

Unbreakable quantum encryption: the 'holy grail'

18 July 2021

Arqit's quantum encryption product aims to protect any form of device from hacking, with a fully scalable, lightweight, cloud-delivered software product backed by its advanced satellite technology in the tech stack. With over US\$130m in contracts and its first product launch - QuantumCloud™ Release 1 - in H2 2021, Arqit's QuantumCloud™ is a commercial reality with a range of major corporate and government customers already signed up.

Traditional encryption is now inadequate. The frequency and scale of information breaches, hack events and cyber-security failures highlight both our dependence on secure information flows and the vulnerability of traditional encryption. The standard and most widely used form of encryption, Public Key Infrastructure (PKI), relies on establishing, trusting, and protecting encryption keys. The complexity involved in this process and difficulty of coordinating parties means that PKI is now essentially overwhelmed by the volume of data and operations it must protect.

Arrival of 'Quantum 2.0'. Quantum-based encryption is now a reality and offers encryption which, backed by the laws of physics, is demonstrably unbreakable. Quantum mechanics, operating at the sub-atomic level, has generated a number of paradoxes which challenge not only Newtonian and relativity physics, but common sense. Nevertheless, 'Quantum 1.0' has enabled the development of semiconductors – the core of computing – lasers and optic communications, CD and DVD players and MRI scanners, etc. 'Quantum 2.0' computing sits alongside other new developments such as artificial intelligence, nano-scale engineering and the internet of things (IoT), set to impact our lives.

ARQ19 has solved problems in quantum encryption and its distribution that had previously made the concepts unusable. Arqit's quantum-based encryption system encodes information into the quantum properties of individual particles of light to transmit information from space to Earth. The laws of physics prove this information cannot be stolen and so datacentres all over the world can use the quantum information to create secure (symmetric) encryption keys which are unbreakable, even by the power of future quantum computers. Crucially, Arqit has developed a novel cryptographic protocol which translates the benefit of the quantum keys that the satellites distribute to global data centres into keys on software end points. So, two or more end-point devices to create locally *identical* copies of symmetric keys, with infinite frequency and group sizes. Arqit's simple and elegant **QuantumCloud™** product offering is software-light, suitable for even miniature IoT devices, and does not require customers to deploy expensive infrastructure.

Quantum technology is rapidly becoming mainstream. Arqit's offering is differentiated by being a commercial reality which will generate revenues in the current financial year: one of the most advanced ways to gain exposure to the emerging Quantum 2.0 sector.

Arqit Federated Quantum System (FQS). At the G7 Leaders Conference on 11th June, Arqit announced the formation of an international group to provide its quantum encryption technology to governments for the protection of strategic assets and communications, The Federated Quantum System (FQS). In addition to the British Government major customer partners include BT, Sumitomo Corporation, Northrop Grumman, Leonardo, QinetiQ Space N.V., and Honeywell. Agencies and companies of other Western Allied countries are expected to join during 2021. The first FQS satellites are scheduled for launch in 2023 subsequent to the launch of the first commercial Arqit satellites.

Arqit has signed **over US\$130m** of contracts with telecoms, government, and defence customers. There are other target verticals with contracted proof-of-concept projects with major corporates. **The potential market (2024) at c. US\$198bn looks sizeable. Given Arqit's positioning and opportunity it is understandable why NASDAQ listed Centricus Acquisition Corp. is seeking to combine with Arqit, with a pro forma enterprise value of US\$1bn.**

Introduction

Arqit is an innovative developer and provider of quantum-based encryption services based on its expertise in the combined fields of quantum cryptography, cyber security software and satellite technology.

It has turned deep tech into a platform-as-a-service offering which is software-light and highly scalable, with worldwide distribution capability.

Online sales target every vertical, with direct sales in initial specific sectors: telcos, defence, automation, and financial services.

Arqit has assembled a Management Team that is rich in technology skills and contacts with top-level decision takers in leading companies and government bodies.

An estimated market opportunity is \$198bn, as reflected in the current value and shares' rating of leading listed cybersecurity companies: over \$350bn and forward EV/revenue of 22.9x, respectively.

Contracts worth US\$130m have already been agreed, and the first software product release from Arqit is expected in the second half of 2021.

NB this note is not to be read by, or sent to, private investors in North America

Mike Jeremy (Analyst)

0207 065 2690

mike.jeremy@equitydevelopment.co.uk

Andy Edmond

0207 065 2691

andy@equitydevelopment.co.uk

Proposed combination and NASDAQ presence

Arqit has entered into a definitive agreement to combine with Centricus Acquisition Corp. (ticker CENHU, CENH, CENHUW), a publicly traded, special-purpose acquisition company (SPAC) with a market value on NASDAQ of c.US\$430m. At its IPO in February 2021 Centricus raised US\$345m.

