LÖSUNGSDATENBLATT

Calico für Kubernetes-Sicherheit

Kubernetes ist die De-facto-Plattform zur Arrangierung containerisierter Zugriffe und Dienste für Hybrid- und Multi-Cloud-Bereitstellungen sowie Multi-Clusterumgebungen, die alle zu den Bausteinen cloudnativer Applikationen gehören.

Sicherheitstechnische Herausforderungen

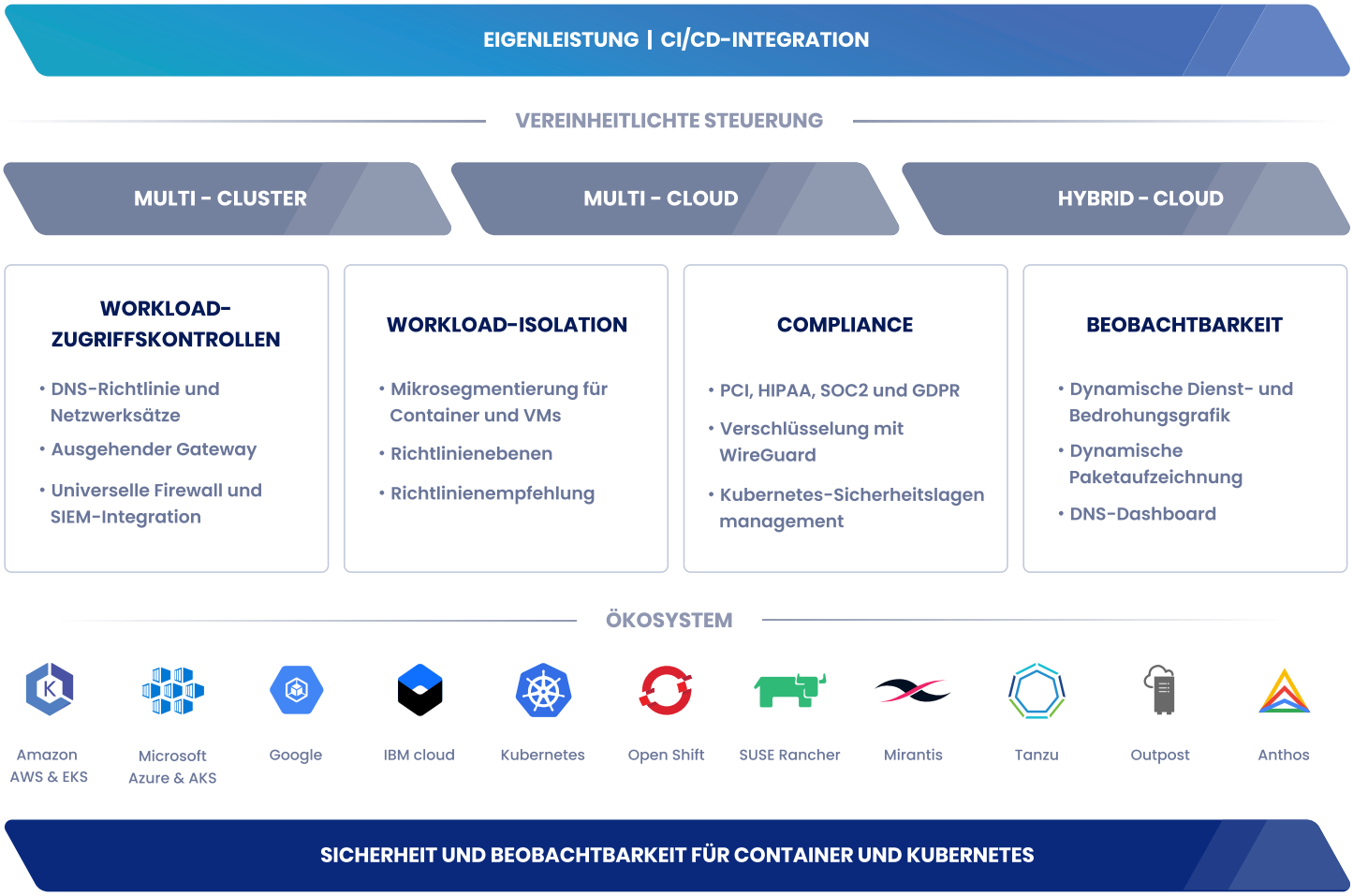
Kubernetezugriffe sind hochdynamisch, kurzlebig und in einer verteilten und agilen Cloudinfrastruktur wie Red Hat OpenShift, SUSE Rancher, Amazon EKS und Microsoft AKS beheimatet. Folglich müssen Cloudplattformarchitekten und -ingenieure sich zahlreichen sicherheitstechnischen Herausforderungen stellen, wenn sie Kubernetezugriffe bereitstellen.

