

Magic Quadrant for Network Performance Monitoring and Diagnostics

6 March 2014 ID:G00258107

Analyst(s): Jonah Kowall, Vivek Bhalla, Colin Fletcher

VIEW SUMMARY

Network professionals must support an increasing number of technologies and services. With adoption of software-defined networking and network function virtualization, troubleshooting becomes more complex. NPMD tools help detect application issues, identify root causes and perform capacity planning.

Text

Market Definition/Description

Network performance monitoring and diagnostics (NPMD) enable network professionals to understand the performance of applications and infrastructure components via network instrumentation. Other users and use cases exist, especially because these tools provide insight into the quality of the end-user experience. The goal of NPMD products is not only to monitor the network components to facilitate outage and degradation resolution, but also to identify performance optimization opportunities. This is conducted via diagnostics, analytics and debugging capabilities to complement additional monitoring of today's complex IT environments.

At an estimated \$1 billion, the NPMD market is a fast-growing segment of the larger network management space (\$1.8 billion in 2012), and overlaps slightly with aspects of the application performance monitoring (APM) space (\$2 billion in 2012).

[Return to Top](#)

Magic Quadrant

Figure 1. Magic Quadrant for Network Performance Monitoring and Diagnostics



[Return to Top](#)

Learn how
Gartner can
help you succeed

Become a Client now ▶

NOTE 1 SPECIFIC HARDWARE LIFE SPAN CONSIDERATIONS FOR NPMD SYSTEMS

When evaluating and selecting an NPMD solution, it is important to keep in mind that any packet-data-storing hardware (whether derived from the NPMD vendor or a third party) will be subjected to heavy amounts of strain due to network input/output (I/O) and disk I/O activity. This will have an impact on the life span of the hardware equipment.

NOTE 2 HONORABLE MENTIONS

The following vendors were close to passing the requirements to be included in this research, and we hope to include them in future versions of this Magic Quadrant:

Blue Coat — Did not qualify due to the products not being unified between the recent Solera Networks security-focused offering and the prior Packeteer bandwidth management technologies. Blue Coat will be integrating these technologies more tightly to improve visibility for security, bandwidth optimization, and network and application visibility for buyers. The integrated offering could provide detailed measurement and control over the quality of application delivery.

Cisco — Did not qualify due to the lack of JFlow and sFlow support in the Cisco Prime Infrastructure software offering. Cisco's Prime, Network Analysis Module (NAM) and embedded AVC technologies can be combined to improve application visibility across the network, leveraging existing investments in Cisco network equipment.

Emulex (Endace) — Did not qualify due to the lack of flow analysis in the offering. Emulex (Endace) builds custom hardware solutions that provide detailed packet recording, and offer associated monitoring software for those organizations with requirements that require accuracy.

ExtraHop — The company did not qualify for inclusion due to the lack of NetFlow collection in the offering. ExtraHop's easily deployed appliances and deep visibility into applications and network topology make it an excellent jumping-off point for those looking for an easy approach to solving application performance needs.

Ixia-Net Optics — Did not qualify due to the lack of support for sFlow technologies. The downmarket Net Optics' Spyke offering is targeted at branch offices. It is launching a data center product in 2014, and is expected to invest in these technologies with the recent acquisition of Net Optics by Ixia.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Vendor Strengths and Cautions

AppNeta

AppNeta offers the only dedicated SaaS solution in this research for NPMD purposes. AppNeta is one of a select few vendors that are bridging both APM and NPMD use cases, but on a different path, converging these two offerings to build complementary technologies between both offerings. The offering consists of PathView 7.2, providing multiple deployment options for the on-premises component of the solution (including software, virtual appliances and/or hardware appliances). The solution includes deep packet inspection capabilities in most form factors and also includes flow ingestion. The product has voice analysis capabilities, and the unique path mapping and diagnostics capabilities useful for troubleshooting. AppNeta has a completely Web-based user interface, and packets can be stored based on criteria matching. The appliances hold data for up to 24 hours, based on the available storage, if the service disconnects.

Strengths

AppNeta's products are low cost and paid via monthly subscription, making them suitable for large distributed environments, which need some level of packet visibility.

Multiple form factors and plug-and-play deployment make this one of the simplest solutions to maintain day-to-day.

AppNeta delivers both APM and network performance monitoring functionality as a service, in a unified, easy-to-use interface.

Cautions

Low-cost SaaS deployment sacrifices granularity and throughput (no support for 40 Gbps platforms).

AppNeta is a startup with limited revenue.

AppNeta's weaker analytics capabilities prevent automated root cause analysis. This capability only functions in Layer 3 and Layer 4 versus Layer 7, the critical application layer.

[Return to Top](#)

CA Technologies

CA Technologies focuses on the broader IT operations management (ITOM) market and additionally on application delivery, service management, portfolio and project management, and security. With broad offerings in the availability and performance monitoring segment, the vendor has extensive coverage for network management and APM areas. The offering evaluated in this Magic Quadrant was CA Performance Management 2.3, which was complemented by several products from the NetQoS acquisition in 2009 and earlier CA acquisitions (e.g., Concord Communications). Deep packet inspection is done with a combination of CA Application Delivery Analysis (ADA), and a white-box OEM of JDSU-Network Instruments' GigaStor product known as CA GigaStor. CA ADA components are used as part of the APM offering, providing end-user experience monitoring and component latency measurement. The NPMD solution includes CA Network Flow Analysis and CA Unified Communications Monitor for voice and video monitoring. CA's new CEO was appointed in early 2013, and is attempting to dramatically change the way the vendor delivers products and solutions. With a focus on SaaS delivery and organic modernization of the product portfolio, many changes have already started to take place. CA has also embarked on a journey to become more agile, releasing software more frequently with public code drops, enabling customers to see progress quickly.

