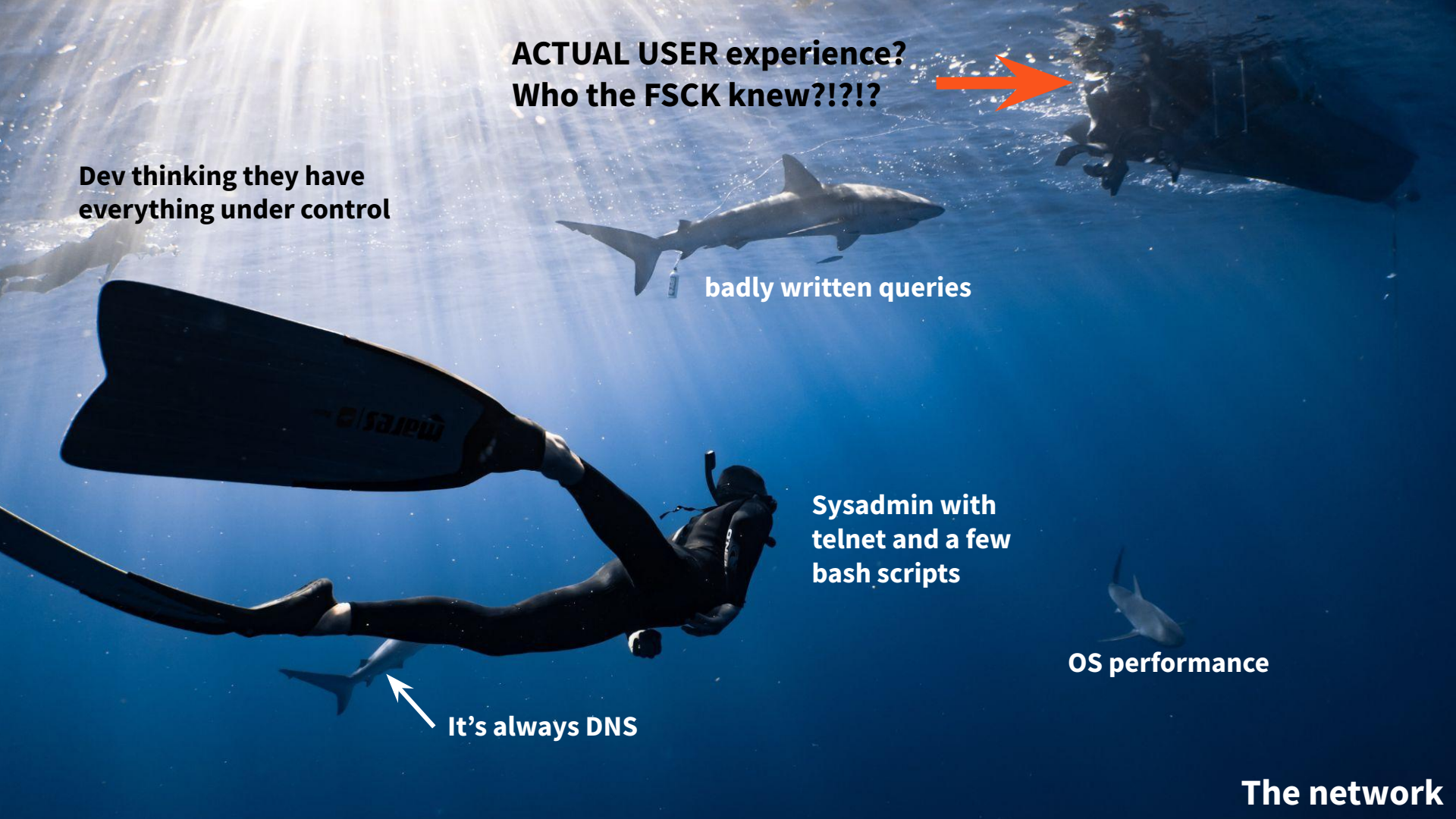
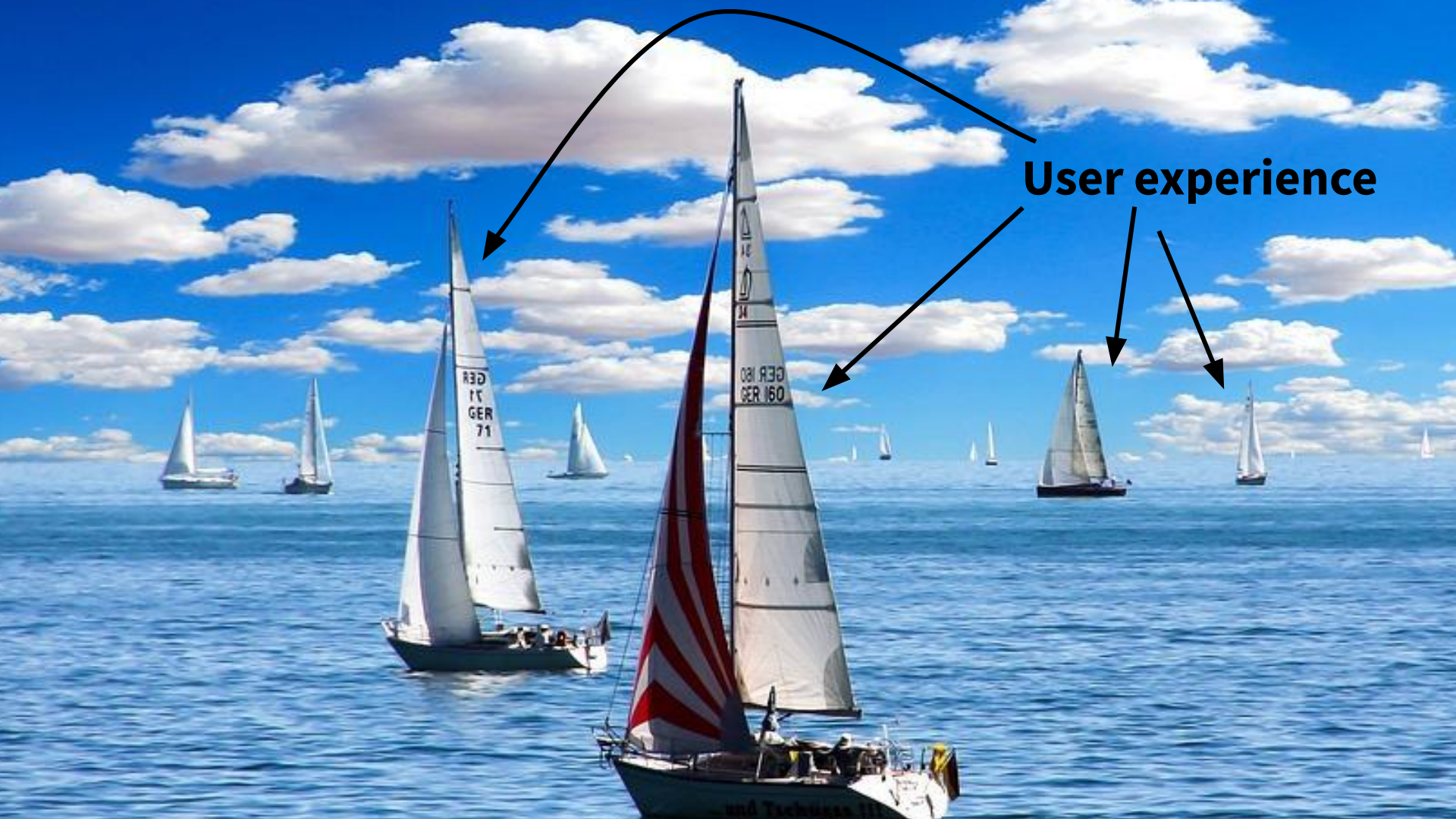
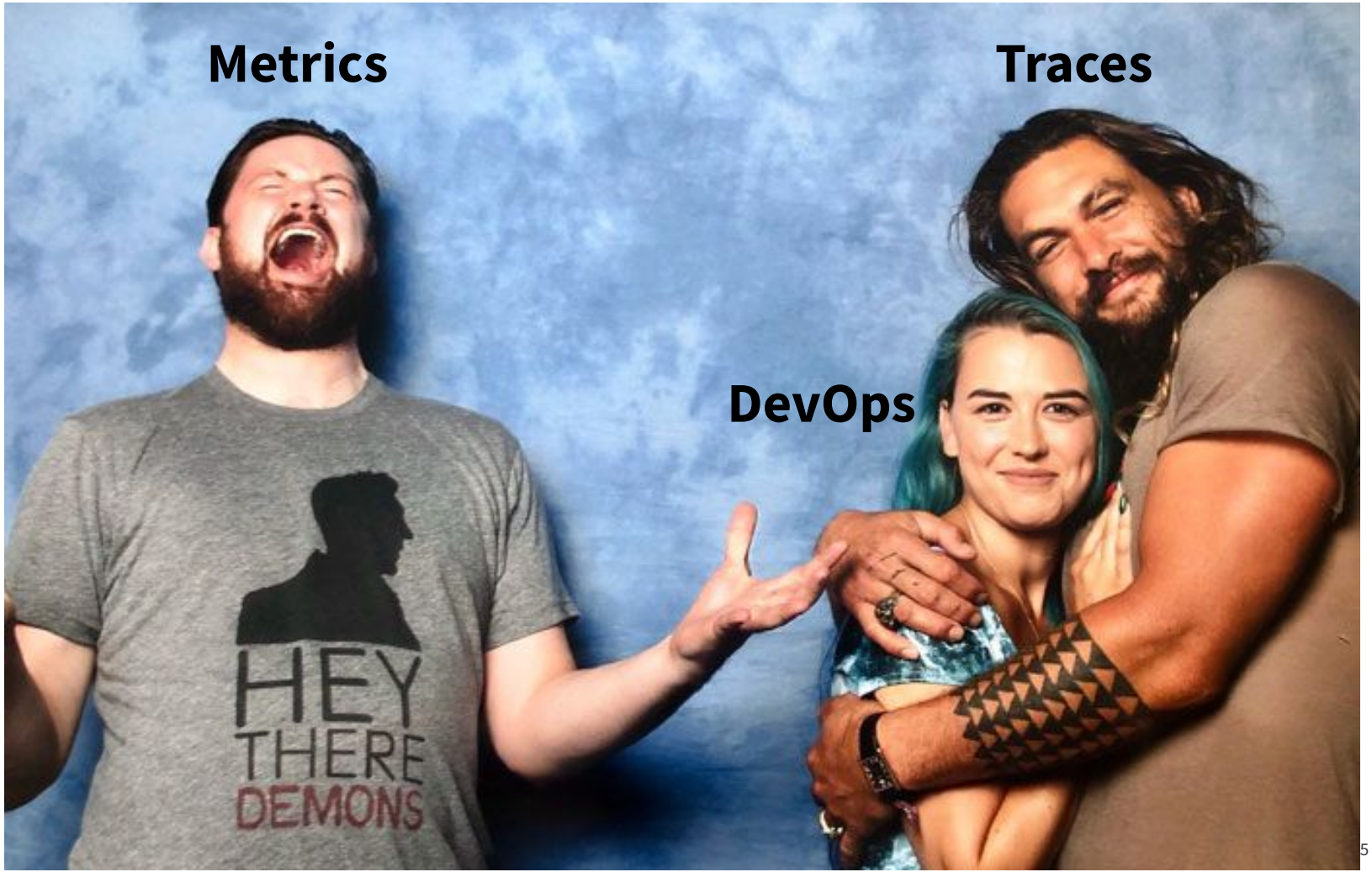
OBSERVABILITY

Back in my day


ACTUAL USER experience?
Who the FSCK knew?!?!?
Dev thinking they have everything under control
badly written queries
Sysadmin with telnet and a few bash scripts
OS performance
It's always DNS
The network

