Network Monitoring Equipment

Annual Market Report: *Excerpts*

26 June 2018

Matthias Machowinski
Senior Research Director and Advisor
Enterprise Networks and Video

IHS Markit Technology | **Report**

Contents

Top takeaways: Monitoring equipment revenue declines in 2017 as transition to software impacts hardware revenue 3
Background 4
After two strong years, CY17 revenue dips slightly 5
Government drives growth in CY17 7
Advanced switches decline 8
The need for more speed: 40G out, 100G in 10
EMEA drives growth in CY17 11
Market share 12
Market drivers 14

Exhibits

Exhibit 1 Monitoring equipment diagram 4
Exhibit 2 Monitoring equipment forecast 6
Exhibit 3 Monitoring equipment by vertical 7
Exhibit 4 Monitoring switches: Advanced versus standard 9
Exhibit 5 Monitoring switch port shipments 10
Exhibit 6 Monitoring equipment revenue by region (percentage) 11
Exhibit 7 Monitoring equipment market share (revenue) 13
Exhibit 8 WAN changes 14
Exhibit 9 Top WLAN changes 15
Exhibit 10 Reducing the impact of ICT downtime 16

Top takeaways: Monitoring equipment revenue declines in 2017 as transition to software impacts hardware revenue

After two strong years of double-digit growth, network monitoring equipment revenue declined 3% to $561M in 2017 because of lower service provider demand and adoption of lower cost standard Ethernet switch–based solutions. Still, 2017 revenue is up 10% over 2015, and the number of monitoring ports shipped rose grew significantly in 2017, showing that organizations are continuing to make significant investments to monitor more pervasively, improve network visibility, and make networks more secure and reliable. Although service provider demand declined, enterprise held mostly steady and government growth accelerated. We expect a return to growth as service provider demand recovers and project revenue of $776M by CY22 for a five-year CAGR of 7%.

Key data points:

- Advanced switches account for 75% of monitoring switch sales in CY17; their contribution declined by 7 points this year due to adoption of standard Ethernet switch–based monitoring solutions.
- The number of monitoring ports shipped grew 45% in CY17 to over 400K.10G ports are most common on monitoring switches today and had a strong year but are getting near their peak. 40G growth slowed dramatically in CY17 while 100G had a banner year, with ports growing almost three-fold and exceeding the number of 1G ports for the first time in CY17. 100G will be the high growth market going forward as production networks shift rapidly from 40G to 100G and monitoring networks follow suit.
- Government continued the strong performance from CY16 and was the only vertical to grow in CY17. Enterprise declined 2%, and service provider was down 10%.
- North America is the largest region, accounting for almost three-quarters of total revenue. North America declined after two years of strong growth as companies capped investments and adopted lower cost standard Ethernet switch–based solutions. EMEA returned to growth in CY17 because of solid GDP growth across Europe while Asia Pacific declined owing to slowing growth in China.
- Gigamon is the largest network monitoring equipment vendor, accounting for 37% of revenue in CY17 (same as CY16), and is 21 points ahead of the next closest competitor, NetScout with 16.2% of revenue (down 1.8 points). Ixia rounds out the top three with 16.0% of revenue (up 1 point).

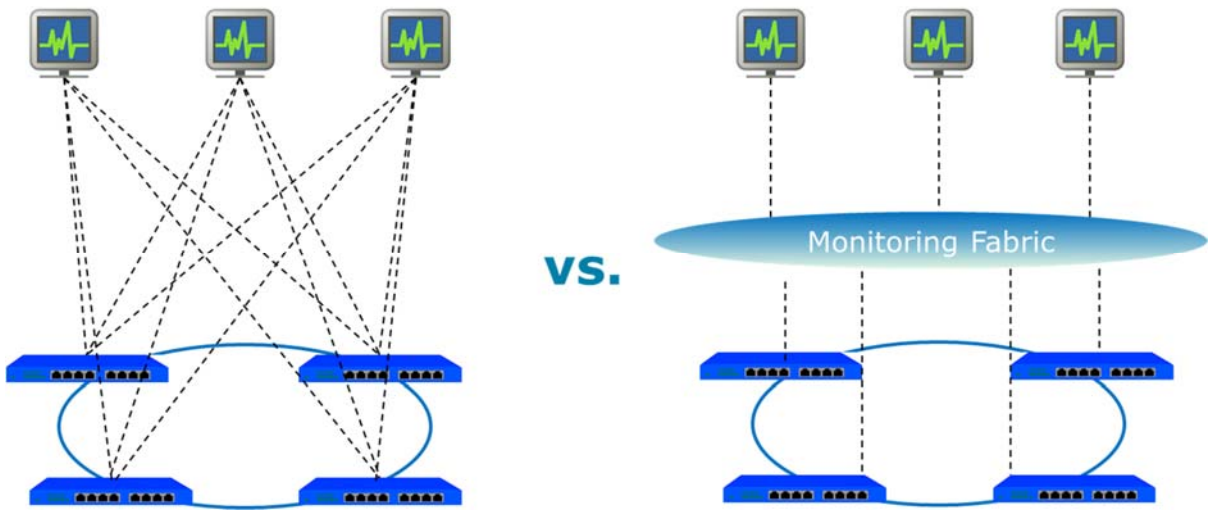
Background

This report tracks the network monitoring equipment market, which consists of network monitoring switches and taps/bypass switches. Network monitoring equipment is used to build parallel monitoring networks that coexist alongside production communication and data networks, capturing network traffic and sending it to traffic analysis tools, such as network monitoring systems, application performance tools, and security appliances.

Organizations that want to capture network traffic don't need to use dedicated network monitoring switches—alternatively, they can mirror traffic using the built-in SPAN (switched port analyzer) ports on Ethernet switches or by inserting network taps on the links that need to be monitored and sending the traffic directly to the analysis tools. This approach will serve the average organization well and avoids the expenditure of a dedicated monitoring network. However, for organizations with a more complex network infrastructure and for whom the performance of their network plays a critical role in their day-to-day operations, a dedicated network monitoring solution provides a more robust and scalable approach to traffic capture.

The act of monitoring should not impact the performance of the network, but mirroring traffic using SPAN ports adds additional processing load to the switch ASIC, which can impact the performance of the switch when links are highly utilized or result in dropped SPAN traffic, making monitoring more difficult when it counts the most. Captured traffic may also need to be sent to several tools at the same time (e.g., performance monitoring, security), not just a single tool. Not all switches support this feature, and those that do end up allocating an even greater portion of processing resources to network monitoring rather than the core task of moving production traffic. Network monitoring switches solve these issues by providing an infrastructure dedicated to monitoring that does not impact production traffic and is scalable as monitoring needs increase. The following diagram shows the difference between a network where tools receive traffic directly (left) and one where traffic is first tapped by a monitoring fabric and then sent on to the tools. With a fabric, traffic is tapped once and retransmitted to the tools as needed.

Exhibit 1 Monitoring equipment diagram



Source: IHS Markit

After two strong years, CY17 revenue dips slightly

Network monitoring equipment growth was brisk in CY15 and CY16, growing 27% and 14%, respectively, as vendors moved past the integration of acquisitions, service provider demand stabilized, and organizations of all types made investments to improve the traffic visibility and security of mission-critical networks. Growth finally cooled off in 2017, and worldwide network monitoring equipment revenue declined 3% to $561M. We attribute the decline to

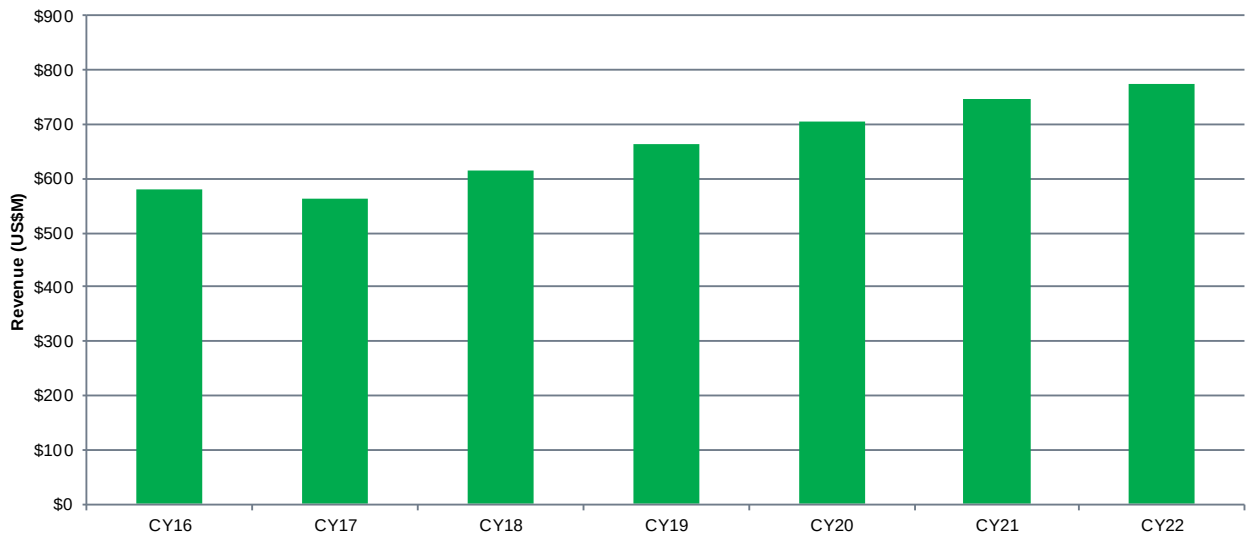
- Short-term demand fluctuations; for example, the service provider segment remains challenging as service providers grapple with bringing capex in line with revenue
- The rise of standard Ethernet switch–based monitoring solutions, which allows end users to monitor more pervasively (monitoring ports grew 45% in CY17) but is putting pressure on revenue growth

The above factors mostly impacted the monitoring switch segment—taps/bypass switches bucked the downward trend as vendors reported growing interest in bypass solutions (which command higher prices than taps), and there is a less of a focus on cost containment given the much smaller size of this segment.

The trend toward standard Ethernet switch–based fabrics has manifested itself in a number of ways over the past few years. Initially, start-ups like Big Switch developed proprietary monitoring software that leveraged standard commercially available Ethernet switches. This was followed by traditional network monitoring vendors launching their own turnkey standard Ethernet switch–based offerings (integrated hardware/software, rebranded, and fully supported) to offer a lower cost alternative. More recently, traditional vendors have made their software available on a standalone basis, allowing end users or system integrators to select their own (compatible) hardware. The net effect of this trend is that the revenue contribution of hardware is declining, which isn't necessarily a negative development as margins and differentiation are in software; however, during this transition vendors will find it difficult to grow their top-line revenue. Although standard Ethernet switch–based monitoring switches don't yet offer the same feature set as purpose-built switches, they will be sufficient for networks with less complex needs or to serve as aggregation switches to feed traffic to advanced switches for further processing.

