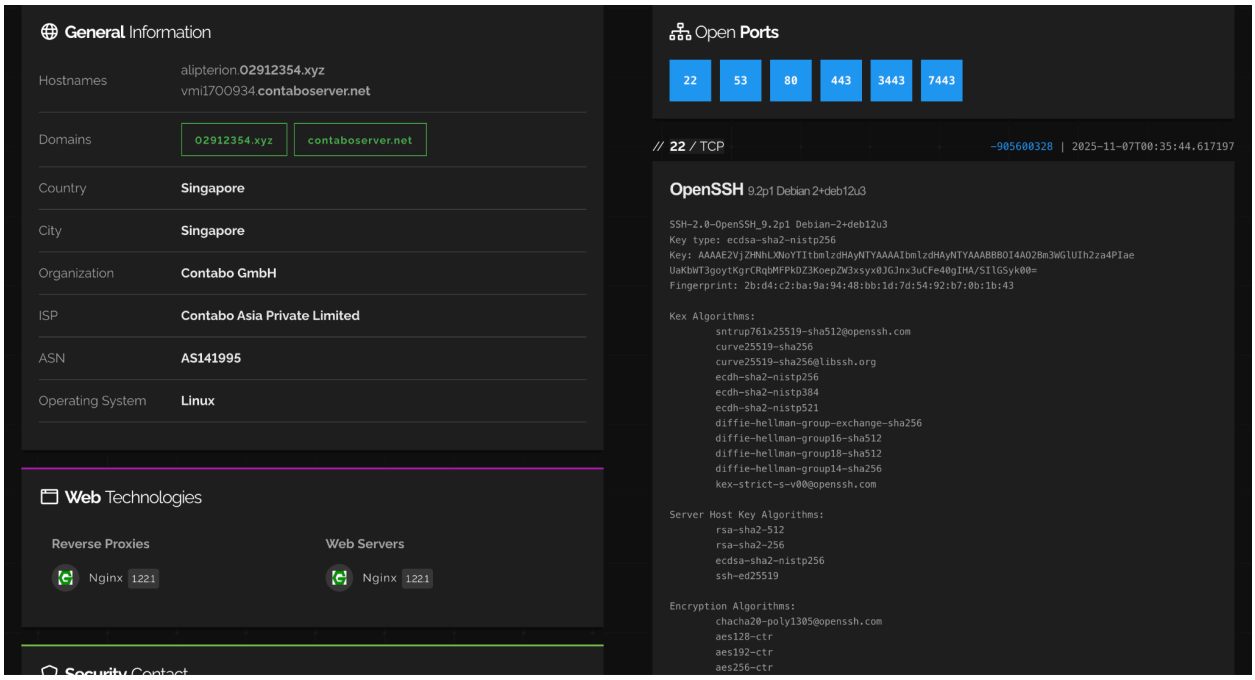
Findings from Shodan

Shodan search results revealed several hosts related to Cloudflare's network infrastructure. The total number of visible records was **686**, distributed across multiple regions including the **United States, Singapore, Japan, Germany, and Hong Kong**. This geographic diversity confirms the use of Cloudflare's **Anycast global network**, where the same IP ranges are announced from multiple data centers worldwide.

Most of the discovered IPs belong to **AS13335 (CLOUDFLARENET)** and are associated with Cloudflare's edge nodes. These nodes act as **reverse proxies** and perform content delivery, TLS termination, and web application firewall (WAF) inspection. The Shodan results consistently displayed Cloudflare's response banners such as Server: Cloudflare and HTTP return codes like 403 Forbidden or direct IP access not allowed, indicating the hosts are intentionally configured to block raw IP access.



Shodan Results


General Information
Hostnames
alipterion.02912354.xyz
vmi1700934.contaboserver.net
Domains
02912354.xyz
contaboserver.net
Country
Singapore
City
Singapore
Organization
Contabo GmbH
ISP
Contabo Asia Private Limited
ASN
AS141995
Operating System
Linux
Web Technologies
Reverse Proxies
Nginx 1221
Web Servers
Nginx 1221
Open Ports
22
53
80
443
3443
7443
// 22 / TCP
-905600328 | 2025-11-07T00:35:44.617197
OpenSSH 9.2p1 Debian 2+deb12u3
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOI4AO2Bm3WGlUIh2za4PIae
UaKbWT3goytKgrCRqbMFPkDZ3KoepZW3xsyx0JGJnx3uCFe40gIHA/SIlGSyk00=
Fingerprint: 2b:d4:c2:ba:9a:94:48:bb:1d:7d:54:92:b7:0b:1b:43
Kex Algorithms:
sntrup761x25519-sha512@openssh.com
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256
kex-strict-s-v00@openssh.com
Server Host Key Algorithms:
rsa-sha2-512
rsa-sha2-256
ecdsa-sha2-nistp256
ssh-ed25519
Encryption Algorithms:
chacha20-poly1305@openssh.com
aes128-ctr
aes192-ctr
aes256-ctr

Open Ports

Port	Protocol	Service Detected	Version	Inference
22/tcp	SSH	OpenSSH	9.2p1 (Debian 12)	Administrative access for server maintenance and management within colocation data centers. Appears on partner-hosted nodes (e.g., Contabo GmbH, Singapore).
53/tcp	DNS	–	–	Likely DNS resolver service supporting Cloudflare's authoritative and recursive DNS operations.
80/tcp	HTTP	nginx	1.22.1	Redirects inbound requests to HTTPS endpoints. Confirms Cloudflare enforces secure transport by default.
443/tcp	HTTPS	nginx	1.22.1	Primary secure web service at the edge; handles TLS termination, WAF inspection, and cookie/session management.
3443/tcp	HTTPS-alt	nginx	1.22.1	Alternate TLS port commonly used for API endpoints and administrative interfaces.
7443/tcp	HTTPS-alt	nginx	1.22.1	Secondary TLS endpoint seen on Singapore nodes; returns Cloudflare headers (CF-RAY) and HSTS policies.

Each service presented Cloudflare's standard TLS response behavior, including the **CF-RAY identifier**, **Strict-Transport-Security (HSTS)** enforcement, and **X-Frame-Options**

headers — all characteristic of Cloudflare's Web Application Firewall (WAF) and HTTP response hardening.

The **SSL certificate data** indicates certificates issued by *Acme Inc. Root CA* (a test or internal CA used for infrastructure validation), while the HTTP headers show the presence of tracking and diagnostic cookies (**_cf_bm, cfz_google-analytics_v4, cfz_adobe**), demonstrating Cloudflare's content delivery and analytics integrations.

Findings from crt.sh

The query site: crt.sh/?q=www.cloudflare.com returned **dozens of valid certificates** recently issued for Cloudflare-managed domains. The screenshot illustrates multiple certificate entries with **issuance dates ranging from October to November 2025**, each valid through early 2026. All observed certificates were issued by **Google Trust Services (CN = WE1 / WR1)**, one of Cloudflare's trusted public Certificate Authorities.

crt.sh Identity Search Group by Issuer

Criteria: Type: Identity Match: ILIKE Search: 'www.cloudflare.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
22240344686	2025-11-05	2025-11-05	2026-02-03	www.cloudflare.com	*.www.cloudflare.com www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
22189652613	2025-11-04	2025-10-24	2026-01-22	th-th.www.cloudflare.com	th-th.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
22173688582	2025-11-03	2025-10-23	2026-01-21	pl-pl.www.cloudflare.com	pl-pl.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
22028910293	2025-10-27	2025-10-23	2026-01-21	www.cloudflare.com	blog.api.www.cloudflare.com www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21997873881	2025-10-25	2025-10-24	2026-01-22	en-gb.www.cloudflare.com	en-gb.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21996127262	2025-10-25	2025-10-23	2026-01-22	en-ca.www.cloudflare.com	en-ca.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21977667264	2025-10-24	2025-10-24	2026-01-22	pt-br.www.cloudflare.com	pt-br.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21978814205	2025-10-24	2025-10-24	2026-01-22	pt-br.www.cloudflare.com	pt-br.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21978810658	2025-10-24	2025-10-24	2026-01-22	pt-br.www.cloudflare.com	pt-br.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21974061450	2025-10-24	2025-10-24	2026-01-22	es-la.www.cloudflare.com	es-la.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21974041135	2025-10-24	2025-10-24	2026-01-22	es-la.www.cloudflare.com	es-la.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21974040999	2025-10-24	2025-10-24	2026-01-22	es-la.www.cloudflare.com	es-la.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21962286304	2025-10-24	2025-10-24	2026-01-22	th-th.www.cloudflare.com	th-th.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21962284028	2025-10-24	2025-10-24	2026-01-22	th-th.www.cloudflare.com	th-th.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21956931839	2025-10-24	2025-10-24	2026-01-22	en-gb.www.cloudflare.com	en-gb.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21956926491	2025-10-24	2025-10-24	2026-01-22	en-gb.www.cloudflare.com	en-gb.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21956268797	2025-10-24	2025-10-24	2026-01-22	ja-jp.www.cloudflare.com	ja-jp.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21956222023	2025-10-24	2025-10-24	2026-01-22	ja-jp.www.cloudflare.com	ja-jp.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21956214998	2025-10-24	2025-10-24	2026-01-22	ja-jp.www.cloudflare.com	ja-jp.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21955226403	2025-10-24	2025-10-23	2026-01-22	es-es.www.cloudflare.com	es-es.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21955224761	2025-10-24	2025-10-23	2026-01-22	es-es.www.cloudflare.com	es-es.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21955202114	2025-10-24	2025-10-23	2026-01-22	es-es.www.cloudflare.com	es-es.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21954916128	2025-10-24	2025-10-23	2026-01-22	en-ca.www.cloudflare.com	en-ca.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21954913115	2025-10-24	2025-10-23	2026-01-22	en-ca.www.cloudflare.com	en-ca.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21954245994	2025-10-23	2025-10-23	2026-01-21	pl-pl.www.cloudflare.com	pl-pl.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21954247849	2025-10-23	2025-10-23	2026-01-21	pl-pl.www.cloudflare.com	pl-pl.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21953505973	2025-10-23	2025-10-23	2026-01-21	id-id.www.cloudflare.com	id-id.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21953496399	2025-10-23	2025-10-23	2026-01-21	id-id.www.cloudflare.com	id-id.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21953490010	2025-10-23	2025-10-23	2026-01-21	id-id.www.cloudflare.com	id-id.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21953319545	2025-10-23	2025-10-23	2026-01-21	en-au.www.cloudflare.com	en-au.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21953294877	2025-10-23	2025-10-23	2026-01-21	en-au.www.cloudflare.com	en-au.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21952511021	2025-10-23	2025-10-23	2026-01-21	en-us.www.cloudflare.com	en-us.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21952513038	2025-10-23	2025-10-23	2026-01-21	en-us.www.cloudflare.com	en-us.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21952503588	2025-10-23	2025-10-23	2026-01-21	en-us.www.cloudflare.com	en-us.www.cloudflare.com	C=US, O=Google Trust Services, CN=WR1
21950487792	2025-10-23	2025-10-23	2026-01-21	pages.www.cloudflare.com	pages.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1
21950497550	2025-10-23	2025-10-23	2026-01-21	pages.www.cloudflare.com	pages.www.cloudflare.com	C=US, O=Google Trust Services, CN=WE1

crt.sh findings

The listed **Common Names (CN)** and **Matching Identities** include a wide range of regional subdomains, such as:

- pl-pl.www.cloudflare.com (Poland)
- blog.api.www.cloudflare.com (API infrastructure)

This broad distribution of localized domains reflects Cloudflare's multilingual and regionally optimized web architecture. Each certificate corresponds to a local content delivery edge node, enabling secure encrypted communication between users and the nearest Cloudflare data center.

2.3 *Company Website*

Articles or blog posts discussing technology used by the company

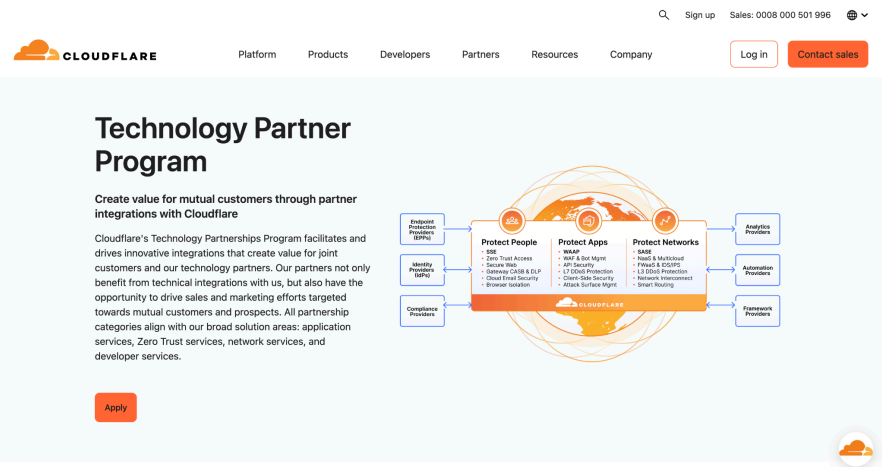
Cloudflare's official website provides extensive information about the technologies it uses, the services it integrates with, and the partnerships that support its global infrastructure. Several sections across the site, including the Technology Partner Program and the Zero Trust Services pages, clearly highlight how Cloudflare collaborates with other major technology providers to deliver its products. *tech partners*

Technology Partner Program

The Technology Partner Program page explains how Cloudflare creates value for customers through collaborations with third-party vendors. It organizes its integrations into three main categories: Protect People, Protect Apps, and Protect Networks.

Protect People focuses on Zero Trust Access, CASB and DLP solutions, Email Security, and Browser Isolation. Protect Apps focuses on Web Application and API Protection, Bot Management, DDoS Defense, and Attack Surface Management. Protect Networks includes network-level technologies such as Secure Access Service Edge, Firewall as a Service, Intrusion Detection and Prevention Systems, and Smart Routing.

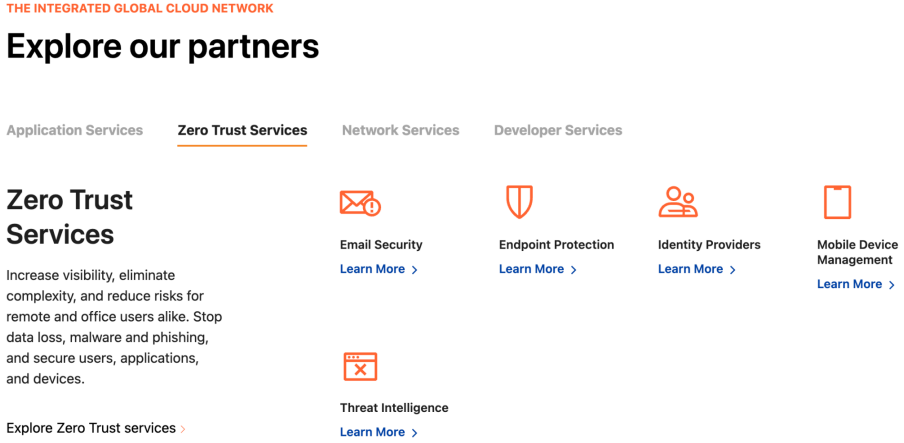
This program demonstrates how Cloudflare aligns its security and networking infrastructure with the needs of enterprises and government clients. The visual on this page clearly represents how Cloudflare connects with multiple categories of partners including endpoint protection, identity management, analytics, automation, and compliance.



Zero Trust Services and Partner Integrations

The Zero Trust Services section describes how Cloudflare helps organizations protect data, users, and devices. It focuses on visibility, risk reduction, and protection against phishing and malware attacks. This section lists specific categories of partners including Email Security, Endpoint Protection, Identity Providers, Mobile Device Management, and Threat Intelligence.

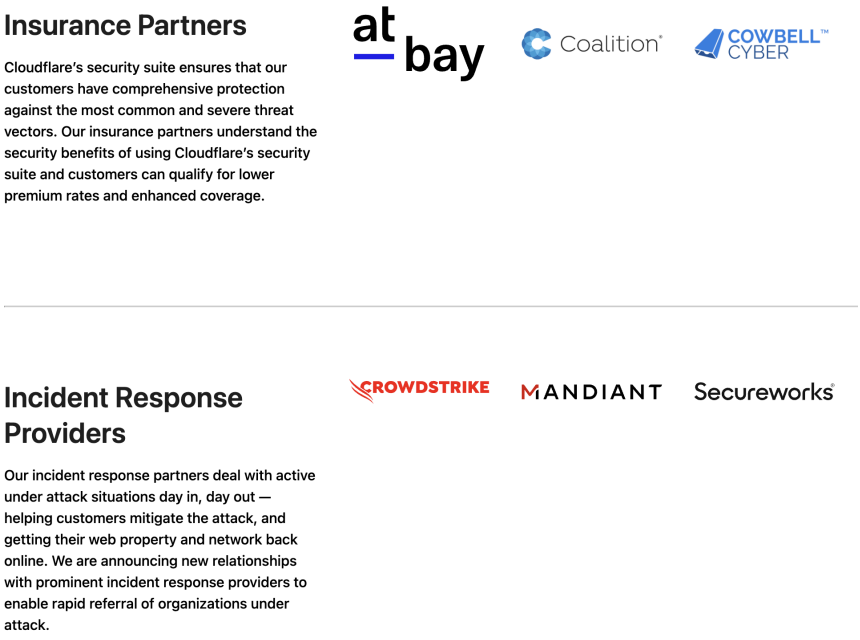
Some of the listed partners are well-known cybersecurity vendors such as Okta, Ping Identity, SentinelOne, and CrowdStrike. Their presence confirms Cloudflare's integration with established identity management and endpoint security platforms. These integrations are crucial for enabling single sign-on, identity-based access, and coordinated response to security incidents.



Incident Response and Insurance Partners

Cloudflare also maintains partnerships with companies that specialize in incident response and cyber insurance. The Incident Response Partners section highlights collaborations with CrowdStrike, Mandiant, and Secureworks. These firms are recognized for their expertise in responding to active security threats and helping organizations recover quickly after an attack.

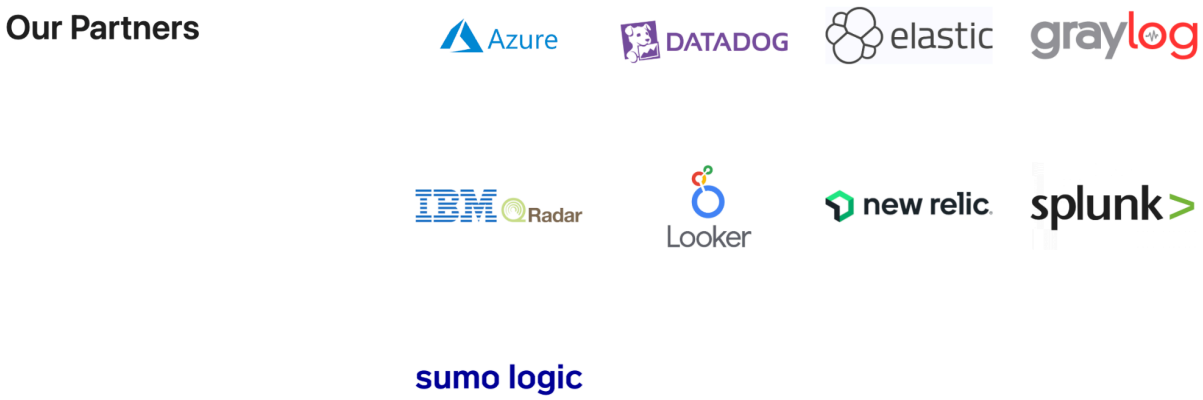
The Insurance Partners section lists At-Bay, Coalition, and Cowbell Cyber. This indicates that Cloudflare's customers can benefit from improved insurance coverage and reduced premiums when using Cloudflare's security products. These partnerships reflect Cloudflare's effort to combine preventive and reactive security measures for comprehensive risk management.



Analytics and Observability Partners

The Partners page also lists vendors that integrate with Cloudflare to enhance monitoring, analytics, and performance management. These include Datadog, Elastic, Graylog, IBM QRadar, New Relic, Sumo Logic, Splunk, and Looker. Such integrations allow Cloudflare's customers to analyze web traffic, application performance, and security logs directly through their existing observability tools.

These partnerships provide valuable insight into the organization's operational visibility strategy. They show that Cloudflare supports a diverse set of enterprise analytics platforms, ensuring interoperability between its edge network and customer monitoring environments.



The company's website features many more collaborations across security, networking, analytics, and cloud infrastructure categories. Listing every vendor is unnecessary for this report, but it is clear that Cloudflare maintains an extensive and well-structured partner ecosystem that supports nearly every aspect of its platform. This broad network of integrations demonstrates Cloudflare's scale and flexibility, allowing it to combine its own products with leading technologies across the cybersecurity and enterprise cloud industries.

Job postings containing information of technical requirements

Cloudflare's career listings provide detailed insights into the company's technical environment and the skills expected from its engineering staff. The job descriptions reveal the internal technology stack, development tools, and automation frameworks used across various departments. jobs

For instance, the **Engineering Manager, Support Operations** position outlines Cloudflare's primary technical environment, including the use of **Workers**, **Durable Objects**, **D1**, **KV**, and **Vectorize** within the Cloudflare platform. It also highlights automation practices using **Python**, **TypeScript**, and **JavaScript**, along with REST and GraphQL API integration and modern CI/CD development pipelines. This reflects Cloudflare's commitment to scalable automation, real-time event processing, and integration of AI workflows into its systems. *Eng-Manager role*

Technical Environment

Primary Stack: Cloudflare platform (Workers, Durable Objects, D1, KV, Vectorize)
Automation: Custom tooling (Python, TypeScript/JavaScript), workflow automation
Integration: REST/GraphQL APIs, Salesforce Service Cloud, internal systems
AI Workflows: Workers AI, agent orchestration, real-time event processing
Development: Modern CI/CD, monitoring and observability tools

Who You Are

Required Experience

- **5+ years** as an Engineering Manager or Senior Engineer leading technical teams
- **Full-stack engineering**: Strong coding ability in modern languages (TypeScript, Python, JavaScript)
- **Automation focus**: Track record building workflow automation and productivity tools
- **API integration**: Experience integrating enterprise systems and managing data pipelines
- **Stakeholder partnership**: Comfort working with non-technical stakeholders to translate business needs into technical solutions
- **Hands-on leadership**: Ability to code and architect solutions while managing a small team

Preferred Background

- **Cloudflare platform experience**: Workers, Durable Objects, or other Cloudflare developer tools (strongly preferred)
- **Support operations domain**: Experience with support ticketing systems (Salesforce Service Cloud, Zendesk) and agent workflows
- **AI/ML integration**: Experience integrating AI capabilities into operational workflows
- **Enterprise B2B**: Experience with SaaS platforms, high-availability systems, and security requirements
- **Product mindset**: Comfort designing solutions vs executing detailed tickets

Engineering Manager tech requirements

The **Network Security Engineer** posting focuses on operational defense capabilities, specifying experience in troubleshooting **DNS**, **SSL/TLS**, and **HTTP** protocols, alongside

skills in **Bash**, **Python**, and **JavaScript** scripting. It also emphasizes practical experience with tools such as **curl**, **traceroute**, **openssl**, and **git**, as well as a solid understanding of **network protocols** like TCP, UDP, BGP, and GRE. *Security Engineer*

Skills, Knowledge, and Experience

- Fluent English speaker is a requirement
- Minimum 3 years working within a Technical Support team solving various technical issues
- Self-driven and capable of learning new technologies / systems / features with little guidance
- Fundamental understanding how the Internet works (OSI Model)
- Advanced understanding of internet protocols like TCP and UDP
- Computer Networking fundamentals, experience with iptables and looking glass
- Experience troubleshooting network connectivity issues, BGP routing, and GRE tunnels
- Packet capture analysis
- Experience in command line and tools, including curl, dig, traceroute, openssl, git
- Experience troubleshooting DNS, SSL / TLS, HTTP
- Experience in a web development and / or hosting environment such as installing and configuring web servers like Apache, Nginx, Caddy and IIS
- Experience writing scripts in Bash, Python, JavaScript or other scripting language
- Experience in working as part of a team in a customer-facing role

Responsibilities

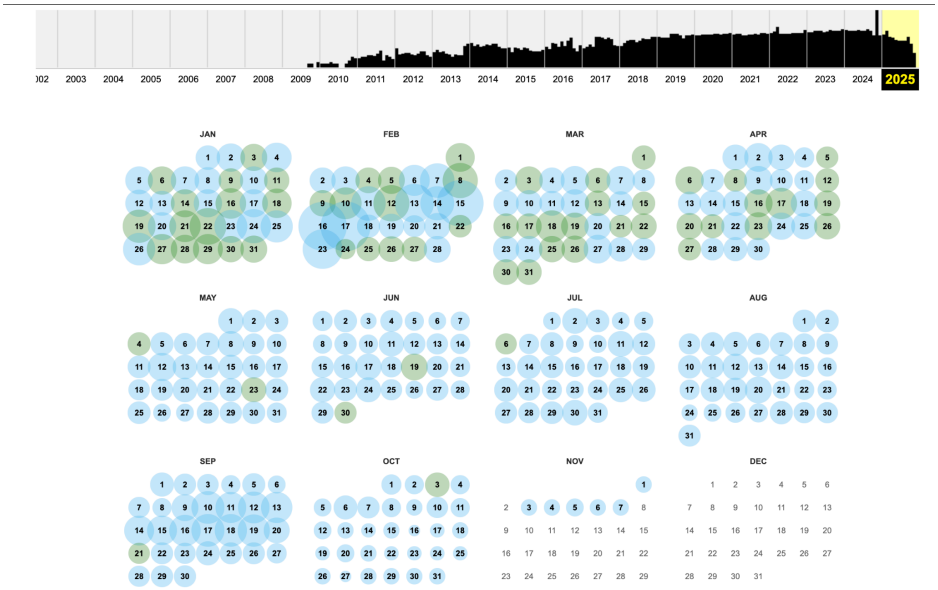
- Communicate with customers via chat, email, and phone
- Compare traffic signatures and attributes including IP addresses, cookie variations, HTTP headers, and JavaScript footprints to determine what is good traffic and what is malicious
- DDoS mitigation for OSI layers 3,4, & 7: advise customers on how to filter malicious traffic using Cloudflare tools like Magic Transit, Network Firewall, WAF, IP reputation lists, packet inspection, blocklisting, allowlisting, and rate limiting
- Work with Engineering and Operations teams to mitigate attacks, suggest steps to mitigate, and apply the appropriate mitigation when applicable
- Work with Engineering and Product teams to improve products and tools

Network Security Engineer requirements

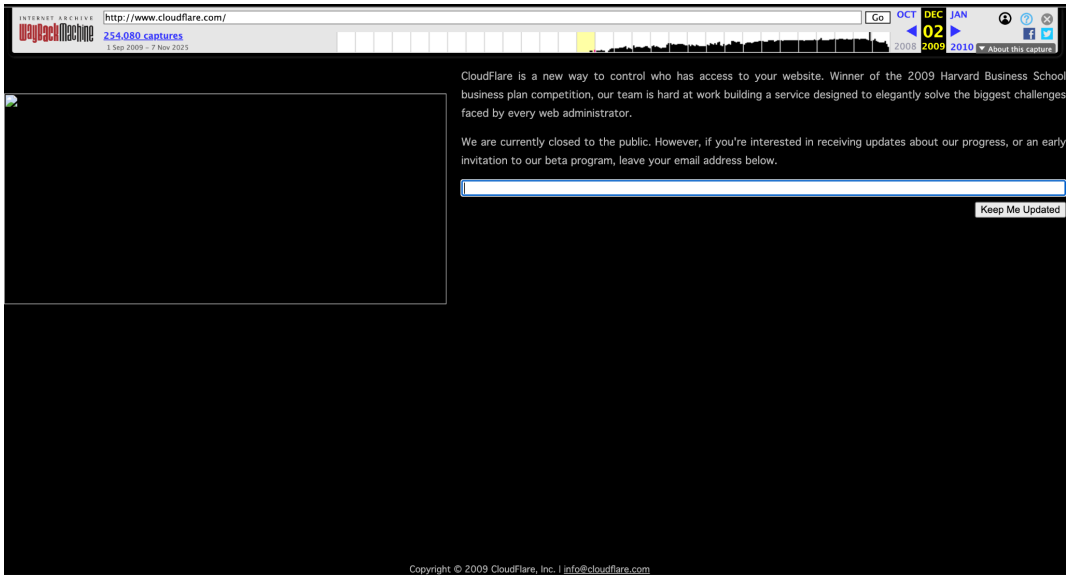
Both listings collectively indicate Cloudflare's preference for candidates with strong knowledge of networking fundamentals, cloud automation, and distributed systems management. The mention of **DDoS mitigation**, **packet analysis**, and **traffic signature inspection** suggests that Cloudflare integrates its employees directly into its global defense and incident response infrastructure.

These job postings serve as clear evidence of the organization's modern, cloud-centric engineering environment. They reveal that Cloudflare prioritizes skills related to **web security**, **DevOps automation**, and **API-driven system design**, offering a transparent view of the technical ecosystem that supports its worldwide operations.

Archived Website Analysis

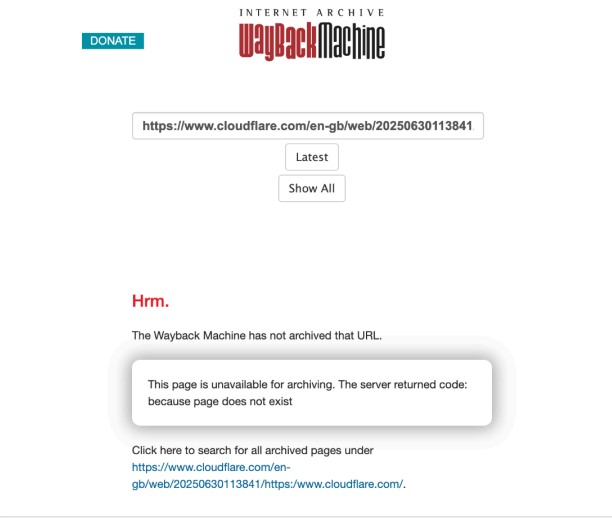


An archived analysis of Cloudflare's website using the **Wayback Machine** provides insight into the organization's online evolution and the technological shifts since its early development phase. The earliest available snapshot, dated **December 2009**, presents a simple landing page where Cloudflare describes itself as a "new way to control who has access to your website." At that time, the company was in its **beta stage**, accessible only by invitation. The design and structure of the archived site were minimal, featuring no visible front-end framework or advanced web technologies, indicating the company's early-stage focus on functionality rather than full-scale deployment.



darivxe - Cloudflare footprint

This early version provides a historical reference point showing Cloudflare's origins as a small startup emerging from a Harvard Business School project. No traces of the advanced services now synonymous with the platform, such as CDN optimization, DDoS protection, or edge computing were evident in that archive. This confirms that the company's infrastructure and technology stack expanded progressively over time as its network grew into a globally distributed cloud service provider.



