WHITE PAPER

The Power of MultiCloud:

Unleashing a Transformative Power for Digital Ecosystems

The transformative power of multi-cloud environments is enabling organizations to capitalize on the unique strengths of different cloud providers, realize unparalleled system resilience, and optimize cost and performance for strategic agility. In multi-cloud environments, entities use multiple cloud computing and storage services in a single network architecture which allows customers to capitalize on different offerings and expertise in artificial intelligence, machine learning, and advanced analytics.

Building on Partnerships

In September 2023, Microsoft joined Oracle as the only other hyperscaler to offer Oracle Cloud Infrastructure database services, simplifying cloud migration, multi-cloud deployment, and management. For the United States Department of Defense, the multi-cloud environment is becoming a strategic asset for enhancing national security and defense operations. Such platforms can store and process data across multiple secure locations, thereby ensuring redundancy and resilience against cyber-attacks or physical disasters. The strategic partnership between Microsoft and Oracle allows customers to connect their Oracle Cloud Infrastructure and Microsoft Azure resources via a dedicated private connection, utilize single sign via identity federation, and access collaborative technical support from both Oracle and Microsoft. This is the future of reliability, security, and effectiveness."

The DoD has solicited AWS, Microsoft, Google and Oracle to support its Joint Warfighting Cloud Capability (JWCC) program, a multibillion-dollar project which replaced the JEDI cloud contract. These cloud services support all security classification levels and span the entire Defense enterprise from the continental United States to the deployed tactical edge. The multi-cloud approach facilitates advanced data analysis and intelligence gathering through specialized services from these different providers, and enables secure, real-time communication and coordination across various military branches and global bases. This brings a technological edge and operational efficiency in defense scenarios.

Secure Data Transport in Multi-Cloud Architectures

This shift in tactical network architecture manifests new challenges and risks. One of the primary challenges in maintaining security in multi-cloud environments is managing the diverse security protocols and configurations of different cloud providers. This complexity can create inconsistencies and gaps in security. To address this, Arqit provides a security solution to allow customers to ensure all connections between multiple clouds are encrypted with high-grade, quantum-safe security between the provider environments.

To that end, Arqit has successfully demonstrated a world-first cross-cloud integration of quantum-secure symmetric key agreement for encryption of data in transit. Leveraging Juniper vSRX virtual firewalls deployed within both Azure and OCI environments, Arqit's Symmetric Key Agreement technology was leveraged to allow these network devices to dynamically agree symmetric IPsec session keys on-demand, thereby providing the foundation for quantum-secure data in event is significant step towards securing the wider DoD's tactical multi-cloud network environments against not just the quantum threat, but also the risks presented by the integration of disparate technology stacks.

> **"Customers can only realize the benefits of multi-cloud environments when they can be assured of security across their multi-cloud solutions. This demonstration is a landmark effort in providing that assurance."**
>
> - Michael Murphy, *Arqit CTO*

In a multi-cloud environment, the exchange of data between cloud environments is a critical aspect of cloud computing, and secure data transit is paramount. As data moves across different cloud enclaves it becomes susceptible to interception, unauthorized access, or tampering, posing significant risks to data integrity and confidentiality. Arqit ensures secure data transport which is crucial to maintaining trust in cloud services and protecting sensitive information. The Arqit solution involves the use of robust encryption protocols for data in transit, and NIST cryptography to safeguard data from eavesdropping and man-in-the-middle attacks. Additionally, all keys are created in a "split trust" fashion – with key material being distributed across multiple data paths – and with continuous authentication to guarantee only authorized entities can initiate data transfers. In essence, secure data transport is foundational to the operational security of cloud-based systems, ensuring that data remains protected as it traverses through various cloud platforms and networks. This solution is in alignment with the latest Symmetric Key Management Requirements Annex v2.1 (19 May 22) issued by NSA Commercial Solutions for Classified Program.

Reinforcing Cybersecurity through Diversification

A multi-cloud approach also significantly enhances security by diversifying risk across multiple cloud platforms and enhancing the resilience of critical systems. In this strategy, critical data and applications are distributed among different cloud service providers, which means that a security breach or a system failure in one cloud does not compromise the entirety of an organization's digital assets. This diversification acts as a safeguard against a wide range of potential threats, including localized outages, cyber-attacks, or service disruptions. By not putting all their digital 'eggs' in one basket, organizations can mitigate the impact of a single point of failure. Furthermore, different cloud providers may employ varied security protocols and measures, which add layers of defense against threats. This multifaceted security approach makes it more challenging for attackers to compromise an organization's data, as they would need to breach multiple distinct security systems. Additionally, a multi-cloud environment allows organizations to leverage the unique security strengths and specialized compliance capabilities of different providers, ensuring more comprehensive protection tailored to specific needs and regulatory requirements. In essence, a multi-cloud strategy spreads out the risk and provides a more resilient and robust security posture for organizations navigating the complexities of digital operations.

Organizations can tap into the best of these technologies from various providers to drive innovation. This demonstration achieves a new capability for USG customers to migrate and run business-critical enterprise workloads across Microsoft Azure and Oracle Cloud in a secure manner.

Integrating Land, Air, Sea, and Space: Transforming JWCC's Capabilities

The Joint Warfighter Cloud Capability (JWCC) stands to greatly benefit from a multi-cloud approach in its mission to process data more effectively and seamlessly connect forces across land, air, sea, space, and cyber domains. With unparalleled flexibility and scalability, multi-cloud environments enable JWCC to leverage the specific strengths and capabilities of different cloud providers to optimize data processing for varied military needs and ensure seamless communication and data sharing among different branches of the armed forces.

Data and applications are distributed already across multiple clouds. Hence, by embracing the multi-cloud model, JWCC can achieve higher levels of redundancy and resilience, crucial for maintaining operational continuity even in the face of disruptions or attacks. Moreover, this framework supports advanced analytics and real-time data processing, enhancing decision-making and situational awareness in complex, multi-domain operations.

JWCC can ensure robust protection of sensitive military data, while adhering to stringent compliance and regulatory requirements by using state-of-the-art security measures across various cloud platforms with the Arqit solution. As companies like Microsoft, Oracle and Arqit, build strategic multi-cloud collaborations, JWCC will be empowered to create a more agile, integrated, and secure infrastructure, capable of supporting the dynamic and multifaceted nature of modern military operations.