EMA Vendor to Watch: Kentik

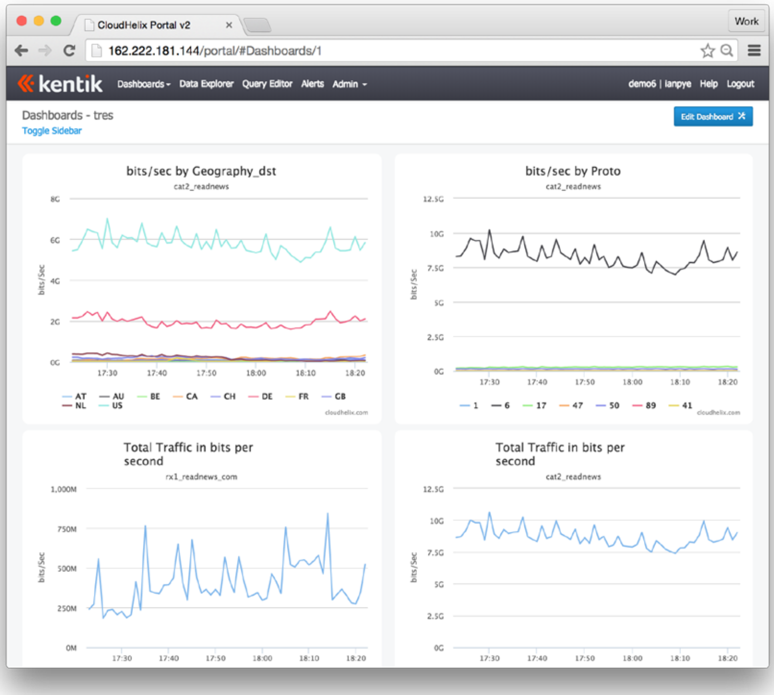
EMA VENDOR TO WATCH

Kentik – July 2015

Value Proposition

Kentik (formerly known as CloudHelix) has emerged from stealth mode with a new cloud-based network visibility and analytics platform that uses big data techniques to process billions of data records per day for real-time visibility.

Kentik offers a software-as-a-service (SaaS) platform that consumes network data from remote sites—including flow records (NetFlow, IPFIX, etc.) and Simple Network Management Protocol (SNMP) and Border Gateway Protocol (BGP) data. Processing this data at terabit rates, thanks to a clustered, scale-out analytics architecture, Kentik offers customers multiple options for accessing its analytics. A network operator can simply access Kentik's portal or integrate the provider's network analytics into their own management tools using Kentik's REST APIs or SQL-standard querying options. Kentik also offers an on-premises version of its platform for network operators whose policies require network analysis to be conducted in-house.



The Kentik solution comprises three primary components: Kentik Agent, Kentik Data Engine, and Kentik Detect. Kentik Agent is an optional component for organizations that want to encrypt data before forwarding it to the main platform. It collects, encrypts and forwards flow, SNMP, and BGP data from any number of network devices on site. If encryption isn't required, network operators can forward the data from their network devices directly to the Kentik Data Engine, a back-end collection and clustered analytics system. Finally, Kentik Detect is the first of what will be multiple front-end SaaS applications that apply the company's analytical capabilities to different use cases. Kentik Detect can serve multiple use cases for network operators, including distributed denial of service (DDoS) detection, network peering efficiency analysis, and real-time traffic monitoring.

Kentik can store raw network data for 90 days or more, allowing for deep forensic analysis. The solution offers real-time alerting and fast-response queries of its cross-data analytics.

EMA Perspective

Most IT management tool vendors specialize in analyzing very specific data types and performing a combination of structured and signature-based analysis to extract information. These tools, which can provide very deep analysis of a specific set of data, are helpful, but they are siloed. ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) research has found that enterprises can have as many as ten or more of these tools for network management alone. While these tools themselves may be effective, the workflows that network managers establish across them are inefficient. As networks become more complex to support mobility, hybrid cloud, and software-defined data centers, this type of Swiss Army–knife approach to management won't scale.

Big data analytics capabilities are finding increased traction with IT engineering and operations teams because they can analyze and correlate multiple data sets and present a broader view of what is happening in a network. The appetite for this type of analytics has prompted many IT management tool vendors to integrate their data analysis streams with third-party databases and analysis tools. Enterprises are finding that by pushing the metadata created by their management vendors into third-party analytical tools, they can extract new insights that help with infrastructure planning, monitoring, and diagnostics. Forthcoming EMA research has found that enterprises that apply big data analytics to infrastructure management are using multiple data types in their analysis and are applying the technology to many use cases. Capacity planning is an early use case, but infrastructure optimization, problem isolation, security analysis, and even IT/business alignment are important use cases that emerge with these technologies.

Big data analytics introduces the ability to correlate events across multiple structured and unstructured data sets to glean more insight. Incumbent vendors might present NetFlow analysis and SNMP analysis side by side for a dashboard-based evaluation of what's happening in the network. Kentik, however, is using big data analytics to provide differentiated network visibility, combining the analytics of multiple data types and analyzing all of them in real time. For instance, it can gather and combine peering information from BGP, network utilization and health statistics from SNMP, and source and destination information from flow data to give enterprises a real-time view of exactly what's happening in the network.

With a recent Series A funding round of $12 million and several high-profile early public customers like OpenDNS, Yelp, and Box, Kentik has some serious momentum behind it. It is one of a new generation of network management vendors emerging in the era of big data. At a time when network scale and network complexity are growing exponentially, this tool and others like it are arriving just in time.

About Vendor to Watch: EMA Vendors to Watch are companies that deliver unique customer value by solving problems that had previously gone unaddressed or provide value in innovative ways. The designation rewards vendors that dare to go off the beaten path and have defined their own market niches.

About EMA: Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn. 3187.072915