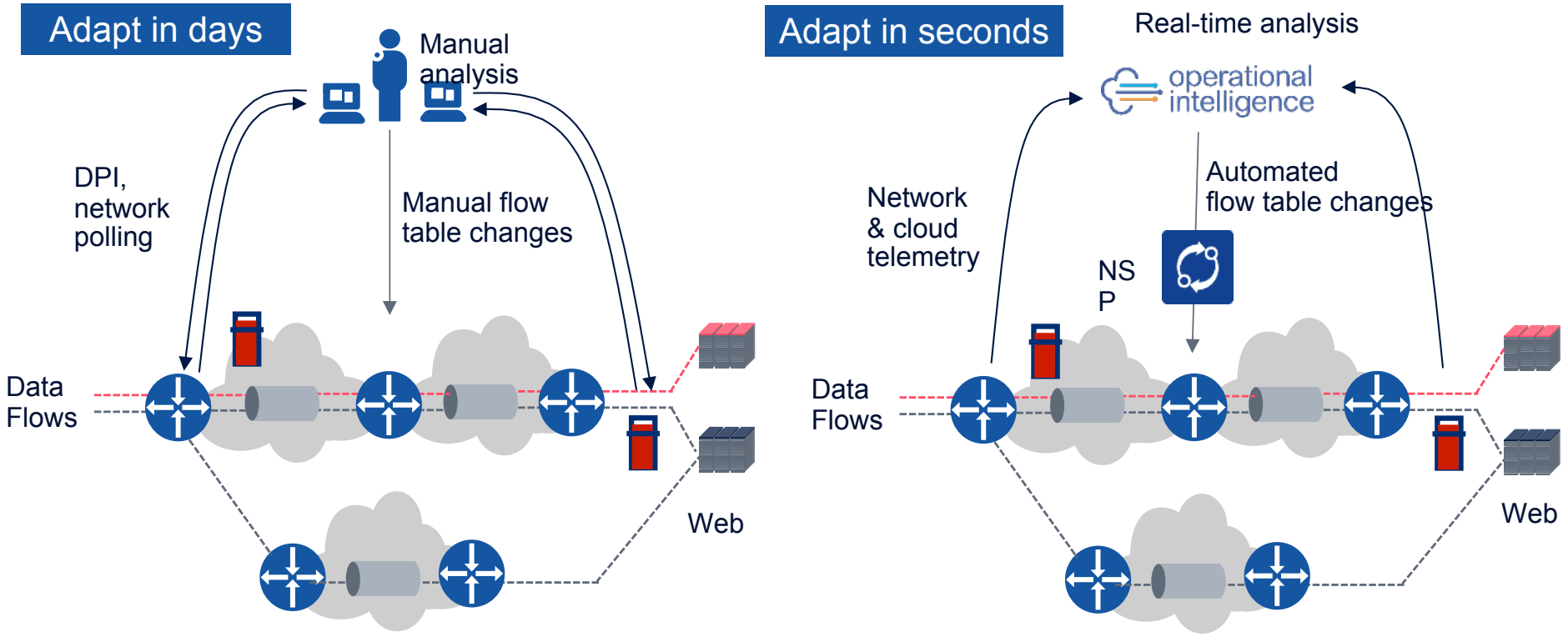
Deepfield: Real-time, Big Data Network Analytics

Stefan Meinders - Senior Consulting Engineer EMEA

2017/03/20

The Better Way to Build a Smart IP Network

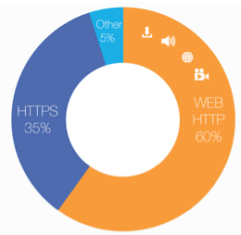
IP network analytics drives closed-loop SDN assurance



Why is there a need for new / next generation traffic analytics?
What has changed?

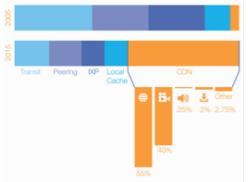
95% HTTP/[s]

- Apps, OTT, REST APIs, ⋯
- Everything runs in a browser
- Services are moved into the cloud or CDNs
- IoT, M2M, ...
- More Encryption



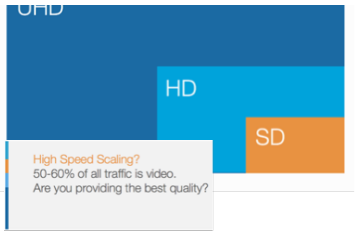
60% CDN

- CDNs: You no longer know the service beeing offered e.g. by Origin_AS, different services being offered by the same CDN like software distribution and video
- CDN on-caches
- Changes in content delivery



⇗ OTT

- A combination of the previous two issues
- Premium OTT services, high expectation by end-customers
- OTT provider is controlling the bandwidth - adaptive bit rate
- 60% is Video traffic, too big to fail
- Slow is the new Down



Next Gen Features

- Flexible data ingestion
- Open integration of 3rd party products. E.g. Mitigation vendors
- Avoid manual configuration

NOKIA

Why is there a need for new / next generation traffic analytics?

Why are traditional solutions failing?

Legacy Flow Analysis

- NetFlow: data up to layer4 only
- SNMP has polling intervals (5min)
- 2 dimensional reports
- Pre-Configuration required
- No deduplication
- No service KPIs

DPI

- Does not scale
- Privacy concerns
- Not network aware
- Bump in the wire
- Challenges with encrypted traffic

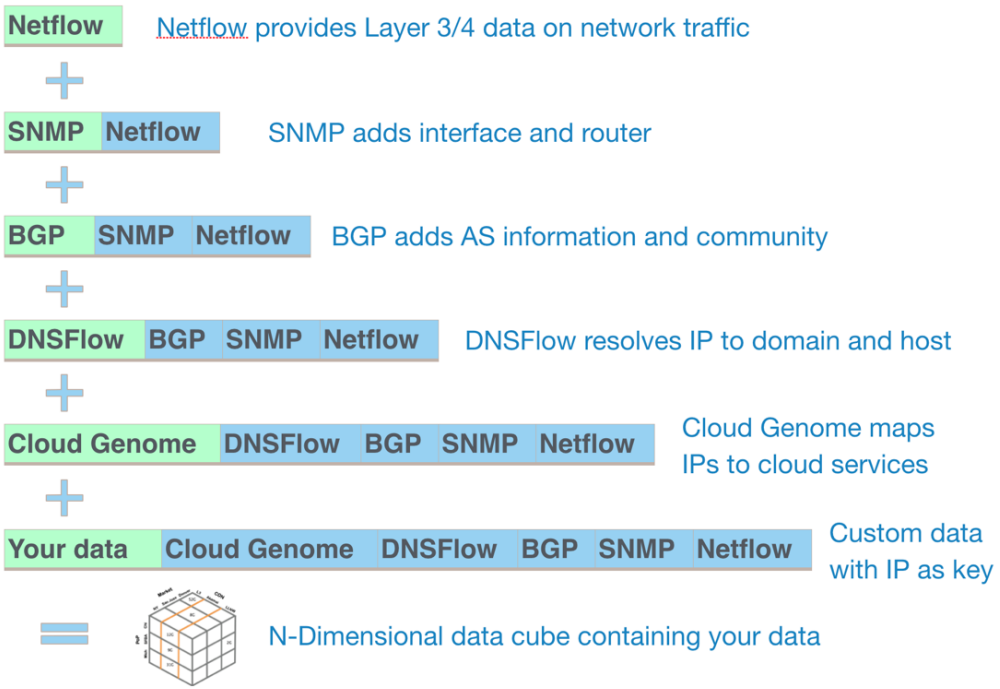
Integration / Isolation

- Limited data ingestion
- Mainly Flow/SNMP/ BGP
- No Flexibility on southbound and northbound interfaces
- Limited data correlation
- Missing context information

