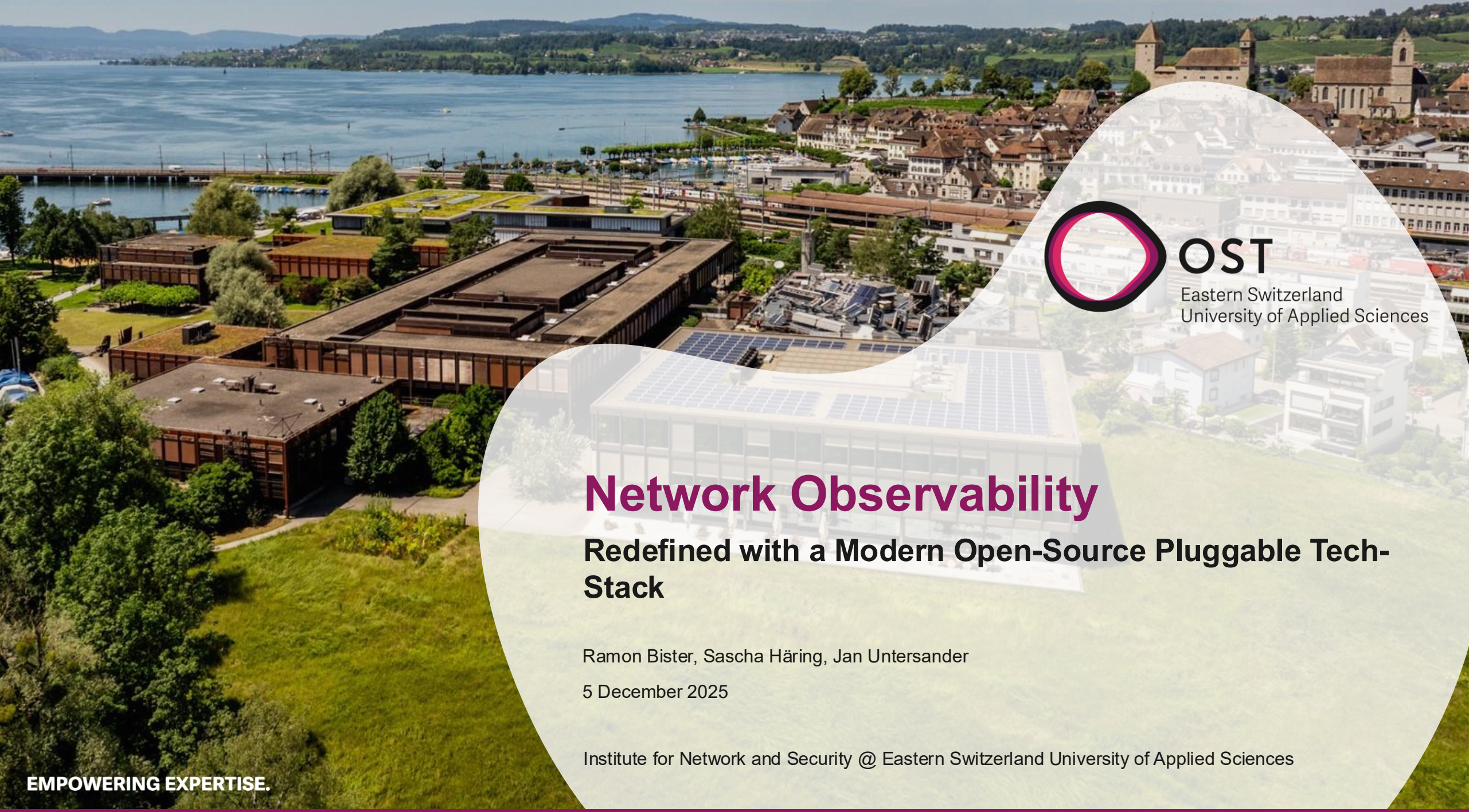


OST
Eastern Switzerland
University of Applied Sciences

Network Observability

Redefined with a Modern Open-Source Pluggable Tech-Stack

Ramon Bister, Sascha Häring, Jan Untersander

5 December 2025

Institute for Network and Security @ Eastern Switzerland University of Applied Sciences

EMPOWERING EXPERTISE.

