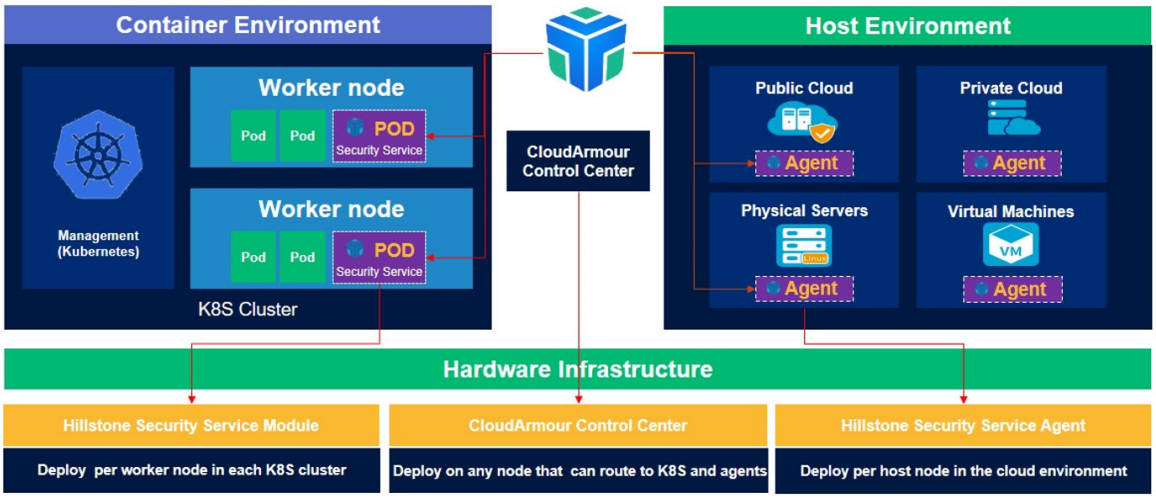
Hillstone CloudArmour:

Una plataforma integral de protección de cargas de trabajo en la nube

A medida que las cargas de trabajo se expanden de las tradicionales basadas en dispositivos físicos o basadas en máquinas virtuales, a las modernas, basadas en contenedores o sin servidor en entornos públicos, privados, híbridos e incluso multinube, la protección de la seguridad y la gestión de riesgos en plataformas en la nube ahora deben abarcar el desarrollo y el tiempo de ejecución. CloudArmour proporciona una visibilidad profunda de las cargas de trabajo en la nube con un control de seguridad total, lo que permite a las organizaciones comprender de manera integral su postura de seguridad en la nube y actuar en consecuencia para satisfacer las demandas de seguridad tanto de la evolución de DevOps como de la nueva arquitectura de infraestructura en la nube. Hillstone CloudArmour combina la microsegmentación y la protección en tiempo de ejecución para proteger las aplicaciones y cargas de trabajo nativas de la nube. También integra la gestión de vulnerabilidades y el cumplimiento de normas en todo el ciclo de vida de las aplicaciones. CloudArmour ayuda a las empresas a adoptar una infraestructura de seguridad en la nube ciber-resistente.



Aspectos destacados del producto

Visibilidad de seguridad completa y profunda de la carga de trabajo convergente en la nube

CloudArmour proporciona un panel centralizado de la postura de seguridad en la nube con información estadística y analítica para hosts y activos en la nube que permite a las organizaciones tener un monitoreo unificado de la carga de trabajo y la administración de activos en tiempo real. El panel proporciona detalles granulares como el estado del sistema del entorno de nube, las vulnerabilidades, los flujos de red, los incidentes de seguridad y las amenazas. CloudArmour se sincroniza automáticamente con registros de contenedores, clústeres de Kubernetes y hosts en tiempo real sobre el estado de componentes clave como imágenes, aplicaciones, servicios y clústeres, así como el sistema operativo, las tarjetas de red y los procesos en el host. La función de perspectiva postural de CloudArmour proporciona una visión profunda de las relaciones de vulnerabilidades y las conexiones de tráfico entre aplicaciones y servicios, lo que proporciona una visión completa de aplicaciones potencialmente vulnerables, tráfico anormal, comportamientos de riesgo y otra información que los operadores de seguridad podrían tomar medidas en contra. A través de nuestra metodología, el primer paso crucial para adoptar una infraestructura de seguridad ciber-resiliente que funcione es recopilar todos los activos y comprender cómo estos encajan en el gran esquema general. Este panel completo permite una vista perfecta de los activos de una empresa, independientemente del factor de forma, el entorno o el proveedor del que se entrega originalmente. Esta capacidad es la esencia de una solución CWPP.

