EMA
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

EMA Radar™ Report for Network Operations Observability

Summary Report Spotlighting Broadcom

October 2024

By **Shamus McGillicuddy**, VP of Research
Network Infrastructure and Operations

Table of Contents

Executive Summary

This EMA Radar Report examines the capabilities of 14 leading vendors of network operations observability solutions. It serves as a buyers' guide for products that network infrastructure and operations teams use to manage the health and performance of modern digital network infrastructure. It examines the overall market position of each vendor based on the capabilities of their products, the total cost of ownership of using these products, and the overall strength of individual vendors. The information in this Radar is delivered via an easy-to-decipher, detailed market map and Radar Chart – which includes a composite score for each vendor – making it simple to see how vendors measure up in the market. It also provides a detailed discussion of methodology and criteria, a review of emerging customer requirements that shaped EMA's evaluation criteria, and a comprehensive analyst writeup on each vendor.

What is Network Operations Observability?

Network operations observability (NOO) is a class of solutions IT organizations use to manage and monitor network infrastructure and services. Key use cases for NOO solutions include network discovery, monitoring, troubleshooting, and capacity planning. Vendors and customers also describe these solutions as network monitoring and network performance management tools. In recent years, vendors embraced the concept of network observability to communicate a more advanced approach to network operations tools, with an emphasis on providing insights and automation rather than simply collecting and presenting network data.

EMA sought to define this concept more concretely in our market research. In October 2022, we published "Network Observability: Delivering Actionable Insights to Network Operations," a research report based on a survey of 402 IT stakeholders. As **Figure 1** reveals, 90% of respondents agreed that "network observability" was a term useful for describing the tools they use to monitor and manage the health and performance of their networks.

FIGURE 1. DO YOU BELIEVE NETWORK OBSERVABILITY IS A USEFUL TERM FOR DESCRIBING THE TOOLS YOU USE TO UNDERSTAND AND MANAGE THE HEALTH AND PERFORMANCE OF YOUR NETWORK?

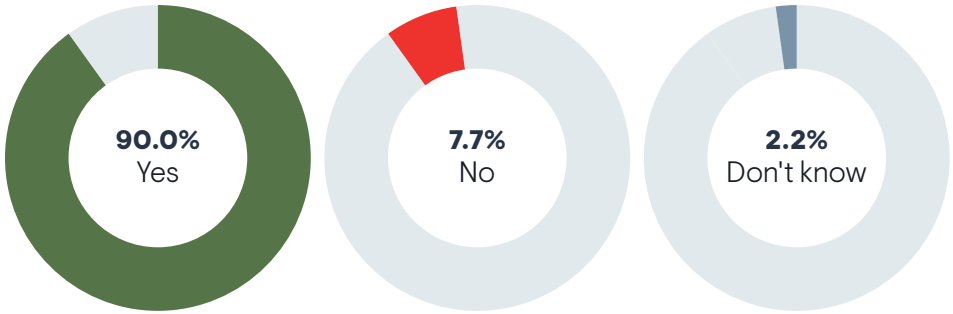
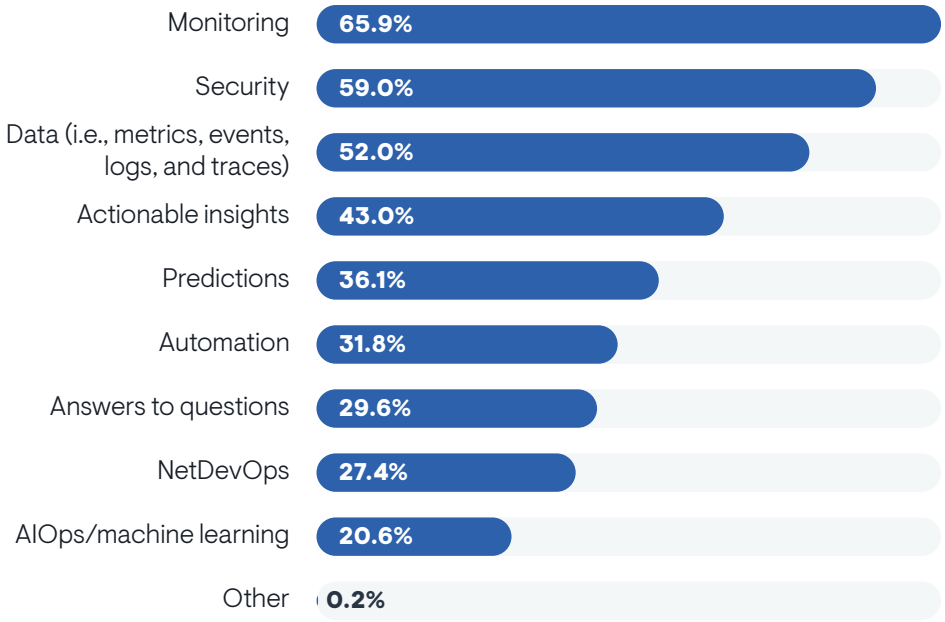


Figure 2 reveals the concepts respondents associated with the term "network observability." The top response was "monitoring," reinforcing EMA's stance that network observability is a subset of network performance management and network monitoring tools. The number two response was security. Given this finding, EMA has begun using the term "network operations observability" to distinguish between observability solutions that support security operations and observability solutions that support network operations and engineering.

Most respondents also associated "data" with network observability. EMA believes this indicates that IT organizations see a need for collecting and analyzing a greater diversity of network data (e.g., streaming network telemetry, synthetic traffic) and higher volumes of network data. Finally, many respondents selected "actionable insights," "predictions," and "automation." This points to a desire for tools that do more than collect data and present data in charts, graphs, dashboards, and reports. They want their tools to help them understand what the data means and to automate how they respond to insights revealed within that data. Thus, EMA defines network operations observability as a class of network monitoring solutions that provides actionable and predictive insights into network infrastructure with the ability to automate aspects of network operations through advanced analytics, including the use of AI and machine learning.

