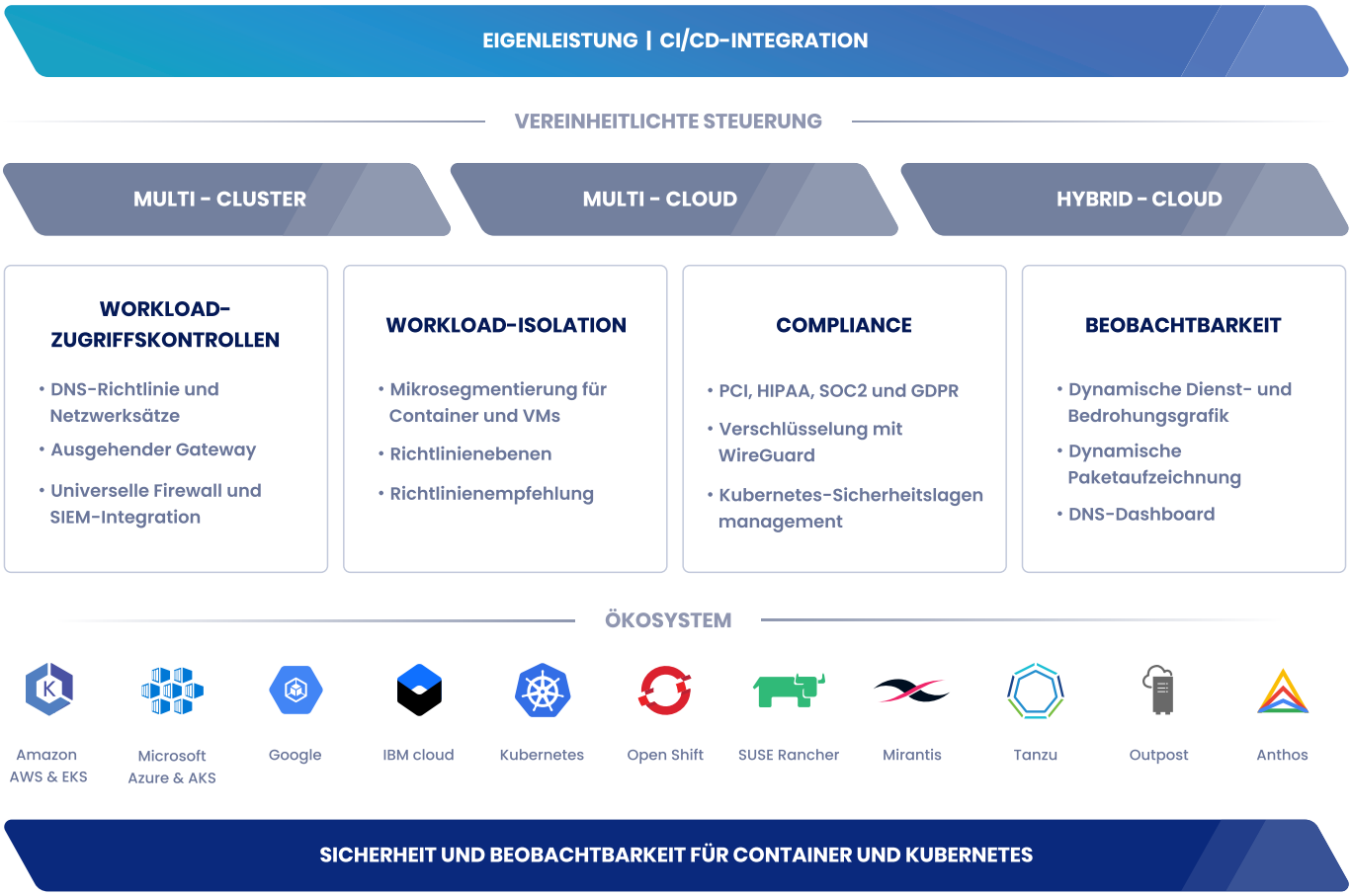
Zero-Trust-Sicherheit für Red Hat OpenShift mit Calico

Reduzieren Sie die Angriffsfläche und minimieren Sie Sicherheitsverletzungen

Übersicht

Cloudplattformingenieure sind mit der Erstellung und Pflege einer sicheren Red-Hat-OpenShift-Plattform beauftragt, sodass Entwickler sich auf die Schaffung von Applikationen konzentrieren können. Calico unterstützt Zero-Trust-Sicherheit, damit Plattformingenieure die Angriffsfläche mikrodienstbasierter Applikationen reduzieren, Sicherheitsverletzungen bekämpfen und Zero-Trust-basierte Defense-in-Depth-Unterstützung für cloudnative Applikationen auf Red Hat OpenShift liefern können.



Eigenschaften und Funktionen

Zero-Trust-Zugriffskontrollen

Calico bietet fein abgestimmte Zero-Trust-Zugriffskontrollen zwischen verschiedenen Abschnitten, Namensräumen und Diensten in Kubernetes-Clustern und externen Ressourcen wie z.B. Datenbanken, internen Applikationen, 3rd-Party-Cloud-APIs und SaaS-Applikationen. Es erlaubt zwei Wege, fein abgestimmte Zugriffskontrollen zu konfigurieren: mittels abgehender DNS-Anfragen und NetworkSets (bei Verwendung von IPs/CIDRs in der Richtlinie). Calicos Zugriffskontrolle sichert die gesamte Kommunikation zwischen Red-Hat-OpenShift-Clustern und externen Ressourcen, um Übernahmen und Angriffe zu verhindern.

Ausgehender Gateway

Da die Abschnitte eines Red-Hat-OpenShift-Clusters dynamisch und kurzlebig sind und keine feste IP-Adresse haben, können Zugriffe aus Abschnitten innerhalb des Clusters auf externe Ressourcen nicht mittels einer traditionellen Firewall abgesichert werden. Calico bietet einen ausgehenden Gateway, der Abschnitten statische IPs vergibt, damit Firewalls außerhalb des Red-Hat-OpenShift-Clusters in der Lage sind, die Abschnitte zu identifizieren und entsprechende Sicherheitsprüfungen durchzuführen. 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

Calicos ausgehender Gateway funktioniert mit jeder Firewall z.B. Palo Alto Networks, Fortinet, Check Point usw. Sie können Ihren Unternehmensfirewallmanager verwenden, um eine zonenbasierende Architektur für Ihren Openshift-Cluster zu schaffen. Calico liest diese Firewallregeln ein und übersetzt sie in Kubernetes-Sicherheitsrichtlinien, die den Datenverkehr zwischen Mikrodiensten steuern. Der Firewallmanager kann dazu verwendet werden, das Durchqueren von Zonen explizit bestimmten Mikrodiensten in OpenShift-Clustern zu erlauben und lässt das Netzwerksicherheitsteam so die zur Beibehaltung der Compliance erforderliche Konfiguration tätigen.

Identitätsbewusste Mikrosegmentierung

Standardmäßig ist laterale Kommunikation zwischen Kubernetes-Clusters nicht gesichert. Calico erzwingt die identitätsbewusste Mikrosegmentation, um Zugriffe voneinander abzuschirmen und laterale Kommunikation zwischen Abschnitten, Namensräumen und Diensten abzusichern. Es werden Labels und Dienstaccounts verwendet, um die Identität eines jeden Zugriffs festzustellen. Calicos Mikrosegmentierung funktioniert über verschiedene Netzwerk- und Applikationsebenenprotokolle hinweg und verwendet ein auf Zugriffs-Metadaten (Abschnittsname, Namensraum, Knoten, Labels und Kommentare) basierendes, dynamisches Zugriffssegmentierungsmodell. Sie können in Ihren OpenShift-Clustern Zugriffe schnell skalieren (im Millisekundenbereich), ohne Sicherheitsrichtlinien zu ändern, sondern einfach durch Verwendung der entsprechenden Labels beim Bereitstellen neuer Zugriffe.

Richtlinienebenen

Calico erlaubt es Red-Hat-OpenShift-Plattformsteams, Sicherheitsrichtlinien zu definieren, die in einer bestimmten Sequenz die Richtlinien anderer Benutzer überschreiben, ohne dass eine bestehende Richtlinie tatsächlich überschrieben oder die höherpriore Richtlinie übergangen werden muss. Es unterstützt die Abtretung von Kompetenzen innerhalb der Organisationsstruktur und dem Zuständigkeitsbereich (Plattform, Sicherheit, DevOps und Standard) laut den rollenbasierten Kubernetes-Zugriffskontrollen (RBAC). Mit Calicos Richtlinienebenen können OpenShift-Plattformteams unternehmensweite Richtlinien ausrollen, die jede applikationsspezifische Richtlinie überschreiben und so durchgängig die Compliance sicherstellen.

