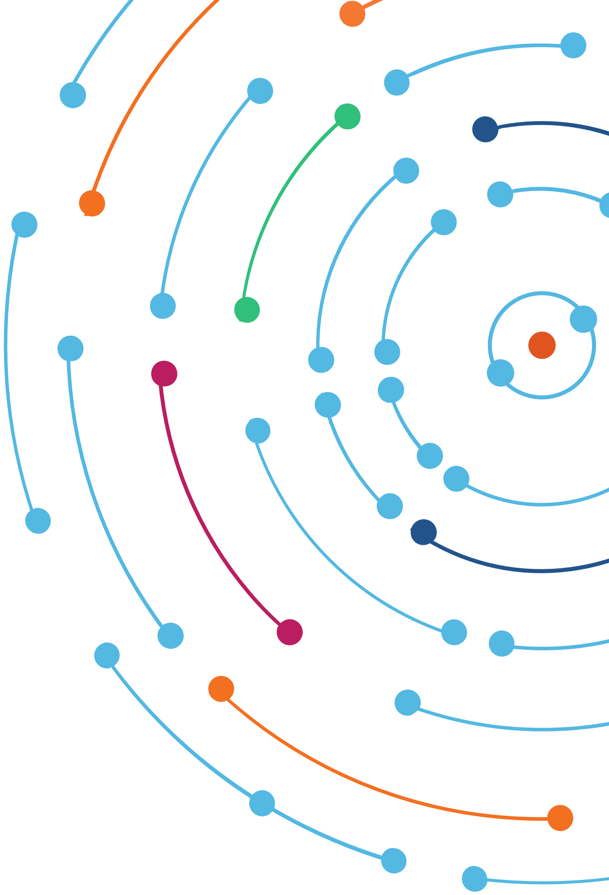
kentik®

# What is Network Observability?

RSNOG November 2021

Nina

Director, GTM Strategy



# A bit about Kentik

**300+**
ENTERPRISE CUSTOMERS

**EVERY**
NETWORK

**EVERY**
COUNTRY

**95%+**
CSAT

**>25%**
INCREASED UPTIME

**TRILLIONS**
RECORDS/DAY

T Mobile · IBM · verizon media · Uber · Principal · zoom

cisco · sky · salesforce · KDDI · ebay · box

# Kentik is the Network Observability Company

**300+**
ENTERPRISE CUSTOMERS

**EVERY**
NETWORK

**EVERY**
COUNTRY

**95%+**
CSAT

**>25%**
INCREASED UPTIME

**TRILLIONS**
RECORDS/DAY

T Mobile | IBM | verizon media | Uber | Principal | zoom

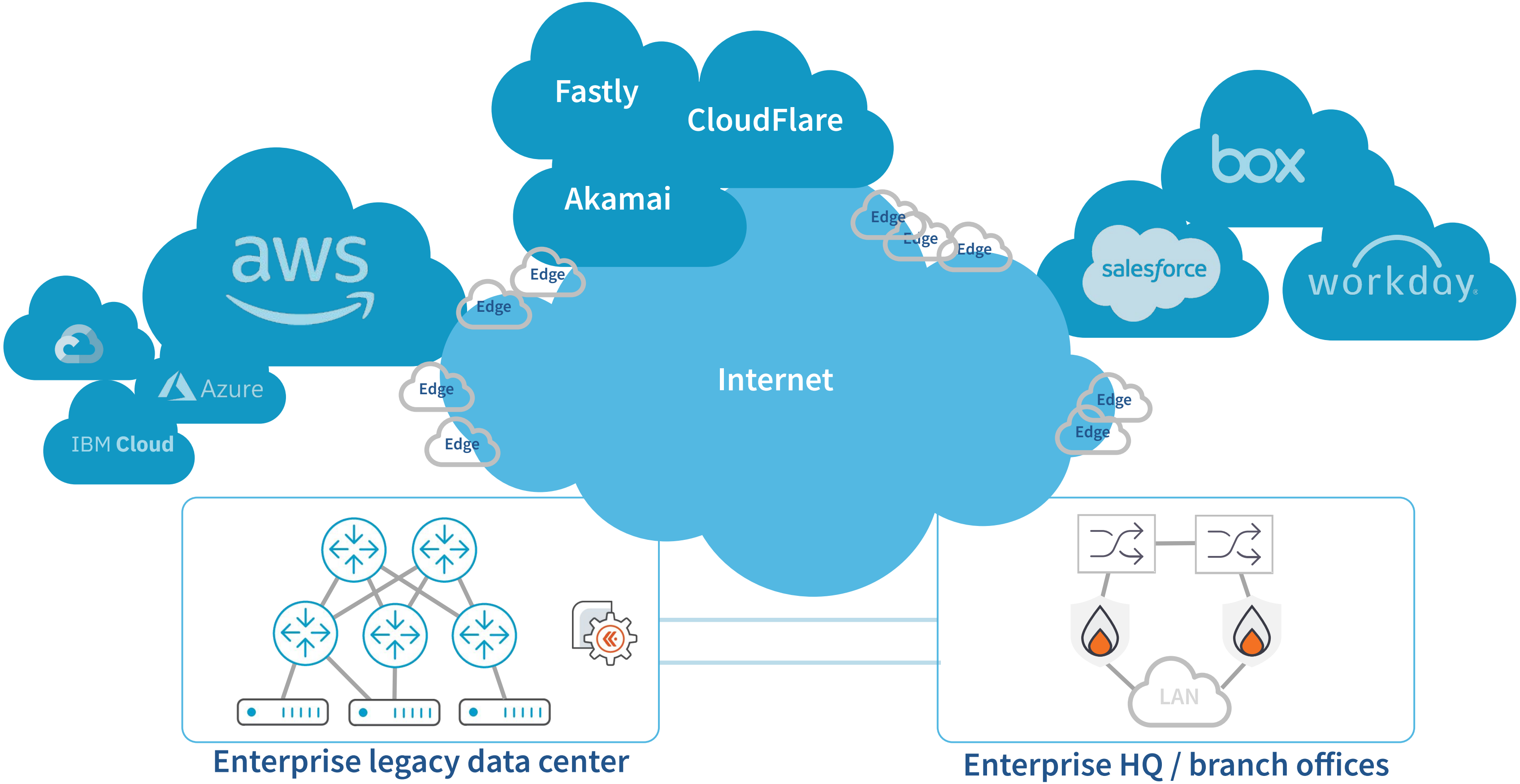
cisco | sky | salesforce | KDDI | ebay | box