FIGURE 2. WORDS AND PHRASES THAT RESEARCH PARTICIPANTS MOST ASSOCIATE WITH THE CONCEPT OF NETWORK OBSERVABILITY



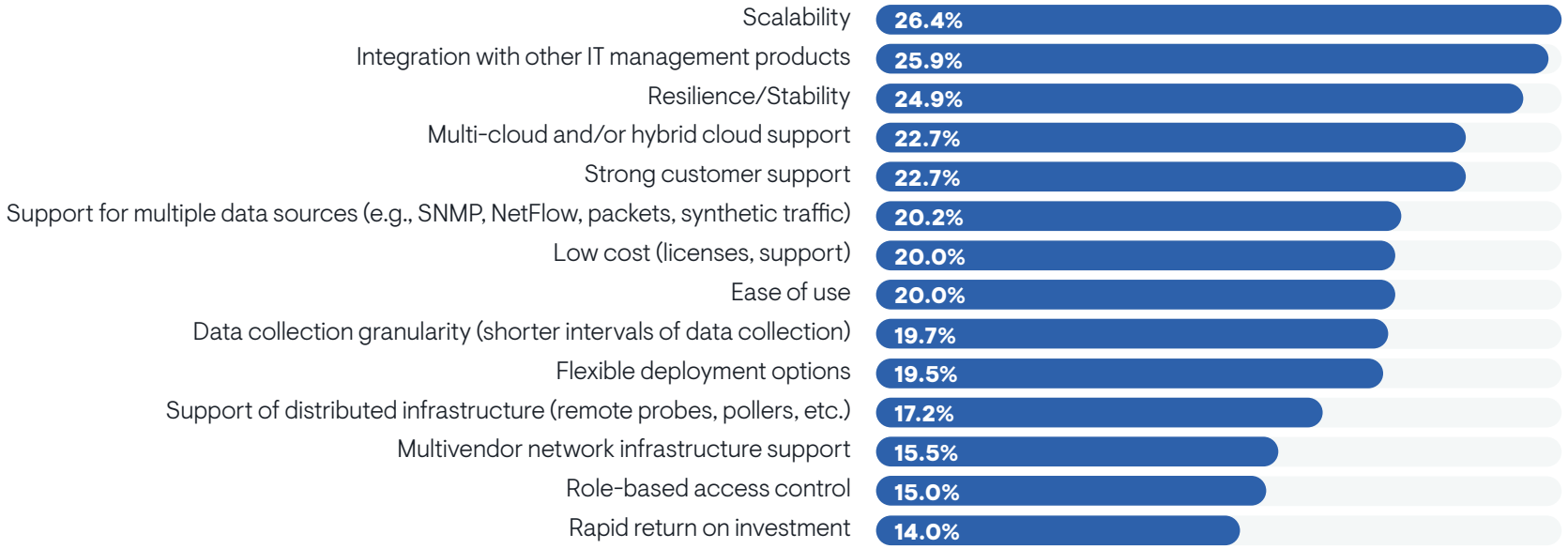
Evolving Requirements for Network Operations Observability: A Market Research Review

A significant portion of this Radar's vendor evaluation process is based on evaluation criteria we used for the EMA Radar for Network Performance Management published in 2021. We updated that criteria to reflect customer interest in observability solutions that offer actionable insights, predictive analytics, and automation. Thus, the results of this Radar are quite different than that of the 2021 report. The following is a review of key findings from EMA's research into network operations observability requirements.

General Platform and Business Requirements

In May 2024, EMA published its biannual "Network Management Megatrends" report based on a survey of 406 IT stakeholders. That research explored current trends in network management tool requirements. **Figure 3** identifies the top platform and business requirements that IT organizations have for network tools. EMA used this data to refine our evaluation criteria. The top five selections in this chart (scalability, integrations, resilience, cloud support, and customer support) all factored heavily in our review of vendors.

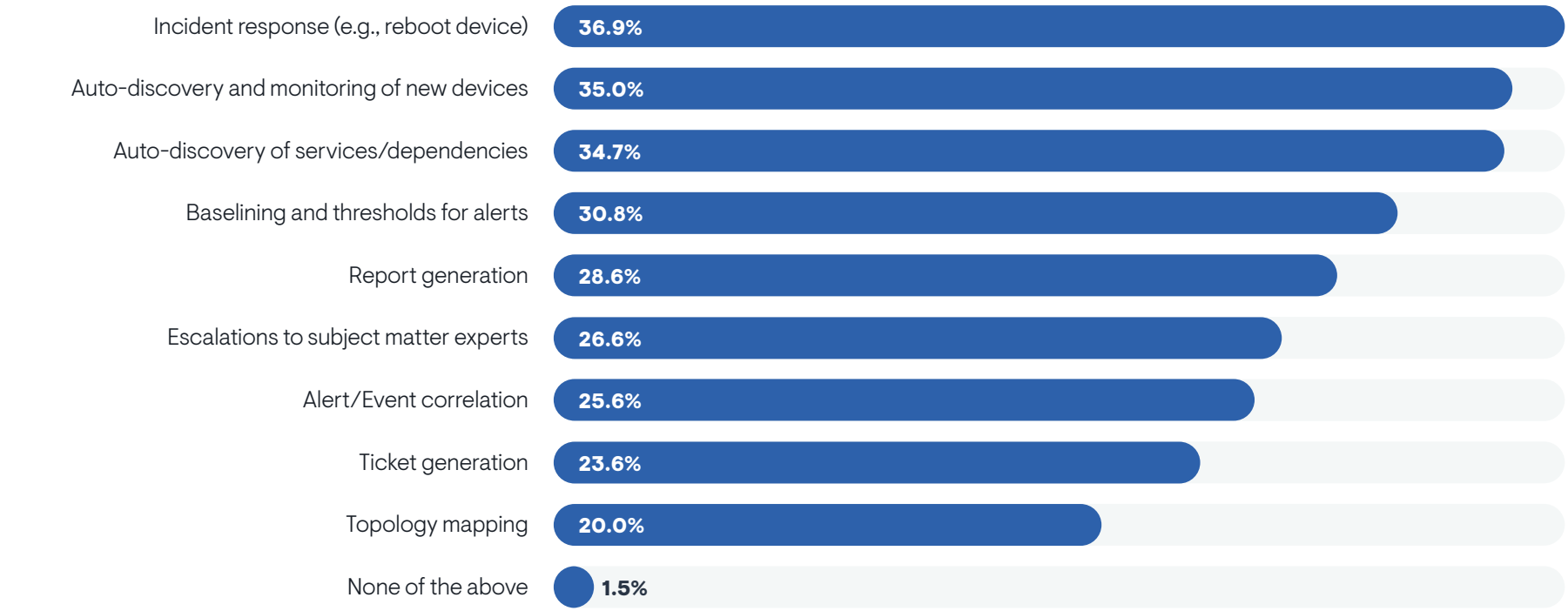
FIGURE 3. WHAT ARE YOUR ORGANIZATION'S TOP BUSINESS AND PLATFORM REQUIREMENTS FOR NETWORK MANAGEMENT PRODUCTS?



Tool Automation Priorities

The Megatrends research also asked respondents to identify what aspects of their network management tools they most want to automate. **Figure 4** shows that they prioritize automation of network incident response, discovery and monitoring of new devices, discovery of services and dependencies, and baselining and thresholds for alerting. EMA's evaluation of vendors included their ability to automate these aspects of network operations.

FIGURE 4. WHAT ASPECTS OF YOUR NETWORK MONITORING TOOLS DO YOU AUTOMATE OR NEED TO AUTOMATE TO IMPROVE OPERATIONAL EFFICIENCY?



Consumption Flexibility

Deployment and license flexibility is increasingly essential for network operations observability tools. Ten years ago, nearly all network management tools were deployed on-premises and sold with a perpetual license. The industry moved away from this legacy consumption model recently.

Figure 5 reveals that 65% of IT organizations want SaaS-based network management tools, and **Figure 6** shows that most want a subscription or pay-as-you-go license rather than perpetual licenses.

FIGURE 5. WHAT IS YOUR PREFERRED DEPLOYMENT MODEL FOR NETWORK MANAGEMENT TOOLS?

