Cloud Cover

Analysts have long waxed lyrical about cloud services coming of age, but it is board directors and business owners who need convincing if the model is to fulfil its true potential. Chris Russell, VP Engineering at Swivel Secure says that only watertight security from cloud service providers will steady corporate nerves.

Chris Russell, VP Engineering at Swivel Secure

Despite the increasing maturity of cloud based solutions, concerns at the board level about data security continue to hold back widespread corporate adoption. As with so many technologies the problem is one of communication; IT managers have always struggled to talk the language of the board, which often means the board does not to fully understand the factors that should influence its decision.

It is no surprise, therefore, that decision makers remain uneasy with the concept of cloud computing and applications. From their perspective the idea of placing their critical systems and confidential data in the hands of a third party is questionable enough, let alone accepting that it could all reside on 'a faceless bank of servers in who-knows-where'.

If cloud service providers are to make the headway their solutions deserve in 2013, reassurances are needed. Board directors must be convinced that their cloud based corporate data is secure. Thanks largely to the media attention that Anonymous is commanding, access control is the first issue to spring to mind. The most powerful persuader, therefore, does not come in the form of a service level agreement promising five nines availability. Neither is it an impressive map of virtual cloud servers dotted around the globe. What's needed is a cloud solution that will build the confidence of the board as each month goes by, together with a rock solid user identification solution that is easy to understand and does exactly what it says on the tin, or in board-speak 'the digital equivalent of a good old fashioned lock and key'.

Tokenless two factor authentication (2FA) delivered as a managed service meets these needs. It is a simple, elegant, cost effective and strong security solution that can be used to verify the identity of anyone looking to gain access to corporate applications and data in the cloud. And because it puts the user right at the heart of the authentication process its power is also remarkably easy to comprehend, which goes a long way to assuaging the suspicions of techno-sceptic board directors.

Winning over a cautious board will not happen overnight, so cloud service providers will also need to be patient and flexible in 2013. That's why authentication vendors like Swivel Secure are aligning their contract and payments terms with a managed services business model. They understand that channel partners need to roll authentication into their own service offerings without incurring the risks associated with traditional annual vendor contracts. Offering resellers short-term contracts and monthly payments will enable them to pass on this flexibility to their corporate customers, giving the freedom for a customer to test the water with a rolling contract, before committing resources to a full blown cloud migration.

The channel should view the widespread reluctance to migrate to the cloud as an opportunity to help organisations to bridge the gap. Virtualisation within an organisation's existing infrastructure is a solution that even smaller organisations, with modest IT requirements can benefit from. Through investing in their own infrastructure, rather than the cloud software licenses, businesses can buy software-as-a-service and run that software on their own virtualised infrastructure. This will expose companies to many of the cloud's benefits, such as replacing cap-ex with op-ex and dispensing with the worry about ongoing operation and maintenance costs, without needing them to commit fully to a public-cloud model.

This is an opportunity for the channel to add real value. If something goes wrong or customisations are required, a smaller managed service provider with, say, twenty customers will be able to respond far quicker than a big cloud services organisation, whose customer base could be in the millions. Most importantly, however, this model acts as a useful halfway house in which companies can familiarise themselves with a cloud-based environment, building their confidence in the model ahead of a possible full migration into the cloud at some point in the future.

It would be a great shame in 2013 if adoption of cloud solutions fell short due to potential adopters not being aware of the security options available. That said, with the introduction of the right kinds of security measures together with some smart service provisioning from the channel, there is no reason why the cloud shouldn't finally come of age. Granted, it won't be an overnight sensation, but if it is pitched appropriately, businesses everywhere should be feeling the benefits of cloud by the end of the year.

2FA in a Nutshell

Two-factor authentication is commonly found in electronic computer authentication, where basic authentication is the process of a requesting entity presenting some evidence of its identity to a second entity. Two-factor authentication seeks to decrease the probability that the requestor is presenting false evidence of its identity. The number of factors is important, as it implies a higher probability that the bearer of the identity evidence indeed holds that identity in another realm (i.e.: computer system vs. real life). In reality, there are more variables to consider when establishing the relative assurance of truthfulness in an identity assertion than simply how many "factors" are used.

Two-factor authentication is often confused with other forms of authentication. Two-factor authentication requires the use of two of the three authentication factors. The factors are identified in the standards and regulations for access to U.S. Federal Government systems. These factors are:

- Something the user knows (e.g., password, PIN, pattern);
- Something the user has (e.g., ATM card, smart card); and
- Something the user is (e.g., biometric characteristic, such as a fingerprint).