CloudHive: Micro-Segmentation Solution for the Cloud

Gartner Peer Insights Customers' Choice 2022

Reshape.Security

Embrace Cyber Resilience

Agenda

- Security Challenges in the Cloud
- Hillstone CloudHive Value Proposition
- Hillstone CloudHive Portfolio
- Deployment Scenarios & Winning Cases

Security Challenges in the Cloud

Security is the Primary Concern in the Cloud

63%

"Security and Privacy are the top reasons for NOT using the Public Cloud"

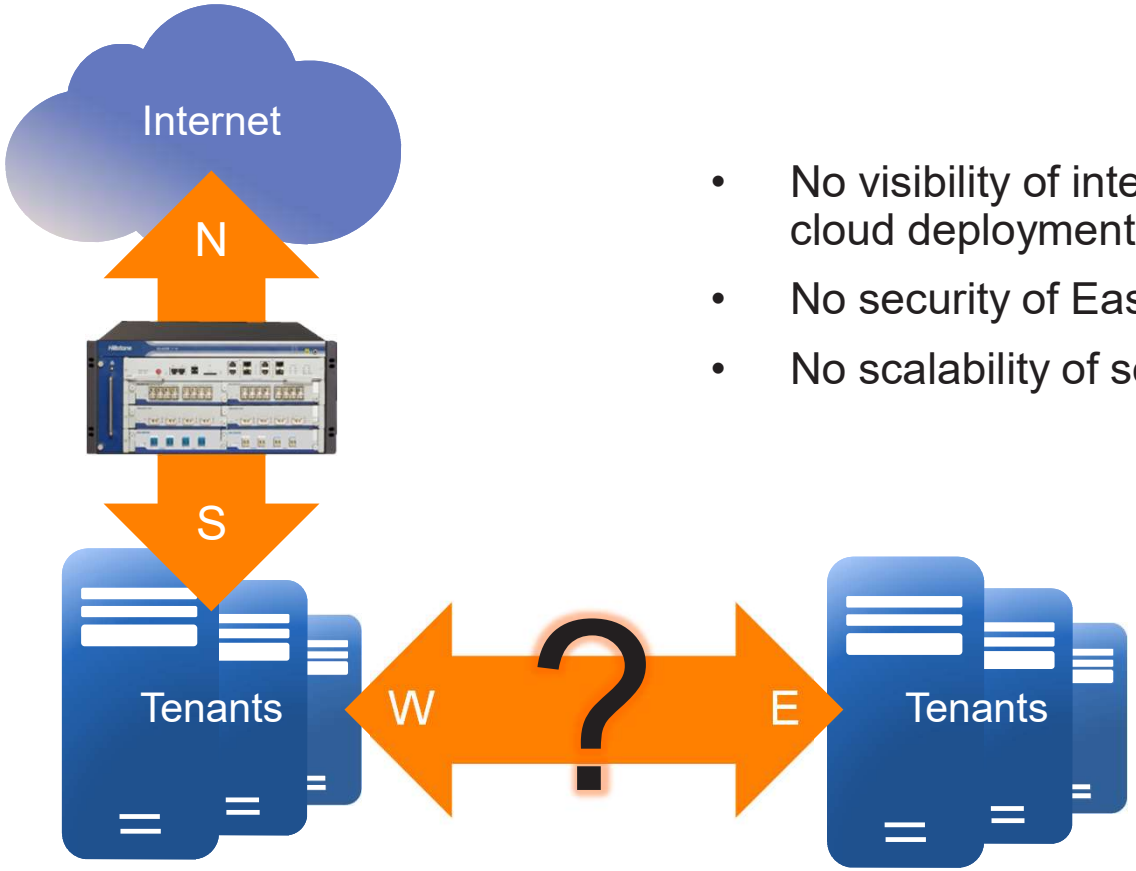
Gartner

83%

"Security is an important criteria to be considered when it comes to Hybrid Clouds."

IDC Analyze the Future

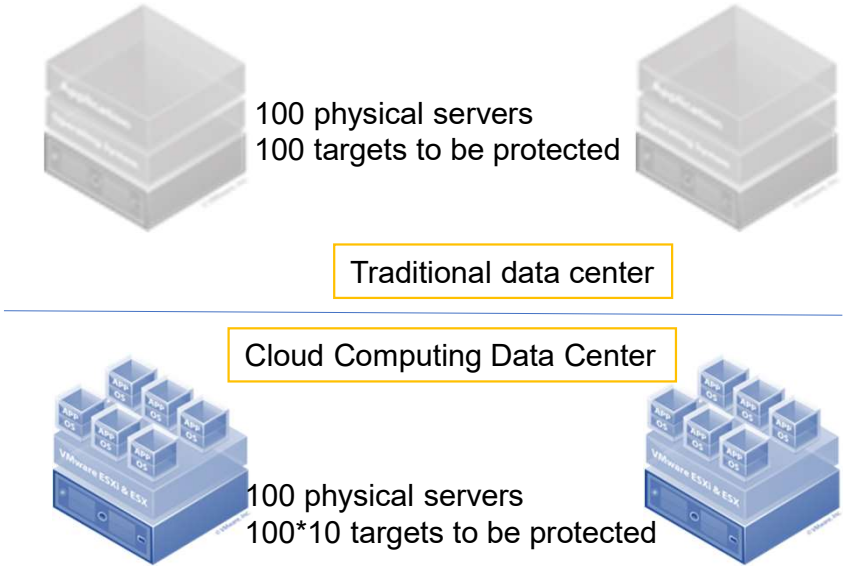
Traditional Perimeter Security Fails



- No visibility of internal traffic and threats in cloud deployments
- No security of East-West workloads
- No scalability of security in cloud environments

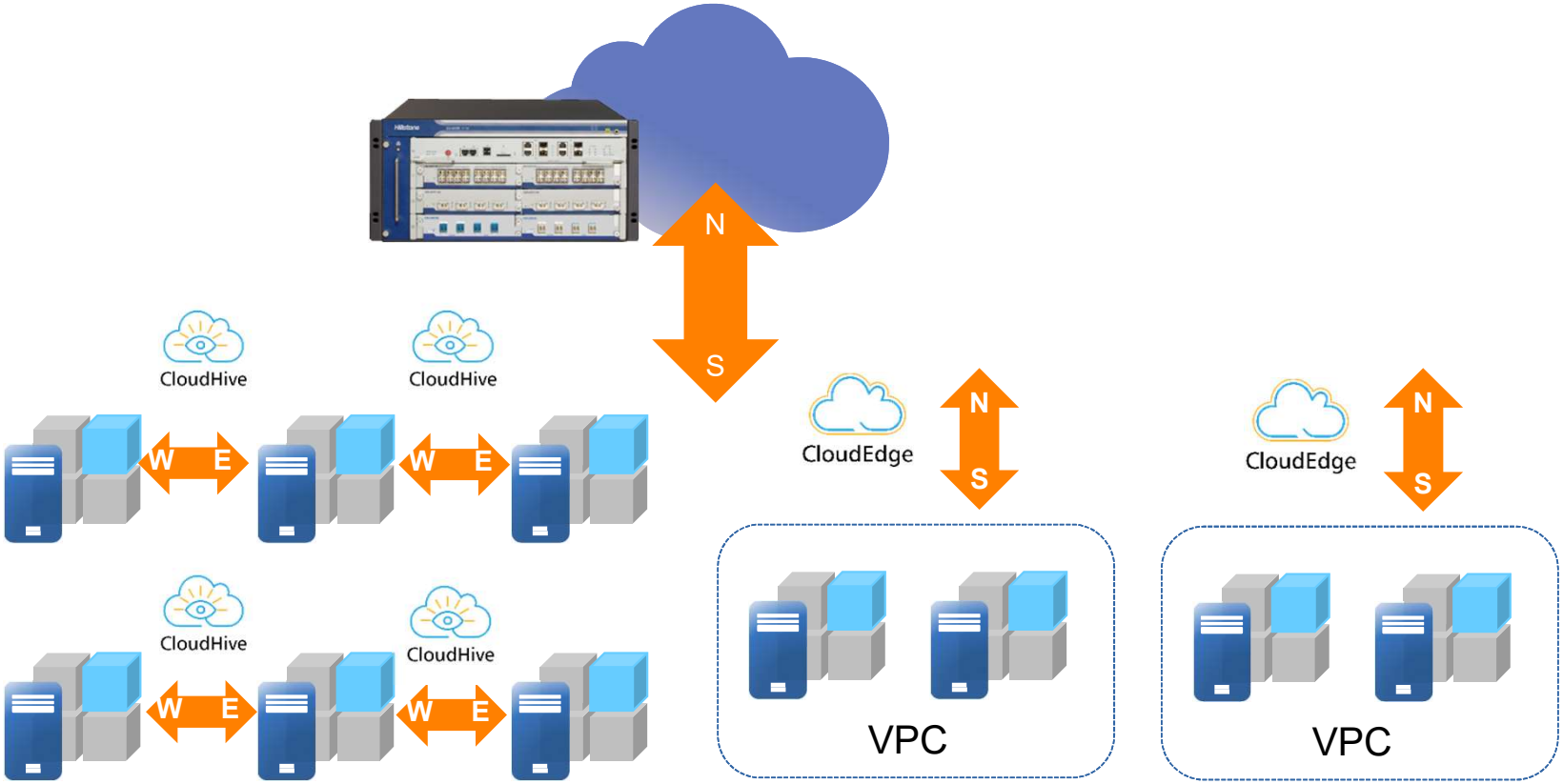
The Challenges of Cloud Security

- Virtualization technology amplifies the traditional security domain
- Virtualization technology leads to lack of clear boundaries
- Invisible within the cloud
- Unclear division of security responsibilities
- Huge maintenance workload



Note: A server in the public cloud can even be sold up to 100 virtual machines!

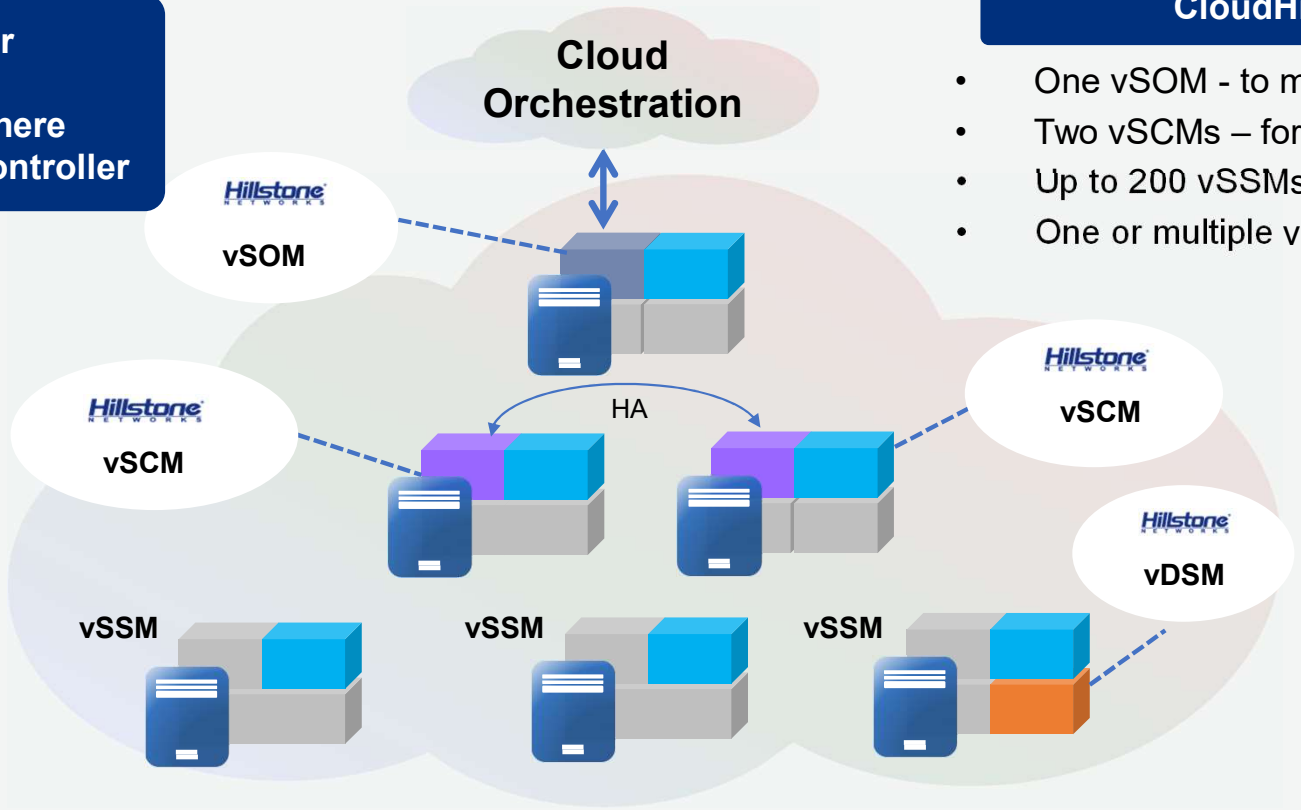
Complete Protection for the Cloud



Hillstone CloudHive Value Proposition: Micro-Segmentation Solution

What is Hillstone CloudHive?

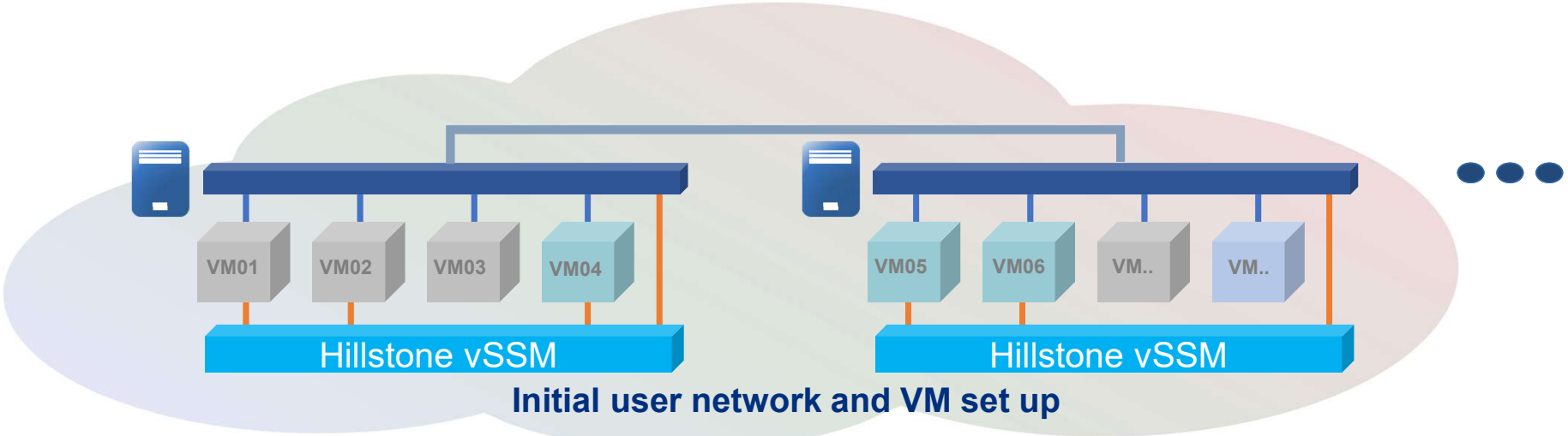
vCenter or FusionSphere OpenStack Controller



CloudHive Modules

- One vSOM - to manage service lifecycle
- Two vSCMs – for High Availability
- Up to 200 vSSMs – in each physical server
- One or multiple vDSM – for log forwarding

How Does Hillstone's CloudHive Work?



Initial user network and VM set up

Deploy vSSM on each host

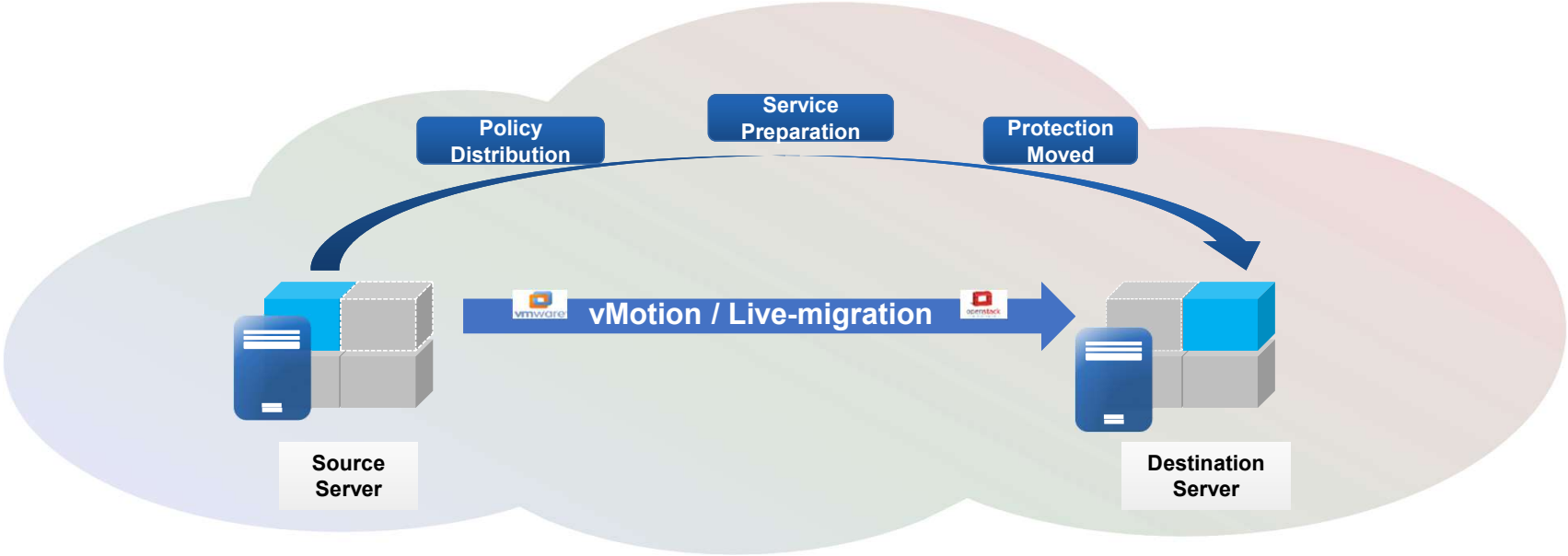
Add security service to VM1 and VM2

Remove security service for VM2

Add security service for a user network

One click protection!

What Happens if a VM Moves?



