Continuous threat intelligence improvements

Leonardas Marozas (CUJO AI, Lithuania)
@CUJOAI

Whoami

- Security researcher/manager @ CUJO AI®
- Lecturer at Vilnius technical university
- Balancing academic and private backgrounds

TI quests to

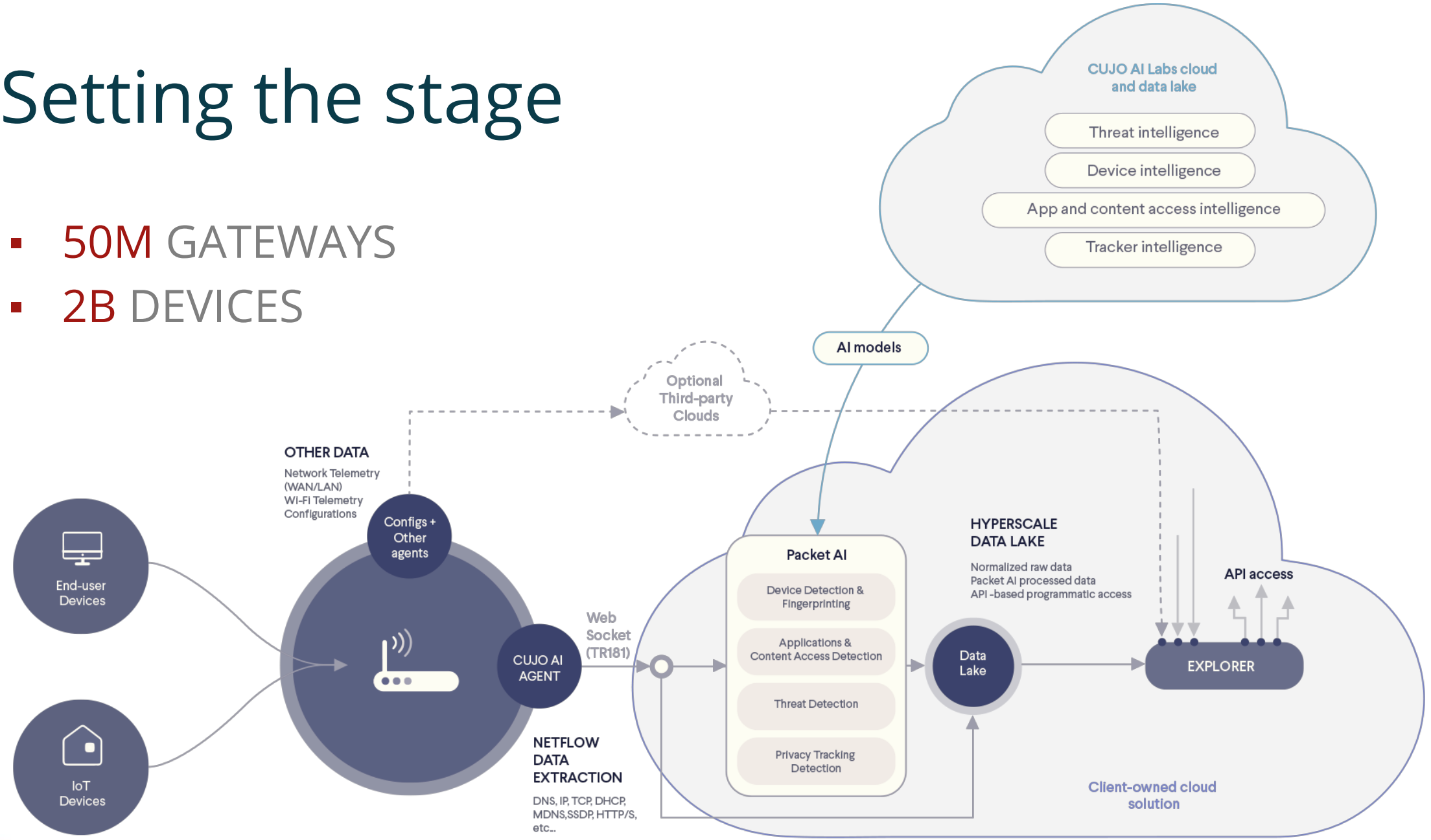
- Find the magical pill in threat intelligence
- Find intelligence
- Find the best sources of IOCs
- Find the best platforms for TI
- <…>

TI related misconceptions

- There is a magical pill in threat intelligence that can fit everyone's need
- You can buy the best threat intelligence
- You can find the best threat intelligence for free

