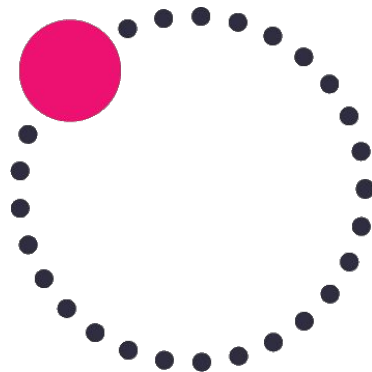


# On The Edge of Small Data

**Shannon Weyrick**

VP Research/Fellow • NSI

[sweyrick@nsi.com](mailto:sweyrick@nsi.com)



**NSI.**



# preface: the case for small data

**NS1.**

# NS1 Case Study

- Managed Authoritative DNS with 26 Global Anycasted POPs
- **>100 billion** DNS queries per average day
- **29 TB** of raw DNS wire packets per day



# The Data Conundrum

## What we think we want:

All The Data

...because we think we *may* use it  
all *someday*



## What we actually want:

Targeted Insights

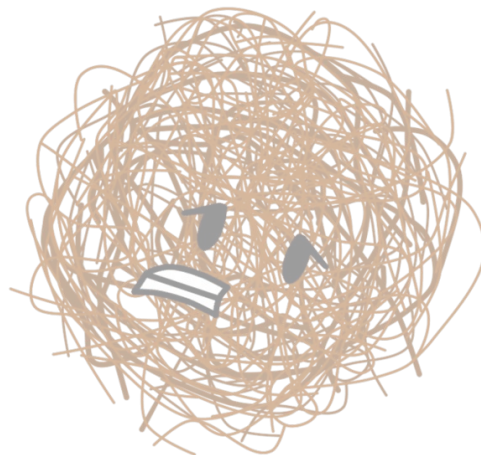
...to help us operate, debug, scale  
and protect our networks *today*



There is a price to pay for streaming raw  
data to a central solution

# The Costs of Raw Data

- Complicated data pipelines for centralized collection
- Batch processing costs to make it actionable
- Inability to make sense of or take advantage of all the data
- Slow dashboards, short retention times
- Slow reaction times to critical events
- Ingestion costs (esp. SaaS)



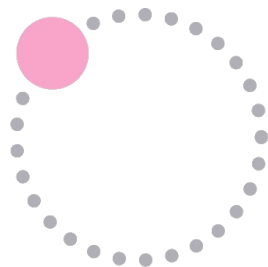
# Paradigm Shift: Small Data

- Push the conversion of raw → actionable to the edge
  - Distribute as close to the source as possible
- React quicker
  - Make those insights available at the edge *and* centrally
- Collect, process and store less
- Don't find the needles in the haystack: just collect the needles
- Dynamically decide what your team needs at any time



# Shannon Weyrick

Orb Founder, VP Research @ NSI



- 26 years in industry, 8 years at NSI
- NSI engineering leadership
- Since start of 2021 focused on Orb open source innovation @ NSI Labs
- [sweyrick@nsi.com](mailto:sweyrick@nsi.com)




If you remember  
just one thing  
from this talk...

**NS1.**





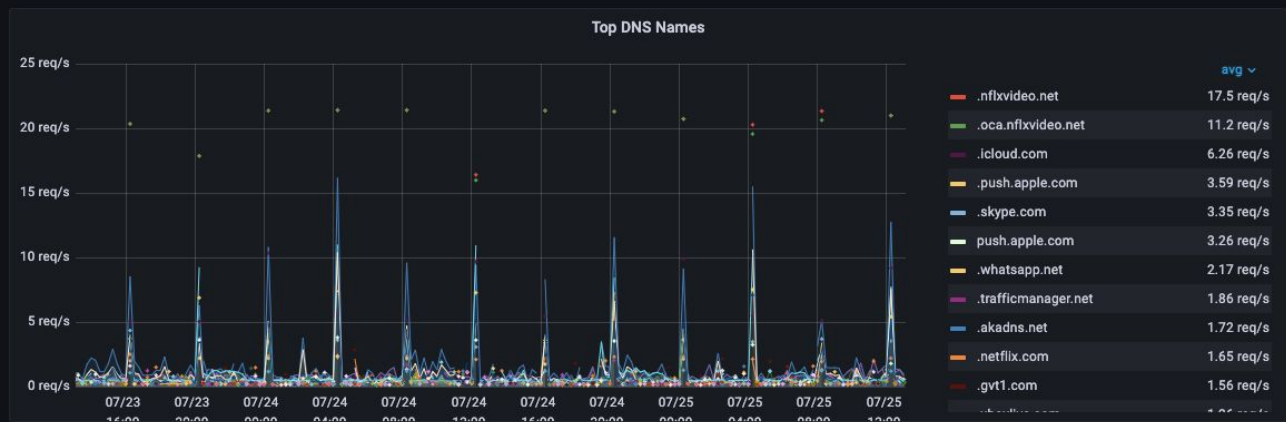
# Orb is Open Source Edge Observability

- **Observability tool** designed for **distributed edge networks**
  - Uses **small data** paradigm with **dynamic policy orchestration**
  - Real-time **insights** into **data flow** on the **distributed edge**
  - Integrates with **modern observability stacks**
  - **Free** and **open source**, backed by NS1
- 
- A decorative graphic consisting of a circle of light gray dots. One dot at the top is highlighted with a larger, semi-transparent pink circle.

