REPORT REPRINT

ExtraHop adds machine-learning SaaS to IT operations monitoring

JIM DUFFY, DONNIE BERKHOLZ

02 MAR 2017

ExtraHop has announced subscription-based Addy, the company's first cloud IT operations monitoring service. Addy applies machine learning to wire data for anomaly detection and provides real-time situational insight into IT performance.

451 Research®

ExtraHop Networks has announced Addy, the company's first cloud IT operations monitoring service. Addy applies machine learning to wire data for anomaly detection and provides real-time situational insight into IT performance. Addy detects anomalies in wire-data metrics collected from ExtraHop's Discover appliances located on-premises. Machine-learning computation occurs in the ExtraHop cloud.

THE 451 TAKE

Network and IT operations insight is increasingly important not only for performance management, but for security. With machine learning, this insight becomes even more valuable as the monitoring devices should be able to adapt to and learn about the anomalies on the wire without preprogramming. As data volumes and network speeds increase, and information is more distributed (on-premises, off-premises and in the cloud) that adaptability will be key to securing the environment, and effectively supervising network and IT behavior.

CONTEXT

ExtraHop has long extolled the virtues of monitoring wire data. Monitoring the data entails using stream processing and reassembly to inspect real-time Layer 2-7 traffic flowing over the wire. The company structures the data into the intended transaction, flow or session, and enables users to drill-down into the individual metrics, users, applications and packets.

Machine learning raises the bar in wire-data monitoring because of real-time and historic monitoring, visibility and dynamic performance optimization. With the ability to learn about changes and anomalies on the wire, machine-learning intelligence and automation have the potential to make problem resolution and security detection far more intuitive, proactive and immediate. Although machine-learning automation is in its infancy, this is an overall industry goal as cloud computing and networking take greater hold over enterprise IT.

Network and application performance management (NPM and APM) are vital components of IT operations management. These tools collect, parse and analyze data from a variety of IT sources to ensure that a business process or transaction is performing optimally within the context of the business objective. The disciplines are blending together as well: pure NPM vendors are bleeding into APM (Riverbed's acquisition of Aternity for end-user experience management, as well as its server-based APM tools, serve as evidence of this), while APM practitioners are looking to buck up their NPM capabilities. Neither discipline wants to leave a stone unturned when it comes to holistic IT operations management, which is critical not only to overall application performance, but to visibility for security initiatives as well. Indeed, 451 Research has identified security as a primary driver of NPM and APM sales growth.

PRODUCTS

The linchpin of Addy is ExtraHop's Discover appliance. Using wire-data metrics from Discover, Addy builds continuous baselines for every device, network and application, and then proactively detects and surfaces potential issues in the environment. The Discover appliance provides visibility into network elements through reassembly and analysis of packet streams at a sustained 40Gbps.

The company's Explore and Trace are optional appliances, which provide different views into the wire data. Explore provides the ability to do NoSQL-type search and query, while Trace enables the deep-dive packet forensics. Trace enables users to drill down into packet transaction records stored in the Explore appliance, and to perform analysis and visual queries.

The ExtraHop Command appliance federates data across multiple appliances and presents them through the ExtraHop user interface. Addy alerts are now an additional tab on the UI. Alerts are presented in near real time, and anomalies and outages are represented graphically. With a humanized name like Addy, we found it surprising that it lacked a chatbot, considering their growing popularity over the past year. With the growing availability of bot toolkits, this would be a minor enhancement that would keep ExtraHop current with machine-learning trends. In general, we expect open, two-way integrations for data and alerts to be increasingly required going forward.

In early-adopter trials, ExtraHop says Addy detected a server that was unexpectedly probing systems in another major datacenter in a large cable provider. A trial at a financial services firm detected the Dyn DDoS attack in real-time and routed DNS traffic through an unaffected region to avoid downtime. At an early adopter trial at a national medical institution, Addy detected international servers probing their DNS, as well as reverse DNS look-ups. We think Addy may require the addition of role-specific anomaly detection. As increasing numbers of developers and DevOps engineers adopt ExtraHop, they may try to hide things they don't want to see, which would mask anomalies that network engineers need.

Addy will be generally available starting in April. Pricing for the service starts at $2,990 per month for the first Discover appliance, and then $990 per month for each additional Discover device. This represents roughly a 20% premium on average for existing ExtraHop customers, although this will vary significantly by customer size. Data is retained in the ExtraHop cloud for 30 days.

COMPETITION

ExtraHop's traditional competitors in NPM, APM, IT-operations analytics and wire-data streaming are Riverbed, NetScout and Corvil. Corvil has found success in wire-data analytics for financial trading. Riverbed has a suite of NPM and APM products, recently acquiring Aternity for endpoint APM and end-user experience management. NPM market leader NetScout recently acquired Danaher Communications, which significantly expanded its DDoS mitigation and service assurance portfolio.

Kentik has been offering a big-data SaaS service for network performance management since 2015, and most recently added support for nProbe host monitoring agents for application and load-balancing servers. The Kentik Detect service uses the Kentik Data Engine to ingest tens of billions of flow and performance records per day, and in real time, from Kentik and nProbe agents. This data can be accessed by Kentik Detect applications for DDoS detection, peering analytics and network visibility. Third-party applications, such as existing network operator management systems, can also access this data via SQL queries or a REST API.

ExtraHop's full packet-capture capabilities puts it in direct competition with traditional packet-capture vendors such as Endace, Viavi (JDSU) and Niksun. The addition of Addy puts it in competition with new network security startups that are performing machine learning in the cloud on network data such as Darktrace and ProtectWise. Both of those vendors take on-premises network data (flows, packet headers and payload data) and then send it up to the cloud for anomaly detection.

SWOT ANALYSIS

STRENGTHS

Incorporating NPM and APM – and now cloud-based machine-learning anomaly detection – ExtraHop has a holistic view of IT operations management via real-time stream processing of wire data.

WEAKNESSES

ExtraHop is new not only to machine learning, but also to SaaS-based subscription NPM and APM services. There could be challenges in rolling out what are essentially two new offerings.

OPPORTUNITIES

Machine learning is becoming the new *lingua franca* in NPM, APM and security. Vendors incorporating this intelligence and automation capability will quickly rise to the top of the customer list.

THREATS

There has been – and always will be – intense competition from many vendors for network visibility and its use cases in security, application performance, and IT operations monitoring and management. Machine learning and SaaS delivery will raise the stakes even higher.