quad9

Preventing Abuse Through the DNS:

An Overview of Activities in Japan Based on Quad9 Observations

John Todd - Chief Technology Officer
jtodd@quad9.net

JPAAWG 8th General Conference
5 November 2025, Kochi Japan

About Quad9

- Provides recursive DNS resolution with threat blocking capability
- Non-profit Foundation
- Based in Zurich, Switzerland 
- Established in 2017
- 9 on the team, plus volunteers
- Estimated >100 million users worldwide
- Major sponsors: IBM, PCH, OTF, Newmark Philanthropies

Key Points Of Quad9 Mission:

- **Security:** Keep users from reaching malicious content
- **Privacy:** Ensure user activities are kept confidential
- **Integrity:** Deliver the correct DNS data that is expected

What does Quad9 do?

- Quad9 protects user security against :
  - Phishing sites
  - Malware distribution sites
  - Botnet command & control sites
  - Malvertising (privacy invasive user tracking or pop-ups)
  - Cryptocurrency hacking / mining
  - Other sites that are harmful and unexpected by users

- Quad9 protects user privacy with encryption and no logging
- Strong DNSSEC validation for supported zones - high integrity answers
- Mail server anti-phishing tooling is never perfect: Multiple layers of defense needed

What does Quad9 not do?

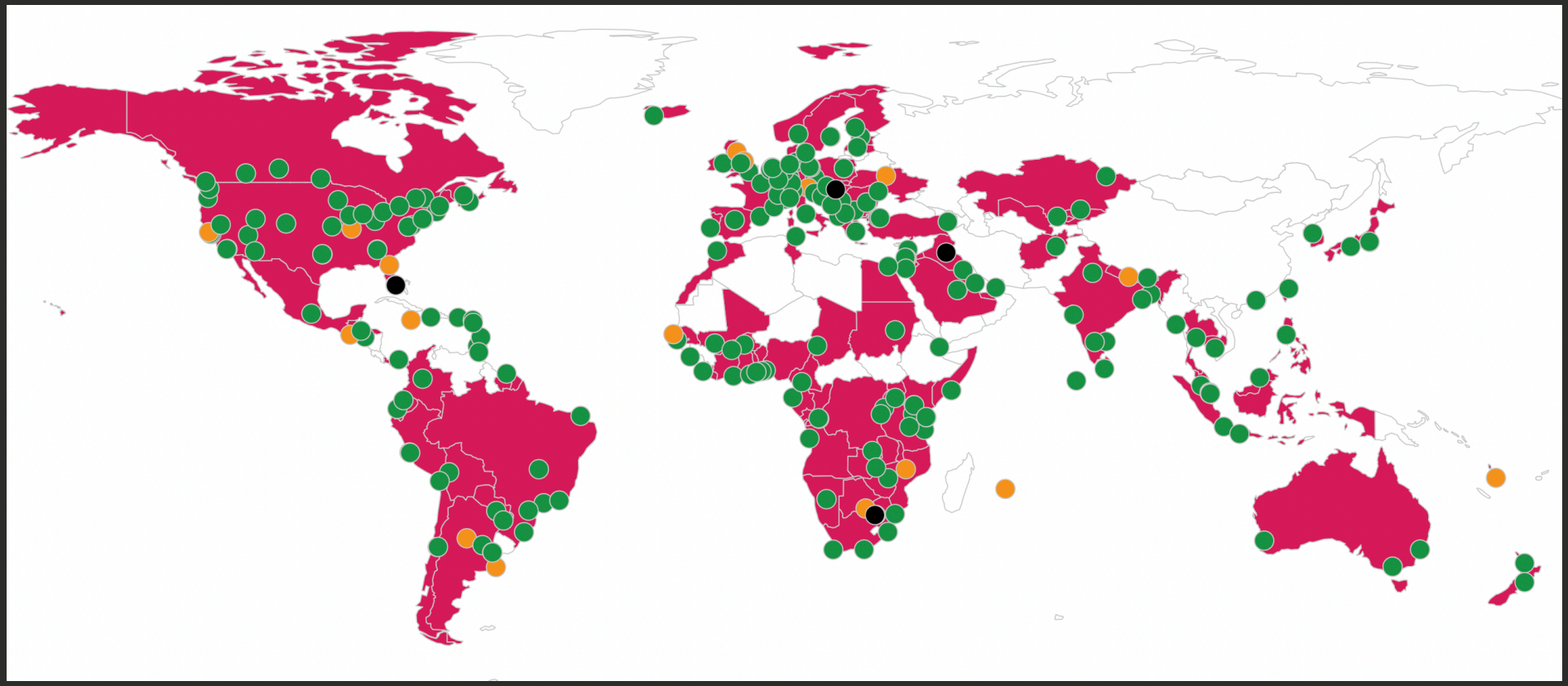
- Does not protect mail servers from spam
- Does not block advertisements
- Does not block content (adult, etc.)
- No logging of IP addresses
- No other service products - only DNS

How do we make money?

