PLURIBUS NETWORKS

Pluribus markets Netvisor, a distributed network operating system, as well as a hardware appliance for those who wish to purchase bundled solutions. One function of Netvisor is visibility and traffic forwarding, similar to OpenFlow-based solutions, but with visibility into both physical network VLANs as well as VXLAN-based overlay networks.

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. Pluribus is also one of only a couple vendors that broker between overlay and underlay.

Learn more at www.pluribusnetworks.com
and @pluribusnet

451 Research®

NETWORK VISIBILITY AND MONITORING FORECAST

MOVING TOWARD COMPREHENSIVE SOLUTIONS

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.

MAY 2015

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.

The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such. 451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

451 Research®

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

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

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

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

SECTION 1
Executive Summary

1.1 INTRODUCTION

Pure-play visibility vendors have continued to innovate within the NVM market, releasing additional traffic grooming capabilities and high-density platforms. In addition, the threat of incursion from upstart competitors has driven at least one vendor to release a lower-cost *network visibility switch based on white-box hardware*.

The broader analytics solution vendors have a renewed focus on the value of raw network traffic (sometimes referred to as 'wire data').

The original momentum of (OpenFlow-based) software-defined networking (SDN) technology was hindered early by the perceived lack of a 'killer app,' an application so demonstrably superior to distributed networking that it would drive a rip-and-replace cycle of legacy networking equipment. For two early SDN advocates the killer app has turned out to be using OpenFlow switches as visibility test access point (TAP) aggregation switches. While the OpenFlow advocates continue to add functionality to their early products, they still constitute a small percentage of visibility infrastructure.

As the market matures, it continues to absorb (or merge with, depending on perspective) APM and NPM functionality, making it harder to segment the market. We anticipate this trend to continue, with the ultimate outcome being on-premises APM/NPM/network visibility tools with extensive log management, virtualized networking support and links to public-cloud visibility interfaces.

The end result is an increased level of attention on traffic analytics and visibility infrastructure. We anticipate the market for network visibility tools – and the closely adjacent market for advanced traffic analysis tools that incorporate multiple sources of data alongside packet captures and flow data – to continue to grow rapidly as enterprises seek to manage new virtual networking.

1.2 REPORT RATIONALE

This report provides a high-level forecast for the market including key assumptions and scenarios that will drive the market forward. Where possible, these will be the high-level forecasts available in 451 Research's Market Monitor product line. Deeper, segment-specific and regional forecasts, including an in-depth analysis of participating vendors, are available in Market Monitor.

1.3 KEY FINDINGS

- The market forecast for the NVM sector has shifted considerably due to industry consolidation, network virtualization and the growth of substitute functionality from networking vendors. We 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 the 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.

SECTION 2

Network Visibility: Changing Market Dynamics

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.

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. These technologies 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.

The rapid adoption of public cloud services, 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.

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 merchant silicon and OpenFlow-based TAP aggregation solutions 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.

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.

A number of options have emerged that make use of traffic data provided by visibility switches. 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.

SECTION 4
New Mousetraps

The growth in the visibility market has not gone unnoticed by incumbent networking vendors, ecosystem analysis tool providers and the startup community, all of which see the visibility spend as a potentially lucrative adjacent revenue opportunity. In addition, the traditional visibility market is facing more underlying changes within enterprise networking, including the growth of cloud-provided networking services and the greater utilization of off-premises private, hybrid and public cloud offerings.

The combination of incremental revenue and structural upheaval in networking has resulted in a number of alternatives to the status quo in network visibility. Broadly, these can be categorized as:

- 'Feature-ization'
- Disaggregated visibility
- Lobotomization
- Virtual balkanization
- Opaque clouds

4.1 FEATURE-IZATION

One key factor impacting the growth of the broader visibility sector is the growing 'good-enough' functionality provided by networking vendors as part of the production networking equipment. The functionality provides rudimentary packet grooming functionality beyond traditional SPAN/remote switched port analyzer (RSPAN) functions of traditional switches, and has been adopted at a quicker rate than many in the industry had anticipated as an 'attach rate' to its highly successful datacenter switches.

In 2014, as network virtualization gained market traction, an early customer request was for greater visibility into both the virtual ('overlay') and physical ('underlay') network traffic in order to identify performance and outage sources.

These efforts are not exact one-to-one feature/functionality equivalents to existing solutions. When combined with the underlying shift within networking to virtualization and cloud services, they structurally erode the overall network visibility segment. Physical networking equipment is shrinking in favor of virtual appliances, and this reduction has ramifications to monitoring infrastructure as well as if the transition or product mix from physical to virtual results in a sudden precipitous drop in revenues.

4.2 DISAGGREGATED VISIBILITY

A second new approach to network visibility is provided by a combination of commodity, white-box switches paired with software from OpenFlow-based software vendors that offer TAP aggregation functionality at a very competitive price. While the early offerings do not have the feature set of mature visibility solutions from incumbent vendors in the segment, we anticipate that they will gain a small percentage of overall market share in the segment driven by customers attracted to the competitive price points.

This is a subset of the broader disaggregation efforts targeted at Web-scale providers and generally driven by the Open Compute Project (OCP). Companies have partnered with large networking vendors such as HP and Dell to provide a choice of switch software on top of these vendors' datacenter switches. Should the disaggregation trend take off beyond the small subset of cloud service providers that are currently testing the available products, it will inevitably bleed over into the monitoring tools as well. The 'rising tide' of disaggregation could accelerate adoption of solutions from these vendors.

