FICHA TÉCNICA DE LA SOLUCIÓN

Calico para la seguridad de Kubernetes

Kubernetes es la plataforma de facto para orquestar cargas de trabajo en contenedores y servicios para despliegues híbridos y multinube y entornos multiclúster, todos ellos componentes básicos de las aplicaciones nativas de la nube.

Retos para la seguridad

Las cargas de trabajo de Kubernetes son muy dinámicas y efímeras, y se implantan en una infraestructura de nube distribuida y ágil, como Red Hat OpenShift, SUSE Rancher, Amazon EKS y Microsoft AKS. Como resultado, los arquitectos e ingenieros de plataformas en nube deben hacer frente a numerosos retos para la seguridad cuando despliegan cargas de trabajo en Kubernetes.

- Comunicar de forma segura la carga de trabajo con recursos externos al clúster.
- Permitir un acceso seguro a los recursos situados detrás de los cortafuegos tradicionales.
- Aislar las aplicaciones y las cargas de trabajo segmentando el clúster de Kubernetes.
- Proporcionar visibilidad de las políticas de seguridad activas e inactivas y de las brechas de seguridad en el clúster.
- Garantizar que la configuración de Kubernetes cumple las normas de referencia del sector, como CIS para Kubernetes.
- Lograr el cumplimiento de normativas como SOC2, PCI DSS, HIPAA y otras.
- Simplificar la administración de las políticas de seguridad con un flujo de trabajo automatizado de principio a fin para crear, escalonar, actualizar y eliminar políticas de seguridad.
- Permitir la conectividad y la comunicación segura entre cargas de trabajo y servicios a través de varios clústeres..
- Cree servicios compartidos en varios clústeres de Kubernetes.

Cómo ayuda Calico

Reducción de la superficie de ataque	Visibilidad y cumplimiento	Controles de seguridad unificados
Se asegura el acceso a los pods y la comunicación dentro y fuera del clúster para mitigar los ataques	Obtención de visibilidad del tráfico de extremo a extremo para identificar brechas en la seguridad, conectividad de servicios y problemas de rendimiento	Un único panel de vidrio para gestionar las políticas de seguridad en entornos Kubernetes multinube y multiclúster

Calico es la única plataforma de seguridad activa de la industria con observabilidad de pila completa que aborda los requisitos de seguridad de los clústeres de Kubernetes y de la carga de trabajo. Tigera ofrece Calico como SaaS totalmente gestionado (**Calico Cloud**) o como servicio autogestionado (**Calico Enterprise**). Ambas plataformas Calico ayudan a las organizaciones a gestionar los controles de seguridad en varias aplicaciones, clústeres y entornos.

Implementación de la seguridad de Kubernetes con Calico

Controles de acceso a la carga de trabajo de confianza cero

Calico proporciona controles de acceso a la carga de trabajo granulares y de confianza cero entre pods individuales en clústeres de Kubernetes a recursos externos, como bases de datos, aplicaciones internas, API en la nube de terceros y aplicaciones SaaS. Proporciona controles de acceso a la carga de trabajo de granularidad fina utilizando políticas de salida de DNS y NetworkSets (utilizando IP/CIDR en la política de redes).

Pasarelas de salida

Las pasarelas de salida le permiten identificar el origen del tráfico a nivel de espacio de nombres o pod cuando sale de un clúster de Kubernetes para comunicarse con recursos externos. Esto hace que sea muy beneficioso para los equipos de seguridad aplicar controles de acceso a un tráfico específico en lugar de abrir un conjunto más amplio de direcciones IP. La pasarela de enlace de acceso de salida de Calico asigna una IP fija y enrutable a un espacio de nombres de Kubernetes. Todo el tráfico de salida de pods de ese espacio de nombres con una dirección IP enrutable asignada identifica la carga de trabajo que se ejecuta dentro de ese espacio de nombres. Esto permite al clúster crecer o decrecer de forma segura preservando el número limitado de IP enrutables y aprovechando las IP no enrutables para el resto del tráfico de pods dentro del clúster.

Integración universal de cortafuegos

Desplegar cortafuegos tradicionales en Kubernetes es todo un reto, ya que las reglas del cortafuegos necesitan una dirección IP de origen y de destino estáticas. La puerta de enlace de salida Calico funciona con cualquier cortafuegos, lo que permite que los recursos de Kubernetes accedan de forma segura a los puntos finales situados detrás de un cortafuegos. Con esta integración, los cortafuegos logran extender sus arquitecturas basadas en zonas (fiables, no fiables y DMZ) a Kubernetes. La integración Calico-Fortinet de Tigera permite a los clientes de Fortinet aprovechar las inversiones existentes en soluciones de Fortinet para aplicar los requisitos de seguridad y cumplimiento, y proteger las cargas de trabajo de Kubernetes nativas de la nube utilizando las mismas herramientas, procesos y flujos de trabajo de seguridad conocidos que utiliza para proteger sus cargas de trabajo que no sean de Kubernetes.