Accessing the latest snapshot of Cloudflare site

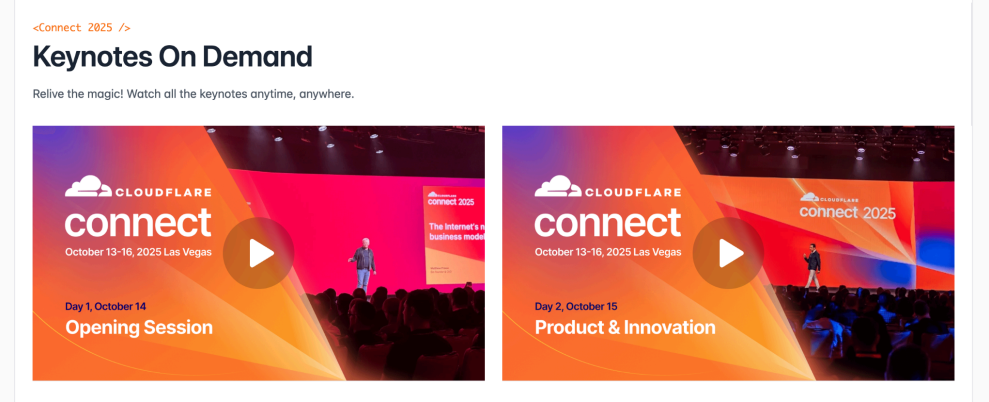
Attempts to access more recent archived versions, such as the **2025 snapshot** of **https://www.cloudflare.com/en-gb/web**, returned an error indicating that the page had not been archived or no longer exists. This is a common occurrence for high-security domains and dynamic, CDN-driven sites like Cloudflare's, which often implement anti-crawling measures and dynamic loading mechanisms that prevent automated archiving tools from capturing full content.

The contrast between the 2009 and 2025 results illustrates Cloudflare's transition from a private, invitation-based startup to a globally recognized cloud security and performance company. The lack of accessible modern archives further highlights the organization's security maturity and content protection posture, suggesting intentional measures to prevent third-party archival of sensitive infrastructure information.

Company Events and Technology Forums

Cloudflare's website shows that the company is consistently involved in active industry engagement through events, webinars, and keynote sessions. The News and Resources section highlights regular insight posts covering topics such as cyber resilience, AI-driven security strategies, and service-focused security outcomes. These articles demonstrate Cloudflare's effort to educate the public on emerging threats and modern defensive approaches.

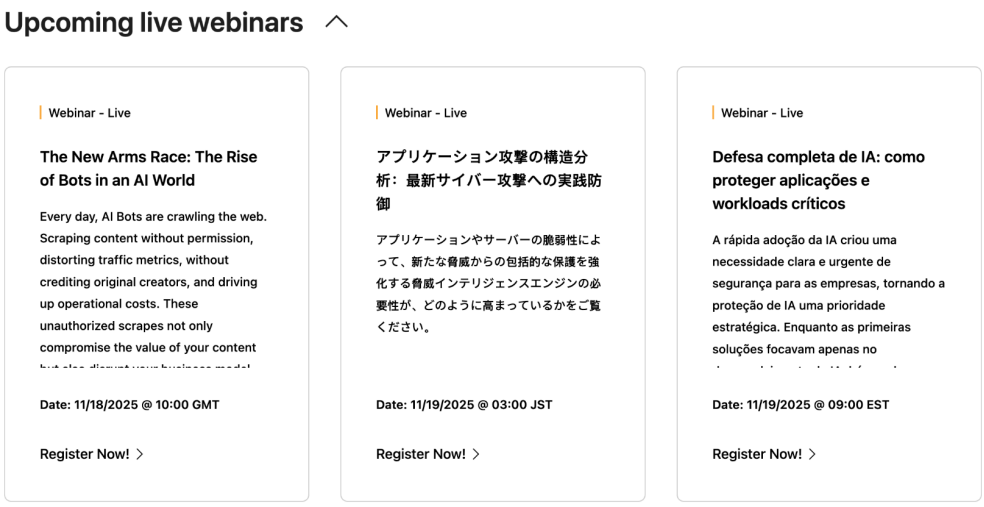
The Events section provides even stronger evidence of Cloudflare's ongoing activity. Cloudflare Connect 2025, held in Las Vegas from October 13 to 16, is featured with full keynote recordings for the opening session and the product and innovation session but can only be accessed by registering with business mail. Cloudflare has already announced the next edition, Cloudflare Connect 2026, scheduled for October 19 to 22 in San Francisco, indicating that these technology-focused gatherings are an annual tradition. *connect-25* *connect-26*



Cloudflare Connect 2025 Keynotes & 2026 Event Details

darivxe - Cloudflare footprint

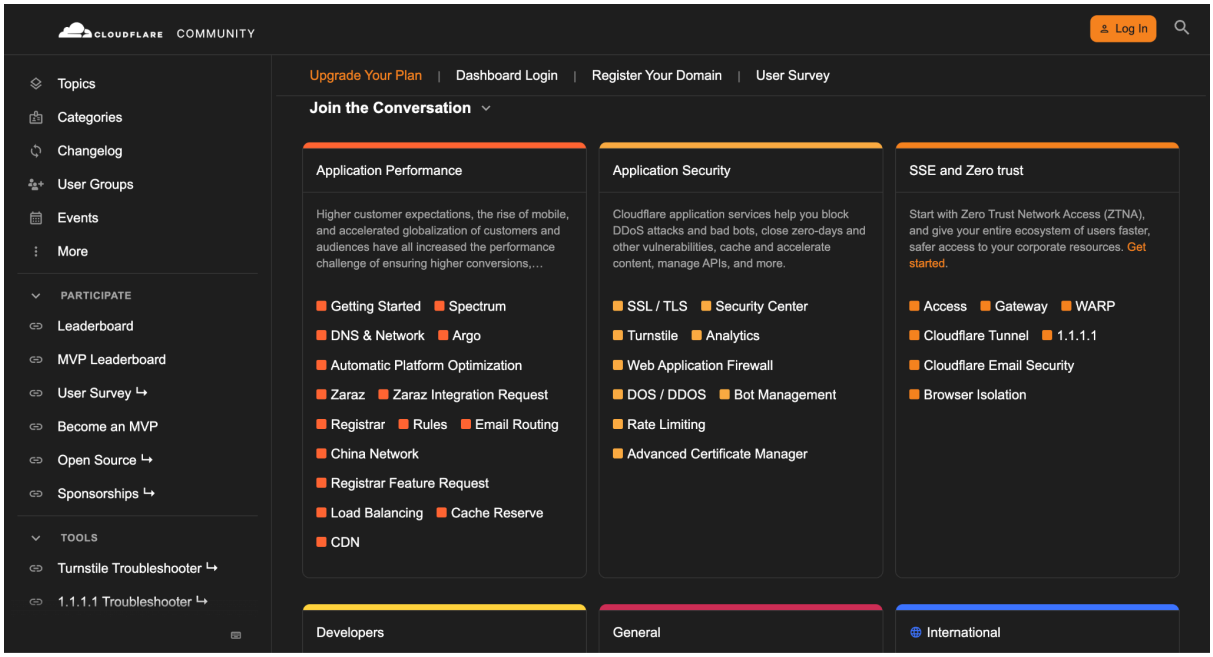
Cloudflare also maintains a steady lineup of **upcoming live webinars** that focus on real-time security challenges and modern threat trends. The schedule features sessions like *"The New Arms Race: The Rise of Bots in an AI World"* and a deep-dive analysis on application-layer attacks, with additional webinars covering advanced defensive strategies across different regions and languages. These events collectively reinforce Cloudflare's commitment to continuous security education, giving global audiences regular opportunities to learn about emerging threats and stay aligned with best practices.



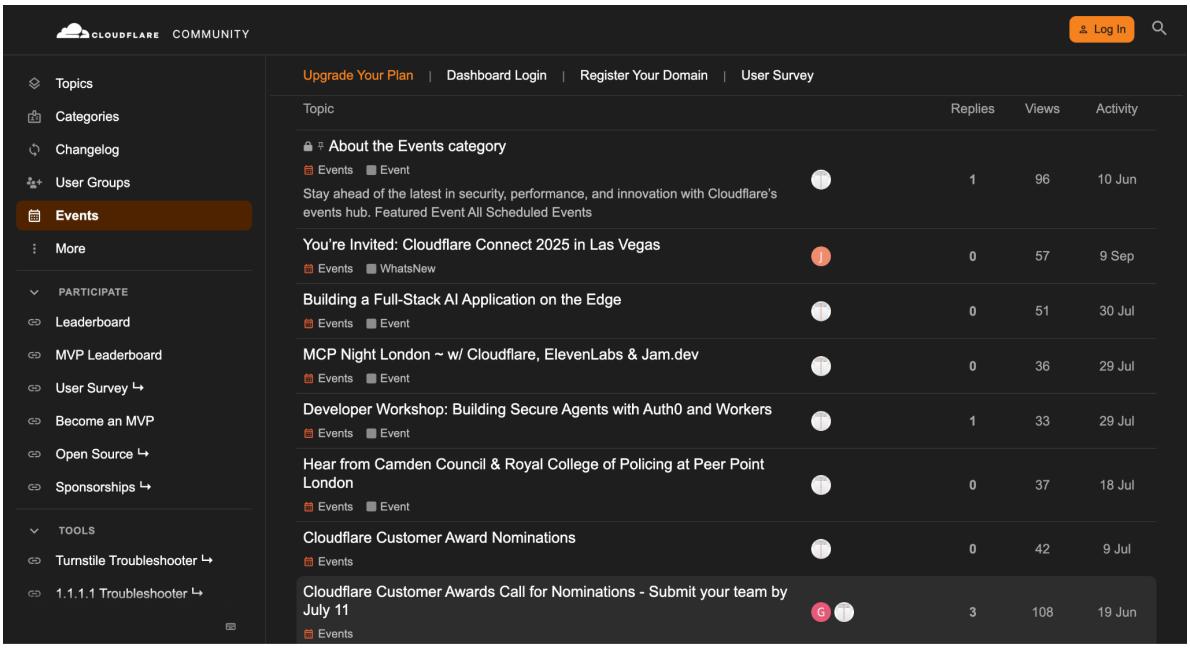
Cloudflare's Upcoming live webinars

Cloudflare's BiWeekly Workshops

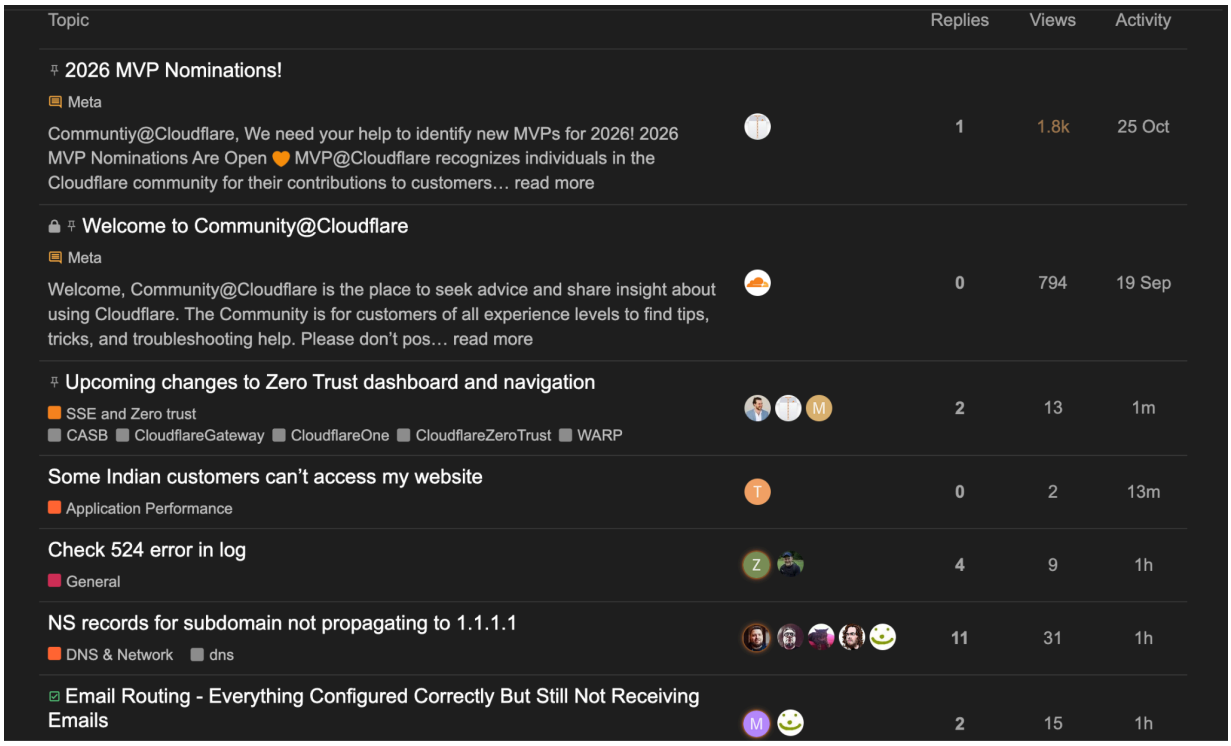
The company's community forum further reinforces this commitment. The Events category lists workshops such as Building a Full-Stack AI Application on the Edge, and in-person meetups hosted in cities such as London. Beyond events, the forum includes active discussions across application performance, application security, and Zero Trust, providing a continuous space for users and Cloudflare engineers to collaborate, troubleshoot, and share knowledge. *community*



Cloudflare's Community and Events



darivxe - Cloudflare footprint



Topic	Replies	Views	Activity
2026 MVP Nominations! Meta — Communtiy@Cloudflare, We need your help to identify new MVPs for 2026! 2026 MVP Nominations Are Open MVP@Cloudflare recognizes individuals in the Cloudflare community for their contributions to customers… read more	1	1.8k	25 Oct
Welcome to Community@Cloudflare Meta — Welcome, Community@Cloudflare is the place to seek advice and share insight about using Cloudflare. The Community is for customers of all experience levels to find tips, tricks, and troubleshooting help. Please don't pos… read more	0	794	19 Sep
Upcoming changes to Zero Trust dashboard and navigation SSE and Zero trust CASB CloudflareGateway CloudflareOne CloudflareZeroTrust WARP	2	13	1m
Some Indian customers can't access my website Application Performance	0	2	13m
Check 524 error in log General	4	9	1h
NS records for subdomain not propagating to 1.1.1.1 DNS & Network dns	11	31	1h
Email Routing - Everything Configured Correctly But Still Not Receiving Emails	2	15	1h

Community Forums

Taken together, the webinars, conferences, and community-driven events demonstrate Cloudflare's consistent investment in open communication and technical outreach. The company does not limit itself to selling security services but places equal importance on fostering education, innovation, and active dialogue across the global technology ecosystem.

2.4 *Personnel*

Cloudflare maintains a highly transparent organizational presence online, making it easy to map parts of its hierarchy through open-source intelligence. The company's official "*People*" page features numerous executives, directors, engineers, and managers across multiple regions, giving a broad initial view of leadership roles and departmental structure.

To keep the scope focused, I narrowed the review to three employees whose publicly available profiles provide clear insight into Cloudflare's skill expectations, professional culture, and technical priorities. These individuals were selected from Cloudflare's own directory and cross-validated through LinkedIn, GitHub, X, and personal websites.

