(https://www.gartner.com/home)

LICENSED FOR DISTRIBUTION

Magic Quadrant for Network Performance Monitoring and Diagnostics

Published: 21 February 2018 **ID:** G00326772

Analyst(s): Sanjit Ganguli, Vivek Bhalla, Pankaj Prasad

Summary

Network performance is intertwined with the success of digital business. NPMD solutions are key to network visibility, performance issue detection and root cause analysis; but network complexity, moves to cloud-hosted workloads, endpoint diversity and software-defined architectures are challenges.

Market Definition/Description

This document was revised on 21 February 2018. The document you are viewing is the corrected version. For more information, see the Corrections (http://www.gartner.com/technology/about/policies/current_corrections.jsp) page on gartner.com.

Network performance monitoring and diagnostics (NPMD) tools allow IT operations to understand the performance of application, network and infrastructure components via network instrumentation, including insight into the quality of the end-user experience. The goal of NPMD products is not only to monitor the network traffic and infrastructure to facilitate outage and degradation resolution, but also to identify performance optimization opportunities. This is conducted via diagnostics, analytics and root cause analysis capabilities to complement monitoring of today's complex IT environments.

Gartner estimates the size of the NPMD tool market at $2.1 billion and growing at a compound annual growth rate (CAGR) of 15.9%, according to Gartner's "Market Share Analysis: Performance Analysis Software, Worldwide, 2016." This market is a growing segment of the larger availability and performance monitoring space, which also includes application performance monitoring (APM), IT infrastructure monitoring (ITIM), artificial intelligence for IT operations platforms (AIOps) and digital experience monitoring (DEM).

This Magic Quadrant research period has seen some reshuffling within the NPMD vendor space, with the completion of the spinoff/merger of HPE's software business to U.K.-based software company Micro Focus, the sale of Performance Vision to Accedian, the sale of AppNeta's APM assets to SolarWinds and Cisco's acquisition of APM vendor AppDynamics.

This research year has evidenced a number of observations about the NPMD space:

Cutting-edge innovation in this mature industry (with vendors having an average life span of 17 years) is muted compared to other monitoring areas, with many vendors focusing on GUI updates, integrations and product rationalization.

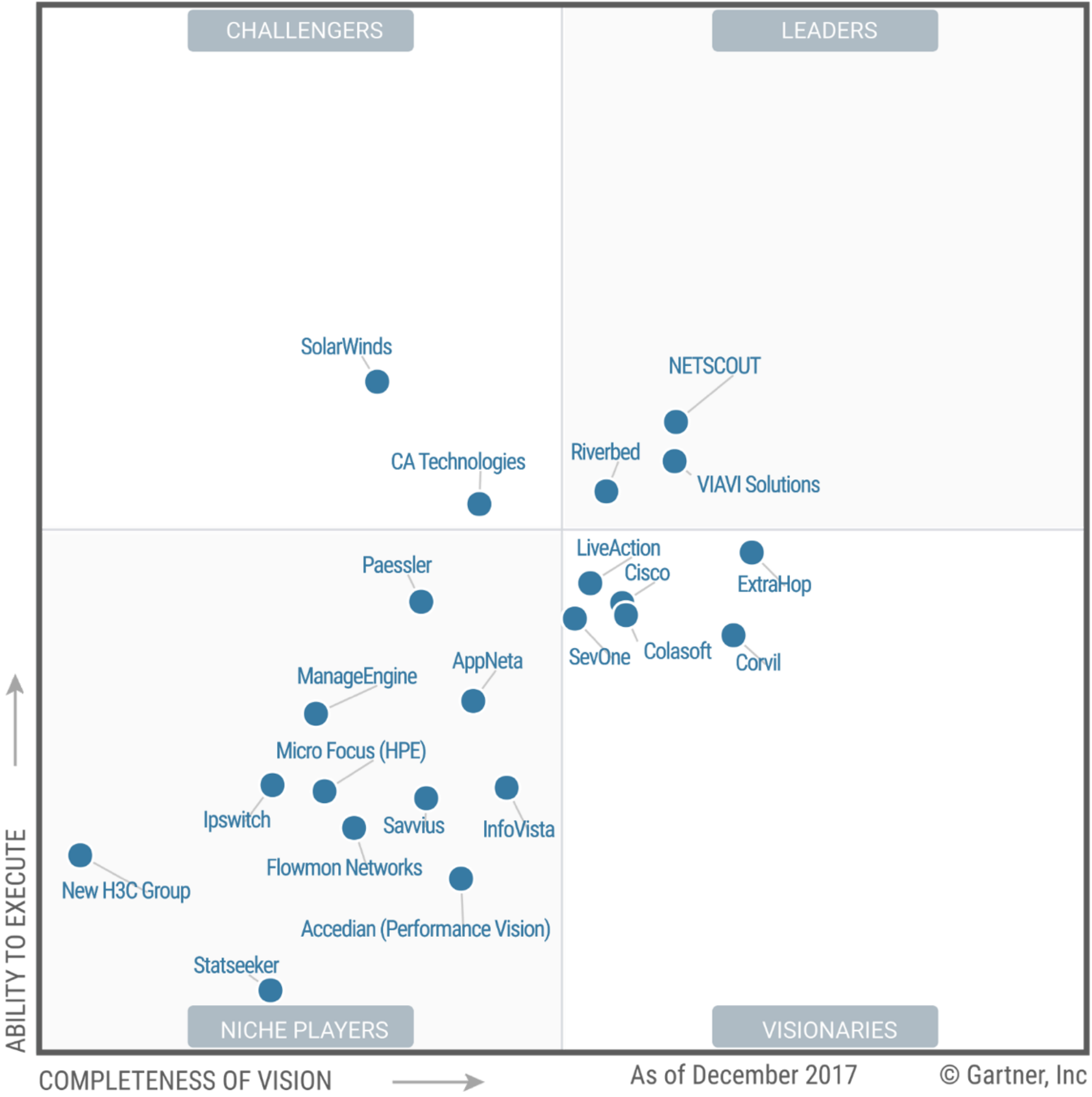
The NPMD vendor market has split into two camps: those focused on polling-based infrastructure monitoring with basic flow and packet monitoring capabilities, and those focused on hardware-based deep packet analysis with basic infrastructure monitoring. While we had expected to see vendors moving toward bringing these two camps together into a single, holistic product offering, we have instead seen an NPMD vendor landscape that has crystallized. This has created distinct patterns among end users:

- Those that tend to invest broadly in packet and infrastructure monitoring solutions, often across different vendors, but still have issues with the consumability of their packet monitoring solution. This is exacerbated by increasing data center data rates, virtualization, cloud migration and encryption.
- Those that invest more narrowly in infrastructure-focused monitoring, and that report frustration in their inability to do root cause analysis without deeper monitoring. Some look to AIOps solutions as a possible remedy.

Finally, a number of vendors have initiated a concerted effort to target the cybersecurity market, given the growing interest in network traffic analytics from security operations teams.

Magic Quadrant

Figure 1. Magic Quadrant for Network Performance Monitoring and Diagnostics



Source: Gartner (February 2018)

Vendor Strengths and Cautions

Accedian (Performance Vision)

Based in Paris, France, Performance Vision (PV) is a new entrant in this year's Magic Quadrant with its NPMD offering. The PV solution can be deployed as a hardware or software appliance. PV is a packet-oriented solution, with software-defined networking (SDN) and network function virtualization (NFV) capabilities, including monitoring of database transactions and unified communications (UC). It classifies applications through analysis of the packet data and captures

end-user experience by computing the total response time for particular applications. The recent product release in April 2017 included a new Micro Capture Appliance that is targeted at small remote sites.

The vendor predominantly sells to customers in EMEA and has a very low penetration in all other regions. Most of PV's customers are midsize enterprises. PV primarily sells through channel partners, which include network integrators, NPMD specialists and service providers. Toward this goal, PV runs a regular partner certification training program.

Performance Vision was acquired by Accedian in December 2017. The change of ownership is not reflected in this research.

Performance Vision's NPMD revenue is estimated to be between $5 million and $10 million per year.

STRENGTHS

Performance Vision's NPMD solution offers reduced deployment and maintenance complexity due to its simple deployment model.

Performance Vision has established a strong technical partnership with VMware, with a majority of customers using PV's virtual appliance within their VMware environment.

The vendor's focus on monitoring SDN, cloud and virtual environments is a differentiator within the NPMD market.

CAUTIONS

The UI is heavily focused on diagnostic capabilities and can present visualization challenges for nontroubleshooting use cases.

Performance Vision has a heavy presence in EMEA, which may present challenges from a support perspective when increasing its penetration in other markets.

Although the deployment model is quite simple, the licensing and pricing model can be quite complex for PV's customers.

AppNeta

Founded in 2011, Boston-based AppNeta offers a SaaS-based solution focused on monitoring the end-to-end network performance of the remote office/branch office. This narrowed focus was a result of the divestiture of its APM capability (TraceView) in a sale to SolarWinds in August 2016.