Don’t e Wheel, Unless Learning Mo eels

Source: blog.codinghorror.com

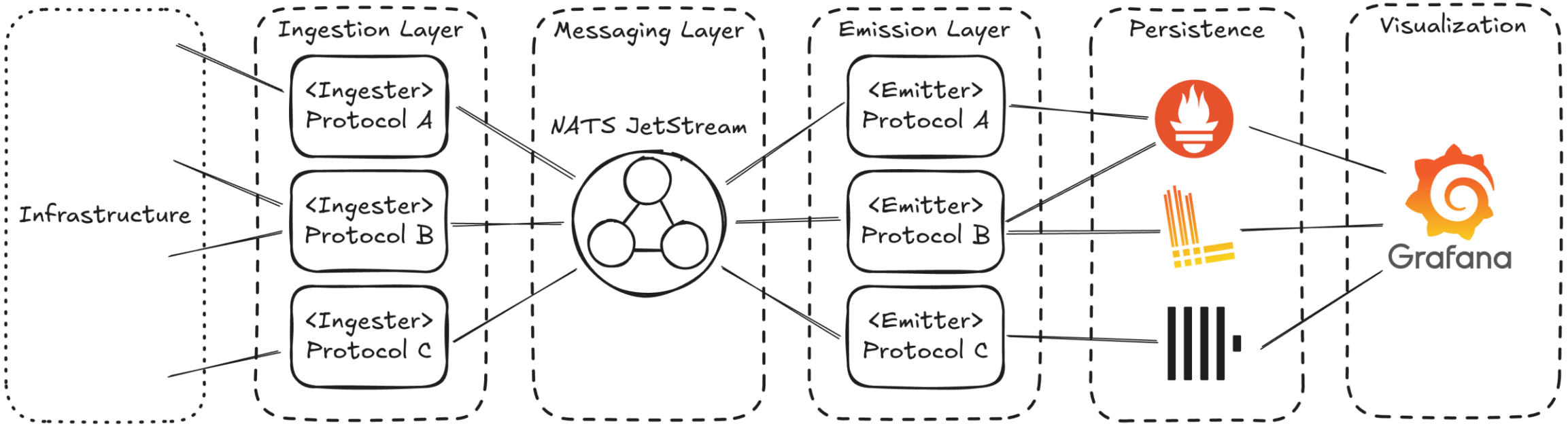
GNP-Stack Vision

For far too long **network operators have been stuck in the SNMP era**. Streaming Telemetry is a very old topic now, and yet for some reason, it has **not penetrated the market outside of Service Providers and Hyperscalers**.

Contribute to this project and help everyone get access to better telemetry.

GitHub Repository: https://github.com/fatred/gnp-stack

Architecture



BMP what? A high-speed recap

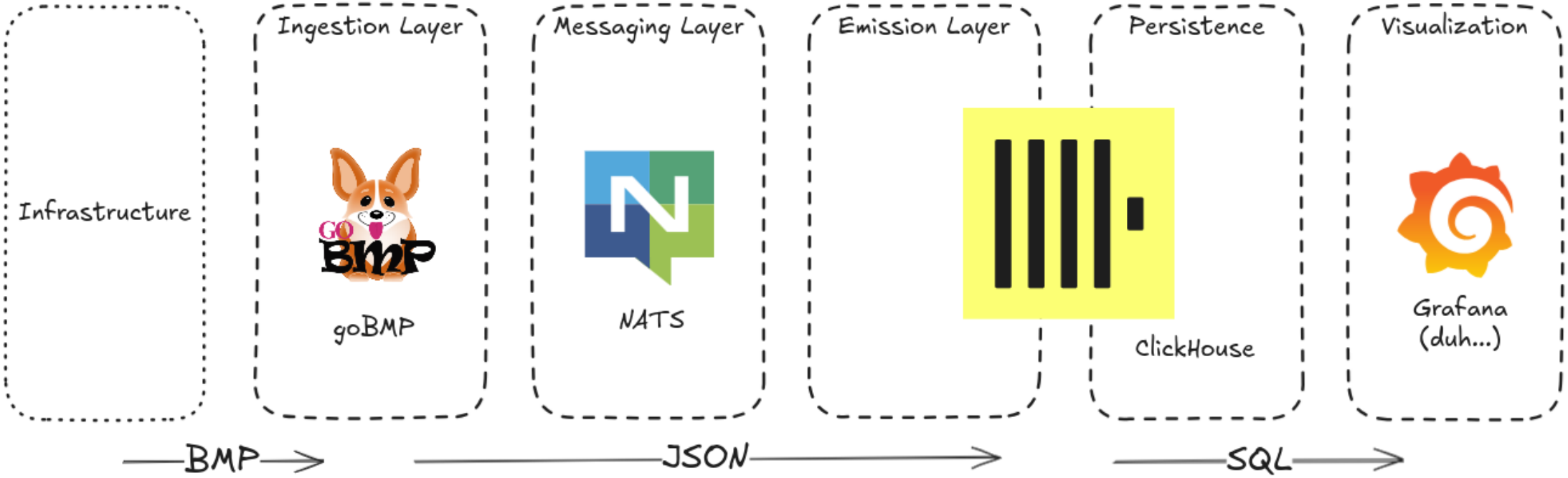
- BGP Monitoring Protocol (BMP): RFC 7854
  - Forward BGP session information to a collector
  - Via advertisements / withdrawals
- Hidden superpowers arise in combination with:
  - RFC 4760: Multiprotocol Extensions for BGP-4
  - RFC 9552: Distribution of Link-State and Traffic Engineering Information Using BGP
  - **Anything distributed by BGP* can be monitored via BMP!**
- (Subsequent) Address Family Identifiers:
  - AFI / SAFI pair identifies specific NLRI (e.g. IPv6 Unicast)

