

Concerns for Cloud security? Best look internally - blueAPACHE

Canonical: <https://www.blueapache.com/blog/concerns-for-cloud-security-best-look-internally>

Details:

2015

Sixty-three percent of IT professionals cite security as a top concern with public cloud according to Tech Buyer Snapshot. A separate survey of 300 IT security professionals conducted last year showed the percentage of respondents who preferred to keep sensitive corporate data on-premises rather than in the cloud was eighty percent. While perceptions of cloud security may be improving, the real threat to cloud security may not have anything to do with the service provider. At the recent Gartner Symposium/ITxpo 2016 in Orlando, Daryl Plummer presented on humanity and technology. He stated that through 2020, 95 percent of cloud security failures will be the customer's fault. While organisations still harbour security concerns about the use of public cloud services, only a small percentage of security incidents impacting enterprises using the cloud have been due to vulnerabilities that were the provider's fault. Cloud providers invest heavily in security, prevention and recovery. Their business relies on it. More often than not, customers will look to blame their service provider for breaches and data loss before assessing internal policies, procedures and security – despite studies showing that the leading cause of data loss is human error. Plummer believes this will lead to customers seeking cloud access security brokers products to manage and monitor their use of SaaS and other forms of public cloud services. Security is key to successfully leveraging the many benefits of the cloud, especially with the lack of clarity on data sovereignty, new data retention laws and recent changes to the Privacy Act. Despite the suggestion that security issues will likely be caused by in-house issues, we strongly encourage organisations to perform due diligence on their cloud providers to ensure they meet the changing compliance and regulatory requirements faced in Australia. To better understand cloud security (and the processes you can put in place to better secure your cloud connectivity), contact the blueAPACHE Cloud team.

What percentage of IT professionals cite security as a top concern with public cloud, according to the blueAPACHE article?

According to the Tech Buyer Snapshot survey cited in our article, sixty-three percent of IT professionals cite security as a top concern with public cloud.

According to Gartner's Daryl Plummer, what proportion of cloud security failures will be the customer's fault through 2020?

At the Gartner Symposium/ITxpo 2016 in Orlando, Daryl Plummer stated that through 2020, 95 percent of cloud security failures will be the customer's fault.

What do customers tend to do when breaches or data loss occur, ?

customers will more often than not look to blame their service provider for breaches and data loss before assessing their own internal policies, procedures and security.

What is cited as the leading cause of data loss ?

studies show human error is the leading cause of data loss.

What solution does Daryl Plummer believe customers will seek in response to cloud security concerns?

Plummer believes customers will seek cloud access security broker products to manage and monitor their use of SaaS and other forms of public cloud services.

Why do you still recommend organisations perform due diligence on their cloud providers despite the customer-fault trend?

Despite the suggestion that security issues will likely be caused by in-house issues, blueAPACHE strongly encourages organisations to perform due diligence on their cloud providers to ensure they meet the changing compliance and regulatory requirements faced in Australia, given the lack of clarity on data sovereignty, new data retention laws, and recent changes to the Privacy Act.

Who should be contacted for help understanding cloud security according to the blueAPACHE article?

We advise contacting our Cloud team to better understand cloud security and the processes that can be put in place to better secure cloud connectivity.