POLYGRAPH.io

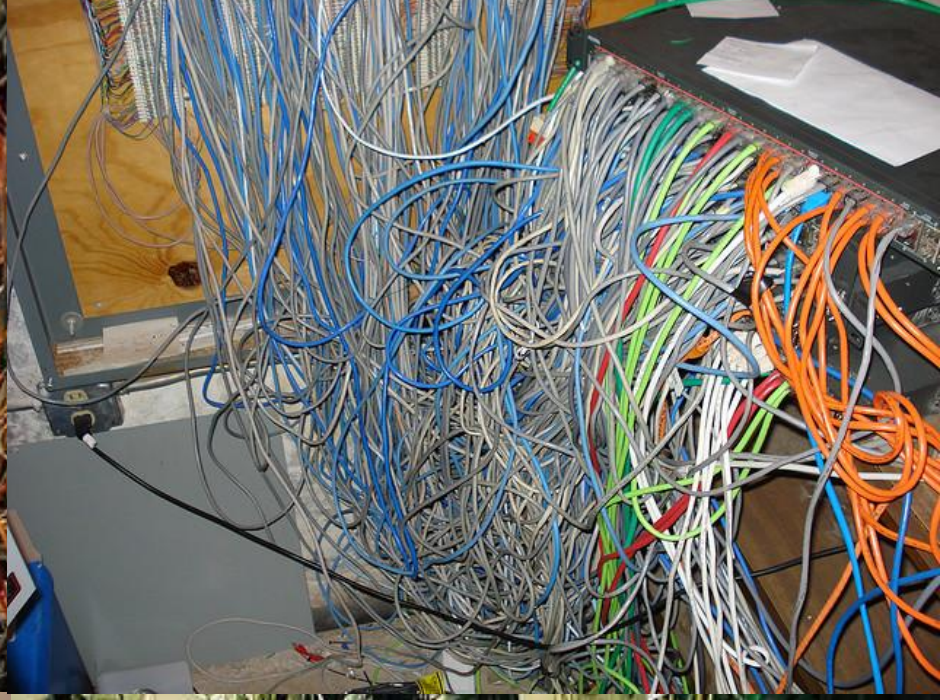
Network Visibility as a Service

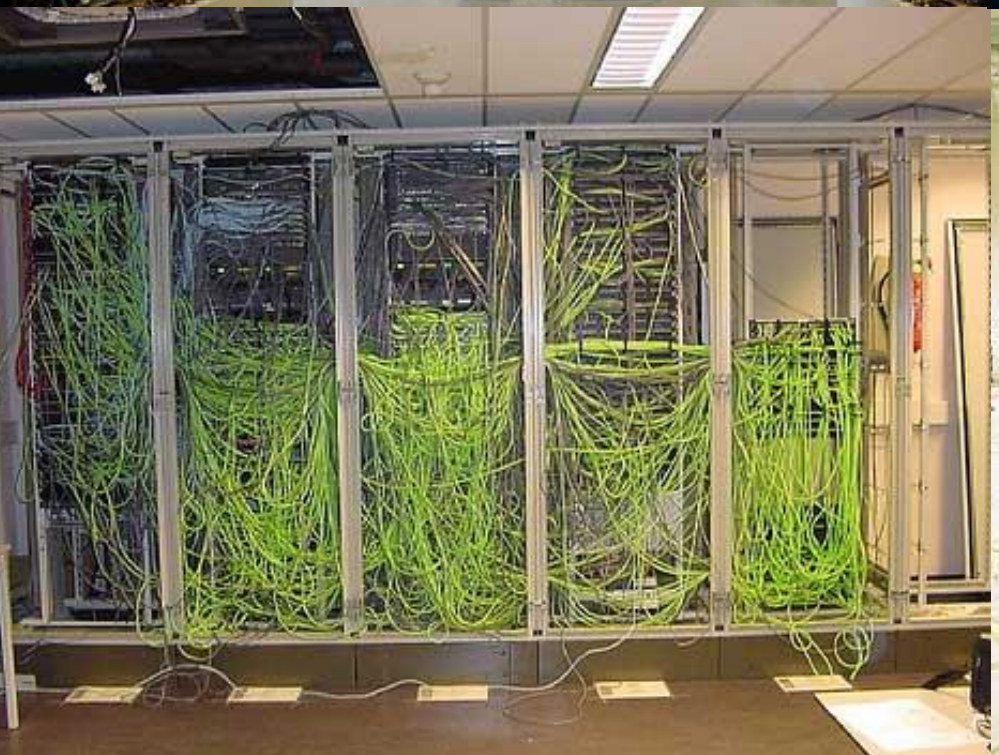
Josep Sanjuas, co-founder & CEO
jsanjuas@polygraph.io