Employee 1: Daniella Vallurupalli – VP, Head of Global Communications

Daniella appears both on Cloudflare's corporate leadership page and across external OSINT sources, including LinkedIn and a public contact site. Her role places her in the upper tier of Cloudflare's organizational hierarchy, overseeing global communications strategy. Through LinkedIn endorsements and her professional history, her core skill set becomes obvious. She demonstrates strong capabilities in public relations, media relations, brand strategy, and marketing communications, each backed by dozens of peer endorsements, including colleagues within Cloudflare itself. *contactout*

Daniella Vallurupalli

Vice President, Head of Global Communications at Cloudflare | San Francisco, California, United States

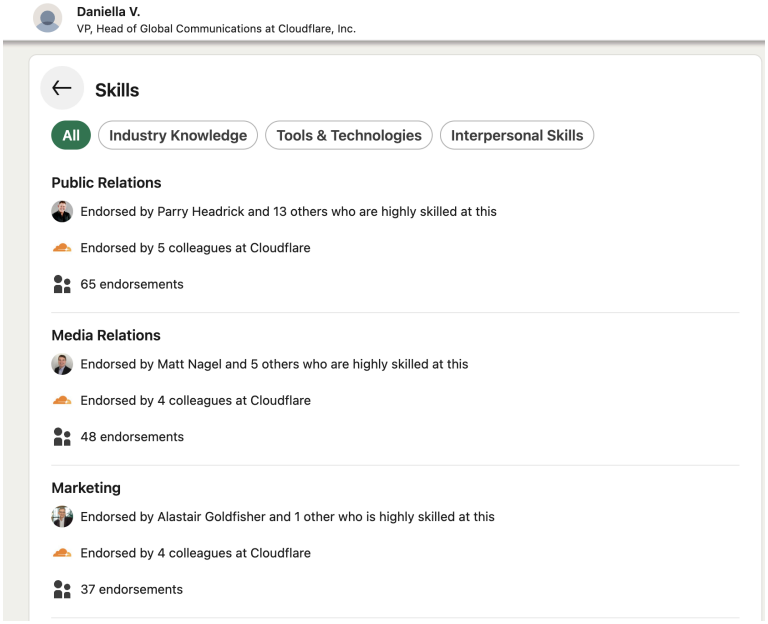
View Daniella Vallurupalli's Email & Phone Number

Daniella Vallurupalli Socials

Daniella Vallurupalli Work

- Vice President, Head of Global Communications at Cloudflare in June 2014 to Present
- Head Of Global Communications at Cloudflare in June 2014 to Present
- Vice Chair, Board of Directors at Saint Francis Foundation, San Francisco in December 2019 to August 2021
- Senior Manager, Global Public Relations at Appirio in August 2013 to May 2014
- Public Relations Manager at SAP Cloud/ SuccessFactors in October 2012 to August 2013
- Senior Account Executive at SHIFT Communications in November 2011 to August 2012
- Account Executive at SHIFT Communications in July 2010 to November 2011

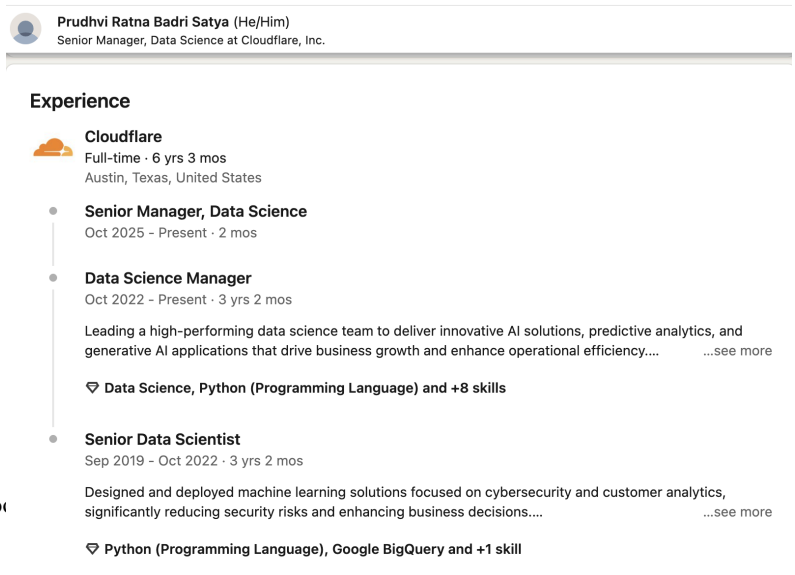
Her career progression highlights the company's expectations for senior communication leadership: expertise in strategic storytelling, crisis communication, media engagement, cross-department coordination, and stakeholder relationships. Her long tenure at Cloudflare further confirms her alignment with the company's cultural emphasis on transparency, brand trust, and rapid communication during high-visibility technical incidents. *linkedin-profile*



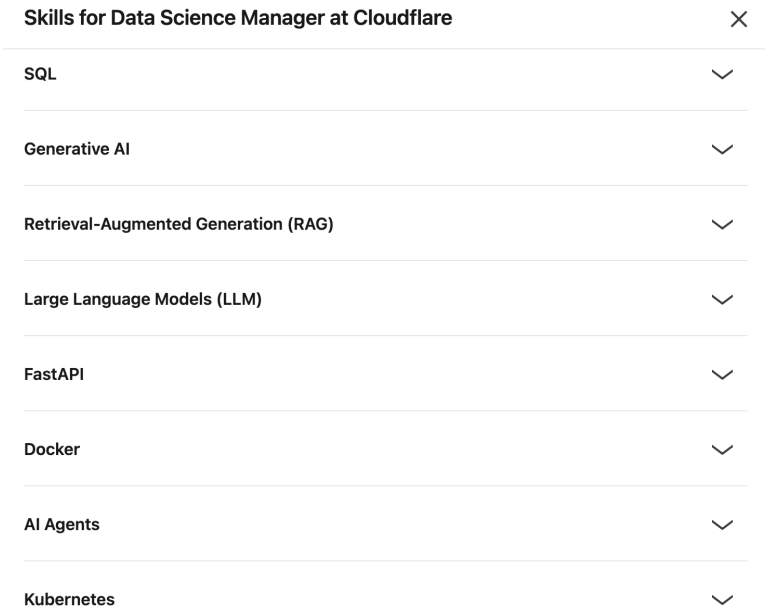
Danielle's Skills

Employee 2: Prudhvi Ratna Badri Satya – Senior Manager, Data Science

Prudhvi's LinkedIn and GitHub profiles provide a clear OSINT trail that reflects Cloudflare's data-driven engineering culture. *linkedin profile*



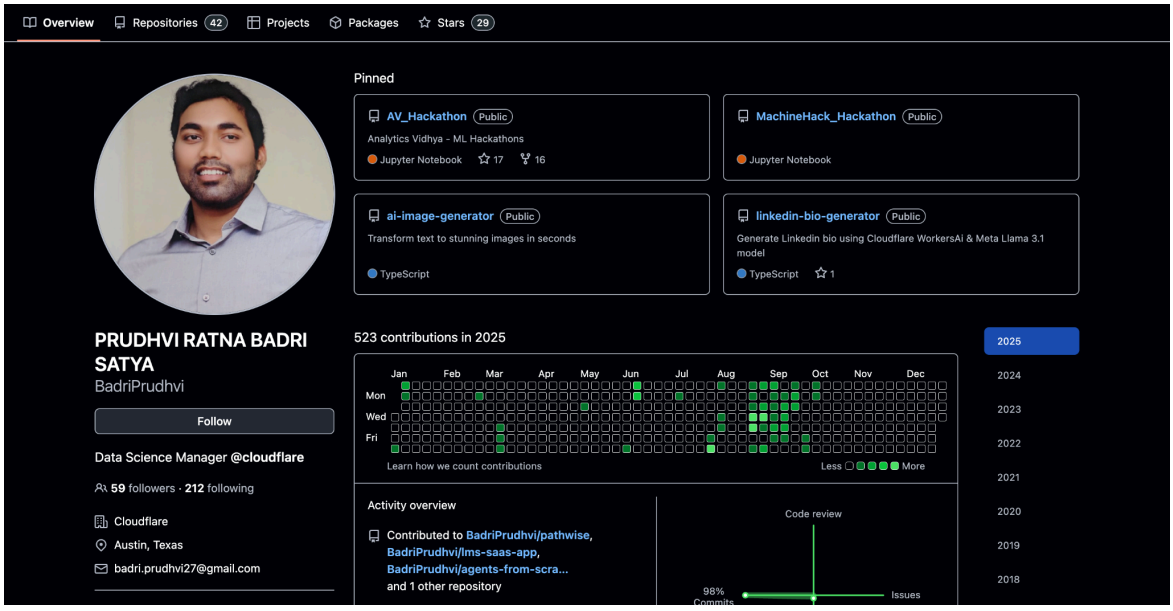
darivxe - Cloudflare fo



Additional skills of a Data Science Manager at Cloudflare

LinkedIn expands this picture with a detailed skill profile. Cloudflare endorses him for advanced capabilities in SQL, generative AI,

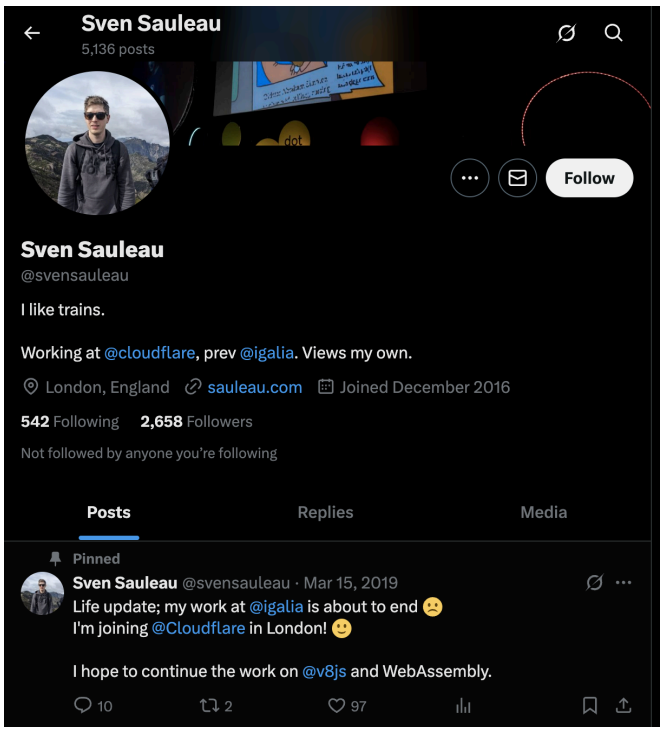
His *GitHub* shows active involvement in machine learning, generative AI, and analytics-focused repositories, some of which directly use Cloudflare Workers and AI tooling. His contribution timeline indicates ongoing work throughout 2025.



darivxe - Cloudflare footprint

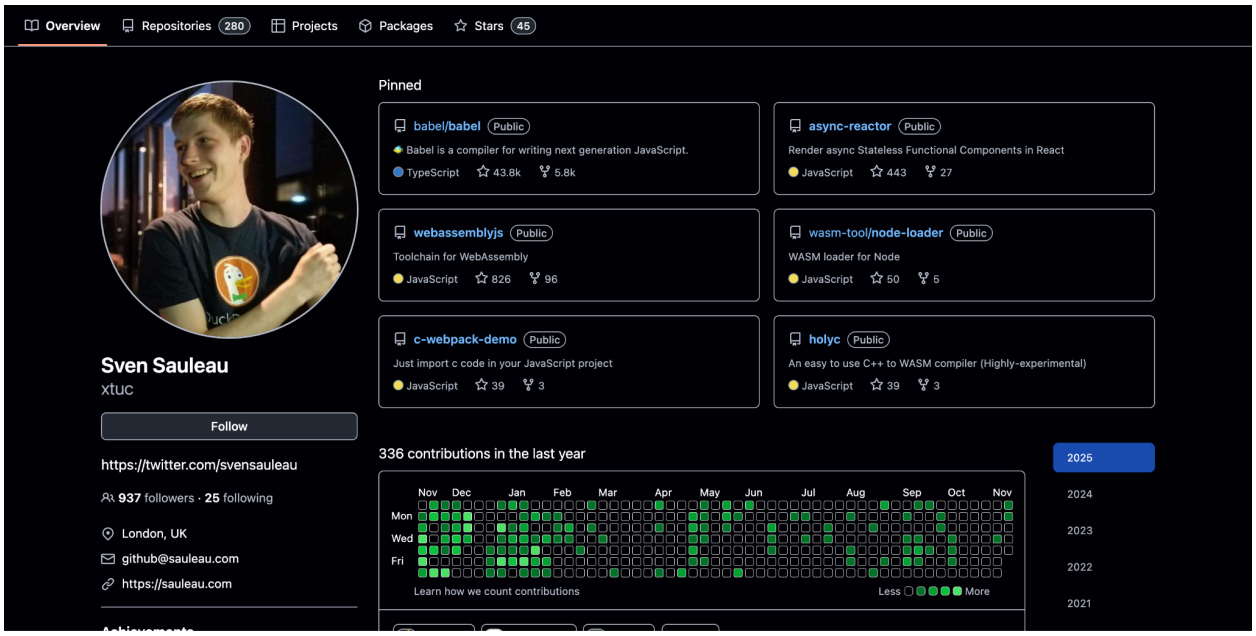
Employee 3: Sven Sauleau – Software Engineer, Open Source Contributor

Sven is listed among Cloudflare's engineering staff and maintains a strong footprint across X, personal blogs, and GitHub. His public posts confirm his long-term engineering position at Cloudflare, while his GitHub activity and portfolio reveal his technical specialties. He actively contributes to high-impact open-source ecosystems like Babel, JavaScript engines, and WebAssembly. *sven's portfolio* *X-profile*

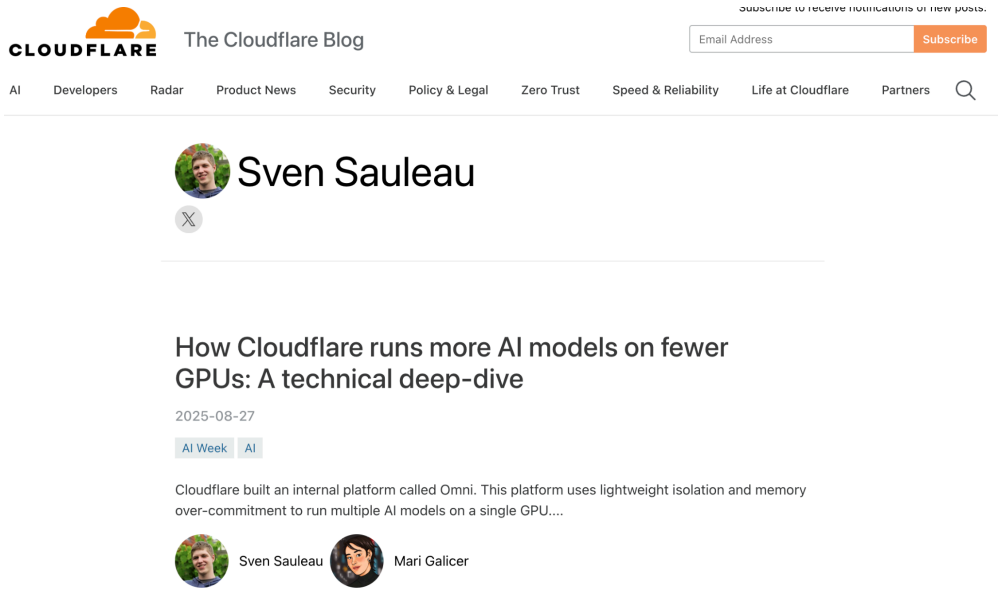


Sven's X profile

His GitHub repositories and contribution graph confirm constant hands-on engineering activity throughout the year. His personal website complements this by showing his professional identity as a JavaScript and WebAssembly specialist with additional interest in Rust. These combined indicators reveal the technical skill expectations for Cloudflare's engineering teams: deep JavaScript knowledge, familiarity with distributed systems, open-source engagement, and comfort working with cutting-edge runtimes like Workers and WASM. *github profile*



