Organizations may create, implement, and manage scalable workloads in dynamic environments with the help of cloud native technologies. Applications built for the cloud don't have the rigid borders of traditional IT. Because of this, static firewalls are rarely effective in securing applications that are used by on-premises, off-premises, or multi-cloud cloud instances. (Sengupta, 2021)

One of the most important aspects of resource management in cloud systems is cloud security.

The benefits and drawbacks of several cloud native security tool solutions are outlined below, along with a suggestion:

**Cloud-Native Security Tools**:

The cloud service provider (CSP) such as Amazon Web Services, Microsoft Azure, or Google Cloud Platform owns these unique technologies. They can be simpler to set up and are integrated within the platform. They are, nevertheless, restricted to the platform for which they were designed. (Cloud Identity Security Platform, n.d.) (Cloud Native Security vs. Third-Party Tools: How to Choose (and Why You Might Not Have To), 2024)

**Pros:**

Integration: Closely linked with the platform of the CSP, perhaps providing a more seamless user experience and simpler implementation in the cloud.

Support: Take advantage of the CSP's assistance for their own tools, which may make problem solving and troubleshooting easier.

Familiarity: The interface and workflow of these tools may be recognizable to you if you are already familiar with the CSP platform.

**Cons:**

Vendor lock-in: If you depend too much on the CSP's tools, you may be locked into their platform and find it challenging to move to a new provider down the road.

Limited Functionality: Compared to certain open-source or third-party solutions, CSP tools may not provide the same degree of customization or sophisticated capabilities.

**Third-Party Tools:**

These tools are **not tied to a specific CSP** and can work across different cloud vendors. They provide **flexibility** and allow to manage security consistently across various platforms. (Cloud Native Security vs. Third-Party Tools: How to Choose (and Why You Might Not Have To), 2024)

**Pros:**

Greater Feature Set: Compared to certain CSP technologies, third-party suppliers typically focus on security and offer a greater range of features and functions.

Vendor Agnostic: If you employ a multi-cloud strategy, these technologies offer greater flexibility as they may be utilized on several cloud platforms.

Cons:

Integration: Compared to native tools, integration with the platform of the particular CSP may take more work.

Support: If the third-party vendor's offerings diverge from the CSP's support framework, you will be dependent on them for assistance.

**Open-Source Tools**

**Pros:**Cost-effective: Since open-source technologies don't require license, they are free to use.

Customisation: You can customize open-source solutions to meet your unique requirements because they offer a great degree of customisation. (22 Best Cloud Security Tools Reviewed For 2024, 2024)

Huge Community: A big developer community is frequently present in open-source projects, offering access to resources and the possibility of contributions.

**Cons:**

Support: Using community forums or paid help options may be necessary for troubleshooting and issue resolution.

Maintenance: In-house knowledge is needed to maintain the security and keep open-source tools current.

**Combination Approach**:

Most of the time, a mix of these strategies could be the most advantageous choice.

**Reasons for the combination approach**

Utilize CSP provided tools that made it simple to integrate and support them in a cloud environment, particularly for essential features.

If the CSP's services fall short of your specific security needs, consider using third-party technologies.

For more advanced customisation and cost-effectiveness, investigate open-source technologies; nevertheless, be ready to invest in internal expertise for upkeep and support.

We can create a strong cloud native security posture that takes advantage of each method's advantages and meets business unique security needs by carefully combining these solutions.

Remember that security is a shared responsibility between the cloud provider and the user. Evaluate your specific needs, consider the complexity of your environment, and choose the approach that aligns with your organization’s goals and expertise.

Ultimately, there’s no one-size-fits-all answer. Assess your requirements, explore the available options, and tailor your security strategy accordingly.

# References

*22 Best Cloud Security Tools Reviewed For 2024*. (2024, March 25). Retrieved from thectoclub.com: https://thectoclub.com/tools/best-cloud-security-tools/

*Cloud Identity Security Platform*. (n.d.). Retrieved from sonraisecurity.com: https://sonraisecurity.com/solutions/cloud-security-platform/

*Cloud Native Security vs. Third-Party Tools: How to Choose (and Why You Might Not Have To)*. (2024, March 8). Retrieved from www.puppet.com: https://www.puppet.com/blog/cloud-native-security-vs-third-party

Sengupta, S. (2021, September 1). *Cloud Native Security: A Beginner’s Guide*. Retrieved from www.bmc.com: https://www.bmc.com/blogs/cloud-native-security/