THE CHANNEL

| Channel Issues and Advice |

Feb 2016

Contents

This Service has been designed specifically for Senior level Channel executives. It provides guidance and highly strategic advice on the channels focussing on the issues of which Senior Channel Executives should be aware. It will guide the management team on the impact of competitor announcements, insights into the market, brief focus on services sub-segments, value stack, vertical focus and Key Director Messages.

1 SLA – Senior Level Advisor

Atos

Key Executives:

Thierry Breton
Chairman and CEO

Michel-Alain Proch
Senior Executive Vice President

Charles Dehelly
Senior Executive Vice President

Gilles Grapinet
Senior Executive Vice President

Atos

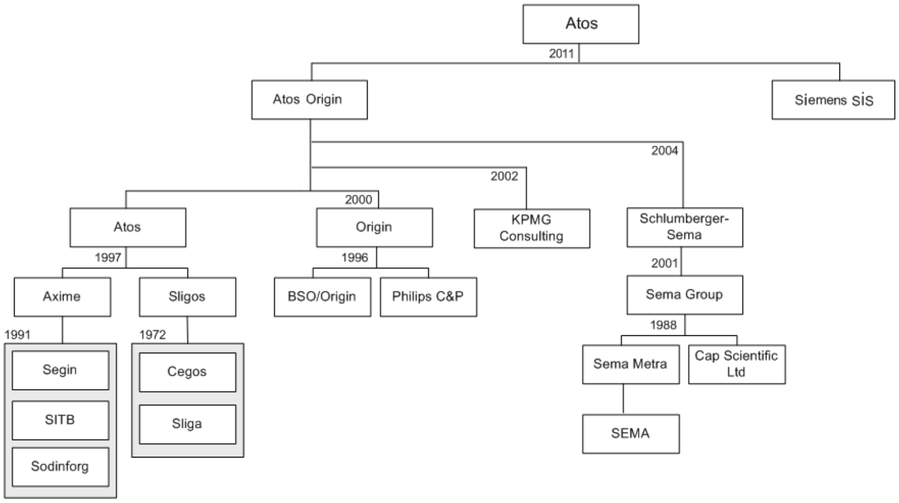
Atos SE (Societas Europaea) is a leader in digital services with circa 100,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry.

Acquisitions

In 2011 Atos acquired the French software company blueKiwi and in early 2012, rolled out its ZEN social networking software across its organization (gleaning a great deal of publicity in banning email which employees in France are not required to read after work hours). In August, 2014 Atos announced that it had acquired a controlling stake in Bull SA through a tender offer launched in May and gained full control in 2014.

In December 2014, Atos announced the acquisition of Xerox's IT Outsourcing business for $1.05B to increase its presence in the US.

In November 2015 Atos announced the acquisition of Unify from Gores and Siemens for $340M. The close relationship with Siemens, a $100M joint venture is still in place (since 2009), continues with this acquisition which was finalized at Unify’s Industry Analyst Event in Bermuda in January.



By Original uploader was PïcsLogoLoader at fr.wikipedia. Later version(s) were uploaded by Doudou38 at fr.wikipedia. - Transferred from fr.wikipedia; transferred to Commons by User:Bloody-libu using CommonsHelper., CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=19286998

Brands

Bull atos technologies · worldline e-payment services · canopy the atos cloud · bluekiwi An Atos Company · Atos Consulting · Atos Worldgrid · UNIFY atos collaboration solutions

The Unify brand will be retained for the communication products but the services will move to the Atos organization in a similar way that Bull has been managed.

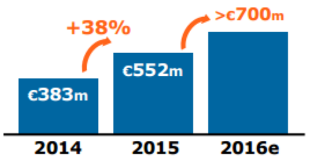
Markets

With its deep technology expertise and industry knowledge, the Atos Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

