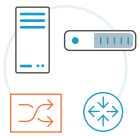
Kentik Detect Key Capabilities

Kentik Detect is the first Big Data SaaS that's purpose-built for network analytics. Architected for the terabit scale of today's traffic, Kentik Detect unifies flow records, BGP, and GeoIP in real time into a correlated time-series database. Run ad-hoc queries on billions of records with results in seconds. Drill deep on unsummarized data that's retained for months. Automatically detect attacks and other anomalies as they develop. The result is rich, actionable intelligence that you can use to assure service, cut costs, and spur operational innovation. Kentik Detect delivers network traffic intelligence at unprecedented speed, efficiency, and scale.



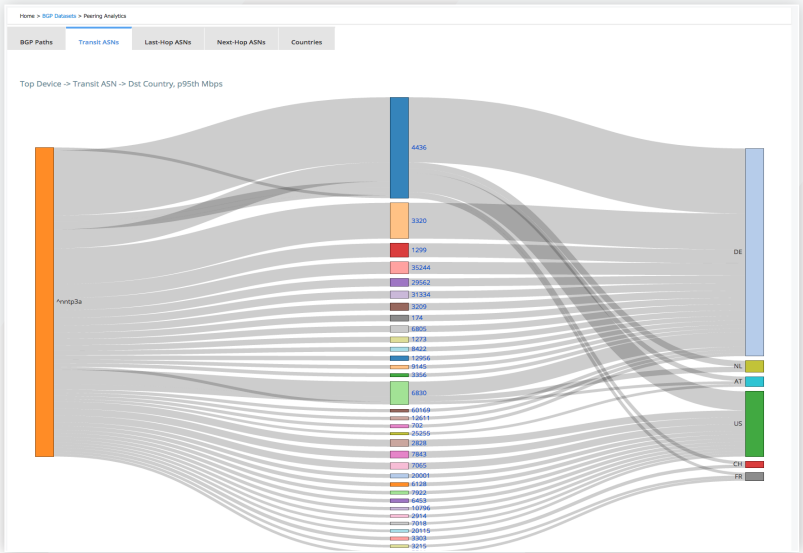
Data Ingest and Correlation

- Ingest flow records (NetFlow, sFlow, IPFIX) and SNMP (v2 or v3) interface data from routers, switches, and host agents
- Ingest pcap-derived network performance data — plus DNS/WWW data — from cloud-friendly host agents
- Ingest BGP routing updates from peering edge routers
- Correlate Kentik-sourced geolocation data
- Match flows to custom source and destination tags

Data Explorer: Ad-hoc Analysis

- Analyze traffic in a powerful GUI with ad-hoc multi-dimensional queries and visualizations
- < 2-second 95th percentile query response times, even for network-wide queries across carrier-sized networks
- Select up to eight group-by dimensions:
  - **Source/Destination** fields: Country, Region, City, AS Number, Interface, Interface Capacity, Port, MAC Address, VLAN, IP/CDR, Route Prefix/LEN, Route LEN, BGP Community, BGP AS_Path, BGP Next Hop IP/CDR, Next Hop AS Number, 2nd BGP_HOP As Number, 3rd BGP_HOP AS Number, BGP Next Hop Interface, BGP Ultimate Exit Site, BGP Ultimate Exit Device, Protocol: IP Port, Connectivity Type, Network Boundary
  - **Full** fields: Total flow, Device, Site, Protocol, INET Family, TOS, TCP Flags, Packet Size, Sampling Rate
  - **DNS/WWW** fields: DNS Query, DNS Query Type, DNS Return Code, DNS Response, HTTP URL, HTTP Return Code, HTTP Referer, HTTP User Agent, HTTP Host Header
- Choose from multiple reporting metrics:
  - Bits/s, Packets/s, Flows/s, Unique Src IPs, Unique Dst IPs, Unique Src/Dst Ports, Unique Src/Dst ASNs, Unique Src/Dst Countries/Regions/Cities, Unique Sr/Dst Nexthop ASNs, Retransmits/s, % Retransmits, Out of Order/s, % Out of Order, Fragments/s, % Fragments, RTT/2 Client Latency, RTT/2 Server Latency, RTT/2 Application Latency, Max Sampling Rate, Avg Sampling Rate
  - Sort by Average, 95th Percentile, Maximum
- Select date/time range over 90-day standard window
- Include any or all of your devices (routers, switches, hosts)
- Apply extensive filtering:
  - Unlimited filter groups, each with multiple filters
  - Filter on all source, destination, and total fields, tags, and user-defined sites, matched against Boolean expressions
- View informative, attractive visualizations:
  - Graph types: time series (stacked, line, bar), comparison bar, pie chart, Sankey diagram, matrix, table
  - Customizable visualization depth
  - Overlays: Total value and historical total value
- Export charts and tables:
  - Chart as PDF, PNG, JPG, SVG, or CSV
  - Chart + Table as PDF, PNG, JPG
  - Table as CSV
- SQL syntax: View/modify/copy the underlying SQL statement behind any UI graph or table.
- Show API call: Data or Chart
- Share a view with other users via portal URL
- Save the query for future use

Peering Analytics



- Generate analysis and reports on peering and transit
- Customize BGP dataset selection:
  - Create dataset for time range, expire in *n* days
  - Filter on Src/Dst ASNs, device keywords, Src/Dst interfaces, Dst flow tag
  - Automate generation of recurring reports
- See BGP-based path visualizations:
  - BGP paths: outbound traffic by major network path
  - Transit ASNs: summed through/to for each AS past first-hop
  - Last-Hop ASNs: where traffic is ultimately going
  - Next Hop ASNs: flow from your network to the ASNs with which you have a transit/peering relationship
  - Countries: source and destination of traffic flowing through your network
  - Click any ASN for details on in/out volume
- Apply filters to visualizations and tables:
  - Choose path depth, time range, and direction
  - Select peering device
  - Limit by interfaces and ASNs

