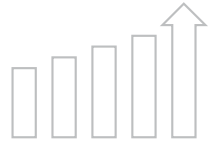# kentik

Kentik Detect
Purpose-Built Big Data Network Analytics

Network Data is Big Data

Every day, your network infrastructure generates vast amounts of data about your traffic. Effectively utilized, this data — NetFlow, IPFIX, sFlow, BGP, GeoIP, and SNMP — can be a rich source of insight for traffic analysis, day-to-day diagnostics, capacity planning, and peering optimization. So why are your network operations, engineering, and security teams often short of the actionable intelligence they need? Because they're up against the limits of legacy tools.

Traditional network analytics systems weren't architected to handle the scale of today's networks. To cope with ever-increasing traffic, they discard nearly all raw data and focus instead on predefined summary reports. In the process, they waste most of your data's value. The result is that engineers are left with a tiny fraction of the detailed intelligence they need to support real-world decisions in operations, security, and planning. Productivity, efficiency, and service-assurance are all compromised, and opportunities to enhance your business through innovation are lost.

Kentik Detect: Big Data Network Analytics

What's the alternative? A network analytics solution built on the premise that network data is Big Data. A distributed post-Hadoop backend that enables traffic details to be captured, correlated, and retained at massive scale. An engine for real-time ad-hoc querying of unsummarized data, so you don't have to guess in advance what you might need to see. And an easy-start SaaS model that makes comprehensive visibility affordable. To get all that, you need Kentik Detect™.
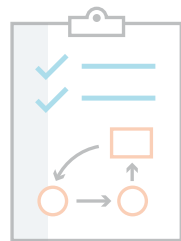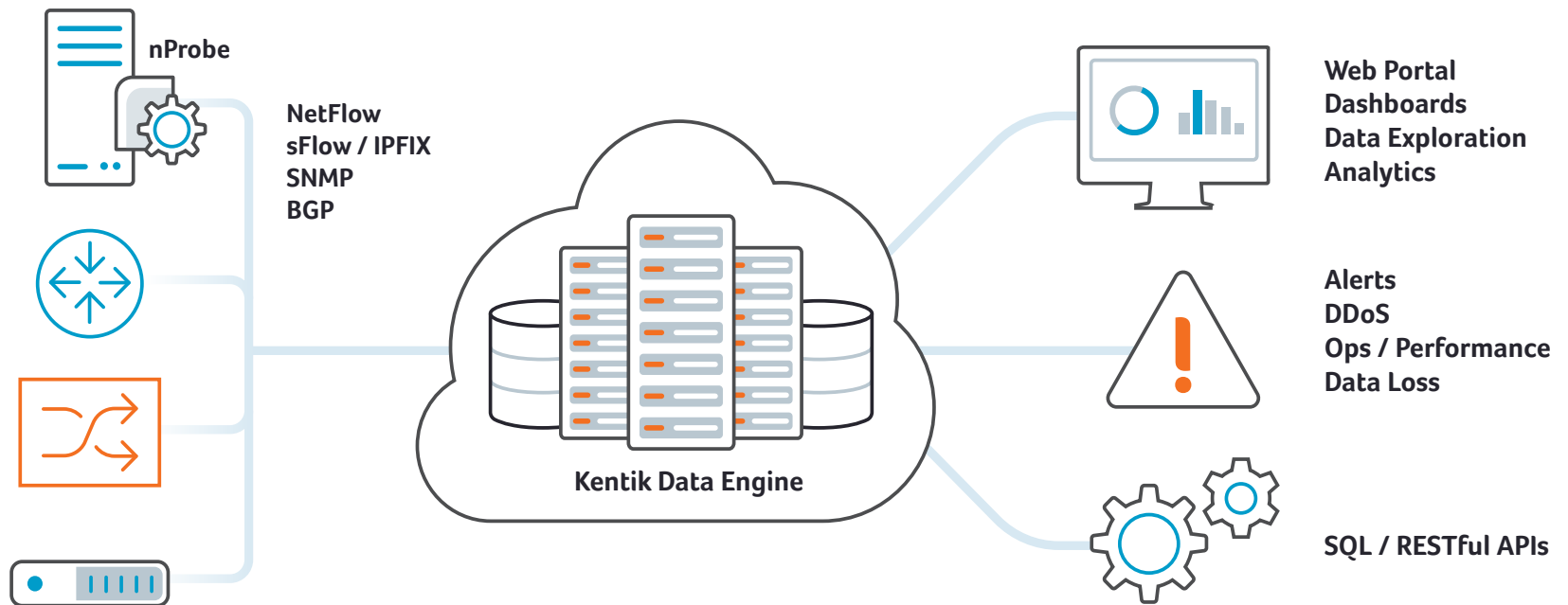
Kentik Detect is the industry's first purpose-built Big Data solution for network traffic and performance analysis. Architected for the true breadth and volume of today's traffic, Kentik Detect unlocks the value of network data by ingesting in real-time, correlating multiple data types, and retaining raw data for deep analytical drill-down. The result is rich, actionable intelligence that you can use to assure service, achieve operational excellence, and unleash innovation. Offered as an easy-on cloud service or deployed on-premises, Kentik Detect delivers network traffic insight at unprecedented speed, efficiency, and scale.

