



Network
Visibility for All

- » To really ensure user experience...
- » Need network, system, and application visibility, all integrated.
- » But network, APM, logs, and metrics, have all been siloed systems.
- » Kentik takes network traffic data; solves network nerd problems.
- » Like peering, planning, DDoS, performance, and security analytics.
- » W/ backend storing all the data, with no aggregates or roll-ups.
- » But what about the rest of the company?
- » Grafana is everywhere ☺
- » So we had Grafana Labs develop the Kentik Connect app.

- » Why > than metrics for network?

- » “Is it the Network?” is WAY too common

- » “How can we not know?”

- » But Network data is big data

- » Kill “Aggregate and Discard”

- » And kill Siloes

- » But DIY is a large effort



Network traffic & performance data

Servers/
Agents



Routers



Switches



Sensors



Secure Multi-Tenant SaaS or On-Premises Option



Cross-Organizational Network Visibility



NetOps



Network Security



Network Planning

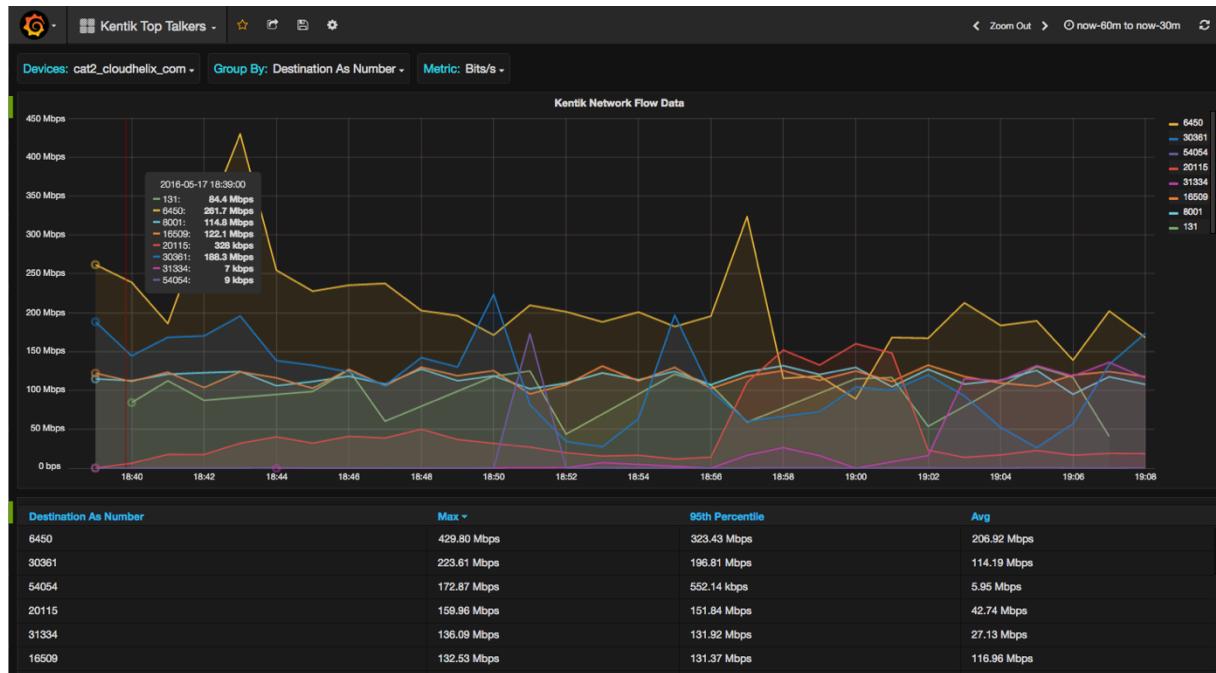


Finance



Sales

- » Root cause involves systems, network, & apps.
- » Grafana integration fills traffic and netperf gap for correlating and exposing on metrics dashboard.
- » Providing all three critical views.
- » For many kinds of groups and users.





