451 Research®

ixia

REPORT EXCERPT

Network Visibility and Monitoring Forecast

MOVING TOWARD COMPREHENSIVE SOLUTIONS

The network visibility and monitoring (NVM) market has experienced a number of changes in the 10 months since our last Technology & Business Insight report on the sector. There have been two multibillion-dollar M&A transactions and the addition of a number of new vendors and solutions to the segment. The ever-present security challenges facing the changing network landscape, as well as the ongoing adoption of public cloud and network virtualization, will ensure that the network visibility tool market will continue grow rapidly for the foreseeable future.

KEY FINDINGS

- The market forecast for the NVM sector has been scaled back to reflect a more specific cross-section of the market, representative of industry consolidation, network virtualization and the growth of substitute functionality from networking vendors. We now anticipate it to grow to over $1.6bn by 2019.
- Security has emerged clearly as the key revenue driver for the network visibility sector as security projects have dragged through new visibility infrastructure buildouts.
- The combination of network traffic data with other reported (log, alert) data emerged as a distinct sub-segment of network analytics tools, driving further demand for visibility infrastructure.
- The deployment of network virtualization solutions has created a near-term window for current visibility vendors because first-generation network virtualization tools have yet to develop robust internal traffic management, monitoring and performance tools.
- Public cloud infrastructure and cloud-delivered network services continue to present blind spots to network operations personnel beyond reported statistics. This contradiction between how network teams are measured (uptime, performance) and the tools available may slow adoption of these technologies within the enterprise.

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

New York
20 West 37th Street, 6th Floor
New York, NY 10018
Phone: 212.505.3030
Fax: 212.505.2630

London
Paxton House (5th floor), 30 Artillery Lane
London, E1 7LS, UK
Phone: +44 (0) 207 426 0219
Fax: +44 (0) 207 426 4698

San Francisco
140 Geary Street, 9th Floor
San Francisco, CA 94108
Phone: 415.989.1555
Fax: 415.989.1558

Boston
1 Liberty Square, 5th Floor
Boston, MA 02109
Phone: 617.275.8818
Fax: 617.261.0688

SECTION 2

Network Visibility: Changing Market Dynamics

The NVM market boundaries have shifted in the last year, with large M&A transactions, new market entrants to the segment and substitutes for parallel visibility networks. As anticipated, APM and NPM vendors have integrated (or partnered on) components of network visibility into existing platforms, notably *Splunk App for Stream*. This has served to blur the boundaries of what constitutes APM, NPM and NVM even further than was previously the case. Moving forward, the capture and integration of multiple data sources (see ExtraHop, above), including reported data such as log files, raw traffic data and summarized (NetFlow, sFlow) traffic, will build an increasingly comprehensive snapshot of how traffic is traversing a network.

The visibility space, traditionally dominated by enterprise datacenter applications, has been impacted by two additional major trends as well as a number of smaller ones. First and foremost, the increasing importance and urgency of security projects, driven by regulatory strictures and risk of liability, has resulted in a windfall for security vendors with intrusion detection, exfiltration, detection of early denial-of-service attacks and malware detection. In turn, these security tools require access to network traffic at multiple points in the topology, which has resulted in a trickle-down benefit to vendors of network visibility tools. Gigamon and Ixia, two of the largest pure-play visibility vendors, listed security projects within enterprises as a key revenue driver in their most recent quarterly earnings statements.

Virtualization is the second key trend affecting the visibility market. As mentioned in our last NVM report, server virtualization within the datacenter has fundamentally changed the datacenter topology. In doing so, it has impaired the ability for network operations teams to look into network traffic to identify performance issues or root causes of outages. The rapid growth of virtualization has also pulled along new budget dollars for new visibility networks that – via a combination of agent software (virtual TAPs and probes) as well as intelligent placement of switched port analyzer (SPAN) ports at key junctures – monitor both 'North-South' (server to network) traffic and 'East-West' (inter-server) communications. Most importantly, the rise of server virtualization has consolidated servers and applications within the datacenter (indeed, one of the key economic drivers of virtualization adoption), which has reduced the number of devices to monitor.

The broader networking market is in the early stages of deploying network virtualization technologies, incorporating functions that were traditionally on one or more physical appliances as applications or services running within the virtualized server environment. VMware NSX is one example of a network virtualization solution, predominantly software-based, whereas Cisco sells its ACI

technology, which combines enhanced switch hardware, controllers, and software agents and virtual switches. These technologies, as well as alternatives offered by other networking vendors, are in the early stages of market adoption and do not yet offer the full array of tools and interfaces required for network operations systems and processes. This has created yet another opportunity for visibility vendors to insert themselves into the changing network environment.

One consistent component of network virtualization has been the increased computational load on the servers to process network traffic. A number of network component vendors are approaching this problem as an opportunity by using the rapidly increasing capabilities of network adapter cards to preprocess network traffic before it impacts server performance, effectively offloading compute-intensive network tasks onto co-processors on the network cards. The way in which *Napatech* and *Mellanox* are performing VXLAN decapsulation is a key example of this.

The rapid adoption of public cloud services including Amazon Web Services (AWS) and Microsoft Azure, like enterprise datacenter virtualization, has been a boon to the larger IT industry and has created a wealth of new opportunities and business models. As is the case with network virtualization, this rapid growth has often outstripped the management and monitoring capabilities, creating blind spots in network operations' ability to maintain internal uptime and performance benchmarks. Amazon offers its CloudWatch monitoring service to report on utilization of not only server and storage resources, but also self-reported data on traffic volume and utilization of network services such as its DNS service (Route 53) or elastic load balancing service. A number of security and APM/NPM vendors plug into the CloudWatch API to extract other metrics, often via agent software sitting within AWS instances. While this self-reported data is preferable to no data, it still does not provide granular traffic (packet) data for performance or outage analysis at the same level that an enterprise is able to do on-premises.

The growing market of tier-two and tier-three cloud service providers has also been a windfall for visibility vendors as these cloud service providers (CSPs) build out new datacenters at a growing volume. This market segment is highly contested by traditional networking vendors competing against the growing interest in *disaggregated networking*, which has created a window of opportunity for white-box (merchant silicon switch) based networking solutions.

A new breed of competitors leveraging a combination of merchant silicon and OpenFlow-based TAP aggregation solutions, including NEC and Big Switch Networks, seek to disrupt the visibility network (and provide them an easier point of entry into the enterprise network than the production network) using disaggregated visibility software and commodity switches. Cisco began quietly shipping its own visibility offering, Nexus Data Broker – which functions similarly to Arista DANZ in configuring blades (or, in hybrid mode, ports on a blade) on the 3000 series and 9000 series Nexus switches for visibility use – which uses OpenFlow for control-plane functions. This approach is both elegant (repurposing ports on existing switches for visibility applications) and problematic (both DANZ and Nexus Data Broker lack the full suite of packet grooming capabilities offered by pure-play vendors). The potential impact of the switch-vendor-included visibility capability is significant because the incumbent networking vendors are often able to include visibility switch functionality as part of a larger network equipment purchase.

Pluribus Networks offers both software for commodity hardware and a custom hardware platform that integrates compute with switching that is different enough from legacy switch solutions as well as OpenFlow/Merchant Silicon-based solutions to merit its own category. Integrated analytics are part of Pluribus' offering, which resides in the middle of a datacenter fabric, inline or out of band, and can correlate VXLAN overlay networks as well as underlay VLANs. The platform also offers integrated storage, allowing network administrators to rewind flow statistics for a month or more.

A number of options have emerged that make use of traffic data provided by visibility switches, including Splunk and Corvil's traffic analytics and business intelligence offerings. These solutions differ, but they generally seek to correlate reported log data with summarized (flow) and non-summarized (packet) traffic to build a comprehensive picture of network performance. Reported data (generally speaking, the log files and self-reported statistics provided by the network devices themselves) is a frequent source for network analysis tools. However, it was historically known to be inaccurate during periods of high utilization of the network devices themselves (when the router or switch is at 99% utilization, it is often a challenge for it to accurately report that it is so). While modern software architectures that isolate processes from monopolizing computational capacity – paired with high-performance silicon thanks to Moore's Law – have greatly improved the accuracy of self-reported data from network devices, doubts still linger as to the veracity of firsthand device testimony.

The combination of these variables, strong enterprise spending, and an anticipated resurrection of carrier spending has resulted in a growing market and strong prospects for future revenue. Within the sector, the battles will center on where the intelligence (and therefore margin-rich value) resides in the monitoring network, at the switch or in higher-level analysis software. This will continue to stress relationships between the finely meshed partnerships in the space. What could disrupt the space is the degree in which substitute functionality from networking vendors such as Cisco (ACI), VMware (NSX) and Arista (DANZ) begins to cannibalize parallel monitoring networks with 'good enough' baked-in solutions. This was a primary factor in recalculating our forecasts of market size of the visibility sector through 2019.

SECTION 5
Forecast

Our forecast for the NVM segment has declined from last year's research report. This reduction is not due to shrinking demand in the market for these solutions, as there is healthy growth of the market year over year. It is rather the result of a combination of factors, primarily the choice of which vendors to include (and exclude); which product families were relevant in NVM; and the broader industry trends of the rapid adoption of network virtualization technologies, industry consolidation and substitute functionality offered by large networking vendors.

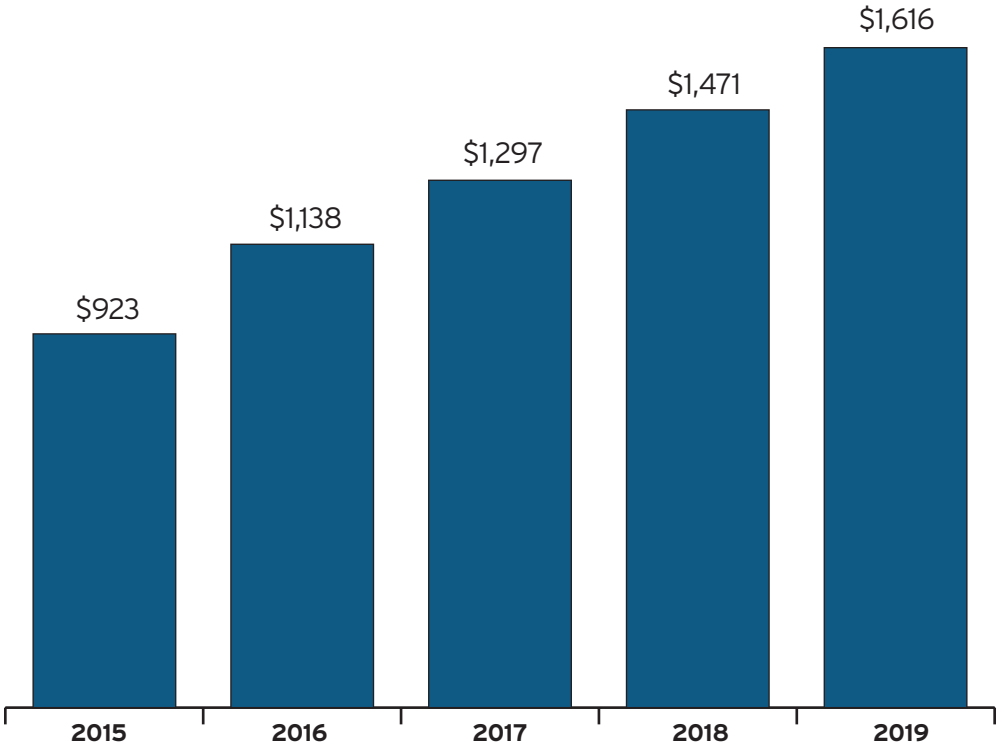
In this forecast, we have included nine additional companies: Brocade, Cisco, Kentik, Corvil, ExtraHop, Jolata, NEC, Network Critical and Pluribus. We dropped Riverbed and carried Arista forward from the last forecast, primarily due to its visibility switch capabilities. However, the substitute functionality from Cisco ACI and VMware NSX were not included. In addition, vendors and tools focused primarily on analyzing traffic on carrier networks, including radio management, have not been included in this study. We have assumed as part of this forecast that the two large M&A transactions (NetScout-Danaher and Thoma Bravo-Riverbed) have been approved and conclude on schedule. We have also made a number of assumptions about product integration and overlap post-transactions.

