Ovum
TMT intelligence | informa

On the Radar: ExtraHop enhances its platform for security teams and nontechnical staff

The vendor targets a wider audience with version 7.0

Publication Date: 19 Sep 2017 | Product code: IT0022-001083

Rik Turner

Summary

Catalyst

ExtraHop provides technology that performs real-time analysis of network communications. The company markets its technology to network, IT operations, and security teams.

Key messages

- ExtraHop works by deploying appliances on corporate networks and in cloud infrastructure.
- It also offers software-as-a-service- (SaaS-) based machine learning for performance and security anomaly detection and alerting.
- Version 7.0 of its underlying software platform adds live activity maps, support for perfect forward secrecy (PFS), automated response to anomalies through machine learning, and data accessibility for a broader audience within an enterprise.
- These enhancements underscore the company's horizontal outreach beyond networking professionals to IT ops and security teams, as well as vertical outreach to board-level and line-of-business executives who need to see operational and/or security data.

Ovum view

With the efficacy of traditional signature-based approaches to security waning, there is a requirement for technology that can analyze network activity for anomaly detection. Wire data is the ultimate source of such information, so ExtraHop's technology is becoming increasingly relevant for security as well as network monitoring and IT operations.

Recommendations for enterprises

Why put ExtraHop on your radar?

ExtraHop aims to make the wire data from your network the go-to data source for security and IT operations monitoring. In a security context, this can help with anomaly detection and speed up threat incident response times. The fact that the company is making its data more accessible to nontechnical staff, including C-level executives, is also a positive development that should make it a contender for any improvements to your monitoring capabilities.

Highlights

Wire data encompasses all communications on a network, spanning private, public, and hybrid infrastructures, and it is derived by decoding wire and transport protocols from raw network data. The challenge in using it for activity monitoring has traditionally been its sheer volume, combined with the time lag required to achieve insights from it. Many monitoring devices sidestep the issue by using event logs, which are summaries of network events recorded by firewalls and other devices. By contrast, wire data is an unadulterated, observed source of all network activity.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

ExtraHop came into existence to address the scale challenge. It inverts the conventional approach of ingesting raw packets and writing them to disk, assembling packets, and then analyzing them. Instead, it performs analysis in real time, before writing to disk. This results in a view of all transactions, from which customers can, if they wish, take a deeper dive into the individual packets.

In addition to overcoming the time lag problem, ExtraHop's streaming approach is inherently parallelizable, since analysis can be spread across multiple CPUs, with more cores added as required. This overcomes the scalability issues that the conventional approach to network monitoring presents.

ExtraHop 7.0

The company is introducing version 7.0 of its eponymous software platform, which underpins all its appliances and will therefore be rolled out as an update to all existing customers. The new version includes the following enhancements.

Live activity maps

ExtraHop has added a visualization capability for network activity. This is a forensic tool that takes anomalies detected by the platform on premises or the vendor's cloud-based machine-learning capability, Addy, and performs root cause analysis, with features such as ad hoc filtering, panning, zooming, and drill-downs.

Support for PFS

PFS is a property of secure communication protocols, in which the compromise of long-term keys does not compromise past session keys. It is scheduled to be added to the TLS standard in version 1.3 in mid-2018, making man-in-the-middle attacks impossible. ExtraHop has already added support for it to enable per-transaction security with continued visibility of the data for monitoring purposes and line-rate performance.

This emerging encryption standard has historically come with trade-offs for IT ops teams, who lose visibility of PFS traffic with traditional monitoring tools. ExtraHop resolves this issue, allowing security teams to implement PFS without compromising application and infrastructure visibility.

Security anomalies via ExtraHop Addy

ExtraHop seeks to close the gap between initial infection and detection, which is still 120–200 days, with anomaly detection of suspicious behavior such as network scans and data exfiltration. Once such behavior is detected, anomaly-initiated workflows allow security teams to quarantine suspect hosts and investigate what stage an attack has reached (initial compromise, remote access, lateral movement, data gathering, or exfiltration) to facilitate prioritization. Data can also be exported to systems such as ServiceNow and Cisco Tetration using ExtraHop's Open Data Stream format.

Enterprise-wide views

To make data accessible to nontechnical users in organizations, ExtraHop has added dashboard and metrics sharing, with access based on user role, plus reports to stakeholders for policy compliance, service-level agreement (SLA) performance, and business operations.

These moves underscore ExtraHop's desire to make the network, and the wire data derived from it, the "ultimate source of truth" for the constituencies it targets within an enterprise. It seeks to widen its

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

appeal horizontally, to IT operations and security, and vertically, to line-of-business and board-level executives.

Background

ExtraHop was founded in Seattle in 2007 by CTO Jesse Rothstein and chief customer officer Raja Mukerji. Both had been senior architects at load balancing vendor F5 Networks, where they had been instrumental in the transformation of load balancers into a new device category called an application delivery controller. They created ExtraHop's network analytics platform to exploit real-time wire data and address the drawbacks of traditional network monitoring techniques.

ExtraHop's CEO since mid-2016, Arif Kareem, spent six years as president of Fluke Networks (now part of NetScout), where he helped increase the company's revenue to more than $350m and oversaw the acquisition and integration of AirMagnet and ClearSight Networks.

ExtraHop has so far received $61.6m in three rounds of funding. Its last round was a Series C round, worth $41m, in May 2014, led by Technology Crossover Ventures (TCV), which has invested in companies such as RealNetworks, Splunk, and RiskMetrics. Other notable investors include Meritech Capital Partners and Madrona Venture Group.

Current position

ExtraHop started life offering complete wire data analytics for network monitoring, and in 2015, it was led by customer demand to expand into security. Its analytical and machine-learning capabilities can clearly contribute to activities such as anomaly detection, and security is now one of the three areas that the company targets. It currently offers more than a dozen security-specific product bundles, as well as integrations with other security platforms.

The vendor now segments its market into three areas: network performance monitoring, IT operations, and security. It delivers its technology via appliances (physical or virtual) deployed in the customer's network or in public cloud environments such as AWS and Azure. Customers can opt for a capex (appliance pricing plus maintenance) or opex (subscription) payment approach.

ExtraHop charges by the capacity of the boxes (i.e. the throughput they can handle) rather than the volume of data analyzed, arguing that this approach avoids the so-called "data tax" scenario.

In April this year, ExtraHop built on its stream analytics capabilities with the launch of its SaaS machine-learning offering, Addy, a service for detecting anomalies, with the machine learning done in AWS. Addy is currently available in the US, Canada, and Australia, and the company plans to extend it to Europe, with the requirement to adjust how it works in order to comply with the EU's General Data Protection Regulation (GDPR).

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Data sheet

Key facts

Table 1: Data sheet: ExtraHop

Product name	ExtraHop	**Product classification**	Software
Version number	7.0	**Release date**	September 2017
Industries covered	All industries, but with a particular focus on financial services, healthcare, retail and e-commerce, telecommunications, manufacturing and industries, and IT	**Geographies covered**	North America, Asia-Pacific, EMEA
Relevant company sizes	Enterprise	**Licensing options**	Perpetual license and subscription
URL	https://www.extrahop.com/	**Routes to market**	Direct and channel
Company headquarters	Seattle, WA, US	**Number of employees**	315

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@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.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo