Akamai

WHITE PAPER

Die Vorteile von Containern zunutze machen

Vereinfachung und Beschleunigung der Segmentierung für kritische Assets und Anwendungen

Einführung

Die Containerisierung hat sich schnell zur bevorzugten Lösung für die Bereitstellung von Anwendungen in Cloud- und hybriden Umgebungen entwickelt – und die Verbreitung von containerisierten Anwendungen nimmt weiter zu. Laut Gartner werden bis 2026 90 % der globalen Unternehmen Containeranwendungen in der Produktion ausführen – gegenüber 40 % im Jahr 2021.[1] Und laut einer Studie von Forrester für Capital One **priorisieren 86 % der befragten IT-Führungskräfte die erweiterte Nutzung von Containern für mehr Anwendungen**.[2]

> Laut Gartner werden **90 % der globalen Unternehmen** bis 2026 containerisierte Anwendungen in der Produktion ausführen – gegenüber 40 % im Jahr 2021

All dies erhöht natürlich den Druck auf die Verantwortlichen für die Sicherung von IT-Umgebungen, mit der Bereitstellung von Containern Schritt zu halten, insbesondere in einem DevOps-Modell, bei dem die schnelle Einführung und Erweiterung im Vordergrund steht. Es gibt zwar eine Reihe von spezialisierten Container-Sicherheitslösungen, doch diese plattformspezifischen, auf Container beschränkten Entitäten erhöhen die Komplexität und den Verwaltungsaufwand, ohne das Rechenzentrum des Unternehmens als Ganzes zu berücksichtigen – wodurch es Sicherheitsteams noch schwerer haben. Was wir brauchen, ist eine individuelle, umfassende Sicherheitslösung, die konsistent für alle Anwendungen und Technologien in lokalen, Cloud- und hybriden Umgebungen, einschließlich Containern, funktioniert.

Bevor wir uns jedoch mit Lösungen befassen, wollen wir uns kurz mit dem Container-Phänomen, den treibenden Kräften und den Auswirkungen in Sachen Sicherheit beschäftigen.

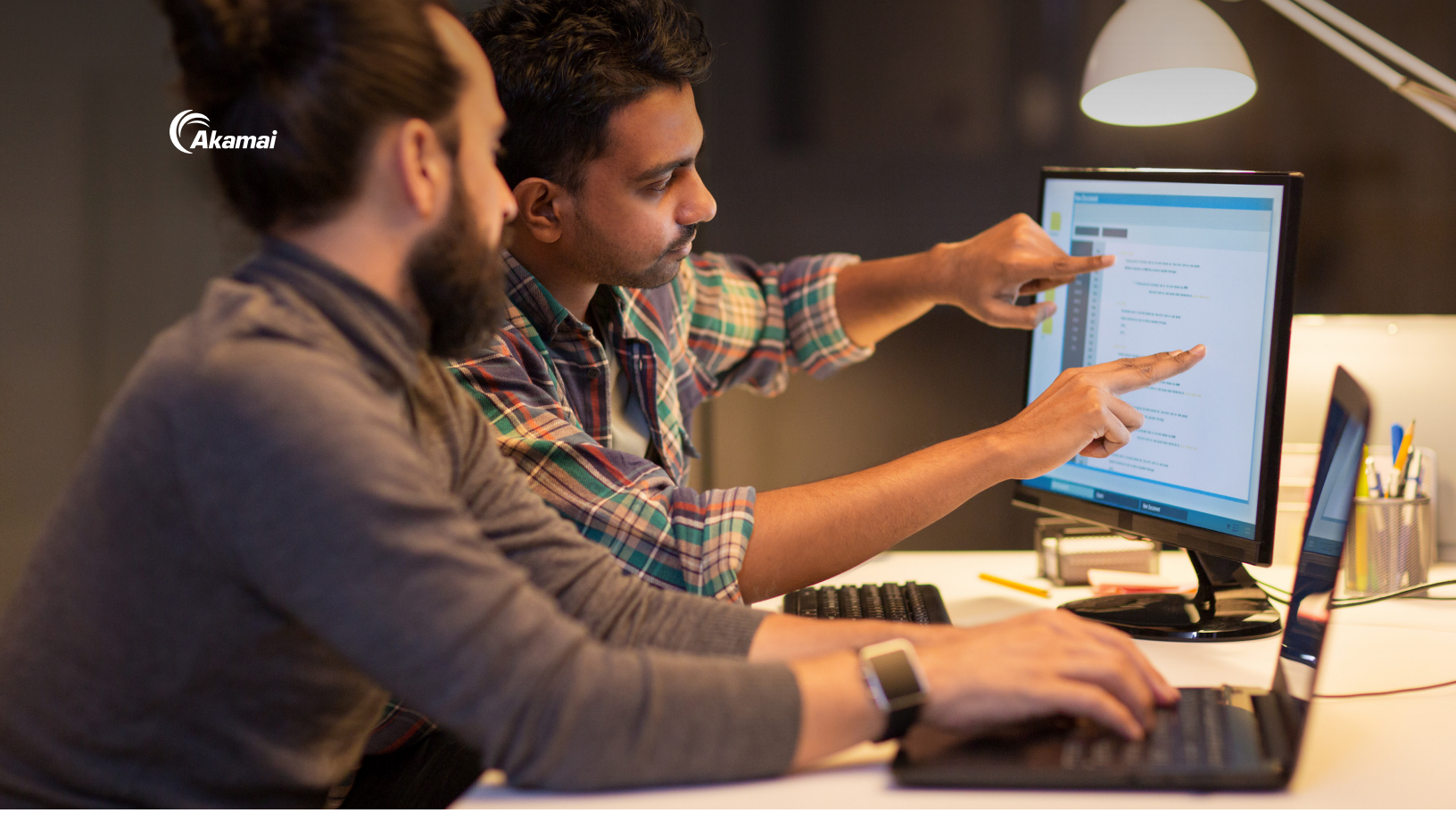
Der Druck wächst: Geschäftliche Anforderungen treiben die Einführung voran