Accompanying this shift, AppNeta has repackaged its monitoring capabilities into a single package called the AppNeta Performance Manager. This combines the capabilities of three previously separate modules (PathView, AppView and FlowView) to provide active network path monitoring of application delivery, application usage analysis and synthetic web transactions for

application experience. The solution requires the installation of a physical or virtual appliance at the end location to perform the synthetic tests and path analysis, from which the SaaS-based analysis occurs, leveraging deep packet inspection and AppNeta's TruPath technology.

AppNeta's plans include enhancing its solutions with technical integrations, particularly for cloud-centric monitoring, while also enhancing its analytics. AppNeta has also hired a new chief customer officer and a SVP of sales over the past year, articulated as part of its plans to improve its global presence and to expand the limited channel partner program. AppNeta currently has a resell relationship with NPMD vendor SevOne, which incorporates several AppNeta capabilities into its solution.

AppNeta's NPMD revenue is estimated to be between $25 million and $50 million per year.

STRENGTHS

A SaaS-focused model allows a high frequency of product enhancement, with Performance Manager receiving updates every two weeks.

Repackaging efforts and a refocus of the company has contributed to a healthy customer growth rate.

AppNeta uniquely addresses a need to manage cloud and UC performance at remote locations that communicate directly to the cloud, as traditional data-center-based monitoring approaches fail to see this traffic.

CAUTIONS

The focus on the remote office/branch office limits AppNeta's ability to meet end-user requirements for a holistic network performance monitoring platform for private data center networks.

Third-party integration with other IT operations tools are lacking, specifically for IT service management platforms, limiting the ability to integrate AppNeta into end-to-end workflows.

Security and privacy perception issues related to SaaS products persist among risk-averse end users. This is a sales inhibitor when competing against traditional on-premises-based tools.

CA Technologies

Headquartered in New York City, CA Technologies has a 24-year history in network performance monitoring, with a software suite built over many years of acquisitions and organic development. Given this history, CA has recently consolidated its APM, ITIM and NPMD business units under a single product management leader.

CA Technologies' NPMD offering has shifted from previous incarnations, and is now branded as the Network Operations and Analytics (NetOps) platform. This platform comprises existing CA products, including CA Performance Management for infrastructure monitoring, CA Network Flow Analysis for flow monitoring, CA Application Delivery Analysis for packet monitoring, CA Spectrum for fault and event management, CA Unified Communications Monitor for voice and

video monitoring, and CA Virtual Network Assurance for SDN/NFV monitoring. Accompanying its NetOps platform is the recently released CA Digital Experience Insights, which is a SaaS-based analytics offering that aims to integrate customer experience, application performance, infrastructure and network management services for a holistic view into performance.

The NetOps platform leverages CA Performance Management as the central point of the new NPMD architecture, which is a departure from CA's previous strategy of leveraging CA Unified Infrastructure Management as its consolidation platform. CA continues to focus its R&D on monitoring modern networking infrastructure, including the cloud, SDN, software-defined WAN (SD-WAN), virtual customer premises equipment (vCPE), Internet of Things (IoT) devices and security devices.

CA's NPMD revenue is estimated to be between $100 million and $250 million per year.

STRENGTHS

Positive financial viability continues to show that there is limited risk to stability in doing business with CA Technologies.

Recent announcements of CA Digital Experience Insights along with a merging of business units represent a much-needed consolidation strategy for CA's disjointed product sets. Execution against this strategy will be critical.

CA is improving its interoperability with APIs, allowing the ingestion of third-party data and the ability to incorporate third-party analytical engines outside of the CA suite of products.

CAUTIONS

CA's focus on infrastructure monitoring limits its ability to compete with leading NPMD vendors that provide modern packet and flow monitoring technologies.

End-user survey results show that CA's cost of implementation, training and professional services is among the highest of NPMD vendors, as a percentage of total solution costs.

Gartner inquiries have shown that unclear development and migration strategies for CA Spectrum and CA eHealth customers have caused confusion among end users.

Cisco

San Jose, California-based Cisco has offered network performance monitoring solutions for 19 years as part of its network-hardware-centric heritage, and it enjoys broad name recognition. The vendor has undergone internal consolidation of its enterprise networking business units to combine various automation and monitoring products into one organization under the Digital Network Architecture (DNA) platform.

Cisco's NPMD capabilities remain distributed across various product lines. Its most widely distributed NPMD offering remains Prime Infrastructure, and it is used for Simple Network Management Protocol (SNMP), Syslog and flow monitoring, configuration management, and provisioning of Cisco network devices. This is supplemented with Prime Network Analysis

Module for packet analysis, and Prime Collaboration Assurance for UC monitoring. Cisco Nexus Data Broker provides network packet broker (NPB) functionality. Cisco also offers Application Policy Infrastructure Controller Enterprise Module (APIC-EM), its policy-based SDN controller, which provides path analytics along with quality of service (QoS) automation capabilities. Cisco Stealthwatch and Cisco Tetration round out the portfolio with security-focused capabilities.

New to the mix is the first incarnation of Cisco's DNA Center, which aims to bring intent-based networking, analytics and programmability to network management. Initially, DNA Center will support Software-Defined Access (SD-Access) and wireless assurance with plans to address big data analytics and intent-based networking use cases. Cisco also entered into the application performance monitoring market with its purchase of a leading APM vendor, AppDynamics, in March 2017. The prospect of integrating AppDynamics with Cisco's NPMD solution is intriguing, but definitive plans have yet to be announced.

Cisco's NPMD revenue is estimated to be between $51 million and $100 million per year.

STRENGTHS

A consolidated organization focused on holistic network management is a welcome start to rationalizing and coordinating Cisco's disjointed NPMD offerings.

DNA Center's promise of providing a single assurance and automation architecture for LAN, WAN, campus and cloud, by leveraging a broad set of data sources, is potentially disruptive. Execution against this promise will be critical.

Positive financial viability continues to show that there is limited risk to stability in doing business with Cisco.

CAUTIONS

While initially promising, Gartner has observed limited market penetration of Cisco Tetration among NPMD buyers, due in part to its focus on security workflows.

Despite Cisco expanding its customer base for its NPMD solution with new license bundles, Gartner has observed a general lack of awareness of its capabilities.

The large majority of Cisco's NPMD sales are tied to Cisco hardware purchases. The vendor misses the ability to cater to general NPMD use cases in an increasingly heterogeneous networking environment.

Colasoft

Colasoft is a privately owned company founded in 2001, headquartered in Chengdu, China, and is a new entrant in this year's Magic Quadrant. Colasoft focuses on visually based and metric-oriented packet analysis to help simplify network management.

Colasoft's NPMD solution consists of three components: Unified Performance Management (UPM), nChronos and Capsa. UPM is the visualization layer that delivers business- and service-oriented performance views, full network path analysis, and proactive performance issue

detection, all based upon data collected by nChronos. nChronos provides packet capture with historical and real-time analysis of application-oriented performance metrics for every TCP conversation. Capsa is a network analyzer that provides packet sniffing and capture where application decoding and deep domain analysis is required. A limited version of Capsa, Capsa Free, is also available to download.

A steady stream of product updates was made throughout 2016 and 2017. Following on from seven product releases in 2016, new releases delivered application analysis for approximately 1,800 predetermined applications. Custom applications could also be defined based on Internet Protocol (IP) address, port number, protocol, packet pattern, or a combination of any or all criteria. The latest release of Capsa added support for Session Initiation Protocol (SIP) and the H.323 protocol, alongside reporting and diagnostics on voice over IP (VoIP) statistics. The latest release of nChronos added NetFlow and agent analysis, as well as the ability to collect network traffic from virtual environments and cloud platforms.

Aside from product development, in June 2017 Colasoft joined the Cisco Solution Partner Program as a Solution Partner. Colasoft has developed significant presence in government organizations, while other vertical industries have yet to be targeted to the same level. Outside of China, the primary route to market for Colasoft is through channel sales, particularly for regions beyond Asia/Pacific (APAC). However, the number of partners are few, and this is an area of focus for the company.

Colasoft's NPMD revenue is estimated to be between $11 million and $25 million per year.

STRENGTHS

Colasoft experienced rapid year-over-year growth of 94% in 2015 and 62% in 2016, with a significant installed base of over 10,000 paying customers and 500,000 freeware users.

The vendor's products provide strong troubleshooting capabilities, with all metrics collected and reported at a one-second granularity rate.

Colasoft has shown a strong focus on R&D, with over 100 engineers dedicated to developing Colasoft's NPMD solution.

CAUTIONS

In-house resources are almost exclusively based in the Asia/Pacific region. Customers from other regions should ensure the reseller resources made available are adequate and sufficiently skilled to provide ongoing support.

Colasoft's channel program is less geographically diverse when compared to leading NPMD vendors, limiting its sales reach globally.

