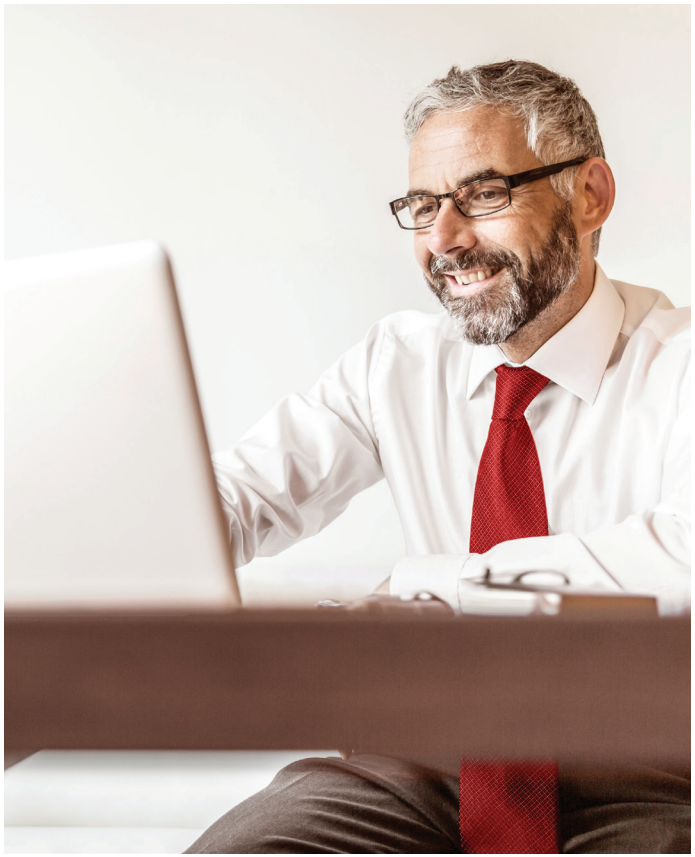
McAfee
Together is power.

Building Trust in a Cloudy Sky

Global views from financial services organizations



According to our study, financial services firms are more likely to use cloud services than any other industry. Cloud functions are utilized by 99% of these organizations, compared to the all-industry global average of 93%. As an industry, they are among the top organizations that have implemented a Cloud First philosophy, choosing to deploy an internal service only if there is no suitable cloud variant available, with 87% implementing this philosophy, compared to a global average of 82% of organizations. We further discovered that IT architectures for financial services organizations are rapidly 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 14 months.

99%

of financial services organizations **run some type of cloud services**

57%

of financial services organizations **use hybrid public/private solutions**

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

Key Findings—Financial Services

Financial services organizations are leading cloud adoption (99% of organizations surveyed), tied only with technology firms in the percent of their industry that are using some type of cloud service. Cloud architectures for these firms changed significantly over the past year. Firms with private-only cloud services dropped from 50% in 2015 to 26% in 2016, as more moved to hybrid private/public solutions, which are now utilized by 57% of financial services organizations.

Almost half (48%) of the financial services professionals surveyed stated that they had slowed their cloud adoption due to a lack of cybersecurity skills among their IT staff. While security skills and concerns may be slowing adoption, the trust and perception of public cloud services continues to improve year over year. Most financial 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 provide data visibility than private clouds. Being secure from hackers was the only benefit that they thought was more likely to be realized through private clouds that public clouds.

Cloud applications continue to be a vector for cyberattacks, and over half (54%) of the financial services respondents indicate that they have definitively tracked a malware infection to a Software-as-a-Service (SaaS) application. However, they are among the least likely to have experienced data loss or breaches (19% vs global average of 22%).

Financial services organizations that trust public clouds now outnumber those who distrust public clouds by more than 2:1

This 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. Possibly due to the ubiquitous nature of online financial transactions and other services, financial service organizations are among the most likely to store some or all of their sensitive customer data in the public cloud (64%).

Senior IT professionals in the financial services industry reported that they are most likely to use SaaS (64%), closely followed by Infrastructure-as-a-Service (IaaS) (57%), with Platform-as-a-Service (PaaS) offerings a distant third (38%). However, their investment plans for the coming year are weighted more towards IaaS, with 69% planning to increase activity in that area, compared to 60% planning increases in SaaS and 52% planning increases in PaaS.

Their primary concern with using SaaS was the same as other organizations, protecting sensitive data as it moves to and from the cloud. With IaaS offerings, their

48%

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

54%

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

64%

of financial service organizations **stored some of all of their sensitive customer data** in public clouds

39%

of cloud services are **commissioned without the involvement of IT** and **IT has visibility over only 45%** of them

top concerns were maintaining compliance and the potential for unauthorized access in a multitenant public cloud, while the top IaaS concern for other organizations was consistent security controls. The average number of cloud services in use at financial organizations dropped from 40 in 2015 to 29 in 2016, indicating potential consolidation of cloud providers.

Shadow IT is an issue for financial services IT departments, as it is for IT departments in most industries. Financial IT professionals report that cloud services commissioned without the involvement of IT is 39% of their service usage, and they have visibility over less than half (45%) of these applications. Most financial organizations are relying primarily on next-generation firewalls to monitor non-IT approved cloud usage (59%). When they find an unauthorized Shadow IT app, the most likely responses were blocking access to the app completely (28%) or relying on identity and access management (27%) to limit access. Surprisingly, given their higher-than-average concern about protecting data as it moves to and from the public cloud, they were slightly below average users of DLP and encryption tools. Overall, financial services IT professionals are among the most concerned about Shadow IT, with 72% of them stating that this phenomenon is interfering with their ability to keep the cloud safe and secure.

While financial organizations are embracing the pubic cloud, 26% remain using private cloud-only services and 57% are using a hybrid mix of public and private. On the private side, the current percentage of data center server virtualization is above the global average, at 55% versus 52%, and financial professionals reported that they are adopting containers on par with the global average of 80% of organizations. The majority (73%) expect to complete the transition to a fully software-defined data center within two years.

Conclusions and Recommendations

It appears that financial services organizations are among the top industries in both cloud usage and security maturity. They reported higher cloud usage but lower breaches than their counterparts in other industries.

Clouds are here to stay, and security operations in the financial services sector are working to stay ahead of the cloud adoption curve. 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.

Financial services organizations have valuable payment records, and they have long been the target for cybercriminals. Attackers will continue to look for the easiest targets, regardless of whether they are in public, private, or hybrid clouds. Integrated or unified security solutions are a strong defense against these threats by providing security operations visibility across all services the organization is using and what data sets are permitted to pass between them.

According to the **McAfee® Labs 2017 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, multifactor 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 IT 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. If you haven't already, 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.

Learn More

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

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com