Expectation vs. Reality:

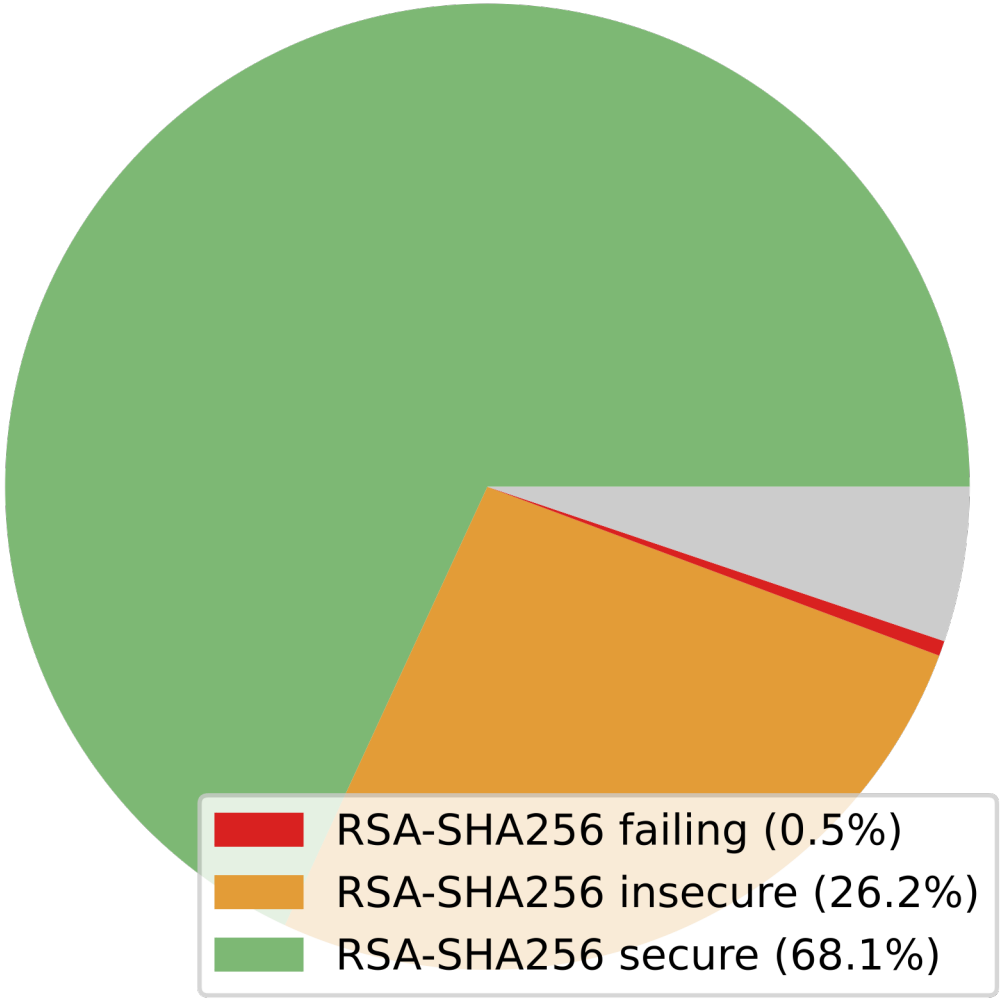
The Impact of DNSSEC Validation on Recursive Resolver Operations

Moritz Müller, Elmer Lastdrager, Cristian Hesselman | OARC 40

10 February 2023

The current situation

DNSKEY Algorithm
RSA-SHA256 support
of 24,113 resolvers used
by RIPE Atlas probes[1]



[1] https://dnsthought.nlnetlabs.nl/#rsasha256

Why are resolvers not validating DNSSEC?