PANDORA®

OpenDNS

instartlogic



dailymotion

neustar®





Architecture ➤

Kentik | Kentik By The Numbers

3 SECOND
ingest-to-query latency

90+ DAYS
raw data retention

15 multi-terabit
customers

<2 SECOND
95th percentile response time

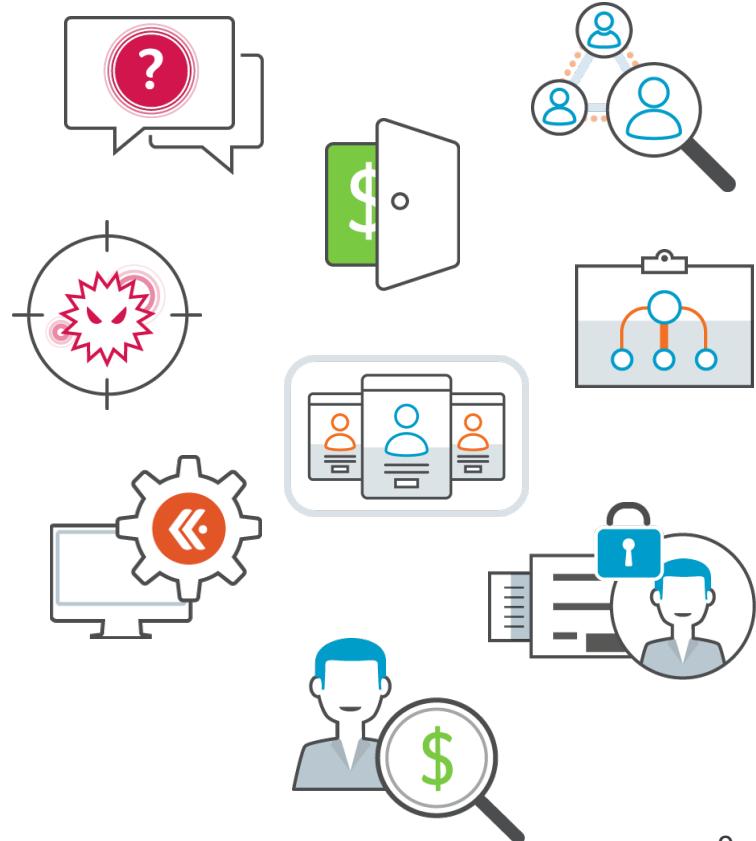
20 billion avg.
daily flow records


100x faster than


15 MINUTES
to production from
initial registration

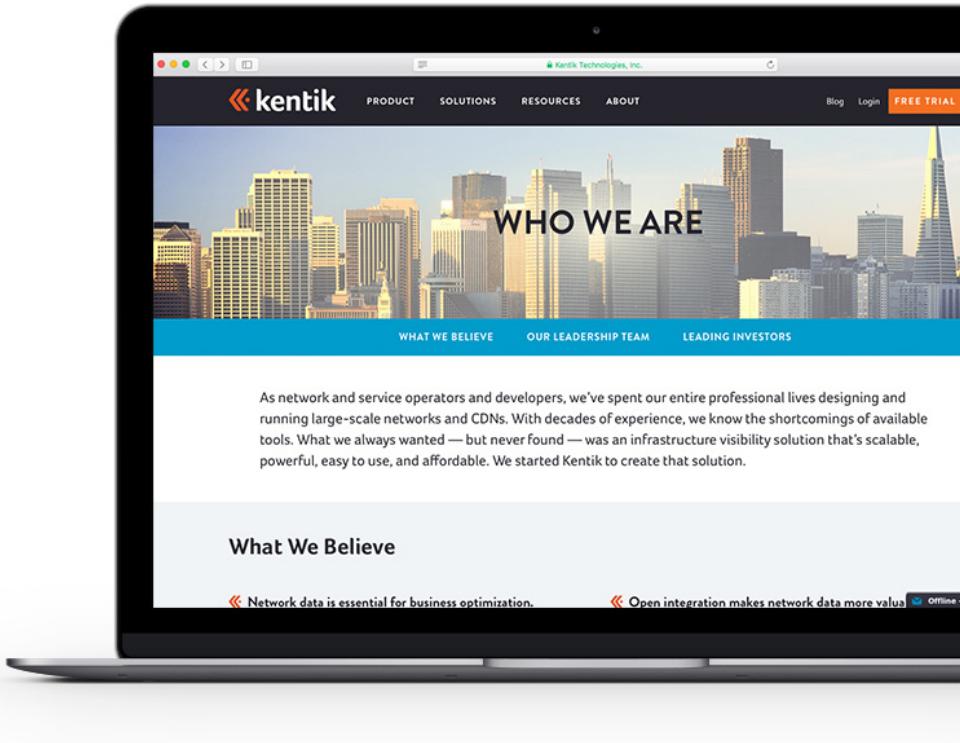
10x more efficient than


- » Instant, escalation-free troubleshooting
- » Peering and transit analytics
- » Sales prospecting & customer success
- » DDoS detection and mitigation
- » Capacity planning
- » Cross-team access and collaboration
- » Portal integration
- » Infrastructure & customer security
- » Customer cost analytics



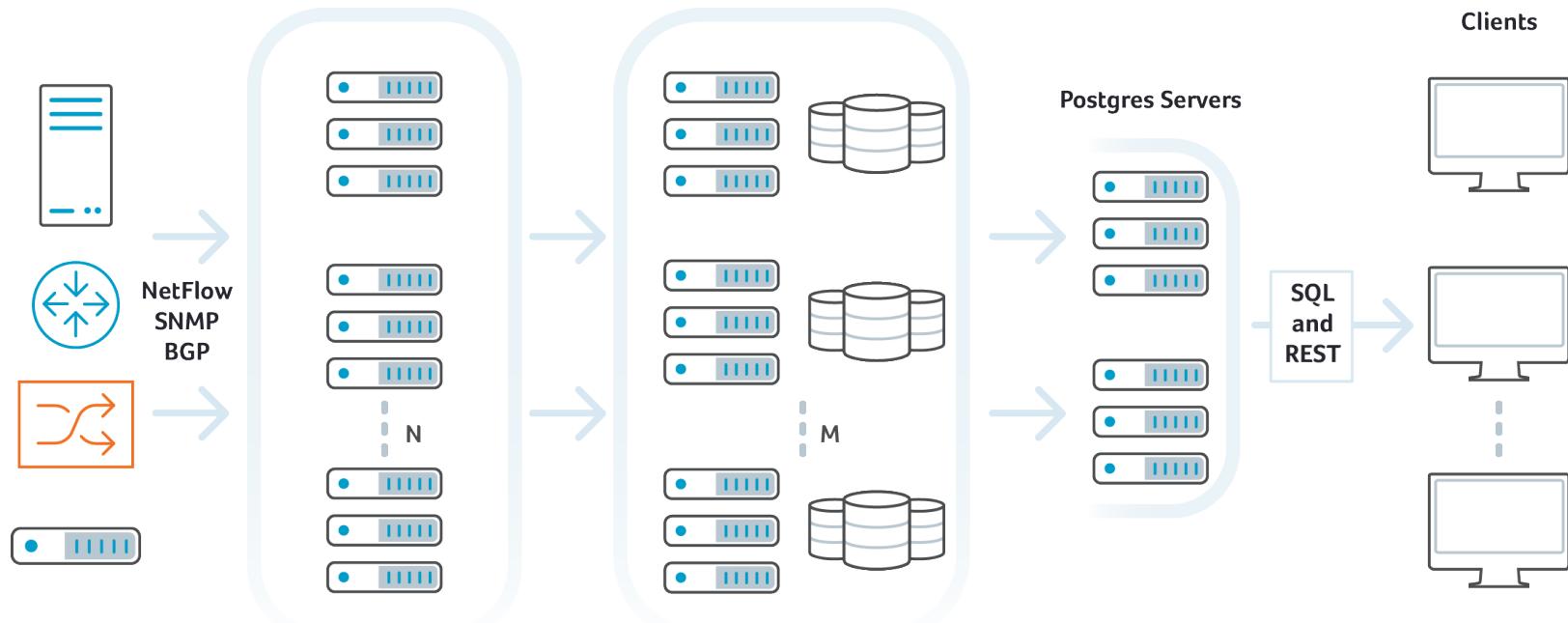
Note: Service Provider audience

- » 3 year old company, HQ in San Francisco
- » SaaS network traffic visibility provider
- » Founders from Akamai, Netflix, YouTube, CloudFlare