Die Entwicklung hin zu Containern und deren prognostizierter Anstieg können auf die geschäftlichen Anforderungen zurückgeführt werden, die den IT-Abteilungen des Unternehmens auferlegt werden. Moderne Unternehmen erwarten, dass sie schnell und flexibel auf neue Konkurrenten und Marktchancen reagieren können. Sie benötigen Lösungen, die Innovationen unterstützen und die Markteinführungszeit verkürzen. Und sie sind immer auf der Suche nach kontinuierlicher Effizienzsteigerung. In einer zunehmend vernetzten Welt wollen sie die digitale Abwicklung von Geschäften mit Lieferanten und Anbietern, Geschäftspartnern und vor allem mit ihren Kunden erleichtern.

Dies sind einige der Hauptgründe, warum die Unternehmens-IT in die Cloud verlagert wird, genauer gesagt in hybride Modelle aus On-Premises und Cloud. Sie sind auch die treibenden Kräfte hinter dem DevOps-Trend, die Bereitstellung kritischer Anwendungen zu beschleunigen, indem Reibungspunkte von der Idee bis zur Implementierung beseitigt und mithilfe von Automatisierung und automatischer Skalierung Anwendungen schneller in Produktion gebracht werden.

> **„Unternehmen unterschätzen oft den Aufwand für den Betrieb von Containern in der Produktion.“**
>
> **– Gartner**

All dies erklärt, warum IT-Abteilungen die Containerisierung befürworten. Im Vergleich zu virtuellen Maschinen lassen sich Container viel einfacher und schneller starten, sodass sie Just-in-Time-Bereitstellung praktisch ohne Latenz ermöglichen und Teams sich auf die „Inbetriebnahme von Services statt von Servern“ konzentrieren können. Ein wichtiger Vorteil von Containern ist im Hinblick auf die dynamischen Rechenzentrumsumgebungen von heute ihre Portabilität; sie erleichtern die Migration von Anwendungen zwischen lokalen Umgebungen und Multicloud-Instanzen. Dies wird durch die Orchestrierung von Containern über Kubernetes, oder „K8s“, noch weiter verbessert, wodurch Teams größere Mengen von Containeranwendungen skalierbar über mehrere Umgebungen hinweg bereitstellen und verwalten können. Die Orchestrierung wird bei der Implementierung und Verwaltung von Containern zunehmend als Best Practice angesehen.



Kurz gesagt: Mithilfe von Containern kann die IT-Abteilung also besser auf Geschäftsanforderungen in Bezug auf Geschwindigkeit, Automatisierung, Ausfallsicherheit und Verfügbarkeit reagieren und dies zu niedrigeren Gesamtbetriebskosten im Vergleich zu anderen Technologien. Die Umsetzungsbemühungen sind jedoch nicht frei von Problemen. „Unternehmen unterschätzen oft den Aufwand für den Betrieb von Containern in der Produktion“, so ein Gartner-Bericht aus dem Jahr 2019 über Best Practices bei der Containerisierung.[3] Trotz der weitverbreiteten Attraktivität der Containerisierung ist die Technologie noch nicht ganz ausgereift, und umfassende Best Practices für eine sichere Bereitstellung lassen noch auf sich warten. Laut dem „State of Kubernetes Security“-Bericht von Red Hat aus dem Jahr 2022 ist „die Sicherheit noch immer eines der größten Probleme bei der Containereinführung, und Sicherheitsprobleme verursachen weiterhin Verzögerungen bei der Bereitstellung von Anwendungen in der Produktion.“[4] Es liegt auf der Hand, dass Unternehmen nicht alle potenziellen Vorteile von Containern ohne eine Implementierungsstrategie nutzen können, die notwendigerweise auch die Cybersicherheit umfasst.

