Cybersecurity

Insights From Cloudflare's Network

Hector Gutierrez
Cloudflare / Territory Manager Caribbean
hector@cloudflare.com
M +14079464611

A single network that delivers local capabilities with global scale

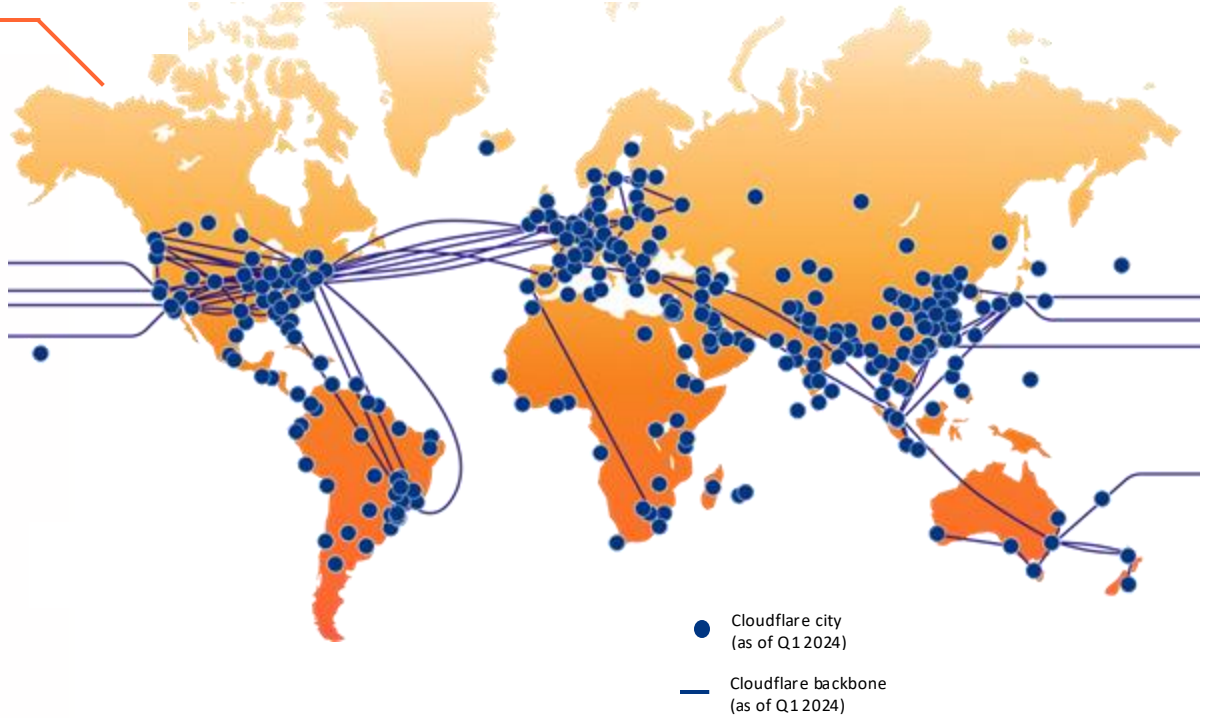
330+ cities
in 120+ countries, including mainland China

→ **w/160+ cities**
for AI inference powered by GPUs

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

~12,500 networks
directly connect to Cloudflare, including ISPs, cloud providers, and large enterprises