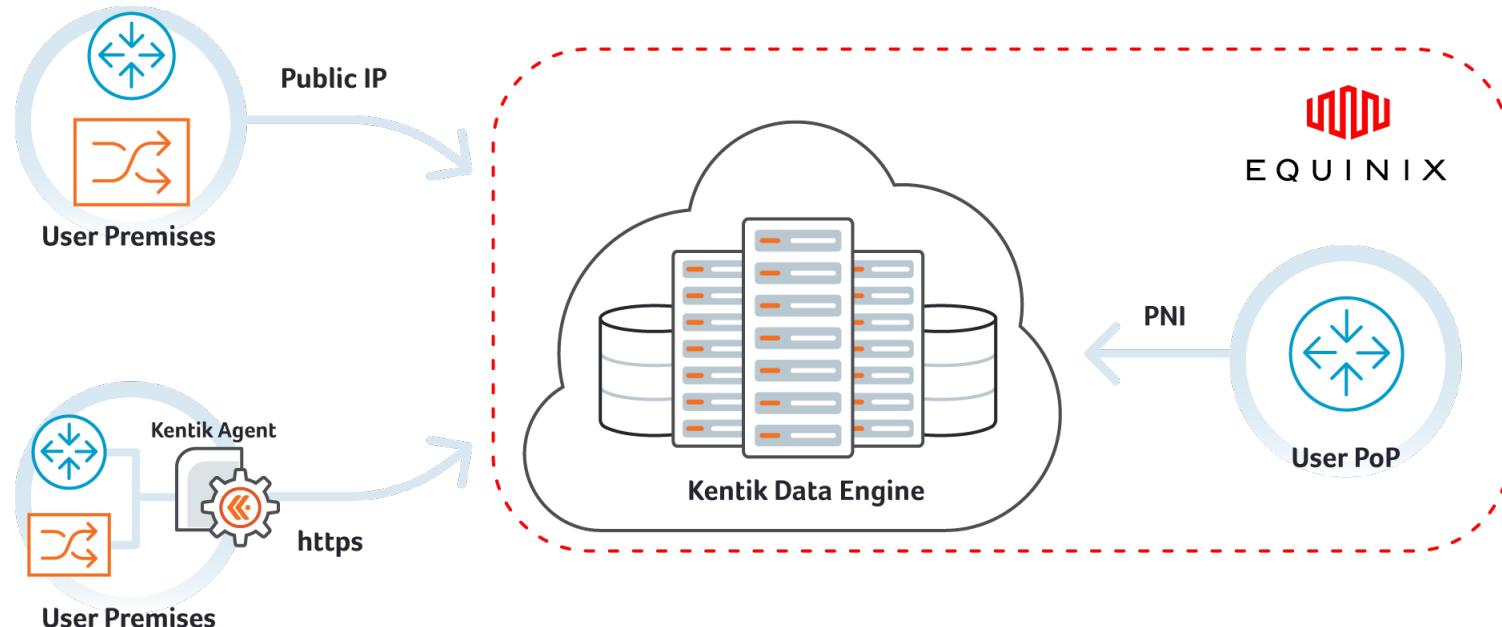


The Need	Fast, unlimited drill-down, full retention back-end
Kentik Data Engine	Column-store, distributed system supporting SQL, REST, multi-tenancy, and extensible schema. Bare-metal, containerized, micro-services architecture
Modeled After	Akamai Query and Google Dremel
Comparatives	10x to 100x speed and 10x+ advantage over Hadoop, Impala, Drill, Spark, Cassandra, and Red Hat

