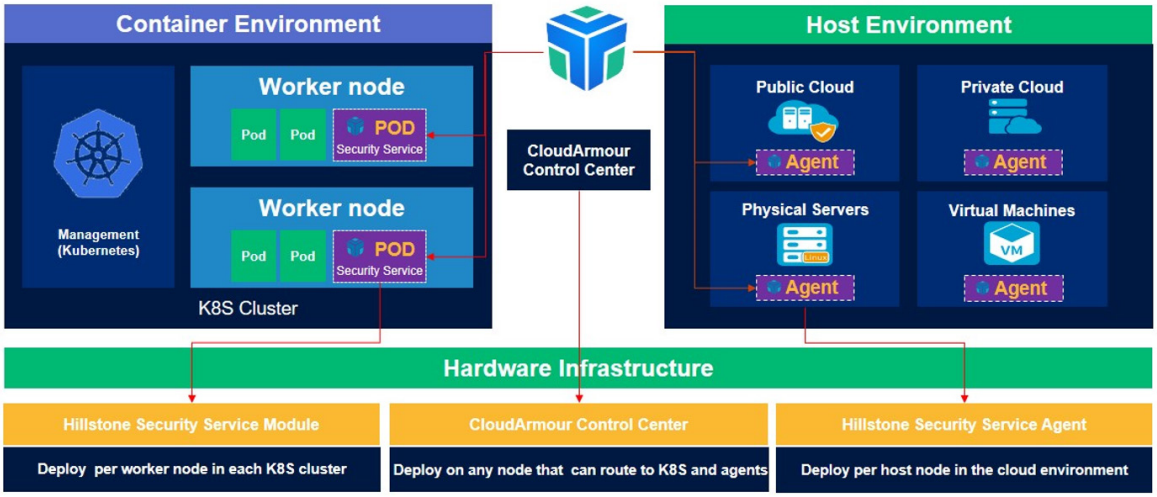
Hillstone CloudArmour:
Comprehensive Cloud Workload Protection Platform

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 its 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 also integrates vulnerability management and compliance across the entire lifecycle of applications. CloudArmour helps enterprises embrace a cyber-resilient cloud security infrastructure.



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 perspective function provides a deep insight into vulnerabilities relations and traffic connections between applications and services, which provides a comprehensive view of potentially vulnerable applications, abnormal traffic, risky behaviors, and other info that security operators could take actions against. Via our methodology, the first crucial step to embracing a cyber-resilient security infrastructure that works

Product Highlights (Continued)

is to collect all assets and understand how these assets fit into the overall grand scheme. This comprehensive dashboard allows for a seamless view of an enterprise's assets, regardless of form factor, environment, or which vendor it is originally delivered from. This ability is the essence of a CWPP solution.

Unified and Granular Network Micro-segmentation

Extensive firewall micro-segmentation allows for network micro-segmentation, such that the access from one asset to another is restricted according to policy. The extensive firewall 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 patented traffic steering technology, providing point-to-point network visibility and granular control based on apps, services or work nodes. CloudArmour's Insight, a multi-view dashboard allows for a clear display of all existing policies and interactions between assets. This is critical for helping users understand the security posture before delineating micro-segmentation policies. When creating policies, CloudArmour's smart policy assistant will additionally aid in generating the appropriate policies and actions to best optimize its zero-trust strategy across their private, public or hybrid cloud.

ML-powered Intelligent Threat Detection and Runtime Protection

The advanced threat detection and prevention capability can intelligently help detect threats and mitigate risks during runtime on all cloud workloads, including containers, VMs, and bare-metal servers. CloudArmour leverages machine learning algorithms to build behavior models based on the activities of workloads, which are collected by monitoring the processes, syscalls, files, networks, and other behaviors of hosts and containers. CloudArmour can detect abnormal behaviors via these models and deploy rules to detect and prevent advance threats. Meantime, CloudArmour integrates cloud threat intelligence to further enhance threat detection capability.

