Harnessing Global Threat Intelligence to Stay Ahead of the Game

Steve Molloy
Principal Solution Engineer
Cloudflare

For threat intelligence to be useful, it must be...

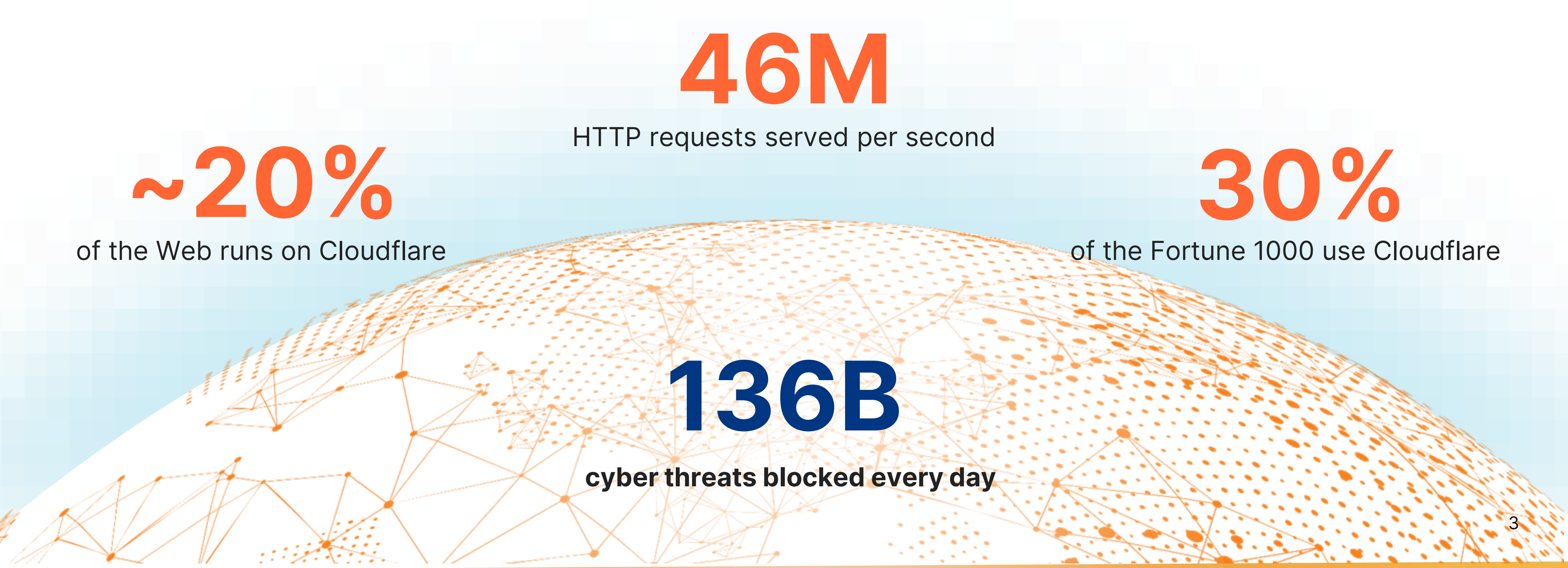
Accurate

Actionable

Automated

CLOUDFLARE

Our global network provides the broadest real-time threat intelligence



46M

HTTP requests served per second

~20%

of the Web runs on Cloudflare

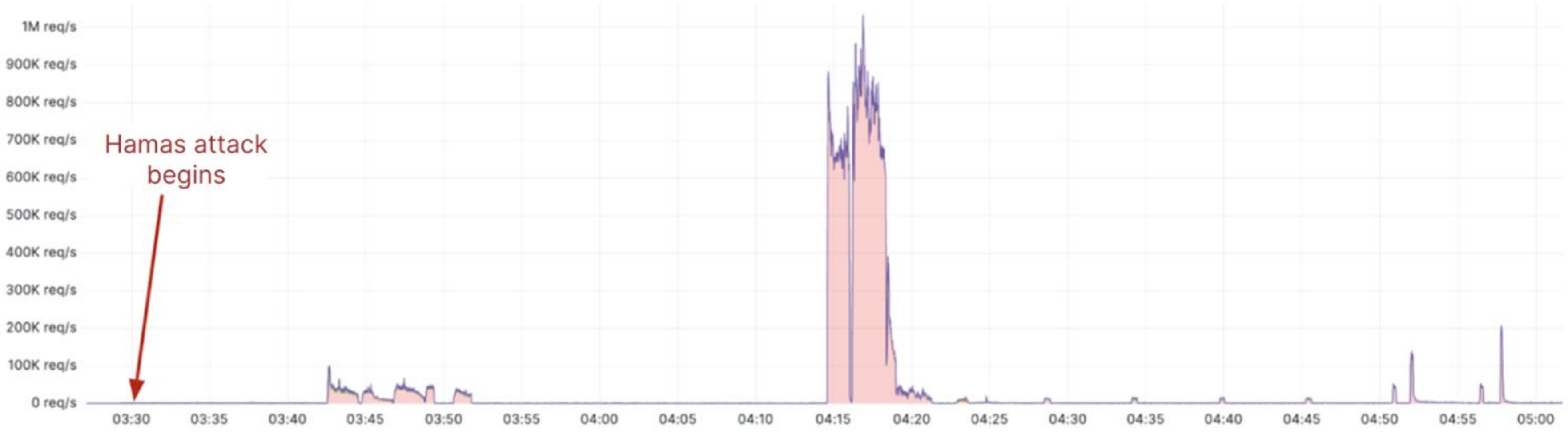
30%

of the Fortune 1000 use Cloudflare

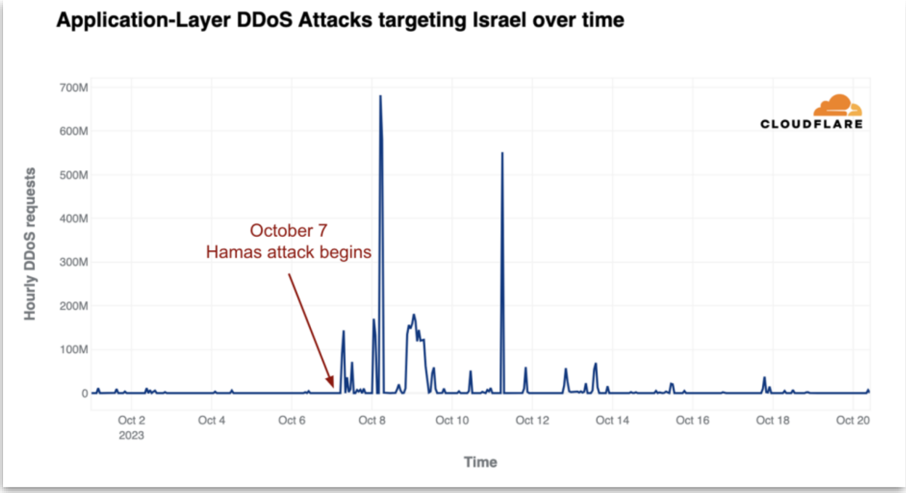
136B

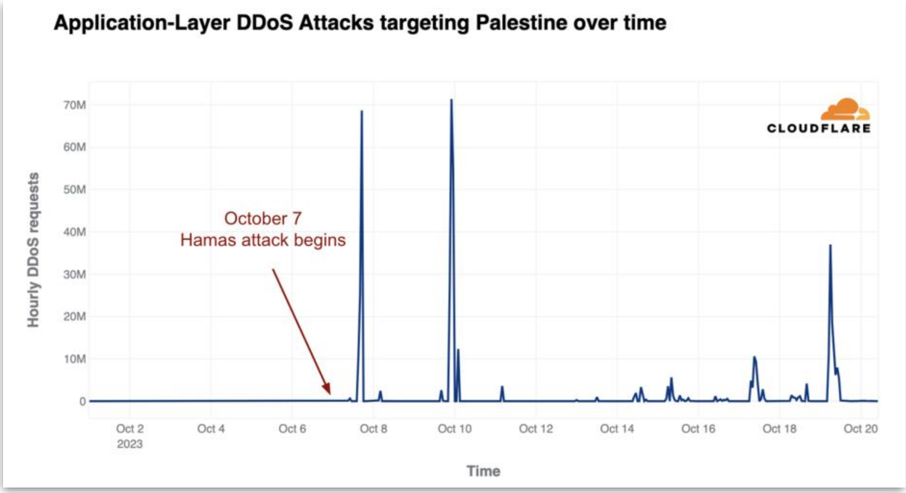
cyber threats blocked every day

DDoS attacks against Israeli assets

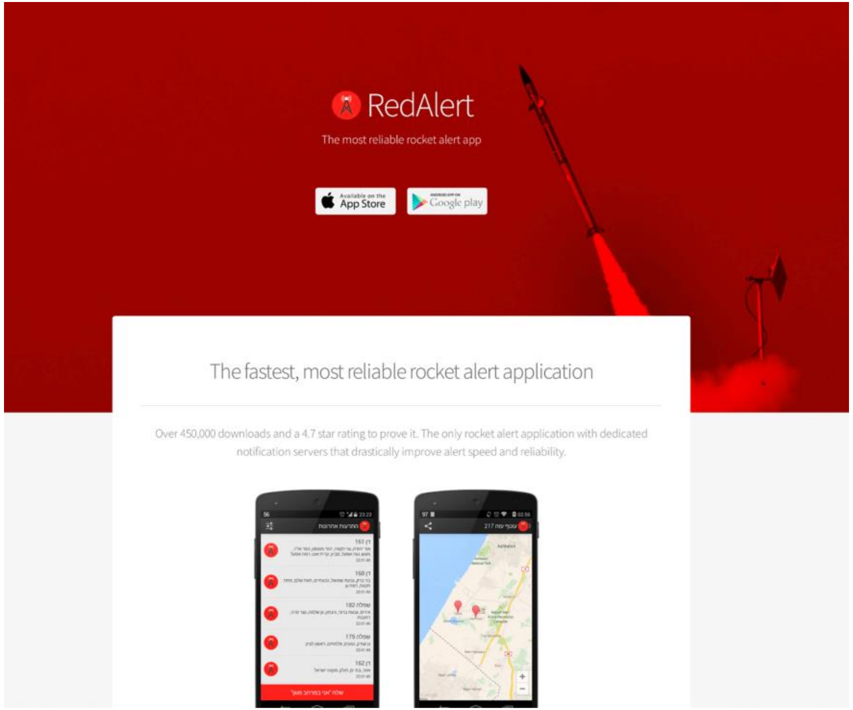


Cyber attacks in the Israel-Hamas war





“RedAlert - Rocket Alerts” Malware



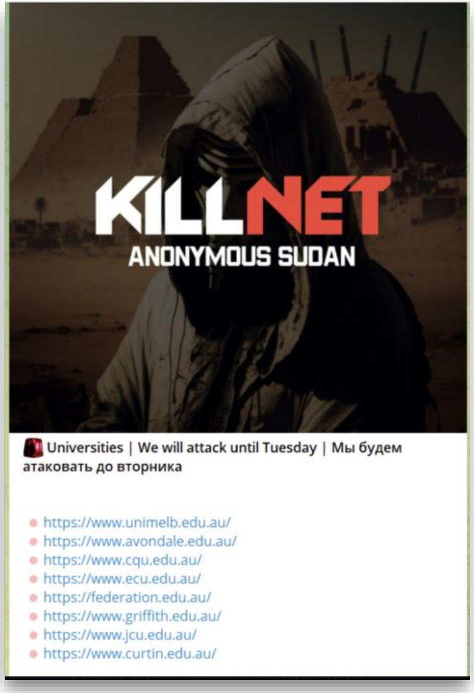
RedAlert

The most reliable rocket alert app

The fastest, most reliable rocket alert application

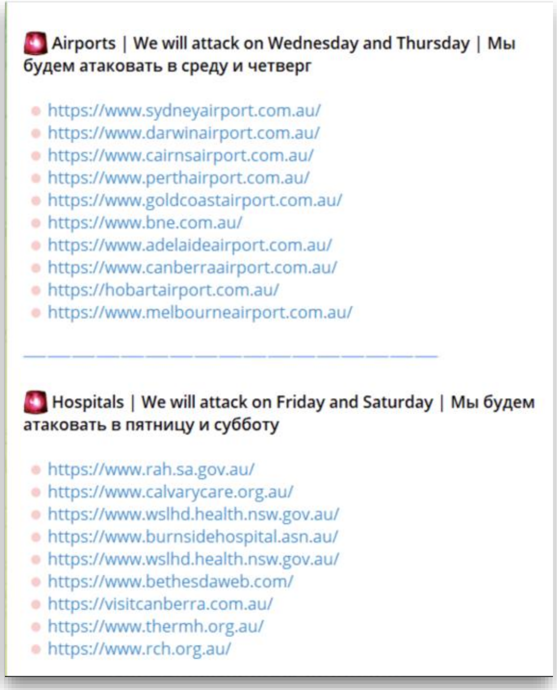
