FICHE TECHNIQUE DE LA SOLUTION

Calico pour la sécurité Kubernetes

Kubernetes est la plate-forme de facto pour orchestrer les charges de travail et les services conteneurisés pour les déploiements hybrides et multi-cloud et les environnements multi-cluster, qui sont tous les éléments constitutifs des applications cloud natives.

Défis de sécurité

Les charges de travail Kubernetes sont hautement dynamiques, éphémères et sont déployées sur une infrastructure cloud distribuée et agile, telle que Red Hat OpenShift, SUSE Rancher, Amazon EKS et Microsoft AKS. Par conséquent, les architectes et les ingénieurs de la plate-forme cloud doivent relever de nombreux défis de sécurité lors du déploiement de charges de travail sur Kubernetes.

- Sécuriser la communication de charge de travail avec les ressources extérieures au cluster.
- Activer l'accès sécurisé aux ressources derrière les pare-feux traditionnels.
- Isoler les applications et charges de travail en segmentant le cluster Kubernetes.
- Donner une visibilité sur les stratégies de sécurité actives et inactives et les failles de sécurité dans le cluster.
- S'assurer que la configuration de Kubernetes conforme aux références du secteur telles que CIS pour Kubernetes.
- Assurer la conformité avec les réglementations telles que SOC 2, PCI DSS, HIPAA, etc.
- Simplifier l'administration des stratégies de sécurité avec un flux de travail automatisé de bout en bout pour créer, organiser, mettre à jour et supprimer les stratégies de sécurité.
- Activer la connectivité et la communication sécurisée entre les charges de travail et les services à travers plusieurs clusters.
- Créer des services partagés à travers plusieurs clusters Kubernetes.

Comment Calico peut vous aider

Réduire la surface d'attaque	Visibilité et conformité	Contrôles de sécurité unifiés
Sécuriser l'accès aux pods et communication à l'intérieur et à l'extérieur du cluster pour atténuer les attaques	Bénéficier d'une visibilité du trafic de bout en bout pour identifier les failles de sécurité, la connectivité des services et les problèmes de performances	Panneau de verre unique pour gérer les stratégies de sécurité à travers les environnements Kubernetes multi-cloud et multi-cluster

Calico est la seule plate-forme de sécurité active du secteur avec une observabilité complète de la pile, qui répond aux exigences de sécurité des clusters et des charges de travail Kubernetes. Tigera propose Calico sous la forme d'un SaaS entièrement géré (**Calico Cloud**) ou d'un service autogéré (**Calico Enterprise**). Les deux plates-formes Calico aident les organisations à gérer les contrôles de sécurité à travers plusieurs applications, clusters et environnements.

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

Copyright © 2023 Tigera, Inc. All rights reserved

Mettre en œuvre la sécurité Kubernetes avec Calico

Contrôles d'accès aux charges de travail confiance zéro

Calico donne des contrôles d'accès granulaires en confiance zéro à la charge de travail entre les pods individuels des clusters Kubernetes et les ressources externes, y compris les bases de données, les applications internes, les API cloud tierces et les applications SaaS. Il donne des contrôles d'accès précis à la charge de travail à l'aide de politiques de sortie DNS et NetworkSets (en utilisant des adresses IP/CIDR dans la politique réseau).

Passerelle de sortie

Les passerelles de sortie vous permettent d'identifier la source du trafic au niveau de l'espace de noms ou du pod lorsqu'il quitte un cluster Kubernetes pour communiquer avec des ressources externes. Il est donc très avantageux pour les équipes de sécurité d'appliquer des contrôles d'accès à un trafic spécifique, au lieu d'ouvrir un plus grand ensemble d'adresses IP. La passerelle d'accès de sortie Calico attribue une adresse IP fixe et routable à un espace de noms Kubernetes. Tout le trafic de pod de sortie de cet espace de noms avec une adresse IP routable attribuée, identifie la charge de travail en cours d'exécution dans cet espace de noms. Cela permet au cluster d'évoluer en toute sécurité, tout en préservant le nombre limité d'adresses IP routables, et en tirant parti des adresses IP non routables pour tout autre trafic de pod au sein du cluster.

Copyright © 2023 Tigera, Inc. All rights reserved

Intégration de pare-feu universel

Le déploiement de pare-feu traditionnels sur Kubernetes est un défi, car les règles de pare-feu nécessitent une source statique et adresse IP de destination. La passerelle de sortie Calico fonctionne avec n'importe quel pare-feu, permettant aux ressources Kubernetes d'accéder en toute sécurité aux points de terminaison derrière un pare-feu. Grâce à cette intégration, les pares-feux peuvent étendre leurs architectures basées sur des zones (approuvées, non approuvées, DMZ) à Kubernetes. L'intégration Calico-Fortinet de Tigera permet aux clients Fortinet de tirer parti des investissements existants dans les solutions Fortinet pour faire respecter les exigences de sécurité et conformité, et protéger les charges de travail Kubernetes cloud natives en utilisant les mêmes outils, processus et flux de travail de sécurité que vous connaissez et utilisez pour protéger vos charges de travail non-Kubernetes.

