EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

EMA Radar Report: Network Performance Management

August 2021

By Shamus McGillicuddy, Vice President of Research

EMA RADAR™

Table of Contents

Executive Summary

This Radar Report is aimed at assisting IT organizations that are procuring network performance management solutions for operational monitoring, troubleshooting, and capacity planning. This report should help buyers assemble a shortlist of vendors and guide their selection of a solution. Any of the 15 vendors represented in the report might be the best choice for an organization depending on the tools and solutions they currently have, their level of organizational maturity, their budget, their direction and vision, and their current mix of network technologies.

The Evolving Idea of Network Performance Management

Network performance management (NPM) is a class of technologies that supports multiple enterprise network engineering and operations use cases by collecting and analyzing a range of network data, including infrastructure metrics, network flows, packets and packet metadata, logs, synthetic traffic, and network test data.

These solutions typically offer defined workflows, dashboards, reports, alerts, and network maps and visualizations that support critical network management use cases. Primarily, IT organizations use NPM solutions to support three critical functions:

1. Operational monitoring of network infrastructure and network traffic
2. Network diagnostics and troubleshooting
3. Capacity planning

The NPM market has more or less existed for nearly three decades, and several of the products in this Radar can trace their roots back that far in time. Many other solutions are relatively new, only emerging into the market over the last decade.

The NPM market is a complex space. There are multiple techniques and approaches to measuring the performance of a network. For instance, some network teams may rely heavily on infrastructure monitoring, using tools that collect metrics from infrastructure via SNMP MIBs and traps, APIs, and other mechanisms. Other teams may rely heavily on traffic monitoring tools that collect a mix of network flow records and packet data to analyze network performance. Some vendors are strongest in infrastructure monitoring, while others are strongest in traffic monitoring. In many IT organizations, the network team will use a combination of tools to manage network performance, which is one reason why EMA's research has consistently found that a typical IT organization uses between four and ten tools to monitor and troubleshoot its network.

For that reason, a reader will discover that many of the 15 vendors in this report are complementary, rather than competitive, with each other. Some customers even told EMA that they consider solutions with duplicative functionality to be complementary based on the strengths of each individual tool. It is likely that an IT organization will determine that it needs more than one of the solutions in this Radar Report.

The NPM market is constantly evolving in response to new trends and technologies in the IT industry. EMA's ongoing network management research has identified several trends that are influencing the development of the NPM market today. All of these trends have influenced how EMA conducted its research for this Radar.

The Cloud

IT organizations have migrated (and continue to migrate) applications and data to the public cloud in pursuit of greater flexibility, improved reliability, enhanced scalability, and optimized cost control. This migration has hybridized networks. According to EMA research, 40.4% of all traffic on the average enterprise network originated from cloud applications.[1] To support these new cloud architectures, network operations teams need NPM tools that offer visibility into the cloud so they can manage a multi-cloud network. Unfortunately, many IT organizations are struggling. As **Figure 1** reveals, 61% of network teams believe their network management tools are not fully capable of supporting the public cloud. Additionally, 57% of network teams have acquired specialized tools to close gaps in cloud networking visibility.[2]

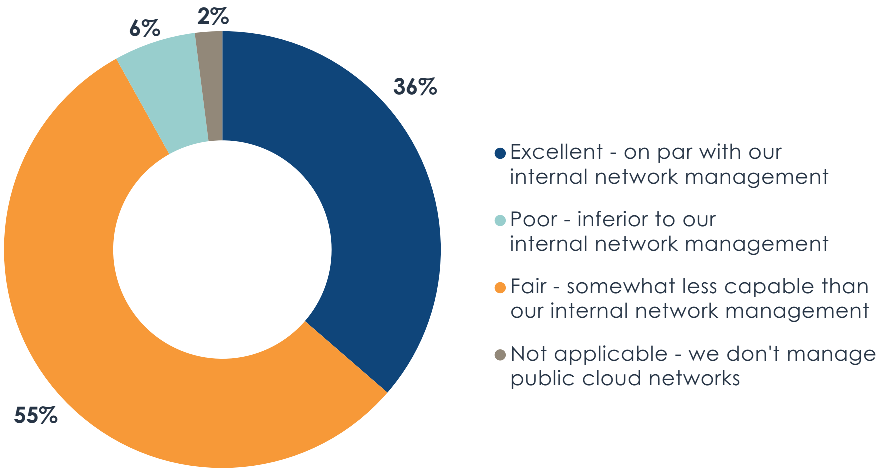


Figure 1. How effective are your network management tools and methods at supporting public cloud networks?

EMA believes that NPM solutions should provide some coverage of cloud monitoring by some combination of the following:

1. Collect metrics from virtual network elements deployed in the cloud
2. Collect flow logs and other telemetry offered by cloud providers
3. Collect network traffic data in the cloud, such as packet flows
4. Analyze synthetic traffic directed at SaaS services

Solution Flexibility

Twenty years ago, the majority of NPM solutions were purchased via a perpetual license and installed on-premises, sometimes on a dedicated appliance. Today, IT organizations want flexibility in how they license and deploy an NPM solution. Perpetual licenses and on-premises installations are still relevant, but many companies want subscription or pay-as-you go licenses that are based on a variety of license measurements. They also want solutions that are SaaS-delivered or hosted and managed by a vendor. Vendors that can offer flexibility around deployment and licensing can serve a larger portion of the market.