Over 450,000 downloads and a 4.7 star rating to prove it. The only rocket alert application with dedicated notification servers that drastically improve alert speed and reliability.

Australian universities, hospitals and airports are targeted



🚨 Universities | We will attack until Tuesday | Мы будем атаковать до вторника

- https://www.unimelb.edu.au/
- https://www.avondale.edu.au/
- https://www.cqu.edu.au/
- https://www.ecu.edu.au/
- https://federation.edu.au/
- https://www.griffith.edu.au/
- https://www.jcu.edu.au/
- https://www.curtin.edu.au/



🚨 Airports | We will attack on Wednesday and Thursday | Мы будем атаковать в среду и четверг

- https://www.sydneyairport.com.au/
- https://www.darwinairport.com.au/
- https://www.cairnsairport.com.au/
- https://www.perthairport.com.au/
- https://www.goldcoastairport.com.au/
- https://www.bne.com.au/
- https://www.adelaideairport.com.au/
- https://www.canberraairport.com.au/
- https://hobartairport.com.au/
- https://www.melbourneairport.com.au/

———————————————————————

🚨 Hospitals | We will attack on Friday and Saturday | Мы будем атаковать в пятницу и субботу

- https://www.rah.sa.gov.au/
- https://www.calvarycare.org.au/
- https://www.wslhd.health.nsw.gov.au/
- https://www.burnsidehospital.asn.au/
- https://www.wslhd.health.nsw.gov.au/
- https://www.bethesdaweb.com/
- https://visitcanberra.com.au/
- https://www.thermh.org.au/
- https://www.rch.org.au/

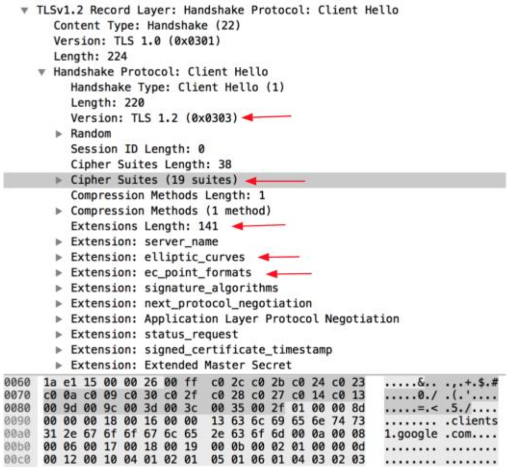
Bot Detections

What’s in a fingerprint?

```
    "type": "clientHelloFingerprint",
    "value":
"03030058130213031301c02cc030c02bc02fcca9cca800a3009f00a2009ec
caac0afc0adc024c028c0a3c09f006b006a00390038c0aec0acc023c027c0a
2c09e0067004000330032009d009cc0a1c09dc0a0c09c003d003c003500ff
01000000000b000403000102000a000c000a001d0017001e0019001800230
0160017000d0030002e0403050306030807080808090080a080b08040805
0806040105010601030302030301020103020202040205020602002b002d
00330015",

“https://github.com/Anorov/cloudflare-scrape/releases/tag/2.0.4",
```