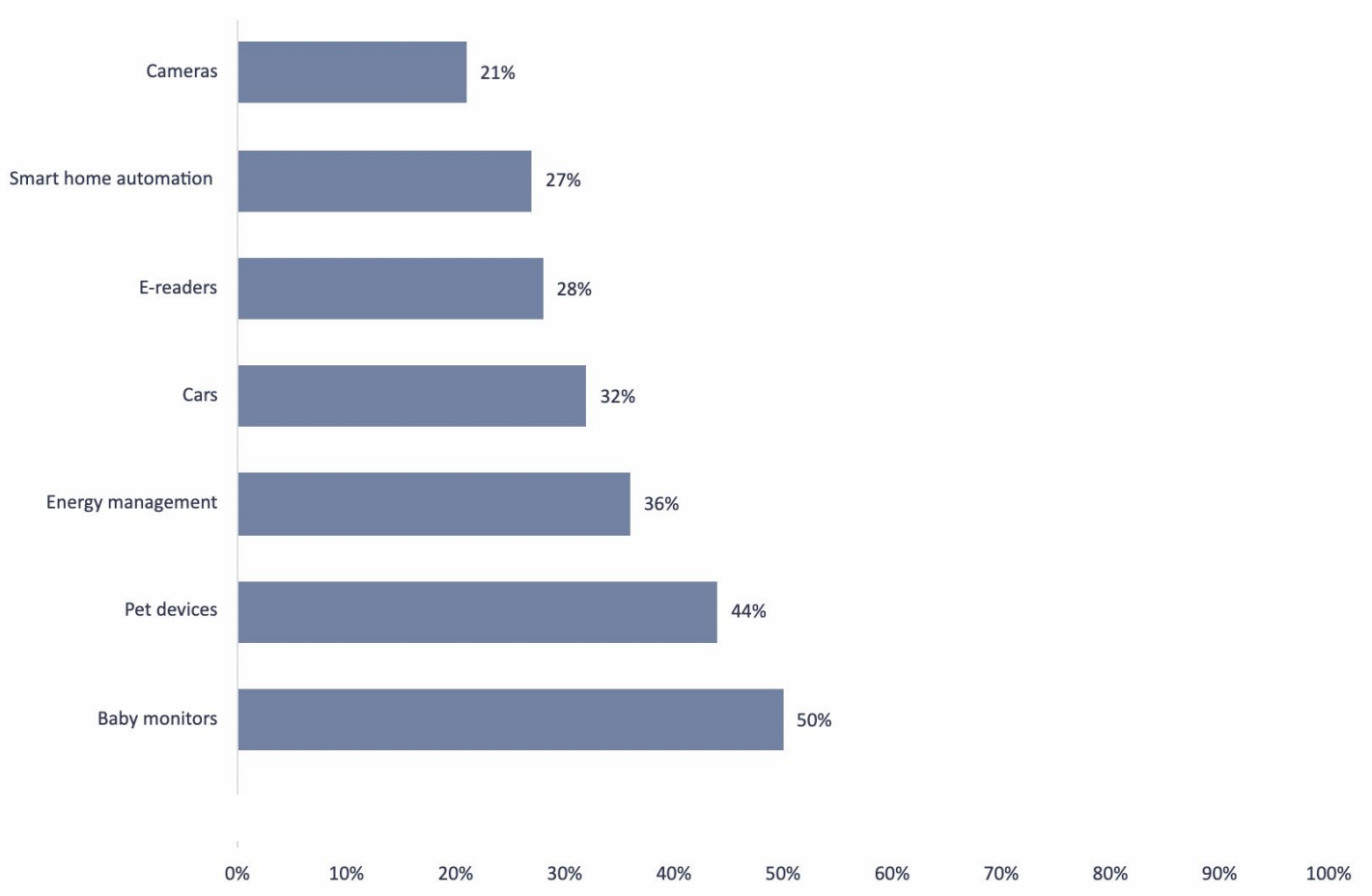
Setting the stage

- 50M GATEWAYS
- 2B DEVICES



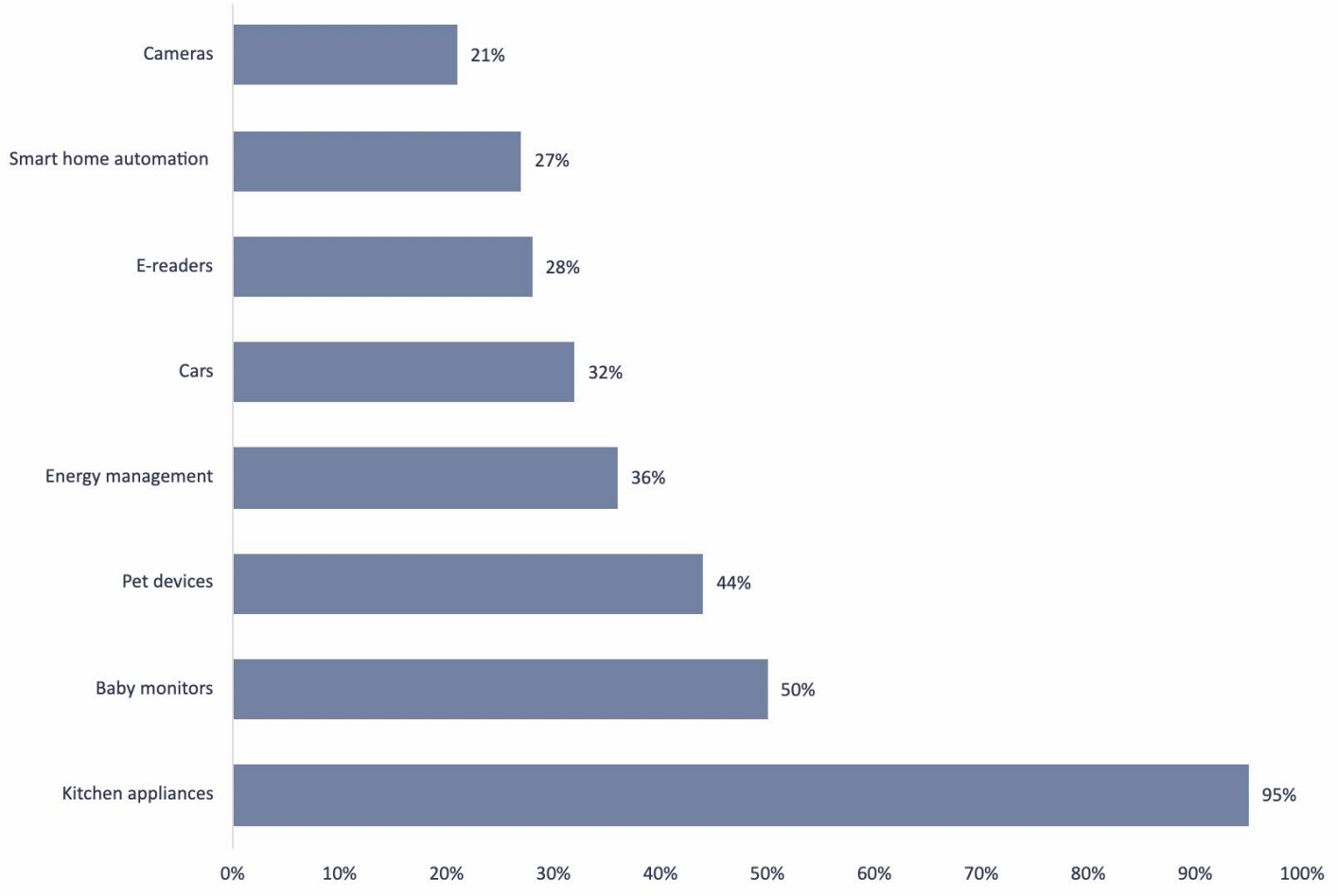
Setting the stage

Home device category growth. 2022/23 compared to 2021/22



Setting the stage

Home device category growth. 2022/23 compared to 2021/22



Story / Timeline

1. Buy the best and use it

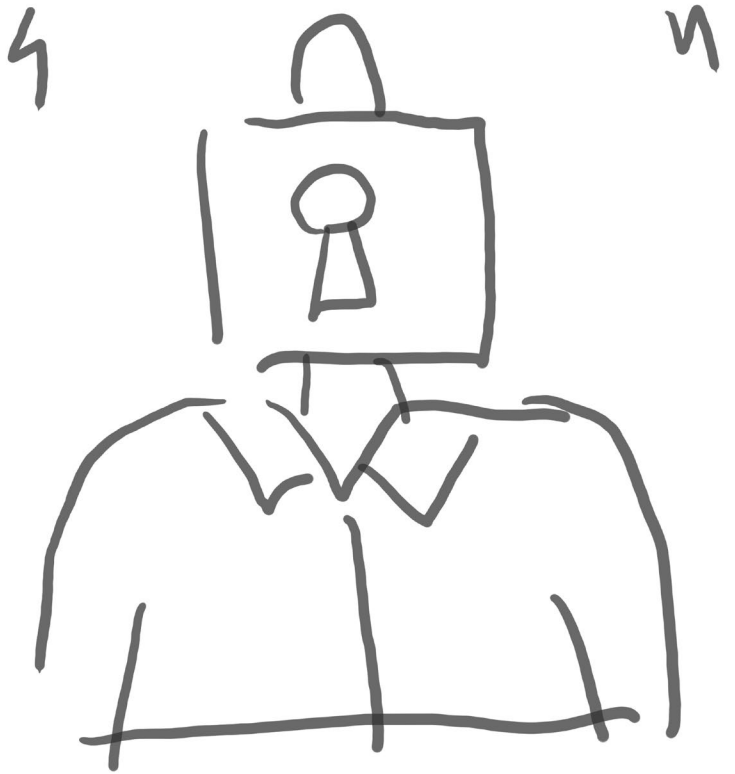
Story / Timeline

1. Buy the best and use it

2. Experiment with additional sources

Story / Timeline

1. Buy the best and use it
