SICHERHEIT IN GROßEM MAßSTAB VERWALTEN

ÜBERLEGUNGEN ZUR CLOUD NATIVE APPLICATION PROTECTION PLATFORM (CNAPP)

ZUSAMMENFASSUNG

Unternehmen jeder Größe setzen auf die digitale Transformation, um sich einen Wettbewerbsvorteil zu verschaffen. DevOps-Teams spielen in diesem Prozess eine wichtige Rolle, da ihre Arbeit unmittelbare Auswirkungen auf die Geschäftsentwicklung hat. Allerdings muss das SecOps-Team gewährleisten, dass die Sicherheitsrisiken Cloud-nativer Anwendungen sowohl in der Entwicklungs- als auch in der Testphase minimiert werden, bevor die Anwendungen wirklich bereitgestellt werden. Erschwerend kommt hinzu, dass die zugrunde liegende Container- und Microservices-Architektur von Cloud-nativen Anwendungen zu einer wachsenden Bedrohungslage führt, da in der Regel Hunderte bis Tausende von Instanzen bereitgestellt werden. Dies steht im krassen Gegensatz zu älteren und monolithischen Anwendungen aus der Vergangenheit, die zwar einfacher im Design sind, aber nicht besonders flexibel oder massiv skalierbar sind.

An wen wenden sich Unternehmen, um ein Höchstmaß an Sicherheit bei der Nutzung Cloud-nativer Anwendungen zu gewährleisten? Und worin bestehen die größten Risiken – bei Pipelines für die kontinuierliche Unternehmensintegration und -bereitstellung (Continuous Integration and Continuous Delivery, CI/CD), bei Compliance-Überlegungen oder bei anderen Verstößen, die zu Sicherheitsverletzungen führen? Wahrscheinlich geht es um all das und noch viel mehr. Daher werden zunehmend Cloud Native Application Protection Platforms (CNAPPs) eingesetzt, um diese Sicherheitsprobleme zu meistern. Allerdings sind nicht alle Lösungen gleich. In dieser Lösungsübersicht werden die Merkmale, Funktionen und allgemeinen Leistungsmerkmale von CNAPP definiert, sowie beschrieben, welche Ziele damit erreicht werden sollen und in welchen konkreten Anwendungsfällen CNAPP einen messbaren Nutzen haben kann.

DEFINITION EINER UMFASSENDEN CNAPP-LÖSUNG

CNAPP integriert und automatisiert Cloud-Sicherheit und vereint alle erforderlichen Funktionen in einer einzigen, integrierten Plattform. Dabei kann CNAPP über den gesamten Lebenszyklus einer Cloud-nativen Anwendung hinweg eingesetzt werden – von der Entwicklung über Tests bis hin zur Bereitstellung und dem dauerhaften Management. Dies ist eine Abkehr von den „Best-of-Breed“-Ansätzen der vergangenen

Jahre, die aufgrund der enormen Verbreitung punktueller Sicherheitslösungen Fragmentierungs- und Managementprobleme begünstigten. Für Unternehmen ist diese Situation inzwischen untragbar geworden, denn sie müssen nun eine Vielzahl von Dashboards und Warnungen verwalten. Angesichts der Komplexität Cloud-nativer Anwendungen führt dieses Phänomen zu reaktiven Managementstrukturen und in der Folge zu Defiziten bei der Transparenz und der entsprechenden Sicherheitsabdeckung.

Bei näherer Betrachtung lässt sich der Ursprung von CNAPP auf den Wunsch zurückführen, die verschiedenen Tools zu konsolidieren, welche das Monitoring, den Erhalt von Warnungen sowie den Status und die Steuerung der Cloud-Security sowie die Prävention und Eindämmung von Sicherheitsverletzungen erleichtern, falls diese auftreten. Im Vergleich dazu setzen Plattformen zum Schutz von Cloud-Workloads (Cloud Workload Protection Platforms, CWPPs) einen Agenten auf einer physischen oder virtuellen Computing-Maschine und in Containern ein und stellen ausschließlich die Workload-Sicherheit sicher. Ihr Nachteil jedoch ist, dass sie nicht immer während der Laufzeit einer Cloud-nativen Anwendung innerhalb des Entwicklungszyklus genutzt werden kann.

Moor Insights & Strategy ist der Ansicht, dass eine umfassende CNAPP-Lösung aus vier entscheidenden Elementen bestehen muss:

1. Sie muss alle Microservices-Architekturen, Container und serverlosen Bereitstellungen schützen.
2. Zudem sollte sie die zuvor erwähnte CWPP-Funktionalität als Grundlage und zwei zusätzliche Elemente umfassen: Managementsysteme für den Cloud-Sicherheitsstatus (Cloud Security Posture Management, CSPM) und Berechtigungsmanagement für Cloud-Infrastrukturen (Cloud Infrastructure Entitlement Management, CIEM). CSPM identifiziert und begegnet Risiken bei der Automatisierung von Observability und daraus resultierenden Bedrohungen.
3. CIEM zielt darauf ab, Echtzeitanalysen von Warnungen bereitzustellen, die von Anwendungen und der zugrunde liegenden Hardware generiert werden.
4. CNAPPs müssen den gesamten Lebenszyklus einer Cloud-nativen Anwendung abdecken – von der Entwicklung über Tests bis hin zum aktiven Einsatz in der Produktion. Auf diese Weise identifiziert eine CNAPP idealerweise Schwachstellen in einem frühen Stadium des Entwicklungszyklus und überwacht die Anwendung während der gesamten Laufzeit kontinuierlich hinsichtlich Schwachstellen oder Fehlkonfigurationen.

