On the Radar: Kentik offers network analysis and DDoS detection at big data scale

Ad hoc, multidimensional queries are enabled on 90 days of data

Publication Date: 24 Mar 2017 | Product code: IT0022-000917

Rik Turner

Summary

Catalyst

Kentik offers technology, delivered in software-as-a-service (SaaS) mode, that leverages big data for network visibility, performance monitoring, and DDoS protection, as well as real-time ad hoc analytics.

Key messages

- Kentik uses a purpose-built big data engine to fit the particular requirements of the company's target market, built on Docker containers with a microservices software architecture.
- It ingests streamed network telemetry data in real time rather than in batches.
- Kentik Detect supports multitenancy, and handles web portal, REST, and SQL queries with data grouping, using up to eight dimensions.
- Kentik is working on a Splunk integration, enabling customers to analyze both structured and unstructured data.

Ovum view

Digital service providers need to query network data for operational and security insights, with volumes precluding traditional on-premise appliances. Kentik’s SaaS approach with its purpose-built big data engine stands it in good stead in this market.

Recommendations for enterprises

Why put Kentik Detect on your radar?

The big data approach to analytics is mandated by the volumes involved in modern networks, and an engine that can handle ad hoc, multidimensional queries is clearly the way forward. The fact that Kentik's customers can deploy an on-premise version of the platform with data lakes to house volumes beyond the 90 days the SaaS version of the platform itself stores makes it a particularly compelling offering against the more restrictive big data platforms the company rejected in creating its service.

Highlights

Given their perception of the shortcomings of traditional appliance-based network analysis platforms that rely on summary data and predefined tables, Kentik's founders started out investigating the leading big data engines on the market at the time.

They found that most such technology took a post facto approach to analysis, looking at large batches of data at the end of the business day, for instance. Many available engines could not ingest streaming data or perform ad hoc, multidimensional queries – they often had to pre-compute data cubes before running queries. As a result, they were too slow for real-time operations.

Google's BigQuery managed data warehouse service can handle both real-time and ad hoc queries, but its primary ingest mode is in batches, in addition to which it is not available as open source.

Another challenge was the sheer volume of data Kentik's target customers would need to store to underpin their analyses. Engines such as Amazon RedShift and the Elastic stack (comprising Elasticsearch, Logstash, and Kibana, and formerly known as ELK) can take streamed data and perform both ad hoc and real-time queries, but Kentik found that they were inefficient in how they stored data. Also, the cost structure of memory-resident engines was prohibitive.

Equally, the Kentik team looked at Splunk, the popular platform for searching, monitoring, and analyzing data, but it does not handle the kind and volume of structured (i.e. protocol-based) data that Kentik's customers require in an economically viable fashion, its primary focus being the unstructured world of logs.

Multitenancy was a key requirement for the engine

Another issue Kentik found was that the majority of the products considered did not support multitenancy, which was a requirement for handling multiple customers on the same infrastructure, and indeed for fair treatment of different user queries within the same customer.

The company eventually opted to build its own big data-style engine for handling multi-field questions rapidly, with no predefined limits. It is a columnar data store that utilizes a Postgres Foreign Data Wrapper to appear row-based, creating a consistent query interface for SQL, REST, and web portal.

Kentik Detect runs in co-location data center space in Equinix points of presence, though customers also have the option to run an instance of it on their own premises, which a number of the larger ones do.

The platform creates two copies of the ingested data, sending one to storage for ad hoc querying, while the other goes to its anomaly detection engine. Even if running on premises, Kentik still charges for it using a SaaS model based on the number of routers submitting data. Pricing is in the range of $600–$6,000 per year for each device submitting data to the Kentik platform.

Kentik's baselining differentiates it from cloud-based competitors in DDoS

In the DDoS market, on-premise equipment is clearly insufficient to handle the volumetric attacks that are becoming ever more commonplace. Moreover, cloud-based DDoS protection services rely on traditional, appliance-based detection devices.