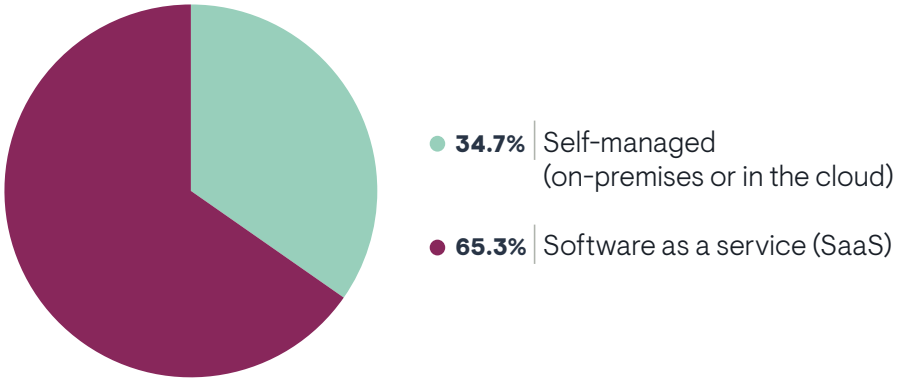
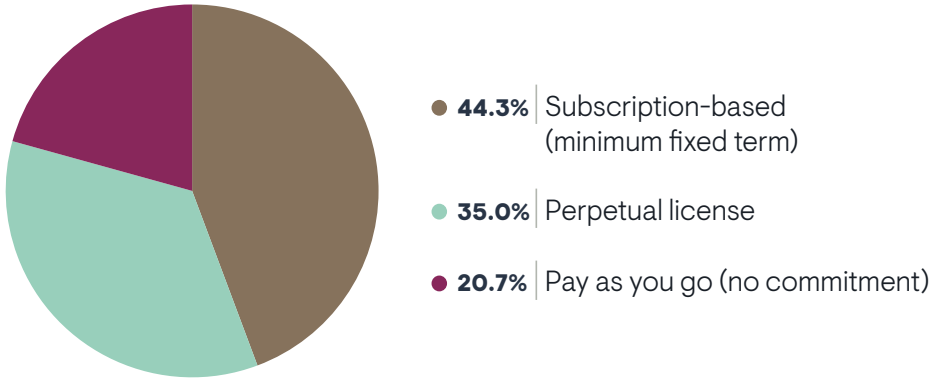


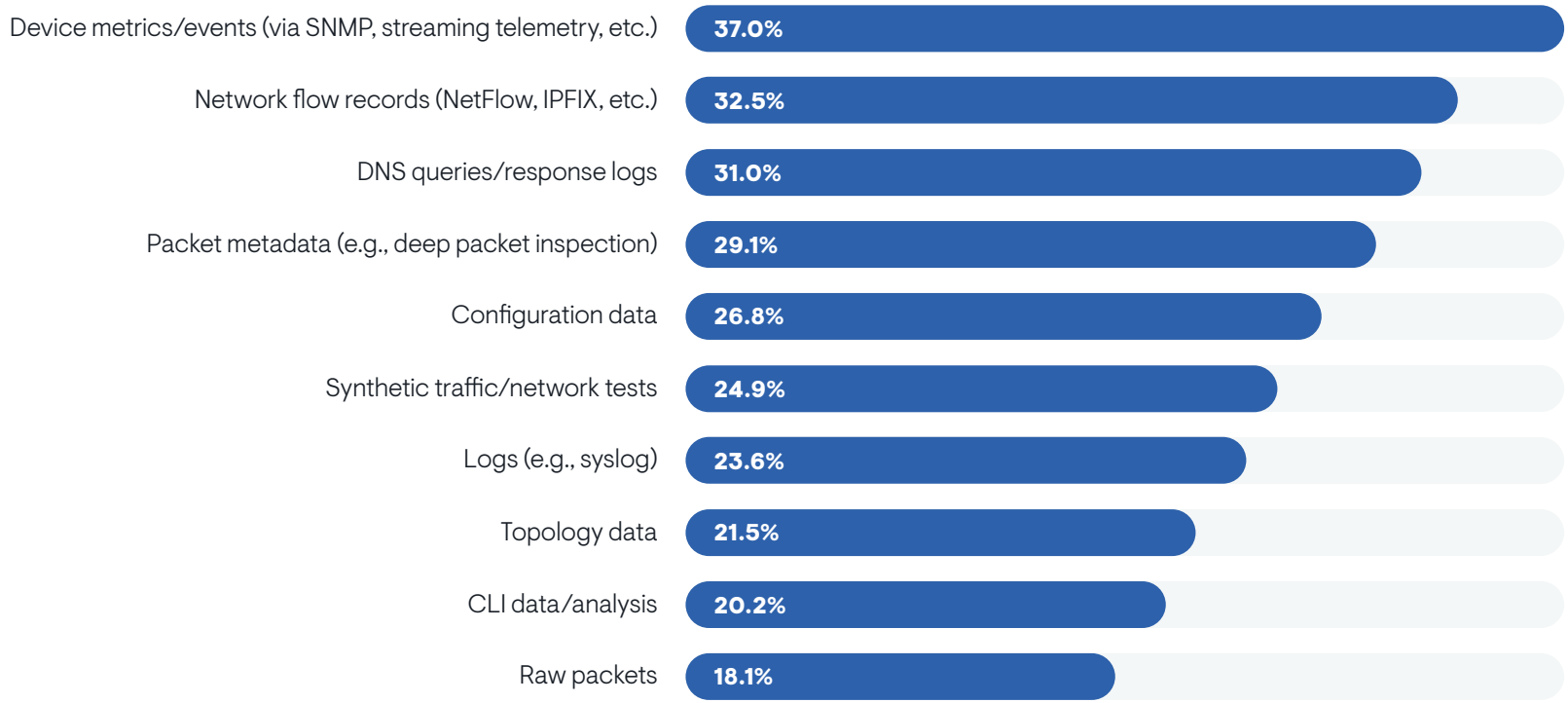
FIGURE 6. WHAT IS YOUR PREFERRED LICENSING MODEL FOR NETWORK MANAGEMENT TOOLS?



Network Data Diversity

Network operations observability tools must collect and analyze a wide variety of data. **Figure 7** reveals what data IT organizations most rely upon for monitoring and troubleshooting. Device metrics (e.g., via SNMP, streaming telemetry) and network flows (NetFlow, IPFIX, etc.) are most important. Most of the vendors in this Radar collect this data. Packet metadata (via real-time deep packet inspection) is also a high priority. Several vendors in this Radar specialize in this data collection and analysis. Configuration data and synthetic network traffic are also important, and EMA particularly focused on vendor support of synthetic traffic for its ability to reveal user experience, internet performance, and cloud application performance.

FIGURE 7. WHICH OF THE FOLLOWING DATA SOURCES DOES YOUR ORGANIZATION MOST RELY UPON FOR MONITORING AND TROUBLESHOOTING ITS NETWORK?



