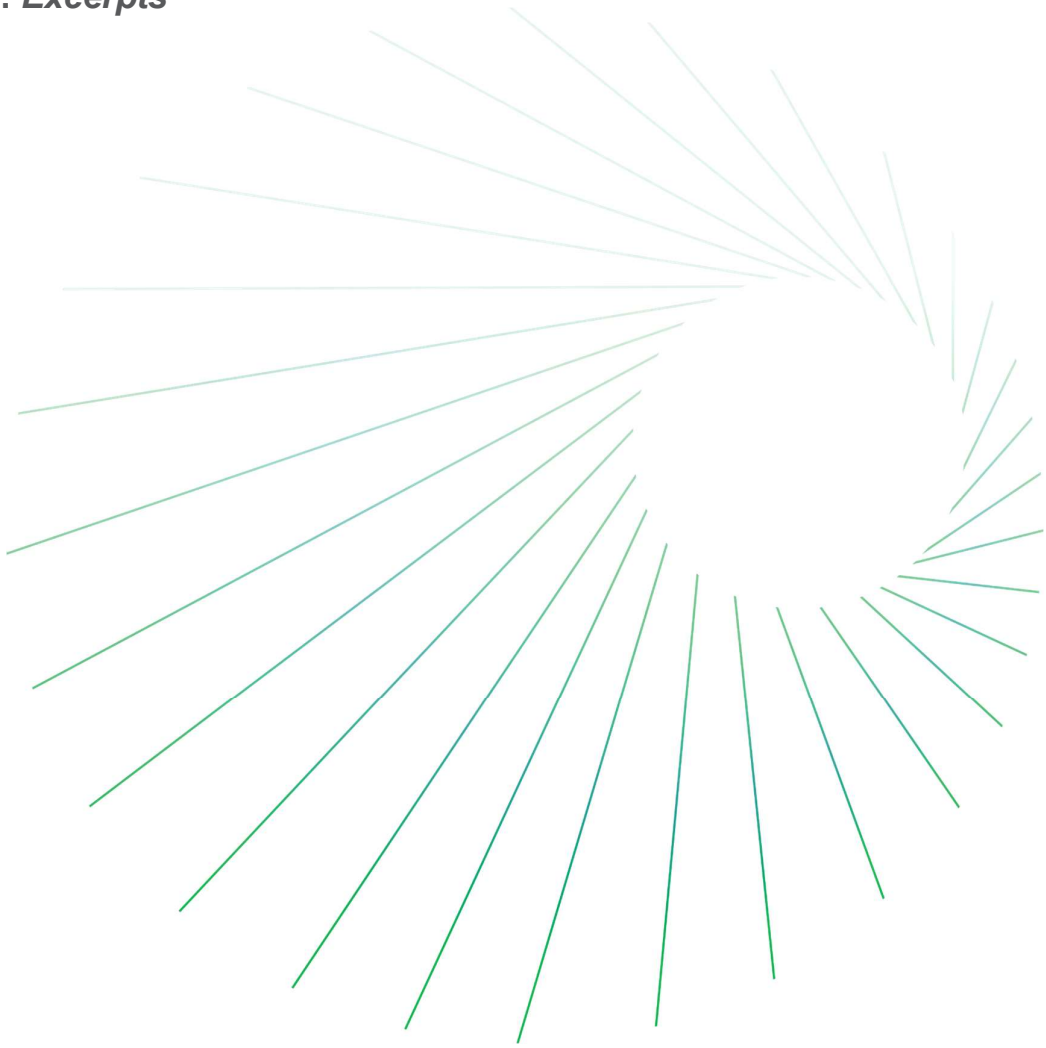
Network Monitoring Equipment

Annual Market Report: ***Excerpts***

9 August 2019



Matthias Machowinski
Senior Research Director and Advisor
Enterprise Networks and Video

IHS Markit Technology | **Report**

Contents

Exhibits

Top takeaways: Monitoring equipment revenue back to growth in 2018; open switches take share

After declining in CY17, the network monitoring equipment market returned to small growth in CY18, up 2% to $593M, driven by strong growth in government and a return to growth in the enterprise market. Service provider demand remains sluggish ahead of broader 5G rollouts in CY20, and adoption of lower cost open switches is putting pressure on revenue growth. But the number of monitoring ports shipped grew significantly in CY18, showing that organizations are continuing to broaden network visibility to make their networks more secure and reliable. We expect growth to accelerate as service provider demand recovers and project revenue of $789M by CY23 for a five-year CAGR of 6%.

Key data points:

- Advanced switches accounted for 71% of monitoring switch sales in CY18 due to growing interest—particularly with service providers—in open switches, which are based on standard Ethernet switches.
- The number of monitoring ports shipped grew 17% in CY18 to nearly 500K. 10G ports are most common and had a good year but are getting near their peak. 40G growth has slowed dramatically over the last two years while 100G nearly doubled in CY18 and are approaching the number of 40G ports. The next phase will be the adoption of 400G. There were a few initial monitoring port shipments in CY18 to service providers in Asia Pacific, and we expect deployments to broaden significantly over the next few years as data center operators go through the next network upgrade cycle from 25/100G to 100/400G.
- Government continued its strong performance from CY17 and grew at a double-digit rate in CY18, up 17%. Enterprise returned to growth (up 1%), and service provider declined again, albeit at a lower rate (-2%).
- North America is the largest region, accounting for almost two-thirds of total revenue. North America declined again after two years of strong growth as companies capped investments and adopted lower cost open switches. EMEA has been growing at a double-digit rate for the last two years, buoyed by solid GDP growth and relatively lower penetration of monitoring equipment. Asia Pacific grew 44%, coinciding with the ramp of 5G deployments in the region. Going forward, we expect above average growth in EMEA and Asia Pacific as adoption ramps up outside North America and vendors look to growth beyond their home markets.
- Gigamon is the largest network monitoring equipment vendor, accounting for 36.0% of revenue in CY18 (up 0.2 points from CY17) and increasing its lead over the next closest competitor to 21 points. Ixia moved into the #2 position with 14.6% of revenue (down 0.9 points), and NetScout rounded out the top three with 13.7% of revenue (down 2 points).

This document is an excerpt; please contact IHS Markit for the full report.