Dashboards

- Save Data Explorer queries as panels in dashboards
- No limit on numbers of dashboards or panels
- Make dashboards private or share across the organization
- Live Update: refresh panel data every 60, 90, or 120 seconds
- Open dashboard panel in Data Explorer for further analysis
- Dashboard-level filters apply to all panels on the page

Anomaly Detection and Alerting

- Define alert policies with powerful, flexible UI:
  - GUI-based query and filter settings
  - Metrics options for traffic, performance, IP, BGP, and Geo
  - Adjustable monitoring depth (number of items tracked)
- Intelligent baselining: self-learning, dynamic, tunable, weekend-aware
- Set multiple triggers thresholds per metric
- Configuration options per threshold:
  - Comparison type: mode, more/less than, frequency
  - Notifications: email, PagerDuty, Slack, syslog, JSON, etc.
  - Automated mitigation:
    - A10 Networks Thunder Threat Protection Systems (TPS)
    - Radware DefensePro
    - Remote Triggered Black Hole (RTBH)
- DDoS detection templates included
- Alerts dashboard to view alerting activity
- Alert logging

APIs

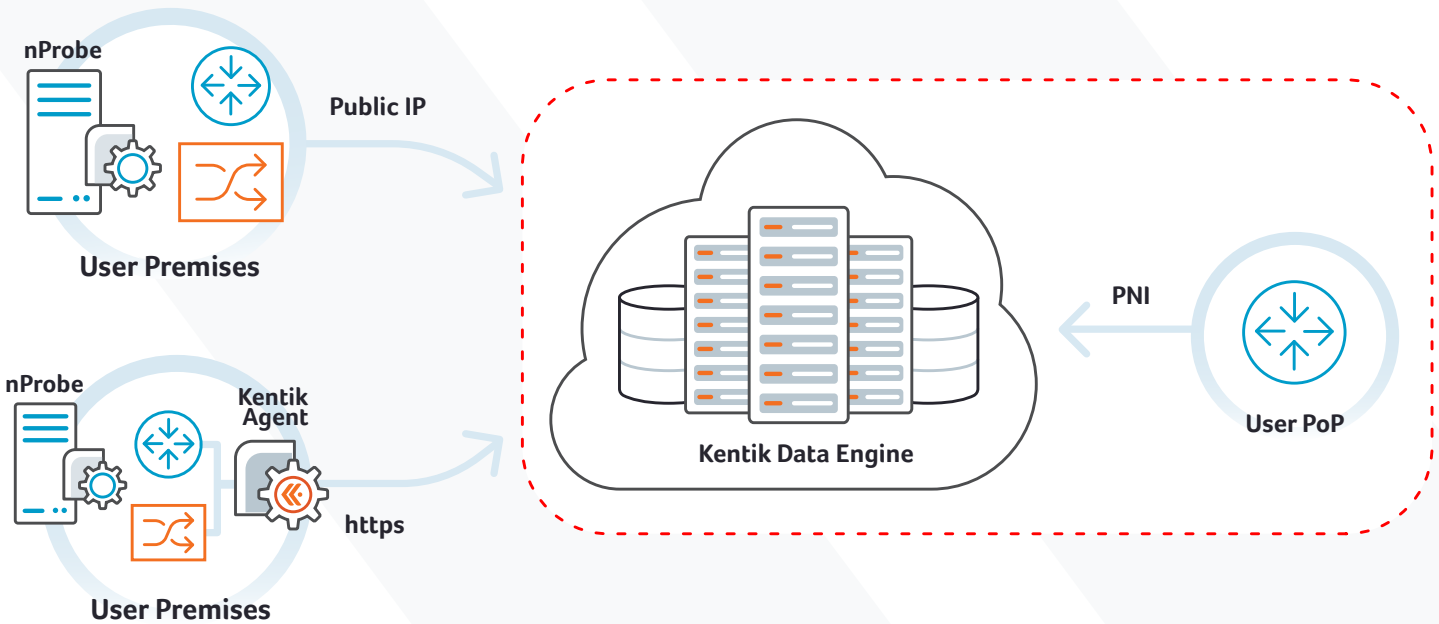
- RESTful API:
  - Model functionality of Data Explorer: query database, return tables (JSON) and charts (JPG, PDF, PNG, or SVG).
  - Perform administrative functions: create, update, and delete Users, Devices, Sites, Tags, Custom Dimensions, and Saved Filters.
- SQL client API:
  - Use PostgreSQL to query network data (flow records, BGP, selected SNMP OIDs) in the Kentik Detect database
- Mitigation integration:
  - Automated 3rd-party mitigations via APIs
- Access Control:
  - Whitelist IPs for portal, agent, API, and database access

Deployment Options

- SaaS with multiple data export options:
  - Send direct to Kentik Detect servers
  - Use encrypted tunneling via agent software running on server or VM
  - Interconnection (PNI) within an Equinix PoP
- Private hosted SaaS in Kentik data center
- On-premises with customer-supplied or Kentik cluster
- Two-factor authentication for secure access

Pricing Model

- Annual subscription fee, based on:
  - Number and type of devices sending flow records
  - Volume (FPS) of flow data sent
  - BGP requirements



Getting data to the Kentik Detect SaaS