kentik | Kentik Data Engine Architecture



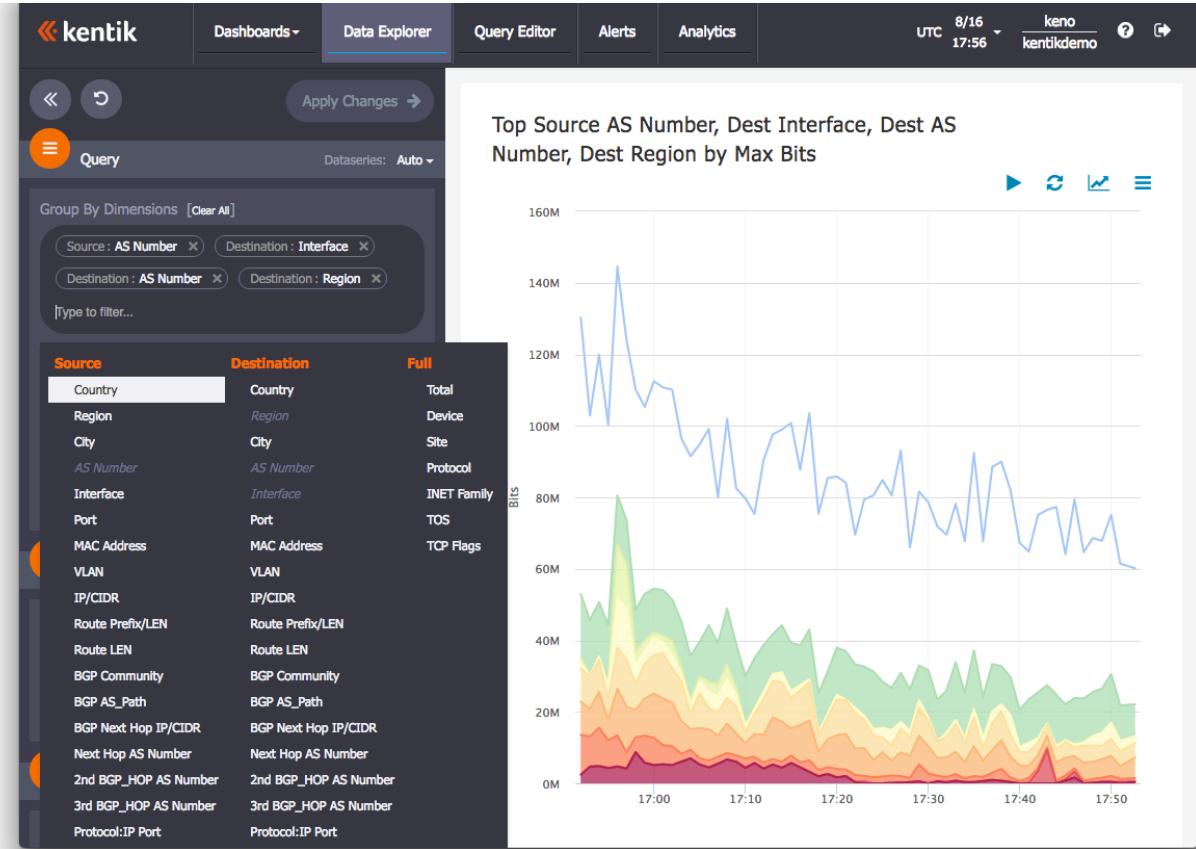
Kentik | Getting Your Data to Kentik



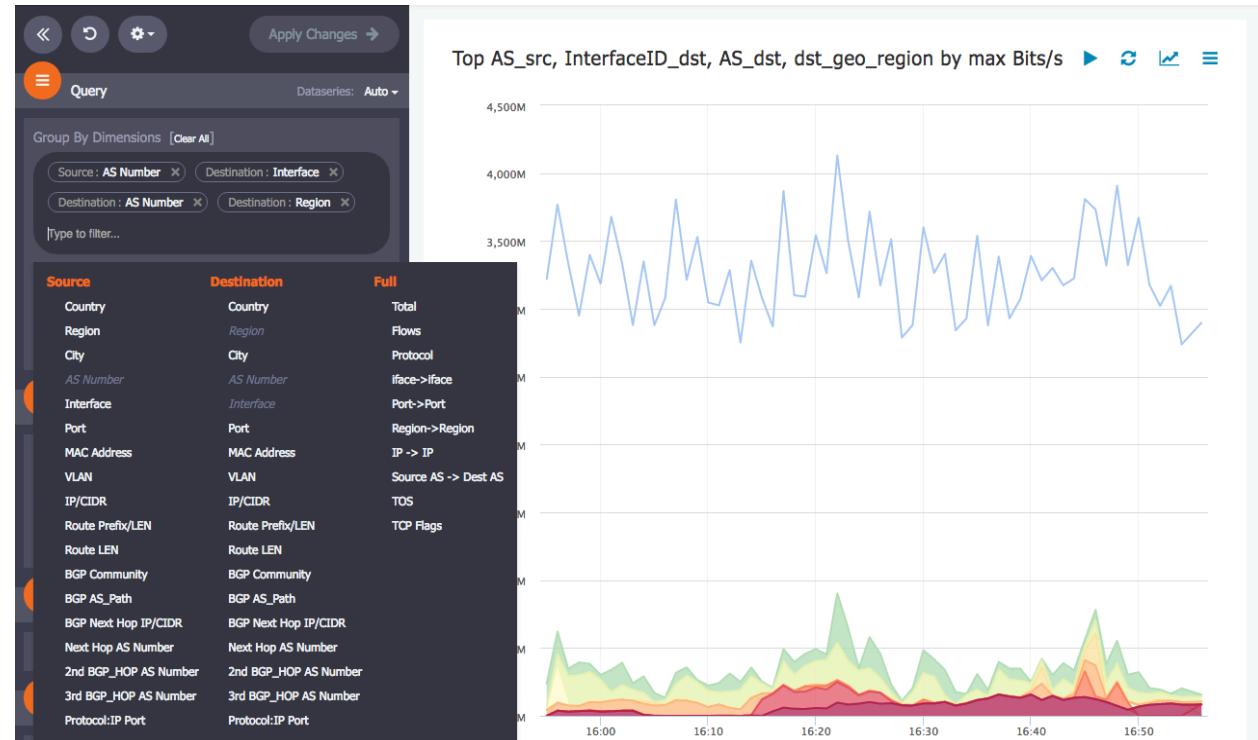
Use Cases



- » 90 days (or more) of instantly accessible raw flows
- » No aggregation, no roll-ups, no data cube fragility
- » Instant data cubes
- » Ad-hoc, raw data query: 95%ile response < 2 seconds
- » Benefits:
 - Service assurance
 - Operational excellence
 - Shift to Innovation



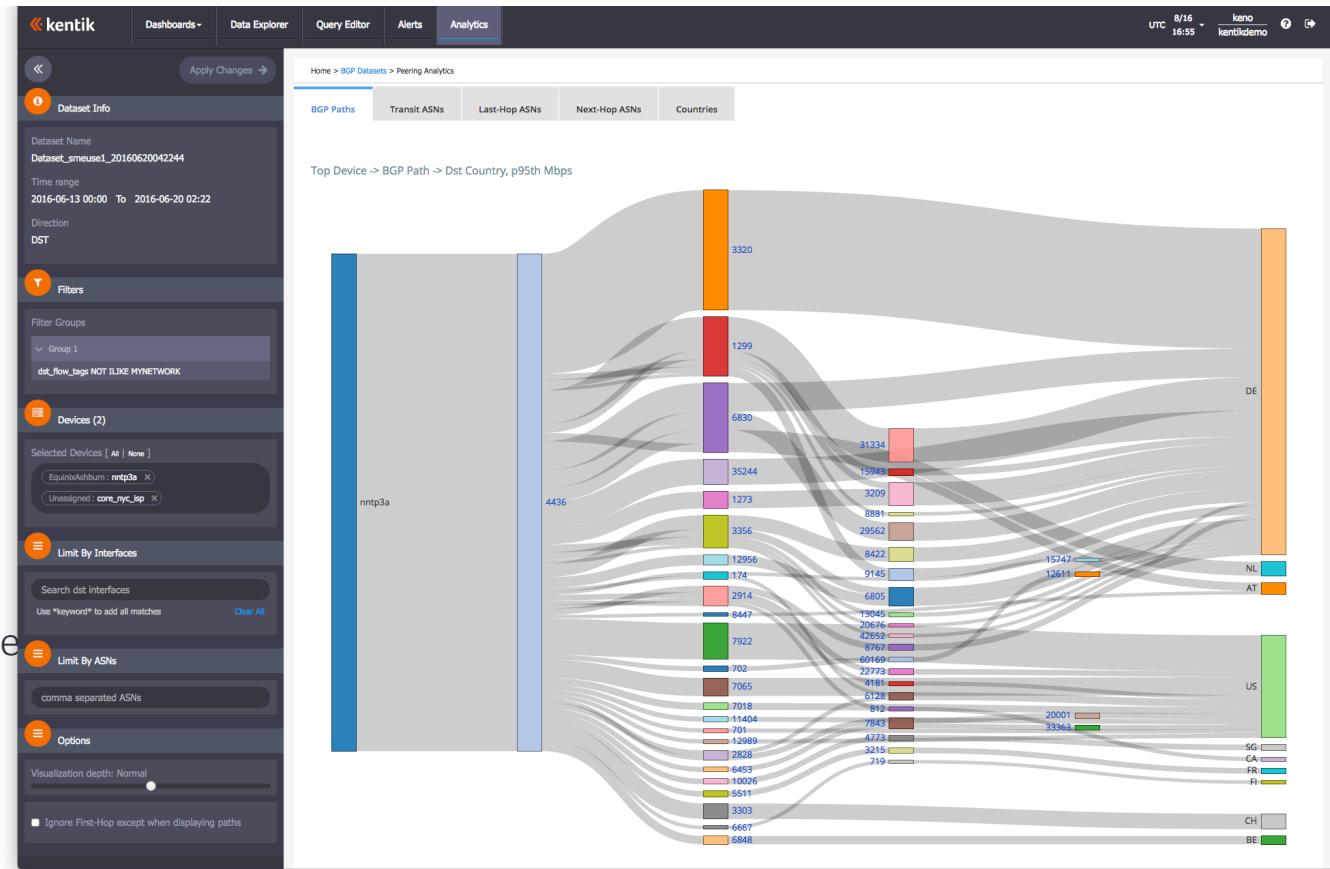
- » 90 days (or more) of instantly accessible raw flows
- » No aggregation, no roll-ups, no data cube fragility
- » Instant data cubes
- » Ad-hoc, raw data query: 95%ile response < 2 seconds
- » Benefits:
 - Service assurance
 - Operational excellence
 - Shift to Innovation



