Link Oregon

Built for Innovation.
Powered by Community.

Link Oregon DDoS Mitigation Capabilities

Presenter: Stephen Fromm

Hey, what is your DDoS protection solution again?”

LINK OREGON

AGENDA

- Link Oregon Mitigation Toolbox
- Network Telemetry & Detection
- BGP Flowspec & Mitigation
- Volumetric mitigation with Radware

LINK OREGON

LINK OREGON

MITIGATION TOOLBOX

OUR MITIGATION TOOLBOX

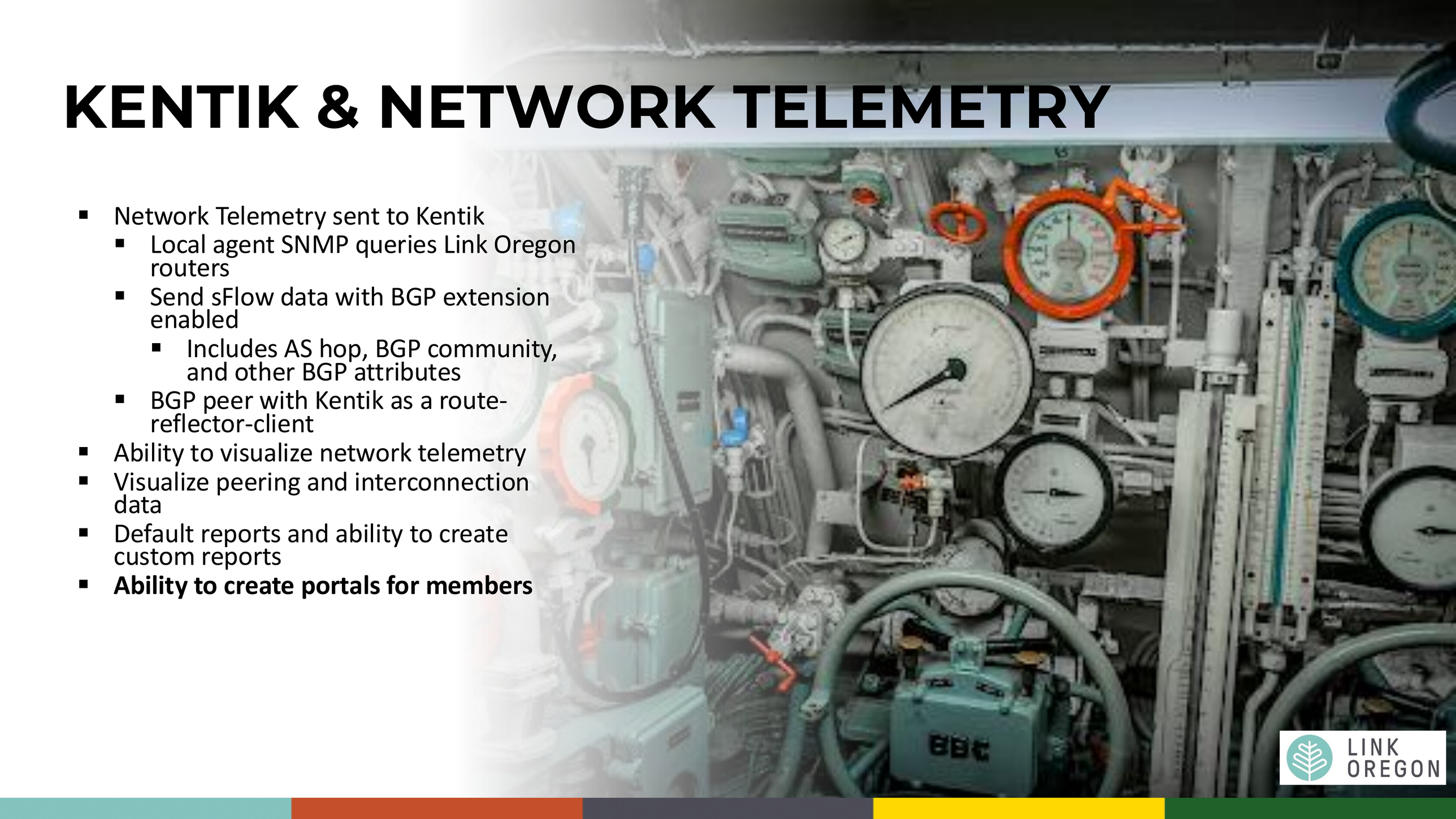
- *Defense in depth* - No single tool is a cure-all.
- Team Cymru Bogon and UTRS feeds
- ACLs on interfaces & BGP peerings to sanitize accepted routes
- RTBH - Remote Trigger Black Hole
- BGP Flowspec with Kentik
- Volumetric attack mitigation with Radware
- BGP communities for traffic engineering
  - https://www.linkoregon.org/tech/bgp/

