

27.11.2025  
**PARIS**

  
**FRANCE-IX**  
TOUR

**15**  
ANS  **ÉDITION SPÉCIALE**



# Kentik x France-IX vs DDoS: smarter detection, stronger defense, shared protection

Jac Kloots - Senior Solution - KENTIK  
Arnaud Gorce - NetOps Engineer -  
FRANCE-IX



# Who I am?

Current  
Senior Solutions - Kentik

**Past**  
25 years in networking  
Ran networks (including  
peering) before migrating  
to the vendor side

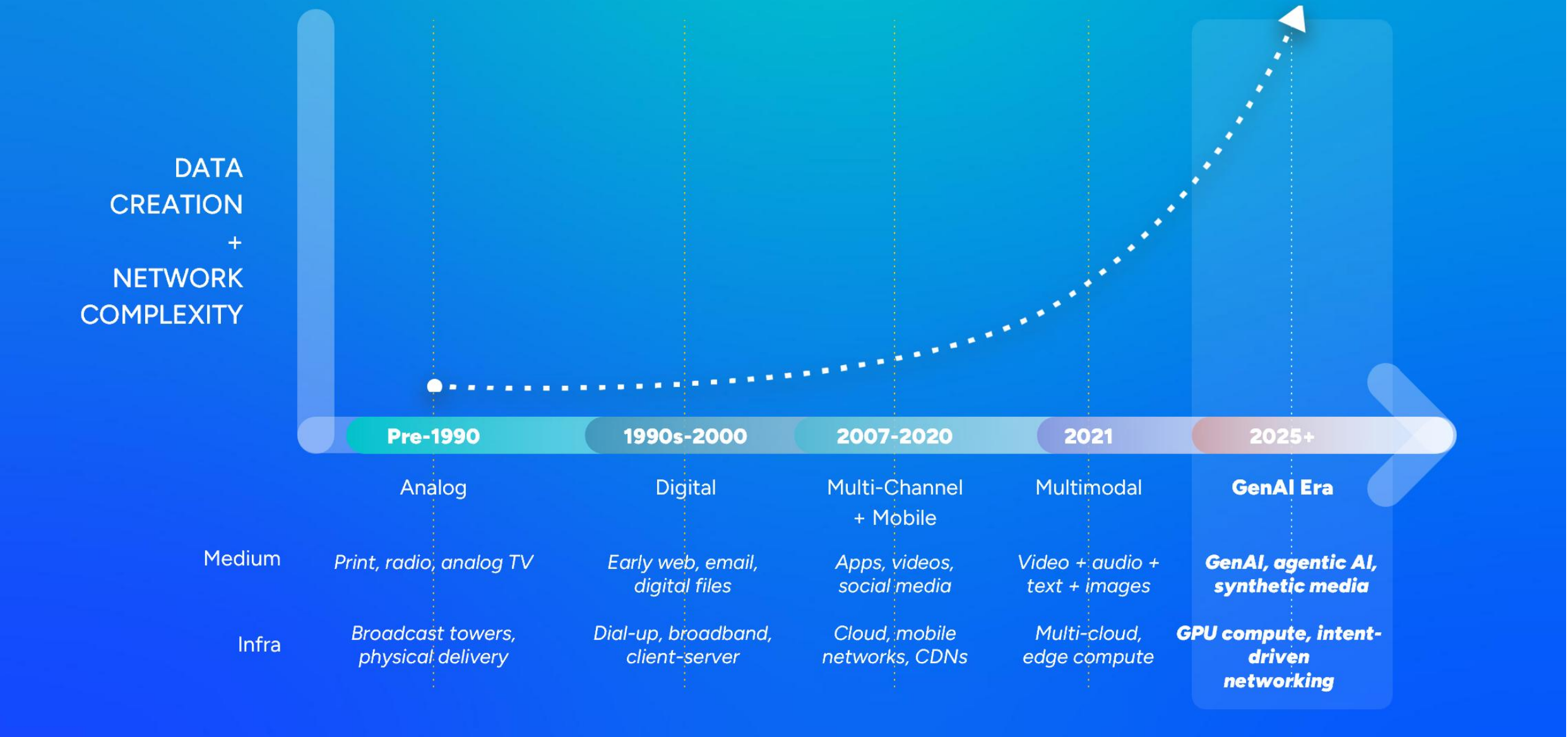


**More details**  
[/in/jackloots](#)



# Kentik: the Network Intelligence Platform

# Change is accelerating



# The most significant risk for network service providers? Inaction.

- ⚠ More complexity
- ⚠ Higher expectations, fewer resources
- ⚠ Mountains of data and noise
- ⚠ Dozens of tools
- ⚠ Manual correlation
- ⚠ Reactive stance

# Kentik | The Network Intelligence Company

**470+**  
CUSTOMERS

2 Fortune 10

9 Fortune 100

23 Fortune 500

- ✓ World's #1 AI hardware company
- ✓ 6 of the world's emerging neoclouds
- ✓ 8 of the world's 14 global tier 1 networks
- ✓ 4 of the world's top 10 media companies
- ✓ World's top data center operators and cloud providers
- ✓ Hundreds of mobile & internet providers in 20+ countries