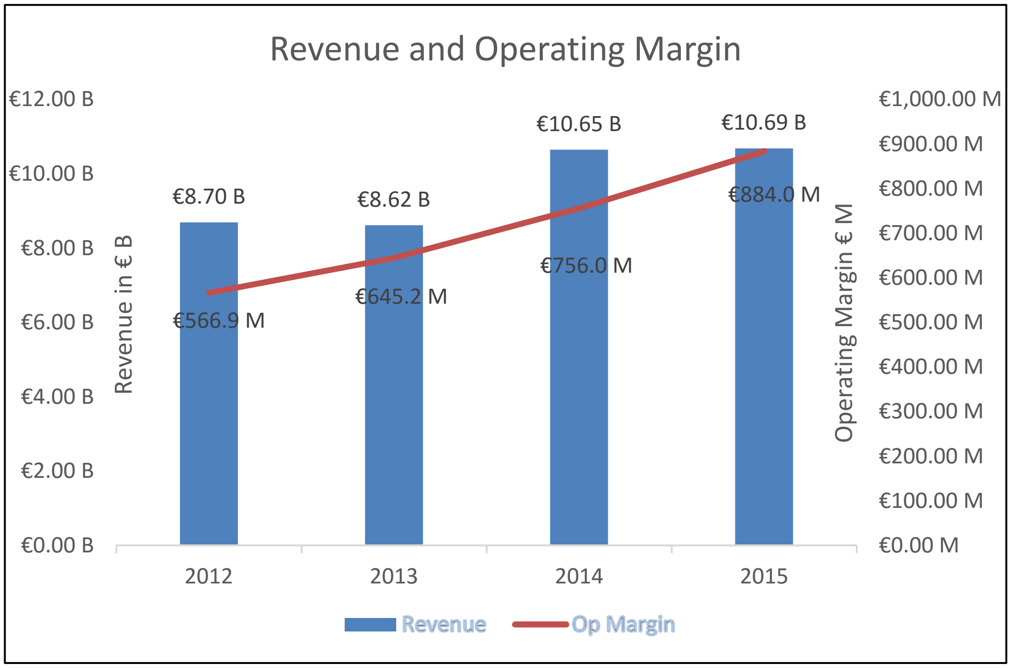
Technologies

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.

Managed Services



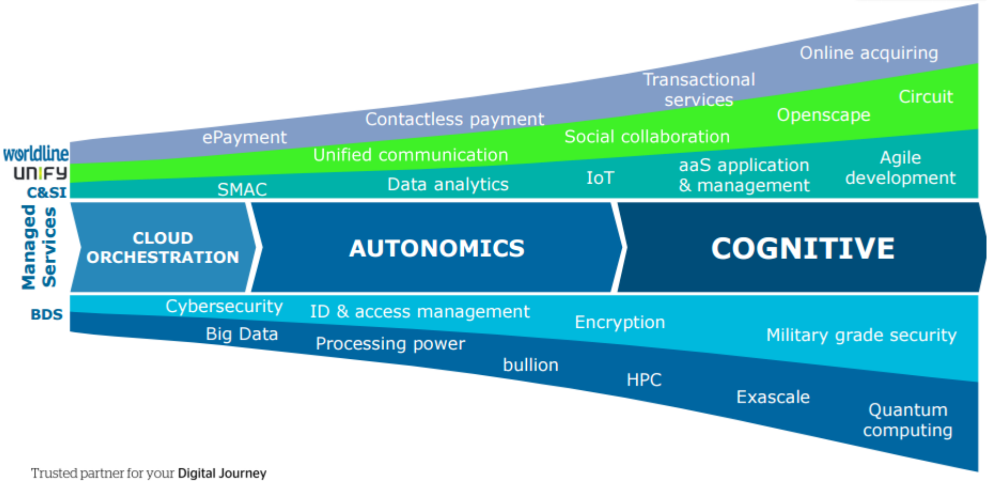
Financials



Source: Company Financial Results Year end 31 December

Strategy

Atos describes its strategy and direction in the following graphic.



Conclusion

One of the 2016 priorities for Atos is to "leverage its Managed Services backbone to enhance all our activities". Canopy, which was formed with EMC and VMware in 2012, has achieved $500B in annual revenues. Atos re-integrated the Canopy subsidiary and make it part of the Atos corporate structure. EMC and VMware intend to continue their strategic long-term investment, now as shareholders of Atos.

NEXT >
2) Key Announcement Implications

2 **Key Announcement Implications**

In 2015 we ended the year with international cyber treaties looking to establish global norms for cyber activities.

Disruption leads to losses

From distributed denial-of-service attacks to company-crippling campaigns, disruption is a valid concern in 2016. The losses associated with business disruption are considered some of the highest over the course of identifying an issue and on through remediation. Since 27 per cent of all attacks are considered advanced and targeted, the potential for an attack to interrupt productivity is great.

In 2016, nations will look for ways to reinforce these global norms.