Der Mehrwert von CNAPP

Die Vorteile der Bereitstellung einer CNAPP sind kaum zu beziffern. Die Konsolidierung der Cloud-Security-Funktionen vereinfacht das SecOps-Management. Darüber hinaus wird durch mehr Transparenz die Erkennung von blinden Flecken drastisch verbessert, was wiederum zu weniger Sicherheitsverletzungen führt. Das Ergebnis ist eine schnellere Bereitstellung Cloud-nativer Anwendungen sowie die Eindämmung kostspieliger Complianceverstöße und Betriebsunterbrechungen – und damit auch eine verbesserte Rentabilität des Unternehmens. CNAPP kann für jedes Unternehmen von Nutzen sein, insbesondere aber für Unternehmen in stark regulierten Branchen wie der Fertigungsindustrie, dem Finanzdienstleistungssektor, dem Versicherungs- und Gesundheitswesen sowie der Pharmaindustrie.

Weitere Schritte

Cloud-native Anwendungen bieten modernen Unternehmen zwar die erforderliche Skalierbarkeit und Funktionalität, jedoch kann sich der Versuch, umfassende Sicherheit sicherzustellen und gleichzeitig die Innovationsfähigkeit der DevOps-Teams aufrechtzuerhalten, als echte Herausforderung erweisen. Angesichts stark dezentralisierter neuer hybrider Arbeitsmodelle sowie der Einführung und Bereitstellung Cloud-nativer Anwendungen werden die Angriffsflächen immer größer. Unternehmen benötigen daher einen vereinfachten Ansatz für das Sicherheitsmanagement von Cloud-nativen Anwendungen über den gesamten Lebenszyklus hinweg, und CNAPP bietet genau diese Möglichkeit. Darüber hinaus sind nicht alle CNAPPs gleich. Aus diesem Grund muss sichergestellt werden, dass jede Plattform die notwendigen Optionen und Funktionen bietet, um die Anforderungen an die Cloud-Security zu erfüllen.

Moor Insights & Strategy hält Cisco für bestens positioniert, um mit Panoptica, einer Multicloud-Anwendungssicherheitslösung von Outshift by Cisco, die Anforderungen von Unternehmen an eine CNAPP zu erfüllen. Panoptica bietet vollständigen Schutz über den gesamten Lebenszyklus hinweg – von der Entwicklung bis zur Laufzeit – und umfasst Anwendungen und Infrastrukturen, die Container, serverlose und API-Umgebungen umfassen. In Verbindung mit AppDynamics von Cisco können Unternehmen so Sicherheitsrisiken beobachten und durch automatische Korrekturmaßnahmen beheben. Durch diese Funktionen profitieren EntwicklerInnen und Sicherheitsteams von einer effizienten und noch einfacheren Zusammenarbeit sowie von einem reibungslosen Entwicklungsprozess.

Weitere Informationen finden Sie auf der Seite Anwendungen neu definieren – mit Lösungen von Cisco.

Mitwirkende
Will Townsend, Vizepräsident & Principal Analyst, Networking & Security Practices bei Moor Insights & Strategy

Herausgeber
Patrick Moorhead, Gründer, Präsident & Principal Analyst bei Moor Insights & Strategy

Anfragen
Wenden Sie sich an uns, wenn Sie Fragen zu diesem Bericht haben oder darin genannte Punkte besprechen möchten. Moor Insights & Strategy wird Ihnen umgehend antworten.

Zitierungen
Die Angaben in diesem Dokument können von der akkreditierten Presse und AnalystInnen zitiert werden, müssen jedoch im Kontext mit dem Namen des Autors, dem Titel des Autors und „Moor Insights & Strategy“ genannt werden. Nicht-Pressemitglieder und Nicht-AnalystInnen müssen für Zitate die vorherige schriftliche Genehmigung von Moor Insights & Strategy einholen.

Angaben
Dieses Dokument wurde von Cisco in Auftrag gegeben. Moor Insights & Strategy leistet Forschung, Analyse und Beratung für viele der in diesem Dokument erwähnten High-Tech-Unternehmen. Keine MitarbeiterInnen halten Aktienbestände bei den in diesem Dokument genannten Unternehmen.

Haftungsausschlusserklärung
Die im vorliegenden Dokument enthaltenen Informationen dienen nur zu Informationszwecken und können technische Ungenauigkeiten, Auslassungen und Tippfehler enthalten. Moor Insights & Strategy übernimmt keine Gewährleistung für die Richtigkeit, Vollständigkeit oder Angemessenheit dieser Informationen und haftet nicht für Fehler, Auslassungen oder Ungenauigkeiten in diesen Informationen. Dieses Dokument basiert auf der Meinung von Moor Insights & Strategy und sollte nicht als Tatsachenfeststellung ausgelegt werden. In dieser Publikation ausgedrückte Meinungen können ohne vorherige Ankündigung geändert werden.

Moor Insights & Strategy liefert Prognosen und zukunftsgerichtete Aussagen als Richtungsindikatoren und nicht als präzise Vorhersagen zukünftiger Ereignisse. Unsere Prognosen und zukunftsgerichteten Aussagen spiegeln unsere derzeitige Einschätzung der Zukunft wider. Sie unterliegen jedoch Risiken und Unsicherheiten, die dazu führen können, dass die tatsächlichen Ergebnisse erheblich abweichen. Wir empfehlen Ihnen, sich nicht zu sehr auf diese Prognosen und zukunftsgerichteten Aussagen zu verlassen, da diese nur zum Zeitpunkt der Veröffentlichung dieses Dokuments unsere Meinung widerspiegeln. Bitte beachten Sie, dass wir uns nicht verpflichten, die Ergebnisse einer Überarbeitung dieser Prognosen und zukunftsgerichteten Aussagen angesichts neuer Informationen oder zukünftiger Ereignisse zu revidieren oder zu veröffentlichen.