Colasoft's ability to monitor infrastructure metrics is limited.

Corvil

Founded in 2000, Dublin, Ireland-based Corvil focuses on short-time scale network monitoring, providing comprehensive multisegment and highly accurate packet analysis. These capabilities have always appealed to the vendor's financial services customer base's heritage; however, Corvil continues its transition — based on its streaming analytics platform — to deliver machine-time data visibility and operational intelligence to a broader target audience.

Product development has progressed with a significant product update released in May 2017. This included a software sensor to instrument network packet data in private cloud, public cloud and private virtualized environments. It should be noted that this is not a virtual appliance nor a synthetic monitoring component. New productized integrations for LiveAction, Cisco Tetration and an additional Splunk app have also been included in the new version.

Aside from product development, Gartner has observed increased collaboration between Corvil and its technology partners in terms of increased presence at key partner events, joining Splunk's Adaptive Responsive Initiative, and holding joint events with Cisco and LiveAction.

Corvil's NPMD revenue is estimated to be between $26 million and $50 million per year.

STRENGTHS

- Corvil has experienced healthy sales performance and growth, with total revenue growing by 36% year over year.
- The machine-time data analytics concept aligns well to end users with IoT initiatives.
- Targeted productized integrations with Splunk, LiveAction and Cisco enhance the overall Corvil value proposition.

CAUTIONS

- Corvil's software sensor provides packet-only visibility for those customers that are migrating critical services into virtual and cloud environments, lacking support for other data sources or synthetic monitoring approaches.
- SNMP and flow-based data source support remain comparatively weak.
- Over the last 12 months, end users have cited increased issues concerning the cost of implementation and maintenance.

ExtraHop

ExtraHop, headquartered in Seattle, Washington, and founded in 2007, focuses on packet analytics for performance and application insights. Over the past year, ExtraHop has released a SaaS-based anomaly detection offering to accompany its hardware and virtual appliances.

The vendor's solution is called the ExtraHop platform, which is sold as a single solution customizable with different appliance configurations, modules and bundles. The ExtraHop stack includes the ExtraHop Discover Appliance, which provides real-time analysis on network data; the ExtraHop Explore Appliance, which provides indexing and storage of transaction records; the

ExtraHop Trace Appliance, which provides continuous packet capture; and the ExtraHop Command Appliance, which provides centralized management. To achieve end-to-end workflows that are common to NPMD, a combination of the Discover, Explore and Trace Appliances must be deployed.

ExtraHop's recent focus has been on improving visualization and analytics capabilities, including the addition of machine-learning-based anomaly detection. Visualization improvements include the new live activity maps, which are real-time views of network traffic and dependencies. ExtraHop Addy is a cloud-hosted anomaly detection service that applies unsupervised machine learning for NPMD data sources. ExtraHop has also invested in security-focused capabilities and workflows based on network-traffic-based data. Integrations with third-party applications and tools, including Cisco Tetration, ServiceNow and Cerner, have also been introduced.

ExtraHop's NPMD revenue is estimated to be between $50 million and $100 million per year.

STRENGTHS

ExtraHop provides network-derived intelligence data that caters to groups outside of network operations, including line of business (LOB) owners.

The vendor's broad support for application layer decodes is a differentiator against other NPMD vendors.

ExtraHop's rate of new customer growth has outpaced those of other NPMD vendors.

CAUTIONS

ExtraHop's focus on packet analysis may cause challenges — data center data rates, cloud migration, encrypted traffic and east-west traffic flows can cause difficulties in accessing packet data.

ExtraHop's focus on both security and performance buyers may hinder its ability to keep pace with NPMD market shifts.

The ability to derive and use application context from network data should not be confused with full APM capabilities.

Flowmon Networks

Flowmon Networks, founded in 2007 and based in Brno, Czech Republic, specializes in scalable flow-based monitoring to meet NPMD and security-focused network behavior analysis (NBA) disciplines. While flow-based monitoring is the focus of the Flowmon Probe and Flowmon Collector, packet capture via Flowmon Traffic Recorder and the Flowmon Application Performance Monitor component also contribute to Flowmon's NPMD capabilities. Flowmon is available as on-premises software and hardware, with a SaaS option recently made available as well.

Product development has continued with a new version of Flowmon released in 2017, providing extended Layer 7 monitoring and support for proprietary flow record fields. Flowmon has augmented its existing agentless monitoring capabilities for HTTP and HTTPS traffic, with synthetic transaction monitoring based on Selenium scripts. Future investment focuses on improving support of cloud environments and the IoT. Flowmon Networks continues its plans to expand to new geographies, with recent investments into the U.K., Nordic region and South Korea.

Flowmon Networks' NPMD revenue is estimated to be between $7.5 million and $10 million per year.

STRENGTHS

Flowmon Networks' roadmap for monitoring cloud-centric data sources, including support for Amazon Web Services (AWS) and Microsoft Azure environments, shows promise as workloads move into the cloud.

Flowmon Networks' products are highly scalable, with the ability to support 100G environments and 400,000 flows per second per appliance.

Flowmon has improved its brand recognition with investments in outbound marketing and its web/social media presence.

CAUTIONS

Focus on flow-centric data sources limits Flowmon's appeal for those buyers looking for holistic NPMD functionality that includes detailed full-packet analysis.

Despite continual improvements, the user interface remains below par compared to leading NPMD vendors, based on Gartner's analysis.

Flowmon's focus on both security and performance buyers may hinder its ability to keep pace with NPMD market shifts.

InfoVista

With worldwide headquarters in Massy, France, InfoVista is a communications service provider (CSP) and large-enterprise-focused NPMD provider, and is owned by private equity firm Apax Partners. InfoVista's offerings span NPMD, wireless network design and planning, and mobile network optimization.

Product offerings focused on NPMD include VistaInsight for Networks, which includes the Vista360 UI for visualization across the interrelated components of the suite. Those components are 5View Service Data Manager for data aggregation and analysis of the raw metric data, which feeds up to VistaInsight for Networks; 5View NetFlow appliances for flow collection; and 5View Applications appliances, which provide deep packet inspection capabilities. The final module is 5View Mediation, which collects data from appliances doing packet and flow analysis for long-term, analytical reporting purposes.

In February 2017, InfoVista launched VistaGO, a cloud-based managed service offering, targeted at small companies, mainly CSPs and MNOs, to provide customer-facing performance visibility. The acquisition of TEMS from October 2016 provides InfoVista with the ability for enhancing active testing of wireless services. In November 2017, the vendor announced the launch of end-to-end transport (Xhaul) QoS over its NFV-based network, including centralized RAN (C-RAN) assurance for its VistaInsight platform.

The vendor recently announced new hires in sales leadership positions. A chief sales officer to oversee global sales was announced in August 2017, and two other regional sales heads, focusing on Americas and Europe, were both announced in November 2017.

InfoVista declined the opportunity to provide a product demonstration as part of the research process that was offered to participating vendors for this research. Gartner's analysis for this vendor is based on other credible sources, including a completed vendor survey response, previous vendor briefings and interactions, the vendor's own marketing collateral, public information and discussions with end users.

InfoVista's NPMD revenue is estimated to be between $26 million and $50 million per year.

STRENGTHS

- The launch of VistaGO eases implementation and maintenance costs while also improving ease of use, to address one of the major challenges toward adoption.
- InfoVista shows a robust focus for the CSP and MNO use cases, with a well-rounded portfolio that extends from the network to customer-centric equipment performance.
- Extensibility of the InfoVista solution and recent product enhancements in radio, optical networks and NFV allow it to meet existing and emerging sophisticated use cases that many other vendors cannot meet.

CAUTIONS

- Integration of the TEMS business from an acquisition in 2016 remains a major focus area and may distract from enterprise-focused NPMD development.
- End users continue to report higher-than-average implementation and maintenance costs, including extended service engagements and challenges with upgrades.
- InfoVista's user interface is dated, with multiple workflows between the various components of its NPMD solution.

Ipswitch

Ipswitch, based in Burlington, Massachusetts, supports a large client base with its product WhatsUp Gold 2017 Plus, which is an on-premises software offering. The monitoring solution comes in four editions — Basic, Pro, Total or Total Plus — reflecting different assortments of modules, with the Network Traffic Analysis module offered under the Total and Total Plus editions.

The product provides a simple and easy-to-use networking monitoring solution, combining both SNMP-based infrastructure health and availability monitoring with the collection and reporting of flow data. Packet data is handled via a packet-to-flow converter agent called Flow Publisher. Product enhancements in July 2017 include support for cloud monitoring, mainly AWS and Azure. WhatsUp Gold also includes support for real-time performance monitors and EMC Unity storage, which aligns with the vendor's roadmap. Planned enhancements include support for SaaS monitoring, including Microsoft Office 365.