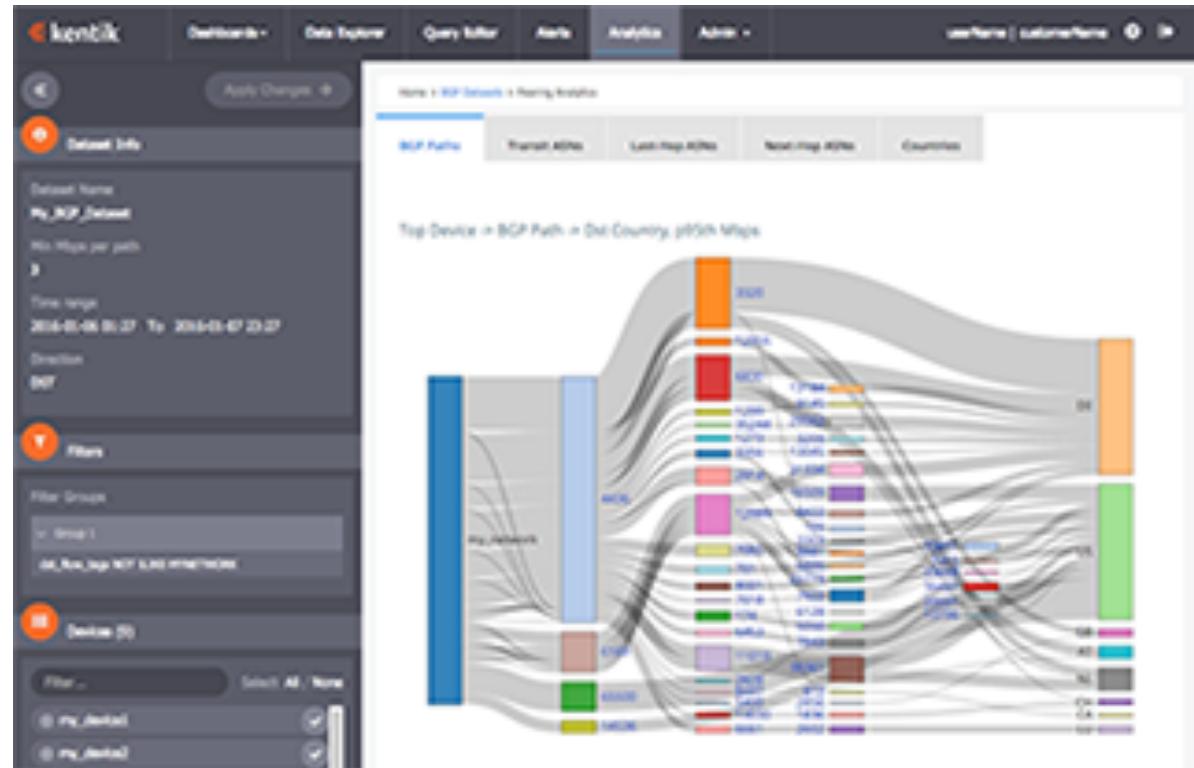
- » Flexible, network-wide detection
- » Alerts operate on order of seconds, not five minute data segments
- » Exploratory analytics to hunt for threats and intrusions
- » Rapidly adjust alerts with new insights
- » Automated mitigation options
- » Benefits:
 - Minimal false positives & negatives
 - Keep up with changing threats

- » New state of the art for peering analytics
- » Interactive BGP path visualizations
- » Instantaneous filtering and drill-down - no waiting!
- » Benefits:

- Reduce costs
- Increase performance and resilience
- Find new business opportunities



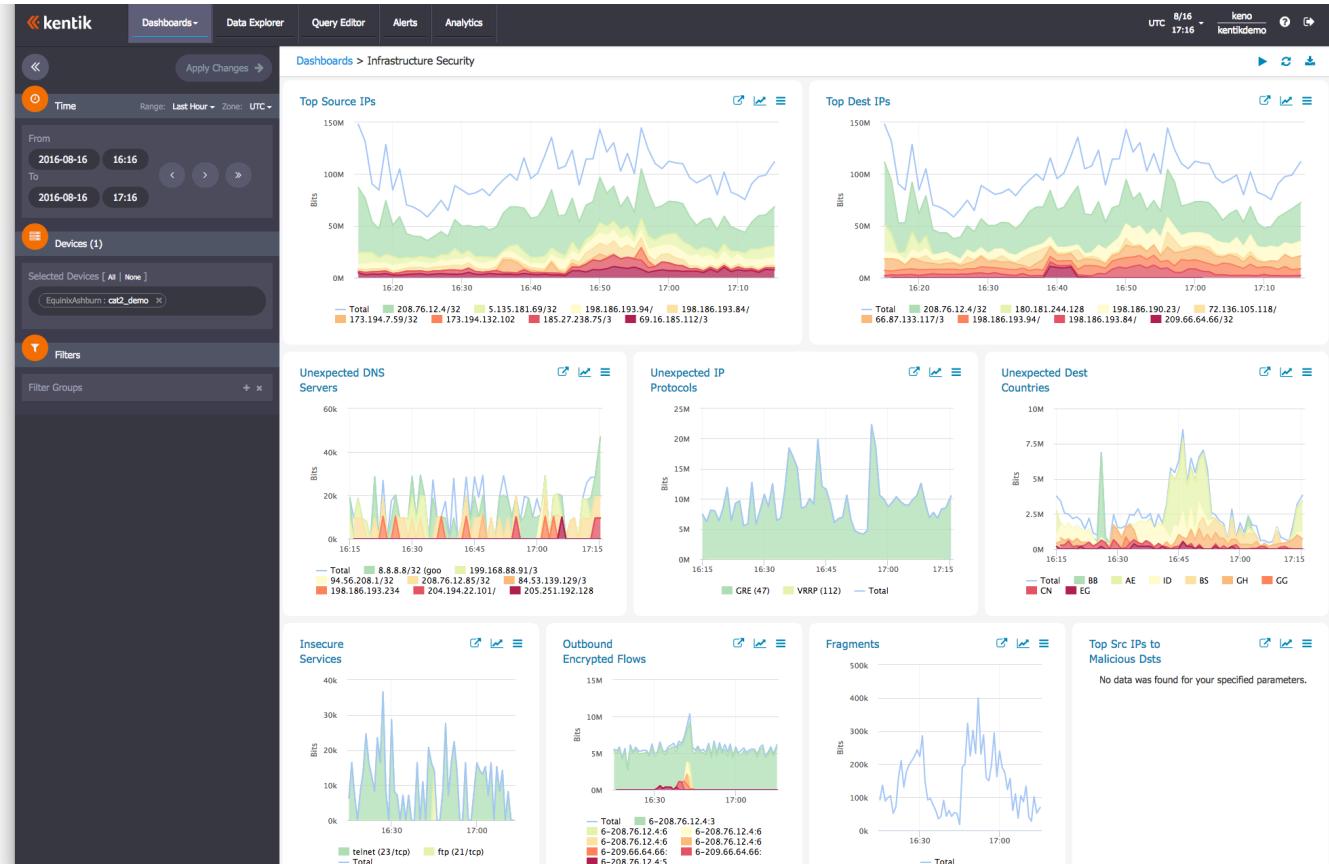
- » New state of the art for peering analytics
- » Interactive BGP path visualizations
- » Instantaneous filtering and drill-down - no waiting!
- » Benefits:
 - Reduce costs
 - Increase performance and resilience
 - Find new business opportunities