FireEye Looking Forward: The 2016 Security Landscape in EMEA

Executive Perspectives

This year had its fair share of incidents potentially carried out by the stereotypical "hacker in the basement." However, 2015 also saw campaigns from state-enabled actors, including the groups responsible for gaining unauthorized access to healthcare organizations and stealing the personal information of millions of customers and employees.

Many people point to companies victimized by cyber attacks, seeking to hold them accountable for not doing enough to protect intellectual property, consumer data, or other assets. And some people recognize that not enough time is being spent on identifying and bringing risks and consequences to bear on the attackers—an acknowledgment that victim organizations have suffered a crime.

All nations are struggling to determine how good cyber defense needs to be within the wide range of industries in the private sector, says FireEye President Kevin Mandia. As nations recognize that much of the private and public sectors are not prepared to prevent or detect sophisticated attacks, nations are exploring ways to establish and enforce behaviors.
However, Mandia is keenly aware that this path may raise privacy issues, which FireEye believes could become a part of the information-sharing dialogue.

Predictions

1. Cyber security will actually become a Board level issue

As much as many boardrooms would count security as an 'important' issue, there will be a bigger focus on this next year within EMEA particularly. Recent incidents at Vtech and TalkTalk have highlighted the need for CEOs particularly to become cyber security conscious. Recent breach situations where the media has highlighted- and arguably latched on to - the fact that senior board members are unaware of the full extent of the breach, has forced boardrooms to take a closer look at their cyber security strategy and examine whether they are properly equipped. It's quite possible that next year we will see a major household name 'mortally wounded' by a cyber attack – with the longer term impact on shareholder relationships becoming apparent. The signs point towards being one year closer to a company becoming insolvent due to a cyber attack. The board level is beginning to see that this is something that can't be ignored, and that the risks are beyond the immediate financial impact and therefore cyber security will become a key agenda item.

The Internet of Things broadens the attack surface

Affordable and internet-connected home security and automation systems could enable attackers to spy on homeowners and disarm security systems, potentially making residential properties bigger targets in the coming year.

In some circumstances, disruption can be more than just the inability to perform regular work operations. Mandia says that due to certain high-profile incidents, chief information security officers have had to change their risk profile. He says it used to be that there were five things we did not want to have become a reality, and now there is a sixth: someone could just hack in and delete everything. Add to that the lack of attribution, he says, and now we have to play goalie against the worst consequences because there is no risk or repercussions for the attackers.

ICS: Infrastructure's weak link

Another valid concern in 2016 is the growth of infrastructure-based attacks. Grady Summers, senior vice president and chief technical officer at FireEye, says that we will start to see more visible attacks against industrial control systems (ICS).

2. Governments will be challenged to scale to address cyber threats in a significant way

Recent terrorist attacks in France will strengthen the resolve of Europe's Governments to devote more resources on fighting all aspects of terror including cyber, and we have seen the beginnings of this recently. The UK Government for example talked much of further boosting the capabilities of GCHQ to tackle Daesh in the recent Strategic Defence Spending Review. Europe's governments must invest in training for the next generation of cyber security professionals, and make their defences scalable and adaptable enough to be able to identify new attack vectors, to respond effectively to an ever evolving threat landscape. Without this nothing much will change and the Internet will continue to be a safe & lucrative place to conduct cyber crime.

3. Data privacy and protection will encourage extra vigilance

Customer data will increasingly be stored locally in European clouds, and EU customers given more choice over which jurisdiction their data is stored in, following growing concerns over data privacy. This means that a wider array of companies will come under the umbrella of the impending EU General Data Protection Regulations, which will mandate that any company that processes data will be held responsible for its protection, including third parties. For the first time, legal obligations and reporting requirements will now be spread across both controllers and processors of customer data anywhere in Europe, precipitating a drive towards a far more secure, transparent and integrated cloud computing supply chain.

As a result we will see third parties taking urgent and visible steps to demonstrate extra vigilance when it comes to securing the data of others and we will also see data owners vetting their suppliers more thoroughly. By working together and learning from each other, we can expect to see third parties and original data owners identifying and plugging common supply chain weaknesses, increasing overall levels of security and create a community that follows best practice and responding faster and better to serious breaches. Harmonised enforcement of the rules among all data will foster greater security co-operation across the supply chain.