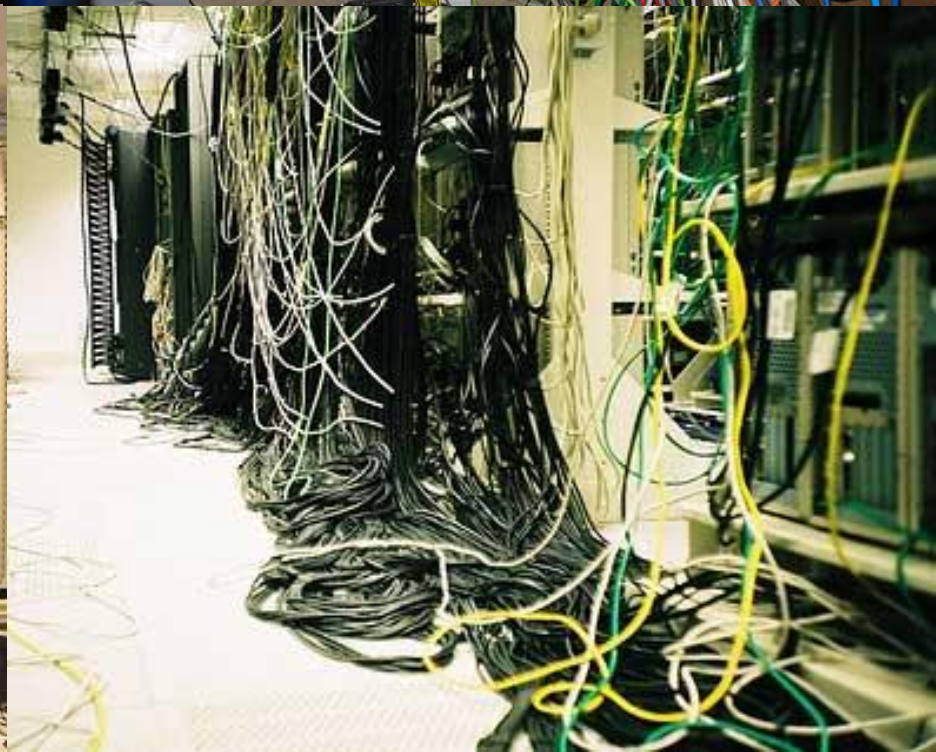
POLYGRAPH.io

Companies depend on Networks

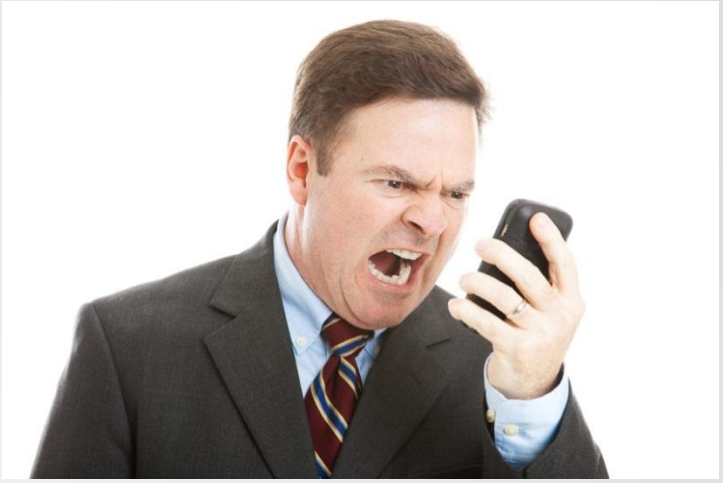
e-mail, databases, shared folders, VoIP, cloud...



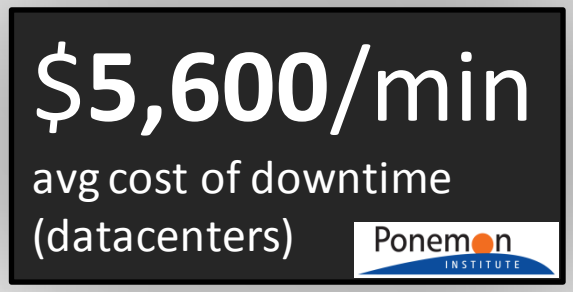




Downtime



Network Downtime equals Cost



“average loss per company > $3.5M/year”

Network Visibility

To properly manage a complex system, you need to

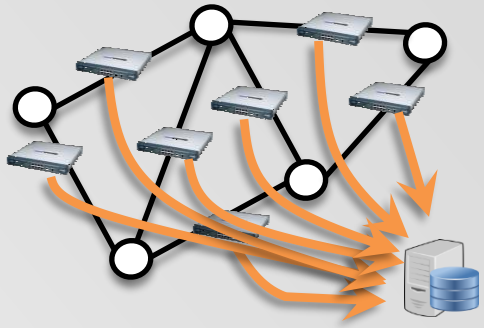
see what happens inside it

Why Network Visibility?

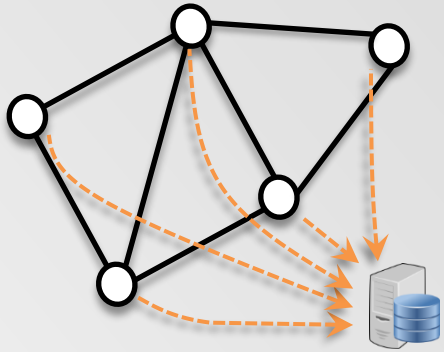
- Identify congested links
- Detect unwanted applications
- Locate sources of congestion / bandwidth abuse
- Analyze performance issues
- Troubleshoot network malfunctions
- Security: detect attacks & anomalies
- Forensics: incident analysis
- Network capacity planning

Two Families of Visibility Products

- Deep Packet Inspection
  - Brute-force approach: inspect all packets
  - High visibility at a **very high cost**
  - Full network coverage often **cost-ineffective**



- Flow-based (NetFlow, IPFIX, sFlow..)
  - Use traffic statistics exported by routers
  - Lower cost but **lower visibility**