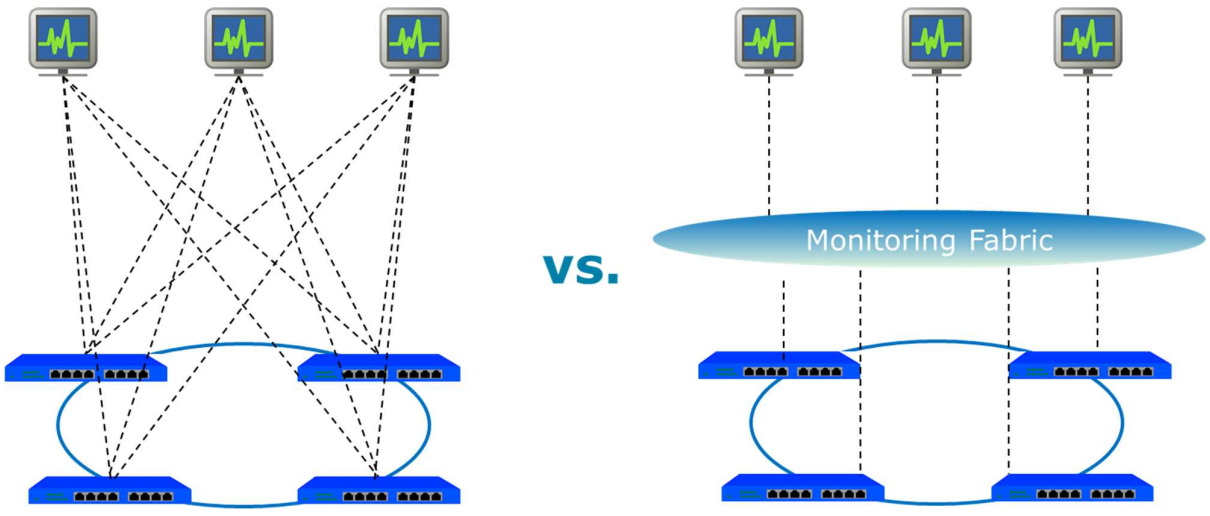
Background

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 side) and one where traffic is first tapped by a monitoring fabric and then sent on to the tools (right side). With a fabric, traffic is tapped once and retransmitted to as many tools as needed.

Exhibit 1 Monitoring equipment diagram



Source: IHS Markit

The adoption of modern IT architectures is creating new blind spots for network monitoring fabrics. Server virtualization and OS containerization means that traffic between virtual machines and/or containers may not leave a physical server at all, making it impossible to tap this traffic at the network core or access layer. Many organizations are adopting infrastructure as a service, such as compute and storage, which is delivered from the data centers of large public cloud services providers, where organizations can't physically place network taps. Vendors have responded by implementing various software connectors for popular public and private cloud infrastructures, including VMware, OpenStack, Amazon AWS, and Microsoft Azure, to extend visibility into these cloud deployments and allow organizations to extract relevant traffic.

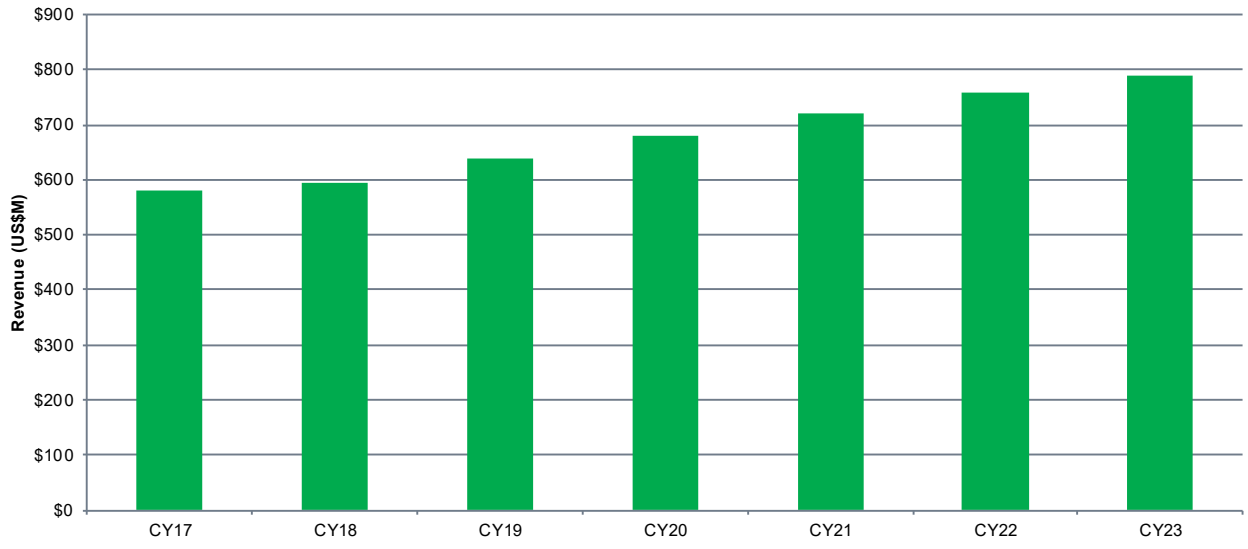
Network monitoring equipment revenue back to growth in CY18

Network monitoring equipment growth was brisk in CY15 and CY16, growing 26% and 17%, 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. In CY17, revenue declined 1% because of weakening enterprise and service provider demand and the adoption of open switches, which carry significantly lower price points. CY18 was back to small growth with revenue reaching $593M, up 2% over CY17, driven by strong growth in government and a return to growth in enterprise but offset by a small decline in service provider demand. The service provider segment remains challenging as service providers grapple with bringing capex in line with revenue. According to IHS Markit's *Service Provider Revenue and Capex* report published in May 2019, service provider revenue grew 2.3% in CY18, and capex spending grew significantly slower, at 0.8%.

Adoption of open switches is putting pressure on revenue growth as the revenue contribution of hardware is declining; this isn't necessarily a negative development as vendors' key differentiators are in their software, and software has much higher margins. Still, during this transition vendors will find it difficult to grow their top-line revenue.