# Kentik | The Network Intelligence Company

Founded 2014  
Born in San Francisco  
US-Based Fully Remote

205 Employees  
19 Countries

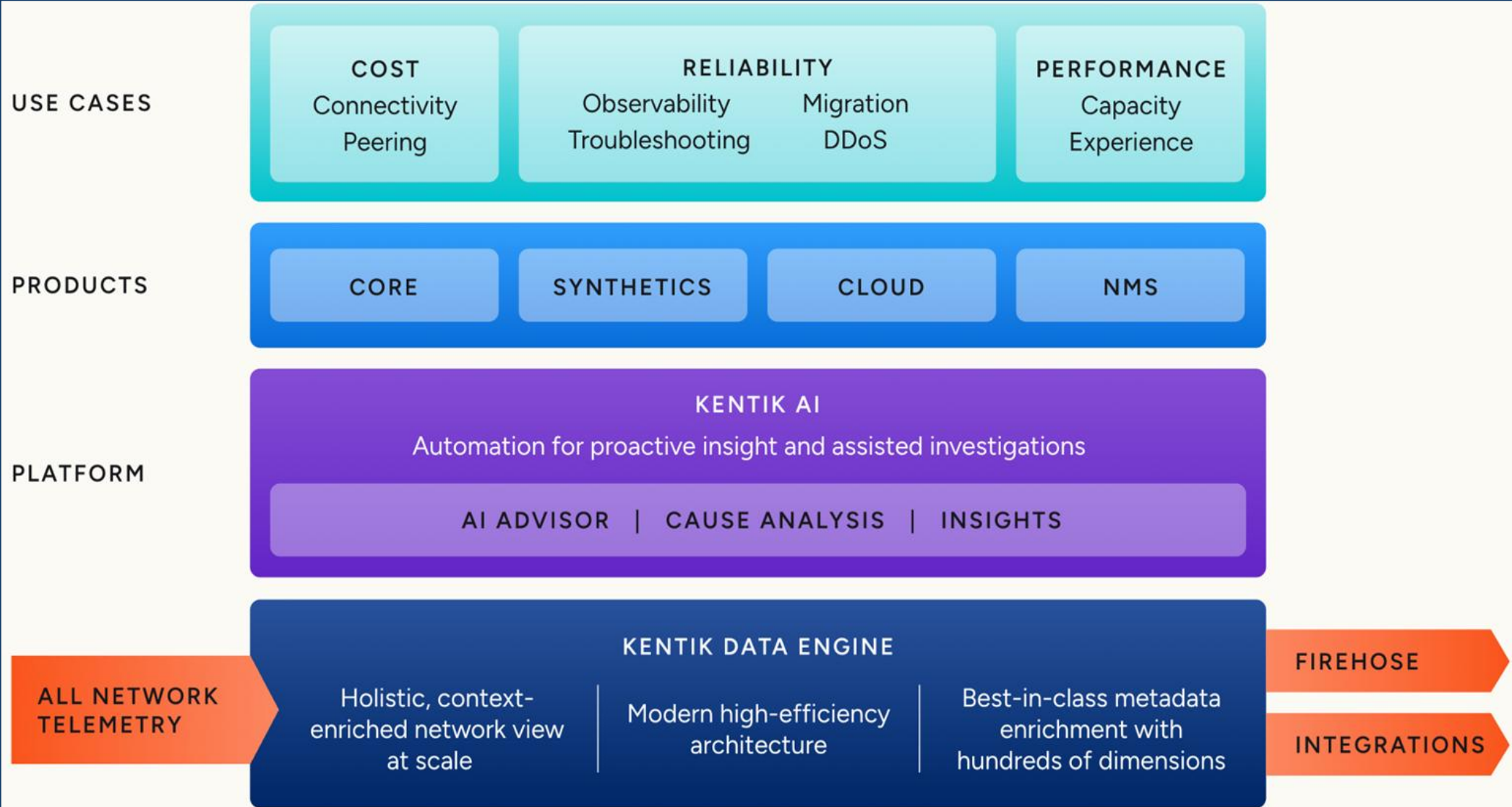
470+ Customers  
>70 NPS SCORE

540 TRILLION  
UNSAMPLED FLOWS  
IN 2024

312.5 TRILLION  
FLOW RECORDS  
STORED IN 2024

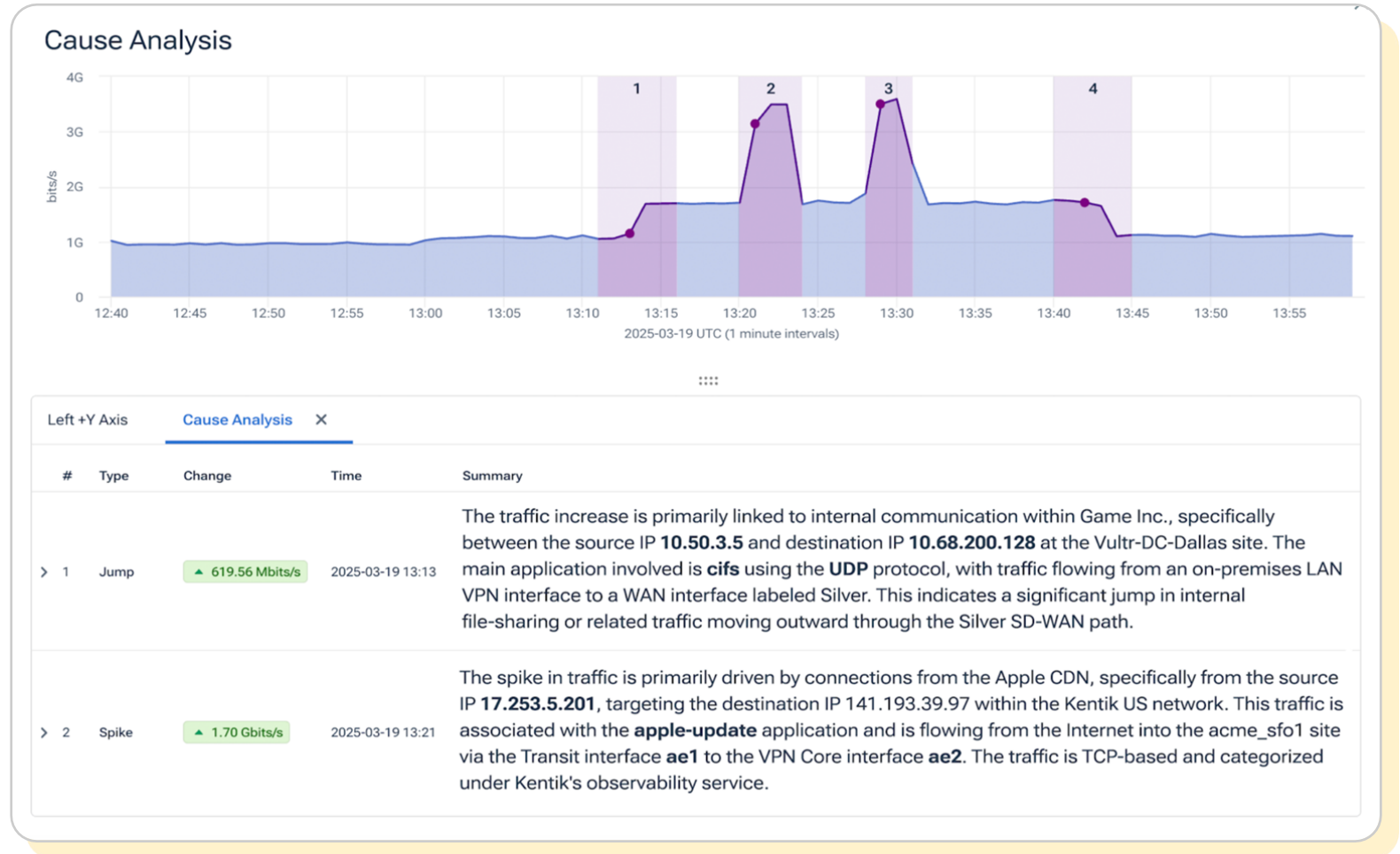
4 MILLION  
ATTACKS MITIGATED/YR

# Kentik | The Network Intelligence Company for Modern Infrastructure Teams



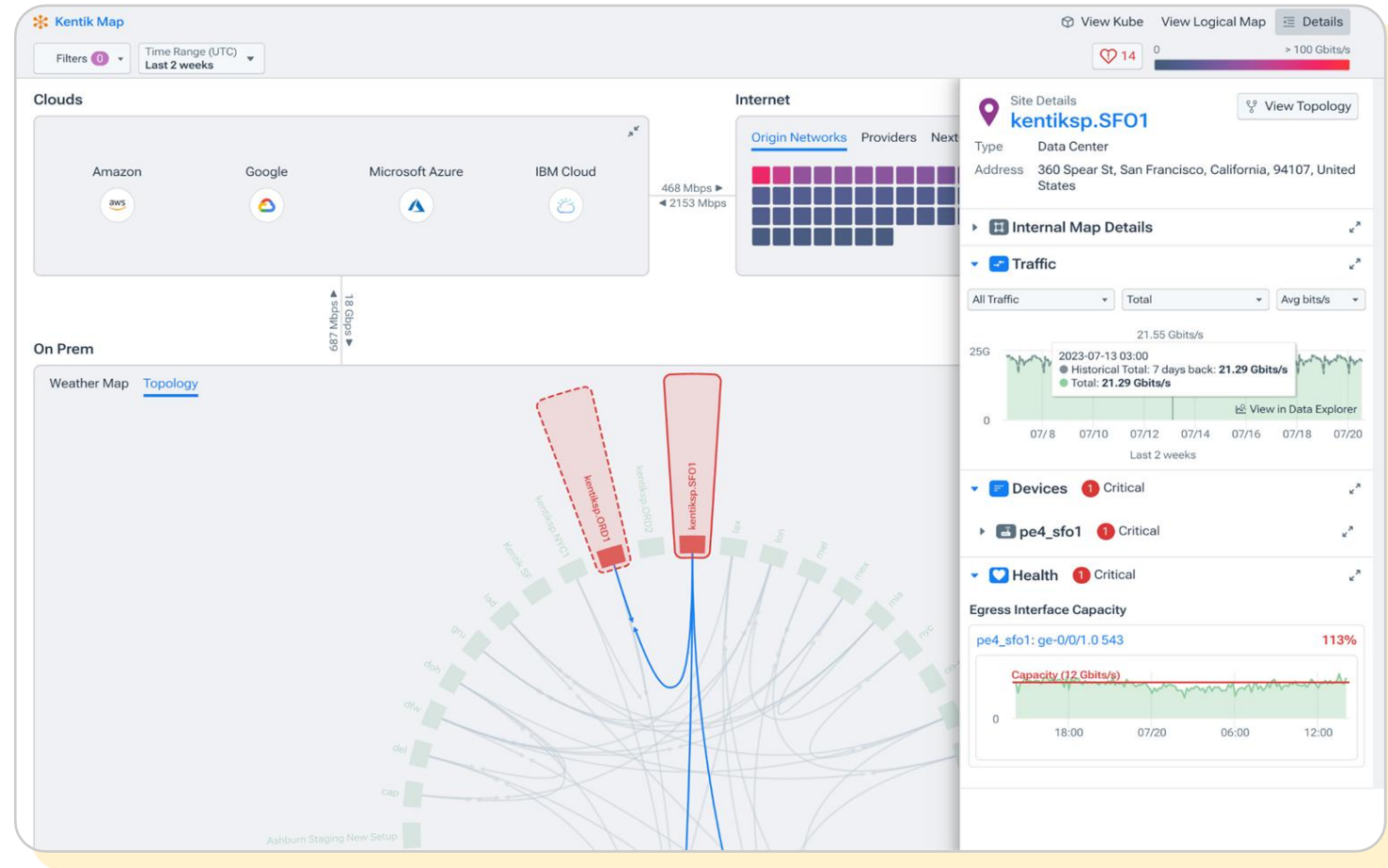
# Network AI

Troubleshoot rapidly and instantly answer complex network questions – from root cause to route optimization – with AI that understands your network in full context.



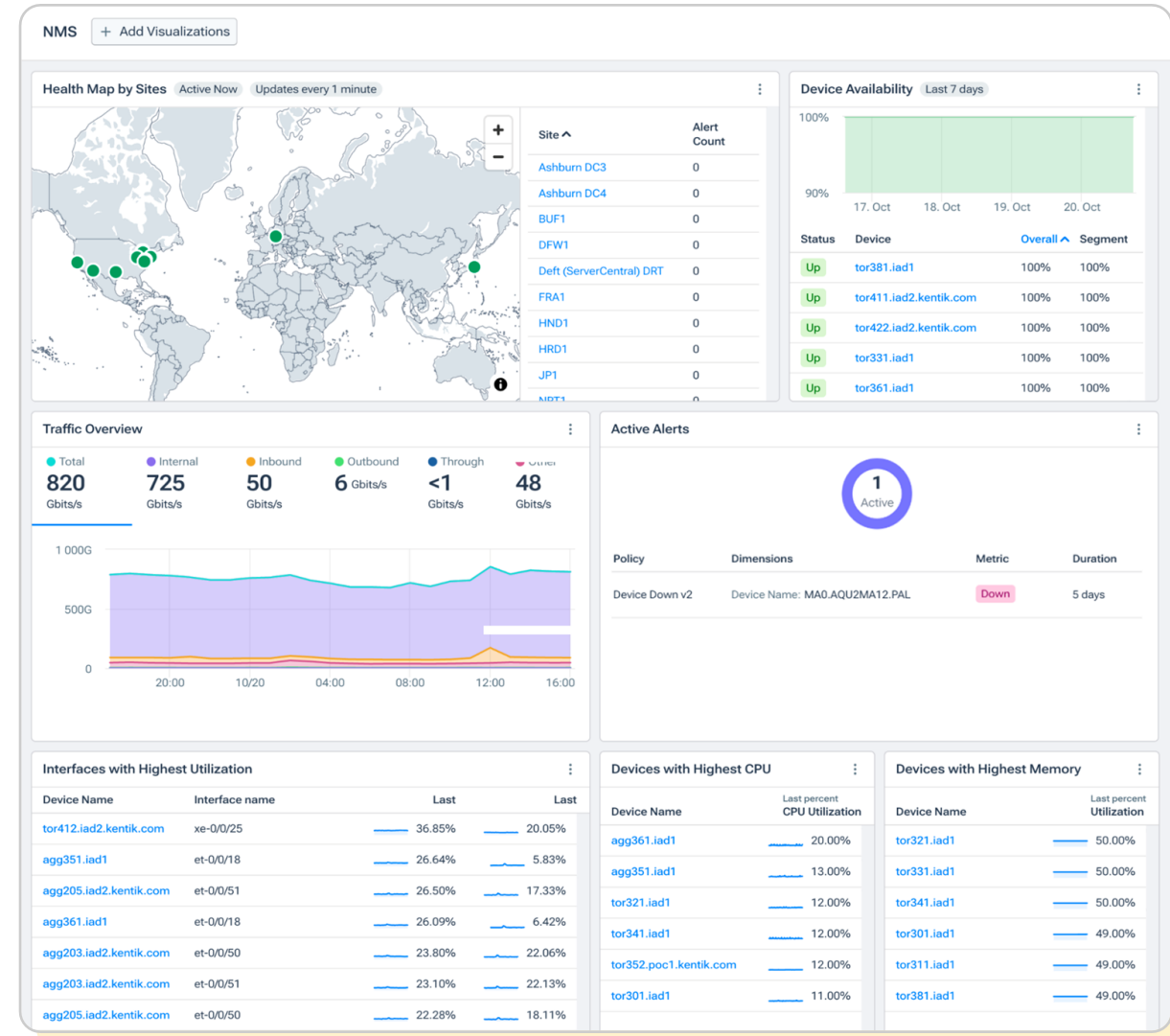
# Network traffic analytics

- Explore top talkers, decongest your edge, and engineer traffic
- Monitor service performance and verify SLAs
- Query mountains of network telemetry data in seconds
- Drill to most granular detail, with deep context
- Troubleshoot quickly & get faster times to repair and recovery



# Network monitoring

- Monitor SNMP, streaming telemetry, and custom metrics in one unified system
- See metrics from all protocols and devices with fast polling that defaults to every minute
- Detect and eliminate faulty network devices with continuous monitoring and alerts
- Ensure data security with advanced BGP state monitoring
- Consolidate traffic flow and metrics monitoring into a zero-maintenance SaaS platform



# Peering and interconnection

- Build data-backed cases for interconnections that lower costs and boost performance
- Easily evaluate peering partners, common footprints, and traffic ratios with flow + PeeringDB integration
- Replace manual peering processes with automated workflows, alerting, and insights

The screenshot displays the PeeringDB interface for Microsoft (AS8075). It includes a traffic profile, network attributes, and a list of peering sites.