- » Long-term storage of detailed records
- » Agile, fast DDoS detection & mitigation
- » Extensible flow data model including security semantics
- » Ease of integration with Splunk and SIEMs
- » Multi-tenant access to protect one analyst or query from swamping the system

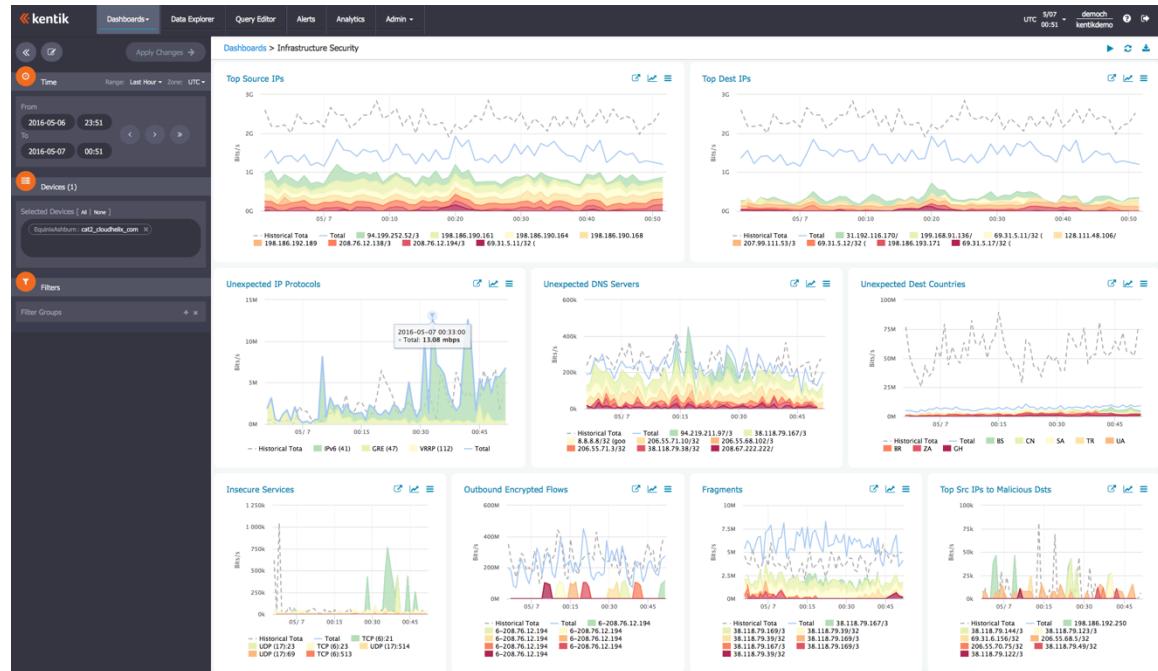
kentik | Build and Share Dashboards for Multiple Teams

- » Any analysis can be saved to a dashboard
- » Build any number of audience-specific dashboards
- » Email PDF reports from any dashboard to configurable subscription list