Hypotheses

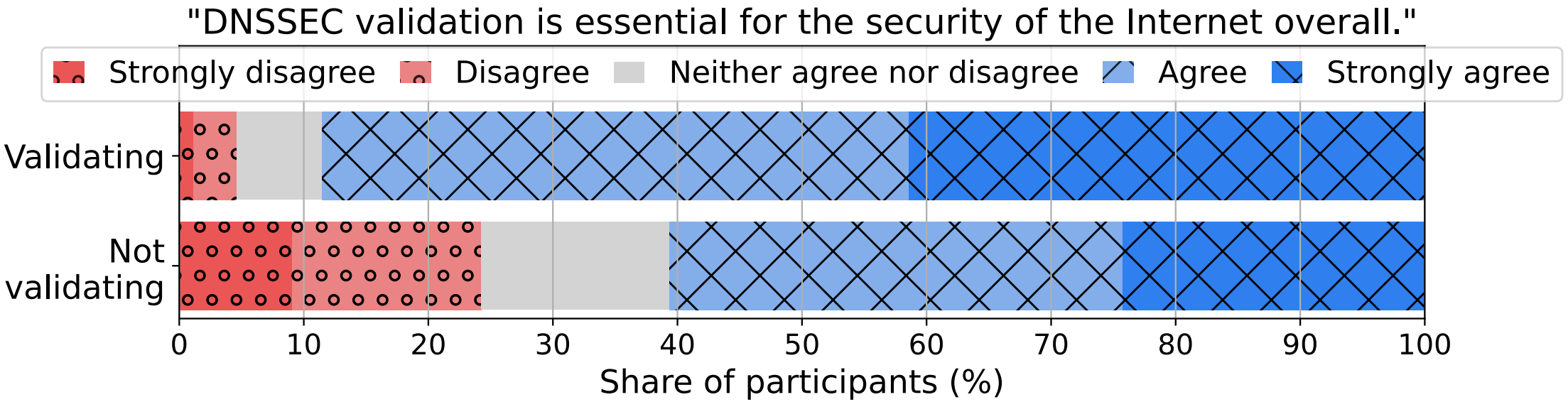
- Operators see DNSSEC validation as a burden
- Operators do not see the benefits of DNSSEC validation

Approach

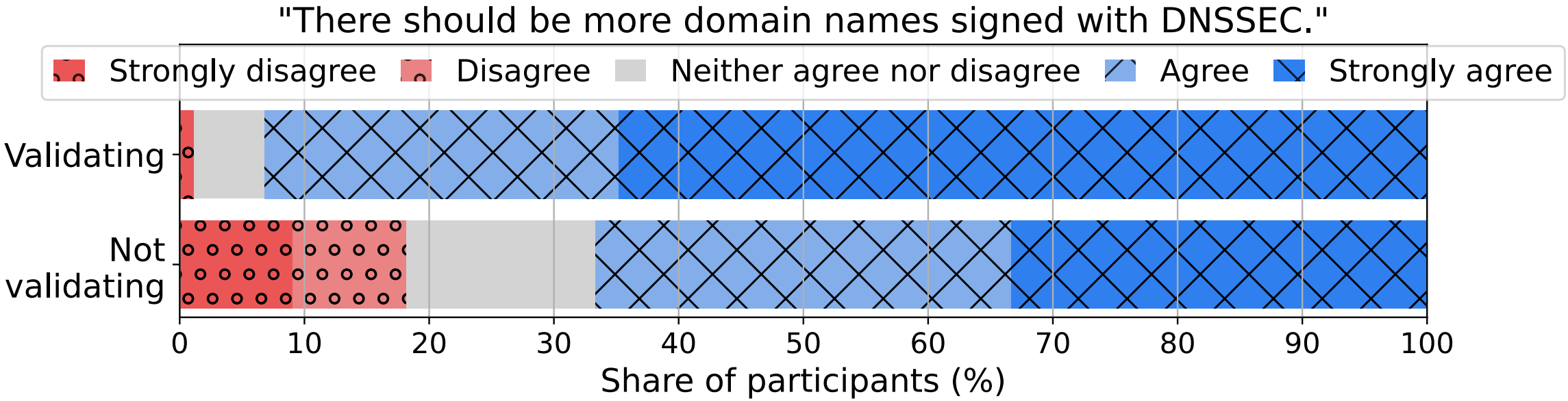
- Carry out a survey among 120 operators of recursive resolvers
  - Of which 87 (72.5%) run validating resolvers
  - That work for a large variety of organizations (e.g. ISPs, educational networks, and public DNS services)
- With a varying number of clients – between a few hundred and a few million
- Additionally, 6 interviews for anecdotal evidence