4.3 LOBOTOMIZATION

The network visibility and monitoring technology space is heavily meshed with partnerships and alliances. Networking equipment vendors partner with network analysis tool vendors, as do pure-play visibility switch vendors. The demarcation line between these vendors (i.e., which vendors perform which functions) is unclear. The potential danger is that the high-level analysis vendors begin to capture more of the high-level value provided from visibility switch vendors, either by the presentation of the traffic data or by redundant post-processing (packet grooming). Such an event could relegate the current vendors in the segment to 'mere packet pushers' status. This could stress current partnerships as the wallet share of combined sales shifts in favor of analysis vendors and away from visibility infrastructure providers.

4.4 VIRTUAL BALKANIZATION

With network virtualization has come a plethora of overlay technologies such as VXLAN and Network Virtualization using Generic Routing Encapsulation (NVGRE).

Current visibility tool vendors are in the process of releasing a combination of enhanced visibility switches that can detect and parse overlay traffic with software-based agents. The agents reside within virtual machines or hypervisors to monitor virtual overlay traffic for correlation with the underlay traffic to identify potential bottlenecks and identify performance and outage root causes.

The proliferation of additional overlay technologies, as well as the myriad network virtualization options will continue to introduce complexity that will create virtual Balkans that visibility tools will be challenged to monitor. Custom platforms ameliorate this balkanization by brokering between the overlay and underlay.

4.5 OPAQUE CLOUDS

Another key trend growing in enterprise deployment is cloud-delivered services, including compute, storage and now network services. As mentioned previously, the current generation of public cloud offerings provides limited visibility into the cloud-provider infrastructure, beyond self-reported (agent) data. This impairs traditional performance tuning and troubleshooting processes within enterprises. While this may not impact native 'born in the cloud' organizations with little internal infrastructure, these organizations currently represent the minority; the majority of organizations have deployed a subset of their internal applications in private or public clouds. We believe that as the public and private cloud providers mature in their offerings and customers demand more visibility into the internal workings of the provider networks as a condition of sales contracts, the general access to these functions will improve. For now, this represents a blind spot for visibility.

A second trend is the delivery of layer 4-7 network services provided as a *cloud managed service*, including security and *WAN optimization*. All of the vendors providing these services are in the same position as public cloud providers, providing limited visibility into their own offerings but otherwise opaque to network monitoring tools and processes. Like the private and public cloud providers, we believe that as the market matures for cloud-delivered network services, customers will demand more transparency into internal traffic to track against existing business compliance, assurance, uptime and performance requirements.

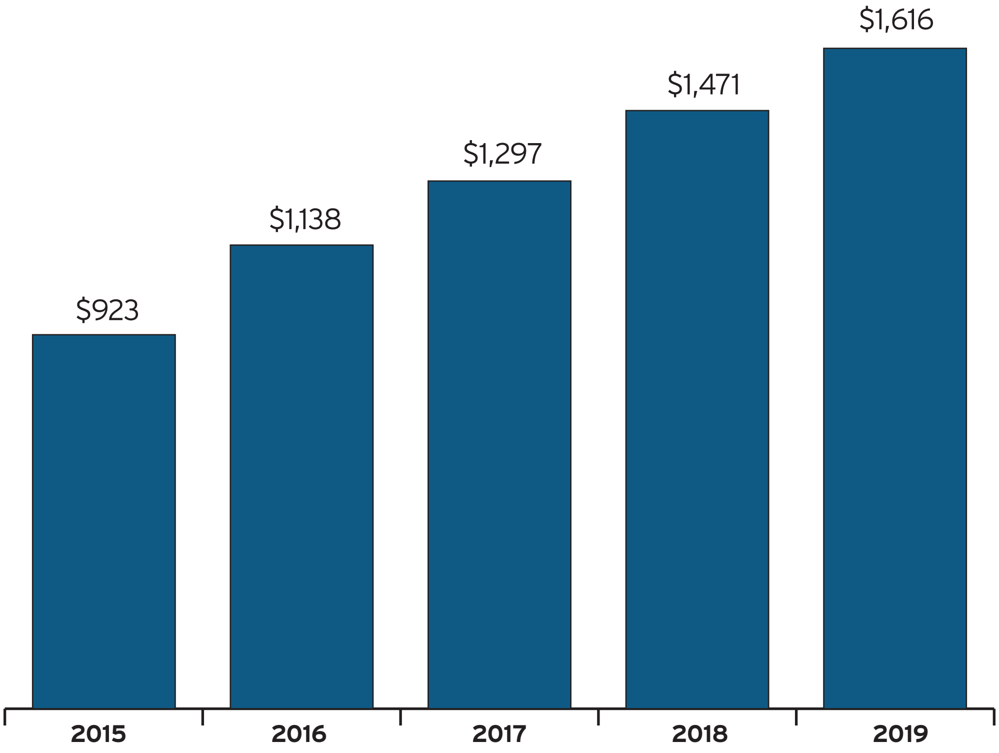
SECTION 5

Forecast

By our measurement, the aggregate network visibility and monitoring revenue 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).

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 from the market size estimates below, based on publicly available data when possible.

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%*