How it Works

Kentik Detect ingests NetFlow, sFlow, IPFIX, SNMP and BGP data sent from network elements like routers, switches, and hosts. It augments that data with GeoIP (geo-location) and creates unified time-series records that are retained without summarization, remaining instantly accessible for 90 days. You can configure real-time alerts, perform ad-hoc data exploration, build customized dashboards, and utilize intuitive BGP peering analytics. And you can access your raw data via SQL and RESTful APIs that allow easy data-sharing and integration with third-party systems.

nProbe

NetFlow
sFlow / IPFIX
SNMP
BGP

Kentik Data Engine

**Web Portal
Dashboards
Data Exploration
Analytics**

**Alerts
DDoS
Ops / Performance
Data Loss**

SQL / RESTful APIs

Kentik Detect is powered by a disruptive innovation, the Kentik Data Engine™ (KDE). KDE is a distributed, containerized, microservices-based compute-and-storage cluster. Scaling horizontally, KDE transcends legacy limits on rate of data intake, breadth of data records, duration of data retention, and volume of ad-hoc queries.

KDE performs low-latency ingest of network data into a distributed columnar time-series datastore, making inbound data available to query immediately. Multi-dimensional custom-filtered queries traversing billions of rows return responses within a few seconds. KDE provides the power of Big Data analytics without the fragility of typical Big Data BI cubes.

Key Features

Data Explorer for fast, flexible ad-hoc traffic analytics

Legacy visualization tools typically limit your view to predefined summaries of one or two fields. But with Data Explorer your queries cover unsummarized data for each of 40+ NetFlow, BGP, and GeoIP dimensions. You can look at data from a minute ago or three months ago, zooming in for the details or out for the big picture. You get multi-dimensional grouping across traffic, host IP, and performance metrics, and unlimited nested filters that help you quickly narrow your inquiry to key factors. Any combination of dimensions, metric, timespan, and devices can be rendered as time-series graphs or traffic flow visualizations with accompanying tables. This is the analytical power you need to make fast, effective decisions.
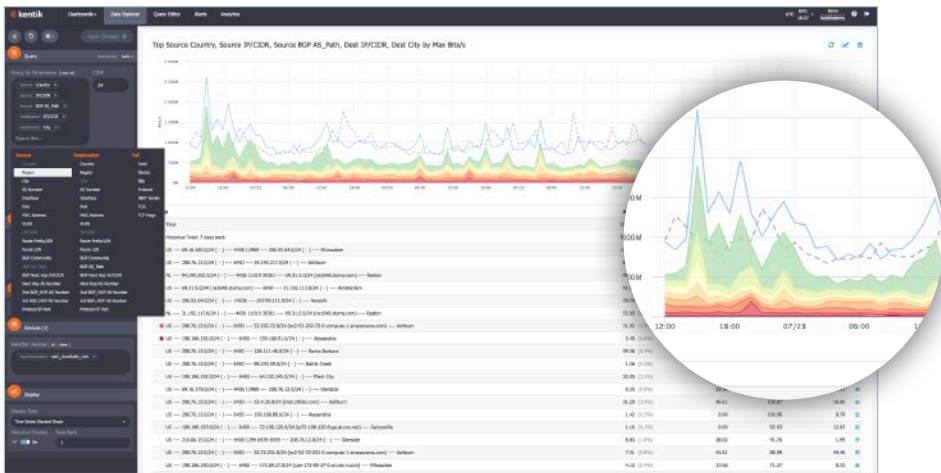
Network performance monitoring

Kentik Detect monitors live traffic sent by the Kentik nProbe host agent and enables lightning-fast visibility and querying of latency, TCP retransmits, and other key measures needed to assess and optimize network performance. With Kentik Detect, you'll know when — and why — user experience is impacted by performance, and what to do about it.