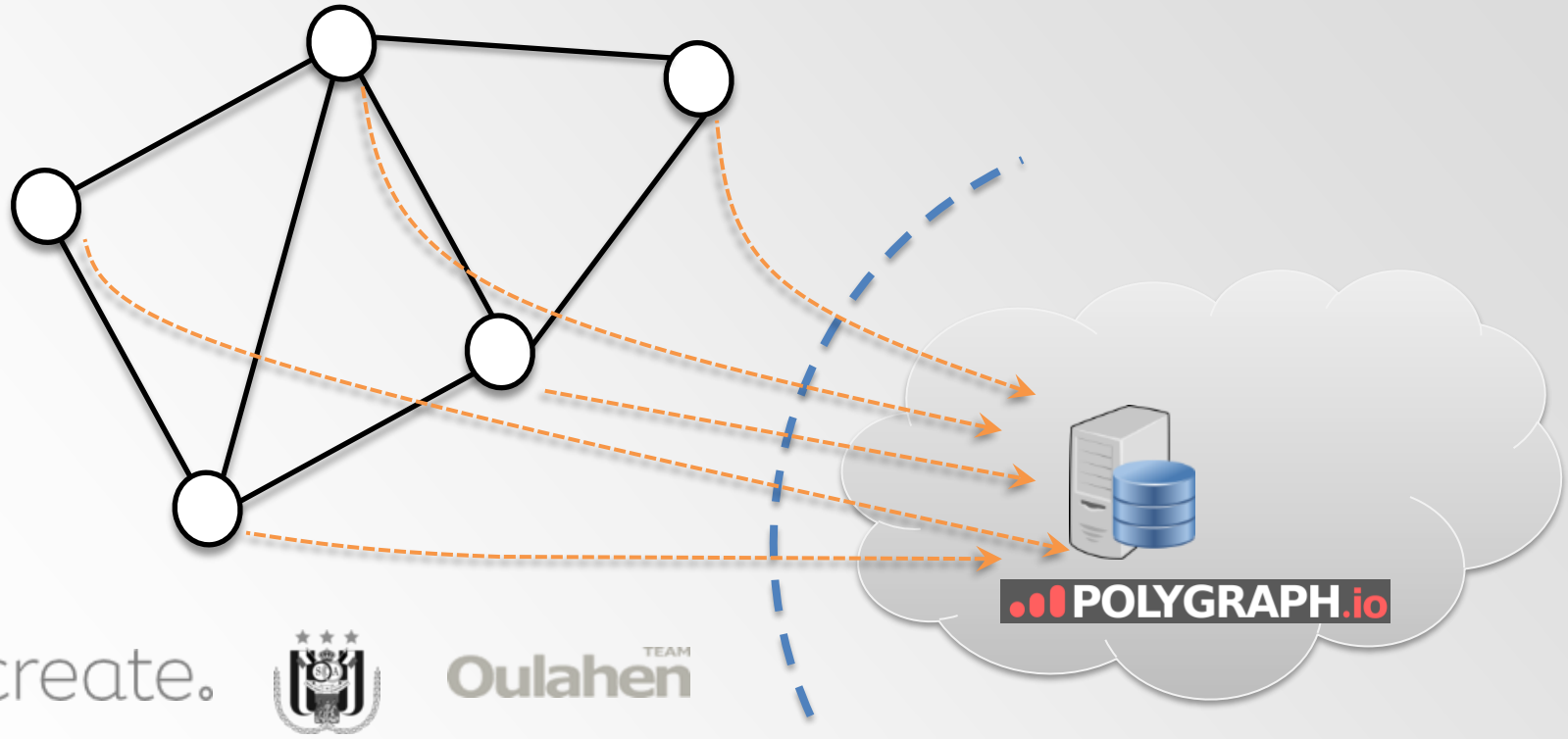


POLYGRAH.io - Overview

- Flow based: instant deployment (SaaS)
- Enhanced visibility: “NetFlow on steroids”
- Aims for the best user experience


Polygraph Demo
from LAN
to LAN
12-04-2014 - 12-04-2014
All applications
bits/s
Top 10
jsanjuas@gmail.com
APPLICATIONS
PROTOCOLS
TOP N
AUTOZOOM
GEOLOCATION
ANOMALIES
FLOWS
REPORTS
All applications
World wide web
Direct Download
Services and Others
DNS
Streaming and P2P TV
File transfer
Encrypted and Tunneling
Games
File Sharing P2P
Instant Messaging
Mail
Voice and Video over IP
Top Addresses - from LAN
Source
Destina
111.79.150.60
111.79.192.166
111.79.55.227
111.79.201.151
111.79.151.181
111.79.181.94
111.79.156.140
111.79.9.113
111.79.170.89
111.79.64.10
140.181.13
144.150.18
236.222.17
67.149.223
157.22.230
179.238.21
70.226.102
108.66.186
152.207.21
152.3.87.215
6 Mb/s
4 Mb/s
2 Mb/s
0 b/s
2 Mb/s
12-04-2014 04:20 - 12-04-2014 09:50
to LAN
Destination
DNS
LLMNR
MulticastDNS
245.156.220.134
111.79.68.236
111.79.190.244
111.79.97.46
111.79.127.137
111.79.59.128
111.79.41.109
111.79.61.35
111.79.64.122
111.79.2.86
111.79.156.75
0 b/s
5 Mb/s
10 Mb/s
12-04-2014 04:20 - 12-04-2014 09:50
Top Autonomous Systems
Src from LAN
Dst from LAN
Src to LAN
Dst to LAN
197518
53064
24120
47696
21753
Unknown
17061
45942
8932
14125
30407
64989
3482
24120
7029
27102
41895
50 Mb/s
0 b/s
50 Mb/s
12-04-2014 04:20 - 12-04-2014 09:50
Top Ports
Src from LAN
Dst from LAN
Src to LAN
Dst to LAN
80 TCP
3389 TCP
443 TCP
62348 UDP
1194 UDP
5060 UDP
53398 UDP
22 TCP
6970 UDP
53839 UDP
22 TCP
443 TCP
59350 TCP
4550 TCP
5060 UDP
993 TCP
20 TCP
56615 TCP
4341 UDP
20 Mb/s
10 Mb/s
0 b/s
10 Mb/s
20 Mb/s
30 Mb/s
12-04-2014 04:20 - 12-04-2014 09:50
Start: 12-04-2014 04:20
End: 12-04-2014 09:50
Sat 12
03 AM
06 AM
09 AM
12 PM
03 PM
06 PM
09 PM
https://demo.polygraph.io/#