[1] EMA, “Network Management Megatrends 2020,” April 2020.
[2] ibid.

New Data Requirements

SNMP MIBs and traps, network flows, and packets remain core sources of data for NPM solutions. However, EMA research found that network managers are interested in analyzing new classes of data.

First, streaming telemetry shows great promise. It offers a more granular and scalable approach to extracting metrics from network devices. Tools can subscribe to telemetry streams, rather than relying on SNMP polling. Streaming telemetry reduces reliance on SNMP, which many network managers believe is inefficient and insecure. Many vendors are waiting for industry standards to develop around streaming telemetry, but 71% of network infrastructure and operations teams say they are interested in this capability today. The majority of them (69%) perceive streaming telemetry as a complement to metrics collected via SNMP, rather than a replacement for SNMP.[3]

Figure 2 reveals what is driving interest in streaming telemetry. Enterprises see it as a more efficient method of collecting data from the network. It is also more secure and reliable than SNMP. Some also see the potential in the extensibility of the technology.

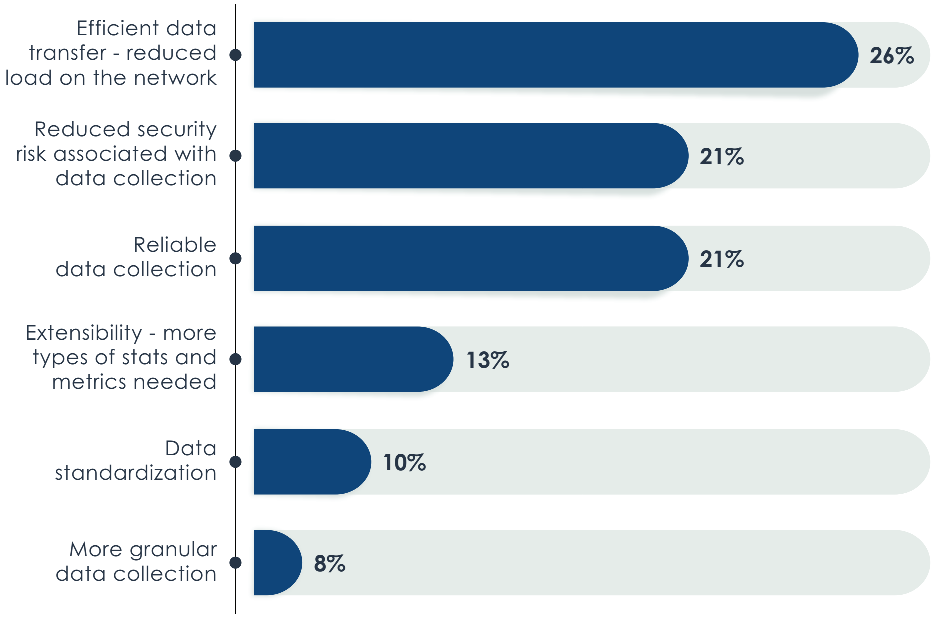


Figure 2. Primary drivers of interest in streaming network telemetry

Active monitoring isn't new, but its relevance has grown. On-premises networks are easy to monitor with passive monitoring data, such as flows and packets. However, the internet and the cloud are forcing enterprises to use active monitoring techniques, from basic ping tests to Layer 7 synthetic monitoring. According to EMA research, at least 21% of network teams use synthetic traffic tools for sustained network availability and performance monitoring.[4]

[3] EMA, "Network Management Megatrends 2020," April 2020.

[4] ibid.

WAN Transformation

Wide-area networks are changing rapidly, with companies adopting software-defined WAN (SD-WAN) solutions to enable hybrid WANs that supplement traditional managed WAN services, like MPLS with broadband internet. These hybrid WANs offer more bandwidth, direct cloud access, and network agility. While SD-WAN solutions typically offer native performance monitoring capabilities, the majority of IT organizations find this visibility insufficient.

Figure 3 reveals that 93% of SD-WAN adopters are monitoring their SD-WAN implementations with a third-party NPM tool, and 41% say this third-party visibility is critical to network operations.[5]

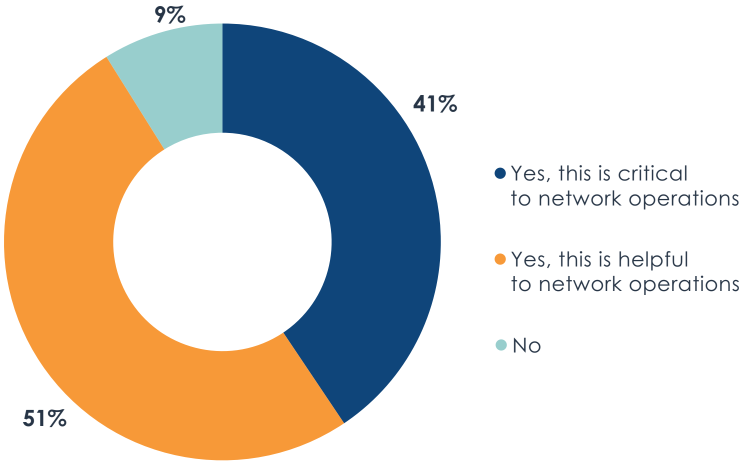


Figure 3. Do you use any third-party network performance management tools to monitor and manage your SD-WAN solution?