LINK OREGON

LINK OREGON

NETWORK TELEMETRY & DETECTION

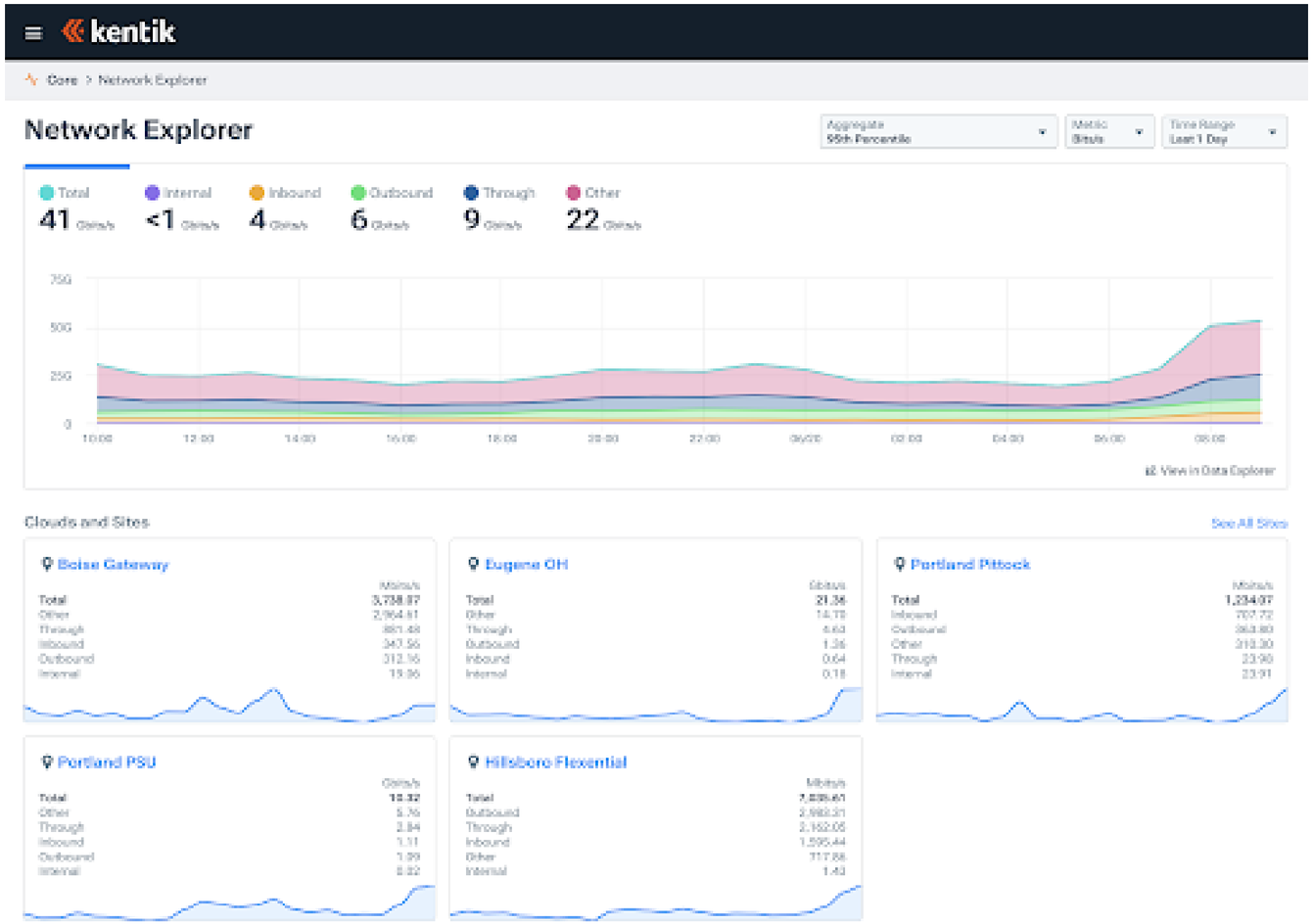
KENTIK & NETWORK TELEMETRY



- Network Telemetry sent to Kentik
  - Local agent SNMP queries Link Oregon routers
  - Send sFlow data with BGP extension enabled
    - Includes AS hop, BGP community, and other BGP attributes
  - BGP peer with Kentik as a route-reflector-client
- Ability to visualize network telemetry
- Visualize peering and interconnection data
- Default reports and ability to create custom reports
- **Ability to create portals for members**

