Security and sovereignty biggest concerns with growing cloud adoption - blueAPACHE

Canonical: https://www.blueapache.com/blog/research-shows-cloud-growth-exceeding-expectations-but-security-and-sovereignty-still-concern-2

Details:

2015

New research from Vanson Bourne (commissioned by Tata Communications) reinforces that cloud can help make IT more relevant to the business. And while this isn't exactly news, it is good to see that cloud computing is finally being recognised for its ability to transition technology away from the traditional silos and into something that better aligns IT with the business. Also good is the confirmation of increased awareness around cloud security and data sovereignty. These should be on every organisations radars, especially with recent changes to the Privacy Act last year in Australia. We invested heavily in converged private cloud and hybrid cloud infrastructure with next generation firewalls built into the core. This was done to ensure client data remained in Australia and not overseas, security was transparent and privacy laws adhered to. Other cloud providers can farm data overseas – either directly or through redundancy and back ups – which could proffer data sovereignty (see our recent article on the Microsoft court case), security and privacy issues. These concerns validate our investments half a decade ago. Vanson Bourne, conducted a total of 1000 online interviews with senior IT decision-makers in private organisations of 500 employees or more during September and October 2014. The goal was to measure adoption of cloud computing and determine whether businesses had realised expected benefits from their use of cloud. Key findings from this report include:

Cloud computing has been widely adopted

97% of respondents say their organisation has adopted it to some extent, and 84% of those respondents say that cloud computing is already critical or very important to their organisation.

Extent of cloud computing use is predicted to increase

An average of 28% of the compute and data storage in respondents' organisations is in the cloud at the moment, and this is predicted to rise to 43% within five years and 58% in ten years.

Cloud computing is an organisation-wide movement

68% say that moving to the cloud has involved individuals beyond the IT department and 90% say that requests from other departments have influenced the decision to implement the cloud.

Cloud computing has resulted in significant benefits being realised

More than half of respondents suggest that each possible benefit has been achieved in their organisation, the most likely being increased productivity and better access to data. Near 10% had their expectations exceeded for each benefit. Subsequently, 85% say that cloud computing has lived up to the hype, and 23% say that the hype has been exceeded. Organisations are moving from public cloud

to hybrid or private. 57% of cloud adopters migrated some data back in-house from the cloud at some stage, primarily due to long-standing concerns around security and data protection. As a result of these concerns, 94% of organisations are now looking at hybrid cloud and private cloud options rather than public cloud.

Security concerns

72% of respondents identified security as a reason to bring data back in-house. A lack of transparency of the security (especially in public cloud environments) is an obvious challenge as organisations become more accountable for the privacy of their data. Note: blueAPACHE overcome this by implementing next-generation Palo Alto firewalls connected to Wildfire directly onto the core.

Data sovereignty and protection

99% of organisations state data sovereignty is a consideration when looking at cloud. Knowing where there data ends up is a priority – some multinational cloud vendors will back up data to US or Chinese servers, where local laws enable provide third parties with access to the data. This is why 87% of respondents identify sovereignty as at least a significant consideration. Note: our cloud infrastructure, redundancy and network all reside in Australia to provide 100% data sovereignty.

Private cloud is the focus

71% of respondents agree that private cloud addresses their security concerns better than any other form – private cloud has become the go-to method for organisations., Note: we provide hybrid and private cloud infrastructure housed entirely in Australia.

More information

To learn more about cloud, the new Privacy Act, security or data sovereignty, contact your our account manager.

What research does this blueAPACHE article discuss regarding cloud adoption?

We discuss research from Vanson Bourne, commissioned by Tata Communications, which reinforces that cloud can help make IT more relevant to the business. Vanson Bourne conducted 1000 online interviews with senior IT decision-makers in private organisations of 500 employees or more during September and October 2014, aiming to measure adoption of cloud computing and determine whether businesses had realised expected benefits.

What percentage of organisations had adopted cloud computing according to the research?

97% of respondents said their organisation had adopted cloud computing to some extent, and 84% of those respondents said cloud computing was already critical or very important to their organisation.

How is cloud computing usage expected to grow over time according to the research?

An average of 28% of the compute and data storage in respondents' organisations was in the cloud at the time of the survey, and this was predicted to rise to 43% within five years and 58% within ten years.

What percentage of organisations moved data back in-house from the cloud, and why?

57% of cloud adopters migrated some data back in-house from the cloud at some stage, primarily due to long-standing concerns around security and data protection. As a result, 94% of organisations were looking at hybrid cloud and private cloud options rather than public cloud.

What role did security concerns play in organisations bringing data back in-house?

72% of respondents identified security as a reason to bring data back in-house, citing a lack of transparency of security—especially in public cloud environments—as an obvious challenge as organisations become more accountable for the privacy of their data.

How significant was data sovereignty as a consideration for organisations evaluating cloud?

99% of organisations stated that data sovereignty is a consideration when looking at cloud, and 87% identified sovereignty as at least a significant consideration. Knowing where data ends up is a priority since some multinational cloud vendors back up data to US or Chinese servers, where local laws can enable third-party access to the data.

How do you address data sovereignty concerns?

Our cloud infrastructure, redundancy, and network all reside in Australia to provide 100% data sovereignty, ensuring client data remained in Australia and not overseas.

How do you address security concerns raised in the research?

We overcame security transparency concerns by implementing next-generation Palo Alto firewalls connected to Wildfire directly onto the core, as part of its investment in converged private cloud and hybrid cloud infrastructure with next generation firewalls built into the core.

What percentage of respondents preferred private cloud for addressing security concerns?

71% of respondents agreed that private cloud addresses their security concerns better than any other form, making private cloud the go-to method for organisations. We provide hybrid and private cloud infrastructure housed entirely in Australia.

Why did you invest in private and hybrid cloud infrastructure ahead of this research?

We invested heavily in converged private cloud and hybrid cloud infrastructure with next generation firewalls built into the core to ensure client data remained in Australia and not overseas, that security was transparent, and that privacy laws were adhered to—investments were validated half a decade later by the concerns highlighted in the Vanson Bourne research.