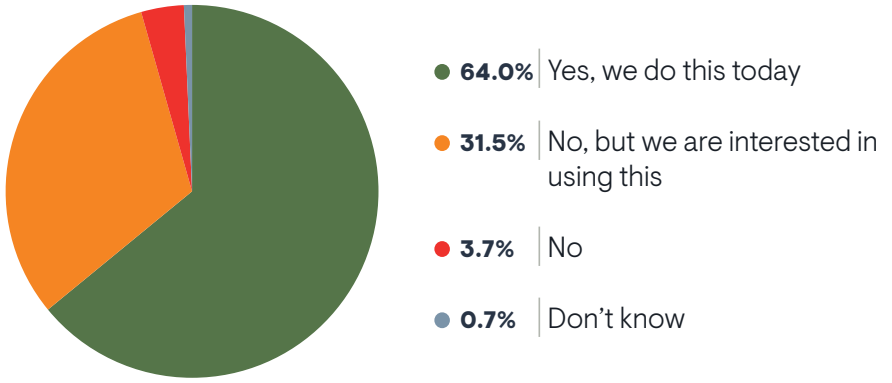
Evolving Networks

Network operations observability tools must evolve to address the changes that are occurring in enterprise networks. IT organizations are now responsible for hybrid networks that are a combination of managed and unmanaged infrastructure. Most network operations teams are still monitoring and managing data center networks, local-area networks in corporate facilities, and managed wide-area network services. Now, those networks have been hybridized with connectivity that the network team does not own or directly control, including public cloud infrastructure, internet-connected branches, and remote workers connecting from home offices. Moreover, they're adopting software-defined technologies in their data centers and across their WAN and cloud infrastructure, such as multi-cloud networking, software-defined networking (SD-WAN), and secure access service edge (SASE), all of which add abstractions and overlays that increase network management complexity.

AI-Driven Tools

Figure 8 reveals that 96% of IT organizations are using or planning to use artificial intelligence and machine learning (AI/ML) capabilities their network management and network infrastructure vendors offer. This is a differentiating factor of network operations observability solutions. AI/ML technology can deliver actionable and predictive insights and drive automation within these tools.

FIGURE 8. DOES YOUR ORGANIZATION USE ANY AI/ML-BASED FEATURES DELIVERED BY YOUR NETWORK MANAGEMENT AND NETWORK INFRASTRUCTURE VENDORS?



Research respondents identified four key network operations use cases for AI/ML-enhanced observability solutions.

1. Automated network problem remediation (37%)
2. Automated network troubleshooting (33%)
3. Anomaly detection and analysis (31%)
4. Intelligent alerting/event management (27%)

EMA considered these use cases in its evaluation of vendors.

Research Methodology

Market Relevance

Dozens of vendors offer network operations observability solutions, more than any analyst firm could reasonably hope to evaluate in a single EMA Radar Report. It is necessary to narrow the scope of such a project to only the leading vendors in the market. Thus, EMA asked each invited vendor to certify that it generated a minimum amount of annual revenue with its product and had a minimum number of paying enterprise customers. To protect the proprietary and sensitive information that vendors shared with EMA to establish their market relevance, we will not publish the criteria we used for this part of the evaluation.

Note on VIAVI Solutions: EMA evaluated VIAVI Solutions for this research, but VIAVI opted not to be included in the report.

Request for Information

EMA developed a 24-page questionnaire that collected answers on hundreds of data points that we used to score each vendor on dozens of key performance indicators (KPIs). These questionnaires collected a combination of public and proprietary information. EMA will not reveal the exact details of vendor responses due to the sensitivity of much of the information that was shared with us. All responses to our request for information had to be based on capabilities that are generally available in products as of August 2024. Vendors did not receive credit for capabilities that were in their roadmaps or planned for future releases.

Product Demos

In our request for information (RFI), we asked each vendor to identify five key differentiators of their products. After receiving completed RFIs from each vendor, EMA met individually with each vendor and asked them for a product demonstration that reviewed each of these differentiators.

Customer Interviews

EMA asked each vendor to provide a minimum of three reference customers. EMA interviewed these customers anonymously. We did not share their comments with vendors, allowing them to be fully transparent in their answers to our questions. That anonymity is maintained in this report. Wherever we quote a customer, that quote is unattributed.

Network Operations Observability Evaluation Criteria

EMA evaluated each vendor's solution along five general dimensions. The following is a high-level explanation of our evaluation criteria.

Deployment and Administration

Ease of Deployment

EMA examined time to value, in terms of how long it takes the typical customer to get a solution installed and operational. We also considered overall deployment flexibility, support offered for a proof of concept deployment, and whether customers typically require professional services during implementation.

Ease of Administration

We evaluated overall administrative overhead in terms how much effort is required to maintain a tool and update and patch it. We also examined the customer support that vendors offer and the training that is available to customers. Finally, we considered how vendors secure the integrity of their products by examining their software supply chain security practices, their cybersecurity plans, and their third-party security certifications.

Architecture and Integration

Architecture

EMA evaluated the data collection capabilities of each vendor, including their approach to collecting device metrics (via SNMP MIBs and traps, logs APIs, streaming telemetry, etc.), network flow records, and packets. We also evaluated their approach to synthetic network traffic monitoring. Each vendor was also evaluated on "hybrid infrastructure data." This term encapsulates a vendor's ability to monitor leading SD-WAN vendors out of the box and their approach to providing network observability in the public cloud (AWS, Azure, Google, and IBM). Next, EMA examined platform scalability, including the scale of each vendor's largest customer deployments and the maximum scalability of the product according to technical specifications. Finally, we examined the options vendors offer for platform resiliency. If they offered a SaaS solution, we examined what availability SLAs they offer customers.

APIs and Integrations

EMA evaluated vendors on the kinds of APIs they offer (REST vs. SOAP, etc.), the amount of product functionality that is exposed through them, and the quality of the API documentation they provide. We also evaluated how they enable integrations of their products with solutions for IT service management, network automation, and cybersecurity monitoring (SIEM, NDR, etc.).

Functionality

EMA scored each vendor on the overall ease of use of their products based on demos and customer interviews. We also evaluated vendors for their strength in each of the following areas.

Network Discovery

Primarily a function that infrastructure monitoring tools offer, this describes a tool's ability to discover physical and virtual devices connected to a given network and collect inventory and configuration data from them. Many IT organizations rely on this capability to get started with a tool and to maintain visibility into the changing state of their network as devices are added and removed.

Application Intelligence

This functionality is a tool's ability to correlate network insights with applications. There are a variety of techniques available, from ports, protocols, and URLs to deep packet inspection.

Metrics and Measurement

This feature set involves a tool's ability to report network data as metrics that users can analyze, from traffic volumes and transaction times to hop-by-hop analysis of loss, latency, and jitter along a network path.

Capacity Management

This refers to how a tool helps network teams align network capacity with changing utilization over time. We evaluated vendors for their ability to present trending reports by various metrics, such as traffic volume, application type, and physical location. We also looked at time-to-exhaustion reporting and what/if analysis features. Finally, we examined any predictive analytics and AI/ML-derived capacity recommendations that a vendor offered.

Alerts and Alarms

EMA examined the kinds of alerts a vendor supported, from static thresholds to behavior anomalies and AI/ML-driven dynamic thresholds. We also examined the extent to which a vendor helps users manage those alarms by enriching them with extra data, minimizing the amount of false and superfluous alarms they generate, and contextualizing them in other areas of the tool, such as in network maps.