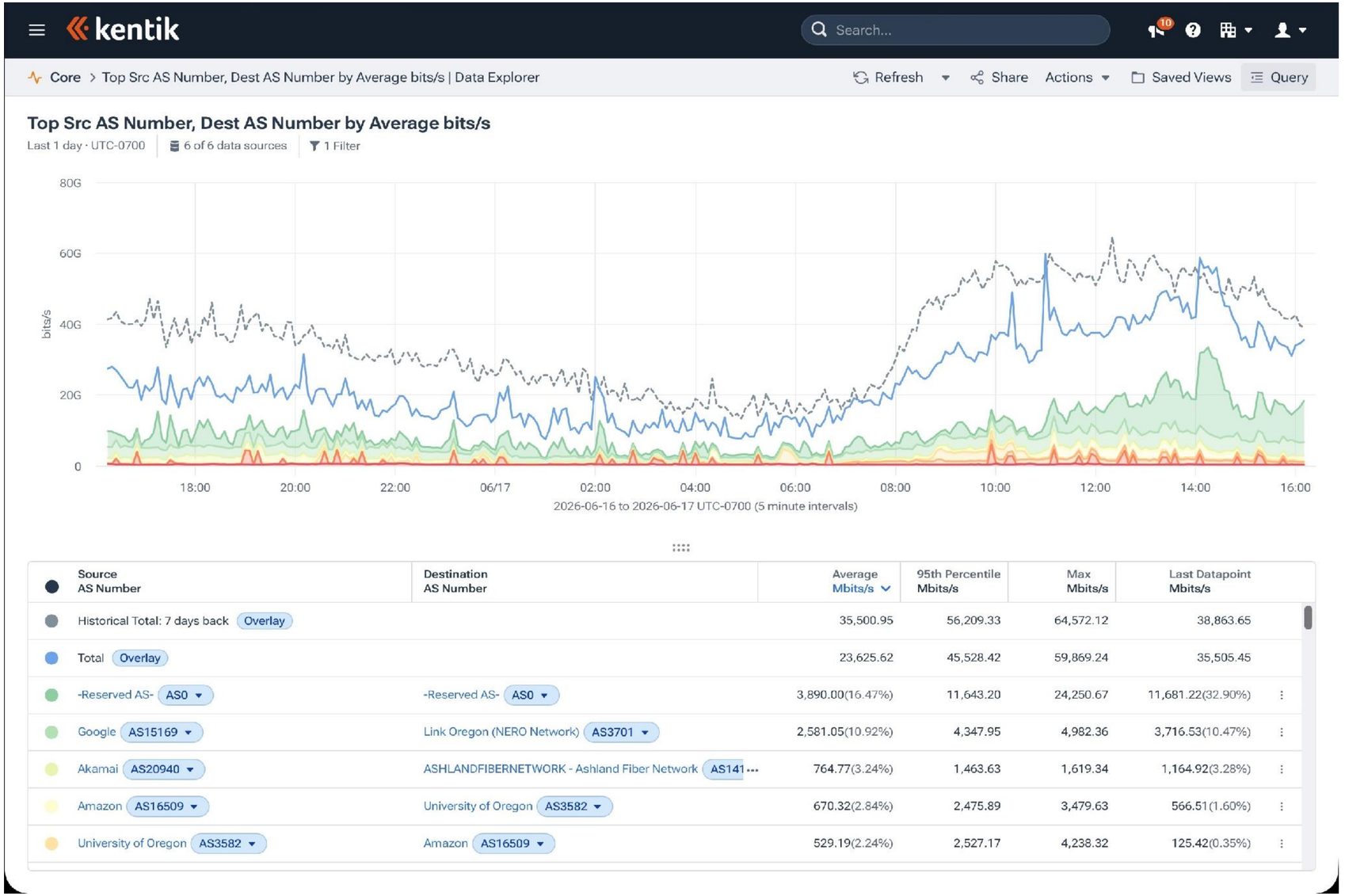
LINK OREGON

VISUALIZE NETWORK TELEMETRY



LINK OREGON

STANDARD FEATURES FOR INSPECTING NETFLOW



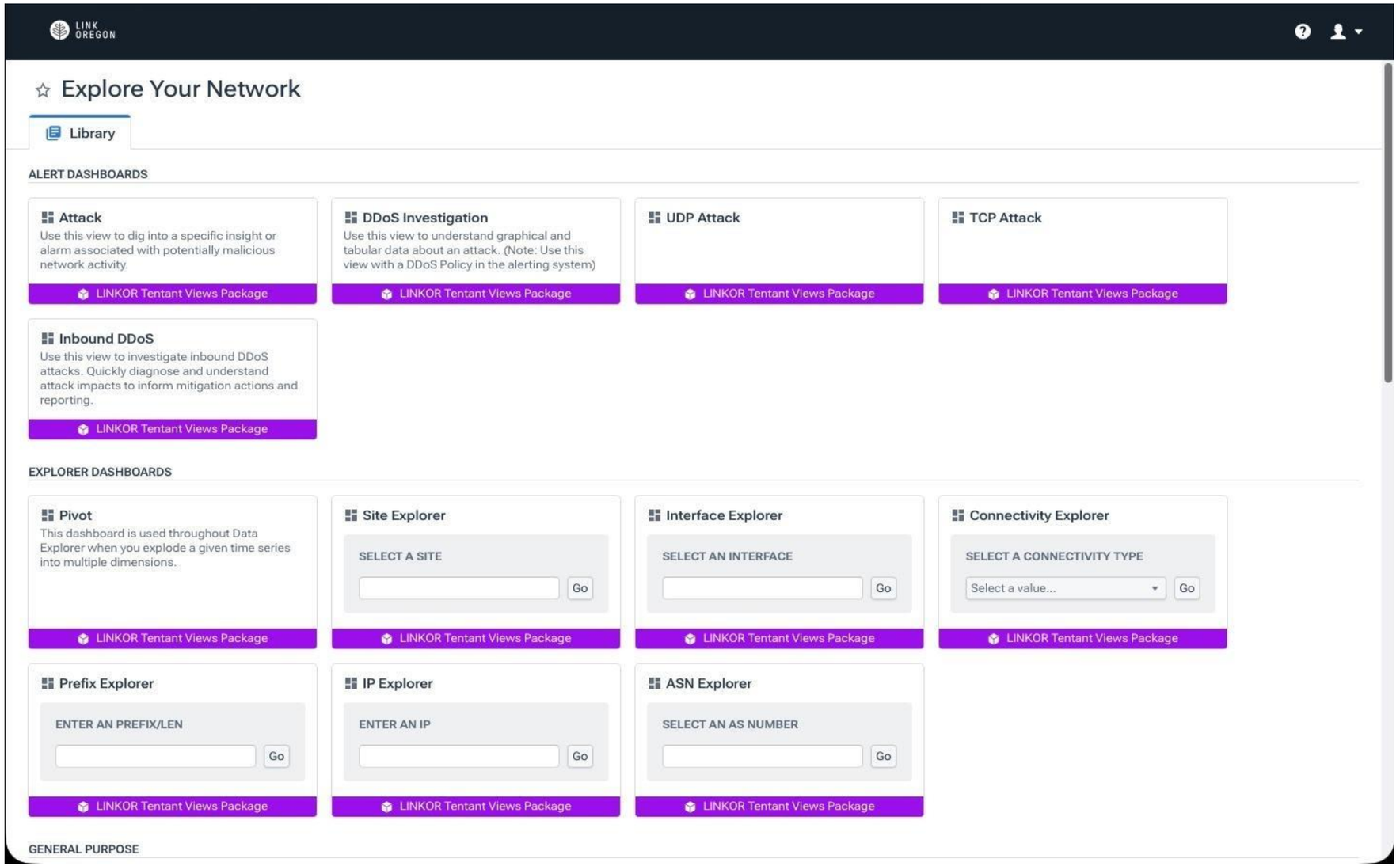
LINK OREGON

KENTIK MEMBER PORTAL

- Link Oregon can create Portals for Members
- Members can view their traffic across Link Oregon Backbone
- Member view limited to their networks
- Traffic Analysis and DDoS Investigation

LINK OREGON

MEMBER PORTAL



LINK OREGON

KENTIK MEMBER PORTAL (cont…)

- There are 25 dashboards available
- Ranges from Traffic Overview, to Top Talkers, to DDoS Investigation
- Includes visualizations and tabular data
- https://portal.kentik.com
- **Please reach out with any questions**