Strengths

The vendor's network monitoring capabilities are broad, but also show depth in the NPMD and APM markets, making them a good choice for a wide area of coverage.

CA has demonstrated an ability to internally develop and enhance its monitoring offerings (including for NPMD), instead of relying solely on acquisitions.

The vendor is transforming its network management and APM portfolio solution development model from a monolithic legacy software provider model to a more modern, quickly iterative SaaS delivery model.

Cautions

CA's pricing and product portfolio complexity are a concern for Gartner clients.

Analytics integration lags competitive offerings, providing limited insight into collected data.

Users report issues implementing and maintaining CA ADA technologies due to complexity.

[Return to Top](#)

Corvil

Corvil's focus traditionally has been in the high-frequency trading market, developing unique intellectual property to allow for accuracy, granularity, and distributed packet collection and analysis. The vendor refocused the offering in 2013 to bring enterprises onboard with several new product features and functions. The offering consists of CorvilNet 8.1, an appliance-based solution consisting of CorvilNet Engines for data acquisition and the Latency Management Center (LMC) for centralized administration and management of the appliances. The appliances analyze and decode the packet data, extracting default and user-defined metrics. Additionally, the product automatically does hop-by-hop latency measurement when deployed in a distributed manner. Packet data can be exported into standard packet capture file types.

Strengths

Fidelity of capture is high, with timing data coming from distributed deployments or from external time sources.

CorvilNet now supports protocols used for storage, databases, Web services, voice over Internet Protocol (VoIP) and video.

Automated correlation and easier autoconfiguration make the product easier to deploy versus

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

prior offerings.

Cautions

The cost of the solution tends to be higher than other NPMD solutions.

Corvil's product capabilities have been designed around the unique, demanding and relatively sophisticated financial vertical customer base, whose needs and resources may not match those of mainstream enterprises.

Corvil lacks 40G support.

[Return to Top](#)

Fluke Networks

Fluke Networks' heritage comes from Fluke's well-known network testing equipment for diagnostic purposes. Fluke and Fluke Networks are wholly owned subsidiaries of Danaher since 1998. Fluke Networks was spun out of Fluke in 2000, and its first product under the Fluke Networks brand was the OptiView network troubleshooting tool. Its offerings have expanded beyond that area, while still leveraging the large footprint it has for those products. Via acquisitions such as Visual Networks in 2006 and ClearSight Networks in 2009, the vendor's NPMD product portfolio has grown considerably, taking the best technology from each acquisition to form Fluke Networks Visual TruView. We evaluated Visual TruView 8.3 (an integrated offering) and Visual Performance Manager 8.3 (a scale-out offering leveraging Visual TruView), and additional data and configuration information comes from the handheld OptiView XG 11 product. Visual TruView is an integrated solution providing the ability to handle packet analysis, flow analysis and SNMP polling in a single offering. The Visual TruView appliances are sized differently, based on the storage and processing requirements of the network. The Visual Performance Manager provides views across multiple TruView appliances. OptiView XG provides an endpoint and additional data to Visual TruView, allowing for better troubleshooting data to be fed to the centralized analysis. Danaher is also the parent company of VSS Monitoring, a network packet broker (NPB) vendor, which it acquired in 2012, but no specific synergies have been announced at this time.

Strengths

Visual TruView is a single product offering and appliance line that allows the customer to repurpose and use each appliance for multiple types of data acquisition.

The product is priced competitively.

The product is easy to implement and use on a daily basis.

Cautions

The product line is new, and, with many changes still taking place, stability, long-term adoption and support are not yet proven.

Danaher, the parent company, has done little to facilitate the sharing of technology between its acquired companies (VSS Monitoring, Arbor Networks, Tektronix and Fluke Networks), often resulting in each vendor creating overlapping technologies.

Analytics and automated analysis of data are limited to baselining, providing less value for automated trouble detection and troubleshooting.

[Return to Top](#)

Genie Networks

From its inception in 2000 through today, Genie Networks has focused on providing network monitoring solutions for communications service providers (CSPs). However, attractive pricing and carrier-grade scalability have generated interest in the vendor from outside of the CSP industry as well. Based in Taiwan, Genie Networks' presence is strongest in the Asia/Pacific region, but it has recently also seen growth in Europe. Building from a competency in traditional SNMP-based network fault and performance monitoring capabilities, the vendor also incorporates deep packet inspection and flow analysis (uniquely including Border Gateway Protocol [BGP] routing analysis) into its current offering, GenieATM v.6.1.2. The appliance-based GenieATM solution includes several reporting templates designed for common CSP support use cases and supports GFlow (a proprietary protocol), alongside all standard flow types.

Strengths

Prebuilt reporting templates support key CSP customer support and operations use cases out of the box.

Attractive pricing and carrier-grade scalability should continue to stimulate enterprise customer interest.

An appliance-based product form factor simplifies implementation, particularly in highly distributed environments.

Cautions

Tight CSP and Asia/Pacific region prioritization compromises adoption beyond these focal points, although the vendor's international client base is growing. The product's user interface, while graphical and functional, is dated compared to more modern products.

Analytics capabilities are basic and centered on automated baselining to support anomaly detection.

[Return to Top](#)

HP

One of the first vendors to offer enterprise network monitoring tools (many will be familiar with its OpenView heritage brand), HP has a long history of investment in this market, and both a substantial portfolio and customer base (particularly in the network fault management space) as a result. HP continues to maintain a strong market position; however, its customers have expressed

concern to Gartner regarding shifts in HP focus, strategy and execution in recent years. Although HP is showing a renewed focus in this specific area, the newer, key technological capabilities are not yet fully built. A key component of HP's Business Service Management (BSM) offering, the NPMD solution is joined by Application Performance Monitoring, Event Correlation and Analysis, and other HP technologies to support many availability and performance monitoring needs. HP's NPMD solution is composed of several products based on and around its heritage SNMP-based fault and performance product, Network Node Manager i (NNMi) v.9.23, supplemented by Smart Plugins for Performance (adding flow collection, among other capabilities) and Advanced Services (adding unified communications visibility and other capabilities), as well as HP Real User Monitor (RUM) v.9.23 for deep packet inspection.