- We do not charge for end-user services
- All network (space, power, transit) are donated
- All threat data is donated in exchange for insights
- Staffing and equipment cost are funded through industry partnerships, grants, & donations
- All DNS resolution services are entirely free
- We do provide aggregate information (example: NOD lists) for partners who sponsor our mission

quad9

250+ Sites in more than 120 Nations



3 in Japan: NRT2, ITM, QHND2

Who can use Quad9?

- Individuals / Households
- Schools
- ISPs
- Businesses
- Hospitals
- Government
- Anyone - there are no limitations.

(*) Sites over 10,000 users - please ask us first so we can ensure capacity

How to use Quad9?

quad9

- Change recursive resolver settings to:
  - 9.9.9.9
  - 149.112.112.112
  - 2620:fe::fe
- That is all that is needed. No account, no software, no sign-up.
- We also support DOH/DOT/DNSCrypt encryption!

Threat Intelligence Partners

quad9

Threat domains in .jp TLD

1,888 domains ending in .jp (2025-10-28)

Random Examples:

```
mamazon.jp
cocorost-556.jp
www.csltovuq.yaginobouken.jp
googler.jp
rbrnbtrntntmtm.jp
netaflix.jp
agtjtgtnja.jp
```

quad9

What can we show about DNS-based blocking in Japan?

quad9

Inputs for Data Examination

Inputs:

- **Threat list:**

  4.3 Million names in malicious domain list
  (2025/10/28) (+/- .5M names daily)

- **Locations in Japan:**

  NRT2: Tokyo (PCH - Equinix)
  QHND2: Tokyo (i3D - Equinix)
  ITM: Osaka (PCH - Equinix)

quad9

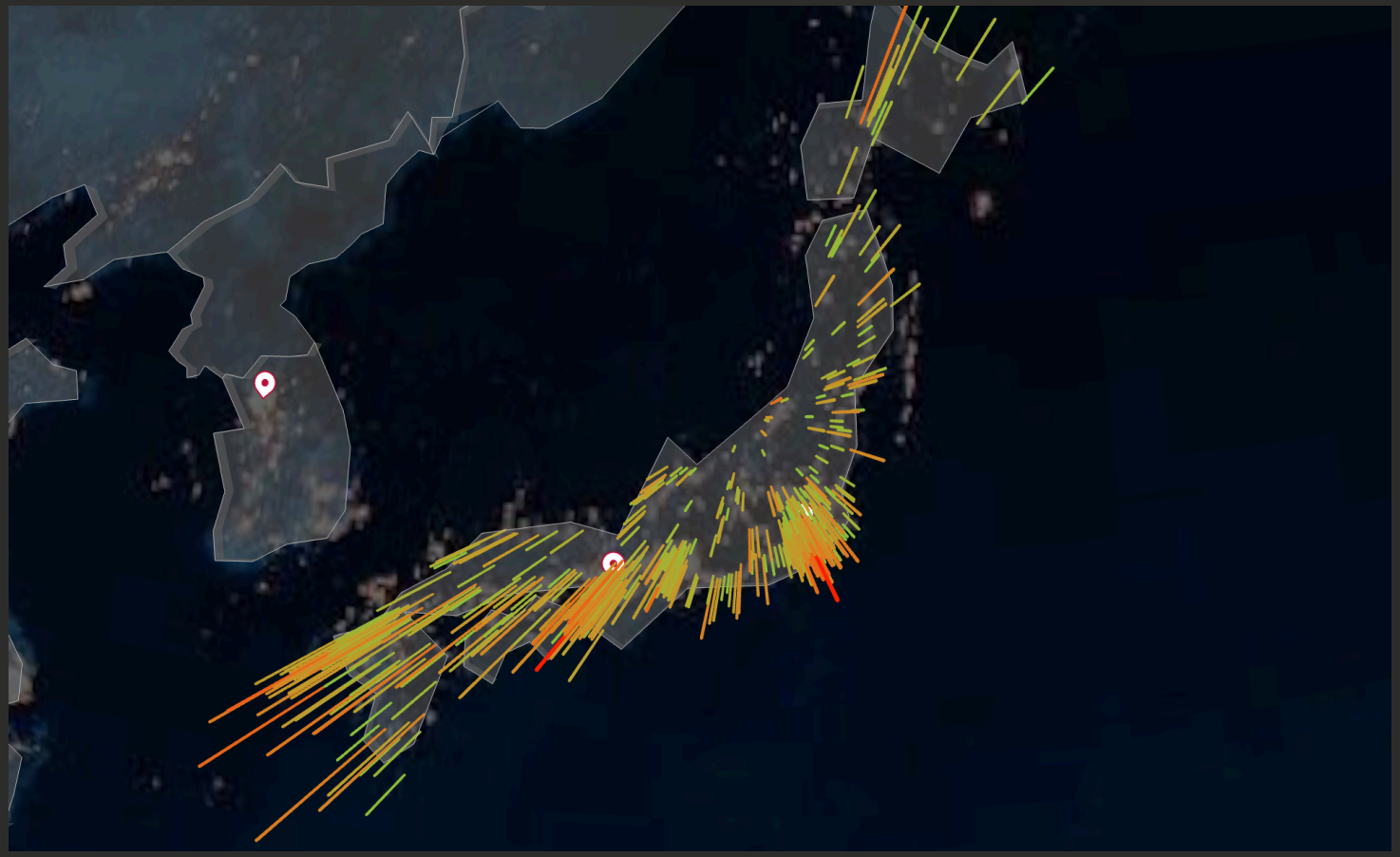
Inputs: How many Quad9 users are in Japan?