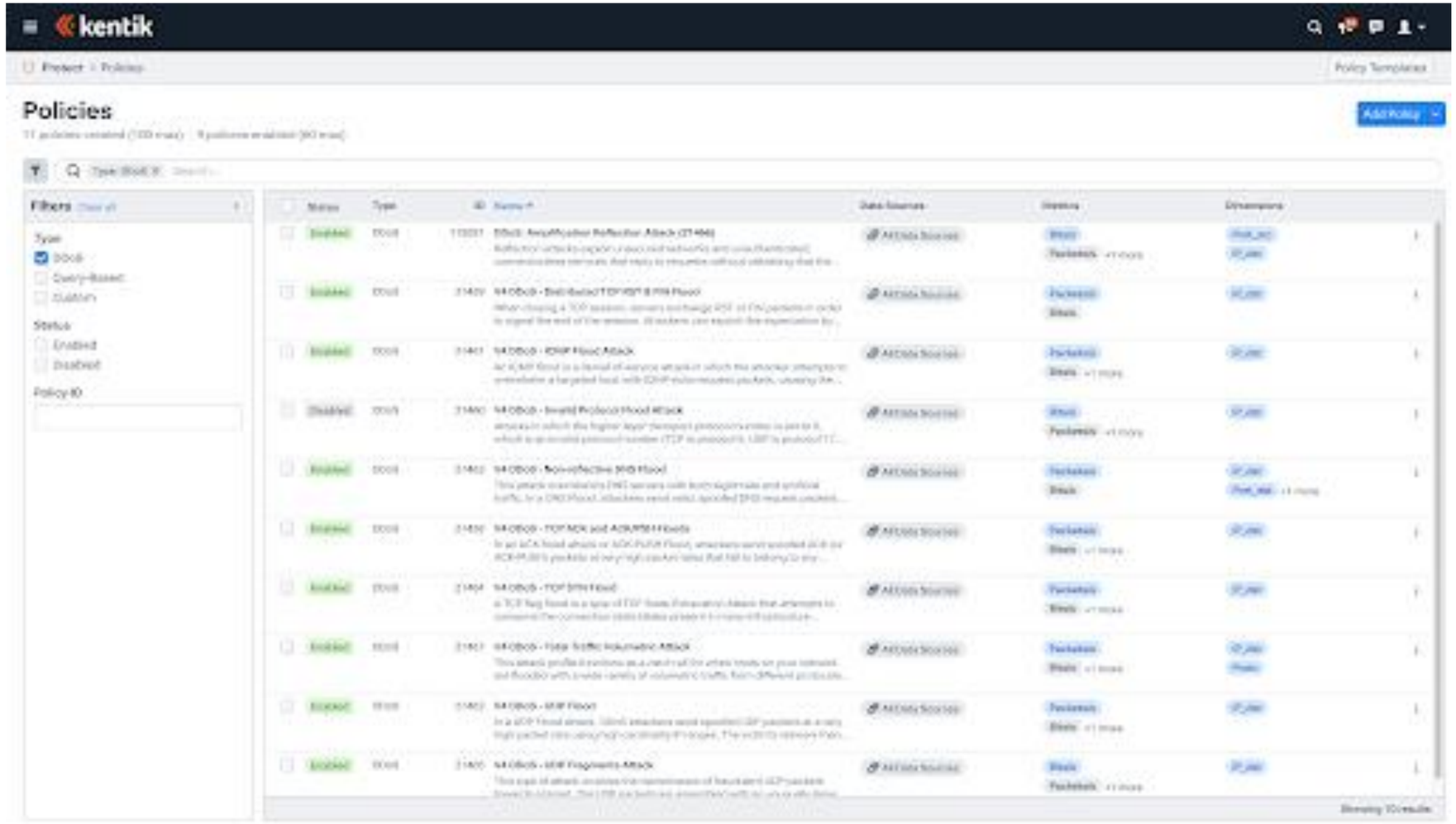
LINK OREGON

LINK OREGON

DDoS DETECTION & MITIGATION

KENTIK AND DDoS MITIGATION

Baked in DDoS Detection & Reporting



LINK OREGON

DDoS DETECTION– TYPES OF ATTACKS

- Total Traffic Volumetric Attack
- Amplification Reflection Attack
- ICMP Flood Attack
- UDP Flood
- UDP Fragments Attack
- And more …

LINK OREGON

DDoS DETECTION– Continued

- Build filters of what to include/exclude
- Example: DDoS Amplification Reflection filters
  - 19/udp
  - 53/udp
  - 123/udp
  - 161/udp
  - 162/udp
  - Others per CISA
- Link Oregon NOC uses Kentik API to report detected and mitigated events to members

LINK OREGON

BGP FLOWSPEC

- Kentik supports several platforms for mitigation
- Link Oregon is using BGP Flowspec, RFC-5575
- Use BGP to disseminate rules for traffic flow specifications

LINK OREGON

BGP FLOWSPEC RULES

- Flowspec rule can match on (not exhaustive):
  - Source and/or destination IP
  - Protocol
  - Source and/or destination port
  - DSCP
  - TCP Flags
  - Packet Length
- Filters are typically inferred from the triggered DDoS Policy