Sven's Github

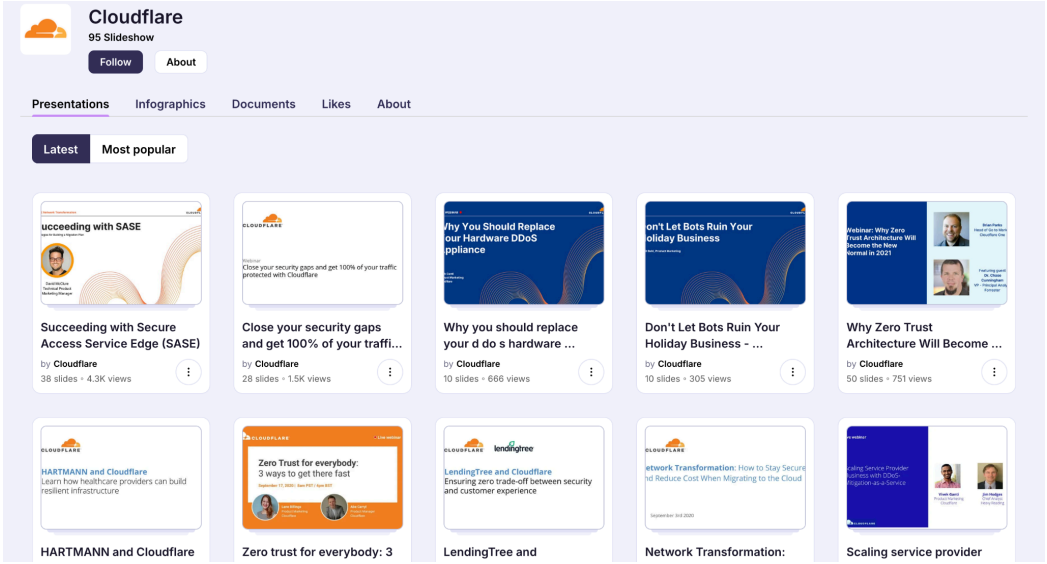


Sven's Articles on Cloudflare Blog

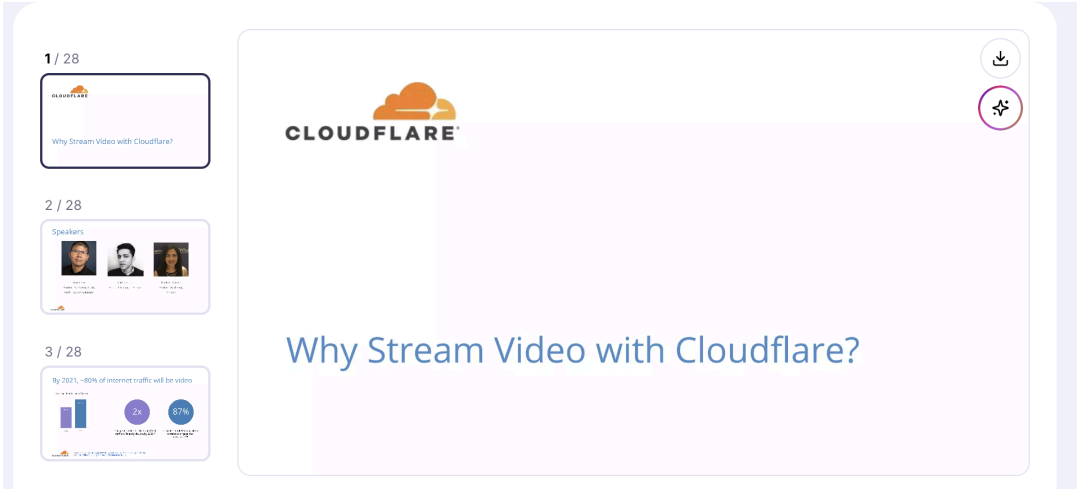
2.5 *Public Documents*

Shared Presentation Slides

Several Cloudflare employees have previously uploaded conference slide decks to public platforms such as Slideshare. These presentations usually cover topics like web performance optimization and several others. The availability of these decks indicates that Cloudflare regularly participates in public conferences, technical meetups, and industry events where staff present their work, research, or new product capabilities. *slideshare profile*



Slideshare Profile

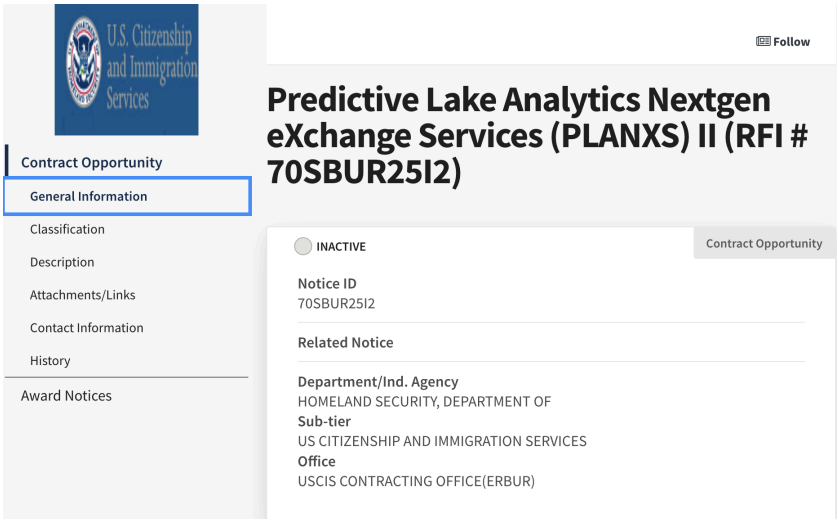


darivxe - Cloudflare footprint

Documents, invoices and Forms

PLANXS Contract

The SAM.gov procurement notice for the PLANXS II program lists Cloudflare among the required operations technologies, which indicates the government contract is specifying Cloudflare as a purchased or planned technology component. *sam.gov*

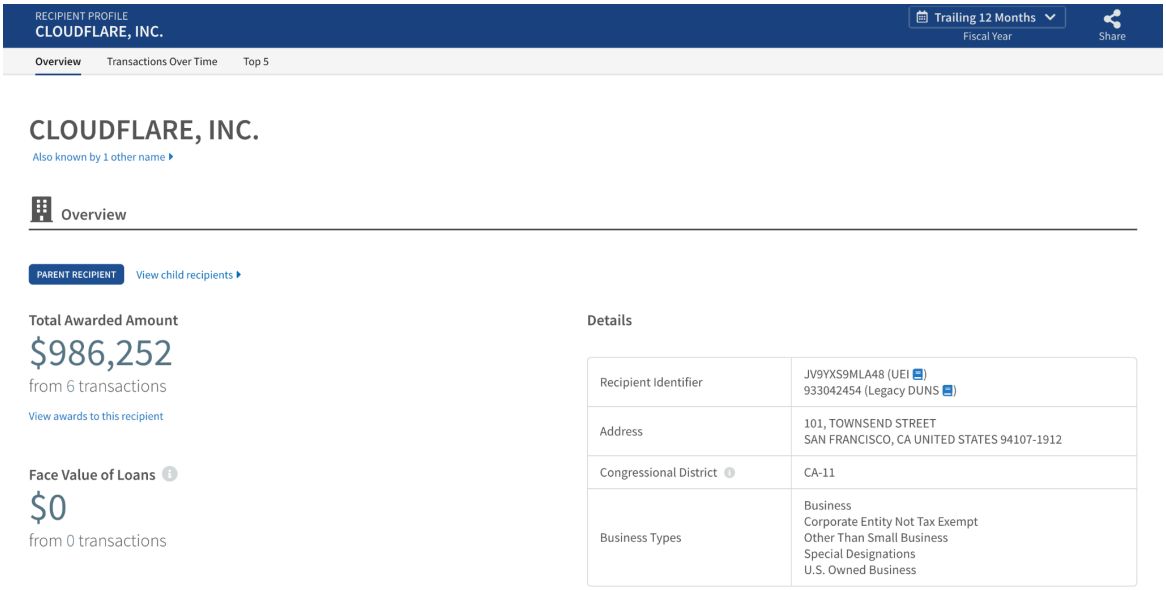


Contract Opportunity

Cloudflare being listed

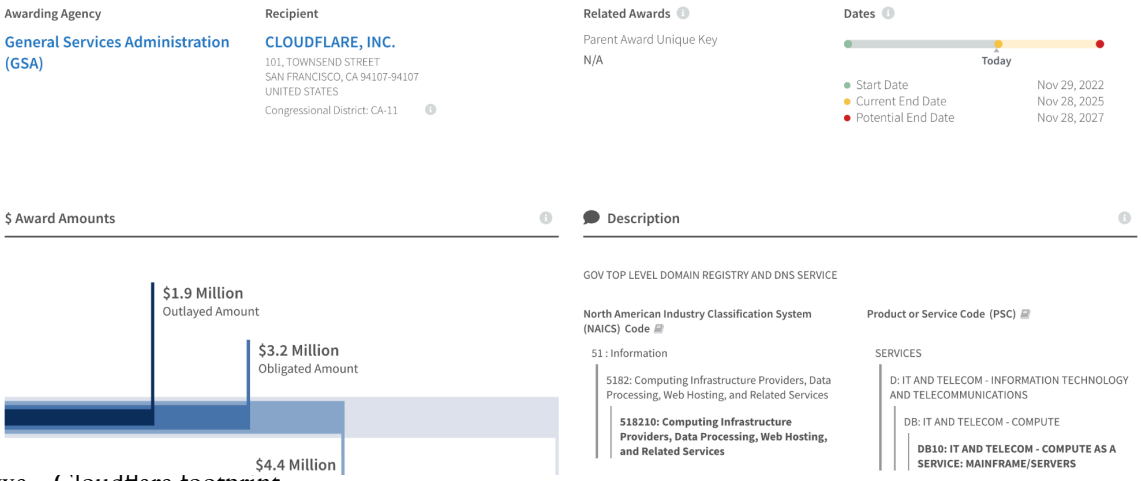
CloudFlare Award Contract

A second relevant document appears on USAspending.gov, which lists an active federal contract awarded to Cloudflare, Inc. by the General Services Administration (GSA). The contract profile clearly lists Cloudflare as the recipient, and the award remains in progress, with its performance period extending from November 29, 2022 to November 28, 2025, and a potential extension through 2027. *usaspending contract*



Cloudflare being listed

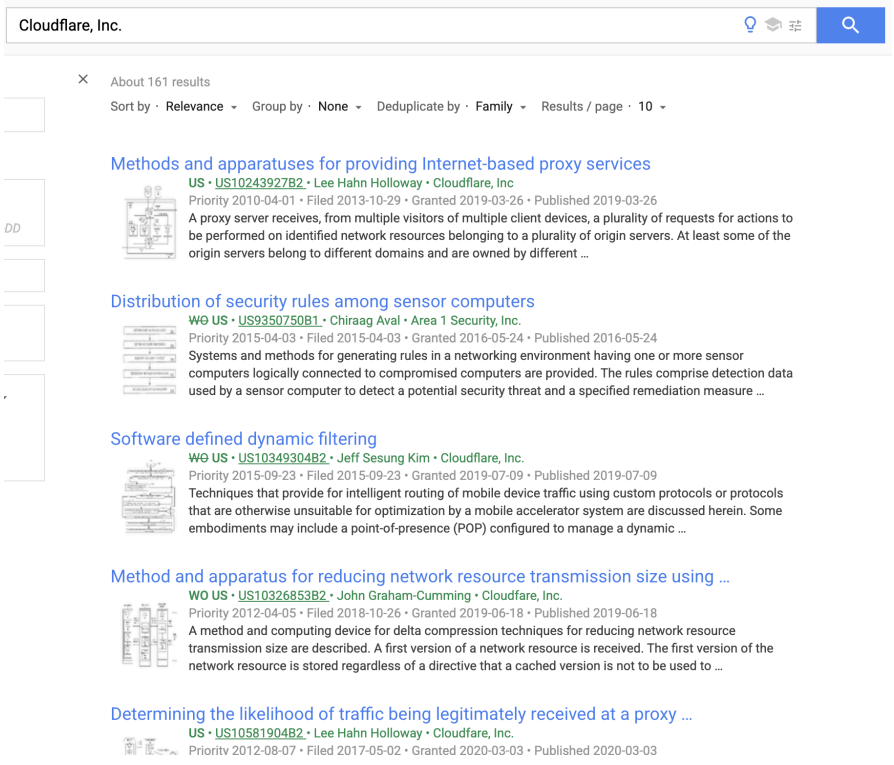
The award amount information shows a total obligation exceeding 3.2 million USD, with 1.9 million USD already outlaid. The description states that the contract covers Top-Level Domain Registry and DNS services, linking Cloudflare directly to federal infrastructure for domain and DNS operations.



darivxe - Cloudflare footprint

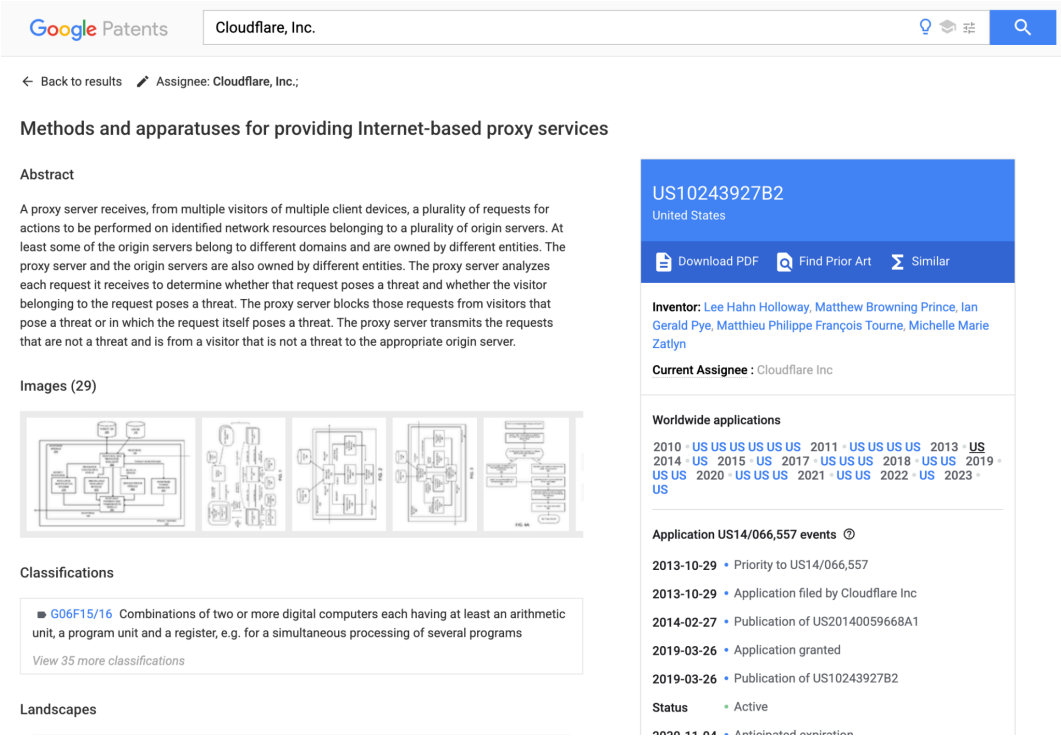
The document further categorizes the work under the **North American Industry Classification System (NAICS)** code *518210*, which corresponds to **Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services**. This confirms Cloudflare is being purchased specifically for hosting, DNS, and IT service capabilities within government operations.

Patent Filings



Cloudflare on Google Patents

A search on Google Patents for the assignee Cloudflare, Inc. returned multiple filings, confirming that the company actively develops proprietary technology. One of the patents identified is US10243927B2. The patent describes a system where a proxy server processes requests from multiple client devices, determines whether each request is a threat, and selectively blocks or forwards traffic to origin servers.



One of the Patents

Industry Reports Indicating Use of Specific Technology

Multiple publicly available industry and analyst reports reference Cloudflare's technology stack, strategic positioning, and product capabilities. These reports provide third-party validation of the company's technical direction and adoption across sectors.