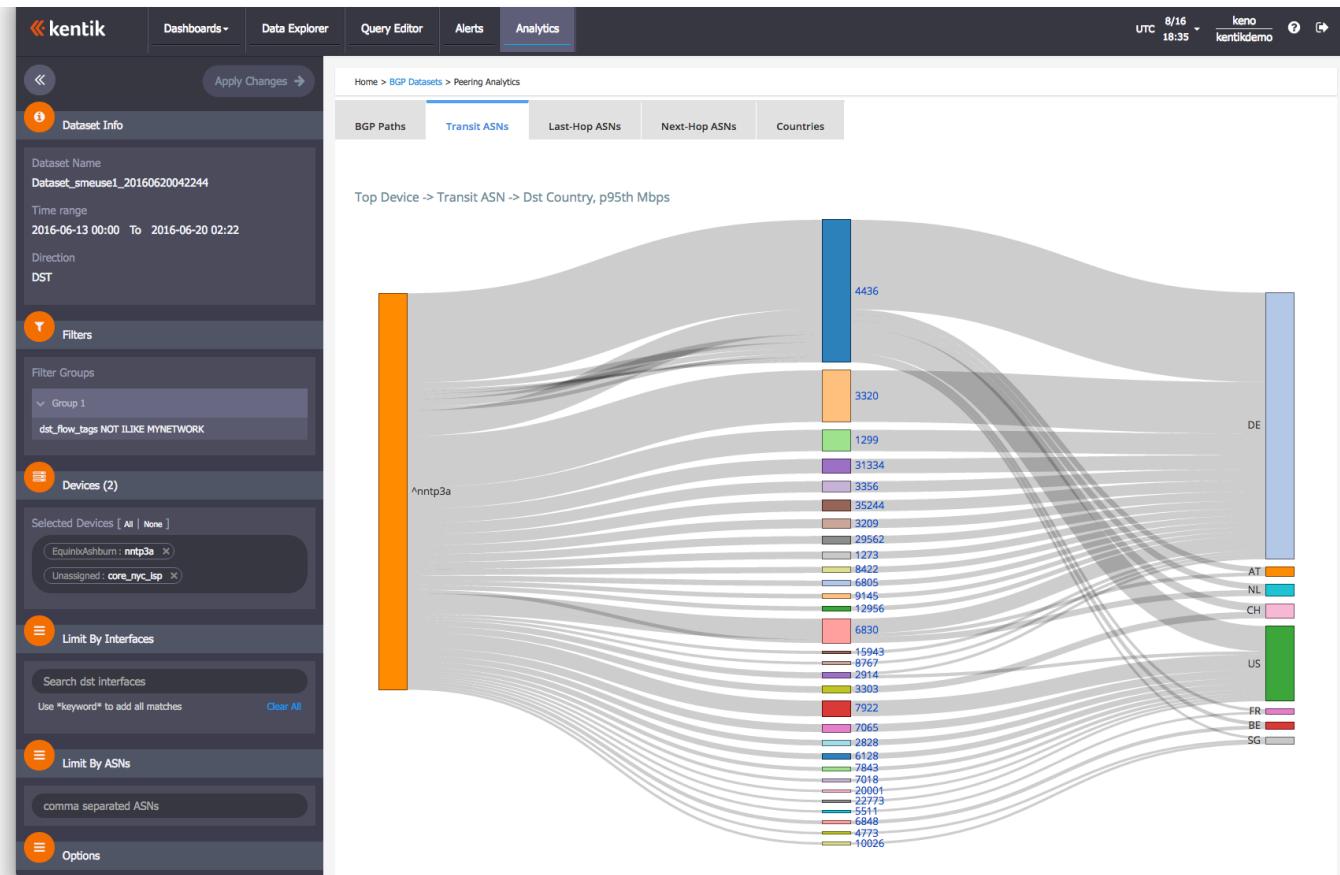
kentik | Build and Share Dashboards for Multiple Teams

- » Any analysis can be saved to a dashboard
- » Build any number of audience-specific dashboards
- » Email PDF reports from any dashboard to configurable subscription list

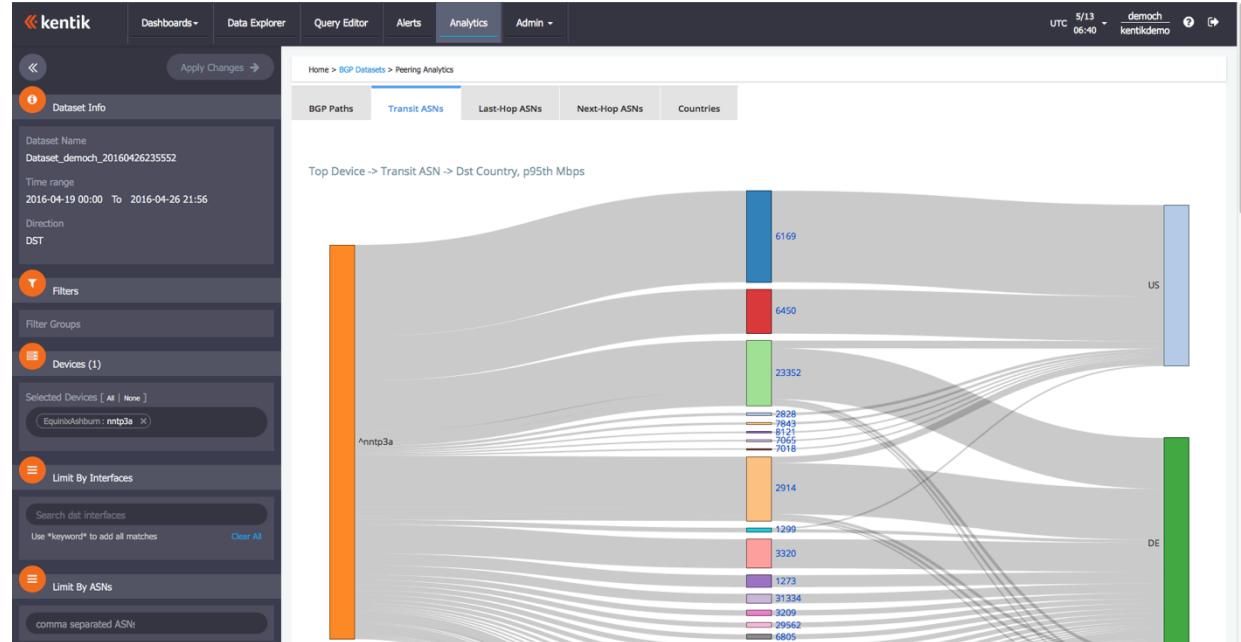


kentik | Sales Prospecting: Transit ASNs View

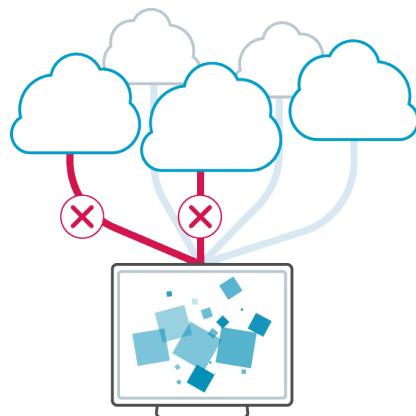
» Find transit networks that are potential customers