Strengths

Data interchange, modeling and process-level integration with other HP solutions is robust.

There is an established network monitoring technology and customer ecosystem.

The vendor offers a broad portfolio of complementary availability and performance monitoring products.

Cautions

Customers report difficulty in implementation and management of the complex solution.

Usability is hindered by multiple, varied and dated user interfaces across the NPMD solution.

Deep packet inspection is accomplished via RUM, which has not been tuned to specifically suit NPMD use cases.

[Return to Top](#)

InfoVista

While InfoVista's primary focus has been to provide NPMD solutions for the telecom and carrier space, we evaluated 5View Service Data Manager v.3.3 for data consolidation off other appliances, such as 5View NetFlow v.6.2, 5View Applications v.5.1 for deep packet inspection, 5View Mediation v.5.1 for online analytical processing (OLAP) business intelligence reporting, 5View TeraCap for long-term packet storage, VistaInsight for Networks v.5.1 for polling data collection (including SNMP, WMI, CLI, XML, VMware and SMI-S data), and Vista360 v.2.2 for dashboarding and reporting. Some of these solutions will merit consideration for larger enterprises and government organizations. The products are designed for multitenancy and scalability to meet the demands of the CSP space, particularly in terms of providing the network service assurance component of open-source software (OSS) architectures. Application visibility and customer reporting are key elements of the solution, both of which are delivered by collecting traffic usage, application and network response time, and quality of service (QoS) metrics. These metrics are consolidated from the 5View appliances into Vista360's repository for dashboarding and reporting of the data. Identification of degrading application performance and network traffic, as well as service-level management, are typical use cases for the deployment of the solution. Recent product updates have improved application visibility by providing flexible NetFlow support, in addition to already supporting Cisco's Network Based Application Recognition (NBAR), NBAR2, Application Visibility and Control (AVC) and various standard flow types.

Strengths

The ability to monitor end to end in large distributed carrier and mobile operator networks allows CSPs to gain application visibility.

Multitenancy enables distributed external customer reporting. This not only will appeal to CSPs and managed service providers (MSPs), but also is increasingly important for large enterprises attempting to operate as internal service providers.

The framework architecture enables the normalization of key performance indicator (KPI) data across multiple vendors and domains.

Cautions

A lack of lower-end packaged solutions marginalizes all but the largest of enterprises and government organizations.

Deployments typically require greater levels of professional services engagement.

The vendor lacks a significant presence in the U.S.

[Return to Top](#)

JDSU-Network Instruments

Network Instruments' acquisition by JDSU was not factored into this Magic Quadrant evaluation, as it occurred after the assessment cutoff. As indicated by its name, Network Instruments is a vendor with a singular focus on network monitoring solutions, which is reflected in its homegrown, vertically integrated technology development strategy. Established in 1994, Network Instruments has grown its portfolio from a Windows-based monitoring application to a full NPMD offering primarily composed of physical appliances. The vendor generates revenue through direct sales, partner channels and a significant OEM agreement. While Network Instruments has self-sufficiently funded its own growth over the bulk of its existence, in 2012, private equity firm Thoma Bravo took a controlling interest in the company. In the transaction, Network Instruments retained its leadership team, including co-founder and current CEO Douglas Smith, and, to date, the vendor has continued to grow its portfolio and customer base. Network Instruments' current NPMD solution is composed of Observer (v.16), Observer Reporting Server (v.16), GigaStor (v.16) and Observer Infrastructure (v.4). AppFlow protocol support is provided in addition to standard flow types.

Strengths

Data- and process-level integration workflows are well-thought-out across the solution's component products.

Network Instruments is fast to respond to customer and market demands, due to expertise in both hardware and software design.

Packet capture and inspection (via GigaStor) capability is well-regarded; this product is repackaged and sold by CA.

Cautions

The NPMD solution requires multiple components with differing user interfaces that are not consistent across products, making learning the platform more of a challenge.

The solution is focused on physical appliances, with limited options beyond proprietary hardware.

Customers report no hardware warranty beyond four years, requiring new purchases to maintain hardware support (see Note 1).

[Return to Top](#)

Lancope

Founded in 2000, Lancope's StealthWatch System is focused toward security buying centers; however, the vendor has looked to provide NPMD coverage where opportunities to do so present themselves. Packet capture is conducted on demand in a standardized format to enable its consumption by third-party protocol analyzers. Likewise, StealthWatch FlowSensor enables the identification of applications and their performance metrics. The product enables easy exporting of flow records to external products. Lancope's recent StealthWatch System 6.4 includes a performance optimization feature for both flow and packet-based data collection. The StealthWatch FlowReplicator component provides the ability to estimate the number of flows per second that an environment is capable of, to assist in determining monitoring requirements. For packet capture, StealthWatch FlowSensor has improved its small-packet processing capabilities. Lancope has recently been added to Cisco's Global Price List, which should help it reach a wider customer base and gain greater exposure than was previously the case.

Strengths

Lancope's understanding of security-related incidents enables it to provide a greater understanding of how malware, network abuse and distributed denial of service (DDoS) attacks affect network performance than do traditional NPMD solutions.

The vendor is an active thought leader on flow-based technology support, actively participating in industry and trade events to encourage the use of and development of flow-based technologies.

Lancope offers strong data mining capabilities due to the NPMD solution being designed around OLAP concepts.

