CxO Trust Newsletter - November 2021

Convergence of Cloud Security Solutions

Vinay Patel, CxO Trust Advisory Council & Finastra CISO

Cloud adoption and building cloud native applications is no longer an emerging trend. It is the current reality for most enterprises.

Enterprise security teams are challenged with protection and continuous monitoring of their cloud environments and workloads. These environments and workloads are frequently built using DevOps techniques and programmatically deployed using Infrastructure as Code (IaC).

Several categories of cloud security solutions are employed to secure cloud infrastructure and applications.

- Cloud workload protection platforms (CWPP) - focused on securing VMs, containers, and serverless functions deployed in cloud environments.
- Cloud security posture management (CSPM) - scans cloud environments for improperly configured security settings or ones that violate corporate security policies or regulatory compliance requirements.
- Cloud infrastructure entitlement management (CIEM) - solutions to manage identities and access privileges in cloud and multi-cloud environments.
- Infrastructure-as-Code security - Identify weaknesses within IaC deployment templates/manifests

Several vendors offer solutions in the above categories and frequently have different definitions or implementations for each. The challenge for security teams extends beyond implementing these solutions. A security solution that operates in isolation without being integrated into the overall protection processes and organizational workflows (DevOps, Incident Response, etc) will add friction during adoption and gaps in coverage.

The capabilities offered by CWPP, CSPM, CIEM and IaC security solutions are complementary to each other. Recognizing this, along with the implementation challenges/overhead of multiple solutions, many vendors have bundled together these capabilities into an emerging category that Gartner[1] calls "Cloud-Native Application Protection Platforms" (CNAPP).

For enterprise security practitioners looking to cover security in the enterprise life cycle of a cloud workload/application while minimizing implementation complexity is an appealing prospect. However, we've seen this trend before in other areas of security technology and should proceed with caution. Simply having fewer logos should not be an end goal unto itself.

Consolidation generally is a good thing but also concentrates your dependencies/risks to a single solution provider.

1 https://www.gartner.com/en/documents/4005115/innovation-insight-for-cloud-native-application-protection-platforms

Ultimately, it's a balancing act that needs to consider various factors:

> - How well does it embed into the workflows for DevOps and Security teams?
> - Complexity of implementing a modular multi-vendor cloud security solutions vs. an integrated CNAPP offering.
> - Is an integrated offering sacrificing capability in sub-areas compared to alternatives?
> - How difficult would it be to replace the solution with alternatives in years ahead?

Irrespective of the above, the convergence of cloud security solutions into the category of Cloud-Native Application Protection Platforms is a positive development for the industry as it acknowledges the need for a holistic approach to securing cloud workloads.