~ DNS Overview (Now)



~ DNS Name Overview



**Top NXDOMAIN**

Metric	Value (sum)
iad07.nsonce.co	32
6b7b001b-ec4a-fbd...	13
epc.geo.mnc260.m...	11
lb_dns-sd_udp.mo...	11
lb_dns-sd_udp.0.1...	5
apple-cloudkit.fe.ap...	5
local	4
lb_dns-sd_udp.0.0...	2

**Top SRVFAIL**

Metric	Value (sum)
api.fitbit.com	
epdg.epc.mnc240....	

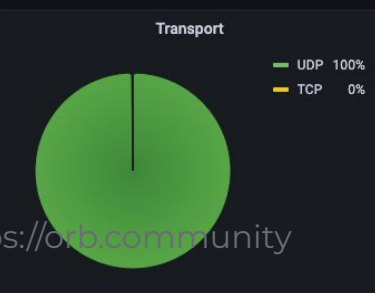
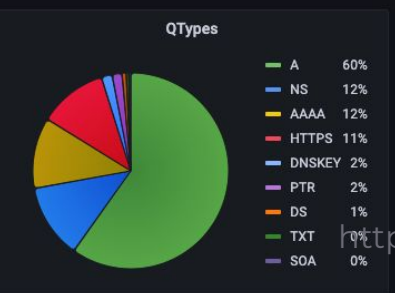
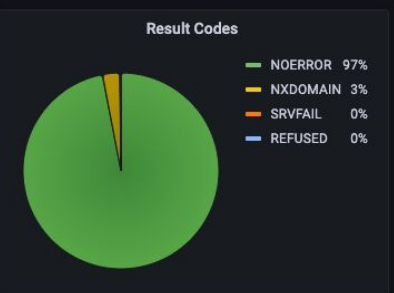
~ DNS QName Tables

**Names Agg3**

Metric	Value (sum)
.logs.roku.com	4.88
.com.akadns.net	3.35
.elb.amazonaws.com	2.09
com.akadns.net	1.94
.fe.apple-dns.net	1.82
.clients6.google.com	1.72

**Top REFUSED**

Metric	Value (sum)
unity.rokuapi.net	



~ DNS Overview (Now)



~ DNS Name Overview

Top DNS Names

### Network (L2-L3)

- Top IPs
- Top Geo/ASN
- IP Cardinality
- Rate Percil.
- Payload Perc.
- Throughput
- Protocol
- ...

### DNS

- Top QNames
- Geo by ECS
- Transactions
- Protocol
- Rate Percil.
- QName Card.
- Timer Percil.
- Amplification
- ...

### Flow

- Top flows
- Flow rates
- Protocols
- Ports
- Interfaces
- Throughputs
- ...

Top SRVFAIL

Metric	Value (sum)
api.fitbit.com	32
epdg.epc.mnc240...	13
...	11
...	11
...	5
...	5
...	4
...	2

~ DNS QName Tables

Names Agg3

Metric	Value (sum)
.logs.roku.com	4.88
.com.akadns.net	3.45
.elb.amazonaws.com	2.09
com.akadns.net	1.94
.fe.apple-dns.net	1.82
.clients6.google.com	1.72