Cautions

Lancope's NPMD solution is comparatively more expensive than alternative offerings, due to it supporting both IT operations and security use cases.

Due to the vendor's security focus, only a limited number of resources are dedicated to addressing NPMD feature requirements.

Company size and growth in the security market make Lancope an acquisition target, which may de-emphasize the NPMD focus.

[Return to Top](#)

NetScout Systems

NetScout Systems was founded in 1984 and has been a mainstay in the NPMD space ever since, providing network performance solutions across the enterprise, service provider and government markets. Since assuming the dominant position in the market, NetScout has combined internally grown technology with sound acquisitions to augment its existing portfolio and capabilities. Significant acquisitions include Network General in 2007 and a trio of acquisitions in 2011 (Simena, Fox Replay and Psytechnics), covering such areas as security, voice and video analytics, and network packet brokering technologies. The latest acquisition was of Accanto Systems, which helped enhance NetScout's voice monitoring capabilities. Earlier this year, NetScout consolidated much of its portfolio into the nGeniusONE 5.1 solution, which supersedes the outgoing nGenius Service Assurance Solution offering. It should be noted that there remain some elements of the previous platform that have yet to be incorporated into nGeniusONE, namely the nGenius Voice/Video Manager, although indications suggest this is a temporary situation that NetScout is looking to address. Given the coverage of the NetScout offering and its dual-market strategy of meeting the needs of both the enterprise and service provider markets, customers in those markets should find stability in a NetScout solution.

Strengths

The vendor has a sound acquisition history, with a track record of absorbing new technology into a unified NPMD platform.

NetScout has a large market share in the NPMD market space, with a strong and loyal customer base.

The patented Adaptive Session Intelligence technology allows the solution to scale toward the support of 40 GbE and 100 GbE environments, while optimizing storage requirements and enhancing the visibility of data.

Cautions

NetScout has a limited ability to expand beyond its network management heritage, which would be the next logical step (for example, into APM or IT operations analytics).

Offering only a hardware-based deployment model limits NetScout's ability to address growing software and SaaS solution demand.

NetScout is perceived as a conservative stalwart in the NPMD space, and lacks the reach and mind share that many smaller competitors have.

[Return to Top](#)

Niksun

Founded in 1997 and still led by its founder, Dr. Parag Pruthi, Niksun offers both network performance and security products. While offering appliances and architectures to suit network infrastructures of all sizes, the vendor recently released its Supreme Eagle platform, which supports high-fidelity data capture and analytics at speeds of up to 100G. Niksun has, to date, focused on ISP and other highly network-dependent industries, but has increasingly found itself being evaluated by enterprises of all types due to its highly scalable design. The vendor's current NPMD solution consists of NetVCR (for line-rate packet capture and analytics) and NetOmni for centralized management of products running the Niksun Alpine 4.4.

Strengths

Up to 100G packet capture and analysis support in recent releases makes Niksun one of the first to reach these speeds.

The vendor has been an innovator in the space by introducing new features before competitors.

Niksun's NPMD solution has a highly scalable design, supporting high traffic capture rates.

Cautions

Niksun's NPMD solution is designed to support both NPMD and security use cases, but is not optimized for either use case.

Market presence and messaging are limited and outdated.

The user interface is dated, making usability and learning more difficult.

[Return to Top](#)

Orsyp

Headquartered in Paris, Orsyp has become an increasingly active participant in the NPMD space. This involvement is rooted in QoS-oriented deep packet inspection capabilities that were developed internally. However, two recent acquisitions — Sysload in 2009 and Streamcore in 2012 — have expanded the original feature set. The two technologies complemented Orsyp's existing deep packet inspection heritage well. Sysload 5.60 provides performance and endpoint monitoring capabilities, while Streamcore 6.1 adds WAN optimization and network performance monitoring. Recent feature inclusions are the ability to deliver NetFlow collectors and the management console as virtual appliances, as well as the enhancement of overall NetFlow collection and reporting. The solution can support network links up to 1 Gbps and uses agents that run on and gather data from endpoints, storing the collected records locally before pushing them to a central repository on a 24-hour cycle. Since the acquisition of Streamcore, Orsyp has since concentrated on bringing its acquired technology sets together into a unified offering to address the NPMD space, and this is evident with a well-designed and intuitive single user interface.

Strengths

Complementary technologies have been consolidated to provide a well-rounded overall solution, including the ability to not only monitor, but also affect the QoS and application delivery.

The user interface captures typical operator workflows well, including troubleshooting and optimization use cases.

Orsyp's NPMD solution is priced attractively, considering its capabilities beyond monitoring needs.

Cautions

Appliance options are limited, and cannot currently scale past 1 Gbps; 10 Gbps support is expected in mid-2014, but there are no immediate plans to support 40 Gbps or 100 Gbps.

While Orsyp conducts business globally, it has not yet broadly expanded its NPMD installed base outside of EMEA.

Resources devoted to NPMD are limited for this midsize organization.

[Return to Top](#)

Paessler

Paessler focuses on offering network monitoring software, with a unified offering called PRTG Network Monitor. The tool has a broad set of capabilities, including agentless server monitoring, network fault monitoring, flow monitoring and packet sniffer technology to determine application usage. The solution is priced very attractively, based on the number of monitors set up in the product, and is available via a try-before-you-buy go-to-market strategy. While, the NetFlow monitoring sensor can ingest all standard flow type technologies, the product does not yet support custom IPFIX templates.

Strengths

This easy-access try-before-you-buy solution offers a simple, low-cost option.

PRTG Network Monitor covers monitoring of network elements for fault, flow analysis, and packet sniffing with a single simple solution. Additionally, the product supports health monitoring of application instances, servers and virtual environments.

Simple clustering allows for fault-tolerant monitoring easily, without complex clustering software or third-party technology.