Kentik considers its main advantage over DDoS detection appliances is its baselining: the competition baselines per router on large pools of IP addresses, so detection fails to get a full picture if the attack happens across multiple data centers and connections. Kentik Detect, by contrast, baselines on individual IP addresses across the entire network and applies multidimensional detection policies. It can then automate traffic redirection to mitigation devices from Radware and A10.

Background

Kentik was founded as CloudHelix in 2014 by CEO Avi Freedman, who was formerly Chief Network Scientist at Akamai; Principal Engineer Ian Pye, who was previously at Cloudflare; and VP Sales Justin Biegel, who was head of sales in Northern California and the Pacific Northwest at Internap. The company's CTO is Dan Ellis, who came from the post of Director of Content Delivery Operations at Netflix.

The rationale for the creation of the company was to develop a network analytics capability, looking at operations, management, and security information, that would draw upon the big data technology approach. This came from the perception that the previous generation of analytics tended to be based upon a 1U server deployed in a company's data center, in which the analytical capacity was restricted by the device's limitations in terms of storage and memory.

Kentik has so far raised some $35m in VC funding, more recently announcing the closure of a $23m Series B round led by Third Point Ventures, with participation by existing investors August Capital, Data Collective (DCVC), First Round Capital, and Engineering Capital, and new investors Glynn Capital and David Ulevitch.

Current position

Kentik launched the Kentik Detect service in June 2015, which was also when the company renamed as Kentik. It refers to Kentik Detect as a network traffic intelligence platform, and has so far unveiled one major bevy of enhancements. In June 2016, it announced the addition of multidimensional traffic analytics, "enabling access to billions of possible analyses operating on trillions of instantly accessible data records," as well as new traffic flow visualizations and support for network performance metrics.

Kentik Detect performs ad hoc queries on up to 90 days of network data to detect anomalies, with the queries capable of encompassing up to eight different data dimensions. The company has opted not to offer its customers a huge data lake, hence the 90-day limit, but of course the customers themselves can opt to deploy on premises and create such capacity if required.

The company currently has in excess of 100 customers and stores some 125 billion new data records every day, with expectation that it will exceed 200 billion in the next few months. The natural constituency for Kentik is, of course, the "digital business natives" and big web properties such as Yelp (the crowdsourced review publisher), file-sync-and-share provider Box, and streaming music service Spotify.

That said, it is also of interest to any company that operates a network and relies on it for revenue generation. Thus, digital service providers of all shapes and sizes are within its purview, with one of the top five cloud service providers and a tier-1 telco already using its technology. The company also counts some very large financial services institutions among its customers.

While Kentik could not use Splunk to underpin its own activities, the company recognizes that a lot of its customers are using Splunk to analyze log data, making Kentik Detect a complementary tool for the network telemetry data Splunk is less suited to handling. To this end, it is now working on a Splunk integration, though a number of customers have already integrated the two platforms via DIY projects of their own.

Data sheet

Key facts

Table 1: Data sheet: Kentik

Product name	Kentik Detect	**Product classification**	Network analytics, DDoS protection
Version number	n/a – SaaS product	**Release date**	Launched June 2015
Industries covered	Enterprises, web company/OTT, service providers including telcos, mobile operators, cable, cloud, hosting companies	**Geographies covered**	North America, EMEA, Asia
Relevant company sizes	Depending on sector: mainstream enterprise – large; web companies, service providers – SME and larger	**Licensing options**	Annual subscription on a per network data exporter basis
URL	https://www.kentik.com	**Routes to market**	Direct sales, channel partners, technology partnerships
Company headquarters	San Francisco, California, US	**Number of employees**	50+

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

On the Radar: Big Switch touts SDN for high-bandwidth DDoS mitigation, IT0022-000889 (March 2017)

On the Radar: Nexusguard Cyber Security Platform provides cloud-based DDoS protection, IT0022-000775 (September 2016)

"Neustar forms partnership with Limelight for turbocharged DDoS mitigation," IT0022-000723 (June 2016)

Arbor's Move to Address an Expanding DDoS Market, IT0022-000515 (November 2015)

Author

Rik Turner, Senior Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo