

# Using Sources of Truth to Enrich and Understand Network Telemetry

Jac Kloots  
Senior Solutions Engineer



# Who am I?

## Current

Senior Solutions Engineer - [Kentik](#)

## Past

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

## More details



[/in/jackloots](#)

# Network observability

The difference between **more data** and **more answers**



Traditional monitoring  
lets you see **what's**  
happening on your  
network.



Network observability  
helps you understand  
**why** it's happening and  
automate a response.

# Network observability

What are the building blocks?



Ingest of a huge amount of data from many sources



Classify, cluster, group, scale, and normalize data

*(create structure among unstructured data)*



Recognize patterns in data



Automate baselining and perform anomaly detection



Correlate to learn how data points relate to each other

# Context is needed for network observability



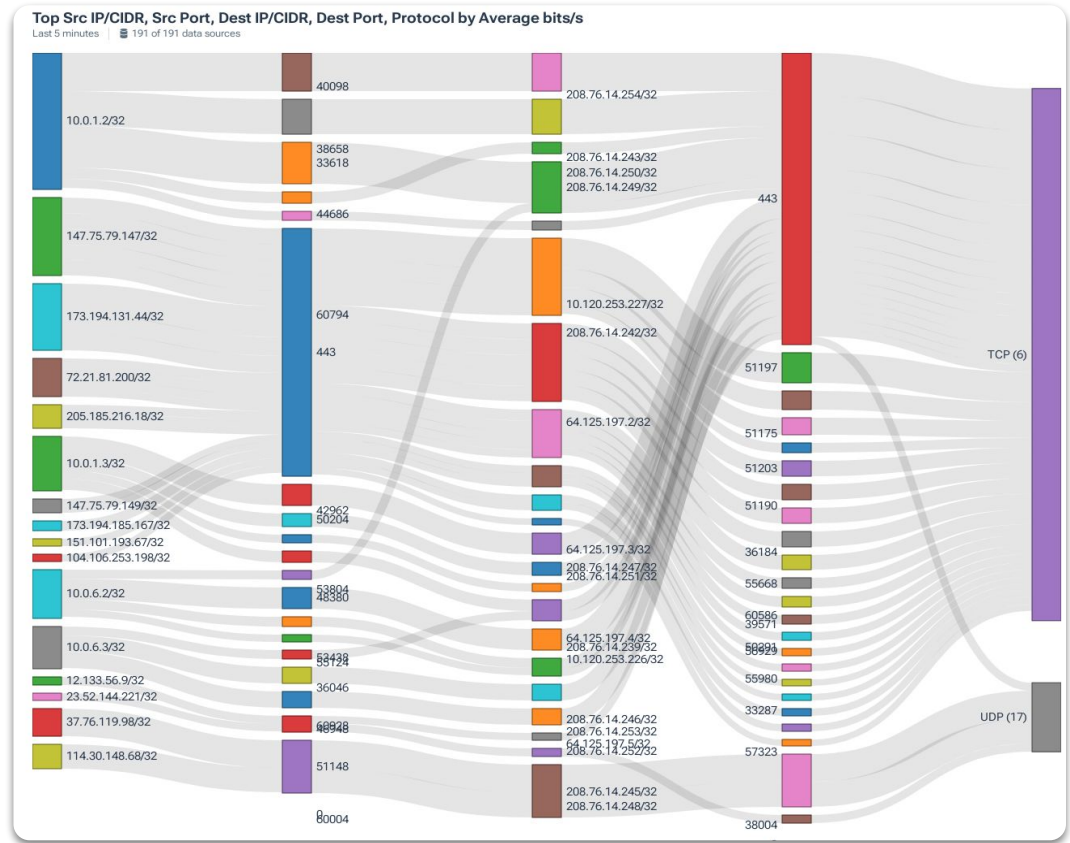
# NetFlow is a good step

Source	Destination	Non-Directional / Other
<b>Network &amp; Traffic Topology</b>		
<ul style="list-style-type: none"><li><input type="checkbox"/> Interface</li><li><input type="checkbox"/> Connectivity Type</li><li><input type="checkbox"/> Network Boundary</li><li><input type="checkbox"/> Provider</li><li><input type="checkbox"/> Traffic Origination</li><li><input type="checkbox"/> Interface Capacity</li><li><input type="checkbox"/> VLAN</li><li><input type="checkbox"/> MAC Address</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Interface</li><li><input type="checkbox"/> Connectivity Type</li><li><input type="checkbox"/> Network