Automation

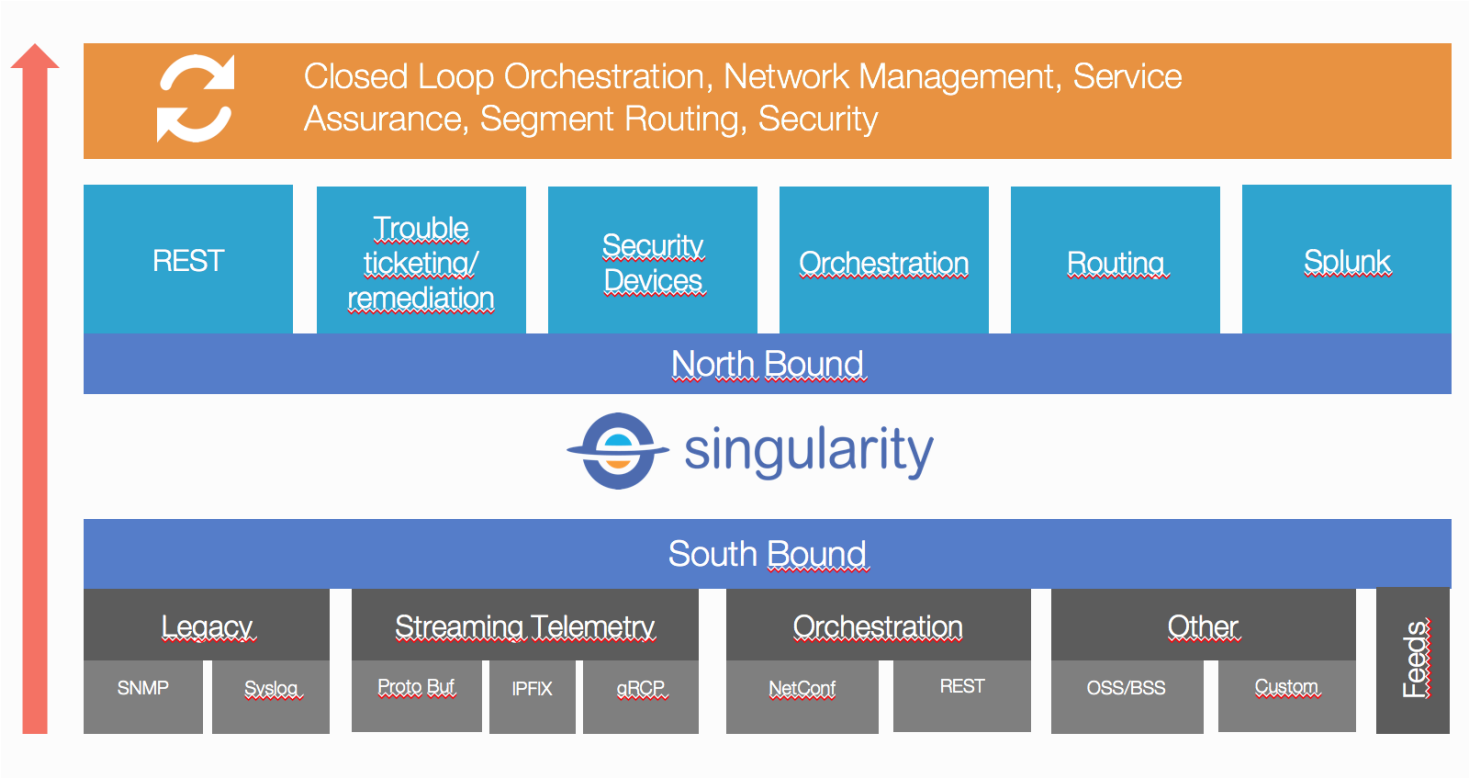
- Requires a deep understanding of the state of the network
- False positives and false negatives
- Requires real-time observation
- No open / flexible connectors
- Just simple use-cases

The Nokia Deepfield approach
How to adapt to the dynamics?