Unified Policy configuration keeps security services consistent

Dynamic session synchronization ensures non-business interruption

Automatic protection for moving VMs without administrative intervention

Hillstone CloudHive Value Proposition

Hillstone NETWORKS

Get Unparalleled Live Traffic Visibility

Reduce Attack Surface to Near-zero

Effortlessly Scale Security Through Active Orchestration

Improve Efficiency While Reducing Cost

High Available Distributed Architecture

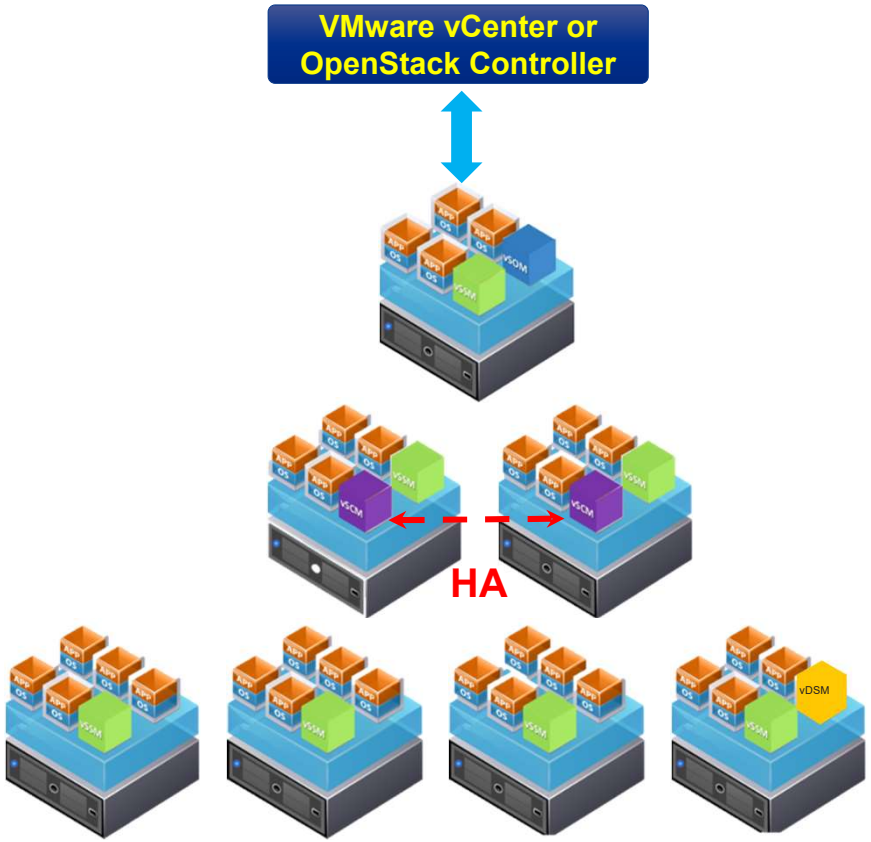
Deep Visibility

Improved Productivity

Micro-Segmentation

High Available Distributed Architecture

CloudHive Architecture



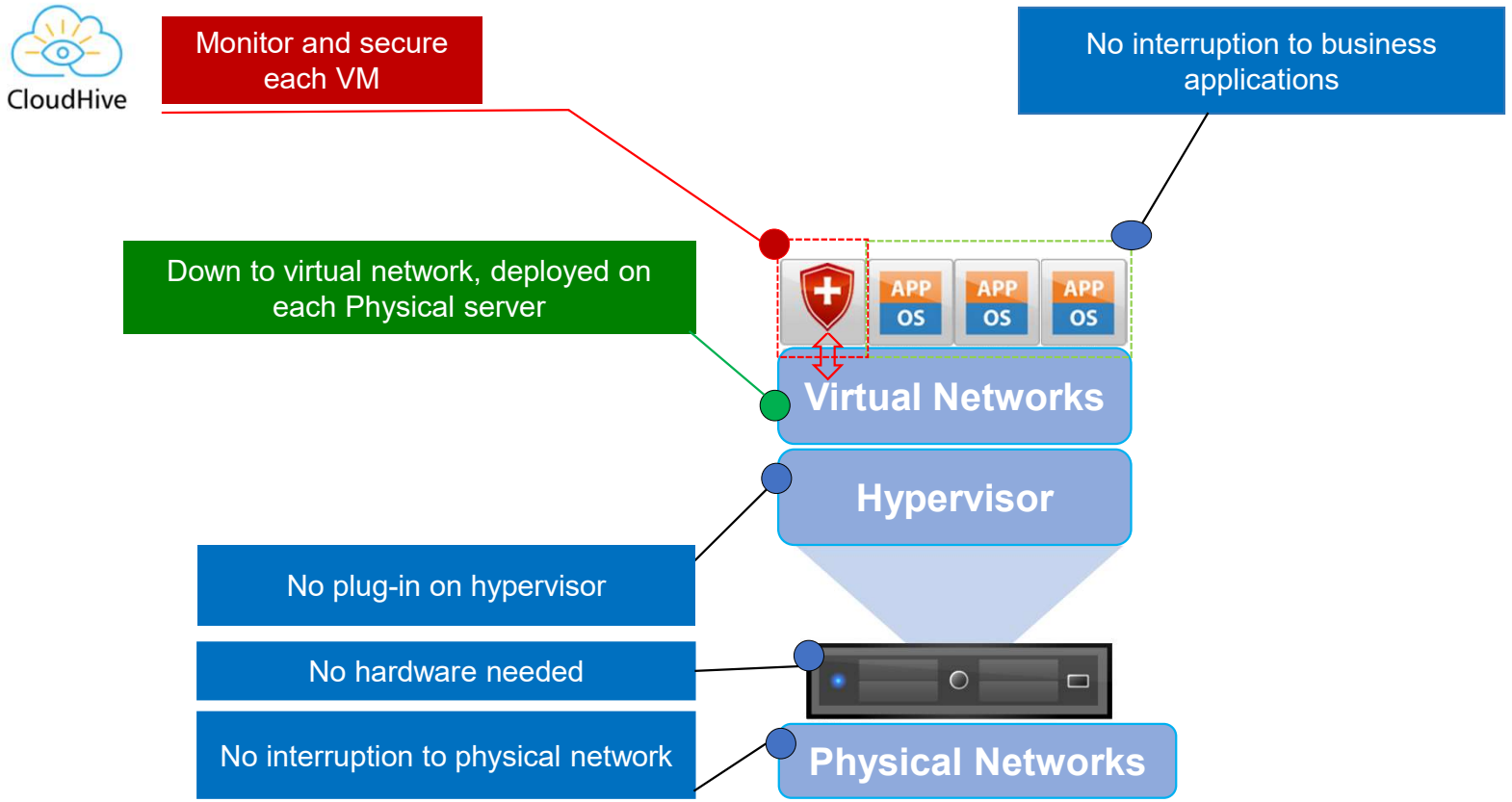
vSOM, virtual Security Orchestration Module
Integrates with third-party CMP, manages service lifecycle

vSCM, virtual Security Control Module
Centralized management and configuration for all vSSMs

vSSM, virtual Security Service Module
Traffic monitor and security service enablement

vDSM, virtual Data Service Module
High speed log forwarding

Designed for the Virtual Environment



Fully Distributed

Distributed

- Distributed deployment
- Centralized management

Scalability

- Scale up or down
- Ease of deployment

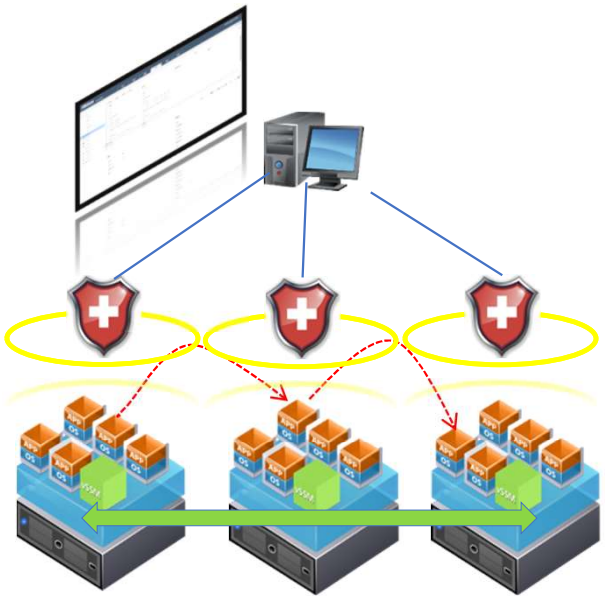
VM level

- vSSM on each server
- Monitor traffic between VMs

Synchronization

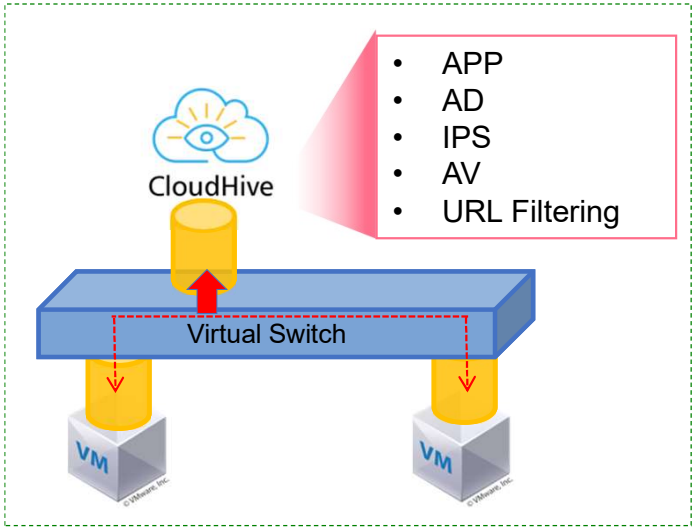
- Session
- Policy

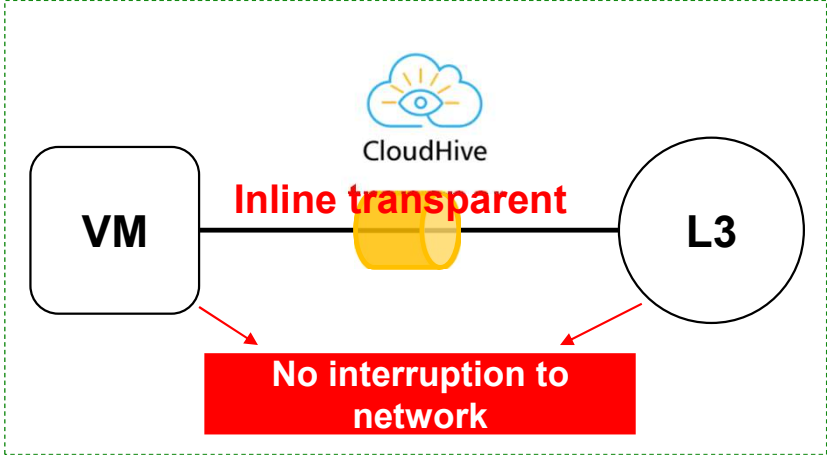
Unified Management Interface,
Managed as a single appliance



Non- disruptive protection

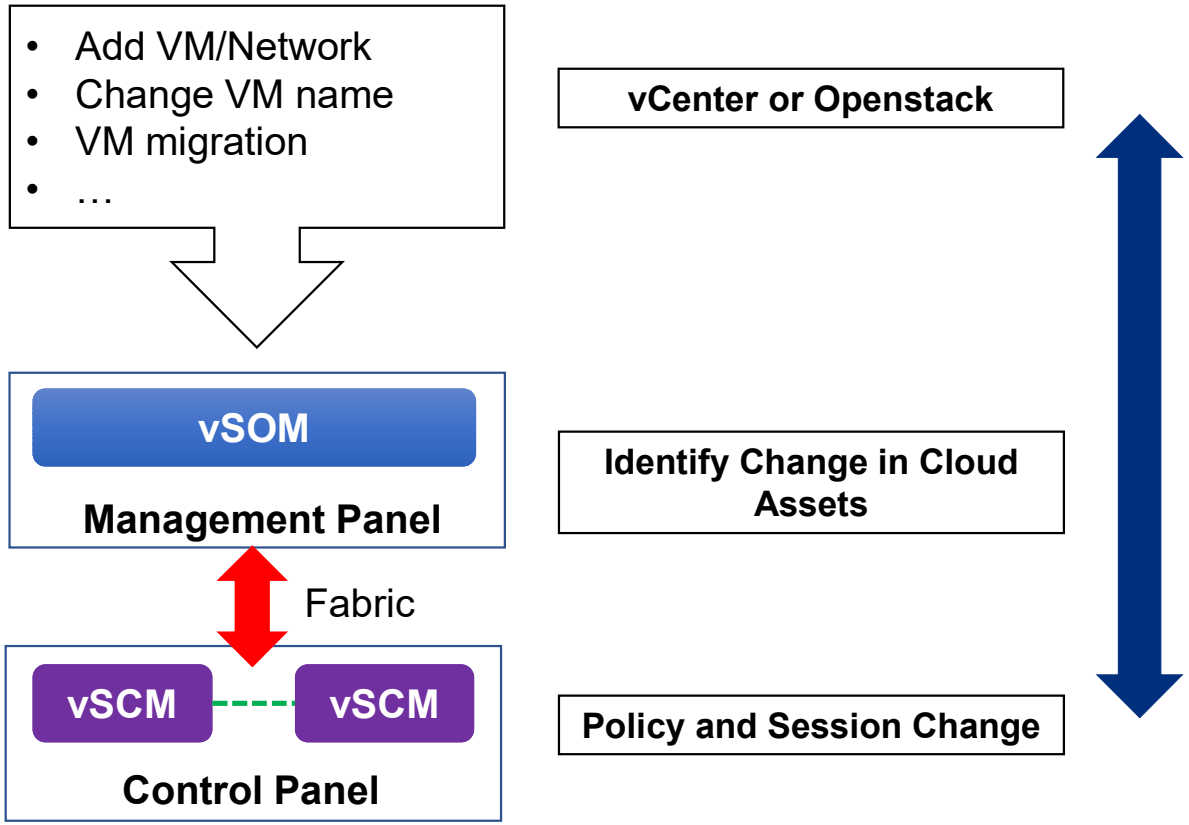
Non-Disruptive



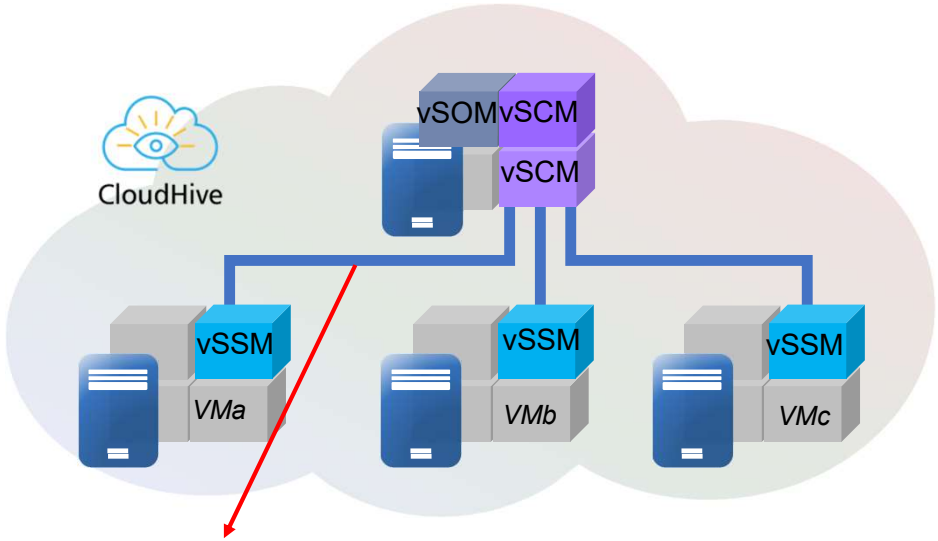


Non-Disruptive	Virtualization Support	Monitor and Protect	Complete Security
• L2/ L3 deployment • TAP or inline transparent mode	• Standard API • Support major virtualization platforms	• VM traffic monitor • Threat detection and prevention	• APP, AD, IPS, AV, URL Filtering

Change Recognition in Cloud Assets



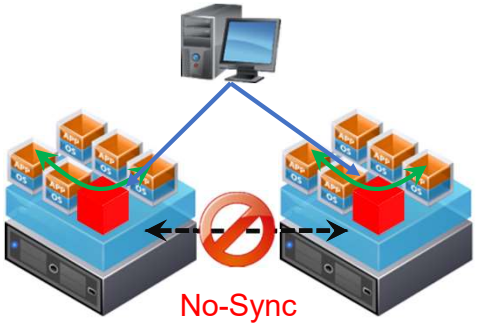
Separation of Data and Management Network



Independent Communication Channel

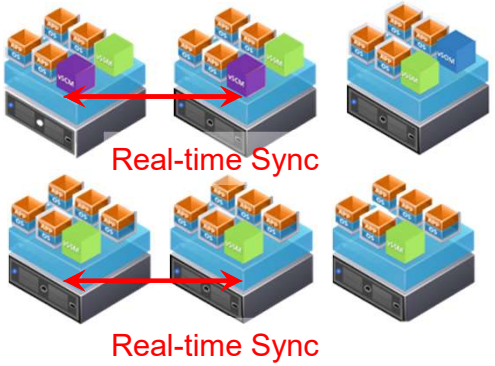
- Separation of data and management/control communication channels
- Private proxy instead of IP for management

Highly Available Distributed Architecture



Distributed Processing & Non-Distributed Architecture

Distributed Processing & Fully-Distributed Architecture



- vSOM “VM shutdown” does not affect CloudHive service
- Separation of management, control and service plane ensures 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)

Deep Visibility

Deep Visibility

Improved Productivity

Micro-Segmentation

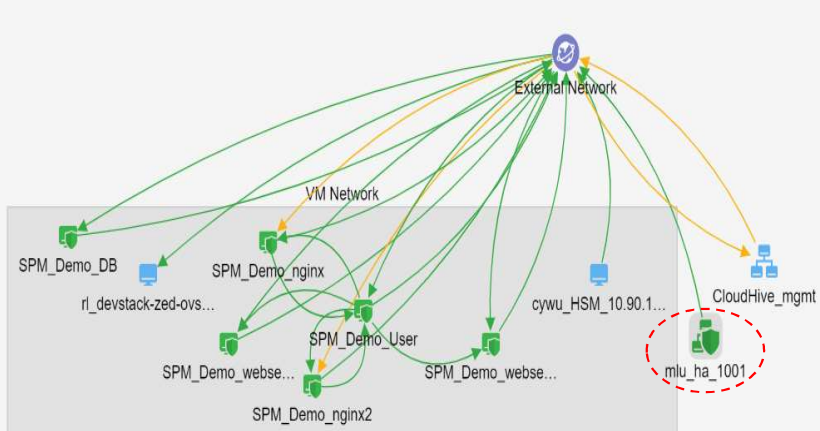
High Available Distributed Architecture

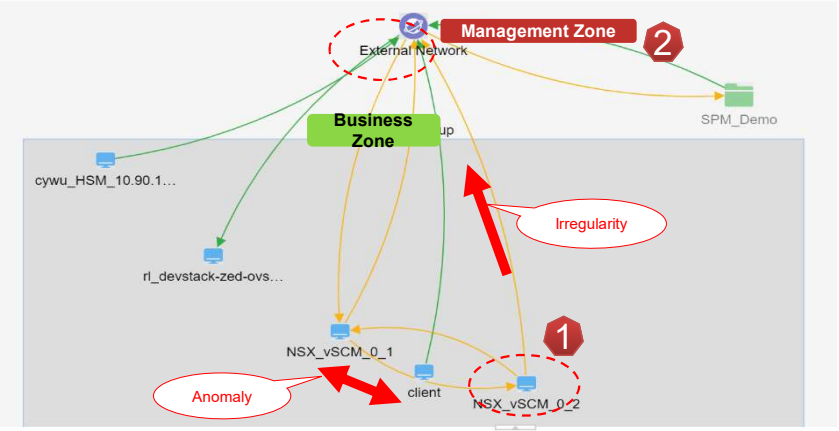
Visibility of Virtual Assets

Cloud Monitoring Statistic

Components Running Status Monitoring

Virtual Network Resource Topology





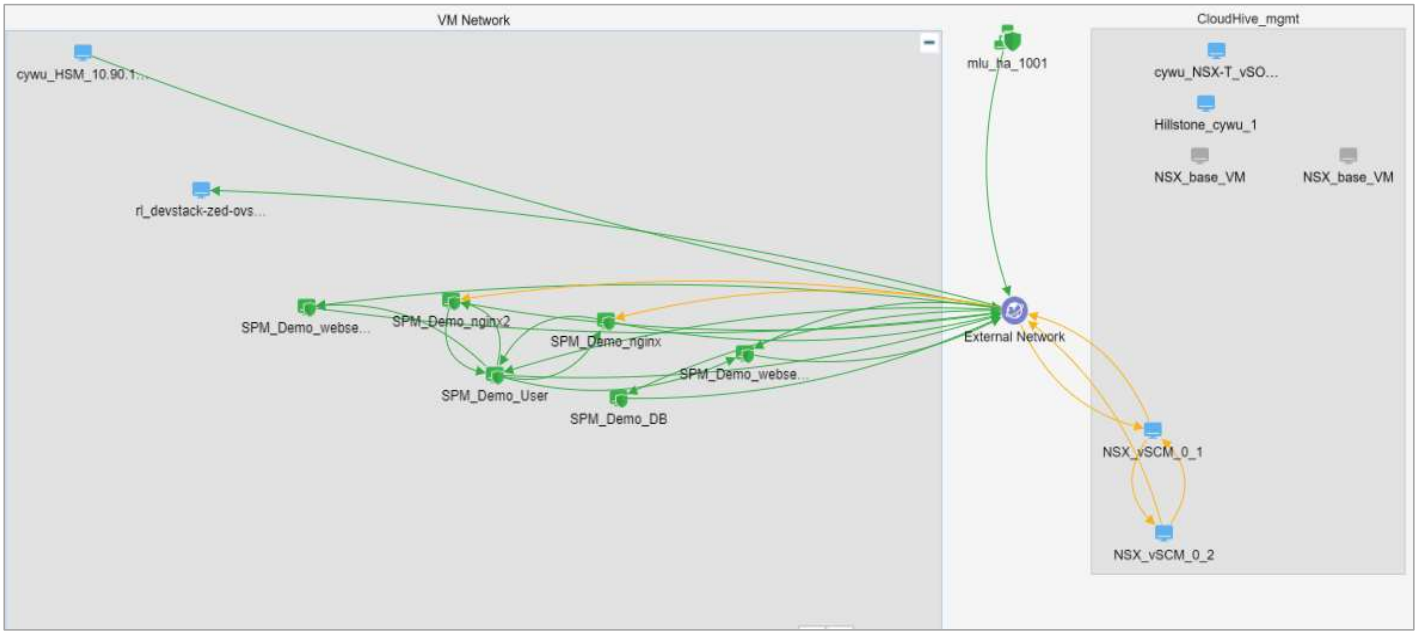
Overview

- Network architecture
- Virtual machine density
- The complexity of interaction between virtual machines