Klover.AI Report

This document evaluates Cloudflare's approach to AI-driven infrastructure, including Workers AI, R2 Storage, Vectorize, and AI Gateway. It highlights how Cloudflare is positioning its network and serverless platform as an alternative to hyperscale cloud providers for AI workloads, essentially confirming Cloudflare's active use of edge-based AI technologies. *klover.ai*

Cloudflare's AI Strategy: Analysis of Dominance in Cloud, CDN, Cybersecurity AI

The report explores how Cloudflare's AI strategy will dominate in cloud: content delivery network services, cybersecurity, DDoS mitigation. The report includes the most exhaustive ai strategy analysis complete with references and works cited by Dany Kitishian of Klover.AI.

Cloudflare AI Strategy Executive Summary

This report presents an exhaustive analysis of Cloudflare, Inc.'s strategic positioning within the artificial intelligence (AI) sector, concluding that the company is poised to achieve a dominant market position. This dominance will not be achieved through a direct, capital-intensive war with hyperscale cloud providers—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—over the market for large-scale AI model training. Instead, Cloudflare is executing a sophisticated, asymmetric strategy to redefine the AI value chain around the network edge.

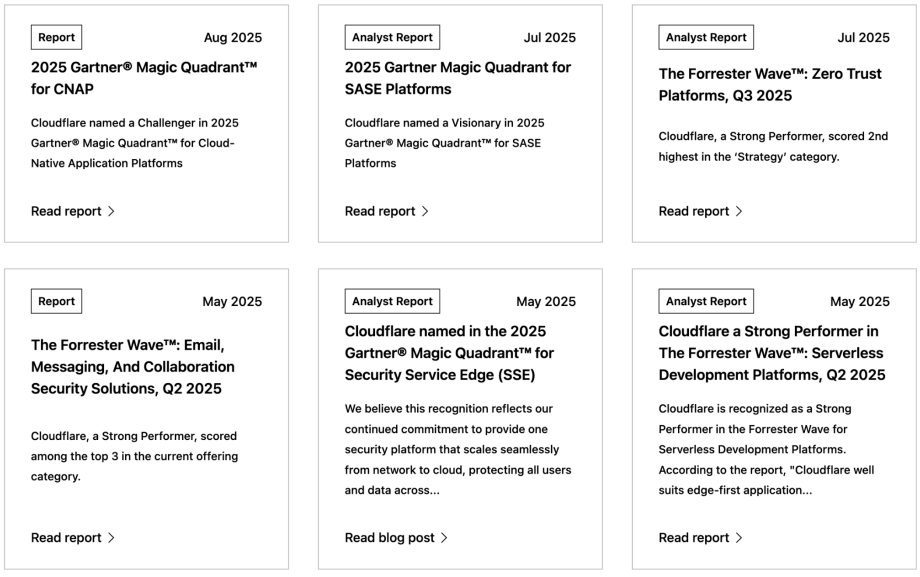
Cloudflare's path to dominance is built upon four key pillars. First, it is leveraging its pre-existing, mature, and inimitable global edge network as a foundational "unfair advantage," perfectly suited for the high-volume, low-latency demands of AI inference. Second, it has developed a deeply integrated and cost-disruptive developer platform—comprising Workers AI, R2 Storage, Vectorize, and AI Gateway—that systematically attacks the hyperscalers' primary profit centers, particularly data egress fees, while offering a superior developer experience. Third, Cloudflare has undertaken a bold strategic maneuver to become the indispensable arbiter of the internet's data economy by unilaterally blocking AI crawlers and proposing a "Pay Per Crawl" model, positioning itself as the gatekeeper for the data that fuels the entire AI industry. Fourth, its financial trajectory demonstrates disciplined execution, with strong revenue growth and improving profitability providing the capital to fund its ambitious roadmap from a position of strength.

Klover.ai Report on Cloudflare's AI Strategy

Additional Reports *Analyst Reports*

From Cloudflare's official **Analyst Reports** portal, several independent reports from Gartner, Forrester, and IDC. These specifically reference Cloudflare's technologies and product categories, including:

• **Gartner Magic Quadrant (2025) for Cloud-Native Application Platforms (CNAP) —** Cloudflare recognized as a Challenger, confirming its investment in cloud-native developer tools and scalable application platforms.

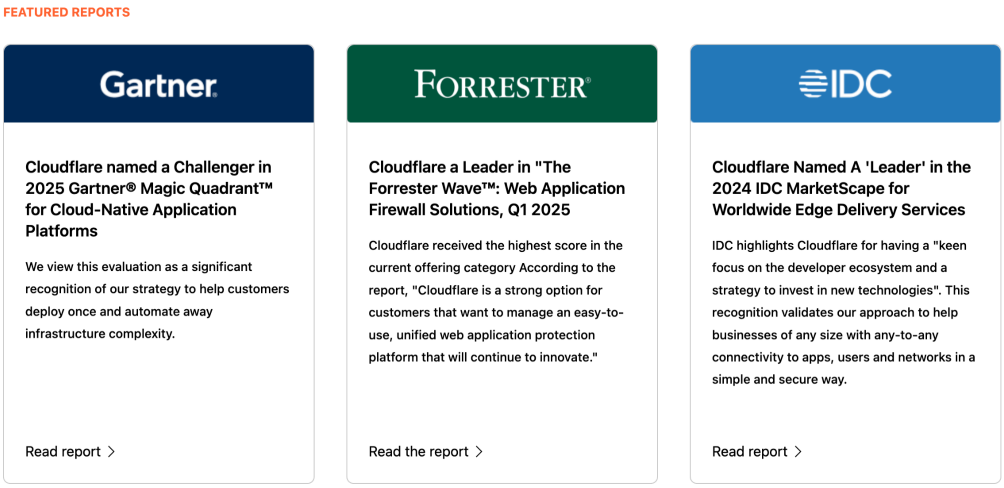


darivxe - Cloudflare footprint

• **Gartner Magic Quadrant (2025) for SASE Platforms —** Cloudflare named a Visionary, validating its use of Zero Trust, secure networking, and edge security technologies.

• **The Forrester Wave Q3 (2025): Zero Trust Platforms —** Cloudflare ranked as a Strong Performer, referencing its Zero Trust network architecture, threat intelligence layers, and secure access technologies.

• **IDC MarketScape (2024)**, naming Cloudflare a *Leader* in Worldwide Edge Delivery Services, citing its emphasis on developer-focused tools and continued investment in new technologies.

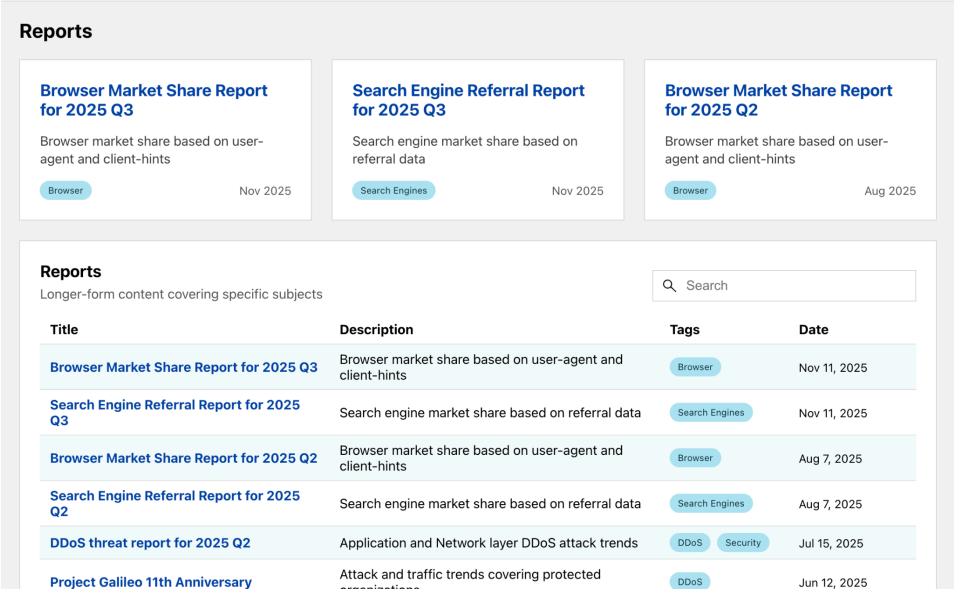


Featured Reports on Cloudflare

Collectively, these reports show how Cloudflare is consistently evaluated by established industry research firms for its performance in security, edge networking, serverless computing, and cloud-native technologies. They also illustrate the company's growing influence within the AI, CDN, and Zero Trust markets, supported by third-party assessments rather than internal marketing.

Annual Reports *Radar Reports*

Cloudflare publishes detailed annual-style reports on its website that provide insight into market trends, product adoption, and customer behavior. One example is the **Browser Market Share Report for 2025 Q3**, authored by the Cloudflare Data Insights Team. This report breaks down browser usage based on user-agent and client-hint data collected through HTTP/S requests. It includes global and country-level statistics, operating-system segmentation, and in-app browser breakdowns. The methodology section outlines how Cloudflare maps user agents to browser families and how operating systems are categorized.



Annual Reports

The dataset is presented through interactive tables such as “Market Share by Country and OS” which show granular percentages for each browser in each region. For instance, in the Australia/Android segment for September 2025, Chrome maintains a dominant share of over 77%, followed by Samsung Internet and Firefox, with smaller slices distributed across alternative browsers like Brave, DuckDuckGo, Opera, and others.

These types of reports appear to be released quarterly and consistently maintained across prior quarters as well (Q2, Q1, and 2024 Q4 are all listed as related reports). Collectively, they function as Cloudflare’s recurring analytical publications, offering visibility into global traffic trends and the broader technology ecosystem that Cloudflare’s network observes at scale.

Market Share by Country and OS

2025-09 | Australia | Android

Date	Country	Operating System	Browser	Market Share
2025-09	Australia	Android	Chrome	77.393%
2025-09	Australia	Android	Samsung Internet	17.590%
2025-09	Australia	Android	Firefox	1.654%
2025-09	Australia	Android	Brave	1.152%
2025-09	Australia	Android	Edge	0.895%
2025-09	Australia	Android	DuckDuckGo	0.617%
2025-09	Australia	Android	Opera	0.267%
2025-09	Australia	Android	Other	0.150%
2025-09	Australia	Android	Aloha Browser	0.115%
2025-09	Australia	Android	Ecosia	0.077%
2025-09	Australia	Android	Oculus Browser	0.049%
2025-09	Australia	Android	Huawei Browser	0.042%

Market Share of Australia and Android OS

2.6 *News*

Recent Security Breaches

2025 Third-Party Vendor Data Breach (Salesloft & Drift)

A recent breach disclosed by Huntress Labs revealed that third-party vendors Salesloft and Drift, both used extensively by Cloudflare for customer engagement operations, experienced security incidents that indirectly impacted Cloudflare. *Huntress article*

Cloudflare Data Breach Timeline

- **Early 2025:** Security incidents occur at third-party vendors Salesloft and Drift, used by Cloudflare.
- **March 21, 2025:** Cloudflare is notified of the breaches by the vendors and begins its investigation.
- **March 21, 2025 (Later that day):** Cloudflare publicly discloses the incident via a blog post, explaining the scope and what data was potentially exposed.
- **Post-Disclosure:** Cloudflare suspends the use of the affected vendor platforms, initiates a password rotation for impacted employees, and works to notify affected customers.

This incident demonstrates Cloudflare's operational dependence on third-party SaaS platforms for customer relationship management and communications. It highlights an important component of the organization's technology footprint: **Salesloft and Drift are**

integrated into Cloudflare's external communication and support ecosystem, and compromise of these systems can propagate security risk to Cloudflare's infrastructure.

2023–2024 Unauthorized Access via Stolen Authentication Tokens (Atlassian Environment Compromise)

A more severe compromise was documented by GitGuardian, involving unauthorized access to Cloudflare's internal **Atlassian server**, which hosts critical infrastructure such as:

- **Confluence** (internal wiki)
- **Jira** (issue tracking)
- **Bitbucket** (source code repositories) *gitguardian blog*

Attack Details:

- On November 14, attackers—suspected to be state-sponsored—gained access to Cloudflare's Atlassian environment.
- Access was achieved using **one authentication token and three service account credentials** that had been stolen during the **Okta breach in October 2023**.
- The attackers leveraged **ScriptRunner**, a Jira automation and scripting tool, to maintain persistent access.
- Despite Okta revoking many stolen session tokens, several Cloudflare-related tokens had not been rotated, which enabled prolonged unauthorized access to internal systems.

This breach reveals critical information about Cloudflare's internal tooling and development workflow, including:

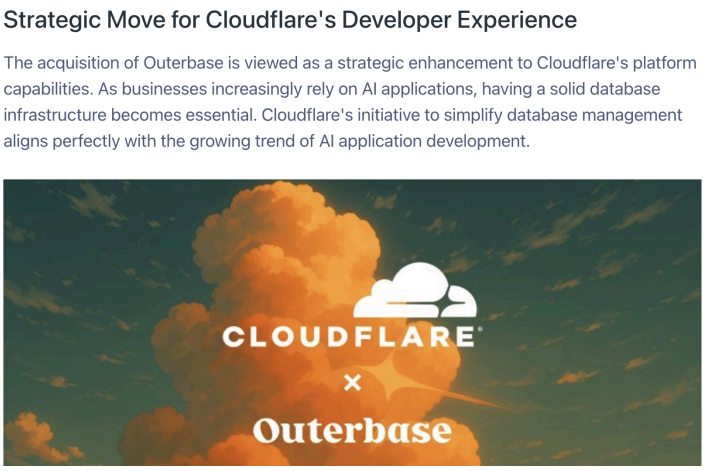
- Heavy reliance on the **Atlassian suite** (Confluence, Jira, Bitbucket) for documentation, operational planning, and source code management
- Use of **ScriptRunner** for administrative automation within Jira
- Integration with **Okta** for identity and access management
- Existence of service accounts tied to internal software pipelines

These insights collectively map out significant components of Cloudflare's backend infrastructure, identity management approach, and operational security posture.

Mergers and Acquisitions

Acquisition of Outerbase (2025)

Cloudflare recently acquired **Outerbase**, a company focused on simplifying database management and improving developer workflow efficiency. The acquisition is positioned as a strategic enhancement to Cloudflare's platform, particularly as the industry increasingly shifts toward AI-driven application development. *ssojet blog*



According to the report, Cloudflare views this acquisition as a way to:

- Strengthen its backend infrastructure for developers
- Streamline database interactions within Cloudflare's platform

- Support the growing demand for scalable AI applications
- Expand its developer experience offerings

The available technical analysis suggests that Cloudflare aims to integrate Outerbase to create a more unified and frictionless development ecosystem, potentially reinforcing its vision of becoming a comprehensive serverless and application-delivery platform.

Cloudflare's 2025 Expansion into Clientless Remote Access (RDP) Technology

In 2025, Cloudflare unveiled a significant enhancement to its Zero Trust access ecosystem: a **fully clientless, browser-based Remote Desktop Protocol (RDP) solution**. While not explicitly framed as a traditional acquisition, OSINT analysis strongly suggests that this launch resulted from Cloudflare's continued investment in — and possible integration of — acquired technologies, as well as internal development following its earlier security-focused acquisitions.

The new offering fundamentally changes how organizations provide remote Windows Server access. By eliminating the need for traditional VPNs, RDP clients, or exposed public endpoints, Cloudflare introduces a security-forward access model designed for both internal teams and third-party vendors. *Acquisitions*

- **Browser-Native RDP Access:** Users can connect to Windows servers directly through the browser, removing dependency on thick clients or corporate VPNs.

- **Zero Trust Enforcement:** Authentication and authorization controls are applied before any connection attempt, minimizing exposure to brute-force attacks and credential-based compromises.
- **Granular Access Controls:** Administrators can define fine-grained policies for contractors, employees, and external partners without modifying network topology.