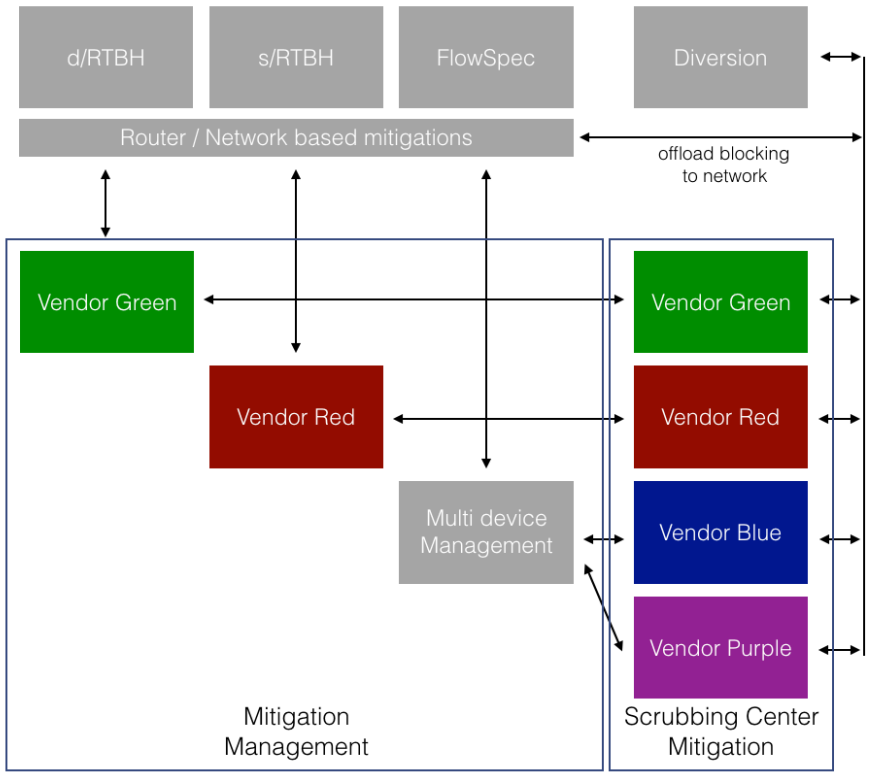


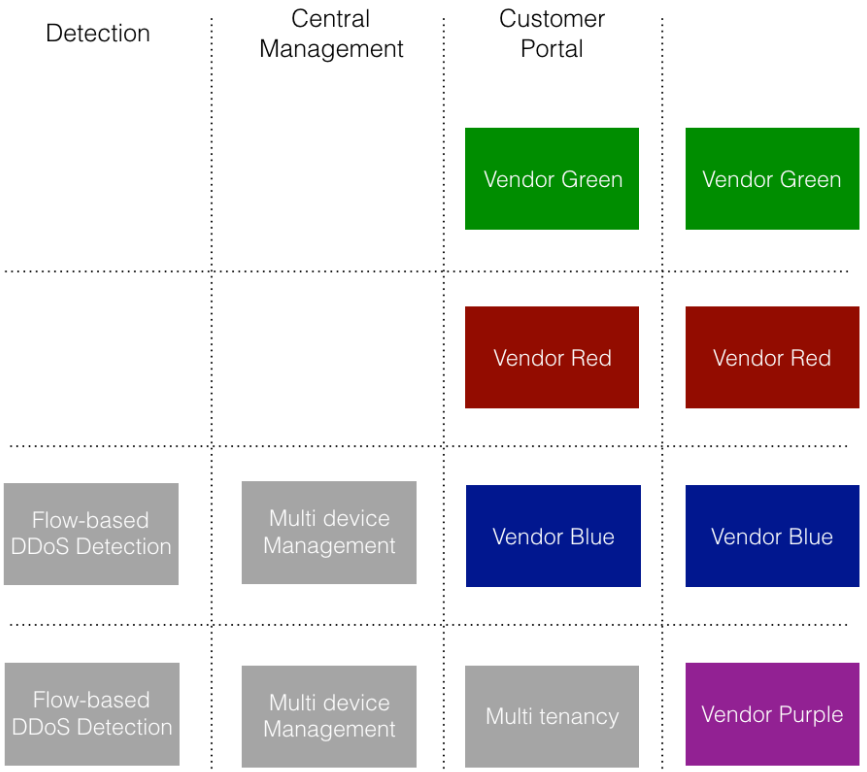
- Correlate legacy telemetry data with additional information