Troubleshooting

EMA explored how solutions support troubleshooting workflows, such as providing side-by-side metric comparisons, multi-layer overlays of metrics for deeper comparisons, and relationship mapping. We also examined any features vendors offer around automated root-cause analysis and problem remediation.

Visualization/Reporting

EMA examined how vendors group and map metrics and data in their tools, both in reports and dashboards and geographic and topology maps. We looked at whether they could present real-time stateful topology maps with contextualized insights into the health of network infrastructure and connectivity. We examined the extent to which vendors can provide customized views of visualizations and reports based on various user requirements.

Active Controls

Each vendor was evaluated for their ability to push changes to the network, whether to modify or optimize traffic or to make automated changes to network devices. Vendors received credit for doing this via third-party integrations, but native support for active controls earned higher scores.

Cost Advantage

EMA attempted to evaluate how much each solution typically costs a customer. It is difficult to develop a singular approach to this evaluation because vendors price their products in vastly diverse ways, including by device, by metric monitored, by network flow, by bandwidth, by number of synthetic tests, by number of sites monitored, and so on. EMA based its analysis on each vendor's MSRP pricing, self-reported average deal sizes, maintenance and support fees, licensing flexibility, and customer sentiment.

Vendor Strength

EMA sought to evaluate the near-term and long-term viability of each vendor along five dimensions.

Vision

Their vision for network operations observability, including what they want to deliver to customers long-term and how they want to differentiate their solutions.

Strategy

Their concrete plan to execute on their market vision over the long term and how they want to advance their product value and capabilities.

Financial Strength

Each vendor's overall financial position and the trends they are seeing, specifically with network operations observability product revenue.

Research and Development

The percentage of their network operations observability revenue that is reinvested annually into ongoing product development and innovation.

Partnerships and Channel

Their channel strategy and their top channel partners. Also, their most important technology partners (e.g., network infrastructure vendors, cloud providers, IT service management vendors).

EMA Network Operations Observability Radar Results

Understanding the Chart

The total product value of each NOO solution is revealed in the bubble chart on this page. Product value is defined by comparing the overall Product Strength of a solution (y-axis) with its Cost-Efficiency (x-axis). Vendors that place in the upper right corner of the chart have the highest scores for both criteria.

Product Strength combines scores for Functionality, Architecture, and Integration. Functionality scores are based on the breadth and depth of product features and the usability of such capabilities. Architecture and Integration reviews the scalability, data collection capabilities, resiliency, and stability of a solution, along with the quality of the APIs and supported product integrations that the vendor offers. It is important to note that a solution with a modest Architecture and Integration score may still receive a high Product Strength rating if its Functionality score is high, and vice versa.

Cost-Efficiency is calculated by combining scores for Cost Advantage and Deployment and Administration. Cost Advantage considers overall pricing and licensing models, along with support and maintenance costs. Deployment and Administration reviews ease of deployment and ongoing administration of a tool. A high-priced vendor may still receive a strong Cost-Efficiency rating if its Deployment and Administration score is strong, and vice versa.

The size of each vendor's bubble on the chart indicates Vendor Strength. In this context, Vendor Strength does not affect overall product value. Instead, Vendor Strength adds context to buying decisions, allowing buyers to understand current state and long-term prospects of a vendor. EMA considers the financial health of a vendor, its overall market vision and product strategy, the amount of resources it devotes to product innovation, its go-to-market capabilities, and its technology partnerships with key third-party vendors.

Value Leaders are vendors with solutions that offer a balance of high Product Strength and high Cost-Efficiency. **Strong Value** vendors offer a more nuanced balance of Product Strength and Cost-Efficiency. One of the two will be very strong, while the other will be more moderate. These solutions will appeal to IT organizations that are willing to devote more internal resources and/or budget to acquire a strong product that meets or exceeds its requirements, or to organizations that want to conserve resources by acquiring a product with moderate Product Strength that can meet its essential requirements.

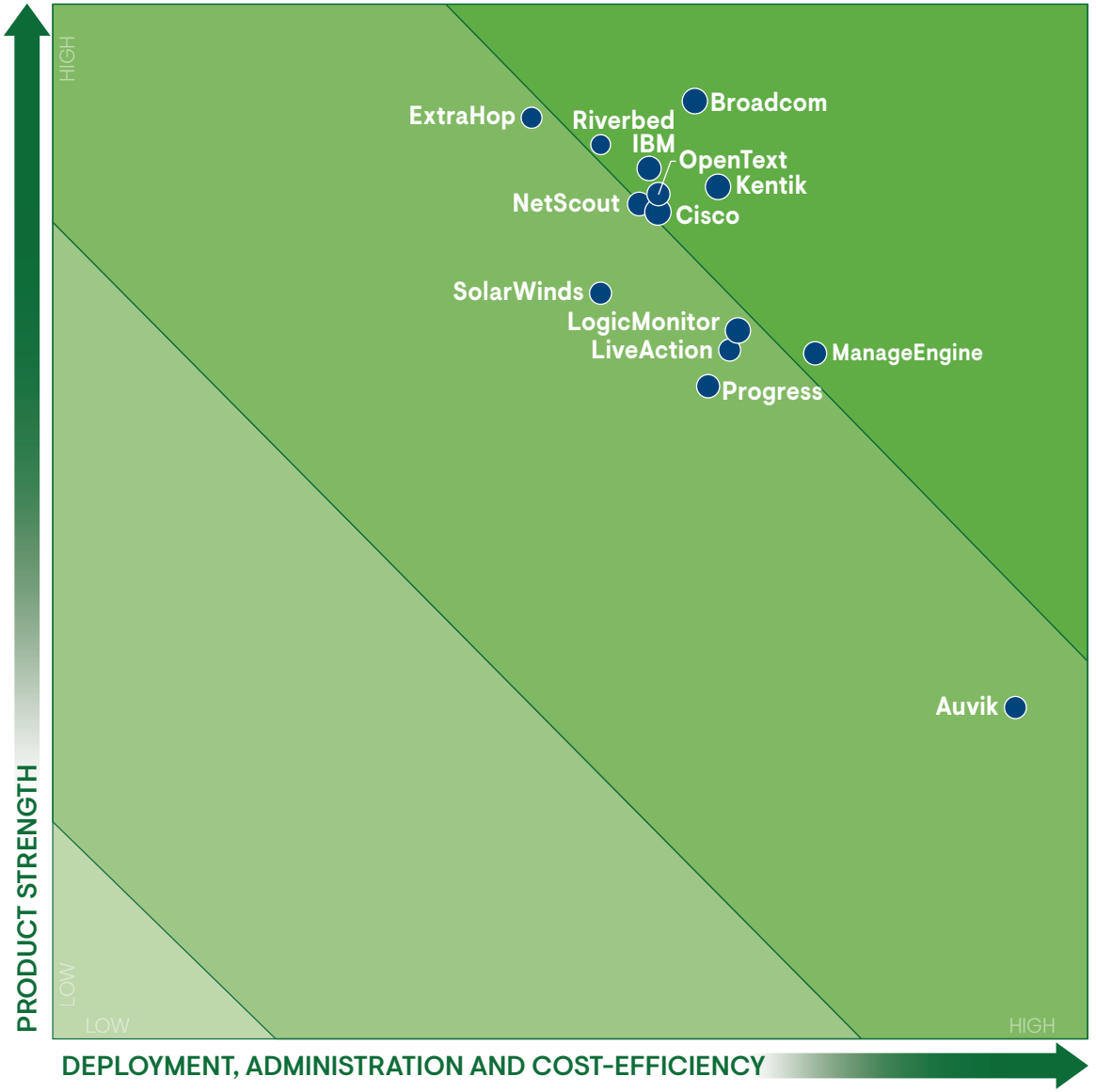
Selective Value and **Limited Value** vendors offer more niche products with medium to low Product Strength and Cost-Efficiency. This Radar Report did not include any vendors that fit into this category. EMA believes there are vendors (and some open source technologies) on the market that would fit into these latter tiers; however, those solutions did not meet the minimum revenue and customer count requirements to be included in this study.

