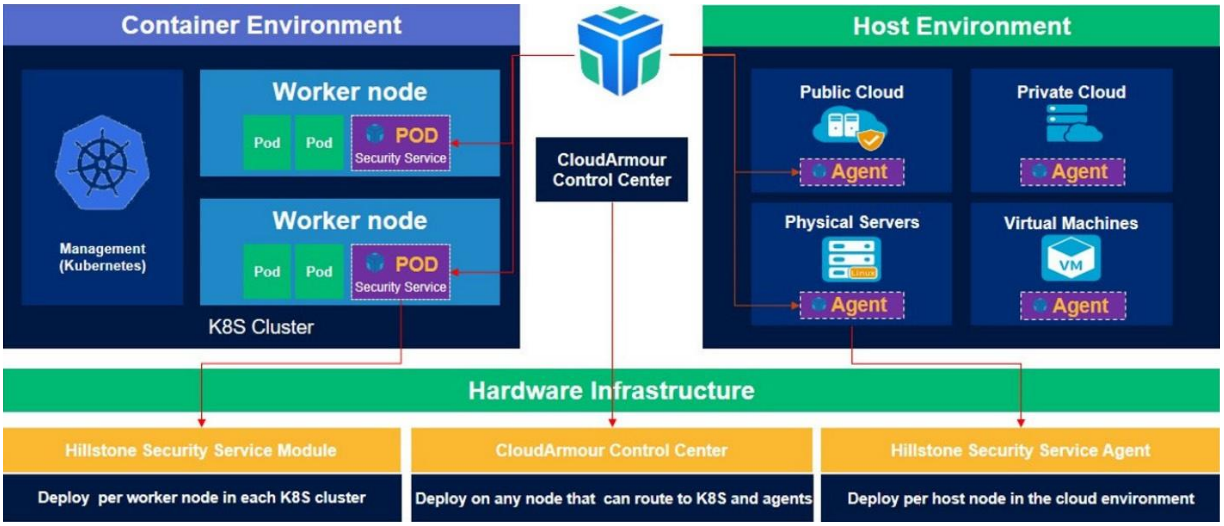
# Hillstone CloudArmour

## Comprehensive Cloud Workload Protection Platform

As workloads expand from traditional physical appliance-based or virtual machine-based to the modern container-based or serverless in public, private, hybrid, and even multi-cloud environments, security protection and risk management on cloud platforms must now span development and runtime. CloudArmour provides deep visibility of the cloud workloads with full security control, allowing organizations to comprehensively understand their cloud security posture, and act accordingly to meet the security demands of both the evolution of DevOps and the new cloud infrastructure architecture. Hillstone CloudArmour combines micro-segmentation and runtime protection to protect cloud-native applications and workloads. It delivers advanced intrusion prevention and  powerful anti-virus capabilities. It also integrates vulnerability management and compliance across the entire lifecycle of applications. CloudArmour helps enterprises embrace a cyber-resilient cloud security infrastructure.


Container Environment
Management (Kubernetes)
Worker node
Pod
Pod
POD
Security Service
Worker node
Pod
Pod
POD
Security Service
K8S Cluster
CloudArmour Control Center
Host Environment
Public Cloud
Agent
Private Cloud
Agent
Physical Servers
Linux
Agent
Virtual Machines
VM
Agent
Hardware Infrastructure
Hillstone Security Service Module
Deploy  per worker node in each K8S cluster
CloudArmour Control Center
Deploy on any node that  can route to K8S and agents
Hillstone Security Service Agent
Deploy per host node in the cloud environment

## Product Highlights

### Full and Deep Security Visibility of Converged Cloud Workload

CloudArmour provides a centralized dashboard of the cloud security posture with statistical and analytical information for hosts and cloud assets that allow organizations to have a unified workload monitoring and real-time assets management. The dashboard provides granular details such as cloud environment system status, vulnerabilities, network flows, security incidents and threats. CloudArmour automatically synchronizes with container registries, Kubernetes clusters and hosts in real-time about the status of key components such as images, apps, services, and clusters, as well as the OS, network cards, and processes in the host. CloudArmour's posture insight function provides a deep insight into vulnerabilities relations and traffic connections between applications and services, which provides a comprehensive view of poten-

# Product Highlights (Continued)

tially vulnerable applications, abnormal traffic, risky behaviors, and other info that security operators could take actions against. This empowers security operators to make informed decisions and take swift actions to strengthen cloud security.

