**Using Sources** of Truth to **Enrich and** Understand Network Telemetry

Jac Kloots Senior Solutions Engineer



The network observability company



#### Who am I?

#### **Current** Senior Solutions Engineer - <u>Kentik</u>

#### Past

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



## **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?



# Context is needed for network



#### NetFlow is a good step

Source	Destination	Non-Directional / Other	✓ IP & BGP Routing		
<ul> <li>Network &amp; Traffic Topology</li> <li>Interface</li> <li>Connectivity Type</li> <li>Network Boundary</li> <li>Provider</li> <li>Traffic Origination</li> <li>Interface Capacity</li> <li>VLAN</li> <li>MAC Address</li> </ul>	<ul> <li>Interface</li> <li>Connectivity Type</li> <li>Network Boundary</li> <li>Provider</li> <li>Traffic Termination</li> <li>Interface Capacity</li> <li>VLAN</li> <li>MAC Address</li> </ul>	<ul> <li>Ultimate Exit Interface</li> <li>Ultimate Exit Connectivity Type</li> <li>Ultimate Exit Network Boundary</li> <li>Ultimate Exit Provider</li> <li>Simple Traffic Profile</li> <li>Traffic Profile</li> <li>Site</li> <li>Device</li> <li>Site Market</li> <li>Ultimate Exit Site Market</li> <li>Ultimate Exit Site Ultimate Exit Site</li> <li>Ultimate Exit Device</li> <li>Host Direction</li> <li>Device Sample Rate</li> </ul>	<ul> <li>IP/CIDR</li> <li>Site by IP</li> <li>Site Type by IP</li> <li>Port Number</li> <li>Route Prefix/LEN</li> <li>Route LEN</li> <li>AS Number</li> <li>Next Hop IP/CIDR</li> <li>Next Hop AS Number</li> <li>2nd Hop AS Number</li> <li>3rd Hop AS Number</li> <li>3rd Hop AS Number</li> <li>AS Path</li> <li>BGP Community</li> <li>VRF Name</li> <li>VRF Route Distinguisher</li> <li>VRF Extended Route Distinguisher</li> </ul>	IP/CIDR         Site by IP         Ste Type by IP         Port Number         Route Prefix/LEN         Route LEN         AS Number         Next Hop IP/CIDR         Next Hop AS Number         2nd Hop AS Number         3rd Hop AS Number         AS Path         BGP Community         VRF Route Distinguisher         VRF Route Target         VRF Extended Route Distinguisher	<ul> <li>Protocol</li> <li>INET Family</li> <li>DSCP</li> <li>ToS</li> <li>Packet Size</li> <li>Packet Size (nearest 100)</li> <li>Sampling Rate * 100</li> </ul>

- RPKI Quick Status
- Comment Doutine CID

### IP Addresses, Po And Protocols A Not Enough

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



#### **Best Practices for Leveraging Contextual Data**



## **Telemetry Enrichment**



Enrichment with metadata provides context



# **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

#### **Context for the win!**

Source	Destination	Non-Directional / Other	Source	Destination	Non-Directional / Other	
<ul> <li>Network &amp; Traffic Topology</li> </ul>			- Application Context & Secu	rity		
<ul> <li>IP &amp; BGP Routing</li> <li>Cloud</li> </ul>			<ul><li>Public Cloud Provider</li><li>Public Cloud Service</li><li>CDN</li></ul>	<ul> <li>Public Cloud Provider</li> <li>Public Cloud Service</li> <li>CDN</li> </ul>	Application TCP Flags OTT Service	
Geolocation	Custom Geo	Site Country	<ul><li>Service (Port+Proto)</li><li>Bot Net CC</li><li>Threat List Host</li></ul>	Service (Port+Proto) Bot Net CC Threat List Host	OTT Service Type OTT Service Provider	
Country Region	Country Region	Ultimate Exit Site Country	- Custom			
City	City		<ul> <li>Source Location</li> <li>Source Site</li> <li>Source CMTS</li> </ul>	Dest Location Destination Site Subscriber	Customer ID Service Name VXLAN Name	

### **There's no Right Answer**

- Many tools can be used for flow collection and enrichment
- 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**

🔅 General		Populators 24		
Search Populators	4		+ Add Populato	
Value	Direction	ID		
The Acme Packet Com	Destination	417035	/ 8	
The Acme Packet Com	Source	417034	/ 8	
Pear Inc.	Source	417104	/ 8	
Pear Inc.	Destination	417105	/ 8	
Wally World	Source	400466	/ 8	



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

Top OTT Service, Device, Site, Subscriber by Average bits/s

Last 1 hour 196 of 196 data sources T 1 Filter



#### Business Context: Customer Contract Negotiations



#### Business Context: Discover Sales and Upsell Opportunities



# But now what?



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





# **Thank you!**

#### Jac Kloots jac@kentik.com

🥑 @jkloots

in/jackloots

Join Kentik on Slack

#### **Contact Ayscorp**m.com +34 91 3768225

