ExtraHop Unveils Blueprint for Effective NDR to Improve Security Postures

Submitted by: Positive Marketing
Tuesday, 28 February 2023

New insights highlight five key capabilities to enhance your security strategy

SEATTLE – February 28, 2023 – ExtraHop, the leader in cloud-native network intelligence, today published, “The Role of NDR in Your Security Strategy,” a new white paper detailing a technology blueprint for effective network detection and response (NDR) to help organizations improve their security posture. This must-read report shares five key capabilities to help CISOs and IT security leaders derive greater value from their security strategy.

Today, more and more organizations are looking to NDR to strengthen their security posture and overcome a range of visibility and resource challenges associated with traditional endpoint detection and response (EDR) and security information and event management (SIEM) solutions. Validating growing demand, the Gartner® Market Guide for Network Detection & Response, December 2022 found the NDR market continues to grow steadily at 22.5%.

As the market becomes more crowded, the white paper aims to provide IT and security teams with a greater understanding of what NDR is, how it works, and what makes for a successful implementation, so organizations can extract immediate and lasting value. Readers will walk away with a greater understanding of the technical capabilities required for an NDR strategy to confidently move forward in their cybersecurity journey.

The five key capabilities include:

Cloud-scale machine learning: Utilize cloud-scale machine learning to ensure all environments are secure, without slowing business down.

Continuous and on-demand packet capture (PCAP): Look for solutions that offer both continuous and on-demand PCAP.

Internal traffic decryption: Ensure you have the ability to decrypt internal traffic across a range of protocols to detect attackers earlier in the attack cycle.

Clear intuitive workflows: Streamline investigations with clear, intuitive, and automated workflows to more easily understand the data.

Automated asset discovery: Automate managed and unmanaged asset discovery to discover new devices as soon as they communicate.

“As attackers’ techniques mature, organizations have realized they cannot rely solely on logs or endpoints for early threat detection – the network is where they’ll get the clearest picture of what is going on,” said Jesse Rothstein, co-founder and CTO, ExtraHop. “However, with the NDR market

widening, there’s been a muddying of the waters with different claims and value propositions. When moving forward with NDR, it is important that organizations look carefully at the technical components within their solutions to ensure they will have a clear view of the attack surface, so they can more quickly detect, investigate, and respond to threats across cloud, on-premises, and hybrid environments.”

To learn more, download “The Role of NDR in Your Security Strategy” (https://www.extrahop.com/resources/papers/role-of-ndr-in-your-security-strat/) and read the blog (https://www.extrahop.com/company/blog/2023/harnessing-the-power-of-network-data/).

Additional Resources

Learn more about ExtraHop NDR solutions: https://www.extrahop.com/solutions/

Read the 2022 Gartner Market Guide for Network Detection and Response: https://www.extrahop.com/resources/papers/gartner-ndr-market-guide-2022/

Download the Beginner's Guide to Network Detection and Response for Hybrid Security: https://www.extrahop.com/resources/papers/beginners-guide-to-ndr/

Evaluate your NDR ROI: https://www.extrahop.com/resources/papers/forrester-tei-study/

Required Disclaimer: Gartner, Market Guide for Network Detection and Response, Jeremy D'Hoinne, Nat Smith, Thomas Lintemuth, 14 December 2022. The Market Guide for Network Detection and Response was previously published as the Market Guide for Network Traffic Analysis in 2019.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

ABOUT EXTRAHOP

Cyberattackers have the advantage. ExtraHop is on a mission to help you take it back with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, enterprises can detect malicious behavior, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others.

When you don't have to choose between protecting your business and moving it forward, that's security uncompromised. Learn more at www.extrahop.com.

© 2023 ExtraHop Networks, Inc., Reveal(x), Reveal(x) 360, Reveal(x) Enterprise, and ExtraHop are registered trademarks or marks of ExtraHop Networks, Inc.

EXTRAHOP CONTACT

Daisy Pledge
Account Director
dpledge@positivemarketing.com

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Positive Marketing

Copyright © 1999-2024 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com

responsesource