What is the perceived value of DNSSEC for resolver operators?

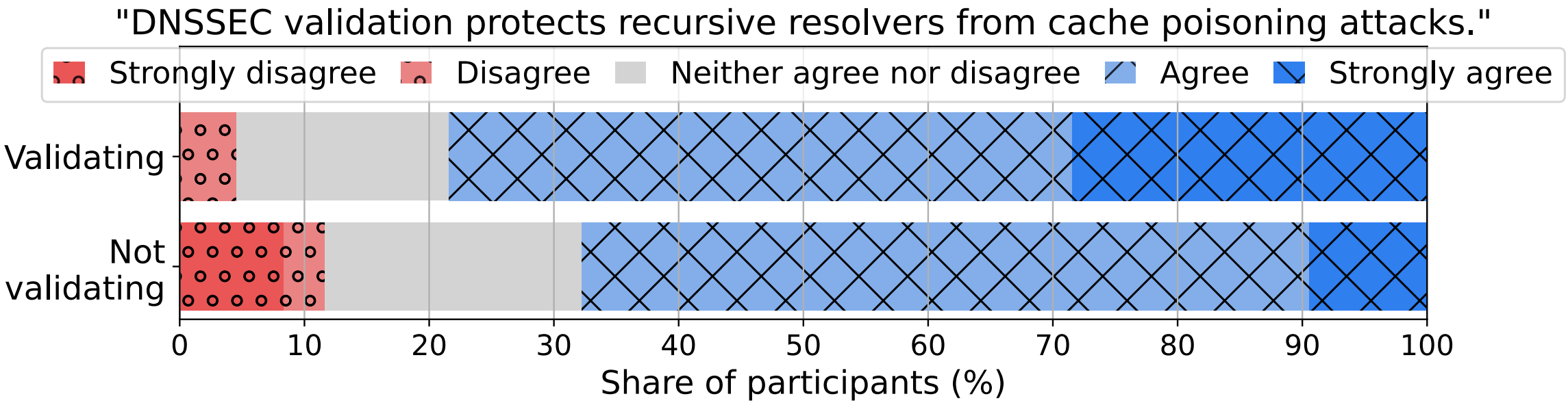
What is the perceived value of DNSSEC for resolver operators?



