Custom Report

Contents

This report was made from the following documents:

Network Visibility, Detection and Response: Modern Analytics for Today's Threats

Key Findings

- Network visibility, detection and response (NVDR) is an emerging segment of information security (infosec) technology, intersecting with network technology, that seeks to surpass legacy techniques and provide more realistic insight into malicious activity within the environment. The technology is often seen as a successor to network intrusion detection and prevention systems, but in fact represents the latest culmination of trends going back to network anomaly detection techniques instrumental in uncovering worms, to more recent applications of behavior analytics to identify ransomware and tackle high-profile (and high-impact) attacks.
- As with other technologies that have had an impact on changing the nature of the infosec market, NVDR is distinguished from past techniques by the application of modern analytics and machine learning to network activity data, to better identify threats and improve security response.
- The network remains not only a primary source of security insight – it is also the most sought-after skill among enterprise security teams. Eighty-one percent of respondents to 451 Research's Voice of the Enterprise (VotE): Information Security, Organizational Dynamics 2019 study identify network security as the most important skillset for security professionals, ahead of security architecture (68%), regulatory compliance/audit (59%) and operations (58%). Technology refresh is a significant driver in NVDR evaluation and adoption, with intrusion detection and prevention systems among the top targets.
- Unacceptable evidence of penetration and 'dwell time' – the length of time an attack remains on a network before response mitigates the threat – are among the drivers of generational change in this arena, reflecting similar trends in other areas of security technology where the application of machine learning is a primary focus.
- The IoT explosion further drives need, especially where legacy technologies have little or no existing foothold, and where adversary tactics and targets may differ significantly when it comes to operational or industrial environments. A dearth of security functionality on consumer endpoints may exacerbate this need, where they become a significant factor for enterprises.
- NVDR faces challenges in adoption, however. Machine learning has become one of the most buzzy terms in the security industry; vendors will have to substantiate their claims with tangible results and reduced workloads for human experts. Automation features will be expected to further optimize offerings, while NVDR must also embrace cloud and cloud-native technologies to be relevant in the world of modern IT.

451 Research

Source: 451 Research, LLC

451 Research

Executive Summary

Introduction

If there is one constant that defines IT, it is change – ongoing innovation that redefines the nature of technology every few years. This evolution, however, also introduces new risks that adversaries can capitalize on.

Two key factors highlight a primary focus of security in mitigating these risks:

- No matter how new or evolved enterprise computing becomes, one common theme – the network – will continue to connect everything. Networking may manifest in a variety of new ways, from virtual concepts implemented within a specific cloud architecture, to the nature of high availability in the field being defined by emerging 5G. Yet through it all, the network will remain the fabric that weaves technologies together and makes possible much of the innovation that will drive the enterprise of the future.
- The evolution of computing at cloud scale made available to organizations of all sizes has also made possible the evolution of analytic techniques that can be applied to security. Among these are the strides made in areas such as machine learning – a key component with high expectations for helping to alleviate dependence on human expertise to better understand and identify where, when and how human adversaries can seek to outwit each other in the gamesmanship of threat and defense.

In this report, we explore the intersection of these two realities defining emerging defense, as manifested in the technology of network visibility, detection and response (NVDR). NVDR goes beyond prior generations of network-based threat detection to take advantage of the unique perspective of the network to see, and better respond to, the scope and variety of modern threats. We explore the three key domains of NVDR:

- Enhanced visibility extended from existing and legacy environments into emerging domains, from legacy environments to emerging cloud and cloud-native architectures, to enterprise-grade connectivity in the field no matter how dispersed or challenging.
- Detection supported by the recognition capabilities of technologies that can learn.
- Improved response through the application of automation for handling the findings of NVDR, as well as integration with both existing and emerging technologies and tools for more comprehensive defense.

Source: 451 Research, LLC

We look at the drivers shaping this market, how NVDR compares with previous techniques, and some of the strategic players and emerging vendors in NVDR with a view toward their strengths and challenges. We conclude with guidance for vendors and enterprises alike seeking to make the most of the NVDR opportunity.

Methodology

This report leverages our security experiences, relationships, and interviews with vendor and enterprise security executives. The bulk of the research is derived from vendor briefings, customer reference checks and publicly available information.

We are also guided by quantifiable research, as found in 451 Research's Voice of The Enterprise (VotE) survey data research on cloud, IT, networking and security trends, as well as our Merger & Acquisitions KnowledgeBase (MAKB), which details acquisitions of technology product and service vendors. Finally, the Universal Risk chapter within 451 Research's comprehensive 4Sight Report provided an excellent framework for describing the network security maturity model.

This report represents a holistic perspective on the transforming NVDR segment within the enterprise security market. This and related markets evolve quickly, though, so 451 Research offers additional services that provide critical marketplace updates. These updated reports and perspectives are presented on a daily basis via the company's core intelligence service, 451 Research Market Insight. Forward-looking M&A analysis and perspectives on strategic acquisitions and the liquidity environment for technology companies are also updated regularly via Market Insight, which is backed by the industry-leading 451 Research M&A KnowledgeBase.

Emerging technologies and markets are covered in 451 Research channels including Applied Infrastructure & DevOps; Cloud Transformation; Customer Experience & Commerce; Data, AI & Analytics; Datacenter Services & Infrastructure; Information Security; Internet of Things; Managed Services & Hosting; and Workforce Productivity & Collaboration.

Beyond that, 451 Research has a robust set of quantitative insights covered in products such as Voice of the Enterprise, Voice of the Connected User Landscape, Voice of the Service Provider, Cloud Price Index, Market Monitor, the M&A KnowledgeBase and the Datacenter KnowledgeBase.

All of these 451 Research services, which are accessible via the web, provide critical and timely analysis specifically focused on the business of enterprise IT innovation.

For more information about 451 Research, please go to: *www.451research.com*.

Source: 451 Research, LLC