296 Tbps
of network capacity and growing

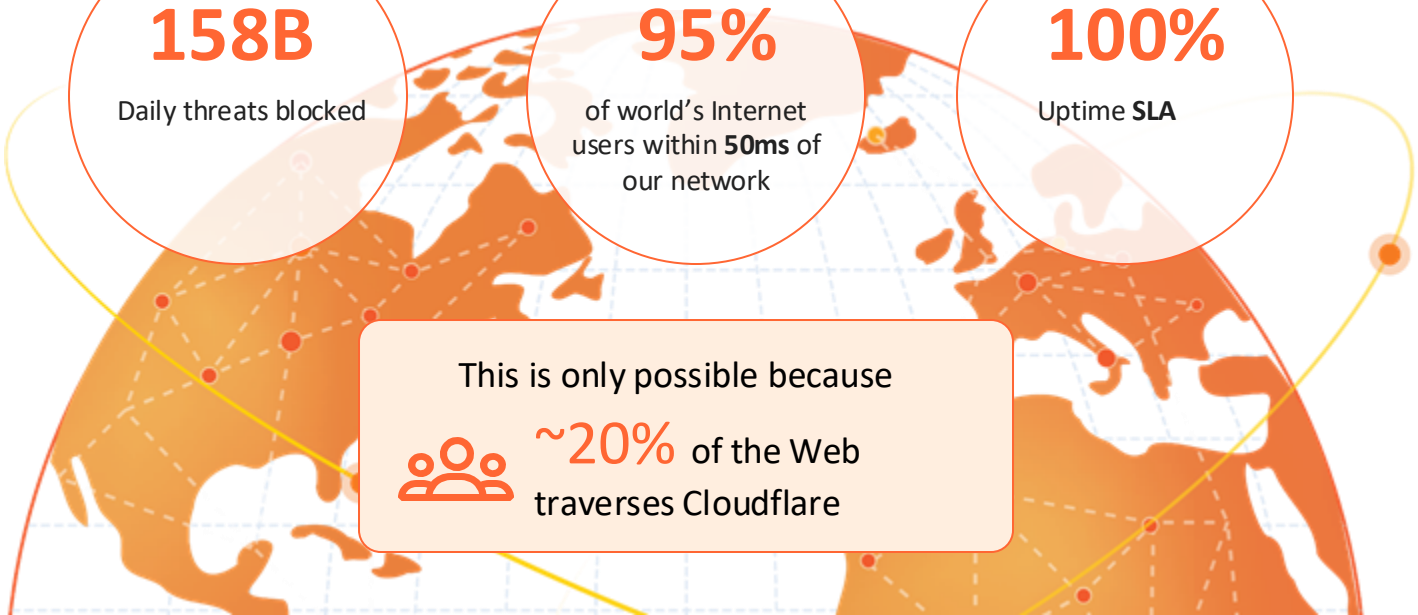


To provide a private, secure, reliable, performant, agile enterprise-grade Internet experience, Cloudflare is everywhere