Boundary</li><li><input type="checkbox"/> Provider</li><li><input type="checkbox"/> Traffic Termination</li><li><input type="checkbox"/> Interface Capacity</li><li><input type="checkbox"/> VLAN</li><li><input type="checkbox"/> MAC Address</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Ultimate Exit Interface</li><li><input type="checkbox"/> Ultimate Exit Connectivity Type</li><li><input type="checkbox"/> Ultimate Exit Network Boundary</li><li><input type="checkbox"/> Ultimate Exit Provider</li><li><input type="checkbox"/> Simple Traffic Profile</li><li><input type="checkbox"/> Traffic Profile</li><li><input type="checkbox"/> Site</li><li><input type="checkbox"/> Device</li><li><input type="checkbox"/> Site Market</li><li><input type="checkbox"/> Ultimate Exit Site Market</li><li><input type="checkbox"/> Ultimate Exit Site</li><li><input type="checkbox"/> Ultimate Exit Device</li><li><input type="checkbox"/> Host Direction</li><li><input type="checkbox"/> Device Sample Rate</li></ul>

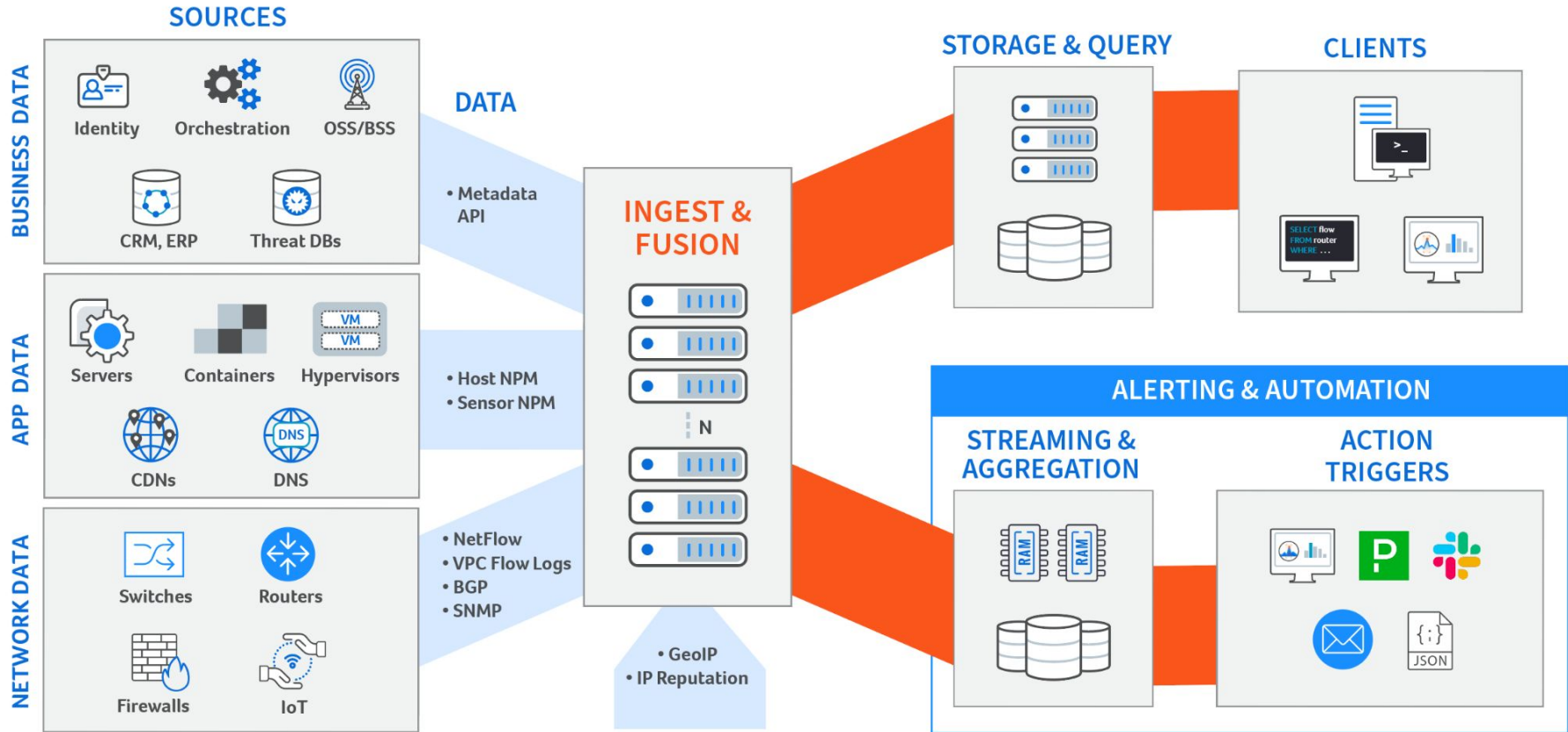
IP & BGP Routing		
<ul style="list-style-type: none"><li><input type="checkbox"/> IP/CIDR</li><li><input type="checkbox"/> Site by IP</li><li><input type="checkbox"/> Site Type by IP</li><li><input type="checkbox"/> Port Number</li><li><input type="checkbox"/> Route Prefix/LEN</li><li><input type="checkbox"/> Route LEN</li><li><input type="checkbox"/> AS Number</li><li><input type="checkbox"/> Next Hop IP/CIDR</li><li><input type="checkbox"/> Next Hop AS Number</li><li><input type="checkbox"/> 2nd Hop AS Number</li><li><input type="checkbox"/> 3rd Hop AS Number</li><li><input