For CY18, we expect growth to resume, albeit at a lower rate than in past years, driven by the need for robust network monitoring capabilities to ensure the performance of mission-critical network infrastructure. We project CY18 revenue to grow 10% to $615M and long-term revenue of $776M by CY21, a five-year CAGR of 7% (versus a CY13–17 CAGR of 9%).

Exhibit 2 Monitoring equipment forecast



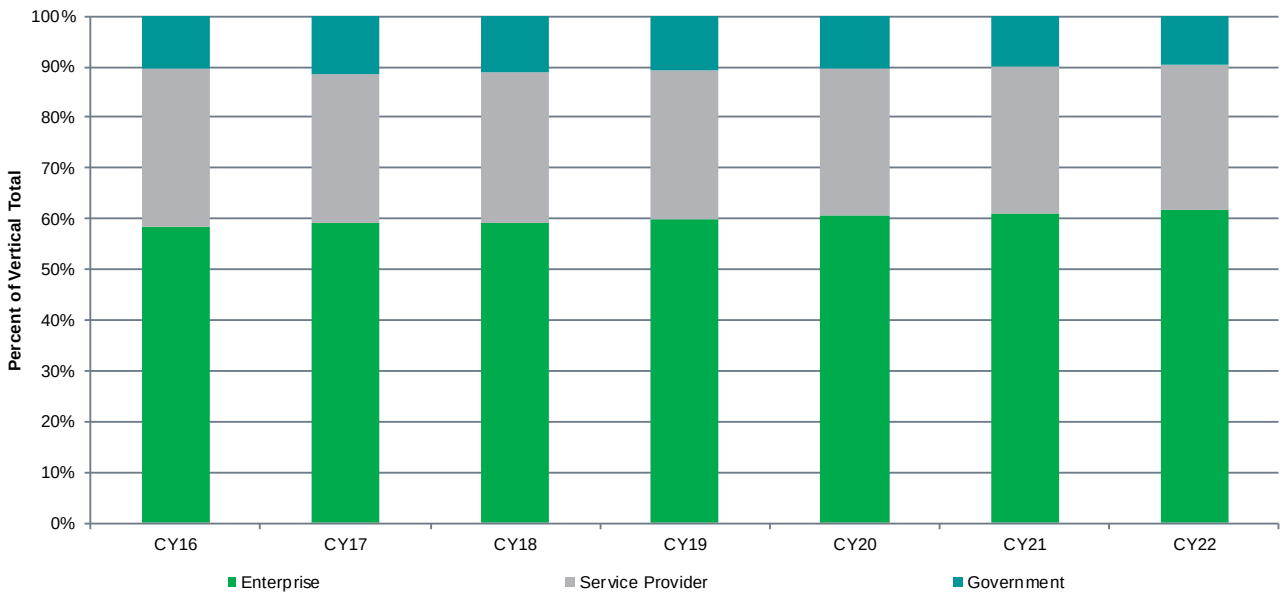
Source: IHS Markit

Government drives growth in CY17

The government vertical continued its strong performance from CY16 and was the only vertical to grow in CY17. Enterprise demand held steady, declining only 2%, while service provider revenue was down 10% as they try to balance their capex budgets against revenue projections and have been early adopters of standard Ethernet switch–based solutions.

There will be annual growth variations due to cyclical buying patterns, and long-term, we expect government demand to lag behind enterprise and SP. Enterprise will be the high growth market going forward as there is room for down-market expansion, followed by SPs, for whom monitoring is critical to delivering their services.

Exhibit 3 Monitoring equipment by vertical



Source: IHS Markit

Advanced switches decline

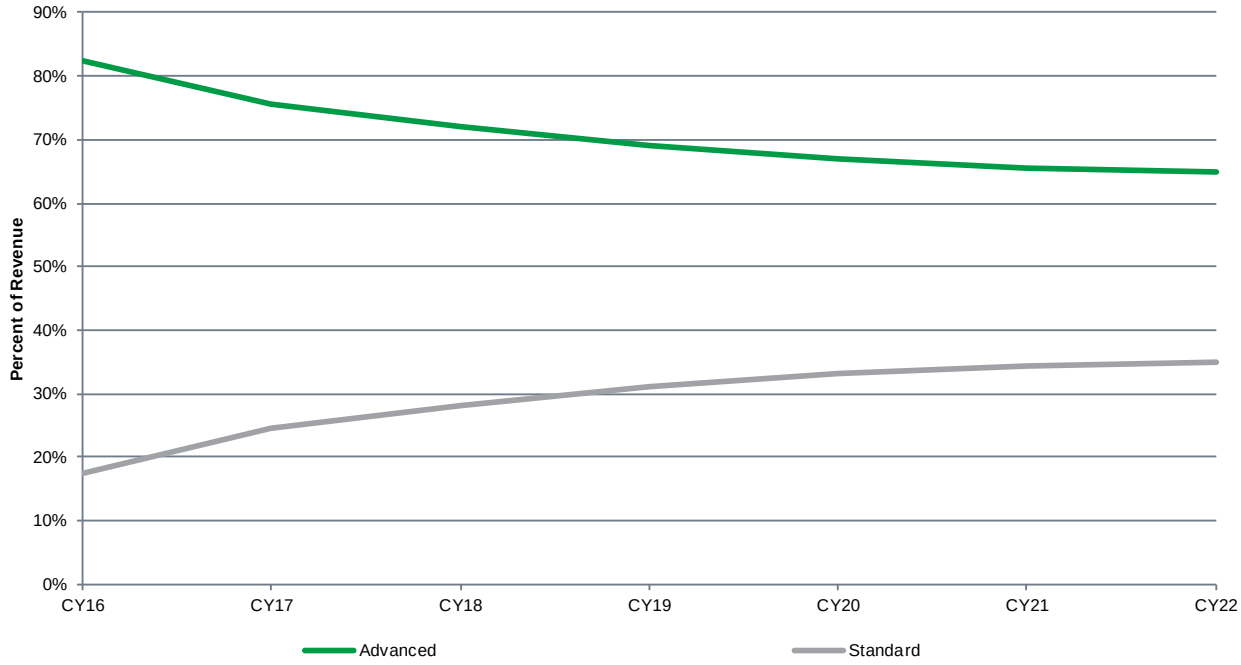
Standard switches simply forward traffic to the relevant tools. Advanced switches have additional packet processing capabilities built in that can be applied to captured traffic. These include among others:

- Header modification
- Deep packet inspection
- Packet slicing
- Data masking
- Traffic deduplication
- Load balancing
- SSL decryption
- NetFlow statistics generation

Advanced switches offload and prolong the longevity of the tools by reducing the amount of traffic that is generated by network monitoring and by offloading some of the processing from the tools to the monitoring switch. For some deployments, advanced switches are also a necessity to remain compliant with regulations, such as stripping sensitive personal data from monitored traffic. Advanced features increase the utility of monitoring switches and drive even greater efficiency into the monitoring infrastructure. For many buyers, investing in advanced switches will be cheaper than replacing monitoring tools that no longer can handle the traffic loads directed at them.

Advanced switches account for the vast majority of monitoring switch sales (75% in CY17), but their contribution declined by 7 points this year, and we expect this trend to continue as interest in standard Ethernet switch–based solutions gain traction. These are tracked as standard monitoring switches as they don't currently support advanced packet processing, which is done on external service nodes or advanced switches.

Exhibit 4 Monitoring switches: Advanced versus standard



Source: IHS Markit

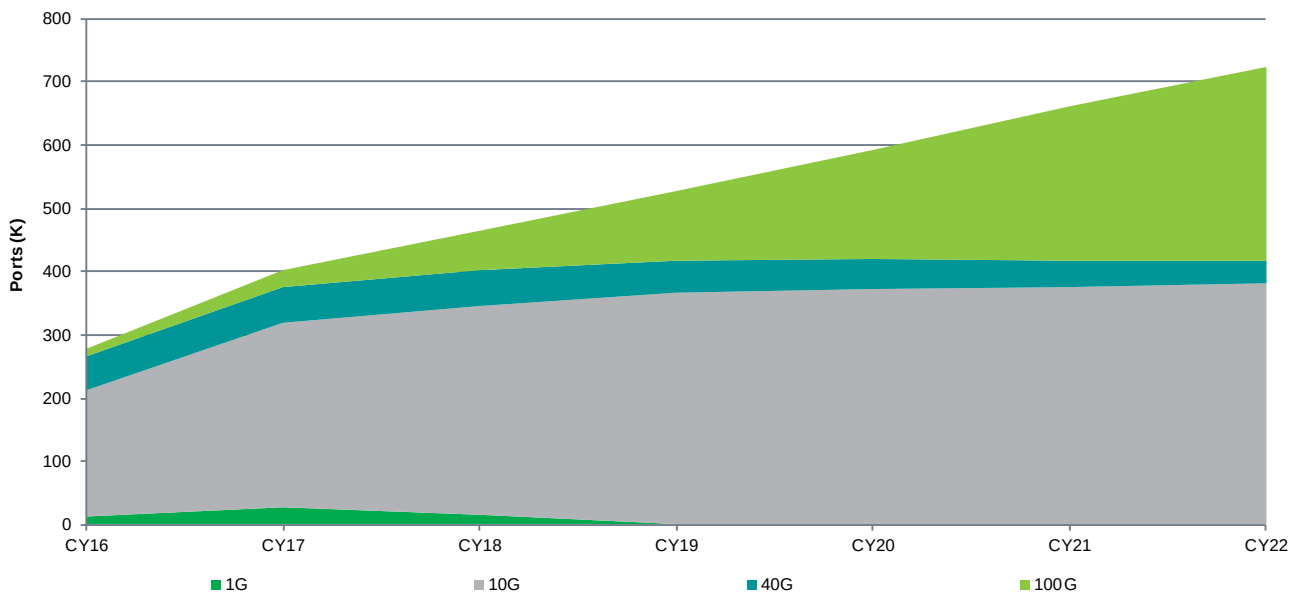
The need for more speed: 40G out, 100G in

Unsurprisingly, 1G ports are on the way out, relegated to low-bandwidth applications and legacy devices (although CY17 produced unexpected yet inconsequential growth). The most common type of port on monitoring switches now is 10G by far, a reflection of the fact that monitoring switches capture traffic from access switch uplinks and aggregation/core switches, which usually run at speeds of 10G and higher. 10G had a strong year, buoyed by growth in standard Ethernet switch–based monitoring switches, but looking ahead, we think 10G is getting near its peak and will see only small growth in the coming years.

40G was the new high-growth market until CY16, but growth slowed dramatically in CY17, in line with trends in production networks, where 40G port shipments declined for the first time in CY17 as data center operators shift to 25/100G.

100G had a banner year in CY17 with ports growing almost three-fold and exceeding the number of 1G ports for the first time. Service providers initially embraced 100G, and it is now expanding to enterprises and data center operators. The launch of QSFP28-based 100G technology has improved the density and cost of 100G solutions and has driven a surge in 100G adoption in production networks over the past two years, which in turn is accelerating demand for 100G on monitoring switches.

Exhibit 5 Monitoring switch port shipments



Source: IHS Markit

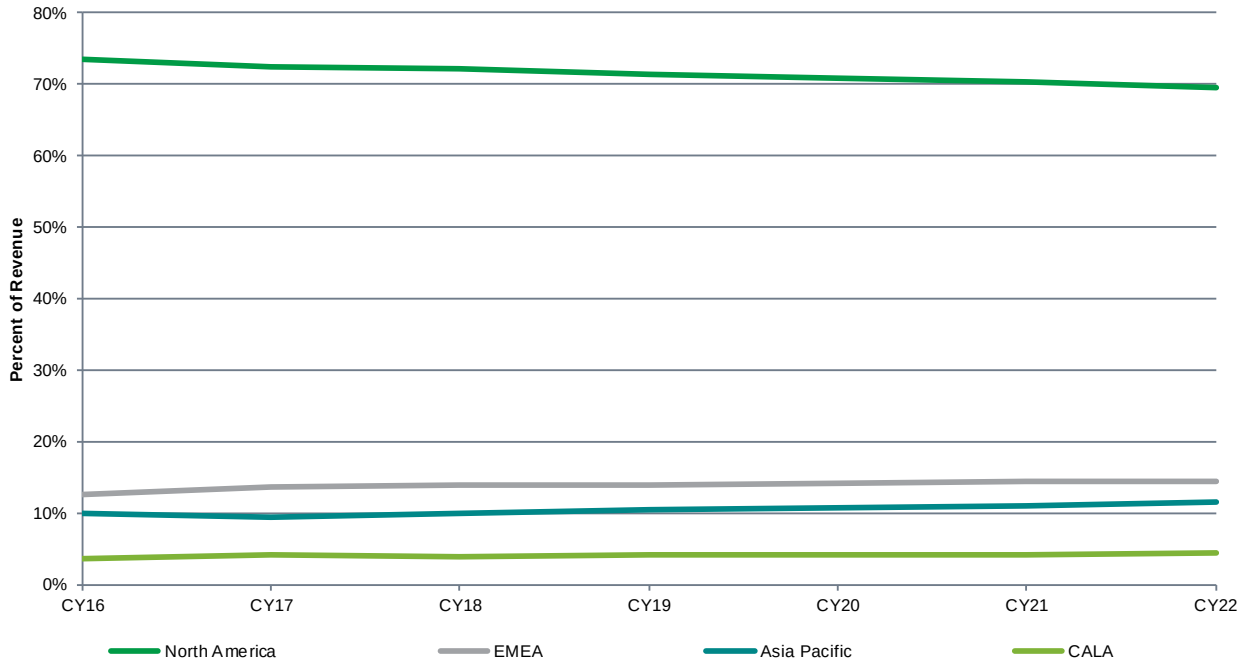
EMEA drives growth in CY17

Revenue in North America declined after two years of strong growth as companies capped investments and adopted lower cost standard Ethernet switch–based infrastructure. Still, 2017 revenue was up 12% over 2015, and monitoring ports grew 37% over 2016, showing that companies are continuing to make significant investments in monitoring infrastructure. North America is the largest region for network monitoring equipment (~3/4 of worldwide revenue), home to some of the world's largest companies, data centers operators, and service providers. They operate critical communication networks, and their networking requirements tend to be more advanced than in other regions, making them a natural fit for network monitoring deployments.

EMEA and Asia Pacific are the two other major regions for network monitoring equipment sales. EMEA declined in CY16 as companies held off making investments to consider the potential impact of Brexit, but growth returned in CY17 due to solid GDP growth across Europe. Asia Pacific, on the other hand, declined in CY17, and although vendors didn't provide specific reasons, we've seen weak results in Asia Pacific in various other equipment markets owing to slowing growth in China, the biggest economy in the region.

Looking ahead, we expect Asia Pacific to reclaim its growth leadership as most economists expect above average GDP growth in the region. EMEA and Asia Pacific will grow faster than North America, benefitting from the adoption of critical communication and networking technologies that will drive companies to deploy network monitoring equipment, as well as vendors looking beyond their home markets to drive new growth.

Exhibit 6 Monitoring equipment revenue by region (percentage)



Source: IHS Markit

Market share

Gigamon is dedicated exclusively to the network monitoring equipment market and is perhaps the best-known vendor in this space. The company was founded in 2004, went public in 2013, and was taken private by Elliott Management in 2017. Gigamon has over 2,700 customers, including 83 of the Fortune 100 companies, the 10 largest US Federal Government agencies, and 50 of the top 100 global service providers. Key enterprise buyers include government, technology, financial services, and healthcare verticals. Gigamon has a full portfolio of network monitoring equipment, addressing the whole range of deployments from small to very large.