158B
Daily threats blocked

95%
of world's Internet users within **50ms** of our network

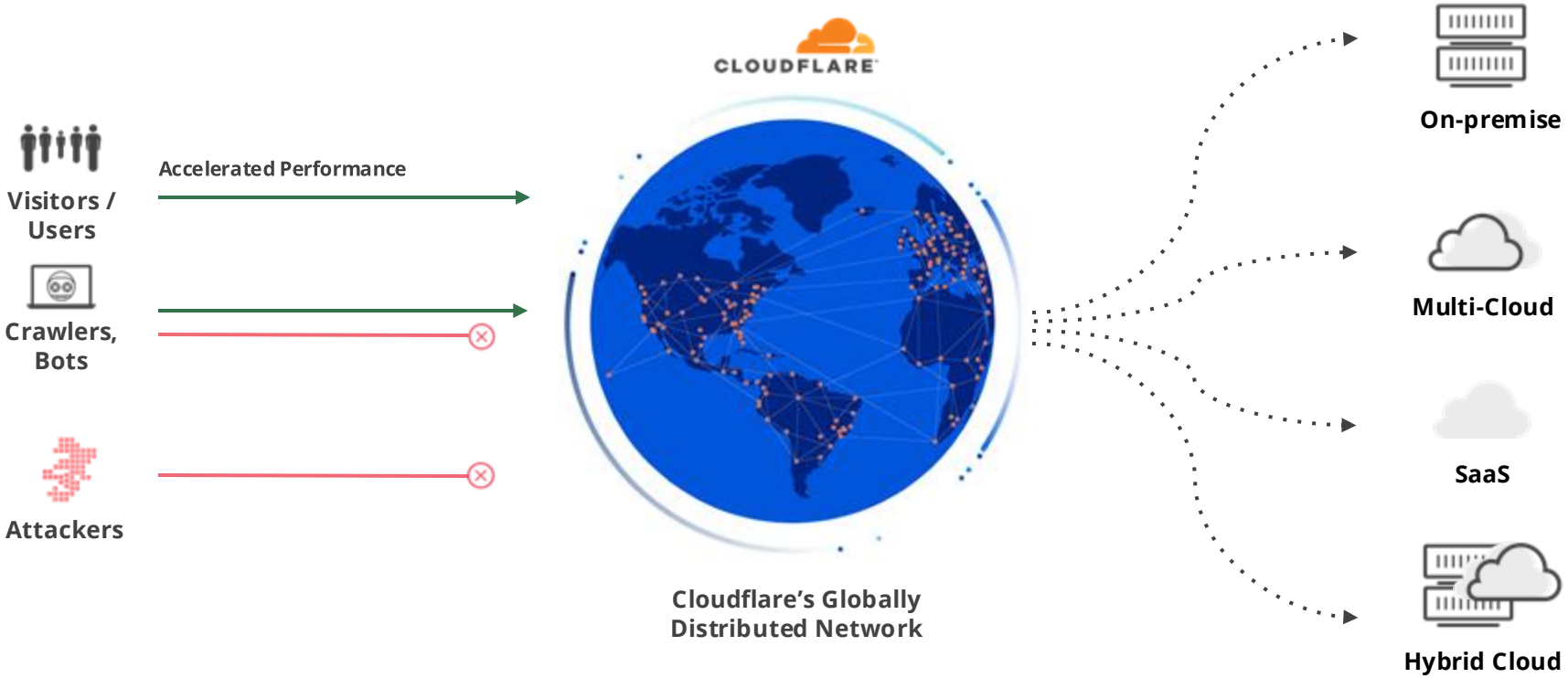
100%
Uptime **SLA**



This is only possible because

~20% of the Web traverses Cloudflare

How does it works ?



Shared intelligence provides comprehensive coverage against threats

Block

Isolate

Log

<500ms updates

Threat Types

Stop threats before they cause harm

- Web Attacks
- Zero Days
- Phishing
- Malware
- DDoS
- Malicious URLs

Protecting Cloudflare Customers Across

People

- Secure Web Gateway
- Cloud Email Security
- Browser Isolation
- Brand Protection