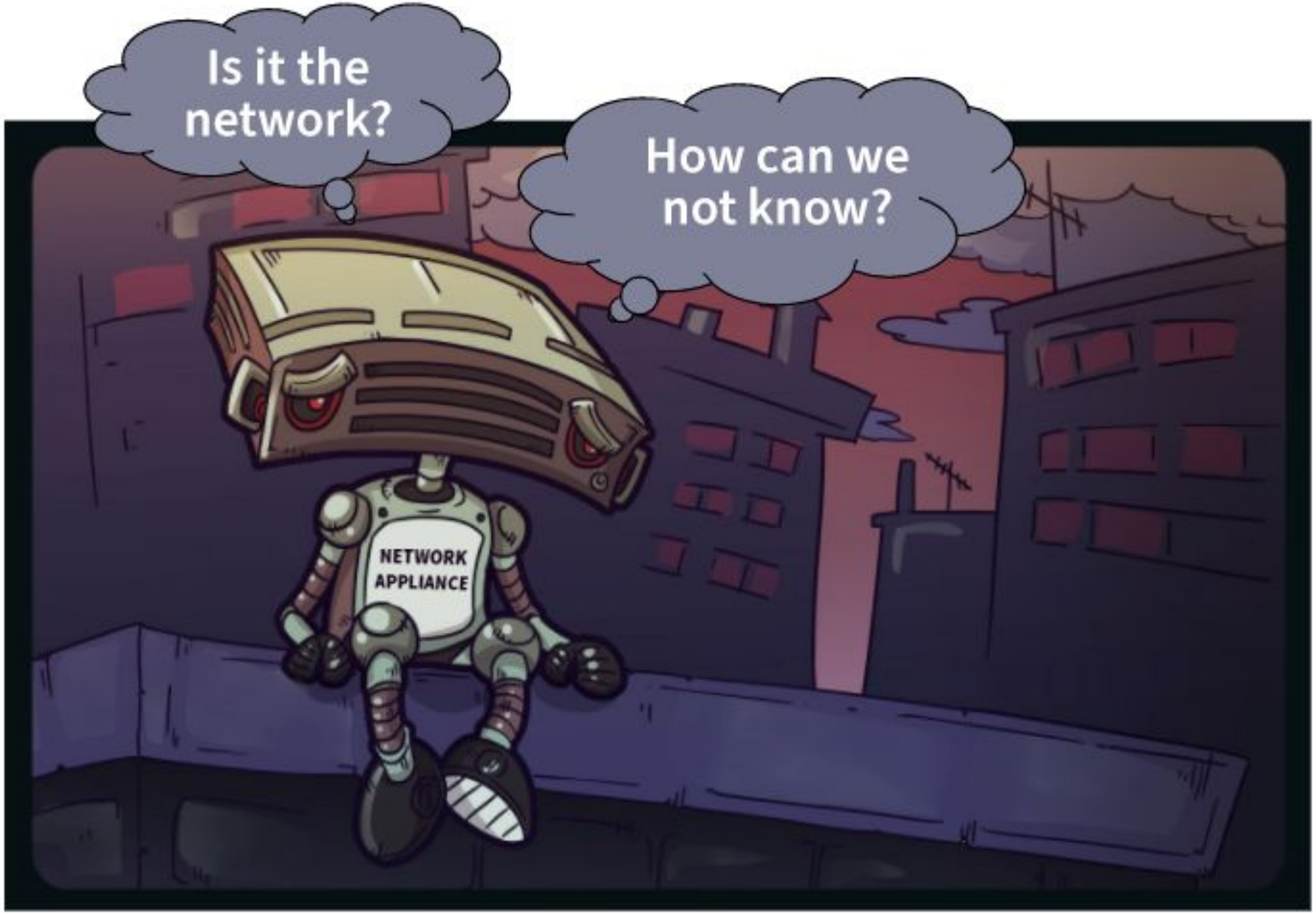
# And a bit about me

## Nina Bargisen

- Director, Go To Market Strategy
- **Prior to this** I  spent a couple of decades building the internet at Subspace, Netflix and TDC
- A passionate sailor

# It’s not all your network anymore




Is it the network?
How can we not know?
NETWORK APPLIANCE

# The observability wave

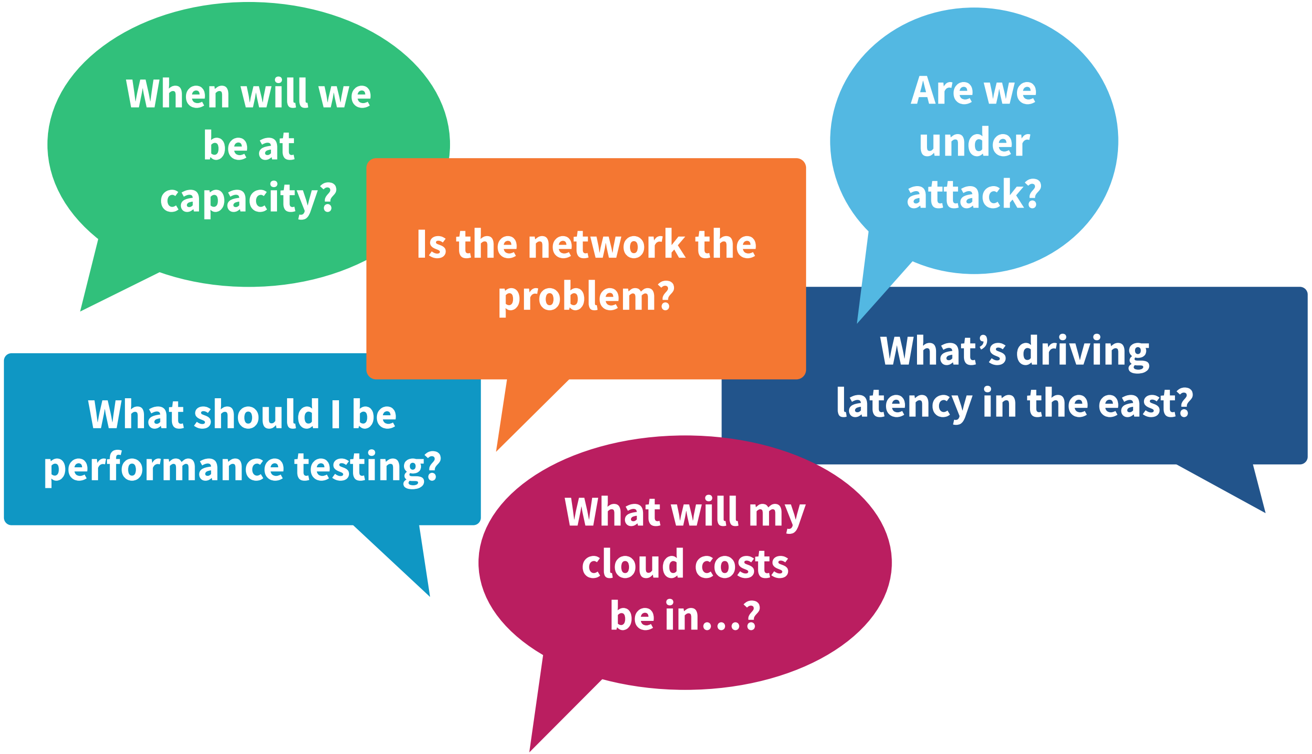
- **Observability** is the ability to understand system behavior by looking at its outputs