For CY19, we expect growth to accelerate as enterprise spending benefits from a positive economic backdrop, government spending stays strong, and service provider capex enters a new growth cycle. Fundamentally, this market is driven by the need for robust network monitoring capabilities to ensure the performance of mission-critical network infrastructure. We project CY19 revenue to grow 8% to $638M and long-term revenue of $789M by CY23, a five-year CAGR of 6% (versus a CY13–17 CAGR of 10%). Since the last edition of this service, we have reduced the five-year forecast by 2%, primarily due to a declining TAP/bypass switch contribution.

Exhibit 2 Monitoring equipment forecast



Source: IHS Markit

Gray right-side border denotes analysis updated since the last edition of this report.

Government continues to drive growth

The government vertical continued its strong performance over the past few years, growing at a double-digit rate in CY18. Enterprise demand returned to small growth, buoyed by generally positive economic conditions. This year, we asked vendors for additional feedback on their enterprise customers, and although we didn't get enough data to add official segmentation to the tracker, our discussions revealed the following:

- The majority of enterprise demand comes from large enterprises (>1,000 employees), which have very large networks with hundreds of network elements dispersed around the globe underpinning mission-critical business processes. There is very little demand (<5%) coming from small businesses (<100 employees), whose IT needs are less demanding, with networks small enough to negate the need for monitoring networks. The balance, about 1/3, comes from medium enterprises (100–1,000 employees), and we expect them to be a growth area as they have historically lagged in adoption but now seek to make their infrastructure as secure and reliable as those of large organizations.

- Finance is the #1 vertical by far, and we estimate that it is on par if not bigger than government. The finance industry is well known for running extremely high-performing networks to ensure timely transmissions of transactions, has the resources to invest, and must adhere to numerous regulations.

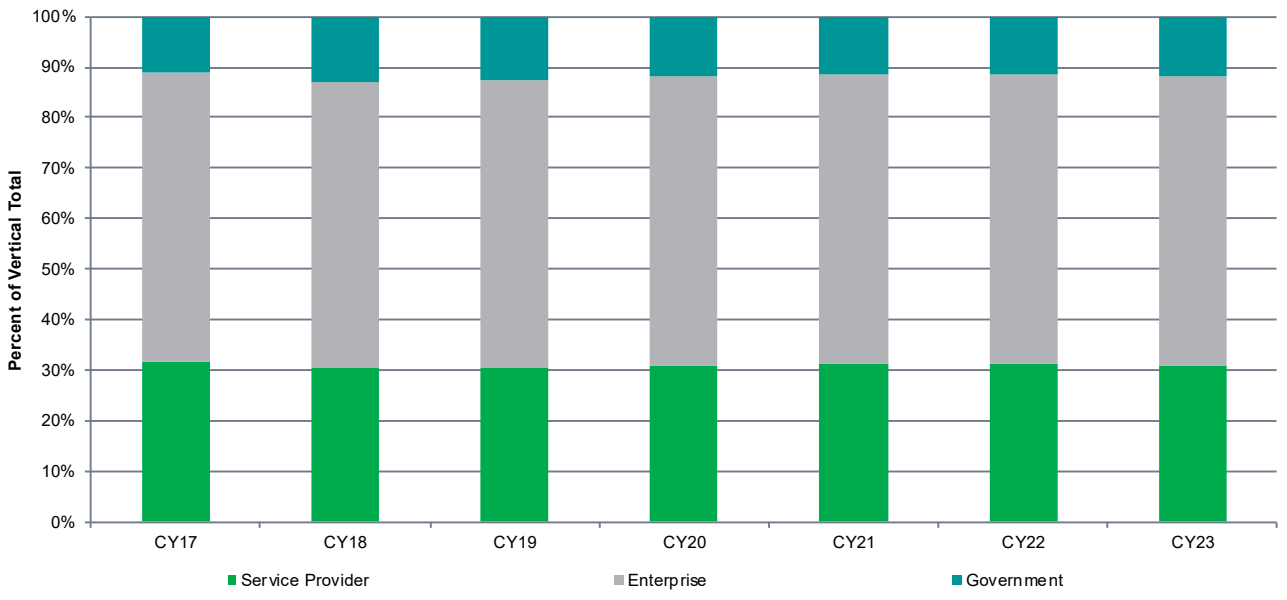
- The #2 vertical is technology, which includes SaaS providers and other companies that rely heavily on web technologies to deliver their services. Because network performance directly impacts their customers' experience, they invest heavily in monitoring.

- Beyond the top two verticals, the field widens: vendors mentioned demand from healthcare, manufacturing/industrials, higher education, transportation, and energy. Retail was mentioned as an emerging opportunity.

Service provider revenue was down 2% as they kept capital expenditure growth below revenue growth projections and have been early adopters of open switches, which have significantly lower ASPs.

There will be annual growth variations due to cyclical buying patterns, and long-term, we expect government demand to lag enterprise and service provider. Enterprise growth will be driven by down-market expansion, e.g. into medium enterprises. Service provider growth will be driven in part by the next capex cycle, which is centered on spending on 5G networks, which started in 2018 (less than $1B) but will really take off over the next few years and peak in CY20 at $20B. In general, monitoring is critical for service providers to deliver their services, and they will need to upgrade monitoring infrastructure to keep up with the significantly higher capacity and resulting traffic growth enabled by 5G. In addition, 5G is expected to support new edge computing intensive use cases like autonomous vehicles, which will further drive the need for pervasive monitoring as mobile networks underpin mission-critical communications.