Subject to the conclusion of the standard SEC review process, approval of Centricus shareholders, and certain other customary closing conditions, the combined entity is expected to be listed on NASDAQ in Q3 2021. As a result of the combination, to implement and accelerate its strategic plan Arqit will have access to funds of up to approximately US\$400m, inclusive of up to US\$345m of Centricus' cash in trust account and a PIPE commitment of US\$71m, which includes participation from Arqit partners Virgin Orbit and Sumitomo Corporation plus sponsor Heritage Group.

Shares in the Centricus SPAC are 'redeemable'; i.e., prior to finalisation of the business combination, a shareholder in Centricus may elect to redeem shares at US\$10.0 each out of cash held in an AA-rated Trust Account.

Why is a cash-rich entity so keen to acquire Arqit's know-how, rather than other proven or nascent technologies?

Quantum cryptography is made possible by the process of 'quantum key distribution' in which the keys to encrypt and decrypt information are created instantaneously. Arqit's achievement is to have developed novel technologies that resolve two major barriers to the practicable deployment of quantum encryption. These are:

- **Secure distribution.** Arqit uses satellite-based distribution, but in a way that removes the vulnerability of having a 'trusted' crypto key stored onboard, and is therefore 'trustless', an essential feature in quantum encryption; and
- **Global distribution.** Arqit's solution overcomes prior limitations which confined distribution to a sub-global scale through the configuration of its satellite network and links with terrestrial end points.

With these problems overcome Arqit has been able to proceed to full commercial-scale deployment.

This report introduces the opportunity represented by quantum computing and encryption against the background of the fragile nature of current encryption methods and describes how Arqit solved problems which means it is now able to access the huge global market opportunity in secure quantum encryption.

Arqit QKD satellite due for launch in 2023



Source: Qinetiq, Space.com

The origins of quantum technology

Early sub-atomic quantum physics

Following on the discovery, in 1909 by Ernest Rutherford and Ernest Marsden, that the positively charged nucleus of an atom is surrounded by a negatively charged cloud of electrons, it was the Danish physicist **Niels Bohr** who suggested that the reason that (negative) electrons did not collapse towards the (positive) nucleus is that the number of electrons determines an orbit in which they remain fixed unless they emit or gain energy from photons. He termed this a '**quantum**' of energy.

It was **Werner Heisenberg** who, in 1925, developed the famous 'uncertainty principle'; that it is possible to know either the location of an electron or its speed, but *not both*, i.e. that in the quantum universe it is only possible to think in terms of probabilities - Einstein's dictum "God does not play dice", reflected his unease with quantum theory.

In 1935 **Edwin Schrödinger** encapsulated the weirdness of quantum mechanics in his famous 'cat in a box' thought experiment, in which he imagined the fate of a cat shut in a box with poison which would be released only when a radioactive material in the box emitted a particle. Since quantum theory states that this moment cannot be predicted, until the box is opened it would not be possible to know the cat's fate. Thus, on the basis of quantum probability, the radioactive particle would be in a state of having been *both* emitted *and* not emitted, a quantum state known as 'superposition'.

Still stranger, at the subatomic level, is the quantum feature known as '**entanglement**' in which two separated particles are 'connected' to the extent that any change affecting one will instantaneously affect the other. This is also 'non-local'; it bears no relation to physical proximity and follows from the treatment of light as a wave, i.e. as a connected entity. Reintroducing the quantum feature of superposition – being in two states at once – a change to one particle will inevitably, automatically, and instantaneously place its partner in the same state. Conversely, measuring one particle will eliminate its superposition, and therefore that of its partner. Einstein called this "spooky action".

Quantum cryptography: the 'Global versus Trustless Conundrum'

Physicists have been working for decades on various applications of quantum mechanics in computing, timing, sensing and communications. Only with the massive rise in the data capacity of the Cloud and the miniaturisation of control electronics are quantum technologies now sufficiently commercial to be capable of launching to markets.

Scientists derived cryptographic applications of quantum mechanics in the 1980s and 90s, but they are badly flawed. There are two previously known quantum encryption protocols – 'prepare and measure' and 'entanglement-based' - each of which has fundamental issues that Arqit describes as the '*Global vs Trustless Conundrum*'.

Prepare and Measure protocol keys can be distributed by satellite to locations globally, but the satellite must remember the key in its onboard computer memory. Therefore, although the space to Earth transmission benefits from the security guarantee of physics, simple access to the satellite payload would reveal the key and the satellite would be a "trusted node" – a bad thing in cyber security. This protocol fails because although it is global it is not *trustless*; it has the same weak point as traditional encryption.