- Sichern Sie Ihre Kommunikation durch Ressourcen außerhalb des Clusters ab.
- Ermöglichen Sie sicheren Zugriff auf Ressourcen hinter traditionellen Firewalls.
- Isolieren Sie Applikationen und Zugriffe durch Segmentierung des Kubernetes-Clusters.
- Bieten Sie Einblick in aktive und inaktive Sicherheitsrichtlinien und Sicherheitslücken im Cluster.
- Stellen Sie sicher, dass Ihre Kubernetes-Konfiguration Branchenvorgaben wie CIS für Kubernetes erfüllt.
- Stellen Sie die Einhaltung der Vorgaben von SOC 2, PCI DSS, HIPAA, und anderen sicher.
- Vereinfachen Sie die Verwaltung von Sicherheitsrichtlinien durch automatisierte End-to-End-Workflows zu deren Erstellen, Bereitstellen, Aktualisieren und Löschen.
- Stellen Sie Konnektivität und sichere Kommunikation zwischen verschiedenen Zugriffen & Diensten über mehrere Cluster hinweg sicher.
- Gestalten Sie gemeinsam genutzte Dienste über mehrere Kubernetes-Cluster hinweg.

Wie Calico Abhilfe schaffen kann

Angriffsfläche reduzieren	Sichtbarkeit und Compliance	Vereinheitliche Sicherheitskontrollen
Secure pod access and communication within and outside of the cluster to mitigate attacks	Gain end-to-end traffic visibility to identify security gaps, service connectivity, and performance issues	Single pane of glass to manage security policies across multi-cloud and multi-cluster Kubernetes environments

Calico ist die einzige aktive Sicherheitsplattform der Branche mit Full-Stack-Beobachtbarkeit, die sich an Kubernetes-Cluster und Anforderungen an die Zugriffssicherheit richtet. Tigera liefert Calico als vollverwaltete SaaS- (**Calico Cloud**) oder selbstverwaltete Dienst-Lösung (**Calico Enterprise**) aus. Beide Calico-Plattformen helfen Organisationen bei der Verwaltung von Sicherheitsrichtlinien über mehrere Applikationen, Cluster und Umgebungen hinweg.



Implementieren von Kubernetes Security mit Calico

Zero-Trust-Zugriffskontrollen

Calico bietet fein abgestimmte Zero-Trust-Zugriffskontrollen zwischen einzelnen Abschnitten in Kubernetes-Clustern auf externe Ressourcen, wie z.B. Datenbanken, interne Applikationen, 3rd-Party-Cloud-APIs und SaaS-Applikationen. Es bietet fein abgestimmte Zugriffskontrollen durch Richtlinien für abgehende DNS-Anfragen und NetworkSets (bei Verwendung von IPs/CIDRs in der Richtlinie).