- Leading platforms are **challenged by networking constructs** (paths, prefixes, maps) and the numbers, particularly of IP addresses

- **But observability CAN be for networks too!** It requires:
    - Consuming high volume of network data
    - Learning and asking in network terms
    - Integrating with traditional observability data and platforms

# What is network **OBSERVABILITY**?

It’s the ability to answer *any* question about your network



When will we be at capacity?

Is the network the problem?

Are we under attack?

What should I be performance testing?

What’s driving latency in the east?

What will my cloud costs be in…?

# The six requirements for network observability

**See**
all networks

**Correlate**
traffic and
performance

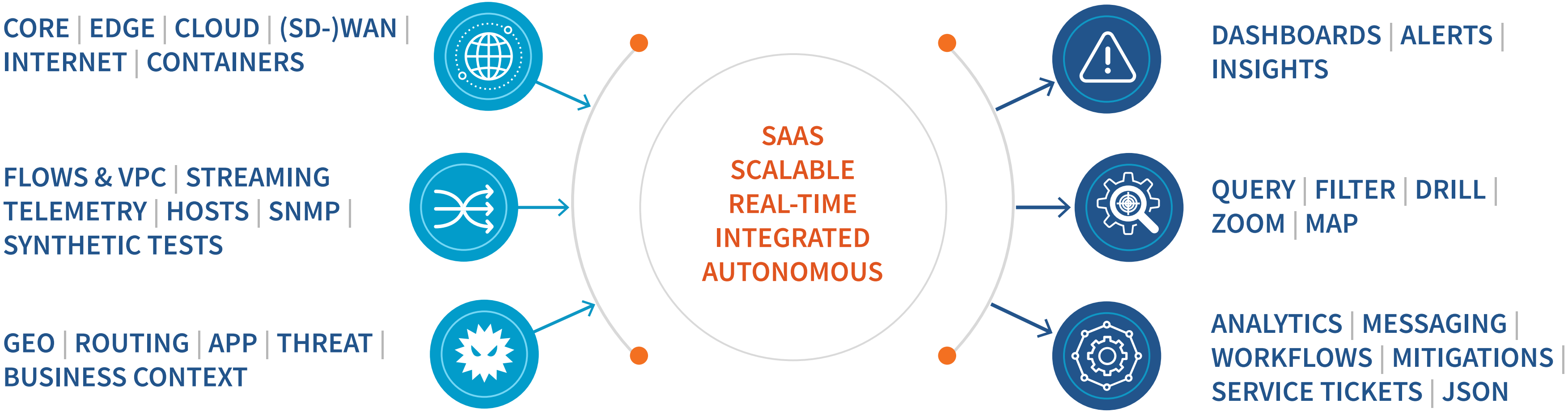
Add **context**
(business,
app, cloud)

Get **Insights**
that provide
clarity

**Ask**
any question

**Automate**
routine tasks

# What Good Network Observability Looks Like



CORE | EDGE | CLOUD | (SD-)WAN | INTERNET | CONTAINERS

FLOWS & VPC | STREAMING TELEMETRY | HOSTS | SNMP | SYNTHETIC TESTS

GEO | ROUTING | APP | THREAT | BUSINESS CONTEXT

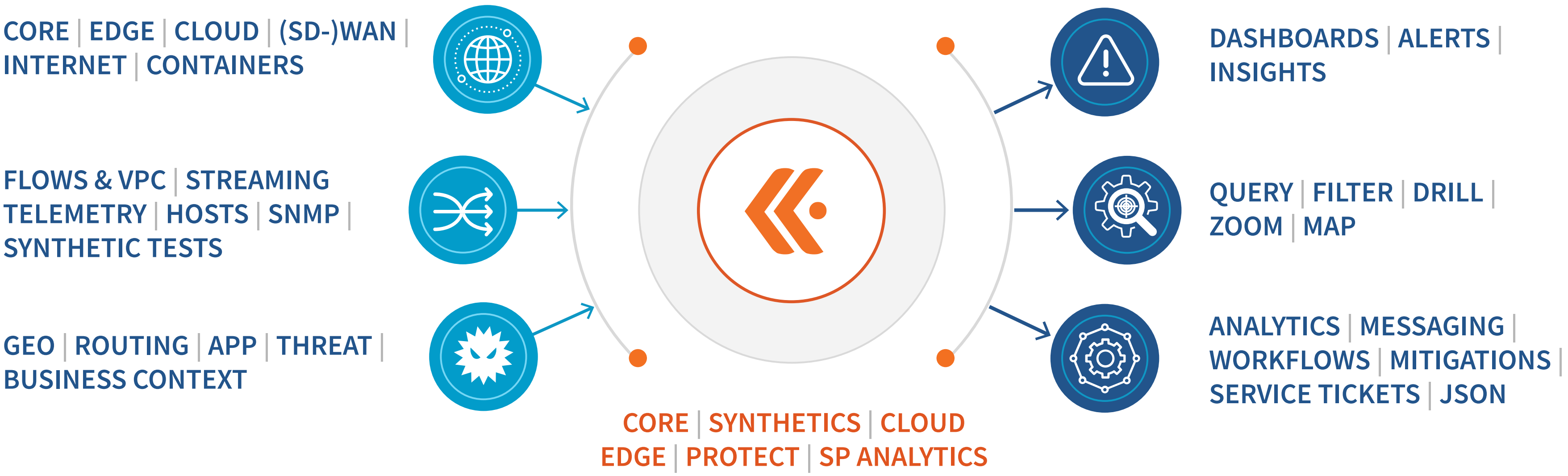
SAAS
SCALABLE
REAL-TIME
INTEGRATED
AUTONOMOUS