The field order is as follows:
TLSVersion,Ciphers,Extensions,EllipticCurves,EllipticCurvePointFormats
Example:
769,47–53–5–10–49161–49162–49171–49172–50–56–19–4,0–10–11,23–24–25,0

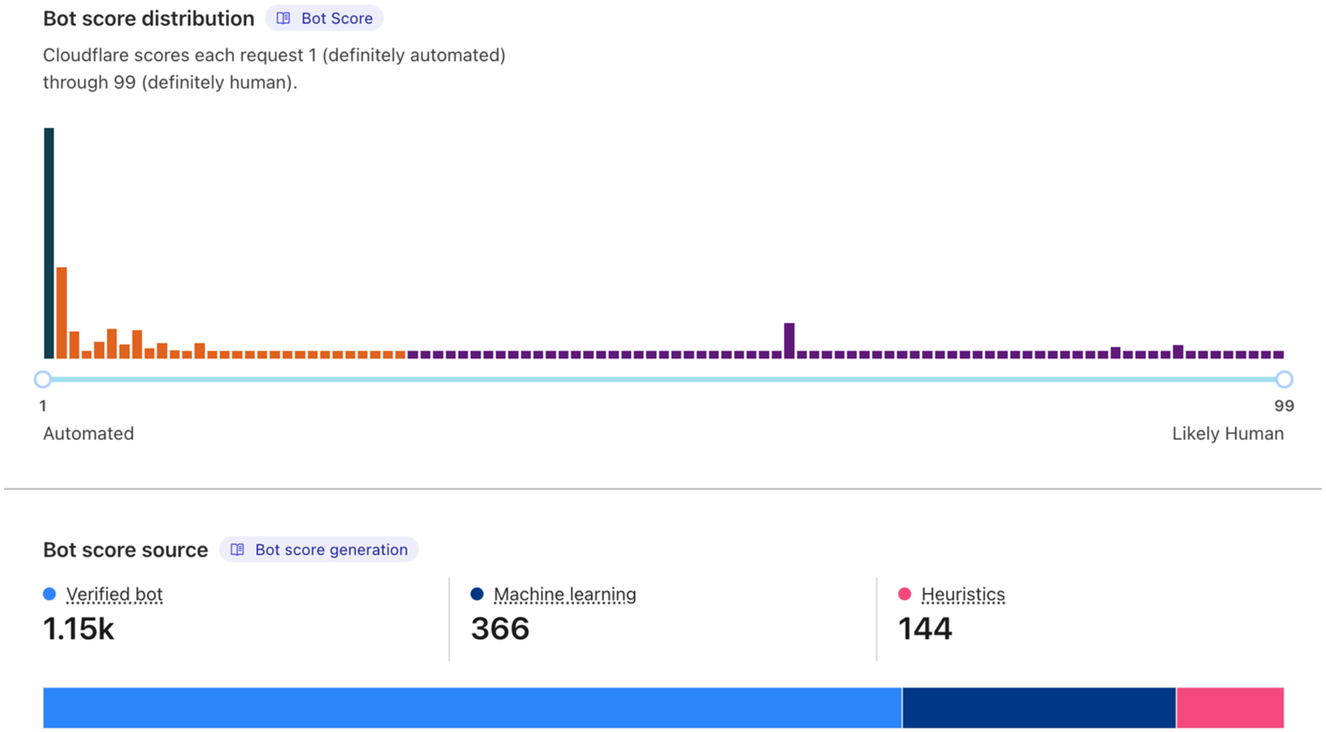


```
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 224
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 220
      Version: TLS 1.2 (0x0303)
    ▶ Random
      Session ID Length: 0
      Cipher Suites Length: 38
    ▶ Cipher Suites (19 suites)
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)
      Extensions Length: 141
    ▶ Extension: server_name
    ▶ Extension: elliptic_curves
    ▶ Extension: ec_point_formats
    ▶ Extension: signature_algorithms
    ▶ Extension: next_protocol_negotiation
    ▶ Extension: Application Layer Protocol Negotiation
    ▶ Extension: status_request
    ▶ Extension: signed_certificate_timestamp
    ▶ Extension: Extended Master Secret
0060  1a e1 15 00 00 26 00 ff  c0 2c c0 2b c0 24 c0 23   .....&.. .,.+.$.#
0070  c0 0a c0 09 c0 30 c0 2f  c0 28 c0 27 c0 14 c0 13   .....0./ .(.'....
0080  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 01 00 00 8d   .....=.< .5./....
0090  00 00 00 18 00 16 00 00  13 63 6c 69 65 6e 74 73   ........ .clients
00a0  31 2e 67 6f 6f 67 6c 65  2e 63 6f 6d 00 0a 00 08   1.google .com....
00b0  00 06 00 17 00 18 00 19  00 0b 00 02 01 00 00 0d   ........ ........
00c0  00 12 00 10 04 01 02 01  05 01 06 01 04 03 02 03   ........ ........
```

de350869b8c85de67a350c8d186f11e6 ✓

Bot Detections

Making intel actionable…



Bot score distribution

Bot Score

Cloudflare scores each request 1 (definitely automated) through 99 (definitely human).