The bad news: We don't know.

The good news: We don't know.

Quad9 never tracks user data.
This is our pledge to keep data private.
>100 million users estimated worldwide

Inputs: User Distribution (30s sample)



quad9

Outputs: 24 hour sample
Japan Only

quad9

Malicious Blocking Events: Japan 2025-10-28

- 4,450,000 blocked connection attempts
- 37,615 unique names blocked
- Block rate is below 0.1 % of DNS query volume
- No reported false positives in this interval

Blocks: TLD Distribution

TLD Percentage of blocking events, sorted by TLD in Japan 24hr (2025/10/28)

TLD	total_count	percentage
biz	2858978	64.56
com	442602	9.99
info	265453	5.99
live	256511	5.79
cn	202955	4.58
net	57354	1.30
shop	52146	1.18
top	39528	0.89
io	37650	0.85
app	29843	0.67
vip	22668	0.51
xyz	16785	0.38
cc	14779	0.33
kr	13280	0.30
org	12703	0.29

... etc. ...

Blocks: Second Level Domain Uniqueness

18,662 second level unique zones in block data for Japan 24hr (2025/10/28)

SLD	total_count	percentage
gaihwstpzuomtfnu	497625	11.24
gpoppa	34109	0.77
uyabbt	33033	0.75
xmcxmr	29499	0.67
hzyidc	28698	0.65
cloudfront	28646	0.65
polyfill	27839	0.63
vnvbt	23802	0.54
dyjdrp	23758	0.54
sctmku	23681	0.53
qvuhsaqa	23608	0.53
sewlqwcd	23560	0.53
vgypotwp	23543	0.53
kkqypycm	23508	0.53
wluwplyh	23461	0.53

... etc. ...

Blocks: FQDN Uniqueness

37,615 Unique FQDN in 24 hours blocked by Quad9 in Japan 24hr (2025/10/28)

domain_name	total_count	percentage
khbw.gaihwstpzuomtfnu.info	62840	1.42
kdxa.gaihwstpzuomtfnu.info	62831	1.42
eicp.gaihwstpzuomtfnu.info	62789	1.42
yfrv.gaihwstpzuomtfnu.info	61684	1.39
khbw.gaihwstpzuomtfnu.live	61524	1.39
eicp.gaihwstpzuomtfnu.live	61371	1.39
yfrv.gaihwstpzuomtfnu.live	61197	1.38
kdxa.gaihwstpzuomtfnu.live	60761	1.37
pic.uyabbt.cn	33033	0.75
kinh.xmcxmr.com	29499	0.67
opencdnv6.f24i25ec.hzyidc.com	28698	0.65
d27xxe7juh1us6.cloudfront.net	28646	0.65
polyfill.io	24936	0.56
vnvbt.biz	23802	0.54
dyjdrp.biz	23758	0.54
sctmku.biz	23681	0.53
qvuhsaqa.biz	23608	0.53
sewlqwcd.biz	23560	0.53
vgypotwp.biz	23543	0.53
kkqypycm.biz	23508	0.53

... etc. ...

quad9

SUCCESS!

Now what do we do?

3.3% weekly growth for last 2 months in Japan

Overall growth: >1.6% weekly, worldwide

Data Exchange Wanted

- We need new partners in Japan for threat data:
  - Japanese-specific phishing domains
  - SMS-based phishing domains
  - IDN-based data (non-Latin) alphabet threat domains needed!
- We offer in return: detailed data on volumes and patterns of usage of those domains

Quad9 Expansion in Japan

Continue the Good Work!

- Quad9 needs new financial sponsors who wish to protect Japanese citizens and networks by funding existing or new sites
- We need Japanese-language promotion of our services - outreach to:
  - ISPs
  - Individuals
  - Networking Expert Groups
  - Civil Society groups (protection of individuals)
  - Law Enforcement / Anti-Crime groups

quad9

end

9.9.9.9 / 149.112.112.112 / 2620:fe::fe

jtodd@quad9.net