Top REFUSED

Metric	Value (sum)
unity.rokuapi.net	4.88

Result Codes

- NOERROR 97%
- NXDOMAIN 3%
- SRVFAIL 0%
- REFUSED 0%

QTypes

- A 60%
- NS 12%
- AAAA 12%
- HTTPS 11%
- DNSKEY 2%
- PTR 2%
- DS 1%
- TXT 0%
- SOA 0%

Transport

- UDP 100%
- TCP 0%



# control tower for the edge

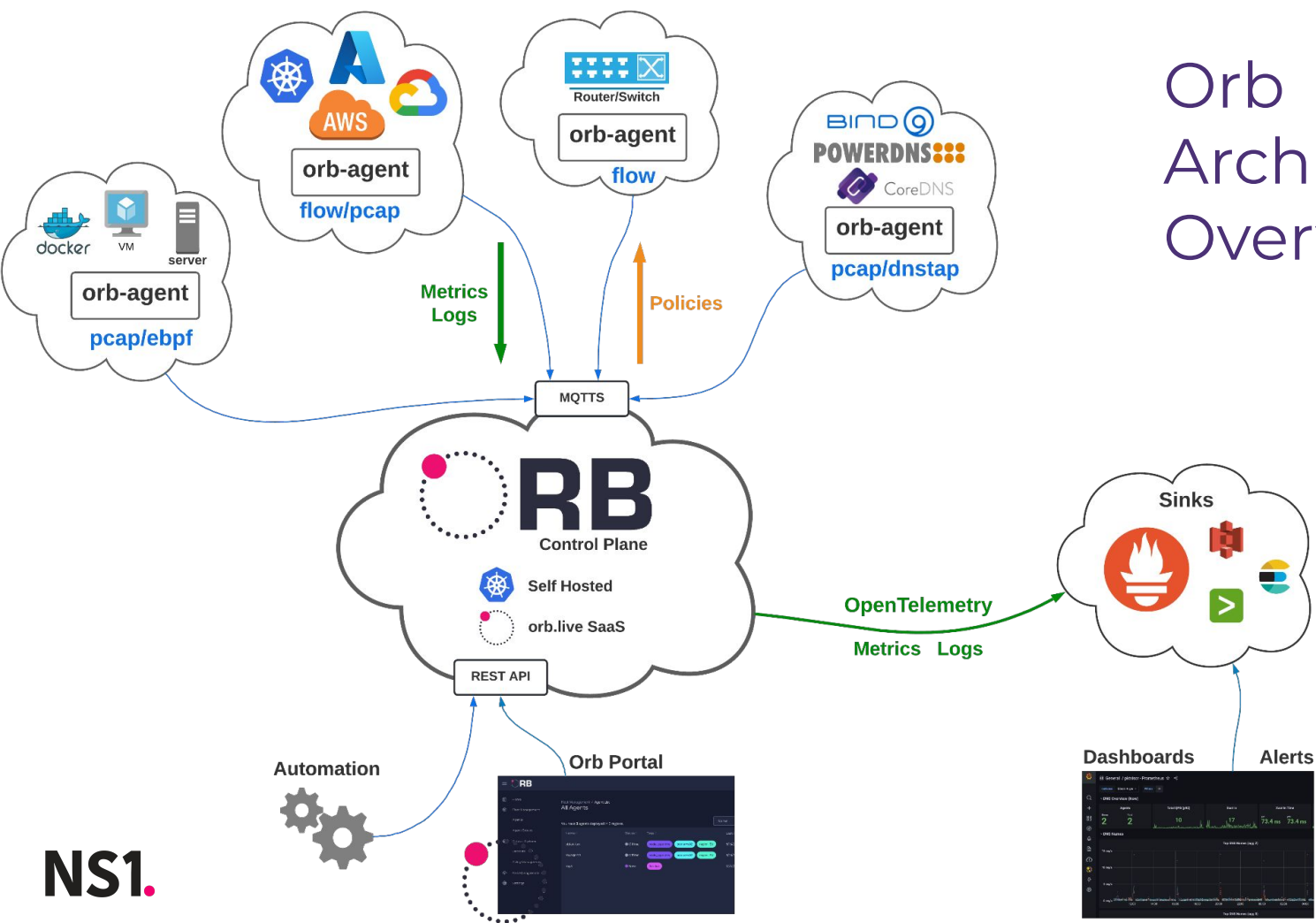
Orb control plane: cloud native application

**NS1.**

# Control Tower for Dynamic Edge Observability

- **Usability & Automation:** Portal UI & REST API
- **Fleet management:** connect, organize, and manage edge agents
- **Policy management:** recipes for analyzing data streams, deciding which agents should receive which policies in real time
- **Data collection & Sinking:** scrape lightweight metric output from all policies across all agents and push to the proper databases and dashboards

# Orb Architecture Overview



# Fleet Management

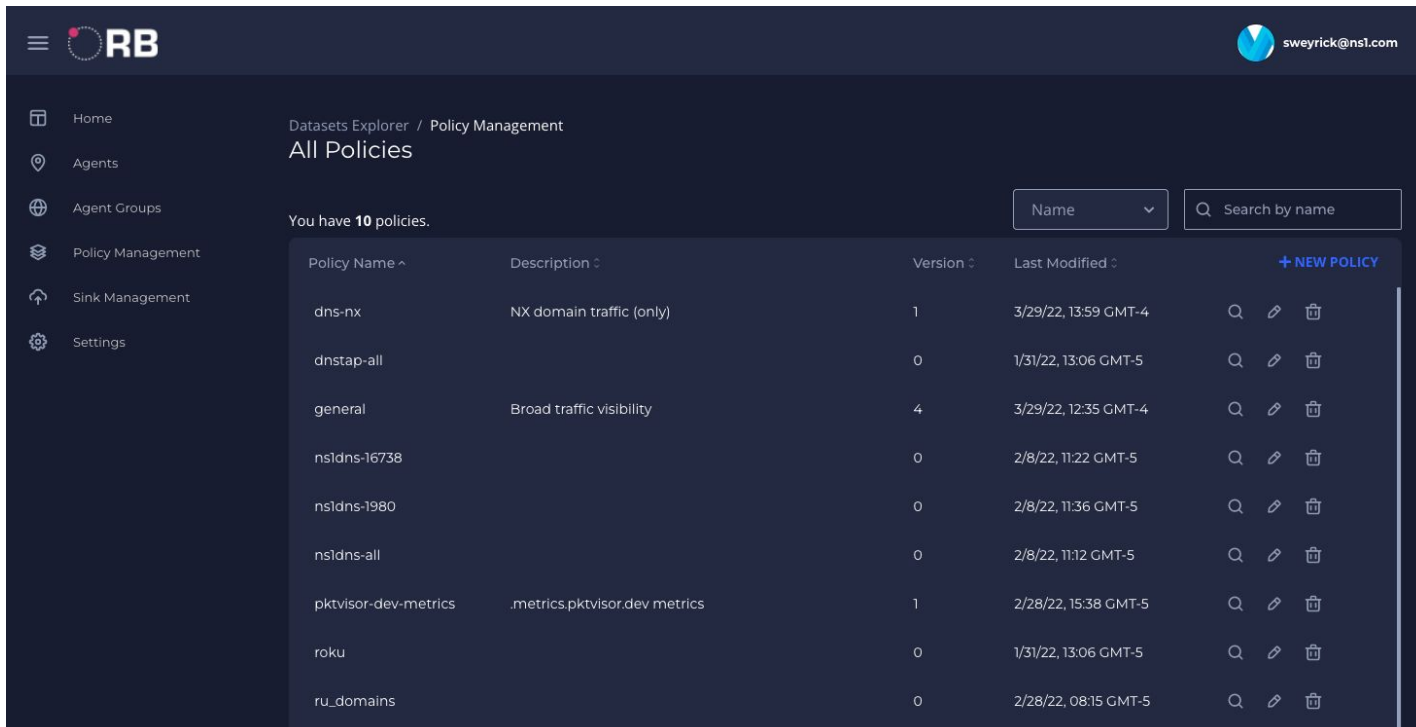
Connect, organize, and manage edge agents