Ipswitch has the majority of its customer base situated in North America. The vendor is focused on expanding its market share through broader support for IT infrastructure monitoring, including increased support for storage, cloud and IoT monitoring. It has added a senior leadership position for exploring business development through partnerships with managed service providers (MSPs).

Ipswitch's NPMD revenue is estimated to be between $26 million and $50 million per year.

STRENGTHS

Ipswitch offers a low-cost and easy-to-license NPMD solution.

The vendor's low-friction sales model, with a "try and buy" option, is optimal for small and midsize business (SMB) organizations.

The vendor has a good roadmap to align with some pressing challenges of a modern IT infrastructure, including hybrid cloud.

CAUTIONS

Ipswitch does not have deep packet inspection capabilities.

Scalability and granularity of data are below the level of leading NPMD solutions.

Despite its many years in the market, Ipswitch suffers from less market awareness when compared to similar NPMD vendors.

LiveAction

LiveAction is a privately owned company, founded in 2007 and headquartered in Palo Alto, California. LiveAction's LiveNX product is focused on visibility and analytics to help simplify network management. Additionally, LiveAction's LiveSensor module provides packet analysis and performance metrics collection for network elements that do not export NetFlow records. A LiveAgent component allows for the transmission of KPI data from endpoints and servers.

For 2017, LiveAction consolidated its NPMD offering by incorporating the previously separate product of LiveUX as a capability of LiveNX. This was supplemented with LiveNCA delivering configuration automation and LiveInsight providing machine learning capabilities. Endpoint monitoring is made available with LiveAgent. Product development cadence continues to be healthy, with significant updates in April 2017 and July 2017. The April release included simplified workflows for SD-WAN troubleshooting, integration with Cisco APIC-EM and Viptela, support for

cloud licensing with monthly usage, and billing for large MSP deployments. The July release saw the launch of LiveAction's machine-learning-driven analytics and an expansion of device support to 107 networking vendors. The most recent version of LiveNX was delivered in November 2017, and included a publisher/subscriber API, a ServiceNow app, support for Viptela BFD and further developments to the analytics capabilities launched earlier in the year. Note that this version was launched after Gartner's analysis for this report, and therefore was not factored into LiveAction's Magic Quadrant placement.

Aside from product development, over the last 12 months LiveAction has invested in expansion of its EMEA sales and support teams, and its in-house marketing team, with a new VP of marketing, two new directors and additional resources hired. This has resulted in a new website that was launched in 4Q17; joint events with technology partners, such as Cisco, Corvil, FireMon, Palo Alto Networks and Presidio; and an active social media presence that has a substantial following. The overall primary route to market for LiveAction is through channel sales.

LiveAction's NPMD revenue is estimated to be between $11 million and $25 million per year.

STRENGTHS

- Customers report high satisfaction with product capabilities, service and support offered.
- Collaboration with third-party vendors such as Cisco, PagerDuty, ServiceNow and Splunk, is well-coordinated and cohesive.
- LiveAction has had strong growth over the last two years with a significant ramp-up of customers and the total installed base, partially driven by Cisco channel sales.

CAUTIONS

- In-house resources are almost exclusively focused on the North American region. Customers from other regions should ensure the reseller resources made available are adequate and sufficiently skilled to provide ongoing support.
- The vendor's heavy focus toward supporting Cisco infrastructure may inhibit opportunities where there is a requirement to manage a more heterogeneous environment.
- LiveAction is frequently cited by end users as offering a premium-priced solution.

ManageEngine

Founded in 1999 and headquartered in Pleasanton, California, ManageEngine offers a low-cost and simple NPMD solution, with a focus on infrastructure monitoring for small and midmarket enterprises. ManageEngine has a substantial portfolio and customer base, with thousands of installations worldwide. ManageEngine is new to the NPMD Magic Quadrant this year.

ManageEngine's OpManager is an integrated network management platform that provides network performance monitoring, physical and virtual server monitoring, and flow-based bandwidth analysis. Deep packet inspection (DPI) was added as a capability in February 2017, then later fully incorporated into the new release, OpManager Plus, in August 2017.

From a commercial perspective, ManageEngine has focused on global expansion by recently appointing its first Australia and New Zealand (ANZ) regional manager in February 2017. In September 2017, ManageEngine revamped its Brazilian website and partner strategy to aid services and support for the region. ManageEngine has a strategy of monthly seminars and workshops on a country level to ensure regular customer feedback and engagement.

ManageEngine's NPMD revenue is estimated to be between $26 million and $50 million per year.

STRENGTHS

Ancillary tools beyond NPMD provide useful complementary capabilities, including APM, IP Address Management (IPAM), service desk, log monitoring and security compliance capabilities.

End-user surveys cite satisfaction with ManageEngine's cost and ease of maintenance.

ManageEngine's tight packaging of a wide variety of IT operations capabilities into a single package offers total cost of ownership (TCO) savings for its end users.

CAUTIONS

ManageEngine's software-only solution limits scalability compared with hardware-based solutions.

While the vendor offers basic packet monitoring, this capability is below par compared to equivalent offerings from the leading NPMD vendors.

End users cite user interface, workflow and navigation as areas for improvement.

Micro Focus (HPE)

Micro Focus' NPMD solution, through the acquisition of HPE's NPMD products, represents one of the first enterprise network monitoring tools. Based in Newbury, United Kingdom, Micro Focus has a substantial portfolio and customer base, with thousands of installations worldwide.

Micro Focus' NPMD solution is composed of Network Node Manager i (NNMi) and Real User Monitoring (RUM). Micro Focus gained ownership of these products in the September 2016 HPE spin-off/merger of its software business with Micro Focus, as part of an $8.8 billion deal. NNMi provides a consolidated view of fault and performance data, while RUM monitors actual user interaction with a website or application from client desktops and mobile devices.

NNMi's most recent update was released in June 2017. The new version delivers support for Border Gateway Protocol (BGP) session monitoring and reporting, including BGP-based Virtual Private LAN Services (VPLS), and MPLS discovery and monitoring for Draft Kompella. Scalability was also improved with this release. The latest RUM version was released in September 2017 and delivered more flexible deployment options, performance improvements, VXLAN support, enhanced reporting and support for IBM Message Queue (MQ) v.8.0.

Micro Focus did not respond to requests for supplemental information and/or engage in Gartner's standard procedures to address the contents of this document. Gartner's analysis for this vendor is therefore based on other credible sources, including previous vendor briefings and interactions, the vendor's own marketing collateral, public information, and discussions with end users that have either evaluated or deployed each NPMD product.

Micro Focus' NPMD revenue is estimated to be between $101 million and $250 million per year.

STRENGTHS

Micro Focus offers a broad portfolio of complementary availability and performance monitoring products, with integration with products such as Micro Focus (HPE) Network Automation.

The vendor's channel partner program and professional services resources have a global presence.

Opportunities are available to utilize existing operations analytics and UCM capabilities that reside in Micro Focus' broader IT operations portfolio.

CAUTIONS

With ongoing organizational changes, customers continue to express concern over Micro Focus' direction and vision in the NPMD space, with others unaware that the NPMD products' ownership is now under Micro Focus.

Planned 2017 features for a number of OpenStack integrations and plug-ins have not yet been delivered, and have been deprioritized in favor of other customer requirements.

End users report that implementation, training and professional services account for a greater proportion of total Micro Focus NPMD deployment costs than observed by Gartner for other vendors.

NETSCOUT

NETSCOUT, based in Westford, Massachusetts, has been in the network performance monitoring space for 30 years. With a large and loyal customer base, NETSCOUT has the largest market share in the NPMD space. NETSCOUT's focus is selling its hardware-centric packet analysis solutions to customers in the large enterprise, service provider and public sector industry verticals.

NETSCOUT's enterprise NPMD solution consists of the nGeniusONE platform, InfiniStream platform, nGeniusPULSE and TruView. NETSCOUT's service assurance platform is nGeniusONE, which provides service dashboards and analysis. It also integrates with the InfiniStream platform, which gathers and stores traffic data from the network, and enables troubleshooting and forensic workflows. The nGeniusPULSE platform provides synthetic testing focused on verifying the

performance of cloud applications. Finally, the TruView appliance provides unified network performance management with application awareness, and overlaps somewhat with nGeniusONE.

New to NETSCOUT's product suite are vSTREAM and vSCOUT, which provide software-based instrumentation of traffic data primarily for hybrid cloud environments, and extend NETSCOUT's traditional data center hardware solution into the cloud. Supplementing their NPMD products, NETSCOUT also has solutions in the network packet broker and security analytics space. NETSCOUT's new InfiniStreamNG (ISNG) offering is a first step in integrating security analytics with NPMD, and provides a common data platform for both network and security teams.

NETSCOUT did not respond to requests for supplemental information and/or engage in Gartner's standard procedures to address the contents of this document. Gartner's analysis for this vendor is therefore based on other credible sources, including previous vendor briefings and interactions, the vendor's own marketing collateral, public information, and discussions with end users that either have evaluated or deployed each NPMD product. NETSCOUT filed a lawsuit against Gartner over the content of the 2014 NPMD Magic Quadrant. The court dismissed the lawsuit, and NETSCOUT has appealed the court's ruling.