### Unified and Granular Network Micro-segmentation

Extensive micro-segmentation allows for network micro-segmentation, such that the access from one asset to another is restricted according to policy. The extensive micro-segmentation on CloudArmour adapts to multiple cloud platforms and workloads in a loose-coupling manner, meaning it is non-invasive, and there are less dependencies, so changes or exploits in one component or asset may not necessarily result in changes or exploits in another component. It automatically discovers the application dependencies and dynamically enforces the micro-segmentation policies to avoid the proliferation of potential threats among an enterprise's assets. CloudArmour can minimize the threat attack surface via industry-leading micro-segmentation and traffic steering technology, providing point-to-point network visibility and granular control based on apps, services or work nodes. This is critical for helping users understand the security posture before delineating micro-segmentation policies. When creating policies, CloudArmour provides a Smart Policy Assis -tant that uses advanced traffic log analysis to intelligently model traffic and generate microsegmentation policies. With its Policy Simulation functionality, administrators can safely validate and fine-tune policies in a risk-free environment, ensuring accuracy without impacting live operations. This robust combination boosts both the efficiency and accuracy of policy management, streamlining security operations while reducing operational risks.

### Advanced Threat Detection and Runtime Protection

The advanced threat detection and prevention capability can help detect threats and mitigate risks during runtime on cloud workloads, including containers, VMs, and bare-metal servers. It builds behavior models by monitoring the activities of workloads, such as processes, syscalls, files, and networks. Through these models, CloudArmour can detect abnormal behaviors and deploy rules to identify and prevent advanced threats effectively. With robust monitoring and blocking capabilities, CloudArmour effectively safeguards against high-risk behaviors like abnormal logins, reverse shells, webshells, and local privilege escalation. Moreover, CloudArmour utilizes a powerful virus scanning engine, conducting thorough scans of host and container image files to detect viruses. Upon detecting any malicious files, CloudArmour promptly takes appropriate actions like isolation, deletion, repair, or trust, effectively eliminating threats to ensure a secure environment.

### Complete Vulnerability Management Across the Entire Application Lifecycle

CloudArmour provides deep insights and management of the vulnerabilities of images, containers, working nodes and hosts. CloudArmour integrates security as part of the Continuous Integration and Continuous Deployment workflow. It continuously monitors and scans vulnerabilities of VMs, cloud hosts, and bare metal servers throughout the lifecycle from application development to daily operation, triggering alerts if necessary to mitigate potential risks ahead of time. Vulnerability scanning is also continuously performed on repositories, and images with serious vulnerabilities can be alerted and blocked from reaching production.

### Out-of-the-box Security Compliance Assessments and Enforcement

CloudArmour assesses the compliance posture of cloud workloads with recommendations based on the industry's best practices. It leverages the pre-configured compliance checks from CIS Benchmarks for Kubernetes, Docker, Linux, images and application runtime configurations, and provides a standard list of recommendations of remediations for each compliance risk. Compliance check results can be exported for further analysis or auditing.