Each individual vendor profile in this report also includes a pentagon chart, which reveals the overall score a vendor received for each category (Functionality, Architecture and Integration, Cost Advantage, Deployment and Administration, and Vendor Strength). The chart also indicates how the vendor's score on each of these criteria compares to the average score across all vendors in this Radar.

VALUE RATING

- VALUE LEADER
- STRONG VALUE
- SELECTIVE VALUE
- LIMITED VALUE

VENDOR STRENGTH



Broadcom

Multinational technology company Broadcom offers two network operations observability solutions that are often purchased together. The first solution is DX NetOps, a highly scalable and integrated suite of network infrastructure and flow monitoring products. The second solution is AppNeta, a synthetic network monitoring solution that extends the visibility of DX NetOps from traditional enterprise networks into internet performance, SaaS performance, and digital experience management. Broadcom offers a strong feature set with very powerful scalability. It also offers a formidable combination of observability for corporate networks, the internet, and the cloud.

Cisco

Cisco is a leading provider of networking, collaboration, and security solutions. It submitted two products for consideration in this Radar. First, ThousandEyes is a synthetic monitoring solution that specializes in internet observability and digital experience management for enterprises of all sizes. Customers deploy ThousandEyes agents across their networks, but Cisco also maintains a network of ThousandEyes sensors to provide a global view of cloud and internet performance. Second, Cisco offers Provider Connectivity Assurance (PCA), formerly known as Accedian Skylight. It conducts both packet monitoring and synthetic network monitoring, and it specializes in revealing network connectivity health and performance across the networks of communications service providers and very large enterprises. Cisco offers a powerful combination of observability capabilities for both corporate networks, the internet, and cloud providers.

IBM

Multinational technology company IBM offers IBM SevOne, a highly scalable solution that primarily monitors network infrastructure and network flows. Its core customers are large enterprises, communications service providers, and managed service providers. The solution has two main components. SevOne NMS is the core system that collects and analyzes data and offers users administrative access and control over the system. SevOne Data Insight is the frontend reporting and visualization platform that supports network operations workflows. IBM enhanced the solution in recent years with machine learning technology that provides actionable insights and early warnings about network problems. It is a very scalable platform with a promising set of AIOps capabilities at a competitive price.

Kentik

Kentik is a provider of SaaS-based network observability solutions. Its core technology is the Kentik Observability Platform, which monitors and analyzes network flows, BGP routing data, synthetic traffic, and device metrics. The company's cloud-based solution is highly scalable, which won it early success with communications service provider customers. The company has been expanding its focus to the enterprise market by adding new product modules, such as Kentik NMS (a traditional network infrastructure monitoring feature set). Kentik also maintains a global network of monitoring vantage points, which allows it to contextualize a customer's network with global internet and cloud performance insights. It is a highly scalable solution with many advanced features that also received high scores for ease of deployment and administration.

ManageEngine

ManageEngine is an IT software subsidiary of multinational technology company Zoho Corporation. Its network operations observability solution is OpManager, primarily a network infrastructure monitoring and management solution with an add-on module for network flow monitoring. It also offers a license-bundled OpManager Plus solution, which includes modules for full-stack observability. ManageEngine enhances OpManager with Site24x7, a SaaS-based AIOps solution that streamlines and automates workflows within OpManager. It offers a strong set of features at an affordable price.

OpenText

OpenText is an information management company that offers Network Operations Management (NOM). It supplies a strong combination of scalability and affordability. The NOM suite includes two core products. Network Node Manager (NNM) provides network infrastructure and network flow monitoring. Network Automation (NA) offers network change and configuration management. Through integration of the two tools, the NOM suite can contextualize network fault and performance issues with network configuration change insights. It is a highly scalable solution that comes at a relatively affordable price.

Riverbed

Riverbed is a performance management and acceleration company that offers the broadest suite of network operations observability products for midsized and large enterprises. AppResponse is a packet-capture appliance with real-time analytics capabilities. NetProfiler supports network flow monitoring. NetIM offers network infrastructure monitoring and management. NPM+ is a new edge performance monitoring tool that analyzes connectivity data that endpoint agents capture. Finally, Riverbed IQ is an AIOps solution that pulls data from all Riverbed solutions to correlate insights and trigger runbook automation. Riverbed's suite is the most comprehensive, with strong support for collecting and analyzing all types of network data, from SNMP MIBs and traps to packets. Its approach to end visibility with NPM+ is unique.

Auvik

Auvik, a provider of SaaS-based IT management solutions, offers Auvik Network Management for network operations observability. This solution provides network infrastructure monitoring through SNMP and syslog, network configuration discovery and monitoring, and network flow monitoring. Auvik offers a solid overall feature set for network observability and its customers tend to use the solution to manage and monitor enterprise LAN networks (switching and Wi-Fi) and WAN routing. It is a highly affordable solution that is very easy to deploy and use, making it ideal for smaller IT organizations with less complex networks.

ExtraHop

ExtraHop offers RevealX Network Performance Monitoring (NPM), which is primarily a real-time packet monitoring solution that delivers deep visibility into network health and performance, from Layer 2 to Layer 7, with line-rate packet decryption. RevealX NPM converts packets into metadata for real-time analytics, but it also offers packet capture appliances to support forensic analysis. Its sensors and packet capture appliances are deployed on-premises, but frontend user consoles and management components can deploy anywhere. It also offers a cloud-delivered AIOps module that can identify anomalies and performance problems. ExtraHop is a great option for enterprises that need deep, real-time visibility into network traffic.

LiveAction

LiveAction offers two integrated products for network operations observability for midsized and large enterprises. LiveNX is primarily a network flow monitoring solution with infrastructure monitoring capabilities. The company also offers LiveWire, a packet capture and forensics appliance. Users can pivot from performance alerts, reports, and dashboards in LiveNX directly to relevant captured packets in LiveWire to troubleshoot issues quickly. LiveAction also maintains a longstanding partnership with Cisco, allowing it to add support for Cisco infrastructure solutions rapidly while also integrating with Cisco observability products, like ThousandEyes. LiveAction offers deep and broad visibility with its ability to combine flow and packet monitoring and analysis.