Exhibit 3 Monitoring equipment by vertical



Source: IHS Markit

Advanced switches decline

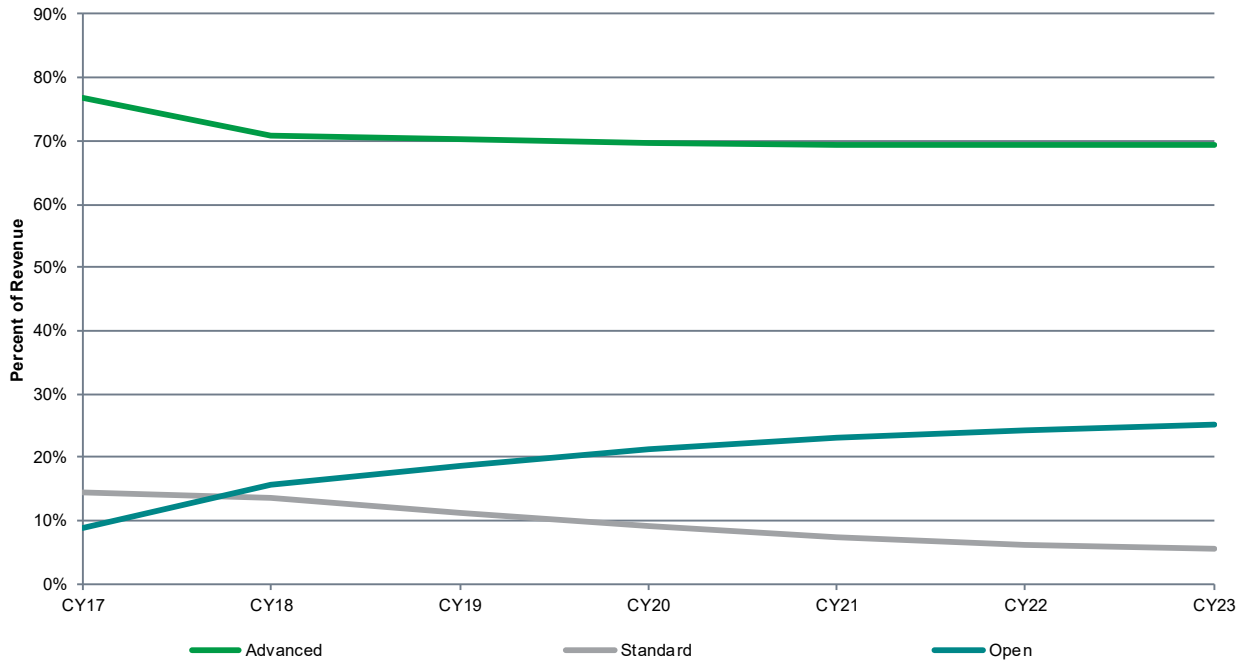
Standard switches simply forward traffic to the relevant tools. Advanced switches have additional packet processing capabilities built in that can be applied to captured traffic. These include among others:

- 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 (71% in CY18), but their contribution is declining (down 6 points this year) because of growing interest—particularly with service providers—in open switches, which are based on standard commercially available Ethernet switches. The trend toward open switches (16% of revenue in CY18, up 7 points) has manifested itself in a number of ways over the past few years. Initially, startups like Big Switch developed proprietary monitoring software that leveraged standard 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 monitoring 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. Open switches don’t support advanced packet processing (yet), which is done on external service nodes or advanced switches, but 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.

Exhibit 4 Monitoring switches: Advanced versus standard versus open



Source: IHS Markit

Need for speed: 100G takes off, 40G hangs on, 400G coming

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 good year, but looking ahead, we think 10G is getting near its peak and will see only small growth in the coming years.

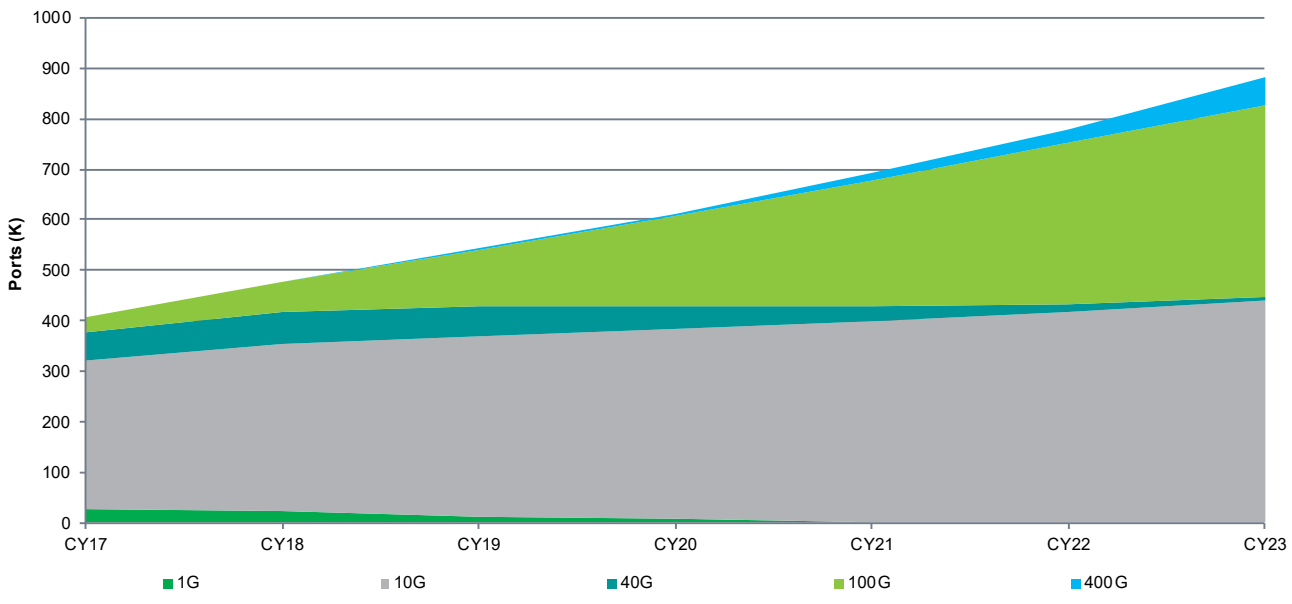
40G was the new high-growth market until CY16, but growth has slowed dramatically since. This is in line with trends in production networks, where 40G port shipments declined for the first time in CY17 as data center operators shift to 25/100G.

100G had a banner year in CY18 with ports nearly doubling and approaching the number of 40G ports. 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, which in turn is accelerating demand for 100G on monitoring switches.

The next phase in port speeds will be the adoption of 400G. 400G is in its very beginning in production networks, and there were a few initial monitoring port shipments in CY18 to service providers in Asia Pacific. We expect deployments to broaden significantly over the next few years as data center operators go through the next network upgrade cycle from 25/100G to 100/400G.

Finally, port shipments overall experience healthy growth at roughly twice the rate of revenue growth. Improving performance and security is a perennial goal of network operators, and availability of lower cost solutions will enable companies and service providers to monitor their networks more pervasively.

