The challenges facing cloud computing for security conscious government communities

Cloudy with a Chance of Transformation

GOVERNMENT INSIGHTS
Cloudy with a Chance of Transformation

Cloud computing has rapidly become an accepted and widespread feature of the IT landscape, and is a transferable concept to security conscious government communities. However, Andrew Wilson explains that challenges still remain – not least when it comes to security, policy and skills...

There was a time, not so long ago, that any mention of “cloud” would automatically refer to something in the sky above, as opposed to anything else. No longer.

Today, cloud computing has taken firm root amongst organisations large and small. Its countless benefits – empowering mobile workforces, for example, or reducing IT costs, increasing efficiency and reducing time to market – have helped transform the way organisations, both public and private, do business.

Partly this is because cloud is not actually as new and shiny as it may seem on first appearances. Far from being something clad in technological mystery, in reality its development is not that different from incremental advances of the past. Back in the day, we had VT terminals and central processing/data storage which in turn morphed into the next new approach to computing, the network computer and thin clients – lightweight computers optimised for establishing a remote connection with a server-based computing environment.

Cloud is kind of the same – only bigger, faster and less focused on the terminal and instead enabling the open and interchangeable delivery of applications and complex services. This means organisations don’t have to rely on bespoke cloud providers in order to reap its benefits. This is because the use of cloud has been made incredibly simple and repeatable, reducing the barrier to entry by providing the necessary complex data science and machine learning platforms on demand. In essence, cloud has greatly facilitated access to enterprise level IT and services.

Executive Summary

Cloud computing has taken firm root amongst organisations large and small – but that doesn’t mean challenges don’t remain. Is cloud as secure as more traditional methods of data storage? Can organisations – particularly those in government or national security – justify outsourcing security concerns to their cloud service providers 24/7?

The good news is that leveraging the cloud securely can be done – either from at home or in the office. Government departments can protect their most sensitive information assets by deploying Cross Domain Solutions and ensure that security is an intrinsic function of every government cloud deployment. Andrew Wilson explains more…
Challenges aplenty

But that doesn’t mean challenges don’t remain. For example, even as data and applications have increasingly taken up a cloud-based residence, the security, reliability and availability implications remain open to question: is cloud as secure as more traditional methods of data storage? Can organisations – particularly those in government or national security – justify outsourcing security concerns to their cloud service providers 24/7? Can organisations be assured that at peak times their workloads will get prioritised and delivered against competing demands from other ‘tenants’?

Such questions were even before COVID-19 cast its long shadow. Now, since the pandemic struck, all government organisations have shifted the majority of their developers to working from home. This has included a significant amount of work that previously defaulted to secure systems, but the development work can often be done in cloud environments and then securely migrated across – thereby facilitating a significant increase in those who can work remotely.

Something many in the community now wish to explore is a new cultural way of working to retain the agile benefits which result from access to cloud technologies and open source tools and data. And that’s not all.

Skills, too, remain something of a perennial problem. Of course, governments of every political stripe have long sought to attract the best and brightest, but when it comes to cloud development there remains a significant gap which needs addressing. The problem is that government has a huge number of engineers using its software, but they don’t necessarily have the skills around cloud or insight into how to operate and exploit an internet-connected environment.

There is also the adoption and through-life supportability issue to be addressed. The flexibility of the cloud, when looking at options for everything from storage and security to applications (including machine learning and analytics), is incredibly empowering. However, translating that agility and evergreen architecture to internal legacy IT systems is very difficult.
So what then can be done? It’s important to first understand the background. Departments and agencies across government have been on a digital journey in recent years. Programmes such as the Royal Navy’s NELSON are spearheading an innovative charge towards the sunlit uplands of digital transformation, but that’s not to say it is always a smooth process.

To take the Defence sector as an example, the Ministry of Defence now operates across five domains. In addition to the traditional land, sea and air, cyber and space have been added to the areas which have to be defended. As a result, critical information now needs to be shared across all five, as well as partner organisations and coalition allies, all of which have different security classifications, legalities and compliance policies. This is hugely challenging, especially in a diverse set of independent computing infrastructures.

Defence also has to utilise a wide array of technology – including ruggedized equipment from the 1960s that’s stood the test of time but which is built upon now-obsolete technology platforms. This means that in an operational zone, limited bandwidth, connectivity and interoperability with modern systems can limit collaboration potential with coalition partners.

All this means that skilled and experienced professionals are essential to navigate this tricky terrain and in doing so help overcome the security concerns which are the biggest barrier to cloud uptake, secure collaboration and information exploitation. This also means that we need an environment where cloud best practices can be adopted, but also one that enables easy integration between domains while adhering to compliance standards and automatically applying security overlays.

So how can all this be done in a cost effective and timely way?
Striking the right balance

Finding a way through these issues is not easy. What’s crucial, though, is understanding the business drivers and security concerns. Unfortunately, it’s all too easy to fall into the trap of focusing on getting the tech delivered and operating, and forgetting what the technology is actually intended to support.

When this happens it reduces the chances of learning from what has gone before, thus minimising the business improvement opportunity. Technology should be a catalyst to drive improvements to operational doctrines and transformation – taking advantage of innovation and mitigating the new cyber risks, not just automate an antiquated process.

Government departments obviously need to protect their most sensitive information assets. So when we talk about “secure cloud”, what we really mean is making use of cloud technologies and exploiting everything they offer in a safe way, deploying Cross Domain Solutions (CDS) and ensuring security is always an intrinsic function of every government cloud deployment.

CDS involves creating an air-bridge where it is known exactly what data passed, when, and accessed by whom – with assurances in place to assure compliance standards. CDS have been used for some time to pass pre-defined data sets between different security domains – now we need to do more of it – and faster – for cloud.

Cross Domain working can be further enabled by using homomorphic and obfuscated processing of data between classification levels. This makes it possible to work on data in other domains without sharing sensitive information about search or processing criteria, or having to allow unfettered access to bulk personal data sets – thus limiting intrusion when analysing data.

Click here to find out more about BAE Systems Cross Domain Solutions
Onwards to Secure Cloud

Cloud and close engagement with industry has been a gradual and evolutionary process. The good news is that leveraging the cloud securely can be done – either from home or in the office.

I’ve just marked my 10 year anniversary of working at BAE Systems Applied Intelligence and during this time we’ve helped many organisations close the gap between domains and digitally transform their organisations in a complex multi-domain environment, while still keeping security and compliance paramount. And even during the COVID-19 Pandemic, we’ve helped our secure government clients operate in new homologated ways in the cloud – not easy when the vast majority of IT professionals, like all of us, have been working from home.

Organisations with a long track record of understanding how technology fads wax and wane are well placed to create solutions which combine agility with sustainability. However, the tempo of changing technology and demand to rapidly deliver new services is ever increasing. There is a need to be able to respond to and exploit innovative new technologies and processes but in a measured way.

The bottom line is that a balance is needed as to what happens in the cloud and what happens elsewhere – and that’s not going to change any time soon.

About the author

Andrew Wilson is an Engineering Lead at BAE Systems Applied Intelligence

andrew.wilson18@baesystems.com
We are

BAE SYSTEMS

At BAE Systems, we provide some of the world’s most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.