Cloud service providers are a ubiquitous part of IT today. Security and risk management leaders need to understand if a CSP is secure, and if the CSP can protect itself against ransomware, nation states and other evolving attacks.

Quick Answer

How well can cloud service providers (CSPs) protect themselves from evolving threats and attackers?

- Not all CSPs are equal, and neither is their ability to reliably defend themselves (and, by extension, your data and applications). They must be treated in tiers related to their maturity.

- Third-party attestation and validation are some of the most available windows into the efficacy of the CSP’s program, but are not an infallible guide. The shared responsibility model that exists while using a CSP means that organizations must configure SaaS, IaaS and PaaS securely regardless of the security of the CSP’s underlying infrastructure.

- Few CSPs are willing to disclose details of their internal controls and processes. The default configuration provided by CSPs is usually not the most secure configuration, but instead is the easiest for their customer to use.
Workloads Are Moving to the SaaS and IaaS at an Increasing Rate

Gartner's 2020 Public Cloud Initiative Survey found that 70% of workloads will be hosted in public clouds (combining PaaS, IaaS and SaaS) by 2023.\(^1\) Given the disparity of workloads, the range of SaaS applications, and business drivers like improving availability, need for best-of-breed capabilities, and compliance requirements, many organizations will have their workloads hosted by multiple CSPs. Organizations must be able to trust that their chosen CSPs can protect themselves from a range of attacks and attackers.

Not All CSPs Are Created Equal

Common concerns include determining if a CSP can protect against advanced attacks, if the CSP is secure against ransomware, and what security controls are present and how these are provided. Gathering accurate data is a challenge; CSPs are rarely transparent about their security. This means that in order to make a decision on CSP security, it is first essential to note that not all CSPs are equal.

![Figure 1. Tiers of a CSP](image)

Effective and pragmatic evaluation of how protected a given CSP is requires the use of a tiered model:
Tier 1 CSPs:

- Most public cloud activity is within a small number of well-established, financially secure CSPs (prominent examples include Amazon Web Services [AWS], Google, Microsoft, Salesforce and ServiceNow). All Tier 1 CSPs have undergone multiple third-party security evaluations. These giant CSPs are constantly seeking ways to encourage higher levels of customer trust. In the very rare instances of any vulnerability in their infrastructure being reported, the documented response has been extremely fast. 23

- While Tier 1 CSPs are an enormous target, they are able to operate at scale, have an effective and tested process, and can attract and retain the best security talent. In addition, these CSPs often have few budget limitations when it comes to the technology they choose to deploy; to date, they have proven they are incredibly secure platforms to operate on.

- No one is 100% protected against a targeted and sustained attack from a sufficiently sophisticated and determined (“nation state”) adversary. Given their budgets, staffing and efforts, it can be assumed that a Tier 1 CSP has the best chance of protecting against, detecting and responding appropriately to such advanced attackers. It will be better than almost any other organization at resisting this level of threat.

Tier 2 CSPs:

- A growing number of midsize providers and some large, name brand software providers that lack a significant cloud-first track record represent the middle tier of vendor sophistication and reliability.

- Some Tier 2 providers are relatively immature in their security and operations, and they often lack third-party evaluations (though there will be exceptions, especially with the larger security-as-a-service providers that will fall into this tier). Even where these evaluations do exist, there is evidence of breaches in these providers impacting their clients. 4

- Tier 2 CSPs will be required and used, but should be evaluated to ensure they are suitable and the exposure aligns with your corporate risk tolerance.

- Tier 2 CSPs will vary in their ability to respond to an advanced attacker, and it should not be assumed that all of them can.
Security Is Not Just the Job of the Provider

It is also vital to know that there are two aspects to the security of a CSP (and particularly for a SaaS provider). There is the security that the provider has for the underlying infrastructure, and there are the security controls that the CSPs enable their customers to use to protect their data and assets (see Figure 2).
Both are important, with the second being arguably more so given that Gartner has a Strategic Planning Assumption that anticipates over 99% of “cloud breaches” will be based on a customer error or misconfiguration until 2025. To date, there have been no major breaches associated with a Tier 1 CSP’s native controls, and the number of breaches in Tier 2 CSPs are dwarfed by those created by customer misconfigurations. In addition, the connectivity between CSPs via APIs is often overlooked, where a Tier 1 CSP can be easily connected to a Tier 3 CSP if not managed correctly.

Cloud Provider Controls Are Usually in the Standard Offerings

CSP-managed controls will be on the underlying infrastructure. For SaaS applications, the level of control available to the end-user organization (the client) and configuration may be limited by the options purchased. Identity will be the strongest control, and must be well-managed and enforced by the end-user organization — and should be federated with the corporate standard. Individual controls that must be configured by the client may be add-on purchases.
Evidence

1 Gartner Public Cloud Initiative Study 2020

The Gartner Public Cloud Initiatives Study 2020 was conducted online from 16 September to 3 November 2020 with 400 infrastructure and operations leaders with public cloud migration strategies from the U.S. (n = 208) and the U.K. (n = 192) to explore public cloud migration strategies, challenges and benefits, including total cost of ownership.

Respondents’ organizations had an annual revenue of at least $500 million or more than 1,000 employees for public sector organizations — with more than half with annual revenue of more than $5 billion.

All respondents are at organizations currently engaged in public cloud migration activities and are at a level of involvement to accurately depict budgeting and strategies.

Disclaimer: Results are representative of the respondent base of this survey — and not necessarily projectable to the market as a whole.

2 ChaosDB: How We Hacked Thousands of Azure Customers’ Databases, Wiz.


4 Cybersecurity Incident Update, Cloudstar.