February 26, 2026

62% of respondents cite data sovereignty and privacy risks as the biggest factor slowing AI projects in the public cloud

New survey findings to be unveiled at MWC Barcelona 2026 show sovereignty and privacy risks are now the top barriers to AI adoption for network protection

LONDON, Feb. 26, 2026 (GLOBE NEWSWIRE) -- Data sovereignty is fast becoming make or break for AI-driven network safety projects. Yet new survey data shows that one in six organisations cannot rely on access to facilities with guaranteed data sovereignty, while data sovereignty and privacy risks are cited as the leading factor slowing AI projects in the public cloud. These are the findings of research sponsored by Arqit (Nasdaq: ARQQ, ARQQW) and Intel that are set to be unveiled at MWC Barcelona 2026.

As operators and enterprises push AI deeper into network operations, security teams are being asked to both move faster against escalating threats and ensure sensitive data remains under sovereign control. The latter is becoming more challenging as AI pipelines span public cloud, private infrastructure and edge locations. The result is a growing gap between ambition and practical execution.

The research which included a survey of Mobile World Live (MWL) readers found that data sovereignty has now become a project gating issue. 62% of respondents cite data sovereignty and privacy risks as the biggest factor slowing AI projects in the public cloud. More starkly, one in six (16%) say they have no access to facilities with guaranteed data sovereignty at all, underlining how quickly sovereignty has become king for data security.

Key findings include:

- 62% cite data sovereignty and privacy risks as the biggest factor slowing AI projects when using a public cloud.
- 69% say leveraging AI for network safety is urgent or very important, yet 60% are still testing AI for network security or have not deployed it.
- 80% expect to use confidential computing to achieve data sovereignty in cloud or edge locations in the next 12 months, including 41% planning deployments across both cloud and edge.
- 16% say they have no access to facilities with guaranteed data sovereignty, and only 8% say they have guaranteed sovereignty at the edge.
- Delays to AI transformation are already being felt as operational pain, with impacts on operational efficiency (53%), competitive advantage (48%) and customer experience (45%).

These findings come at a moment when AI and automation are becoming central to the connectivity industry's roadmap. AI can help defenders detect anomalies and harden networks at scale, but it also increases the volume, sensitivity and movement of data. Training and operating models often requires sharing telemetry, logs and security signals between various stakeholders and platforms, making sovereignty constraints harder to ignore.

"AI is quickly becoming part of the network security stack, but the data feeding those systems is among the most sensitive that operators and critical infrastructure providers hold," says Andy Leaver, CEO of Arqit. "This research with MWL shows sovereignty is now a make-or-break requirement, with the majority of teams citing sovereignty and privacy risks as the biggest brake on AI projects in the public cloud.

"At the same time, one in six organisations tell us they cannot guarantee sovereign facilities at all, and only 8% can rely on sovereign edge environments today. That gap is exactly where security leaders need stronger controls for data in transit, better visibility into cryptographies, and a practical means of building trust across cloud and edge."

Arqit's work with telecoms and network operators focuses on protecting data in motion across complex, distributed environments. At MWC 2026, Arqit is demonstrating how operators can move faster on network security without losing control of sensitive data as AI workflows expand across public cloud, private infrastructure and edge locations. On **Stand 7C11 in Hall 7 in the UK Pavilion**, Arqit and Intel will showcase how they are working together to help organisations benefit safely from AI-assisted network safety, and provide genuine, end-to-end sovereignty for enterprise customers.

About Arqit
Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) secures the world's most critical data with quantum-safe encryption software. Simple, scalable, and compliant, its products integrate with existing infrastructure, and requires no rip and replace of hardware.

Arqit provides a complete "Detect, Protect, Comply" solution for governments and enterprises that detects and inventories cryptographic assets, protects data, ensures compliance, and safeguards transition to the post-quantum era.

Arqit's primary product offerings are Encryption Intelligence and NetworkSecure™. Encryption Intelligence detects cryptographic exposure, identifies vulnerabilities, and maps dependencies. NetworkSecure™ protects data in transit with provably secure post-quantum cryptography and contributes to establishment of confidential compute environments for complete data sovereignty.

Arqit is an IDC Innovator for Post-Quantum Cryptography (2024) and a multi-award-winner in quantum-safe security. For more information, visit www.arqitgroup.com

Media relations enquiries:
Arqit: pr@arqit.uk
Investor relations enquiries:
Arqit: investorrelations@arqit.uk

Caution About Forward-Looking Statements

This communication includes forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements, other than statements of historical facts, may be forward-looking statements. These forward-looking statements are based on Arqit's expectations and beliefs concerning future events and involve risks and uncertainties that may cause actual results to differ materially from current expectations. These factors are difficult to predict accurately and may be beyond Arqit's control. Forward-looking statements in this communication or elsewhere speak only as of the date made. New uncertainties and risks arise from time to time, and it is impossible for Arqit to predict these events or how they may affect it. Except as required by law, Arqit does not have any duty to, and does not intend to, update or revise the forward-looking statements in this communication or elsewhere after the date this communication is issued. In light of these risks and uncertainties, investors should keep in mind that results, events or developments discussed in any forward-looking statement made in this communication may not occur. Uncertainties and risk factors that could affect Arqit's future performance and cause results to differ from the forward-looking statements in this release include, but are not limited to: (i) the outcome of any legal proceedings that may be instituted against Arqit, (ii) the ability to maintain the listing of Arqit's securities on a national securities exchange, (iii) changes in the competitive and regulated industries in which Arqit operates, variations in operating performance across competitors and changes in laws and regulations affecting Arqit's business, (iv) the ability to implement business plans, forecasts, and other expectations, and identify and realise additional opportunities, (v) the potential inability of Arqit to successfully deliver its operational technology, (vi) the risk of interruption or failure of Arqit's information technology and communications system, (vii) the enforceability of Arqit's intellectual property, (viii) market and other conditions, and (ix) other risks and uncertainties set forth in the sections entitled "Risk Factors" and "Cautionary Note Regarding Forward-Looking Statements" in Arqit's annual report on Form 20-F (the "Form 20-F"), filed with the U.S. Securities and Exchange Commission (the "SEC") on 9 December 2025 and in subsequent filings with the SEC. While the list of factors discussed above and in the Form 20-F and other SEC filings are considered representative, no such list should be considered to be a complete statement of all potential risks and uncertainties. Unlisted factors may present significant additional obstacles to the realisation of forward-looking statements.

ARQIT

Source: Arqit