analysysmason.com

RESEARCH STRATEGY REPORT

IoT SECURITY: OPPORTUNITIES FOR COMMUNICATIONS SERVICE PROVIDERS

MICHELE MACKENZIE and SHERRIE HUANG

About this report

This report provides an overview of the current status and trends in the IoT security market for communications service providers (CSPs). It analyses the IoT security opportunities for CSPs, as well as the related business models and approaches to building IoT security propositions.

The report also provides recommendations for CSPs on IoT security service development.

It is based on several sources:

- Analysys Mason's internal IoT research and database
- interviews with stakeholders in the IoT security market.

GEOGRAPHICAL COVERAGE	CASE STUDIES
Worldwide	Orange Tele2 Telefónica Telenor Connexion Vodafone

KEY QUESTIONS ANSWERED IN THIS REPORT

- How are CSPs developing IoT security now? In what ways will it develop in the future?
- What are the challenges that CSPs face in the IoT security market?
- Does 'end-to-end' security exist? If so, who should be responsible for it?
- What are the revenue opportunities for CSPs in IoT security?
- What role can CSPs play in the IoT security field? What is the business model and where should CSPs focus their investment?

WHO SHOULD READ THIS REPORT

- Strategy executives and directors who are managing aspects of CSPs' IoT service offerings.
- Strategy executives and directors who are managing IoT security solutions.
- Marketing staff for vendors that offer IoT security solutions or services.
- Chief technical officers of CSPs who are seeking insight into IoT security capabilities.
- End users of IoT solutions and services that are interested in learning more about IoT security.

Executive summary

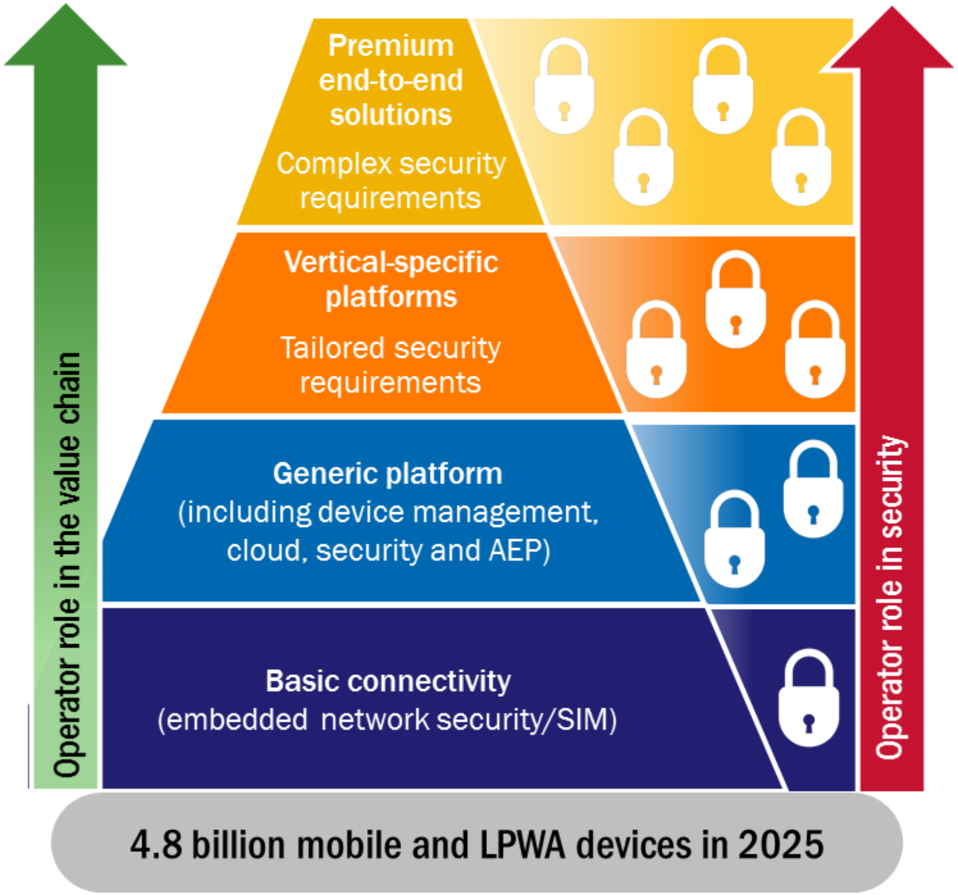
As awareness of IoT security breaches grows, operators with ambitions in IoT will need to highlight network security as a differentiator and match their ambition in IoT by securing the components of the value chain that they address.