In **Entanglement-based protocols** the keys are distributed simultaneously to two end points, so the key does not reside onboard the satellite. However, because this requires a low earth orbit satellite (LEOS) configuration the distribution footprint is limited to approximately 700km (430 miles) so the intended recipients of the keys must be located close to each other. This protocol fails because, although it is trustless, it cannot be distributed *globally*.

From theory to practice

Arqit has solved the Global Versus Trustless Conundrum, not in theory but as a practicable application. Its own satellite will use a proprietary and patented algorithm called ARQ19 which is able to deliver keys globally and in a trustless manner.

This represents a major deep tech innovation. As might be expected, Arqit's technology claims were inspected and verified by advisers in the SPAC transaction - also one of the advantages of a SPAC-based transaction versus a VC round – as part of the due diligence process, and we have had sight of some of this data. Arqit's patent portfolio is beginning to be published but we do not expect full information to be in the public domain in the near-term, nor critical specific aspects of its solution to be revealed in patents.

Finally, that Arqit's QuantumCloud™ offering is software-light provides clients ready access to this encryption service and forms the basis for the commercial deployment now underway.


The limitations of PKI encryption

PKI encryption is the widely used and well-known basis for security in areas such as HTTP-based TLS/SSL (Transport Layer Security / Secure Sockets Layer) internet communication. The kernel of PKI lies in establishing *trust* in its three principal components: **public keys, private keys and certificates**. Each participant has two keys, a public key and a private key, with each a number or bit string connected by an underlying mathematical formula and placed beyond the capabilities of computational-based access.

It must be noted that, although 'brute force' computational hacking is currently not practical, the advent of quantum computing within the foreseeable future - arguably less than a decade or even five years away - means that computational code breaking could soon become a reality. It is also the case that encrypted data, or "cyphertext", is also being intercepted, stolen and stored for future decryption. In PKI the public key is 'open' to anyone and encodes the message, whilst the private key is not revealed and decodes the message. The addition of a PKI certificate establishes the identity of the sender in the message exchange process, which must also be referenced by a trusted source or certificate authority (CA).

Although its processes must be fail-safe, PKI has a long history of failures resulting from weak implementation, ranging from certificate-based failures (e.g. Verisign Microsoft certificates, Superfish Addition of Root Certificates, or Marlinspike Certificate Constraint Omission), to application layer failures in areas such as TLS Protocol and Weak Hash Functions, and simple implementation failures based on poor systems expertise. These challenges faced by Arqit's target clients are summarised below.

Summary of current encryption issues



Our Customers' Challenges

<p>PKI Failures are growing</p> <ul style="list-style-type: none"> • Certificate Authority Failures • TLS Protocol Issues • Weak Hash functions • Implementation Issues 	<p>Quantum Computers will end PKI this decade</p> <ul style="list-style-type: none"> • Quantum Computers will break PKI in 2025-2028 • Post Quantum Algorithms are not provably secure and will take 10 -15year to be stable (NIST April 2021)
<p>PKI has a significant management cost and burden</p> <ul style="list-style-type: none"> • One of the major causes of downtime in SaaS/PaaS platforms has been PKI mismanagement • The costs of PKI management are not scaling well to meet the challenge 	<p>Manual key delivery burden is increasing with increased security risk</p> <ul style="list-style-type: none"> • Networks are getting larger • Increase costs over time • Poor refresh rates

Source: Company

The recent high-profile US Colonial Pipeline hack highlights vulnerability to cyber attack

There are numerous examples of the damage caused by data leaks, hacks, or deliberate cyber-sabotage. Most recently, a cyber-attack shut down a major piece of US infrastructure, the US Colonial Pipeline. As the New York Times described it (May 8th, 2021): “*One of the nation’s largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyber-attacks*”.

The 5,500 miles-long pipeline is responsible for an estimated 45% of the US East Coast’s fuel supply and was forced to shut down as its corporate computer network, operating, monitoring and safety systems, were remotely breached and disabled by ransom software – a bug implanted to exhort financial gain. In addition to embarrassment, the incident resulted in severe service disruption; the operator was forced to resort to delivery by tankers to maintain fuel supplies until systems could be reinstated.

Arqit QuantumCloud™: unbreakable quantum-based encryption

In contrast to PKI where keys are ‘delivered’, encryption based on Quantum 2.0, *creates* matching pair of keys which by definition cannot be accessed. Arqit gives its clients access to ‘borrow’ random numbers from its QuantumCloud™ which are used as an ingredient in their processes. Peripheral devices such as 5G base stations or end-point devices such as smart phones or automobiles create encryption key pairs, which establish unbreakable, end-to-end quantum-based encryption but at the same time remain unknown to the user. Consequently, there is no need from the outset to establish the elements of trust on which PKI relies and which, as a result, weaken PKI-based encryption.