Bot score source

Bot score generation

● Verified bot	● Machine learning	● Heuristics
1.15k	366	144

Phishing is alive and well

91%

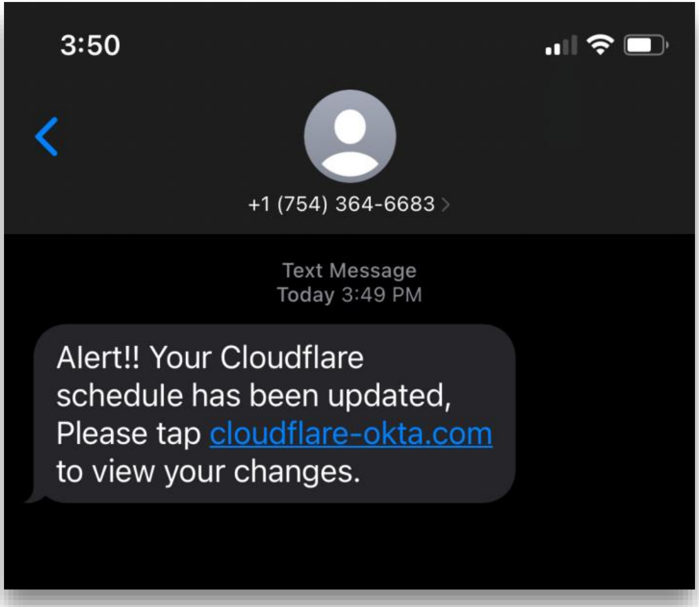
Of cyberattacks start with a phish

32%

Of all successful breaches involve the use of phishing

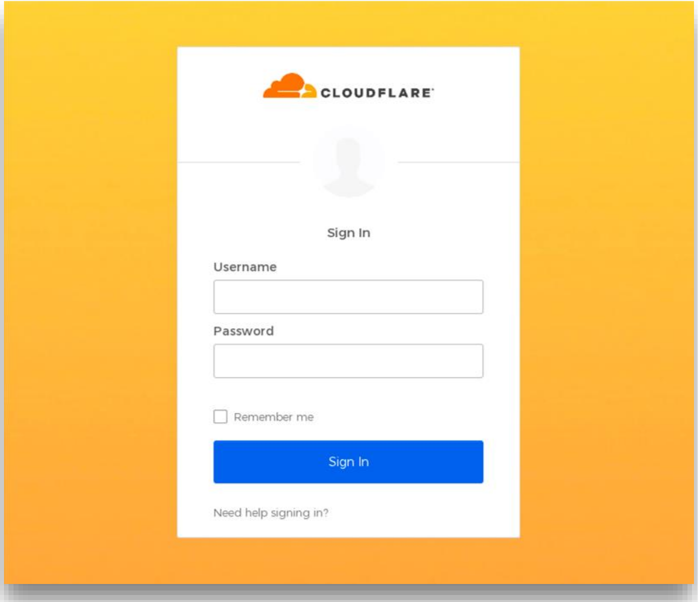
(Source: Deloitte)

It happens to us too...



Text Message
Today 3:49 PM

Alert!! Your Cloudflare schedule has been updated, Please tap cloudflare-okta.com to view your changes.