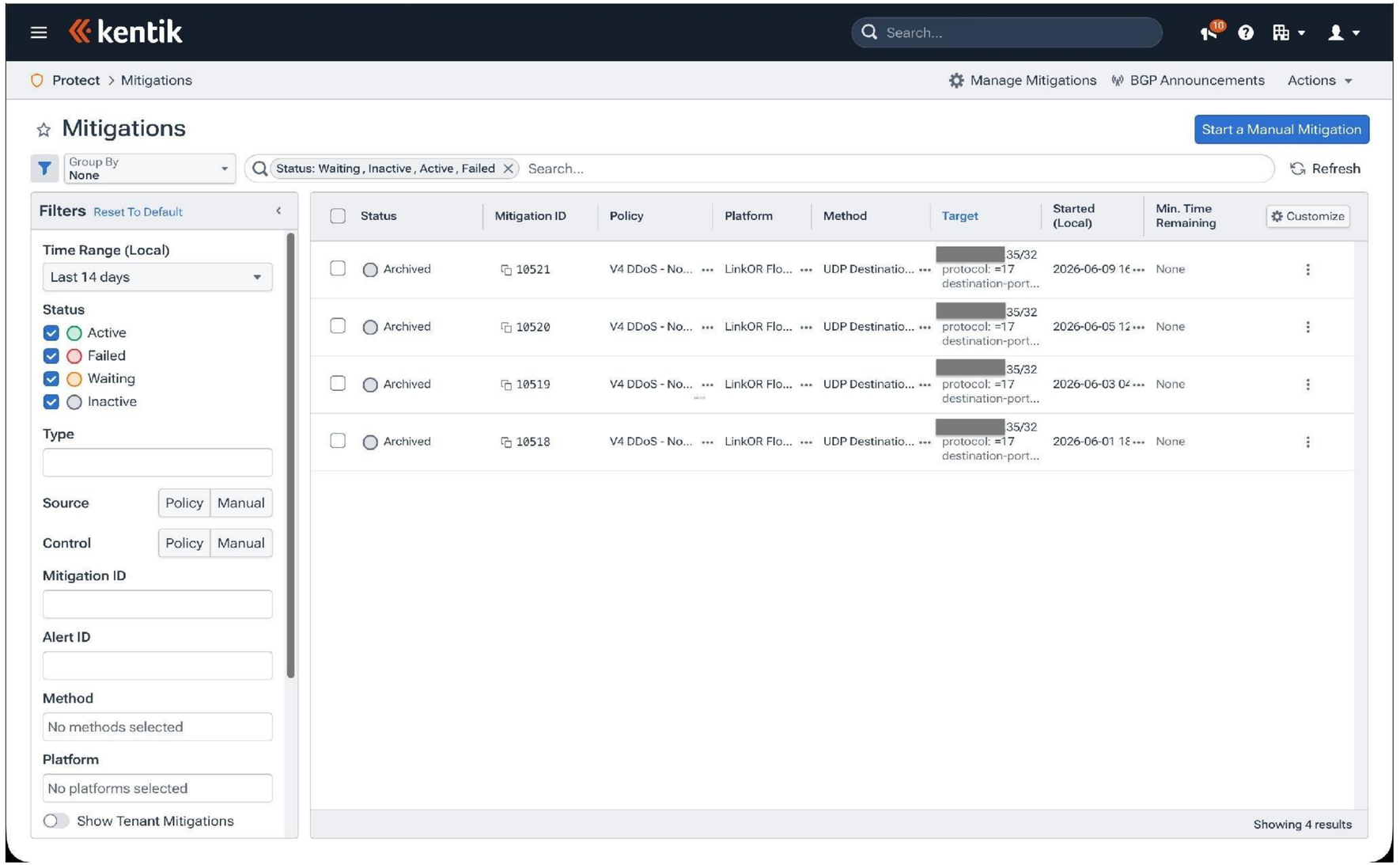
LINK OREGON

BGP FLOWSPEC ACTIONS

- Options for Flowspec actions
  - Rate Limit
  - Discard
  - Mark DSCP
  - Route-Target redirect
  - Next-hop redirect
- Link Oregon approach is to rate limit
  - This is typically *bytes/sec*
  - Endeavour to *do no harm*
- Can take more aggressive stance when working with customer