The power of Arqit’s transmission algorithm - ARQ19 - is that it is entirely ‘trustless’ and ‘global’. Arqit has translated this power in a trustless way to global users with a revolutionary lightweight second end point software algorithm that requires no modification to user devices.

The challenge of trustless Quantum Key Distribution (QKD)

To distribute or create quantum keys over long-distance systems such as optic fibre networks is problematic, notably because the interaction of light-based (optical) quantum states with glass atoms causes severe attenuation. This limits distribution by this means to just a few hundred kilometres. Further, that quantum states cannot survive contact with any intervening equipment means that it is not possible to patch QKD onto established fibre optic cable infrastructure. There is some research into ‘quantum memories’ which could theoretically allow quantum states to be effectively amplified without leaving the quantum form. But such devices are currently impractical even at tiny distances, and it is thought that a global retrofit of every single network switch and router in the world would be required even if such devices could be made practical.

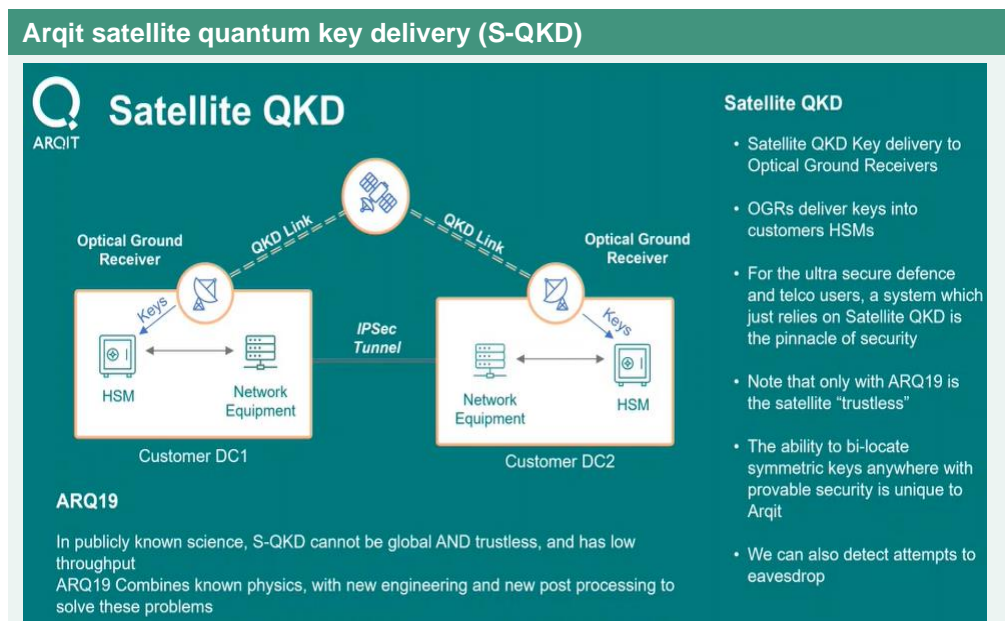
For these reasons satellite-based QKD (S-QKD) emerges as the only viable solution for global distribution of quantum information to end points – *but only if* the global vs trustless conundrum can be solved. Arqit has addressed and resolved this problem with its own version of S-QKD, a Satellite Key Infrastructure (SKI) solution based on its proprietary ARQ19 algorithm. This solution offers:

- Global reach with key data being delivered to any location via a terrestrial Optical Ground Receiver (OGR); and
- Distribution scale. QuantumCloud™ end point innovation means that a two-satellite system has sufficient ‘entropy’ (statistical number capacity) in its data centres to allow digital end points to create and generate 2×10^{15} (two quadrillion) pairs of keys, a huge number of encryption possibilities.

In summary, Arqit’s ARQ19 algorithm addresses and resolves problems that beat standard satellite-based quantum key delivery (S-QKD) using laser delivery to optical ground receivers (OGRs) from which symmetric keys are delivered between any points worldwide.

The S-QKD component of the system should be seen not as a product, but as a component in the tech stack, providing the “root source of randomness” from which all keys are subsequently derived. Putting identical copies of random numbers in multiple locations securely is the ‘holy grail of cyber security’. Given the absence of any mathematical process in the creation of randomness, it follows that a computer cannot reverse engineer it - pure brute force guesswork would be the only means of attack, but for a 256-bit key **this would take even a quantum computer millions of years** to guess all permutations in linear sequence.

In the Arqit solution, satellites in orbit will overpass each location on (Earth $\pm 60^\circ$) three times per day and deposit quantum information to OGRs located at data centres, in addition to which the OGRs which are intended to communicate with each other also undergo a ‘Post Processing’ routine whereby they agree on which bits of quantum information they have in common. This information, often known as “entropy” or “randomness”, is stored for the future construction of keys.



Source: Company

Completing the quantum encryption process

The second feature of Arqit’s solution is that it translates the benefit of its QKD keys into digital keys at end points. An end point – a mobile device, autonomous vehicle or network device – is host to a simple piece of Arqit software, which being less than 200 lines of code, can be stand-alone or embedded/white labelled into another vendor’s application. This software allows **two or more devices** to agree, through interactions with the Arqit network of data centres, to create keys.

The QuantumCloud™ uses the random number synchronised across data centres to orchestrate the creation of a symmetric key at the end points. The datacentre computers only provide clues to the end points, and thus never know the symmetric key or even enough data about it to replicate it, whilst the end points can create almost infinite numbers of such keys at the moment when they are required.

Consequently, keys never exist until they are needed, can be discarded once used and refreshed infinitely across very large groups of devices.

Arqit QuantumCloud™

H2 2021 launch of QuantumCloud™ V1.0 Product offering

The QuantumCloud™ platform-as-a-service V1.0 will be released in H2 2021. We understand that a number of customers have already received and successfully used the software, which is now being productised ready for launch. As outlined, the service enables customers to create and access Symmetric Keys regardless of virtual or physical machine access or location worldwide accessed via QuantumCloud™.

In the Release V1.0, the QuantumCloud™ end point software accesses randomness in data centres which is created using a “emulated” version of the satellite payload, i.e., devices on the ground in data centres create the root source of randomness. As it is not yet based on satellites in orbit currently this solution cannot be regarded as fully-quantum safe, but it is regarded as **sufficiently secure** for the Release V1.0 to be classed as a fully viable product. The entire system will be fully quantum-safe once deployed on satellites set for launch in approximately two years’ time.

Arqit’s customers can today acquire access to the “**Stronger, Simpler**” level of encryption urgently required to face proliferating cyber-attacks to which PKI-based encryption has been shown to be vulnerable. Customers will not experience any change in the method of delivery when the product becomes seamlessly quantum-safe in 2023. The salient features of QuantumCloud™ are:

- Keys are created within a “mixed trust model” which prohibits access by a third-party computer as this information is never transmitted.
- Keys are demonstrably computationally secure, judged impossible for even a quantum computer to unlock in less than *millions of years*.
- There is provision of an unlimited number of Session keys, for encryption of sessions with Arqit client software hosts, and group keys for the encryption of channels with an unlimited number of other user devices (for example, gossip networks).
- Deployment is simple. Symmetric encryption keys are standard in most major software systems making deployment straightforward along with a symmetric algorithm such as AES256; this requires no major change to customer infrastructure. These are also computationally-light allowing deployment on even miniature IoT sensors, an important feature when deployed to secure IoT networks.

QuantumCloud™ can be device-installed as a stand-alone agent or fully integrated into customer software architecture. Arqit judges the only threat to the products to be the standard cyber security measures required to secure physical access to user devices.

Development pathway

Future applications that are under development include: **Managed Quantum Encryption**, a managed service that fragments and encrypts data using quantum keys which can then be stored at any data centre location; **Quantum Digital Signature**, in which transactions are sealed in a quantum key-secured ledger; and **Quantum Streaming**, in which streamed data is separated into 16 segments each secured with a different quantum key, time-bound to create conditional access.

Arqit is also partnering with customers to help them build applications of these encryption techniques into vertical market specific software systems in identity, driverless cars, 5G, blockchain and defence.

Business plan and outlook

Monetising access to *entropy*

We have described how Arqit essentially offers its clients the means to 'access entropy', i.e., the statistical description of the quantum-based random number sets which can be assembled to form encryption keys. Clients 'borrow' from the entropy held in quantum states which enables the creation of pairs of symmetrical encryption keys. This platform-as-a-service offering is the basis of the Arqit business model.

By offering any accredited company the ability to purchase and use in the cloud, Arqit has an opportunity to build a large-scale cloud business. At this stage it also has visibility of early revenues through the sale of the "Private Instance" version of QuantumCloud™ to its government customers. The recent announcement at the 2021 G7 conference illustrates the high visibility of this potential revenue stream.

