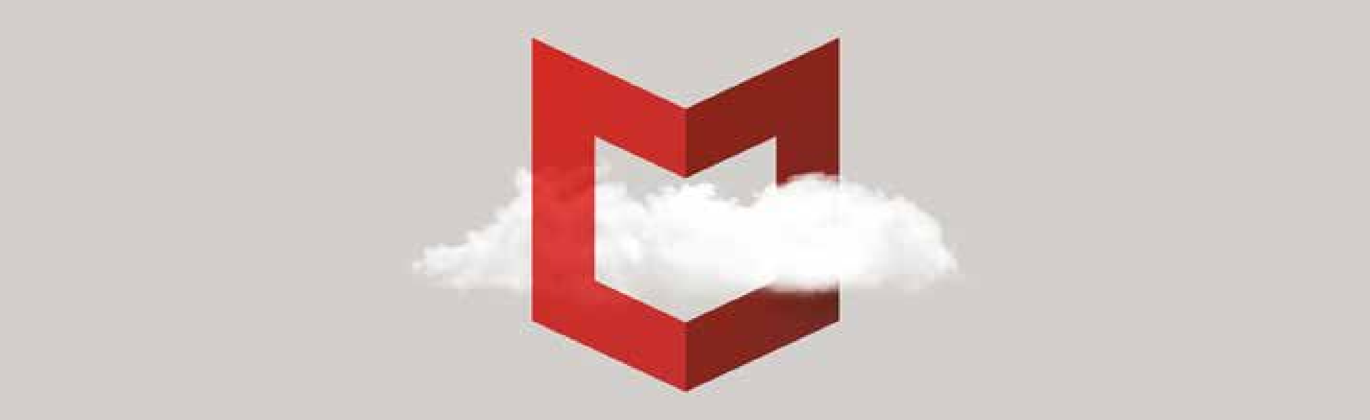
Navigating a Cloudy Sky

Practical Guidance and the State of Cloud Security



Executive Summary

As computing, storage, and collaboration transition to the cloud, IT professionals are finding it difficult to navigate with the confidence that their assets are secure. 97% of organizations worldwide are using some type of cloud service, and are concurrently working through issues related to visibility and control. Some executives are moving slowly due to a lack of visibility, while others move boldly ahead, knowing they face the risk of security incidents along the way.

McAfee® surveyed 1400 IT professionals in late 2017 to produce this annual review of the state of cloud adoption and security, representing a broad set of industries, countries, and organization sizes. Practical guidance on cloud security best practices was a primary objective of this year's report, so we investigated current usage patterns, concerns, and incidents to provide expertise targeted at the most pressing issues organizations face.

Security incidents were found to be pervasive. Prominently, 1 in 4 organizations who use Infrastructure-as-a-Service (IaaS) or Software-as-a-Service (SaaS) have had data stolen, and 1 in 5 have experienced an advanced attack against their public cloud infrastructure. As some organizations prepare for the European Union's General

Key Survey Findings[1]

97% Of organizations use cloud services (public, private, or a combination of both), up from 93% one year ago.

65% Have a cloud-first strategy, down from 82% one year ago.

83% Store sensitive data in the public cloud.

69% Trust the public cloud to keep their sensitive data secure.

1 in 4 Have experienced data theft from the public cloud. (found for both Software-as-a-Service and Infrastructure-as-a-Service).

1 in 5 Have experienced an advanced attack against their public cloud infrastructure.

Data Protection Regulation (GDPR), we also asked about expected impacts to future cloud adoption in light of this new law.

Research participants were 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, Germany, India, Japan, Mexico, Singapore, the United Kingdom, and the United States.

Conclusions and Recommendations

Better visibility enables an organization to confidently adopt transformative cloud services sooner, respond more quickly to security threats, and reap the cost savings the cloud provides. It is better to be able to see everything in the cloud, than to attempt to control an incomplete portion of it.

Visibility-driven organizations are using a full range of cloud services to find the best fit for each business need. They tend to have a more relaxed approach to shadow IT, looking on it as an early indicator of emerging trends and useful applications, instead of an adversarial relationship to be shut down as quickly as possible. They want to see as much as possible, and then make informed decisions about the optimal approach to control.

Based on the findings from this year's study, the report concludes with three best practices that we recommend all organizations should be actively working towards:

1. DevSecOps processes. DevOps and DevSecOps have been demonstrated to improve code quality and reduce exploits and vulnerabilities. Integrating development, QA, and security processes within the business unit or application team is crucial to operating at the speed today's business environment demands.
2. Deployment automation and management tools, such as Chef, Puppet, or Ansible. Even the most experienced security professionals find it difficult to keep up with the volume and pace of cloud deployments on their own. Automation that augments human advantages with machine advantages is a fundamental component of modern IT operations.
3. Unified security with centralized management across all cloud services and providers. Multiple management tools make it too easy to for something to slip through. A unified management system across multiple clouds with an open integration fabric reduces complexity.

For the full report please download here.

40% Of IT leaders are slowing cloud adoption due to a shortage of cybersecurity skills.

2x More likely to have a strategy for securing containers and serverless computing when a DevSecOps function is present.

27% Of IT security budgets on average are allocated to cloud security –estimated to reach 37% in 12 months.

<10% Of organizations on average anticipate decreasing cloud investment as a result of the European Union's General Data Protection Regulation (GDPR).

[1] See full report Appendix for details of the survey methodology and demographics

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com