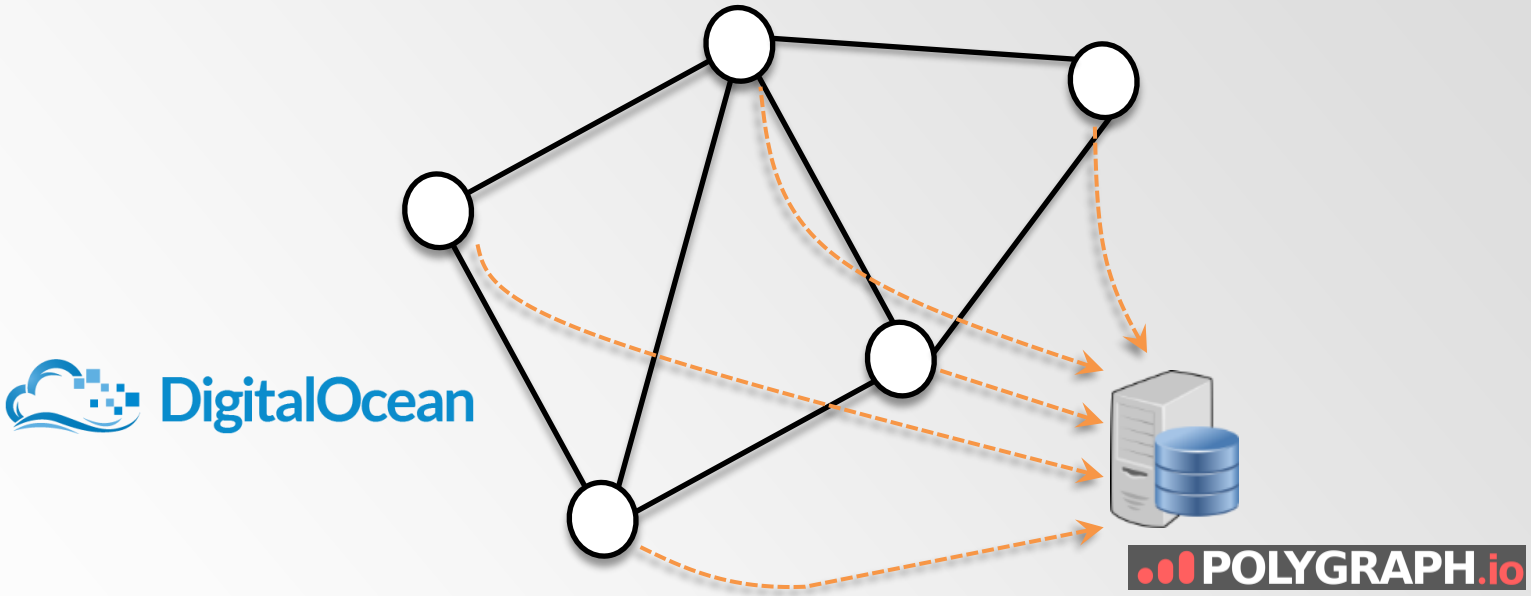
Deployment Models: SaaS



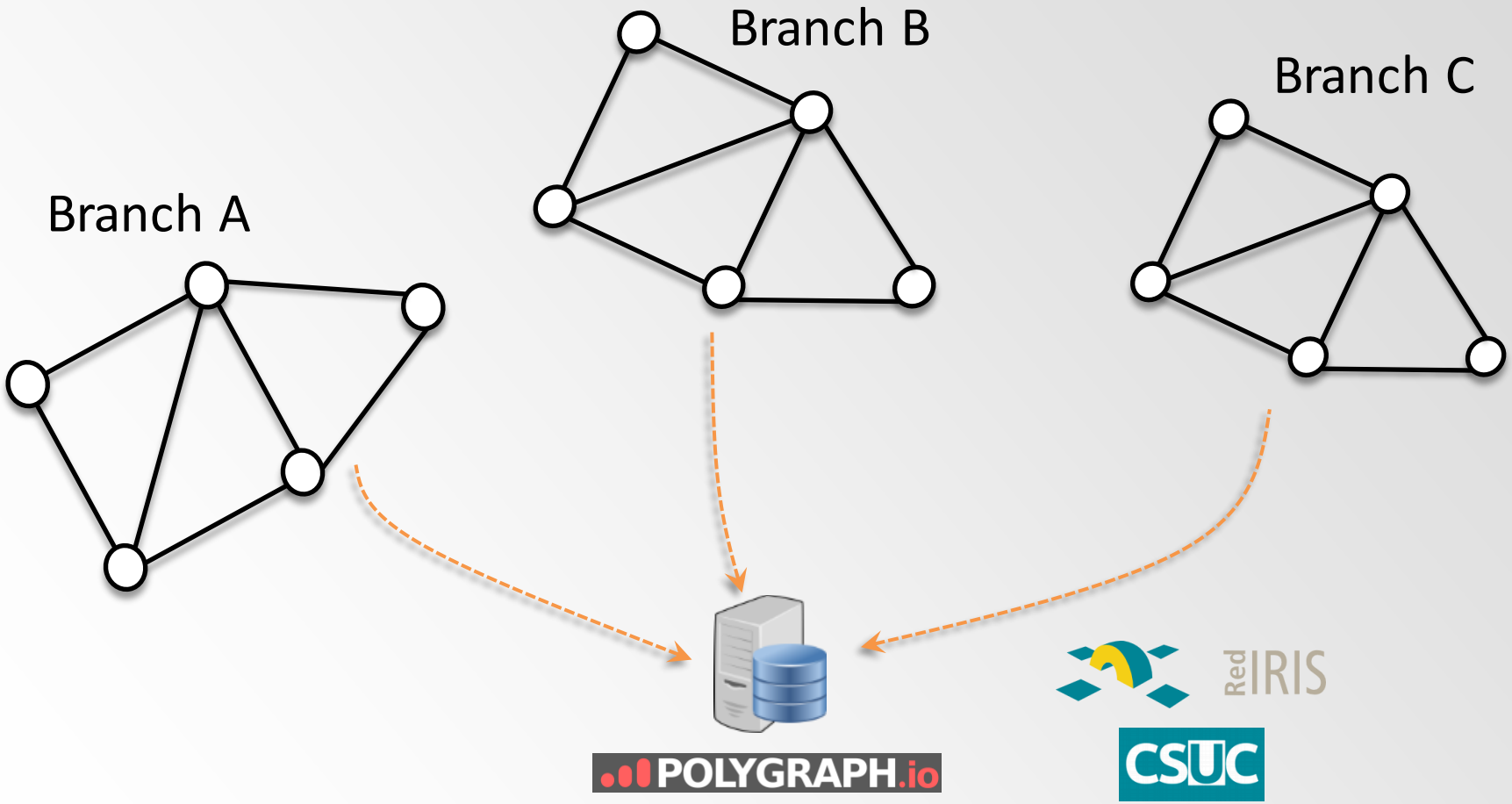
create.

Oulahen TEAM

Deployment Models: Enterprise



Enterprise: Multi-Tenancy



POLYGRAH.io - Technology

- **High visibility** at the cost of **software solutions**

  best visibility-to-cost ratio

- How? **NetFlow** + **artificial intelligence**

  NetFlow on steroids: application identification, SSL domain ID, attack & anomaly detection capabilities

History

- Seed: collaboration UPC + CSUC
- Initial use case: network operation aid in a multi-tenant enviornment
- Draws on tech from research world
- 2 years ago: going comercial
- Spin-off of UPC-BarcelonaTech

Application Identification

- Issue: in flow-based monitoring, it is tough to identify applications!
- Port-based identification is not accurate
  - many applications no longer use well-known ports
- Our solution: **heuristic identification via machine-learning**

Application Identification (2)

1. Capture network traffic in high-volume links
2. Collect NetFlow
3. Combine both inputs
4. Figure out heuristics automatically: machine learning
5. Apply found heuristics to all customers

Web Domain Identification

- Web domains are not included in flow-level data
  - only IP addresses, ports, protocol, bytes…
- Other products…
  - .. expect you to manually maintain mappings, e.g., 1.2.3.0/24 is Facebook
- POLYGRAPH.io:
  - does whatever it takes to figure out web services!
  - check AS numbers, DNS, even *actively connections*

Attack Detection

- Problems of other products:
  - Attack detection often based on “patterns”
  - Often hard to tell why an alarm fired
  - Huge number of false positives
  - What flows are part of an anomaly?

Attack Detection (2)

- Our solution:
  - Behavioral analysis + continuous learning
- Continuous learning:
  - Keep a record of what is *normal*
- Behavioral analysis:
  - Flag clusters of connections that seem related
- Combination:
  - connections from * to 1.2.3.4:80 are normal
  - connections from * to 4.5.6.7:80 are anomalous!