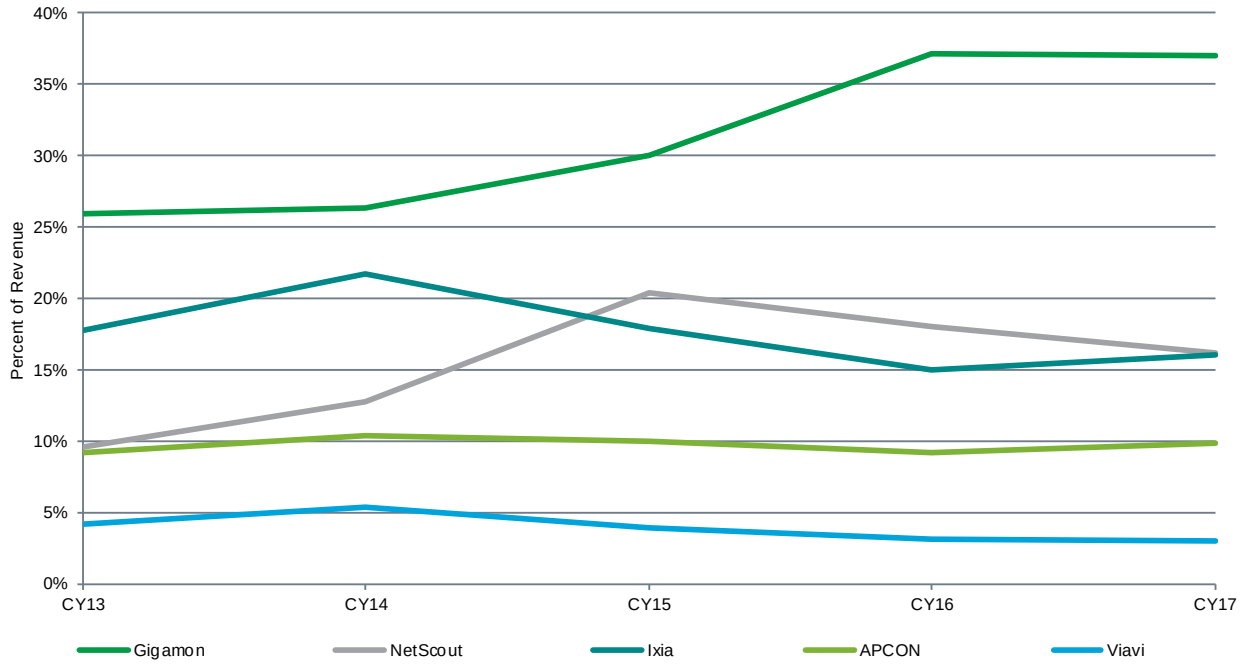
Gigamon's GigaSECURE® Security Delivery Platform interfaces between the network and the operational/security tools and enables network/security operations to capture traffic from key network points, apply services and intelligence to captured traffic, and send it on to the security/monitoring tools. GigaSMART blades are available for most of Gigamon's products and provide advanced features, such as packet filtering, header stripping, load balancing, packet slicing/masking, SSL decryption, deduplication, metadata generation, and NetFlow generation. NetFlow and de-duplication are two of the top-selling GigaSMART applications. Gigamon also offers RESTful APIs that allow third-party applications, SDN controllers, and monitoring tools to program the visibility fabric, e.g., to change traffic forwarding policies.

Gigamon has made its software available for deployment on standard Ethernet switches from Quanta and in virtualized/public cloud environments (e.g. AWS) and launched a series of lower cost traffic aggregation nodes (TA series) to allow customers to cost effectively broaden their monitoring fabrics. Gigamon expanded on its cloud visibility solution by adding support for AWS GovCloud in 2017 and Microsoft Azure in April 2018 to help customers maintain visibility as they migrate applications to cloud services providers. In 2017, Gigamon also released the GigaVUE-HC3, a new high-end platform that can process 3.2 Tbps, to address the needs of large-scale networks.

After surging 40% in CY16, Gigamon's total company revenue held steady in CY17 at $312M, supported by continuing strong enterprise and service provider demand and offset by marginally lower government demand. Security continues to be a major driver, and Gigamon is reporting healthy interest in bypass solutions, which grew 25% last year. Gigamon is the largest network monitoring equipment vendor by a solid margin, accounting for 37% of revenue in CY17, unchanged from CY16 but increasing its lead over the next closest competitor to 21%. In the government market, Gigamon's lead is even bigger at 61% of CY17 revenue.

Rounding out the vendor landscape, NetScout has become the #2 provider of network monitoring equipment (16.2% of revenue in CY17). Ixia is the third-largest vendor and accounts for 16% of revenue in CY17. APCON is the fourth largest vendor with 9.9% of revenue in CY17.

Exhibit 7 Monitoring equipment market share (revenue)



