TIGERA

Calico Cloud: seguridad activa de contenedores plug-and-play

Las aplicaciones nativas de la nube que se ejecutan en contenedores y Kubernetes están expuestas a una gran superficie de ataque a lo largo de todo el ciclo de vida de la aplicación, desde el desarrollo hasta el despliegue y la producción. Esta gran superficie de ataque, combinada con la naturaleza altamente dinámica y efímera de las cargas de trabajo nativas de la nube, exige un tipo diferente de postura de seguridad.

Calico Cloud es una plataforma de seguridad de contenedores de nueva generación que equilibra la prevención y la mitigación de riesgos con la detección de amenazas para reducir la superficie de ataque, detectar activamente las amenazas y desplegar controles de seguridad mitigadores para limitar los riesgos de exposición. Calico Cloud es la única plataforma de seguridad activa del sector con capacidad de observación de pila completa. Permite a las organizaciones prevenir ataques utilizando la confianza cero, y detectar, solucionar problemas y remediar automáticamente los riesgos de exposición derivados de las brechas en la seguridad en despliegues híbridos y multinube. Calico Cloud se basa en Calico Open Source, la solución de seguridad y redes de contenedores más ampliamente adoptada.

Retos para la seguridad

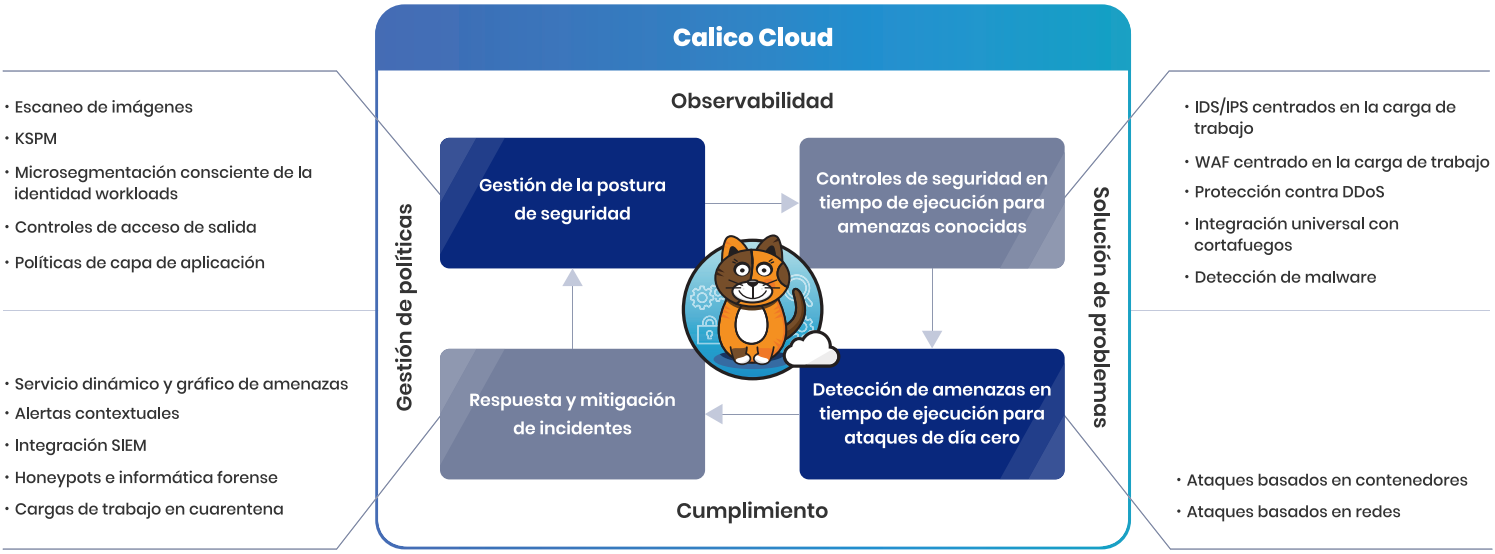
- Gran superficie de ataque en todo el ciclo de vida de la aplicación.
- La falta de visibilidad crea puntos ciegos en materia de seguridad.
- La seguridad centrada en la detección crea falsos positivos que provocan la fatiga de las alertas y la sobrecarga de los equipos de seguridad.
- Lograr el cumplimiento de normativas como SOC2, PCI DSS e HIPAA, es laborioso.
- Dada la red plana de Kubernetes, la seguridad perimetral tradicional es inadecuada.

Cómo ayuda Calico

Calico es la única plataforma de seguridad activa plug-and-play del sector con capacidad de observación de toda la pila para prevenir, detectar y mitigar las brechas de seguridad en las aplicaciones contenerizadas.