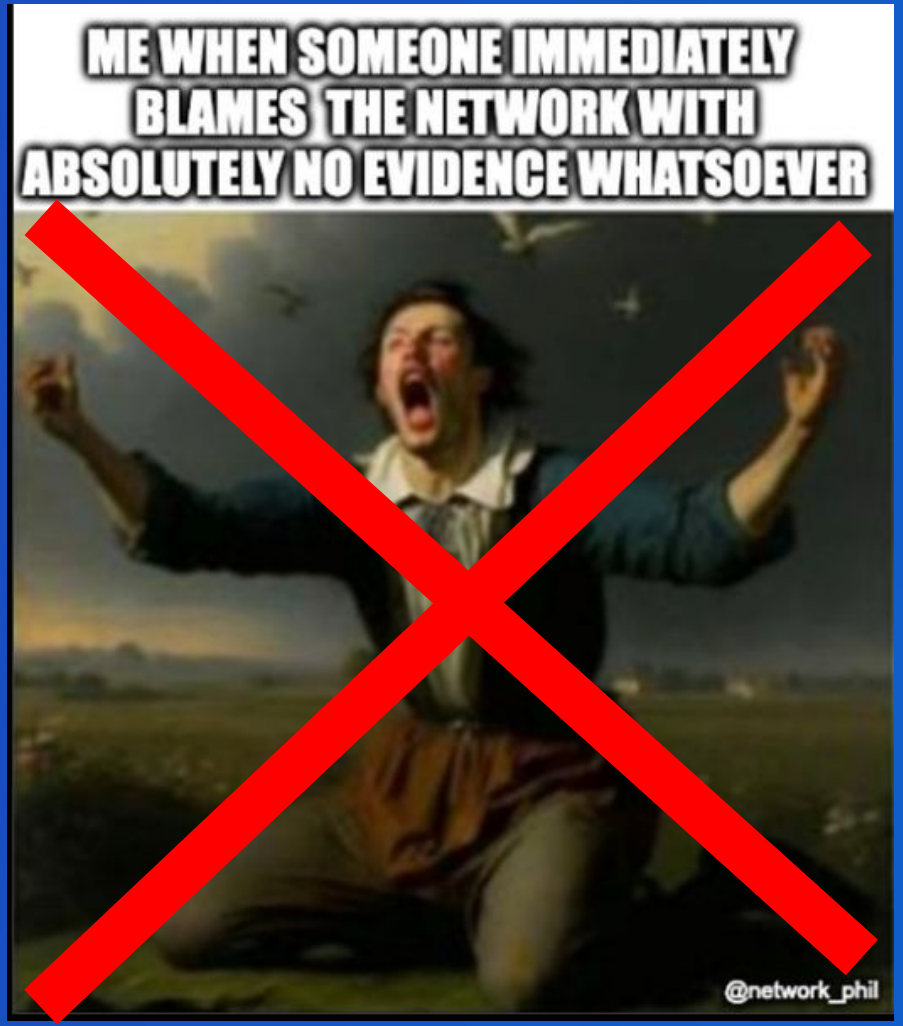

User experience

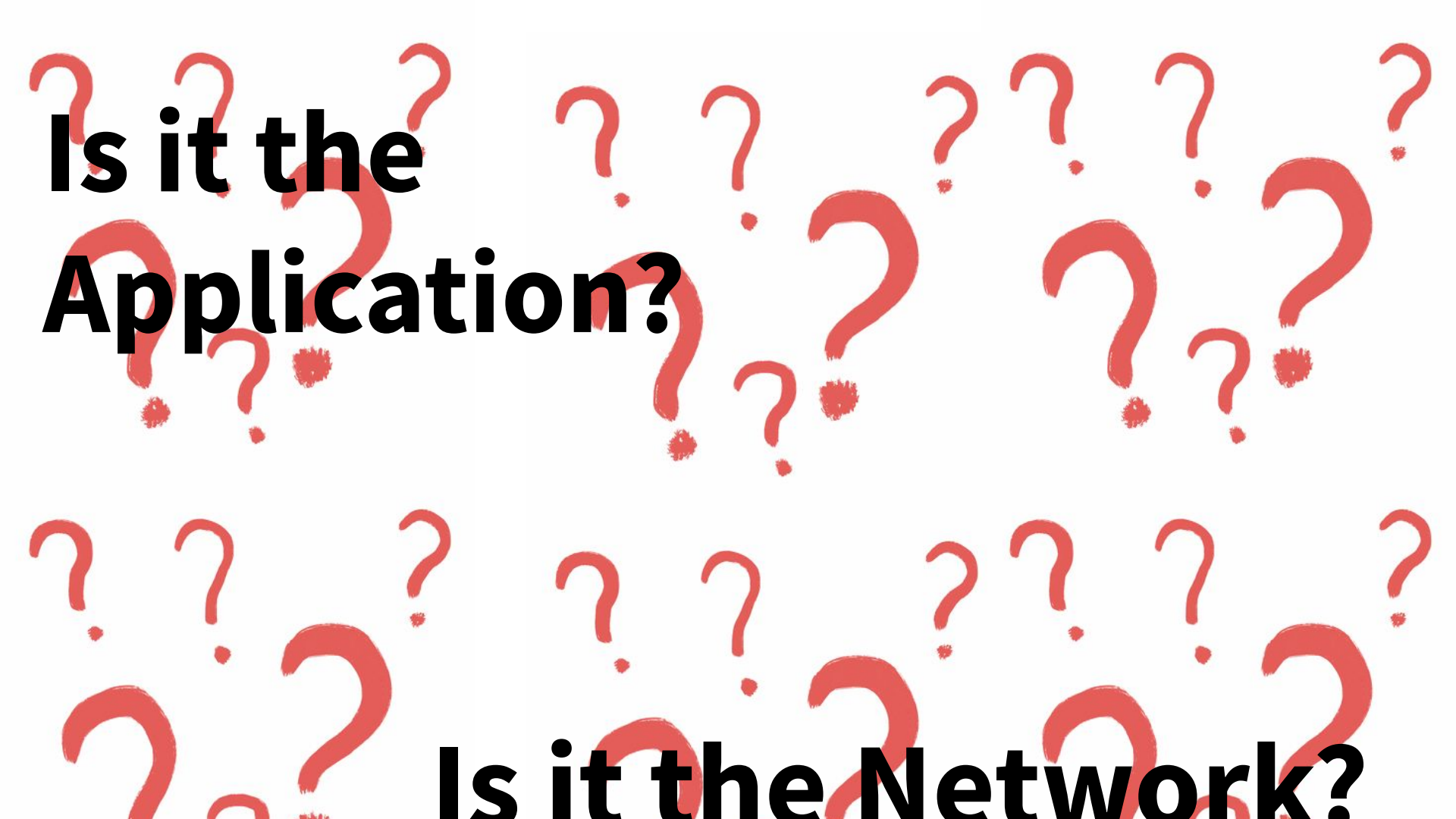

Metrics
Traces
DevOps
HEY
THERE
DEMONS

Love your network

FOR THE LOVE OF PANTS!!!

Learn how IP addresses work.




Is it the Application?
Is it the Network?

Network Observability

Overlooked, Underappreciated, and More Important Than Ever

@LeonAdato
Principal Technical Evangelist

Leon Adato

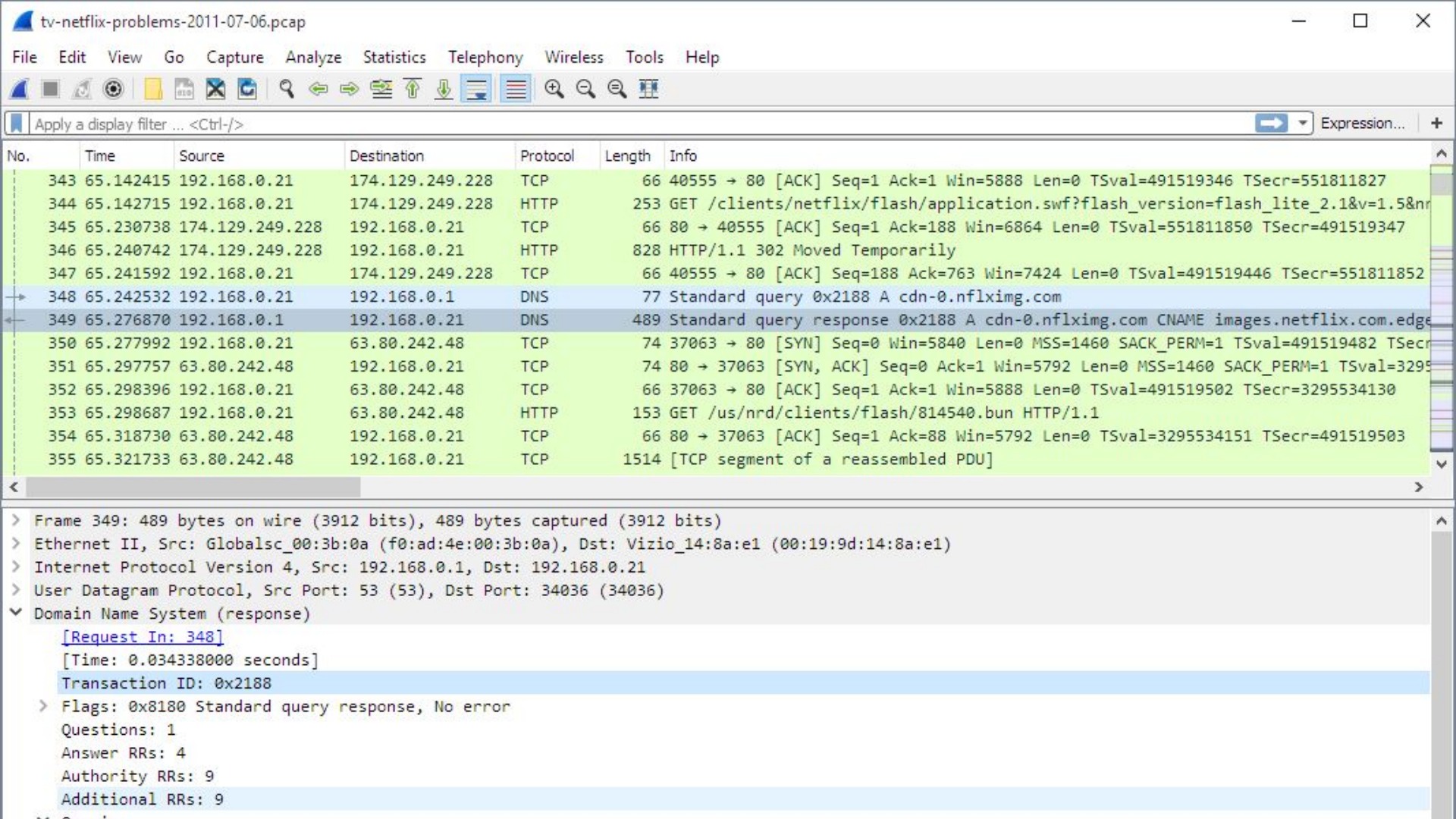
- Principal Technical Evangelist
  - ***at Kentik***
- ~35 yrs in tech.
- ~25 yrs monitoring & observability.
- ~10 yrs as a Tech Evangelist, DevRel Advocate, and (ugh) “Head Geek.”
- Tivoli, BMC, OpenView, janky perl scripts, Nagios, SolarWinds, DOS batch files, Zabbix, Grafana, New Relic, and other assorted nightmare fuel.

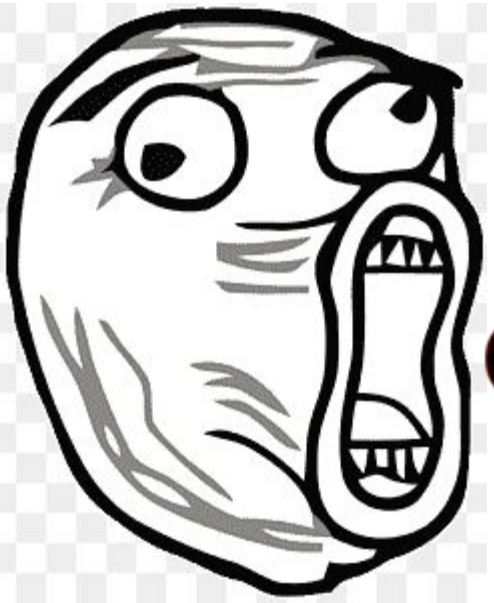
@LeonAdato on almost all social media.

This is an Oyster Talk™

leon@leon-Latitude-7440: ~

```
leon@leon-Latitude-7440:~$ ping kentik.com
PING kentik.com (75.2.60.5) 56(84) bytes of data.
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=1 ttl=239 time=8.95 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=2 ttl=239 time=8.77 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=3 ttl=239 time=8.75 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=4 ttl=239 time=9.35 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=5 ttl=239 time=8.89 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=6 ttl=239 time=8.79 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=7 ttl=239 time=8.90 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=8 ttl=239 time=8.78 ms
64 bytes from acd89244c803f7181.awsglobalaccelerator.com (75.2.60.5): icmp_seq=9 ttl=239 time=8.83 ms
^C
--- kentik.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 12037ms
rtt min/avg/max/mdev = 8.749/8.889/9.345/0.173 ms
```


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
343 65.142415 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344 65.142715 192.168.0.21 174.129.249.228 HTTP 253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
345 65.230738 174.129.249.228 192.168.0.21 TCP 66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346 65.240742 174.129.249.228 192.168.0.21 HTTP 828 HTTP/1.1 302 Moved Temporarily
347 65.241592 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348 65.242532 192.168.0.21 192.168.0.1 DNS 77 Standard query 0x2188 A cdn-0.nflximg.com
349 65.276870 192.168.0.1 192.168.0.21 DNS 489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350 65.277992 192.168.0.21 63.80.242.48 TCP 74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351 65.297757 63.80.242.48 192.168.0.21 TCP 74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352 65.298396 192.168.0.21 63.80.242.48 TCP 66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353 65.298687 192.168.0.21 63.80.242.48 HTTP 153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354 65.318730 63.80.242.48 192.168.0.21 TCP 66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355 65.321733 63.80.242.48 192.168.0.21 TCP 1514 [TCP segment of a reassembled PDU]
Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
Domain Name System (response)
[Request In: 348]
[Time: 0.034338000 seconds]
Transaction ID: 0x2188
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 9
Additional RRs: 9



OBSERVABILITY

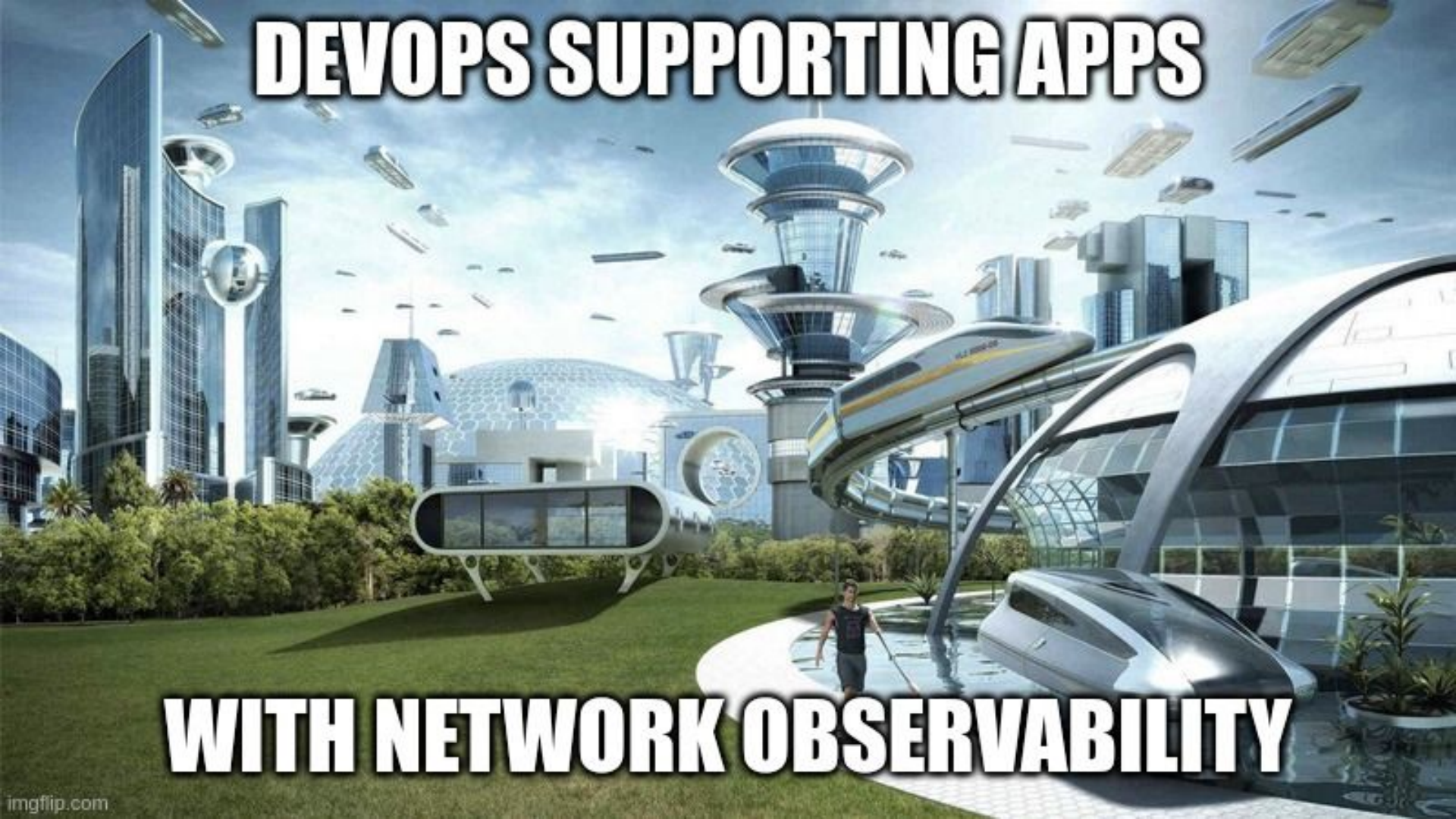
Let’s add a little nuance

Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals
  (latency, traffic, errors, saturation)