IoT security has featured widely in recent headlines for all the wrong reasons. The size and scale of some of the breaches has alarmed governments and regulators, raising questions about national security, as well as public safety. There are also concerns that security issues could dampen the demand for IoT solutions.

CSPs will need to work hard to demonstrate their expertise in providing security for IoT services in order to win new IoT business, differentiate their connectivity services and defend their brand reputation. Operators' incremental revenue generated from IoT security will not be high overall, but securing IoT services beyond connectivity may generate some extra value. This report makes the following recommendations to support operators in this space.

- For connectivity-only contracts, security will form a basic component of any RFP; CSPs will need to provide evidence of the security measures that they have implemented. Embedded security is inherent in the cellular network and considered to be a basic service. Its value should be marketed effectively to reinforce the value of the connectivity versus substitute technologies.
- CSPs can provide a premium security service for some elements of the value chain, particularly for IoT projects requiring more than just connectivity. This may generate modest incremental revenue.

Figure 1: The operator's role in IoT security must match the operator's role in the IoT value chain


Operator role in the value chain
Premium end-to-end solutions
Complex security requirements
Vertical-specific platforms
Tailored security requirements
Generic platform (including device management, cloud, security and AEP)
Basic connectivity (embedded network security/SIM)
Operator role in security
4.8 billion mobile and LPWA devices in 2025

Source: Analysys Mason

If operators fail to secure their IoT solutions, they risk losing IoT projects to other providers; a total of USD201 billion in revenue is at stake

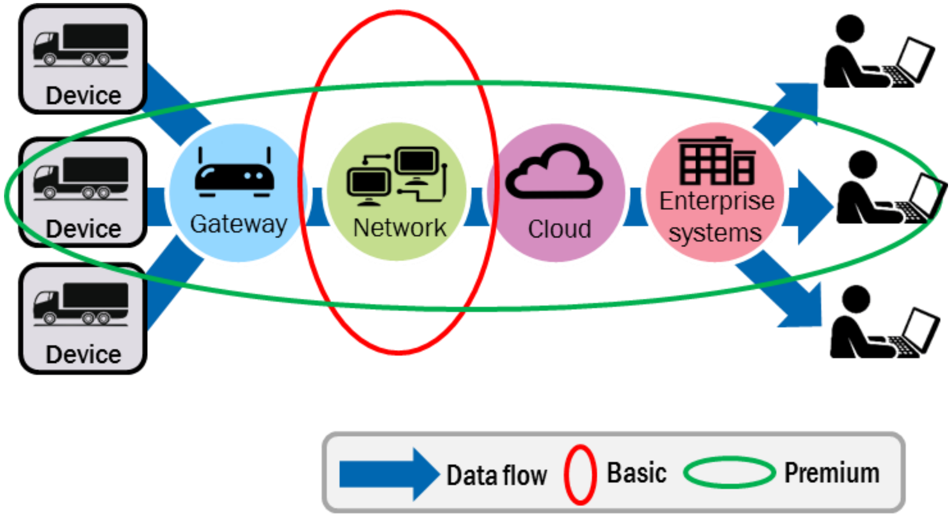
Although CSPs have focused on developing viable strategies for targeting IoT as a new growth opportunity, IoT security has not been, until recently, an explicit requirement. This is primarily because the number of connections was low, many networks were proprietary or private, and networks were assumed to be secure.

In the early days of cellular IoT, demand for additional security was negligible. Most IoT contracts consisted of simple connectivity solutions for a relatively small number of devices; security was not a key consideration as cellular networks benefited from embedded security and were largely assumed to be secure. They were subject to international standardisation and network security protocols were deemed sufficient.

CSPs increasingly address other components of the IoT value chain to capture a larger share of IoT revenue (see Figure 2). This requires specialist security expertise, which CSPs do not always have. CSPs with ambitions beyond connectivity now face the challenge of how (rather than if) to provide IoT security solutions. They will, however, be able to generate a revenue premium from value-added security.

CSPs also have to consider brand reputation – both their own and that of their enterprise customers. A data breach can damage confidence in a company’s brand, although the consequences of this in terms of costs can be difficult to quantify.

Figure 2: Connectivity security is a basic service, but premium value will be created by securing other elements of the value chain



Source: Analysys Mason

Selling IoT security solutions will not generate substantial revenue, but it will help operators to win IoT contracts

Robust IoT-embedded security solutions will bolster most CSPs' IoT connectivity offerings and reinforce their value.

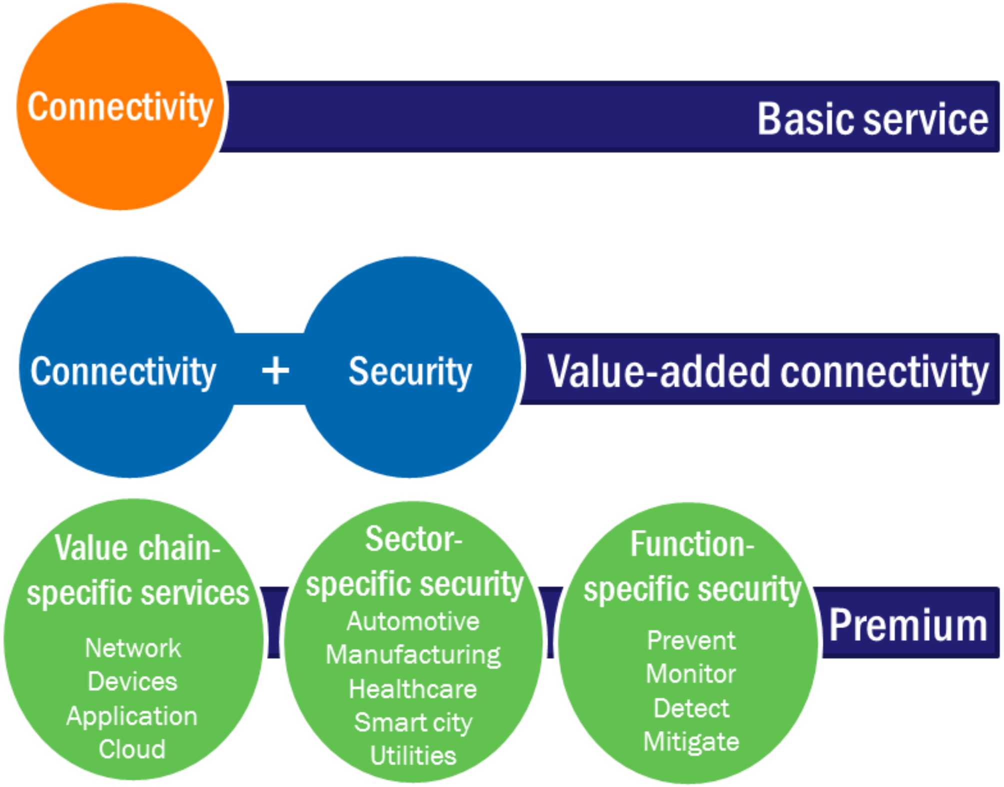
Operators should explore how to provide better security for their basic (connectivity-only) IoT offering because enterprises will increasingly want operators to demonstrate how their networks are secure. This may take the form of private APNs or enhanced security on the SIM.

For operators that are providing more than just connectivity (for example, devices or applications), there is an opportunity to provide enhanced or premium security solutions. This could include value-chain-specific services, sector-specific security or solutions that address specific functions. CSPs will have to offer IoT security to:

- differentiate their IoT service from those of other operators and other network technologies and reinforce its value
- defend their IoT business: CSPs will lose business if they cannot demonstrate robust security
- enhance their IoT offering and build trust in their brand. Trust is growing but the telecoms sector has no room for complacency.[1]

This report examines operator approaches to offering IoT security, securing the connectivity layer and providing services beyond connectivity for devices and applications.

Figure 3: CSPs could specialise in specific sectors or functions of IoT security



Source: Analysys Mason

[1] Edelman Insights, *2017 Edelman Trust Barometer.* Available at: https://www.slideshare.net/EdelmanInsights/2017-edelman-trust-barometer-technology.

Recommendations

1

CSPs must make connectivity secure for all network types. Security will increasingly represent a basic feature of any IoT RFP and CSPs are in a strong position to demonstrate expertise in this area for cellular networks.

Embedded network security is a basic service; some CSPs will develop value-added features including APN and VPN services, as well as connectivity and device management services. CSPs should market the enhanced, embedded security in their networks to support their connectivity offering and demonstrate the value of cellular over other network technologies. There is an early opportunity to differentiate their security offering for LPWA.

2

CSPs' security offering will need to closely mirror their IoT strategies. End-to-end IoT offerings require end-to-end security.

CSPs that are providing end-to-end IoT solutions will need to **build**, **partner** and possibly **acquire** solutions to ensure that they can secure the value chain. End-to-end security will help to differentiate CSPs' IoT offerings. and generate modest additional revenue, but they will need to work hard to demonstrate that their solutions are secure for all services beyond connectivity.

3

CSPs should not expect IoT security to drive significant revenue growth, but they can increase the value of their IoT proposition by developing expertise in this market.

Security is no longer an optional feature. CSPs will need to educate customers to the benefits of security by design and also demonstrate to enterprise CISOs that they have the relevant expertise to provide the security layer. Most CSPs will not generate significant additional revenue from security itself, but it will be instrumental in boosting their IoT propositions against those of the competition if security is inherent in the network and the broader offering.

CONTENTS

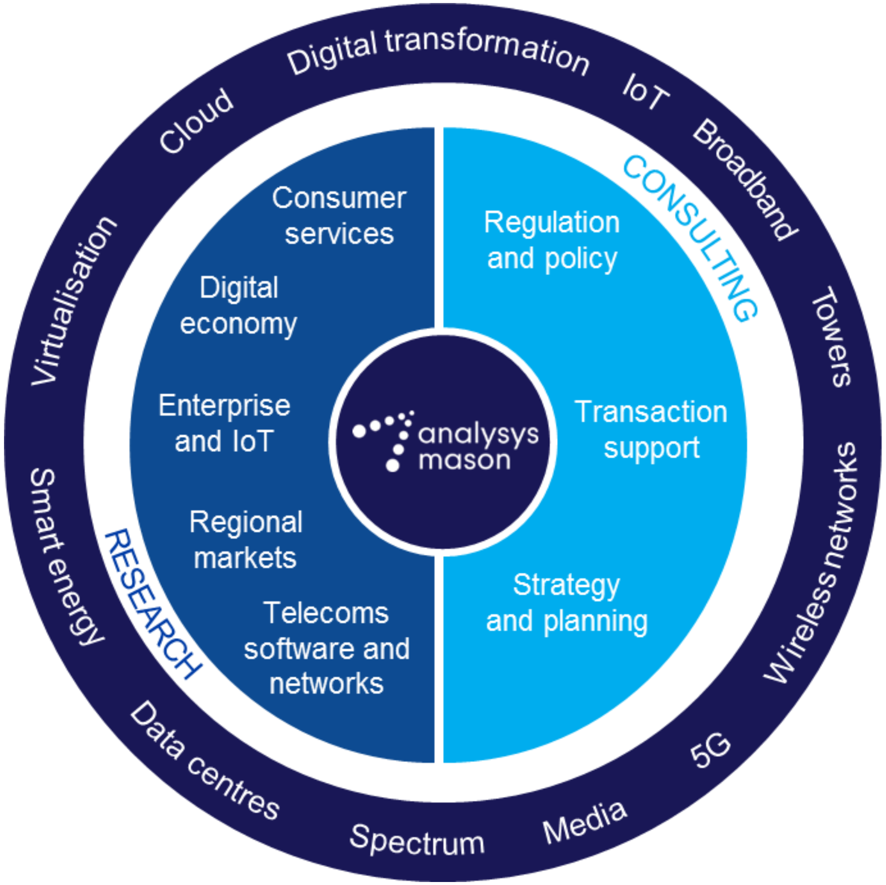
About the authors

Michele Mackenzie (Principal Analyst) is an analyst for Analysys Mason's *IoT and M2M Services* research programme, with responsibility for M2M and LPWA forecasts. She has 17 years of experience as an analyst. She produces reports and forecasts on M2M and IoT in industry sectors, such as transport, healthcare and smart cities, and analyses the impact of IoT network technologies, such as LPWA networks. Prior to joining Analysys Mason in February 2014, Michele was a freelance analyst with a focus on M2M and IoT technology and trends. She has written reports for Machina Research and produced research for other clients in areas such as mobile broadband and digital media.

Sherrie Huang (Research Programme Head, Asia–Pacific) is the lead analyst for our *Asia–Pacific* research programme and is based in our Singapore office. Her research covers the entire Asia–Pacific region, and includes market data and forecasts for 17 key markets, as well as thematic reports covering key telecoms industry trends including IoT/M2M, video and multi-play, and enterprise services. Sherrie has extensive expertise on the telecoms industry from various angles, including strategy, market sizing and forecast, end-user research, cost modelling and regulatory issues. She previously worked at IDC, Ovum and ZTE in various Asia–Pacific countries.

Analysys Mason’s consulting and research are uniquely positioned

Analysys Mason’s consulting services and research portfolio



CONSULTING

- We deliver tangible benefits to clients across the telecoms industry:
  - communications and digital service providers, vendors, financial and strategic investors, private equity and infrastructure funds, governments, regulators, broadcasters, and service and content providers.
- Our sector specialists understand the distinct local challenges facing clients, in addition to the wider effects of global forces.
- We are future-focused and help clients understand the challenges and opportunities that new technology brings.

RESEARCH

- Our dedicated team of analysts track and forecast the different services accessed by consumers and enterprises.
- We offer detailed insight into the software, infrastructure and technology delivering those services.
- Clients benefit from regular and timely intelligence, and direct access to analysts.

Research from Analysys Mason

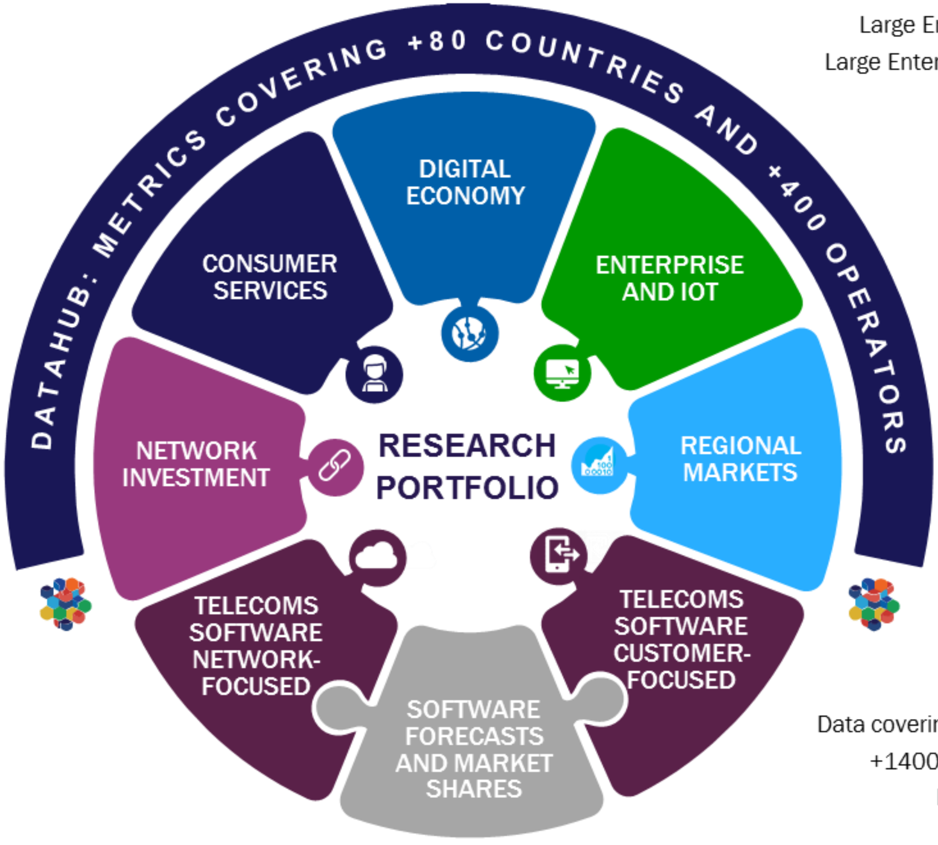
Consumer services programmes
- Mobile Services
- Mobile Devices
- Fixed Broadband Services
- Convergence Strategies
- Video Strategies

Network investment programmes
- Network Investment Strategies
- Network Traffic
- Spectrum

Telecoms software and networks programmes
- Software Forecast and Strategy
- Telecoms Software Market Shares

Network-focused
- Next-Generation Wireless Networks
- Service Delivery Platforms
- Service Fulfilment
- Service Assurance
- Network Orchestration
- Software-Controlled Networking

Customer-focused
- Digital Experience
- Customer Care
- Revenue Management
- Analytics


DATAHUB: METRICS COVERING +80 COUNTRIES AND +400 OPERATORS
DIGITAL ECONOMY
CONSUMER SERVICES
ENTERPRISE AND IOT
NETWORK INVESTMENT
RESEARCH PORTFOLIO
REGIONAL MARKETS
TELECOMS SOFTWARE NETWORK-FOCUSED
TELECOMS SOFTWARE CUSTOMER-FOCUSED
SOFTWARE FORECASTS AND MARKET SHARES

analysysmason.com/research

Enterprise and IoT programmes
- Large Enterprise Voice and Data Connectivity
- Large Enterprise Emerging Service Opportunities
- SME Strategies
- IoT and M2M Services
- IoT Platforms and Technology

