Calico Cloud: Sécurité active des conteneurs prêt à l'emploi

Les applications cloud natives exécutées sur des conteneurs et Kubernetes sont exposées à une large surface d'attaque tout au long du cycle de vie de l'application, du développement au déploiement et à la production. Cette grande surface d'attaque, en combinaison avec la nature hautement dynamique et éphémère des charges de travail cloud natives, exige un autre type de posture de sécurité.

Calico Cloud est une plate-forme de sécurité de conteneur de nouvelle génération qui équilibre la prévention et l'atténuation des risques avec la détection des menaces pour réduire la surface d'attaque, détecter activement les menaces et déployer des contrôles de sécurité d'atténuation afin de limiter les risques d'exposition. Calico est la seule plate-forme de sécurité active du secteur avec une observabilité complète de la pile. Il permet aux organisations de prévenir les attaques à l'aide de la confiance zéro, et de détecter, dépanner et corriger automatiquement les risques d'exposition aux failles de sécurité dans les déploiements multi-cloud et hybrides. Basé sur Calico Open Source, Calico Cloud est la solution de mise en réseau et de sécurité de conteneurs la plus largement adoptée.

Défis de sécurité

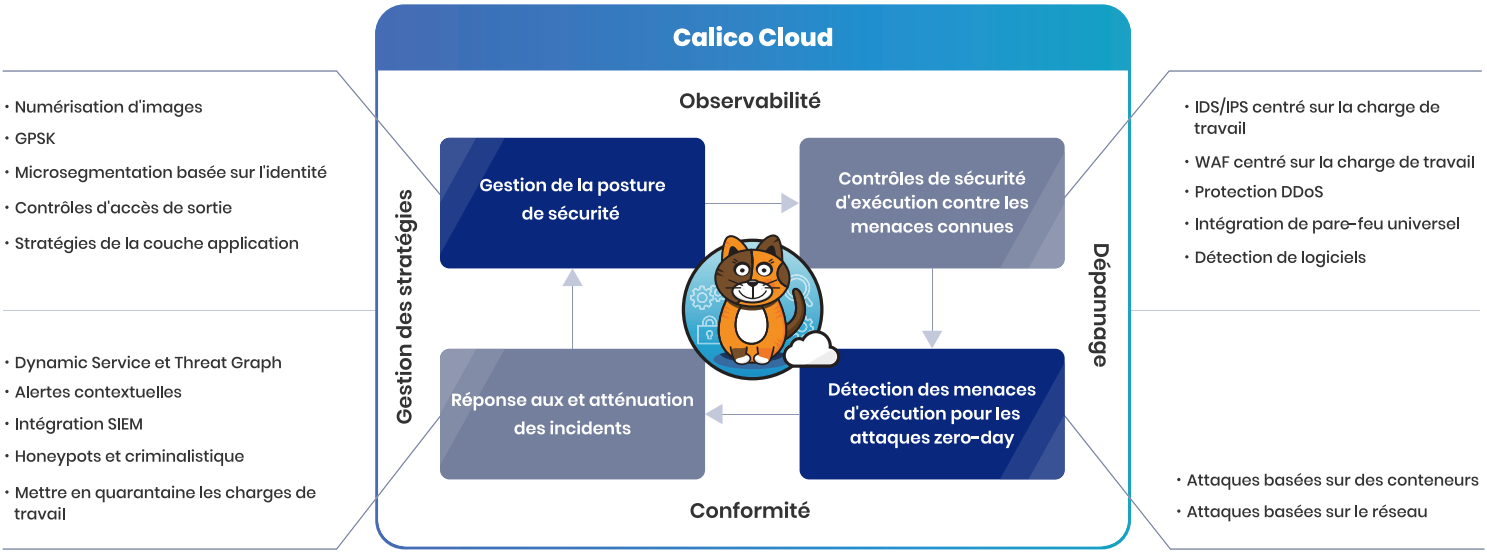
- Grande surface d'attaque tout au long du cycle de vie de l'application
- Le manque de visibilité crée des angles morts de sécurité
- La sécurité centrée sur la détection crée des faux positifs qui entraînent une fatigue des alertes et des équipes de sécurité surchargées
- La mise en conformité avec les réglementations telles que SOC 2, PCI DSS et HIPAA est fastidieuse
- Compte tenu du réseau Kubernetes plat, la sécurité périmétrique traditionnelle est dès lors inadéquate

Comment Calico peut vous aider

Calico est la seule plate-forme de sécurité active prêt à l'emploi du secteur avec une observabilité complète de la pile pour prévenir, détecter et atténuer les failles de sécurité dans les applications conteneurisées.

