ExtraHop leaps ahead with high-performance virtual appliance for cloud traffic visibility

Analyst: Christian Renaud

9 Jun, 2015

Network traffic visibility firm ExtraHop announced the EH6100v, a virtual appliance for network traffic capture and analysis for use in virtualized datacenters and public cloud deployments. ExtraHop positions itself as a creator, aggregator and analysis approach for 'wire data' (processed network traffic), either using its own analysis capabilities or for streaming into third-party tools for correlation with other data sources such as log files and agent data. A key differentiator of the EH6100v is high performance, which the company claims can reach 10Gbps, far greater than competitors' performance claims for their own virtual offerings.

The 451 Take

ExtraHop's approach to high-performance analysis of virtual and cloud traffic is 'on point' in the changing network visibility and monitoring (NVM) market. Unlike many vendors in the NVM sector that depend heavily on hardware revenue streams, ExtraHop can aggressively position high-performance software-based offerings. As traffic within virtualized datacenters and public cloud deployments grows, we anticipate that other visibility vendors will increase their focus on the segment and have to carefully manage their own revenue streams and product mix to avoid disruptions.

Context

Amazon recently began breaking out Amazon Web Services (AWS) revenue (roughly $6bn per year) and is by far the largest of the public cloud offerings in the market. This growth in adoption of AWS

public cloud has outpaced most visibility offerings, leaving enterprises with AWS instances with holes in their traffic visibility and network performance processes. Amazon offers a CloudWatch monitoring service to report on utilization of server and storage resources, as well as self-reported data on traffic volume and utilization of network services such as its DNS service (Route 53) or elastic load balancing service. A number of security and APM/NPM vendors plug into the CloudWatch API to extract other metrics, often via agent software sitting within AWS instances. While this self-reported data is preferable to no data, it still does not provide granular traffic (packet) data for performance or outage analysis at the same level that an enterprise is able to do on-premises. This is one gap that ExtraHop seeks to fill with the EH6100v.

The second gap the company is seeking to fill is in datacenters using VMware's datacenter virtualization offerings. Traditional visibility networks depend heavily on TAP and SPAN ports that mirror traffic from servers and other networked devices, a function that is complicated when many virtual servers can reside on a single switch port, and the amount of server-to-server (East-West) traffic is often greater than the amount of server-to-client (North-South) traffic. Visibility vendors have approached the problem using differing approaches ranging from agent code on the servers or hypervisors to using internal virtual SPAN and port mirroring capabilities within VMware's ESX and vNetwork distributed switch. With the EH6100v, ExtraHop is approaching the problem as a separate virtual machine that ties into VMware mirroring/vSPAN functionality to capture and analyze virtual traffic at very high speed (the company claims up to 10Gbps performance for its virtual appliance).

Company

ExtraHop is an eight-year-old company founded by alumni from F5 Networks and headquartered in Seattle. The company is privately held and has raised three rounds of funding totaling $61m, with repeat participation from Madrona Venture Group and Meritech Capital Partners. The company's 250 employees are led by CEO Jesse Rothstein and president Raja Mukerji, both of whom were instrumental in developing F5's operating system, TMOS.

Competition

ExtraHop competes with both pure-play visibility offerings such as those from Gigamon and Ixia, as well as non-traditional approaches to solving visibility. Gigamon and Ixia have both been successful in selling physical, and recently virtual, switches and TAPs and both grew revenue in the mid-40% range year-over-year. Ixia acquired NetOptics in 2014, which included virtual monitoring software that it has since built upon. Gigamon has identified virtual traffic as a key area in its product

development and is a highlighted visibility partner by VMware for its virtual networking offering, NSX. Non-traditional approaches range from OpenFlow-based products from Cisco, Big Switch, Pluribus and NEC, to hybrid-mode capabilities in existing networking switches from Arista and Brocade that can simultaneously function as a standard Ethernet switch as well as a visibility switch.

A key competitor to ExtraHop is Corvil, which is best known for its early success in traffic analysis in high-performance financial (trading) networks. Corvil markets a range of hardware-based appliances that are tuned for maximum performance and low latency, and has not yet announced a high-performance virtual edition; however, its newest launch set the stage for a virtual offering by separating the physical appliance and software pricing.

The elephant in the room is Splunk, the pervasive analysis system software provider. In 2014, Splunk announced its own network traffic capabilities, Splunk Stream, based on technology acquired in its 2013 acquisition of Cloudmeter. Splunk is a key partner of a number of vendors in the visibility market, including ExtraHop, and the introduction of its own traffic analysis offering was a bit of a shock to the delicate mesh of partnerships between data capture and aggregation vendors and the tool providers they serve. ExtraHop and Splunk continue to list one another as partners despite overlap between their respective offerings.

SWOT Analysis

Strengths

Given its lack of legacy hardware revenue (and shareholder expectations), ExtraHop is free to aggressively pursue new technologies and markets to competitively differentiate it in an increasingly crowded market.

Weaknesses

ExtraHop is far smaller than many of its visibility competitors, which means it needs to work that much harder to gain a seat at the RFP table in the mid- and large-size enterprises most likely to need its virtual offering.

Opportunities

As many existing visibility vendors attempt to gradually transition their product mixes from physical to virtual, ExtraHop has a window of opportunity to aggressively grab share with 'born in the cloud' offerings.

Threats

The incorporation of visibility capabilities in networking devices (Cisco ACI, Arista DANZ) and existing analysis products (Splunk) risks absorbing key visibility functions into existing tools.