Richtlinienempfehlung

Calicos Richtlinienempfehler inspiziert den Datenverkehr innerhalb von Red-Hat-OpenShift-Clustern und empfiehlt angebrachte Sicherheitsrichtlinien auf Zugriffs- und Namensraumebene, um den Datenverkehr abzusichern. Diese Richtlinien können vor der Bereitstellung oder Durchsetzung angesehen und bearbeitet werden. Mit Calicos Richtlinienempfehler können OpenShift-Plattformteams Richtlinien erstellen, anschauen, bereitstellen und verwalten, ohne eine einzige Zeile Code zu schreiben.

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

Calico unterstützt führende Compliancestandards wie PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA sowie benutzerdefinierte Frameworks. Es überwacht kontinuierlich OpenShift-Cluster und die Zugriffe auf diese auf Complianceverstöße, bietet die Möglichkeit, ganz einfach präsentierbare Berichte zu erzeugen und erlaubt Complianceüberwachung und -Berichterstattung in Echtzeit. 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. Calico überwacht und protokolliert ebenfalls alle Änderungen an den Compliancerichtlinien.

Kubernetes-Sicherheitslagenmanagement (KSPM)

Calicos Konfigurationssicherheitsfunktion bewertet Ihre OpenShift-Umgebung gegen branchenübliche CIS-Benchmarks für Kubernetes zur Erkennung von Fehlkonfigurationen. Diese Funktion umfasst eine regelmäßige Auswertung, die bei Audits die Erfüllung des CIS-Benchmark über alle dynamischen Assets in Ihrer OpenShift-Umgebung hinweg belegt. Organisationen können einen Grenzwert konfigurieren, der darüber entscheidet, ob der Test bestanden wurde, um die Sicherheitsvoraussetzungen des Unternehmens einzuhalten. Calico analysiert auch die Einstellungen von Kubernetes‘ RBAC und Abschnittssicherheitsrichtlinie (PSP), um von Ihrer OpenShift-Umgebung ausgehende Risiken zu erkennen.

Überwachbarkeit und Fehlerbehebung

Calico veranschaulicht grafisch Ihre OpenShift-Bereitstellungen, inklusive Abschnitten, Namensräumen und Diensten und bietet zugleich die Möglichkeit, mittels integrierter Tools Sicherheits- und Überwachungslücken, Performanceprobleme, Konnektivitätsverluste, anomales Verhalten und Sicherheitsrichtlinienverstöße zu erkennen und beheben. Calicos dynamische Dienste- und Bedrohungsgrafik bietet zur Laufzeit Sichtbarkeit über den gesamten Stack hinweg, von der Netzwerkebene zur Anwendungsebene, und zeigt, wie Namensräume, Dienste und Abschnitte in Ihrem OpenShift-Cluster laufen sowie die aktuell in Ihrer Umgebung vorhandenen Risiken. Es verfügt außerdem über Dynamic Packet Capture — ein Kubernetes-nativer Weg zur schnelleren Bekämpfung von Performance-Hotspots und Konnektivitätsproblemen durch das Erfassen von Paketen von einem bestimmten Abschnitt oder einer bestimmten Abschnittssammlung mit bestimmten Paketgrößen, Ports, Protokoll und Dauer.

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. Verglichen mit Standardlösungen beseitigt Calico-Verschlüsselung für DevOps und Sicherheitsteams die Betriebskomplexität enorm und kann dazu verwendet werden, Regulierungsaufträge hinsichtlich Verschlüsselung zu erfüllen, z.B. SOX, HIPAA, GDPR und PCI DSS.

Kunden

MARSH & McLENNAN COMPANIES · MEDIDATA · MERCK · opensource.com · orange™ · VERISIGN · SPRIBE

Möchten Sie mehr darüber erfahren? Probieren Sie die Calico-Cloud kostenfrei aus.

Los geht‘s

Tigera. San Francisco, CA | San Jose, CA | Cork, Ireland | Vancouver, Canada | London, UK