type="checkbox"/> AS Path</li><li><input type="checkbox"/> BGP Community</li><li><input type="checkbox"/> VRF Name</li><li><input type="checkbox"/> VRF Route Distinguisher</li><li><input type="checkbox"/> VRF Route Target</li><li><input type="checkbox"/> VRF Extended Route Distinguisher</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> IP/CIDR</li><li><input type="checkbox"/> Site by IP</li><li><input type="checkbox"/> Site Type by IP</li><li><input type="checkbox"/> Port Number</li><li><input type="checkbox"/> Route Prefix/LEN</li><li><input type="checkbox"/> Route LEN</li><li><input type="checkbox"/> AS Number</li><li><input type="checkbox"/> Next Hop IP/CIDR</li><li><input type="checkbox"/> Next Hop AS Number</li><li><input type="checkbox"/> 2nd Hop AS Number</li><li><input type="checkbox"/> 3rd Hop AS Number</li><li><input type="checkbox"/> AS Path</li><li><input type="checkbox"/> BGP Community</li><li><input type="checkbox"/> VRF Name</li><li><input type="checkbox"/> VRF Route Distinguisher</li><li><input type="checkbox"/> VRF Route Target</li><li><input type="checkbox"/> VRF Extended Route Distinguisher</li><li><input type="checkbox"/> RPKI Validation Status</li><li><input type="checkbox"/> RPKI Quick Status</li><li>Segment Routing SID</li><li>Segment Routing SID Path</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Protocol</li><li><input type="checkbox"/> INET Family</li><li><input type="checkbox"/> DSCP</li><li><input type="checkbox"/> ToS</li><li><input type="checkbox"/> Packet Size</li><li><input type="checkbox"/> Packet Size (nearest 100)</li><li><input type="checkbox"/> Sampling Rate * 100</li></ul>

# IP Addresses, Ports And Protocols Are Not Enough

- It is awesome to see what traffic is flowing on the network.
- But what does any of this mean in terms of users, content, or network costs?



# Best Practices for Leveraging Contextual Data





# Telemetry Enrichment

Enrichment with metadata provides context



Geo-location

Threat feeds

Transit costs

BGP table information

Pod names

Public BGP data

PeeringDB information

IPAM

OTT service name

Application identifiers

Process IDs

CDN names

DNS information

Synthetic test results

Customer names

# But how?

- ✓ Controversial opinion → there is no single source of truth
- ✓ The data exists but is spread across numerous sources
- ✓ Automation can pull this data together
- ✓ Using APIs, push it into a network observability platform that can enrich the network traffic

# Automation for Enrichment

```
def pull_clients():
    print("Grabbing client list from controller...")
    client = UnifiClient(host=UNIFI_HOST, port=8443, username=UNIFI_USER, password=UNIFI_PASSWORD, site=UNIFI_SITE)
    client_list = client.list_clients()

    print("Writing client list to a file...")
    outfile = open(csvfile, "w")
    # write a header row for the CSV file
    outfile.write("mac_addr,hostname\n")
    for client in client_list:
        mac_addr = client['mac']
        if 'name' in client:
            hostname = client['name']
        elif 'hostname' in client:
            hostname = client['hostname']
        else:
            hostname = client['oui']
        outfile.write(mac_addr + ',' + hostname + '\n')
    outfile.close()
```