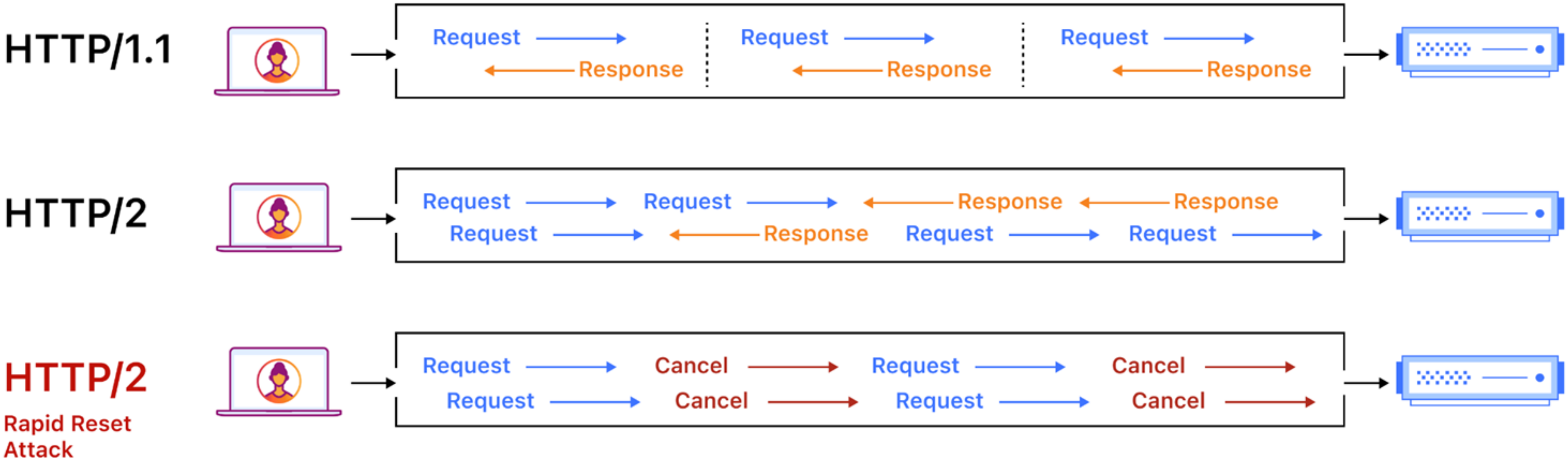
Sign In

Username

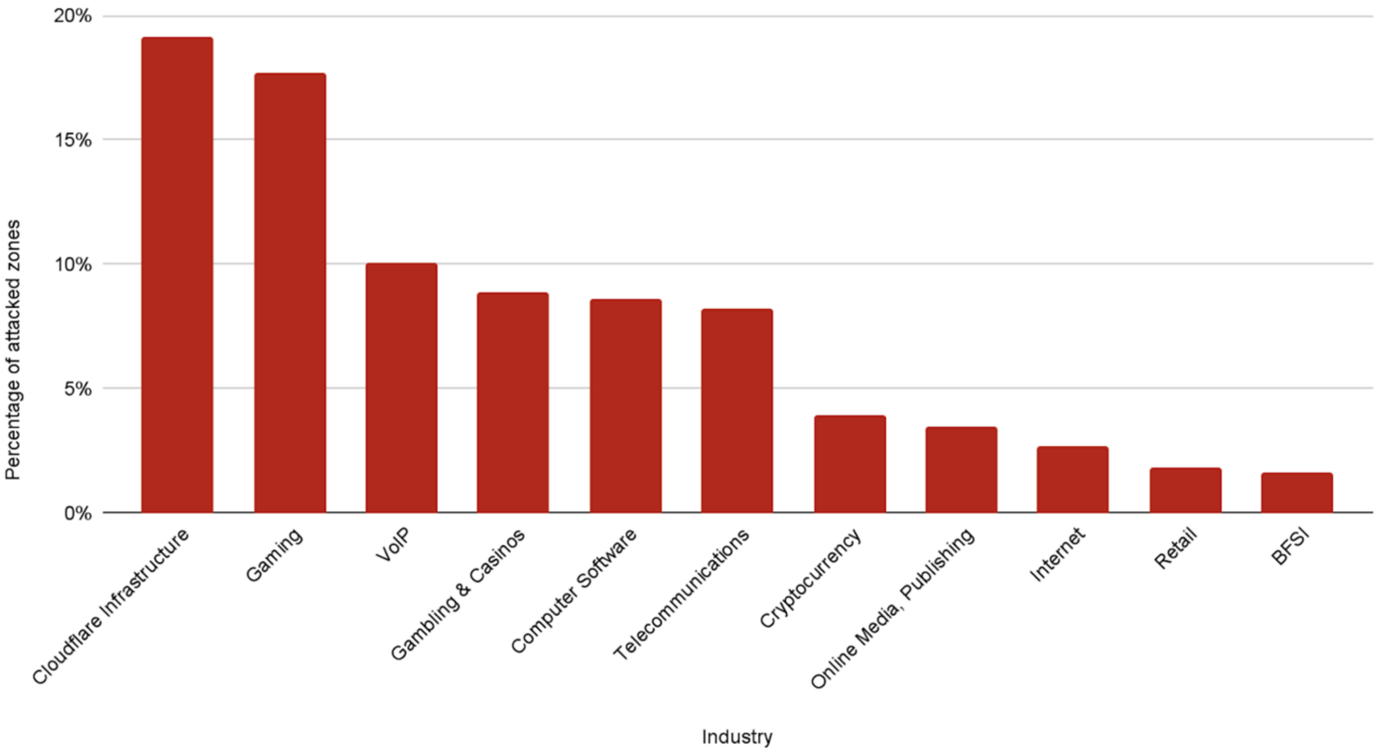
Password

□ Remember me

HTTP/2 Rapid Reset attack exploit

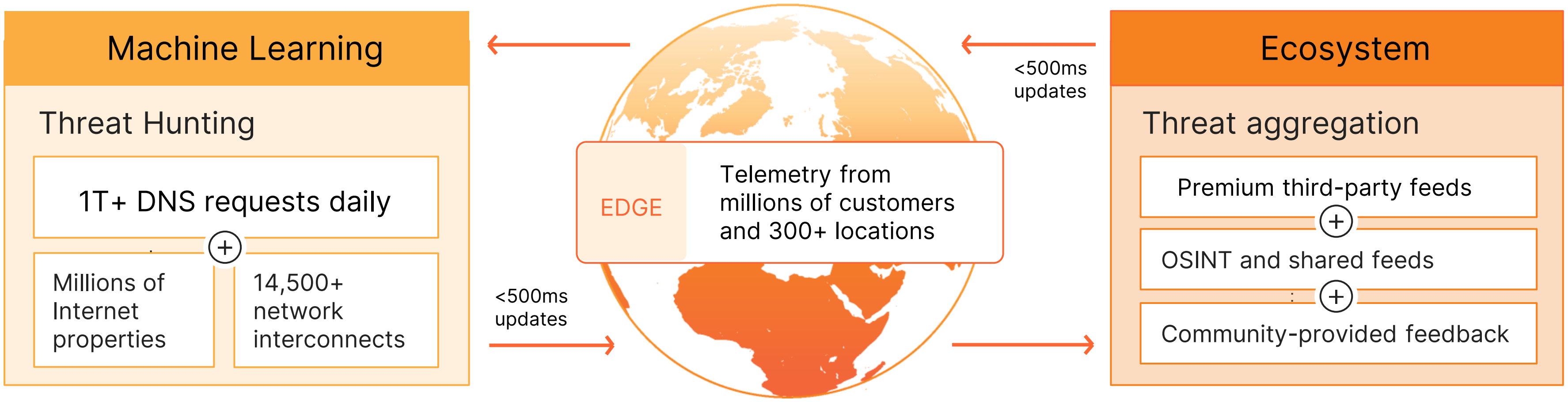


Cloudflare was the main target of the campaign



CLOUDFLARE

Threat Intelligence: Comprehensive coverage against Internet-borne threats



Machine Learning

Threat Hunting

1T+ DNS requests daily

+

Millions of Internet properties

14,500+ network interconnects

<500ms updates

EDGE

Telemetry from millions of customers and 300+ locations

<500ms updates