4. There will be an increased use of legitimate tools and services to conduct sophisticated cyber-attacks

We will see legitimate online tools and services - from supercookies to social media platforms – increasingly exploited by sophisticated threat secretly compromised 100 legitimate websites and used the same web analytics tools deployed by online retailers, to spy on their victims. There will be a growing trend in cyberespionage groups camouflaging their activities among legitimate web traffic, making them more difficult to detect and respond to. The increasing sophistication of legitimate web-analytics tools-from apps to profiling scripts will be exploited by cyberespionage groups to target victims with greater precision and collect more valuable data on their targets.

5. Digitalisation will leave security behind – possibly to its detriment

As the topic of 'Digital transformation' gains more attention next year, with the increased digitalisation of services and government infrastructure

New payment systems, new threats

If attackers are not successful using ransomware to make a quick buck in 2016, they may turn to targeting next generation payment methods, says Lance Dubsky, chief security strategist for the Americas at FireEye. Dubsky says that the world of mobile wallets, magstripe readers and other similar payment systems is growing rapidly but without the protections needed to secure the transactions. As a result, he says, we will likely see an increase in malware targeting these systems throughout the coming year.

and the requirement for end users to share more and more data to accommodate this, we'll see the pace of growth potentially grow faster than the consideration of cyber security. Therefore, a loss of personal identifiable data, for example healthcare data, will most likely increase, and come to the public's attention next year – creating a sobering reminder of the risks involved with ignoring security. The lack of data classification of this sensitive data will also complicate potential investigations and extend the time it takes to detect breaches, causing more issues.

Apple in the Crosshairs

Apple will become more heavily targeted. Apple's market share in desktop and mobile continues to increase, making the tech company's products more valuable for criminals to attack. Apple's traditionally secure software and devices have experienced some interesting threats in recent years, some of which have remained persistent and have evolved over time. Another development involves XcodeGhost, a previously identified iOS malware that managed to make its way past Apple's security checks and into the App Store. Just recently, our researchers identified that the threat had breached U.S. enterprises, that its botnet was still partially active and that a more advanced variant called XcodeGhost S had been previously undetected.

Recommendations

Altogether, Summers urges organizations to focus on prevention in 2016. Echoing Mandia's sentiment, Summers says that compromise is inevitable, and that companies would also do well to work on quick response. He recommends setting products to 'block' and 'protect' instead of 'alert,' as well as whitelisting apps on servers; but ultimately, he says that organizations must improve in rapidly detecting, responding to and stopping attacks in 2016. In 2014, attackers remained on networks for an average of 205 days before being detected, which is far too long.

Boland notes that organizations will have to do their due diligence when it comes to future mergers and acquisitions. He says that acquiring a company in 2016 could also mean acquiring tainted networks and compromised intellectual property. In order to ensure a secure merger, groups will have to increasingly rely on compromise assessments.

Conclusion

Mandia's additional 2016 predictions include more risk of destructive attacks, improved counter forensics, attacks aligned with geopolitical conflicts and a growing number of threat actors. Boland adds that more attackers will move to the cloud, hosting command-and-control servers on popped cloud virtual machines and using social media channels for communications.

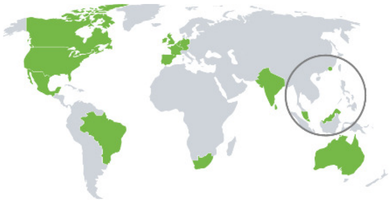
In the constantly evolving world of cyber security, many of these predictions are already beginning to come true. Our experts at FireEye are able to very accurately predict the trends and ultimately stay ahead of the curve due to far-reaching visibility, as well as access to vast amounts of valuable intelligence.

NEXT >
3) In Depth Focus

3 In Depth Focus

dimension data

To get a global perspective, Didata included participants at organisations based in 15 different countries,



Connected Enterprise Report 2016

For the 2016 Connected Enterprise Report, Dimension Data surveyed 580 IT managers, IT directors, CIOs, and others responsible for information systems at their organisations, as well as 320 line of business (LoB) managers.

Key Findings

Many enterprises have not included collaboration in their technology strategy

Nearly 40 per cent of organisations don’t have a defined unified communication and collaboration strategy. However, with the remaining 60% that do have a strategy, line of business (LoB) managers and other non-IT executives have a pivotal role in defining and executing their company’s collaboration strategy – an astounding 89 per cent of research participants. An increasing number of LoBs – one in four organisations – are also taking responsibility to pay for and implement the solutions as well, without the express consent of IT

Enterprises rely on collaboration to drive sales and new revenue

Increasing sales is the most important collaboration strategy at 14 per cent of enterprises, second only to increased productivity, which is most important to 19 per cent.

