ExtraHop Operational Intelligence Platform v3.10

ExtraHop

Reference Code: IT018-001443
Publication Date: 05 Feb 2014
Author: Michael Azoff

SUMMARY

Catalyst

ExtraHop provides advanced technology for realtime monitoring and analysis of wire data. This covers deep TCP/IP stack layers of network traffic up to the application layer. ExtraHop plays in the application performance management (APM) space but its solution has a broader reach, where IT operational intelligence feeds directly into business delivery. This is new territory is enabled by the availability of wire data analytics technology. ExtraHop's platform has extensions that go far beyond traditional APM capabilities, providing deep analysis of wire data, which is one of the key sources of Big Data from which IT organizations and businesses can derive operational intelligence.

Key messages

- ExtraHop provides wire data analytics with advanced context and correlation capabilities for realtime analysis.
- It performs deep inspection of the TCP/IP stack from data link layer to the upper application layer, including the full bi-directional payload.
- It is designed as a best-of-breed platform operating on both physical and virtual appliances, spanning APM, NPM, EUM, DBM, and SRM, resulting in operational intelligence.
- ExtraHop's strategic partners include Splunk and VMware for log data management, and Arista for mining software-defined networks.

Ovum view

The technology that drives ExtraHop is based on realtime wire data streams feeding into ExtraHop's context and correlation engine. The outcome of this analysis is not only application and infrastructure performance, security, and reliability information, but also information that can help drive better business decisions. This is possible because ExtraHop captures and analyzes all TCP/IP communication across layers two to seven and between all systems, including the full bi-directional transactional payload. This means all the layers of the TCP/IP stack (except the physical layer), starting from data link, then network, transport, session, and up to the top application layer. The ExtraHop platform is able to process this rich data in realtime at sustainable speeds of up to 20 Gbps, and extract and visualize performance, reliability, and security data for IT and business insight. The solution therefore offers realtime visibility across operations and the network, and can also provide monitoring capabilities through its programmable extensibility.

ExtraHop plays across a range of APM capabilities, such as monitoring, discovering, visualizing, diagnosing, and optimizing, as well as assisting security with early-warning detection, such as unusual file downloading patterns or unauthorized file access. ExtraHop's platform rests on five dimensions: solution scalability, depth into the TCP/IP stack, realtime passive analysis of wire data (where passive has the advantage of no overheads), simplicity, and flexibility through a programmable framework.

The ExtraHop wire data context goes beyond traditional network probes and tools that rely on virtual path identifier headers in data packets. It provides full-stream reassembly, which means it simulates both sides of the conversation/traffic using full-state machine simulation to monitor traffic, provide deep analysis, and detect anomalous behavior. The next step is full-content and payload analysis using an intelligent protocol framework. For each protocol (for example, Citrix) ExtraHop has a custom parser that understands the protocol, decodes it, and can passively interrogate anything in the per-user session or transaction traffic. ExtraHop's deep inspection of the packets, and the reassembly into complete application transactions, means it understands which data packets belong to which application and what they mean, so response times are accurate and can monitor timed transactions, for example.

To complement its focus on wire data, ExtraHop has a strategic partnership with Splunk, a machine data specialist. This combination provides full coverage of data that can be tapped from the network and from log files. It also helps ExtraHop position itself in the market because customers of Splunk can readily understand ExtraHop's business proposition. ExtraHop finds that its customers turn to it when they do not want a big-bang APM solution from a large IT vendor. It finds a strong market for a solution that can leverage the information content of wire data, and positions itself well as a best-of-breed player, complementing other best-of-breed point solutions in the APM ecosystem.

ExtraHop also has a partnership with Arista, a provider of software-driven network switches and routers for software-defined networks (SDNs). The software-enabled intelligence that is built in to Arista's products enables ExtraHop to capture rich information about traffic in highly dynamic virtualized environments and improve its monitoring capabilities in these environments. SDNs automate network changes, and visibility into what is happening in the network can be lost. In addition, there is the inter-data center tunnel-based SDN approach which again requires visibility. Therefore, as network changes such as virtual machine motion take place, ExtraHop receives the change information as it tracks particular applications, and is able to monitor the whole network ecosystem to provide an improved view of performance-related events. This is what ExtraHop calls persistent mobile visibility.