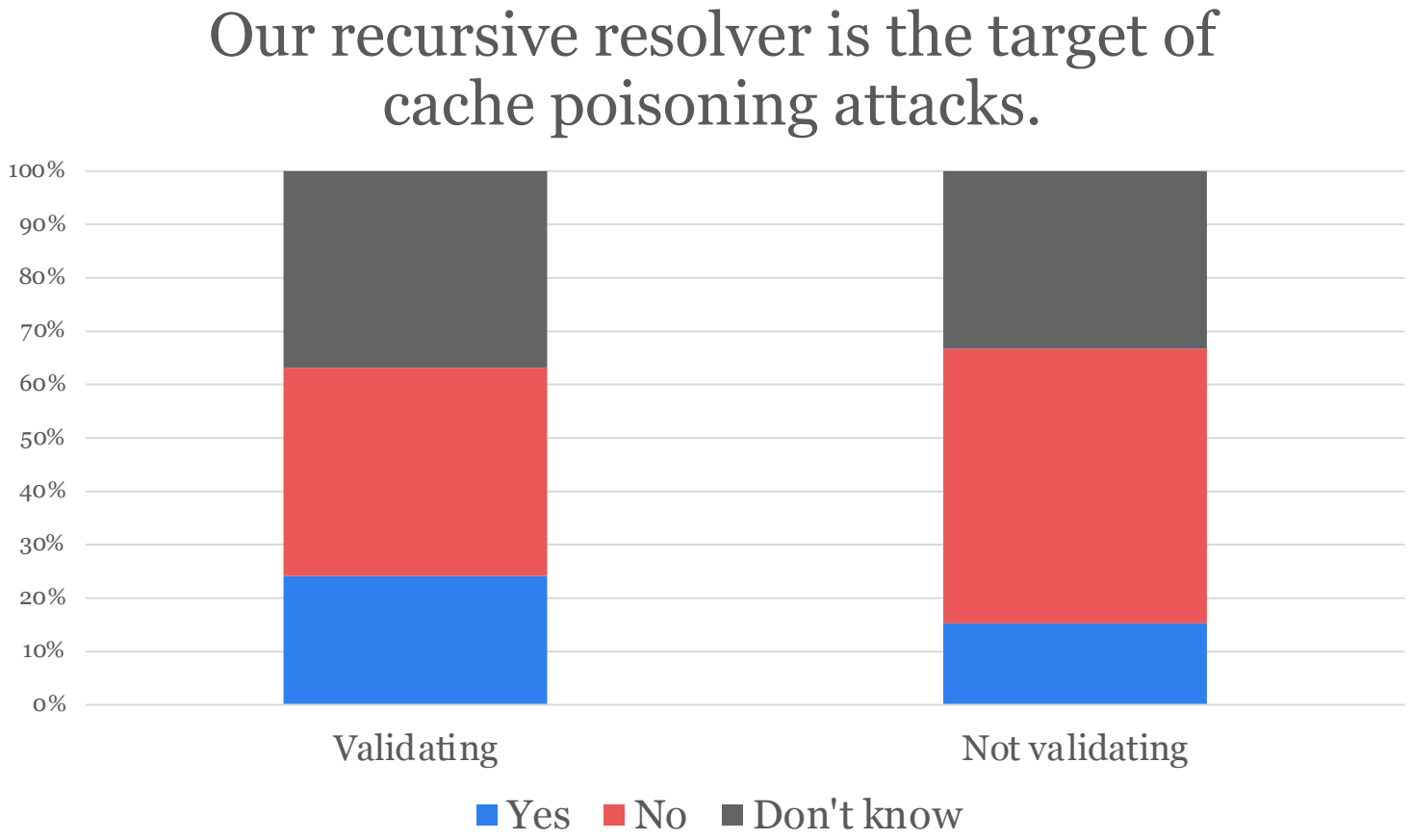
What is the perceived value of DNSSEC for resolver operators?



What is the perceived value of DNSSEC for resolver operators?