Organisations are turning to collaboration to improve sales, with 14 per cent – the second highest number of respondents – saying improving sales is the top goal of their collaboration strategy. And one in three organisations say increased sales is among the top three most important ways of measuring the success of their collaboration projects.

Few enterprises view return on investment as the main way they measure the success of their use of collaboration technology

Only 4 per cent use return on investment (ROI) as the primary method of determining whether their deployment of new collaboration technologies has been a success.

A demonstrable ROI is the least relied on method that organisations use to gauge the success of their use of collaboration technology. Only 4 per cent of organisations measure success by calculating ROI, whereas employee productivity data, user uptake data, and cost savings data are much more common ways to justify their investments in collaboration technology. This is problematic because ROI is an important way of justifying any kind of technology investment.

Not enough focus on what happens after the technology is deployed

A quarter of organisations focus more on the successful implementation of collaboration technology, rather than how it's used and adopted. One out of every four IT departments measure the success of their collaboration projects by how well they've implemented the technology. This is a rather dangerous mindset, since the success of collaboration projects hinges as much on what comes after the technology is implemented as before. If employees don't use the collaboration tool – and use them effectively – then organisations will neither benefit from the technology nor achieve a ROI on it. Related to this, 17 per cent of organisations haven't implemented collaboration training programmes, and 16 per cent haven't changed travel policies to encourage the use of videoconferencing and other collaboration tools. This is a recipe for disaster for many organisations looking to derive maximum value of their use of collaboration technology.

Collaboration improves enterprises' ability to interact with customers

81 per cent of enterprises say collaboration has enhanced their ability to engage with customers and improve customer service. Collaboration technology has a wide range of uses in customer engagement scenarios. Rich communications leveraging technology lets businesses interact with clients in the manner and on the device they prefer. And it improves how contact agents work together and with others in the enterprise to resolve customer issues. However, very few – only 2 per cent of enterprises – identify customer service improvements as the topmost goal of the collaboration strategy. The implication is that better customer experience is an accidental rather than pre-planned outcome for many organisations implementing collaboration technology.

Collaboration accelerates decision making, but many organisations fail to leverage it to improve their competitive position

88% of enterprises say collaboration has improved the decision-making process in their organisations. Enterprises have also become very adept at leveraging collaboration technology to make their employees more productive, with 84 per cent saying collaboration has improved the productivity of individual employees. But many struggle to leverage collaboration to compete in their respective industries, with 20 per cent of organisations saying their use of collaboration technology has failed to improve their competitive positioning.

Cloud-based collaboration is a strategic goal for many enterprises, but it will take some time to achieve

Nearly one in three IT departments see moving UCC to the cloud as the most important technology trend affecting their collaboration strategy. However, organisations are taking a very cautious approach to the cloud, with only 20–25 per cent currently relying on hosted collaboration services. This isn't expected to grow significantly in the next 12 months as enterprises carefully and deliberately execute on their cloud strategies.

LoBs have a prominent role in deciding which collaboration technology to use

Almost 60 per cent of lines of business (LoBs) have their own budget – independent of IT – to purchase collaboration technology.

Didata asked IT and LoB leaders detailed questions about:

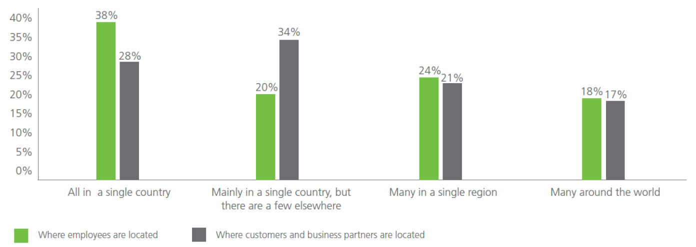
- **corporate strategy as it pertains to** improving communications and collaboration within the company
- which **collaboration tools** are used the most widely
- **how employees most benefit** from collaboration
- **how collaboration technology** is purchased and deployed now and how this will change in the future
- how collaboration **technology is integrated** with other business applications
- how collaboration technology **improves business** processes
- how shadow IT and the **consumerisation of IT** is affecting the collaboration tools in use within the company
- how the success of collaboration **technology is measured**

