Survey Report: Behind the Growing Confidence in Cloud Security

September 2017
More and more businesses trust the cloud. Here’s why.

The more you know, the more you trust the cloud with your most important data.

So said a recent global survey of more than 500 IT decision-makers conducted on behalf of Google Cloud in association with MIT SMR Custom Studio. Those respondents who had the most direct experience with cloud technology were more confident in its security.

It’s no surprise that more companies are looking to cloud computing as a critical component of their IT strategies. But in addition to traditional drivers of cloud adoption, such as speed and agility, security is playing an increasing role in the decision to move to the cloud. And IT leaders with direct cloud experience are leading the charge.

Pockets of doubt remain, of course. And the security of your IT stack will always depend on the partners and implementation models you choose. Here at Google Cloud, we’ve invested deeply in security, all the way from purpose-built hardware to almost every facet of our day-to-day operations. It’s gratifying to see IT leaders recognizing that, in many cases, moving to the cloud can actually enhance security.

Read on to learn more about the top workloads companies are migrating to the cloud, as well as the measures they’re taking to manage security across cloud platforms. And when you’re ready to talk to a cloud partner, contact us at https://cloud.google.com/contact.
Executive summary

• “Increased confidence in cloud security,” along with “increased need for agility and speed,” are the prime drivers for the projected growth in cloud adoption, as are the need for increased business and technical flexibility, as well as improved integration with new tools and platforms.

• Data analytics, data storage and collaboration are the top workloads currently implemented in the cloud or expected to be deployed within the next two years.

• Machine learning and artificial intelligence are the fastest growing workloads, with cloud deployment expected to nearly double by 2019.

• The use of cloud has increased from 24 percent of workloads to 44 percent over the past two years, and it’s expected to rise to 65 percent of workloads in the next two years.

Three of four respondents have become more confident in cloud security

Respondents were asked: Over the last two years, how has your overall confidence in the security of cloud applications and infrastructure changed?

- Increased confidence: 74%
- Stayed about the same: 25%
- Decreased confidence: 1%

Steady growth in use of cloud

Respondents were asked: Please estimate what portion of your applications, data and/or infrastructure...

...were cloud-based two years ago...are cloud-based today...will be cloud-based two years from now

- 24%...+ 20%...44%...+ 21%...65%

N=509
Base: Survey of 509 IT and business executives at midsize and large enterprise organizations worldwide
Source: MIT SMR Custom Studio/Google, June 2017 Cloud Security Survey
Methodology

- Specifically focusing on how companies are adopting and managing cloud security, the 25-question (excluding demographics) online survey was distributed via email invitation and conducted between June 8 and June 22, 2017.

- We received 509 completed survey responses. Thirty-eight percent were from North America (U.S. and Canada); 18 percent from Latin America (Mexico, Brazil); 24 percent from Europe — U.K., France, Germany — the Middle East and Africa (EMEA); and 20 percent from Japan and Asia-Pacific (Australia/New Zealand, India, Japan — JAPAC).

- The survey targeted CIOs and senior business executives (including directors, vice presidents, general managers and C-level executives) who influence or are involved in their company’s IT decisions and initiatives. For enterprise organizations in North America, Latin America, EMEA and JAPAC, 72 percent of survey respondents were in IT and 28 percent represented their firm’s lines of business.

- Only survey respondents with significant awareness of cloud technologies were qualified to complete the survey.

- The survey targeted companies with 1,000+ employees in the U.S. and 500+ employees in other regions. Among survey respondents, 40 percent represented companies with 5,000+ employees, 45 percent represented companies with 1,000–4,999 employees and 15 percent represented companies with fewer than 1,000 employees.

Respondent profile

- Number of employees
  - 5,000+ employees: 40%
  - 1,000–4,999 employees: 45%
  - 500–999 employees: 15%

- Job title
  - C-level: 29%
  - VP/GM: 29%
  - Director: 42%

- Functional area
  - IT: 72%
  - Line of business: 28%

N=509
Base: Survey of 509 IT and business executives at midsize and large enterprise organizations worldwide
Source: MIT SMR Custom Studio/Google, June 2017 Cloud Security Survey
The age of unthinking fears about cloud security is over. Not only is cloud adoption rising steadily across geographies, industries and job functions, but confidence in cloud security is rising as well — to the point where increased security is a major reason enterprises opt for cloud solutions.

