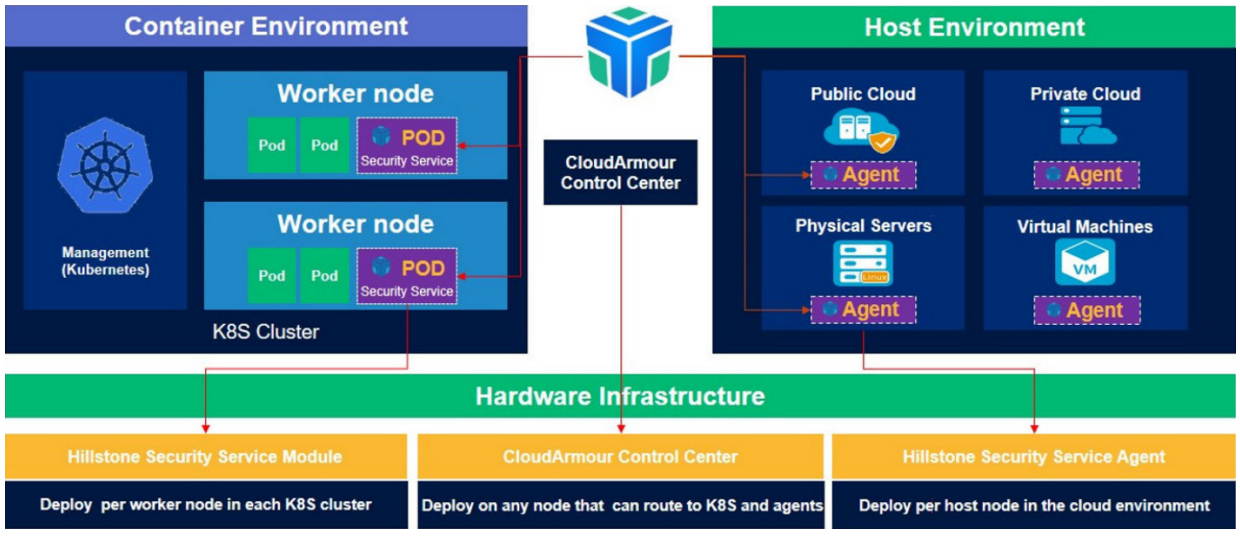
# Hillstone CloudArmour

## 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 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 microsegmentación y protección en tiempo de ejecución para proteger las aplicaciones y cargas de trabajo nativas de la nube. Ofrece prevención avanzada de intrusiones y potentes capacidades antivirus. También integra la gestión de vulnerabilidades y el cumplimiento en todo el ciclo de vida de las aplicaciones. CloudArmour ayuda a las empresas a adoptar una infraestructura de seguridad en la nube cibernética.





# Productos destacados

### 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 una supervisión unificada de la carga de trabajo y la gestión de activos en tiempo real. El panel proporciona detalles granulares, como el estado del sistema del entorno de la 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 información sobre la postura 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 las aplicaciones potencialmente vulnerables, el tráfico anormal, los comportamientos de riesgo y otra información contra la que los operadores de seguridad podrían tomar medidas. Esto permite a los operadores de seguridad tomar decisiones informadas y tomar medidas rápidas para fortalecer la seguridad en la nube.

### Microsegmentación de red unificada y granular

La microsegmentación extensa 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 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. Descubre automáticamente las dependencias de la aplicación 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 tecnología de microsegmentación y dirección de tráfico líder en la industria, proporcionando visibilidad de red punto a punto y control granular basado en aplicaciones, servicios o nodos de trabajo. Esto es fundamental para ayudar a los usuarios a comprender la postura de seguridad antes de delinear las políticas de microsegmentación. Al crear políticas, 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.