[https://github.com/jryburn/unifi-to-kentik-cd/blob/main/update\\_custom\\_dimension.py](https://github.com/jryburn/unifi-to-kentik-cd/blob/main/update_custom_dimension.py)

# Context for the win!

Source	Destination	Non-Directional / Other	Source	Destination	Non-Directional / Other
▶ Network & Traffic Topology			▼ Application Context & Security		
▶ IP & BGP Routing			<input type="checkbox"/> Public Cloud Provider	<input type="checkbox"/> Public Cloud Provider	<input type="checkbox"/> Application
▶ Cloud			<input type="checkbox"/> Public Cloud Service	<input type="checkbox"/> Public Cloud Service	<input type="checkbox"/> TCP Flags
▼ Geolocation			<input type="checkbox"/> CDN	<input type="checkbox"/> CDN	<input type="checkbox"/> OTT Service
<input type="checkbox"/> Custom Geo	<input type="checkbox"/> Custom Geo	<input type="checkbox"/> Site Country	<input type="checkbox"/> Service (Port+Proto)	<input type="checkbox"/> Service (Port+Proto)	<input type="checkbox"/> OTT Service Type
<input type="checkbox"/> Country	<input type="checkbox"/> Country	<input type="checkbox"/> Ultimate Exit Site Country	<input type="checkbox"/> Bot Net CC	<input type="checkbox"/> Bot Net CC	<input type="checkbox"/> OTT Service Provider
<input type="checkbox"/> Region	<input type="checkbox"/> Region		<input type="checkbox"/> Threat List Host	<input type="checkbox"/> Threat List Host	
<input type="checkbox"/> City	<input type="checkbox"/> City		▼ Custom		
			<input type="checkbox"/> Source Location	<input type="checkbox"/> Dest Location	<input type="checkbox"/> Customer ID
			<input type="checkbox"/> Source Site	<input type="checkbox"/> Destination Site	<input type="checkbox"/> Service Name
			<input type="checkbox"/> Source CMTS	<input type="checkbox"/> Subscriber	<input type="checkbox"/> VXLAN Name

# Open Source or Commercial: No Right Answer

- Open Source tools can be used for flow collection and enrichment:
  - Elastiflow
  - Prometheus
- Make sure you do the enrichment at data ingest time or you lose the context and query performance (useability) will suffer
- Like anything Open Source, each organization has to weigh the resource commitment against the cost of commercial offerings
- **Call to Action:** In 2025, you cannot operate a large scale network without a network observability platform that can collect and enrich this data to help your teams make good decisions