The forecast now includes a range of functionality from enabling interfaces (Emulex, Napatech), challengers (Kentik, Jolata, NEC, Big Switch, Pluribus), and visibility hardware and software vendors. It is beginning to include network analysis vendors that choose to integrate traffic data. In this latter category, we have chosen not to include Splunk as we believe that although the Splunk App for Stream traffic analysis offering is strong, it will not pull through incremental, directly attributable revenue to the sector as it is a free offering (although it will inevitably pull through incremental revenue for Splunk's core offering).

By our measurement, the aggregate network visibility and monitoring revenue generated by the 22 companies we have included in this analysis will total $923m in 2015, and we expect that number to grow at a CAGR of 11.85% to exceed $1.616bn in 2019 (see Figure 1). This forecast is the result of a bottom-up analysis that incorporates the current revenue and growth potential of each vendor included.

FIGURE 1: TOTAL MARKET REVENUE AND PROJECTION TO 2019 ($M)

Source: 451 Research, 2015



Note: For the purposes of market sizing, we have chosen to include the services revenue of the companies profiled because the sales models of each of the companies differ, with some companies charging a larger upfront hardware fee with smaller annual maintenance fees, while other firms charge a smaller hardware fee and larger annual maintenance (often software) fees. In addition, a number of these vendors do not focus exclusively on the network visibility and monitoring market, and therefore there is an 'attach rate' estimate to exclude non-NVM products (such as the majority of Arista's Ethernet switches and Ixia and NetScout's test products) from the market size estimates below, based on publicly available data when possible.

Figures 2 and 3 provide vendor characteristics and vendor distribution by revenue for the network visibility and monitoring space. Some high-level takeaways include:

- Nine of the 22 vendors included in this report are publicly traded, with the remaining 13 being private firms. Public vendors represent 76% of total 2015 forecasted market revenue.
- The market is largely segmented into large public companies that are either pure-play NVM vendors (Gigamon, Ixia) or incorporate NVM functions as a feature of a broader offering (NetScout); midsize companies or midsize product offerings of larger companies (VSS Monitoring, Emulex, Apcon); and a good number of smaller vendors that are pursuing OEM or niche-vertical paths to market (cPacket, Interface Masters, Datacom Systems). In this analysis, we have included advanced traffic analysis offerings from ExtraHop, Jolata, Kentik and Corvil, as well as additional OpenFlow-based solutions like those from Cisco, NEC and Big Switch.

FIGURE 2: 2015 NETWORK VISIBILITY AND MONITORING MARKET STATISTICS

Source: 451 Research, 2015

SUMMARY		VENDOR STATISTICS BY REVENUE TIER	
2015E Revenue ($M)	$923	# Vendors $100M +	3
2019E Revenue ($M)	$1,616	*% of total*	*14%*
CAGR	11.85%	Total 2015E Revenue	$570M
Total Vendors	22	*% of total*	*62%*
PUBLIC/PRIVATE SPLIT		# Vendors $30-100M	4
Public Vendors	9	*% of total*	*18%*
% of total	*41%*	Total 2015E Revenue	$147M
Public Vendor 2015E Revenue	$704M	*% of total*	*16%*
% of total	*76%*	# Vendors $15-30M	7
Private Vendors	13	*% of total*	*32%*
% of total	*59%*	Total 2015E Revenue	$170M
Private Vendor 2015E Revenue	$219M	*% of total*	*18%*
% of total	*24%*	# Vendors $1-15M	8
		% of total	*36%*
		Total 2015E Revenue	$35.9M
		% of total	*4%*

FIGURE 3: NETWORK VISIBILITY AND MONITORING VENDORS BY REVENUE TIER (VISIBILITY REVENUE ONLY)

Source: 451 Research, 2015

>$100M	Gigamon, Ixia, NetScout
$30-100M	Apcon, Brocade, Network Critical, VSS Networks
$15-30M	Arista Networks, Cisco, Corvil, Emulex, ExtraHop, Napatech, Savvius
$1-15M	Big Switch, cPacket, Kentik, Datacom Systems, Interface Masters, Jolata, NEC America, Pluribus Networks