Additional Partnerships

Cloudflare–Oracle Cloud Infrastructure (OCI) Integration

Cloudflare announced a significant collaboration with **Oracle Cloud Infrastructure (OCI)** in late 2025. As part of this partnership, Cloudflare's connectivity cloud platform will be offered **natively within OCI**, providing joint customers with enhanced security, resiliency, and performance across hybrid and multicloud environments. *cloudflare x oci*

Cloudflare Integrates Services with Oracle Cloud Infrastructure to Help Customers Supercharge Applications and AI Workloads

Integration enables businesses to run faster and more securely across cloud environments

This Press Release is also available in 日本語, 한국어, Deutsch, Français, Español (Latinoamérica), Nederlands, Bahasa Indonesia, Tiếng Việt, แบบไทย.

San Francisco, California —October 13, 2025 — Cloudflare, Inc. (NYSE: NET), the leading connectivity cloud company, today announced that its connectivity cloud platform will be available natively on Oracle Cloud Infrastructure (OCI) for customers worldwide. This will enable joint customers to leverage Cloudflare's security, performance, and resiliency directly from OCI across hybrid, multicloud, and OCI hosted applications.

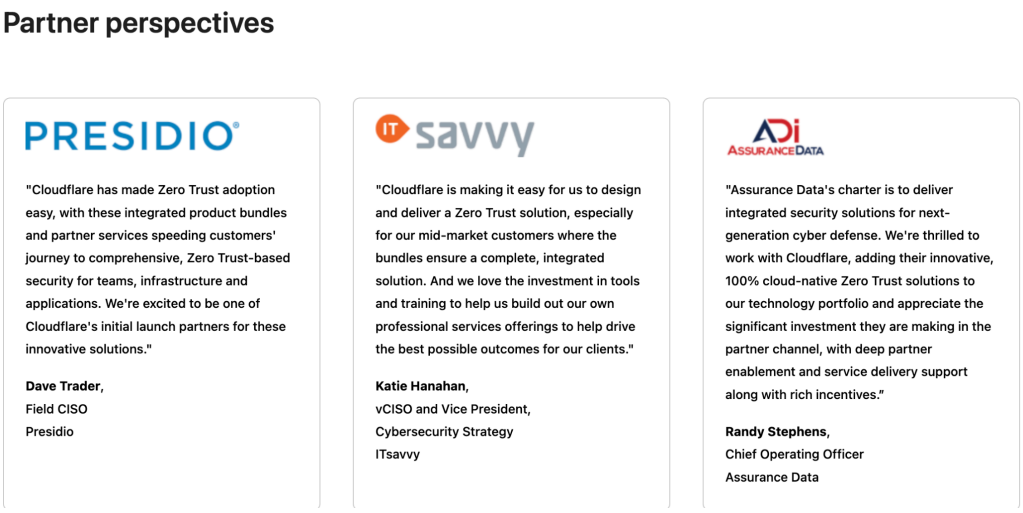
According to the official release, the integration enables customers to:

- Run Cloudflare's security and performance services directly from OCI
- Improve cross-cloud application delivery and AI workload performance
- Strengthen resiliency by leveraging Cloudflare's global network from within Oracle's cloud ecosystem

This collaboration reflects Cloudflare's strategic push into **multicloud interoperability**, positioning its connectivity capabilities as a universal control layer across diverse cloud infrastructures.

Zero Trust Partner Ecosystem Expansion

Cloudflare's strategic collaborations with several cybersecurity and IT service providers, including Presidio, ITsavvy, and Assurance Data. These partnerships focus on accelerating enterprise adoption of Cloudflare's Zero Trust platform through combined service offerings, training, and joint solution delivery. *partners*



1. Presidio

Presidio emphasizes that Cloudflare's integrated Zero Trust bundles significantly simplify customer onboarding and security transformation journeys. As a launch partner, Presidio supports the deployment of Cloudflare's Zero Trust capabilities across enterprise teams and infrastructure.

2. ITsavvy

ITsavvy notes that Cloudflare's investments in tools, training, and professional services support enable them to design and deliver fully integrated Zero Trust solutions for

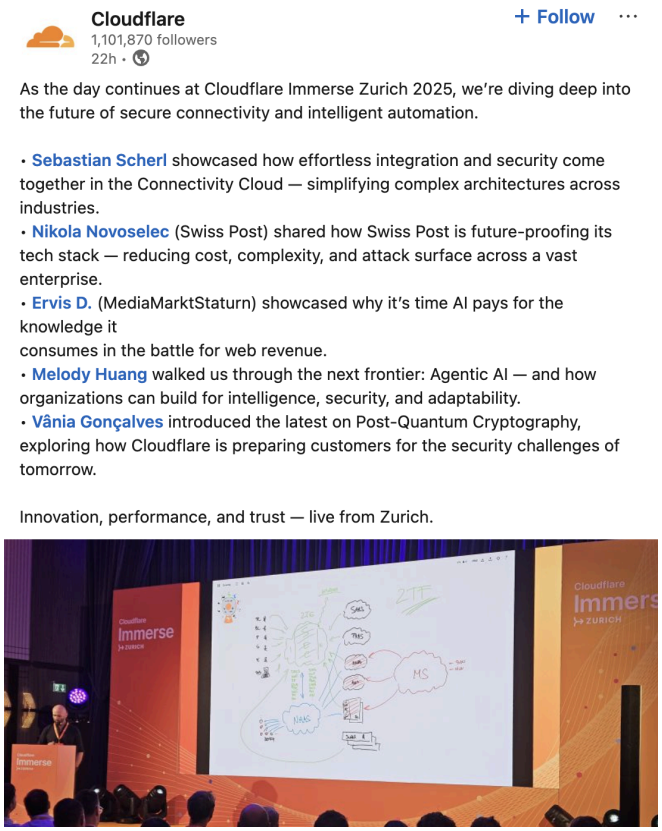
mid-market customers. Their collaboration ensures customers can adopt secure, unified access models aligned with modern cybersecurity demands.

3. Assurance Data

Assurance Data highlights Cloudflare's cloud-native Zero Trust technology as a core enhancement to their security portfolio. The partnership enables delivery of advanced, integrated cyber-defense solutions, with Cloudflare providing substantial support in partner enablement and service delivery.

2.7 *Social Media*

The organization maintains an active and diverse presence across multiple social media platforms, including LinkedIn, Facebook, Instagram, YouTube, and X. These platforms provide valuable insights into Cloudflare's ongoing initiatives, technology priorities, community engagement, and industry-facing activities.



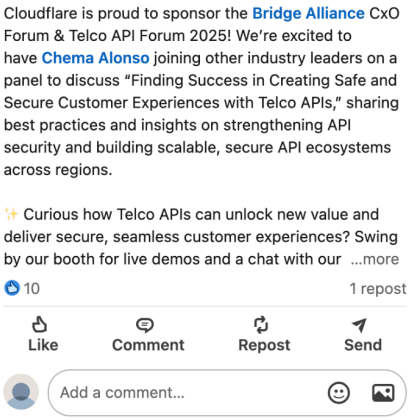
darivxe - Cloudflare footprint

- **Cloudflare Immerse Zurich 2025 (LinkedIn):**

Posts from this event showcase Cloudflare's discussions on future-proofing enterprise tech stacks, intelligent automation, post-quantum cryptography, and security architecture improvements. *evidence*

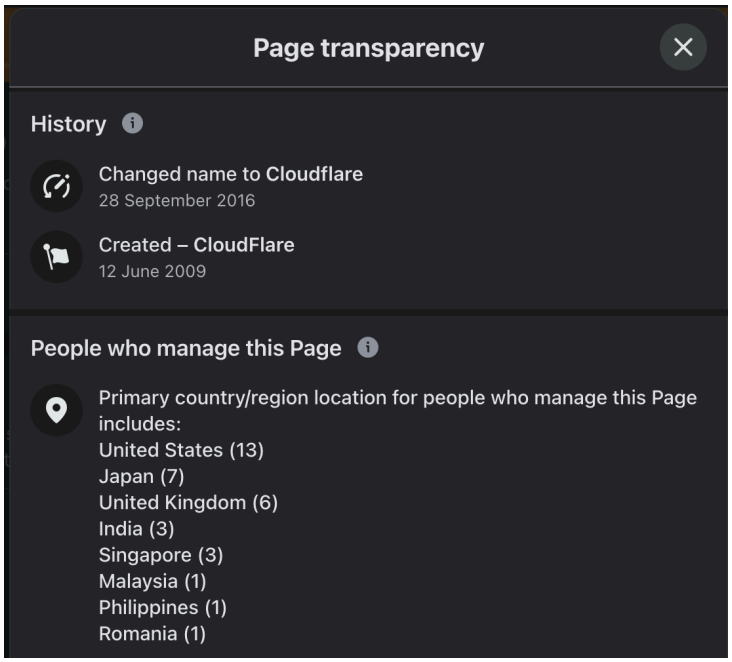
- **Industry Event Participation:**

Posts regarding **Telco API Forum 2025** demonstrate Cloudflare's involvement in strengthening API security and building scalable customer-facing API ecosystems across regions. *evidence*



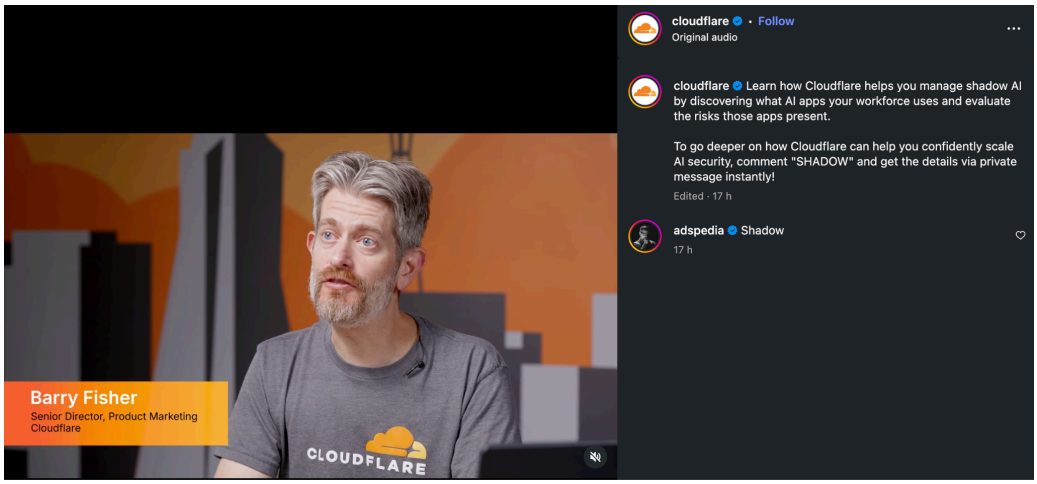
- **Facebook Page Transparency:**

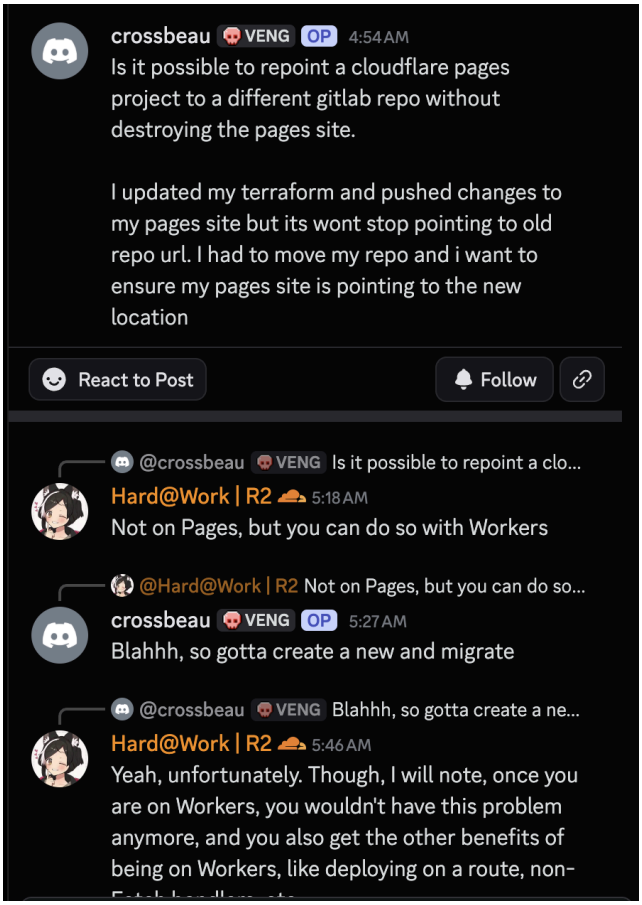
Page transparency data reveals Cloudflare's global social media management footprint, with teams handling the page from various countries. This geographic spread reflects Cloudflare's distributed operations and international communication strategy.



- **Internal Advocacy for AI Security:**

Instagram promotional material includes Cloudflare personnel explaining technologies related to shadow *AI detection and AI security* posture management, suggesting active internal development in these areas.





- **Discord Server - Cloudflare Developers**

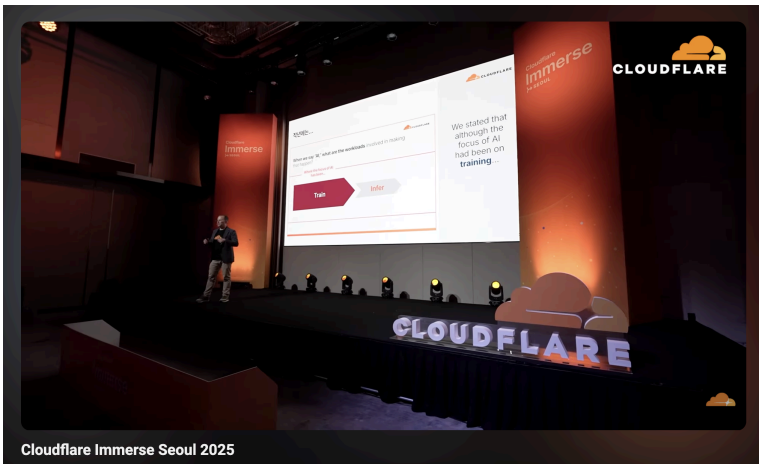
On Cloudflare's developer Discord, employees actively assist users. In one thread, a developer asked about repointing a Pages project to a new GitLab repo, and a Cloudflare staff member clarified the limitation and recommended using **Cloudflare Workers** as the more flexible solution.

- **Cloudflare on X (Twitter)**

Developer engagement, shown through interactive posts like asking users to share early-career tech advice (#CloudflareChat).

Promotion of its Connectivity Cloud, emphasizing simplified infrastructure and unified cloud/SaaS/on-prem workflows. *X profile*

- **Cloudflare Immerse Seoul 2025 – Event Presentation (YouTube)**



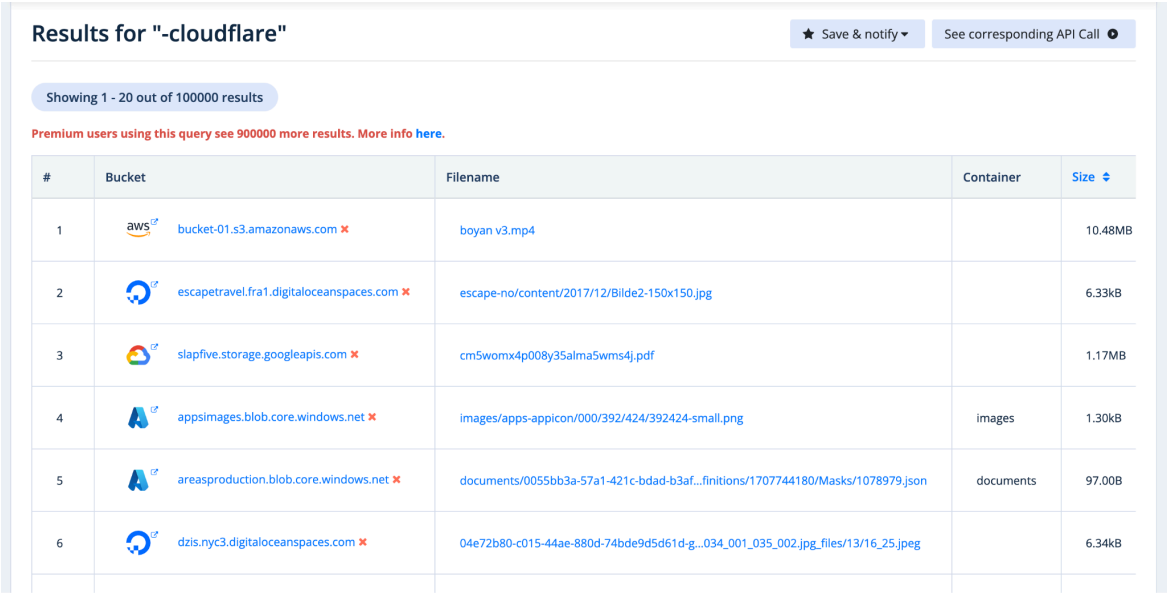
Cloudflare Immerse Seoul 2025

A recorded session from *Cloudflare Immerse Seoul 2025* shows Cloudflare leadership presenting on AI workloads, with slides referencing training vs. inference workflows. This highlights Cloudflare's focus on AI deployment and edge computing. The event also reflects the company's global technical outreach and consistent AI-driven messaging.