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.

With cloud usage skyrocketing, it is critical to deploy an overarching solution that is both vendor-agnostic and environment-agnostic. CloudArmour, as an innovative CWPP solution, enables this broad overview and thorough understanding of the organization's cloud security posture, allowing for the delineation of proper policies that'll help establish cyber-resilience in all cloud workloads. A cloud security infrastructure bolstered by CloudArmour will be ready to tackle the evolving threat landscape in this fast-changing environment.

Features

Asset Management
- Automated access to resource information in hosts and container clusters
- Show the relationship among POD, applications and services, and the relationship among host applications, hosts and host groups with topologies
- Update host application information automatically
- Support group management of host assets
- Support multi-tenant asset management

Visibility
- View the number of K8s deployed services, the number of Ingresses, the number of system images, the number of vulnerable images
- Support application statistics by event risk levels
- Support the statistics of total vulnerabilities by risk levels, and the total vulnerabilities of deployed images
- Support graphic display of traffic trend by namespaces and time
- Support graphic display of security events by namespaces with time and event types
- Support to view the latest list of high-risk security events
- Support the top 10 bandwidth usage of apps and services by namespaces and time

Security Posture Perspective
- Configuration with user-defined display options
- Support the evaluation of the risks of container services by offering vulnerability status, operation status and violation traffic
- Provide the visibility of network connections of services
- Provide impact of risks graphically
- Support creating new security rules against threats in WebUI

Network Micro-Segmentation
- Node or app level granular control to turn on/off micro-segmentation services
- Five-tuple control capability based on TCP/UDP traffic
- App/Service/Custom IP/CIDR/namespace based granular control on network micro-segmentation
- Support setting global default policy
- Query on blocking events triggered by micro-segmentation policies
- Support the creation/ modification/ deletion/ movement/ query of micro-segmentation policies
- Manage east-west direction access between apps within the container cloud
- Manage east-west direction access between app(s) and node(s) within the container cloud
- Manage east-west direction access between app(s) and service(s) within the container cloud
- Manage north-south direction access from resources in the container cloud to the Internet
- Manage north-south direction access to resources in the container cloud from the outside
- Support network access between hosts, between hosts and host applications, between external addresses and hosts/ host applications
- Support automatic generation of micro-segmentation policies
- Support micro-segmentation policy management for multi-tenancy

Image Scanning
- Enable or disable the image management service on the node-level granularity
- Support image repository scanning and filtering of multiple recent versions to scan
- Support local images cached on the Docker host, with options for running images or all images
- Support automatic scan on schedule; support incremental update scan and manual scan
- Support automatic and manual update of vulnerability databases online, and manual import of vulnerability databases offline
- Indicate the image risk trend within 30 days
- Control image startup based on risk levels
- Top 10 image risks

Runtime Security Services
- Enable or disable runtime security services on node-level granularity
- Auto learning and establishment of behavior models for both containers and hosts.
- Automatic learning time can be set globally or by business object
- Behavior modeling based on multiple dimensions, such as process, file reading/writing and network activities
- Configurations of runtime monitoring of cloud host services based on the black or white list
- Provide 4 runtime behavior control operations: alarm, block, stop and ignore

Compliance Baseline Check
- Support container application, Docker, K8s and Linux host compliance checks
- Manually check commands, recommendations of fixes and their references based on the compliance check result
- Export compliance check results

Vulnerability Scanning
- Support scanning for vulnerabilities in physical machines, VMs and cloud hosts
- Support configuration of automatic scanning tasks
- Host risk trends

System Management
- Administrators can be categorized into 3 roles: administrator, operator and auditor
- Mandatory password setting requirements for administrator accounts
- Monitor the health and running time of security guard services globally and allow start/stop for corresponding security functions
- Support filtering, querying and exporting system logs and configuration logs
- Alarms for critical events on the management page

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