DASHBOARDS | ALERTS | INSIGHTS

QUERY | FILTER | DRILL | ZOOM | MAP

ANALYTICS | MESSAGING | WORKFLOWS | MITIGATIONS | SERVICE TICKETS | JSON

# What Good Network Observability Looks Like



CORE | EDGE | CLOUD | (SD-)WAN | INTERNET | CONTAINERS

FLOWS & VPC | STREAMING TELEMETRY | HOSTS | SNMP | SYNTHETIC TESTS

GEO | ROUTING | APP | THREAT | BUSINESS CONTEXT

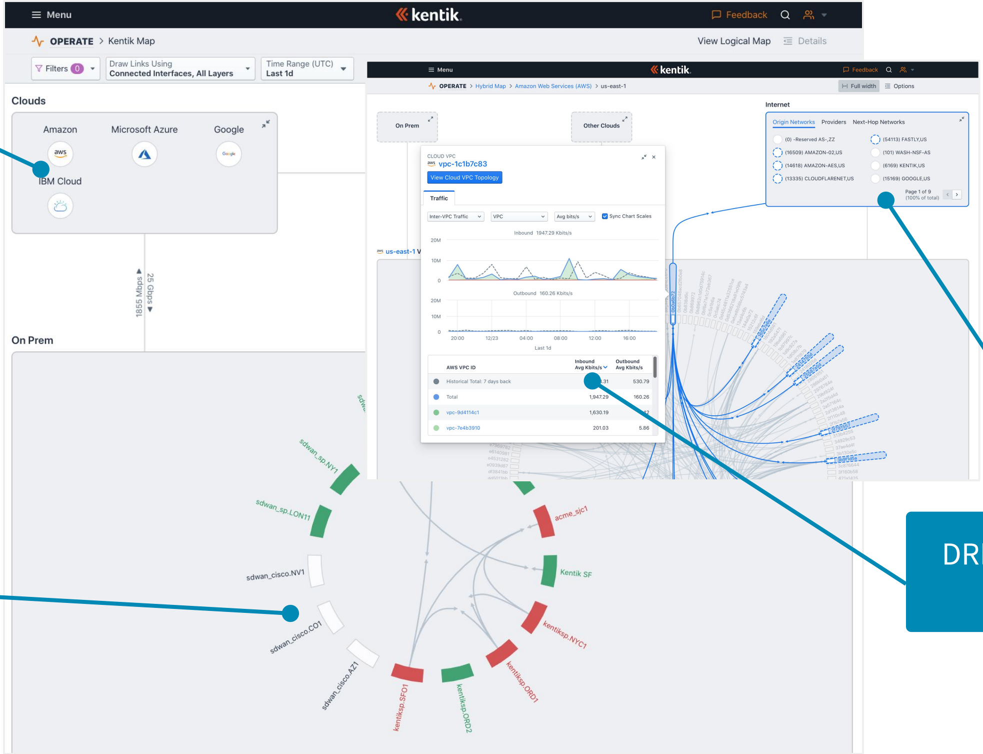
CORE | SYNTHETICS | CLOUD
EDGE | PROTECT | SP ANALYTICS

DASHBOARDS | ALERTS | INSIGHTS

QUERY | FILTER | DRILL | ZOOM | MAP

ANALYTICS | MESSAGING | WORKFLOWS | MITIGATIONS | SERVICE TICKETS | JSON

# Requirement 1: See all networks



| | AWS VPC ID | Inbound Avg Kbits/s | Outbound Avg Kbits/s |
|---|---|---|---|
| ● | Historical Total: 7 days back | [illegible]3.31 | 530.79 |
| ● | Total | 1,947.29 | 160.26 |
| ● | vpc-9d4114c1 | 1,630.19 | [illegible]42 |
| ● | vpc-7e4b3910 | 201.03 | 5.86 |

SEE CLOUDS & NETWORKS TOGETHER

DISCOVER ROUTES & PATHWAYS

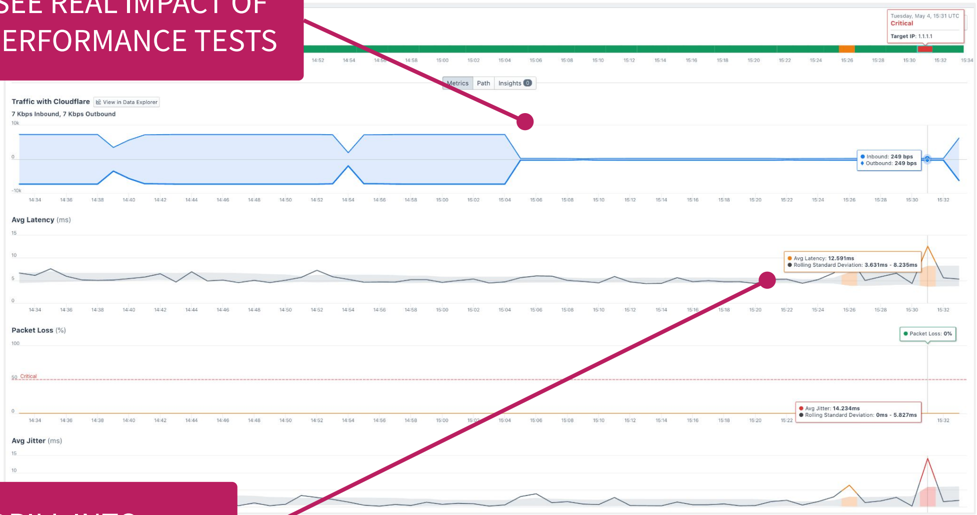
SEE & DRILL INTO PERFORMANCE DETAILS

DRILL TO GRANULAR DETAILS

> “ Why are Boston users having O365 issues? | Why is Azure slow to S3? | Can Fastly get to AWS well?