# Business Context: The Customer

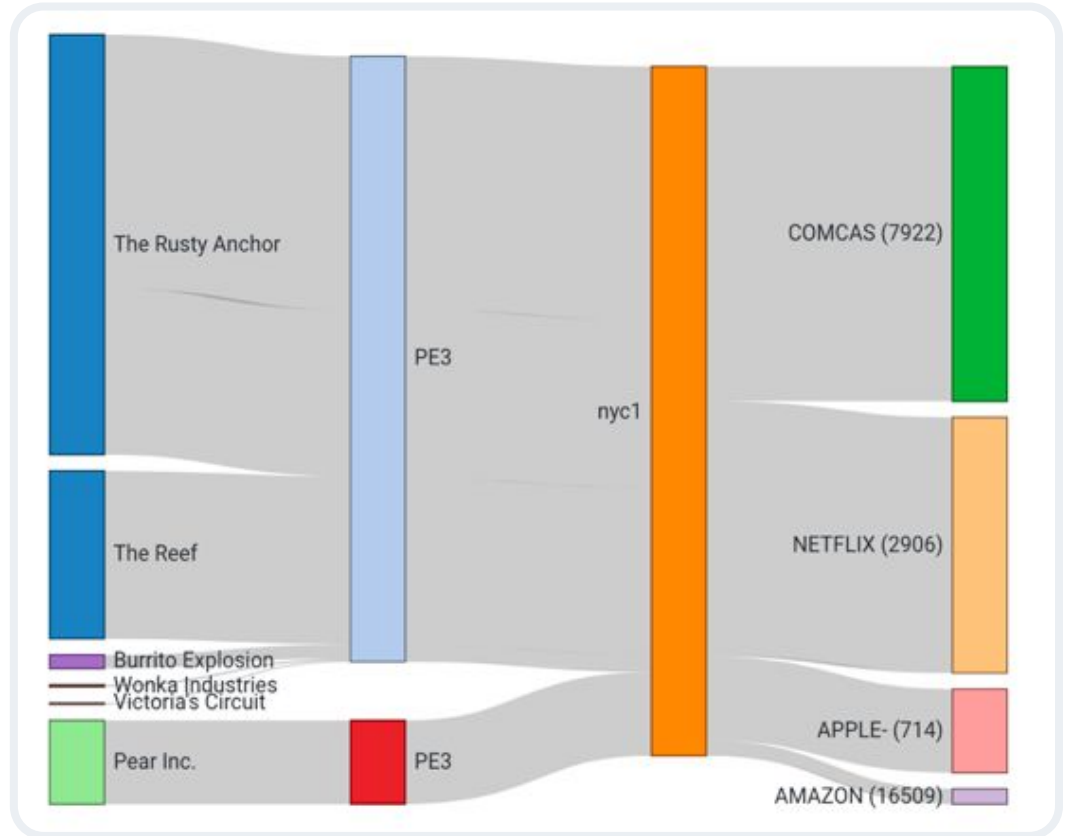
**Edit Custom Dimension** ✕

General Populators 24

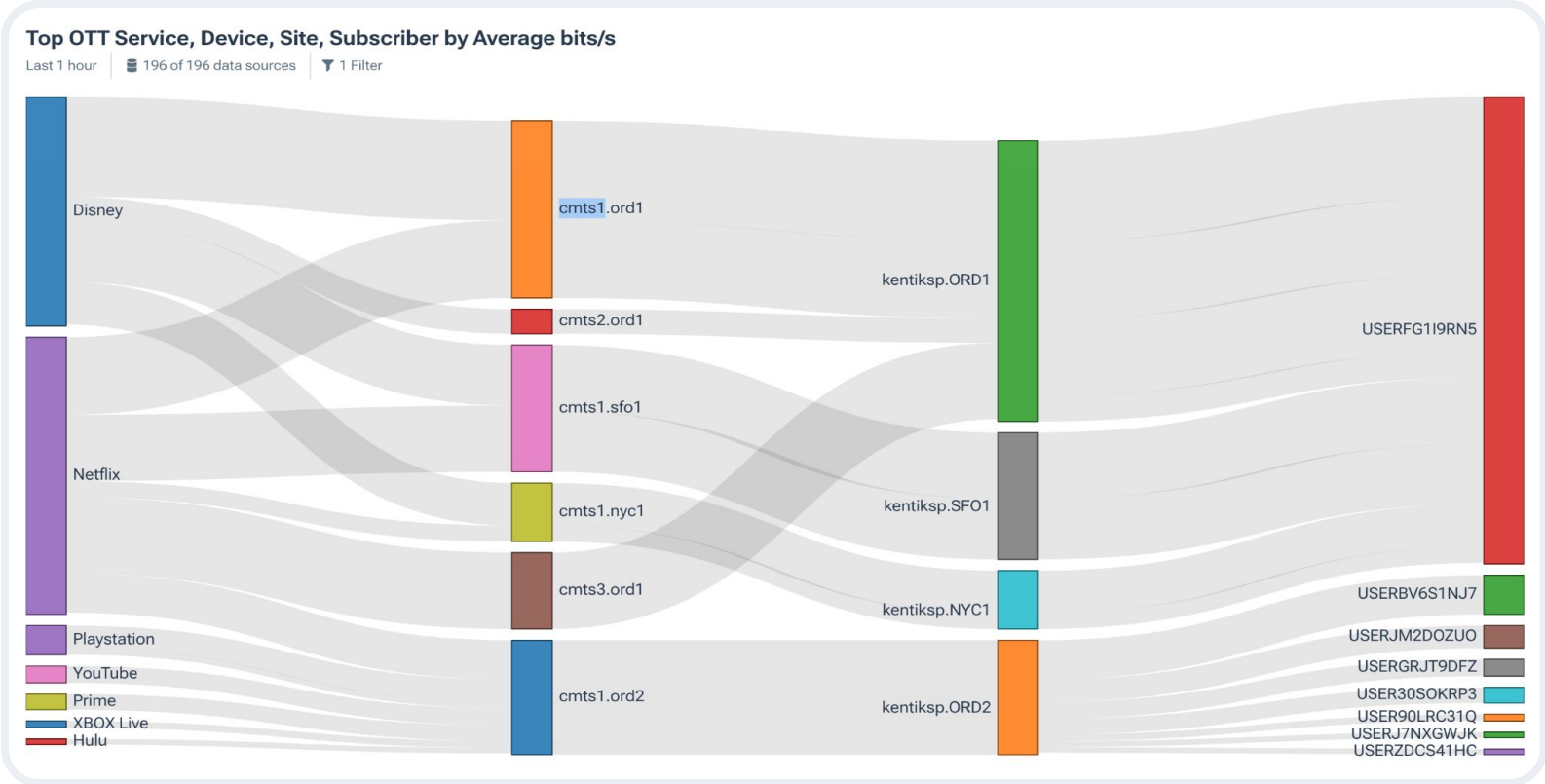
Search Populators... + Add Populator

Value	Direction	ID	
The Acme Packet Com...	Destination	417035	
The Acme Packet Com...	Source	417034	
Pear Inc.	Source	417104	
Pear Inc.	Destination	417105	
Wally World	Source	400466	