Implications

There are estimates that the global information security market will have grown **from US\$126bn in 2019 to US\$198bn by 2024**. The capacity potential of Arqit's SKI suggests that a comparatively modest capital outlay will result in the creation of a disproportionately large capacity for revenue generation. Arqit's reservoir of accessible quantum entropy, its key generation resource for clients and the basis of its platform-as-a-service business model, supports the creation of two quadrillion end point software keys per annum and underpins the potential for scaling the offering, supported by investment in online sales and marketing.

In order to generate early traction, Arqit has conducted direct sales into **four key verticals**. The initial key target verticals in which Arqit has established contracted proof-of-concept projects with major corporates are:

- Network encryption - 5G, Software Defined Networks, and IoT.
- Autonomous vehicles.
- Defence command and control systems.
- Financial services.

Order book

Arqit will deploy its flagship solution, QuantumCloud™, in H2 2021, to be followed by a range of user-specific products currently under development.

The contract order book is currently US\$130m, from clients including the UK and other governments and corporates such as BT and Sumitomo who have signed multi-year contracts exceeding £20m each.

For further information regarding Arqit's financial and other information, please see the proxy statement/prospectus and other information that has been filed with the U.S. Securities and Exchange Commission by Arqit Quantum Inc. and Centricus Acquisition Corp. in connection with the business combination transaction, which can be found at sec.gov.

Arqit Federated Quantum System (FQS)

On 11th June at the Cornwall G7 Leaders Conference, Arqit announced the formation of an international group of companies and government organisation to provide its quantum encryption technology to government customers in a federated system concept: the Federated Quantum System (FQS).

Arqit has designed a version of its technology to address governmental preferences for "Private Instances" access to cloud technology rather than in a managed services format. The founder FQS partners comprise: **BT; Sumitomo Corporation; Northrop Grumman; Leonardo; QinetiQ Space N.V.; and Honeywell.**

Developed with support from the **UK Space Agency** (UKSA) through its National Space Innovation Programme, FQS combines dedicated satellites and control systems with Arqit's QuantumCloud™ software. Available to the UK's 'Five Eyes' allied governments and other international partners, its purpose is to provide sovereign protection of strategic national assets and secure interoperability for joint operations. The first FQS satellites are to be integrated and tested at the National Satellite Test Facility in Harwell and are expected to be launched on Virgin Orbit's LauncherOne in 2023, following the launch of the first commercial Arqit satellites.

Although ultimately Arqit's opportunity lies in providing a commercial platform-as-a-service encryption offering, capable of being bought and fulfilled in the cloud by any accredited company at scale, the FQS system offers the opportunity to immediately underpin the revenue outlook. We understand that each FQS system is likely to be priced at around \$25m per annum, and that Arqit already has buying interest in five countries in addition to the UK.

Cybersecurity valuations

The importance of the Cybersecurity sector that Arqit is already active in is clearly shown in the following table that we have compiled. These leading listed participants have a combined market capitalisation of over US\$350bn and trade on a forward average EV/revenue of 22.9x (mkt cap weighted).

Cybersecurity valuations				
Company	Symbol	Mkt cap. (US\$m)	EV/Rev	EV/EBITDA
CrowdStrike	CRWD	55,154	44.8x	N.M
Fortinet	FTNT	40,722	13.1x	44.8x
Palo Alto Networks	PANW	36,126	7.9x	34.8x
Cloudflare	NET	31,768	56.6x	N.M
Okta	OKTA	30,861	28.0x	N.M
Zscaler	ZS	27,735	40.6x	N.M
Splunk	SPLK	22,677	8.8x	N.M
Akamai Technologies	AKAM	19,175	5.9x	13.5x
Check Point Software	CHKP	16,424	7.1x	14.9x
F5 Networks	FFIV	11,449	4.2x	11.6x
Proofpoint	PFPT	9,963	8.3x	51.3x
BlackBerry	BB	6,730	6.8x	48.6x
Varonis Systems	VRNS	5,552	16.2x	N.M
SolarWinds	SWI	5,342	6.2x	13.2x
CyberArc Software	CYBR	5,114	9.6x	69.6x
Rapid7	RPD	4,934	10.3x	N.M
SailPoint Tech	SAIL	4,545	10.9x	N.M
FireEye	FEYE	4,542	4.3x	29.1x
Tenable	TENB	4,097	7.3x	79.6x
Qualys	QYLS	4,007	8.9x	19.7x
Mimecast	MIM	3,317	5.7x	28.0x
Ping Identity	PING	1,844	6.4x	46.8x
Mean			22.9x	36.1x

Source: S&P Global Market Intelligence, Yahoo Finance, Adams Street, ED.

Management and Key Personnel

An important feature, and indication of the depth of technical expertise and organisational strength in Arqit, is the breadth and experience of its Board, advisors, and key technical personnel.