**Traffic Profile**

In : Out Ratio: 1.4 : 1

**Inbound**: 2,779 Mbps

- Customer: 2,726 Mbps (97.5%)
- Transit: 67 Mbps (2.4%)
- IX: 4 Mbps (0.1%)
- Other: <1 Mbps (0%)

**Outbound**: 2,274 Mbps

- Customer: 2,271 Mbps (99.4%)
- Transit: 13 Mbps (0.6%)
- Other: <1 Mbps (0%)

**Info**

AKA: 8068 8069  
Website: None

**Network Attributes**

AS-Set / Route Set: AS-MICROSOFT  
Looking Glass: None  
Network Type: Content  
IPv4 Prefixes: 2000  
IPv6 Prefixes: 500  
Traffic Levels: Not Disclosed  
Traffic Ratios: Mostly Outbound  
Geo Scope: Global

**Peering Policy**

Policy URL: <https://www.microsoft.com/peering>  
Policy Type: Selective

**Peering Sites (Facilities) 141 IX (Exchanges) 194**

Common	Facility	Organization
✓	Equinix CH1/CH2/CH4 - Chicago	Equinix, Inc.
✓	Equinix DC1-DC15, DC21 - Ashburn	Equinix, Inc.
✓	Equinix NY9 - New York, 111 8th Avenue	Equinix, Inc.
	165 Halsey Meet-Me Room	Tishman Real Estate Service
	2degrees Auckland - Albany	2degrees

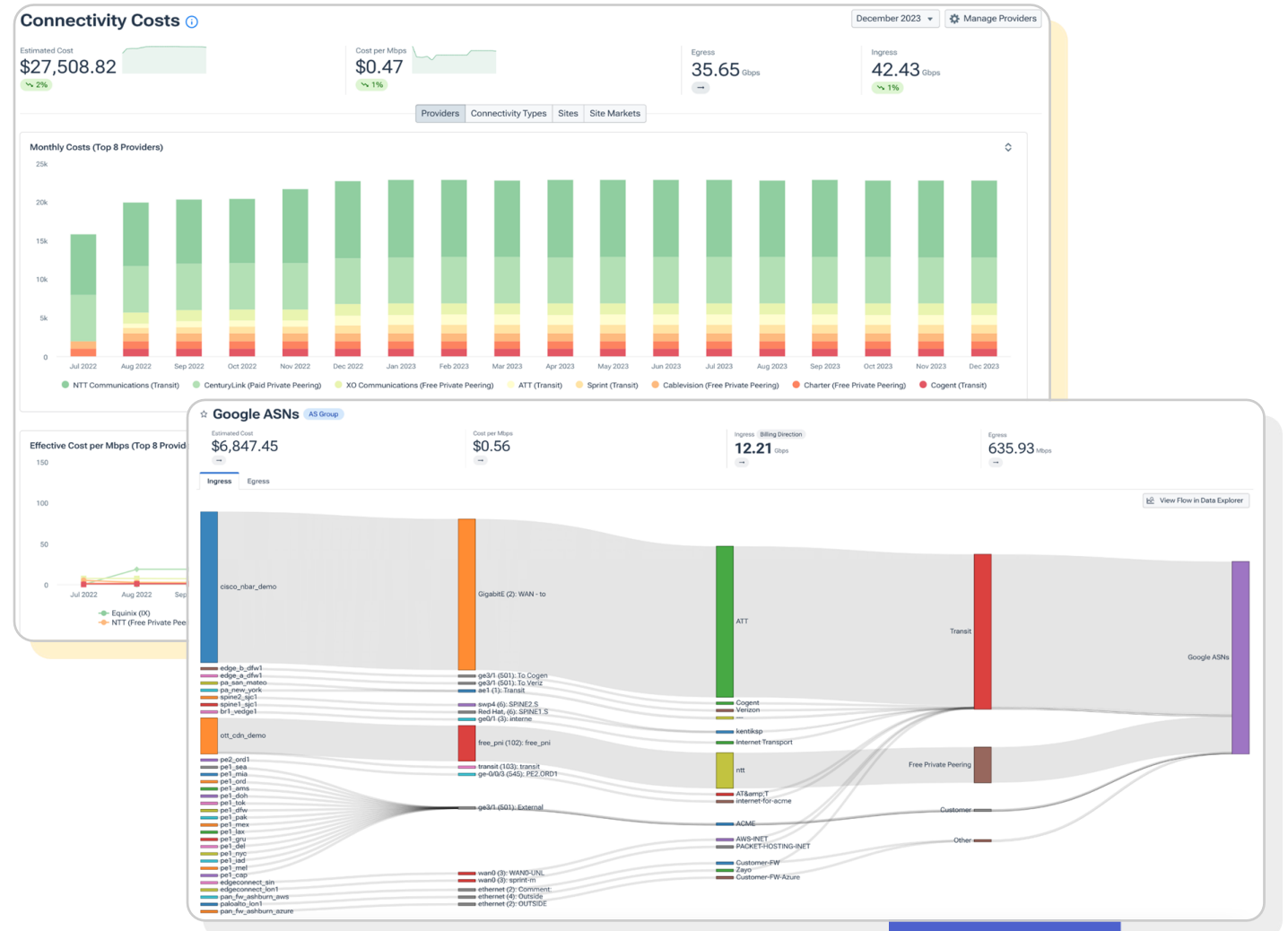
**Facility: Equinix DC1-DC15, DC21 - Ashburn**  
EQUINIX, INC.

Location: 21715 Filigree Ct, Building F, Ashburn, VA, 20147-6205, US  
Networks: 437  
Exchanges: 6

Name	Policy	Traffic Ratios
123.net AS12129	Open	Balanced
365 Data Centers (BroadbandONE) AS19151	Selective	Balanced
8xB AS32308	Open	Balanced
Ace CDN (WeChat,QQ,JooX,WeTV,PUBG,AOV) AS139341	Open	Heavy Outbound
Acreto AS396298	Open	Not Disclosed
Administration Nacional de Telecomunicaciones (ANTEL) AS6057	Open	Mostly Inbound
Adobe Systems (Omnicure) AS15224	Selective	Balanced
Advanced Hosters AS39572	Selective	Heavy Outbound
Afilias AS12041	Selective	Heavy Outbound
AFRIX Telecom AS60171	Selective	Mostly Inbound
Aire Networks del Mediterraneo AS29119	Selective	Mostly Inbound
Airtek Solutions AS61461	Selective	Mostly Inbound
Akamai (InstartLogic) AS33047	Selective	Heavy Outbound
Akamai AS20940	Open	Heavy Outbound
Akamai AS20189	Selective	Not Disclosed
Algar Telecom AS16735	Selective	Mostly Inbound
Algerie Telecom AS36947	Open	Mostly Inbound
AlhambraIT AS265264	Open	Balanced
Alibaba (Taobao) AS24429	Open	Heavy Outbound
All Points Broadband AS393713	Open	Mostly Inbound
Allianz Technology AS8360	Open	Not Disclosed
Allied Telecom Group AS22925	Open	Mostly Inbound