NPM solutions must provide visibility into SD-WAN solutions and the hybrid networks they enable. Collecting telemetry from these SD-WAN solutions is not always straightforward, and EMA research has found that the majority of enterprises are not completely satisfied with the SD-WAN visibility provided by their NPM vendors.

AIOps

Artificial intelligence for IT operations (AIOps) is an emerging set of technologies that combine AI and machine learning algorithms, big data, and other advanced analytics technologies to enhance and automate IT management. AIOps solutions can detect patterns in network data, draw conclusions from those patterns, and communicate those conclusions to network managers. Early use cases for AIOps include anomaly detection, intelligent alerting and escalations, automated root-cause analysis, and guided or automated problem remediation.

Network infrastructure and operations teams have strong interest in adopting AIOps solutions for network management. In fact, 90% of network managers believe that AIOps-driven network management can lead to better outcomes for their overall business.[6] Furthermore, **Figure 4** reveals that nearly 96% of network managers believe that AIOps capabilities are a product differentiator when they evaluate network management solutions, such as an NPM product. The majority of NPM vendors are now developing AIOps capabilities.

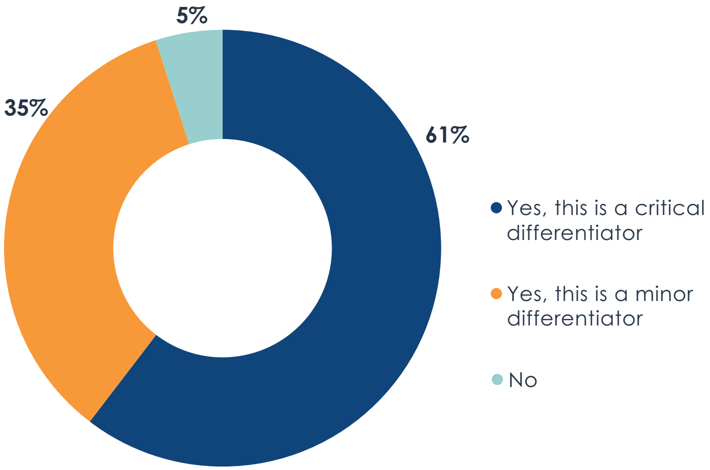


Figure 4. When evaluating network management solutions, do you consider AIOps capabilities a product differentiator?

[5] EMA, "Enterprise WAN Transformation: SD-WAN, SASE, and the Pandemic," December 2020.
[6] EMA, "Revolutionizing Network Management with AIOps," April 2021.

SecOps Collaboration

Eighty-nine percent of network infrastructure and operations teams have increased the amount of collaboration they conduct with their counterparts in information security or cybersecurity.[7] This collaboration runs the gamut from network design to coordinated incident response. Increasingly, network managers are looking for NPM solutions that can support this collaboration. Network managers often provide reports from NPM solutions to security teams, or even provide the security teams with direct access into the NPM solutions.

Figure 5 reveals which network management tools are most useful for supporting this collaboration. Many of the most important tools are typically components of an NPM solution, including network infrastructure monitoring, network flow monitoring, network visualization/mapping, packet metadata monitoring, and active synthetic monitoring. NPM tools aren't necessarily meant to be frontline security analytics solutions, but they should support collaboration by enabling network operations professionals to share data and insights about network behavior and answer questions that the security team might have about an event.

