New Intel Security Cloud Report Reveals IT Departments Find It Hard to Keep the Cloud Safe
Monday, February 13, 2017 05:00:00 AM (GMT)

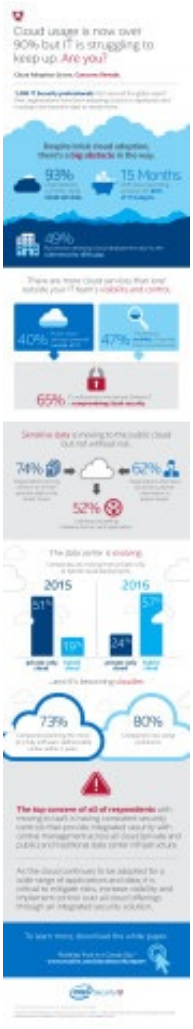
Close to 40 Percent of Cloud Services Are Commissioned Without the Involvement of IT, Leading to More Security Risk for Companies

NEWS HIGHLIGHTS

- Trust now outnumbers distrust for public clouds by more than 2-to-1.
- 49 percent of professionals slowed cloud adoption due to a lack of cybersecurity skills.
- 65 percent think Shadow IT is interfering with keeping the cloud safe and secure.
- 52 percent indicate a malware infection can be tracked to a cloud application.
- 62 percent store sensitive customer information in the public cloud.

RSA SECURITY CONFERENCE – Intel Security today announced its second annual cloud security report, "Building Trust in a Cloudy Sky." The report outlines the current state of cloud adoption, the primary concerns with private and public cloud services, security implications, and the evolving impact of Shadow IT of the more than 2,000 IT professionals surveyed.

This Smart News Release features multimedia. View the full release here: http://www.businesswire.com/news/home/20170212005011/en/



Intel Security on

"The 'Cloud First' strategy is now well and truly ensconced into the architecture of many organizations across the world," said Raj Samani, EMEA chief technology officer, Intel Security. "The desire to move quickly toward cloud computing appears to be on the agenda for most organizations. This year, the average time before respondents thought their IT budgets would be 80 percent cloud-based was 15 months, indicating that Cloud First for many companies is progressing and remains the objective."

Trust in the Cloud on the Rise

The trust and perception of public cloud services continues to improve year over year. Most organizations view cloud services as or more secure than private clouds, and more likely to deliver lower costs of ownership and overall data visibility. Those who trust public clouds now outnumber those who distrust public clouds by more than 2-to-1. Improved trust and perception, as well as increased understanding of the risks by senior management, is encouraging more organizations to store sensitive data in the public cloud. Personal customer information is the most likely type of data to be stored in public clouds, kept there by 62 percent of those surveyed.

Risks Also Rise: Shadow IT and the Cybersecurity Skill Shortage

The ongoing shortage of security skills is continuing to affect cloud deployments. Almost half of the organizations surveyed report the lack of cybersecurity skills has slowed adoption or usage of cloud services, possibly contributing to the increase in Shadow IT activities. Another 36 percent report they are experiencing a scarcity but are continuing with their cloud activities regardless. Only 15 percent of those surveyed state they do not have a skills shortage.

Due to the ease of procurement, almost 40 percent of cloud services are now commissioned without the involvement of IT, and unfortunately, visibility of these Shadow IT services has dropped from about 50 percent last year to just under 47 percent this year. As a result, 65 percent of IT professionals think this phenomenon is interfering with their ability to keep the cloud safe and secure. This is not surprising given the amount of sensitive data now being stored in the public cloud and more than half (52 percent) of respondents reporting they have definitively tracked malware from a cloud SaaS

Intel Security on Monday, Feb. 13, 2017, announced its second annual cloud security report, "Building Trust in a Cloudy Sky." One finding of the more than 2,000 IT professionals surveyed showed that the trust and perception of public cloud services continues to improve year over year. (Credit: Intel Corporation)

application.

Data Center Progression

The number of organizations using private cloud only has dropped from 51 percent to 24 percent over the past year, while hybrid cloud use has increased from 19 percent to 57 percent. This move to a hybrid private/public cloud architecture requires the data center to evolve to a highly virtualized, cloud-based infrastructure. On average, 52 percent of an organization's data center servers are virtualized, 80 percent are using containers and most expect to have the conversion to a fully software-defined data center completed within two years.

Recommendations:

- Attackers will look for the easiest targets, regardless of whether they are public, private or hybrid. Integrated or unified security solutions that provide visibility across all of the organization's services could be the best defense.
- User credentials, especially for administrators, will be the most likely form of attack. Organizations need to ensure they are using authentication best practices, such as distinct passwords, multi-factor authentication and even biometrics where available.
- Security technologies such as data loss prevention, encryption and cloud access security brokers (CASBs) remain underutilized. Integrating these tools with an existing security system increases visibility, enables discovery of shadow services, and provides options for automatic protection of sensitive data at rest and in motion throughout any type of environment.
- Organizations need to evolve toward a risk management and mitigation approach to information security. They should consider adopting a Cloud First strategy to encourage adoption of cloud services to reduce costs and increase flexibility, and put security operations in a proactive position instead of a reactive one.

Find More Information:

- To download the full report, visit www.mcafee.com/cloudsecurityreport.
- RSA Security Conference attendees can view panelist Raj Samani at the session titled, "Security in the Cloud: Evolution or Revolution." The session will take place at 2:00 p.m. Pacific time on Feb. 13 at the Marriott Marquis, San Francisco.
- Read Raj Samani's blog, "Cloud Ubiquity – it's coming, but not yet!"
    - Twitter: Follow @IntelSecurity for cloud security updates and tips.

Survey Methodology

In fall 2016, Intel Security surveyed over 2,000 IT professionals across a broad set of industries, countries and organization sizes. Research participants were senior technical decision-makers from small, medium and large organizations located in Australia, Brazil, Canada, France, Germany, Japan, Mexico, Saudi Arabia, Singapore, the United Arab Emirates, the United Kingdom and the United States.

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. Intel Security is a division of Intel Corporation. Learn more at www.intelsecurity.com.

View source version on businesswire.com: http://www.businesswire.com/news/home/20170212005011/en/

--30-- DK/SF

Contact:

Intel Security
Tracy Holden, 650-245-8466
Tracy.Holden@intel.com

1.2

Industries: Technology, Data Management, Hardware, Internet, Networks, Software, Security, Semiconductor, Mobile/Wireless
Languages: English
Primary Identifiers: INTC-US
Related Identifiers: INTC-US, US458140100
Source: Intel Security
Subjects: Conference, Survey, Trade Show, Photo/Multimedia