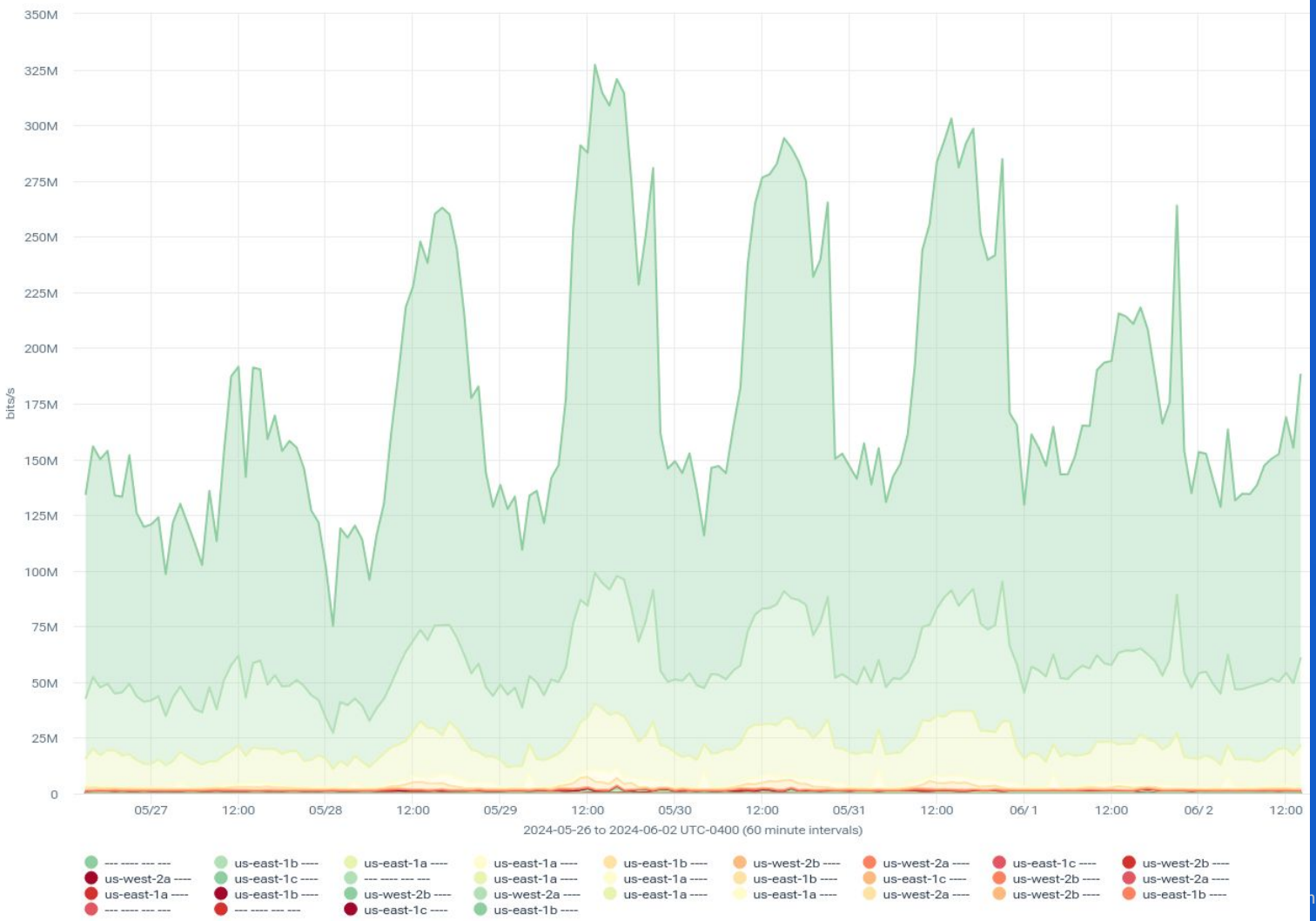
Monitoring

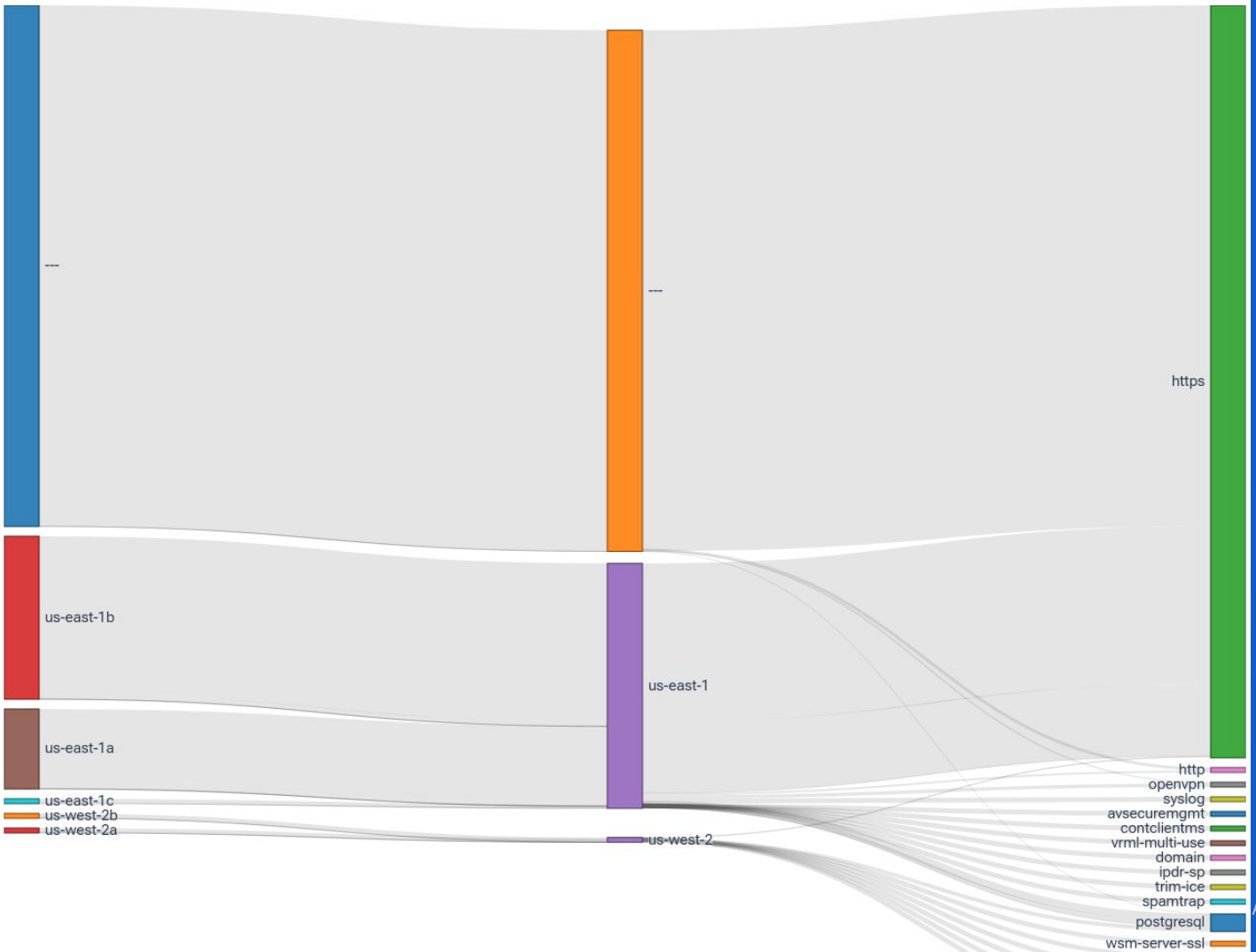
- Known Unknowns
- All cardinalities welcome
- (mostly) manual correlation
- Domain-specific signals