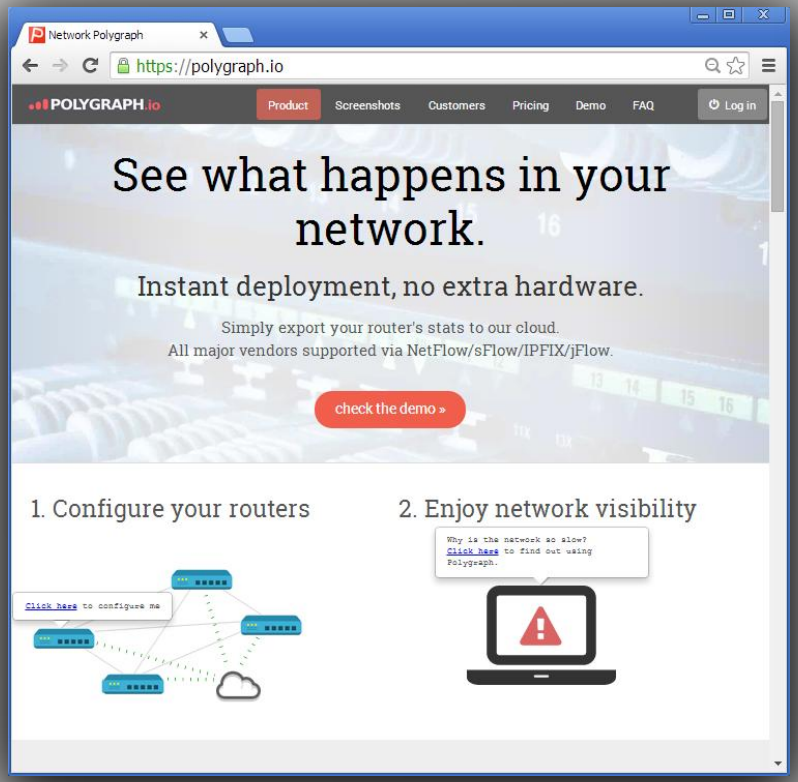
Pre-Computing & Data Aggregation

- Other products take *forever* to get results
  - e.g., “top talkers for last month”? 10 min
  - severily limits their usefulness: can’t drill down
- Our solution:
  - Pre-compute many results at various time scales
- Target outcome:
  - Be very fast for typical use cases

Our Technology: Summary

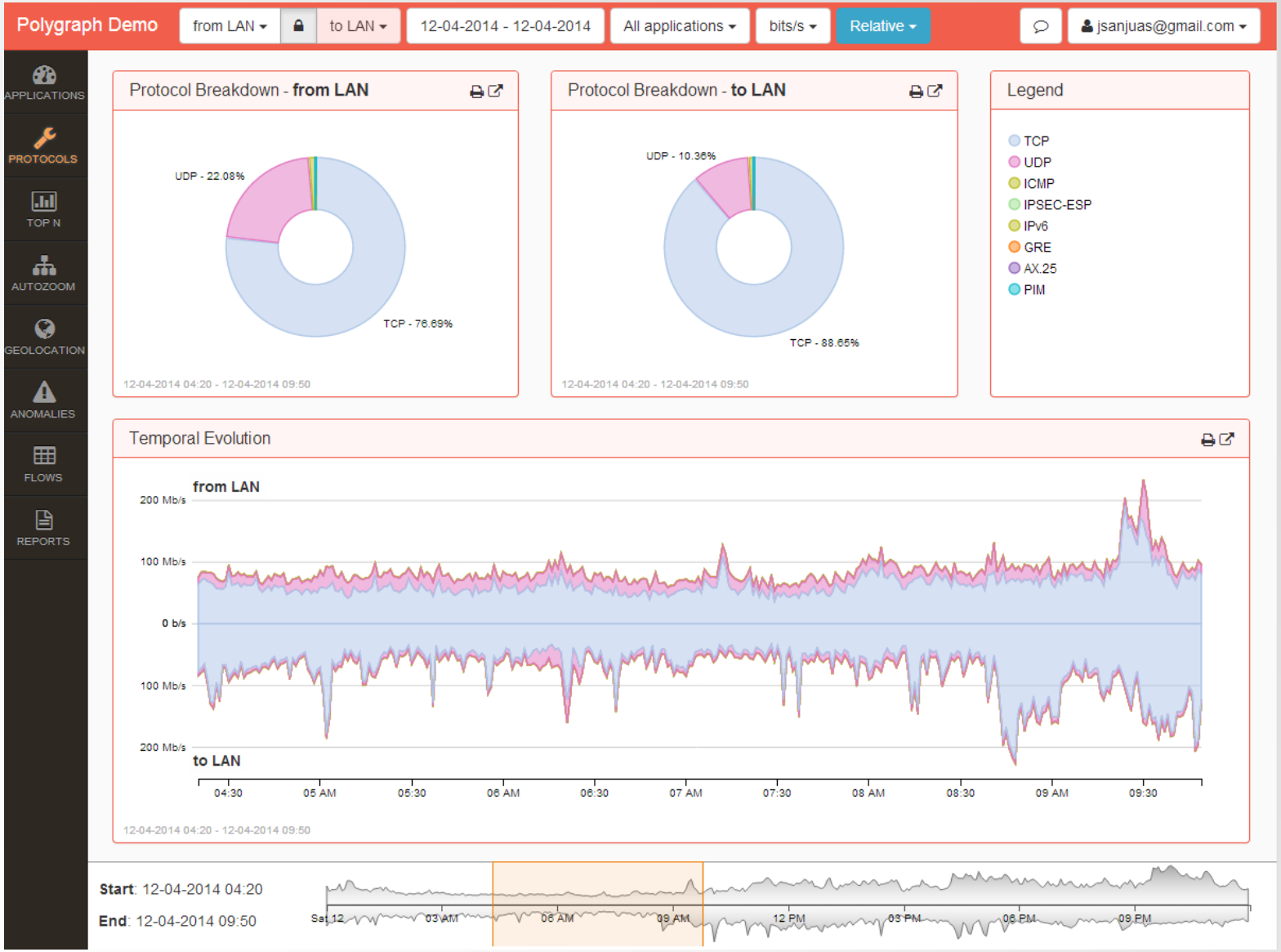
- Identification of applications & domains
  - Heuristics figured out by machine learning
  - Automatically identify web domains
- Attack detection
  - Behavioral analysis + learning about the network
- Data pre-aggregation
  - Resolve common queries *fast*