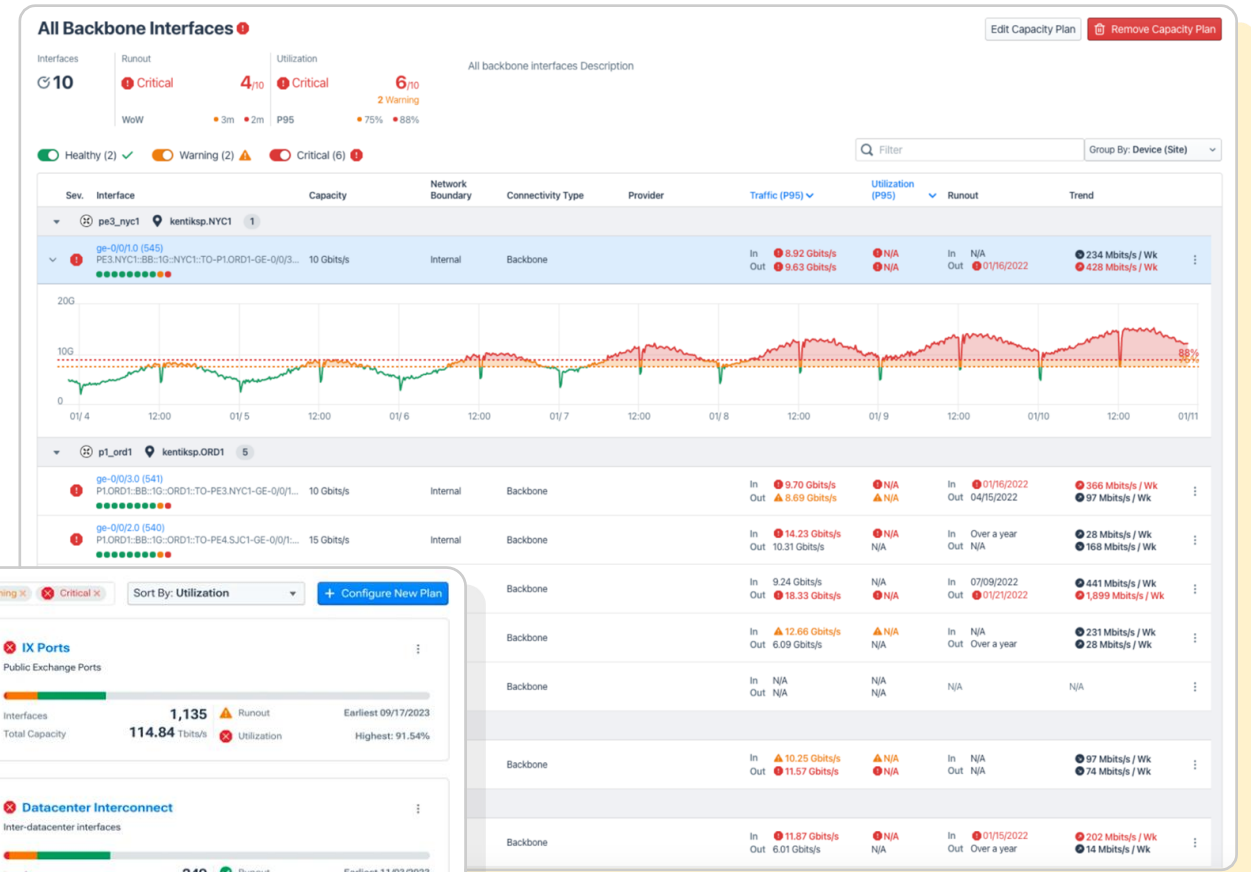
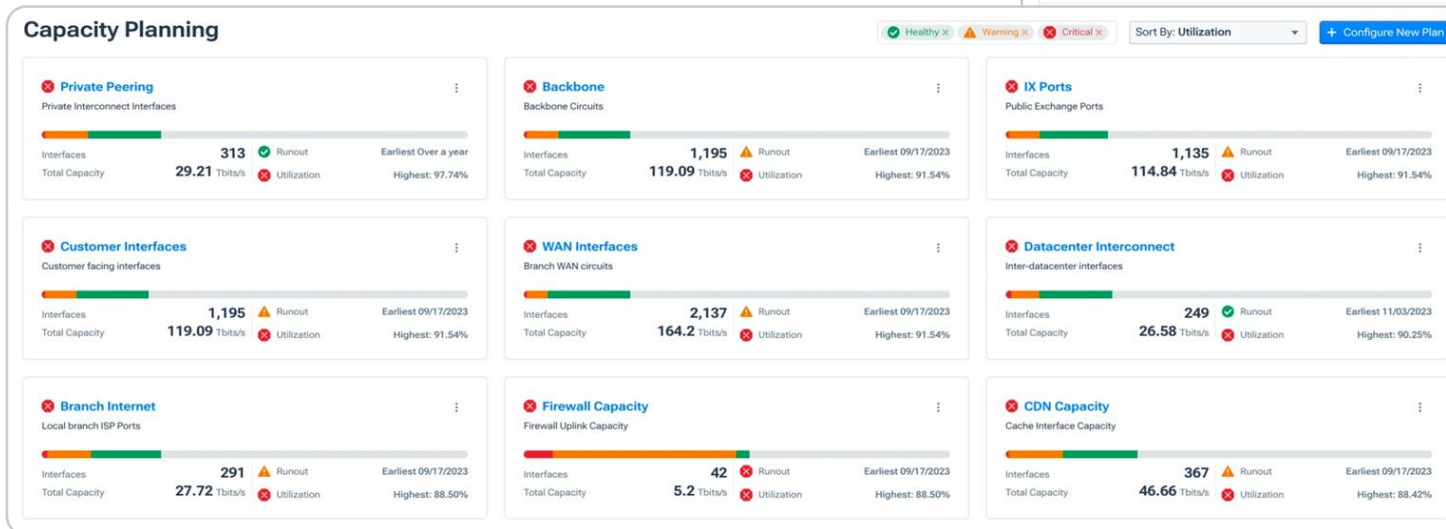
# Network cost intelligence

- **Track connectivity spending** across edge and backbone networks.
- **Surface high-cost paths** driving the most spend, and optimize routing, peering, and interconnects to cut costs and boost performance.
- **Boost margins** by tying cost-to-serve to customers, geographies, and services, and use those insights to guide pricing and renewals.
- **Democratize cost insights** so engineering, finance, sales, and leadership can see the economics behind traffic delivery.