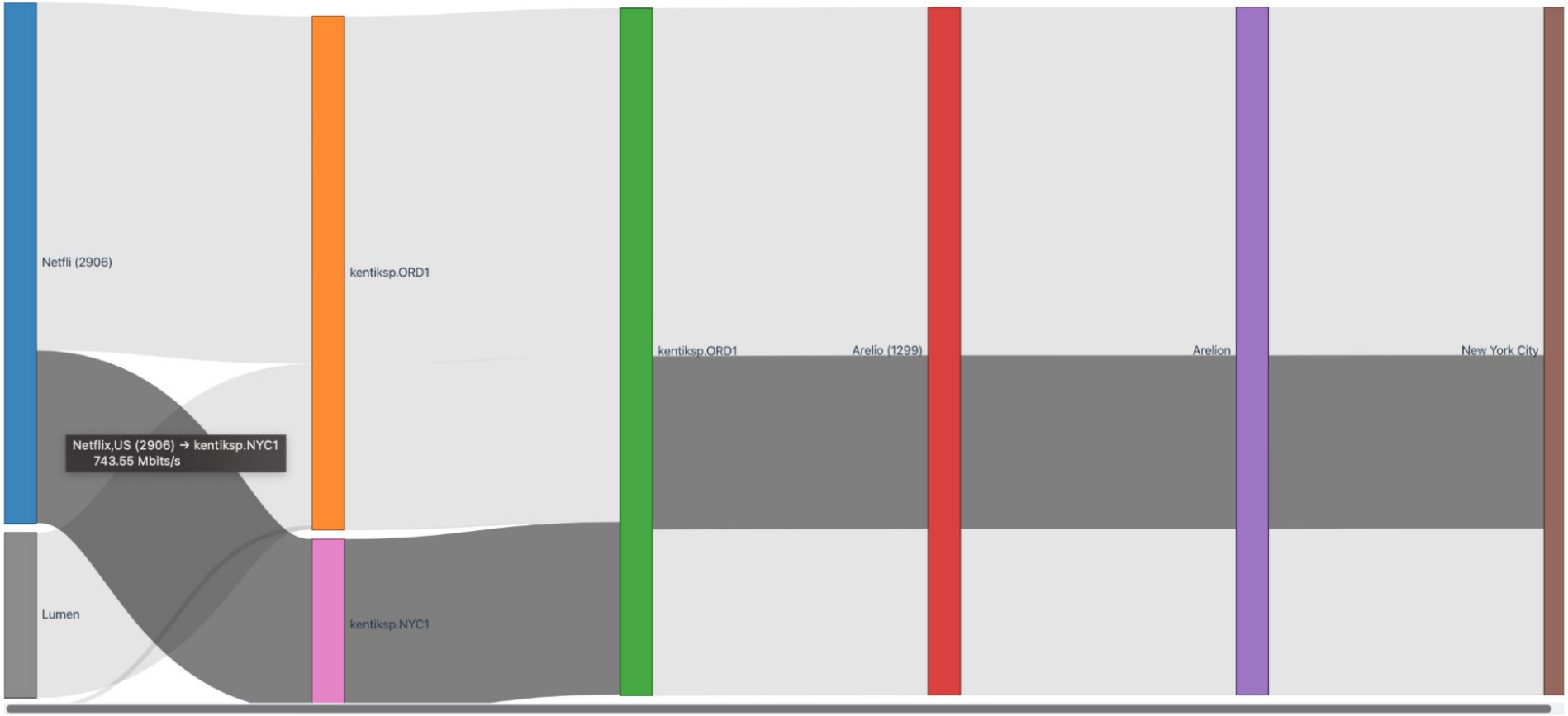

DEVOPS SUPPORTING APPS
WITH NETWORK OBSERVABILITY
imgflip.com

Hold up…

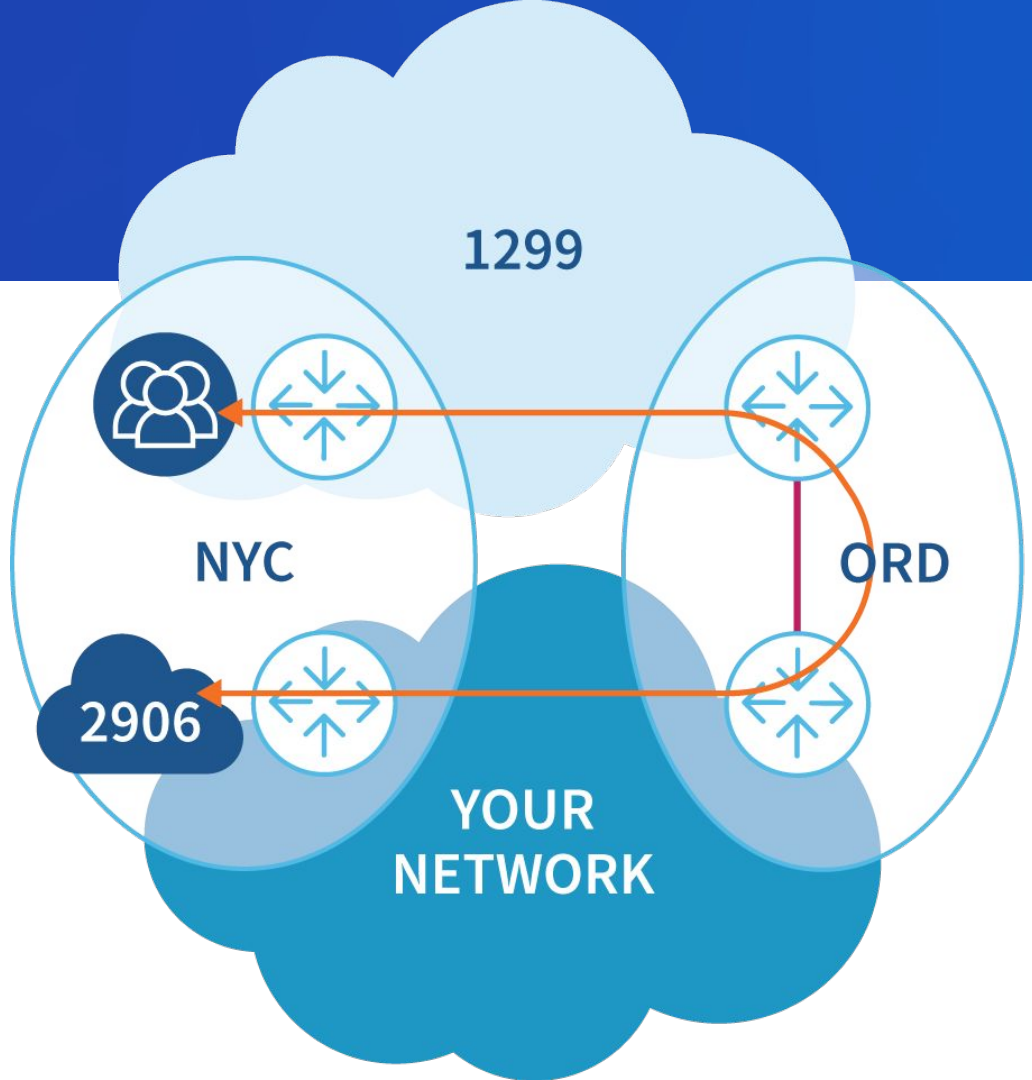

EXTREME TOOLS

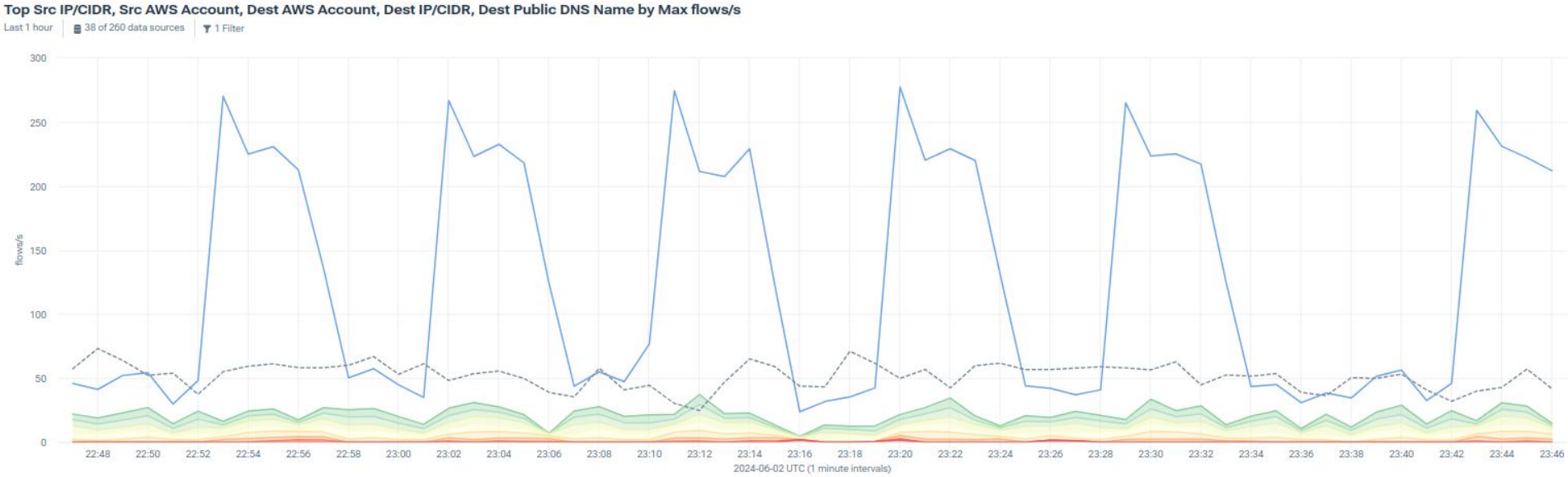


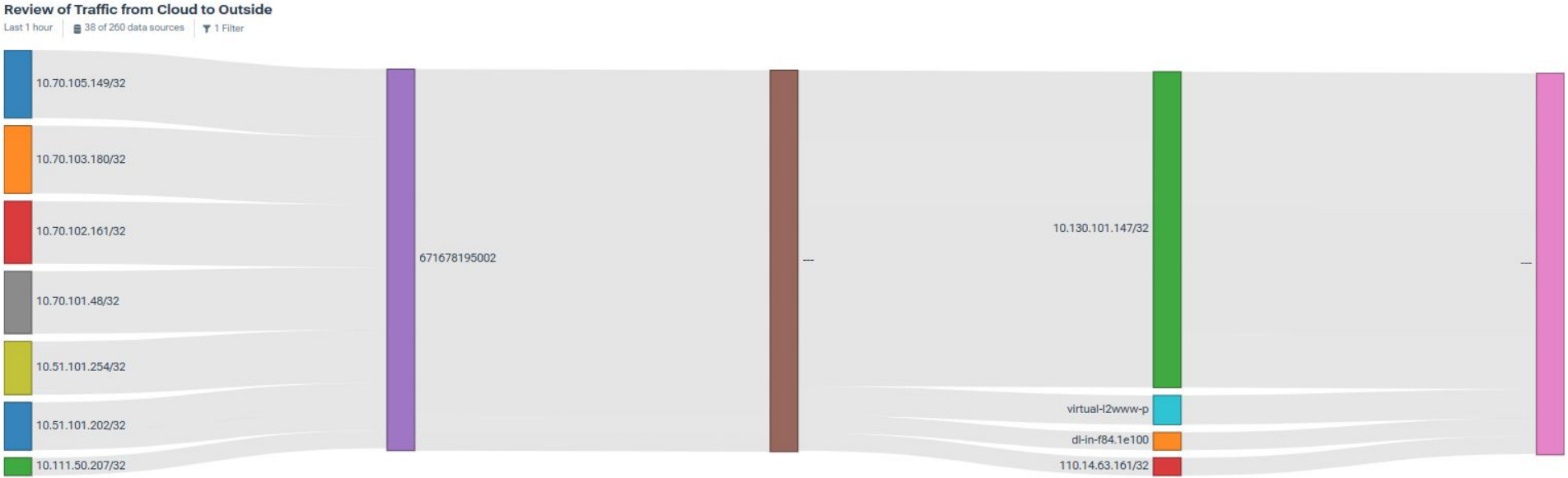


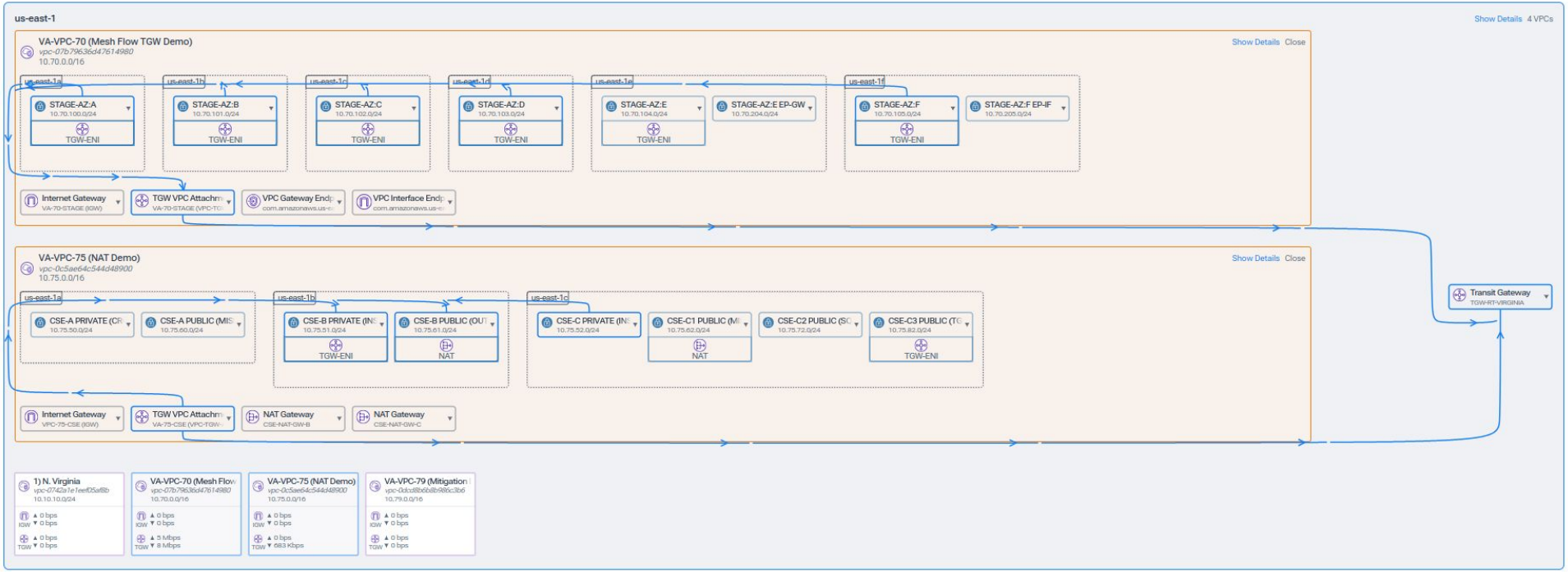


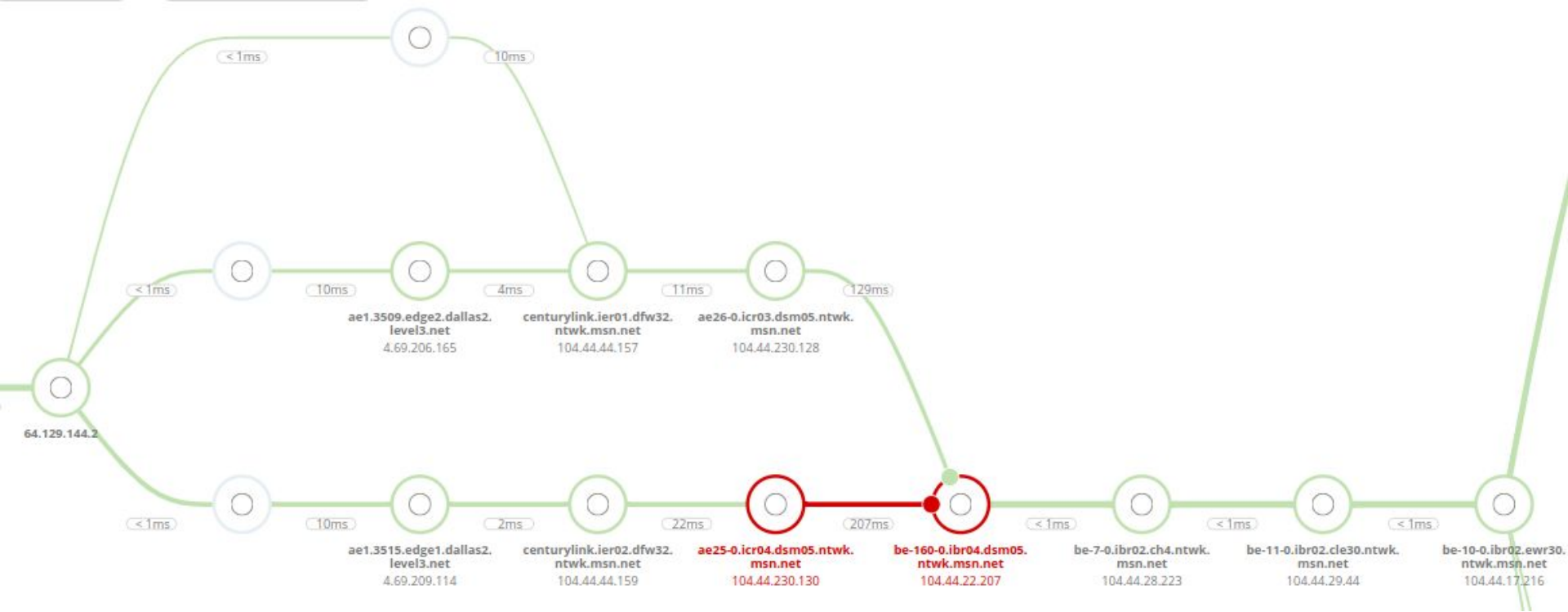
Source AS Number	Site	Ultimate Exit Site	Destination Next Hop AS Number	Destination AS Number	Destination City	Average Mbits/s	95th Percentile Mbits/s	Max Mbits/s	Last Datapoint Mbits/s
2906 - Netflix,US	kentiksp.ORD1	kentiksp.ORD1	1299 - Arelion (Telia Carrier),SE	1299 - Arelion (Telia Carrier),SE	New York City	1,492.22	1,987.23	2,055.64	1,276.01