NETSCOUT's NPMD revenue is estimated to be between $500 million and $750 million per year.

STRENGTHS

- NETSCOUT's strategy for cloud visibility, with vSCOUT, vSTREAM and nGeniusPULSE, is more complete than many of its NPMD competitors.
- NETSCOUT's ISNG initiative to provide a common data platform for network and security teams is a welcome progression to unify two typically siloed organizations.
- NETSCOUT is the only NPMD vendor to offer its own network packet broker, allowing end users to source a single vendor for packet capture and analysis requirements.

CAUTIONS

- NETSCOUT has limited capabilities for NPMD buyers looking for deep application visibility and workflows that cater to the LOB.
- Gartner continues to observe end-user confusion (through client inquiries and one-on-one meetings at Gartner events) regarding NETSCOUT's future plans for the TruView product line.
- NETSCOUT's premium pricing for its hardware-centric solutions impedes deeper penetration into the broad enterprise market, including the midmarket and SMBs.

New H3C Group

Headquartered in Hangzhou, Zhejiang Province in China, New H3C Group (a joint venture between Unisplendour and HPE) is an IT infrastructure solution provider and makes its debut in the 2018 NPMD Magic Quadrant.

H3C's NPMD solution is its Intelligent Management Center (iMC), which is an on-premises software offering. The standard edition includes an embedded database, which has a hard limit on the amount of equipment monitored, while the professional edition is deployed with an external database. The last major release of the iMC product was in November 2016, with monthly cycles of minor version releases.

H3C is the exclusive provider of HPE-branded servers and storage in China, and it sells NPMD overseas through HPE's channel. Through the use of SQL, Windows Management Instrumentation (WMI) and PowerShell, iMC's monitoring capabilities go beyond the network interfaces to include database and server monitoring.

Sales are mainly through channel partners, with a very strong regional focus in the APAC market. Government and energy verticals form a major segment of H3C's customers, a significant majority of which are based in China. A small percentage of its customers is spread across North America, EMEA and Latin America.

H3C's NPMD revenue is estimated to be between $26 million and $50 million per year.

STRENGTHS

- H3C combines infrastructure monitoring and network monitoring to provide a broad service delivery monitoring capability, including the ability for unified communications monitoring.
- H3C leverages the multiple channel partners from its IT infrastructure solutions offerings for selling its NPMD products.
- H3Cs enablement of its upsell strategy of NPMD tooling in China is strengthened by being the sole provider of HPE-branded server and storage products for this region.

CAUTIONS

- The user interface of the NPMD product is not as sophisticated as the leading UIs in this space, and requires comprehensive training and guidance for users.
- H3C has not partnered with technology providers for its NPMD solution.
- H3C has been quite heavily focused on APAC region, mainly China. Given that its sales model is entirely through channel partners, expanding into other regions will be a major challenge due to limited support outside the local market.

Paessler

Based in Nuremberg, Germany, Paessler focuses on infrastructure monitoring software to meet the needs of the midmarket and SMBs through its PRTG Network Monitor offering. The solution covers monitoring of network elements for fault, flow analysis and packet sniffing in a single, simple solution. Additionally, the product supports monitoring of application instances, servers and virtual environments.

The vendor continues to prioritize simplified ease of use and transparent licensing. In October 2017, Paessler announced a SaaS-hosted version of PRTG. In keeping with the regular cadence of releasing new sensors, Paessler has added a sensor for Buffalo storage. The vendor is focusing on performance improvements for the monitoring platform, including performance improvements for some of its existing protocol-based monitoring capabilities.

Aside from product development, Paessler has expanded its presence outside of its home EMEA geography. Paessler founded a new partner alliance program in 2017 with leading technology providers. One of the focus areas is on integration between PRTG and the other vendors' products, as well as co-marketing and co-selling. The addition of monitoring as a hosted service enables Paessler to target a new class of customers that includes some smaller enterprises, enterprises that have a "cloud first" policy and website operators.

Paessler's NPMD revenue is estimated to be between $26 million and $50 million per year.

STRENGTHS

Paessler has a simple licensing model, and the on-premises version provides ease of implementation and upgrade.

The recently announced cloud version enables Paessler to expand its addressable market by tapping into a broader class of customers.

Paessler's rapid development stream means that new and updated sensors are released frequently — on a quarterly basis.

CAUTIONS

Paessler targets midmarket enterprises and SMBs, and is limited in its ability to meet specific large-enterprise scaling requirements.

The packet sniffer and flow modules have limited capabilities, including an inability to save data to disk for historical analysis.

The vendor has had to postpone the development of some roadmap items. This is likely one of the contributing reasons that end users surveyed by Gartner evaluate Paessler's commitment to delivering on requested enhancements as lower than other vendors in this space.

Riverbed

Riverbed, founded in 2002 and headquartered in San Francisco, California, has assembled a set of NPMD capabilities through acquisition, alongside its core WAN acceleration and SD WAN business. Riverbed couples its NPMD offering with APM and endpoint monitoring to offer a broad solution.

The suite, branded as SteelCentral Network Performance Management (NPM), includes several appliance lines and software components that support network data collection, storage and analytics. SteelCentral NPM is headlined by NetProfiler for flow analysis and AppResponse for packet analysis. These capabilities are supplemented by SteelCentral Packet Analyzer Plus,

Transaction Analyzer, NetIM (formerly NetSensor) and UCExpert, which provide additional capability for packet trace analysis, infrastructure monitoring and UC monitoring, respectively. SteelCentral Portal provides a common visualization and analytics framework for the entire SteelCentral line. Recently added SteelCentral Aternity is an agent-based endpoint monitoring capability focused on monitoring cloud-hosted applications from users' desktops.

Riverbed has focused its efforts on rationalizing and integrating its toolset, with expanding Portal integrations and merging the NetShark and AppResponse under the AppResponse name. It has also centered on the digital experience management theme, by integrating Aternity use cases into common NPMD workflows. Riverbed has also released a 40 Gbps appliance with the AppResponse 8170, which allows customer to instrument networks with higher data rates. It has improved its data analysis and visualizations in its NPMD solution with TruePlot Analytics. Riverbed has also started to target the service provider market with the Service Delivery Platform.

In December, 2017, Riverbed acquired security analytics vendor FlowTraq, with the intention to integrate its capabilities with its flow-based monitoring in NetProfiler. This acquisition was not factored into the research.

Riverbed's NPMD revenue is estimated to be between $100 million and $250 million per year.

STRENGTHS

- Integration with Riverbed's SD-WAN solution SteelConnect, coupled with path analytics and configuration management capabilities, is a differentiator for buyers looking for a unified solution.
- End-user survey results point to high satisfaction with Riverbed's ability to do contextual drill-down and troubleshooting.
- Riverbed's improved marketing and social media programs have helped highlight NPMD capabilities beyond WAN optimization.

CAUTIONS

- Riverbed must continue to improve its NPMD strategy to solve the visibility gaps created by the cloud.
- The vendor's cadence of new feature development lags behind those of other NPMD vendors.
- Riverbed's ability to drive value from SteelConnect and SteelCentral integration is limited by the highly competitive and rapidly consolidating SD-WAN market, in which Riverbed has lagged behind its competitors.

Savvius

Based in Walnut Creek, California, Savvius' NPMD products include Omnipliance (for capture, storage and packet analysis), Omnipeek (for analytics), Savvius Spotlight Appliance (for network monitoring) and Savvius Insight (hardware device for edge compute scenarios). The solutions are

on-premises offerings suited for midsize enterprises. Savvius is new to the NPMD Magic Quadrant this year.

Savvius primarily focuses on packet capture for network monitoring, and has different hardware appliance models depending on the volume of network transactions. Network forensics have been a focus area for Savvius through its Omnipeek offering. From a packet capture perspective, it currently has an upper limit of 20 Gbps.

Over the past 15 months, the vendor has seen some leadership changes in sales, including hiring a vice president for worldwide sales, and heads of sales for both APAC and Europe.

Approximately half of Savvius' customers are in North America, followed by APAC and EMEA, with a small fraction in Latin America. In July 2017, it announced an agreement with inTechnology Distribution, a technology distributor for ANZ, as part of its overall channel partner strategy. The roadmap for Savvius includes enhancing its analytics capability and focusing on virtualization toward extending visibility to public and private cloud.

Savvius' NPMD revenue is estimated to be between $10 million and $25 million per year.

STRENGTHS

- Savvius provides a highly scalable solution based on packet analysis, employing dedicated solutions for data capture, analysis and visualization to ensure performance of the platform.
- Savvius has good partnership ecosystem across technology providers, including network packet brokers, to ensure a wide range of sources to route packets to Savvius' tools.
- The vendor offers differentiation with its ability to provide highly scalable packet capture at a competitive price point.