# Requirement 2: Correlate traffic flows and performance tests

SEE REAL IMPACT OF PERFORMANCE TESTS



Tuesday, May 4, 15:31 UTC
Critical
Target IP: 1.1.1.1

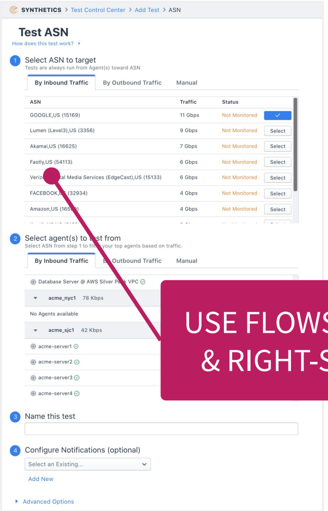
● Inbound: 249 bps
♦ Outbound: 249 bps

● Avg Latency: 12.591ms
● Rolling Standard Deviation: 3.631ms - 8.235ms

● Packet Loss: 0%

● Avg Jitter: 14.234ms
● Rolling Standard Deviation: 0ms - 5.827ms

DRILL INTO SPECIFIC EVENTS



SYNTHETICS > Test Control Center > Add Test > ASN

## Test ASN

How does this test work? ▸

1 Select ASN to target
Tests are always run from Agent(s) toward ASN

| ASN | Traffic | Status | |
|---|---|---|---|
| GOOGLE,US (15169) | 11 Gbps | Not Monitored | ✓ |
| Lumen (Level3),US (3356) | 9 Gbps | Not Monitored | Select |
| Akamai,US (16625) | 7 Gbps | Not Monitored | Select |
| Fastly,US (54113) | 6 Gbps | Not Monitored | Select |
| Verizon Digital Media Services (EdgeCast),US (15133) | 6 Gbps | Not Monitored | Select |
| FACEBOOK,US (32934) | 4 Gbps | Not Monitored | Select |
| Amazon,US (16509) | 4 Gbps | Not Monitored | Select |

2 Select agent(s) to test from
Select ASN from step 1 to filter your top agents based on traffic.

Database Server @ AWS Silver Peak VPC ✓
▾ acme_nyc1 78 Kbps
No Agents available
▾ acme_sjc1 42 Kbps
acme-server1 ✓
acme-server2 ✓
acme-server3 ✓
acme-server4 ✓

3 Name this test

4 Configure Notifications (optional)
Select an Existing...
Add New

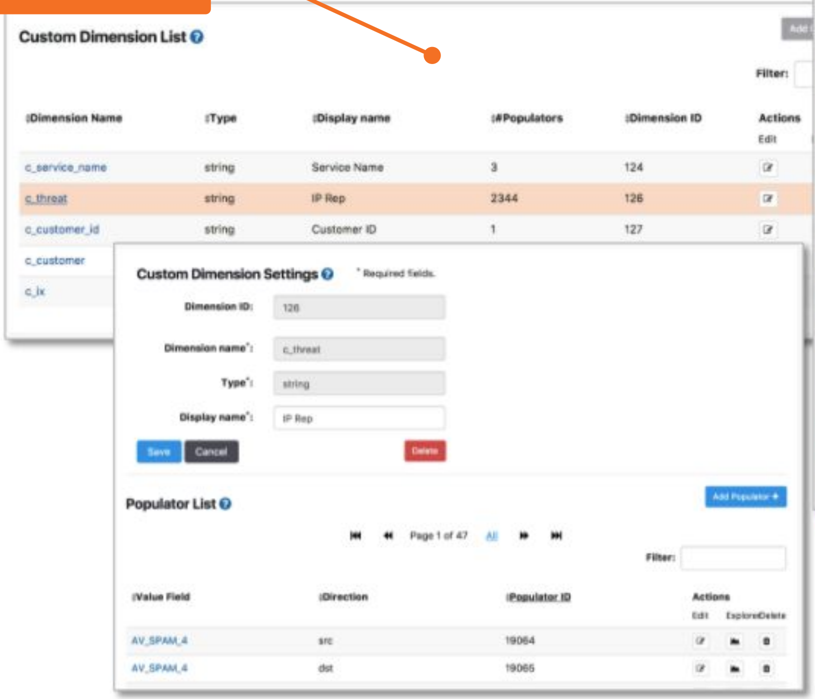
▸ Advanced Options

USE FLOWS TO SET UP & RIGHT-SIZE TESTS

“ Was anything affected by PSI’s outage? | What customers are having access issues?

# Requirement 3: Understand **in context**

ADD ANY CONTEXT



**Custom Dimension List**

Filter:

| Dimension Name | Type | Display name | #Populators | Dimension ID | Actions<br>Edit |
|---|---|---|---|---|---|
| c_service_name | string | Service Name | 3 | 124 | |
| c_threat | string | IP Rep | 2344 | 126 | |
| c_customer_id | string | Customer ID | 1 | 127 | |
| c_customer | | | | | |
| c_ix | | | | | |

**Custom Dimension Settings**

* Required fields.

|  |  |
|---|---|
| Dimension ID: | 126 |
| Dimension name*: | c_threat |
| Type*: | string |
| Display name*: | IP Rep |

Save Cancel Delete

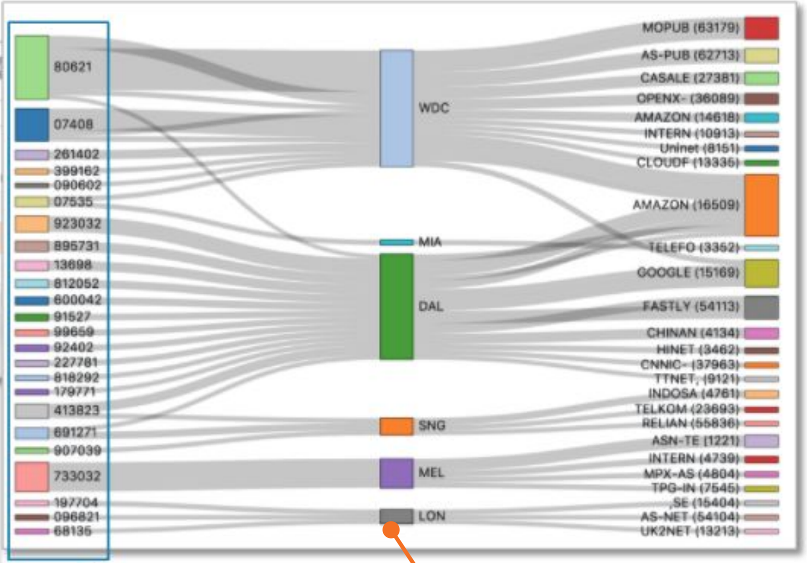
**Populator List**

Add Populator +

Page 1 of 47 All

Filter:

| Value Field | Direction | Populator ID | Actions<br>Edit Explore Delete |
|---|---|---|---|
| AV_SPAM_4 | src | 19064 | |
| AV_SPAM_4 | dst | 19065 | |