Exhibit 5 Monitoring switch port shipments



Source: IHS Markit

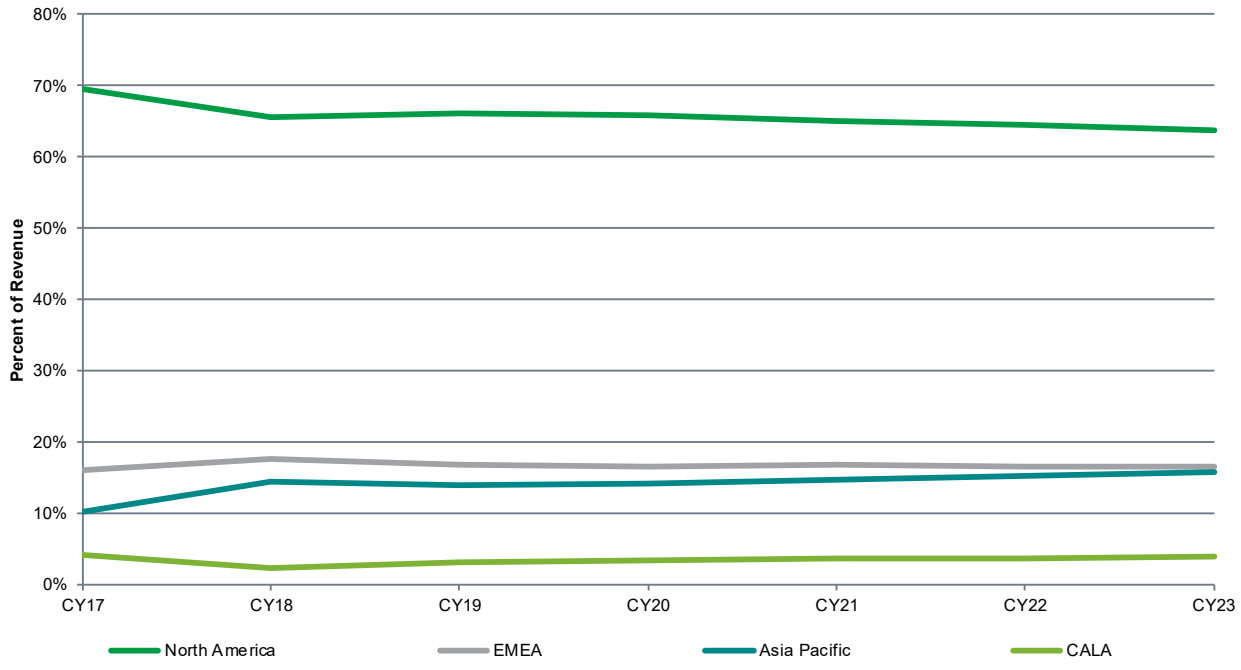
Asia Pacific, EMEA drive growth in CY18

Revenue in North America declined again as companies capped investments after a big ramp in CY15 and CY16 and adopted lower cost open switches. Still, CY18 revenue was up 8% over CY15, and monitoring ports grew 1% over CY17, showing that companies are continuing to make significant investments in monitoring infrastructure. North America is the largest region for network monitoring equipment (~2/3 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. We don't think that's going to change anytime soon, ensuring that North America will remain the top revenue contributor for network monitoring equipment for the foreseeable future.

EMEA and Asia Pacific are the two other major regions for network monitoring equipment sales. EMEA has been growing steadily at a double-digit rate for the last two years, buoyed by solid GDP growth and relatively lower penetration of monitoring equipment. Brexit hasn't had a noticeable impact so far, but we expect slower growth in CY19/20 as the UK leaves the EU. Asia Pacific grew strongly in CY18, up 44%, coinciding with the ramp of 5G deployments in the region. Vendors called out Japan, Korea, Singapore, Vietnam, and Bangladesh for contributing to growth.

Looking ahead, we expect Asia Pacific to continue its growth leadership as economists forecast 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 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 3,000 customers, including 83 of the Fortune 100 companies, 60% of the Fortune 500, and 45% of the Fortune 1000; the 10 largest US Federal Government agencies; and 8 of the top 10 mobile network operators. Key enterprise customers come from the financial services, healthcare, and technology industries. Gigamon has a full portfolio of network monitoring equipment, addressing the whole range of deployments from small to very large.

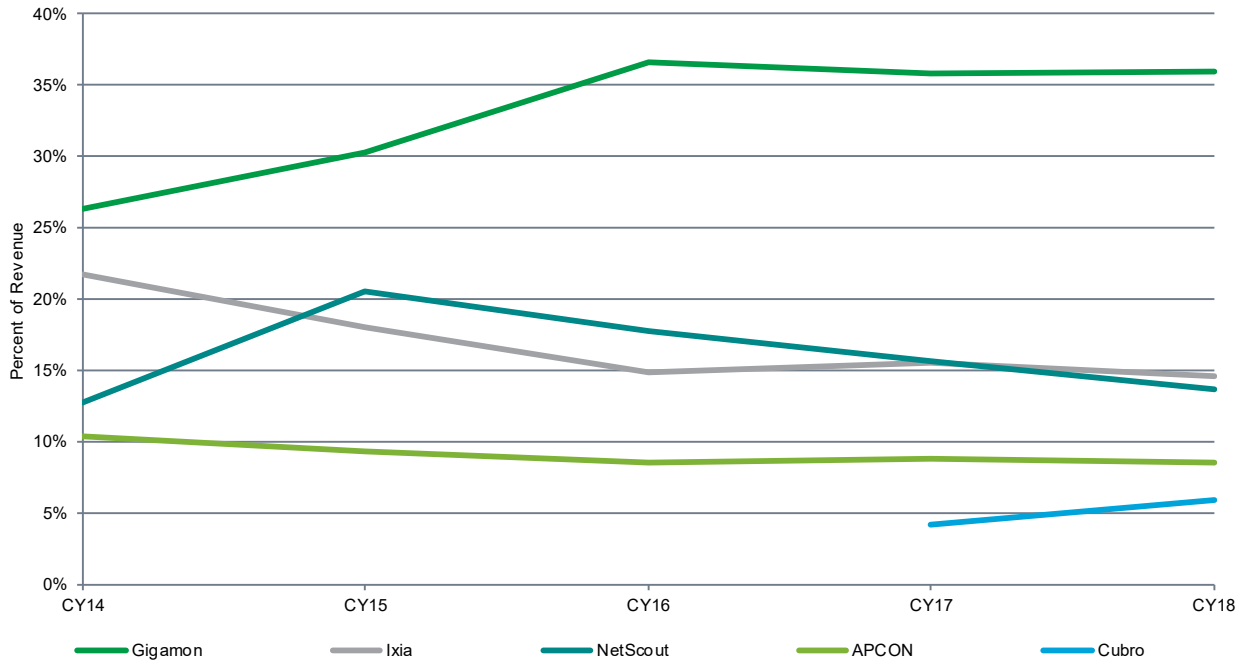
Gigamon's Visibility Fabric enables network and/or security operations teams to extract traffic from key network points, apply services and intelligence to the captured traffic, and send it on to security and monitoring tools. At the core of this platform is the GigaVUE HC series, its latest generation of visibility appliances, all of which support advanced packet conditioning features (GigaSMART), such as packet filtering, header stripping, load balancing, packet slicing/masking, SSL decryption, deduplication, metadata generation, and NetFlow generation. NetFlow and deduplication are among the top-selling GigaSMART applications. To cost effectively broaden the reach of monitoring fabrics, Gigamon offers traffic aggregation nodes (GigaVUE TA series) based on standard Ethernet switch designs and is making its operating system available for deployment on bare metal Ethernet switches from Quanta.