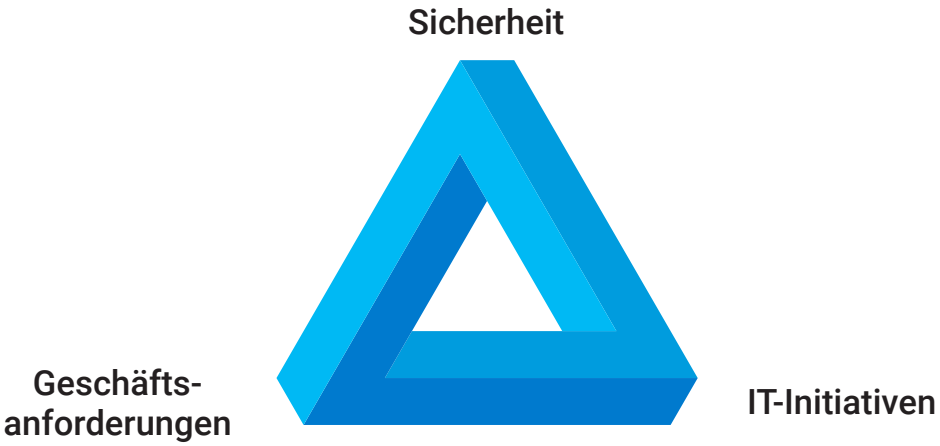
> Laut dem Bericht „State of Kubernetes Security“ 2022 von Red Hat, „**ist Sicherheit [weiterhin] bei der Einführung von Containern eines der wichtigsten Anliegen**, und Sicherheitsprobleme führen bei der Bereitstellung von Anwendungen in der Produktion noch immer zu Verzögerungen”

Was bedeutet das für das Sicherheitsteam?

„Sicherheit lässt sich nicht nachträglich implementieren“, betont Gartner in seinem Bericht über Best Practices. „Sie muss in den DevOps-Prozess eingebettet werden.“ Das ist jedoch leider häufig nicht der Fall. In der Eile, die Containerisierung zu implementieren, haben Sicherheitsteams manchmal das Gefühl, an der Spitze eines „unmöglichen Dreiecks“ zu stehen, einer optischen Täuschung, die auch als „Penrose-Dreieck“ bekannt ist (bei Akamai auch bekannt als Klein & Howard Impossible Triangle).

> Veraltete Sicherheitslösungen lassen sich nicht an die Anforderungen eines modernen Unternehmens anpassen. Sicherheitslösungen müssen schnell, anpassungsfähig, dynamisch sein und sich nahtlos in einen „DevSecOps“-Ansatz einfügen.

Genauso wie der oberste Punkt des Dreiecks scheinbar weiter entfernt ist als die beiden anderen Ecken, scheint die Sicherheit hinter den geschäftlichen Anforderungen und den IT-Initiativen zur Erfüllung dieser Anforderungen zurückzubleiben. Doch so wie das Dreieck eine optische Täuschung ist, liegen Sicherheitslösungen tatsächlich näher, als es scheint. Teams müssen einfach über die umständlichen, veralteten Lösungen hinausdenken, auf die sie sich in der Vergangenheit verlassen haben, und nach Lösungen suchen, die auf die heutige Art und Weise der Unternehmens-IT abgestimmt sind und sich nahtlos in einen „DevSecOps“-Ansatz einfügen. Das heißt: Eine Lösung, die schnell, anpassungsfähig und dynamisch ist und den DevOps-Strategieansatz an sich integriert. Das Wichtigste ist eine Lösung, die von den zugrunde liegenden Betriebssystemen und Plattformen abgekoppelt ist, um Implementierung und Verwaltung zu vereinfachen.