Digital economy programmes
- Digital Economy Strategies
- Future Comms

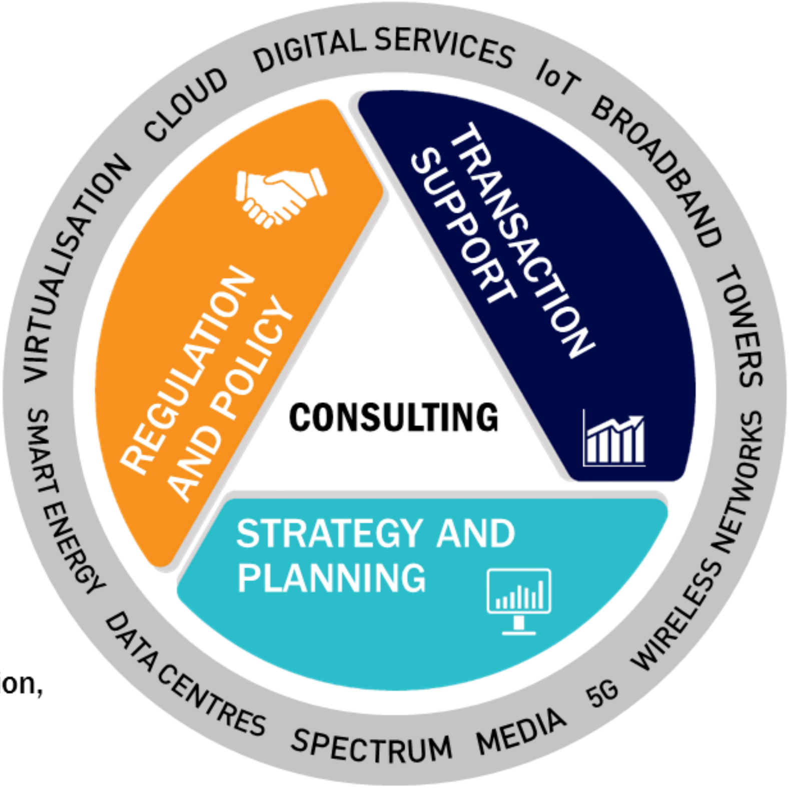
Regional markets programmes
- Global Core Data
- Americas
- Asia–Pacific
- Middle East and Africa
- European Core Forecasts
- European Telecoms Market Matrix
- European Country Reports

DataHub
- Data covering +80 countries and +400 operators
- +1400 forecast and +250 historical metrics
- Regional results and worldwide totals
- Operator historical data
- Compare markets and operators
- Financial values in USD, EUR or local currency
- Export data to Excel and save searches

Consulting from Analysys Mason

REGULATION

- Quality of service
- Market review
- Margin squeeze tests
- Analysing regulatory accounts
- Regulatory economic costing
- Policy development and response
- Media regulation
- Expert legal support
- Radio spectrum management
- Net cost of universal service
- Radio spectrum auction support
- Postal sector policy: USO, liberalisation, costing, pricing and regulation



TRANSACTION SUPPORT

- Commercial due diligence
- Technical due diligence
- Digital services
- Mid-market finance sponsors
- Data centres

STRATEGY AND PLANNING

- Commercial expertise
- Technology optimisation
- New digital frontiers

analysysmason.com/consulting

PUBLISHED BY **ANALYSYS MASON LIMITED** IN **AUGUST 2017**

Bush House • North West Wing • Aldwych • London • WC2B 4PJ • UK

Tel: +44 (0)20 7395 9000 • Email: research@analysysmason.com • www.analysysmason.com/research • Registered in England No. 5177472

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Analysys Mason Limited independently of any client-specific work within Analysys Mason Limited. The opinions expressed are those of the stated authors only.

Analysys Mason Limited recognises that many terms appearing in this report are proprietary; all such trademarks are acknowledged and every effort has been made to indicate them by the normal UK publishing practice of capitalisation. However, the presence of a term, in whatever form, does not affect its legal status as a trademark.

Analysys Mason Limited maintains that all reasonable care and skill have been used in the compilation of this publication. However, Analysys Mason Limited shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising as a result of the use of this publication by the customer, his servants, agents or any third party.