2. Experiment with additional sources
3. Introduce AI, more experiments

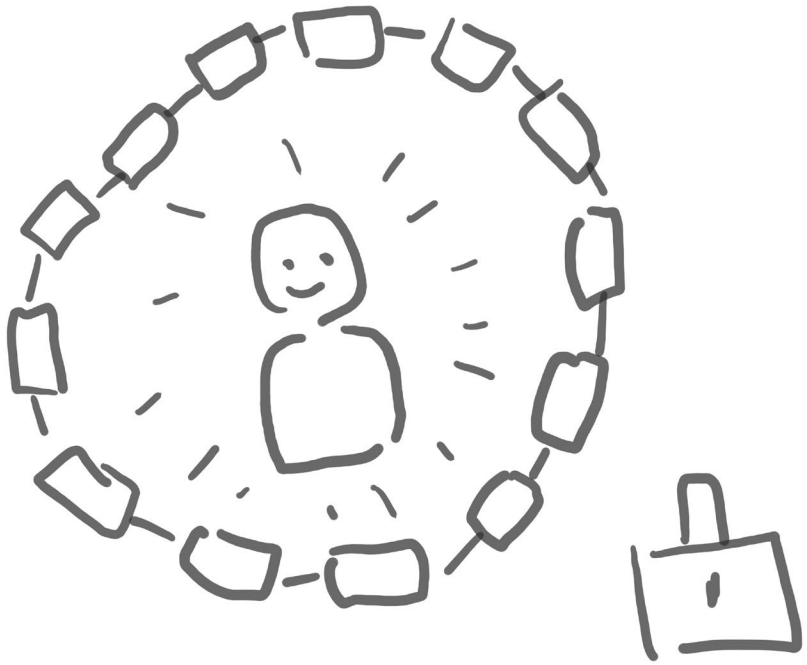


Story / Timeline

1. Buy the best and use it
2. Experiment with additional sources
3. Introduce AI, more experiments
4. We need much much more data…

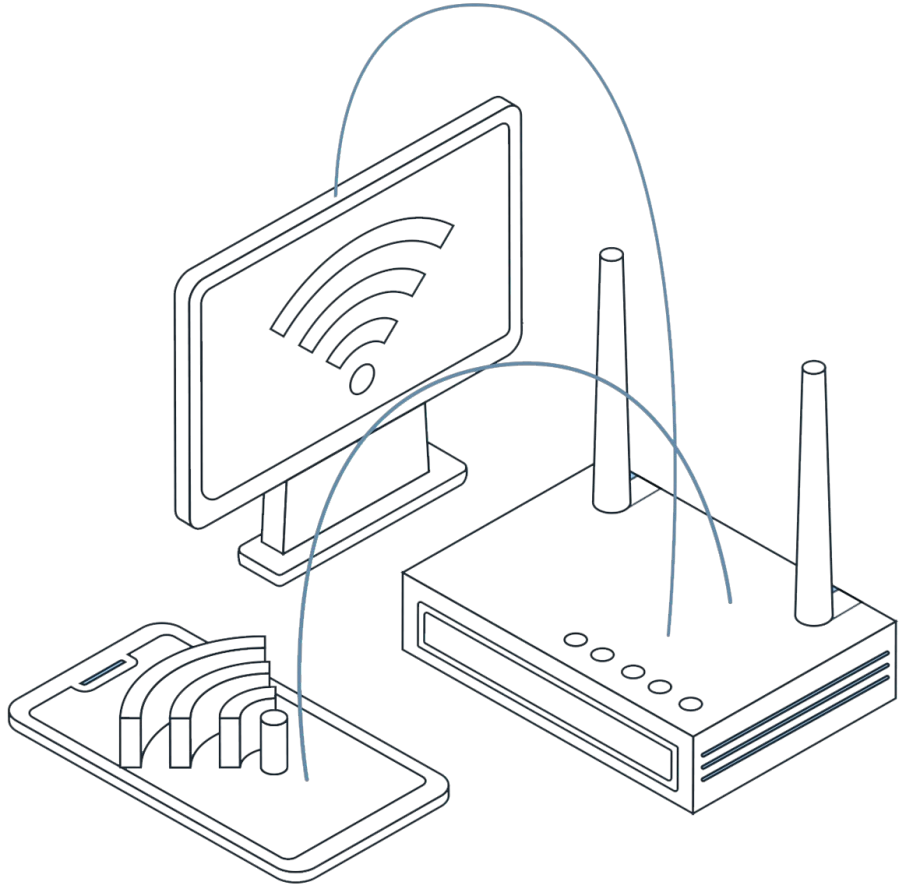
Story / Timeline

1. Buy the best and use it
2. Experiment with additional sources
3. Introduce AI, more experiments
4. We need much, much more data…
5. There is too much data / There is too little data