The screenshot displays the RB Fleet Management interface. The top navigation bar includes the RB logo, a user profile for 'sweyrick@ns1.com', and a sidebar menu with options: Home, Agents, Agent Groups, Policy Management, Sink Management, and Settings. The main content area is titled 'Fleet Management / Agents List' and 'All Agents'. It shows a summary 'You have 4 agents deployed.' and a search bar. Below is a table of agents with columns for Name, Status, Tags, and Last Activity. A '+ NEW AGENT' button is located in the top right of the table area.

Name	Status	Tags	Last Activity	
blesk	Online	dnstap: true, location: home, node_type: dns	5/3/22, 16:51 GMT-4	Q, ✎, 🗑️
dns01-ams99-n0091	Online	network: 91, node_type: dns, pop: ams99	5/3/22, 16:52 GMT-4	Q, ✎, 🗑️
dns01-lga99-n0091	Online	network: 91, node_type: dns, pop: lga99	5/3/22, 16:51 GMT-4	Q, ✎, 🗑️
dns01-sin99-n0091	Online	network: 91, node_type: dns, pop: sin99	5/3/22, 16:52 GMT-4	Q, ✎, 🗑️

# Policy Management

Recipes for analyzing data streams



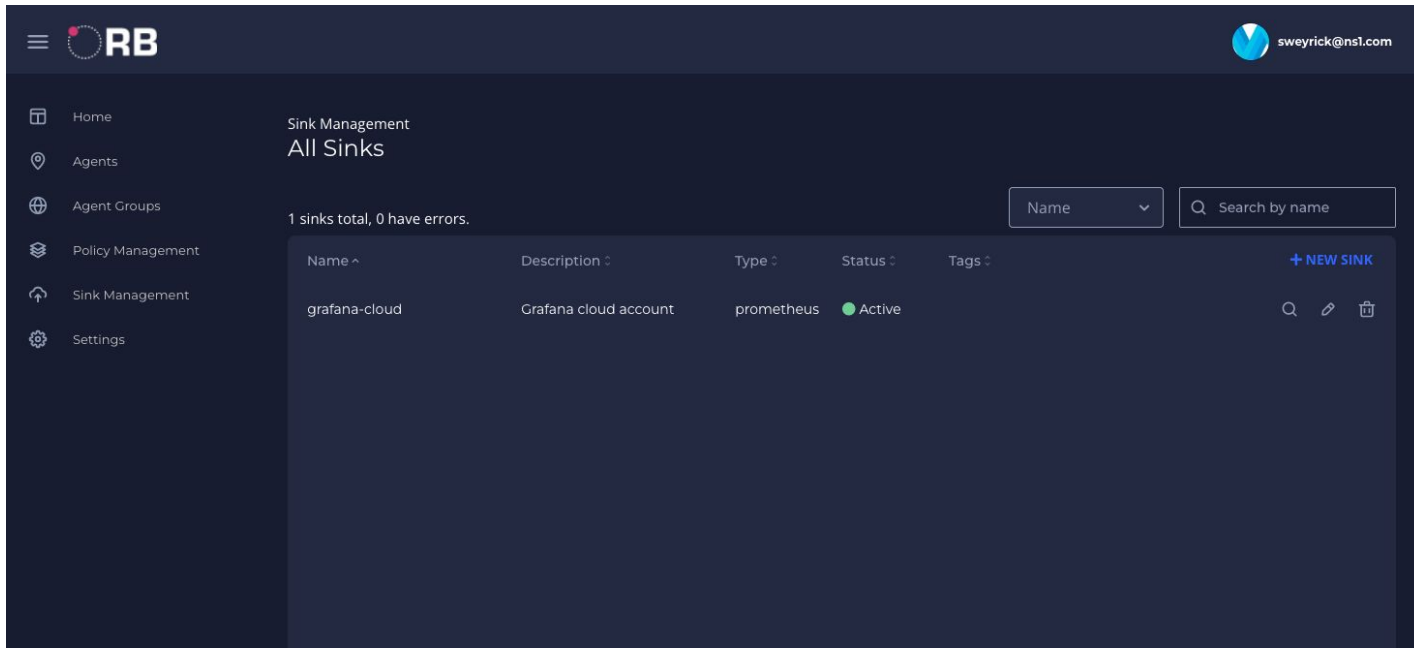
The screenshot displays the NS1 Policy Management interface. The top navigation bar includes the NS1 logo and the user email 'sweyrick@ns1.com'. The left sidebar contains navigation links for Home, Agents, Agent Groups, Policy Management, Sink Management, and Settings. The main content area is titled 'All Policies' and shows a list of 10 policies. A search bar and a dropdown menu for 'Name' are located at the top right of the table. A '+ NEW POLICY' button is visible in the top right corner of the table area.