Scrutiny

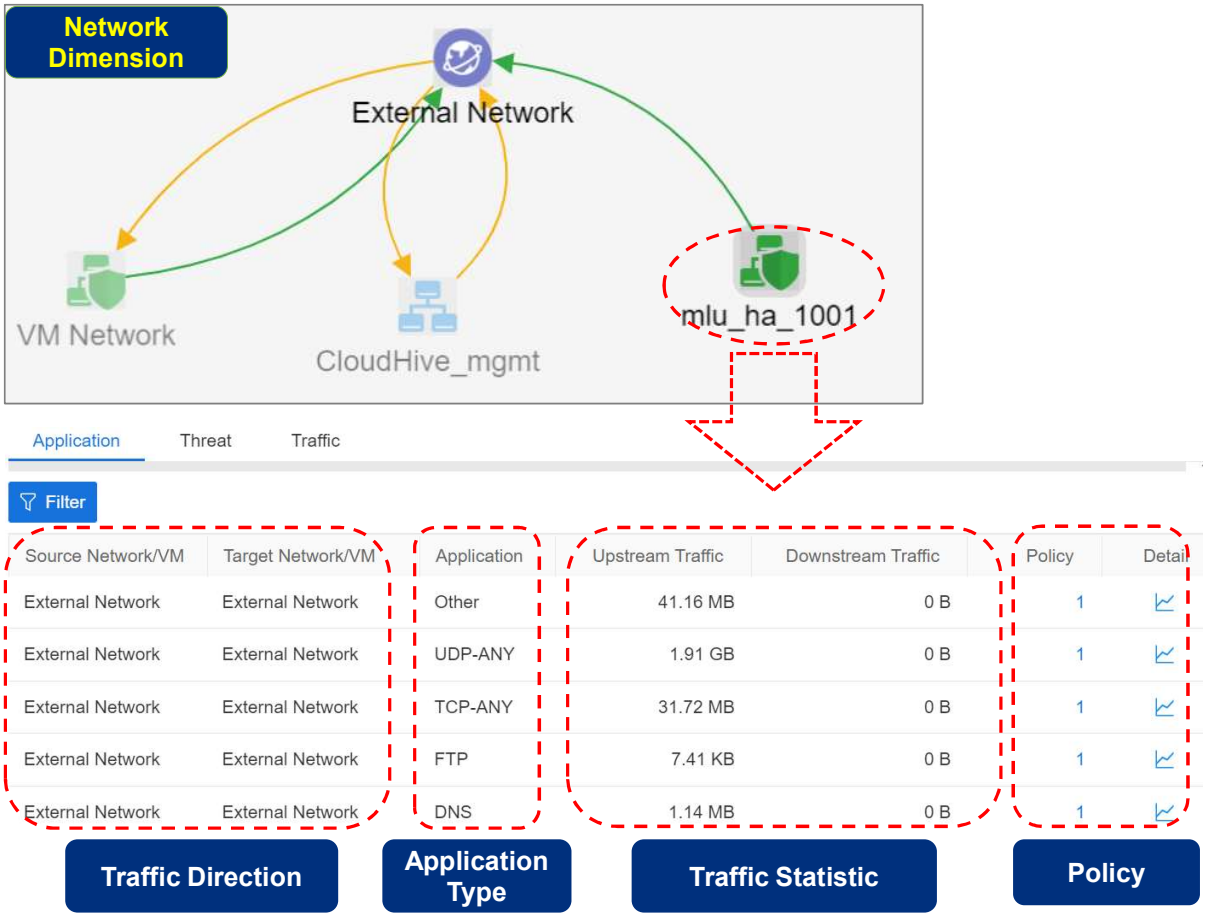
- Affiliation between network and virtual machines
- Traffic interaction in network
- Traffic interaction between virtual machines
- Anomalies and irregularities

Display of Complex Internal Communications

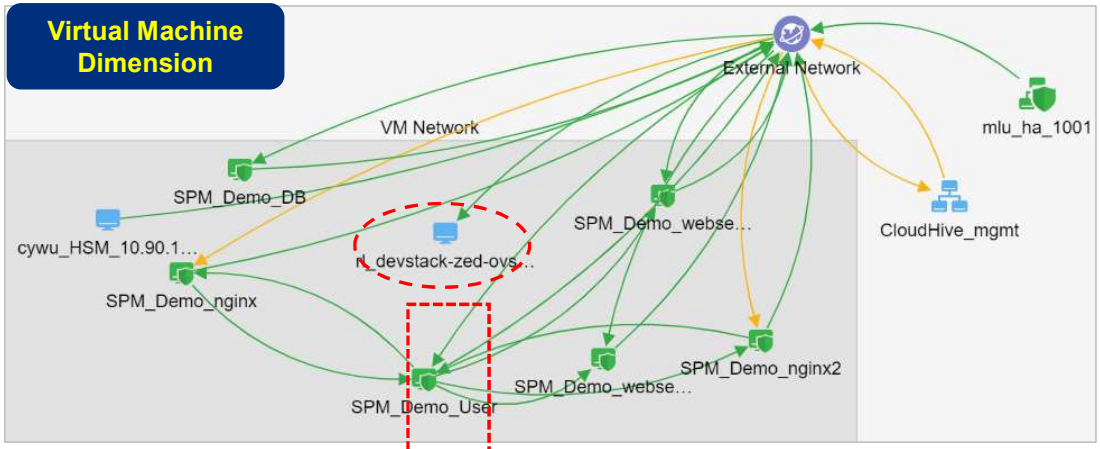


- **Line** stand for flow interaction
- **Arrow** stand for communication direction
- **Red Line** stand for network threat

Application Visibility – Network View



Application Visibility – Virtual Machine View



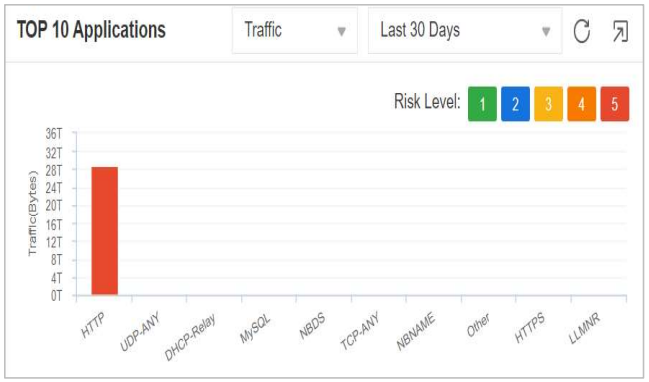
Application | Threat | Traffic

Filter

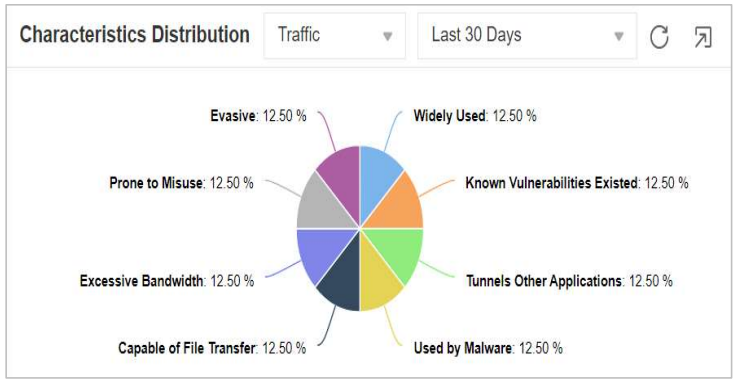
Source Network/…	Target Network/VM	Application	Upstream Traffic	Downstream Traffic	Policy	Detail
External Network	rl_devstack-zed-…	TCP-ANY	45.63 KB	0 B	1	
External Network	rl_devstack-zed-…	HTTP	5.48 KB	0 B	1	
External Network	rl_devstack-zed-…	SSH	396 B	0 B	1	

Traffic Direction | **Application Type** | **Traffic Statistic** | **Policy**

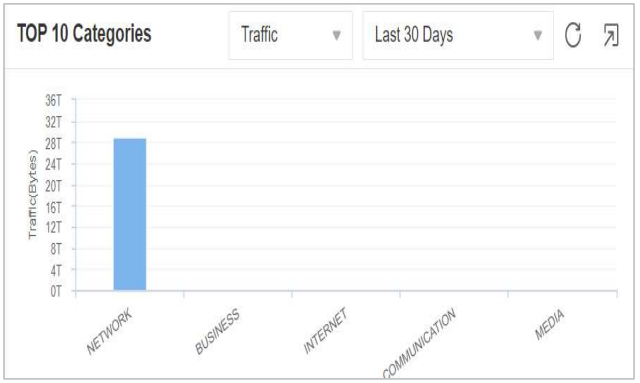
Application View



Top 10 Application

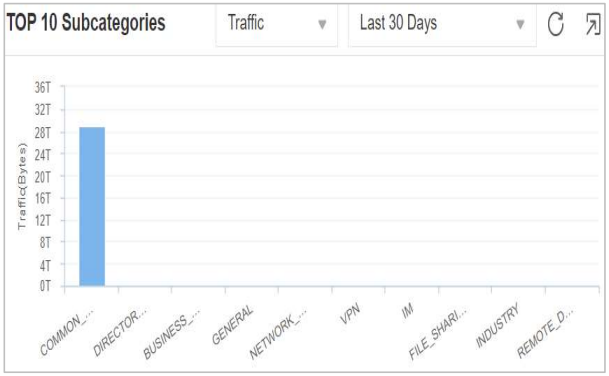


Characteristic Distribution

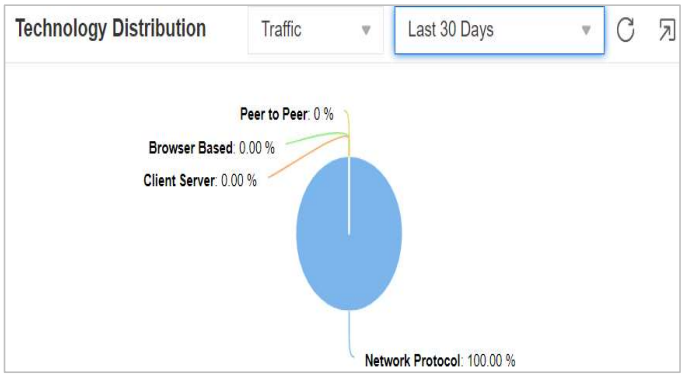


Top 10 Category

Risk Distribution



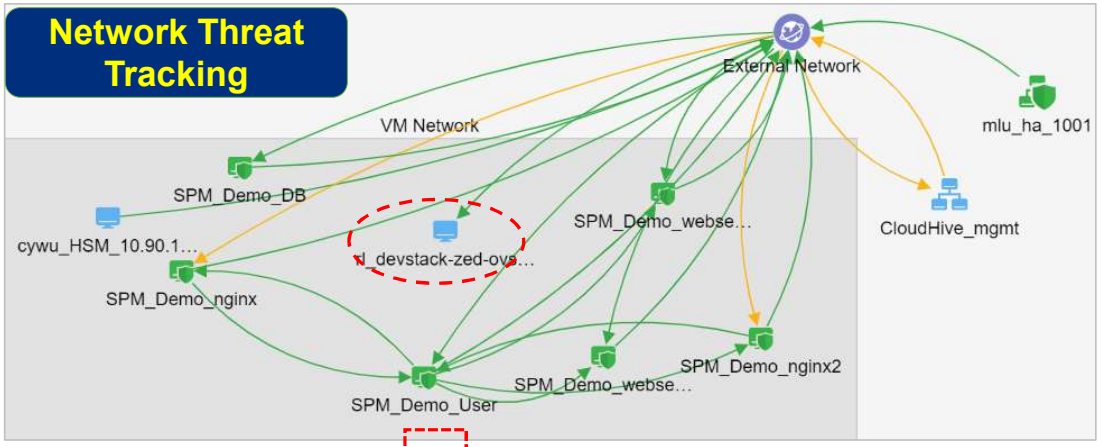
Top 10 Subcategory



Technology Distribution

Network Threat Visibility

- Web attack
- Spoofing
- Hijacking
- DDoS flood
- Cross-site scripting



Application | Threat | Traffic

Filter

Source Network/VM	Target Network/VM	Name	Threat ID	Type	Severity	Application/Protocol	Attacks
External Network	External Network	syn-flood		DoS - DDOS Flood	Medium	Unknown-APP/TCP	2
External Network	VLAN1101	FTP 3Com 3CDaemon I...	205119	Attack - Vulnerability Ex...	Low	FTP/TCP	348
External Network	VLAN1101	FTP CWD Command Bu...	205042	Attack - Vulnerability Ex...	Medium	FTP/TCP	52
External Network	VLAN1101	udp-flood		DoS - DDOS Flood	Medium	Unknown-APP/UDP	2
VLAN1101	External Network	syn-flood		DoS	Medium	Unknown-APP/TCP	71