Amongst these are three former senior members of the **UK GCHQ** intelligence agency, including a former Director and former Chief of Research and Innovation, a former **Four Star General** and **Vice Chief of Staff of the U.S. Air Force**, a former Director of the **United States Air Force's Intelligence Surveillance, Reconnaissance and Cyber Effects** enterprise, and a former **Group Chief Information Security Officer at HSBC** and **Chief Technology Officer at Cisco**, together with a range of technical experts with global standing in the fields of cyber security, communications and satellite operation.

Members of the team include:

- **David Williams**, Founder Chairman and CEO. David was the co-founder and CEO of Avanti, which pioneered the use of Ka band satellite communications to deploy geostationary telecom satellites serving the EMEA region. He was Founder Chairman of the Advisory Board of Seraphim Space Ventures, a \$100m high technology venture capital firm. David was granted the Queens Award for Export in 2015 and Quoted Company Entrepreneur of the Year award in 2006.
- **David Bestwick**, CTO and Co-Founder. David was the co-founder and CTO of Avanti. He worked at the Marconi research Laboratory and at VEGA Group plc on the commercialisation of Earth Observation satellite data, has advised the European Space Agency on its telecommunications research strategy and sits on the Board of the Quantum Technology Industry Group.
- **Dr Geoffrey Taylor**, CB. Advisory Board member and Co-Founder. Geoffrey had a 43-year career at GCHQ, in the last 22 years as a Main Board Director. Dr Taylor was made a Companion of The Order of the Bath in 2006 for contribution to national security and economic well-being of the U.K and in 2016 was awarded the US National Security Agency Director's Medal.
- **Dr Daniel Shiu**, Chief Cryptographer. Daniel worked for GCHQ for 20 years. He was a member of the UK's first National Technical Authority for Cryptographic Design and Quantum Information Processing, part of the National Technical Authority function assumed by the new National Cyber Security Centre.
- **Daryl Burns**, Consultant. Daryl worked for GCHQ, the UK's intelligence, cyber and security agency for 34 years, most recently as the Chief of Research and Innovation and the Deputy Chief Scientific Advisor for National Security. Daryl specialised in cryptologic research, analysis and design, including applications and engineering for very large-scale infrastructure projects.
- **Andrew Yeomans**, Consultant and Co-Founder. Andrew has led Information Security Engineering, Architecture and Strategy in Financial Services for 18 years. Andrew was on the management board of the Jericho Forum, an international information security thought-leadership group. He is co-author of 'Java Network Security', the first book to cover secure multi-tier Java applications.
- **Dr. Taher Elgamal**, Director. Taher is an internationally respected information security leader and cryptographer, recognised as the "father" of SSL and invented several industry and government standards in data security and digital signatures for areas including the DSS government standard.
- **David Webb**, Chief Engineer. In early 2009 David joined McAfee to lead a development team for the McAfee enterprise encryption product set, taking over as Director of Engineering and Site Leader at McAfee's Brighton development centre in 2015 with an engineering organisation of over 60 across Brighton, Cork and Bangalore. He was named Leader in the Gartner MQ for Mobile Data Protection for seven successive years.

