Seguridad de confianza cero para Red Hat OpenShift con Calico

Reduzca la superficie de ataque y mitigue las brechas de seguridad

Resumen

Los ingenieros de plataformas en la nube tienen la tarea de crear y mantener una plataforma Red Hat OpenShift segura para que los desarrolladores se centren en diseñar aplicaciones. Calico proporciona seguridad de confianza cero para que los ingenieros de plataformas reduzcan la superficie de ataque de las aplicaciones basadas en microservicios, mitigar las brechas de seguridad y ofrecer una capacidad de defensa robusta basada en la confianza cero para las aplicaciones nativas de la nube en Red Hat OpenShift.

Características y funcionalidades

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, espacios de nombres y servicios en clústeres de Kubernetes y recursos externos, como bases de datos, aplicaciones internas, API en la nube de terceros y aplicaciones SaaS. Se ofrecen dos formas de habilitar controles de acceso a la carga de trabajo de grano fino: utilizando políticas de salida DNS y NetworkSets (utilizando IP/CIDR en la política de la red). Los controles de acceso a la carga de trabajo de Calico aseguran todas las comunicaciones entre los clústeres de Red Hat OpenShift y los recursos externos para prevenir cualquier ataque de comando y control.

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

Pasarela de salida

Dado que los pods dentro de un clúster de Red Hat OpenShift son dinámicos, efímeros y no tienen una dirección IP fija, el acceso desde los pods dentro del clúster a los recursos fuera del clúster no puede asegurarse utilizando un cortafuegos tradicional. Calico proporciona una pasarela de salida que asigna IP estáticas a los pods para permitir que los cortafuegos fuera del clúster de Red Hat OpenShift identifiquen estos pods y apliquen los controles de seguridad apropiados. Esto permite al clúster incrementarse o reducirse 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

La pasarela de salida de Calico funciona con cualquier cortafuegos, como los de Palo Alto Networks, Fortinet, Check Point y otros. Los gestores de cortafuegos empresariales pueden utilizarse para crear una arquitectura basada en zonas para su clúster de Openshift. Calico lee esas reglas de cortafuegos y las traduce en políticas de seguridad de Kubernetes que controlan el tráfico entre microservicios. El gestor de cortafuegos puede utilizarse para permitir explícitamente en una lista qué microservicios de los clústeres de OpenShift pueden atravesar las zonas, proporcionando al equipo de seguridad de la red los controles que necesita para mantener el cumplimiento.

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 consciente de la identidad para lograr el aislamiento de las cargas de trabajo y asegurar la comunicación lateral entre pods, espacios de nombres y servicios. Se utilizan etiquetas y cuentas de servicio para establecer la identidad de cada carga de trabajo. La microsegmentación de Calico funciona a través de protocolos de red y de capa de aplicación, y utiliza un modelo dinámico de segmentación de cargas de trabajo basado en los metadatos (nombre del pod, espacio de nombres, nodo, etiquetas y anotaciones) adjuntos a cada carga de trabajo. Puede aumentar o reducir rápidamente las cargas de trabajo en milisegundos en sus clústeres de OpenShift sin tener que cambiar las políticas de seguridad, simplemente utilizando las etiquetas adecuadas al desplegar nuevas cargas de trabajo.

Nivelación de políticas

Calico permite a los equipos de la plataforma Red Hat OpenShift definir políticas de seguridad que tengan prioridad sobre las políticas de otros usuarios en una secuencia determinada sin sobrescribir una política existente ni omitir la política de mayor prioridad. Admite la delegación de autoridad por estructura organizativa y área de responsabilidad (plataforma, seguridad, DevOps y predeterminada) definida con los controles de acceso basados en roles (RBAC) de Kubernetes. Con la jerarquización de políticas de Calico, los equipos de la plataforma OpenShift son capaces de aplicar políticas para toda la empresa que tengan prioridad sobre cualquier política específica de la aplicación, garantizando así un cumplimiento continuo.

Recomendación política

El recomendador de políticas de Calico inspecciona el tráfico dentro de los clústeres de Red Hat OpenShift y recomienda las políticas de seguridad apropiadas a nivel de carga de trabajo y espacio de nombres para asegurar el tráfico. Estas políticas pueden revisarse y modificarse antes de su puesta en escena o aplicación. Con el recomendador de políticas de Calico, los equipos de la plataforma OpenShift logran crear, previsualizar, desplegar y gestionar políticas sin escribir una sola línea de código.

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

Calico es compatible con las principales normas de cumplimiento, como PCI DSS, HIPAA, RGPD, SOC 2, NIST, CCPA y cualquier marco personalizado. Supervisa continuamente los clústeres de OpenShift y las cargas de trabajo dentro de los clústeres en busca de infracciones en el cumplimiento, proporciona la capacidad de crear fácilmente informes listos para auditoría, y proporciona monitorización e informes de cumplimiento en tiempo real para garantizar el cumplimiento. Calico le permite escribir controles de cumplimiento como código y recopila, correlaciona y prepara datos continuamente para proporcionar pruebas de cumplimiento. Calico también monitoriza y registra todos los cambios en las políticas de cumplimiento.

Gestión de la postura de seguridad de Kubernetes (KSPM)

La característica de seguridad de configuración de Calico evalúa su entorno de OpenShift contra los puntos de referencia de CIS estándar de la industria para Kubernetes para identificar configuraciones erróneas. Esta característica incluye un informe de evaluación periódica que muestra el cumplimiento de los puntos de referencia de CIS en todos los activos dinámicos que puedan haber existido en su entorno de OpenShift durante el período del informe. Las organizaciones pueden establecer umbrales configurables como aprobado/no aprobado para alinearse con las necesidades de seguridad de la empresa. Calico también analiza Kubernetes RBAC y la configuración de la política de seguridad de pods (PSP) para detectar riesgos dentro de su entorno de Red Hat OpenShift.

Observabilidad y resolución de problemas

Calico proporciona una visualización basada en gráficos de sus despliegues de OpenShift, como pods, espacios de nombres y servicios, que se completa con herramientas integradas de solución de problemas para identificar y resolver brechas en la seguridad y la auditoría, problemas de rendimiento, averías en la conectividad, comportamientos anómalos e infracciones de las políticas de seguridad. El gráfico dinámico de servicios y amenazas de Calico proporciona visibilidad en tiempo de ejecución en toda la pila, desde la capa de red hasta la de aplicación, mostrando cómo funcionan los espacios de nombres, los servicios y los pods en su clúster de OpenShift y los riesgos presentes en todo su entorno. También incluye la captura dinámica de paquetes, una forma nativa de Kubernetes de solucionar más rápidamente los puntos conflictivos de rendimiento y los problemas de conectividad mediante la captura de paquetes de un pod específico o un conjunto de pods con tamaños de paquete, puertos, protocolo y duración especificados.

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 y proporciona un rendimiento mejorado con un menor consumo de CPU. En comparación con los métodos estándar, el cifrado de Calico elimina la complejidad operativa para los equipos de DevOps y de seguridad, y puede utilizarse para cumplir los mandatos normativos que especifican el uso del cifrado, como SOX, HIPAA, RGPD y PCI DSS.

Clientes

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

¿Desea más información? Pruebe gratis Calico Cloud.

Empezar