# Features

### Asset Management

- Support asset management with two-tier grouping based on clusters and host groups/ namespaces
- Support defining host cluster and host group labels
- Support inventory of container services, image files, and asset labels
- Support synchronizing local images with container repositories
- Support global Windows/Linux asset analysis, including account, software package, process, service, web, and database information, and support software package information query

### Security Posture Insight

- Support insights into microsegmentation events, as well as internal and external traffic within clusters
- Support visibility of network connections of services
- Support displaying asset communication details in a list view
- Support creating microsegmentation policies based on forensics during policy simulation

### Vulnerability Management

- Support vulnerability scanning for hosts and images
- Support on-demand and scheduled scanning tasks
- Provide risk detection dashboards for hosts and images
- Provide visibility into vulnerability information and the affected component packages
- Support manual, automatic, and offline updates of signature databases
- Support vulnerability allowlists

### Weak Password Detection

- Support custom weak password dictionaries
- Support defining weak password scanning tasks
- Support weak password allowlists

### Compliance Check

- Support compliance checks for hosts, containers, and images
- Support custom compliance check scope and compliance policies
- Support on-demand and scheduled compliance checks
- Provide visibility into compliance risk trends, compliance rate, risk details
- Support exporting compliance check results

### Intrusion Prevention

- Support detecting abnormal host login behavior
- Support detecting webshell on hosts/containers
- Support detecting reverse shell and local privilege escalation behavior on hosts/containers
- Support WebRCE detection for hosts and containers
- Support memory shell detection on hosts
- Support sensitive file alteration detection
- Support detection of high-risk comman execution such as reverse shells, malicious commands, file modifications,etc.
- Support custom signatures and custom detection rules

### Antivirus

- Support multi-engine virus scanning
- Support virus scanning of host files and image files
- Support three scanning modes: fast, balanced, and low resource consumption
- Support custom path, critical path, and complete virus scanning
- Support on-demand and scheduled scanning
- Support management of isolation and trusted files
- Support scanning for various virus types, including spyware, adware, spam, trojans, auto-dialers, malicious applications, and compressed file bombs
- Support detection of compressed viruses
- Support batch handling of viruses with options for repairing, deleting, isolating, trusting, or ignoring
- Provide virus risk trend visualization and detailed scan results
- Support manual, automatic, and offline updates of signature databases

### Micro-segmentation

- Support node or app level granular control to turn on/off micro-segmentation services
- Support micro-segmentation policy configuration based on various dimensions, including cluster, host group, host, namespace, Kubernetes application, Kubernetes service, custom IP, address book, and domain book
- Support five-tuple control for TCP/UDP traffic
- Support configuration of policy validity periods
- Support micro-segmentation policy simulation
- Support group-based micro-segmentation policy management
- Support atomated generation of micro-segmentation policies
- Support blocked policy event query
- Support global policy configuration

### Behavior Monitoring

- Support establishing behavioral models based on dimensions including processes, file read/write operations, and network behaviors
- Support behavior rule configuration for hosts, Kubernetes applications, and host containers
- Support behavioral learning capability with automatic generation of behavior rules
- Support node level granular control to turn on/off behavior monitoring services
- Support blacklist/whitelist protection based on behavioral models
- Support multiple mitigation actions including alerting, blocking, disabling, and ignoring

### Container Security

- Support manual configuration file compliance check for Docker images and Kubernetes clusters
- Support compliance checks, vulnerability scanning, virus scanning, and secrets scanning for local images and image repositories
- Support creating admission control policies based on compliance, vulnerability, and virus scan results
- Support querying alert events related to admission control policies
- Support global configuration management for admission control policies
- Support anomaly detection for the Kubernetes API

### Log Management

- Support detailed display of micro-segmentation, behavior, Kubernetes admission control, intrusion events
- Support access to system, configuration, and audit logs
- Support log forwarding

### System Management

- Support multi-tenant management
- Support mandatory password setting requirements for administrator accounts
- Support automatic bypass of security features based on global settings
- Support real-time monitoring of the operational status of the security guard service across the entire system
- Support proactive alert notifications for critical events on the management interface
- Support role-based access control, including administrator, operator, auditor, and other roles
- Support Radius login authentication
- Support single sign-on (SSO) integration with Hillstone iSource
- Support threat event submission through Syslog
- Support API integration for third-party platforms to retrieve asset and vulnerability information
- The controller supports high availability

Version: EX-08.01-CloudArmour-V1.0R4-0924-EN-01