- **Nick Pointon**, CFO. Nick is a highly experienced CFO with significant NASDAQ, NYSE and M&A experience. After an LLB in Law at Kings College London Nick trained as a Chartered Accountant with Moore Stephens and KPMG. After roles as Financial Controller in private and public telecoms and tech businesses, Nick became Finance Director of King Digital, the NASDAQ-listed operator of Candy Crush games sold to Activision Blizzard for US\$5.9bn. Nick joined Arqit in 2021.
- **Jon Dapre**, CISO. Jon is an experienced leader, CISO, Chief Security Architect and Cyber Security professional, responsible for delivering security risk controls for a range of large corporate and defence contractors including BAE Systems, UK Ministry of Defence and the Atomic Weapons Establishment.
- **Air Vice-Marshal Peter “Rocky” Rochelle** CB OBE DFC MA RAF, Chief Operating Officer. Rocky spent 34 years in the RAF with wide operational experience in Iraq (awarded OBE) and Afghanistan, Kosovo (awarded DFC), in Libya as Tornado Force Cdr and as CO Marham. He has extensive experience in acquisition and Government Strategic Programme Delivery (awarded CB) including: MOD Strategic Programme and Planning; Chief of Staff for the DG FMC; programme Director for Carrier-Enabled Power Projection.
- **General Stephen “Seve” Wilson**. Director, Arqit Inc. General Wilson served as Four Star Vice Chief of Staff of the U.S. Air Force, Arlington, Va. until December 2020 as Chief of the Air Staff and a member of the Joint Chiefs of Staff Requirements Oversight Council and Deputy Advisory Working Group. This involved assisting the Chief of Staff in organising, training, and equipping of 685,000 active-duty, Guard, Reserve and civilian forces serving in the United States and overseas. General Wilson has held numerous command positions, including the Joint Functional Component Commander for Global Strike and Air Force Global Strike Command.
- **Lt General Veralinn Jamieson**, Director Arqit Inc. Lt. Gen. Jamieson is experienced in data management, cloud technology, artificial intelligence and machine learning with over 37 years of government experience. She served as the Director of the United States Air Force’s Intelligence Surveillance, Reconnaissance and Cyber Effects enterprise, conducting operations for the Department of Defence. Prior to assuming her position as Deputy Chief of Staff, Lt. Gen. Jamieson served as the Deputy Commander, Joint Functional Component Command for ISR, U.S. Strategic Command, Washington, D.C.
- **Stephen Holmes**, Chief Product Officer. Stephen has 30 years of experience in IT, including appointments as CTO, Consultant, Architect and product management of disruptive innovation. Stephen has a wide range of experience in commercialising disruptive technologies and has worked at IBM laboratories, Hewlett Packard and was co-founder and CTO of Virtusa Xlabs. Stephen holds an MBA, specialising in marketing innovative products and services and is a certified Enterprise Architect. He represents the UK as an expert on ISO tc307 blockchain and DLT systems.
- **Omar Iqbal**, Space Engineering Director. Omar is a Technology Leader with 17 years’ experience in Satellite Systems and Telecommunications. He held senior engineering roles at Airbus Defence & Space, CGI and Avanti Communications and has delivered pioneering technology in fields including satellite 5G, next generation Very High Throughput Satellites, secure Government communication networks, airborne satcom systems, software defined radios and safety critical satellite applications.
- **Paul Feenan**, Chief Revenue Officer. He has over 26 years of Defence, Security and Global Government experience, including 16 years with the British Army in command and operational roles including Northern Ireland, Bosnia, Afghanistan, Middle East and Africa. He led the UK’s Domestic Counter-Terrorism strategy and planning for the 2012 London Olympics. Paul also has global stakeholder management and sales experience, including four years in a senior management position in Cape Town, building a big data and predictive analytics Fintech Platform across Sub-Saharan Africa in collaboration with AWS, Google and Goldman Sachs as well as several Tier 1 Telcos and Banks.



Contacts

Andy Edmond

Direct: 020 7065 2691

Tel: 020 7065 2690

andy@equitydevelopment.co.uk

Hannah Crowe

Direct: 0207 065 2692

Tel: 0207 065 2690

hannah@equitydevelopment.co.uk

Equity Development Limited is regulated by the Financial Conduct Authority

Disclaimer

Equity Development Limited ('ED') is retained to act as financial adviser for its corporate clients, some or all of whom may now or in the future have an interest in the contents of this document. ED produces and distributes research for these corporate clients to persons who are not clients of ED. In the preparation of this report ED has taken professional efforts to ensure that the facts stated herein are clear, fair and not misleading, but makes no guarantee as to the accuracy or completeness of the information or opinions contained herein.

This document has not been approved for the purposes of Section 21(2) of the Financial Services & Markets Act 2000 of the United Kingdom ('FSMA'). Any reader of this research should not act or rely on this document or any of its contents. This report is being provided by ED to provide background information about the subject of the research to relevant persons, as defined by the Financial Services and Markets Act 2000 (Financial Promotions) Order 2005. This document does not constitute, nor form part of, and should not be construed as, any offer for sale or purchase of (or solicitation of, or invitation to make any offer to buy or sell) any Securities (which may rise and fall in value). Nor shall it, or any part of it, form the basis of, or be relied on in connection with, any contract or commitment whatsoever.

Research produced and distributed by ED on its client companies is normally commissioned and paid for by those companies themselves ('issuer financed research') and as such is not deemed to be independent as defined by the FCA, but is 'objective' in that the authors are stating their own opinions. This document is prepared for clients under UK law. In the UK, companies quoted on AIM are subject to lighter due diligence than shares quoted on the main market and are therefore more likely to carry a higher degree of risk than main market companies. This note is not intended to be read by, or sent to, private investors in the USA and Canada.

ED may in the future provide, or may have in the past provided, investment banking services to the subject of this report. ED, its Directors or persons connected may at some time in the future have, or have had in the past, a material investment in the Company. ED, its affiliates, officers, directors and employees, will not be liable for any loss or damage arising from any use of this document, to the maximum extent that the law permits.

More information is available on our website www.equitydevelopment.co.uk

Equity Development, 15 Eldon Street, London, EC2M 7LD

Contact: info@equitydevelopment.co.uk | 020 7065 2690