Microsegmentación de red unificada y granular

La microsegmentación extensa del firewall permite la microsegmentación de la red, de modo que el acceso de un activo a otro está restringido de acuerdo con la política. La extensa microsegmentación de firewall en CloudArmour se adapta a múltiples plataformas y cargas de trabajo en la nube de una manera de acoplamiento flexible, lo que significa que no es invasiva y hay menos dependencias, por lo que los cambios o exploits en un componente o activo pueden no necesariamente resultar en cambios o exploits en otro componente. Detecta automáticamente las dependencias de las aplicaciones y aplica dinámicamente las políticas de microsegmentación para evitar la proliferación de amenazas potenciales entre los activos de una empresa. CloudArmour puede minimizar la superficie de ataque de amenazas a través de la microsegmentación líder en la industria y la tecnología patentada de dirección de tráfico, proporcionando visibilidad de red punto a punto y control granular basado en aplicaciones, servicios o nodos de trabajo. Insight de CloudArmour, un panel de control de múltiples vistas, permite una visualización clara de todas las políticas e interacciones existentes entre los activos. Esto es fundamental para ayudar a los usuarios a comprender la postura de seguridad antes de delinear las políticas de microsegmentación. Al crearlas, el asistente de políticas inteligentes de CloudArmour también ayudará a generar las políticas y acciones adecuadas para optimizar mejor su estrategia de confianza cero en su nube privada, pública o híbrida.

Detection y Runtime de Amenazas Inteligentes impulsados por ML

can La capacidad avanzada de detección y prevención de amenazas puede ayudar de forma inteligente a detectar amenazas y mitigar los riesgos durante el tiempo de ejecución en todas las cargas de trabajo en la nube , incluidos los contenedores, las máquinas virtuales y los servidores bare-metal. CloudArmour aprovecha los algoritmos de aprendizaje automático para crear modelos de comportamiento basados en las actividades de las cargas de trabajo, que se recopilan mediante la supervisión de los procesos, syscalls, archivos, redes y otros comportamientos de hosts y contenedores. CloudArmour puede detectar comportamientos anormales a través de estos modelos e implementar reglas para detectar y prevenir amenazas anticipadas. Mientras tanto, CloudArmour integra la inteligencia de amenazas en la nube para mejorar aún más la capacidad de detección de amenazas.

Aspectos destacados del producto (Continuado)

Gestión completa de la vulnerabilidad a través del ciclo de aplicación Entire

CloudArmour proporciona información detallada y gestión de las vulnerabilidades de imágenes, contenedores, nodos de trabajo y hosts. CloudArmour integra la seguridad como parte del flujo de trabajo de integración y despliegue. Monitorea y escanea continuamente las vulnerabilidades de las máquinas virtuales, los hosts en la nube y los servidores bare metal a lo largo del ciclo de vida, desde el desarrollo de aplicaciones hasta la operación diaria, activando alertas si es necesario para mitigar los riesgos potenciales con anticipación. El escaneo de vulnerabilidades también se realiza continuamente en repositorios, y las imágenes con vulnerabilidades graves pueden ser alertadas y bloqueadas para que no lleguen a producción.

Evaluaciones y aplicación de cumplimiento de seguridad listas para usar

CloudArmour evalúa la postura de cumplimiento de las cargas de trabajo en la nube con recomendaciones basadas en las mejores prácticas de la industria. Alivia las comprobaciones de cumplimiento preconfiguradas de CIS Benchmarks para Kubernetes, Docker, Linux, imágenes y configuraciones de tiempo de ejecución de aplicaciones, y proporciona una lista estándar de recomendaciones de correcciones para cada riesgo de cumplimiento. Los resultados de la comprobación de conformidad se pueden exportar para su posterior análisis o auditoría.

Con el uso de la nube disparado, es fundamental implementar una solución global que sea tanto independiente del proveedor como del medio ambiente. CloudArmour, como una solución INNOVADORA de CWPP, que permite una amplia visión general y una comprensión profunda de la postura de seguridad en la nube de la organización, lo que permite adicionalmente delinear las políticas adecuadas que ayudarán a establecer la ciber-resiliencia en todas las cargas de trabajo en la nube. Una infraestructura de seguridad en la nube reforzada por CloudArmour estará lista para abordar el panorama de amenazas en evolución en este entorno que cambia rápidamente.

Funciones

Gestión de activos

- Acceso automatizado a la información de recursos en hosts y clústeres de contenedores
- Muestra la relación entre POD, aplicaciones y servicios, y la relación entre aplicaciones host, hosts y grupos host con topologías.
- Actualiza la información de la aplicación host automáticamente
- Soporta de grupos de administración de activos host
- Soporta gestión de activos multi-tenant

Visibilidad

- Ver el número de servicios implementados de K8, el número de entradas, el número de imágenes del sistema, el número de imágenes vulnerables
- Estadísticas de aplicaciones de soporte por niveles de riesgo de eventos
- La solución admite las estadísticas de vulnerabilidades totales por niveles de riesgo y las vulnerabilidades totales de las imágenes implementadas
- Admite la visualización gráfica de la tendencia del tráfico por espacios de nombres y tiempo
- Admite la visualización gráfica de eventos de seguridad por espacios de nombres con tiempos y tipo de eventos
- Permite ver la lista más reciente de eventos de seguridad de alto riesgo
- Permite el monitoreo del uso de ancho de banda de aplicaciones y servicios de los 10 principales por espacios de nombres y tiempo