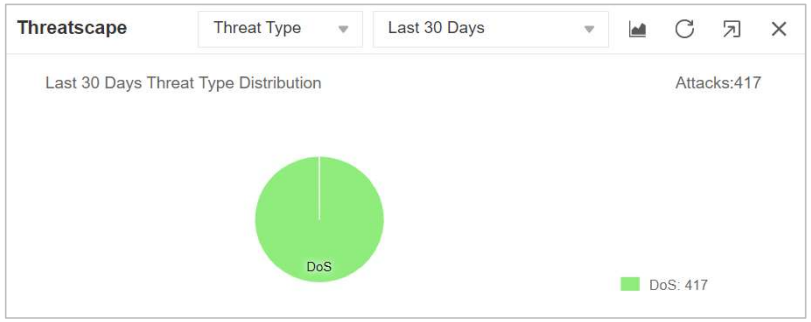
Traffic Direction

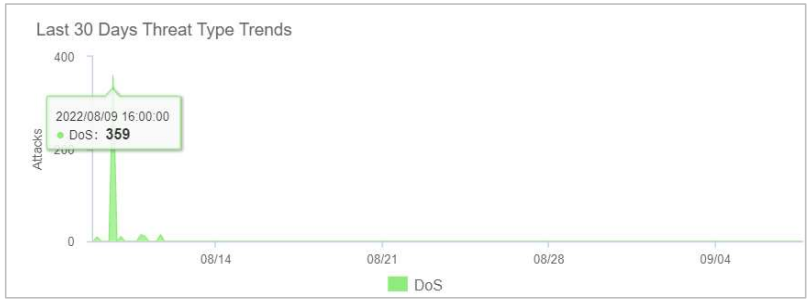
Threat Name

Detail

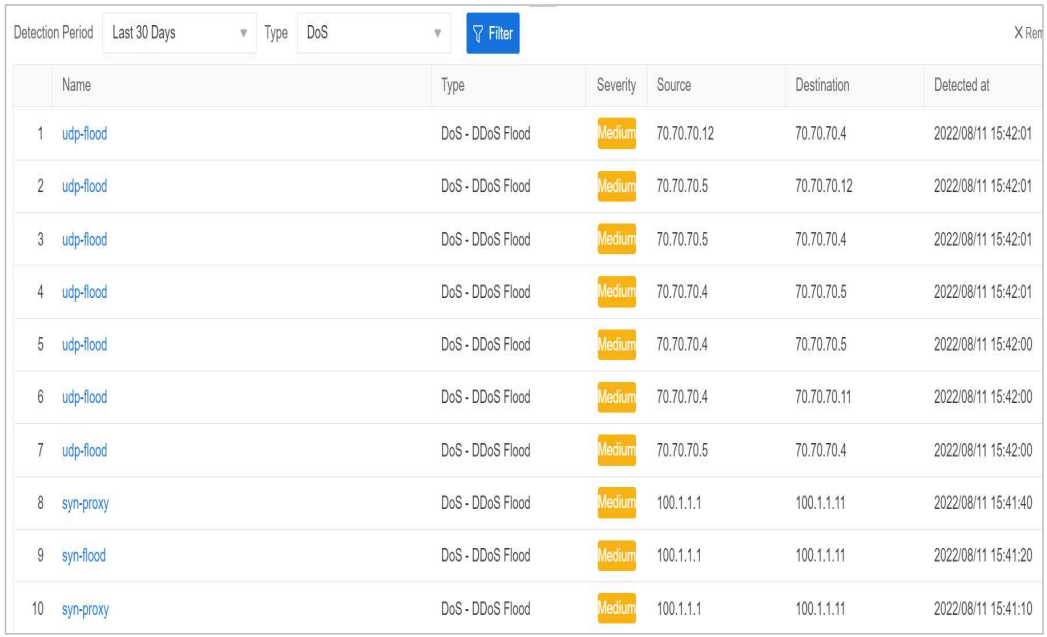
Network Threat Statistic

Threat Distribution



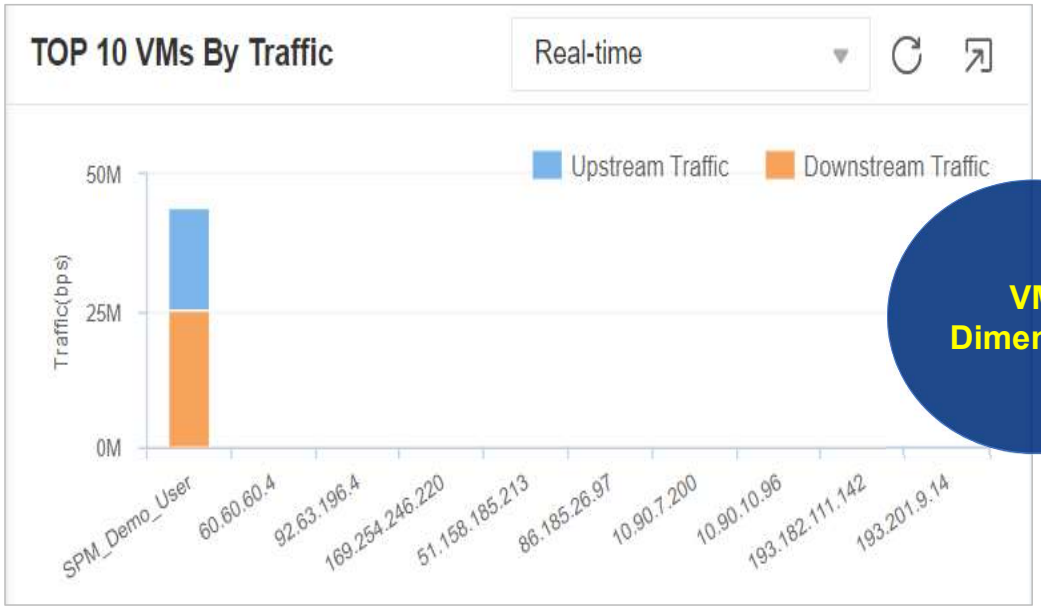


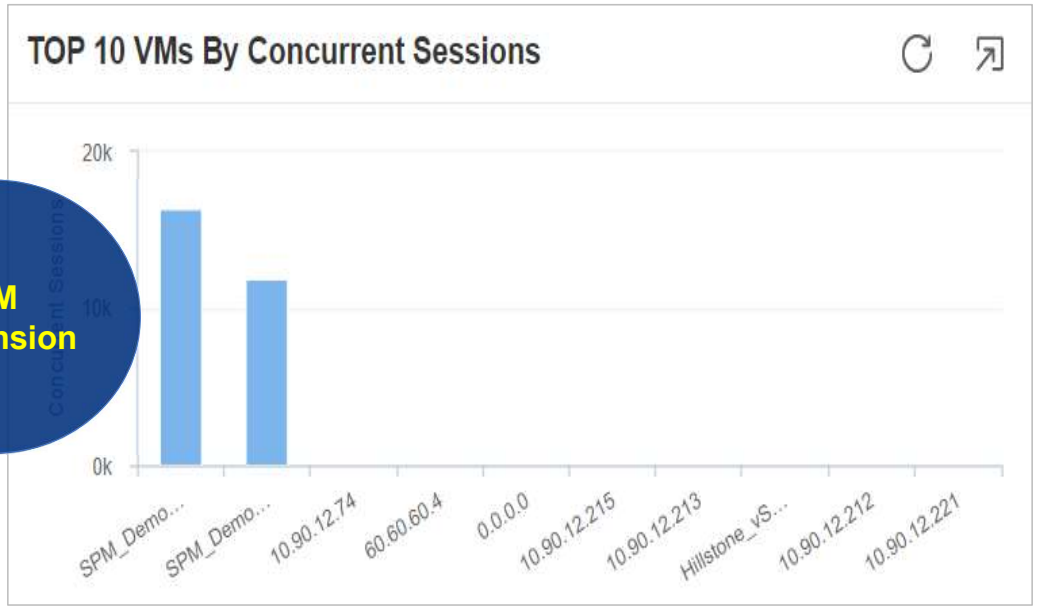
Threat Details



	Name	Type	Severity	Source	Destination	Detected at
1	udp-flood	DoS - DDoS Flood	Medium	70.70.70.12	70.70.70.4	2022/08/11 15:42:01
2	udp-flood	DoS - DDoS Flood	Medium	70.70.70.5	70.70.70.12	2022/08/11 15:42:01
3	udp-flood	DoS - DDoS Flood	Medium	70.70.70.5	70.70.70.4	2022/08/11 15:42:01
4	udp-flood	DoS - DDoS Flood	Medium	70.70.70.4	70.70.70.5	2022/08/11 15:42:01
5	udp-flood	DoS - DDoS Flood	Medium	70.70.70.4	70.70.70.5	2022/08/11 15:42:00
6	udp-flood	DoS - DDoS Flood	Medium	70.70.70.4	70.70.70.11	2022/08/11 15:42:00
7	udp-flood	DoS - DDoS Flood	Medium	70.70.70.5	70.70.70.4	2022/08/11 15:42:00
8	syn-proxy	DoS - DDoS Flood	Medium	100.1.1.1	100.1.1.11	2022/08/11 15:41:40
9	syn-flood	DoS - DDoS Flood	Medium	100.1.1.1	100.1.1.11	2022/08/11 15:41:20
10	syn-proxy	DoS - DDoS Flood	Medium	100.1.1.1	100.1.1.11	2022/08/11 15:41:10

Network Traffic Statistic



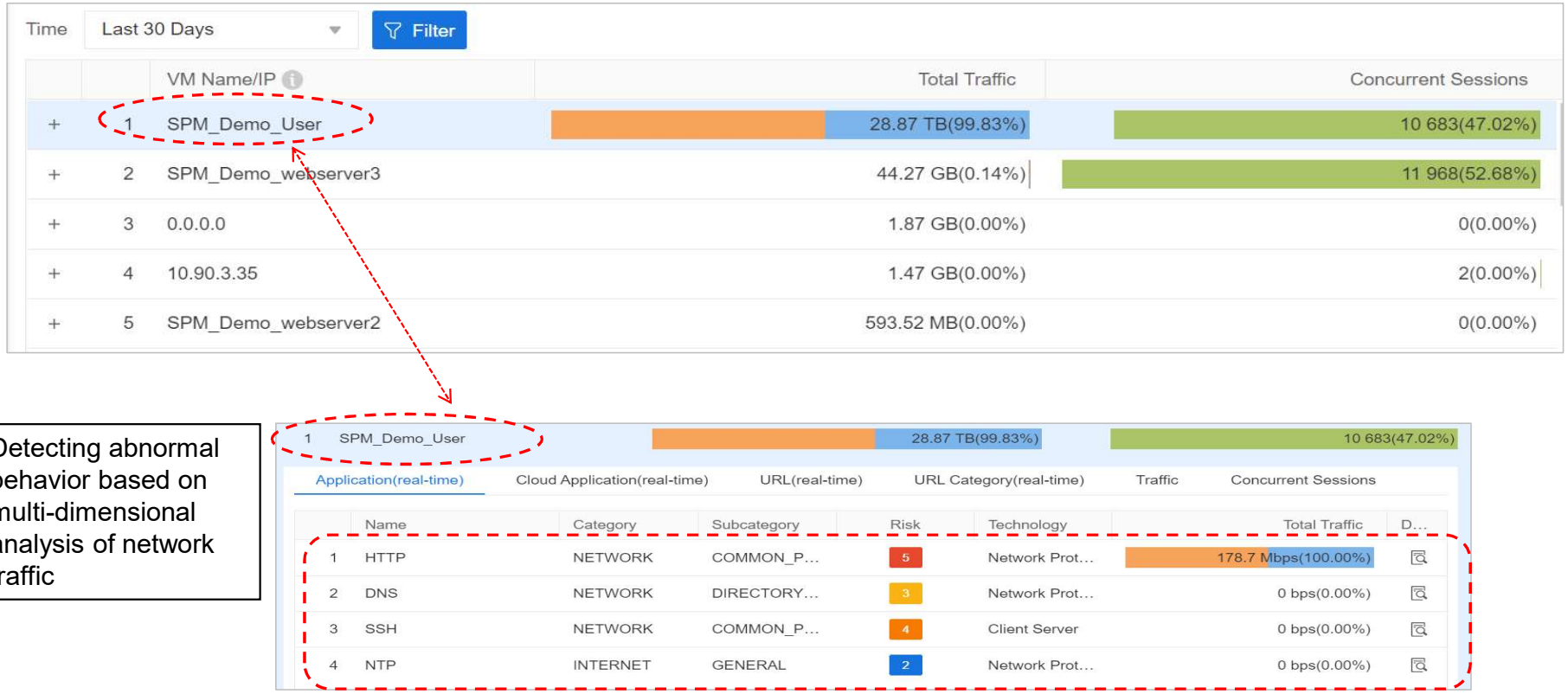


VM Dimension

Top 10 VMs by Traffic

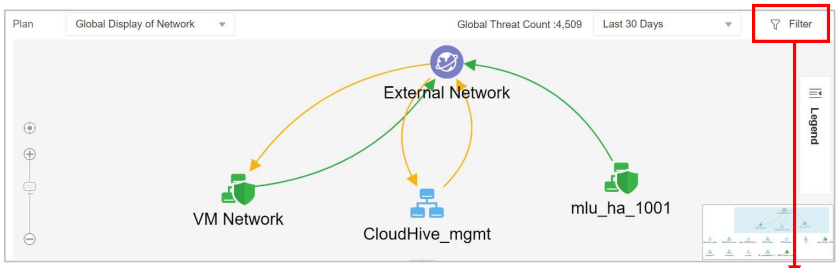
Top 10 VMs by Concurrent Sessions

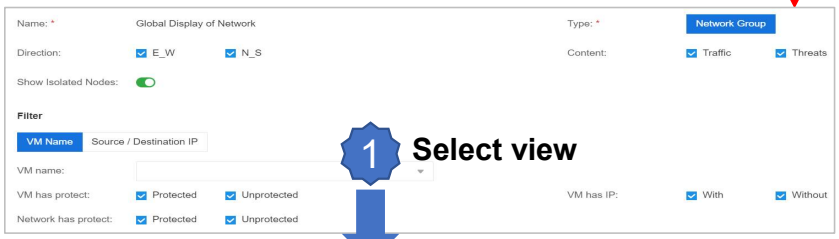
Network Traffic Tracking



Detecting abnormal behavior based on multi-dimensional analysis of network traffic

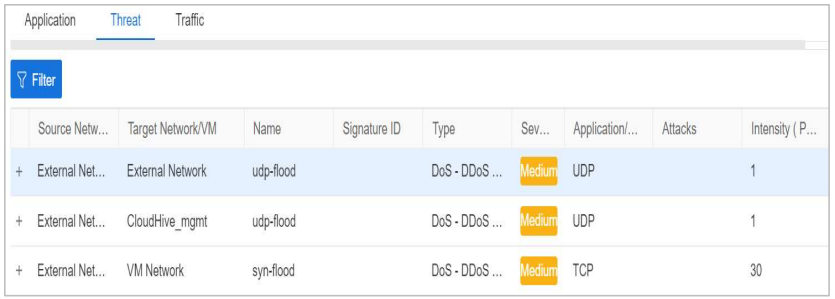
Visibility - Accurate Depiction of Threat

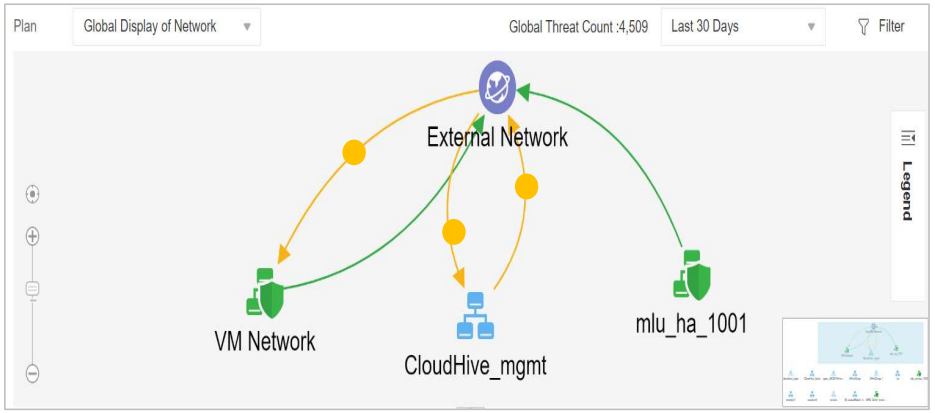




1 **Select view**

2 **Select application/threat**





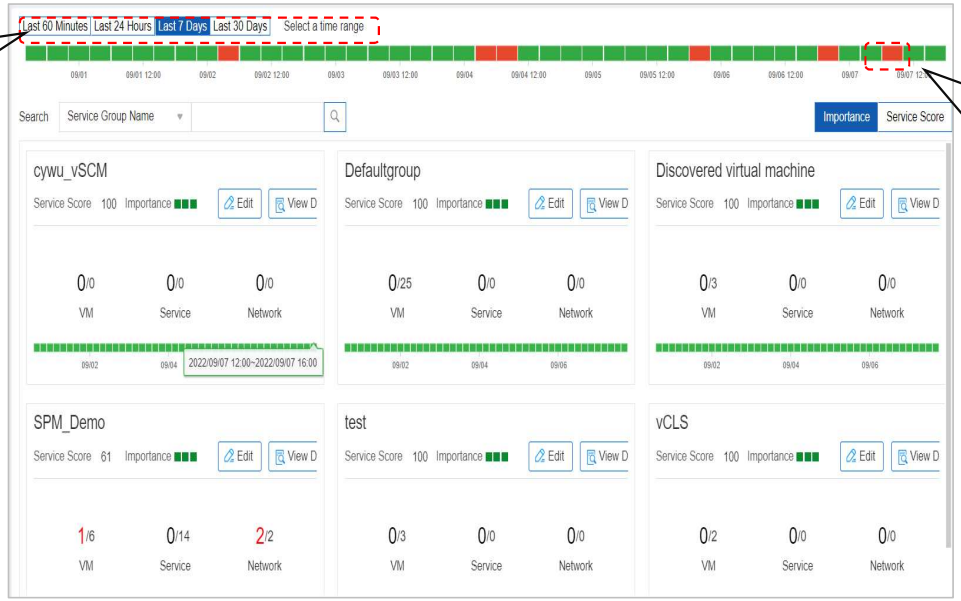
3 **Where does the particular application/threat occur**

Service Performance Monitor (SPM) - Overview

Displays the performance data of virtual machines, services, and networks in the service group synchronized from the group management function.

view monitoring data during the past hour/day/week/month period

The time interval can be 1 minute / 1 hour / 4 hours / 12 hours according to the selected monitoring period

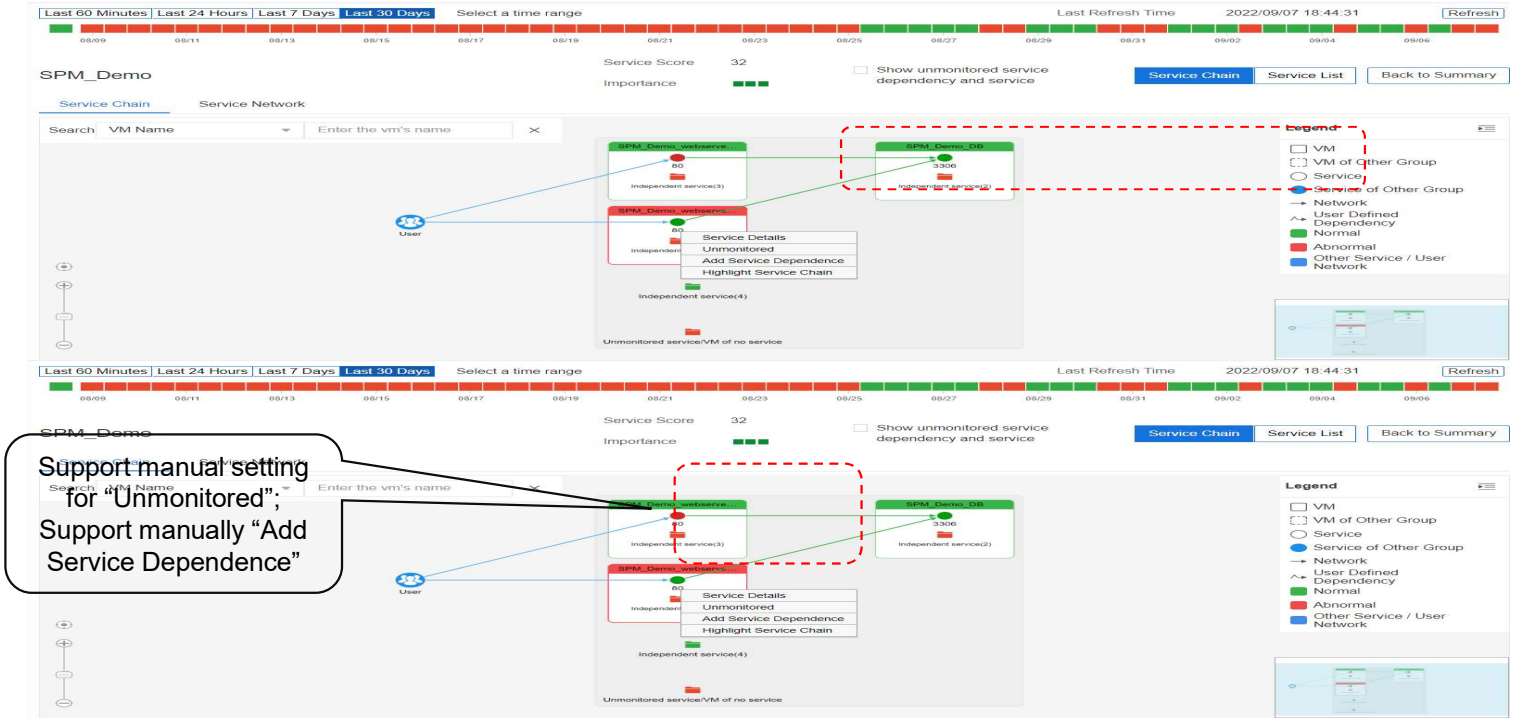


Green column: virtual machine / service / network is normal
Red column: The performance of a certain business exceeds the set threshold within that time range.

Note: Upon modifying the monitoring threshold, the alarm information in the historical data will not be updated.

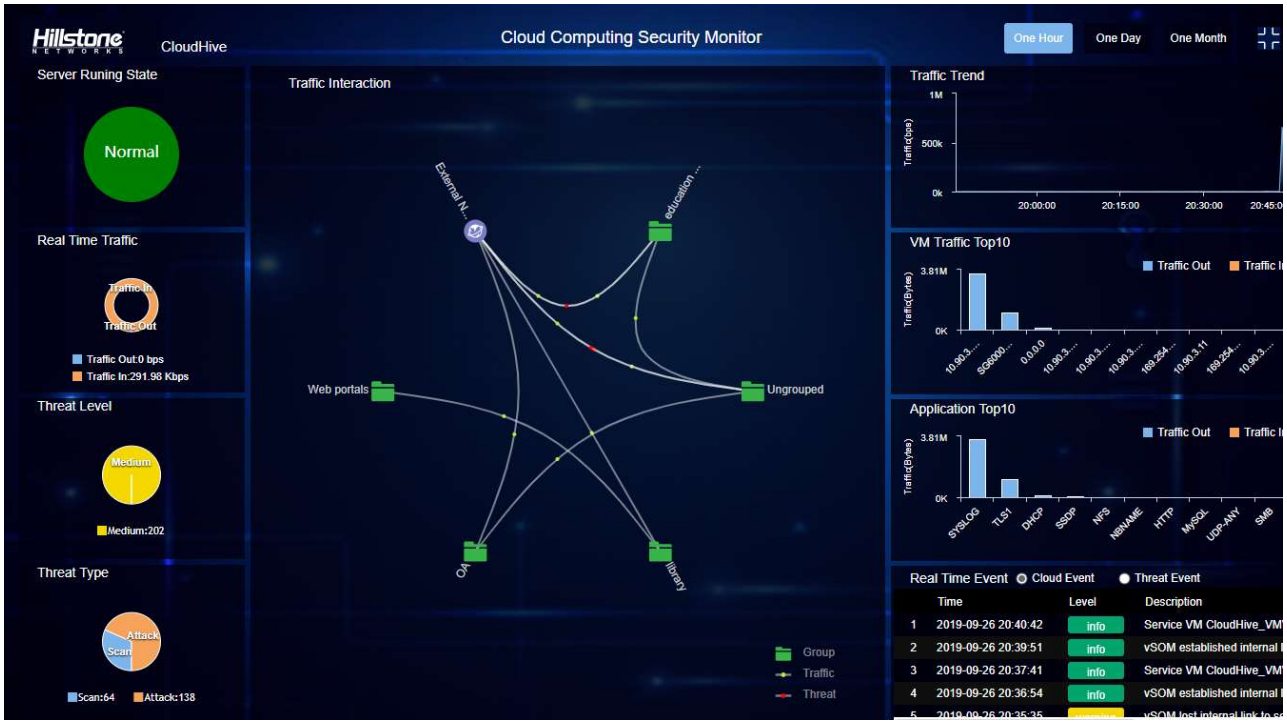
Service Performance Monitor (SPM) - Details

Display services and their internal and external connections in a topology view.