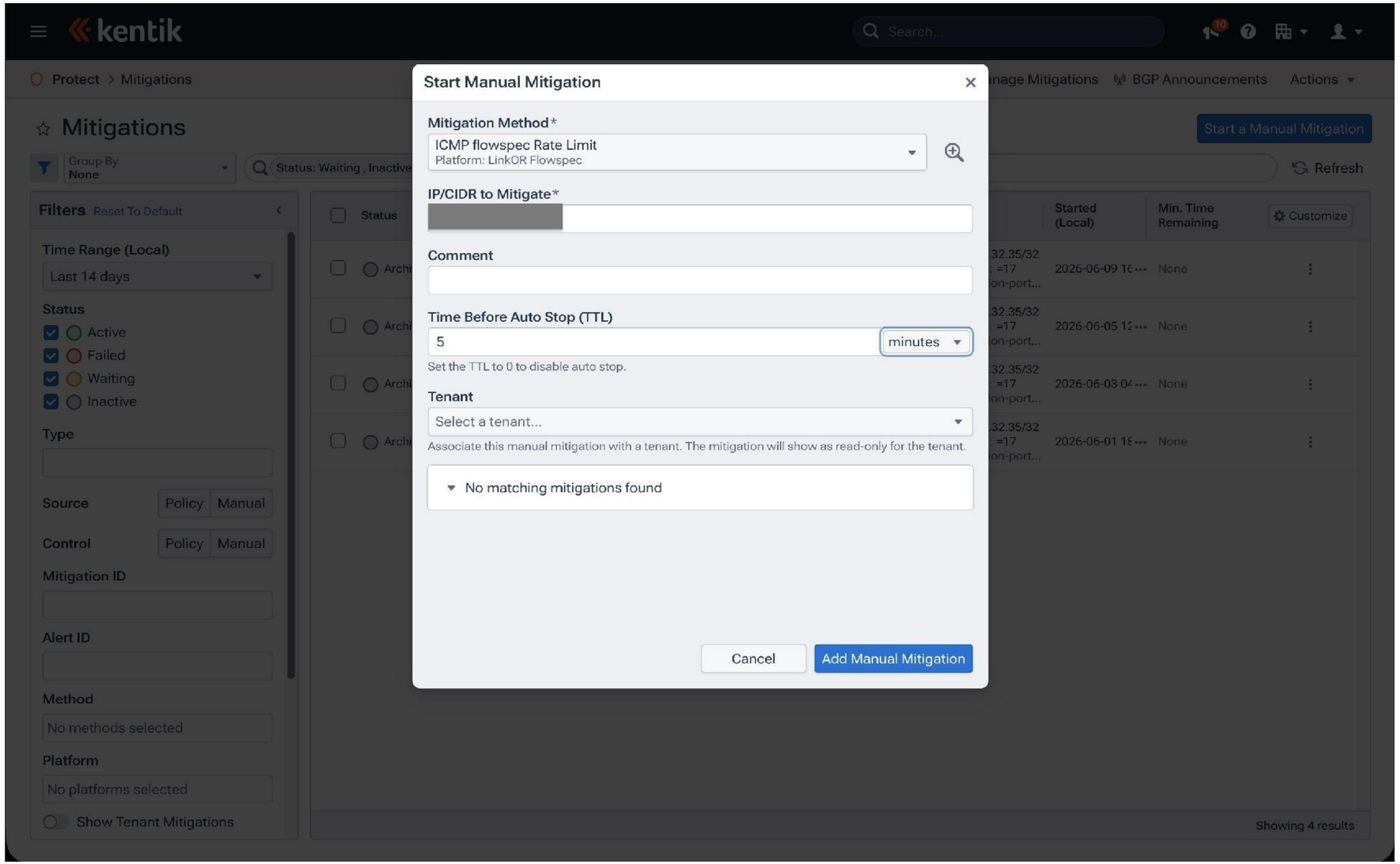
LINK OREGON

KENTIK MITIGATION VIEW



LINK OREGON

MANUAL MITIGATION TRIGGER VIA KENTIK



LINK OREGON

MANUAL MITIGATION FLOWSPEC

```
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#show bgp flow-spec ipv4
BGP Flow Specification rules for VRF Internet_3701
Router identifier 207.98.127.249, local AS number 3701
Rule status codes: # - not installed, M - received from multiple peers

   Matching Rule                                                Actions
   [redacted]*;IT:=8|=3|=0|=4|=5|=9;                            Police: 8 Mbps (1 MBps)
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#
eugn-oh-pe-02(vrf:Internet_3701)#show bgp flow-spec ipv4 detail
BGP Flow Specification rules for VRF Internet_3701
Router identifier 207.98.127.249, local AS number 3701
BGP Flow Specification Matching Rule for [redacted]*;IT:=8|=3|=0|=4|=5|=9;
 Rule identifier: 139716912222928
 Matching Rule:
   Destination Prefix: [redacted]
   Source Prefix: *
   ICMP Type: =8 | =3 | =0 | =4 | =5 | =9
 Paths: 1 available
  Local
    from 208.76.14.223 (208.76.14.223)
      Origin IGP, metric -, localpref 100, weight 0, valid, internal, best
      Actions: Police: 8 Mbps (1 MBps)
eugn-oh-pe-02(vrf:Internet_3701)#
```

LINK OREGON

LINK OREGON

VOLUMETRIC MITIGATION

VOLUMETRIC MITIGATION WITH RADWARE

- **On-demand** cloud-based DDoS mitigation
- Radware scrubbing service is available through Internet2 agreement
- Contract established in 2022 as part of preparation for *Oregon22*
- Best suited for volumetric attacks and member wants to push the mitigation further upstream
- Needs collaboration with Radware SOC to target less obvious or application-specific vectors

LINK OREGON

VOLUMETRIC MITIGATION WITH RADWARE (Continued)

- Link Oregon, or partner, BGP announces more specific IP prefix to Radware
- Clean traffic comes back via peering with Internet2/Radware
  - A total of 1G of clean traffic is currently supported
- Tested multiple times in preparation for Oregon22 event
- Successfully used in several real-world member security incidents
- Requires LOA between member and Link Oregon

LINK OREGON

RADWARE DEDICATED TENANCY

- For a separate recurring fee:
  - Link Oregon members can peer with Radware and directly trigger mitigation
  - Link Oregon gets separate Radware portal to manage mitigations
  - Requires LOA between member and Radware

LINK OREGON

BGP SIGNAL TO BEGIN MITIGATION

```
port-psu-pe-01(vrf:Internet_3701)#show ip bgp nei 163.253.4.182 advertised-routes detail
BGP routing table information for VRF Internet_3701
Router identifier 207.98.127.252, local AS number 3701
Update wait-install is disabled
BGP routing table entry for 140.211.4.0/24
 Paths: 1 available
  3701
    163.253.4.183 from 207.98.127.254 (207.98.127.254), imported EVPN route, RD
207.98.127.249:15001
      Origin INCOMPLETE, metric -, localpref -, IGP metric -, weight -, tag 0
      Received 00:00:28 ago, valid, internal, best, AS Origin not validated
      Extended Community: Route-Target-AS:3701:15001 Route-Target-AS4:396450:723
TunnelEncap:tunnelTypeMpls
      Rx SAFI: Unicast
```

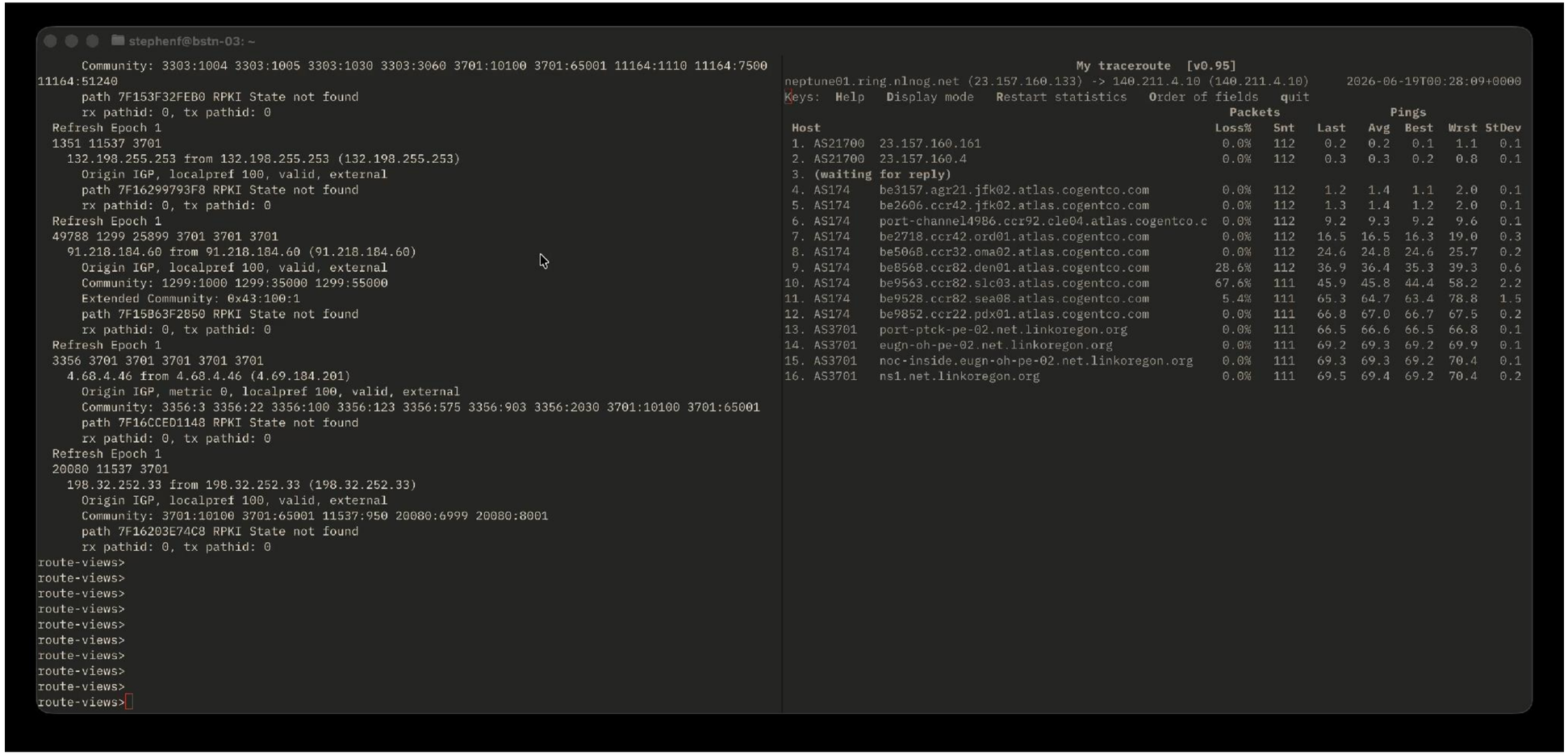
LINK OREGON

MORE SPECIFIC ADVERTISED ROUTE

```
route-views>sh ip bgp 140.211.4.0/24
BGP routing table entry for 140.211.4.0/24, version 1259985930
Paths: (14 available, best #3, table default)
  Not advertised to any peer
  Refresh Epoch 1
1351 174 1299 198949 396450 3701
    132.198.255.253 from 132.198.255.253 (132.198.255.253)
      Origin IGP, localpref 100, valid, external
      path 7F16CC07BD98 RPKI State not found
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  3356 198949 396450 3701
    4.68.4.46 from 4.68.4.46 (4.69.184.201)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 3356:3 3356:22 3356:100 3356:123 3356:575
3356:903 3356:2011 64777:0 64777:4101 64777:11103 64777:11202
65000:700
      unknown transitive attribute: flag 0xE0 type 0x20 length
0x24
        value 0003 0925 0000 0000 0000 09C4 0006 0CA2
              0000 0000 0000 038E 0006 0CA2 0000 0003
              0000 02D3
      path 7F158C7EB830 RPKI State not found
      rx pathid: 0, tx pathid: 0x0
```

LINK OREGON

EXAMPLE– REDIRECTION SCREENCAST



LINK OREGON

THANK YOU!

QUESTIONS?