Policy Name	Description	Version	Last Modified	
dns-nx	NX domain traffic (only)	1	3/29/22, 13:59 GMT-4	🔍 ✎ 🗑️
dnstap-all		0	1/31/22, 13:06 GMT-5	🔍 ✎ 🗑️
general	Broad traffic visibility	4	3/29/22, 12:35 GMT-4	🔍 ✎ 🗑️
ns1dns-16738		0	2/8/22, 11:22 GMT-5	🔍 ✎ 🗑️
ns1dns-1980		0	2/8/22, 11:36 GMT-5	🔍 ✎ 🗑️
ns1dns-all		0	2/8/22, 11:12 GMT-5	🔍 ✎ 🗑️
pktvisor-dev-metrics	.metrics.pktvisor.dev metrics	1	2/28/22, 15:38 GMT-5	🔍 ✎ 🗑️
roku		0	1/31/22, 13:06 GMT-5	🔍 ✎ 🗑️
ru_domains		0	2/28/22, 08:15 GMT-5	🔍 ✎ 🗑️



# Sink Management

Which databases and dashboards to send metrics to



The screenshot displays the NS1 Sink Management interface. The top navigation bar includes the NS1 logo and the user email 'sweyrick@ns1.com'. A sidebar on the left lists navigation options: Home, Agents, Agent Groups, Policy Management, Sink Management, and Settings. The main content area is titled 'Sink Management' and 'All Sinks'. It shows a summary: '1 sinks total, 0 have errors.' Below this is a table with columns for Name, Description, Type, Status, and Tags. A single sink is listed: 'grafana-cloud' with description 'Grafana cloud account', type 'prometheus', and status 'Active'. A '+ NEW SINK' button is visible in the top right of the table area.

Name	Description	Type	Status	Tags
grafana-cloud	Grafana cloud account	prometheus	Active	

# Configuration Management

Which agents should run which policies, update in real time

The screenshot displays the ORB Configuration Management interface. The top navigation bar includes the ORB logo, a user profile for 'admin@example.com', and a 'Duplicate Policy' button. The left sidebar contains navigation links: Home, Agents, Agent Groups, Policy Management (selected), Sink Management, and Dev. The main content area is titled 'Policy View' and is divided into several sections:

- Agent Policy Details:** Shows the 'Policy Name' as 'policy' and an 'EDIT' button.
- Active Datasets (1):** A table with columns for Name, Agent Group, Valid, and Sinks. It contains one entry: 'dataset' for 'group', which is 'Valid' (indicated by a green dot) and has a 'sink'.
- Assigned Groups:** Shows 'group (1 / 1)'.
- Agent Policy Configuration:** A code editor showing the configuration for the policy:

```
1 handlers:
2   modules:
3     default_dns:
4       type: dns
5     default_net:
6       type: net
7     default_dns_2:
8       type: net
9   input:
10    input_type: pcap
11    tap: default pcap
```

# Data Collection & Sinking

Scrape lightweight metric output from all policies across all agents and push to the proper databases and dashboards





# edge agent for streaming analysis

orb-agent

**NS1.**

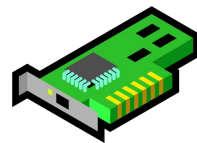
# What Is The Orb Edge Agent?

- **Taps into** multiple, concurrent data streams at the edge
- Uses **fast streaming algorithms** to **analyze deeply** in real time
- **Efficiently summarizes** important insights, generate metrics
- Can be **reprogrammed in real time** with dynamic policies
- Can **scale up** and **scale down**



# What Can It Tap Into?

- Packet capture (with BPF filters)
- dnstap (socket, TCP)
- Network flow (sFlow, Netflow/IPFIX)
- future: envoy taps, eBPF, WebAssembly...
- Expandable via custom loadable modules



