Building Trust in a Cloudy Sky

Cloud services are now a regular component of IT operations, and are utilized by more than 90% of organizations around the world. Many are working under a Cloud First philosophy, only choosing to deploy an internal service if there is no suitable cloud variant available. As a result, IT architectures are rapidly shifting to a hybrid private/public cloud model, with those surveyed expecting 80% of their IT budget to be cloud-based within an average of 15 months.

93%

of organizations **utilize cloud services** in some form

49%

of respondents had **slowed their cloud adoption** due to a lack of cybersecurity skills

62%

of organizations reported **storing personal customer information** in public clouds

Intel Security surveyed over 2,000 IT professionals in September 2016 to produce this annual review of the state of cloud adoption, representing a broad set of industries, countries, and organization sizes. In the face of a continuing shortage of skilled security personnel, the impact of this scarcity on cloud adoption was a priority for this year's report. Other objectives included understanding the adoption of different cloud usage models, identifying the primary concerns with private and public cloud services, and investigating the evolving impact of Shadow IT.

Research participants were senior technical decision makers from small (500-1,000 employees), medium (1,000-5,000 employees), and large (more than 5,000 employees) organizations, located in Australia, Brazil, Canada, France, Gulf Coast (Saudi Arabia & United Arab Emirates), Germany, Japan, Mexico, Singapore, the United Kingdom, and the United States.

Key Findings

- Cloud services are widely used in some form, with 93% of organizations utilizing Software-, Infrastructure-, or Platform-as-a-Service offerings.
- The average number of cloud services in use in an organization dropped from 43 in 2015 to 29 in 2016, indicating potential consolidation of cloud providers or solutions. Cloud architectures also changed significantly, from predominantly private-only in 2015 to increased adoption of public cloud resulting in a predominantly hybrid private/public infrastructure in 2016.
- Almost half (49%) of the professionals surveyed stated that they had slowed their cloud adoption due to a lack of cybersecurity skills, with the worst shortages in Japan, Mexico, and the Gulf Coast countries.
- 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 much 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 2:1.

intel Security

Executive Summary

52%

of respondents have tracked a **malware infection to a SaaS application**

40%

of cloud services are **commissioned without the involvement of IT**

65%

of IT professionals believe that **Shadow Cloud is interfering** with their ability to keep the cloud safe and secure

2 years

Time in which respondents expect to have a fully **software-defined data center**

- 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% of those surveyed.
- Cloud applications continue to be a vector for cyberattacks, and over half (52%) of the respondents indicate that they have definitively tracked a malware infection to a SaaS application.
- Shadow IT is a growing concern for the IT department. Driven by the slower adoption of IT or the mainstream acceptance of clouds, almost 40% of cloud services are commissioned without the involvement of IT. As a result, 65% of IT professionals think that this phenomenon is interfering with their ability to keep the cloud safe and secure.
- Virtualization of private data center architectures is progressing. On average, 52% of an organization's data center servers are virtualized, and most expect to have the conversion to a fully software-defined data center completed within 2 years.

Conclusions and Recommendations

Businesses are trusting cloud services with a wide range of applications and data, much of it sensitive or business critical. Data goes to where it is needed, most effective, and most efficient, and security needs to be there in advance to quickly detect threats, protect the organization, and correct attempts to compromise the data. Cost and resource savings of cloud services are real, and the wide variety of offerings makes it possible to choose the best fit for the organization. Security vendors are delivering tools to address fundamental security concerns, such as protecting data in transit, managing user access, and setting consistent policies across multiple services.

The movement of sensitive data to the public cloud may attract cybercriminals. Attackers will look for the easiest targets, regardless of where they are located. Integrated or unified security solutions are a strong defense against these threats, giving security operations visibility across all of the services the organization is using and what data sets are permitted to traverse them.

User credentials, especially for administrators, will be the most likely form of attack. Organizations should ensure that they are using authentication best practices, such as distinct passwords, multi-factor authentication, and even biometrics where available.

Despite the majority belief that Shadow IT is putting the organization at risk, security technologies such as data loss prevention (DLP), 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.

While it is possible to outsource work to various third-parties, it is not possible to outsource risk. Organizations need to evolve towards a risk management and mitigation approach to information security. 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.

For full report please **download here**.

intel Security

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com