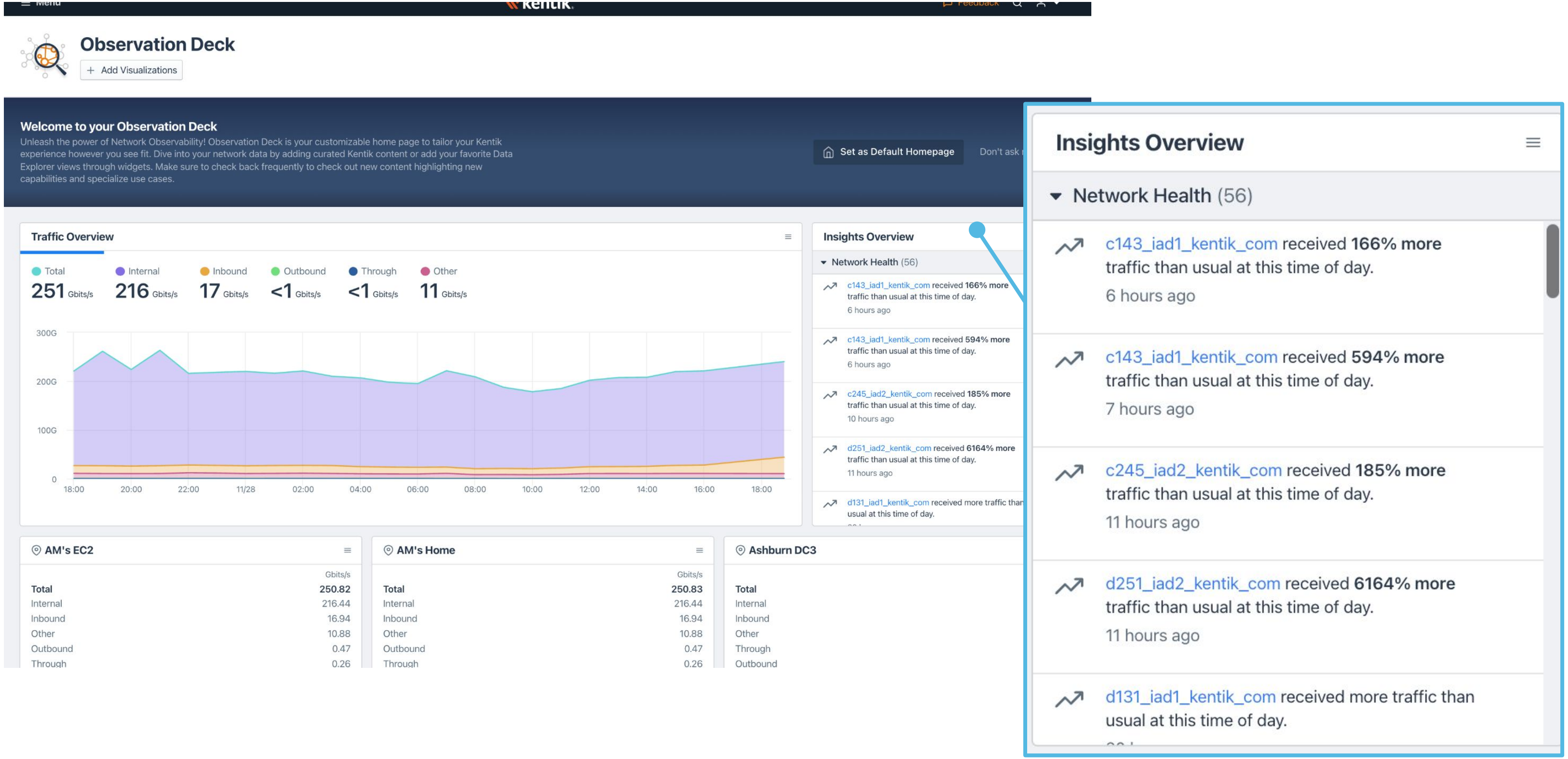


Internal Customer IDs

CUSTOMER DATA CENTER USAGE

“ Which customers are filling my AWS interconnect? | What users are crypto mining?

# Requirement 4: get insights that provide clarity



## Observation Deck

**Welcome to your Observation Deck**

Unleash the power of Network Observability! Observation Deck is your customizable home page to tailor your Kentik experience however you see fit. Dive into your network data by adding curated Kentik content or add your favorite Data Explorer views through widgets. Make sure to check back frequently to check out new content highlighting new capabilities and specialize use cases.

**Traffic Overview**

| Total | Internal | Inbound | Outbound | Through | Other |
|---|---|---|---|---|---|
| 251 Gbits/s | 216 Gbits/s | 17 Gbits/s | <1 Gbits/s | <1 Gbits/s | 11 Gbits/s |

**Insights Overview**

Network Health (56)

- c143_iad1_kentik_com received 166% more traffic than usual at this time of day. 6 hours ago
- c143_iad1_kentik_com received 594% more traffic than usual at this time of day. 6 hours ago
- c245_iad2_kentik_com received 185% more traffic than usual at this time of day. 10 hours ago
- d251_iad2_kentik_com received 6164% more traffic than usual at this time of day. 11 hours ago
- d131_iad1_kentik_com received more traffic than usual at this time of day.

**AM's EC2**

| | Gbits/s |
|---|---|
| Total | 250.82 |
| Internal | 216.44 |
| Inbound | 16.94 |
| Other | 10.88 |
| Outbound | 0.47 |
| Through | 0.26 |

**AM's Home**

| | Gbits/s |
|---|---|
| Total | 250.83 |
| Internal | 216.44 |
| Inbound | 16.94 |
| Other | 10.88 |
| Outbound | 0.47 |
| Through | 0.26 |

**Ashburn DC3**

Total
Internal
Inbound
Other
Through
Outbound

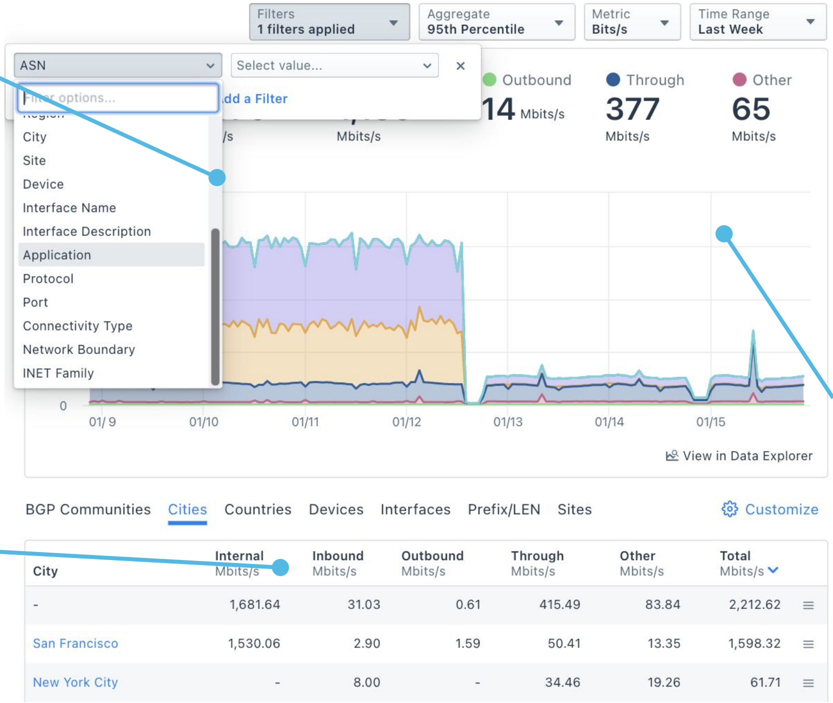
**Insights Overview**

Network Health (56)

