Cloud security solutions offer a way for businesses to be more secure, efficient, and strategic in their use of cloud computing—regardless of the cloud providers or services they choose.

For would-be buyers, the decision hinges on how well the product ties into your broader cloud strategy and fits the needs of your business.

When looking for a cloud security solution to meet your needs, you should consider the following checklist of questions:

- Does the solution support multiple public clouds, such as AWS, Azure, and GCP?
- Can you manage multiple accounts across multiple cloud providers?
- Can you control who has access to different features and functionalities of the solution?
- Does the solution provide out-of-the-box support for standards like CIS, NIST, PCI etc.? Can you create customizable policies and compliance controls?
- Can the tool detect security vulnerabilities in real-time? Can it also provide real-time alerts and notifications?
- How does the solution handle exceptions?
- How long does the tool store information and data?
- Can the solution identify relationships between cloud objects and services?
- Can you visualize and take action on security violations according to severity? Can this be customized?
- Does the solution have the ability to execute actions automatically without requiring write privileges? Can you set up approval and authorization workflows?
- Can you audit changes and track progress developers are making by resolving security violations across cloud accounts?
- Does the solution support third-party integrations?
- What functionality is available via API? Does the vendor provide API and supporting documentation?
- Is the tool easy-to-use? Does the vendor provide support, documentation, and or dedicated resources?
- How often are new updates or enhancements released? How are these communicated?

It’s also important to clarify that the ideal approach for cloud security posture management does not necessarily entail 100% reliance on one tool over another. In fact, many organizations use third-party platforms alongside their cloud service provider’s native tools as part of a holistic cloud security and compliance practice.

Ultimately, the decision comes down to the number of tools and the amount of manual work your teams will be responsible for in order to manage complex, heterogeneous cloud environments.

CloudHealth Secure State is an intelligent cloud security and compliance monitoring platform that helps organizations reduce risk and protect millions of cloud resources by remediating security violations and scaling best practices at cloud speed. Get in touch with our team to learn more.