Ovum
TMT intelligence | informa

ExtraHop enters network detection and response with Reveal(x)

Publication Date: 10 Jul 2018 | Product code: INT003-000191

Rik Turner

Ovum view

Summary

ExtraHop, a developer of real-time analytics technology on wire data in corporate networks for IT operations and security, has released its first security-specific product called Reveal(x). It analyzes all network interactions, applying machine learning to detect abnormal behavior, and then automates basic functions to streamline threat investigations. The launch of Reveal(x) takes ExtraHop into the network detection and response (NDR) market.

This is ExtraHop's first purpose-built security product

Though it came into existence in 2007 specifically to facilitate performance monitoring for both networks and applications, ExtraHop became aware that some customers use the ExtraHop Platform for purposes of security, enabling them to get a better handle on what is underway in their networks. In recognition of this fact, in 2017 the company made enhancements to version 7.0 of the software that underpins its appliances, enabling certain security features.

Among them was support for perfect forward secrecy (PFS), even before it was included in the latest version of the Transport Layer Security (TLS) standard (version 1.3). The company also launched its cloud-based machine learning service, called ExtraHop Addy, which offers security capabilities that include anomaly detection and the prioritizing of alerts so that busy SOC analysts can distinguish the key threats from the cacophony of noise coming at them.

Now ExtraHop has gone a step further with the launch of Reveal(x), a purpose-built platform for security.

Goals are visibility, traffic analysis, and automated response

ExtraHop set itself three objectives for Reveal(x):

- to provide enterprise visibility of threats
- to deliver advanced behavioral analytics on network traffic
- to automate as much of the investigative process as possible, enabling tier-3 SOC analysts to be more effective in the use of their time and tier-1 analysts to punch above their weight.

Like ExtraHop's eponymous performance monitoring product (i.e., the ExtraHop platform), Reveal(x) is based on the use of passive appliances – that is, deployed out of band on the SPAN port of a switch or as a TAP, and thus not actually in the flow of traffic across a network.

These devices extract features and metrics from the wire data traversing the network, with the vendor boasting the ability to inspect more than 50 protocols and analyze them for some 4,600 different features. The platform also detects and classifies all devices on the network, providing a lot of analysis before having recourse to the cloud-based machine learning capabilities.

Reveal(x) already covers protocols specific to certain verticals, such as HL7 for the healthcare sector and Modbus for supervisory control and data acquisition (SCADA) systems in industry. In other words, the product can be used in Internet of Things (IoT) environments as well as conventional IT networks.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

The idea is for the system to highlight anomalies it has detected in the wire data and enable the SOC analyst to investigate, via the activity map visualization tool launched last year, to see exactly which systems have been talking to one another and what changes have been made in the connections, for instance. The analyst can inspect DNS, NFS, CIFS, SSH, and AAA ("triple-A") traffic, with Reveal(x) having pre-selected anything of interest before the analyst gets to it.

ExtraHop can not only address physical networks, but also cloud environments via the RPCAPD technology, which is effectively a software TAP, deployed as an agent directly into the virtual machines a customer is running in the cloud.

Reveal(x) comes in Standard, Premium, and Ultra versions

Reveal(x) comes in three flavors:

- Standard, which provides full stream analysis, detection of security anomalies, and coverage of all standard and premium protocols. This version is suited to companies whose SecOps team has a modest security program and some degree of incident response.
- Premium, which adds an out-of-band decryption capability, as well as integration with downstream platforms such as ServiceNow, Splunk, and Phantom (recently acquired by Splunk), using ExtraHop's Open Data Stream format. This is for companies with a more mature security program, a security incident and event management (SIEM) platform, and an encryption system in place.
- Ultra, which adds full packet capture for companies with a sophisticated and proactive security program, typically performing threat hunting or setting triggers for certain actions, and teams with forensic and compliance requirements.

In all three cases, the charging model for the technology is a subscription, the size of which is based on the number of assets monitored by the system and the range of feature/functions included in the package.

NDR is part of xDR and a component of MDR services

The launch of Reveal(x) puts ExtraHop in the NDR market, competing with the likes of Darktrace, Vectra, and ProtectWise. In this context, Ovum would like to see the company adding more response features to its product, which could take the form of recommended actions for incident responders or possibly even certain automated mitigation and remediation capabilities.

Of course, NDR is one half of the xDR continuum, the other being the more widely known endpoint detection and response (EDR). It will be interesting to see whether ExtraHop feels the need to partner with an EDR player, just as NDR provider eSentire has done with Carbon Black, for a complete offering. It would also make sense for the vendor to forge relationships with managed security service providers (MSSPs) that seek to offer a managed detection and response (MDR) service featuring both pillars of the xDR spectrum.

Appendix

Further reading

On the Radar: ExtraHop enhances its platform for security teams and nontechnical staff, IT0022-001083 (September 2017)

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.

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

ovum.informa.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo