Building Trust in a Cloudy Sky

Global Views from Healthcare Organizations

Possibly driven by cost-saving opportunities and rapid digitization of medical information, usage of cloud services by the healthcare industry is slightly above the global industry average, utilized by 96% of these organizations, compared to the global average of 93%. Like their counterparts in other industries, 81% 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, healthcare IT architectures are gradually shifting from a private cloud data center infrastructure to a hybrid private/public cloud model, with those surveyed expecting their IT budget to be 80% cloud-based within an average of 15 months.

This analysis of healthcare adoption of cloud services, their concerns, and future plans was extracted from **Intel Security's 2016 Cloud Research**. Research participants were senior technical IT security decision makers, located in Australia, Brazil, Canada, France, Gulf Coast (Saudi Arabia & United Arab Emirates), Germany, Japan, Mexico, Singapore, the United Kingdom, and the United States.

96%

cloud adoption rate puts healthcare organizations in the **top three industries** for cloud adoption

24%

of healthcare organizations use **public-only** (SaaS, IaaS, or PaaS) cloud services

Key Findings—Healthcare

According to our research, healthcare organizations are now in the top three industries for cloud adoption (96%), behind only finance (99%) and technology firms (99%) in the percent of their industry that are running some type of cloud services. The average number of cloud services in use at healthcare organizations dropped from 41 in 2015 to 33 in 2016, less of a drop than the global average, which fell from an average of 43 to 29 services, but still indicating potential consolidation of cloud providers or services.

Cloud architectures changed significantly, from predominantly private-only in 2015 to predominantly hybrid private/public, although healthcare organizations were the lowest reported users of hybrid architecture. Surprisingly, healthcare organizations were among the highest users of public-only (SaaS, IaaS, or PaaS) cloud services, at 24%, well above the global average of 19%. Senior IT professionals in the healthcare industry reported that they are almost twice more likely to be using SaaS than either IaaS or PaaS offerings. SaaS is also their primary focus for the coming year, with 67% of them planning to increase their investment in these services.

intel Security

Executive Summary

46%

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

60%

of healthcare organizations **store customer (patient) data** in public clouds

52%

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

38%

of cloud services in healthcare organizations are **commissioned without the involvement of IT** and IT has visibility into only half of these

Almost half (46%) of the healthcare professionals surveyed stated that they had slowed their cloud adoption due to a lack of cybersecurity skills. This was especially true when asked specifically about IaaS concerns. Skills required by IT security staff was the top IaaS concern of healthcare respondents, and was ranked higher than consistent and integrated security controls, the top IaaS concern of the global survey group.

While security skills may be slowing adoption, the trust and perception of public cloud services continues to improve year-over-year for healthcare organizations. Most of these organizations view public cloud services as or more secure than private clouds, and consider public clouds to be much more likely to deliver lower costs of ownership and overall data visibility than private clouds. Those who trust public clouds now outnumber those who distrust public clouds by more than 2:1. Improved trust and perception, as well as increased understanding of the risks by senior management, is encouraging more healthcare organizations to store sensitive data in the public cloud. This may be due to their higher than average concern (37% vs the survey global average of 30%) about unauthorized access of sensitive data in a private cloud. Possibly due to electronic health records and the interconnected nature of the healthcare system, these organizations are among the most likely to store some or all of their sensitive data in the public cloud, especially customer (patient) data (60%) and staff data (54%).

However, cloud applications continue to be a vector for cyberattacks, and over half (52%) of the healthcare respondents indicate that they have definitively tracked a malware infection to a SaaS application. They are also among the most likely to have experienced data loss (25% vs global average of 22%) or malware incidents (13% vs global average of 10%) with cloud service providers.

Shadow IT remains an issue for healthcare IT departments, as it is for IT departments from most industries. Not all of the SaaS usage in healthcare is sanctioned by IT. Healthcare professionals report that cloud services commissioned without the involvement of IT is 38% of their service usage, and they have visibility over only half of these applications. When they find an unauthorized Shadow IT app, the most likely response was blocking access to the app completely. Overall, healthcare IT professionals are quite concerned about Shadow IT, with 63% of them stating that this phenomenon is interfering with their ability to keep the cloud safe and secure.

While healthcare organizations are embracing SaaS, and have higher-than-average usage of public-only cloud services, 26% remain using private-only services, and 50% are using a hybrid mix of public and private. On the private side, the current percentage of virtualized data center servers is just a bit below the global average, at 51% vs 52%, and healthcare professionals reported that they are among the leading users of containers. The majority (76%) expect to complete the transition to a fully software-defined data center within 2 years.

Conclusions and Recommendations

It appears that healthcare organizations are more likely to use and trust SaaS apps than other industries. They are in the middle of the pack using private clouds, and among the lowest users of hybrid clouds. Whether caused by this public cloud usage, the increasing value of their data, or some combination of the two, they are seeing more cyberattacks, malware incidents, and data loss than their counterparts in most other industries.

Clouds are here to stay, and healthcare security operations need to stay ahead of the adoption curve to protect the organization. The wide variety of cloud offerings available makes it possible to choose the best fit for the organization, addressing both cost-savings and security needs. Security vendors are delivering the necessary tools to address fundamental security concerns, such as protecting data in transit, managing user access, and setting consistent policies across multiple services.

Executive Summary

Healthcare organizations have valuable health records, and have attracted the attention of cybercriminals for ransomware attacks in the past year, according to the **December 2016 McAfee Labs Threats Report.** At the same time, healthcare practitioners are actively embracing new technologies that help improve the quality and effectiveness of patient care. Attackers will continue to look for the easiest targets, regardless of where they are located. Integrated or unified security solutions are a strong defense against these threats by providing security operations visibility across all of the services the organization is using and what data sets are permitted to pass between them.

According to the **2017 McAfee Labs Threat Predictions Report**, user credentials, especially for administrators, will be the most likely form of attack. Ensure that you are using appropriate protection on all endpoints, including tablets and smartphones. Authentication best practices, such as distinct passwords, multi-factor authentication, and biometrics where available, are essential preventative strategies that substantially reduce the risk of infection or compromise.

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 more detailed information, please read the full report, **Building Trust in a Cloudy Sky**.

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

JANUARY 2017