Deloitte.

Which cloud services are right for your security and compliance needs?

Contributors: Anil Ramcharan, Mason Evans, and Dean Lee

MAKING AN IMPACT THAT MATTERS since 1845

Cloud services have seen a rapid growth in capability over the past decade. Cloud security features may have once lagged other functionality in release priority, but Cloud service providers (CSPs) now offer a myriad of choices and dizzying flexibility to meet security and compliance needs ranging from building your own solutions on virtual machines or utilizing cloud-native tools. Even within a single CSP, there are often several options for a single security capability, so it can be difficult to digest these options, as well as to understand what functionality is gained or lost from those options. So how do you navigate the CSP service offerings before you? Here are considerations that can help:

1. Architecture

To determine what security services to use, you should start with defining what they will be protecting. How many systems and applications, where they will reside, and how they will be accessed should all be captured to better refine what security measures should be in place. Take the time to clearly define your architecture, including data flow, micro-service dependencies and security control boundaries.

2. Multi/Hybrid Cloud

Are you using (or plan to eventually use) a multi or hybrid cloud environment? It is important to document and understand what security functions are going to occur in which environment. Is each environment going to have a full set of security tools or are certain aspects of security going to be centralized into one environment? Centralizing some tools may be beneficial, such as deploying an identity solution in one environment that all the environments will utilize but may result in higher data transfer and connection costs.

3. Compliance

Your cloud environment will likely have a minimum set of security requirements driven by regulation or organizational governance that must be adhered to, depending on the sensitivity and classification of the data in your environment. In some cases, these requirements are clear cut and mandatory – a directive to use a specific security tool, for instance. However, many requirements will require a risk-based approach for identifying an appropriate solution, such as logging, which creates flexibility in determining the appropriate services to use. For U.S. Government organizations, compliance standards and guidance (e.g., MARS-E, FTI, PCI-DSS, FISMA, FedRAMP, DoD CC SRG) can vary depending on the cybersecurity governance authority body. Defining security and compliance requirements early on will help you better determine what security tools make sense for your situation.

4. Certification/Authorization Approval

For many organizations, cloud service offerings must be approved for use according to a specific standard. Approval represents a significant level of scrutiny beyond that of typical governance, risk, and compliance, and often requires third-party assessors. Some well-known examples include FedRAMP for Federal Agencies and PCI-DSS for environments that process credit card data. CSPs publish matrices describing each service's compliance status against the assessed standard., as not all services are authorized for every standard. Validate with the cloud provider(s) that the security services you want to use are authorized for your use cases during the design phase of your application and/or service.

5. Capability

What capability does the cloud service offering provide, and how does it provide it? The how is just as important as the "what" for cloud security. For instance, a cloud security offering might provide an automated patching capability, but also might require you to install agents on your virtual machines. This can raise a separate set of questions such as if the agent is approved for use and if the agent is communicating to the service in a secure manner (e.g., encryption in transit). Study the service offerings you intend to use and understand the trade-offs in the implementation of those services in your architecture.

6. Cloud Native

The term "cloud native" may have different definitions depending on your perspective. Broadly defined, cloud native services are built to take advantage the scalability, flexibility, and resiliency of the cloud. Cloud native is often associated with the Platform-as-a-Service (PaaS) offerings provided by the CSPs. Your security requirements may dictate the use of a specific security software and therefore may not allow you to leverage a CSP's offering. In these cases, though, take advantage of cloud native technologies such as serverless, containerization, or API hooks to integrate that software with the rest of your security environment.

7. Risk Tolerance

At times, you may encounter situations when, all things are considered, there are several security services you could use. The tiebreaker in these cases may come down to your risk tolerance for a specific service. For instance, does a CSPs key management tool fit within your risk profile? As part of that risk decision, you should consider whether your organization can handle learning and managing the cloud-native security tools as well as its ability to automate the use of the tools to reduce management overhead.

8. Scalability

Cloud environments tend to grow over time – the security services you select should scale with that growth. Inability of security services to match the elasticity of your environment could introduce "blind spots" and other vulnerabilities. Work with your CSP to understand how these services scale in relation to one another, as well as the cost implications for that scaling.

9. Cost

As with all cloud services, it is important to understand the pricing structure for each security service, especially as CSPs often change how a service is priced and charge different rates for different cloud regions. Security design patterns, particularly centralized logging or extended detection and response, for traditional or on-premises workloads may generate unplanned costs that must be considered. Pricing can be a monthly flat-rate, consumption-based, or even based on the amount of data that is fed into the service. Additionally, pricing can be tiered based on requirements and consumption. There can also be hidden costs related to other CSP capabilities that must be used for a service to work properly. For instance, you might want to use a cloud-native firewall for your environment, which includes the cost for that service, but also might have associated data ingress/egress costs.

In determining what consideration factors are important to you and your organization, you should weigh, evaluate, and select the cloud security tools that can help you achieve, maintain, and potentially automate your security baseline. Additionally, collaborate with the CSPs to understand their roles in important use-cases (for example, incident response) as it pertains to the security services you plan to use, as well as to account for the CSPs recommendations on how to deploy services to best suit your needs.

Deloitte.