Microsegmentación consciente de la identidad

Por defecto, la comunicación lateral entre cargas de trabajo en clústeres de Kubernetes no está asegurada. Calico aplica la microsegmentación para lograr el aislamiento de las cargas de trabajo y asegurar la comunicación lateral entre pods, espacios de nombres y servicios. Permite a los equipos dividir lógicamente las cargas de trabajo en segmentos de seguridad distintos y definir después controles de seguridad granulares para cada segmento único. Los equipos son capaces de aislar las cargas de trabajo en función de los entornos, los niveles de aplicación, las necesidades de cumplimiento, el acceso de los usuarios y los requisitos de cada carga de trabajo.

Gestión de políticas de seguridad

Calico proporciona un marco de políticas para crear, probar, desplegar y gestionar las políticas de seguridad. Recomienda políticas y proporciona niveles jerárquicos y paneles de control para dichas políticas con el fin de reforzar la seguridad de los clústeres de Kubernetes y de las cargas de trabajo para entornos de Kubernetes compartidos por varios equipos con diferentes partes interesadas. Calico proporciona a los equipos de plataforma, seguridad y aplicaciones la autonomía necesaria para crear y desplegar políticas específicas para clústeres, espacios de nombres y cargas de trabajo. Los usuarios obtienen métricas en tiempo real sobre cómo se evalúan las políticas dentro y a través de los niveles de políticas. Pueden ver todas las políticas de seguridad activas e inactivas de su clúster de Kubernetes con una jerarquía basada en roles y permisos en una sola interfaz.

Observabilidad y resolución de problemas

El gráfico dinámico de servicios y amenazas de Calico proporciona una visualización basada en gráficos de sus despliegues de Kubernetes, incluyendo imágenes, pods, espacios de nombres y servicios. Cuenta con funciones integradas de solución de problemas para identificar y resolver brechas de seguridad y conformidad, problemas de rendimiento, averías en la conectividad, comportamientos anómalos e infracciones de las políticas de seguridad. Por ejemplo, la captura dinámica de paquetes está integrada en Dynamic Service y Threat Graph para ofrecer una forma más rápida y nativa de Kubernetes a la hora de solucionar los puntos conflictivos de rendimiento y los problemas de conectividad mediante la captura de paquetes de un pod específico o de una colección de pods, utilizando tamaños y duración de paquetes específicos.

Cifrado de datos en tránsito con WireGuard

Calico utiliza WireGuard para implementar el cifrado de datos en tránsito. WireGuard se ejecuta como un módulo dentro del núcleo de Linux para proporcionar un mejor rendimiento y un menor consumo de CPU. El cifrado de Calico elimina la complejidad operativa para los equipos en comparación con los enfoques de cifrado estándar. Puede utilizarse para abordar mandatos normativos que especifican el uso del cifrado, como SOX, HIPAA, RGPD y PCI DSS.

Gestión de la postura de seguridad de Kubernetes (KSPM)

Calico evalúa su entorno de Kubernetes frente a los puntos de referencia CIS estándar de la industria para identificar errores de configuración en todos sus entornos de Kubernetes. Esta función incluye un informe de evaluación periódica que muestra el cumplimiento de los puntos de referencia de CIS en todos los activos dinámicos de su entorno de Kubernetes durante el periodo del informe. Se dispone de una puntuación global para cada activo incluido, que puede compararse con umbrales de aprobado/no aprobado configurables. Calico también analiza los controles de acceso basados en roles (RBAC, por sus siglas en inglés) de Kubernetes y la configuración de las políticas de seguridad de pods (PSP) para detectar riesgos en su entorno de Kubernetes.

Cumplimiento (PCI DSS, SOC 2, RGPD, HIPAA, marcos personalizados, etc.)

Calico Cloud es compatible con las principales normas de cumplimiento, como PCI DSS, HIPAA, RGPD, SOC 2, NIST, CCPA y cualquier marco personalizado. Ofrece una monitorización continua en tiempo real para detectar infracciones de cumplimiento, y es capaz de generar informes listos para auditoría. Calico le permite escribir controles de cumplimiento como código, lo que le permite recopilar, correlacionar y preparar datos continuamente para proporcionar pruebas de cumplimiento en cualquier momento. La plataforma también monitoriza y registra todos los cambios en las políticas de cumplimiento.

Malla de clústeres

Calico proporciona un plano de gestión centralizado y multiclúster para permitir la seguridad, la observabilidad y la creación de redes avanzadas para cargas de trabajo y servicios a través de varios clústeres en entornos híbridos y multiclúster. Calico proporciona controles unificados de políticas de seguridad y puntos finales y servicios federados.

Clientes

Obtenga experiencia práctica con nuestros próximos seminarios web y talleres en línea en directo.

Empezar

TIGERA

Tigera, Inc.

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