CAUTIONS

- The vendor's Omnipeek UI is not web-based and is in need of modernization.
- Savvius has limited support for flow data, relying on packet streams to create a flow or add to an existing flow, which can be costly as compared to products that capture flow data for certain noncritical network segments.
- The analytics capability is limited compared to other vendors, and is almost exclusively based on network packets.

SevOne

Headquartered in Boston, Massachusetts, SevOne focuses on network and infrastructure monitoring, complemented with capabilities for log monitoring. SevOne markets primarily to the large enterprise and service provider markets, based on its scalability and a flexible distributed architecture.

The vendor announced release of the SevOne Data Platform in September 2017 and it refers to its solutions as part of the new offerings. The SevOne Data Platform consists of integrated products, including SevOne NMS Cluster, SevOne Data Insight and SevOne Data Bus. SevOne User Experience is a SaaS offering based on a resell from AppNeta. SevOne Data Insight enables real-time visualizations and shareable reports, whereas SevOne Data Bus enables sharing of real-time data with third-party applications, including business intelligence systems. The SevOne Data Platform and its three components supersede the legacy products, namely the SevOne Platform and SevOne RetinaVu. The SevOne platform consisted of SevOne Performance Appliance Solution (PAS), Dedicated NetFlow Collector (DNC) and Performance Log Appliance (PLA).

SevOne had seen significant layoffs in 2016, in addition to the resignation of its two founders. The vendor seems to have renewed its focus on its technology and product strategy. Over the past 12 months, it has pivoted to focusing on software-defined and cloud-centric architectures. A new chief revenue officer and CTO were hired in 2017, while its co-founder and prior CTO transitioned to serving solely as a board member.

A majority of SevOne customers are in North America, followed by EMEA and APAC. The vendor mainly sells products and professional services directly to large enterprises, CSPs and MSPs, complemented with multiple regional partners. Expanding the number of its strategic partners over the past 12 months, SevOne has added Verizon Enterprise Solutions to its list.

SevOne's NPMD revenue is estimated to be between $51 million and $100 million per year.

STRENGTHS

SevOne integrates metric, flow and log data into an enterprise-class, carrier-grade platform, with one-second polling granularity.

SevOne has renewed its focus with a well-defined strategy toward product and technology focus areas.

The vendor has a regular cadence of upgrades across its NPMD product portfolio, with a focus on SDN and NFV over the past couple of releases.

CAUTIONS

SevOne is very focused as an ITIM tool, with drill-downs into flow or log data, but is missing workflows derived from more holistic network performance monitoring based on packet data.

SevOne's continued focus on large enterprises and communications service providers puts its solution out of reach of the broader NPMD buying market.

End users have expressed concerns about SevOne's ease of implementation and upgrading.

SolarWinds

Founded in 1999 and headquartered in Austin, Texas, SolarWinds offers a low-cost and simple NPMD solution that also meet the needs of ITIM requirements for small and midmarket enterprises. SolarWinds has a substantial portfolio and customer base, with thousands of

installations worldwide.

In June 2017, SolarWinds released Network Operations Manager (NOM). This is a new product that combines the features and functionality of SolarWinds' previous NPMD offerings of Network Performance Monitor (NPM), NetFlow Traffic Analyzer (NTA), VoIP and Network Quality Manager (VNQM), NetPath, PerfStack and User Device Tracker (UDT). NOM also includes some enhancements specific to the new platform — for example, a single install and upgrade process, and node-based licensing. In addition to NOM, SolarWinds provides its Quality of Experience (QoE) software agents for packet monitoring.

SolarWinds' appointment of a new executive VP of products and a new CTO at the beginning of 2016 is now yielding results, as an increase in engineering investment and process improvement has been observed, with a priority for the network management portfolio in particular. Following on from the 2016 senior management appointments, a new CMO and two new senior VPs for North American sales and international sales, respectively, were announced in February 2017. SolarWinds relies on an inside sales model that focuses on digital marketing, and offers no professional services.

SolarWinds' NPMD revenue is estimated to be between $250 million and $500 million per year.

STRENGTHS

Ancillary tools beyond NPMD provide useful complementary capabilities, including topology mapping, network configuration management and APM capabilities.

SolarWinds hosts a substantial and active user community, called Thwack, consisting of over 130,000 IT professionals.

NOM provides a consolidated NPMD offering and is targeted to appeal to larger deployments than its predecessor.

CAUTIONS

SolarWinds has a limited focus on introducing cutting-edge new features, specifically in the area of network root cause analytics.

The vendor's software-only solution limits scalability compared with hardware-based solutions.

While the vendor offers basic packet monitoring through its QoE agents, this feature is not used or known by much of its customer base, nor has it seen significant investment from SolarWinds.

Statseeker

Headquartered in San Diego, California, Statseeker makes its debut in the Magic Quadrant this year. Targeted at small to midsize enterprises, Statseeker is an on-premises software offering, primarily focusing on SNMP, syslog and flow as main data sources for NPMD.

Statseeker offers basic NPMD capabilities with graphs for tracking performance across multiple devices, including visual comparison across devices. The tool uses syslog for log reporting, whereas packet-level monitoring is enabled through a Statseeker module. The vendor has historically focused on the education, banking, financial services and insurance (BFSI) and retail verticals. It has a majority of its deployments in North America, with some presence in APAC and EMEA.

Statseeker has a regular cadence of product upgrades. Over the past 12 months, it has released three major versions of its product. The main theme across these upgrades are support for cloud deployments and APIs for access to additional data. The latest release in November 2017 extends support for deployment of Statseeker to Azure and OpenStack environments, in addition to AWS.

Statseeker predominantly works with IT MSP channel partners for sales and support. From a technology perspective, it has partnered with some major network equipment manufacturers and security information and event management (SIEM) providers. Along those lines, it announced Plixer as a technology partner in April 2017.

Statseeker's NPMD revenue is estimated to be between $5 million and $10 million per year.

STRENGTHS

Statseeker provides a lean and simple tool that reduces the complexity for an IT operations team, easing implementation and maintenance of the tool.

Statseeker performs at scale, which includes capturing data in all discovered network interfaces every 60 seconds and visualization in real time.

The vendor shows high renewal rates when compared with some of the other NPMD vendors.

CAUTIONS

The UI is dated, with limited analytics capability, mostly relying on IT operators to perform any kind of analysis.

The current focus and roadmap do not adequately target the changing and expanding roles that leverage NPMD solutions.

Statseeker's marketing presence is behind that of other competitors, with very limited product management and marketing resources.

VIAVI Solutions

VIAVI Solutions is headquartered in Milpitas, California, and is one-half of the entity previously known as JDSU. The VIAVI NPMD solution is based on heritage technology that was obtained during the acquisition of Network Instruments in 2014. This forms part of the enterprise and cloud performance management business unit that is headquartered in Minneapolis, Minnesota.

The current VIAVI NPMD solution set consists of the Observer Performance Management Platform, which includes Observer Apex, Observer Analyzer, ObserverLIVE, Observer Management Server (OMS), Observer GigaStor, Observer Probes and Observer SightOps. SightOps is an OEM arrangement with ScienceLogic that replaced Observer Infrastructure in 2016, and is aimed at extending the VIAVI polling-based monitoring into hybrid environments. ObserverLIVE is a new SaaS-based synthetic monitoring solution suitable for remote monitoring of cloud workloads.

For 2017, the primary development themes have been to improve application awareness and troubleshooting, deliver a simplified and consistent UI to aid user experience, and increase network utilization rates and network speeds by shortening time to resolution for IT and network operations teams.

VIAVI's appointment of a new VP and general manager for the enterprise and cloud business unit in mid-2016, alongside several additional senior executives, is now yielding results with the delivery of two major releases in 2017 and a burgeoning product roadmap. In addition, the VIAVI three-tier Velocity channel program, which was rolled out in late 2016, is now fully implemented and provides several online tools to enable partners. In 2017, a Salesforce business planning portal was added to that list of tools.

VIAVI NPMD revenue is estimated to be between $100 million and $250 million per year.

STRENGTHS

The packet capture and inspection capability (via GigaStor) continues to be well-regarded by VIAVI clients, with in-house-designed packet capture hardware.

SightOps and ObserverLIVE address the visibility challenge created by hybrid IT by combining cloud infrastructure monitoring with NPMD workflows.

Overhauled UI and navigation based upon a "three steps to resolution" workflow align well with diagnostics and troubleshooting scenarios.

CAUTIONS

VIAVI suffers from poor name recognition among the NPMD customer base, having gone through two name changes over the last few years.

VIAVI's primary corporate focus in the service provider vertical contrasts with Observer's enterprise user base, and must continue to be aligned to find synergies across these business units.

Large enterprise customers have started raising concerns over the last 12 months around the cost of implementation and maintenance of their NPMD solutions.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant 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.