Website + On-Line Demo



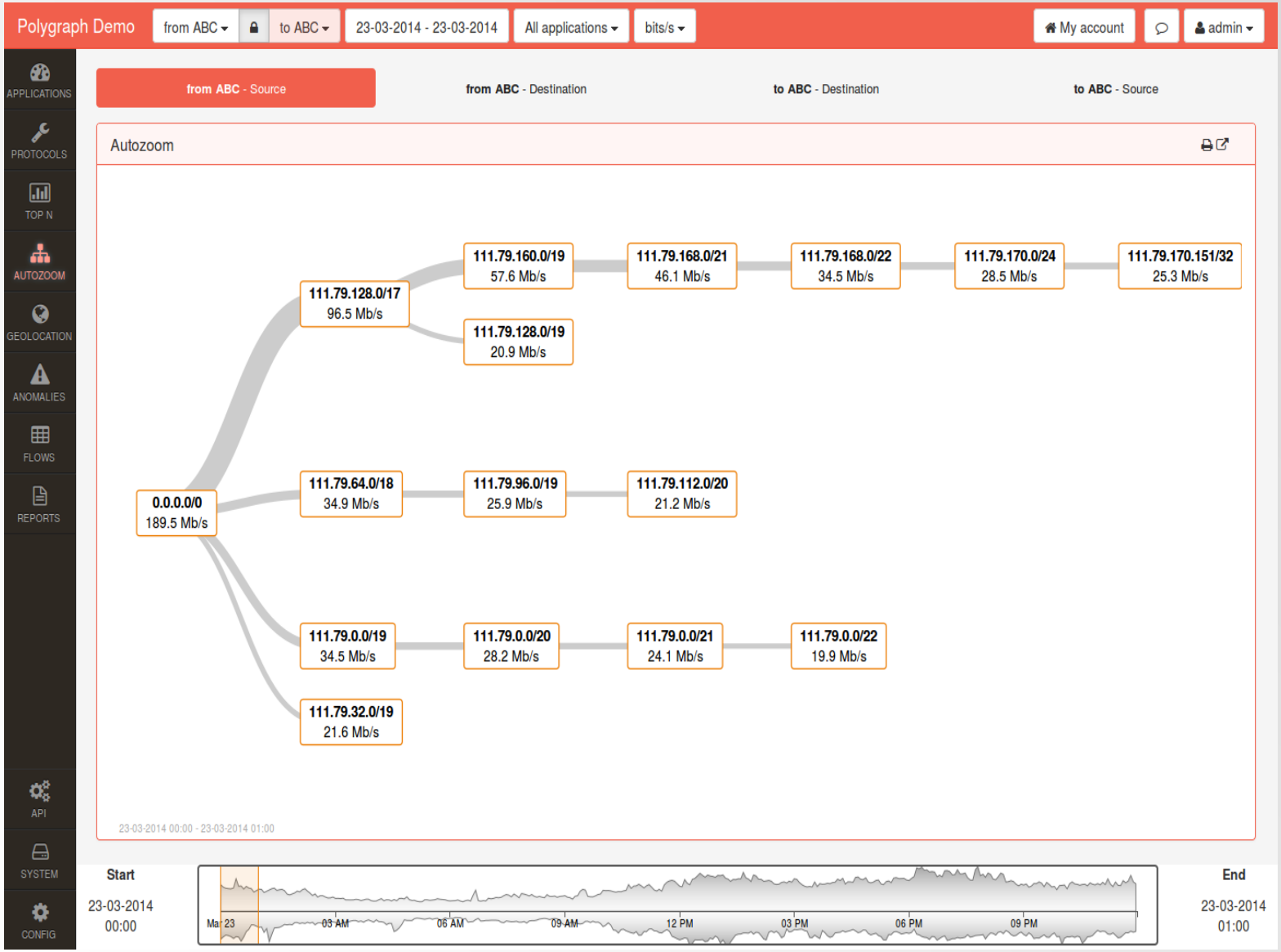
https://polygraph.io

traffic volume, breakdown by application