Ecosystem

Threat aggregation

Premium third-party feeds

+

OSINT and shared feeds

+

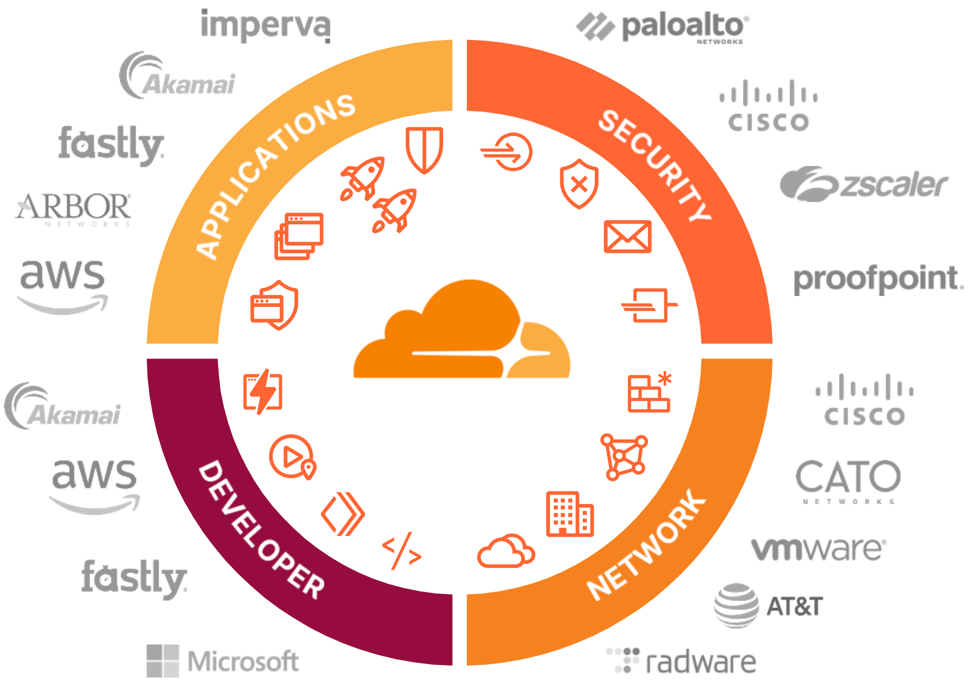
Community-provided feedback

LOG4J Protecting a full business day faster than leading competitor

Confluence Protections in place in 30 minutes; attacks began in 3.5 hours

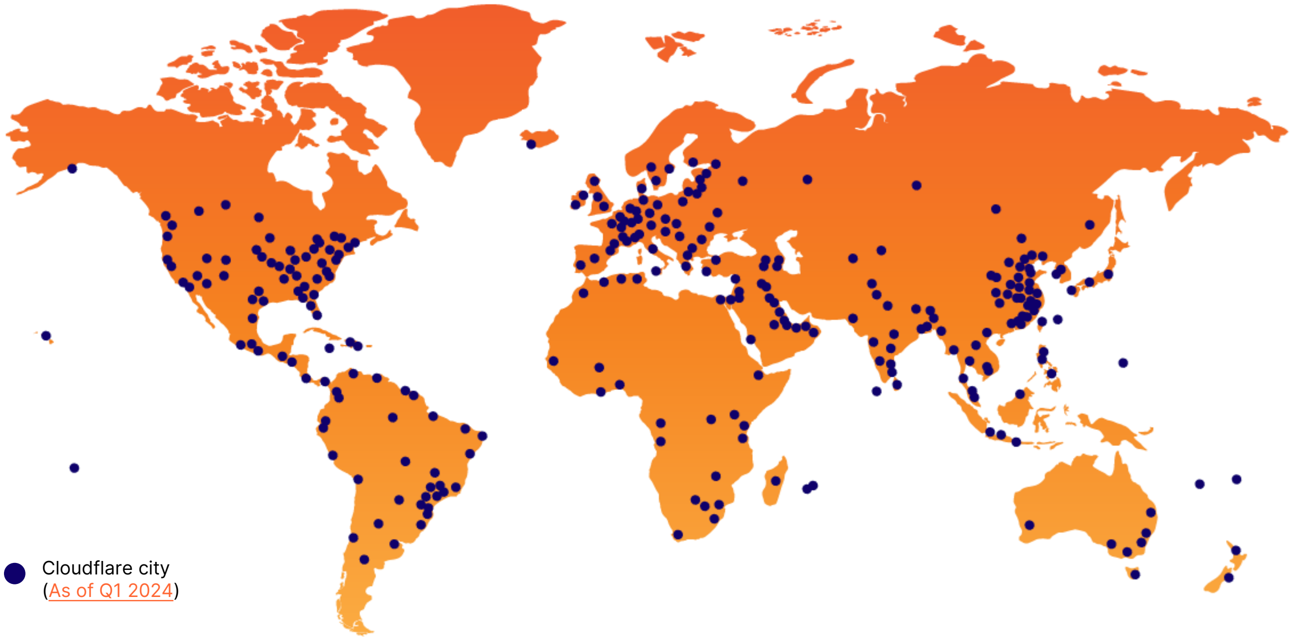
REPLACE MULTIPLE PRODUCT VENDORS ACROSS THESE CORE IT CATEGORIES

Our platform consolidates critical functions via a single, easy-to-use UI



Cloudflare is the only composable, Internet-native platform...