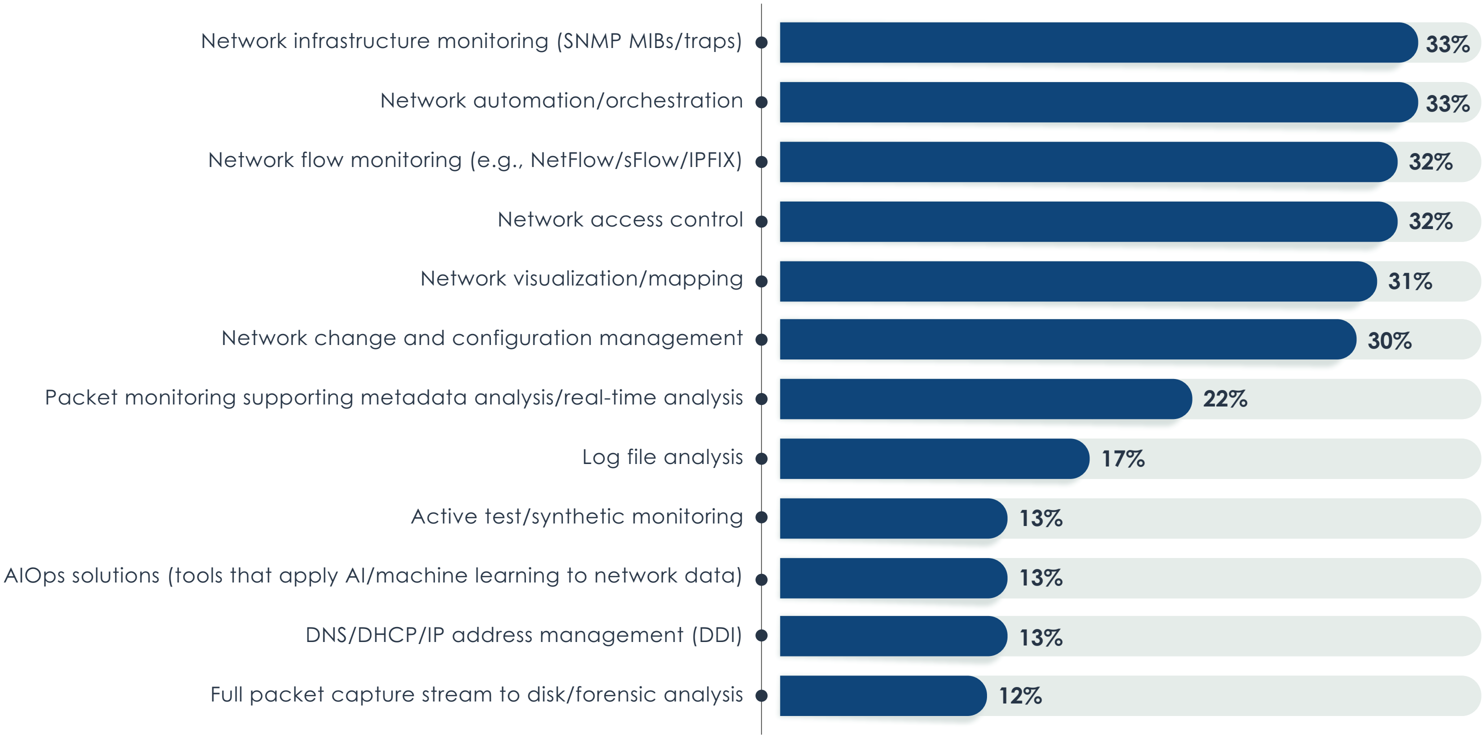


Figure 5. Network management solutions most helpful for enabling and supporting the network team's collaboration with the security team

[7] EMA, "Network Management Megatrends 2020," April 2020.

Work-From-Anywhere

The COVID-19 pandemic has fundamentally changed the nature of work. Millions of people have worked from home during the global health crisis, and many of them will not be returning to the office. EMA research found that 85% of enterprises have experienced a permanent increase in the number of employees who work from home at least some of the time.[8]

EMA research also found that network operations teams are struggling to support the user experience of people working from home. Here's one fundamental question that many of them cannot answer easily: Is the user's problem related to their local Wi-Fi or their internet provider? As a result, they need to upgrade their tools or acquire new tools. **Figure 6** reveals that 95.5% of network operations teams have allocated budget to improve the ability of their monitoring tools to support the user experience of people who work from home. The NPM market has a role to play here. Some enterprises have considered turning on NetFlow generation on their VPN clients. Others are installing active monitoring agents in homes. Quite a few are installing network hardware in home offices, which will provide NPM tools a variety of ways to collect metrics and telemetry from these locations.

All of these trends are influencing developments in the NPM industry. EMA considered these trends when developing the research methodology and evaluation criteria that underpin this Radar Report.

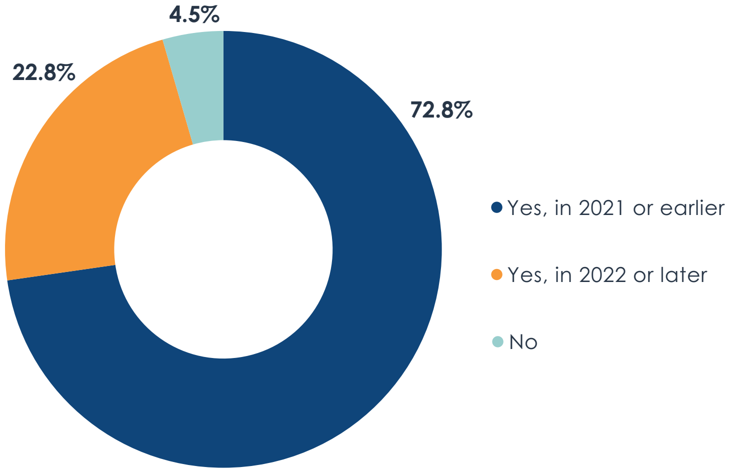


Figure 6. Has your IT organization allocated budget for improving the ability of its network monitoring and troubleshooting tools to support the user experience of users who work from home?

[8] EMA, "Post-Pandemic Networking: Enabling the Work-From-Anywhere Enterprise," July 2021.

Research Methodology

Research and evaluation for this report took place beginning in February 2021. Each solution in this report was evaluated based on what it offered in February 2021. Please note that many of the vendors in this report have enhanced their solutions since that time, and those enhances are not reflected in EMA's evaluation.

EMA acknowledges that it is nearly impossible to do an apples-to-apples comparison between vendors in the NPM market. It is very rare that a single solution will meet all the NPM requirements of an IT organization. EMA interviewed dozens of NPM customers for this Radar, and we found that many of them use more than one of the vendors evaluated in this report. In some instances, IT organizations used two products that one might consider direct competitors with feature parity in multiple dimensions.