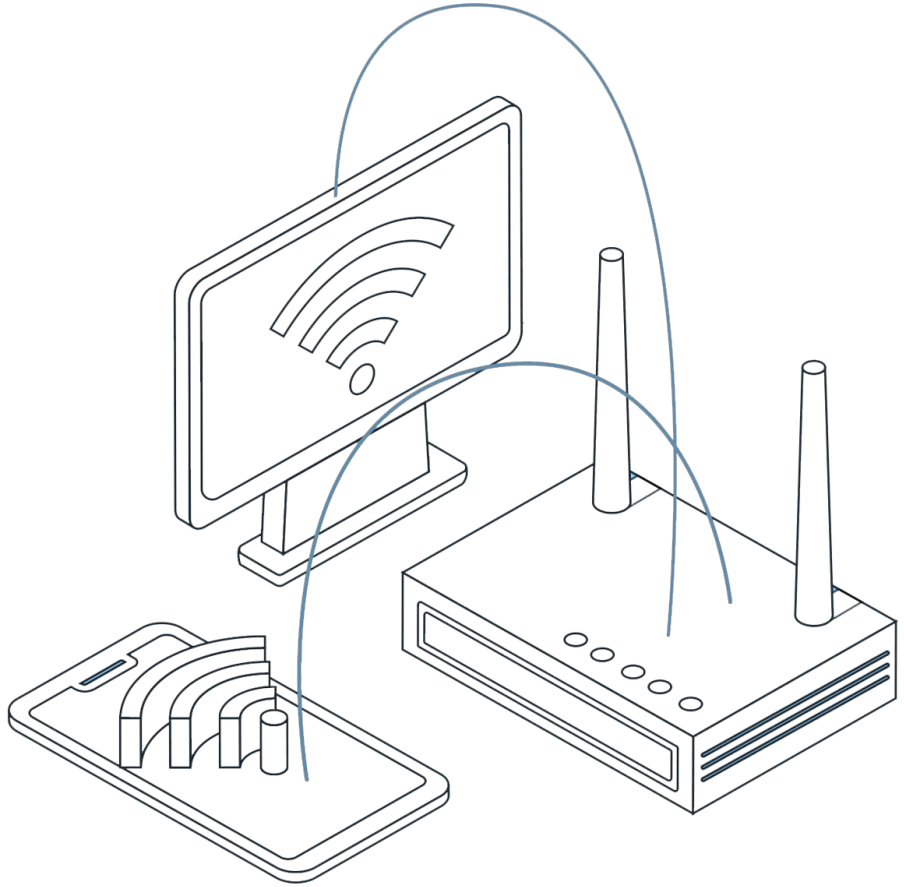
Paradox of working on a network level

- Large quantities of data.
- Not enough contextual data.