- c143_iad1_kentik_com received 166% more traffic than usual at this time of day. 6 hours ago
- c143_iad1_kentik_com received 594% more traffic than usual at this time of day. 7 hours ago
- c245_iad2_kentik_com received 185% more traffic than usual at this time of day. 11 hours ago
- d251_iad2_kentik_com received 6164% more traffic than usual at this time of day. 11 hours ago
- d131_iad1_kentik_com received more traffic than usual at this time of day.

# Requirement 5: Ask (and get an answer to) any question

ASK ANY WAY: ZOOM, FILTER, DRILL



Filters: 1 filters applied

Aggregate: 95th Percentile

Metric: Bits/s

Time Range: Last Week

| City | Internal Mbits/s | Inbound Mbits/s | Outbound Mbits/s | Through Mbits/s | Other Mbits/s | Total Mbits/s |
|---|---|---|---|---|---|---|
| - | 1,681.64 | 31.03 | 0.61 | 415.49 | 83.84 | 2,212.62 |
| San Francisco | 1,530.06 | 2.90 | 1.59 | 50.41 | 13.35 | 1,598.32 |
| New York City | - | 8.00 | - | 34.46 | 19.26 | 61.71 |

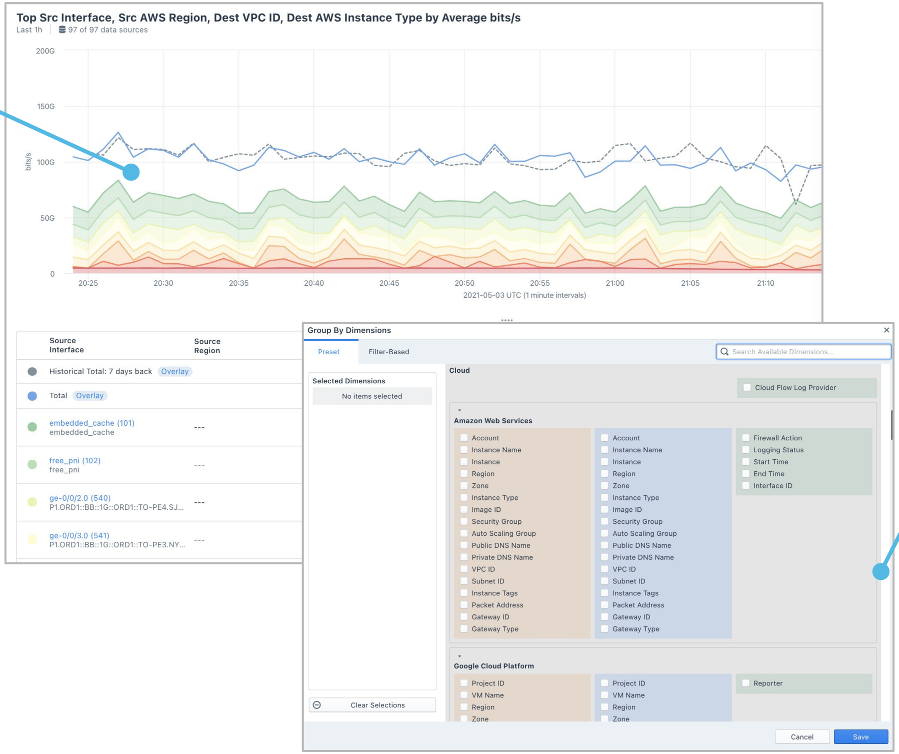
DETAILEED, HI-FI VISUALIZATIONS

ORGANIZED DATA THAT’S EASY TO SEE

“ What’s going on in Dallas? | Who’s using 8.8.8.8? | Why is there still app traffic in that DC?

# Requirement 5: Ask (and get an answer to) any question

INSTANTLY QUERY AND SHARE



**Top Src Interface, Src AWS Region, Dest VPC ID, Dest AWS Instance Type by Average bits/s**

Last 1h | 97 of 97 data sources

| | Source Interface | Source Region |
|---|---|---|
| ● | Historical Total: 7 days back Overlay | |
| ● | Total Overlay | |
| ● | embedded_cache (101)<br>embedded_cache | --- |
| ● | free_pni (102)<br>free_pni | --- |
| ● | ge-0/0/2.0 (540)<br>P1.ORD1::BB::1G::ORD1::TO-PE4.SJ... | --- |
| ● | ge-0/0/3.0 (541)<br>P1.ORD1::BB::1G::ORD1::TO-PE3.NY... | --- |

**Group By Dimensions** ×

Preset | Filter-Based | Search Available Dimensions...

Selected Dimensions

No items selected

⊖ Clear Selections

**Cloud**

□ Cloud Flow Log Provider

**Amazon Web Services**

□ Account
□ Instance Name
□ Instance
□ Region
□ Zone
□ Instance Type
□ Image ID
□ Security Group
□ Auto Scaling Group
□ Public DNS Name
□ Private DNS Name
□ VPC ID
□ Subnet ID
□ Instance Tags
□ Packet Address
□ Gateway ID
□ Gateway Type

□ Account
□ Instance Name
□ Instance
□ Region
□ Zone
□ Instance Type
□ Image ID
□ Security Group
□ Auto Scaling Group
□ Public DNS Name
□ Private DNS Name
□ VPC ID
□ Subnet ID
□ Instance Tags
□ Packet Address
□ Gateway ID
□ Gateway Type