As organizations migrate their applications to cloud architectures, Gigamon has implemented various software connectors for private and public cloud environments, including AWS, Microsoft Azure, VMware, and OpenStack, to help customers maintain complete visibility. Container visibility is currently under development. Gigamon also offers RESTful APIs that allow third-party applications (e.g. Ansible), SDN controllers, and monitoring tools to program the visibility fabric (e.g., to change traffic forwarding policies).

Over the past year, Gigamon has focused on expanding its analytics capabilities. In July 2018, it acquired security firm ICEBRG (since rebranded to Gigamon Insight), which is a cloud-based application that detects network security threats and recommends responses. In May 2019, it launched its Application Intelligence framework, which can identify over 3,000 IT applications, visualize network usage of applications, forward specific application traffic to operational tools for further analysis, and send application metadata (e.g., file names, time stamps) to security/performance tools.

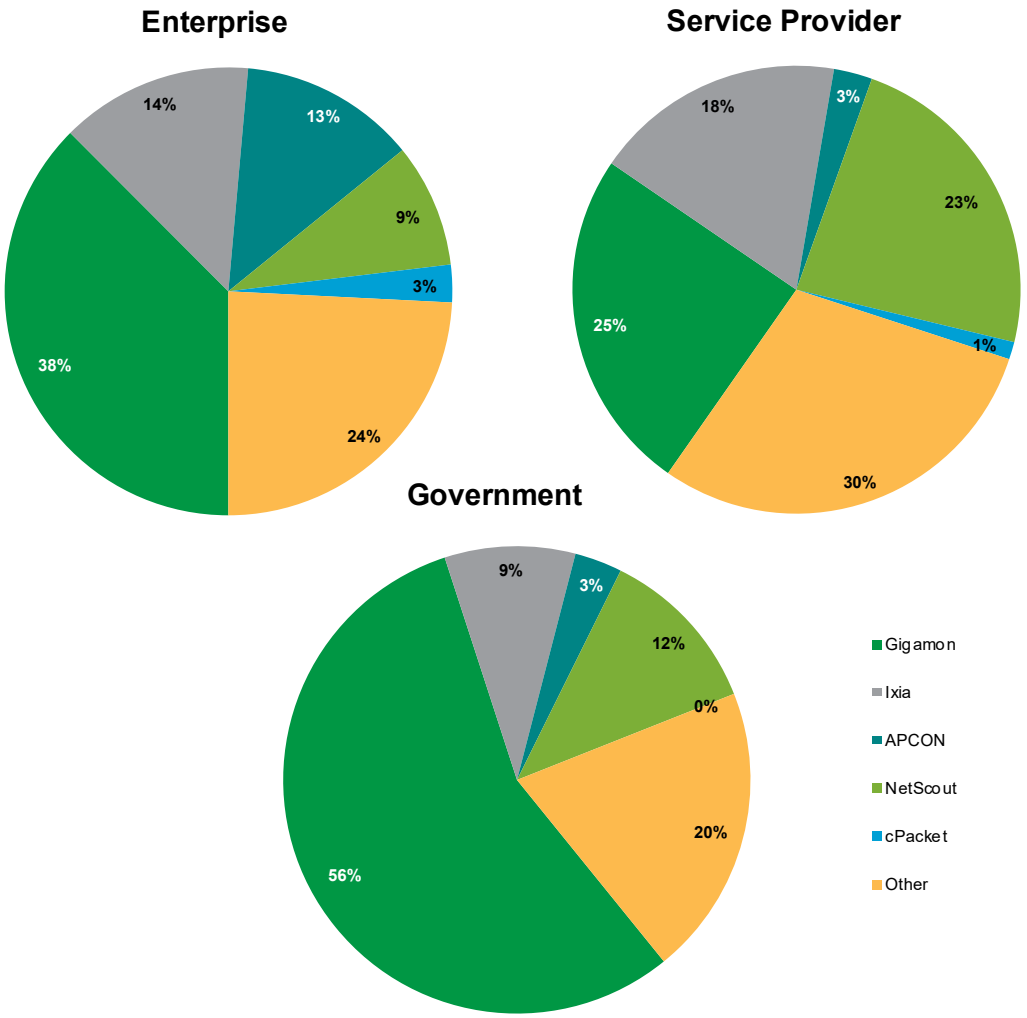
Gigamon's network monitoring equipment revenue grew 3% in CY18, supported by continuing enterprise demand and growth in government and offset by marginally lower service provider demand. Gigamon reported strong demand in advanced services, 100G solutions, and high-end monitoring switches like GigaVUE HC3, as well as expansion in entry-level solutions like GigaVUE HC1. Gigamon is the largest network monitoring equipment vendor by a solid margin, accounting for 36.0% of revenue in CY18, up 0.2 points from CY17 and increasing its lead over the next closest competitor to 21 points. In the government market, Gigamon's lead is even bigger at 56% of CY18 revenue, and Gigamon also leads the service provider market with 25% share.