Cautions

The Packet Sniffer module has limited capabilities, including a finite ability to save packet data to disk and fewer supported application types than other market entrants.

Paessler focuses on selling via Web and resale channels. The product is often implemented in parts of environments, versus being an enterprise standard.

Scalability has yet to be proven, with no known deployments over 100,000 configured monitors (devices typically require multiple monitors).

[Return to Top](#)

Riverbed

Riverbed focuses on application delivery, acceleration and performance monitoring. During the past four years, Riverbed has built the popular Cascade product suite, composed of several acquisitions, including Mazu Networks and Cace Technologies. The vendor has taken a large leap into the performance monitoring space with the Opnet Technologies acquisition, which closed in early 2013 to form the Riverbed Performance Management (RPM) offerings. The products span both NPMD and APM technologies, composed of Cascade Profiler 10.5 for flow analysis and analytics; Opnet AppResponse Xpert 8.6 for deep packet inspection, including end-user experience monitoring and application visibility; Cascade Shark and Cascade Pilot 10.5, which together perform more simplistic deep packet inspection packet capture and analysis; Opnet AppTransaction Xpert 17.0, which provides application transaction tracing and analysis; Opnet AppSensor Xpert 2.0, which collects SNMP and other agentless performance data; Opnet AppResponse Xpert BrowserMetrix 2.2, providing a true end-user experience monitoring capability from the browser perspective; Opnet Unified Communications Xpert 4.1.2, focusing on unified communications management supporting components from Avaya and Cisco; and, finally, the offering is brought together with RPM Dashboards 2.2 for rollup visibility and reporting across the NPMD and APM products. The solution includes several appliance lines and software components, but provides technology support and depth often not matched by other solutions. The solution supports packet inspection, storage and advanced analysis of collected data. AppFlow, NetStream and Cascade Flow (a proprietary protocol) support is provided, in addition to standard flow types.

Strengths

Riverbed's NPMD market offering includes analytics both in a distributed and centralized manner, creating a high degree of usefulness from the captured data for troubleshooting, capacity planning and monitoring.

The depth offered in the Riverbed solution is often cited as the differentiator in the offerings; technologists appreciate this detail and the strong analytics across the offerings.

The ability to see deep into Citrix, voice and other distributed applications from the network and application instrumentation perspective (APM) makes Riverbed a vendor with broad performance monitoring offerings.

Cautions

The RPM offerings include a fragmented and complex set of hardware and software technologies, which need more software and user interface integration work to improve consistency and ease of use.

The solution is priced at a premium.

Product line and naming changes prior to and between acquisitions have created confusion.

[Return to Top](#)

SevOne

Founded in 2005 by a serial entrepreneur and a technologist, SevOne has had rapid growth and secured \$150 million in venture funding from Bain Capital in January 2013. This represented one of the largest venture financings of the year and the largest in the history of the NPMD market. Management changes followed the investment and their implications have yet to be fully realized. The vendor had initially targeted larger enterprises that were well-suited to leverage the peer-to-peer-based appliance platform. SevOne boast support for 200,000 objects from a single appliance. While maintaining its position as one of the fastest and most scalable NPMD solutions remains a priority for SevOne, it has limited depth into packet data. The vendor is building a targeted strategy to address the needs of the midmarket going forward. The recent 5.3 version of the Performance Appliance Solution was released in August 2013 and helped enhance the solution's usability and workflow interface, to appeal to both large enterprise and midmarket customers.

Strengths

The scalable and distributable peer-to-peer architecture lends itself well to a "buy as you grow" deployment approach.

A rapid flow analysis engine enables the highest-reported flows and polling instances on a single appliance.

The vendor has significant financial backing and interest from a key venture capital firm, coupled with strong marketing.

Cautions

Management changes have yet to be fully realized, including new senior management and board members.

SevOne relies heavily on third-party repackaged technologies to provide deep packet inspection capabilities, which are critical to a holistic NPMD solution; however, the customer deals directly with SevOne.

Analytics are largely based around the concept of baselining and are more limited than other NPMD offerings.

[Return to Top](#)

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that

vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

[Return to Top](#)

Added

None; this Magic Quadrant is in its first release.

[Return to Top](#)

Dropped

None; this Magic Quadrant is in its first release.

[Return to Top](#)

Inclusion and Exclusion Criteria

Vendors will be required to meet the following criteria to be considered for the 2014 NPMD Magic Quadrant:

Offer the ability to monitor, diagnose and generate alerts for:

Network endpoints — Servers, virtual machines, storage systems or anything with an IP address by measuring these components directly in combination with a network perspective.

Network components — Routers, switches and other network devices.

Network links — Connectivity between network-attached infrastructure.

Offer the ability to monitor, diagnose and generate alerts for dynamic end-to-end network service delivery as it relates to:

End-user experience — The capture of data about how end-to-end application availability, latency and quality appear to the end user from a network perspective. This is limited to network traffic visibility and not within components, such as what APM is able to accomplish.

Business service delivery — The speed and overall quality of network service and/or application delivery to the user in support of key business activities, as defined by the operator of the NPMD product. These definitions may overlap as services and applications are recombined into new applications.

Infrastructure component interactions — The focus on infrastructure components as they interact via the network, as well as the network delivery of services or applications.

Provide support for analysis of:

Real-time performance and behaviors — Essential for troubleshooting in the current state of the environment. Analysis of data must be done within three minutes under normal network loads and conditions.

Historical performance and behaviors — To help understand what occurred or what is trending over time.

Predictive behaviors by leveraging IT operations analytics technologies — The ability to distill and create actionable advice from the large dataset collected across the fourth requirement.

Leverage the following data sources:

Network-device-generated data, including NetFlow, sFlow, JFlow and IPFIX flow-based data sources.

Network device information collected via SNMP.