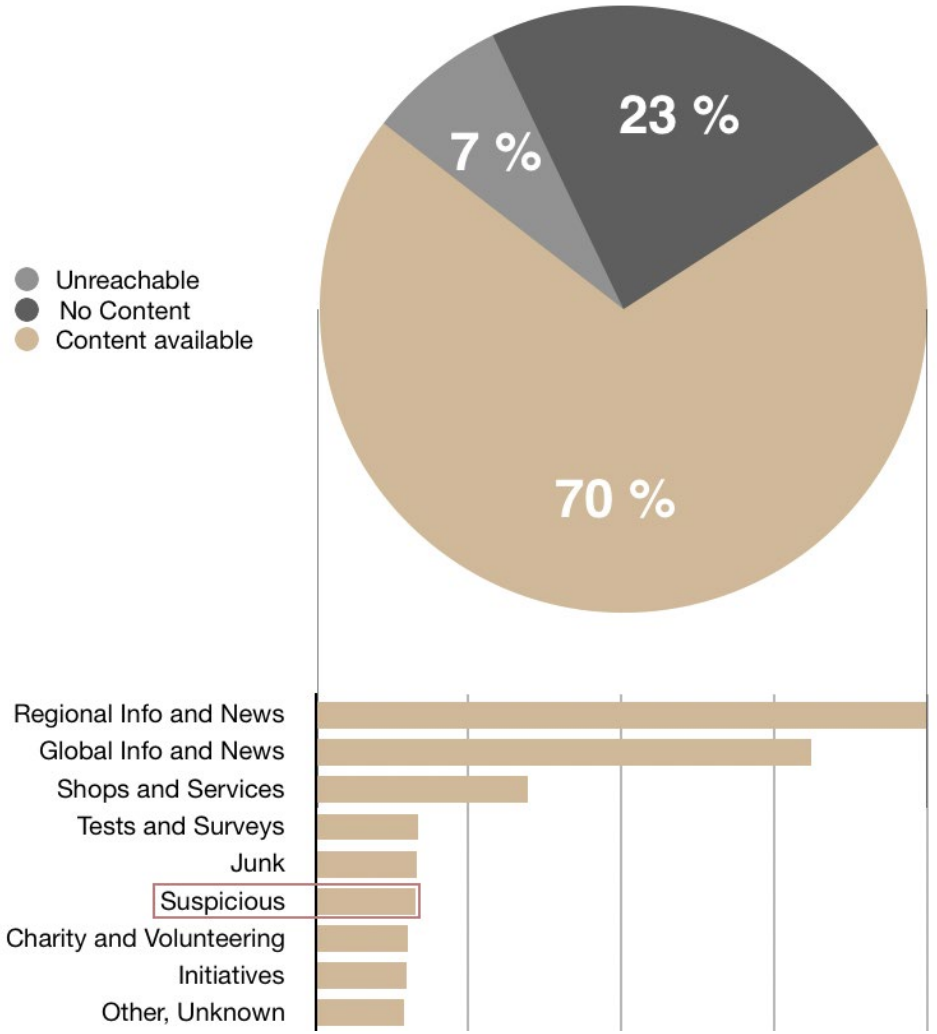


Paradox of working on a network level at homes

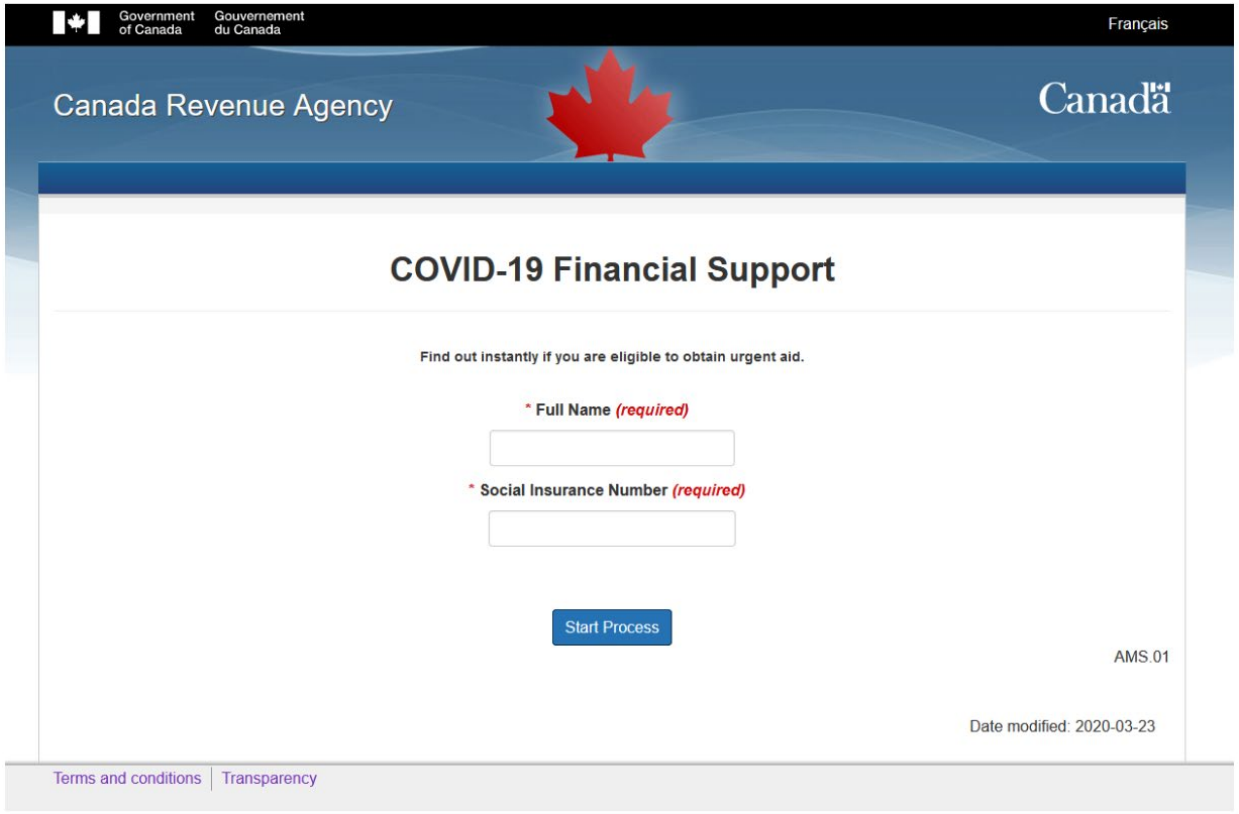
- Large quantities of data.
- Not enough contextual data.
- Protection cannot be too strict

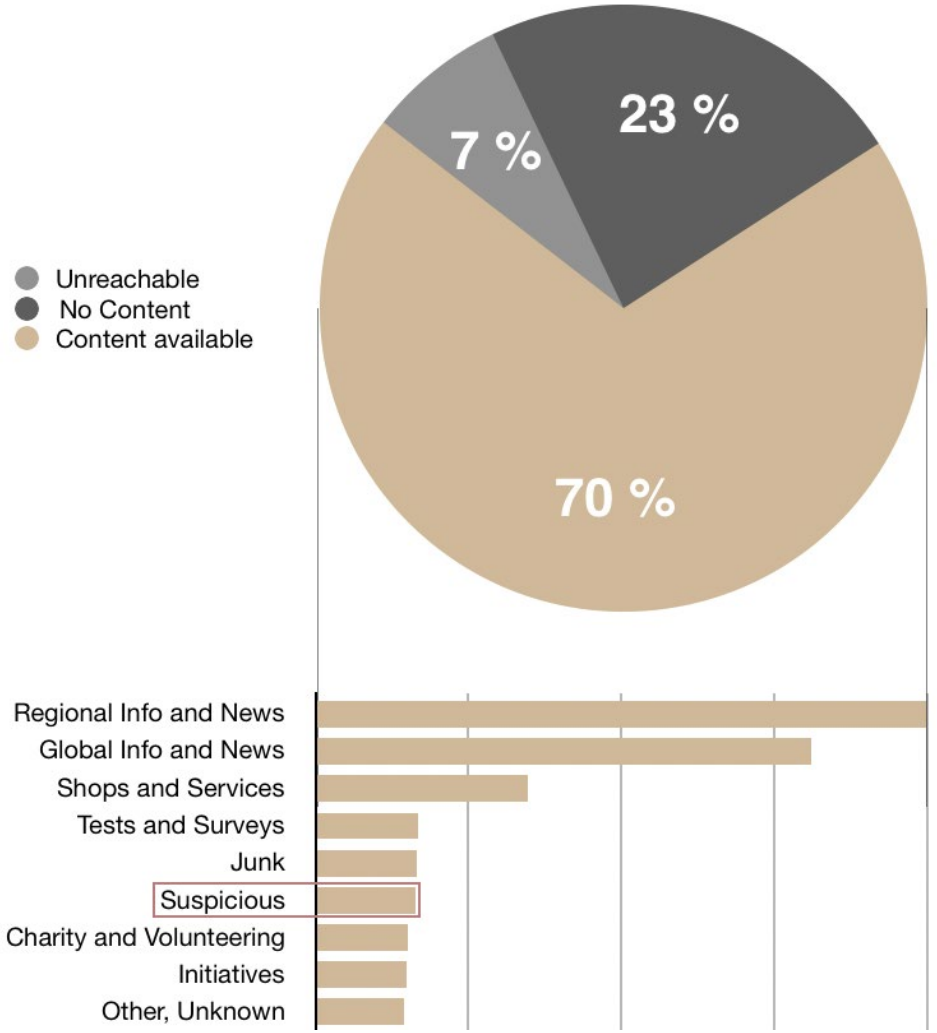


Case study


7 %
23 %
70 %
Unreachable
No Content
Content available
Regional Info and News
Global Info and News
Shops and Services
Tests and Surveys
Junk
Suspicious
Charity and Volunteering
Initiatives
Other, Unknown

