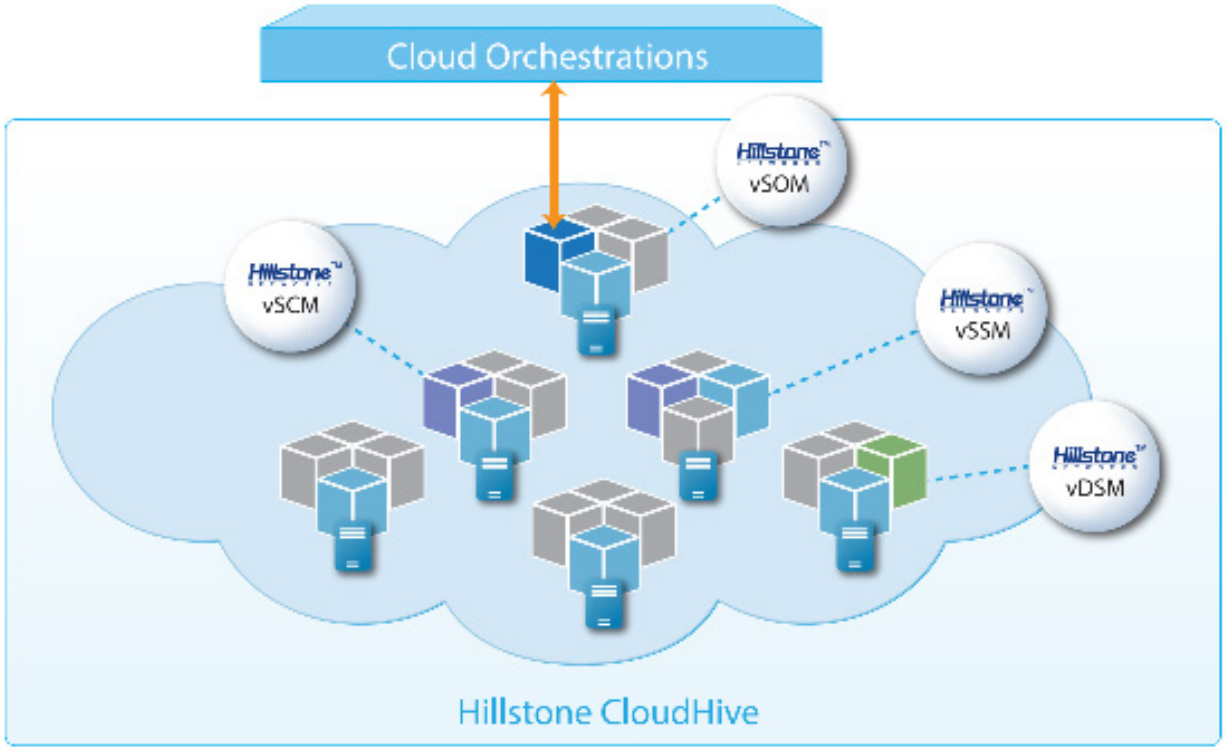
# Hillstone CloudHive

## Micro-segmentation Solution for the Cloud

Hillstone CloudHive provides micro-segmentation technology to secure each virtual machine (VM) in cloud deployments. It provides comprehensive visibility of East-West traffic and provides complete protection to stop lateral attacks between VMs. In addition, the CloudHive security service can easily scale to meet business needs without interruption.

Hillstone CloudHive is comprised of four types of virtual modules that work together as a single appliance to provide complete security to each VM.

- Virtual Security Orchestration Module (vSOM), integrated and connected with Cloud Management Platforms (CMPs), manages the CloudHive service lifecycle.
- Virtual Security Control Module (vSCM) is the control panel, supporting policy configuration and distribution, as well as managing the lifecycle of the vSSM.
- Virtual Security Service Module (vSSM) is deployed on each physical server to implement micro-segmentation and provide L2-L7 security services.
- Virtual Data Service Module (vDSM) is an optional log forwarding module which forwards CloudHive logs to external syslog servers. It supports massive log forwarding via multi-module load balancing deployment.





# Product Highlights

### Achieve Unparalleled Live Traffic Visibility

All access points for virtual machines can be monitored to provide visibility of traffic, applications and threats related to the VM or port group, which is the cornerstone for enabling East-West traffic control and protection. New traffic and application during a specific period can be monitored and visualized to show the subtle changes in the virtual network. VM topology, traffic insight, application identification, as well as comprehensive log features allow Cloud Service Providers (CSPs) to meet compliance and security audit requirements.

### Reduce Attack Surface to Nearly Zero

Each CloudHive Virtual Security Service Module (vSSM) is deployed on a physical server, enabling micro-segmentation for inter-VM or inter-network communication. East-West traffic is secured with L2-L7 security services, including firewall features such as policy control and session limits, advanced security features such as Intrusion Prevention System (IPS), Antivirus and Attack Defense (AD), as well as fine-grained application control. Real-time mitigation also blocks, impedes or quarantines active attacks.