Ausgehender Gateway

Ausgehende Gateways erlauben Ihnen die Erkennung der Datenverkehrsquelle im Namensraum oder auf Abschnittsebene, wenn er einen Kubernetes-Cluster verlässt, um mit externen Ressourcen zu kommunizieren. Dies ist für Sicherheitsteams äußerst nützlich, um die Zugriffskontrolle nur auf bestimmten Traffic anzuwenden anstatt einen größeren IP-Adressbereich zu öffnen. Calicos Gateway für ausgehende Zugriffe stellt einem Namensraum ein festes, routbares IP zur Verfügung. Sämtlicher ausgehender Abschnittsdatenverkehr von einem Namensraum mit zugewiesener routbarer IP-Adresse fällt unter die von diesem Namensraum getätigten Zugriffe. Dies ermöglicht dem Cluster die sichere Skalierung, während die begrenzte Anzahl routbarer IPs beibehalten und nicht routbare IPs für den restlichen Datenverkehr aus dem Abschnitt des Clusters verwendet werden.

Universelle Firewall-Integration

Der Einsatz traditioneller Firewalls in Kubernetes ist eine Herausforderung, da Firewallregeln auf feste Quell- und Ziel-IP-Adressen angewiesen sind. Calico ausgehender Gateway funktioniert mit jeder Firewall, indem er Kubernetes-Ressourcen den sicheren Zugriff auf Endpunkte hinter einer Firewall ermöglicht. Durch diese Integration können Firewalls ihre zonenbasierenden Architekturen (trusted/untrusted/DMZ) auf Kubernetes erweitern. Tigeras Calico-Fortinet-Integration ermöglicht es Fortinet-Kunden, vorhandene Fortinet-Lösungen zu nutzen, um Sicherheits- und Compliance-Anforderungen umzusetzen und cloudnative Kubernetes-Zugriffe mittels der vertrauten Tools, Prozessen und Sicherheitsworkflows zu schützen, die Sie aus der kubernetesfremden Welt kennen.

Identitätsbewusste Mikrosegmentierung

Standardmäßig ist laterale Kommunikation zwischen Kubernetes-Clusters nicht gesichert. Calico erzwingt die Mikrosegmentation, um Zugriffe voneinander abzuschirmen und laterale Kommunikation zwischen Abschnitten, Namensräumen und Diensten abzusichern. Es erlaubt es Teams, Zugriffe logisch in verschiedene Sicherheitssegmente zu unterteilen und für diese dann individuelle, feingranulare Sicherheitsregeln zu definieren. Teams erreichen Zugriffsisolierung basierend auf Umgebungen, Applikationsebenen, Complianceanforderungen, Nutzerzugriffen sowie individuellen Anforderungen.

Sicherheitsrichtlinienverwaltung

Calico bietet ein Richtlinien-Framework, um Sicherheitsrichtlinien zu erstellen, zu testen, bereitzustellen und zu verwalten. Es empfiehlt Richtlinien und bietet hierarchische Richtlinienebenen sowie ein Dashboard zur Stärkung des Kubernetes-Clusters und der Zugriffssicherheit für gemeinsam genutzte Kubernetes-Umgebungen, auch über verschiedene Arbeitsgruppen unterschiedlicher Organisationen. Calico lässt Plattform-, Sicherheits- und Anwendungsteams die Freiheit, Cluster, Namensräume und zugriffsspezifische Richtlinien zu erstellen und in Betrieb zu nehmen. Die Benutzer erhalten Metriken zur Auswertung der Richtlinien innerhalb und über Richtlinienebenen hinweg in Echtzeit. Es sind alle aktiven und inaktiven Sicherheitsrichtlinien für den eigenen Kubernetes-Cluster in einem Interface einzusehen, mit einer rollen- und berechtigungsbasierten Hierarchie.

