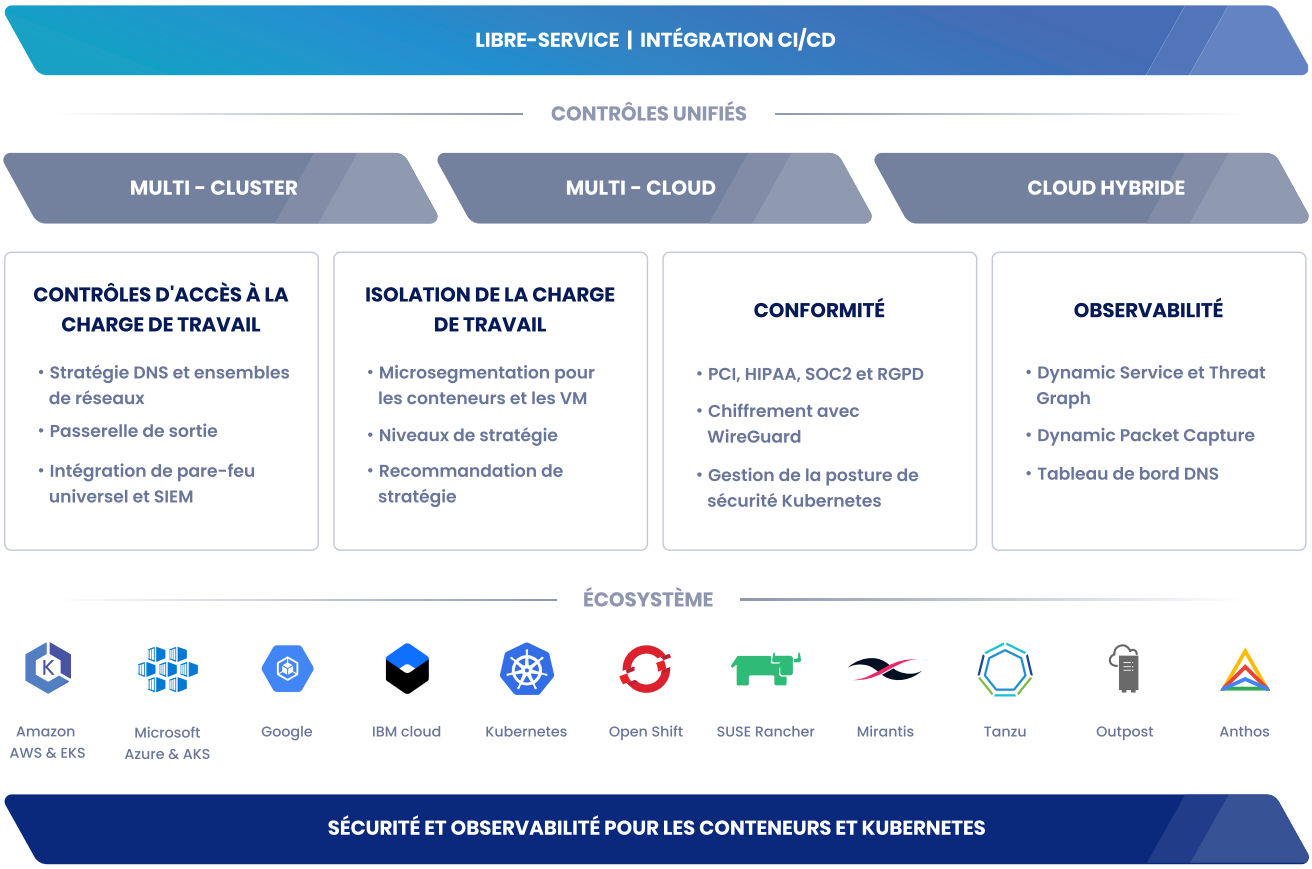
Sécurité confiance zéro pour Red Hat OpenShift avec Calico

Réduire la surface d'attaque et atténuer les failles de sécurité

Aperçu

Les ingénieurs de la plate-forme cloud sont chargés de créer et maintenir une plate-forme Red Hat OpenShift sécurisée afin que les développeurs puissent se concentrer sur la création d'applications. Calico fournit une sécurité confiance zéro pour permettre aux ingénieurs de plate-forme de réduire la surface d'attaque des applications basées sur les microservices, atténuer les failles de sécurité et fournir une capacité de défense en profondeur basée sur confiance zéro pour les applications cloud natives sur Red Hat OpenShift.



Fonctionnalités et capacités

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 offre deux façons d'activer 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). Les contrôles d'accès aux charges de travail de Calico sécurisent toutes les communications entre les clusters Red Hat OpenShift et les ressources externes pour empêcher toute attaque de commande et de contrôle.

Passerelle de sortie

Étant donné que les pods d'un cluster Red Hat OpenShift sont dynamiques, éphémères et n'ont pas d'adresse IP fixe, l'accès des pods du cluster aux ressources extérieures au cluster ne peut pas être sécurisé à l'aide d'un pare-feu traditionnel. Calico fournit une passerelle de sortie qui attribue des adresses IP statiques aux pods pour permettre aux pares-feux à l'extérieurs du cluster Red Hat OpenShift d'identifier ces pods et d'appliquer les contrôles de sécurité appropriés. 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.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.