Given these dynamics, this Radar is not intended as a vendor-to-vendor comparisons. Instead, it evaluates each vendor on multiple key performance indicators that are grouped into five basic dimensions:

- Functionality
- Architecture and Integration
- Deployment and Administration
- Cost Advantage (price and licensing models)
- Vendor Strength

Based on these dimensions, an NPM buyer might select a solution that only rates as "average" in overall functionality, but its price and cost of ownership might be significantly lower. On the other hand, a buyer with a premium set of requirements for product architecture and overall functionality will budget for the high price that such a platform commands. It's up to the buyer to balance requirements with available resources. The purpose of this Radar is to help buyers create a shortlist of appropriate vendors when preparing a RFP process for an NPM solution.

Evaluation Criteria

EMA used dozens of key performance indicators (KPIs) to measure and evaluate each NPM solution. Those KPIs were organized into five dimensions of Evaluation Criteria, as follows.

Cost Advantage

Price: EMA asked vendors to provide price quotes with typical discounts for initial installation and annual recurring costs with the highest level of customer support for medium and large network deployment scenarios. In the individual vendor profiles, prices are represented by a scale of one to four dollar signs, with "$" representing least expensive and "$$$$" representing most expensive.

Licensing Model: EMA reviewed the flexibility of licensing models for each NPM solution, such as metrics used for license costs and the license terms offered.

Deployment and Administration

Ease of Deployment: EMA examined the complexity of installing and configuring NPM solutions and the time it takes to get a solution fully operational. We also looked at deployment flexibility and the breadth of training for customers who need to learn how to implement and use the product. EMA's ratings in this area reflected that some enterprises have scalability and flexibility requirements that drive up complexity.

Ease of Administration: EMA evaluated how easy an NPM solution is to maintain once the product is up and running, in terms of the amount of resources required to manage it and administrative automation features that simplify management of the product. EMA also evaluated how product updates impact overall availability and stability, and we investigated the administrative security that vendors offer for their platforms.

Support and Services: EMA considered the breadth and quality of customer support offerings, as well as product release cycles. We also examined whether solutions require professional services to implement the product.

Architecture and Integration

Platform Design: EMA evaluated the core platform of solutions by reviewing their scalability, performance, stability, and extensibility. EMA also examined the data collection and data retention capabilities of solutions.

Integration/Interoperability: EMA evaluated the ability of NPM solutions to integrate with other systems. We examined the open APIs that vendors offer and the out-of-the-box integrations vendors ship with their products, particularly around IT service management, security monitoring, and network configuration management. EMA research found that many customers value open APIs more than out-of-the-box integrations. The evaluation model reflected this preference.

Functionality

Core Features: EMA examined the core features and workflows of NPM solutions, including application recognition and monitoring, network metrics measurement and presentation, capacity planning, alerts and alarms configuration and management, network troubleshooting, and visualization and reporting. EMA's model also considered complementary core features—network discovery and active network controls.

Network Analytics and AIOps: EMA evaluated the core analytics features of solutions and any so-called AIOps capabilities that NPM solutions offer. We examined whether vendors could provide basic features, such as thresholding and threshold deviations, but also whether they can support use cases associated with AIOps, such as anomaly detection, root-cause analysis, and predictive capacity analysis.

Cloud Management: EMA examined each NPM platform's ability to monitor and manage the external cloud, including SaaS applications, IaaS and PaaS environments, and virtual network elements that are deployed in the public cloud.

Security Support: EMA recognizes that enterprises are starting to use NPM solutions to support collaboration between NetOps and SecOps teams. EMA examined whether NPM solutions are directly supporting this effort by offering security insights or workflows that might facilitate collaboration.

Ease of Use: EMA considered the overall usability of products. Some NPM solutions can be daunting for people who lack advanced networking skills. EMA examined whether products offer functionality and workflows that can be used by a wide range of personas in an organization. We also evaluated the customizability of reports that NPM solutions generated, which network managers often share with other groups within IT.

Vendor Strength

Financial Strength: The financial health of a vendor is important for determining the long-term viability of a solution. While public companies provide a great degree of financial transparency, not all the vendors considered for this Radar are public companies. EMA used whatever data and insight it could find to make a determination in this area.

Vision and Strategy: EMA asked each vendor to share its vision of the NPM industry and the strategy it has established to execute that vision. We evaluated these responses based on the technology trends and tool requirements EMA identified in its ongoing research into the network infrastructure and operations industry.

Research and Development: Where available, EMA examined how much NPM-related revenue each vendor reinvests into the ongoing development of their products.

Partnerships and Channel: EMA examines the sales channels of each NPM vendor and the technology partnerships and alliances they have. A strong sales channel can lead to better outcomes for customers who rely on channel partners to implement and support NPM solutions. Technology partnerships can ensure that NPM vendors are able to monitor and manage next-generation technologies as leading networking vendors introduce them to the market.

Inclusion Requirements for Market Relevance

EMA considered approximately 30 vendors for this Radar Report. Vendors had to demonstrate market relevance by meeting minimum revenue and customer count requirements. EMA asked vendors to base this on 2019 statistics, rather than 2020, given the unusual market conditions created by the COVID-19 pandemic in 2020.

