Cloud security strategies rest too heavily on blind trust according to survey commissioned by iland

Submitted by: C8 Consulting
Tuesday, 24 May 2016

As business and IT finally align on security priorities, companies throw technology at issues, fail to validate claims and struggle to manage resources

News highlights

• Forty-seven percent of security personnel “simply trust” their cloud providers meet security agreements without further verification
• Forty-eight percent more security technologies are deployed in the cloud than on-premises, and security now tops the list of cloud priorities
• Business and IT agree they would rather delay a product launch or application deployment than risk security vulnerabilities
• Ninety-one percent of respondents reported they need cloud providers to help with security integration, reporting and/or leveraging analytics

LONDON — 24th May, 2016 — iland (http://www.iland.com/), an award-winning enterprise cloud hosting provider, today announced findings of a new cloud security survey it commissioned independent analyst firm Enterprise Management Associates (EMA) to conduct. The study reveals that companies now consider cloud security to be superior to on-premises environments, but often expose themselves to risk by blindly relying on a glut of technology they are unable to actively manage.

Analysing insights from 100 IT decision makers and security experts who leverage cloud infrastructure and/or Disaster-Recovery-as-a-Service in North America, the findings are published in a study entitled, “Blind Trust Is Not a Security Strategy: Lessons from Cloud Adopters (http://info.iland.com/ema-cloud-security-survey).”

“Companies can no longer combat security threats by simply throwing technology at perceived vulnerabilities,” said David Monahan, research director, security and risk management at Enterprise Management Associates. “Though teams are using more security tools in the cloud than on-premises, they still face major risks as they struggle with staffing and skills shortages that make it extremely difficult to adequately evaluate, integrate and manage solutions.”

Key survey findings put spotlight on evolving security perceptions and practices:

• As IT recognises cloud as an imperative, teams focus on fortifying environments with significantly more tools than are used on-premises. In fact, 48 percent more security technologies are deployed in the cloud than on-premises (See report (http://info.iland.com/ema-cloud-security-survey) for detailed tools). Further, “security features” now tops the list of priorities companies consider when selecting a cloud provider, ahead of performance, reliability, management tools and cost.

• IT now sees cloud adoption as an opportunity to improve security with previously unused technology. When asked why they had not deployed specific security features in the cloud, respondents indicated they

were currently in the evaluation phase twice as often as any other reason for non-deployment, including cost, complexity, availability or that the technology was unnecessary.

• Business and IT finally agree on the priority of cloud security. While business teams have often used cloud to bypass IT, the two teams are now more aligned on security priorities than ever before. For example, respondents indicated IT would rather delay a new application deployment due to security concerns than deploy it in a potentially insecure environment, and business agrees in a nearly 3 to 1 margin. This represents a fundamental shift in organisational dynamics, where business should no longer view security personnel as naysayers, but allies who are committed to fighting threats.

However, the survey also points to important underlying flaws and opposing perceptions that must be addressed:

• Cloud customers do not validate security claims. Forty-seven percent of security personnel reported they “simply trust” their cloud providers are delivering on security agreements, rather than verify it independently or through a third party.

• While organisations cite advantages of cloud security over on-premises, they also report it is lacking in key ways. Fifty-five percent of respondents said cloud uses superior technology to on-premises, and 56 percent indicated that security technology is more consistently applied in cloud. However, cloud customers admit they need more help from their cloud providers when it comes to integrating security technology (52 percent), improving security reporting (49 percent) and improving security analytics (44 percent).

• There is a significant gap in IT’s understanding of compliance requirements and related workloads. While 96 percent of security professionals acknowledge that their organisations have compliance related workloads in the cloud, only 69 percent of IT teams identified the same. This gap could lead to exposures for the organisation if IT were to place a compliance-related workload into a non-compliant cloud provider.

“EMA research also identified that 68 percent of organisations have staffing shortages and 34 percent have skills shortages, which directly correlates to flaws and opposing perceptions uncovered in this study,” said Monahan. “While IT has made monumental progress in identifying and adopting necessary security technologies, cloud providers must do more to ensure teams can easily validate claims, manage disparate tools, anticipate threats and take action when needed.”

“As is often the case in technology, the crux of the problem when it comes to cloud security has shifted from the technology of securing the cloud to the operations and management – the people side – of securing the cloud,” said Justin Giardina, CTO at iland. “At iland, we’ve designed our offerings with the mindset that technology, alone, does not solve a problem. Not only are we committed to supporting customers with our expert compliance team, we will also continue to evolve our platform to integrate more turnkey, automated security functionality that enables teams of all sizes and expertise levels to protect themselves against increasing cyber threats.”

The results of the findings as well as recommendations will be discussed at length on 8th June in an

iland webinar featuring David Monahan of EMA Research. To register for the webinar, visit www.iland.com/webinar/cloud-security-blind-trust (https://www.brighttalk.com/webcast/13901/204773).

For more information on iland Enterprise Cloud Hosting or the EMA survey, go to:
• iland Enterprise Cloud Services – Advanced Security (http://www.iland.com/services/)
• iland Disaster-Recovery-as-a-Service (http://www.iland.com/services/cloud-disaster-recovery/)
• Blind Trust Is Not a Security Strategy: Lessons from Cloud Adopters (http://info.iland.com/ema-cloud-security-survey)

About iland

With data centres in the U.S., U.K. and Singapore, iland delivers the only enterprise cloud solutions in the market today with true innovation, transparency, intelligent management and advanced security built in. iland's technology and consultative approach mean anyone– regardless of expertise, location or business objective–can benefit from a hassle-free cloud. From scaling production workloads, to supporting testing and development, to disaster recovery, iland's secure cloud and decades of experience translate into unmatched service. iland has been recognised as Veeam's Service Provider of the Year as well as VMware's Service Provider Partner of the Year, Global and Americas. iland is also part of the Cisco Cloud Managed Service Provider Program for IaaS and DRaaS and partners with other industry leaders including Zerto, Trend Micro, Hytrust and Nimble Storage. Visit www.iland.com (http://www.iland.com/).

Trademarks
All registered trademarks and other trademarks belong to their respective owners.

# # #

Media contacts
Kellie Willman
iland
+1 713-337-1347
kwillman@iland.com

UK Media contact:
Paula Elliott
+44 1189 497736
paula@c8consulting.co.uk