...that delivers local capabilities with global scale.


● Cloudflare city
(As of Q1 2024)

310+

cities in 120+ countries, including mainland China

120+

AI inference locations powered by GPUs

14,500

networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise

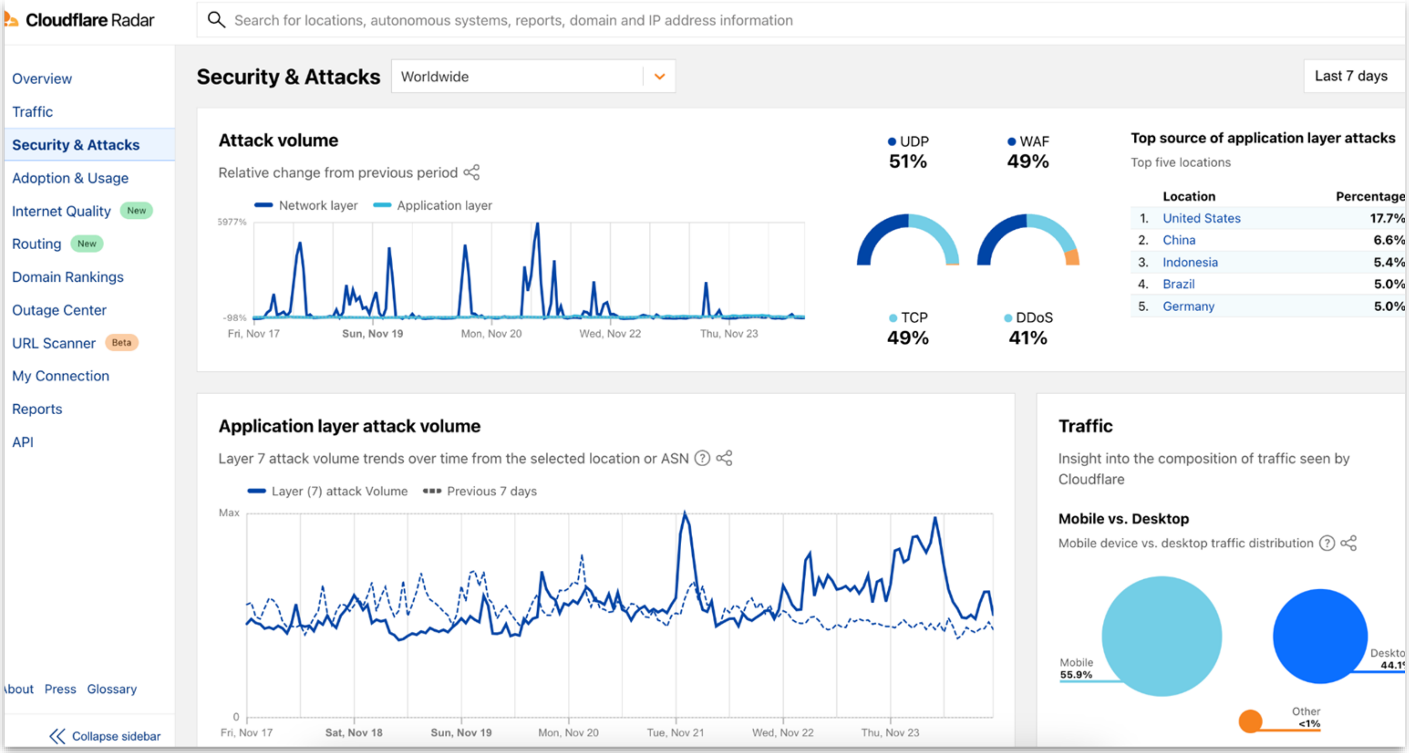
248 Tbps

global network edge capacity, consisting of transit connections, peering and private network interconnects

~50 ms

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

Dive in Deeper with Cloudflare Radar



Cloudflare Radar

Search for locations, autonomous systems, reports, domain and IP address information

Security & Attacks

Worldwide

Last 7 days

Attack volume

Relative change from previous period

UDP 51%

TCP 49%

WAF 49%

DDoS 41%

Top source of application layer attacks

Top five locations

	Location	Percentage
1.	United States	17.7%
2.	China	6.6%
3.	Indonesia	5.4%
4.	Brazil	5.0%
5.	Germany	5.0%

Application layer attack volume

Layer 7 attack volume trends over time from the selected location or ASN

Traffic

Insight into the composition of traffic seen by Cloudflare

Mobile vs. Desktop

Mobile device vs. desktop traffic distribution

https://radar.cloudflare.com/security-and-attacks

CLOUDFLARE

Thank You