### Detección avanzada de amenazas y protección en tiempo de ejecución

La capacidad avanzada de detección y prevención de amenazas puede ayudar a detectar amenazas y mitigar los riesgos durante el tiempo de ejecución en cargas de trabajo en la nube, incluidos contenedores, máquinas virtuales y servidores sin sistema operativo. Crea modelos de comportamiento mediante la supervisión de las actividades de las cargas de trabajo, como procesos, syscalls, archivos y redes. A través de estos modelos, CloudArmour puede detectar comportamientos anormales e implementar reglas para identificar y prevenir amenazas avanzadas de manera efectiva. Con sólidas capacidades de monitoreo y bloqueo, CloudArmour protege eficazmente contra comportamientos de alto riesgo como inicios de sesión anormales, shells inversos, webshells y escalada de privilegios locales. Además, CloudArmour utiliza un potente motor de análisis de virus, que realiza análisis exhaustivos de archivos de imagen de host y contenedor para detectar virus. Al detectar cualquier archivo malicioso, CloudArmour toma rápidamente las medidas apropiadas como el aislamiento, la eliminación, la reparación o la confianza, eliminando eficazmente las amenazas para garantizar un entorno seguro.

### Gestión completa de vulnerabilidades en todo el ciclo de vida de la aplicación

CloudArmour proporciona información detallada y gestión

## Aspectos destacados del producto (Continuado)

de las vulnerabilidades de imágenes, contenedores, nodos de trabajo y hosts. CloudArmour integra la seguridad como parte del flujo de trabajo de integración continua e implementación continua. 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 los 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. Aprovecha 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.

# Funciones

### Gestión de activos

- Compatibilidad con la gestión de activos con agrupación de dos niveles basada en clústeres y grupos host/espacios de nombres
- Compatibilidad con la definición de clúster de hosts y etiquetas de grupos de host
- Inventario de soporte de servicios de contenedores, archivos de imagen y etiquetas de activos
- Compatibilidad con la sincronización de imágenes locales con repositorios de contenedores
- Admitir el análisis global de activos de Windows/Linux, incluida la información de cuentas, paquetes de software, procesos, servicios, web y bases de datos, y consultar información de paquetes de software de soporte

### Información sobre la postura de seguridad

- Compatibilidad con esquemas de visualización definidos por el usuario
- Información de soporte, incluido el estado de vulnerabilidad, los riesgos de cumplimiento, el tráfico de infracciones, los riesgos de intrusión, el tráfico no conforme, los riesgos de virus y los riesgos de contraseñas débiles
- Soportar la visibilidad de las conexiones de red de servicios
- Admite el acceso con un solo clic al ambiente de microsegmentación y configuración de políticas de control de admisión de Kubernetes

### Gestión de vulnerabilidades

- Compatibilidad con el análisis de vulnerabilidades para hosts e imágenes
- Compatibilidad con tareas de análisis programadas y bajo demanda
- Proporcionar paneles de detección de riesgos para hosts e imágenes
- Proporcionar visibilidad de la información sobre vulnerabilidades y los paquetes de componentes afectados
- Admite actualizaciones manuales, automáticas y sin conexión de bases de datos de firmas

### Detección de contraseñas débiles

- Admite diccionarios de contraseñas débiles personalizadas
- Soporte para definir tareas de escaneo de contraseñas débiles

### Comprobación de cumplimiento

- Admite comprobaciones de cumplimiento para hosts, contenedores, e imágenes
- Admite el alcance de la comprobación de cumplimiento personalizado y Políticas de cumplimiento
- Compatibilidad con comprobaciones de cumplimiento programadas y bajo demanda
- Proporcionar visibilidad de las tendencias de riesgo de cumplimiento, la tasa de cumplimiento y los detalles de riesgo
- Compatibilidad con la exportación de resultados de comprobación de cumplimiento

### Prevención de intrusiones

- Soporte para detectar comportamiento anormal de inicio de sesión en el host, incluido el tiempo sospechoso, IP, cuenta y ataques de fuerza bruta y alertas de soporte, bloqueo de IP y listas blancas
- Soporte de detección Webshell en hosts/contenedores y alertas de soporte, aislamiento de archivos y listas blancas
- Admite la detección de shell inverso y el comportamiento de escalada de privilegios locales en hosts/contenedores, y admite alertas, deshabilitación de procesos/contenedores y listas blancas
- Compatibilidad con firmas personalizadas y reglas de detección personalizadas