sFlow



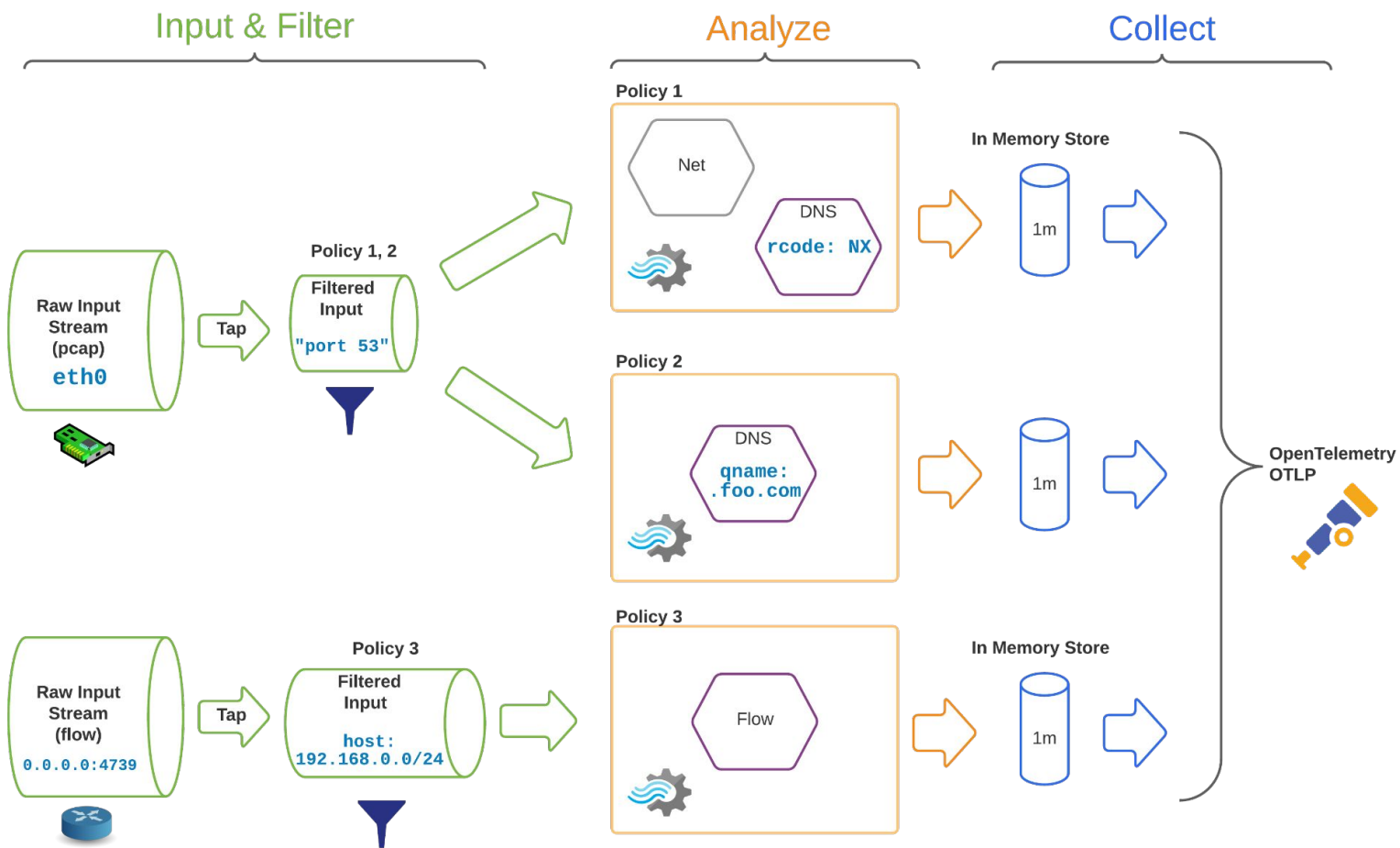
# What Can It Generate Metrics For?

- L2-L3 Network
- DNS
- DHCP
- Flows
- Policy resource usage
- Expandable via custom loadable modules



# Orb Edge Agent

Embedded  
Stream  
Processing  
powered by pktvisor

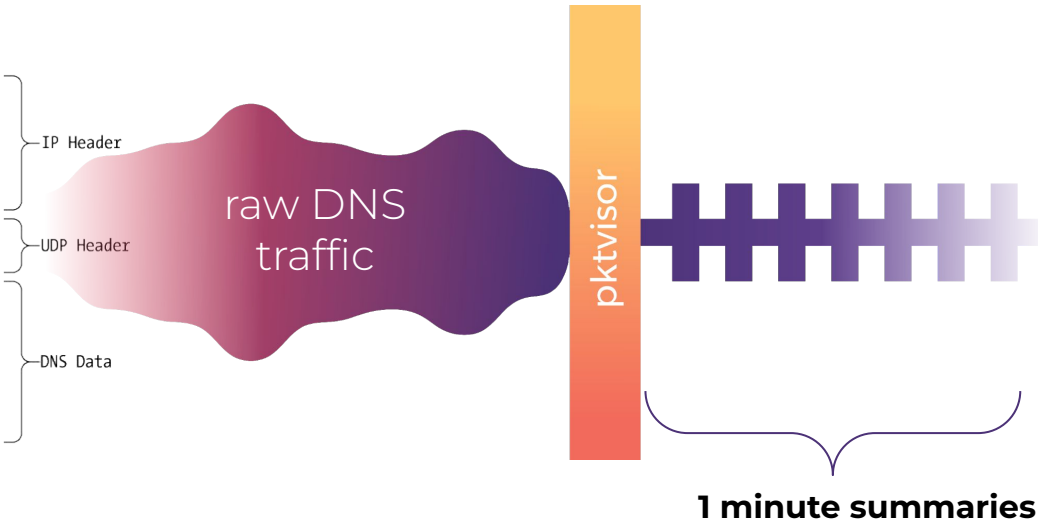




# Use Case: DNS Analysis

← 32 bits →				
ver	hlen	TOS	pkt len	
identification		flg	fragment offset	
TTL	protocol	header cksum		
Source IP address				
Destination IP address				
Source port		Destination port		
UDP length		UDP cksum		
Query ID	opcode	AA	TC	RA
Question count	Answer count			
Authority count	Addl. Record count			
DNS question or answer data				