Reducción de la superficie de ataque	Detección y detención de los ataques	Mitigación activa de los riesgos
Se asegura el acceso a la carga de trabajo y la comunicación dentro y fuera del clúster para mitigar los ataques	Protección las cargas de trabajo contra las amenazas conocidas y de día cero en los contenedores y en la red durante el tiempo de ejecución	Despliegue los controles de seguridad recomendados para mitigar los riesgos de exposición

Cómo transforma Calico la seguridad de los contenedores



Postura de seguridad robusta para cargas de trabajo en contenedores

Gestión automatizada de vulnerabilidades

Escanee continuamente las imágenes en busca de CVE conocidas y evite que se desplieguen cargas de trabajo vulnerables mediante una canalización CI/CD automatizada y totalmente integrada. Aproveche la vista en tiempo de ejecución de las cargas de trabajo vulnerables para evaluar los riesgos y desplegar controles de seguridad mitigadores para minimizar el radio de explosión.

Gestión de la postura de seguridad de Kubernetes (KSPM)

Endurezca su entorno Kubernetes frente a los puntos de referencia CIS estándar del sector para identificar y corregir los errores de configuración en sus entornos Kubernetes dinámicos.

Controles de acceso a la carga de trabajo de confianza cero

Implemente 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. Asegure los pods utilizando políticas de salida DNS de grano fino y NetworkSets.

Microsegmentación consciente de la identidad

Asegure la comunicación lateral entre pods, espacios de nombres y servicios. Consiga el aislamiento de las cargas de trabajo en función de los entornos, los niveles de aplicación, las necesidades de conformidad, el acceso de los usuarios y los requisitos de las cargas de trabajo individuales.

Políticas de capas de aplicaciones

Aplique las políticas de capas de aplicaciones para la microsegmentación y el control de acceso con atributos específicos de L7 como los métodos HTTP y las rutas URL.

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

Protección en tiempo de ejecución frente a amenazas conocidas

IDS/IPS centrados en la carga de trabajo

Bloquee la comunicación con IP maliciosas conocidas y reciba alertas sobre dominios sospechosos mediante la integración de canales de noticias de inteligencia sobre amenazas globales.

WAF centrado en la carga de trabajo

Proteja las cargas de trabajo de los ataques basados en HTTP, como OWASP Top Ten y otras cabeceras HTTP no conformes, especialmente para la comunicación lateral.

Detección de malware

Detecte y alerte sobre malware conocido con un enfoque basado en firmas. Descubra incidentes de ransomware y minería de criptomonedas con funcionalidades de detección y alertas cuidadosamente diseñadas.

Protección DDoS

Prevenga y mitigue los ataques DDoS con políticas de seguridad a nivel de anfitrión y de aplicación.

Integración universal de cortafuegos

Amplíe las arquitecturas basadas en zonas (de confianza, no de confianza, DMZ) a Kubernetes. Proteja las cargas de trabajo de Kubernetes nativas de la nube utilizando herramientas, procesos y flujos de trabajo de seguridad conocidos que protegen sus cargas de trabajo que no sean de Kubernetes.

Protección en tiempo de ejecución frente a las amenazas de día cero

Detección de anomalías basada en la red para detectar ataques de día cero

Detenga los ataques de día cero con un aprendizaje basado en la heurística de la actividad anómala de la red. Detecte indicadores de ataque (IoA) a partir de registros de flujo de red, DNS y HTTP.

Detección de anomalías basada en contenedores para detectar ataques de día cero

Detecte amenazas de día cero con detectores listos para usar y basados en el comportamiento que analizan la actividad de los contenedores mediante procesos, sistemas de archivos y llamadas al sistema recopiladas con sondas eBPF.

Respuesta a incidentes y mitigación de riesgos

Observabilidad y resolución de problemas

Obtenga una visibilidad completa mediante una visualización basada en gráficos de sus despliegues de Kubernetes, incluyendo imágenes, pods, espacios de nombres y servicios con el gráfico dinámico de servicios y amenazas de Calico. Diseñado específicamente con funcionalidades de resolución de problemas para identificar y resolver brechas de seguridad y cumplimiento, problemas de rendimiento, averías de conectividad, comportamientos anómalos e infracciones de las políticas de seguridad.

Alerta y cuarentena

Vea y gestione todas las alertas procesables relacionadas con la seguridad, la red y el rendimiento desde un único panel de alertas con filtros personalizables. Aplique políticas de cuarentena para aislar las cargas de trabajo vulnerables y permitir los esfuerzos de las soluciones.

Gestión y cumplimiento

Cifrado de datos en tránsito con WireGuard

Elimine la complejidad operativa de los métodos de cifrado estándar con la integración de WireGuard de Calico. Aborde los mandatos normativos para el cifrado, incluidos SOX, HIPAA, RGPD y PCI DSS.

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

Cumpla siempre con la normativa gracias a la monitorización continua en tiempo real para detectar infracciones y generar informes listos para la auditoría. Compatible con PCI DSS, HIPAA, RGPD, SOC 2, NIST, CCPA y cualquier marco personalizado.

Gestión de políticas de seguridad

Cree, escenifique, previsualice, aplique y gestione políticas de seguridad con nuestro marco unificado de políticas. Calico recomienda políticas y proporciona niveles jerárquicos de políticas basados en roles y permisos. La interfaz de usuario del gestor incluye un panel de control de políticas para que los equipos puedan ver y gestionar fácilmente todas las políticas de seguridad activas e inactivas del clúster de Kubernetes.

Clientes

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

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