Added

- Colasoft
- ManageEngine
- Micro Focus (HPE)
- New H3C Group
- Performance Vision
- Savvius
- Statseeker

Dropped

- HPE — The NPMD suite formerly associated with Hewlett Packard Enterprise (HPE) was evaluated under the "Micro Focus (HPE)" label following the acquisition of HPE's software assets by the U.K.-based firm.
- Genie Networks — Focus is on security workflows and use cases.

Inclusion and Exclusion Criteria

Product-Related Criteria

Vendors are required to meet the following criteria to be considered for the 2017 NPMD Magic Quadrant and Critical Capabilities research:

- 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. This includes cloud-hosted and wireless endpoints.
  - Network components — Routers, switches and other network devices. This includes SDN and NFV components.
  - Network links — Connectivity between network-attached infrastructure.
- 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 application performance monitoring 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.

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 algorithmic IT operations (AIOps) technologies — The ability to distill and create actionable advice from the large dataset collected across the various data sources.

Leverage the following data sources:

Network-device-generated traffic data, including flow-based data sources inclusive of NetFlow and IPFIX.

Network-device-generated health data.

Network packet analysis to identify application types and performance characteristics.

The ability to support the following scalability and performance requirements:

Real-time monitoring of 10G Ethernet networks at full line rate.

Ingesting of sampled flow records at a rate of 75,000 flows per second via a single instance of the product.

Non-Product-Related Criteria

Total NPMD product revenue (including new licenses, updates, maintenance, subscriptions, SaaS, hosting and technical support) must have exceeded $7.5 million for 3Q16 through 2Q17, excluding revenue derived from security-related buying centers.

The vendor must have at least 75 customers that use its NPMD product actively in a production environment.

The vendor must have at least 10 customers located in at least two of the following geographic locations: North America, Latin America, EMEA and/or APAC that use its NPMD product actively in a production environment.

Honorable Mentions

The following sample vendors were unable to meet the inclusion criteria to be included in this research, but do come up in NPMD-related inquiries:

- Dynatrace
- Empirix
- Endace
- FixStream
- Kentik
- LogicMonitor
- Microsoft
- NETIS SYSTEMS
- Nyansa
- Splunk
- ThousandEyes

Evaluation Criteria

Ability to Execute

Please note that none of the weightings on any of the evaluation criteria have changed since the 2017 Magic Quadrant.

Product or Service: Gartner makes judgments from a variety of inputs to evaluate the capabilities, quality, usability, integration and feature set of the solution, including the following functions:

- Data source support, including application visibility
- Analytics
- Diagnostic workflows
- Real-time monitoring
- Day-to-day maintenance and management of the product
- Ease and simplicity of deployment and configuration
- Ease of use and richness of functions within the product
- Product deployment options and usability

Overall Viability: 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/Record: We evaluate the execution in delivering and upgrading products consistently, in a timely fashion, and meeting roadmap 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.

Operations: We evaluate the ability of the organization to meet goals and commitments. Factors include quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	
Product or Service	
Weighting	
	High
Overall Viability	
Weighting	
	High

Sales Execution/Pricing	
Weighting	
	Medium
Market Responsiveness/Record	
Weighting	
	High
Marketing Execution	
Weighting	
	Medium
Customer Experience	
Weighting	
	High
Operations	
Weighting	
	Not Rated

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	
Product or Service	

Weighting	High
Overall Viability	
Weighting	High
Sales Execution/Pricing	
Weighting	Medium
Market Responsiveness/Record	
Weighting	High
Marketing Execution	
Weighting	Medium
Customer Experience	
Weighting	High
Operations	
Weighting	Not Rated

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	
Product or Service	
Weighting	High
Overall Viability	
Weighting	High

Sales Execution/Pricing	
Weighting	Medium
Market Responsiveness/Record	
Weighting	High
Marketing Execution	
Weighting	Medium
Customer Experience	
Weighting	High
Operations	
Weighting	Not Rated

Source: Gartner (February 2018)

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 visibility

Analytics

Diagnostic workflows

Real-time monitoring

Virtualization (NFV and SDN)

Hybrid IT support

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, tradeshows, 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	
Market Understanding	
Weighting	
	High
Marketing Strategy	
Weighting	
	Medium
Sales Strategy	
Weighting	

	Medium
Offering (Product) Strategy	
Weighting	
	High
Business Model	
Weighting	
	Low
Vertical/Industry Strategy	
Weighting	
	Low
Innovation	
Weighting	
	High
Geographic Strategy	
Weighting	
	Low

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria

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

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria
Market Understanding

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

Source: Gartner (February 2018)

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 broad sets of data inputs and analytics techniques. They offer a choice of hardware or software appliances for optimum

flexibility, while making formerly premium-priced NPMD solutions attainable to the broader market. All Leaders offer a high degree of application-aware insight and visibility, along with advanced troubleshooting and diagnostics workflows.

Challengers

Challengers typically consist of those vendors with high market reach and large deployments. Stalwarts in the network performance monitoring and diagnostics market, they are currently striving to deal with new technical demands and rising expectations. These established NPMD vendors generally 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.

Visionaries

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

Niche Players

Niche Players are those vendors 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.

Context

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

As part of the Magic Quadrant research process, Gartner conducts a survey of NPMD end users, supplied as references by the vendors listed in this research. This year's survey included 152 respondents from enterprises across a broad array of industries and company sizes, and included a number of findings:

- The end-user survey shows only modest growth in the use of packet analysis, reinforced by several major packet monitoring vendors reporting slowing new customer growth.

The same survey showed that 35% of the end users of NPMD solutions were outside of infrastructure and operations, with a large segment listing themselves as enterprise architects. This underscores a greater trend that NPMD tools not only are used by network teams, but also are leveraged across the IT organization, and sometimes even by the line of business.

Regarding future investment in NPMD, 43% of respondents reportedly will be increasing investment, 50% will have no change and 7% will be decreasing investment.

When asked to name other vendors considered in NPMD buying decisions, end users from the survey listed the following vendors most often: SolarWinds, NETSCOUT, Cisco and Riverbed.

Just over one-third of end-user survey respondents reported using their NPMD solutions for security analytics (34%), an increase from the 29% reported in 2017. A number of NPMD vendors have pivoted strongly toward security operations workflows, citing the growing synergy between NetOps and SecOps (see "Align NetOps and SecOps Tool Objectives With Shared Use Cases").

Product functionality, product roadmap and cost were the top three factors driving NPMD buying decisions.

The top three use cases for NPMD solutions were real-time diagnostics, real-time monitoring and alerting, and historical analysis for capacity planning.

Increasing overlaps with IT infrastructure monitoring, APM and AIOps tools are impacting buying decisions. As an example, Splunk was considered as an alternative NPMD vendor for 20% of end users surveyed.

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

Several large NPMD vendors have undergone reorganizations in order to align various monitoring assets, often those acquired via acquisition.

Normalization of UI and workflows across several vendor's toolsets has shown increasing progress.

Ease of use remains an area that needs improvement, and it varies significantly both across vendors and within solutions.

Existing support for monitoring cloud and hybrid IT environments remains limited, but this is increasingly appearing on vendor roadmaps. Infrastructure as a service (IaaS) providers and, more specifically, Microsoft Azure have introduced their own NPMD solutions — in the latter case, in the form of Network Watcher, which is focused exclusively on network monitoring within the Azure environment.

Path analytics, as part of a cloud monitoring strategy, has seen some investment from NPMD vendors, while stand-alone vendors such as ThousandEyes have emerged in this space.

Vendors have increasingly begun to leverage big data back ends or have built operational analytics overlays to facilitate data analytics across all captured data.

NPMD solutions have a primary data source (infrastructure metric, flow or packet), and have a difficult time leveraging the benefits of each data source for the maximum value to the user.

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. 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 IT operations assess its current state of maturity on a regular basis, both individually and at the organizational level, to provide this perspective.

I&O leaders should not utilize the Leaders quadrant as a shortlist of appropriate vendors, but instead should build a list of criteria describing their current and future needs, and then select from vendors that best meet those requirements (see "Critical Capabilities for Network Performance Monitoring and Diagnostics"). They 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.

Market Overview

NPMD: A Tale of Two Cities

Over the past year, we have increasingly seen the NPMD vendor market split into two camps:

Those focused on polling-based infrastructure monitoring with basic flow and packet monitoring capabilities

Those focused on hardware-based deep packet analysis with basic infrastructure monitoring

While we had expected to see vendors moving toward bringing these two camps together into a single, holistic product offering, we have instead seen an NPMD vendor landscape that has crystallized. Broadly speaking, infrastructure monitoring vendors invest little in expanding flow and packet monitoring, while the packet monitoring vendors pay little heed to expanding their infrastructure monitoring capability. Instead, infrastructure-focused vendors invest primarily in broadening their device support and visualization, while packet vendors focus on improving scalability of their appliances and adding better analytics and packet inspection capabilities.

