The Three Pillars of a Secure Hybrid Cloud Environment
Introduction

How sound risk management, transparency and a sharp focus on compliance lay the foundation for a hybrid cloud environment that won’t compromise your business’ security posture.

For most businesses, a move to the cloud isn’t an ‘all or nothing’ affair and it certainly doesn’t happen overnight. Many organisations initially build a private cloud independently. As their confidence grows, they’ll typically move to a hybrid model, that is, a blend of public and private cloud services. Whatever the mix of cloud services an organisation opts into, security can’t be considered as an afterthought. Dimension Data security experts, Tom Gilis and Stefaan Hinderyckx, turn a critical eye to the areas where businesses may run into trouble.
Pillar 1: risk assessment and management

‘All too often, organisations’ journeys to the cloud veer off course as they’ve not thoroughly evaluated the impact of moving a particular asset – be it a service or data – to the cloud,’

says Gilis.

‘At the same time, many organisations simply assume that a move to the cloud will inevitably involve greater levels of risk. What’s called for is an in-depth risk assessment.’

Gilis believes that ideally, the assessment should include the following steps:

- A **definition of the risks** that apply to various asset(s), based on their business criticality.
- An **assessment of the current status** of each risk before it’s moved to the cloud. Using this information, each risk can be accepted, mitigated, transferred or avoided.
- An **assessment of the risk profile** of each asset, assuming it has been moved to the cloud.

The outcome will allow the business to compare the different level of risk associated with its current state and the ‘desired’ cloud solution.

‘Assets with higher risk profiles may be better suited to a private cloud environment. The results may even lead you to conclude that a particular business service or asset can’t or shouldn’t be moved to the cloud at all,’ explains Gilis.

‘Interestingly, such assessments often reveal that a move to the cloud actually won’t open the business up to security vulnerabilities in the ways originally assumed. Counter to popular stereotypes, security isn’t necessarily always a cloud inhibitor. But success lies in gathering sound data and then managing your risks proactively.’

It’s also important to bear in mind that a ‘hybrid’ cloud environment can also include scenarios in which private clouds and applications ‘burst’ out to a public cloud provider for additional capacity as required.

This is something organisations may not have considered, but it represents a key benefit of a move to the cloud. However, it’s important that this flexibility is considered as part of the overall risk assessment.
Pillar 2: provider transparency

The importance of clear and transparent communication on the part of cloud providers regarding the security embedded in their offerings shouldn’t be underestimated. For businesses, moving to the cloud is something of a leap of faith. Cloud involves relinquishing a degree of control – which means sleepless nights for security professionals. Providers would do well to share as much information as possible with prospects about their environment, offerings, controls and configurations in order to build a foundation of trust and allay any concerns, early on in the sales cycle.

Hidden costs often derail cloud implementations. Here Gilis believes that businesses need to look for providers that aren’t afraid to explore these as part of the negotiation process.

‘Organisations need to factor in the costs associated with changing their processes, for example. Providers need to demonstrate that they’re aware of the various risks associated with implementing a cloud strategy and put forward suggestions on how to mitigate them, based on their experiences with other clients,’ he says.

Gulis believes that another effective way for cloud providers to gain and retain their customers’ trust – so their customers become more comfortable in relinquishing control – is to formalise the handover process.

‘Once policies and procedures are set up, schedule weekly, monthly or quarterly meetings, reviews and audits, and thoroughly assess any areas of poor performance or concern. Providers should also be upfront about any security incidents that have occurred, and willing and able to explain how these were attended to.’

Hinderyckx adds that, when evaluating cloud providers, oftentimes IT security leaders aren’t clear about what kinds of questions they should be asking.

‘Dimension Data often assists clients by providing them with a list of questions that we believe they should be posing to cloud providers as part of the evaluation process, to ensure they’re covering all the bases.’

Pillar 3: policy and compliance

Cloud providers need to understand that simply listing compliance certifications isn’t sufficient. In line with the mantra of transparency explored in the previous point, providers should take a proactive stance to sharing their security implementations and controls.

‘While adherence to standards and regulations should be a minimum baseline for the consideration of any provider, alone it’s not enough to engender a buyer’s confidence that everything it wants from a compliance perspective will be covered,’ says Hinderyckx.

‘Organisations should look for providers that don’t only provide proof of their certification, but can also explain how they achieve and maintain their compliance levels, what problems they’ve encountered in this area and how these have been overcome.’

‘Dimension Data often assists clients by providing them with a list of questions that we believe they should be posing to cloud providers as part of the evaluation process, to ensure they’re covering all the bases.’