RECOMMENDATIONS FOR ENTERPRISES

Why consider the ExtraHop Wire Data Analytics Platform?

ExtraHop's approach is different to many traditional approaches in that it passively mines the wire (network) to manage application performance, availability, and security. The increasingly heterogeneous, distributed, and dynamic nature of applications across physical and virtual environments is causing IT organizations to look for approaches that are better able to monitor these applications. ExtraHop is at the forefront of tapping data on the wire for use in APM, including the full bi-directional transactional payload underlying all on-the-wire communications. Its solution is designed to be simpler to deploy and maintain, and will work for all applications.

IT organizations have to maintain legacy applications while supporting new IT initiatives, such as cloud migration, BYOD, DevOps collaboration, VDI, and more, and this will cause organizations to seek out solutions that work for all their networked applications, whether custom-developed or off-the-shelf.

SWOT ANALYSIS

Strengths

Realtime processing of wire data based on Big Data analytics technology

The ability to track vast amounts of network traffic in realtime is a major accomplishment. The platform is built on Big Data technology, with an advanced context and correlation engine that does the equivalent of complex event processing but for L2 through L7 traffic.

Business use cases go beyond traditional APM scope

ExtraHop has released a number of free extensions to its platform, including SharePoint, cloud, and WAN analytics. It has developed a security module for monitoring security-related events, because its customers want to use its extensibility for pervasive monitoring. The security module detects anomalous activity around storage and database access, such as a user accessing more than 100 files an hour.

IT operational intelligence for virtual and dynamic applications

ExtraHop is at the forefront of new APM technologies. Its ability to mine wire data complements the rise in log management solutions for machine data. The combination of wire and machine data is complementary, and ExtraHop's partnership with Splunk is a good match.

Weaknesses

ExtraHop is aimed squarely at IT operations but also has a DevOps role

ExtraHop’s ability to deliver operational intelligence is aimed at operations and is not specifically designed to offer features of interest to developers, such as source code level detail of issues, or to QA for performance testing. However, the solution can play a role in DevOps as part of the support that IT operations staff requires to monitor the health of applications.

Best-of-breed product requires complementary solutions to cover gaps for full APM coverage

ExtraHop does one job extremely well: tapping wire data. This has multiple uses within IT operations, but users will also require other solutions to ensure that gaps are covered. This includes developer-oriented APM, end-user experience monitoring, and mainframe performance monitoring.

Opportunities

The synergy between machine and wire data means a single solution would be a powerful product

ExtraHop has a partnership with Splunk, and the alliance begs the question of whether ExtraHop should evolve to cover log data itself. The use of Big Data realtime analysis is common between the two approaches, and having both wire and machine-mining technologies under the same hood may yield even better synergies.