Incumbent vendor minimum:

- $40 million GAAP NPM product revenue in 2019
- 75 customers actively using the NPM product on a production network

Emerging vendor minimum:

- $15 million GAAP NPM product revenue in 2019, with a 25% growth rate from 2018 to 2019
- 30 customers actively using the NPM product on a production network, with 25% growth rate in customer count between 2018 and 2019

Several vendors failed to meet these minimum requirements. Several others declined to participate. Network performance and security monitoring vendor Plixer initially agreed to participate, but later withdrew, saying that it didn't believe it necessarily competed in the exact market defined by this Radar Report. A reader should not assume that a vendor's absence from this Radar Report indicates that they lack market relevance or that their solution isn't competitive.

Evaluation Methodology

- **Survey:** Each vendor completed a detailed questionnaire about their NPM solutions and their NPM strategies. All responses to the survey had to be based on what was generally available in a vendor's NPM solution before February 28, 2021, when the Radar evaluation began.
- **Product demonstrations:** EMA analysts conducted in-depth briefings and received product demonstrations from each vendor.
- **Reference customers:** EMA interviewed several customers provided by each vendor to get their confidential opinions about doing business with these NPM vendors and deploying, administering, and using their products in their experiences.

EMA Network Performance Management Radar Results

Understanding the Chart

The total product value of each NPM solution is revealed in the bubble chart on this page. Product value is defined by comparing the overall Product Strength of each NPM solution (y-axis) with its Cost-Efficiency (x-axis). Product Strength combines evaluation scores for Functionality and Architecture and Integration. 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.

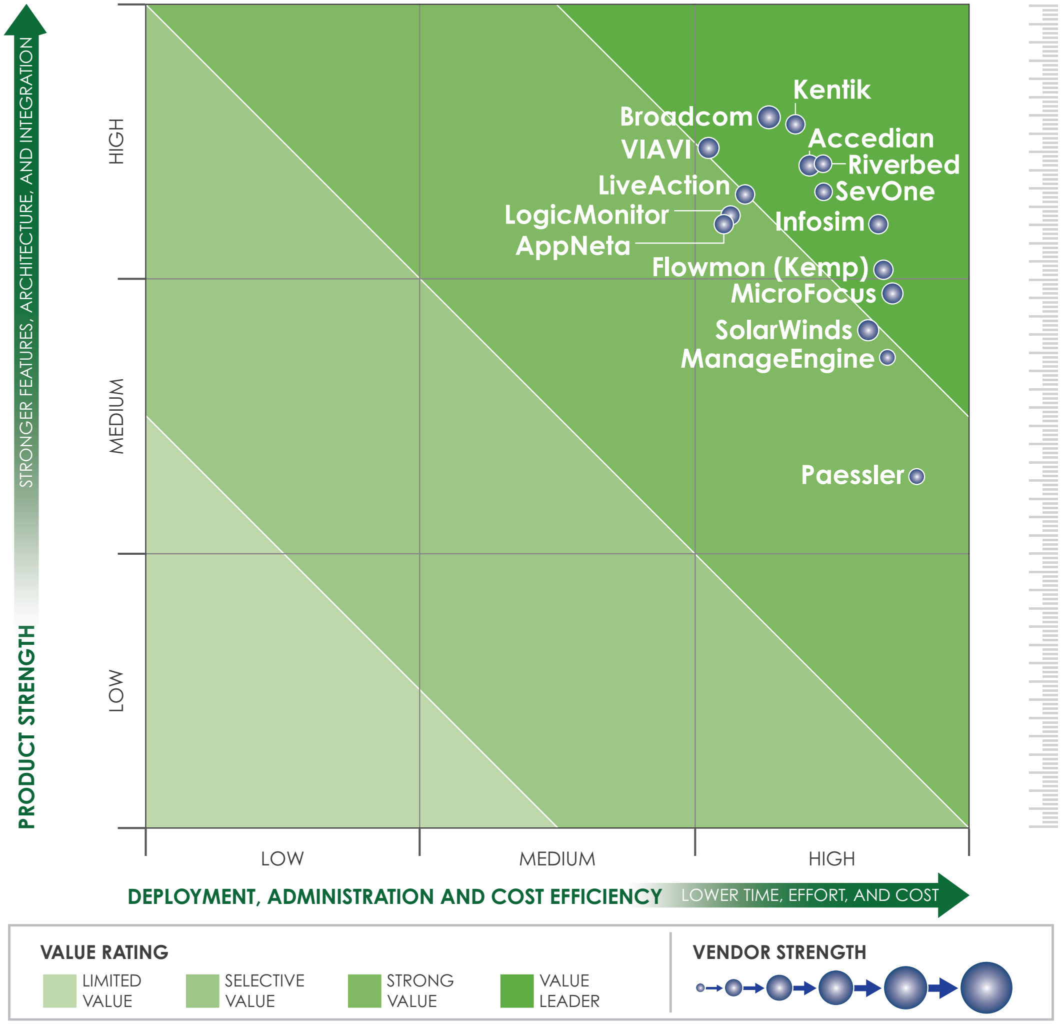
Cost-Efficiency is calculated by combining scores for Cost Advantage and Deployment and Administration. A high-priced vendor may still receive a strong Cost-Efficiency rating if its Deployment and Administration score is strong, and vice versa.