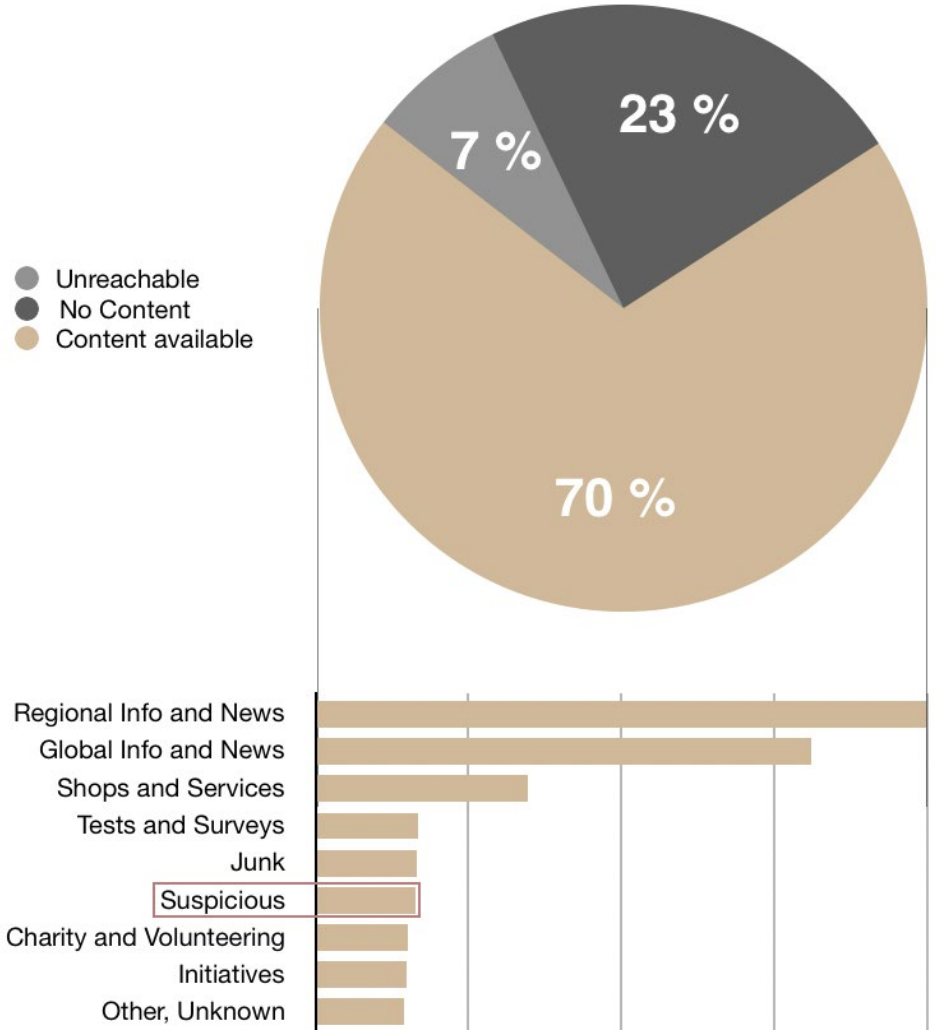
Case study


Government of Canada
Gouvernement du Canada
Français
Canada Revenue Agency
Canada
COVID-19 Financial Support
Find out instantly if you are eligible to obtain urgent aid.
* Full Name (required)
* Social Insurance Number (required)
Start Process
AMS.01
Date modified: 2020-03-23
Terms and conditions
Transparency


Unreachable
No Content
Content available
7 %
23 %
70 %
Regional Info and News
Global Info and News
Shops and Services
Tests and Surveys
Junk
Suspicious
Charity and Volunteering
Initiatives
Other, Unknown

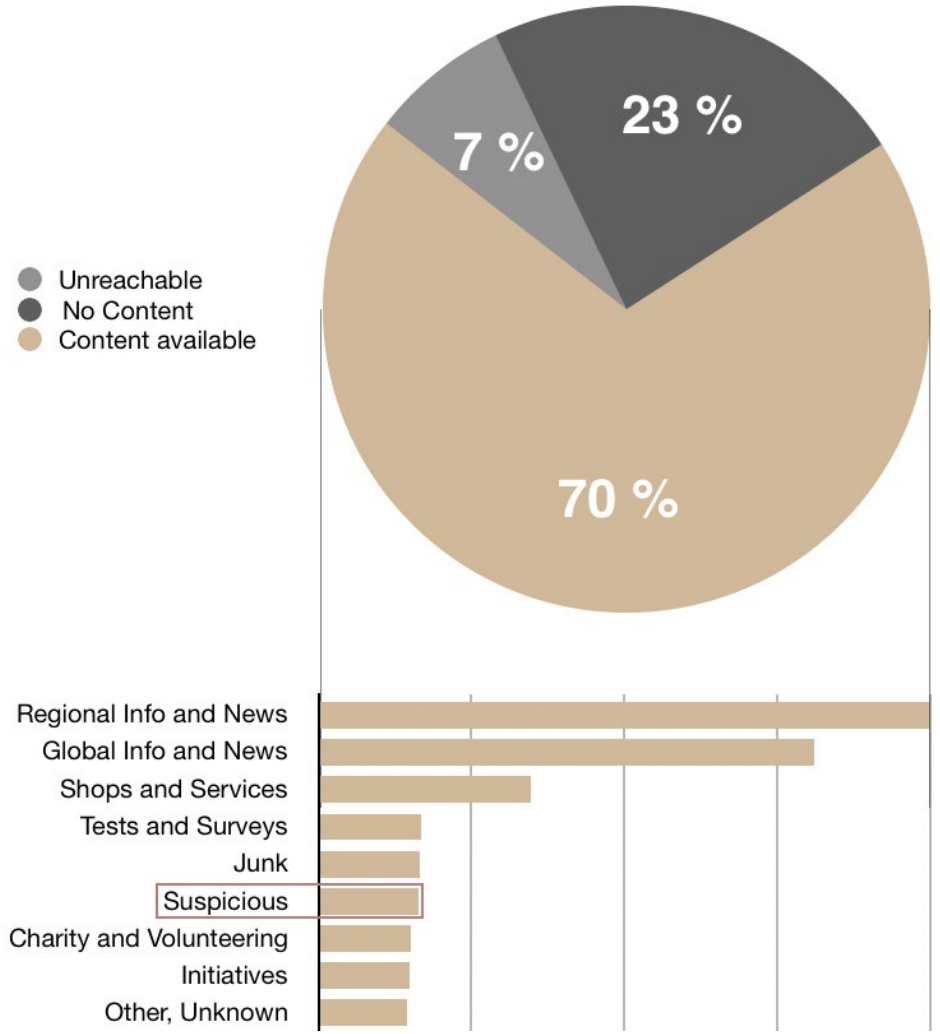
Case study


HOME
ABOUT
CORONA
SHOP
ARTICLES
DISCLOSURE
TESTIMONIALS
More
Music and Tones
to strengthen your Immune System
against the Coronavirus
Free Hour of Downloads
What is this all about?
Read the About Section!
Jill
Mattson
CORONA
VIRUS
FREQUENCY
DEFENSE
Based on The Original Work of
Sharry Edwards


Unreachable
No Content
Content available
7 %
23 %
70 %
Regional Info and News
Global Info and News
Shops and Services
Tests and Surveys
Junk
Suspicious
Charity and Volunteering
Initiatives
Other, Unknown