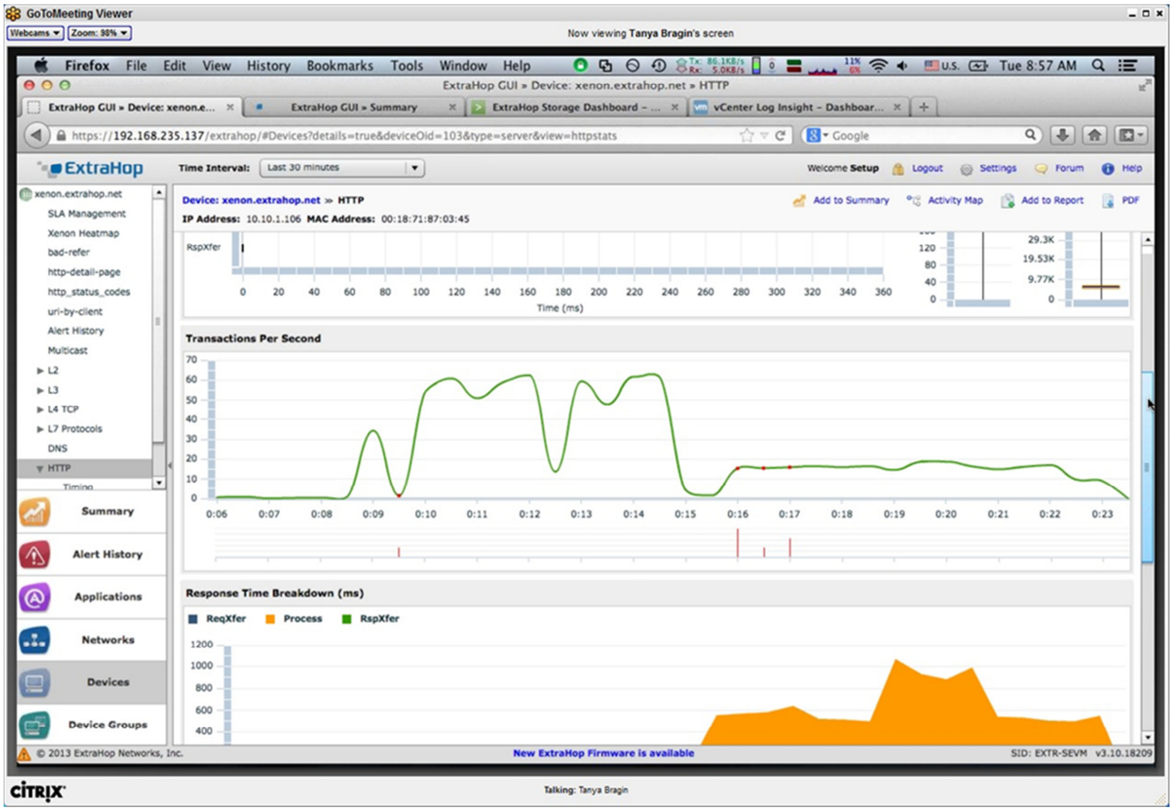
ExtraHop's strategic partnerships are a sound marketing strategy

ExtraHop is proving adept at strategic partnerships, and the evolution of data centers to software-defined data centers and networks creates a rich source of operational intelligence. Additional partnerships would help ExtraHop expand its reach and proving point.

Threats

ExtraHop founders came from F5 Networks, having created new and patented technology built on their network expertise. It is unlikely that F5 will make a move into APM, but there is the possibility that a larger APM vendor may take an interest in ExtraHop.

Figure 1: ExtraHop http analysis



Source: ExtraHop

DATA SHEET

Key facts about the solution

Table 1: Data sheet: ExtraHop Operational Intelligence Platform

Product name	ExtraHop Operational Intelligence Platform	**Product classification**	APM
Version number	3.1	**Release date**	Current
Industries covered	All	**Geographies covered**	All
Relevant company sizes	All	**Platforms supported**	Physical appliances: all environments. Virtual appliances: VMware ESX, Microsoft Hyper-V, Amazon Web Services AMI.
Languages supported	English	**Licensing options**	Perpetual and subscription
Deployment options	ERSPAN, SPAN, RPCAP, Port Mirroring, TAP aggregation to virtual and physical appliances	**Route(s) to market**	Reseller and direct sales, integration partnerships with VMware, Cisco, Arista, F5, Citrix, Microsoft, others.
URL	www.ExtraHop.com	**Company headquarters**	Seattle, WA US

Source: Ovum

APPENDIX

Methodology

Ovum SWOT Assessments are independent reviews carried out using Ovum's evaluation model for the relevant technology area, supported by conversations with vendors, users, and service providers of the solution concerned, and in-depth secondary research.

Author

Michael Azoff, Principal Analyst

michael.azoff@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.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.