



What is the future for hybrid cloud strategies and the role of the IT department?

Corporate data compliance policies are under pressure from the ease and the lure of cloud technologies as well as the runaway mobilization of the workplace. Hybrid strategies offer some respite from the relentless drive to the cloud - but long term for the true economies and benefits of the cloud to be realized there must be innovation in and delivery of cloud friendly security solutions.

Many companies are operating a hybrid cloud strategy today - in fact, they may have been for some time - it's not really anything new. A hybrid cloud means that you have some technology and infrastructure that you operate and manage in house - and some that you rely on 3rd parties to operate and manage for you. Payroll functions have, for many companies, been handled and processed by 3rd

parties - but other HR functions have been kept in internal IT systems. There are real economies and benefits that can be derived from operating IT services on public and shared infrastructure - as well as some risks. Companies have access to elastic, instant and easy to manage services that reduce the burden on IT operations as well as increase employee productivity and communications. However, in an unregulated manner, employees inadvertently allow sensitive information to sit in potentially exposed areas outside of corporate policies and enforcements for data.

The drive to maintain corporate compliance as well as benefit from the economies of the public cloud will drive more innovations around solutions that provide compliance in these environments. Therefore the strategy will be for the hybrid cloud to continue a shift away from the private infrastructure in to the public infrastructure. The hybrid will be more public. Mobile and remote access, instant provisioning and more manageable IT costs provide inevitable momentum that will force the market to deliver solutions to the problems around governance and compliance of data.

This momentum will also drive more generalized cloud oriented solutions for businesses. Software startups today rarely consider developing software for on-premise deployment -

because they know that business will prefer to acquire new solutions and innovations as a service. Large businesses today already rely on cloud based collaboration, CRM, payroll, accounting, data archival, anti-spam and anti-malware technologies. The next wave will come in the form of more generalized desktop applications such as presentation, document editing and, importantly email solutions. Cloud based solutions naturally solve problems of access in every corner of the globe and on every device.

These trends also reduce the complexity and costs of managing software licenses. SafeNet helps companies manage licensing for the products they build - their customers also have to manage the costs and complexities of the licenses they consume. The ability to be nimble and to shift software platforms are hampered not only by data migration, security and training factors - but also because of license agreements that entrap companies financially. Moving to cloud based software solutions reduces the financial constraints of traditional on premise software - and greatly relieves the burden of managing deployed software. Cloud based software solutions provide easy, centralized and instantly variable options - they also shift the compliance burden on to the vendor and away from the customer - relieving customers from the constraints of an audit and so on. However the ease in which software can be accessed on demand has to be tempered with the ease at which sensitive data can fly out of a company.

Solutions to both cloud data governance (an enterprise problem) and cloud software access control and security (an ISV/service provider problem) will accelerate the already rapid move in favor of the public side of the hybrid equation.

How will this affect IT departments? Over the long term the focus of the IT department will be much less around managing equipment either in the server room, the desktop or the employees pocket and more on accessing control interfaces that manage security, policy and governance of data. The era of controlling data by firewalling, end point control and physical access will give way to authentication, policy/key management and solutions for virtual machine security. Public cloud providers will deploy more sophisticated security technologies that enable strong, cryptographically provable protection while their customers retain the electronic keys that govern their data. Data compliance solutions will shift from the end-point to the server side (in the cloud) - providing IT with more effective means for controlling and managing policies. This inevitably leads to greater compliance with less complex tools for the IT department. IT departments will therefore re-focus on their core mission on solving higher level business problems and delivering greater efficiencies and opportunities for their business - without spending resources on buying, managing, replacing and controlling complex software and sensitive data across thousands of globally dispersed desktop and mobile devices.

This interview was published in [SIIA's Vision from the Top](#) , a Software Division publication released at [All About the Cloud](#) 2012.