### Effortlessly Scale Security Through Active Orchestration

CloudHive seamlessly integrates with major virtualization platforms including VMware, FusionCompute and FusionOne HCI, and has the VMware Ready certificate with the NSX integration.

On-demand security services can be applied to any and all new workloads and VMs through the scalability of vSSM. The deployment of vSCM enables unified security policy configuration for each VM. CloudHive supports vMotion to ensure security services persist in the event the VM moves. Existing VM flows will not be interrupted by vMotion.

### Improve Efficiency While Reducing Costs

CloudHive Layer 2 deployment does not impact existing network topology. Layer 3 deployment is supported in VMware vSphere, which offer the scalability and flexibility to meet different network requirements now and in the future. Along with unique configuration optimization tools and features, it minimizes deployment and configuration overhead, without business impact or network interruption. In addition, the advantage of the ease of management of a single appliance reduces operational errors and improves overall efficiency. Total cost of ownership is also reduced as CloudHive security services do not need any upgrade or expansion of the current cloud platforms.

### Real-time Monitoring of Service Performance

CloudHive dives deep into the cloud environment to build the first line of security and defense for virtual machines and the critical data and applications that reside upon them. Because the interrelationships between various business systems and services in the cloud environment are complex, CloudHive provides network performance management from a business point of view. CloudHive automatically discovers and defines service dependencies both within and external to the data center, and establishes a reference relationship between the services of a given business. It then monitors the delay and jitter of each service, the delay, jitter and packet loss of each network, and the utilization of virtual machine CPU and memory. Thus, CloudHive provides complete monitoring of service chains in terms of service quality, network quality and computing resources, and provides rapid troubleshooting capability with advanced data analysis.

# Features

### Application Control
- Over 4,000 applications that can be filtered by name, category, subcategory, technology and risk
- Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
- Actions: block, reset session, monitor, traffic shaping
- Real-time application database upgrade

### Visibility
- Virtual asset auto discovery: networks and VMs
- Dynamic virtual asset monitor, auto/manual VM/IP/MAC address book update
- Virtual asset group management, auto/manual synchronize the asset grouping information
- Visualization of virtual network topology, VMs, trafffic, user-defined plan, and different colors for threat level classifications
- Deep insight and monitoring of all traffic between VMs or port group
- Rank of traffic, application and threat, drill down to related information
- Customized Visualization options: Sort, inquiry, filtering, zoom in/zoom out
- Log support: session logs, threat logs and system logs

### Service Performance Monitor
- Multi-dimensional cloud service performance quality monitoring, including resource utilization, quality of network and services
- Query of monitoring data with flexible monitoring point and interval
- Automatic service chain topology presenting the internal and external communications of the cloud services
- Screen casting for a global overview

### Firewall
- Layer 2-Layer 7 access control
- VM and port group based access control
- AD account based access control
- Time Table Based Access Control
- Domain name based access control
- Geo-location/IP based access control
- Application Layer Gateway (ALG)
- Session limit: New Session/Concurrent Session
- Support detection, filtering and alarm for files of HTTP, FTP, SMTP, SMB protocols

### Attack Defense
- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense
- ARP attack defense
- Port Scan detect and defense

### Intrusion Prevention
- IPS Actions: default, monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
- Protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- Packet logging option
- Filter Based Selection: severity, target, OS, application or protocol
- IP exemption from specific IPS signatures
- IDS sniffer mode
- IPv4 and IPv6 rate based DoS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/ICMP session flooding (source/destination)
- Active bypass with bypass interfaces
- Predefined prevention configuration
- Support whitelist configuration

### Antivirus
- Manual, automatic push or pull signature updates
- Flow-based antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
- Compressed file virus scanning

### Cloud-Sandbox
- Upload malicious files to cloud sandbox for analysis
- Support file types including PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP, Script
- Support protocols including HTTP, POP3, IMAP4, SMTP, FTP, SMB
- Provide complete behavior analysis report for malicious files
- Support threat / trust list management

### Botnet C&C Prevention
- Discover intranet botnet host by monitoring C&C connections and block further advanced threats such as botnet and ransomware
- Regularly update the botnet server addresses
- Prevention for C&C IP, domain and URL
- Support traffic detection for TCP, HTTP, and DNS protocols
- C&C address database supports customized IP and domain
- Supports DNS sinkhole check
- C&C profile supports DGA
- Supports DNS tunneling detection
- Supports DGA detection
- Supports bulk import of customized domain names

### URL Filtering
- Web page access control based on IP, VM, service group attributes
- Support more than 60 categories, tens of millions of URL signatures, customizable URL categories
- Realtime update of URL signature database