Microsegmentation basée sur l'identité

Par défaut, la communication latérale entre les charges de travail au sein des clusters Kubernetes n'est pas sécurisée. Calico applique la microsegmentation pour isoler la charge de travail et sécuriser la communication latérale entre les pods, espaces de noms et services. Il permet aux équipes de diviser logiquement les charges de travail en segments de sécurité distincts, puis définir des contrôles de sécurité granulaires pour chaque segment unique. Les équipes peuvent isoler les charges de travail en fonction des environnements, niveaux d'application, besoins de conformité, l'accès des utilisateurs et exigences de charge de travail individuelles.

Gestion de la stratégie de sécurité

Calico fournit un cadre de stratégie pour créer, tester, déployer et gérer des stratégies de sécurité. Il vous recommande des stratégies, fournit des niveaux de stratégie hiérarchiques et un tableau de bord des stratégies pour renforcer la sécurité du cluster Kubernetes, et des charges de travail pour l'environnement Kubernetes partagé entre plusieurs équipes avec différentes parties prenantes. Calico offre aux équipes de plate-forme, sécurité et application, l'autonomie nécessaire pour créer et déployer des stratégies spécifiques au cluster, à l'espace de noms et à la charge de travail. Les utilisateurs obtiennent des métriques en temps réel sur la façon dont les stratégies sont évaluées au sein et entre les niveaux de stratégie. Ils peuvent afficher toutes les stratégies de sécurité actives et inactives pour leur cluster Kubernetes avec une hiérarchie basée sur les rôles et autorisations sur une seule interface.

Observabilité et dépannage

Le Dynamic Service et Threat Graph de Calico donne une visualisation graphique de vos déploiements Kubernetes, y compris des images, pods, espaces de noms et services. Il dispose de capacités de dépannage intégrées pour identifier et résoudre les failles de sécurité et conformité, problèmes de performances, pannes de connectivité, comportements anormaux et violations des stratégies de sécurité. Par exemple, la capture dynamique de paquets est intégrée dans Dynamic Service et Threat Graph pour donner un moyen natif Kubernetes, et plus rapide, de dépanner les points chauds de performance et problèmes de connectivité, en capturant des paquets à partir d'un pod spécifique ou d'un ensemble de pods utilisant des tailles et durées de paquet spécifiées.

Chiffrement des données en transit avec WireGuard

Calico utilise WireGuard pour mettre en œuvre le chiffrement des données en transit. WireGuard s'exécute en tant que module dans le noyau Linux pour offrir de meilleures performances et une consommation CPU plus faible. Le chiffrement Calico élimine la complexité opérationnelle pour les équipes par rapport aux méthodes de chiffrement habituelles. Il peut être utilisé pour répondre aux mandats réglementaires qui spécifient l'utilisation du chiffrement, y compris SOX, HIPAA, GDPR et PCI DSS.

Copyright © 2023 Tigera, Inc. All rights reserved

Gestion de la posture de sécurité Kubernetes (GPSK)

Calico évalue votre environnement Kubernetes contre les normes de références CIS de l'industrie pour identifier les erreurs de configuration à travers vos environnements Kubernetes. Cette fonctionnalité inclut un rapport d'évaluation régulier, qui montre la conformité aux normes de référence CIS pour tous les actifs dynamiques de votre environnement Kubernetes pendant la période de référence. Une note globale est disponible pour chaque actif concerné, qui peut être comparée à des seuils configurables de réussite/échec. Calico analyse également les paramètres de contrôles d'accès en fonction des rôles (CAFR) et la stratégie de sécurité des pods (SSP) de Kubernetes pour détecter les risques au sein de votre environnement Kubernetes.

Conformité (PCI DSS, SOC 2, GDPR, HIPAA, cadres personnalisés, etc.)

Calico Cloud prend en charge les principales normes de conformité, notamment PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA et tout cadre personnalisé. Il fournit une surveillance continue en temps réel pour détecter les violations de conformité et peut générer des rapports prêts pour l'audit. Calico vous permet d'écrire des contrôles de conformité sous forme de code, ce qui vous permet de collecter, corréler et préparer les données en permanence pour fournir une preuve de conformité à tout moment. La plate-forme surveille et enregistre également toutes les modifications apportées aux politiques de conformité.

Clustermesh

Calico fournit un plan de gestion multi-cluster centralisé pour permettre la sécurité, l'observabilité et la mise en réseau avancée pour les charges de travail et services sur plusieurs clusters dans des environnements hybrides et multi-cloud. Calico fournit des contrôles de stratégie de sécurité unifiés et des terminaux et services fédérés.

Clients

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

Bénéficiez d'une expérience pratique grâce à nos prochains webinaires et ateliers en ligne en direct.

Démarrez

TIGERA

Tigera, Inc.

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

"Tigera", the Tigera logo, Calico and Calico Cloud are trademarks of Tigera, Inc. All rights reserved. Other trademarks are the property of their respective owners. For more information, email us at contact@tigera.io.

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

Copyright © 2023 Tigera, Inc. All rights reserved