REPORT REPRINT

ExtraHop goes with the NetFlow

JIM DUFFY

29 SEP 2016

The wire-data analytics specialist is now shipping ExtraHop 6.0, which provides broader visibility into network data through NetFlow support and a packet capture appliance.

THIS REPORT, LICENSED EXCLUSIVELY TO EXTRAHOP, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR REPOSTED, IN WHOLE OR IN PART, BY THE RECIPIENT, WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.

451 Research®

©2016 451 Research, LLC | WWW.451RESEARCH.COM

ExtraHop Networks is now shipping ExtraHop 6.0, which provides broader visibility into network data via NetFlow support and a packet capture appliance. The major aim of the 6.0 release is to enable IT teams to streamline the workflow of real-time performance metrics for application, security, network and business services to associated packets in 'five clicks or less.' It is also designed to transform the network from a transport medium to a rich-data source.

THE 451 TAKE

NetFlow support and packet capture enhance the network data collection and performance management of ExtraHop's wire-data analytics tools. These had previously been gaps in ExtraHop's NPM/APM offerings that the company acknowledges had cost it business in some competitive bids. NetFlow and packet capture have essentially been table stakes for years in NPM, so for ExtraHop it's better late than never. It will make the vendor more competitive in the network data collection aspects of various NPM/APM projects.

CONTEXT

Network and application performance management (NPM/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/APM sales growth.

ExtraHop is one of the few NPM/APM vendors to offer analytics of wire data. Wire-data devices use stream processing and reassembly to inspect real-time Layer 2-7 traffic flowing over the wire. They structure the data into the intended transaction, flow or session, and enable drill-down into the individual metrics, users, applications and packets. Another wire-data analytics vendor in the NPM space is Corvil, a direct competitor of ExtraHop's that is branching into IT analytics from its roots in analysis of financial trading networks.

ExtraHop argues that traditional instrumentation techniques like agents alter the monitored environment, potentially skewing data vital for analyzing IT operations. Installing and managing individual agents on every server, machine, device or other IT asset is also a challenge, the company asserts. And packet capture, widely used in NPM, is just that: it captures network packets, not the wire data that's also associated with a transaction. Also, after a packet is captured, it is stored to disk for inspection. ExtraHop argues that this limits monitoring to post-hoc analysis that in turn is limited by disk speed and space, and requires sifting gigabytes of network data to find and reconstruct relevant information.

PRODUCTS

Yet to offer the most granular details of network data, you need packet capture capabilities. This, and NetFlow visibility, are typically found in network packet brokers, a hotly competitive NPM area that ExtraHop has avoided until now. The new ExtraHop Trace Appliance (ETA) performs continuous packet capture and write-to-disk at a sustained 10Gbps. It ingests data from a SPAN port or TAP monitoring tool, and encrypts the packet data at-rest.

ETA also enables users to drill down into packet transaction records stored in the ExtraHop Explore Appliance (EXA) and from auto-discovered devices for analysis and other visual queries. NetFlow collection in the ExtraHop Discover Appliance (EDA) gives the device visibility into remote sites and edge routers. It ingests NetFlow v5, v9, and IPFIX flow reports for storage and query, where they are combined with wire-data metrics for a more holistic view of the IT environment. With the NetFlow data, ExtraHop 6.0 users can view custom or built-in NetFlow dashboards to spot top-talkers, protocols, conversations and interface utilization, and perform a flow record search.

With NetFlow and packet capture, ExtraHop 6.0 now gives users transaction-to-packet correlation capabilities to search and download packets linked to a specific device, application or transaction record. This capability is woven into the ExtraHop 6.0 workflow so that IT administrators can quickly zero in on any transaction, message or flow on the network and identify the records tied to any particular incident.

ExtraHop 6.0 also supports the SSH protocol for visibility into sessions, with metrics for compression and key-exchange, among others, to determine security posture.

COMPETITION

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

NetFlow and packet capture will add NPM stalwarts Gigamon and Ixia to ExtraHop's competitive roster. Gigamon built its business on network visibility and has offered network packet brokers with NetFlow and packet capture for a few years. Gigamon cites security as a key driver for its growth. Ixia has also been offering NetFlow generation in its NTO packet brokers since 2014, specifically for its Application Threat Intelligence Processor.

A number of other NPM and network visibility vendors offer NetFlow generation and/or packet capture capabilities as well, including SolarWinds, Paessler, Endace, APCON, Plixer, ManageEngine and of course Cisco, which invented the protocol for collecting and analyzing router data on network users and applications, peak usage times, traffic routing, source and destination, class of service and usage patterns. This data is useful for network traffic accounting, usage-based network billing, network planning, security, denial-of-service monitoring capabilities and network monitoring.

SWOT ANALYSIS

STRENGTHS

Incorporating NPM and APM, ExtraHop has a holistic view of IT operations management via real-time stream processing of wire data.

WEAKNESSES

ExtraHop is late to the game in offering network packet broker capabilities, like NetFlow and packet capture, for network visibility. Purer NPM vendors have at least a couple years' head start in this area.

OPPORTUNITIES

The network is a rich data source for NPM, APM, IT operations management, application performance and security. Its importance, and the demand for visibility tools, will only grow with the rise of cloud, mobility and IoT.

THREATS

Beginning with Cisco, 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.