White Paper

Questions to Ask Your Cloud Service Provider

Know how your data will be protected in the cloud

intel Security

Table of Contents

Vetting Potential CSPs at a High Level . . . 3

Security Questions . . . 4

- Who has access to my data, both physically and virtually? . . . 4
- Does the CSP outsource data storage? . . . 4
- How does the provider handle legal requests for data review? . . . 4
- How and when is data deleted? . . . 4
- What is the data architecture? . . . 4
- What certifications and/or third-party audits are performed? . . . 4

Privacy Questions . . . 5

- What data is collected from our organization and how is it kept private? . . . 5
- What is the data used for? . . . 5
- How long does the CSP retain that data? . . . 5
- Does the CSP encrypt your data and in what manner? . . . 5
- Where is data stored? . . . 5
- Is data rolled up and transmitted to other internal or external entities? . . . 5

Operational Questions . . . 5

- What is the database and storage architecture redundancy model? . . . 5
- What is the backup frequency? . . . 5
- What is the recovery time from failure? . . . 6
- How can we access or download data from the service? . . . 6
- Which analytical tools are available to view our data? . . . 6
- If there is data corruption, what is the maximum data loss that we can expect? . . . 6

Summary . . . 6

About the Author . . . 7

Engaging a cloud service provider (CSP) for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) is now common practice for enterprise IT. It is essential to make the right choice of providers and services, particularly as it relates to security practices, data privacy, and operational capabilities. Be sure to put potential Cloud Service Provider (CSP) partners under the microscope by asking them the right questions about how they will secure your most essential information.

As demand for cloud services continues to explode, finding the right CSP (or multiple providers) is a major responsibility for enterprise IT and security professionals. CSPs come in all shapes and sizes—from massive global organizations delivering a wide range of cloud services to small shops specializing in a limited number of capabilities. There are even cloud services brokerages that aggregate cloud services from a number of different suppliers across different service delivery models—from systems integrators and outsourcing companies to independent software vendors and value-added resellers.

This makes it difficult, but mandatory, for organizations to sort out the options in this labyrinth of CSP options. To normalize the many differences among potential providers, you need to ask them consistent questions about key issues. Security should be at or near the very top of your list as you go about selecting the right CSP partners in your journey to the cloud.

The essential aspects of security should be zeroed in on with a series of questions when narrowing down your choices. These questions will help you determine which CSPs really understand all security-related issues and implications, and which ones have an approach that is most consistent with your organization's priorities, practices, and risk tolerance. We'll devote much of the paper to specific questions in three areas—security, privacy, and operations—all in relation to data protection. If you follow these suggestions and filter it through the lens of your own experience, good judgment, and advice of colleagues who already have been through this process, you'll increase the odds of finding one or more CSPs that will help ensure robust security for your most important data assets.

Vetting Potential CSPs at a High Level

An essential first step is to avoid making assumptions on what security is and isn't with respect to a provider. Every provider is different, with different rules, service-level agreements (SLAs), and terms and conditions. Make sure you thoroughly understand what each service provider commits to you, the customer.

Second, be sure to ask questions about how data security and privacy are handled. You need to know what they expect your organization to do, what they do as a provider, and how they do it—among other things.

Third, look closely at their terms and conditions. Of course, no one likes to read through many pages of fine print in the contract, but you need to understand those details so you can choose a provider that delivers the right service and provides you with the right trust level. So, don't shirk your duties in this area—don't simply click "accept" and move on. Dig in and look deeply at different sections within the terms and conditions, and hone in on the data aspects of those details.

Fourth and finally, don't assume that each cloud service has the same guidelines and service delivery targets even within the same provider. Look at terms and conditions for each service. Review them all, and do not make unsupported assumptions, or you may end up with a huge, costly surprise.

Security Questions

The good news is that cloud security concerns have diminished greatly in recent years as CSPs develop a track record for successful security practices. Still, many senior business executives, as well as many boards of directors, are concerned about whether organizational data is truly secure in the cloud. You should ask specific questions of potential CSPs in order to achieve the high level of confidence and trust necessary to minimize concerns and risks.

Who has access to my data, both physically and virtually?
Physical access is totally different than virtual access. It's important to ask about both types of access questions.

- What security posture does the organization have in place when their data center is accessed?
- Do their personnel have security clearance, and are they protecting the physical access of data from outsiders?
- What are the institution's or the data center's policies, and how are they protected?
- Who has access to the data virtually? Where is accessed from and why?
- How are they accessing it? Do they use VPN, and is the data encrypted? If it is encrypted, how are the encryption keys secured?

Does the CSP outsource data storage?
Many companies leverage outsourcing companies to provide services, but it's possible that your CSP is outsourcing your data to another location or even to another vendor. If so, you need to decide if you're comfortable with that arrangement.

How does the provider handle legal requests for data review?
Whether those requests come from their customers or from governmental bodies stemming from legal or regulatory issues, handling these requests requires finesse, experience, and sensitivity to corporate governance policies, as well as compliance mandates. It's not unheard of for the quality of your data to be impacted by legal requests, and you need to understand the traceability of the data and how requests are handled.

How and when is data deleted?
Because every provider is different, it's important to understand that there are storage complications given how much data is traversing the world nowadays. You will want to understand how much data is stored by your CSP and, in particular, how much of your specific data is stored. In addition, ask how long your data will be stored, when is it deleted, and how data deletion decisions are made.

What is the data architecture?
Specifically, ask how your data is isolated from that of other customers in a multi-tenant environment. Ask your provider to explain how your data is segmented from other customers' data and how that may change in the future.

What certifications and/or third-party audits are performed?
Certifications will provide you with a better understanding of how mature the provider is, what things they are concerned about, and whether they are are committed to continuous improvement. From a third-party audit perspective, you'll want to know how frequently the provider is looking at changes and making sure that they are meeting the expectations of their customers and vendors.

Privacy Questions

Security and privacy are tightly intertwined, but there are a number of questions unique to privacy that you should ask your CSP. And privacy questions, while obviously rooted in compliance, aren't limited only to regulatory issues.

What data is collected from our organization and how is it kept private?

Privacy is a little bit different for each organization, so it's especially important to define what privacy means for your key stakeholders within your organization.

What is the data used for?

It's often amazing to learn about the different uses for your data—some of which will surprise or perhaps even concern you. Be sure your CSP understands your governance policies on acceptable use of data.

How long does the CSP retain that data?

The terms and conditions may state that data is collected for 30 days or perhaps 90 days or even a year. But that does not necessarily dictate how long the organization may keep your data. This will be very different for every provider, for every service, and for every piece of data that's collected. You could have data that is anonymized, stored, and utilized for testing for many, many years, so make sure to ask about retention.

Does the CSP encrypt your data and in what manner?

This is important to know, to ensure that anything that you deem classified or private or that you're otherwise concerned about, will not be leveraged for other uses by the CSP.

Where is data stored?

Do you have any geographical data storage rules or regulations that CSPs need to follow? Cloud service providers are storing data in a lot of different locations for a lot of different purposes, and you need to understand that and how it aligns with your business practices.

Is data rolled up and transmitted to other internal or external entities?

We all know that this is pervasive across the Internet and that there are lots of different opt-in/opt-out programs. It's really important to understand if the CSP shares data with anyone, how they share it, when they share it, why they share it, and where is it transmitted.

Operational Questions

Beyond security and privacy, your CSPs' activities will intersect with many of your organization's day-to-day operations. Understanding this will help you determine if the ways in which the CSPs handle your data and serve it to your constituents supports or impacts your operations.

What is the database and storage architecture redundancy model?

Redundancy, in particular, is important because it focuses on how to deal with infrastructure failure without impacting business continuity.

What is the backup frequency?

We've all heard this mantra since computers were introduced: back up, back up, back up. And it is extremely important to understand the frequency with which CSPs do backups. Obviously, the more frequent the backup, the better your redundancy will be. It will make it easier for your provider to restore service to a specific point and time if there is any failure.

What is the recovery time from failure?
It is inevitable that your provider will have an issue at some point in time. It is imperative that you understand how long it will take your CSP to recover your data. Is it minutes, hours, days, or weeks? Failures will happen, but you need to know how quickly it will take to recover from that failure when you're leveraging a service provider.

How can we access or download data from the service?
Asking this question helps you to understand the different philosophies of service providers and get better insight into how those steps align or conflict with your operational processes.

Which analytical tools are available to view our data?
The service provider may have a wealth of your data in their service, and you might not want to have to pull all that data out and leverage third-party analytics tools to compress it and make sense of it. It's much more beneficial if the service provider provides you that service so that you can do aggregation and modeling of the data.

If there is data corruption, what is the maximum data loss that we can expect?
This should tie into the redundancy and recovery questions, noted earlier, and they should be closely aligned. How long will it take to recover from a data failure, and how will that recovery process actually affect the data quality?

Summary

These suggested questions should help in your process of identifying, evaluating, selecting, and working with CSPs. These questions also act as important reality checks on your ongoing assessment on your current CSP's performance, and they serve as a periodic level set for new services you may need as your business evolves.

Remember that selecting a CSP isn't a trivial task. Making the wrong selection can have a big, even potentially catastrophic, effect on your organization if the CSP's security readiness doesn't match your needs—now and in the future. At the same time, selecting the right CSPs can help your organization in so many ways—in an economic sense, with in-house resource allocation, with respect to confidence in the security and integrity of your data, and so much more.

As you go about the process of evaluating potential CSPs, these security, privacy, and operational questions can improve your confidence in the ultimate selection of CSP partners. Of course, these questions should be weighted and adjusted to reflect your organization's business model, operational priorities, and corporate culture. But using these questions will be an effective and efficient way to make smarter partnering decisions as you ramp up your use of cloud services.

This may seem like a lot of questions, but trust us—in the long run, you'll be glad you spent the time to go through it all. It's a lot better to have the information these questions can yield than it is to have to guess at the answers.

For more information, please go to **www.intelsecurity.com/cloudsecurity**.

About the Author

Jamie Tischart

CTO Cloud/SaaS, Intel Security

Jamie Tischart is the CTO for Cloud/SaaS at Intel Security and is responsible for leading the creation of Intel Security's future-generation cloud solutions and creating sustainable competitive advantage. He has been with Intel Security for more than 10 years in a wide variety of technical roles, including Senior Director of Cloud Engineering, Operations and Research and Senior Director at McAfee® Labs, Quality Engineering and Operations. Prior to joining what was then McAfee, Tischart held several executive, QA architect, management, and engineering positions at such companies as MX Logic, Blackbaud, Openwave, Newbridge Networks, and Corel. Tischart holds an MBA from Aspen University. He lives with his family in Colorado where he pursues his passions for SaaS development, DevOps, and cloud operations, along with Agile Coaching and Quality Engineering Leadership, while enjoying skiing, writing, and hockey. He is an active volunteer for many organizations, including Habitat for Humanity, Ronald McDonald House Charities of Denver, Inc., and Food Bank of the Rockies.

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. **www.intelsecurity.com**. Intel Security is a division of Intel.

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