### Antivirus

- Soporte de escaneo de virus de archivos host y archivos de imagen
- Admite tres modos de escaneo: rápido, equilibrado y de bajo consumo de recursos
- Soporte de escaneo de archivos críticos o completos Escaneo
- Admite análisis bajo demanda y programados
- Compatibilidad con la gestión de archivos de aislamiento y de confianza
- Admite el análisis de varios tipos de virus, incluidos spyware, adware, spam, troyanos, marcadores automáticos, aplicaciones maliciosas y bombas de archivos comprimidos
- Soporte de detección de virus comprimidos
- Admite el manejo por lotes de virus con opciones para reparar, eliminar, aislar, confiar o ignorar
- Proporcionar visualización detallada de tendencias de riesgo de virus y Resultados del análisis
- Admite actualizaciones manuales, automáticas y sin conexión de bases de datos de firmas

### Microsegmentación

- Admite el control granular a nivel de nodo o aplicación para activar Servicios de microsegmentación on/off
- Admite la configuración de políticas de microsegmentación basadas en varias dimensiones, incluidos clúster, grupo host, host, espacio de nombres, Kubernetes aplicación, servicio Kubernetes, IP personalizada, libreta de direcciones y libreta de dominios
- Admite control de cinco tuplas para el tráfico TCP / UDP
- Compatibilidad con la configuración de períodos de validez de directivas
- Apoyar la microsegmentación específica de activos Administración
- Apoyar la política de microsegmentación basada en grupos Administración
- Apoyo Generación atomizada de políticas de microsegmentación
- Compatibilidad con la consulta de eventos de directiva bloqueados
- Compatibilidad con la configuración de directivas globales

### Monitoreo del comportamiento

- Admite el establecimiento de modelos de comportamiento basados en dimensiones, incluidos procesos, operaciones de lectura/escritura de archivos y comportamientos de red
- Configuración de reglas de comportamiento de soporte para hosts, Aplicaciones de Kubernetes y contenedores de host
- Admite la capacidad de aprendizaje conductual con la generación automática de reglas de comportamiento
- Admite el control granular a nivel de nodo para activar / desactivar los servicios de monitoreo de comportamiento
- Soporte de protección de lista negra / lista blanca basada en Modelos de comportamiento
- Admite múltiples acciones de mitigación, incluidas alertas, bloqueo, deshabilitación e ignorar el evento.

### Control de admisión de Kubernetes

- Admite la prohibición del lanzamiento o alerta de contenedores que no cumplan con las políticas de control de admisión
- Admite la definición de políticas de control de admisión basadas en el cumplimiento, análisis de vulnerabilidades, análisis de virus y otras evaluaciones de riesgos
- Soporte para consultar la alerta de directiva de control de admisión Eventos
- Admite el interruptor de control global para administrar las políticas de control de admisión

### Administración de registros

- Admite la visualización detallada de microsegmentación, comportamiento, control de admisión de Kubernetes, eventos de intrusión
- Admite el acceso al sistema, la configuración y Registros de auditoría
- Soporte de reenvío de registros

### Administración del sistema

- Compatibilidad con la administración de múltiples inquilinos
- Compatibilidad con los requisitos obligatorios de configuración de contraseñas para cuentas de administrador
- Admite la omisión automática de las funciones de seguridad basadas en la configuración global
- Admite la supervisión en tiempo real del estado operativo del servicio de guardias de seguridad en todo el sistema
- Admite notificaciones de alerta proactivas para críticos Eventos en la interfaz de administración
- Compatibilidad con el control de acceso basado en roles, incluido Administrador, operador, auditor y otros roles
- Admite la autenticación de inicio de sesión de Radius
- Admite la integración de inicio de sesión único (SSO) con Hillstone iSource
- Compatibilidad con el envío de eventos de amenaza a través de Syslog
- Compatibilidad con la integración de API para plataformas de terceros para recuperar información de activos y vulnerabilidades



Version: EX-08.01-CloudArmour-V1.0R3-0823-SP-01