Exhibit 7 Monitoring equipment market share (revenue)



Source: IHS Markit

Exhibit 8 Monitoring equipment market share by vertical (revenue)



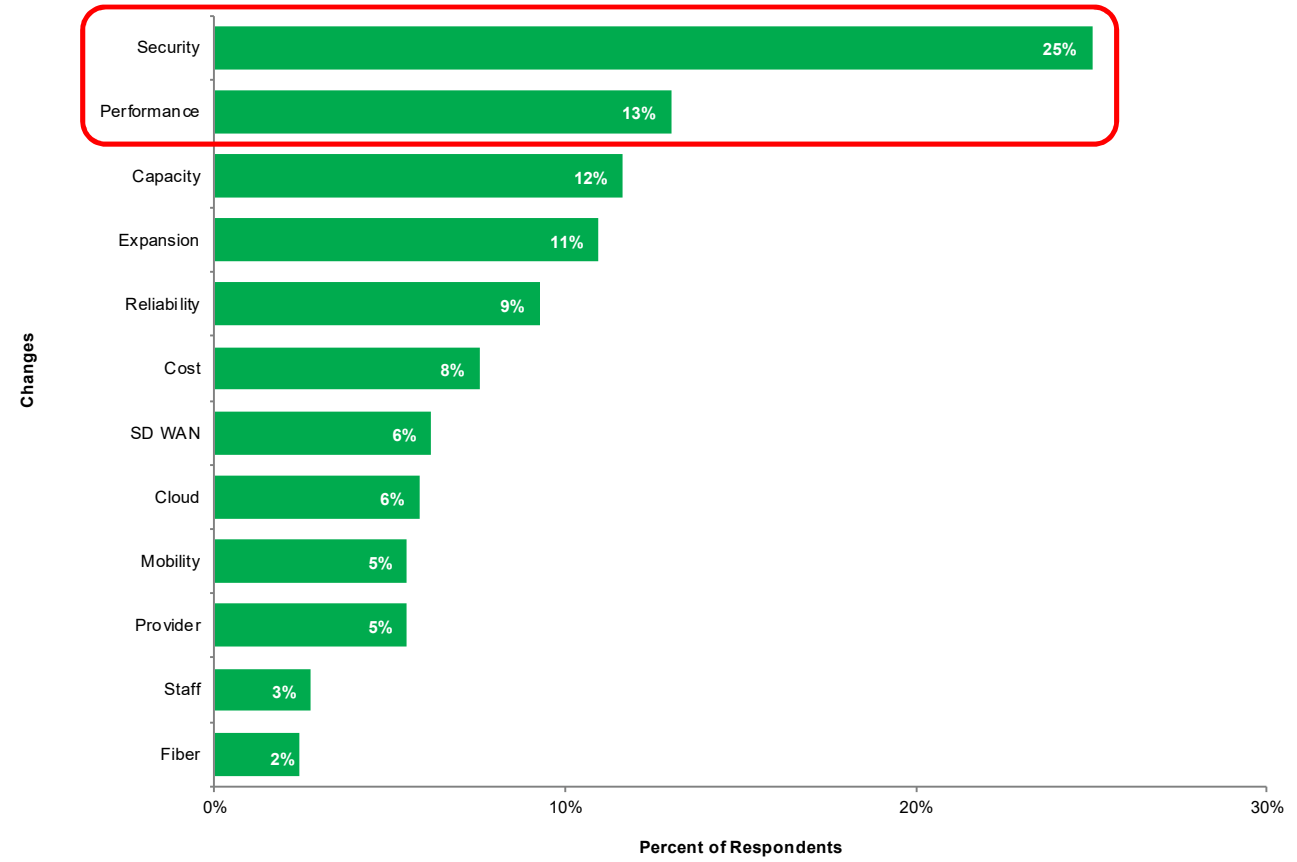
Source: IHS Markit

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.

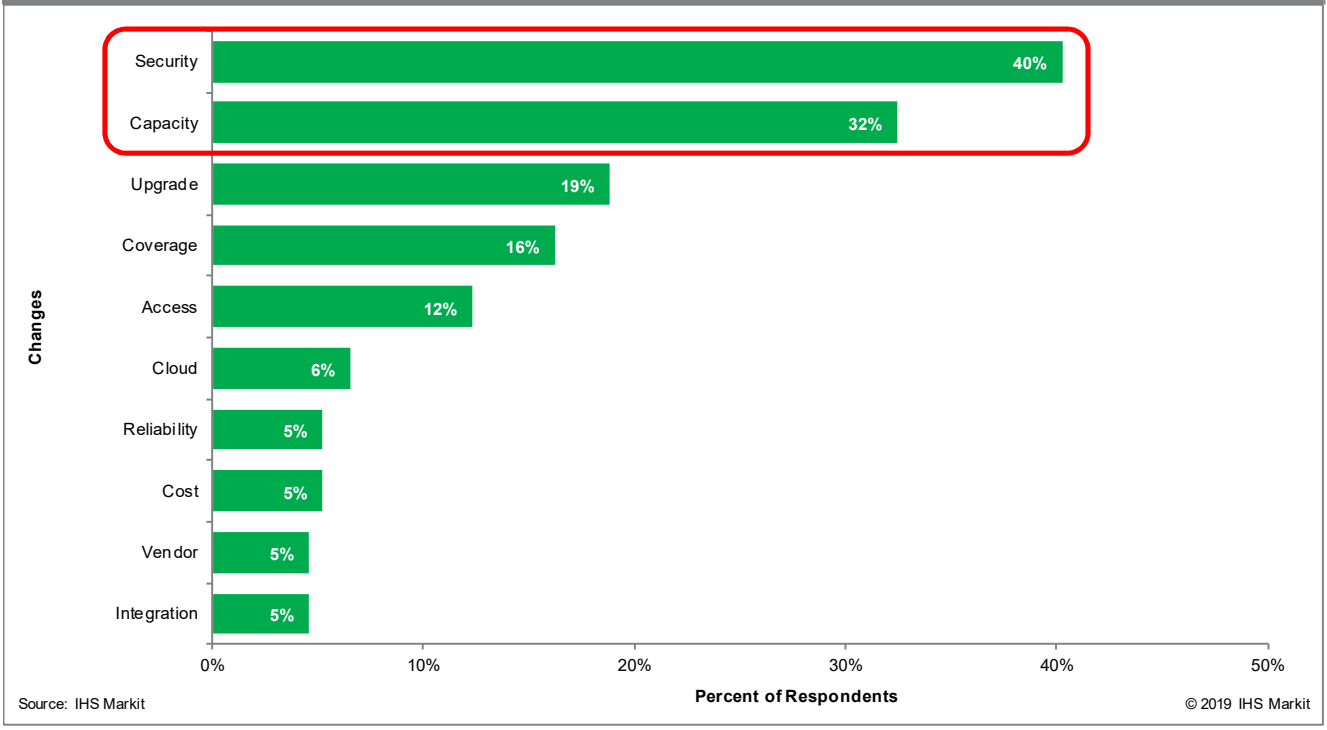
The next two charts are taken from our February 2019 *Enterprise Edge Connectivity Strategies* and our June 2018 *WLAN Strategies and Vendor Leadership* studies and show the top three changes companies plan to make to their WAN and LAN, respectively, over the next 12 months, and the relative importance of security and performance.