Intégration de pare-feu universel

La passerelle de sortie Calico fonctionne avec n'importe quel pare-feu, y compris Palo Alto Networks, Fortinet, Check Point et autres. Les gestionnaires de pare-feu d'entreprise peuvent être utilisés pour créer une architecture basée sur les zones pour votre cluster Openshift. Calico lit ces règles de pare-feu et les transforme en stratégies de sécurité Kubernetes qui contrôlent le trafic entre les microservices. Le gestionnaire de pare-feu peut être utilisé pour autoriser explicitement la liste des microservices des clusters OpenShift autorisés à traverser les zones, fournissant à l'équipe de sécurité du réseau les contrôles dont elle a besoin pour maintenir la conformité.

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 basée sur l'identité pour isoler la charge de travail et sécuriser la communication latérale entre les pods, espaces de noms et services. Les étiquettes et comptes de service sont utilisés pour établir l'identité de chaque charge de travail. La microsegmentation de Calico fonctionne sur les protocoles réseau et couche application, et utilise un modèle de segmentation dynamique de la charge de travail basé sur les métadonnées (nom de pod, espace de noms, nœud, étiquettes et annotations) attachées à chaque charge de travail. Vous pouvez rapidement faire évoluer les charges de travail en quelques millisecondes dans vos clusters OpenShift sans avoir à modifier les stratégies de sécurité, mais en utilisant simplement les étiquettes appropriées lors du déploiement de nouvelles charges de travail.

Hiérarchisation des politiques

Calico permet aux équipes de la plate-forme Red Hat OpenShift de définir des stratégies de sécurité qui prévalent sur les politiques des autres utilisateurs dans une séquence particulière, sans écraser une politique existante ni ignorer la politique la plus prioritaire. Il prend en charge la délégation d'autorité par la structure organisationnelle et domaine de responsabilité (plate-forme, sécurité, DevOps et par défaut) définis avec les contrôles d'accès en fonction des rôles Kubernetes (CAFR). Grâce à la hiérarchisation des politiques de Calico, les équipes de la plate-forme OpenShift peuvent appliquer des politiques à l'échelle de l'entreprise qui prévalent sur toute politique spécifique à l'application, garantissant ainsi une conformité continue.

Recommandation politique

L'outil de recommandation de politiques Calico inspecte le trafic au sein des clusters Red Hat OpenShift et recommande des stratégies de sécurité appropriées au niveau de la charge de travail et l'espace de noms pour sécuriser le trafic. Ces politiques peuvent être révisées et modifiées avant la mise en place ou l'application. Avec l'outil de recommandation de politiques Calico, les équipes de la plateforme OpenShift peuvent créer, prévisualiser, déployer et gérer des politiques sans écrire une seule ligne de code.

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

Calico prend en charge les principales normes de conformité, notamment PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA et tout cadre personnalisé. Il surveille en permanence les clusters OpenShift et les charges de travail à l'intérieur des clusters pour détecter les violations de conformité, offre la possibilité de créer facilement des rapports prêts pour l'audit, et fournit une surveillance et des rapports de conformité en temps réel pour garantir l'application. Calico vous permet d'écrire des contrôles de conformité sous forme de code, et il collecte, corrèle et prépare en continu les données pour fournir une preuve de conformité. Calico surveille et enregistre également toutes les modifications apportées aux politiques de conformité.

Gestion de la posture de sécurité Kubernetes (GPSK)

La fonctionnalité de sécurité de la configuration de Calico évalue votre environnement OpenShift par rapport aux normes de références CIS de l'industrie pour Kubernetes afin d'identifier les erreurs de configuration. Cette fonctionnalité inclut un rapport d'évaluation régulier qui montre la conformité aux normes de référence CIS pour tous les actifs dynamiques qui ont pu exister dans votre environnement OpenShift pendant la période du rapport. Les organisations peuvent définir des seuils configurables de réussite/échec pour s'aligner avec les besoins de sécurité de l'entreprise. Calico analyse également Kubernetes CAFR et les paramètres de stratégie de sécurité des pods (SSP) pour détecter les risques au sein de votre environnement Red Hat OpenShift.

Observabilité et dépannage

Calico fournit une visualisation graphique de vos déploiements OpenShift, y compris des pods, espaces de noms et services, avec des outils de dépannage intégrés pour identifier et résoudre les failles de sécurité et d'audit, problèmes de performances, pannes de connectivité, comportements anormaux et violations des stratégies de sécurité. Le Dynamic Service et Threat Graph de Calico offre une visibilité d'exécution sur la pile, de la couche réseau à la couche application, montrant comment les espaces de noms, services et pods fonctionnent dans votre cluster OpenShift et les risques présents dans votre environnement. Il dispose également de Dynamic Packet Capture, un moyen natif de Kubernetes pour résoudre plus rapidement les points chauds de performances et problèmes de connectivité en capturant des paquets à partir d'un pod spécifique ou d'un ensemble de pods avec des tailles de paquets, ports, protocoles et durées spécifiés.

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. Par rapport aux méthodes habituelles, le chiffrement Calico élimine la complexité opérationnelle pour les équipes de DevOps et sécurité, et il peut être utilisé pour répondre aux mandats réglementaires qui spécifient l'utilisation du chiffrement, y compris SOX, HIPAA, GDPR et PCI DSS.

Clients

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

Voulez-vous en savoir plus ? Testez gratuitement Calico Cloud.

Démarrez