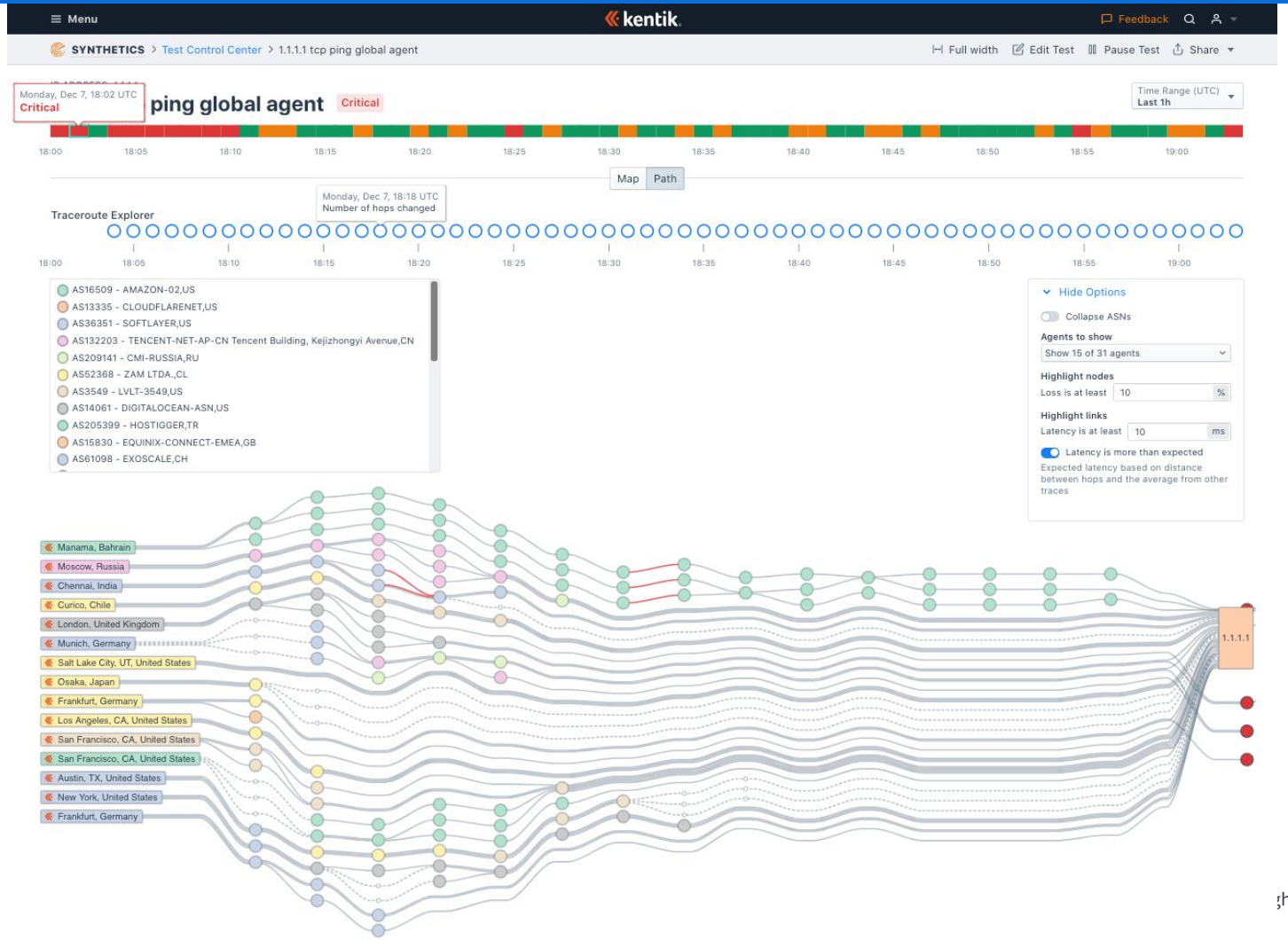




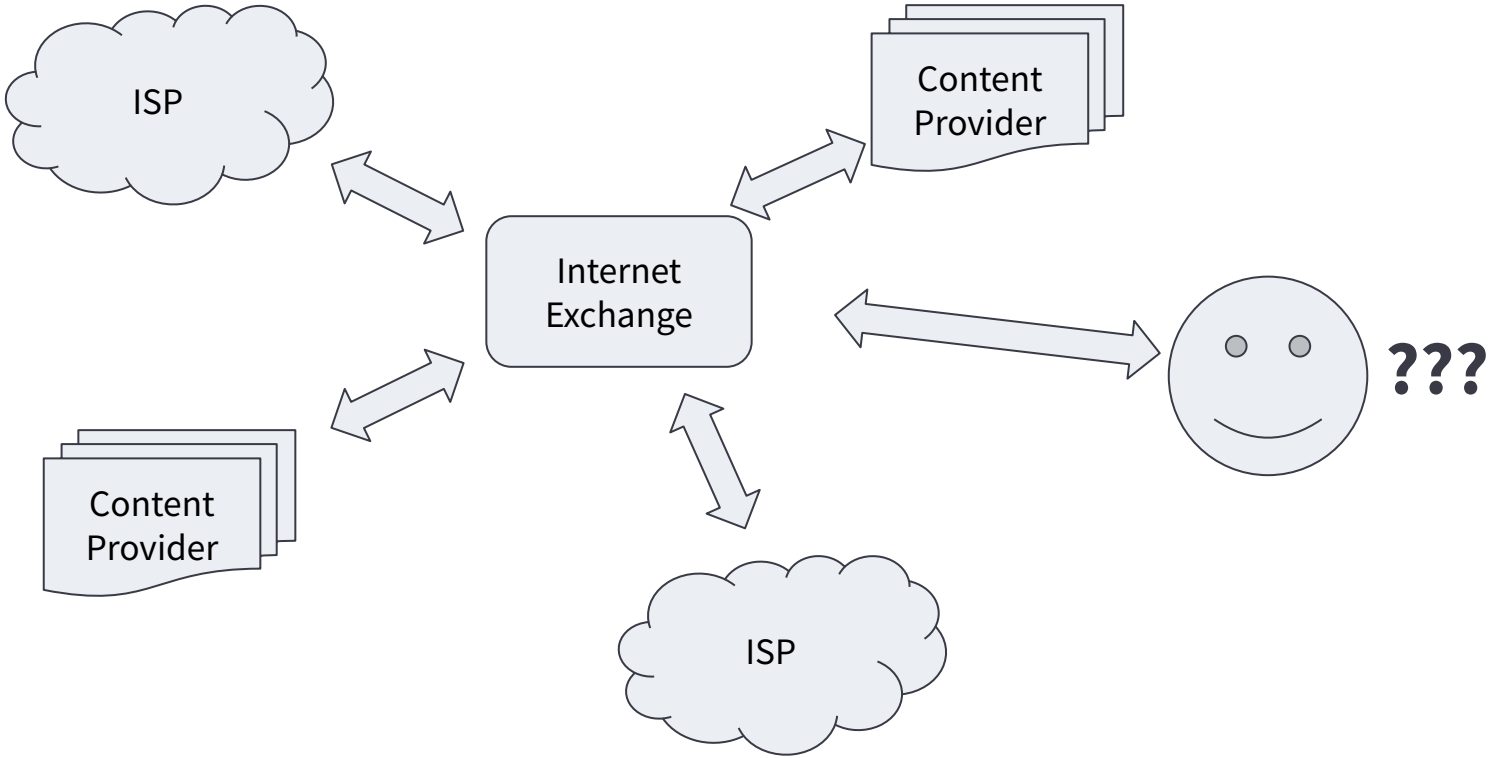


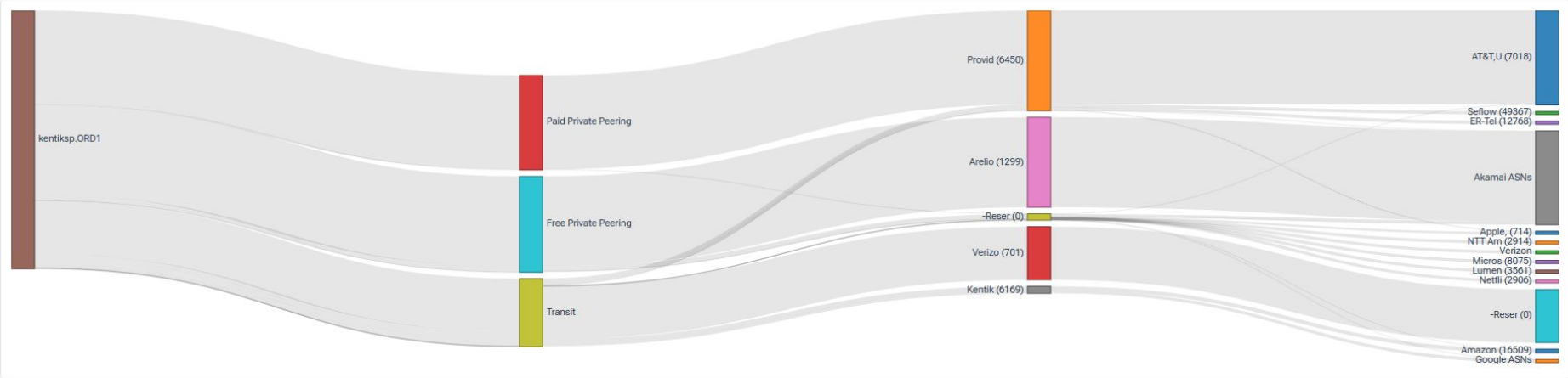





Menu
kentik
Feedback
SYNTHETICS > Test Control Center > 1.1.1.1 tcp ping global agent
Full width
Edit Test
Pause Test
Share
Monday, Dec 7, 18:02 UTC
Critical
ping global agent
Critical
Time Range (UTC)
Last 1h
18:00
18:05
18:10
18:15
18:20
18:25
18:30
18:35
18:40
18:45
18:50
18:55
19:00
Map
Path
Traceroute Explorer
Monday, Dec 7, 18:18 UTC
Number of hops changed
AS16509 - AMAZON-02,US
AS13335 - CLOUDFLARENET,US
AS36351 - SOFTLAYER,US
AS132203 - TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue,CN
AS209141 - CMI-RUSSIA,RU
AS52368 - ZAM LTDA.,CL
AS3549 - LVLT-3549,US
AS14061 - DIGITALOCEAN-ASN,US
AS205399 - HOSTIGGER,TR
AS15830 - EQUINIX-CONNECT-EMEA,GB
AS61098 - EXOSCALE,CH
Hide Options
Collapse ASNs
Agents to show
Show 15 of 31 agents
Highlight nodes
Loss is at least
10
%
Highlight links
Latency is at least
10
ms
Latency is more than expected
Expected latency based on distance between hops and the average from other traces
Manama, Bahrain
Moscow, Russia
Chennai, India
Curico, Chile
London, United Kingdom
Munich, Germany
Salt Lake City, UT, United States
Osaka, Japan
Frankfurt, Germany
Los Angeles, CA, United States
San Francisco, CA, United States
San Francisco, CA, United States
Austin, TX, United States
New York, United States
Frankfurt, Germany
1.1.1.1

What is an IX (Internet Exchange) point?