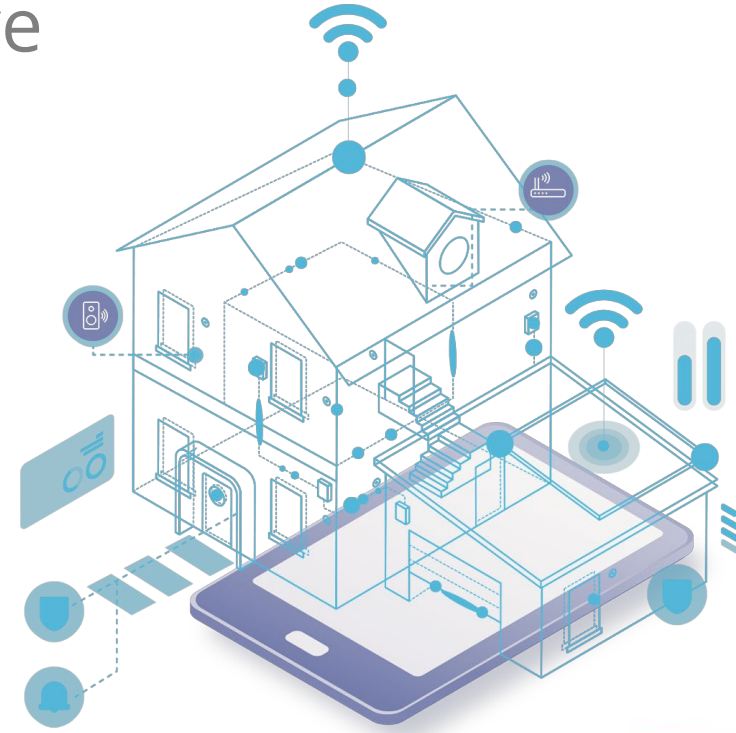
Case study

Quod liced Iovi, non licet bovi



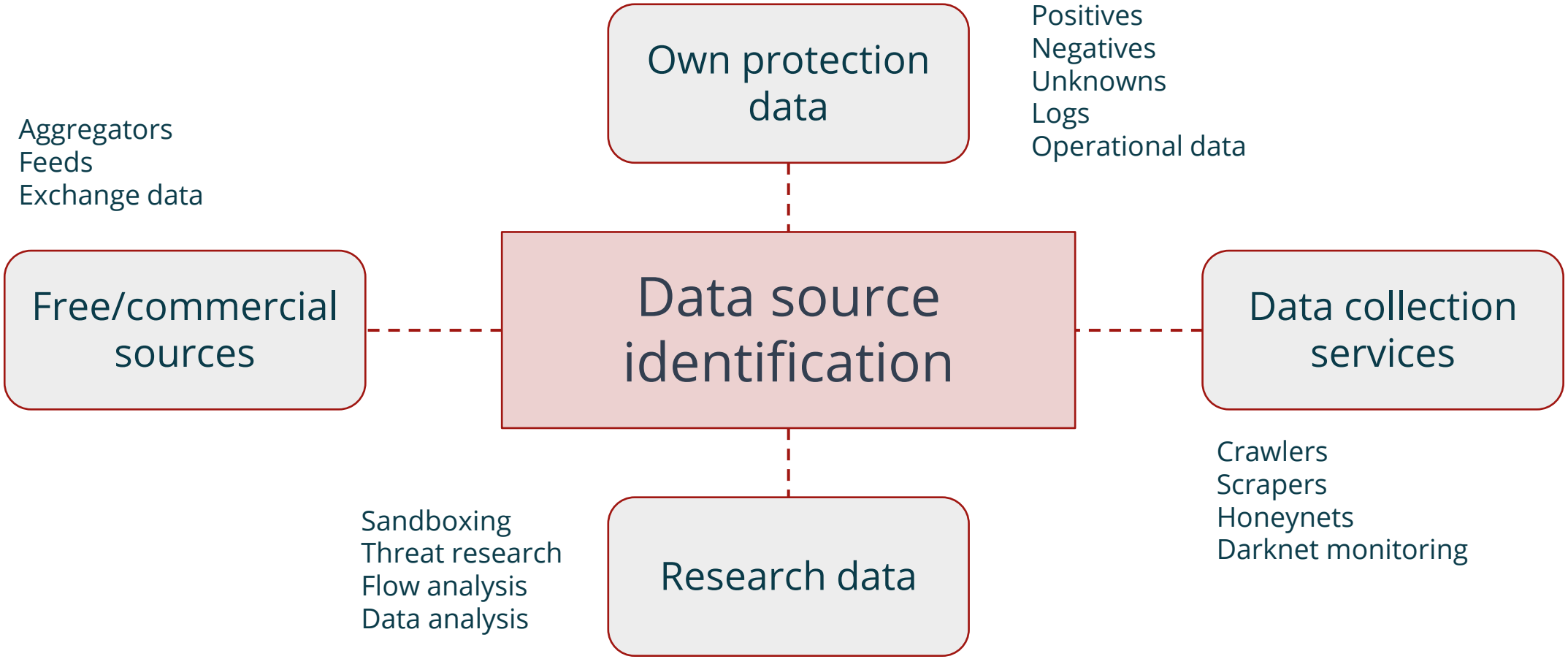
So, what are the challenges?

- Analysis of unbalanced dataset of everyday activity
- Even the fastest 3rd party engine is still reactive
- ML is not suitable to solve everything