The size of each vendor's bubble 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 which vendors have a stronger balance of financial strength, vision, strategy, research and development resources, and partnerships.

Value Leaders are vendors whose solutions 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.

EMA RADAR REPORT FOR NETWORK PERFORMANCE MANAGEMENT



2021 VALUE LEADER EMA

INFOSIM
Network Performance Management

Customer Perspectives

"I like the XML discovery feature that makes it easier to maintain and automate everything."

"The product is easy to keep up to date and it is stable."

"Their customer support in Germany is very good. They are very willing to help and support their customers."

"It's a state-of-the-art tool with state-of-the-art APIs."

infosim

Overview

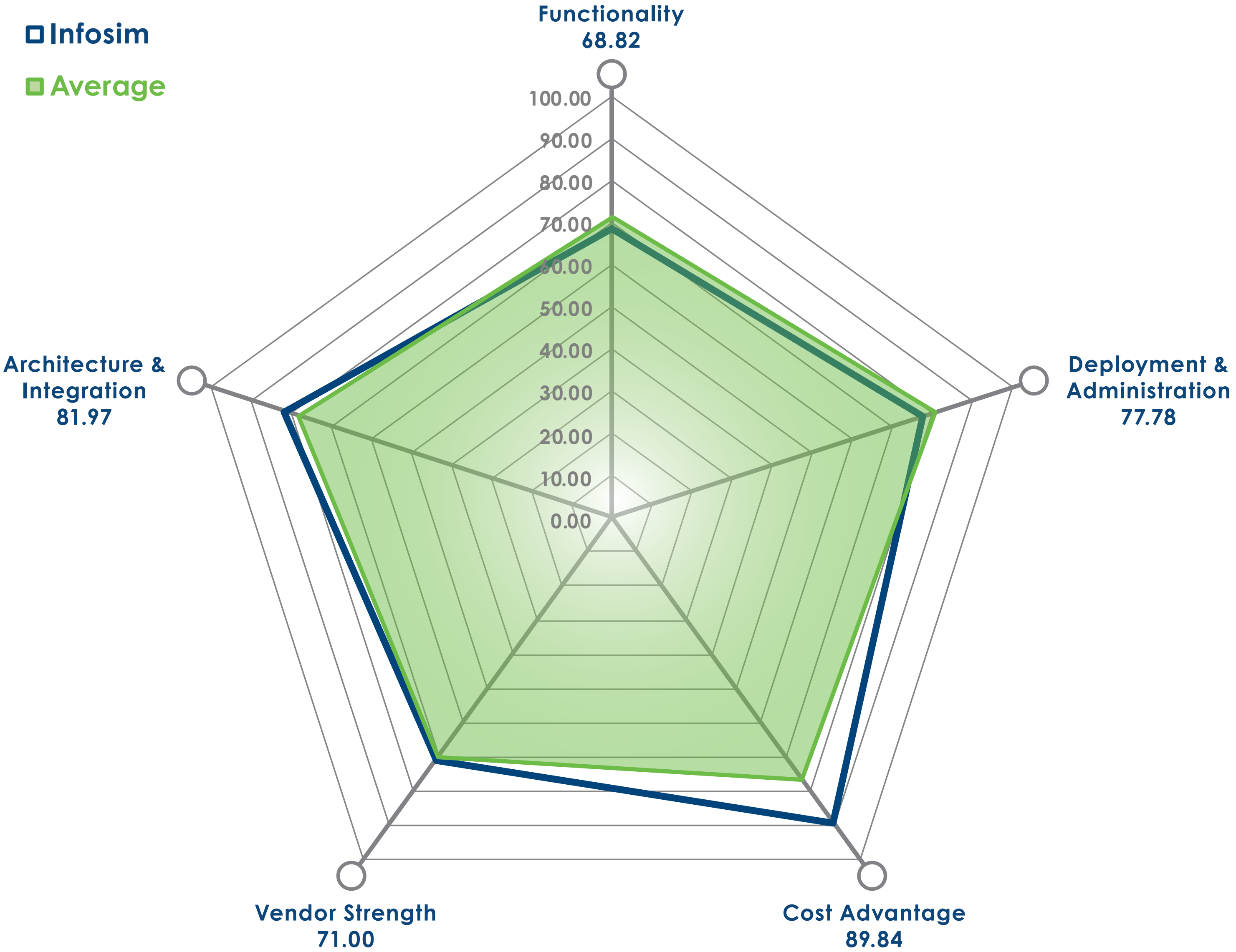
Based in Wuerzburg, Germany, Infosim is a privately held NPM vendor that began life as a research project at the University of Wuerzburg. Infosim was spun out of the university in 2003 and remains a privately owned company today. Its core product, StableNet® Automated Network and Service Management, serves the network monitoring needs of mid-tier to very large enterprises, as well as communications service providers.

StableNet® is a broad network management solution that addresses a variety of use cases rather than specialize in network performance management. StableNet®offers a wide array of automation capabilities for fault, performance, resource management, and service management in a single platform and with a single codebase. The solution also provides a native network change and configuration management capability in the core platform. Infosim promotes its NPM solution as a highly scalable and customizable platform that can monitor access, edge, and core networks, as well as IT infrastructure, IoT, and the cloud.