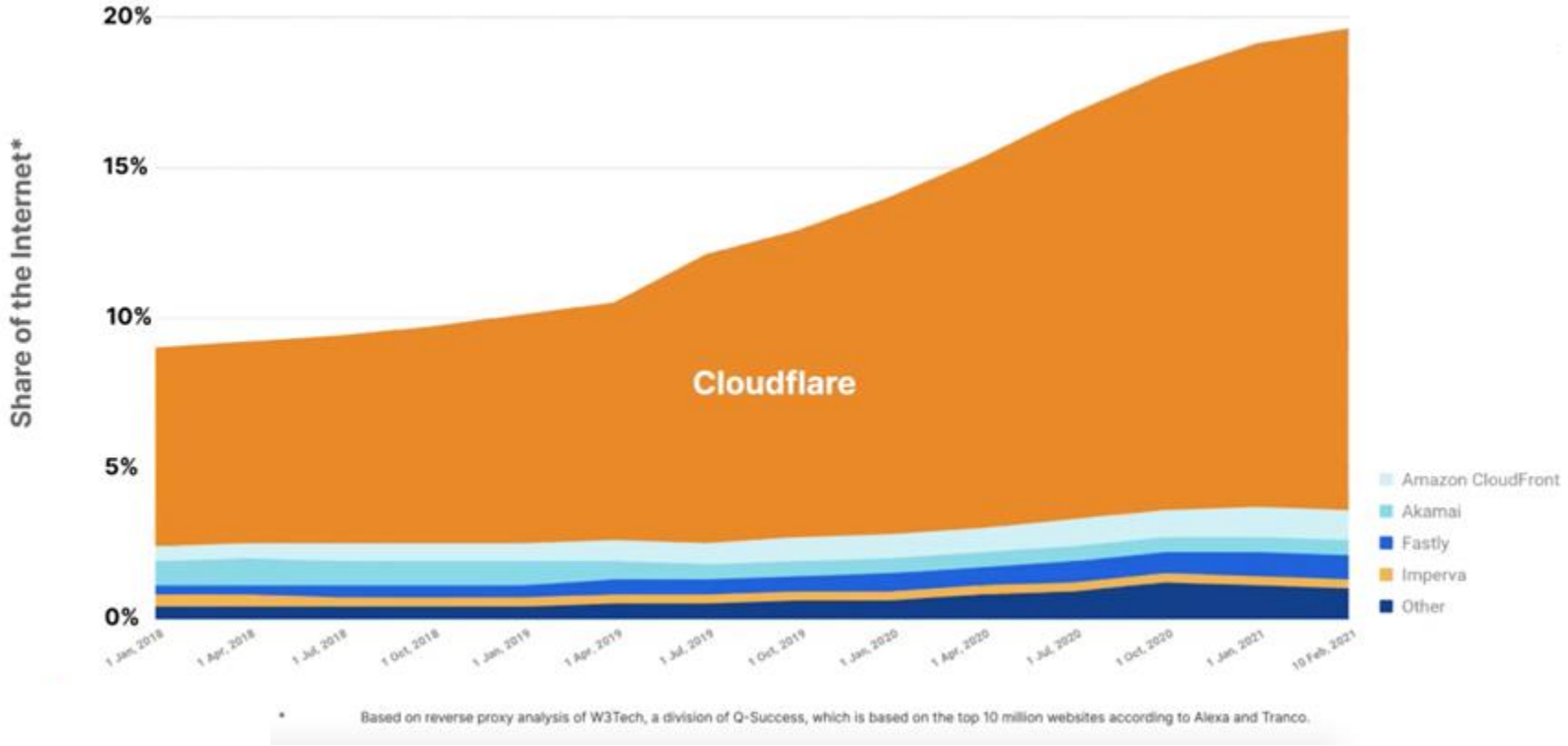
Applications

- Web Application Firewall
- Bot Management
- API Gateway
- L7 DDos Protection
- Client-Side Security
- Fraud Detection

Networks

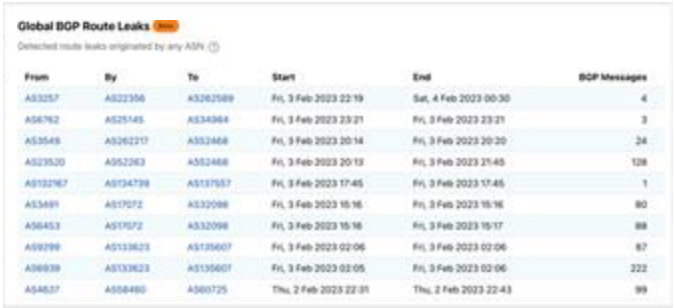
- Firewall as a Service
- L3/L4 DDoS Protection