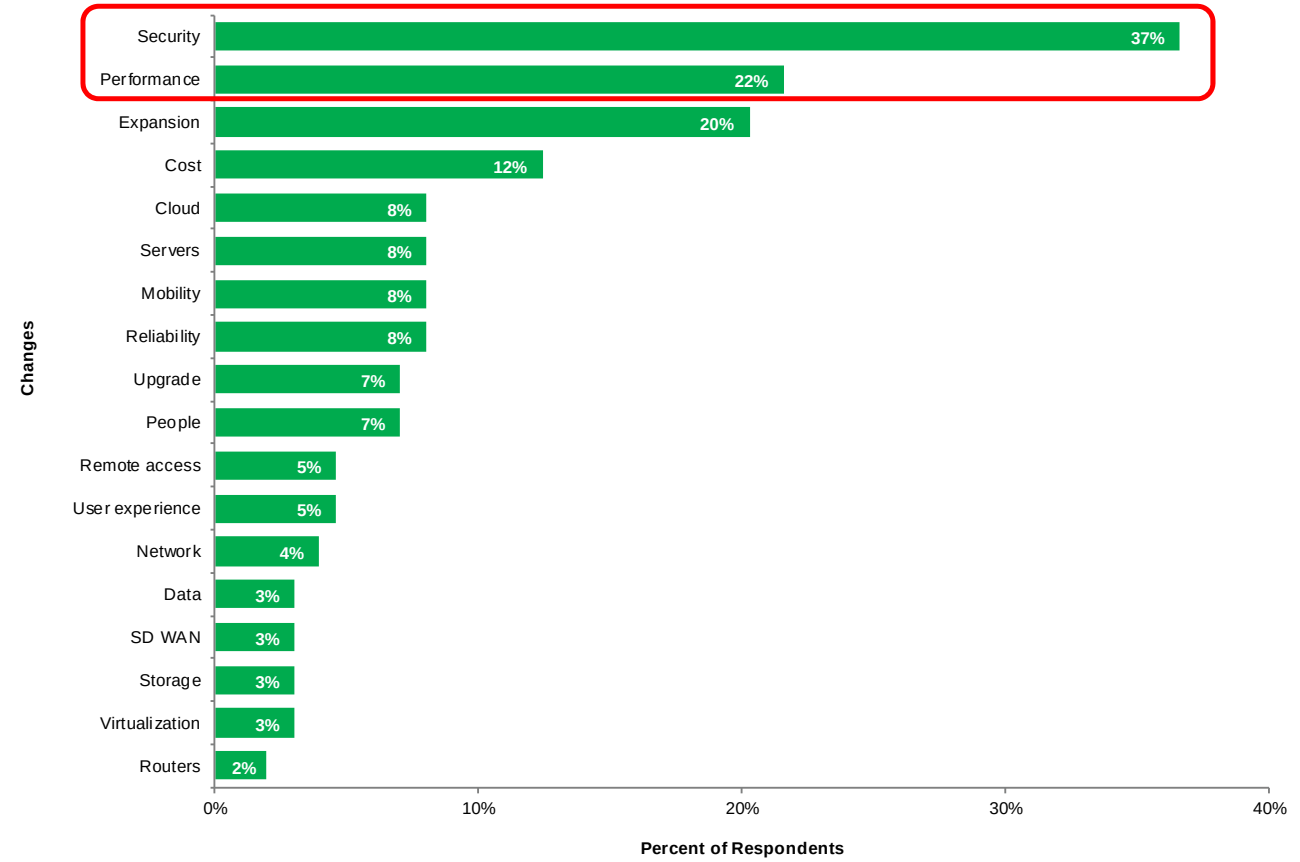
Source: IHS Markit

Market drivers

When we survey organizations about what major changes they are planning to make to their networks, time and again, the top unprompted responses revolve around improving network security and network performance. Security is a major concern for companies as hacking has evolved from hobby into a multi-billion-dollar industry. Security breaches are not some obscure event but affect millions of people, cost significant resources to remedy, and can lead to loss of customer confidence, lost revenue, fines, and in some cases bankruptcy. New applications and changes in IT architectures are driving significant growth in network traffic, driving organizations to make upgrades to ensure adequate network performance.

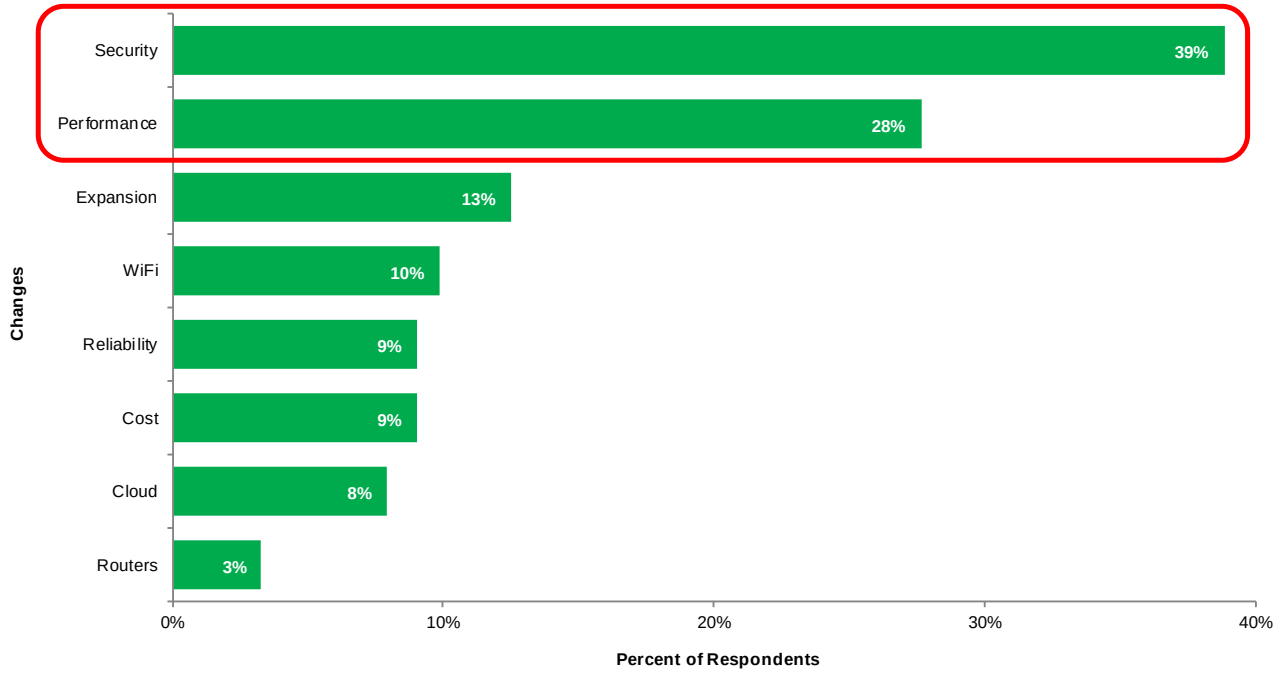
The next two charts are taken from our November 2017 *WAN Strategies* and our July 2017 *WLAN Strategies* studies and show the top three changes companies plan to make to their WAN and LAN, respectively, over the next 12 months, and the relative importance of security and performance.