Screen Casting

Users can intuitively understand the overall situation of the entire cloud environment from this interface.



Comprehensive Threat Report

The report can generate necessary information for users to perform data retention, reporting, and other tasks on network data, and can provide important support for compliance audits.

Cloud Network Security Assessment Report

1. Security Status Assessment of Cloud Network

Assessment of the security status of cloud network:Analyze the coverage of CloudHive's security protection.

1.1. Overview of Network Isolation Status

The overview of network isolation status displays the protection scope of CloudHive.

1.1.1. Statistics of CloudHive's Protection Scope

The total number of virtual machines protected by CloudHive : 4, accounting for : 9.3%.

The coverage rate of CloudHive (micro-isolation) security service in the host : 2, accounting for 20%.

Traffic Assessment Report

2. Traffic Status Assessment

Assessment of Traffic status : Analyze the ranking of traffic data in both applications and virtual machines in two directions, inside the cloud and from the inside cloud to the outside cloud. Focus on the statistics of applications which may bring security risk to the cloud platform.

2.1. Statistics of Application Traffic

2.1.1. Overview of Application Risk

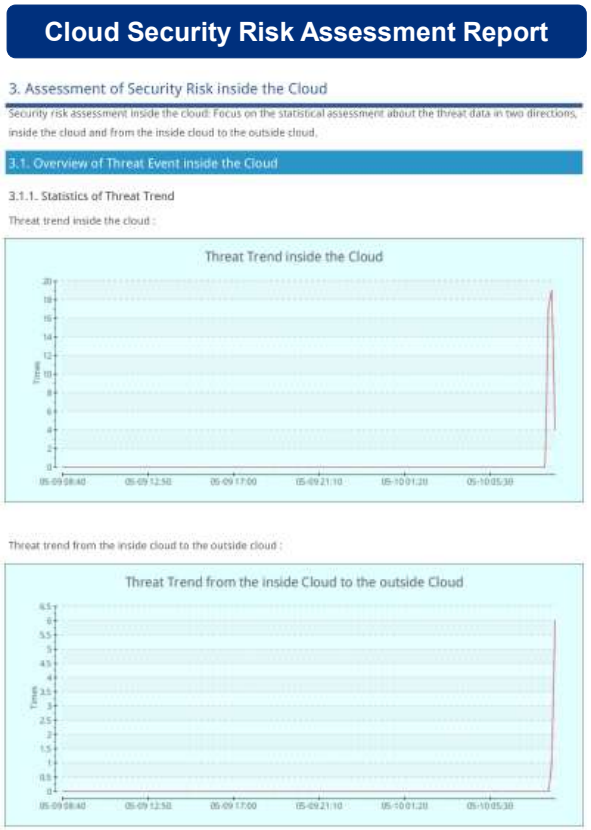
The statistics of number of applications inside the cloud is as follows, which are classified by 5 risk levels:

#	Risk Level	Number of Applications
1	Risk Level 1 (None)	0
2	Risk Level 2 (Low)	2
3	Risk Level 3 (Medium)	0
4	Risk Level 4 (High)	0
5	Risk Level 5 (Extremely High)	0

The statistics of number of applications from the inside cloud to the outside cloud is as follows, which are classified by 5 risk levels:

#	Risk Level	Number of Applications
1	Risk Level 1 (None)	1
2	Risk Level 2 (Low)	5
3	Risk Level 3 (Medium)	3
4	Risk Level 4 (High)	2
5	Risk Level 5 (Extremely High)	2

Cloud Security Risk Assessment Report



3. Assessment of Security Risk inside the Cloud

Security risk assessment inside the cloud: Focus on the statistical assessment about the threat data in two directions, inside the cloud and from the inside cloud to the outside cloud.

3.1. Overview of Threat Event inside the Cloud

3.1.1. Statistics of Threat Trend

Threat trend inside the cloud :

Threat Trend inside the Cloud

Threat trend from the inside cloud to the outside cloud :

Threat Trend from the inside Cloud to the outside Cloud

Comprehensive Threat Report

Application risk level overview

2. Traffic Status Assessment

Assessment of Traffic status : Analyze the ranking of traffic data in both applications and virtual machines in two directions, inside the cloud and from the inside cloud to the outside cloud. Focus on the statistics of applications which may bring security risk to the cloud platform.

2.1. Statistics of Application Traffic

The statistics of number of applications inside the cloud is as follows, which are classified by 5 risk levels:

#	Risk Level	Number of Applications
1	Risk Level 1 (None)	0
2	Risk Level 2 (Low)	2
3	Risk Level 3 (Medium)	0
4	Risk Level 4 (High)	0
5	Risk Level 5 (Extremely High)	0

The statistics of number of applications from the inside cloud to the outside cloud is as follows, which are classified by 5 risk levels:

#	Risk Level	Number of Applications
1	Risk Level 1 (None)	1
2	Risk Level 2 (Low)	5
3	Risk Level 3 (Medium)	3
4	Risk Level 4 (High)	2
5	Risk Level 5 (Extremely High)	2

High risk traffic statistics

Statistics of high-risk application traffic flowing from the inside cloud to the outside cloud:

Details of the high-risk application traffic from the inside cloud to the outside cloud :

#	Application	Number of Virtual Machines	Total Traffic	Traffic Out	Traffic In
1	HTTPS	1	61.76MB	1.74MB	60.01MB
2	HTTP	1	6.86MB	578.69KB	6.29MB
3	Skype	1	67.65KB	9.07KB	58.57KB
4	TLS1	1	792.00B	792.00B	0.00B

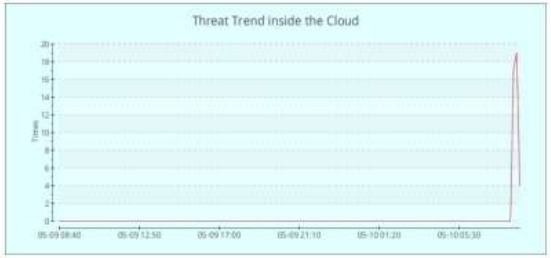
Cloud threat trends

3. Assessment of Security Risk inside the Cloud

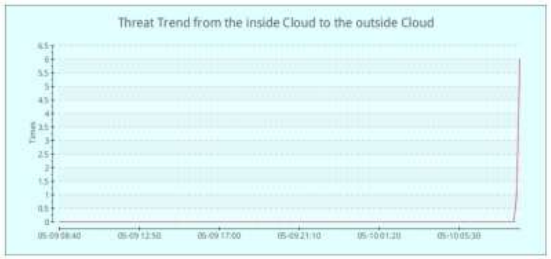
Security risk assessment inside the cloud: Focus on the statistical assessment about the threat data in two directions inside the cloud and from the inside cloud to the outside cloud.

3.1.1. Statistics of Threat Trend

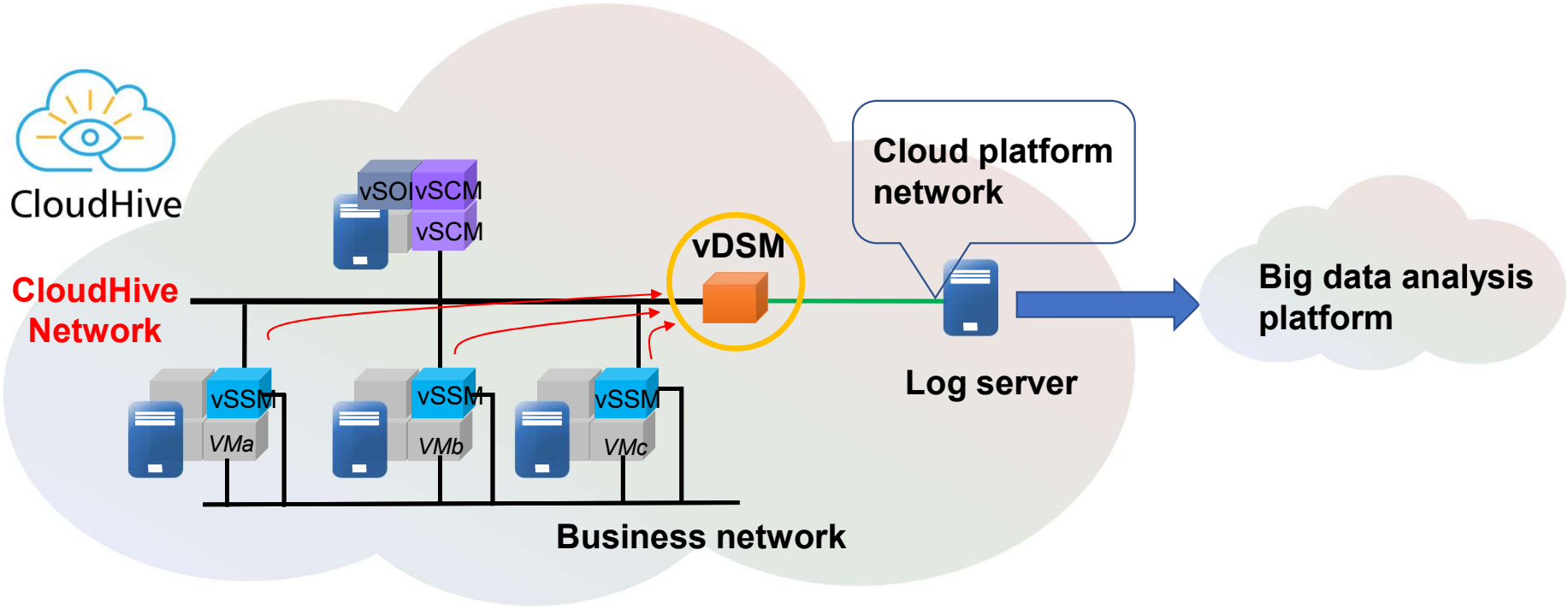
Threat trend inside the cloud :



Threat trend from the inside cloud to the outside cloud :

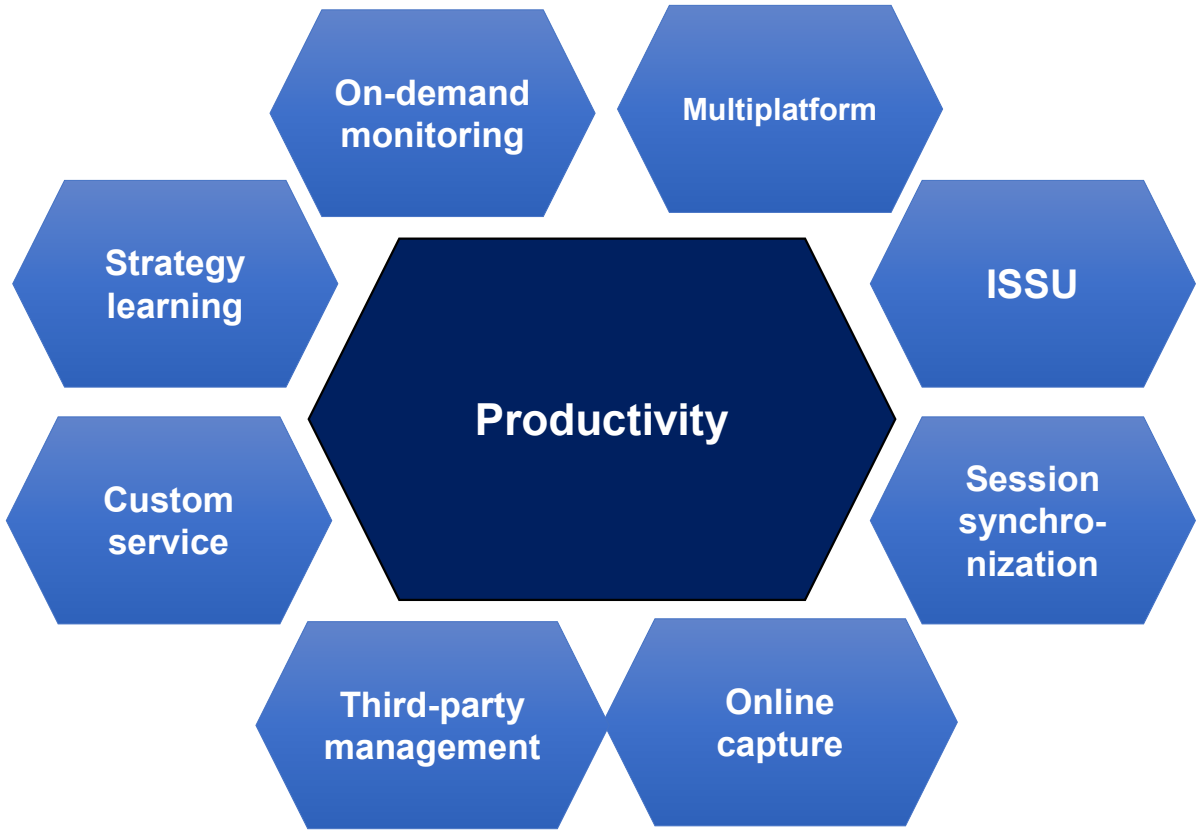


Threat/Session Log Output at a High Speed

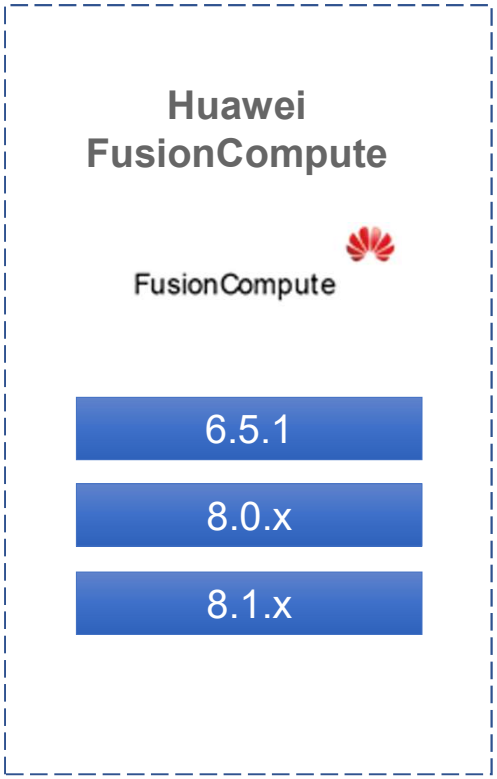


High Productivity

Productivity: Automation, Compatibility and Scalability

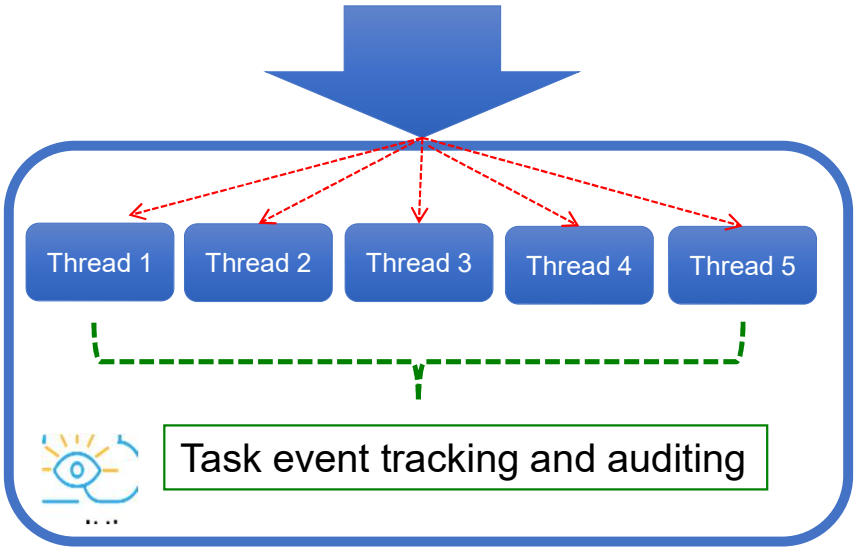


Support for Multiple Virtualized Platform



Efficient Processing

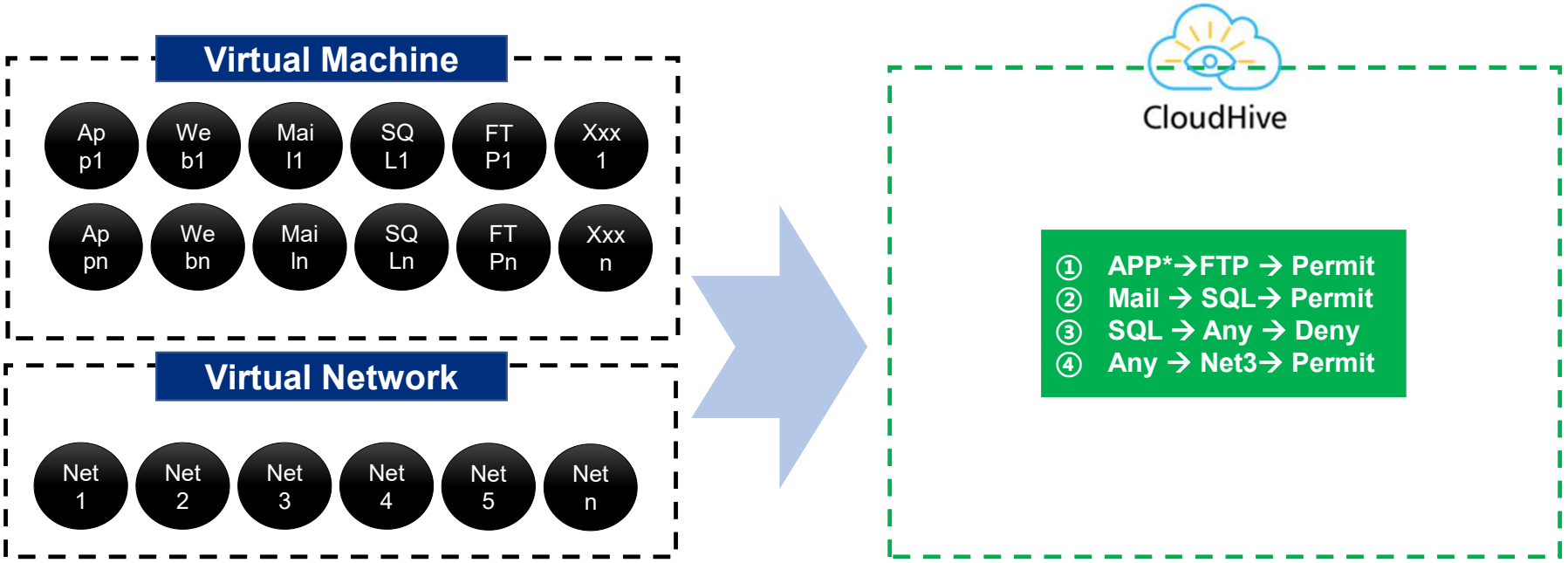
Concurrent transactions



5 **Provide 5 threads, parallel processing**
No waiting, continuous operation

3 **Faster, 3x more efficient**

On-Demand, Flexible Control



Faster, 3x more efficient

- On-demand based on VM or virtual network dimension, achieving security monitoring elastic scaling
- Support wildcard matching virtual machine names security policy control, achieving rapid batch control

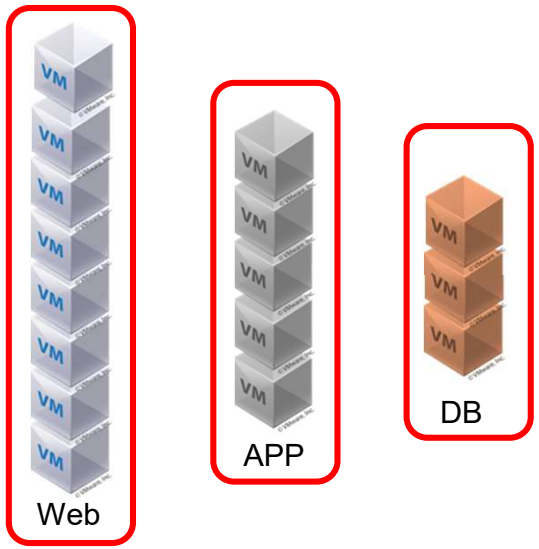
Increase Policy for Same Type of VMs

Hillstone NETWORKS

- Separate security domains for each type of VMs
- Deploy appropriate security policies for each type VM security domain