LogicMonitor

LogicMonitor is a full-stack IT monitoring vendor that offers the SaaS-delivered LM Envision solution. Customers deploy local collectors on-premises and in the cloud for gathering IT data for analysis by the core SaaS solution. While positioning itself as a full-stack observability solution, many customers consider LM Envision a leading network operations observability tool that can gather network metrics, network flows, logs, and synthetic network traffic. LM Envision ships with a library of preconfigured alerts and dashboards for accelerated implementation. It also offers a growing AIOps capability, including anomaly detection for logs. It offers excellent monitoring of hybrid infrastructures of any scale with a great feature set.

NETSCOUT

NETSCOUT is a provider of network management and cybersecurity solutions for large enterprises and communications service providers. For network operations observability, it offers the NETSCOUT nGenius Enterprise Performance Management solution, which provides primarily real-time packet monitoring and synthetic network monitoring. The core components of the solution are its nGenuisOne analytics software, Infinistream NG hardware probes, vStream software probes, and the nGeniusPULSE synthetic network monitoring module. NETSCOUT emphasizes the value of the Layer 2 through Layer 7 metadata it generates from packets, which it brands as Application Service Intelligence (ASI). It's a great solution for companies that need deep visibility into network traffic and network edge visibility via synthetic traffic monitoring.

Progress

Progress is an infrastructure software company that offers two network operations observability solutions. WhatsUp Gold is a network infrastructure monitoring tool that can discover, map, and monitor network devices automatically. Flowmon is a traffic monitoring solution that uses distributed probes that convert packet streams into Layer 7-enriched flow records for traffic visibility that is deeper than a typical network flow monitoring solution. Flowmon users can also trigger packet captures when they detect network problems in order to perform on-demand forensic analysis. Progress offers a strong combination of infrastructure mentoring and traffic monitoring at a competitive price.

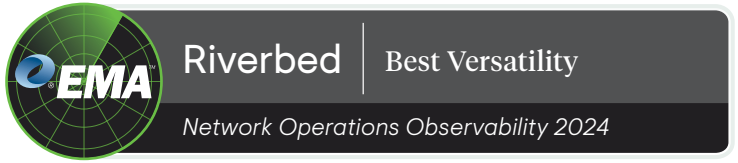
SolarWinds

SolarWinds is an IT management solutions provider that offers two overlapping solutions for midsized and large enterprises. Network Performance Monitor (NPM) primarily conducts infrastructure and flow monitoring. It is usually deployed on-premises and self-managed by the customer. The company also offers SolarWinds Observability, a SaaS-based solution that offers much of the same capabilities as NPM. Both products can be expanded into full-stack IT management solutions, sold as add-on modules for NPM and license-activated capabilities for SolarWinds Observability. SolarWinds offers a proven, scalable platform with strong features for network infrastructure monitoring.

Awards

Best Affordability – Auvik

For its combination of ease of deployment and administration and its competitive pricing, Auvik is recognized for offering the most affordable solution in this Radar. It offers a solid baseline network operations observability feature set for smaller IT organizations with limited budget and network engineering expertise.



Best Versatility – Riverbed

More than any other vendor, Riverbed offers a suite of products that cover nearly every aspect of network observability. Across its suite, Riverbed collects all classes of passive network data at scale, from device metrics to flows and packets. It also provides AI-driven capabilities with IQ and new edge visibility with NPM+. This versatility allows customers to purchase only the tools they need.

Best NetSecOps Option – ExtraHop

EMA recognized ExtraHop for its ability to support network operations and security operations teams with the same platform. It offers a powerful core solution for network operations observability that customers can easily upgrade to a network detection and response solution tool. Many ExtraHop customers today share the platform across both groups, and EMA research shows strong interest in such solutions.

BROADCOM

Customer Perspectives

"I was blown away by the fact that it's gotten not hundreds of metrics, but millions. The quality of that information has been immense,"

"I really like the integration of the three products in the DX NetOps suite. And I know they are working on making integration of AppNeta more seamless."

"Customer support is really good. We've used them for many years. I can't say anything but good things about that support team. They are stellar about going above and beyond what's needed."

Overview

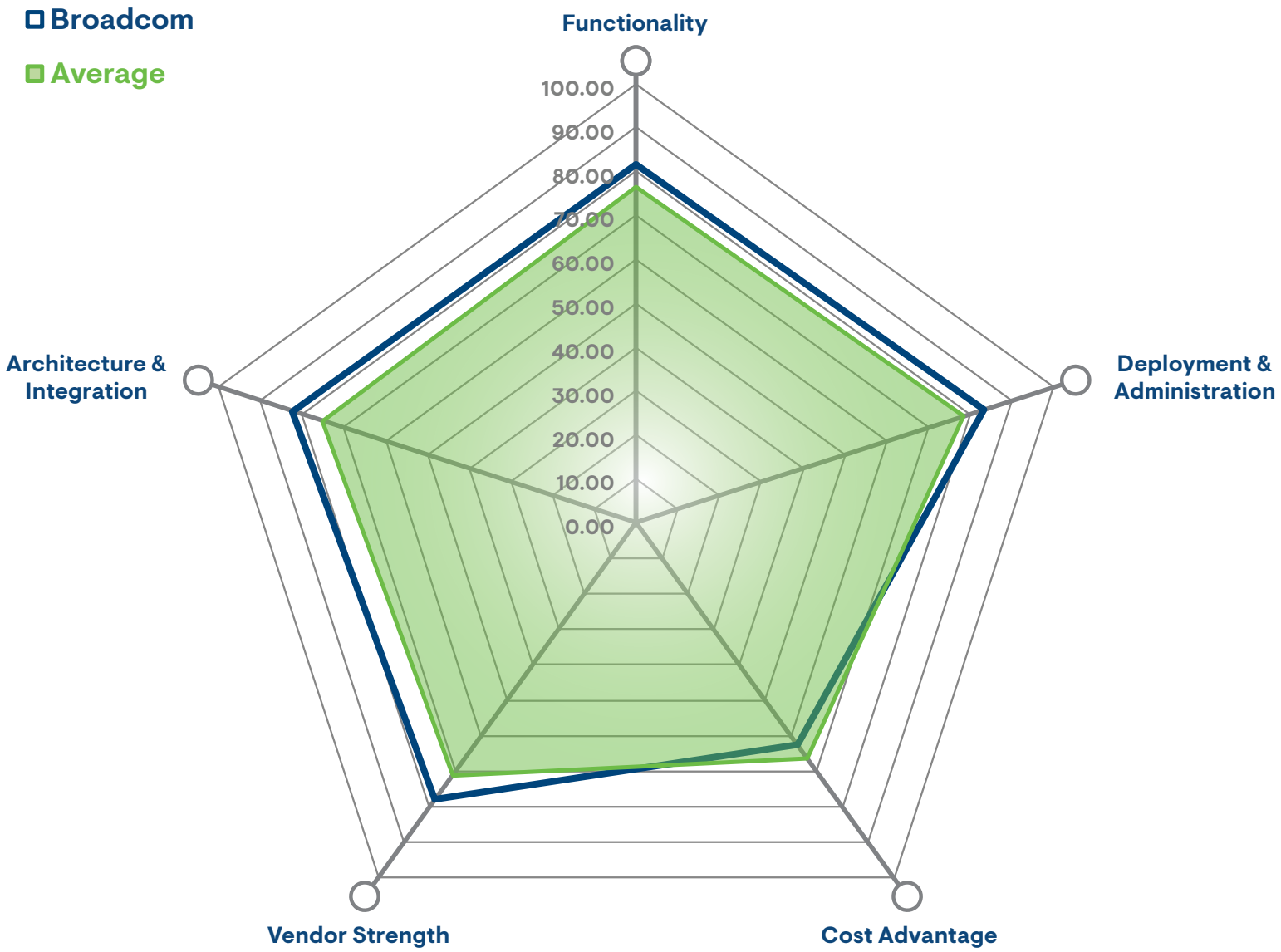
Broadcom is a multinational technology company that offers a wide portfolio of solutions, from microprocessors to software. Broadcom's network operations observability solution is branded as Network Observability by Broadcom. It includes DX NetOps and AppNeta. DX NetOps is a suite of products formerly offered by CA, which Broadcom acquired in 2018. The DX NetOps suite includes Spectrum for SNMP-based fault management, Network Flow Analyzer for flow monitoring, Performance Management for network performance reporting and analysis, and Virtual Network Assurance for monitoring of software-defined technology, like SD-WAN solutions. Broadcom rarely markets these as separate products, instead emphasizing the power of the full DX NetOps suite. Customers will find the Performance Management component of the suite as a primary interface for users of all skill levels.