Introduction

According to a recent survey of more than 500 global respondents conducted on behalf of Google Cloud in association with MIT SMR Custom Studio, use of the cloud has increased from 24 percent of workloads to 44 percent over the past two years, and is expected to rise to 65 percent of workloads by 2019.

Gone are the days when organizations accessed applications and infrastructure over the internet only because it was the least expensive way to scale compute, storage and networking resources as business needs changed. The cloud today is a strategic necessity, with increased agility, integration and speed (as well as security) being the prime drivers of its increased adoption (see Figure 1, “Agility, security and speed top cloud benefits,” on page 6).

This more strategic approach extends to how organizations manage the cloud. The survey results show that these companies are taking a thorough,
systematic approach to assessing the security of applications, infrastructure and platforms accessed over the internet. Also shown by the results is that firsthand experience often separates cloud believers from skeptics.

As another indicator of the growing maturity in cloud management, there is substantial agreement across industries, regions and roles about the capabilities necessary to achieve the required levels of cloud security.

But whether out of uncertainty about how their applications will fare in the cloud or how regulators will treat cloud-based data, not everyone is convinced: Among those still hesitant to adopt the cloud, security remains the primary concern.

This report examines the growing confidence companies have in cloud security, how they are basing their hosting decisions on the flexibility and integration offered by the cloud, and their plans to use the cloud for future workloads such as artificial intelligence (AI) and machine learning (ML). It also drills deeper into these organizations' perceptions of the security capabilities they need from vendors, as well as why the skeptics remain unconvinced.

**Strategic Adoption**

In this digital age, businesses must quickly deploy new applications and services, share data with new devices and business partners, and adopt new technology. When asked why they currently deploy, or plan to deploy, specific workloads to the cloud, survey respondents consistently cited “increased flexibility in business processes and vendor choices” and the “ability to integrate with new tools and platforms” as the top two reasons for deploying most workloads.

“The cloud has the state-of-the-art development tools and enables things like DevOps and container technology” that developers want to use to design and deploy applications more rapidly, says Jim Reavis, co-founder and chief executive officer of the Cloud Security Alliance, a non-profit organization that promotes best practices in cloud security. The cloud also enables organizations to ramp their resources without having to order and install servers and to “quickly test an application or pilot a new business process and then iterate it,” he says. Indeed, 31 percent of cloud survey respondents cited the “ability to integrate with new tools/platforms” as a main reason for choosing to deploy workloads to the cloud.
Late adopters just moving to the cloud first deploy methodologies such as agile development, continuous integration and continuous delivery of applications in-house “as part of their plan to get ready for the cloud,” says Doug Cahill, a senior analyst at consultancy Enterprise Strategy Group. He says the approach these laggards often take is to begin continuous integration and delivery on-premises so that they understand how to expand their use as they move to the cloud.

When asked why their use of the cloud has increased over the past two years, respondents cited the top three drivers as “increased need for agility/speed to market” (45 percent), “increased confidence in cloud security” (44 percent) and “cost savings” (34 percent).

It doesn’t provide much to boost an organization’s flexibility and business processes “if you’re using the cloud just to displace hardware down in your basement,” says Stuart Madnick, professor of information technology at the MIT Sloan School of Management. He asserts that more significant benefits come from combining a move to the cloud with a more modular, web services architecture that makes it easier to share important data both within the organization and with business partners.

Among respondents, data storage was the workload most commonly implemented or planned to be implemented in the cloud, followed by collaboration/productivity, application development and the Internet of Things (IoT). Respondents also indicated that almost 90 percent of each of those workloads would be deployed in the cloud by 2019. The IoT was a popular use case for cloud (56 percent currently deployed to the cloud and 90 percent deployed by 2019) – a somewhat surprising finding, given that much of the growth in such internet-connected devices is still expected to come (see Figure 2, “Data storage the top cloud workload; ML/AI projects the most growth,” above).