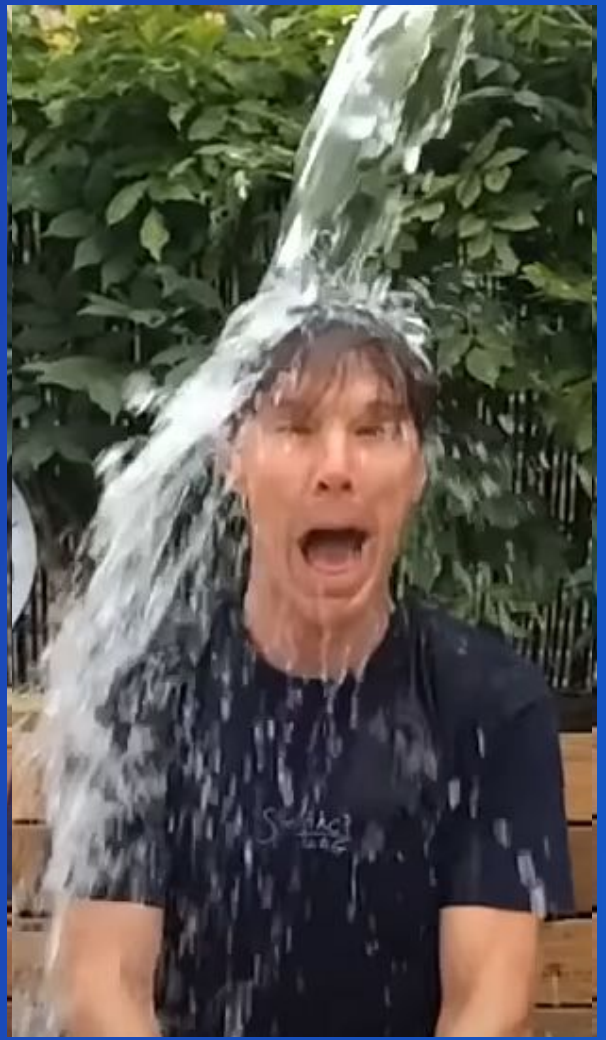




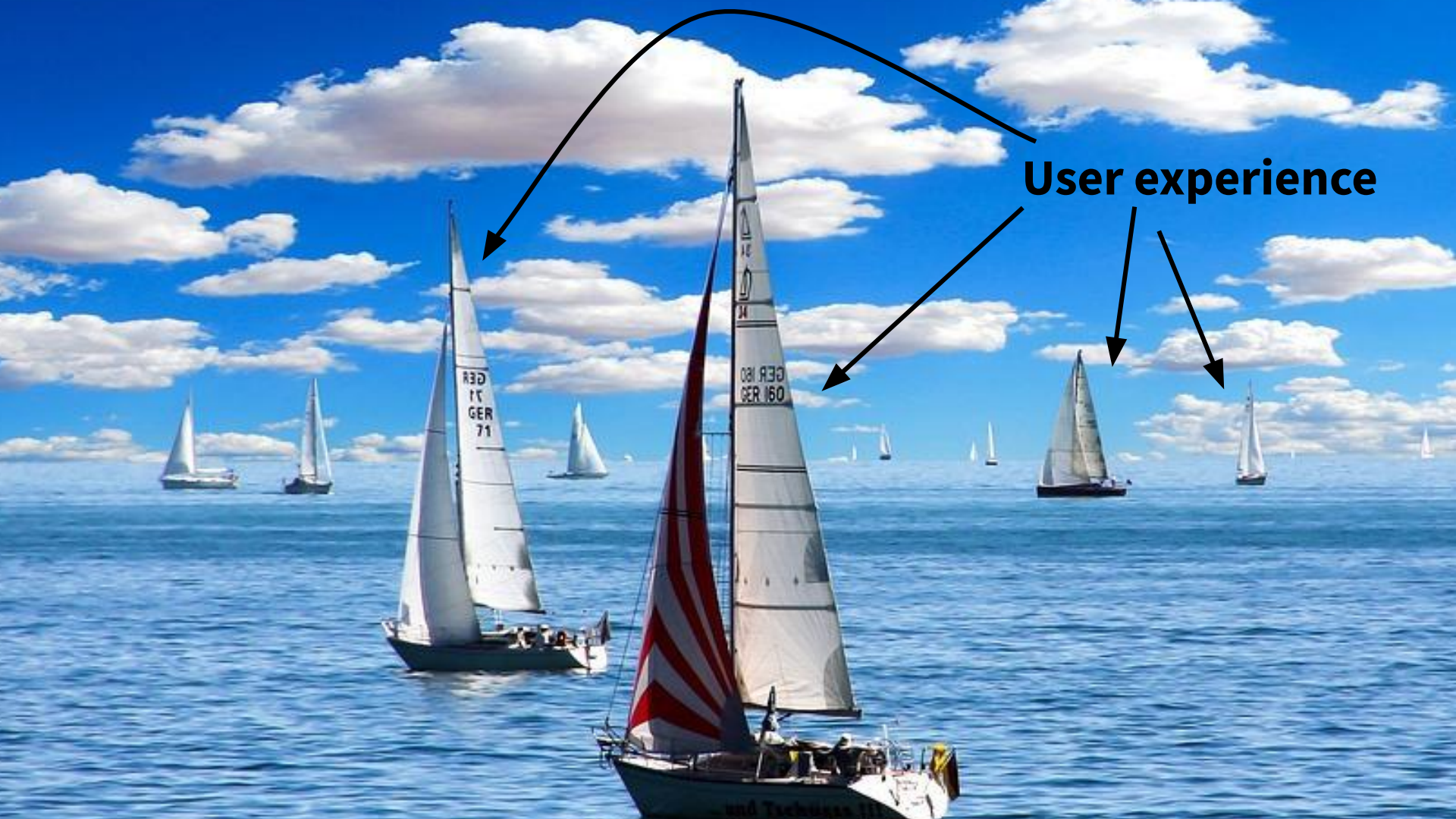
Potential Peers

Time Range: Last 30 Days

Peer Name	AS Name	Shared Facilities	Average Traffic (Gbps)	
AT&T US - 7018	7018 - AT&T,US		1.20	×
Akamai,US (16625)	16625 - Akamai,US		1.19	×
Nathan Sales0	0 - -Reserved AS-,ZZ		0.68	×