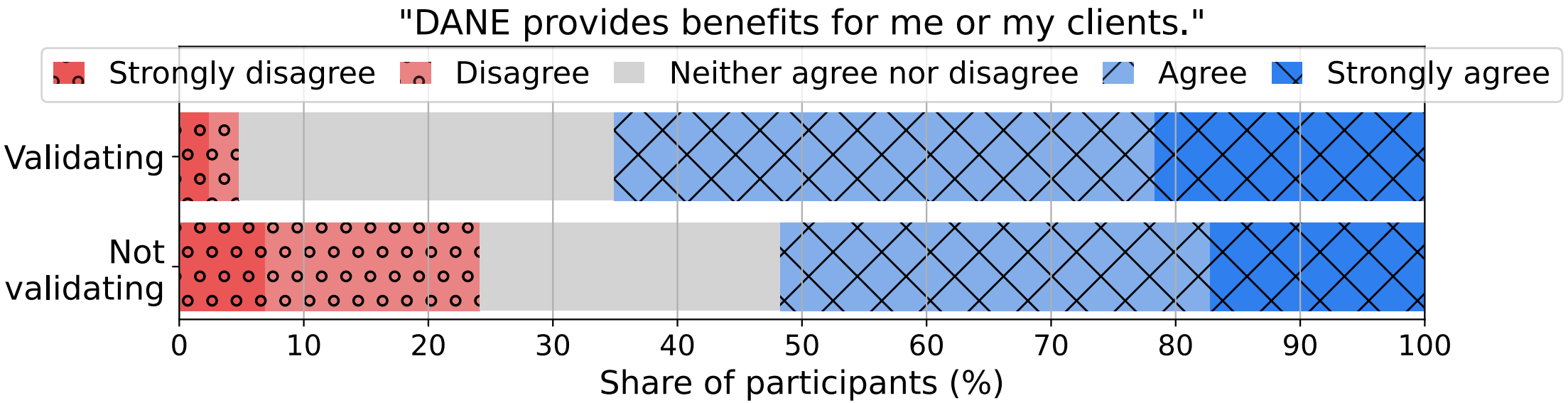
What is the perceived value of DNSSEC for resolver operators?



Do protocols and technology based on DNSSEC increase the value?

Do protocols and technology based on DNSSEC increase the value?

DANE



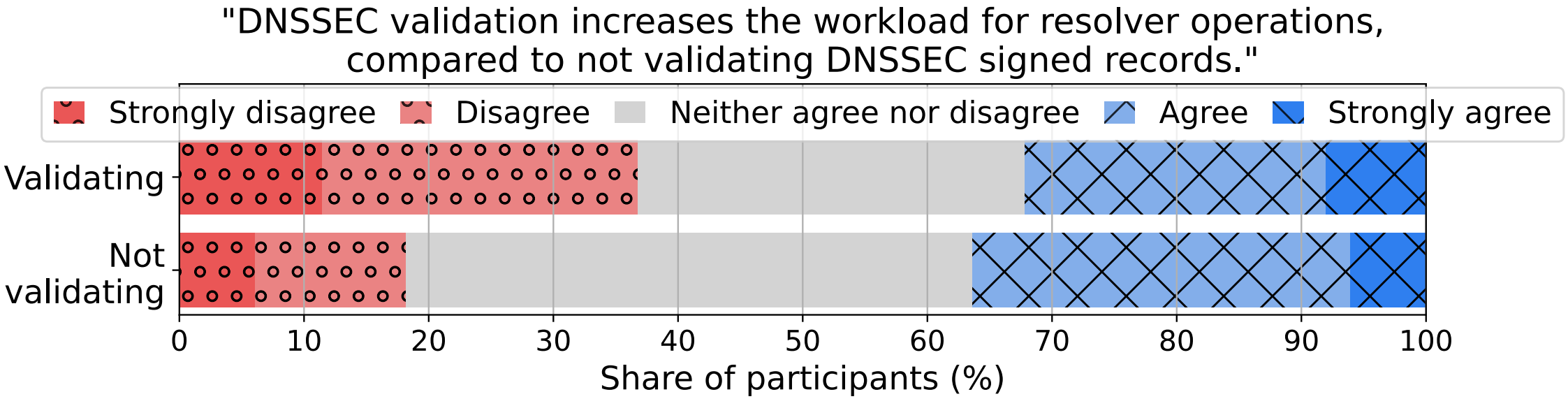
Do protocols and technology based on DNSSEC increase the value?