Réduire la surface d'attaqu	Détecter et arrêter les attaques	Atténuer activement les risques
Sécuriser l'accès aux charges de travail et communication à l'intérieur et à l'extérieur du cluster pour atténuer les attaques	Protéger les charges de travail contre les menaces connues et zero-day dans les conteneurs et le réseau pendant l'exécution	Déployer les contrôles de sécurité recommandés pour atténuer les risques d'exposition

Comment Calico transforme la sécurité des conteneurs



Une posture de sécurité solide pour les charges de travail conteneurisées

Gestion automatisée des vulnérabilités

Analyser en continu les images à la recherche des CVEs connus et empêcher le déploiement de charges de travail vulnérables à l'aide d'un pipeline CI/CD automatisé et entièrement intégré. Tirer parti de la vue d'exécution des charges de travail vulnérables pour évaluer les risques, et déployer des contrôles de sécurité atténuants afin de minimiser le rayon d'explosion.

Gestion de la posture de sécurité Kubernetes (GPSK)

Renforcer votre environnement Kubernetes par rapport aux normes de références CIS de l'industrie, afin d'identifier et corriger les erreurs de configuration dans vos environnements dynamiques Kubernetes.

Contrôles d'accès aux charges de travail confiance zéro

Déployer des contrôles d'accès granulaires en confiance zéro aux charges 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. Sécuriser les pods à l'aide de politiques de sortie DNS et NetworkSets précises.

Microsegmentation basée sur l'identité

Sécuriser la communication latérale entre les pods, espaces de noms et services. Réaliser l'isolation de la charge de travail en fonction des environnements, niveaux d'application, besoins de conformité, l'accès des utilisateurs et exigences de charge de travail individuelles.

Politiques de la couche application

Appliquer des politiques de couche application pour la microsegmentation et le contrôle d'accès avec des attributs spécifiques à L7 tels que les méthodes HTTP et les chemins d'URL.

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

Protection contre les menaces connues pendant l'exécution

IDS/IPS centré sur la charge de travail

Bloquer la communication vers les adresses IP connues comme malveillantes et recevoir des alertes sur les domaines suspects grâce à l'intégration du flux mondial de renseignements sur les menaces.

WAF centré sur la charge de travail

Protéger les charges de travail contre les attaques basées sur HTTP telles que OWASP Top Ten et d'autres en-têtes HTTP non conformes, en particulier pour les communications latérales.

Détection des logiciels malveillants

Détecter et alerter sur les logiciels malveillants connus grâce à une approche basée sur les signatures. Découvrir les rançongiciels et les incidents de crypto-minage avec des capacités de détection et alertes organisées.

Protection DDoS

Prévenir et atténuer les attaques DDoS avec des stratégies de sécurité aux niveaux de l'hôte et l'application.

Intégration de pare-feu universel

Étendre les architectures basées sur des zones (approuvées, non approuvées, DMZ) à Kubernetes. 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.

Protection contre les menaces zero-day pendant l'exécution

Détecter les attaques zero-day avec la détection d'anomalies basée sur le réseau

Bloquer les attaques zero-day grâce à l'apprentissage heuristique de l'activité anormale du réseau. Détecter les indicateurs d'attaque (IoA) à partir des journaux de flux réseau, DNS et HTTP.

Détecter les attaques zero-day avec la détection d'anomalies basée sur les conteneurs

Détectez les menaces zero-day avec des détecteurs prêts à l'emploi basés sur le comportement, qui analysent l'activité des conteneurs à l'aide de processus, système de fichiers et appels système collectés avec des sondes eBPF.

Réponse aux incidents et atténuation des risques

Observabilité et dépannage

Obtenir une visibilité complète avec une visualisation graphique de vos déploiements Kubernetes, y compris des images, pods, espaces de noms et services avec Dynamic Service et Threat Graph de Calico. Spécialement conçu avec des capacités de dépannage pour identifier et résoudre les failles de sécurité et conformité, problèmes de performances, pannes de connectivité, comportements anormaux et violations de la stratégie de sécurité.

Alerte et quarantaine

Afficher et gérer toutes les alertes actionnables liées à la sécurité, au réseau et aux performances à partir d'un tableau de bord d'alerte unique avec des filtres personnalisables. Appliquer des stratégies de quarantaine pour isoler les charges de travail vulnérables afin de permettre les efforts de correction.

Gestion et conformité

Chiffrement des données en transit avec WireGuard

Éliminer la complexité opérationnelle des méthodes de chiffrement habituelles grâce à l'intégration WireGuard de Calico. Répondre aux mandats réglementaires de chiffrement, y compris SOX, HIPAA, GDPR et PCI DSS.

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

Atteindre et maintenir la conformité avec une surveillance continue en temps réel pour détecter les violations, et générer des rapports prêts pour l'audit. Prendre en charge PCI DSS, HIPAA, GDPR, SOC 2, NIST, CCPA et tout cadre personnalisé.

Gestion de la stratégie de sécurité

Créer, mettre en œuvre, prévisualiser, appliquer et gérer des stratégies de sécurité avec notre cadre stratégique unifié. Calico recommande des stratégies et fournit des niveaux de stratégie hiérarchiques basés sur des rôles et autorisations. L'interface utilisateur du gestionnaire est fournie avec un tableau de bord permettant aux équipes de visualiser et de gérer facilement toutes les stratégies de sécurité actives et inactives dans le cluster Kubernetes.

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