Unmögliches Dreieck, Klein & Howard

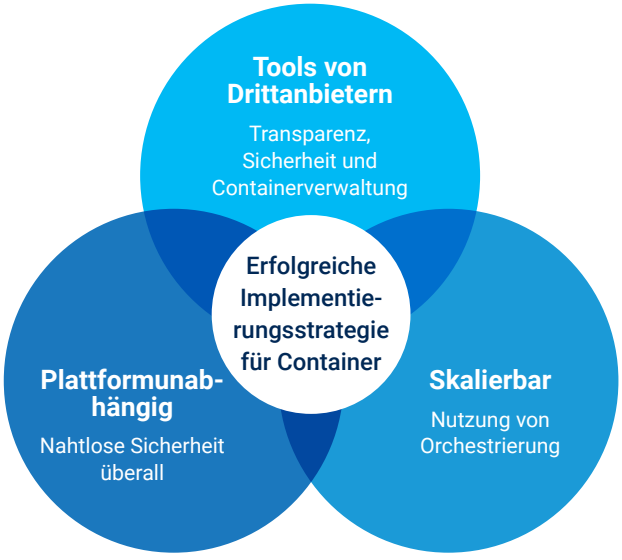
Warum „nativ“ nicht ausreicht

In den Anfängen der Virtualisierung und Cloudmigration waren Unternehmen häufig davon überzeugt, dass Cloud-native Kontrollmaßnahmen für die Visualisierung, Verwaltung und den Schutz ihrer Workloads ausreichen. Erst nach intensivem Trial-and-Error erkannten die IT-Manager, dass sie ein Overlay-Management-Modell brauchten, das Lösungen von Drittanbietern einbezieht, die über die nativen Kontrollmechanismen hinaus Sicherheit bieten.

Wie Gartner und Forrester Research bereits bemerkten, basiert eine erfolgreiche Implementierungsstrategie für Container auf einem „Container-Dreigespann“:

- Ausführen von Containern in einer portablen, plattformunabhängigen Art und Weise, die überall und nahtlos in verschiedenen Cloud- und On-Premises-Architekturen implementiert werden kann
- Einsatz von Orchestrierung zur skalierbaren Ausführung und Verwaltung von Containern
- Verwendung von Drittanbieter-Tools für Container-Management, -Transparenz und -Sicherheit

Im Gegensatz zu früheren Virtualisierungs- und Cloud-Bestrebungen hat die Containerbranche von Anfang an erkannt, dass Cloud-native Managementsysteme, und insbesondere Sicherheitskontrollen, für eine effektive Containerstrategie ungeeignet sind. In einer Studie von Gartner zu Container-Management-Lösungen **gaben 65 % der Befragten an, dass sie die Nutzung von Verwaltungstools von Drittanbietern zur Visualisierung, Verwaltung und Sicherung von Containerarbeitslasten beabsichtigen**.[5] Diese Tools von Drittanbietern müssen jedoch nahtlos sowohl mit lokalen als auch mit Cloud-Instanzen zusammenarbeiten und einen granularen Ansatz verfolgen, um die Fallstricke umständlicher, gemischter Methoden zu vermeiden, die in der Vergangenheit verwendet wurden – wie Sicherheitsgruppen, VLANs und Firewalls, die keinerlei Transparenz und kaum Granularität bieten.



Containereinführung mit Akamai Guardicore Segmentation

Akamai Guardicore Segmentation wurde entwickelt, um die Herausforderungen der dynamischen, hybriden Rechenzentrumsinfrastrukturen von heute zu bewältigen. Wir bieten umfassende Transparenz über alle Anwendungen und Workloads hinweg, die in mehreren Umgebungen ausgeführt werden, und ermöglichen eine einfach zu implementierende, granulare softwaredefinierte Segmentierung durch die schnelle Erstellung, Bereitstellung und Durchsetzung von Sicherheitsrichtlinien für einzelne oder logisch gruppierte Anwendungen.

Lassen Sie uns eines klarstellen: Akamai Guardicore Segmentation ist kein reines Containerprodukt. Vielmehr ist die Containersicherheit eine Schlüsselfunktion der Plattform, die konsistent in gemischten Umgebungen funktioniert, die auch Bare-Metal-Server, virtuelle Maschinen, serverlose Workloads und Remote-Geräte umfassen können. Dementsprechend bieten wir Unternehmen eine einzige, umfassende Lösung für die Sicherung aller Assets im Rechenzentrum und in der Cloud, unabhängig davon, wo sie sich befinden oder wie sie bereitgestellt werden. So müssen sie nicht mehr mehrere Einzellösungen verwalten. Und da unsere Lösung unabhängig von den zugrunde liegenden Plattformen und Betriebssystemen funktioniert, können die Sicherheitsrichtlinien an die Anwendungen und Workloads angepasst werden, wenn sie zwischen lokalen und Cloudumgebungen verschoben werden. Dadurch wird der Portabilitätsfaktor erhöht, der Container für die Anwendungsbereitstellung in Hybrid-Cloud-Infrastrukturen attraktiv macht.

> Containersicherheit ist eine wichtige Funktion von Akamai Guardicore Segmentation, die konsistent in dynamischen, heterogenen Rechenzentrumsumgebungen funktioniert

In Bezug auf Container platziert Akamai Guardicore Segmentation Agenten auf Container-Host-Knoten und ermöglicht so einen Einblick in das gesamte Container-Cluster, einschließlich der Kommunikationsflüsse von Pod zu Pod und Pod zu virtueller Maschine. Dies ermöglicht eine sehr fein abgestufte Implementierung und Durchsetzung von Sicherheitsrichtlinien nach Prozess, Nutzer und vollständig qualifiziertem Domainnamen (FQDN). In einem Orchestrierungsszenario unterstützen wir die K8s-Orchestrierung und ermöglichen Transparenz in Kubernetes- und OpenShift-Metadaten für einen umfassenden Kontext. Mit einem flexiblen Kennzeichnungsmodell können Bediener Richtlinien mithilfe nativer K8s-Terminologie formulieren. Für die K8s-Durchsetzung nutzen wir die native CNI (Container Network Interface), eine nicht-intrusive Methode zur Durchsetzung von Richtlinien in K8s ohne Skalierungseinschränkungen. Mithilfe spezieller Vorlagen können Nutzer geschäftskritische Kubernetes-Anwendungen abschirmen. Dabei spielt es keine Rolle, ob es sich um einen Namespace, eine Anwendung oder ein anderes Objekt handelt. Wir bieten auch eine Skalierung von K8s Workload-Mengen und Änderungsraten an. Da unsere Lösung auch mit allen anderen Unternehmens-Workloads in ähnlicher Weise funktioniert, dient sie als eine einzige Lösung zur Visualisierung, Verwaltung und Sicherung von Assets in Ihrem gesamten Unternehmen.

In einer DevOps-Umgebung ist es besonders wichtig, dass die von Ihnen erstellten Sicherheitsrichtlinien effektiv in CI/CD-Prozesse (Continuous Integration/Continuous Deployment) integriert werden. So wird sichergestellt, dass die Sicherheit nicht erst im Nachhinein Beachtung findet, sondern vollständig in das Bereitstellungsmodell integriert ist.

Fazit

Container werden zunehmend integraler Bestandteil vieler Geschäftsumgebungen. Sie können die Effizienz der Ressourcennutzung steigern, Prozesse optimieren und eine höhere Portabilität und Skalierbarkeit ermöglichen. Gleichzeitig reichen die integrierten Sicherheitsfunktionen nicht aus, insbesondere wenn Unternehmen eine hybride Umgebung nutzen.

Wenn Sie nach einer Sicherheitslösung suchen, die mit Ihrem Unternehmen wächst, sollten Sie sich für ein plattformunabhängiges Tool entscheiden, das detaillierte Einblicke in Ihre End-to-End-Prozesse bietet, unabhängig davon, wo sie stattfinden. Akamai Guardicore Segmentation bietet genau das und noch mehr: die Funktionen und Fähigkeiten, die moderne Unternehmen heute und in Zukunft benötigen.

Mit Akamai Guardicore Segmentation kann Ihr Sicherheitsteam konsistente Sicherheit in dynamischen, heterogenen Rechenzentrumsumgebungen erreichen. Auf diese Weise können Sie IT-Teams dabei unterstützen, das Potenzial der Containerisierung auszuschöpfen und die schnelle, kostengünstige und sichere Entwicklung und Implementierung wichtiger Anwendungen zu realisieren, die für die Geschäftsanforderungen Ihres Unternehmens unerlässlich sind.

Vereinfachen Sie die Sicherheit in Ihrer gesamten Umgebung. Weitere Informationen zu unserer leistungsstarken, einheitlichen Sicherheitslösung für Container finden Sie unter: akamai.com/guardicore.

1 Chandrasekaran, Arun und Wataru Katsurashima. „The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem", Gartner, 18. August 2021.

2 „Cloud Container Adoption In The Enterprise", Forrester, Juni 2020.

3 „Best Practices for Running Containers and Kubernetes in Production", Gartner, 25. Februar 2019.

4 „State of Kubernetes Security Report", Red Hat, Mai 2022.

5 „Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024", 25. Juni 2020.