- Quite young (2016)
- Observability of
  - Adj-RIB-In
  - Adj-RIB-Out
  - Loc-RIB

NLRI	AFI / SAFI
IPv6 Unicast	2 / 1
IPv4 Unicast	1 / 1
Link-State	16388 / 71
L2VPN (EVPN)	25 / 70

OST

Data Flow



https://github.com/sbezverk/gobmp
https://nats.io/
https://clickhouse.com/
https://grafana.com/

Challenges

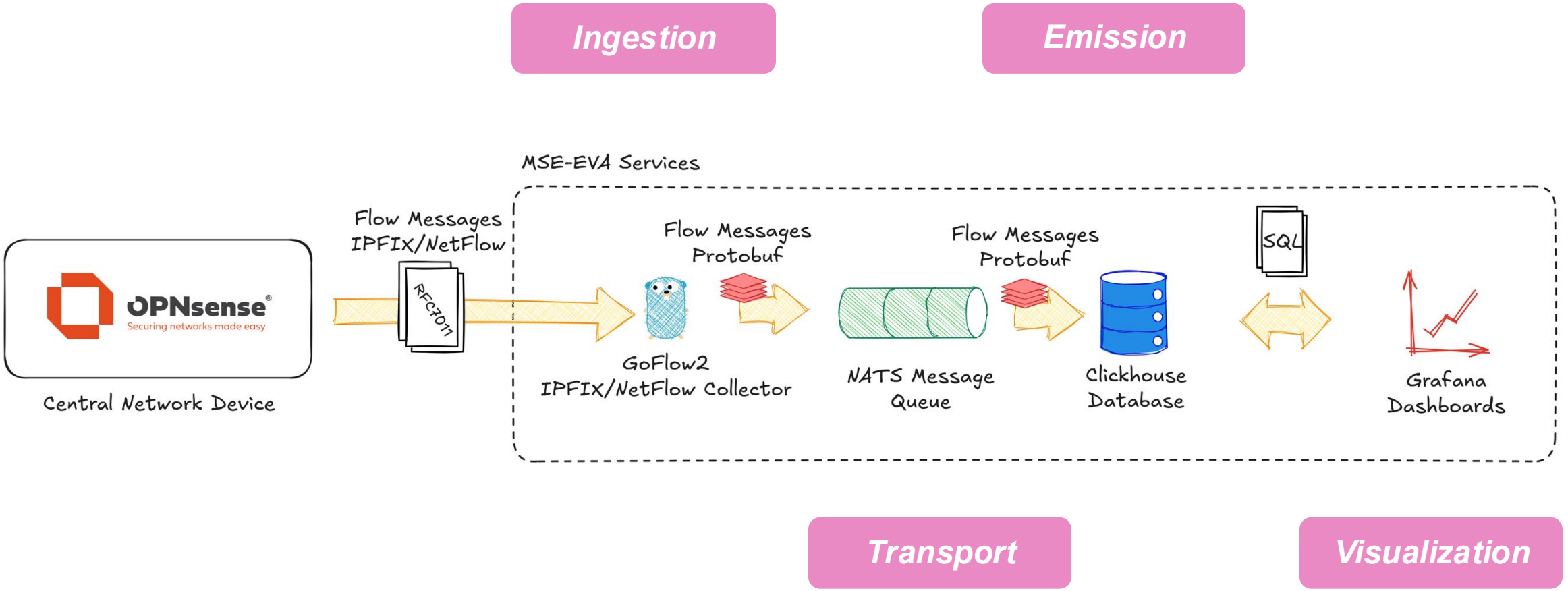
- Translation of events to state 🤔
  - Advertisement ("action": "add")
  - Withdrawal ("action": "del")
  - 🤦♂️🤦♂️🤦♂️
- Performance when working with large data volumes (e.g. RIPE RIS):
  - When should we evaluate the current state?
    - At insertion time? (Higher load, faster queries)
    - At query time? (Lower load, slow queries)
- Creating a good data model (adaptability vs. speed)
  - Do we only parse some fields and accept losing information?