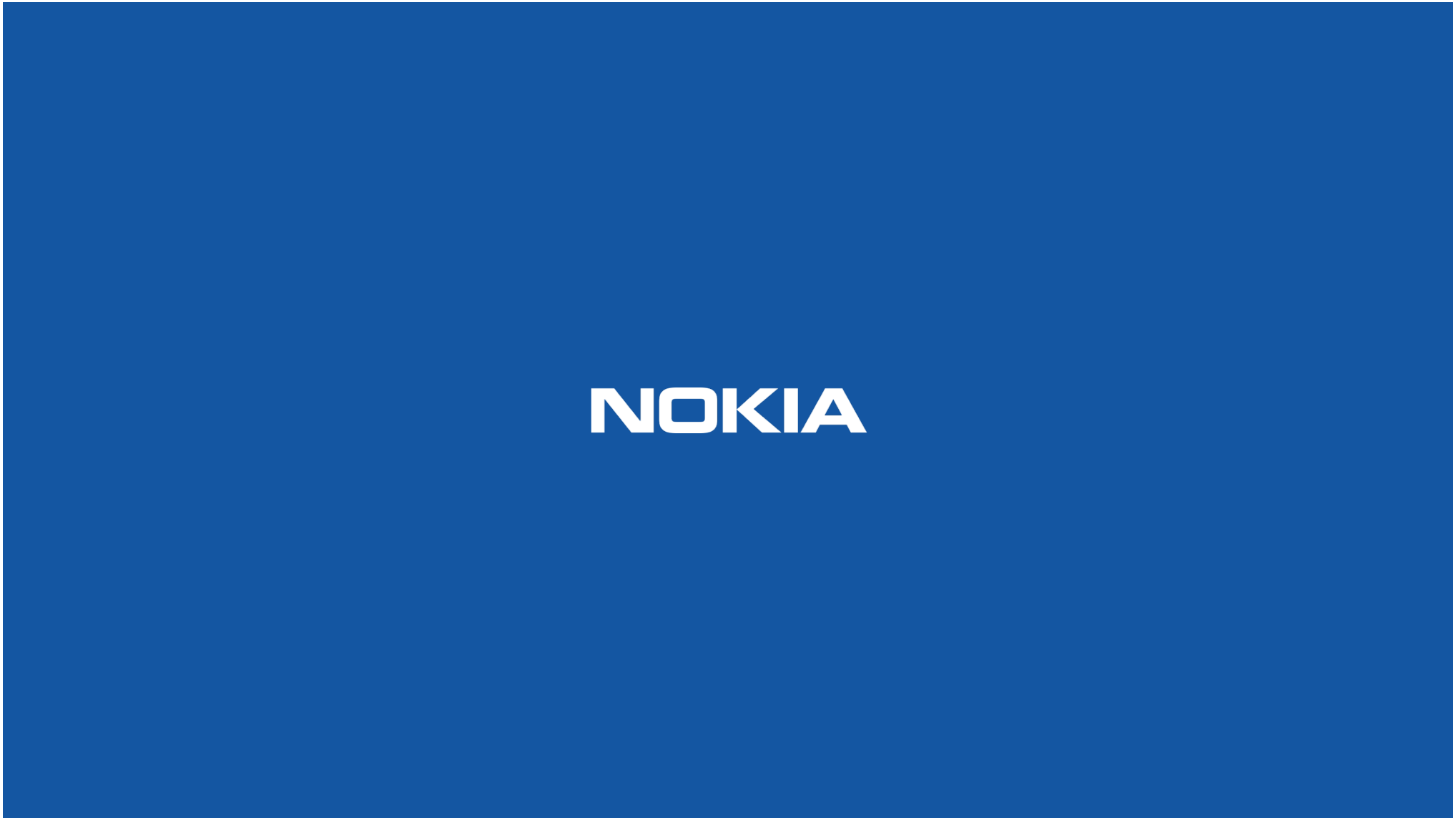
Our singularity platform
Get as much data as you can



Defender - Mitigation Strategies
Orchestration of DDoS Mitigation






NOKIA