Aggressive Use of DNSSEC-Validated Cache (RFC 8198)

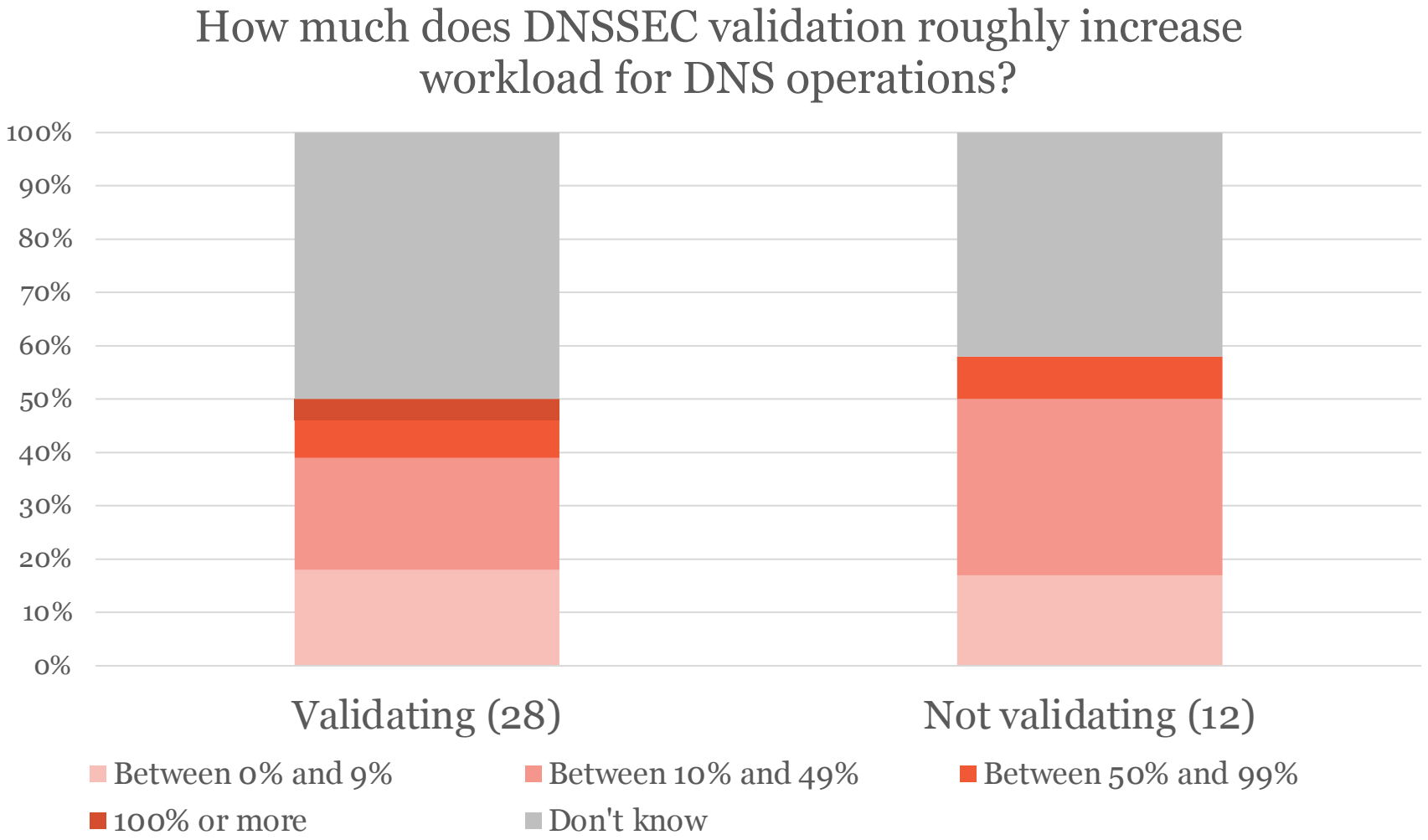
- 56% of all operators have heard of RFC 8198
- 28% of non-validating operators might turn on RFC 8198 in the future

What is the perceived (and experienced) operational and organizational overhead of DNSSEC?