□ Firewall Action
□ Logging Status
□ Start Time
□ End Time
□ Interface ID

**Google Cloud Platform**

□ Project ID
□ VM Name
□ Region
□ Zone

□ Project ID
□ VM Name
□ Region
□ Zone

□ Reporter

Cancel | Save

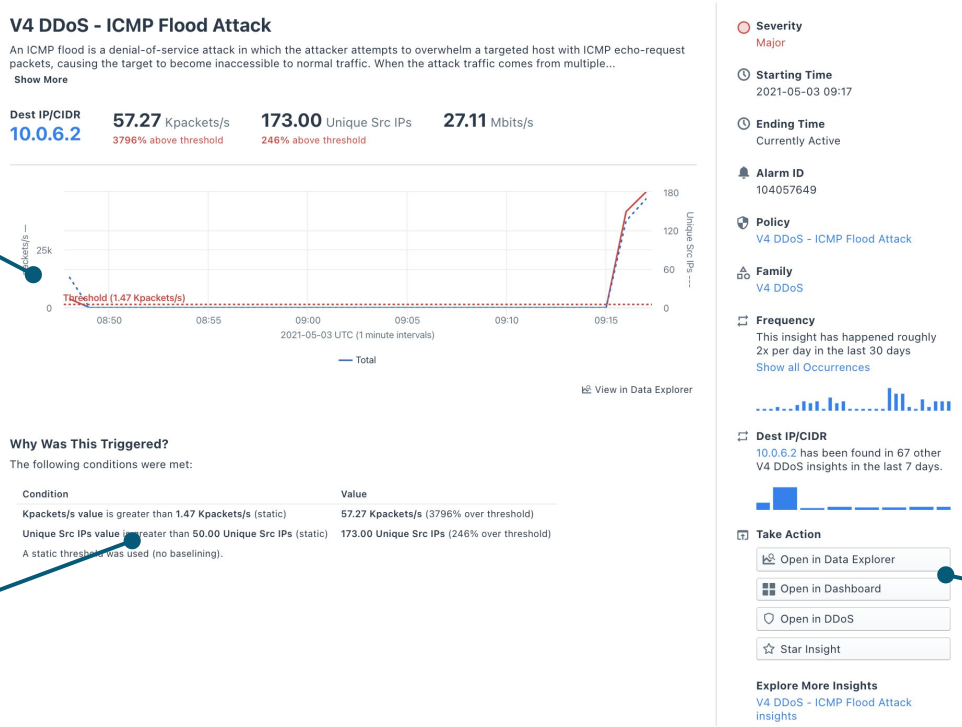
QUERY AND FILTER ANY DIMENSION

# Requirement 6: Automate routine tasks

VISUALIZE TASK IN ACTION

BACKTRACK TO UNDERSTAND WHY

JUMP OFF TO NEXT LOGICAL STEP



### V4 DDoS - ICMP Flood Attack

An ICMP flood is a denial-of-service attack in which the attacker attempts to overwhelm a targeted host with ICMP echo-request packets, causing the target to become inaccessible to normal traffic. When the attack traffic comes from multiple...

**Show More**

**Dest IP/CIDR** 10.0.6.2

57.27 Kpackets/s — 3796% above threshold

173.00 Unique Src IPs — 246% above threshold

27.11 Mbits/s

View in Data Explorer

**Why Was This Triggered?**

The following conditions were met:

| Condition | Value |
|---|---|
| **Kpackets/s value** is greater than **1.47 Kpackets/s** (static) | **57.27 Kpackets/s** (3796% over threshold) |
| **Unique Src IPs value** is greater than **50.00 Unique Src IPs** (static) | **173.00 Unique Src IPs** (246% over threshold) |

A static threshold was used (no baselining).

**Severity**
Major

**Starting Time**
2021-05-03 09:17

**Ending Time**
Currently Active

**Alarm ID**
104057649

**Policy**
V4 DDoS - ICMP Flood Attack

**Family**
V4 DDoS

**Frequency**
This insight has happened roughly 2x per day in the last 30 days
Show all Occurrences

**Dest IP/CIDR**
10.0.6.2 has been found in 67 other V4 DDoS insights in the last 7 days.

**Take Action**

**Explore More Insights**
V4 DDoS - ICMP Flood Attack insights

Automate cost reporting | Manage capacity with no touch | Mitigate attacks as soon as we see them

# What happens when you do it right

## Uptime

25% MTTR Improvement

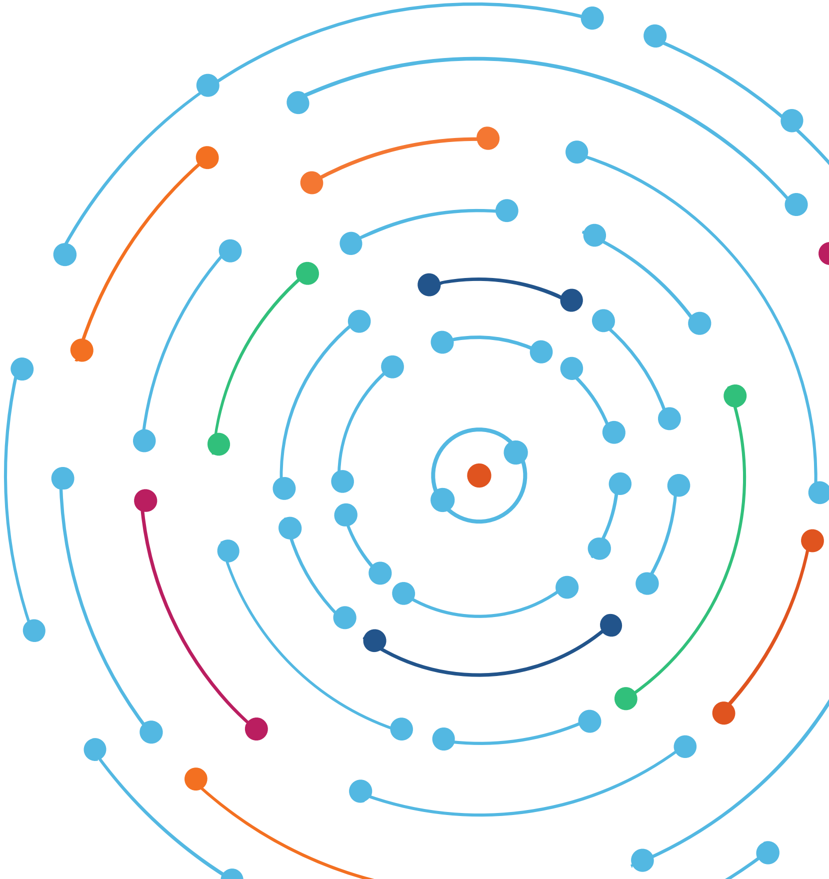
## Productivity

30% Faster Ops Task Completion

## Cost

20% OPEX Savings

# Questions?



# THANK YOU!

nina@kentik.com
@nisssen333

Join Kentik Community on Slack:

https://www.kentik.com/go/kentik-community-slack-signup/