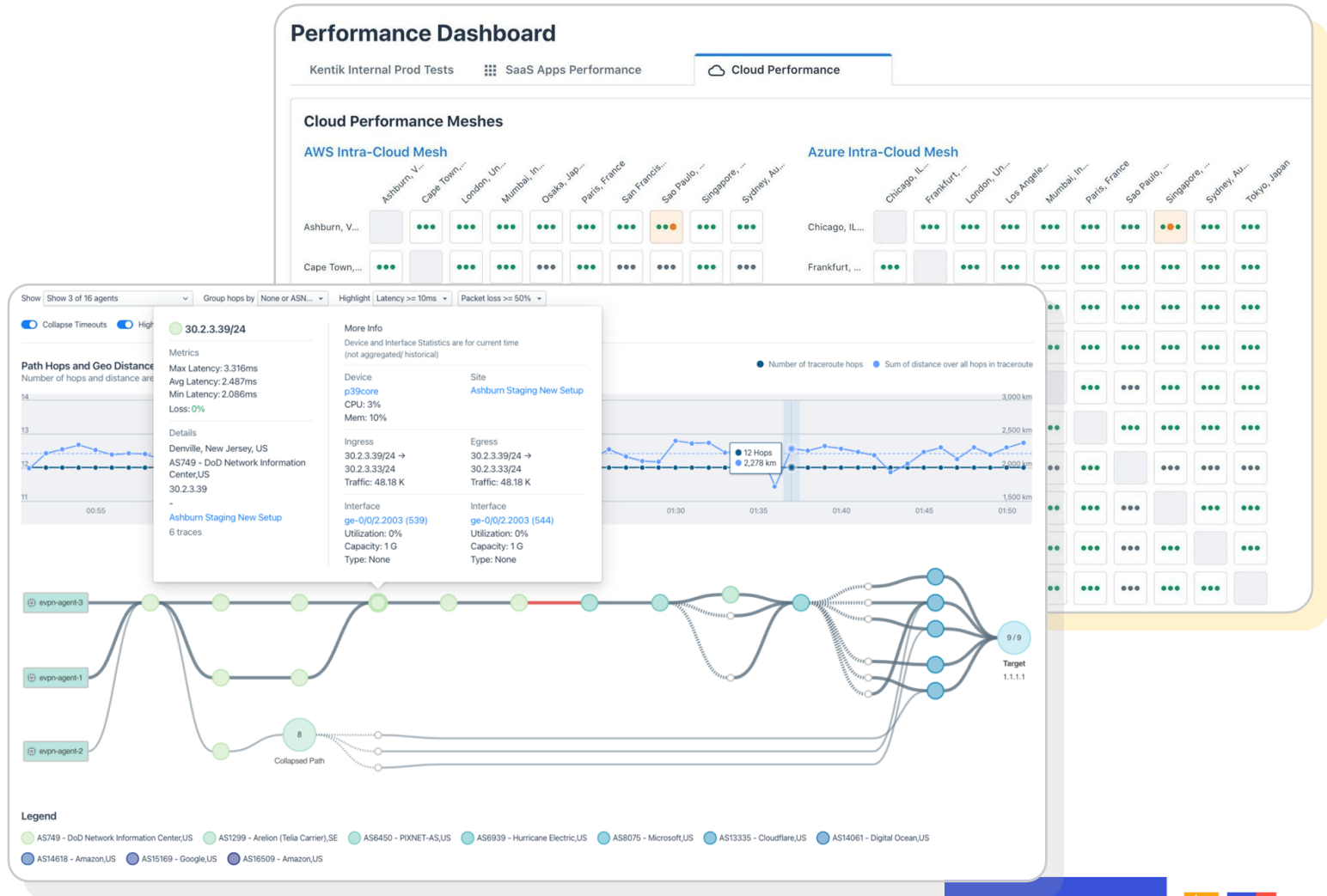
# Capacity planning

- Plan network capacity with confidence
- Identify bandwidth hogs, forecast growth, and prevent runout with utilization insights, historical trends, and automated projections



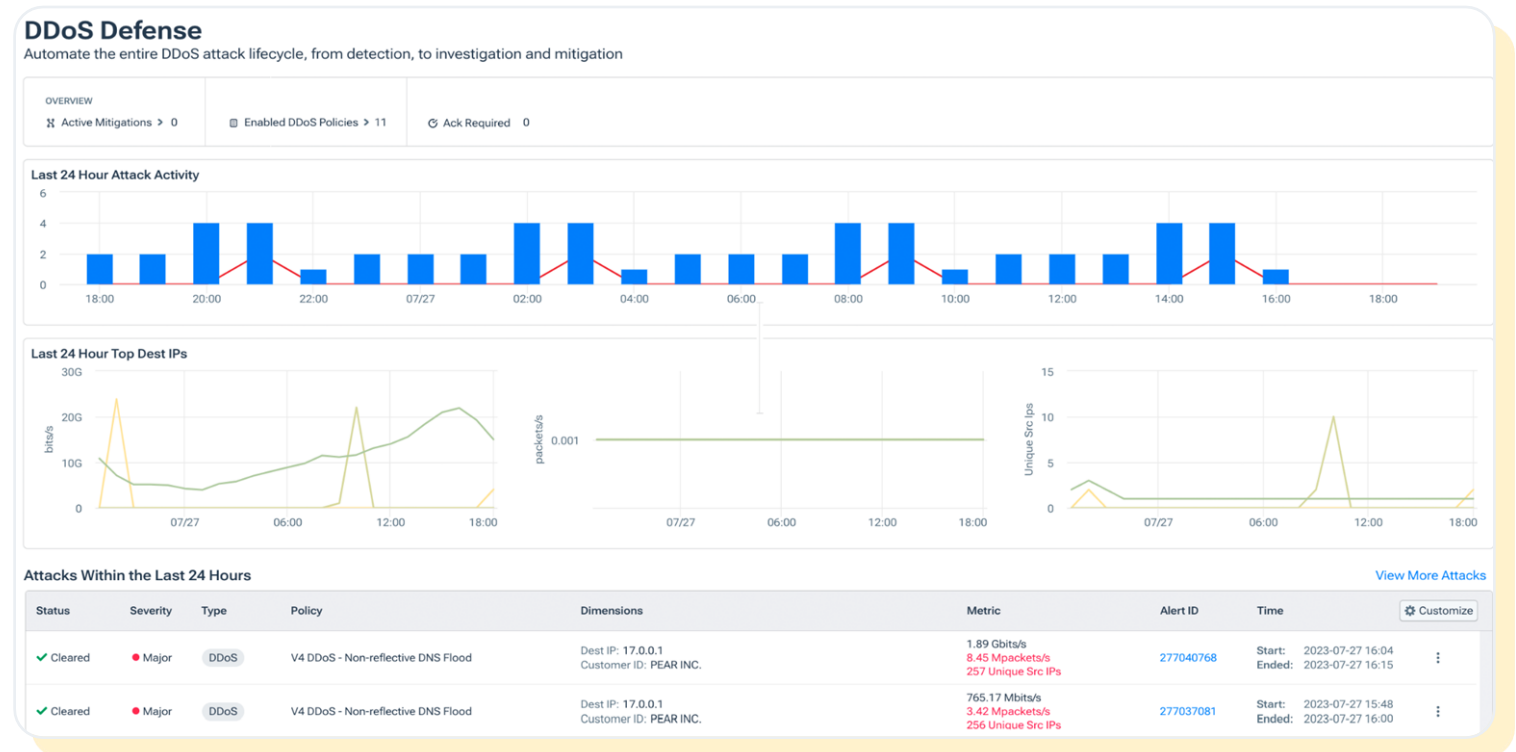
# Performance monitoring

- Proactively monitor digital experience across network infrastructure, CDNs, multi-cloud, and SaaS applications
- See real and test traffic in the one platform
- Monitor and uphold SLAs
- Get alerted to performance issues and investigate with ease



# DDoS protection and network security

- Detect a wide range of DDoS attack types and anomalies
- Automate mitigation via RTBH, BGP Flowspec, or through 3rd party partners – Cloudflare, Radware, Palo Alto, A10
- Monitor the performance of attack mitigations in real-time
- Drill down for ad-hoc forensic analysis on years of network traffic



# Kentik within France-IX: network observability and beyond

# Who am I?

**Arnaud GORCE**

- NetOps Engineer @ France-IX (since February 2024)

What do I do?