Challenges

```
AreaID              string                    `json:"area_id"`
Protocol            string                    `json:"protocol,omitempty"`
ProtocolID          base.ProtoID              `json:"protocol_id,omitempty"`
NodeFlags           *bgpls.NodeAttrFlags      `json:"node_flags,omitempty"`
Name                string                    `json:"name,omitempty"`
SRCapabilities      *sr.Capability            `json:"ls_sr_capabilities,omitempty"`
SRAlgorithm         []int                      `json:"sr_algorithm,omitempty"`
SRLocalBlock        *sr.LocalBlock            `json:"sr_local_block,omitempty"`
SRv6CapabilitiesTLV *srv6.CapabilityTLV       `json:"srv6_capabilities_tlv,omitempty"`
NodeMSD             []*base.MSDTV             `json:"node_msd,omitempty"`
FlexAlgoDefinition  []*bgpls.FlexAlgoDefinition `json:"flex_algo_definition,omitempty"`
```

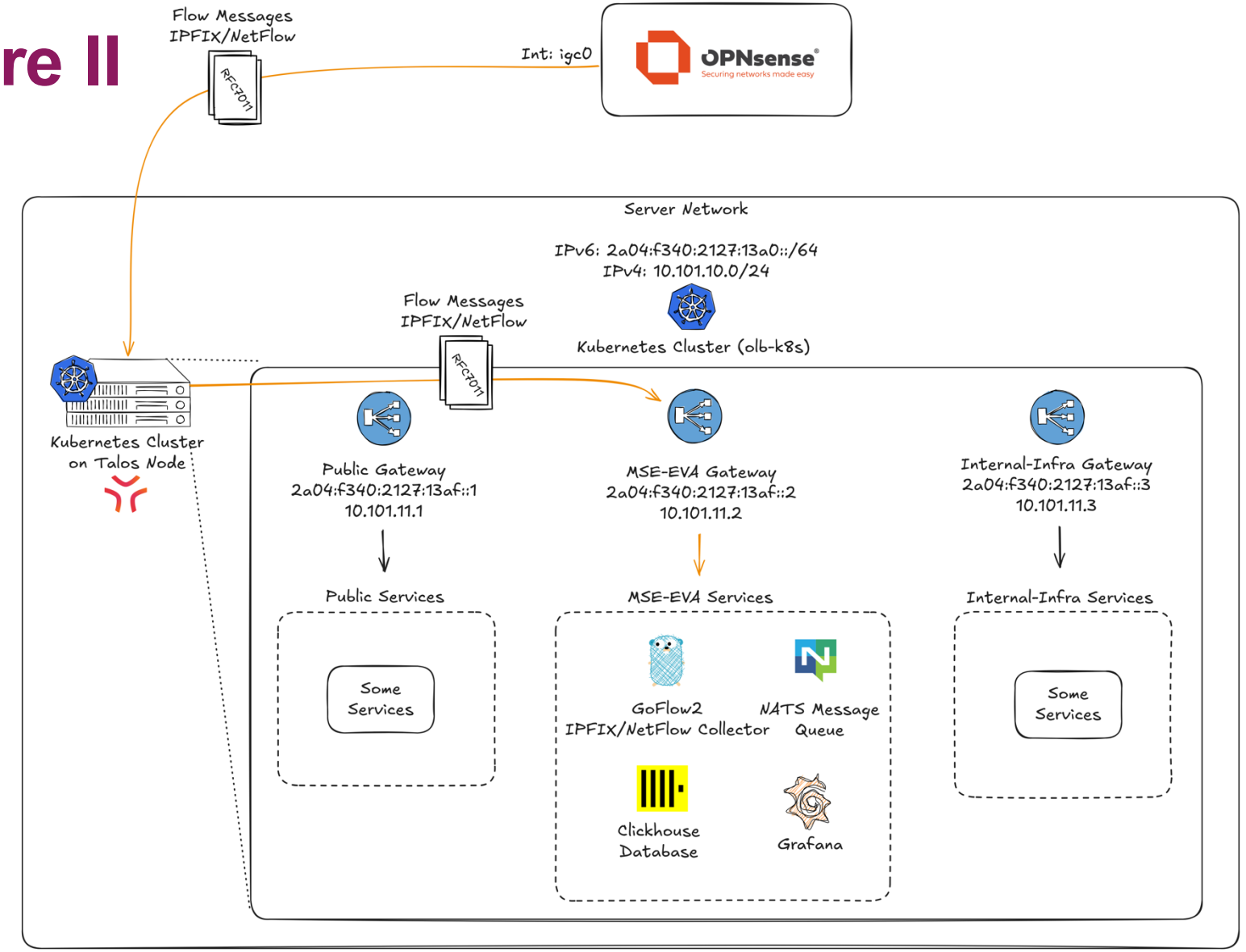
https://github.com/sbezverk/gobmp/blob/master/pkg/message/types.go