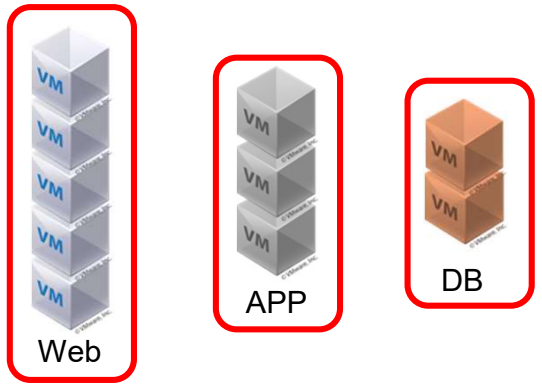
Daily 1

- The same type of newly-added virtual machine is automatically put into the corresponding security domain
- Deploy similar security policies for the same type of newly-added virtual machines



Double 11 shopping season

- Reduced virtual machine, automatic adjustment of security domain



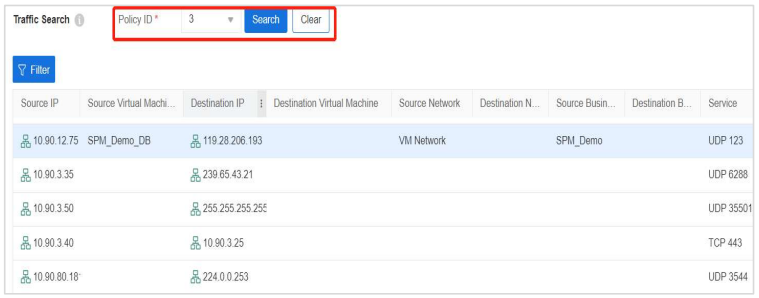
New Year shopping season

Policy Assistant

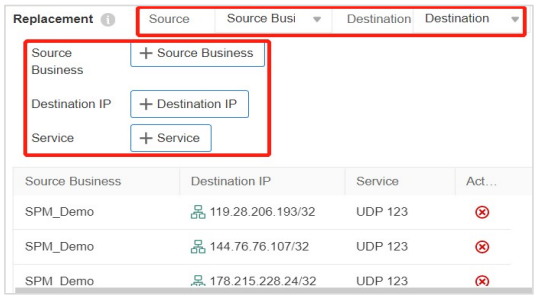
Policy Assistant

1 Display Traffic — 2 Replace — 3 Aggregate — 4 Generate Address Book — 5 Generate Service Book — 6 **Generate Policy**

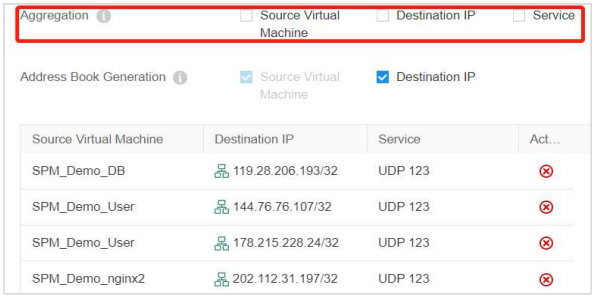
Micro-segmentation Policy



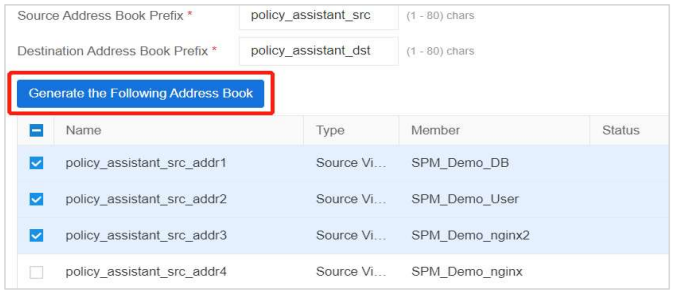
Step1: Display Traffic (view session log)



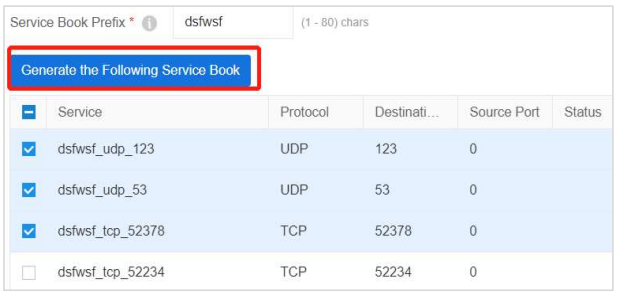
Step2: Replace (replacement based on Source VM/ Dest IP/ Service)



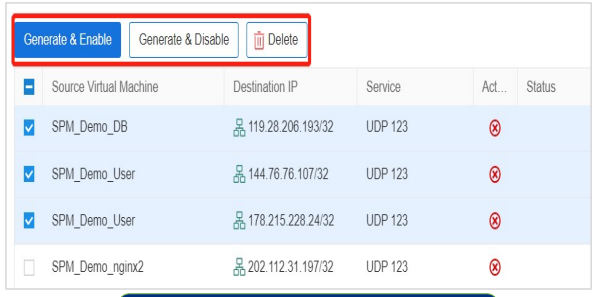
Step3: Aggregate (aggregation based on Source VM/ Dest IP, Service)



Step4: Generate Address Book

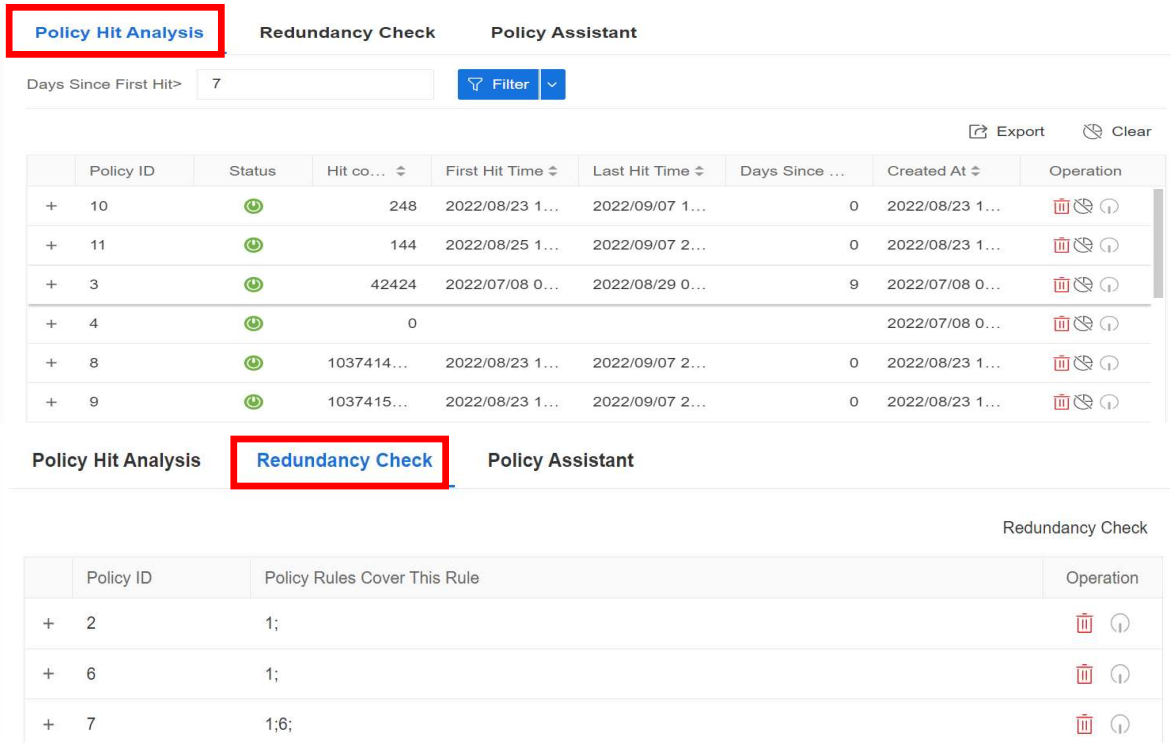


Step5: Generate Service Book



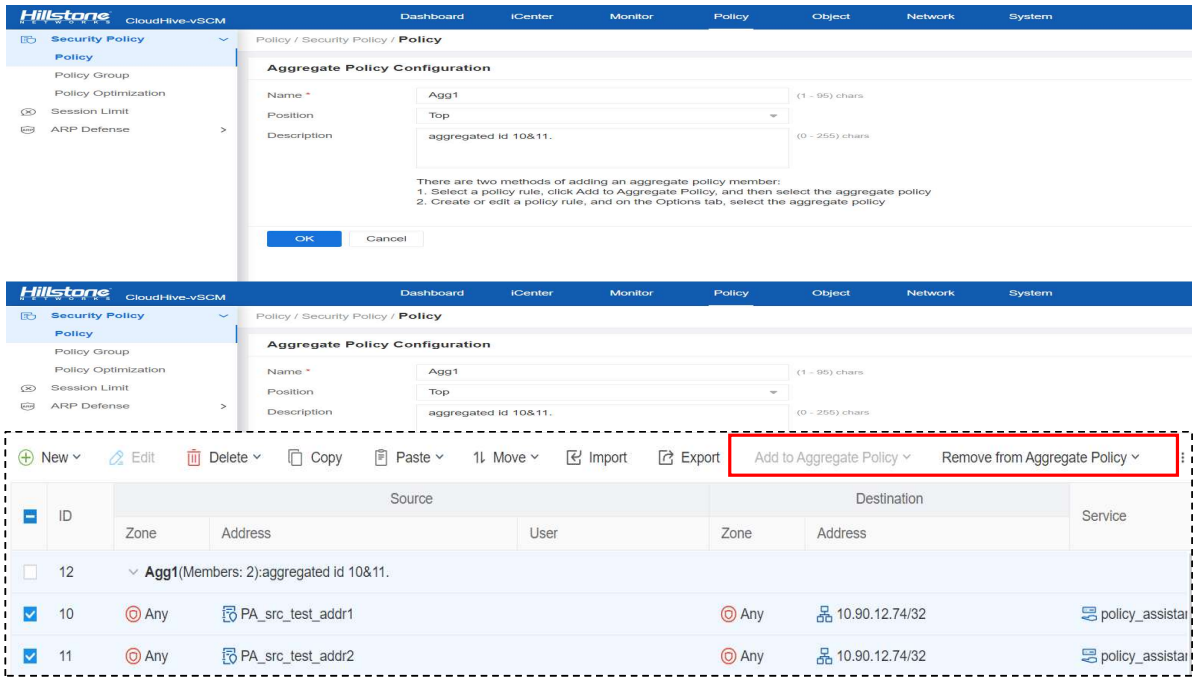
Step6: Generate & Enable/Disable Policy

Policy Hit and Redundancy Check



- Develop and execute on an overarching network strategy
- Standardize and make mass policy proliferation more efficient

Policy Aggregation



- Aggregate a set of policies that with similar attributes or functions, to meet the specific needs
- Improve O&M efficiency of policies

Customized Services

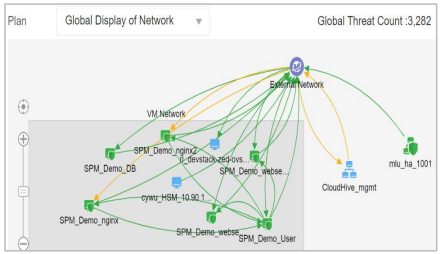
Communication Traffic:
TCP: 8888
TCP: 4321
TCP: 33389, …..

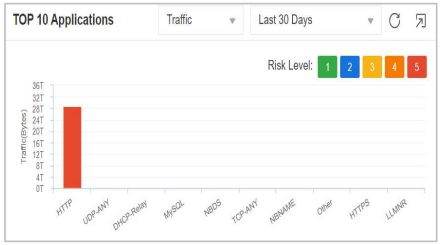
What is this application/service?

Customized Server Name

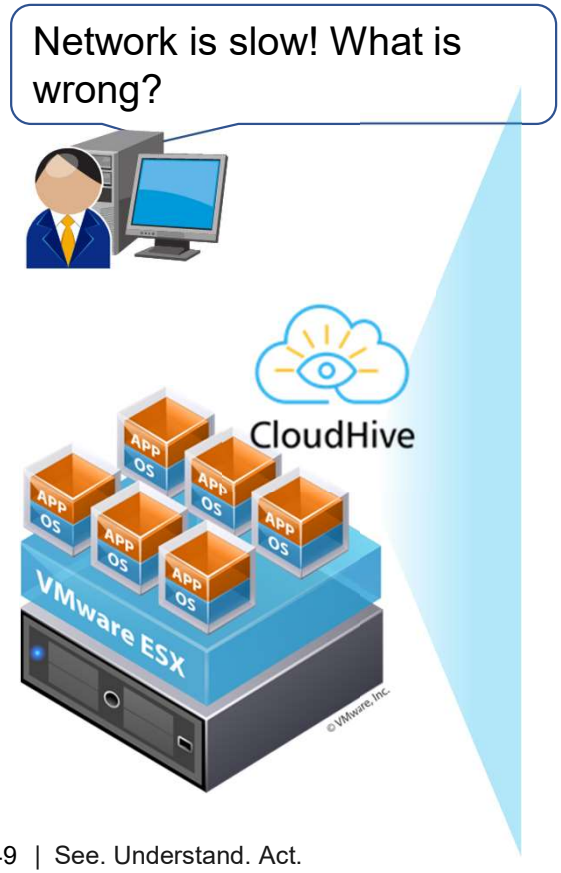
① TCP: 8888 → Front Web server
② TCP: 4321 → FTP serer
③ TCP: 33389 → The fortress machine remote desktop

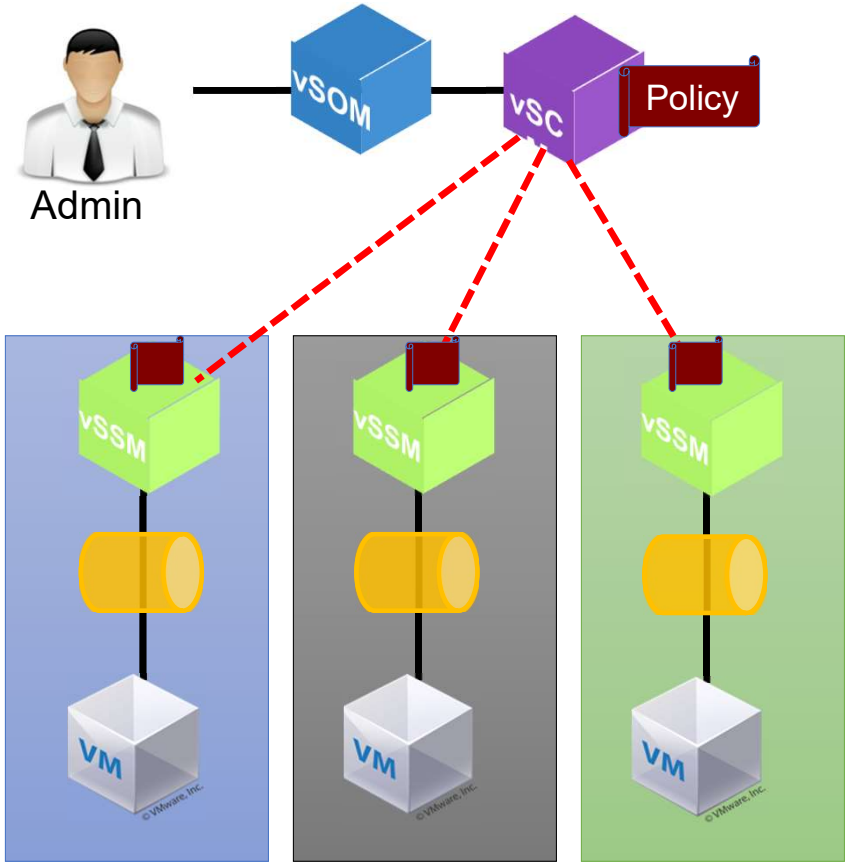
Dashboard





Packet Capture in the Cloud





Steps:

① Configure capture policy
② Distribute to all vSSM modules
③ Deliver captured data

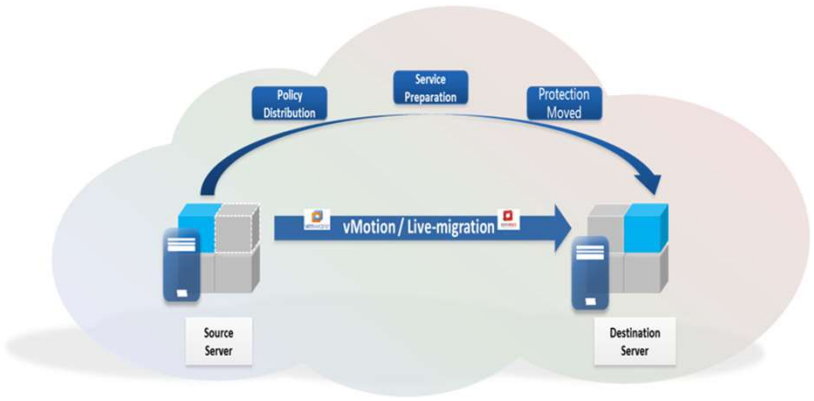
Benefit:

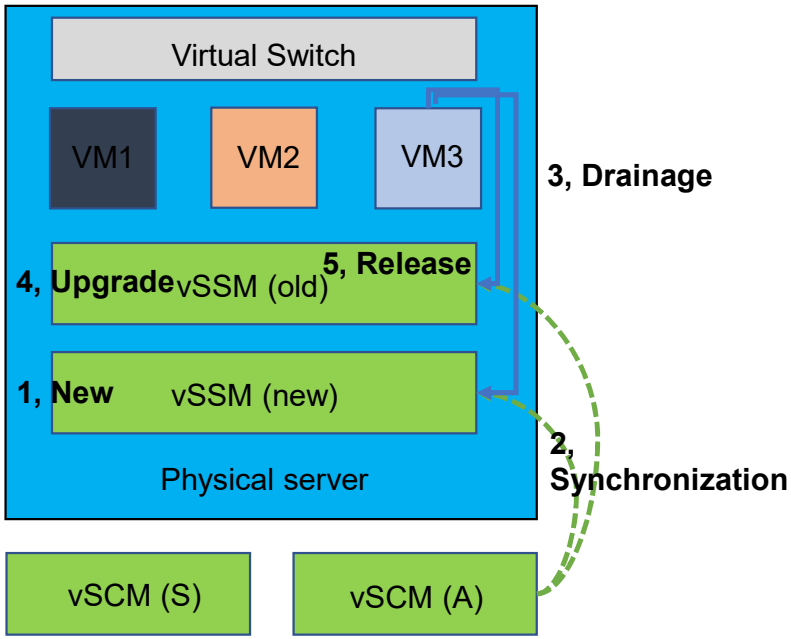
Help the administrator locate any gaps in the cloud, regardless of:

- Data source
- Destination
- Simultaneous and multiple capture points

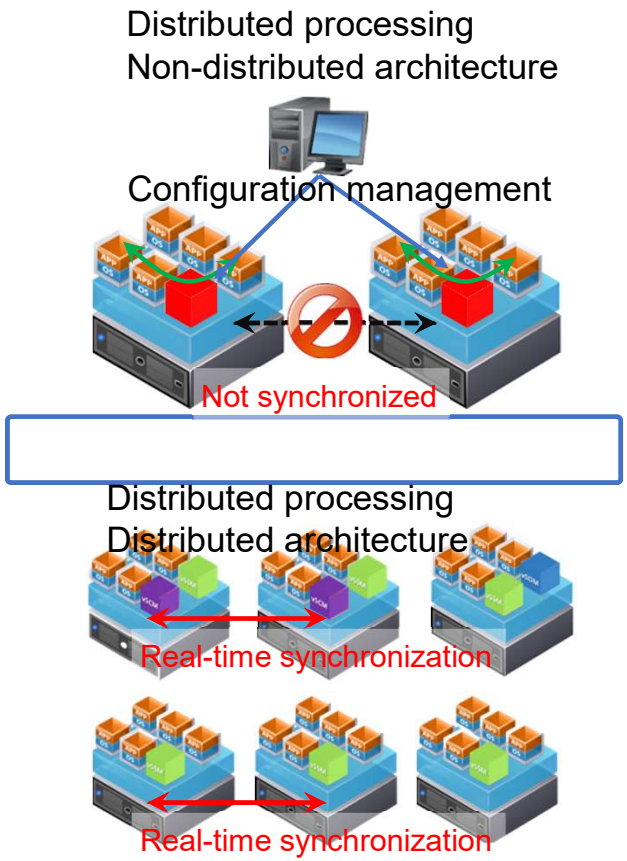
Guarantee Business Continuity

Prevent disruptions during VM migrations





HA of Distributed Architecture



- **Redundancy protection:** main control module HA, real-time synchronization
- **Support migration:** HA based on universal mature virtualization migration technology (vSOM and vSCM only)
- **Bypass function:** vSSM module failure leads to unlock protection
- **Self-recovery capability:** system automatically rebuilt after the vSSM module lost
- **Security Service Following:** automated Session and Policy Following in Virtual Machine Migration

Micro-Segmentation

Deep Visibility

Improved Productivity

Micro-Segmentation

Highly Available Distributed Architecture

Common Micro-Segmentation Solutions

CloudHive + VDS&VSS OVS

CloudHive + NSX

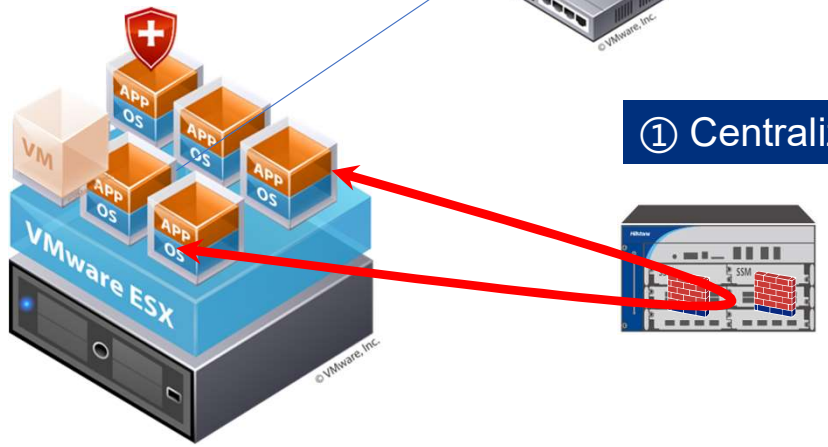
⑤ Does not rely on virtual machine monitors

④ Virtual Machine Monitor Agent Software

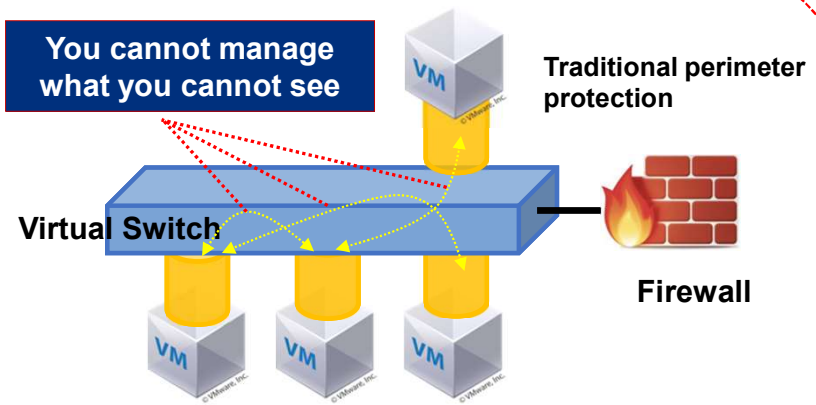
② Host agent protection

③ Network switch control

① Centralized physical protection

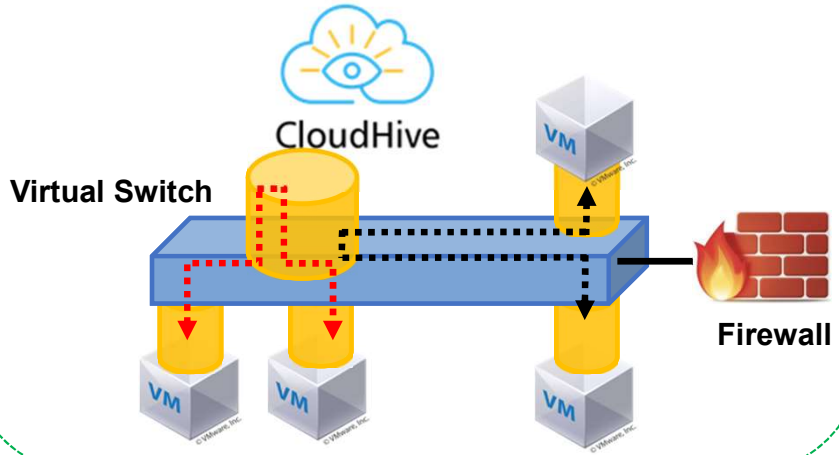


CloudHive Micro-Segmentation

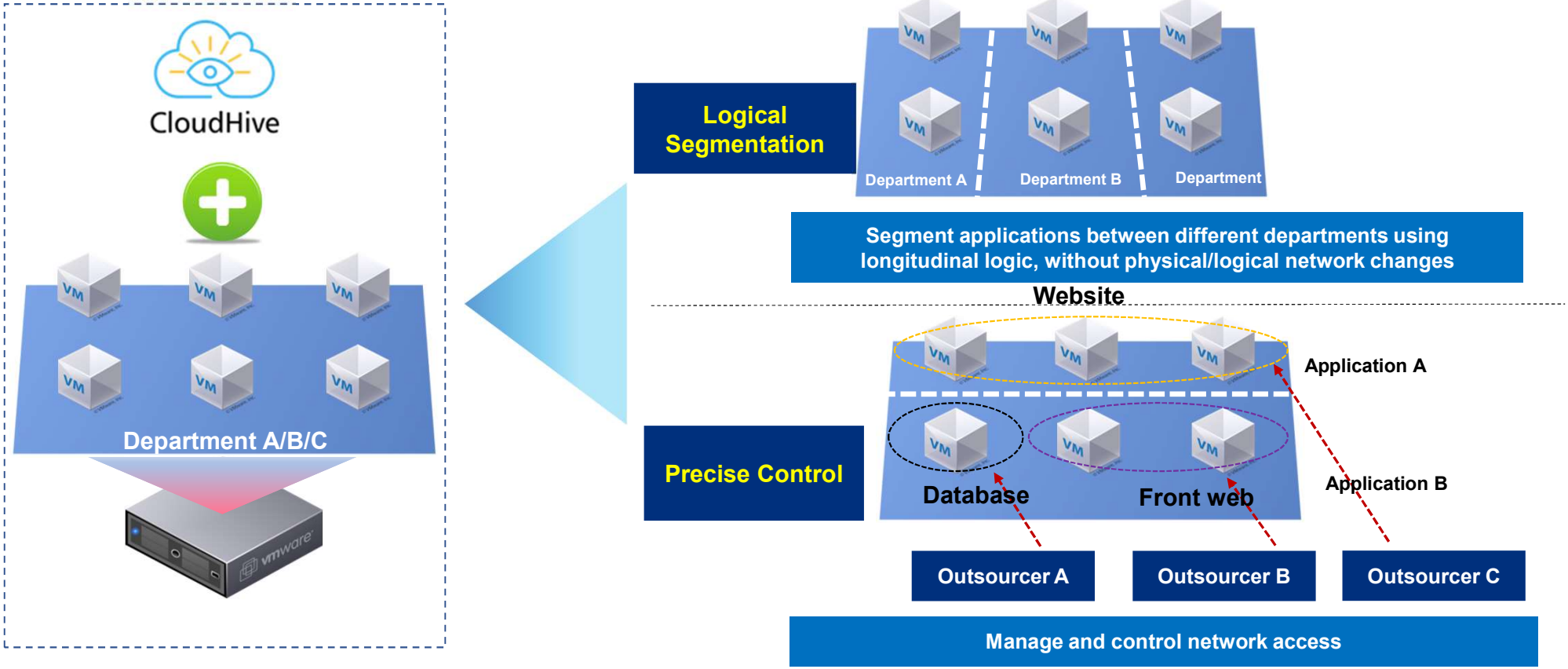


- Internal communication is not visible
- Difficult to control internal risk propagation
- Perimeter protection has limits
- Limited endpoint protection

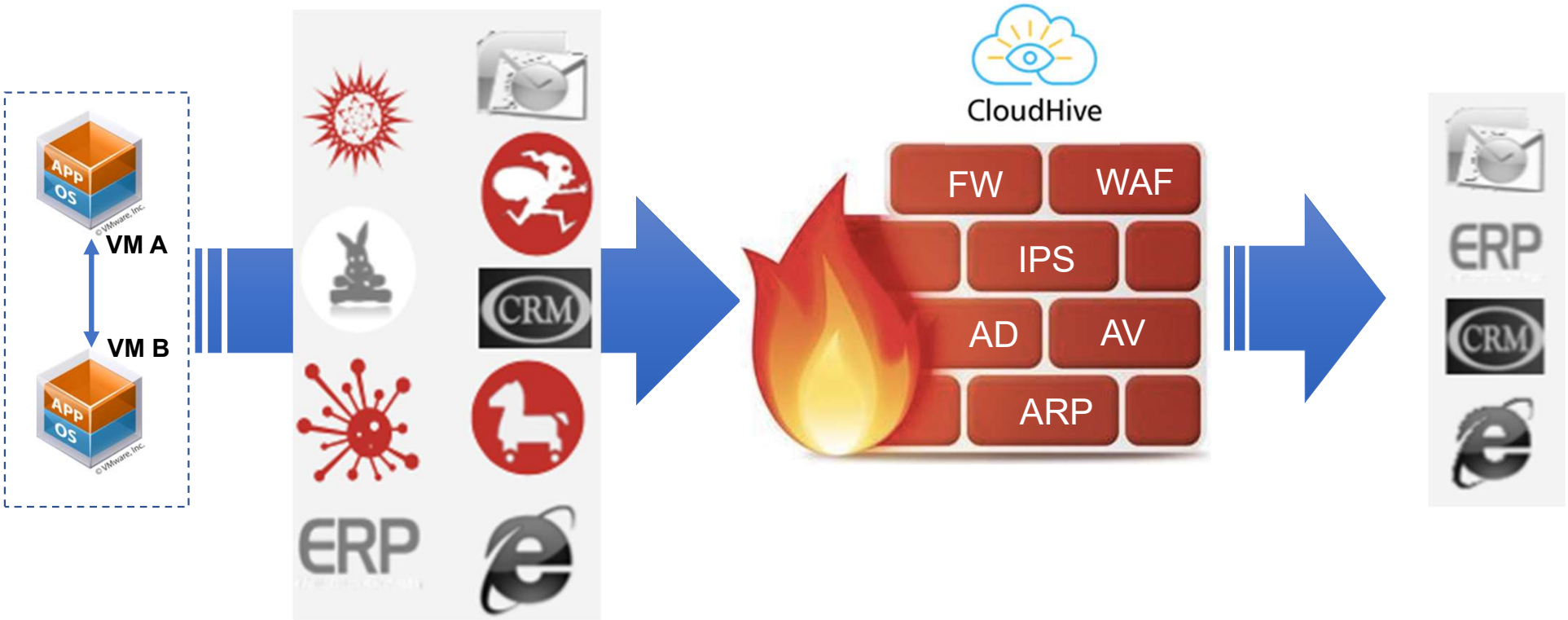
- Threat/ application/ traffic visibility Provide 2 layers of network control
- Provide L2-L7 security service for VMs



CloudHive Micro-Segmentation

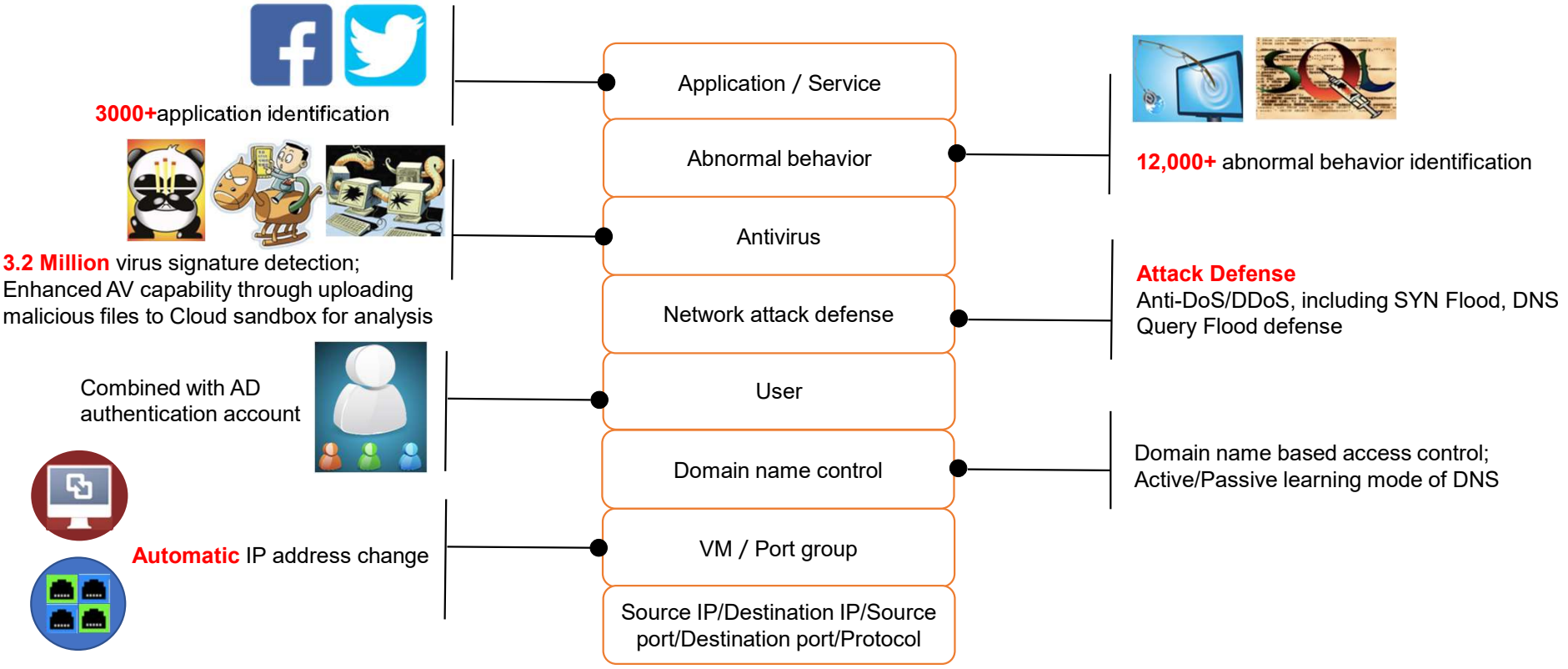


Security Protection Features



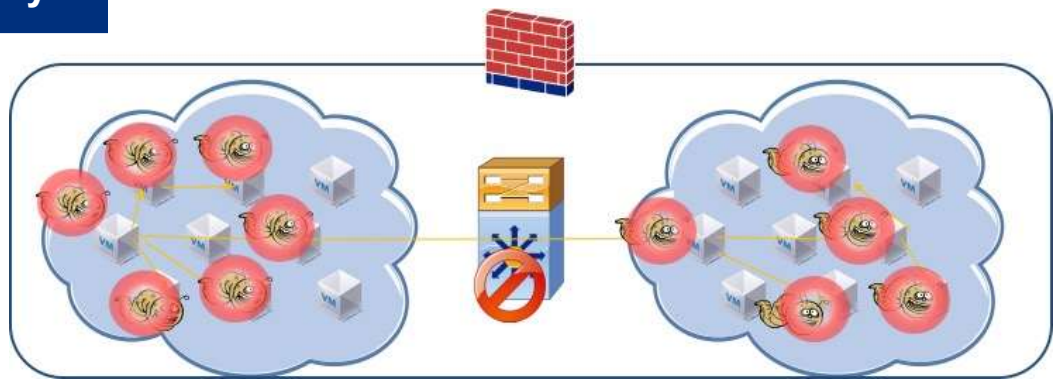
Integrated, critical security features to protect East-West traffic

Multiple Dimension Security Control



Attack Defense

Distributed Processing Guarantees High Efficiency



Risk：

- Internal sniffing after VM is compromised
- Critical asset is not protected
- Abuse of cloud computing resources

Influence：

- Provide feasible channels for authority control and data breach
- Using cloud resources, generate external attack
- Quality of cloud services are impacted

Solution

- Limit **high frequency visits** of internal virtual machines
- Mitigate depth damage caused from **proximal attack**

Highlights：

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense
- Port scan detect and defense

ARP Attack Protection - Escort the Underlying Network of the Cloud Platform

Basic Defense is Never out of Date

Risks and problems:

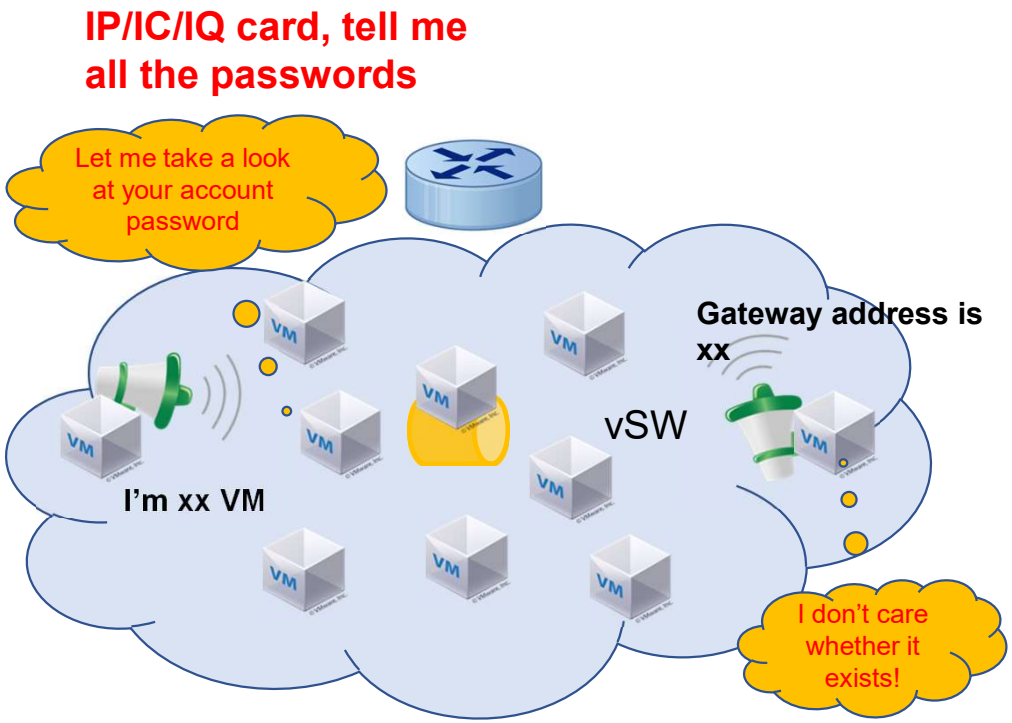
- Internal virtual machine is infected by malware
- The internal virtual machine was breached to steal or tamper with sensitive data