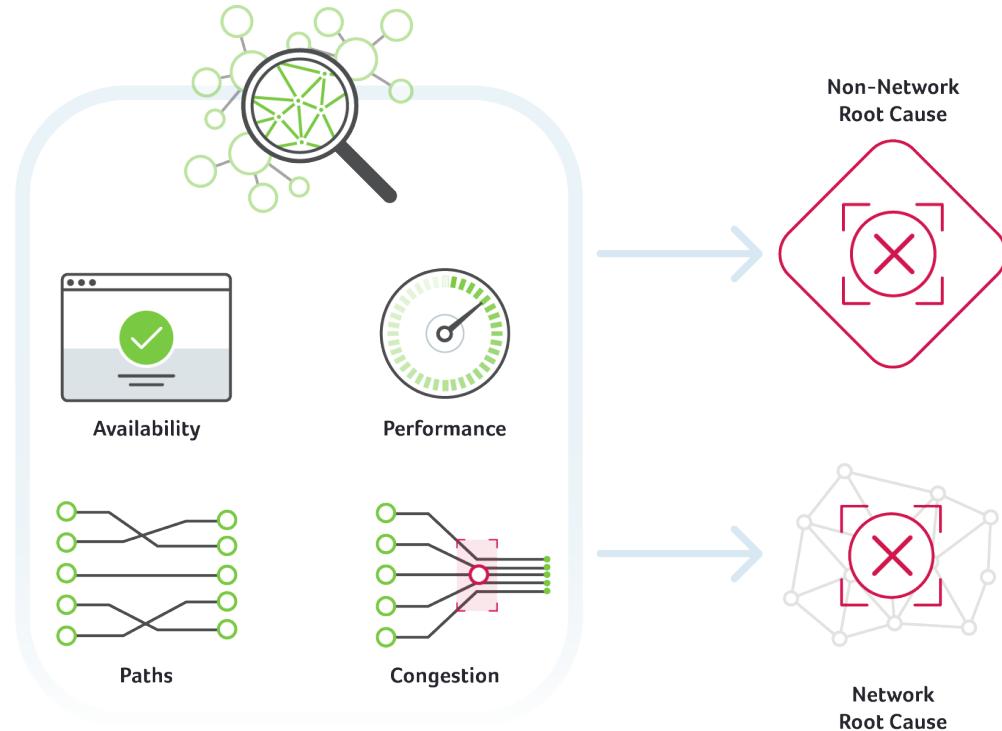
» Find transit networks that are potential customers



Application Performance Issues



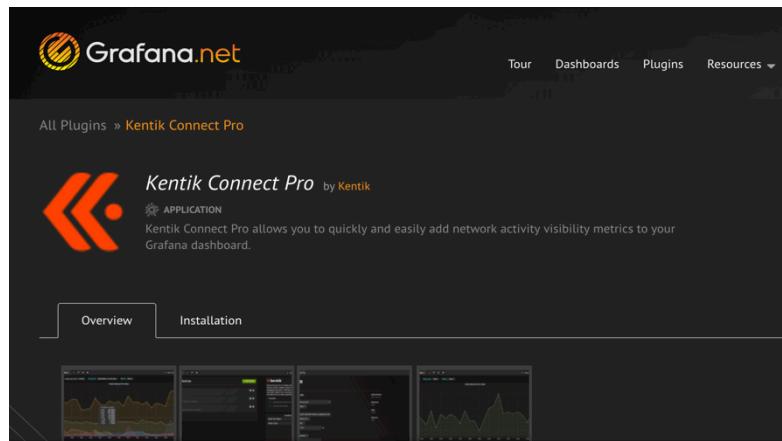
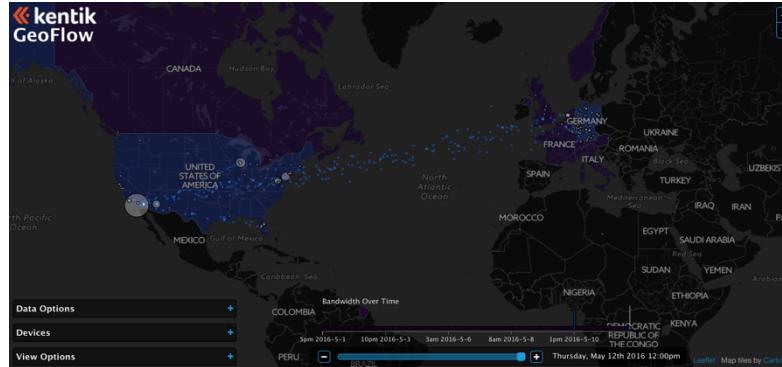
Analyze Network



- » **Problem:** “Our customers know about issues before we do!”
 - » **Solution:** Find & mitigate issues faster!
 - » Flexible alerting for many use cases:
 - Security, ops, availability, performance
 - » Network-wide scope with raw data granularity
 - » Very low latency

Alert Dashboard											UTC 7/14 21:22	democh	kentikdemo	?	✉		
Group By		Key	Alert Log										Clear Selected		All times are in UTC		
	Key	Alert Name	Criticality	State	Key Type	Output 1 Name:Value	Output 2 Name:Value	Alert ID	Start	End	Time Over Threshold	Recent Comment					
■	207.44.120.174	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-05 19:17	2016-07-05 19:18	2%						
■	198.186.190.161	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 1	mbps : 0	3483	2016-07-05 19:14	2016-07-05 19:21	3%						
■	204.186.2.126	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 03:12	2016-07-02 03:12	1%						
■	204.186.80.230	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 03:09	2016-07-02 03:09	1%						
■	66.152.151.99	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 02:41	2016-07-02 03:14	2%						
■	66.152.151.101	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 02:37	2016-07-02 02:38	2%						
■	204.186.129.159	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 02:33	2016-07-02 02:55	3%						
■	70.44.184.217	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 02:30	2016-07-02 02:31	2%						
■	66.152.138.19	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 02:27	2016-07-02 02:57	2%						
■	24.115.201.50	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 02:12	2016-07-02 02:12	1%						
■	24.115.63.149	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 01:51	2016-07-02 02:58	2%						
■	204.186.110.113	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 01:50	2016-07-02 03:11	3%						
■	70.15.241.182	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 01:23	2016-07-02 01:51	2%						
■	204.186.74.73	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 01:20	2016-07-02 02:43	2%						
■	204.186.62.206	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 01:19	2016-07-02 03:16	0%						
■	209.173.16.222	JSON_test2	Critical	ACK_REQ	ipv4_dst_addr	pps : 34	mbps : 0	3483	2016-07-02 01:17	2016-07-02 01:36	2%						

- » Highly performant APIs
- » REST & SQL
- » Sample integrations:
 - Grafana.net
 - Auvik.com
 - ServerCentral
 - GeoFlow (Tor)



- » Identify critical ‘digital trading partners’ in your supply chain
 - E.g. Key API partners and external users
- » Monitor and analyze in real-time
- » Ensure performance and availability
- » Establish and manage advantageous peerings

- » Add traffic tags for each service, user, sub-network
- » Leverage routing information to support “packet mile” cost analysis
- » Analyze patterns for upstream and downstream traffic
- » Analyze individual or groups of links by customer or application
- » Variable granularity from high-level aggregation to individual flows



Thank You!



| www.kentik.com