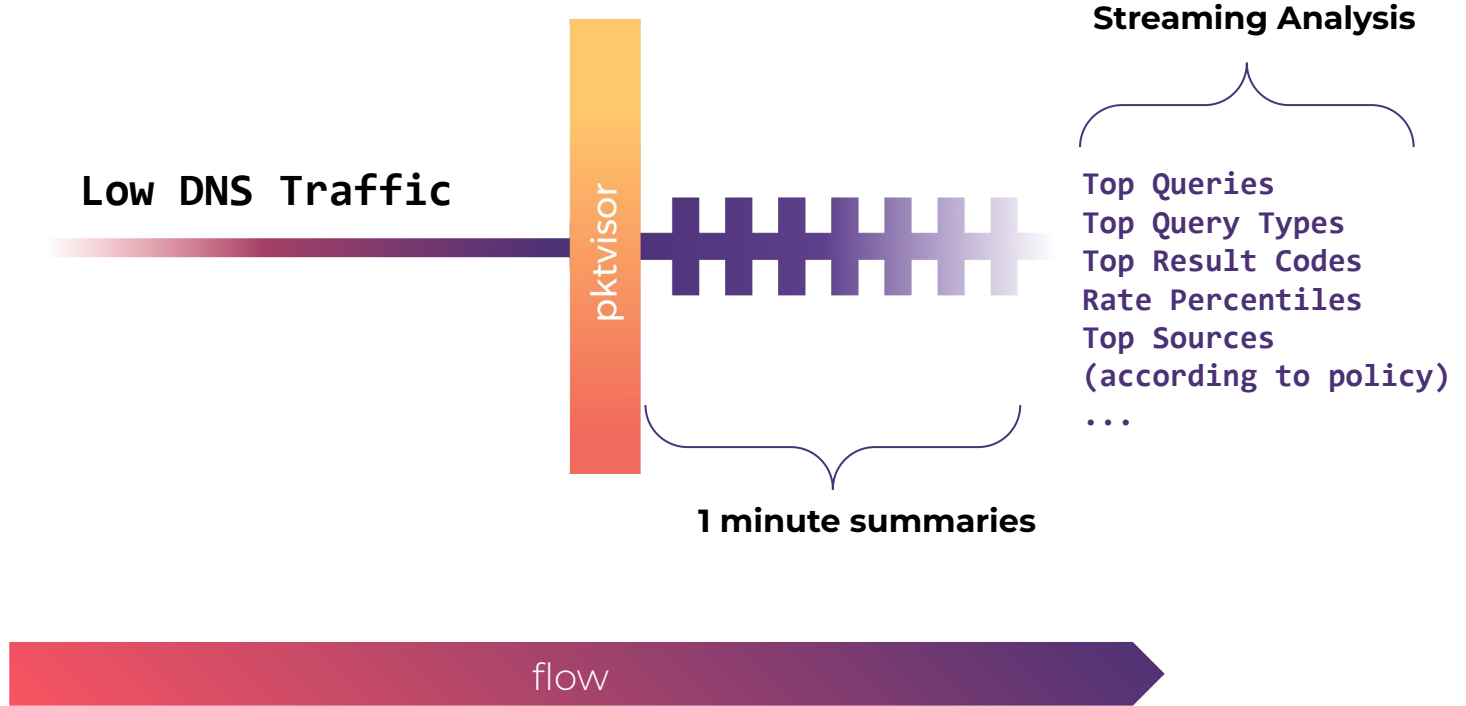
*DNS packet on the wire*



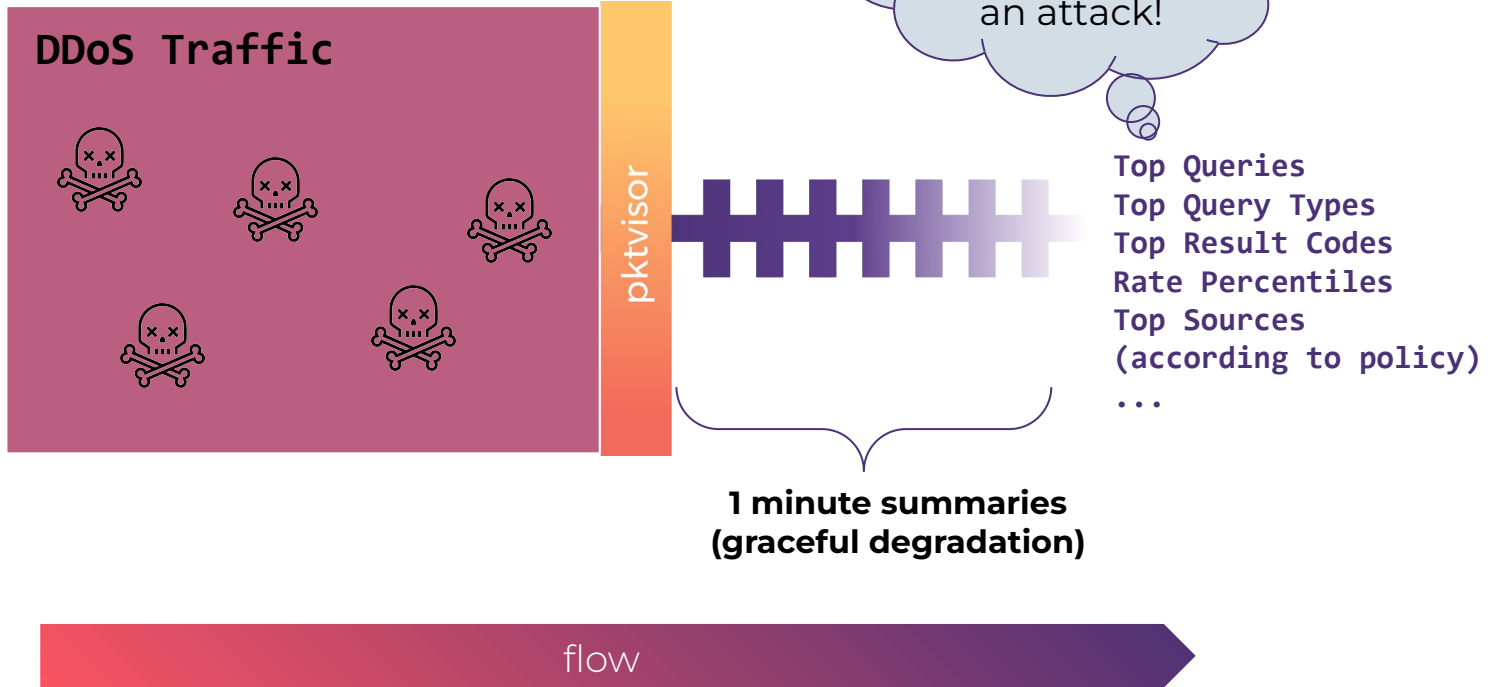
## Streaming Analysis

- Top Queries
- Top Query Types
- Top Result Codes
- Rate Percentiles
- Top Sources (according to policy)
- ...

# Use Case: DNS Analysis



# Use Case: DNS Analysis





# project status

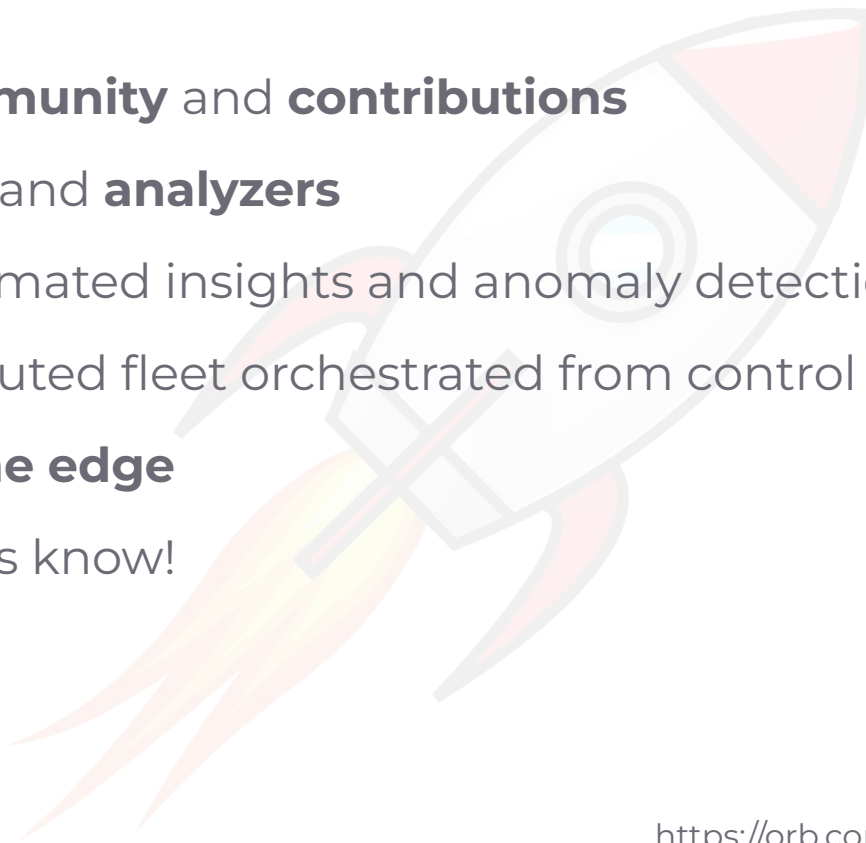
**NS1.**

# Open Source, Backed by NS1

- Core tech has **powered NS1 operational** visibility for years
- Powers NS1 **DNS Insights** product for NS1 customers today
- All development done on **GitHub**
- Now working with **design partners** to develop the project towards various edge network, IT, and NetDevOps use cases
- **Join us!**

# Exciting Future

- Expanding our active **community** and **contributions**
- New input stream sources and **analyzers**
- **Machine learning** for automated insights and anomaly detection
- **pcap samples** from distributed fleet orchestrated from control plane
- Policy driven **actions on the edge**
- What are your ideas? Let us know!

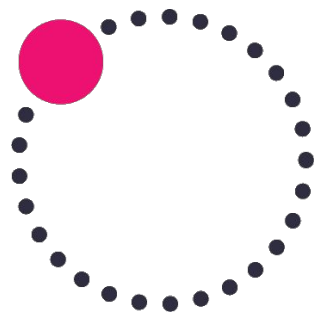




conclusion

**NS1.**

# Remember This



- **Observability tool** designed for **distributed edge networks**
- Uses **small data** paradigm with **dynamic policy orchestration**
- Real-time **insights** into **data flow** on the **distributed edge**
- Integrates with **modern observability stacks**
- **Free** and **open source**, backed by NS1
- You can **POC in 10 minutes** on orb.live



# Do This

- Join the community: <https://orb.community>
- Try Orb SaaS for free: <https://orb.live>
- Star the project: [github.com/ns1labs/orb](https://github.com/ns1labs/orb)
- Contact us! We're seeking development partners like you.



thank you

**NS1.**