Best security partner



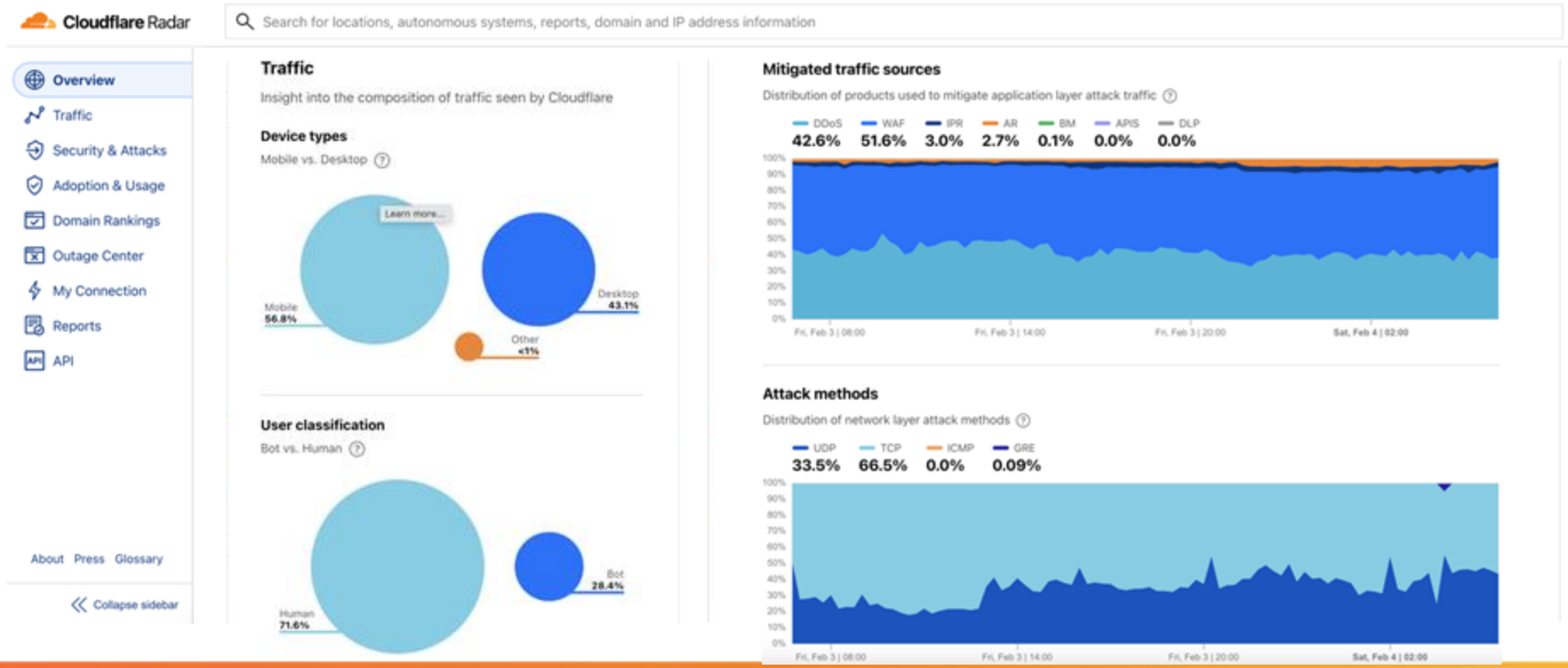
CLOUDFLARE

radar.cloudflare.com



CLOUDFLARE

radar.cloudflare.com



Cloudflare Threat Visibility and Intelligence

Threat trends overview

CLOUDFLARE

773%

Increase in size of largest DDoS attack

From 26 million requests per second in 2022, to 201 million in 2023

33%

More APIs found via ML than what orgs self-reported

Organizations have larger API attack surface than they think

74%