Exhibit 8 WAN changes
n=153



Source: IHS Markit

Exhibit 9 Top WLAN changes
n=152



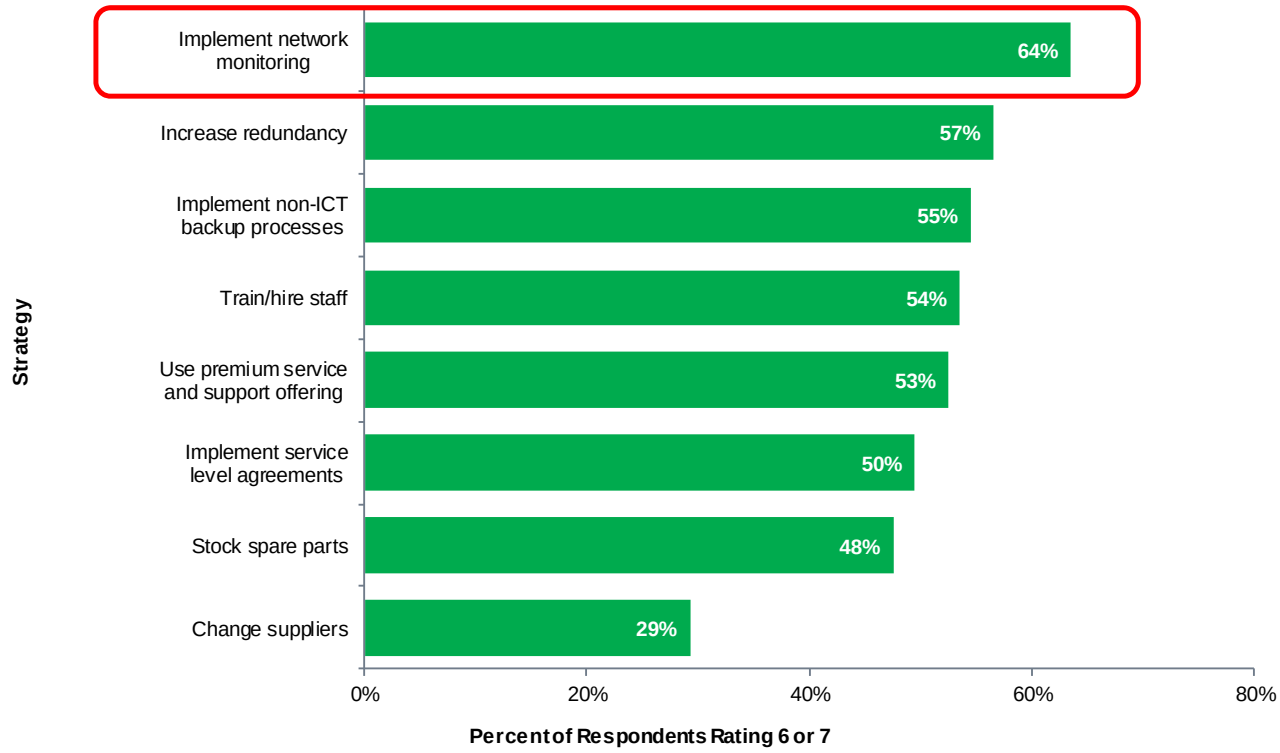
Source: IHS Markit

Improving the security and reliability of networks are the key drivers of the network monitoring equipment market. As a critical component of IT and communication infrastructure, network outages or degradations have a widespread impact on the availability of IT applications, which in turn reduces productivity and leads to lost revenue. When outages and degradations are caught early on, their impact on the organization can be minimized. Organizations understand this relationship, which is why they are making network performance and security a priority.

In our January 2016 study *The Cost of Server, Application, and Network Downtime*, which examined the frequency, length, cost, and causes of information and communication technology (ICT) downtime, such as servers, applications, and the network, we found that the cost of ICT downtime is substantial, from $1M/year for a typical mid-size company to over $60M for a large enterprise. In aggregate, downtime is costing North American organizations $700B per year. The biggest impact of downtime is on employee productivity, which accounts over 70% of total downtime cost, followed by revenue losses at 20% of the cost. Network interruptions are the top source of downtime and have far-reaching consequences: applications, servers, and devices may all be working fine, but they can't communicate with each other when the network is down, and all activity reliant on access to applications stops.

The top strategy to reduce downtime is to implement network monitoring. Downtime events are going to happen no matter what, and the key to reducing the impact of downtime on the organization is to shrink the duration of each event. This starts with identifying the beginning of the event as soon as it happens, not by learning about it from end-users, or worse, customers. The high level of service degradations, rather than complete outages, makes downtime events even harder to identify. Monitoring systems alert IT staff right away when performance metrics aren't met, allowing them to work on a fix immediately and shave crucial minutes or hours off the length of each downtime event.

Exhibit 10 Reducing the impact of ICT downtime



Source: IHS Markit

Contacts

Matthias Machowinski
Senior Research Director and Advisor
Enterprise Networks and Video
+1 617.914.0240
Matthias.Machowinski@ihsmarkit.com

IHS Markit Customer Care:

CustomerCare@ihsmarkit.com
Americas: +1 800 IHS CARE (+1 800 447 2273)
Europe, Middle East, and Africa: +44 (0) 1344 328 300
Asia and the Pacific Rim: +604 291 3600