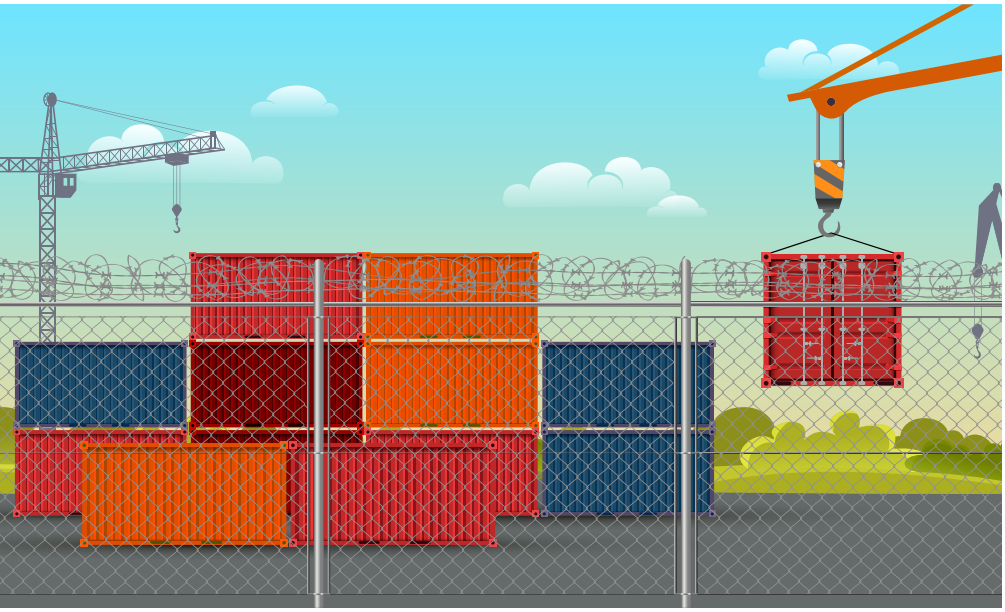


NeuVector Cloud Workload Security ist Open Source

Eingezäunt

Christoph Puppe

Mit NeuVector gibt es jetzt eine konkurrenzfähige Open-Source-Plattform für Containersicherheit: SUSE hat die CWPP-Software nach der Übernahme unter Apache-2-Lizenz gestellt.

Eine Cloud Workload Protection Platform (CWPP) überwacht und schützt Container in Kubernetes-Umgebungen und liefert damit eine wesentliche Grundlage für den sicheren Betrieb containerisierter Anwendungen in der Cloud. Bislang waren hier nur proprietäre Produkte erhältlich. Nun hat SUSE die vor wenigen Monaten übernommene CWPP-Software NeuVector unter Apache-2.0-Lizenz als Open Source komplett auf GitHub veröffentlicht. Alle anderen Hersteller in diesem Markt – Sysdig, Palo Alto, Aqua Security sind die wichtigsten Konkurrenten – veröffentlichen zwar auch etliche Komponenten als Open Source, aber nur einzelne Werkzeuge und nicht die gesamte Plattform.

Ein schon länger etabliertes CWPP-Tool

So bietet Sysdig sein Tool Falco für das Erkennen von Angriffen als OSS an und Aqua Security ist mit seinem OSS-Image-Scanner Trivy einer der Marktführer. Andere freie Werkzeuge wie der OPA (Open Policy Agent) dringen zwar in den CWPP-Markt ein, haben aber deutlichen Nachholbedarf bei der Benutzbarkeit. Und eine ansprechende grafische Oberfläche ist für viele potenzielle Nutzer auch in Zeiten weitgehender Automatisierung immer noch ein wichtiges Thema. Natürlich lassen sich alle CWPP auch in die CI/CD-Pipelines einbinden, so auch NeuVector. Schon im 2017 erschienenen Artikel „Sicher am laufenden Band“ [1] war der damalige Neuling NeuVector das Produkt mit der besten UI und bot ein auch vom Funktionsumfang her vollständiges Angebot.

Eine besondere Stärke von NeuVector ist die Sichtbarkeit des Datenverkehrs zwischen den Pods. Als einziges Produkt kann es einzelne Verbindungen aufzeichnen und es liefert neben Mikrosegmentierung auch Netzwerk-Mapping und Deep Packet Inspection. Eine elementare Funktion für die teilweise oder ganz automatisierte Überwachung des Verhaltens ist die Option, anhand des beobachteten Verhaltens der Container Regelwerke zu erstellen. Hier kann das CWPP seine Stärken auch gegenüber den OSS-Konkurrenten ausspielen, deren SECCOMP-, SELinux- und Network-Policy-Einstellungen von der Anwendungsentwicklung vorzunehmen sind. Und die Erfahrung lehrt, dass dies kaum jemand auf sich nimmt, geschweige denn einen Whitelisting-Ansatz implementiert, in dem dem Container nur ausgewählte System Calls, Netzwerkverbindungen und Zugriffe gestattet sind. Wer dies konsequent einsetzt, ist vor den meisten bekannten Angriffen sehr gut geschützt und kann im Containerbetrieb eine Sicherheit erreichen, die auch über der vom Hypervisor separierter und auf traditionelle Weise gesicherter Umgebungen liegt.