Network packet analysis to identify application types and performance characteristics.

Non-Product-Related Criteria

Customer references must be located in at least two of the following geographic locations: North America, South America, EMEA and/or the Asia/Pacific region/Japan.

Total revenue (including new licenses, updates, maintenance, subscriptions, SaaS, hosting and technical support) must have exceeded \$5 million in 2013.

The vendor should have at least 50 customers that use its NPMD product actively in a production environment.

The product must have been shipping to end-user clients for production deployment and designated with general availability by November 2013.

[Return to Top](#)

Evaluation Criteria

Ability to Execute

Product/Service: Gartner evaluates the capabilities, quality, usability, integration and feature set of the solution, including the following functions:

Data source support, including application and network device log data

Behavioral analysis

Diagnostic workflows

Real-time monitoring

Day-to-day maintenance of the product

Ease and management of deployment and configuration

Ease of use and richness of functions within the product

Product deployment options and usability

Overall Viability (Business Unit, Financial, Strategy and Organization): We consider the vendor's company size, market share and financial performance (such as revenue growth and profitability). We also investigate any investments and ownership, and any other data related to the health of the corporate entity. Our analysis reflects the vendor's capability to ensure the continued vitality of its NPMD offering.

Sales Execution/Pricing: We evaluate the vendor's capability to provide global sales support that aligns with its marketing messages; its market presence in terms of installed base, new customers and partnerships; and flexibility and pricing within licensing model options, including packaging.

Market Responsiveness and Track Record: We evaluate the execution in delivering and upgrading products consistently, in a timely fashion, and meeting road map timelines. We also evaluate the vendor's agility in terms of meeting new market demands, and how well the vendor receives customer feedback and quickly builds it into the product.

Marketing Execution: This is a measure of brand and mind share through client, reference and channel partner feedback. We evaluate the degree to which customers and partners have positive identification with the product, and whether the vendor has credibility in this market.

Customer Experience: We evaluate the vendor's reputation in the market, based on customers' feedback regarding their experiences working with the vendor, whether they were glad they chose the vendor's product and whether they planned to continue working with the vendor. Additionally, we look at the various ways in which the vendor can be engaged, including social media, message boards and other support avenues.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	Medium
Operations	Not Rated

Source: Gartner (March 2014)

[Return to Top](#)

Completeness of Vision

Market Understanding: This criterion evaluates vendor capabilities against future market requirements. The market requirements map to the market overview discussion and look for the following functionality:

- Data source support, including application and network device log data
- Behavioral analysis
- Diagnostic workflows
- Real-time monitoring
- Virtualization (network function virtualization [NFV] and software-defined networking [SDN])

Marketing Strategy: We evaluate the vendor's capability to deliver a clear and differentiated message that maps to current and future market demands, and, most importantly, the vendor's marketing effectiveness to the NPMD market through its website, advertising programs, social media, collaborative message boards, tradeshow, training and positioning statements.

Sales Strategy: We evaluate the vendor's approach to selling NPMD in the appropriate distribution channels, including channel sales, inside sales and outside sales.

Offering (Product) Strategy: We evaluate product scalability, usability, functionality and delivery model innovation. We also evaluate the innovation related to the delivery of products and services.

Business Model: This is our evaluation of whether the vendor continuously manages a well-balanced business case that demonstrates appropriate funding and alignment of staffing resources to succeed in this market. Delivery methods will also be evaluated as business model decisions, including the strength and coherence of on-premises and SaaS solutions.

Vertical/Industry Strategy: We evaluate the targeted approaches in marketing and selling into specific vertical industries.

Innovation: This criterion includes product leadership and the ability to deliver NPMD features and functions that distinguish the vendor from its competitors. Specific considerations include resources available for R&D and the innovation process.

Geographic Strategy: This is our evaluation of the vendor's ability to meet the sales and support requirements of IT organizations worldwide. In this way, we assess the vendor's strategy to penetrate emerging markets.

Table 2. Completeness of Vision
Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Low

Source: Gartner (March 2014)

[Return to Top](#)

Quadrant Descriptions

Leaders

The Leaders quadrant represents those vendors that are pushing the NPMD market forward, including those with comprehensive portfolios and the ability to handle multiple application and technology types. They offer a choice of hardware or software appliances for optimum flexibility. Additionally, the use of SaaS delivery methods within portfolios gives enterprise IT teams more choices, while making formerly premium priced NPMD solutions attainable by midsize organizations.

[Return to Top](#)

Challengers

Challengers consist of those with high market reach and large deployments. Once leaders in the network performance monitoring market, they are currently struggling to deal with new technical demands and rising expectations. These established NPMD vendors bring a substantial installed base, but also architectures, feature sets and pricing structures that require modernization (often in progress) to better compete with those in the Leaders quadrant.

[Return to Top](#)

Visionaries

Visionaries have built a compelling plan to competitively address current and future NPMD customer demands. The Visionaries are combining elements of APM and NPMD in ways that provide deeper visibility than is currently available from other vendors. Currently, execution is limited either by limited market reach or the extension of existing tools and technologies not initially designed to meet these needs.

[Return to Top](#)

Niche Players

Niche Players are those with solutions catering to specific audiences or with limited use case support today. They have often been unable to address the needs of larger enterprises or have only done so within specific verticals or market segments. Each of these vendors is working to appeal to the broader NPMD buying community, versus the targeted use cases they serve today. With the right changes to their product plans, positioning and/or business execution strategies, any of these vendors could successfully shift their differentiated technologies to address use cases in ways that today's Leaders might have a hard time matching.

[Return to Top](#)

Context

NPMD solutions should be considered as part of a larger network management initiative — as part of an overall availability and performance monitoring strategy. Utilizing these additional points of reference will yield additional unique criteria (existing investments, investment plans, vendor relationships, etc.) that, when combined with Gartner analysis, can prove critical to proper solution selection.