Exhibit 9 WAN changes
n=292



Source: IHS Markit

Exhibit 10 Top WLAN changes
n=154

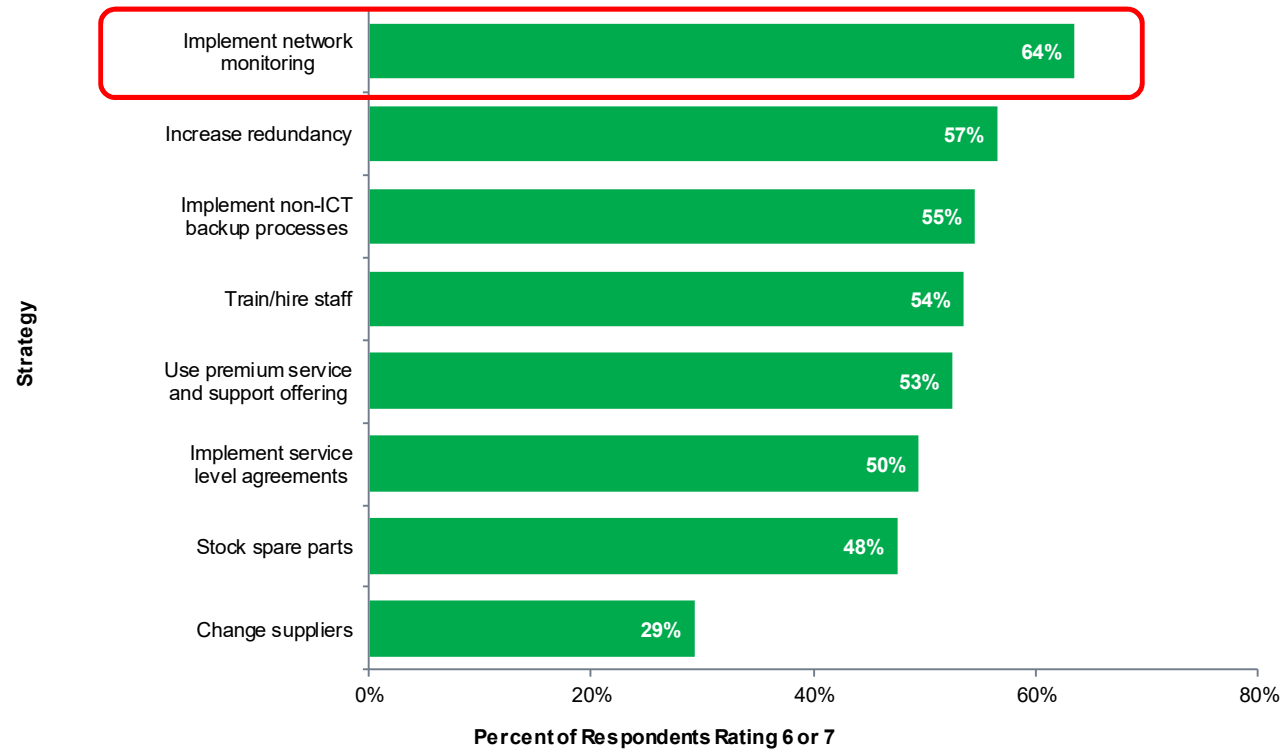


Improving the security and reliability of networks are the key drivers of the network monitoring equipment market. As a critical component of IT and communication infrastructure, network outages or degradations have a widespread impact on the availability of IT applications, which in turn reduces productivity 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 11 Reducing the impact of ICT downtime



Source: IHS Markit

Category definitions

Below are the definitions for the products included in this service. Please see *Methodology* in the market size/share/forecasts Excel file, located in the service portal section for this report.

Network monitoring equipment: Used to build parallel monitoring networks that coexist alongside production communication and data networks; consists of the following segments

- **Monitoring switches:** Dedicated switches that duplicate and forward network traffic to network management, monitoring, and/or security systems for network visibility and traffic analysis
    - **Standard:** Monitoring switches that only forward traffic; may have filtering capabilities
    - **Advanced**: Proprietary switches with additional packet processing capabilities such as header modification, deep packet inspection, packet slicing, data masking, deduplication, SSL decryption, etc.
    - **Open:** Based on off-the-shelf Ethernet switch hardware designs; includes both the switch hardware and switch operating system software (if sold separately)
- **Taps/bypass switches:** Devices that are inserted into network links; taps send copies of network traffic to out of band monitoring devices; bypass switches can redirect traffic to in-line monitoring/security appliances or let traffic flow unimpeded, depending on the health of the appliance

Customer types: Network monitoring equipment sold to the following types of organizations:

- **Service provider:** Provide IT and communication services; includes telcos, competitive and mobile carriers, and cloud services providers
- **Enterprise:** Small, medium, and large businesses
- **Government:** Governmental organizations

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