Network-wide alerting for DDoS and anomaly detection

Kentik Detect alerting applies the power of KDE to protect your network from performance anomalies and DDoS attacks. Any query defined in the Data Explorer can be configured as an alert that is tailored to reflect your specific infrastructure, business, and traffic norms. Alerts are always based on network-wide data, resulting in fewer false positives than systems that only evaluate traffic in line or from a limited subset of interfaces. And KDE's near-instant ingest of traffic data means that notification of alert-triggering conditions occurs without the five-minute delay common to legacy systems. With Kentik Detect, you get exceptionally flexible alert customization and the fastest possible notification of service-impacting issues.

Key Features

Dashboards that are easy to customize, easy to share

Kentik Detect's dashboards let you see fast what you need to see most. A dashboard is a user-defined set of panels that each contain a single visualization that you specify in Data Explorer.

Devices, timespan, and filters can be fixed at creation or follow settings in the dashboard sidebar. A dashboard can be made visible only to its creator or shared with team members across an organization. You can also set up dashboard-based reports for scheduled distribution to subscribers.
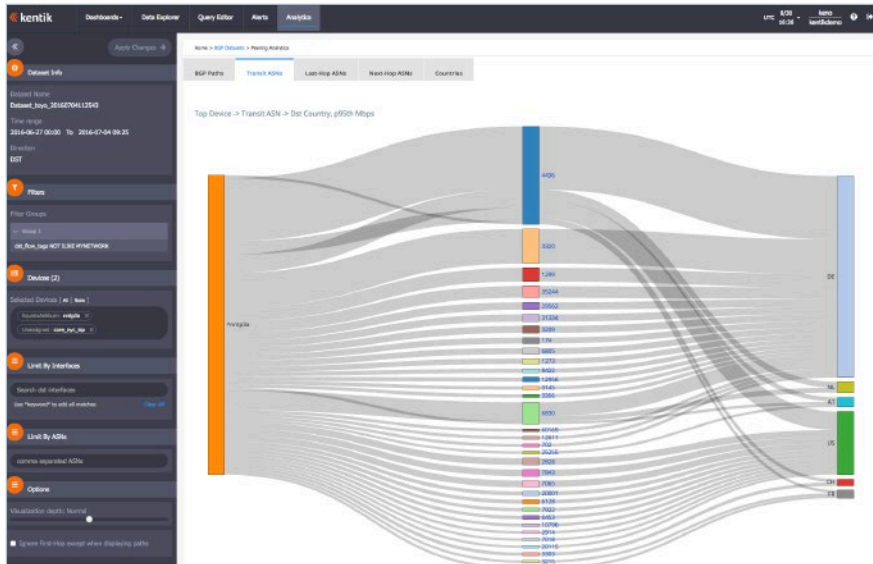
Peering analytics to manage costs and make opportunities

If you sell or consume large amounts of multi-homed Internet bandwidth, success depends on building relationships and making smart deals. For that you need a clear view of the interaction between traffic volumes, BGP paths, interconnects, and geographical reach. Kentik Detect includes a dedicated peering analytics solution that clarifies traffic flow, providing visualizations and tables organized around path, neighbor, transit, origin, and country. Web enterprises and retail service providers can use these views to manage cost and performance, while wholesale transit providers can assess peering efficiency and identify new prospects. With on-the-fly filtering and instant single-ASN drill-downs, Kentik Detect's peering analytics is the most intuitive way to quickly grasp both the big picture and details of your Internet routing.

APIs for open access and flexible integration

Kentik Detect doesn't lock your data into hard-to-access appliances, or build summaries and then discard the details. Instead, third party systems for functions such as DDoS mitigation, log management, and security information and event

management (SIEM) can all have direct access your network data from KDE. Using straightforward non-proprietary integration via PostgreSQL client or RESTful APIs, Kentik Detect makes it easy to leverage your investment by extracting the full value of your data for both business and technical goals.

Flexible Deployment Options

Kentik Detect offers all of the cost and resource advantages of a SaaS, including fast time-to-value and zero overhead for hardware, software, or IT operations. Optional agent software can be deployed on a server or VM to provide encrypted tunneling transport of your data to our public cloud. If your organization has a presence within an Equinix PoP, private interconnection (PNI) is available to satisfy the most stringent data privacy requirements. Kentik Detect can also be deployed on-premises for organizations that prefer to host their own Kentik Data Engine cluster.