And 57 per cent have staff within the department to both implement and support collaboration technology. Selecting, purchasing, and implementing collaboration technology are no longer just the IT department's responsibilities. At many enterprises, IT needs to work hand-in-hand with LoBs that not only understand what they seek to gain from collaboration but are also capable of purchasing and supporting the technology

Implications for semiconductor players

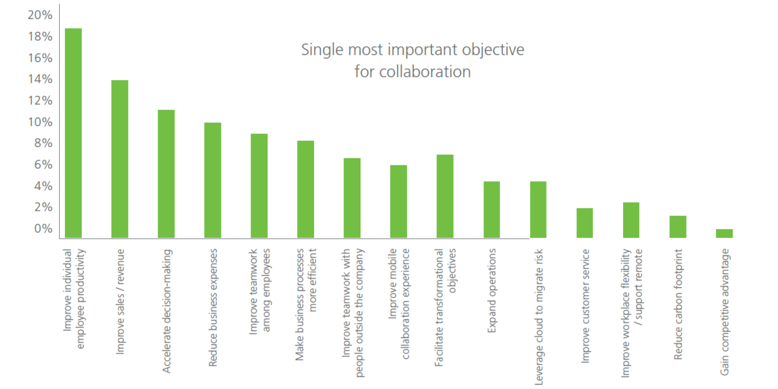
A quarter of those organisations polled said they measure the success of their collaboration projects by how well they've implemented the technology, rather than how it's used and adopted throughout the organization. One out of three IT departments see moving unified communication and collaboration to the cloud as the most important technology trend affecting their collaboration strategy. However, less than 25 per cent of organisations currently rely on hosted collaboration services.

Figure 1: Enterprises support a very highly distributed set of customers and partners



At one out of three organisations, enterprise social collaboration is used by all - or most - employees, and nearly half of all companies that were surveyed said they expect social collaboration usage to increase over the next year.

Figure 2: Most enterprises see productivity gains as the top goal when deploying collaboration technology



Conclusion

According to one in five organisations polled, collaboration technology had failed to improve their competitive positioning. However, 87 per cent of organisations said the use of collaboration technology had improved teamwork, and 88 per cent of enterprises had accelerated decision making.

Please email press@eurolanresearch.com for a copy of the report

NEXT >
4) Financial Roundup

4 Financial Roundup

	Income $M	Latest quarter Sales $M	
Juniper	197.8	1319.6	↗
Mitel	-6.3	342.0	↗
Ciena	-11.5	573.1	↗
Cisco	3147.0	11834.0	↗
Brocade	93.7	574.0	→
Netgear	21.8	360.9	→
Avaya	-27.0	958.0	↘
Extreme	-7.2	139.3	↘

Source: Company Financials - all based on latest released quarters ended Dec except Brocade and Cisco is Jan

Recently Released Financials

Avaya Q116 – Sales were down by $121M Y on Y and down $50M sequentially

○ Americas	64 (63) per cent
○ EMEA	25 (28) per cent
○ Asia	11 (9) per cent

Brocade Q116 – Sales flat Y on Y and down 2 per cent sequentially

○ Channel sales	33 (33) per cent
○ International	45 (42) per cent
○ OEM	67 (67) per cent

Ciena Q116 – Sales up 8 per cent Y on Y down 17 per cent sequentially

○ North America	68 (63) per cent
○ EMEA	14 (21) per cent
○ CALA	8 (8) per cent
○ APAC	10 (8) per cent

Cisco Q216 – Sales were up 2 per cent Y on Y excluding SP Video CPE Business

○ North America	58 (60) per cent
○ EMEA	26 (26) per cent
○ Asia	16 (15) per cent

Extreme Q216 – Sales were down 8 per cent Y on Y and down 8 per cent sequentially

○ Americas	52 (48) per cent
○ EMEA	39 (43) per cent
○ Asia	9 (9) per cent

Juniper Q415 – Sales were up 20 per cent Y on Y and up 6 per cent sequentially

○ Service Provider	71 (68) per cent
○ Switching	21 (16) per cent

Mitel Q415 – Sales were up 13 per cent Y on Y and up 18 per cent sequentially

Netgear Q415 – Sales were up 2 per cent Y on Y up 6 per cent sequentially

○ Retail	56 (42) per cent
○ Commercial	18 (23) per cent
○ SP	28 (36) per cent

For further information, please contact:

Keith Humphreys – Managing Consultant at **euroLAN** – keith@eurolanresearch.com