- **Network Observability (Flows)**
- Yes, I'm the "Kentik guy" at France-IX*
- Network Automation
  - Network Engineering
  - Level-2 Support
  - Client Provisioning
  - And a few other things...



# What do we do with Kentik?

- We send some flows (IPFIX):

**Between 25 000 and 80 000 flows/seconds** (following the evolution of the traffic during the day)

- Data enrichment:

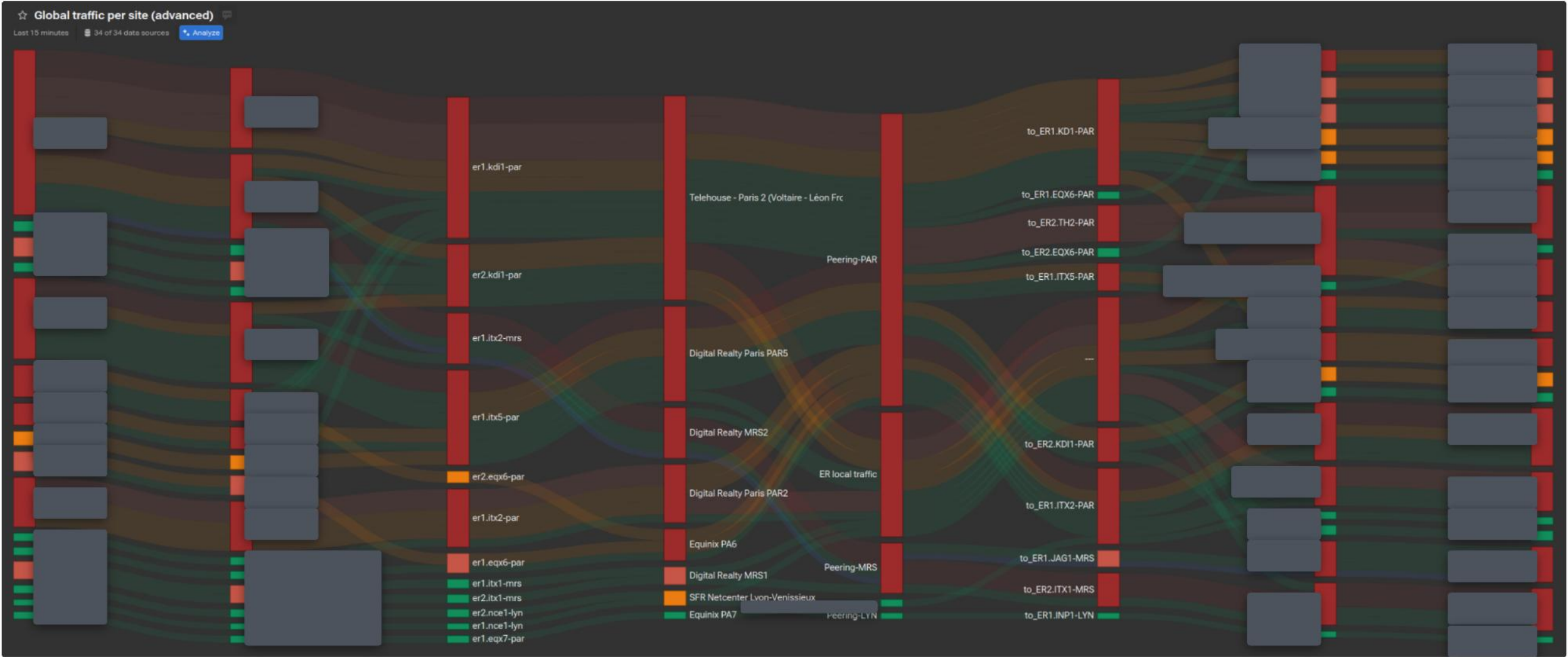
- Through SNMP with the Kentik proxy tool
- Through homemade data import from our Source of Truth tool

⇒ Which MAC address = which customer

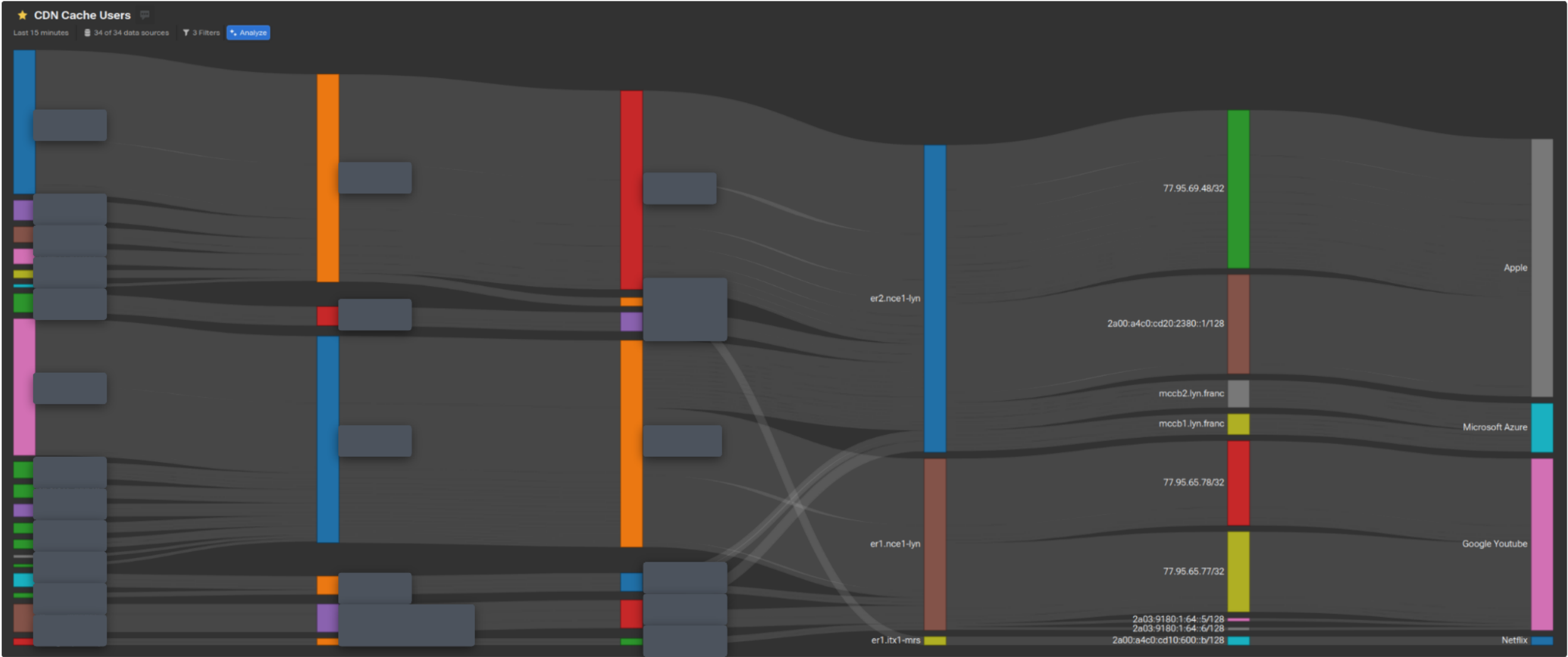
- Better understanding of what is going through our infrastructure:

- Which peer exchanges traffic with which other peers
- Who are the source and destination autonomous systems

# Top talkers traffic across France-IX backbone



# Traffic delivered from our CDN cache appliances



# DDoS in the IXP landscape

# DDoS in the IXP landscape

Like every Internet network platform, DDoS can go through an IX peering LAN.