### Deployment
- Support both tapping mode and transparent in-line mode
- L2 deployment and L3 deployment (VMware vSphere only)
- Ease of deployment without root authority and any plug-in, minimized affect to VM and hypervisor
- vSSM can scale up without interrupting security service, up to 200 vSSM modules
- Achieve VM based policy configuration through automatic learning on virtual assets
- Detect the state of the VM (up or down), and update VM IP change automatically
- Enable or disable security service on VM or port group through one click
- Support VMware VSS/VDS, vSAN deployment
- Support Openstack OVS deployment

### High Availability
- vSOM "VM shutdown" does not affect the CloudHive service
- vSOM can be deployed in pairs (Active/Passive) to provide high availability
- Separation of management, control and service plane ensures the service stability
- vSCM are deployed in pairs (Active/Passive) to provide high availability
- Single vSSM "VM down" does not affect the system; the user VM traffic can bypass the vSSM
- vSCM can reboot and restart security service automatically after "VM down"
- vMotion support: security policy and flow sessions automatically synchronize across multiple service modules
- Support In Service Software Upgrade (ISSU)
- Support trusted network admin host control and control over login trying times

### Management
- Interface: RESTful API, CLI, WebUI
- Distributed architecture, centralized and unified management through a single interface
- Support single sign on (SSO) for multiple CloudHive
- vSOM supports regular backup of global configuration, and delivery through FTP/SMTP
- Log forwarding to external syslog servers through vDSM, support massive and high-speed log forwarding
- Support 3rd party Radius/Active Directory/TACACS+

- Support IP/Port/App based control and VM/Port group based control
- Support policy self-learning/grouping/convergence, duplication removing and hit counting
- Fully support IPv6, support upgrade from IPv4 to IPv6
- RestAPI to partner for further automation development and integration
- SNMP monitoring and SNMP trap alarm, NTP support
- Multi-layer administration mode for the separation of operation and management
- Package capture and download, environment change diagnosis for fault location
- Import/ Export policy files and configuration files
- Supports report for cloud network security assessment, traffic status assessment, cloud security risk assessment, and unblocked threat event statistics

### Virtualization Compatibility

- VMware vSphere 5.5/6.0/6.5/6.7/7.0/8.0
- VMware Horizon VDI platform
- FusionCompute 6.5.1/8.0.x/8.1.x
- FusionOne HCI 23.1.0 or above

# Specifications

| Module | Description | System Resource | Module # |
|---|---|---|---|
| vSOM | Virtual Security Orchestration Module | 2*vCPU, 6GB Memory, 60GB Hard Disk | 1 Standard, HA supported |
| vSCM | Virtual Security Control Module | 2*vCPU, 8GB Memory, 17GB Hard Disk | 1 Min., 2 Recommended |
| vSSM (Standard) | Virtual Security Service Module 02 | 2*vCPU, 6GB Memory, 5GB Hard Disk | 200 Max. |
| vSSM (Advanced) | Virtual Security Service Module 04 | 4*vCPU, 10GB Memory, 5GB Hard Disk | When deployed in Jumbo Frame mode, the memory requirement will be increased by 2G on the original basis. |
| vDSM | Virtual Data Security Module | 2*vCPU, 6GB Memory, 5GB Hard Disk | Optional, multiple mode supported |

| CloudHive System | vSSM 02 | vSSM 04 |
|---|---|---|
| Firewall Throughput (Maximum) | 1 Tbps | 1 Tbps |
| Maximum Concurrent Sessions | 340 Million | 680 Million |
| New Sessions/s (HTTP) | 6 Million | 10 Million |
| IPS Throughput (Maximum) | 300 Gbps | 1 Tbps |
| AV Throughput (Maximum) | 300 Gbps | 1 Tbps |
| vSSM Scalability (Maximum) | 200 | 200 |

| Individual vSSM | vSSM 02 | vSSM 04 |
|---|---|---|
| Firewall Throughput [1] | 5 Gbps | 5 Gbps |
| Firewall Throughput (NSX) [2] | 16 Gbps | 16 Gbps |
| Maximum Concurrent Sessions | 1.7 Million | 3.4 Million |
| New Sessions/s (HTTP) | 30,000 | 50,000 |
| IPS Throughput [3] | 1.5 Gbps | 5 Gbps |
| AV Throughput [4] | 1.5 Gbps | 5 Gbps |

**NOTES:**

(1) All performance data is obtained under DellR720, VMware, VDS environment;

(2) All performance data is obtained under DellR720, VMware(6.0U2), VDS, NSX(v6.4) environment;

(3) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on;

(4) AV throughput data is obtained under HTTP traffic with 512K file attachment.

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R8 Actual results may vary due to the CloudHive software versions and deployment environment.



Version:EX-08.01-CloudHive-V2.9.4-0124-EN-01