Architecture I



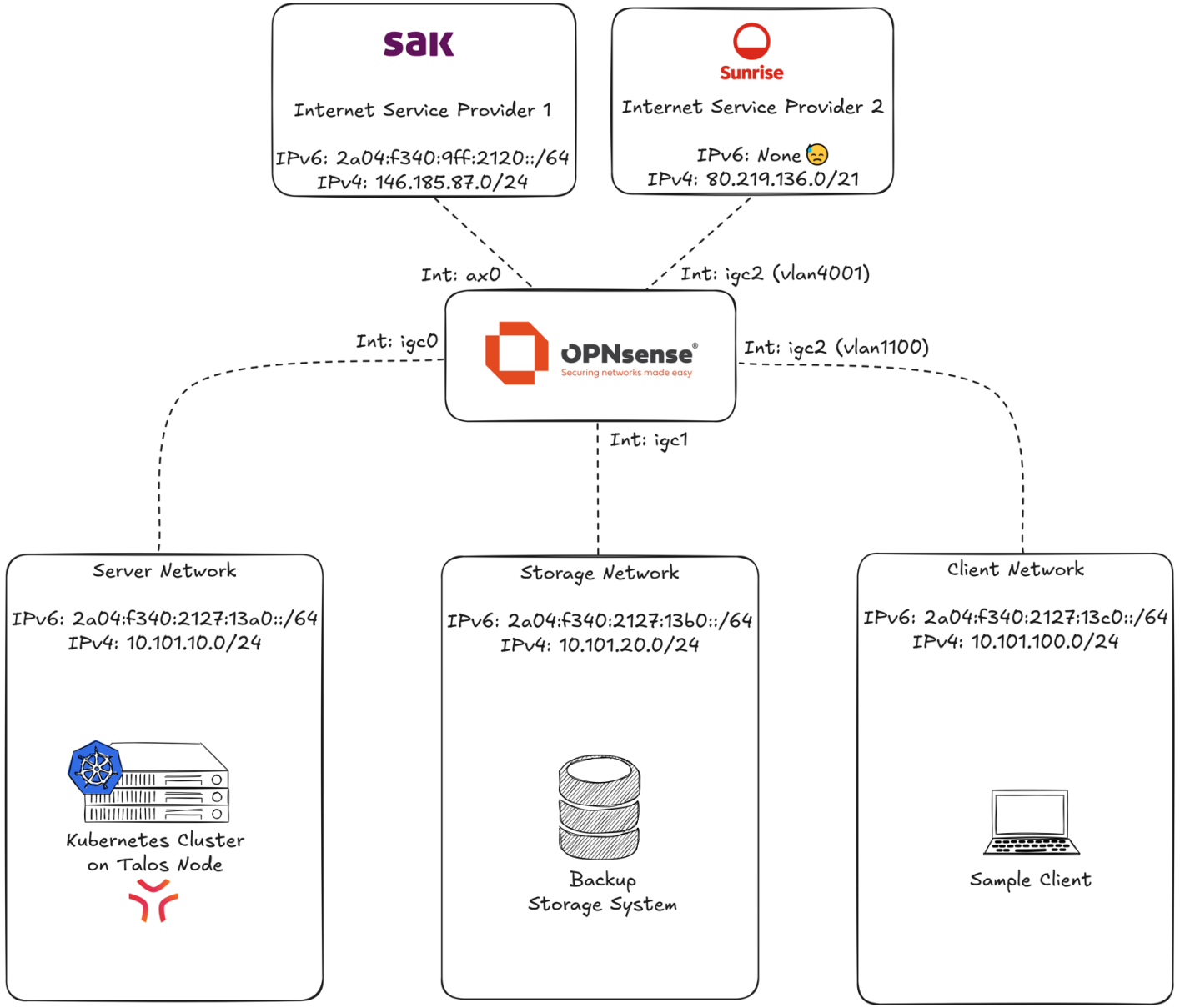
IPFIX/NetFlow Integration

Architecture II

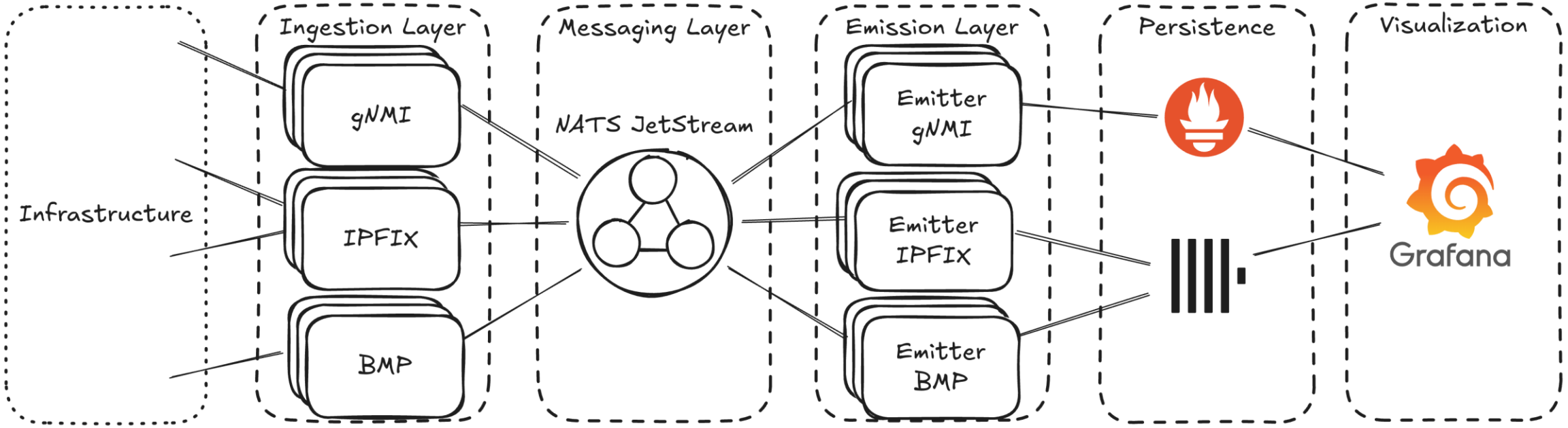


Challenges

- Double Flow Count
  - NAT Traffic 🥲
  - Same flow counted once as ingress flow and once as egress flow
- Statistics by Flow Direction
  - Inbound
  - Outbound
  - Local
- Creating Grafana Dashboards.. It takes forever. 😂