Multiple scenarios are possible:

- From one peer to another peer
- From multiple peers to one peer
- From multiple peers to multiple peers

Source IP addresses can be spoofed (or not) but the source MAC address(es) won't be.

## Evolution of the global Internet architecture

- More and more networks from Asia are being connected to the western Europe IXPs (development of more submarine cables)
- Same thing with East Europe networks
  - ⇒ They are often the source of some DDoS attacks we observe...

# DDoS in the IXP landscape

## What can we do against it?

The peers connected to the IXP can do something against DDoS:

- Eyeball ISPs and Cloud/hosting providers
  - **RFC2827/BCP38** and **MANRS**
  - Not announcing the IP prefix of the peering LAN into their IGP or within their iBGP
- Internet users
  - Be careful with your IoT devices
  - Stop using residential proxies please...
- Etc...

But what can an IXP do against DDoS? **Aren't we just a “switch”?**

- Blackholing community on route-servers (RFC7999).
- Filtering? Maybe.
- Visibility? **For sure.**

# Kentik for us... and for you?

# Kentik for us... and for you?

**How could we give visibility about your network  
to you with Kentik?**

# Kentik for us... and for you?

You just suffered from a DDoS attack and you noticed that it went through your France-IX connection.

→ We can help you!

- Reports detailing what happened on your port during the related timestamp

**OR**

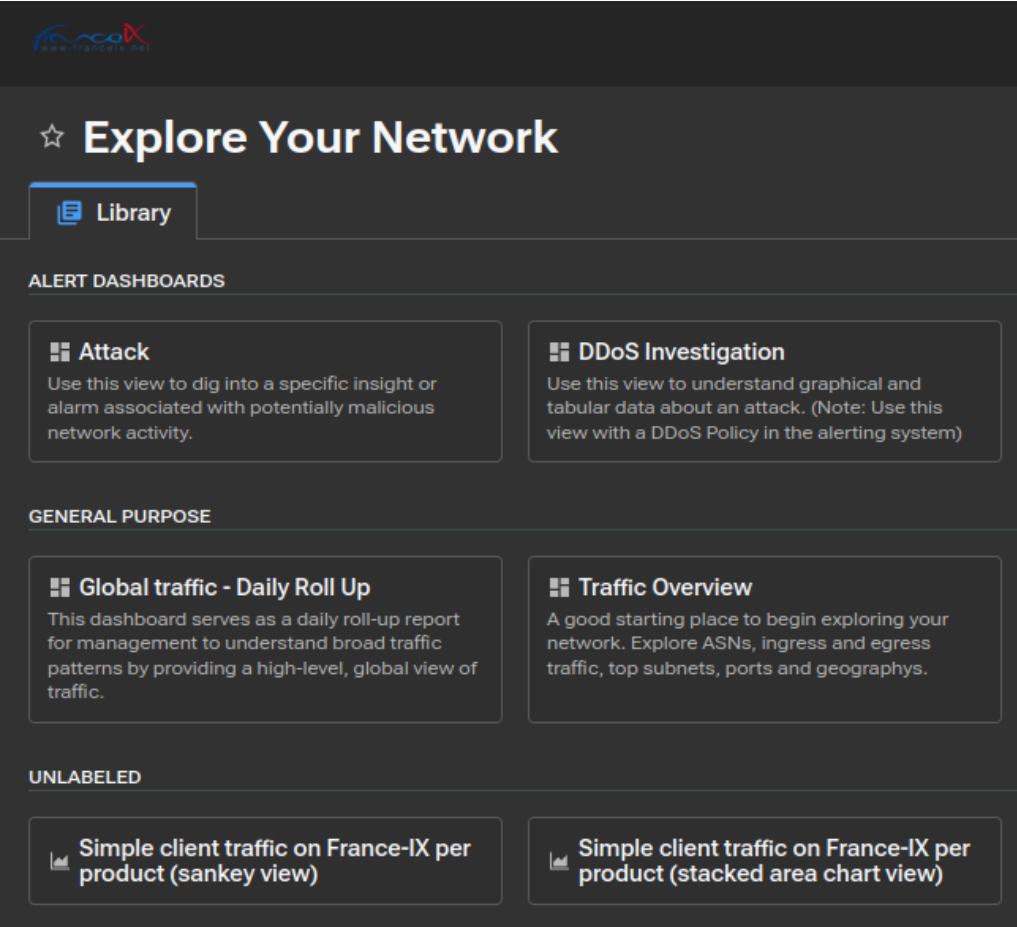
- Access to dashboards directly on Kentik to check this by yourself ⇒ **How?**

# Kentik for us... and for you?

## My Kentik Portal (Extranet solution)

The idea: giving you access to the Kentik portal with an account related to the France-IX org

- Selection of dashboards made by the France-IX team and adapted for the Peering use-case
- Flows filtered with your MAC addresses ⇒ you only see your traffic (both egress and ingress)



The screenshot displays the Kentik portal interface with the following sections:

- Explore Your Network** (starred)
- Library** (selected)
- ALERT DASHBOARDS**
  - Attack**: Use this view to dig into a specific insight or alarm associated with potentially malicious network activity.
  - DDoS Investigation**: Use this view to understand graphical and tabular data about an attack. (Note: Use this view with a DDoS Policy in the alerting system)
- GENERAL PURPOSE**
  - Global traffic - Daily Roll Up**: This dashboard serves as a daily roll-up report for management to understand broad traffic patterns by providing a high-level, global view of traffic.
  - Traffic Overview**: A good starting place to begin exploring your network. Explore ASNs, ingress and egress traffic, top subnets, ports and geographies.
- UNLABELED**
  - Simple client traffic on France-IX per product (sankey view)**
  - Simple client traffic on France-IX per product (stacked area chart view)**

# Conclusion

## **The Internet changes**

Only protecting its transit is not enough today, you also need to care about your peering links

## **Having visibility is key**

You need to know and understand what is happening on your infrastructure

## **Everyone is concerned, even the IXPs**

More and more IXP operators are seeking a way to fight DDoS attacks at their level.

## **What about France-IX? We are also trying to find solutions so we can do our part**

The idea: configuration of filters pushed with NETCONF or Flowspec following the detection of an attack on one of our peering LANs.

# Any questions? Thank you!

Jac Kloots - Senior Solution - KENTIK

Arnaud Gorce - NetOps Engineer -  
FRANCE-IX

in

<https://fr.linkedin.com/company/france-ix>

X

<https://x.com/ixpfranceix>