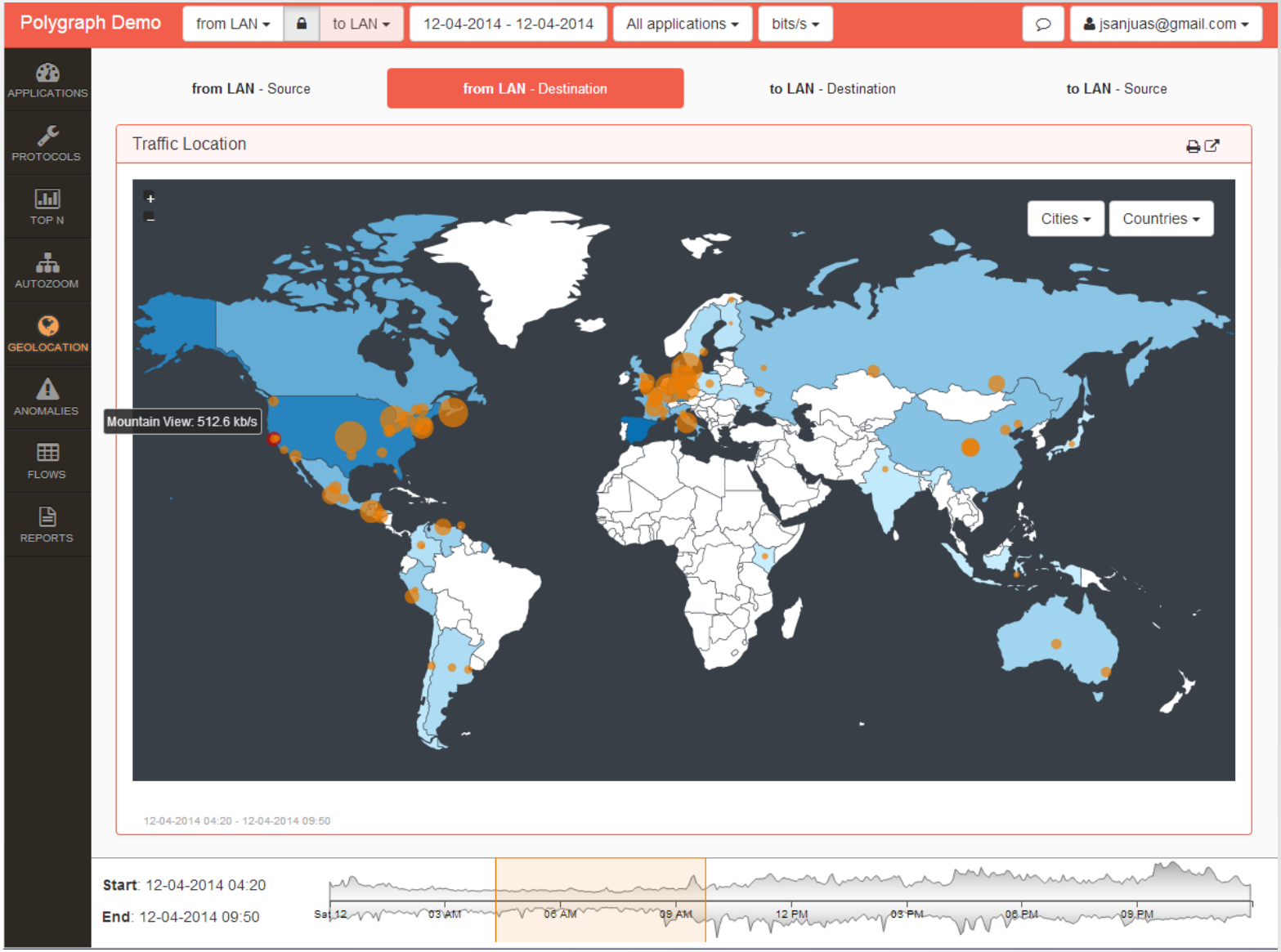


protocol breakdown

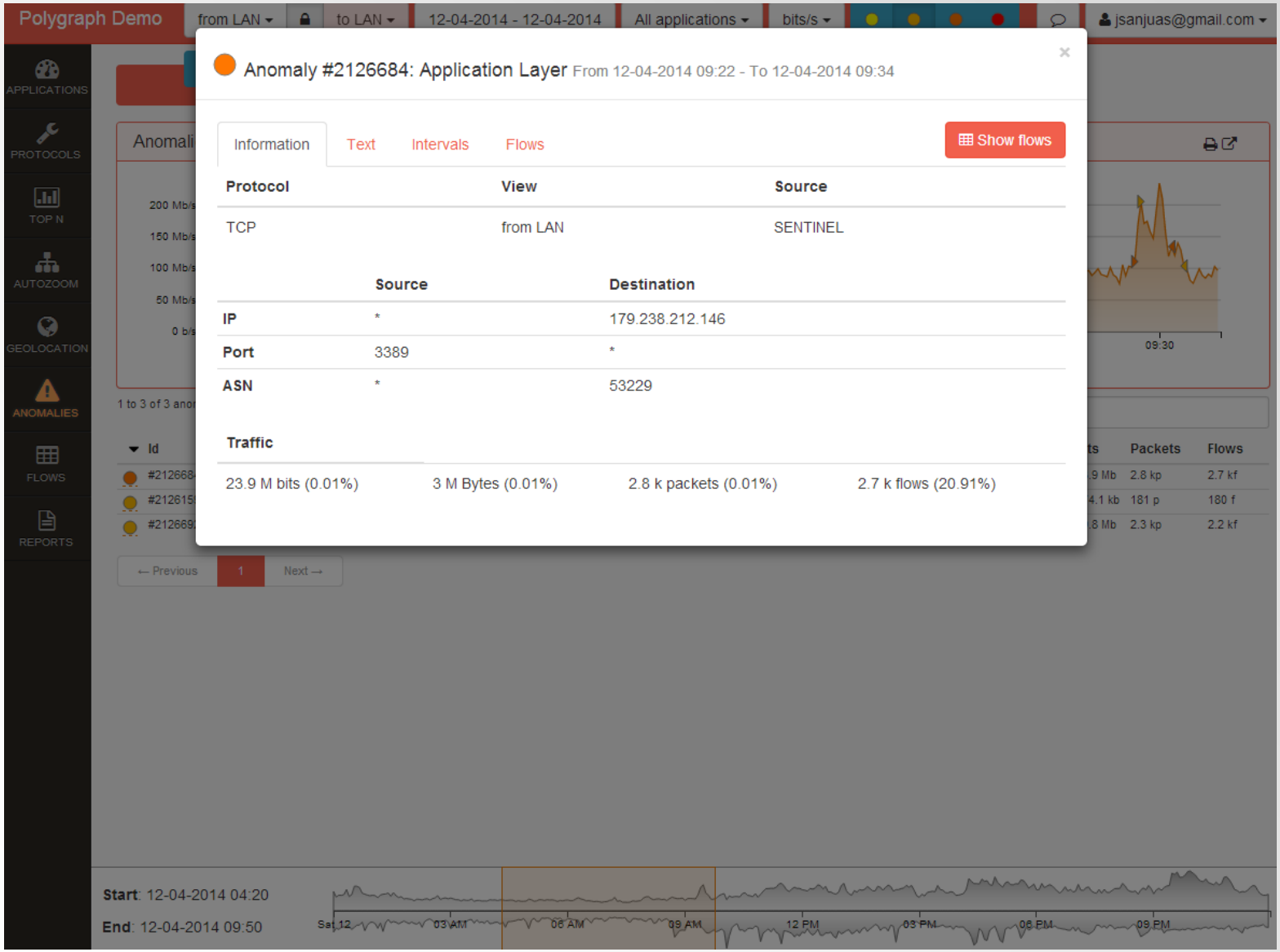
top talkers (addresses, ports, autonomous systems)



