Vier Möglichkeiten für mehr Cloud-Sicherheit

Ein sicherheitsorientierter Ansatz mit den Cloud-Services von Red Hat OpenShift

Um wettbewerbsfähig zu bleiben, modernisieren viele Unternehmen ihre Technologien und Prozesse. Dies kann jedoch die Wartung und Sicherung der Cloud-Umgebung erschweren. Cloud-Sicherheit liegt in der gemeinsamen Verantwortung von Cloud-Anbietern und Nutzenden. Wenn letztere die Anwendung von Best Practices versäumen, kommt es jedoch häufig zu Sicherheitsmängeln. Gemanagte Cloud-Services mit integrierten Sicherheitsfunktionen können dazu beitragen, Modernisierungsmaßnahmen zu vereinfachen.

Mit diesen vier Möglichkeiten kann Ihre Organisation die Cloud-Sicherheit erhöhen.

1 Schnellere Implementierung durch integrierte Sicherheit

Machen Sie Sicherheit in Ihrer gesamten Cloud-Umgebung zur Priorität. Mit einer sicheren Software-Lieferkette, automatisierten DevSecOps-Praktiken und Anwendungssicherheit zur Laufzeit können Sie Sicherheitsmaßnahmen vorverlegen und in den gesamten Entwicklungszyklus einbauen.

Die Cloud-Services von Red Hat® OpenShift® bieten integrierte Sicherheitsfunktionen, die Ihr Unternehmen bei Folgendem unterstützen:

- Vereinfachtes Software-Deployment und geringere operative Komplexität dank automatisierter Sicherheitswartung, kontinuierlicher Überwachung und präventiver Problembehebung – integriert in Ihre vollständig gemanagten Services
- Bewertung der Konfiguration Ihrer Kubernetes-Plattform und Sicherung über automatisierte Deployment-Richtlinien mithilfe von integrierter Plattformkonfigurations- und Lifecycle-Verwaltung, Identitäts- und Zugriffsverwaltung, Sicherheit für Plattformdaten und angehängtem Storage
- Integration von DevOps-Praktiken und internen Kontrollen in Überprüfungen der Sicherheitskonfiguration Ihrer Plattform

2 Delegation von Risikomanagement zur Steigerung der Produktivität

Erreichen Sie mehr Effizienz und beschleunigen Sie die Anwendungsentwicklung, indem Sie Ihren Teams ermöglichen, sich auf höherwertige Initiativen zu konzentrieren. Wenn das Sicherheits- und Infrastrukturmanagement als gemeinsame Verantwortung angesehen und Aufgaben delegiert werden, ist Folgendes möglich:

- Um 70 % kürzere Anwendungsentwicklung und -bereitstellung sowie schnellere Skalierung und kontinuierliche Weiterentwicklung von Anwendungen[1]
- Bessere operative Effizienz durch Entlastung der zuvor für die Infrastrukturverwaltung verantwortlichen DevOps-Teams
- Unterstützung des Entwicklungsteams bei der Zerlegung von Updates in kleinere Schritte zur Verringerung des Drucks durch umfangreiche Tests innerhalb kurzer Fristen
- Ein optimiertes und kuratiertes Entwicklungserlebnis in Ihren Hybrid Cloud-Umgebungen

[1] Forrester Consulting, gesponsert von Red Hat. „The Total Economic Impact von Red Hat OpenShift Cloud Services", Januar 2022.

3 Reduzierung von Risiken durch Automatisierung und proaktive Verwaltung

Sie können auf die Einstellung von dedizierten Sicherheitsfachkräften für Ihre Anwendungsplattform verzichten und die Kosten und Ressourcen reduzieren, die für die Wartung Ihrer Cloud-Umgebung erforderlich sind. Vorteile vollständig gemanagter Cloud-Services:

- Sie können sich auf wertorientierte und wachstumsbezogene Aufgaben konzentrieren und entledigen sich der Belastung durch die manuelle Anwendung von Sicherheits-Updates und -Patches, da diese durch das SRE-Team (Site Reliability Engineering) von Red Hat gemanagt wird.
- Indem Sie die Notwendigkeit interner Infrastrukturverwaltung reduzieren, verringern Sie gleichzeitig die Verantwortung und Risiken für Ihre Entwicklungsteams. Unternehmen, die die Cloud-Services von OpenShift verwenden, gewannen 20 % der Arbeitszeit von Entwicklungsteams zurück[1].
- Sie können für weniger Fehlkonfigurationen in Ihren Kubernetes- und Container-Plattformen sorgen, die laut IT-Fachkräften fast dreimal so besorgniserregend wie Cyberangriffe sind.

4 Wahl eines Anbieters mit nachgewiesener Sicherheitserfahrung

Sorgen Sie für ein konsistentes und zuverlässiges Nutzungserlebnis, das mit allen wichtigen Cloud-Anbietern funktioniert, einschließlich Amazon Web Services (AWS), Microsoft Azure, IBM Cloud und Google Cloud.

Dank tiefer Wurzeln in Open Source-Sicherheit unterstützt Red Hat Sie dabei, Sicherheit durchgehend in Lifecycle, Infrastrukturen und Anwendungsstacks zu integrieren, und zwar durch:

- Eine Defense-in-Depth-Strategie mit standardmäßigen Zero-Trust-Richtlinien und einem Partnernetzwerk für die Ausweitung von Sicherheitsprinzipien
- Integrierte Sicherheit bei Teams, Prozessen und Technologien zur Verwaltung, Automatisierung und Anpassung der Infrastruktur für eine dauerhafte Sicherheit und Compliance
- Ein globales, rund um die Uhr verfügbares SRE-Team für die Verwaltung und Sicherung von Anwendungsplattformen, Management und Datenservices
- Cloud-Sicherheitsservices zur Reduzierung von Unterbrechungen und Systemausfällen mit einem finanziell gesicherten SLA von 99,95 %

Einstieg

Weitere Informationen zur Zuverlässigkeit der Red Hat OpenShift Cloud-Services finden Sie im Red Hat OpenShift Sicherheits-Guide.

[1] Forrester Consulting, gesponsert von Red Hat. „The Total Economic Impact von Red Hat OpenShift Cloud Services", Januar 2022.

Über Red Hat

Red Hat unterstützt Kunden dabei, ihre Umgebungen zu standardisieren, cloudnative Anwendungen zu entwickeln und komplexe Umgebungen mit vielfach ausgezeichnetem Support, Training und Consulting Services zu integrieren, zu automatisieren, zu sichern und zu verwalten.

EUROPA, NAHOST, UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com
#F31854_202207