Of orgs adopting Zero Trust **plan to or have replaced VPN** for all employees*

22 minutes

from POC to exploitation

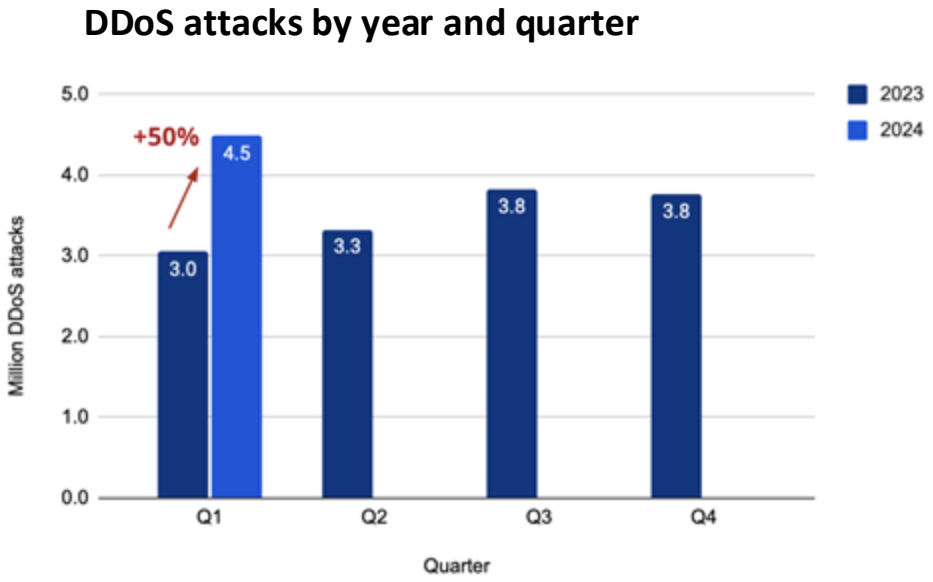
Vulnerability weaponization is accelerating

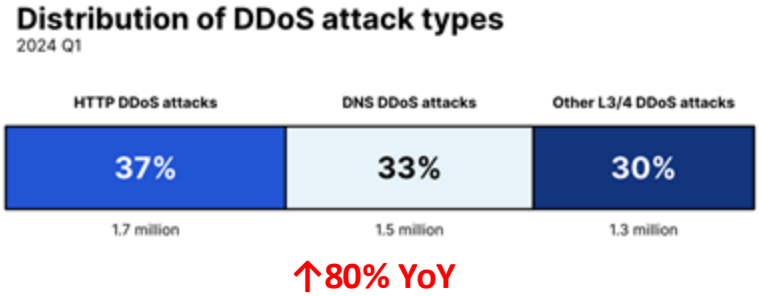
Phishing is still the #1 initial attack vector

*Source: IT & security professionals implementing Zero Trust. Enterprise Strategy Group, a division of TechTarget, Inc. Research Survey, Cloudflare Zero Trust for the Workforce Survey, May 2024.