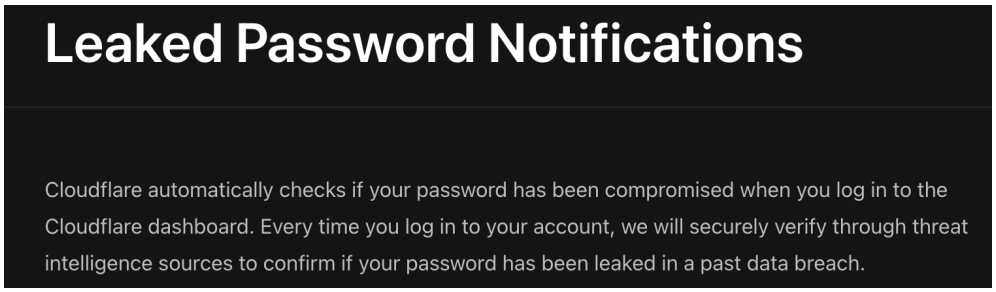
2.8 *Leaked Data*

A search on **GrayHatWarfare**, a public index of exposed cloud storage buckets, returned numerous results containing the keyword *"cloudflare."* While none of the files originated from Cloudflare-owned buckets, the presence of Cloudflare references in filenames and bucket metadata indicates that third-party systems frequently store Cloudflare-related content (such as configuration files, screenshots, logs, and API-related material).

The exposed buckets belonged to platforms such as AWS S3, DigitalOcean Spaces, Google Cloud Storage, and Azure Blob Storage. These findings demonstrate that Cloudflare-related data can surface indirectly through third-party environments, even though no internal Cloudflare assets were found exposed.

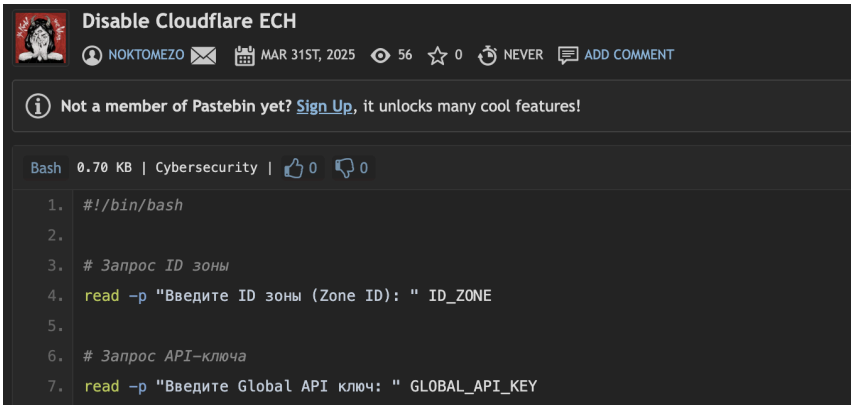


Cloudflare publishes a public page explaining its policy for detecting when **customer passwords appear in external data breaches.** *cloudflare docs*



A Pastebin entry titled **"Disable Cloudflare ECH"** was discovered, containing a bash script that interacts with the Cloudflare API. *pastebin link*
While the script itself is not a Cloudflare leak, it demonstrates:

- Users publicly sharing Cloudflare-related automation scripts
- Potential exposure risks when individuals paste API usage examples online
  No Cloudflare internal credentials were present.



2.9 *Source Code Repositories*

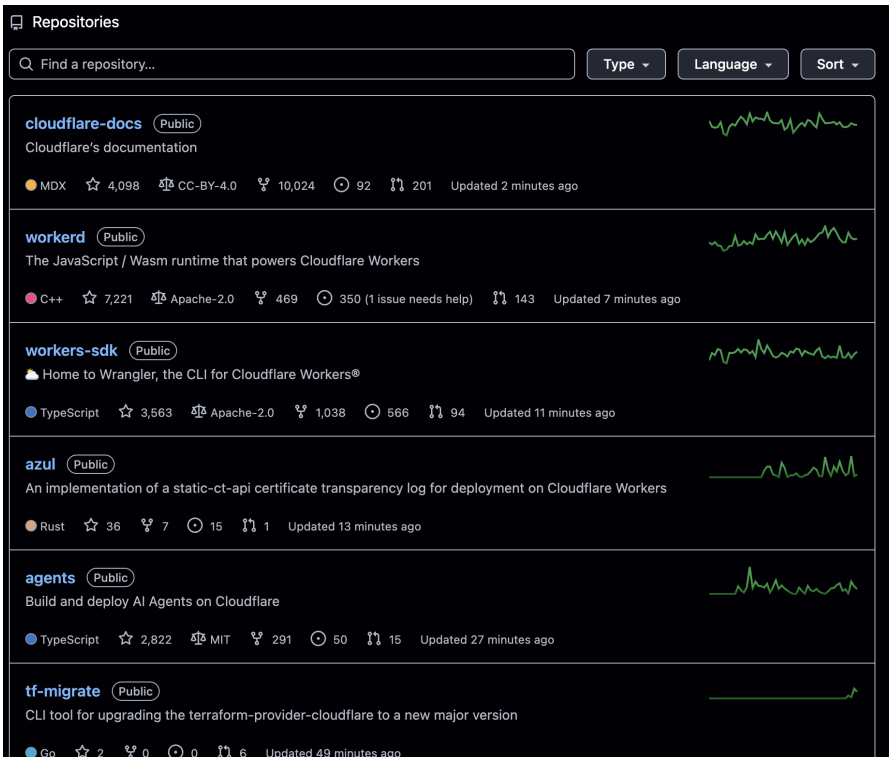
Public Repositories belonging to Cloudflare

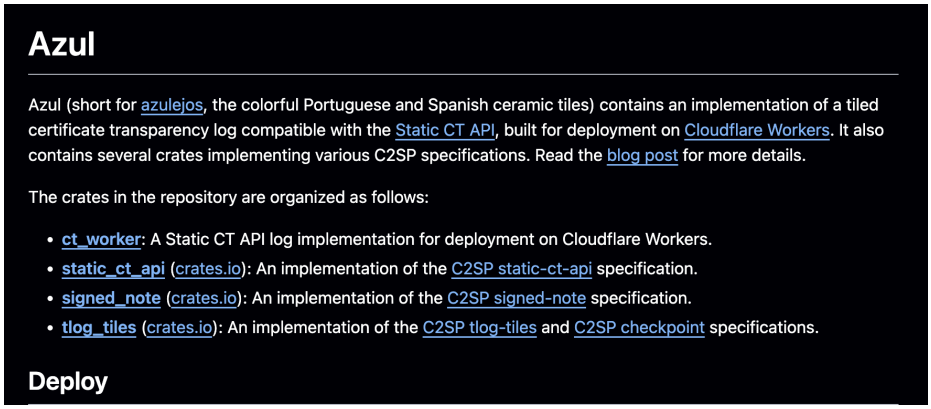
A review of Cloudflare's official *GitHub* organization revealed extensive open-source activity. Cloudflare maintains a large number of public repositories covering documentation, infrastructure tooling, AI deployment, certificate transparency, and Cloudflare Workers development.

Examples include:

- **workerd** – the JavaScript/Wasm runtime behind Cloudflare Workers
- **workers-sdk** – tooling for building and deploying Workers
- **agents** – tools for deploying AI agents on Cloudflare
- **azul** – a certificate transparency log implementation built for Cloudflare Workers

These repositories demonstrate Cloudflare's strong commitment to open-source development and provide insight into the technologies supporting its platform.



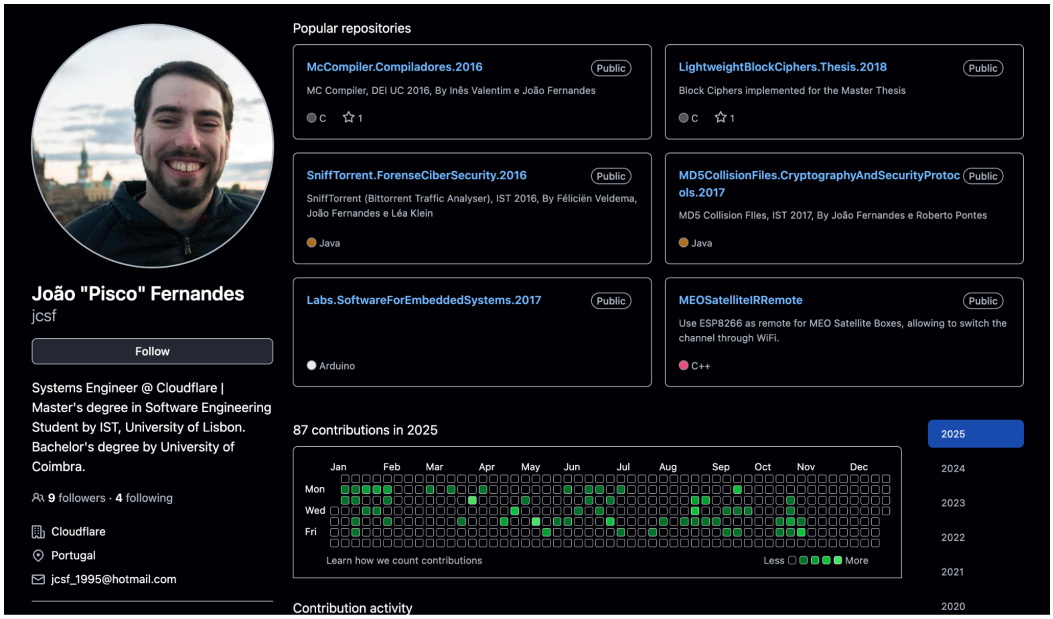


Repositories belonging to Cloudflare's Employees

Several Cloudflare engineers maintain personal GitHub profiles where they publish open-source projects, templates, and experimental tools. These accounts publicly list Cloudflare as their employer and include repositories unrelated to Cloudflare products but demonstrating their technical work.

- ***Edmund Hung*** (System Engineer @ Cloudflare) – publishes tools such as *remix-cloudflare-template* and contributes to frameworks commonly used with Workers.

- ***João "Pisco" Fernandes*** (Systems Engineer @ Cloudflare) – maintains repositories related to cryptography, compilers, and embedded systems.



3. *Conclusion*

The OSINT investigation into Cloudflare reveals a sophisticated, mature, and highly transparent technology ecosystem. Cloudflare's infrastructure is built on a resilient global Anycast network, supported by strong Zero Trust principles, multilayered partnerships, and extensive automation. The company publicly discloses much of its technology stack through documentation, open-source repositories, and technical events, which contributes significantly to its discoverability.

The investigation also highlights Cloudflare's deep involvement in open-source development, with employees contributing to major JavaScript, WebAssembly, and cloud-native projects. Public job listings confirm Cloudflare's preference for modern development stacks, distributed systems expertise, and automation-heavy workflows.

Security incidents involving third-party vendors (Drift, Salesloft, Okta) exposed additional internal details about Cloudflare's Atlassian environment, identity provider usage, and reliance on service accounts. Importantly, no direct Cloudflare database or code repository leaks were identified during the investigation.

Overall, Cloudflare maintains a robust security posture while exposing a significant amount of architectural insight through public sources.

3.1. *References*

2.1

https://blog.cloudflare.com/cloudflare-investigation-of-the-january-2022-okta-compromise/#how-cloudflare-uses-okta
https://www.pagerduty.com/customer/cloudflare/
https://crt.sh/?q=www.cloudflare.com
Shodan.io

2.2

https://blog.cloudflare.com/cloudflare-investigation-of-the-january-2022-okta-compromise/#how-cloudflare-uses-okta
https://www.pagerduty.com/customer/cloudflare/
https://www.cloudflare.com/en-in/partners/technology-partners/
https://www.cloudflare.com/en-in/careers/jobs/
https://job-boards.greenhouse.io/cloudflare/jobs/7312774?gh_jid=7312774
https://job-boards.greenhouse.io/cloudflare/jobs/7365381?gh_jid=7365381

2.3

https://events.cloudflare.com/connect/2025/
https://www.cloudflare.com/en-gb/lp/cloudflare-connect-2026/
https://community.cloudflare.com/

2.4

https://www.cloudflare.com/en-in/people/
https://contactout.com/Daniella-Vallurupalli-1510861
https://www.linkedin.com/in/daniellavallurupalli/
https://www.linkedin.com/in/prudhvibadri/
https://github.com/BadriPrudhvi?tab=overview&from=2023-12-01&to=2023-12-31
https://sauleau.com/
https://x.com/svensauleau
https://github.com/xtuc?tab=overview&from=2025-11-01&to=2025-11-13

2.5

https://www.slideshare.net/cloudflare
https://sam.gov/opp/9195dbf0178642d087e3ec0b0802a570/view#general

https://www.usaspending.gov/recipient/7d1eac33-f87a-7f1c-3029-054d8e5684b5-P/latest
patents.google.com
https://www.klover.ai/cloudflare-ai-strategy-analysis-of-dominance-in-cloud-cybersecurity-ai/
https://www.cloudflare.com/en-gb/analysts/
https://radar.cloudflare.com/reports

2.6

https://www.huntress.com/threat-library/data-breach/cloudflare-data-breach
https://blog.gitguardian.com/the-secrets-out-how-stolen-auth-tokens-led-to-cloudflare-breach/
https://blog.cloudflare.com/tag/acquisitions/
https://ssojet.com/blog/cloudflare-acquires-outerbase-to-enhance-ai-development-efforts#strategic-move-for-cloudflares-developer-experience
https://www.cloudflare.com/en-in/press/press-releases/2025/cloudflare-integrates-services-with-oracle-cloud-infrastructure-to-help/
https://www.cloudflare.com/en-gb/partners/

2.7

https://www.linkedin.com/posts/cloudflare_as-the-day-continues-at-cloudflare-immerse-activity-7394776011562881024-iit3?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEMHdXUB34fPrSWumJo_WrQIUoMN3yHUqMU
https://www.linkedin.com/posts/cloudflare_everywheresecurity-telcoapi-apimanagement-activity-7395086138161528832-nqKP?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEMHdXUB34fPrSWumJo_WrQIUoMN3yHUqMU
https://www.instagram.com/reel/DRAyCkfiPr4/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==
https://x.com/Cloudflare
https://youtu.be/OZMBEyi69rc?si=c7o1-2gOO9vU0wtN

2.8

https://developers.cloudflare.com/fundamentals/account/account-security/leaked-password-notifications/
https://pastebin.com/pXXAgpSx

2.9

https://github.com/cloudflare
https://github.com/edmundhung
https://github.com/jcsf