One approach to solve these challenges

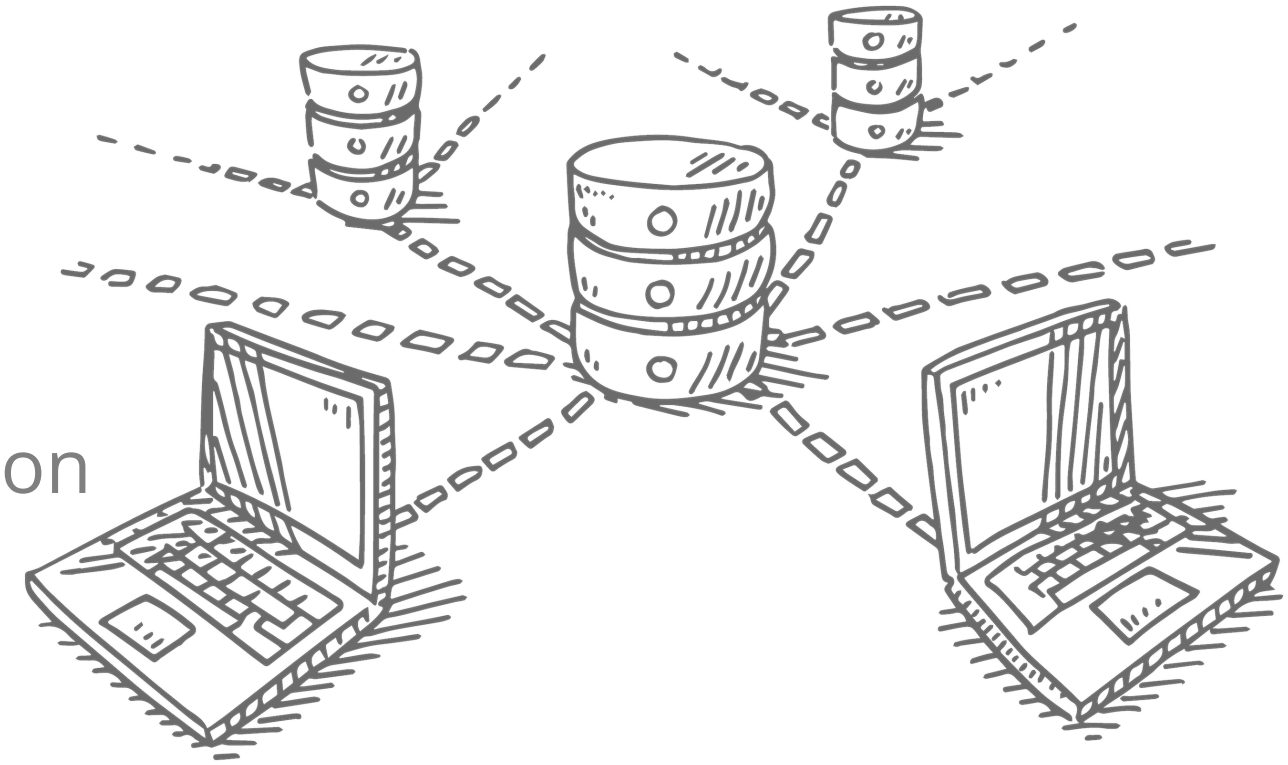
Data source identification



Data source identification

What are the data source *qualities* that our usecases need?

Before choosing between vendor A, B, C, ***extensive*** benchmark on ***your*** production data is a ***must!***



Quality gates

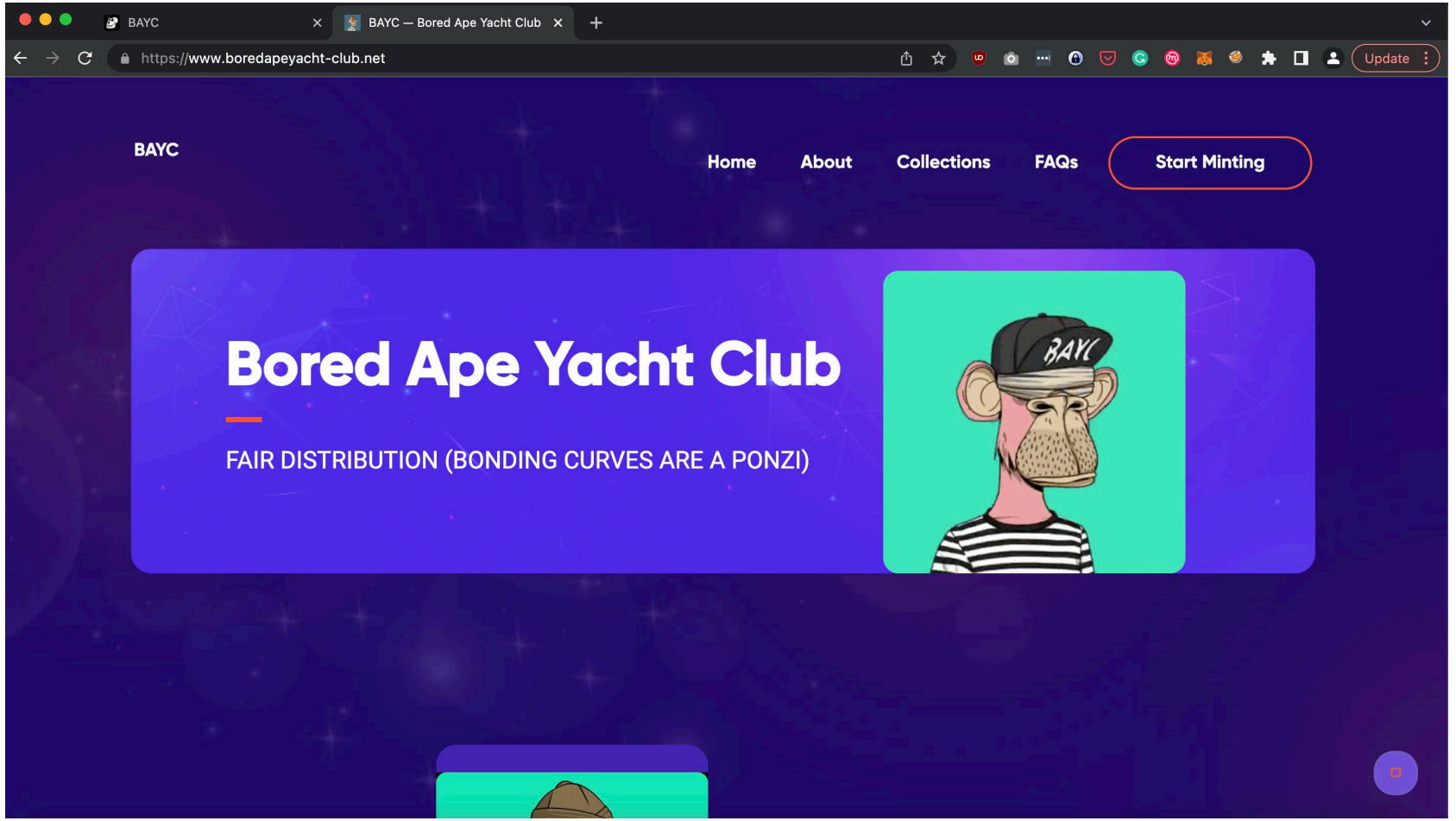
Quality gates

- Tolerance for false positives
- Tolerance for false negatives
- Tolerance for unknowns
- How quality gates affect other parts of threat intel flow

So where does ML/AI come in?

ML/AI is good when we can add context to data

Web3 scam case study



Two final notes

- Continuous threat intelligence improvements are mainly driven by:
  - Contextualized data challenges
  - Balancing inhouse/3rd party/other solutions

Thank you!

Q&A

leonardas.marozas@cujo.com