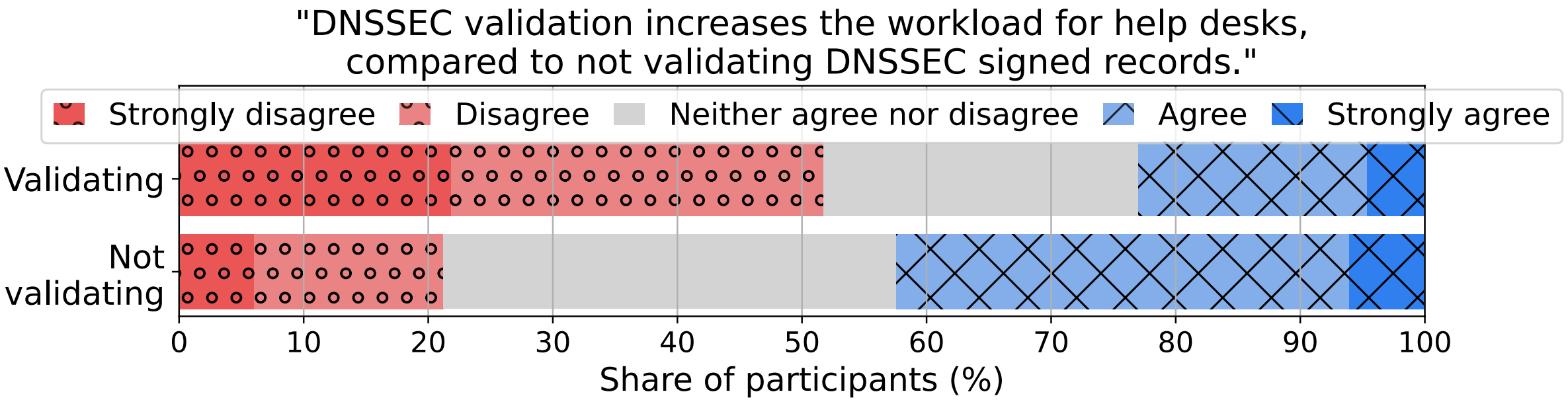
What is the perceived (and experienced) operational and organizational overhead of DNSSEC?



What is the perceived (and experienced) operational and organizational overhead of DNSSEC?



What is the perceived (and experienced) operational and organizational overhead of DNSSEC?



What causes the overhead?

What causes the overhead?

- Misconfigurations at the domain name
  - At operations: 64% validating, 83% not validating
  - At help desks: 80% validating, 57% not validating

Does the type of DNS service and organization play a role?

Does the type of DNS service and organization play a role?

Type	Total (%)	Validating	Not validating	Validation Rate %	Dedicated Team %
ISP	45 (37.5)	31	14	68.9 ↘	31.1 ↘
Education	19 (15.8)	15	4	79.0 ↗	31.6 ↘
Commercial	16 (13.3)	9	7	56.2 ↘	25.0 ↘
Hosting	11 (9.2)	8	3	72.7	18.2 ↘
Public DNS	9 (7.5)	8	1	88.9 ↗	55.5 ↗
Cloud	8 (6.7)	6	2	75.0 ↗	37.5 ↗
Private	8 (6.7)	8	0	100 ↗	–
Governmental	4 (3.3)	2	2	50.0 ↘	25.0 ↘
All	120	87	33	72.5 ($\bar{x}$)	34.9 ($\bar{x}$)

Conclusions

- DNSSEC is perceived useful
- DNSSEC validation can increase the workload, but by how much differs
- DNSSEC sceptics vs DNSSEC sympathizers

Discussion and Recommendations

- How to convince the DNSSEC sympathizers?
  - More signed domain names
  - Improve DNSSEC signing further
  - Hope that DNSSEC validation becomes the new default “by its own”
  - Move validation to the client

Follow us

SIDN.nl


@SIDN

SIDN

Thank you for your attention!