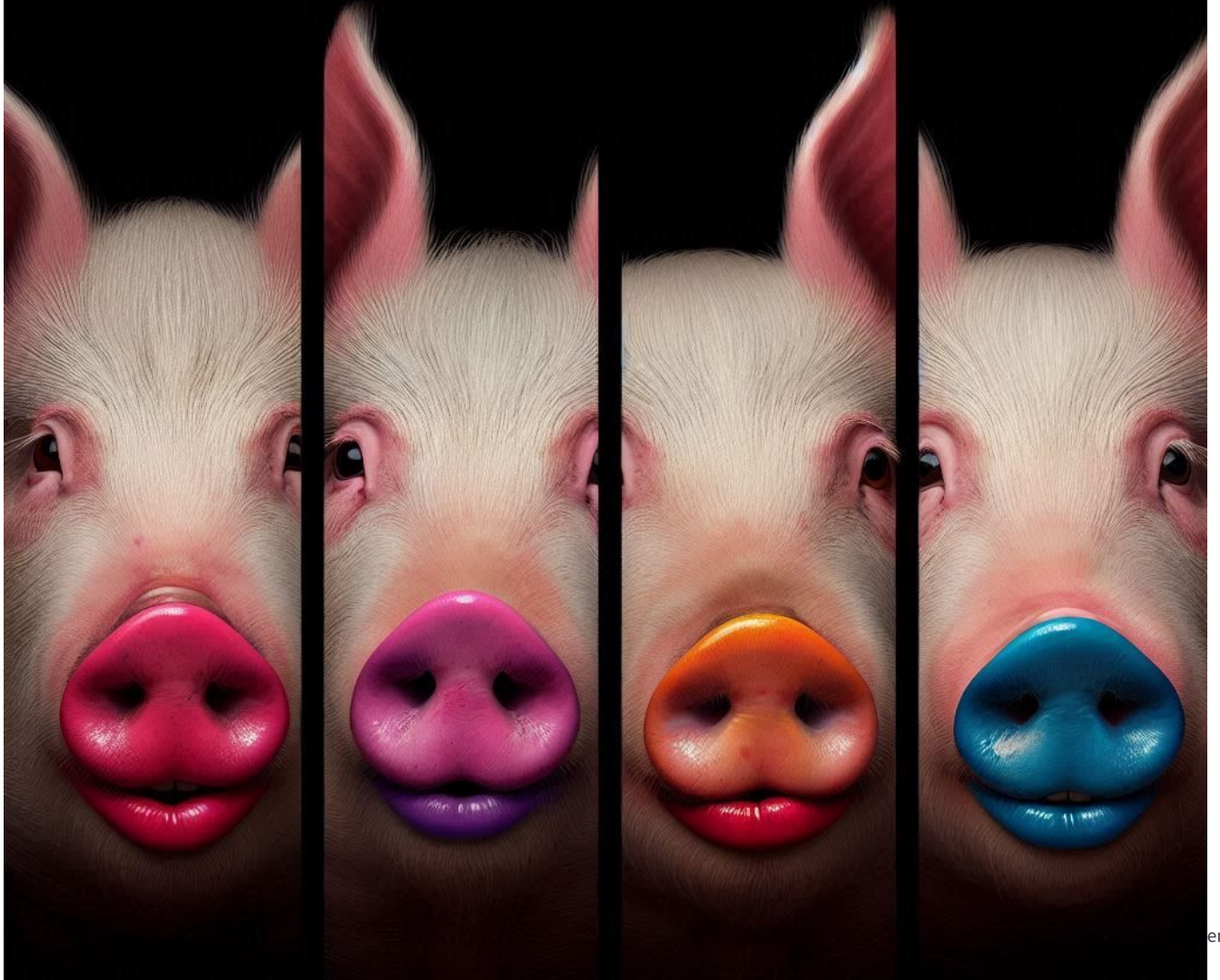
Network Observability is NOT


User experience

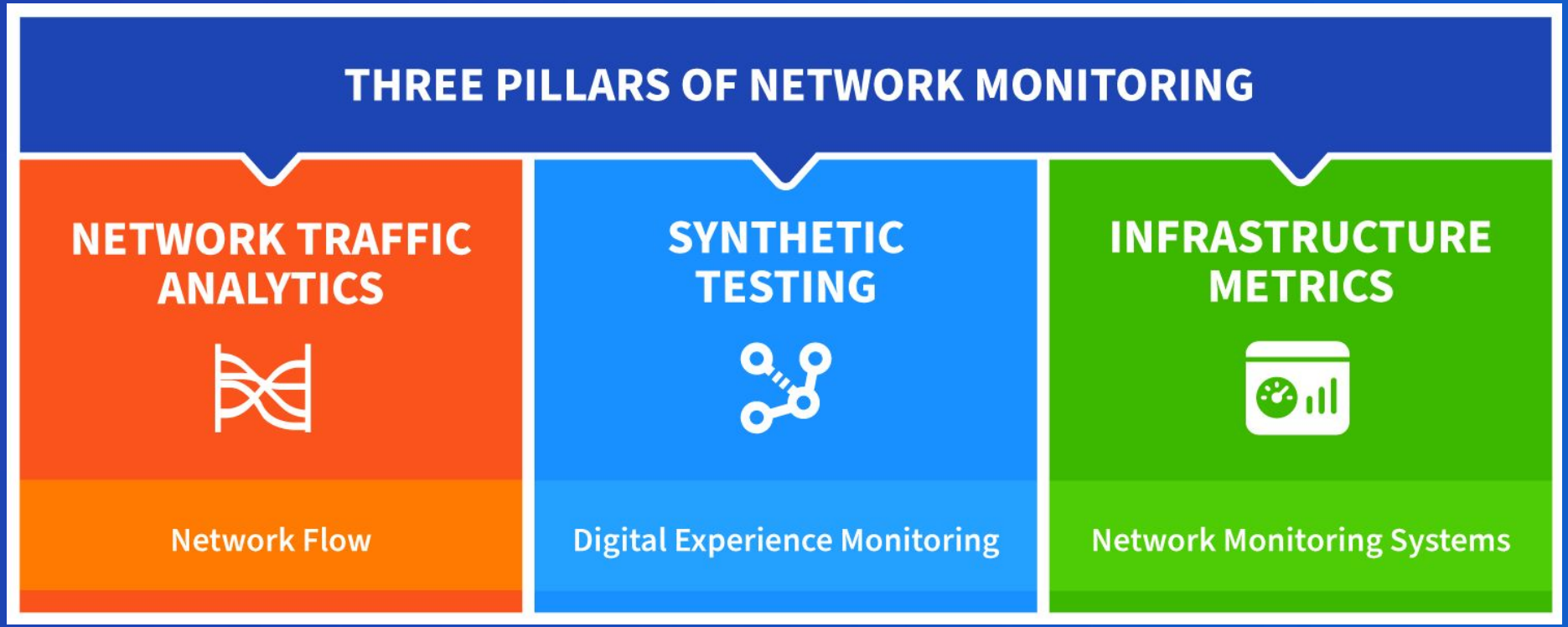
Observability / Monitoring

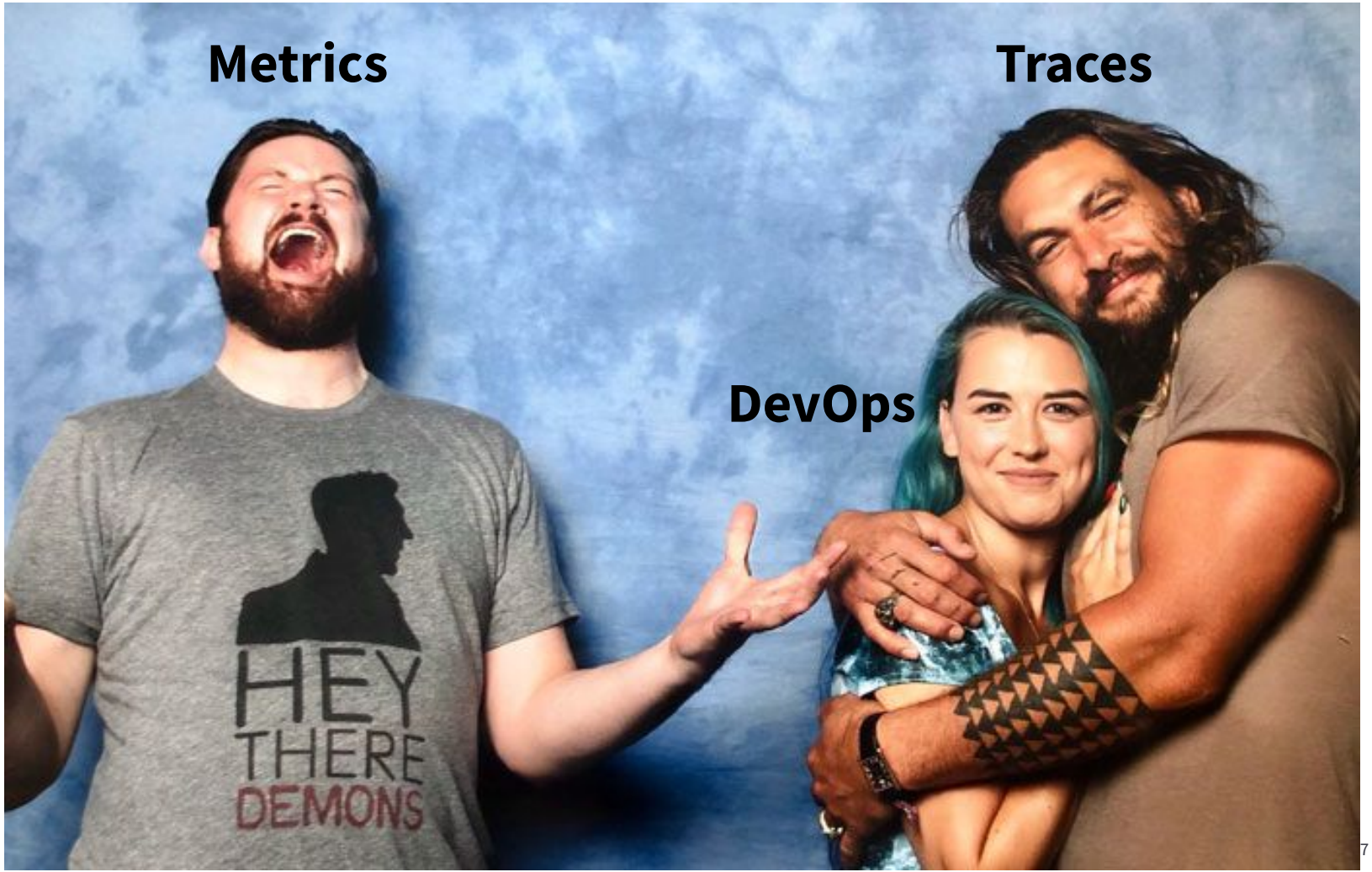
Management

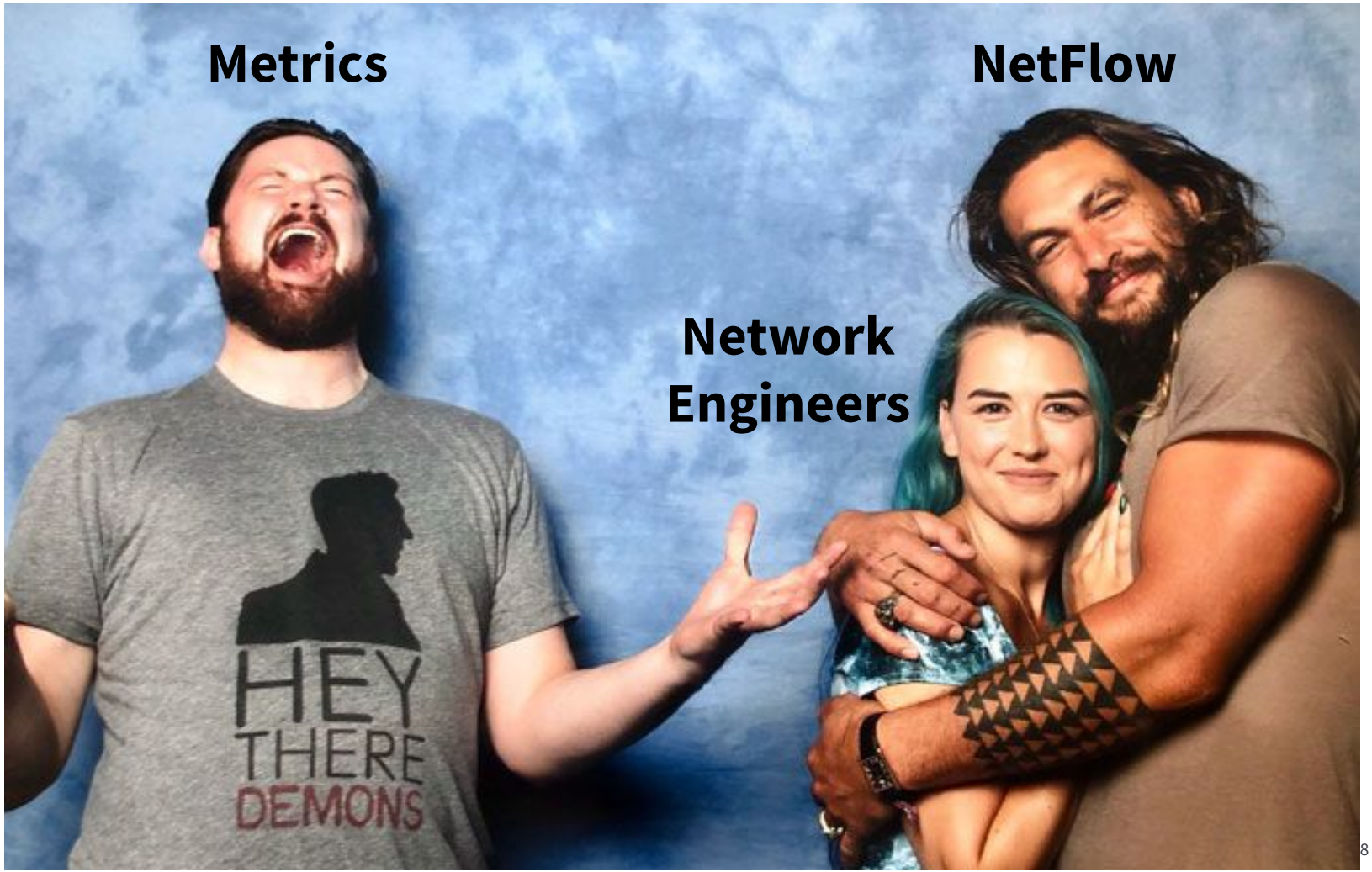

Anyone who says otherwise
is selling something



Network Observability Pillars

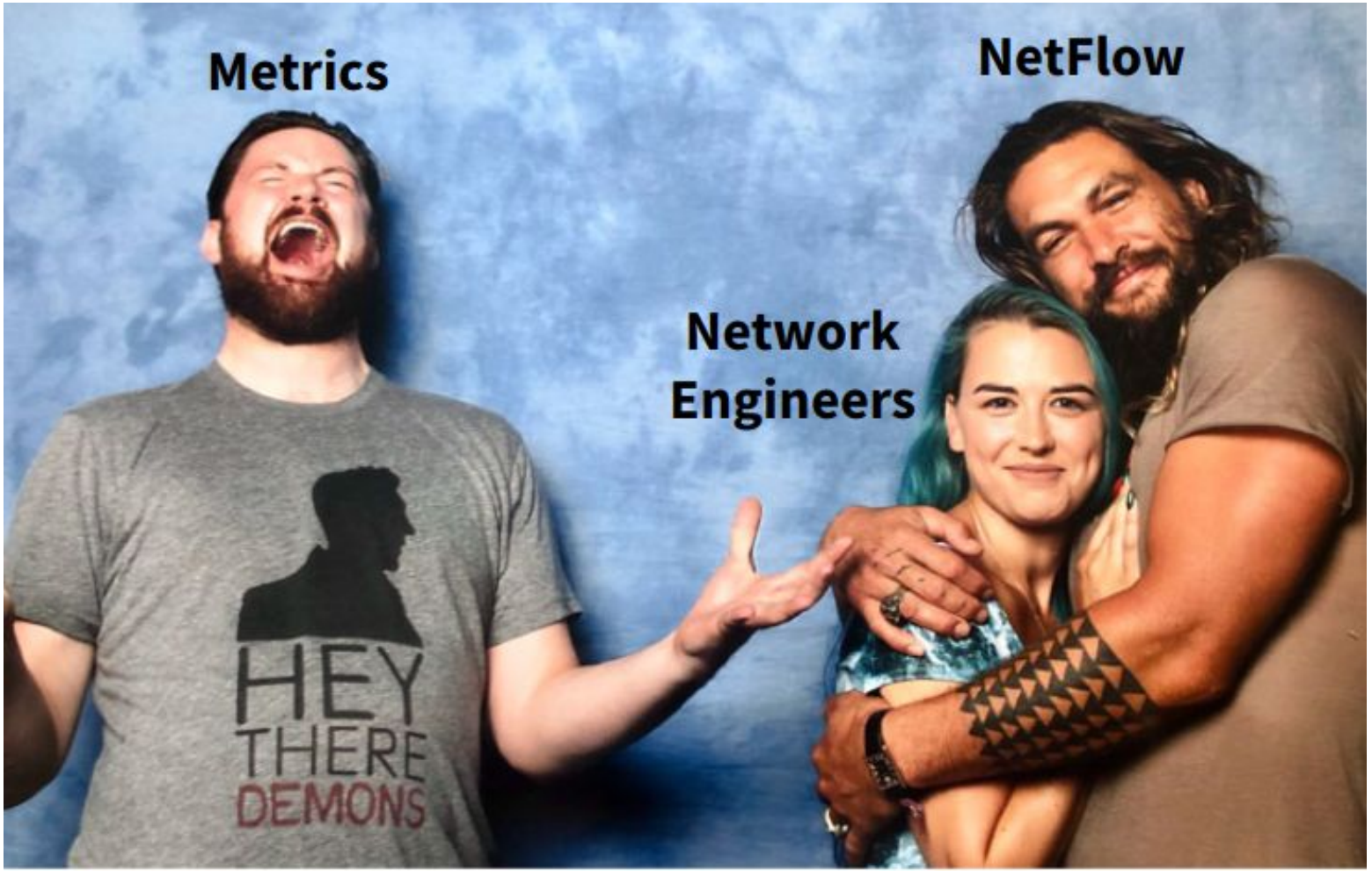



Metrics
Traces
DevOps
HEY
THERE
DEMONS

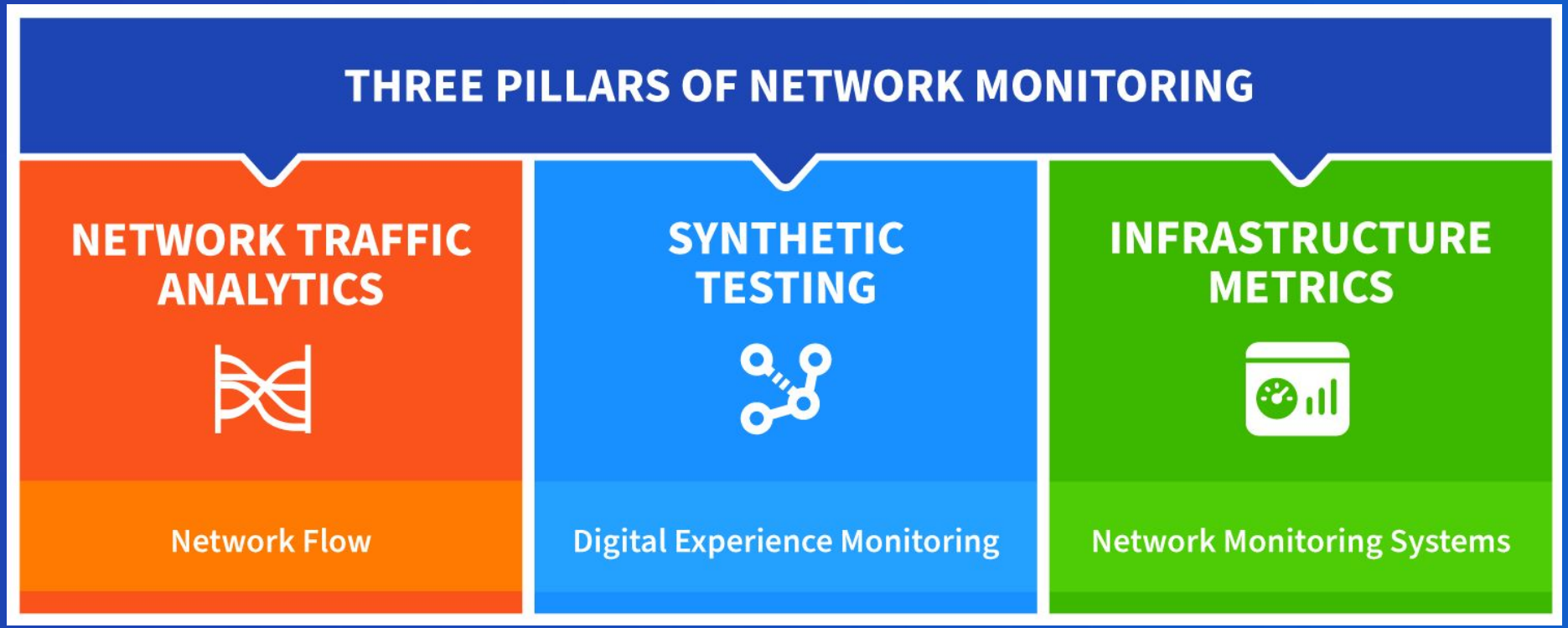

Metrics
NetFlow
Network
Engineers
HEY
THERE
DEMONS

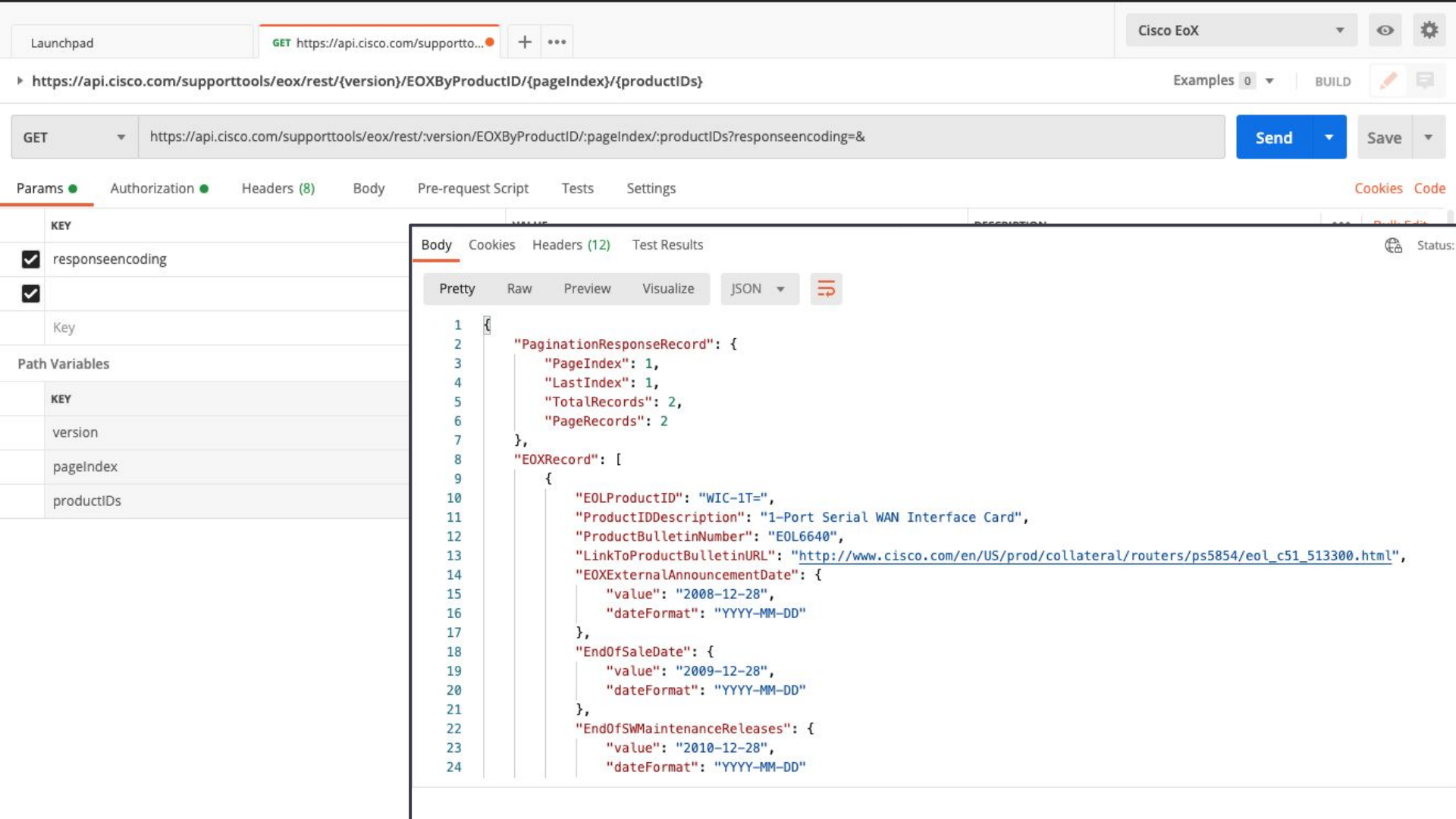
Netflow Options

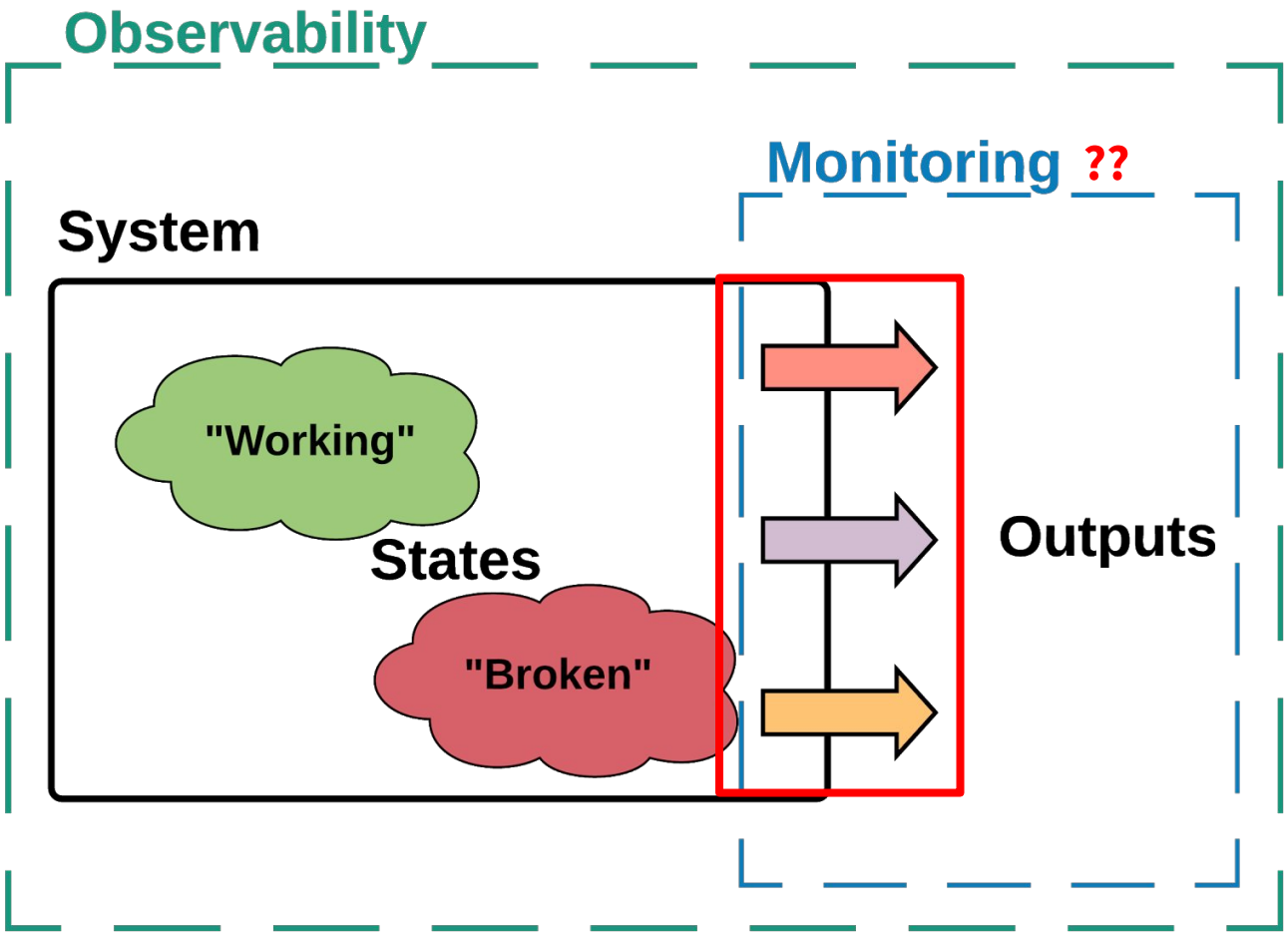
- By source / destination
- By port
- By protocol
- By application
- By geography (based on IP)

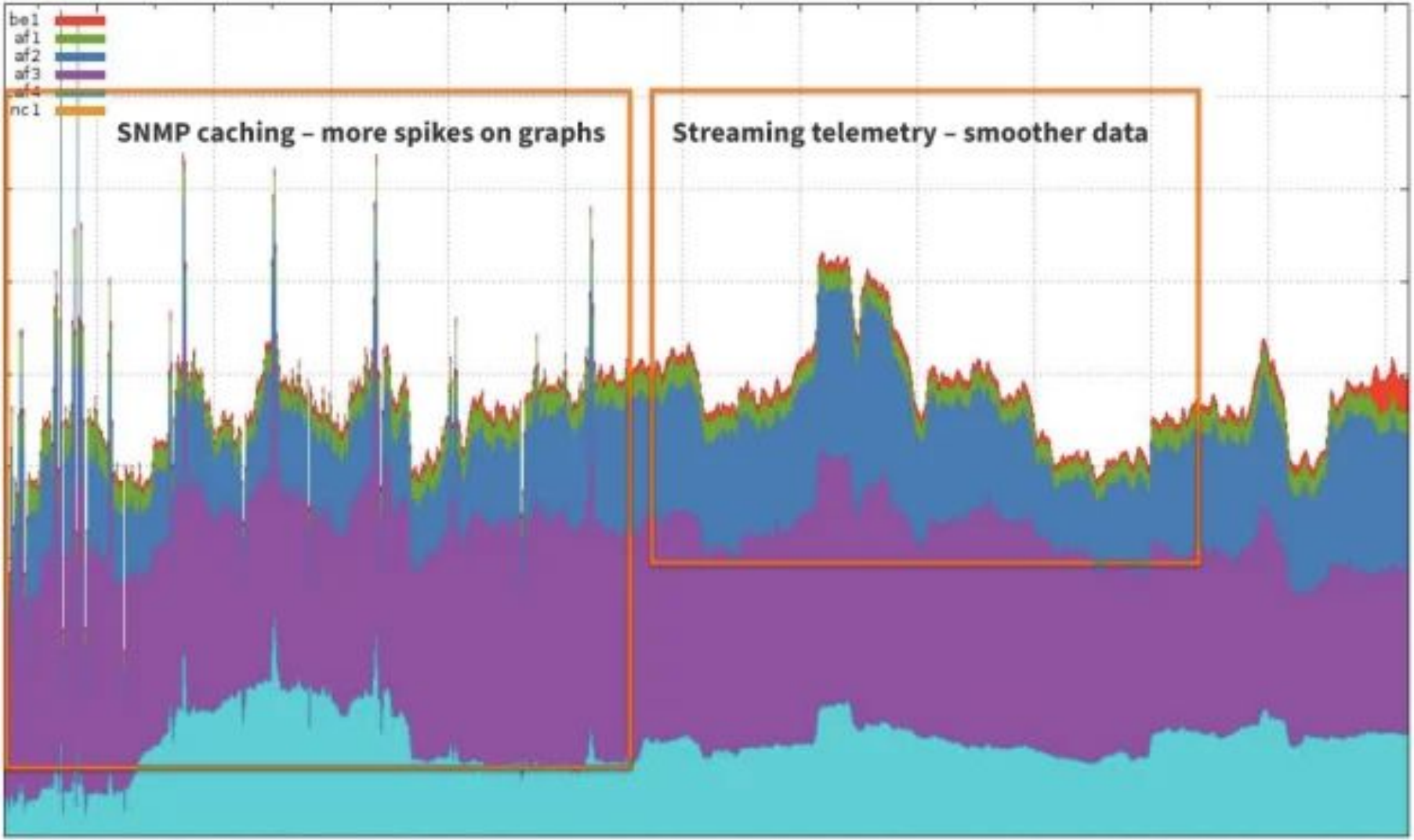


Network Observability Pillars

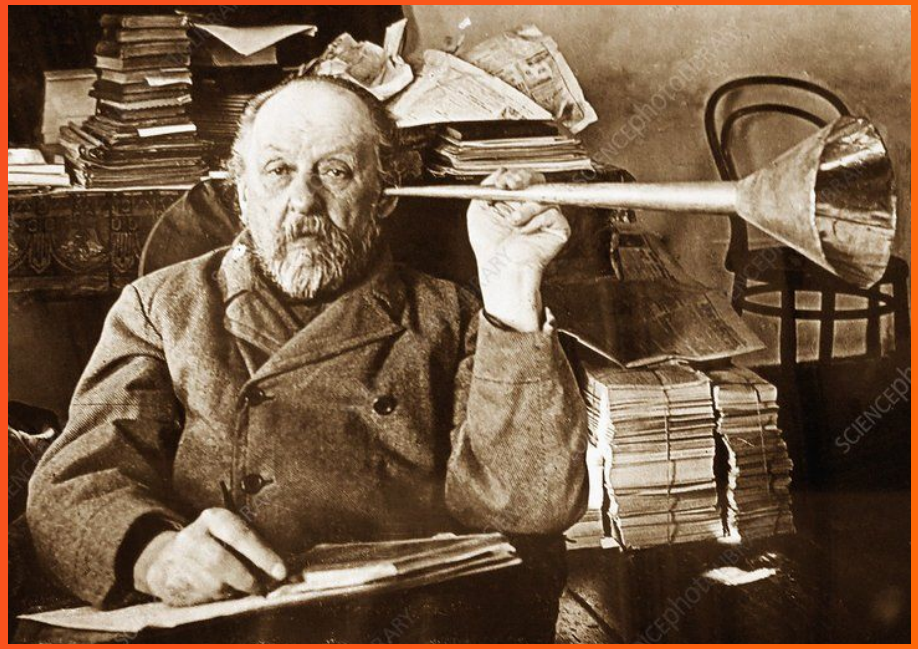



Launchpad
GET https://api.cisco.com/supportto...
Cisco EoX
https://api.cisco.com/supporttools/eox/rest/{version}/EOXByProductID/{pageIndex}/{productIDs}
Examples 0
BUILD
GET
https://api.cisco.com/supporttools/eox/rest/:version/EOXByProductID/:pageIndex/:productIDs?responseencoding=&
Send
Save
Params
Authorization
Headers (8)
Body
Pre-request Script
Tests
Settings
Cookies
Code
KEY
responseencoding
Key
Path Variables
KEY
version
pageIndex
productIDs
Body
Cookies
Headers (12)
Test Results
Status:
Pretty
Raw
Preview
Visualize
JSON
{
"PaginationResponseRecord": {
"PageIndex": 1,