iX-Wertung

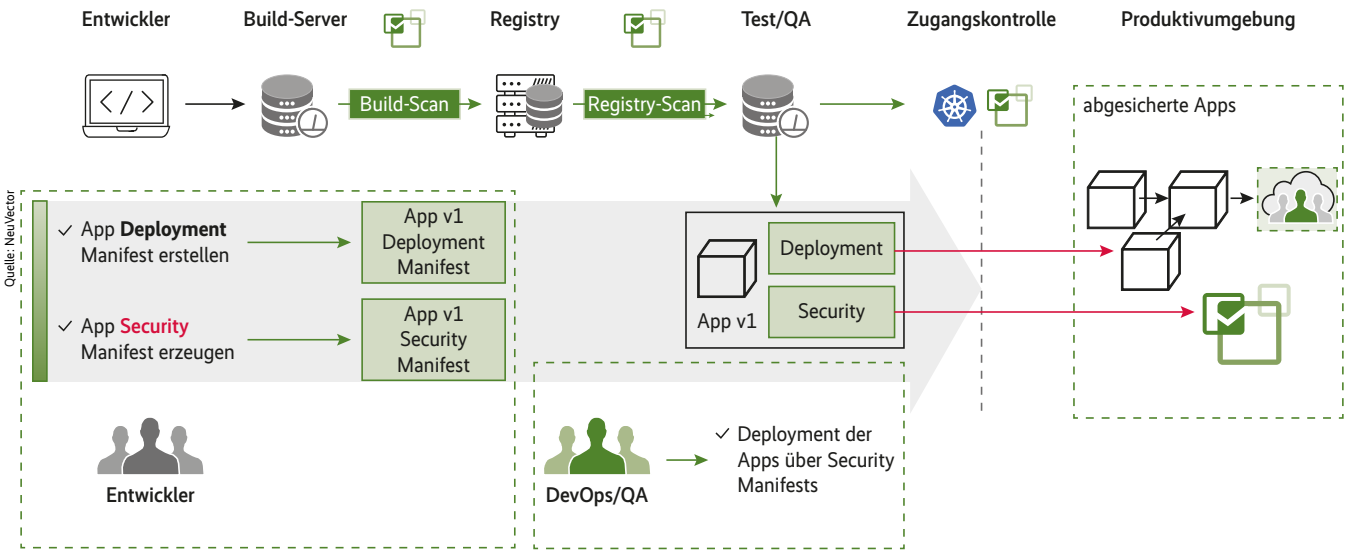
NeuVector Cloud Workload Security

- ⊕ GUI mit Stärken bei der Netzwerküberwachung
- ⊕ in den Marketplaces aller Hyperscaler verfügbar
- ⊕ als Open-Source-Software auch on Premises nutzbar

SUSE ist in guter Gesellschaft

Auf den ersten Blick mag der Schritt von SUSE verwundern, die bislang proprietäre Cloud Workload Protection Platform (CWPP) NeuVector bei GitHub zu veröffentlichen, schließlich war der Kauf der Firma nicht billig (siehe ix.de/zkuy). Im Vergleich zur Konkurrenz sind die 130 Millionen US-Dollar für NeuVector dennoch ein Schnäppchen. So werden die letzten noch nicht aufgekauften Start-ups im CWPP-Segment, Aqua Security und Sysdig, mit jeweils über einer Milliarde US-Dollar bewertet. Palo Alto Networks holte sich für 410 Millionen US-Dollar Twistlock ins Portfolio und integrierte es in sein neues Angebot Prisma Cloud. IBM / Red Hat sicherte sich Gerüchten zufolge StackRox für etwas über 100 Millionen US-Dollar.

Auch im Licht der digitalen Souveränität und gemäß dem Vorsatz der Bundesregierung, mehr OSS einzusetzen, ist SUSEs Schritt nachvollziehbar. Damit wandelt sich NeuVector für Bundesbehörden mit einem Federstreich zum CWPP mit der höchsten Compliance gegen die Anforderungen des IT-Planungsrats. Dieser fordert seit Jahren – wenn auch mit mäßigem Erfolg – die Nutzung von OSS, aber auch



In einer geschützten Umgebung kann NeuVector das Verhalten von Containern selbstlernend in Richtlinien abbilden, die dann zur Laufzeit in der Produktion verhindern, dass sich der Container ungewöhnlich verhält. Das lässt sich als automatisierter Schritt in eine CI/CD-Pipeline integrieren und kann erfolgreich viele Angriffe abwehren.

von IPv6, KI, Blockchain und anderen Techniken, die die Zukunftsfähigkeit der IT in Deutschland sicherstellen sollen. Zur Sicherheit des Containerbetriebs kann NeuVector hier jetzt einiges beitragen.

Insofern hat die deutsche Softwareschmiede SUSE hier alles richtig gemacht. Auch ein höherer Marktanteil durch die Nutzer der OSS-Version und somit mehr potenzielle Kunden für Supportverträge sind eine gute Strategie. Ein anderer Grund, warum Firmen ihre teuer erstellten Anwendungen unter eine freie Lizenz stellen, ist die Hoffnung, neue Entwickler anzuziehen und so die Produktentwicklung zu beschleunigen. Ob dies bei den bereits vorhandenen OSS-Werkzeugen zur Absicherung von Containern gelingt, wird die Zeit zeigen. Der Erfolg einer solchen Strategie hängt von vielen Faktoren ab und die Insights auf GitHub werden einen ungefilterten Einblick geben, wie viele Personen aufspringen und aktiv mitarbeiten.

Nach dem nicht so großen Markterfolg des eigenen CaaS-Produkts (Container as a Service) hatte SUSE sich bereits mit Rancher eine im Markt etablierte Kubernetes-Distribution einverleibt. Mit der NeuVector-Akquisition rüstet sich die Firma besser für den bereits stattfindenden Verdrängungswettbewerb in dem strategisch wichtigen Marktsegment, das Red Hat mit OpenShift klar dominiert und in dem schon einige scheiterten. Selbst große Firmen wie IBM, NetApp, Cisco und andere sind hier auf Grund gelaufen. Derzeit ist dort sonst nur noch VMware mit seinen beiden Tanzu-Versionen aus dem Rückkauf von Pivotal erfolgreich aktiv. Recht neu ist Kubermatic aus Hamburg mit dabei. Gute Zahlen sind Mangelware, aber Statista hat 500 ITler aus Firmen mit mehr als 500 Mitarbeitern zum Einsatz von Kubernetes-Plattformen in ihrem Unternehmen befragt. Die Umfrageergebnisse klingen recht glaubwürdig (siehe ix.de/zkuy).

Sich einen Platz in der Zukunft zu erkaufen, ist ja jetzt keine neue Strategie und nicht immer muss es so teuer sein wie der Kauf von Red Hat, mit dem IBM sein Portfolio um OpenShift und viele weitere Cloud-Technologien erweiterte. Ein anderes Beispiel von vielen ist NetApp, die sich mit dem Kauf von Point als Anbieter von Multi-Cloud-Management sehen und ihre Produkte um Cloud-Storage erweiterten, den es jetzt auch direkt beim Hyperscaler gibt. Der Ausgang dieser Abenteuer ist hier zumeist noch offen. Ob die aufgekauften Ex-Start-ups nach der Integration mit dem Wachstum des Markts mithalten können, muss sich erst zeigen. Zwischen too big to fail fast sowie klein und flexibel scheint rund um Kubernetes wenig Raum zu sein. Ähnlich wie bei einem Hurrikan, der einmal über die Landschaft der etablierten Softwarehäuser hinwegzieht und die Küstenlinie mit den Wracks ehemals stolzer Schiffe und neuen Sandbänken hinterlässt.

Gute Aussichten haben zumindest die vier Hyperscaler, die den Markt für Managed Kubernetes unter sich aufteilen. Die meisten Softwareanbieter sind bereits mit virtuellen Appliances und SaaS-Diensten in ihren Marktplätzen vertreten – alles andere wäre der Überlebenswahrscheinlichkeit abträglich. NeuVector ist hier gut etabliert und auch in den Marktplätzen von Oracle, IBM und Alibaba erhältlich. SUSE erweitert damit sein Angebot um einen Dienst, der kein Betriebssystem mit Wartungsvertrag ist.

Fazit

Das Kubernetes-Ökosystem ist kein gemütlicher Ort. Die Updates kommen im Quartal, Long-Term Support ist aktuell nicht mal in Beta und der Markt heftig umkämpft. Eine Nische zu finden ist daher nicht leicht. Sich hier mit Rancher, NeuVector und dem neuen Liberty Linux als Ersatz für Red Hats CentOS über Wasser zu halten, ist sicherlich ein guter Schachzug. Dabei kann es auch nicht schaden, die Anforderungen der Bundesbehörden zu erfüllen. Und vielleicht hilft SUSE beides, verlorene Marktanteile zurückzuerobern. (avr@ix.de)

Quellen

[1] Patrick Münch, Christoph Puppe; Sicher am laufenden Band; Docker-Container und -Hosts überwachen; *iX* 5/2017, S. 78

[2] Details zur Ankündigung und zur Statista-Umfrage: ix.de/zkuy

Christoph Puppe

ist Managing IT Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei SVA System Vertrieb Alexander GmbH, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.