Perspectiva de la postura de seguridad

- Configuración con opciones de visualización definidas por el usuario
- Permite la evaluación de los riesgos de los servicios de contenedores ofreciendo el estado de vulnerabilidad, el estado de operación y el tráfico de infracciones
- Proporciona la visibilidad de las conexiones de red de los servicios
- Proporciona el impacto de los riesgos gráficamente
- Admite compatibilidad con la creación de nuevas reglas de seguridad contra amenazas en WebUI

Microsegmentación de red

- Control granular a nivel de nodo o aplicación para activar/desactivar los servicios de microsegmentación
- Capacidad de control de cinco tuplas basada en el tráfico TCP/UDP
- Control granular basado en App/Servicio/IP customizada/CIDR/espacio de nombre en la microsegmentación de red
- Permite la creación de políticas de seguridad predeterminadas globales
- Consulta sobre el bloqueo de eventos desencadenados por políticas de microsegmentación
- Permite la creación/ modificación/eliminación/ movimiento/consulta de políticas de microsegmentación
- Permite administrar el acceso en dirección este-oeste entre aplicaciones dentro de la nube de contenedores
- Permite administrar el acceso en dirección este-oeste entre aplicaciones y nodos dentro de la nube de contenedores
- Permite administrar el acceso en dirección este-oeste entre aplicaciones y servicios dentro de la nube de contenedores
- Permite administrar el acceso en dirección norte-sur desde los recursos de la nube de contenedores a Internet
- Permite administrar el acceso en dirección norte-sur a los recursos en la nube de contenedores desde el exterior
- Permite el acceso a la red entre hosts, entre hosts y aplicaciones host, entre direcciones externas y hosts/ aplicaciones host
- Soporta la generación automática de políticas de microsegmentación
- Soporta la gestión de políticas de microsegmentación para multi-tenant

Escaneo de imágenes

- Permite habilitar o deshabilitar el servicio de administración de imágenes en la granularidad de nivel de nodo
- Admite el escaneo y filtrado del repositorio de imágenes de múltiples versiones recientes para escanear
- Admite imágenes locales almacenadas en caché en el host de Docker, con opciones para ejecutar algunas o todas las imágenes.
- Admite el escaneo automático programado; admite el escaneo de actualizaciones incremental y el escaneo manual
- Admite la actualización automática y manual de bases de datos de vulnerabilidades en línea y la importación manual de bases de datos de vulnerabilidades sin conexión
- Indica la tendencia de riesgo de la imagen en un plazo de 30 días
- Controla la puesta en marcha de la imagen en función de los niveles de riesgo
- Muestra los 10 principales riesgos de la imagen

Servicios de seguridad en tiempo de ejecución

- Permite habilitar o deshabilitar los servicios de seguridad en tiempo de ejecución en la granularidad a nivel de nodo
- Autoaprendizaje y establecimiento de modelos de comportamiento tanto para contenedores como para hosts.
- El tiempo de aprendizaje automático se puede establecer globalmente o por objeto de negocio
- Modelado de comportamiento basado en múltiples dimensiones, como procesos, lectura/ escritura de archivos y actividades de red
- Configuraciones de supervisión en tiempo de ejecución de servicios de host en la nube basadas en la lista negra o blanca
- Proporciona 4 operaciones de control de comportamiento en tiempo de ejecución: alarmar, bloquear, detener e ignorar

Comprobación de línea base de cumplimiento

- Admite comprobaciones de cumplimiento de host de aplicaciones de contenedores, Docker, K8s y Linux
- Permite comprobar manualmente los comandos, las recomendaciones de correcciones y sus referencias en función del resultado de la comprobación de cumplimiento
- Permite exportar los resultados de la comprobación de cumplimiento

Análisis de vulnerabilidades

- Admite el análisis de vulnerabilidades en máquinas físicas, máquinas virtuales y hosts en la nube
- Admite la configuración de tareas de escaneo automático
- Permite visualizar las tendencias de riesgo del host

Gestión del sistema

- Los administradores se pueden clasificar en 3 roles: administrador, operador y auditor
- Requisitos obligatorios de configuración de contraseñas para las cuentas de administrador
- Monitorea el estado y el tiempo de funcionamiento de los servicios de seguridad a nivel global y permite el inicio/la detención de las funciones de seguridad correspondientes
- Admite el filtrado, la consulta y la exportación de logs del sistema y logs de configuración
- Permite establecer alarmas para eventos críticos en la página de administración

Version: EX-08.01-CloudArmour-V1.1-0422-SP-01