Public IP

User Premises

Kentik Agent

https

User Premises

EQUINIX

PNI

User PoP

Kentik Data Engine
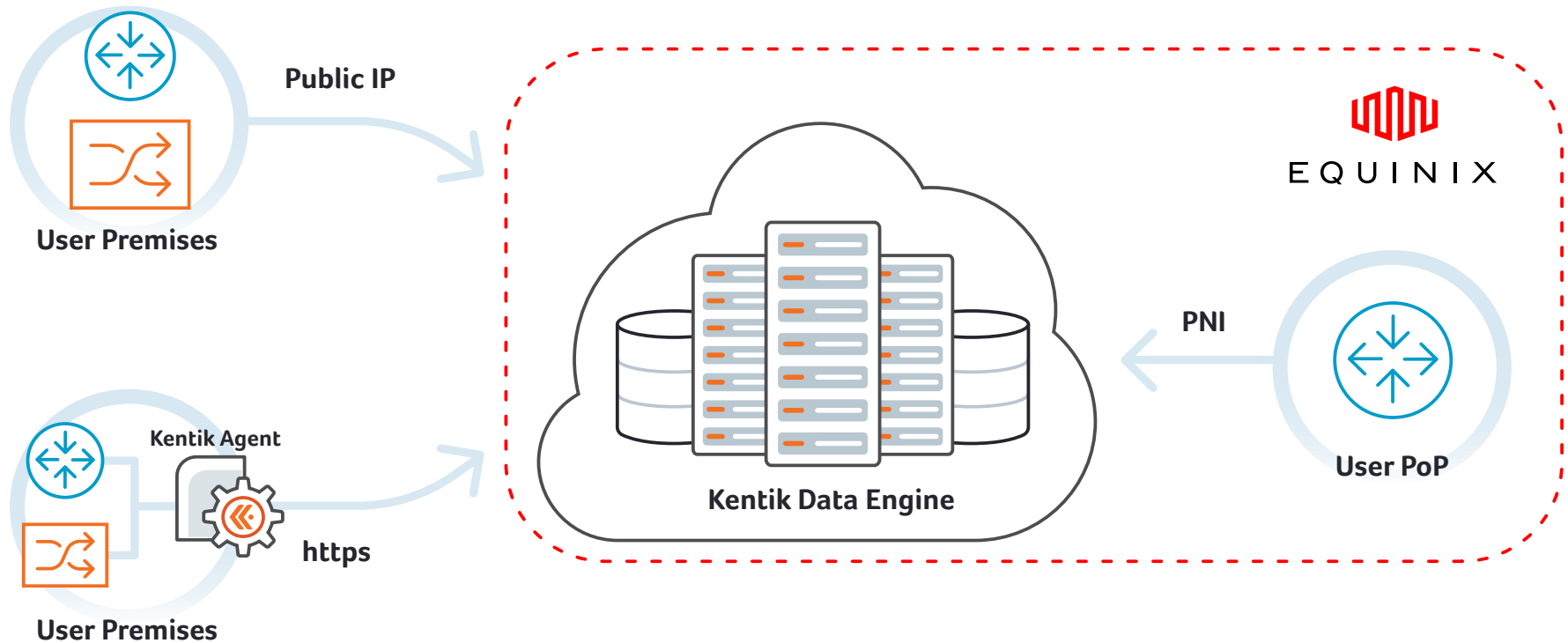
Get Data-Driven Network Operations Now

Today's networks are too massive and too complex to manage effectively based on educated guesswork and summary-only visibility. Instead, network operations, planning, and security teams need to be able to directly query billions of full resolution flow records. They need a single, silo-free view of flow correlated with BGP, GeoIP, and SNMP. They need to be able to look at any timespan ranging from moments ago to months in the past. And they need answers in seconds without having to guess their questions in advance. In short, they need real-time Big Data analytics at scale.

Kentik Detect is the world's first network intelligence solution that meets these requirements. Built by network operators for network operators, Kentik Detect gives you the insights you need when you need them. And it gives you the ability — finally — to implement truly data-driven network operations. That translates into higher service assurance and also enables continuous improvement, which ultimately means happier customers, better cost-performance, and a more competitive and profitable business.