With some exceptions, several NPMD vendors focused on packet analysis have struggled to make packet monitoring consumable to the market. This has been exacerbated by increasing data center data rates, virtualization, cloud migration and encryption. At the same time, users of infrastructure-focused solutions report frustration in the inability to do root cause analysis without deeper monitoring, with some looking to AIOps solutions as a possible remedy. This has led to bloated, poorly integrated and expensive solutions that fail to match the needs of the buyer. To remedy some of this, a few alliances between infrastructure-focused vendors and packet-focused vendors have emerged, with VIAVI and ScienceLogic, ExtraHop and Cisco (Tetration), and LiveAction and Corvil all announcing partnerships.

NPMD vendors have had to contend with several key shifts in the environments they are attempting to monitor:

- Migration toward cloud-hosted workloads and applications fundamentally changing the flow of network traffic
- Increasing virtualization and the explosion of east-west traffic within the data center presenting a data-capture challenge
- Increasing encryption within the data center
- Exponential growth in application and infrastructure dynamism and complexity forcing network instrumentation as the key piece of the visibility puzzle
- 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
- Closer alignment between IT and the business, with an appreciation that network data can provide value through business intelligence

These shifts have begun to pressure network teams to rethink their tooling strategy. The goal today is to 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.

NPMD tools aim to provide the required breadth and depth of visibility in both real-time and historical perspectives by analyzing data from all three of the following techniques: device polling, flow-based technology and packet-based technology. Previous approaches that only take into account one or two of these data sources have proven to be inadequate, so all three must be supported for a tool to be considered an NPMD solution (see the Product-Related Criteria section).

Device Polling Technology

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 information about hardware or software errors (faults) and capacity data (for example, triggering an alert when a hardware fault occurs, or 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 and the overhead it may put on the devices being polled, especially if other tools are also polling. In most NPMD technologies, SNMP is used during troubleshooting to collect additional data, whereas in infrastructure monitoring, it's used more regularly to understand the health of the network devices. In addition to SNMP, the use of APIs as a polling data source is also a common technique to collect health data, and is often used for information from IaaS providers or SDN controllers.

While polling provides information on interface utilization and traffic, it is unable to provide a view into application and end-user usage patterns. To meet this need, consider solutions that provide flow- and packet-based technology.

Flow-Based Technology

Summarized data is generated by the network devices, including 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.

There are several flow collection standards, such as Cisco's NetFlow (v.5/v.9), Juniper Networks' J-Flow, Huawei's NetStream, Citrix's AppFlow, the Internet Engineering Task Force's (IETF's) Internet Protocol Flow Information Export (IPFIX, which is based on 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 record 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 architecture varies among network equipment vendors, but most tools collect and process the data regardless of the network equipment implementation. In addition, it can have a performance impact on the devices exporting flow data.

Flow-based data does not provide details down to a specific set of network packets going between the source and destination, nor does it provide any timing information about the conversation itself or the delay components. For this capability, users must consider packet-based technologies.

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, UC services (such as voice and video delivery) and the growing footprint of virtual desktop infrastructure (VDI) technologies. Because only raw, unmanipulated packet data is 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. Software-based packet capture capabilities have been introduced as cost-sensitive alternatives, but with obvious limitations in scalability and storage.

Analysis offered by packet-based technology is packet-timing-based, allowing vendors to identify sources of delay, measure user response time and ultimately pinpoint the root cause of performance problems. The packet analysis vendors range from those providing measurements from a TCP connection perspective to those reporting on timing on a TCP request/response basis. Other vendors move up the stack to measuring at the application layer, providing measurements from an application session perspective and a much closer representation to real end-user experience.

Through the years, these high-end proprietary packet analysis technologies have commoditized and moved into open source, with tools 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 ntop or Snort (intrusion detection). 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.

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.

Application Performance Monitoring

APM tracks the end-user performance of application components, and provides granular troubleshooting tools for the application and its components through server-based instrumentation. It provides this insight by monitoring three main functional dimensions: digital experience monitoring, application discovery, tracing and diagnostics and application analytics. APM differs from NPMD primarily in its focus on monitoring the quality of the end-user experience via application interactions across all application and infrastructure tiers, including (but not limited to) the network perspective. There are several vendors in the NPMD space that offer accompanying APM solutions, and several vendors offer integrated APM and NPMD solutions. See "Magic Quadrant for Application Performance Monitoring Suites" for further details.

IT Infrastructure Monitoring

IT infrastructure monitoring (ITIM) tools focus exclusively on monitoring the infrastructure topology composed of compute systems, storage, virtualization and network devices, using agent-based or agentless polling technologies, such as SNMP, Windows Management Instrumentation (WMI) or API integration-based data collection. These solutions focus on the availability and health of these systems, as opposed to the performance insight offered by APM and NPMD solutions. The difference between these tools and APM products is that they look at server-level metrics and processes, while also looking at the way servers interact with one another, versus living within the application logic and seeing the code execute. Unlike NPMD products, which cater to network professional use cases and speak in protocols and packet data that those buyers best understand, IT infrastructure monitoring products focus on IT operations generalists and often don't include support for packet- and flow-based technologies. These generalists need to determine which part of the infrastructure is contributing to poor performance, as well as understand the application's topology from an infrastructure perspective. Some ITIM tool vendors have moved partially into the NPMD space with the introduction of flow and packet support. Infrastructure monitoring should be supplemented by log analytics, NPMD and APM tooling to support complex troubleshooting and performance monitoring. See "Market Guide for IT Infrastructure Monitoring Tools" for more information.

Artificial Intelligence IT Operations Platforms

The coordinated deployment of AIOps technologies is used to discover complex patterns in high volumes of "noisy" IT data by providing a real, automated inference capability not available in most tools. These technologies include complex operations event processing (COEP), machine learning/statistical pattern discovery and recognition (ML/SPDR), unstructured text indexing search and inference (UTISI), topological analysis (TA), and multidimensional database search and analysis (MDSA).

IT operations' future as a big data analysis entity has been cemented by an exponential, continual growth of data (IT and business) generated by highly adaptive systems composed of large numbers of moving parts whose interactions are increasingly transient and complex. These

systems' behaviors cannot be characterized, much less managed, by inferring the behavior of the whole from the behavior of any individual part, necessitating the use of AIOps' advanced capabilities (see "Market Guide for AIOps Platforms" for more information).

Digital Experience Monitoring

Digital experience monitoring (DEM) is an availability and performance monitoring discipline that supports the optimization of the operational experience and behavior of a digital agent, human or machine, with the application and service portfolio of enterprises. This discipline also seeks to observe, model and manage the behavior of digital agent communities as they collectively engage with enterprise application and service portfolios. Several NPMD solutions provide DEM capabilities as part of their solution offerings (see "Innovation Insight for Digital Experience Monitoring"). Technologies used for DEM include synthetic monitoring, endpoint monitoring and JavaScript injection.

Network Packet Brokers

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 collaborate 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). Vendors such as NETSCOUT offer NPB solutions as part of their solution set. See "Market Guide for Network Packet Brokers" for further details.

Network Automation

Although traditionally focused on configuration and change of the physical network infrastructure, the desire to support emerging networking requirements has forced automation to take on a broader and more intrinsic role. While network configuration and change management (NCCM) technologies have been around for over a decade, new technologies have emerged to bring programmability, policy-based control and intent-based techniques into the networking arena.

There have been a number of approaches to network approaches beyond traditional NCCM. DevOps solutions like Red Hat's Ansible, traditionally focused on continuous configuration automation (CCA), have introduced network modules that allow those same playbooks to configure not only servers, but network instances as well. Technologies like Ethernet fabrics, SDN overlays and SD-WAN bring policy-based control to the network, abstracting away a device-config-centric view, and replacing it with centralized policy control. Finally, intent-based networking technologies are just beginning to emerge, and provide mathematical validation that business intent and network configurations are in sync (see "Innovation Insight: Intent-Based Networking Systems").

The technologies arising across network automation are examined in depth in the "Market Guide for Network Automation."

Evidence

Press release: "SolarWinds Acquires AppNeta TraceView Solution." (http://www.solarwinds.com/company/newsroom/press_releases/solarwinds-acquires-appneta-traceview-solution.aspx)

Press release: "NETSCOUT Unveils Industry's First Real-Time Information Platform for Service Assurance, Cybersecurity and Big Data." (http://www.netscout.com/press-release/netscout-unveils-industrys-first-real-time-information-platform-for-service-assurance-cybersecurity-and-big-data/)

Press release: "Micro Focus Announces Intent to Merge With Hewlett Packard Enterprise's Software Business Segment." (https://www.microfocus.com/about/press-room/article/2016/micro-focus-announces-intent-to-merge-with-hewlett-packard-enterprise-software-business-segment/)

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.

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.

© 2018 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 (/technology/about/policies/usage_guidelines.jsp) 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. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. 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. (/technology/about/ombudsman/omb_guide2.jsp)"