Überwachbarkeit und Fehlerbehebung

Calicos dynamische Dienst- und Bedrohungsgrafik bietet eine grafische Veranschaulichung Ihrer Kubernetes-Bereitstellungen, wie z.B. Abbilder, Abschnitte, Namensräume und Dienste. Es verfügt über Fehlerbehebungsfunktionen zur Erkennung und Behebung von Sicherheits- und Compliancelücken, Performanceproblemen, Konnektivitätsverlusten, anomalem Verhalten und Verletzungen von Sicherheitsrichtlinien. Beispielsweise ist dynamische Paketerfassung in die Grafik „Dynamische Dienste und Bedrohungen“ integriert, um einen schnelleren, Kubernetes-nativen Weg zu bieten, Performance-Hotspots und Konnektivitätsprobleme zu beheben, indem Pakete von einem bestimmten Abschnitt oder einer bestimmten Abschnittssammlung mit bestimmter Paketgröße und Dauer erfasst werden.

Datenflussverschlüsselung mit Hilfe von WireGuard

Calico setzt für die Datenflussverschlüsselung auf WireGuard. WireGuard läuft als Modul im Linux-Kernel für bessere Performance und niedrigere CPU-Beanspruchung. Die Calico-Verschlüsselung reduziert gegenüber Standard-Verschlüsselungslösungen die Betriebskomplexität für die Teams. Es kann verwendet werden, um Regulierungsauflagen hinsichtlich Verschlüsselung z.B. SOX, HIPAA, GDPR und PCI DSS, zu erfüllen.

Kubernetes-Sicherheitslagenmanagement (KSPM)

Calico bewertet Ihre Kubernetes-Umgebung gegen branchenübliche CIS-Benchmarks, um Fehlkonfigurationen über Ihre dynamischen Kubernetes-Umgebungen hinweg zu erkennen. Diese Funktion umfasst eine regelmäßige Auswertung, die bei Audits die Erfüllung des CIS-Benchmark über alle dynamischen Assets in Ihrer Kubernetes-Umgebung hinweg belegt. Es ist eine Gesamtbewertung für jedes In-Scope-Asset verfügbar, bei der konfigurierbare Grenzwerte darüber entscheiden, ob der Test bestanden wurde. Calico analysiert auch die Einstellungen von Kubernetes' rollenbasierender Zugriffskontrolle (RBAC) und Abschnittssicherheitsrichtlinie (PSP), um von Ihrer Kubernetes-Umgebung ausgehende Risiken zu erkennen.

Compliance (PCI DSS, SOC 2, GDPR, HIPAA, benutzerdefinierte Frameworks und vieles mehr)

Calico-Cloud unterstützt führende Compliancestandards wie PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA sowie benutzerdefinierte Frameworks. Es bietet permanente Echtzeitüberwachung, um Complianceverletzungen zu erkennen und kann auditfertige Berichte erzeugen. Calico erlaubt es Ihnen, Compliancekontrollen zu coden, so dass ständig Daten gesammelt, in Beziehung zueinander gesetzt und aufbereitet werden können, um die Compliance jederzeit belegen zu können. Die Plattform überwacht und protokolliert ebenfalls alle Änderungen an den Compliancerichtlinien.

Clustermesh

Calico bietet eine zentrale Multi-Cluster-Verwaltungsansicht, um Sicherheit, Beobachtbarkeit sowie erweitertes Networking für Zugriffe und Dienste über verschiedene Cluster hinweg in Hybrid- und Multi-Cloud-Umgebungen zu ermöglichen. Calico bietet eine einheitliche Sicherheitsrichtlinienkontrolle sowie Zusammenschlüsse von Endpunkten und Diensten.

Kunden

NBC UNIVERSAL · SIEMENS Healthineers · RBC Royal Bank · DISCOVER · Bloomberg · MERCK · upwork

Sammeln Sie praktische Erfahrungen auf unseren bald stattfindenden Webinaren und Live-Online-Workshops.

Los geht's

TIGERA

Tigera, Inc.

58 Maiden Lane, Fl 5
San Francisco, CA 94108
+1 (415) 612-9546 / www.tigera.io