Architecture

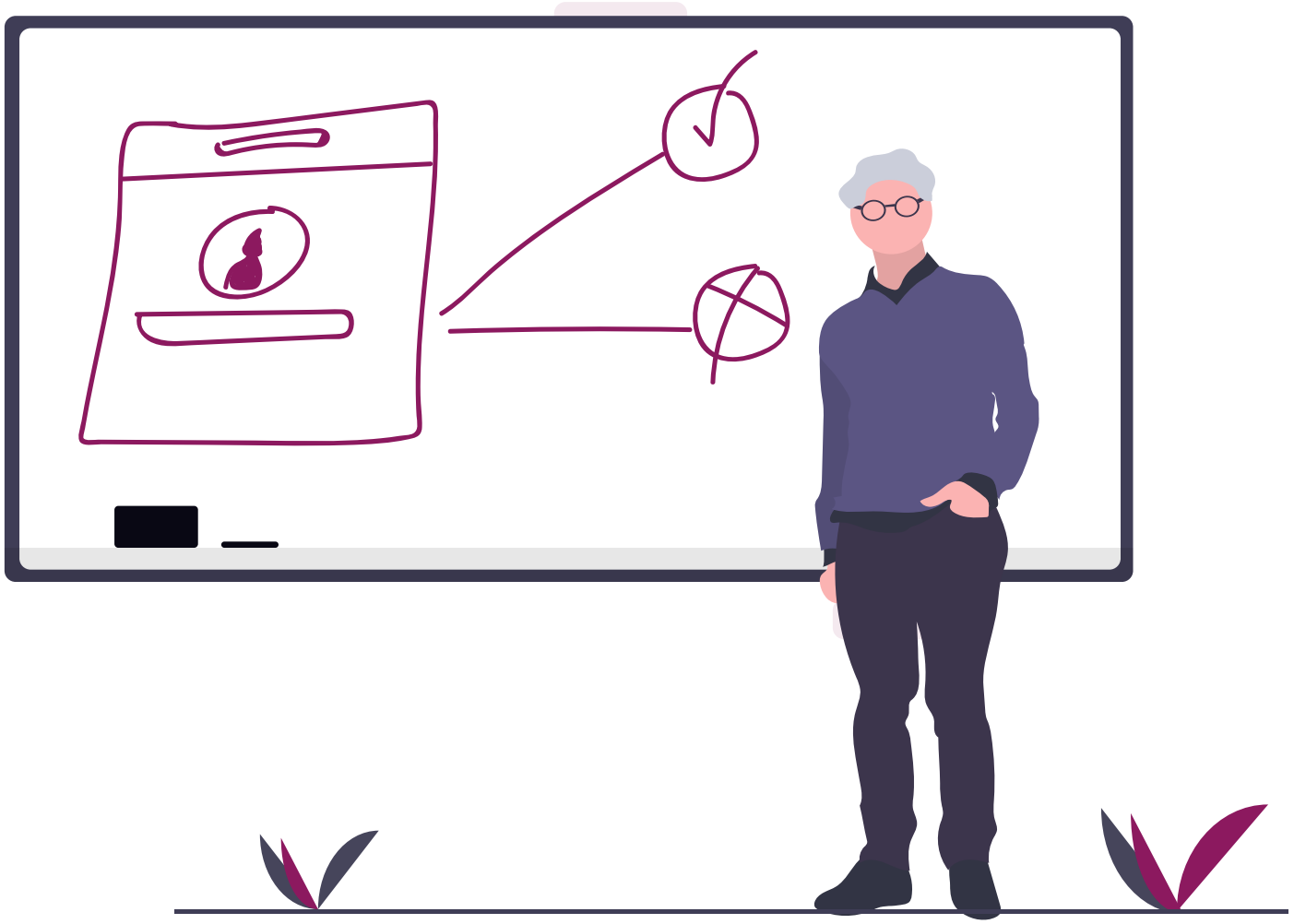


Are you ready to deploy it?

```
git clone https://github.com/Untersander/gnp-stack.git
cd gnp-stack
docker-compose up -d
```

```
helm upgrade --install gnp-stack oci://ghcr.io/untersander/gnp-stack/gnp-stack --namespace gnp-stack --create-namespace
```

Demo



Discussion and Next Steps