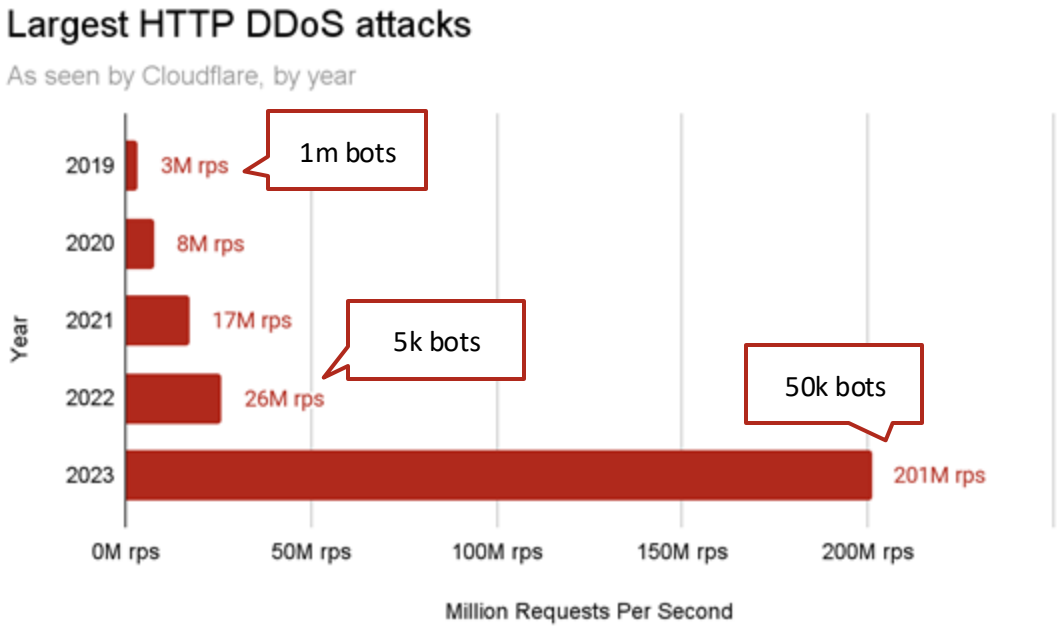
DDoS Attack Trends

DDoS attacks increased in 2024, especially targeting DNS





DDoS attacks are becoming more complex



- In 2023, the max attack size grew by **773% YoY**
- State-level capabilities at the hands of the common cyber criminal
- Increased focus on vulnerabilities in Internet protocols to launch large attacks

DDoS attacks are cheaper than ever to launch

Sites offering DDoS-as-a-service charge as little as $10 USD for a DDoS attack that lasts an hour as of 2023, or $35-170 USD for a full day use of their botnets.

5 years ago, it was closer to $30/hr or $400/day.

Source: Secure List by Kaspersky, 2023

Attacks highly focused on causing disruption

- Attacks coincide with geopolitical events
- Global target base spanning numerous critical infrastructure sectors
- Motivations appears to be disruption of services and political opposition to ideological beliefs (no financial gain)

API Risks

Unmanaged APIs leave organizations exposed

58%

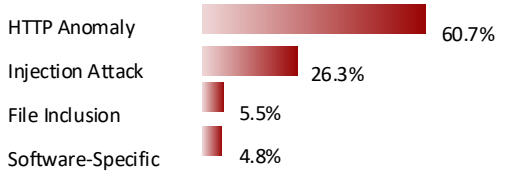
Of dynamic HTTP traffic on Cloudflare network is API related

33%

more API endpoints found by Cloudflare than what organizations self-reported

Top API threats

mitigated by Cloudflare WAF



For more on API risks, see Cloudflare's 2024 API Security & Management Report

Phishing Attack Trends

Phishing is still the #1 attack vector

9 of 10

successful cyber attacks start with phishing

~80%

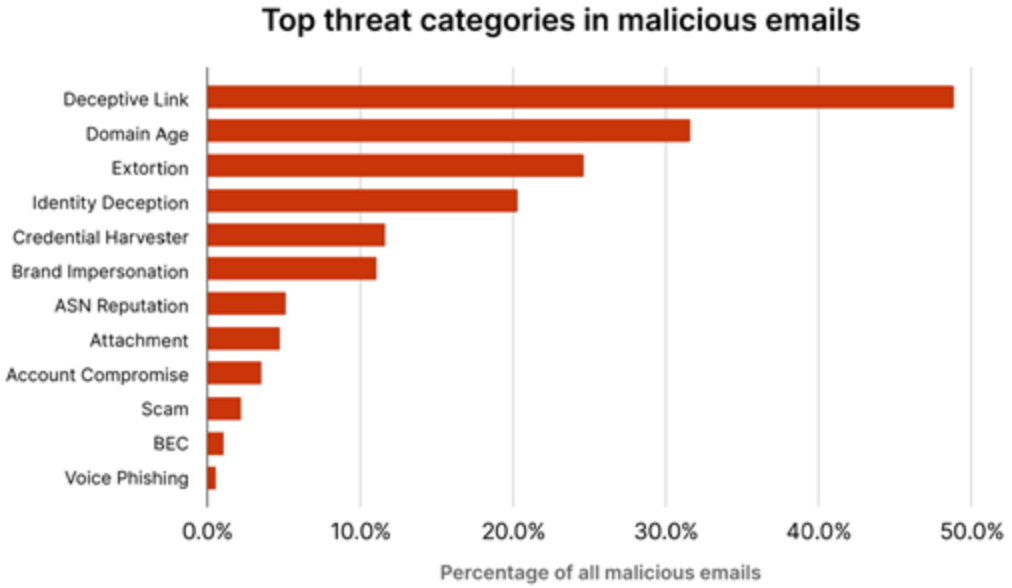
of firms exposed to multi-channel phishing*

$50 Billion

losses in BEC since 2013, up 17% YoY†

* Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, February 2023
† Source: FBI, BEC the $50 Billion Scam

Deceptive links are the most common threat, but BEC poses notable risk



BEC attempt with entire faked conversation thread

I have been told that it is ok to send you the payments ACH.