In the course of this research, several key observations emerged that should be carefully considered in the course of NPMD strategy formulation and solution selection, including:

- Ease of use remains an area of needed improvement and varies significantly both across vendors and within solutions.
- Virtualization and SDN support is minimal in most NPMD solutions.
- Both IT operations analytics vision and execution are lacking in most NPMD solutions.
- Flow protocol support and actual flow data utilization vary significantly across vendors.
- Pricing and product/capability packaging vary significantly across vendors.
- On-premises appliances are the dominant delivery model, but software and SaaS offerings are available.
- Integrations with other ITOM solutions (even other availability and performance solutions) are an afterthought for most solutions, thus encouraging the use of these tools within the network silo.
- Many NPMD solutions are assembled from multiple products, which can enable modular

adoption of NPMD capabilities, but also can add significant complexity to procurement and ongoing maintenance.

It remains imperative that organizations purchase tools that closely match their current maturity levels. It is a current reality that many network monitoring teams have yet to successfully make the leap from basic, reactive network availability management to proactive performance management. While tool investment can play a part in this maturation, it is clear that simply investing in NPMD tooling without similar investments in training, integration and processes will yield limited results at best. Gartner recommends that network teams assess their current state of maturity on a regular basis, both individually and at the organizational level, to provide this perspective. To help, teams can utilize Gartner's ITScore for infrastructure and operations (I&O; ITSIO) (see "How to Improve I&O Maturity by Using the ITScore").

Organizations should not utilize the Leaders quadrant as an effective shortlist of appropriate vendors, but instead should build a list of criteria that describe their current and future needs, and then select from vendors that best meet those requirements. Organizations should select a vendor that has both a history of and future plans for focusing on this market. Careful consideration should be given to required skills, training, process and deployment investments, because these factors will have a much greater impact on the overall value realized from an NPMD investment than any specific functional capability found in a given tool.

[Return to Top](#)

Market Overview

NPMD: A Mature Market Evolves Rapidly in Response to New Demands

For decades, the well-established practice of network management has enjoyed no shortage of available monitoring technologies, tools and vendors; however, the vast majority of those solutions, both acquired and implemented over the years, have been designed to support isolated, reactive resolution of availability issues by network specialists. There have also been many investments in tools and skills, with the specific goal of monitoring the performance of network infrastructure in addition to its availability; however, these efforts have typically been hampered by technology limitations and isolated implementation. This approach, while delivering moderately satisfactory results for many years, has proven inadequate in the face of several key shifts, including:

- Rising demand for network services and end-user expectations of their quality

- Growing appreciation of the network as a critical component of IT services and as an agnostic, trusted source of cross-domain availability and performance data

- Exponential growth in application and infrastructure dynamism and complexity

Each of these shifts has pressured network teams to rethink their tooling strategy, so that they can get the visibility they need to truly monitor and troubleshoot the performance of their network resources in the context of the applications and services they support. A subset of the overall network performance monitoring market, NPMD has emerged as a unique market designed to address these very needs in today's increasingly complex environments. A fast-growing subsegment, the NPMD tool market is currently estimated by Gartner to be approximately \$1 billion in size.

NPMD tools provide this required breadth and depth of visibility in both real-time and historical perspectives by uniquely analyzing data from all three of the following sources. Previous approaches that only take into account one or two of the following data sources have proven to be inadequate, so all three must be supported for a tool to be considered an NPMD solution (see Note 2).

[Return to Top](#)

SNMP Polling

Period polling is one method that looks to quantify network usage of network elements to gauge the requirements of the infrastructure. Each network device has embedded agents that "speak SNMP." These agents can then be interrogated with a polling-based approach, returning metrics from the embedded agent. These collected metrics can be stored, reported on, analyzed for troubleshooting or used for capacity planning. SNMP polling can also be used to gather hardware or software errors (faults) and capacity data (for example, triggering an alert when a hardware fault occurs, the device CPU is above a threshold or the interface capacity is abnormal when compared to a baseline.) Based on the metrics gathered, the network team can estimate the delta between existing and required bandwidth needs on a per-location basis. A limitation with this method is the minimal granularity it offers, which matches the frequency of the polling. In most NPMD technologies, SNMP is used during troubleshooting to collect additional data, whereas in availability monitoring, it's used more regularly to understand the health of the network devices.

[Return to Top](#)

Flow-Based Technology

Summarized data is generated by the network devices, which includes characteristics of the IP conversation between two network nodes, and these characteristics are embedded within flows. Flow data is exported from the network devices to the NPMD technologies, which then collect and process this data stream to provide insight into which devices and applications are consuming bandwidth, how long the conversations are lasting, and who is participating in them. Since the data is summarized, a degree of detail is removed to simplify processing and extract meaning from the actual network data. Flow-based data does not provide details down to a specific set of network packets going between the source and destination, and can have a performance impact on the devices exporting flow data.

There are several flow collection standards, such as Cisco's NetFlow (v.5/v.9), Juniper's JFlow, Huawei's NetStream, Citrix's AppFlow, Riverbed's Cascade Flow, the Internet Engineering Task

Force's (IETF's) IPFIX (which is based off NetFlow v.9) and sFlow from the sFlow.org consortium. Vendor-derived standards are predominant, which hinders integration and comparisons. Flow data collection is a function embedded in the network devices themselves. The device analyzes the network traffic traversing from one interface to another, with the primary purpose of assessing bandwidth consumption, and the level of data being sent and received between various source and destination ports across the network. That data is then summarized into a stream of flow records that is sent to the monitoring tools that collect and assess the flow records.