According to Roy Illsley, a principal analyst with analyst firm Ovum, much of the IoT data currently hosted in the cloud comes from long-established platforms such as industrial control systems. But as companies deploy more data from newer IoT devices to the cloud,
he predicts providers will create new services that store such data on the physical “edge” of the network so it can be analyzed quickly enough for devices to respond to changing conditions in real time. This “edge” data could sit anywhere from small storage devices on telephone poles to shared data centers in industrial areas serving multiple customers, he says. This will enable, for example, data about the performance of a manufacturing robot, pressures in an oil well or traffic on local roads to be analyzed quickly to anticipate and prevent problems.

Customer and employee records (at 59 percent), along with data from the IoT (also 59 percent), were the three data types most likely to be hosted in the cloud today, followed closely by corporate financial data, product development material and corporate human resources (HR) records.

In another sign of growing confidence in cloud security, even organizations with highly regulated data cited “increased security” as an incentive to move to the cloud. Top candidates for increased cloud deployment in the next two years were data governed by medical and financial privacy regulations and corporate financial data (see Figure 3, “IoT will be the most deployed data type to the cloud in two years,” above).

According to Rik Turner, principal analyst, infrastructure solutions at Ovum, even the security-conscious financial services industry “seems to have been won over, by and large.” Ovum recently surveyed 75 top-tier banks around the world, Turner notes. “We...were surprised by the number that said they were migrating workloads to the public cloud on an almost wholesale basis.”

Assessing Cloud Security

What’s behind the rising confidence in cloud security? Firsthand experience, and careful, systematic assessments that tap multiple sources such as detailed audits and comparisons. The most frequent driver of increased confidence was “direct experience of the quality of security in the cloud versus on-premises,” cited by 67 percent of our respondents, followed by the 51 percent who relied on a “detailed audit/examination of on-premises vs. cloud security.”
As the most influential factors in their assessment of cloud security, respondents cited, in order:

- Assessments by their own security team.
- Support for security and compliance standards.
- Security tools provided by the cloud vendor.
- Recommendations from analysts and consultants.

Unsurprisingly, the most frequently mentioned security requirement was data protection (at 71 percent), followed by protecting apps and websites from compromise or downtime, reports on security incidents and how the cloud provider responded to them, and auditability and safeguards against cloud staff accessing customer data (see Figure 4, “Protecting data is the top cloud security requirements,” above).

According to Cloud Security Alliance’s Reavis, cloud providers can still do more to meet users’ needs in terms of reporting, particularly with what they include in log files. Standards for what information can be shared in incident reports may require changes to service provider contracts that currently prohibit a provider from telling one customer another customer’s information was compromised.

However, although “auditability and reporting are very important, those are almost table stakes,” says Michael Fuller, associate principal at consultancy The Hackett Group. “What we hear most often, aside from flexibility and cost, is availability,” such as application uptime or meeting specific objectives for recovery after an outage. This is especially true, Fuller says, for small to midsize businesses with sales of $500 million to $3–$4 billion. Indeed, 59 percent of survey respondents cited “protect applications or websites from compromise/downtime” as one of their top cloud security requirements.

When asked what capabilities they need from a cloud provider to be confident in the provider’s infrastructure security, respondents cited the full range of offerings — essentially, they want it all.

“We are hearing that cybersecurity professionals prioritize encryption of both data at rest and data in motion as the most effective technologies for protecting data in the cloud,” says Holger Schulze, founder of the
350,000-member Information Security Community on LinkedIn. In our survey, nearly 80 of respondents said it was somewhat or very important for their organizations to manage the strength of their encryption or to manage the encryption process itself. However, whether the company or its cloud provider controls the encryption keys is often “a really big bone of contention,” Fuller says.

The ability for a customer to utilize a cloud provider’s encryption but manage their own keys “is kind of the holy grail” of encryption, Reavis says. “But it’s not always realistic, in every instance, depending on how applications are architected.” He also said it’s more difficult with applications that require managing access (and encryption keys) for many users.

**Pockets of Skepticism**

For all the widespread adoption of, and confidence in, cloud computing, a minority of respondents still considered security concerns a barrier to adoption (see Figure 5, “Among skeptics, security concerns still a barrier to cloud deployment,” right). Security was the top reason respondents cited for not moving data storage, customer- or partner-facing websites and IoT data to the cloud. And only 59 percent of business decision-makers said their confidence in the cloud had increased in the last two years, compared to 81 percent of IT respondents.

Overall, IT respondents had more confidence in cloud security than their business counterparts, with those at the director level in their businesses being the most skeptical. Larger companies also tended to have greater cloud security concerns than smaller firms (see Figure 6, “Senior executives in large companies most skeptical of the cloud,” on page 11).

One factor that can increase security concerns, says Enterprise Strategy Group’s Cahill, is the “lack of visibility” into cloud security controls for companies accustomed to running their own infrastructure in-house. The inability to simply “plug in the security controls they’re used to, like a next-generation firewall at the perimeter,” can be disconcerting, he says.

One major reason for corporate security fears, says The Hackett Group’s Fuller, is “a lack of confidence in their own architectural capabilities.” Without a deep understanding of their architectures, many companies are now unsure how to secure them in the cloud.
Future Cloud Usage

As the universe of data expands and organizations seek to mine it for insights, the scalability and flexibility of the cloud will become increasingly important.

The survey results suggest that machine learning and artificial intelligence will be the fastest growing workloads for cloud adoption. Thirty-five percent of respondents said they either currently implement or plan to implement ML/AI in the cloud in the next two years. By 2019, 87 percent of that implementation will be deployed to the cloud. Business continuity/disaster recovery and IoT workloads will also see strong growth in cloud deployment over the same time period.

Respondents indicated that those who seek to deploy ML/AI in the cloud are especially drawn to the speed, flexibility and integrative capabilities it offers (see Figure 7, “ML/AI is ideally suited for the cloud,” on page 12).

“The on-demand compute and storage available in the cloud are very useful for data-intensive compute tasks like machine learning and artificial intelligence,” Cahill says. The scalability of cloud data storage is also an asset, because the more data available for machine learning, the better the result. Cloud-based machine learning and analytics can be used not only for research and business analytics but also to improve IT security by finding signs of potential attacks among otherwise normal data, he says. Additionally, the Cloud Security Alliance’s Jim Reavis says such automated security could help cloud users secure the growing quantities of data needed for ML and AI.

Among survey respondents, those at the director level and those in companies with 5,000+ employees were most likely to indicate concerns about cloud security.

Mid-level executives and those in large companies are most skeptical of cloud

Source: MIT SMR Custom Studio/Google, June 2017 Cloud Security Survey

N=285, N=184
Base: Survey of 509 IT and business executives at midsize and large enterprise organizations worldwide
Cloud providers may also help companies move to the cloud with libraries of easy-to-use analytic algorithms, as well as application programming interfaces (APIs) to ease the exchange of data among cloud providers, Reavis says. Many of them provide big data platforms and capabilities, which save companies the cost of both the equipment and the staff to perform such analysis themselves, says MIT Sloan’s Stuart Madnick.

**Conclusion**

Based on our survey results, the mega-trends that make the cloud so essential — the need for agility, flexibility and security for ever-rising amounts of data — continue to accelerate. Across industries, geographies and lines of business, the cloud is increasingly the preferred choice for companies seeking to move fast, stay flexible and keep their customers’ data secure. Furthermore, transformational technologies will only accelerate this growth. Machine learning is a natural fit for the flexibility, scalability and integration capabilities provided by the cloud because it requires so much data and computing power. So is the IoT, if cloud providers can build the decentralized networks of data centers required to quickly analyze data and deliver the results to decentralized devices.

Although there are still some gaps in cloud confidence and usage, these survey results indicate they are more significantly due to a lack of education and awareness than to actual gaps in cloud security, especially among respondents who are business users.

For today’s cloud user, security and even cost are yesterday’s conversations. The far more compelling vision is of an enterprise empowered by the cloud to continuously deliver ever more efficient, agile and innovative applications and services.