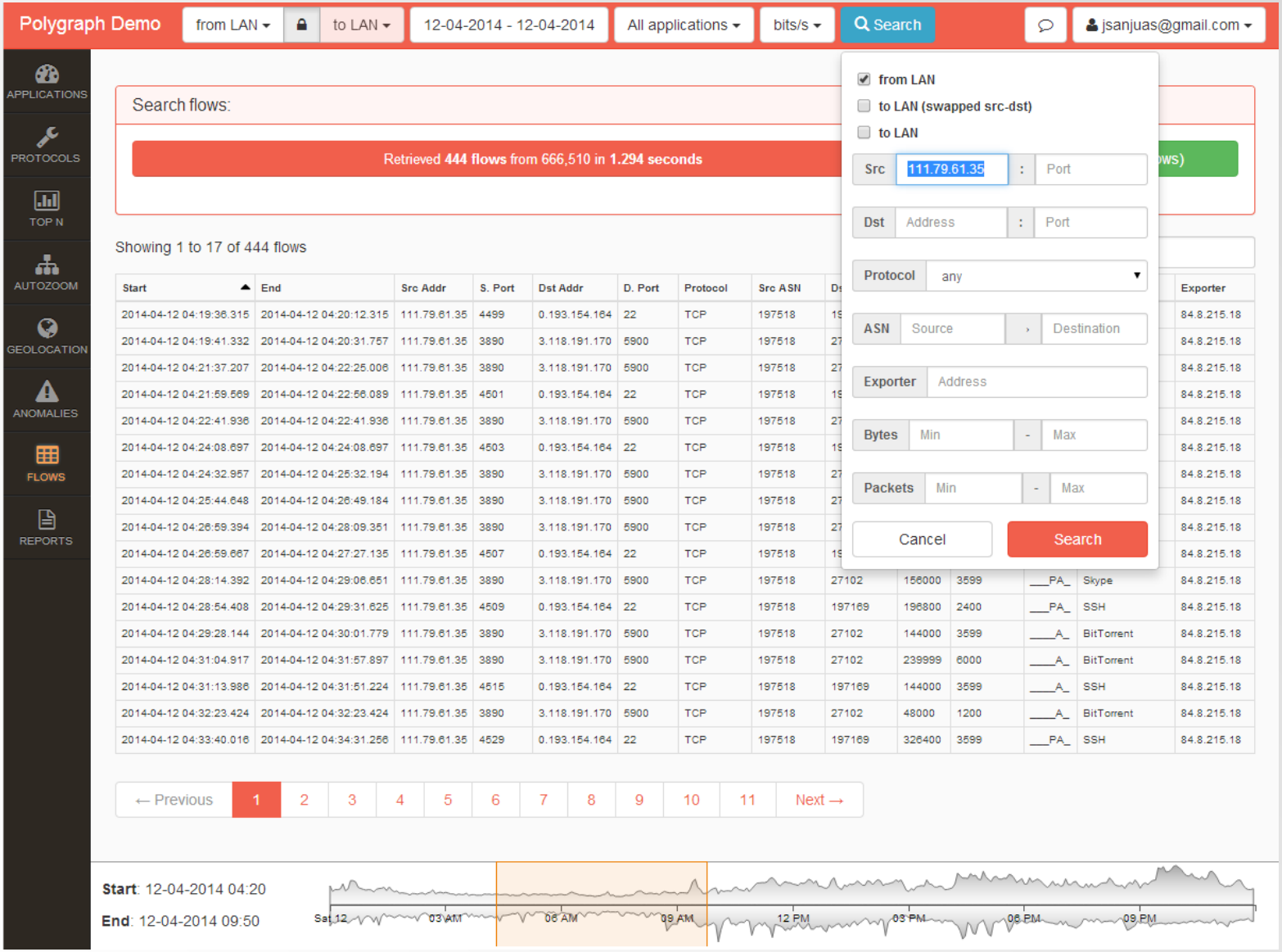
subnetwork-level bandwidth hogs



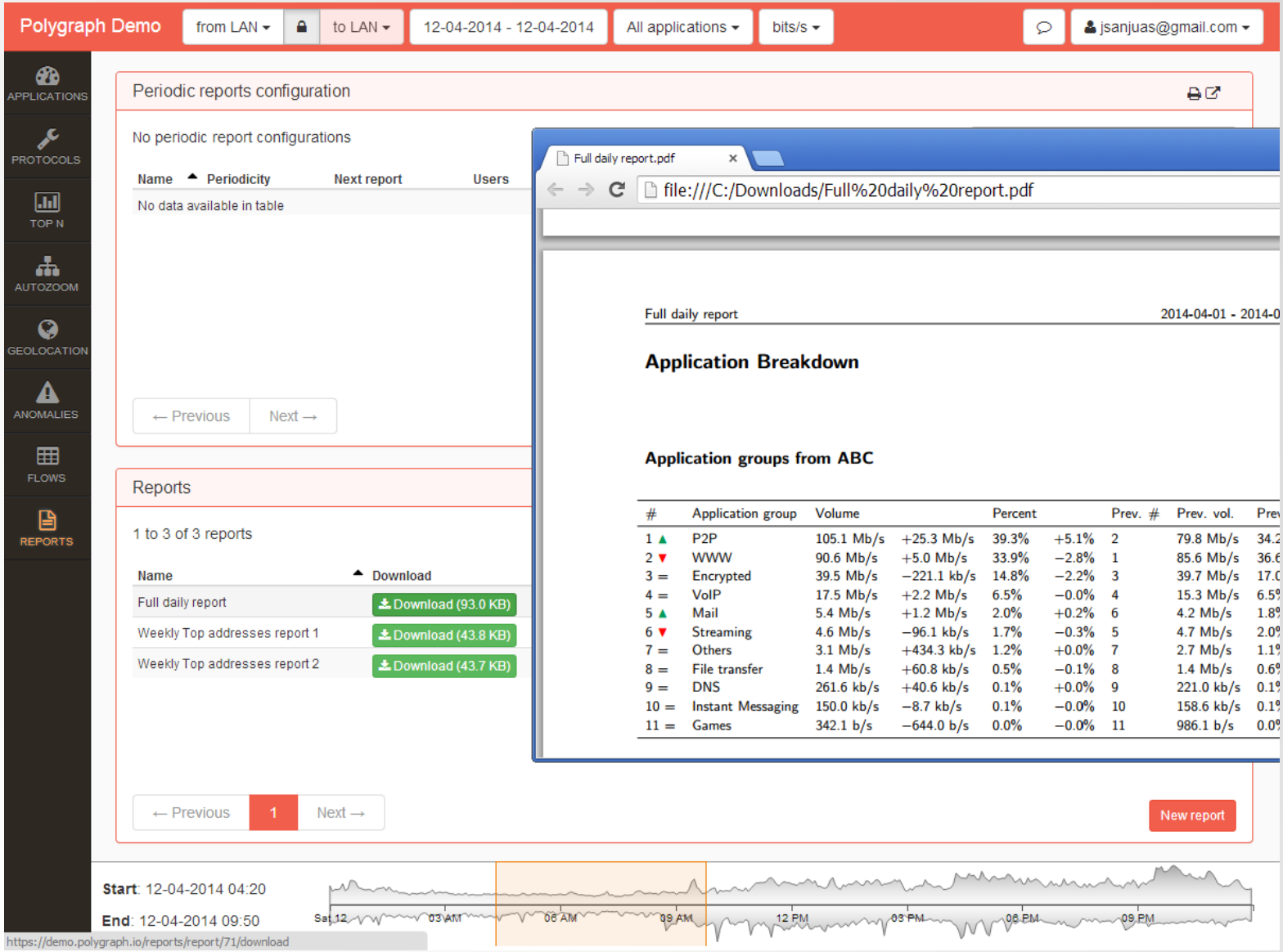
traffic geolocation (origins & destinations)



anomaly and attack detection with automatic baselining



indexed traffic database for forensic analysis



automated downloadable reports

https://polygraph.io

Talaia Networks, S.L.
K2M – Parc UPC Campus Nord
C/Jordi Girona, 1-3
Barcelona (08034) Spain

POLYGRAPH.io