"LastIndex": 1,
"TotalRecords": 2,
"PageRecords": 2
},
"EOXRecord": [
{
"EOLProductID": "WIC-1T=",
"ProductIDDescription": "1-Port Serial WAN Interface Card",
"ProductBulletinNumber": "EOL6640",
"LinkToProductBulletinURL": "http://www.cisco.com/en/US/prod/collateral/routers/ps5854/eol_c51_513300.html",
"EOXExternalAnnouncementDate": {
"value": "2008-12-28",
"dateFormat": "YYYY-MM-DD"
},
"EndOfSaleDate": {
"value": "2009-12-28",
"dateFormat": "YYYY-MM-DD"
},
"EndOfSWMaintenanceReleases": {
"value": "2010-12-28",
"dateFormat": "YYYY-MM-DD"




be1
af1
af2
af3
af4
nc1
SNMP caching – more spikes on graphs
Streaming telemetry – smoother data

I want to hear from you!



@LeonAdato

or

leon@kentik.com

YOU MADE IT!!!

Get our famous TCP/IP cap by scanning the QR code below:

Are you  ?

I’m ready for your questions!

@LeonAdato

YOU MADE IT!!!

Get our famous TCP/IP cap by scanning the QR code below:

Spare slides

When I call a
network design "robust"
instead of really good

Blahblah

Let's add a little nuance

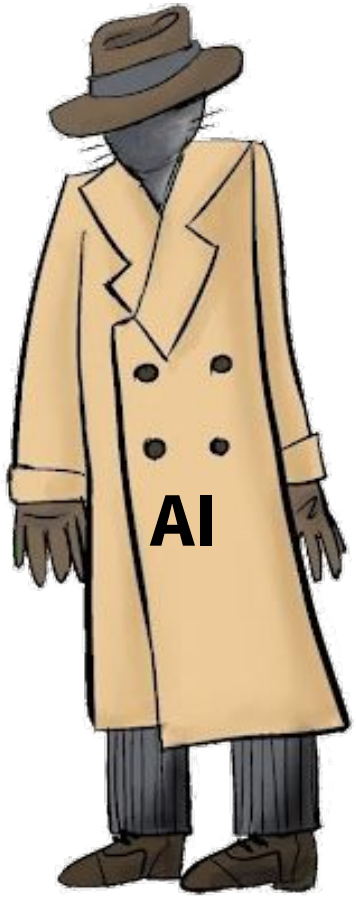
Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals
  (latency, traffic, errors, saturation)

Let's add a little nuance

Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals



Let's add a little nuance

Observability

- Un-Known Unknowns
- High cardinality
- Correlation baked-in
- Golden signals

Designed by M. Scharlock