Additionally, the quality and granularity of flow information are always evolving. Many vendors embed additional data within their flows, especially those implementing flexible record types, such as Cisco's IOS Flexible NetFlow, which allows the user to configure the exported data format. Example data embedded in flows contains wireless protocols, link aggregation, URLs, latency information, and other application or infrastructure monitoring data. With such open standards in flow technologies, the implementation varies between network equipment vendors, but most tools collect and process the data regardless of the network equipment implementation.

[Return to Top](#)

Packet-Based Technology

Examining the current infrastructure in detail on a per-packet basis provides the necessary real-time and historical visibility into volatile traffic behavior from "bursty" modern application types, like today's chatty Web applications, unified communications services (such as voice and video delivery), and the growing footprint of hosted virtual desktop (HVD) and virtual desktop infrastructure (VDI) technologies. Because only raw, unmanipulated packet data is being collected, a vendor-agnostic view of performance can be preserved throughout the analysis. This approach affords far greater insight and precision, but it comes with potentially costly (and for some, impossibly costly) appliance or "probe" implementation requirements.

The modern packet analysis technologies were pioneered more than 20 years ago with Network General's packet Sniffer in 1986. Sniffer was designed to help troubleshoot network issues after they occurred. This technology was acquired several times, and now finds its home with NetScout as of 2007. Through the years, these high-end proprietary packet analysis technologies have commoditized and moved into open source with entrants such as Wireshark, tcpdump and libpcap providing the underpinnings of this technique. These particular open-source technologies have, in turn, been incorporated into countless numbers of other critical open-source projects, such as Snort (intrusion detection system), Nmap (port scanning) and ngrep. These technologies continue to evolve, most recently into enabling real-time visibility and, in many cases, supporting the archiving of packet data for forensics and debugging without requiring the issue to be reproduced for diagnosis.

As the NPMD market continues to grow and develop, Gartner expects that future tool enhancements will center on usability, advanced IT operations analytics and virtualization/SDN support (see "Introducing the Network Performance Monitoring and Diagnostics Market"). Additional vendors are expected to enter the NPMD market, as well as over 30 vendors participating in the larger network performance monitoring market, but they did not meet the criteria specific to the 2014 NPMD Magic Quadrant (see "Criteria for the New Magic Quadrant for Network Performance Monitoring and Diagnostics").

[Return to Top](#)

Adjacent and Overlapping Markets

NPMD is, and will likely continue to be, frequently confused with adjacent and component technologies, as it is both a reasonably recent addition to the dynamic availability and performance monitoring market and a superset of multiple network performance monitoring technologies. Because vendors will both intentionally and unintentionally exacerbate this confusion to their benefit, IT leaders are advised to utilize the following definitions to add clarity to their evaluation efforts.

[Return to Top](#)

Application-Aware Network Performance Monitoring

A wholly contained subset of NPMD, application-aware network performance monitoring is a necessary maturation step that adds some degree of application visibility accomplished via packet-based monitoring, which can provide varying degrees of application context to monitored network traffic.

[Return to Top](#)

APM

APM tracks the end-user performance of application components, and provides granular troubleshooting tools for the application and its components. It provides this insight by monitoring on five main functional dimensions, including: end-user experience monitoring (EUM), application topology discovery and visualization, user-defined transaction profiling, application component deep dive, and IT operations analytics. APM differs from NPMD primarily in its focus on monitoring the quality of the end-user's experience via application interactions across all application and infrastructure tiers, including, but not limited to, the network perspective.

[Return to Top](#)

NPBs

NPBs assist with traffic aggregation, visibility and overall management of the data being sent to monitoring tools. Vendors in the NPB space often partner and team up with NPMD and security vendors as a go-to-market strategy, resulting in marketing messages that can make it difficult to determine which tool is actually performing the monitoring (network performance monitoring or security) and which is facilitating the monitoring by managing the data to be monitored (network packet brokering). We have also seen an increasing number of acquisitions in this space. NetScout

and Network Instruments, both of which are in this Magic Quadrant, pair NPBs and NPMD tools together in deals. Other popular NPB vendors include Gigamon, Ixia (Anue and Net Optics), VSS Monitoring, NetScout, JDSU-Network Instruments, Interface Masters Technologies, Apcon, Datacom, and switch provider Arista Networks.

[Return to Top](#)

Network Fault Monitoring

Network fault monitoring tools indicate the status of network components, such as routers and switches. These tools isolate, aggregate, deduplicate, filter, prioritize and resolve faults/alerts on the network. In some cases, the tools discover and visualize the topology of physical and logical relationships and dependencies among network elements. This helps depict the up/down status of those elements in a contextual map, provide basic root cause analysis (RCA), and enhance error deduplication and suppression capabilities. These tools have been widely deployed, primarily to address the reactive nature of network monitoring in IT operations. They provide network teams with a single location to monitor, alert and coordinate diagnosis of all network-related fault and availability information. These events are useful to help ensure that critical network devices remain available to support the business applications and services that rely on them.

[Return to Top](#)

Unified Monitoring

Unified monitoring is a subset of infrastructure monitoring that relies on primarily agentless and API-integration-based data collection methods to monitor the availability of servers, networks, storage and virtualization layers. These tools also do minimal discovery, and acquire physical, virtual and logical topologies and the relationships between them for the purposes of monitoring. They monitor common application instances on OSs, perform synthetic transactions for checking Web application availability, and support service and infrastructure grouping, and are multitenant by design. Unified monitoring differs from NPMD primarily in its pure focus on infrastructure availability versus NPMD's focus on performance. Unified monitoring should be supplemented by log analytics, NPMD and APM tooling to support complex troubleshooting and performance monitoring.

[Return to Top](#)

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Usage Guidelines for Gartner Services](#) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity](#)."

[About Gartner](#) | [Careers](#) | [Newsroom](#) | [Policies](#) | [Site Index](#) | [IT Glossary](#) | [Contact Gartner](#)