MOOR
INSIGHTS & STRATEGY

MANAGING SECURITY AT SCALE

CLOUD NATIVE APPLICATION PROTECTION PLATFORM (CNAPP) CONSIDERATIONS

EXECUTIVE SUMMARY

Organizations of all sizes are embracing digital transformation to gain a competitive advantage. DevOps teams play an important role in this process, given their efforts have an immediate business impact. However, SecOps must ensure that cloud-native application security risks are mitigated in both the development and testing phases prior to applications going into production. Compounding the challenge is that the underlying containerized and microservices architecture of cloud-native applications drives incremental threat exposure, given hundreds to thousands of instances are typically deployed. This is in stark contrast to legacy and monolithic applications of the past that are simpler in design yet are not as agile nor massively scalable.

Where do enterprises turn to ensure the highest levels of security for cloud-native applications? Furthermore, what is at highest risk – continuous enterprise integration and continuous delivery (CI/CD) pipelines, compliance considerations, and other violations that lead to breaches? It is likely all of that and more. Cloud native application protection platforms (CNAPPs) are emerging to address these security challenges. However, not all solutions are equal. This brief will define the features, functions, and overall capabilities of CNAPP, what it aims to address, and specific use cases in which it can have a measurable impact.

DEFINING A COMPLETE CNAPP

CNAPP integrates and automates cloud security, bringing all of the requisite functionality into a single, integrated platform and, most importantly, over the complete lifecycle of a cloud-native application spanning development, testing, deployment, and ongoing management. This is a departure from "best of breed" approaches in years past that fostered fragmentation and management challenges with a proliferation of security point solutions. The latter has become untenable for enterprises, giving rise to the need for managing multiple dashboards and alerts. Given the complex nature of cloud-native applications, this phenomenon creates reactive management postures and subsequent gaps in visibility and corresponding security coverage.

Diving deeper, CNAPP's origin can be traced back to a desire to consolidate the disparate tools that facilitate cloud security monitoring, alerting, posture, and control, as well as the prevention and mitigation of breaches if they occur. Comparatively, cloud workload protection platforms (CWPPs) employ an agent on a physical or virtual computational machine and containers, targeting only workload security. Its shortcoming is that it cannot always be applied at the run time of a cloud-native application within the development cycle.

Moor Insights & Strategy asserts that a complete CNAPP is comprised of four crucial elements.

1. It must secure any microservices architecture, container, and serverless deployment.
2. It should include the previously mentioned CWPP functionality as a foundation and two additional elements -- cloud security posture management (CSPM) and cloud infrastructure entitlement management (CIEM). CSPM identifies and addresses risks when applying automation to observability and resulting threats.
3. CIEM aims to provide real-time analysis of alerts that are generated by applications as well as the underlying hardware.
4. CNAPPs must span the entire lifecycle of a cloud-native application from development, testing, and production. In doing so, a CNAPP ideally identifies vulnerabilities early in the development cycle and continuously monitors run time for vulnerabilities or misconfigurations.

THE VALUE OF CNAPP

The benefits of deploying a CNAPP are immeasurable. Consolidation of cloud security functionality simplifies SecOps management. Furthermore, visibility to blind spots is dramatically improved, leading to fewer security breaches. The result is faster time to deployment of cloud-native applications as well as the mitigation of costly compliance violations and business disruption – all equating to improved enterprise profitability. CNAPP can benefit any organization, but especially those in highly regulated environments, such as the manufacturing, financial services, insurance, healthcare, and pharmaceutical sectors.

CALL TO ACTION

Cloud-native applications provide the needed scalability and functionality for modern business, but ensuring security while allowing DevOps teams to innovate can be challenging. Threat surfaces will continue to grow given the highly distributed nature of new hybrid work models as well as cloud-native application adoption and deployment. Enterprises require a simplified approach to managing the security of cloud-native applications over the entire lifecycle, and CNAPP is poised to address this need. Furthermore, not all CNAPPs are created equal. Thus, it is incumbent to ensure that any platform provides the necessary capability and functionality to blanket what is needed from a cloud security standpoint.

Moor Insights and Strategy believes that Cisco is well positioned to deliver what enterprises require in a CNAPP with Panoptica, a multi-cloud application security solution from Outshift by Cisco. Panoptica offers full lifecycle protection from development to runtime, spanning applications and infrastructure that includes containers, serverless and application programming interface (API) environments. Coupled with Cisco's AppDynamics, enterprises can also observe and address security risks through automated remediation. All of these capabilities have the potential to facilitate efficient developer and security team collaborations, removing friction from the development process.

To learn more, visit the Panoptica Cloud Security Solution website.

CONTRIBUTOR

Will Townsend, Vice President & Principal Analyst, Networking & Security Practices at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Chief Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES

This paper was commissioned by Cisco. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.