Infosim promotes its "tagging" concept as a key differentiator. Network managers can tag different objects and elements in StableNet's® inventory tree hierarchy and use this concept to create preset and ad hoc views of the networks along multiple dimensions. The solution also offers a built-in root cause analysis algorithm, a capability that automatically scans for dependencies based on the connectivity graph. Correlational data is used to classify subtending alarms and pinpoint the source of the originating fault.

The company is currently investing in AI and machine learning technologies to enhance StableNet® and drive network automation. It is also focused on enhancing capabilities around streaming telemetry, capacity planning, and automated resilience and security.

Infosim earned a very high score for Cost Advantage for being affordably priced for midsized and large enterprises, and for its very flexible licensing model. It received a strong score for Vendor Strength, buoyed in part by the company's very significant ongoing investments in product research and development. It devotes a higher percentage of revenue to research and development than any other vendor in this Radar Report. Infosim also received a very good overall rating for Architecture and Integration, driven by strong scores for scalability and performance, data collection, and data retention, as well as strong open APIs and a solid set of out-of-the-box integrations. StableNet® earned a good score for Functionality and Deployment and Administration. The general network management solution received strong and outstanding scores for its core NPM features.


□ Infosim
🟩 Average
Functionality
68.82
Deployment &
Administration
77.78
Cost Advantage
89.84
Vendor Strength
71.00
Architecture &
Integration
81.97
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00

Deployment & Cost Efficiency

Deployment & Administration

Ease of Deployment	
Time to value	Solid
Deployment flexibility	Outstanding
Deployment disruption	Outstanding
Staff training requirements	Outstanding

Support & Services	
Professional services requirements for implementation	Low (customers often use unpaid professional services)
Customer support	Solid
Product release cycles	Solid

Ease of Administration	
Administrative overhead	Outstanding
Product update impact	Strong
Administrative automation	Outstanding
Administrative security	Limited

Cost Advantage	
Medium enterprise acquisition costs	$
Large enterprise acquisition costs	$
License models/flexibility	Strong

Product Strength

Architecture & Integration	
Data collection	Strong
Scalability and performance	Strong
Data retention	Strong
APIs	Strong
Product integrations	Solid

Functionality

Core Features	
Network discovery	Outstanding
Application discovery/recognition	Solid
Metrics & measurement	Strong
Capacity planning	Solid
Alerting/Alarming	Strong
Troubleshooting	Strong
Visualization/Reporting	Outstanding
Active controls	Outstanding

Value-Added Features	
Security workflows/collaboration	Solid
Core analytics functionality	Solid
AIOps capabilities	Limited

Cloud Monitoring & Management	
SaaS	Solid
IaaS/PaaS	Solid
Cloud networking elements	Solid

Ease of Use	
Usability/Roles supported	Strong
Reporting customization	Outstanding

Vendor Strength	
Market vision	Solid
Product strategy	Strong
Financial strength	Solid
Research & development resources	Outstanding
Partnerships & channel	Solid

Strengths

- The network discovery functionality of StableNet® is outstanding, and it supports root-cause analysis by automatically correlating device connectivity "neighborhood graphs." As the product scans the network, it generates monitoring dependencies between network elements. In case of failures, the built-in algorithm uses the calculated weights to streamline fault isolation, helping users get to the root cause of an issue very quickly.
- StableNet® offers a very strong cost advantage. It is priced quite well for a product with broad functionality coverage and a strong core architecture. IT organizations that need a combination of affordability and scalability should consider Infosim's solution.
- The product's tagging feature adds metadata to all the elements that StableNet® monitors and manages. This enriches the inventory tree model that underpins how users navigate the product, simplifying the process of creating multiple logical and layered views of the network. For example, one can navigate the network from country to city to office, then quickly pivot to another grouping.

Opportunities

- StableNet's® user interface is strong, but there is still a gap between its rich, Java-based client and the web-based GUI. Not all features are available in the web-based GUI, which one customer singled out as a significant issue that affects usability in their particular environment. Infosim's product roadmap demonstrates a strong commitment to completing the implementation of full functionality to the web-based console in the next two years.
- Infosim customer support is strongest in Europe, although basic support services are also offered from their U.S. and Singapore offices. North American customers will discover that complex support issues are often escalated to the core product engineering team in Germany. Customers acknowledged that support out of the German office is excellent, but time zone differences may be an inconvenience for North American users requiring support for complex issues, particularly on the West Coast.
- While the platform's spectrum of use cases and functionalities is strong, certain network analytics features in StableNet® are limited. Its core network analytics capabilities are solid, but its AIOps capabilities are more limited. Infosim is in its early days of developing AIOps features. StableNet® does perform topology-based analytics, which is an important foundation for AIOps, and the company's roadmap includes a strong commitment to developing more AIOps and analytics capabilities, with a focus on anomaly detection and predictive capacity alerting. Given Infosim's industry-leading commitment to research and development, EMA expects the company to start delivering new capabilities in this area in late 2021 or early 2022.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data 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 EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com You can also follow EMA on Twitter or LinkedIn

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 www.enterprisemanagement.com 4105.090321-Infosim