Please send your bank information to me and cc:

She will set you up with the bank.

Good Afternoon

Please be informed that our mailbox was vandalized overnight and any check mailed to us may not deliver till the issue is resolved.
We are hoping to resolve the mailbox issue soon as possible and we can start accepting check payments again.
We are respectfully asking you to kindly put a stop payment on the check that has been sent as we might not receive the check in our mailbox.
We now only accept all invoice payment through ACH
Do you have the ability to initiate ACH ?
Kindly advise so i can provide you with our ACH Banking instructions

Thank you,
Best Regards,

Credit Representative

From:
Sent:
To:
Cc:
Subject: RE: (External)

Good morning

Check # is in the process of getting signed and should be mailed by tomorrow.
Check # pays invoices less $150 Jumper fee.

Best regards.

Vulnerability Exploitation

Vulnerability disclosure and weaponization are accelerating

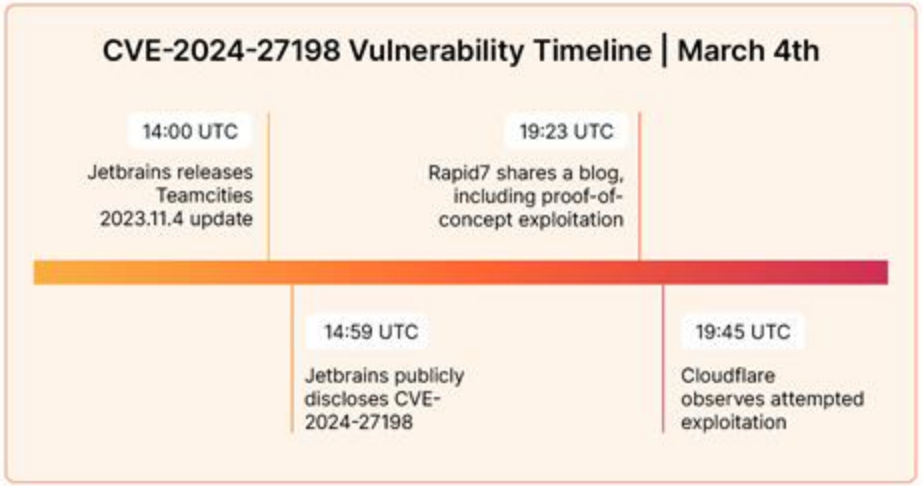
~100

zero-days in 2023, up 50%

29,000+

new CVEs disclosed in 2023

22 minutes from POC to exploitation



Organizations need to respond faster

Recommendations

Recommendations

1. **Implement modern DDoS mitigation best practices**
2. **Adopt a multi-pronged approach to vulnerability response**
3. **Assess and apply phishing controls that span all exposed user channels**
4. **Measure and improve API maturity level over time**
5. **Get involved in LLM projects early**

Under Attack - Always on

Under Attack?

Cyber Emergency Hotline

+1 (866) 325-4810

cloudflare.com/under-attack-hotline

Suffering an Attack?

Your company is currently suffering a cyber attack that threatens the availability, confidentiality or integrity of your internet facing system?

Got a Ransom Note?

You have received a ransom note with the threat of imminent attack or has credible threat intelligence indicating the same threat.

Need immediate onboarding?

You require urgent mitigation of said threat and commits to the immediate on-boarding of the Internet properties targeted by the attack

Cloudflare offers Comprehensive Protection Against Cyber Attacks in minutes

Protection Against DDoS, Website, Application, Workforce and Infrastructure Attacks in minutes

24/7 dedicated team to answer your requests - It only takes us hours to have you onboarded and our solution implemented.