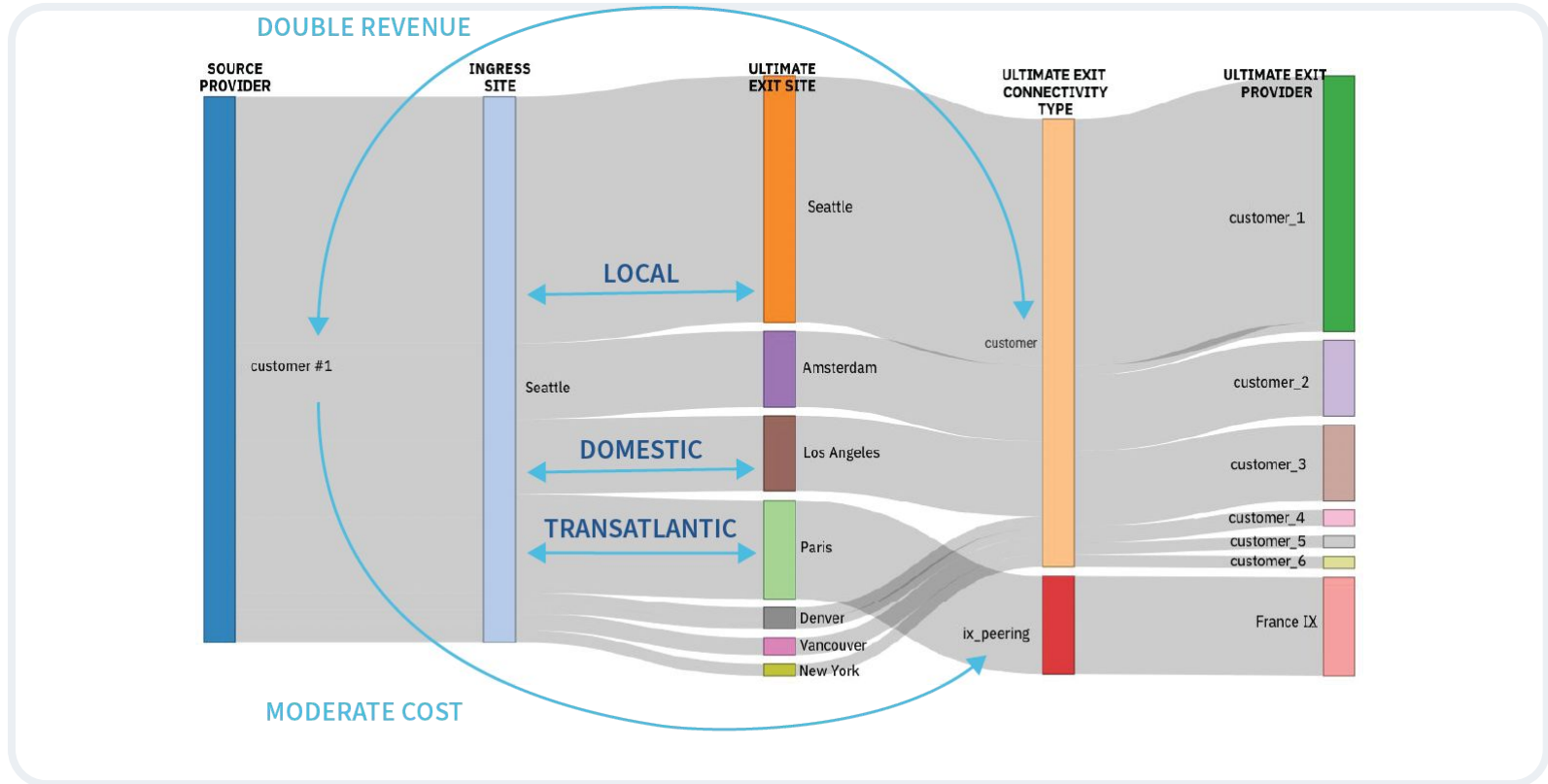
Remove Cancel Save



# Business Context: OTT Service Usage by CMTS, Site, & User

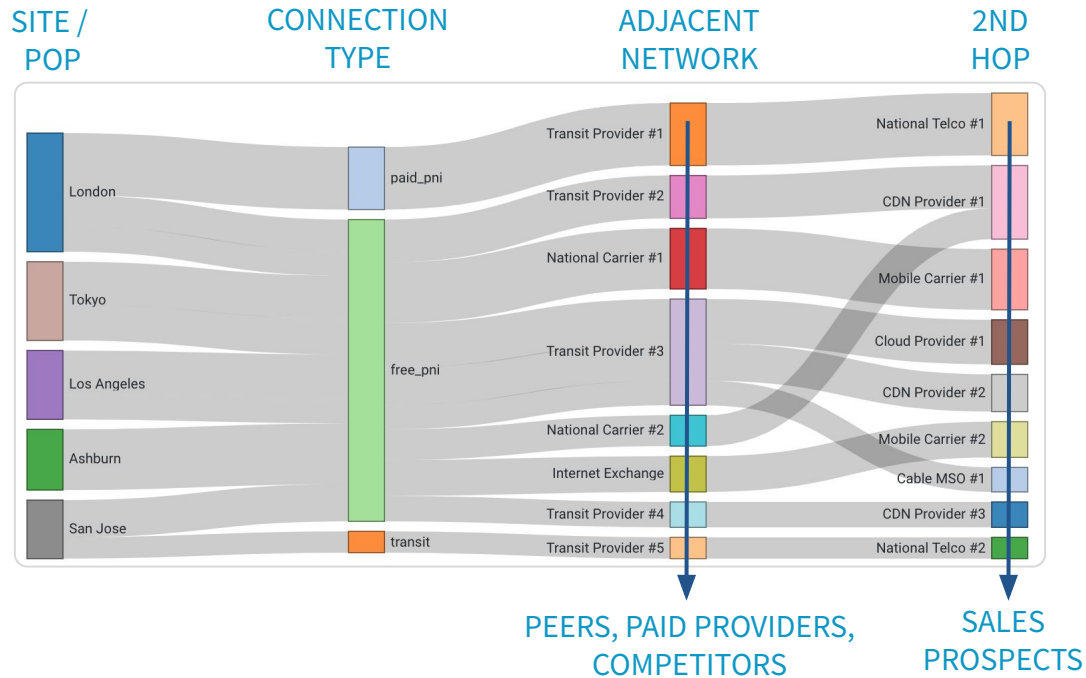


# Business Context: Customer Contract Negotiations





# Business Context: Discover Sales and Upsell Opportunities



# But now what?

- ✓ Alerting with context
- ✓ Outbound API webhooks can trigger network automation workflows
- ✓ Examples:
  - Customized DDoS mitigation
  - Updating ACLs or Firewalls based on dropped traffic
  - Changing routing policies due to congested ports

# Summary



Modern networks are both critical and complex



Network observability is no longer a nice to have



Organizing data by network layer constructs limits the usefulness



Contextual data is needed to fully utilize the power of network data



Network automation can tie the sources of truth into the observability systems to provide this context



Better action can be taken by automation platforms with contextualized observability

**Questions?**



# Thank you!

**Jac Kloots**

**[jac@kentik.com](mailto:jac@kentik.com)**

 [@jkloots](https://twitter.com/jkloots)

 [in/jackloots](https://www.linkedin.com/in/jackloots)

 [Join Kentik on Slack](#)