AppNeta is primarily a synthetic network monitoring solution that also offers passive real-time packet monitoring. Customers typically use it to gain visibility into digital experience and application performance. It was developed by the eponymous company AppNeta, which Broadcom acquired in 2021. Broadcom offers some limited integration between DX NetOps and AppNeta, but EMA expects this integration to expand over time.

With the combination of DX NetOps and AppNeta, Broadcom aims to provide end-to-end observability across any type of connectivity based on any vendor technology. DX NetOps provides deep visibility into managed networks while AppNeta delivers insights into the growing share of enterprise networks that are unmanaged (remote user edge, cloud applications, and internet connectivity).

Broadcom emphasized the following differentiators when interacting with EMA:

1. End-to-end network experience insights across applications, infrastructure, managed and unmanaged networks, and user experience
2. Highly scalable network operations monitoring
3. Single-click from alarm to diagnostics, with single-pane contextual triage workflows across different classes of data and disparate networks
4. Active (synthetic) monitoring and troubleshooting of network delivery across site-to-site, site-to-cloud, and cloud-to-cloud connectivity from all applications and services
5. Algorithmic and patented enhancement of key network operations processes, including alert noise reduction, root-cause analysis, fault isolation, and event correlation


Broadcom
Average
Functionality
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
Deployment & Administration
Cost Advantage
Vendor Strength
Architecture & Integration

Scoring

Deployment & Cost-Efficiency

Deployment & Administration	
Implementation	Strong
Deployment Flexibility	Outstanding
Proof of Concept Support	Strong
Professional Services Requirements	Strong
Customer Support	Outstanding
Customer Training	Outstanding
Administrative Overhead	Strong
Product Update Impact	Strong
Administrative Security	Strong

Deployment & Administration

Overall, deploying the Broadcom solutions is not particularly difficult, although customers reported some variation from component to component within the DX NetOps suite. Also, customers with plans for extensive probe deployments with AppNeta will experience some heavier lifting.

The company has robust customer support and professional services available, and customers noted the quality of customer support improved in recent years after a dip during the transition period that followed Broadcom's acquisition of CA. The products are strong in terms of ease of ongoing administration and maintenance. However, customers reported some variation among products within the DX NetOps suite. Broadcom demonstrated a strong commitment to securing its product from malicious activity.

Cost Advantage	
On a scale of 1 to 100 with 100 being most affordable, Broadcom received a score of	63

Cost Advantage

Overall, Broadcom is a moderately priced solution, but there are nuances between DX NetOps and AppNeta. AppNeta, like many synthetic network monitoring tools, tends to be a premium offering.

Product Strength

Architecture & Integration	
Passive Data Collection	Strong
Synthetic Data	Outstanding
Hybrid Operations Monitoring and Data	Outstanding
Platform Scalability	Strong
Resiliency	Outstanding
APIs	Strong
Product Integrations	Strong

Functionality	
Network Discovery	Outstanding
Application Intelligence	Outstanding
Metrics and Measurement	Outstanding
Capacity Management	Solid
Alerting/Alarming	Outstanding
Troubleshooting	Strong
Visualization/Reporting	Strong
Active Controls	Limited
Ease of Use	Solid

Architecture & Integration

Broadcom offers a robust and scalable platform for passive monitoring of networks through device metrics, logs, and network flows. Its ability to monitor packet data is a complementary capability, but not strong compared to packet specialists. AppNeta's synthetic monitoring capabilities make it a powerful solution for managing hybrid infrastructure, like public clouds, SaaS applications, internet connectivity, and remote user experience.

Broadcom offers strong APIs that are well-documented for users who want to customize the solutions or integrate them with other systems.

Functionality

Broadcom offers a massive amount of metrics and measurements for users to explore and analyze. It also has a powerful network discovery engine. AppNeta assures that it has powerful application intelligence for teams who prefer to take an application-centric approach to network operations. Its alert management capabilities are also very powerful, but they can require some fine-tuning. Customers gave Broadcom a solid rating overall for ease of use across the platforms.

Vendor Strength

Vision	Strong
Strategy	Strong
Financial Strength	Strong
Research & Development	Strong
Partnerships and Channel	Strong

Broadcom is a massive, profitable company with a robust sales channel and strong partnerships with other technology companies. EMA sees evidence of significant investment in innovation. Overall, it has a good vision of the network observability industry and has a strong strategy on how to execute.

Strengths

- AppNeta's synthetic network monitoring provides powerful visibility into hybrid infrastructure, especially SaaS application performance, hybrid WAN (internet) performance, and remote user experience.
- A well-rounded solution that offers a wealth of information about a network with many options for how to visualize and report on that data.
- Excellent customer support, not only in terms of breadth and depth but quality, too. While some industry pundits have claimed that customer support and product innovation suffer when Broadcom acquires a company, customers told EMA that Broadcom's commitment to customer support and customer success with its network observability solutions is excellent.

Opportunities

- Three years after its acquisition, integration between DX NetOps and AppNeta is limited. They are essentially separate products today. There is a significant opportunity to increase the power of the two platforms through deeper integration of data analysis and workflows.
- While overall integration of the various products in DX NetOps is strong, there are some aspects of the individual tools that remain siloed. For instance, some of the individual tools maintain separate inventories of network infrastructure. While working in the suite, customers often have to double check that the individual tools have a complete record of infrastructure covered within the scope of a workflow.
- Broadcom offers limited active network controls in its suite. Customers can configure the solution to automatically launch a script to take correction action in response to alerts and other conditions, but it lacks the ability to take more advanced corrective actions.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**