Impacts:

- Tamper with switch MAC table to make it unable to forward data
- Perimeter equipment can only protect itself
- Network management loss

Solutions:

- **Virtual machine as control unit**
- **Restrict** outgoing ARP information **that does not match the characteristics of the virtual machine itself**
- Improve **the basic reliability** of the cloud platform network



Firewall

Tailored Cloud Security Protection

Risk:

- Lack internal segmentation
- Single access point problem easy to spread globally
- Does not meet classified data protection policies (China)

Influence:

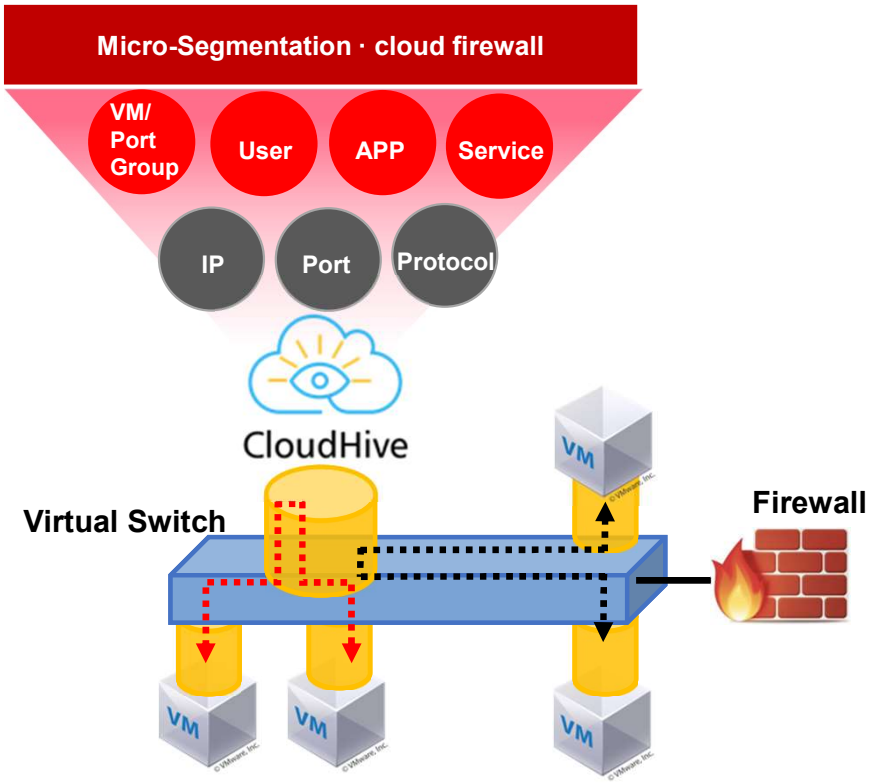
- Springboard access lead to limits in traditional security protection
- Flood attack is easy to spread internally, decreasing the quality and security of network and application

Solution:

- Low threshold - With unique drainage technology, achieve network drainage **without additional plugins**
- No network changes necessary - deployed on the **second layer**,
- Multidimensional - based on traditional protection, provide virtual machine and port group dimensions of access control for **the cloud environment**
- Versatile - suitable for **server virtualization** scenarios, also applies to **VDI desktop virtualization** scenarios

Highlights:

- Access control based on L2-L7, VM and port group, AD account, time table, domain name, geo-location and IP
- Application Layer Gateway (ALG)
- Session limit
- Various protocols support



Intrusion Prevention

Powerful and Trustworthy Abnormal Behavior Detection

Risk:

- Network layer attack：vulnerability scan, buffer overflows, and network worm
- Application layer attack/spread：Trojan, SQL injection，XSS attack，CC attack

Influence:

- Abnormal access between VM
- Indirectly influencing network quality of service

Solution:

- **Recognize, locate and visualize** VM with abnormal behavior, **reduce** possibility of compromising internal VM
- **Interception/blocking** the spread of the abnormal behavior, **mitigate** internal risk spread after the virtual machine is compromised

Highlights:

- **Distributed detection mechanism,** avoid access bottlenecks
- **12,000+** abnormal behavior signature base
- **NSS Labs** recommended
- Forensics
- Whitelist

- Detect malicious action from compromised host

- Known vulnerability attack
- Unusual protocol access
- SQL injection，XSS attack

- Network congestion caused by internal violation/exception

- Phishing
- Trojan

Anti-Virus

Necessary feature for business assurance

Risk:

- Application layer threats: Worm, Trojan, malware, etc.

Influence:

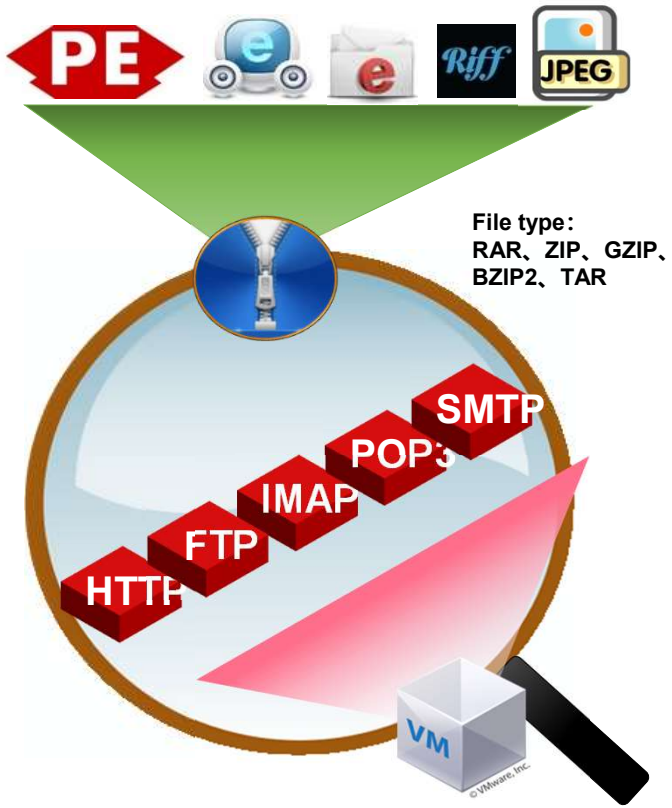
- Direct/indirect influence of network quality of service
- Compromised confidential data
- Damage to network assets

Solution:

- **Detect: Recognize, locate and visualize** threats, **reduce** possibility of compromising internal VMs
- **Control:** Intercept virus transmission in **network layer**
- **Assistant: Assist the host antivirus software solution** to prevent the spread of the virus to the network

Highlights:

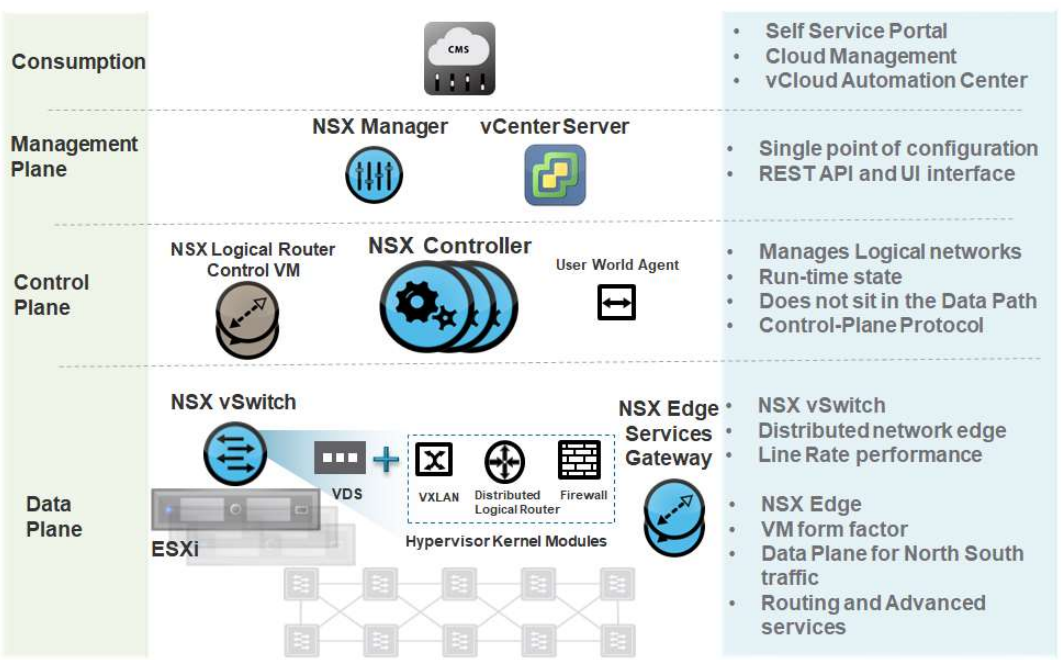
- **Distributed detection mechanism,** high performance, low latency
- Virus detection on various file transmission protocols
- Virus detection on various file types
- Support for **compressed** file virus scanning
- **3.2 million** virus signature library
- Forensics



Hillstone CloudHive Value Proposition: Joint Solution with NSX

What is NSX?

NSX is a Pure Software Defined Network Solution



NSX Partner Ecosystem

CloudHive Uses the NetX Interface to Provide NGFW

VMware Network Extensibility (NetX) for vSphere

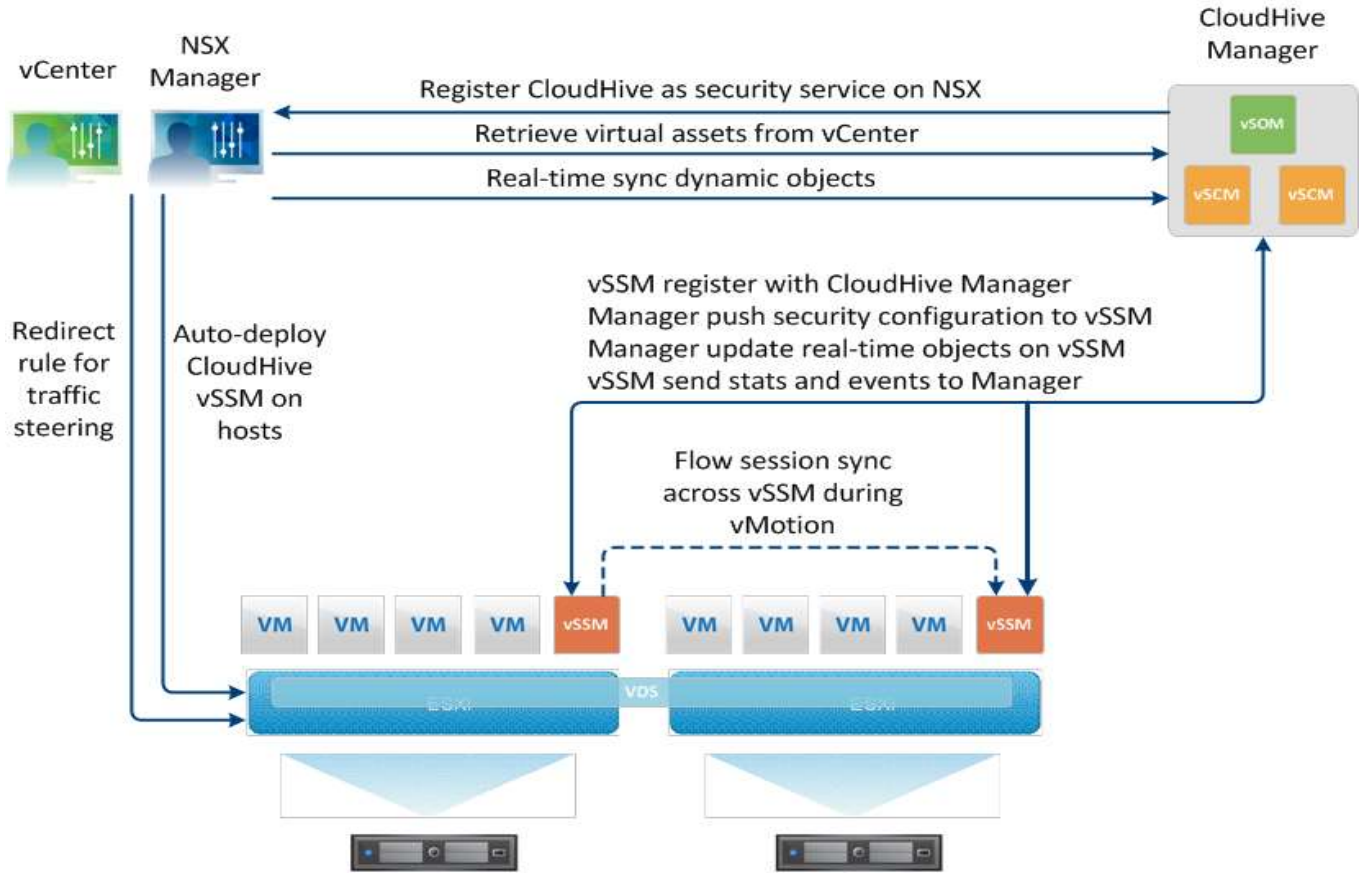
NetX APIs are used to build networking and security services over VMware infrastructure. NetX APIs allows partners to integrate their existing or new solutions inside the VMware work flow management and tap valuable information inside vSphere to provide services. Currently, solutions supported by these APIs include load-balancing (LB), WAN Optimization and intrusion detection and prevention (IDS/IPS) service integration.

vi_security_guide.pdf

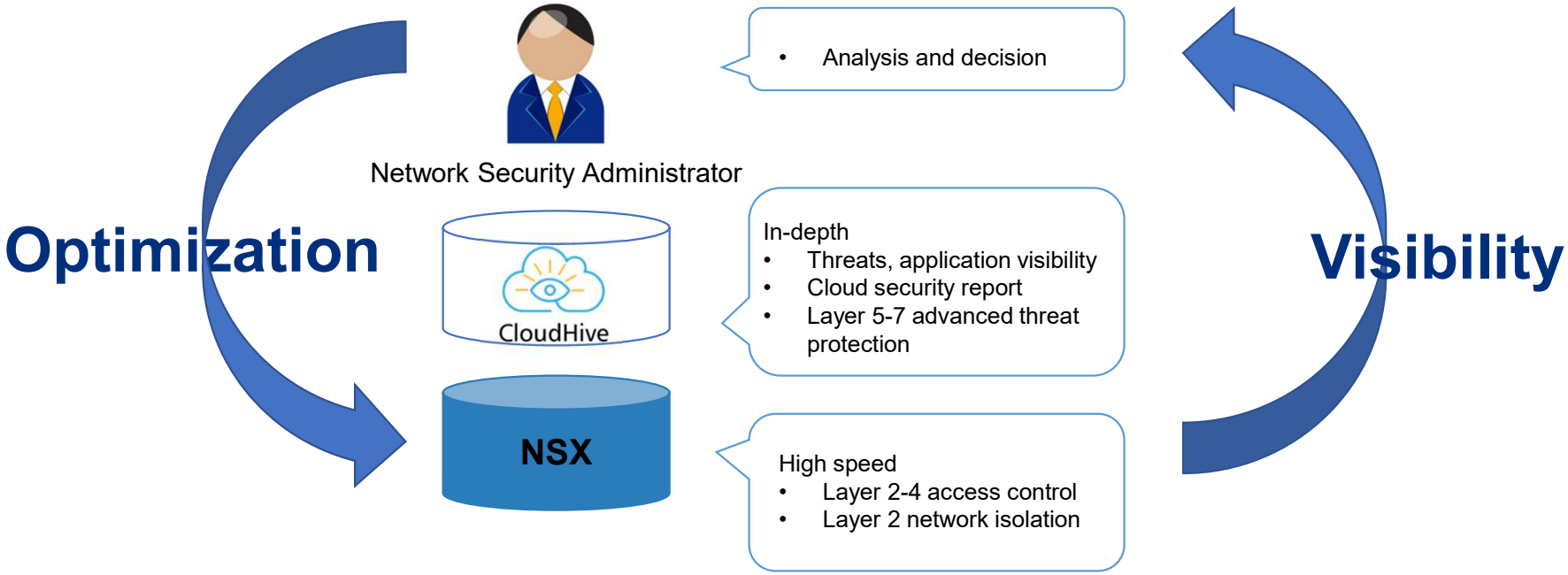
VMware Endpoint security (EPSec) for vSphere

EPSec APIs are used to deliver endpoint security solutions in a more efficient manner that does not require the management of resource-intensive agents inside the guest VM. The VMware EPSec APIs allows partners to eliminate the requirement for these agents and instead consolidate security intelligence into a single Security Virtual Appliance (SVA) per ESXi host. Currently, solutions supported by these APIs include anti-virus (AV), and file integrity monitoring (FIM).

System Architecture Process



NSX(SDN) and CloudHive Integration Solution

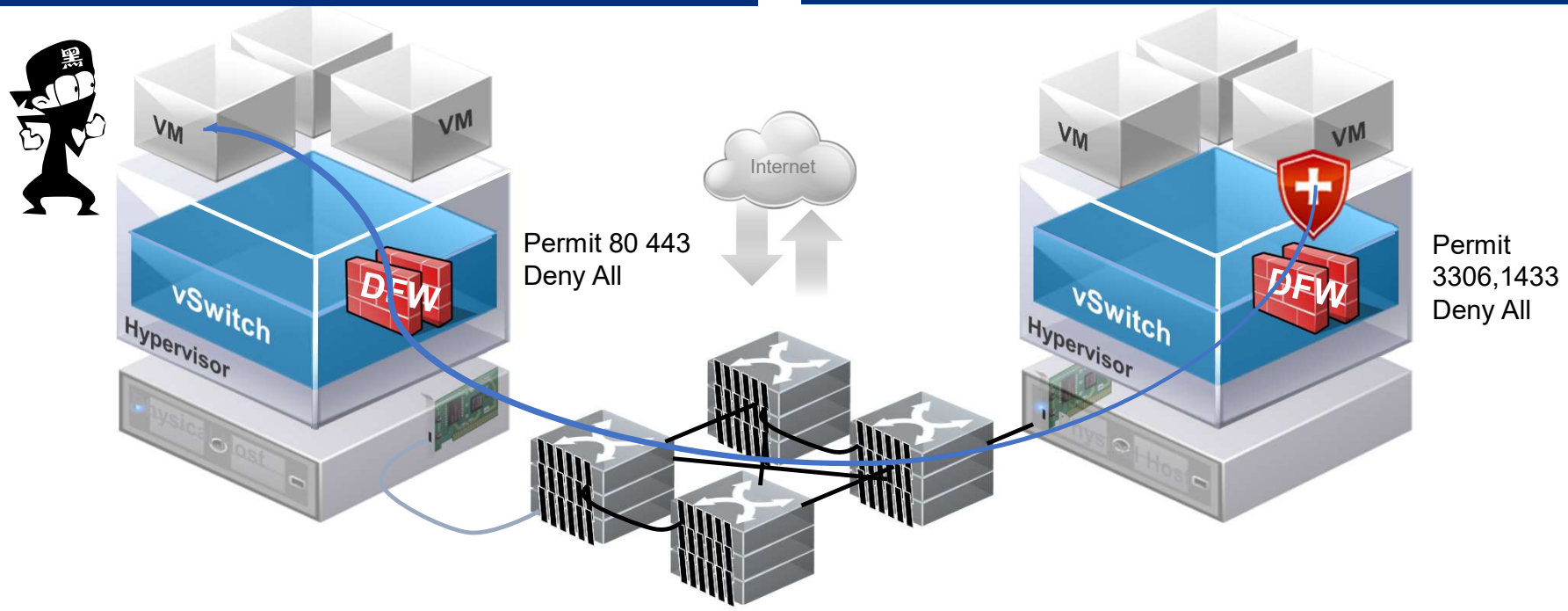


NSX DFW Protects the Internal Network Separately

Hillstone NETWORKS

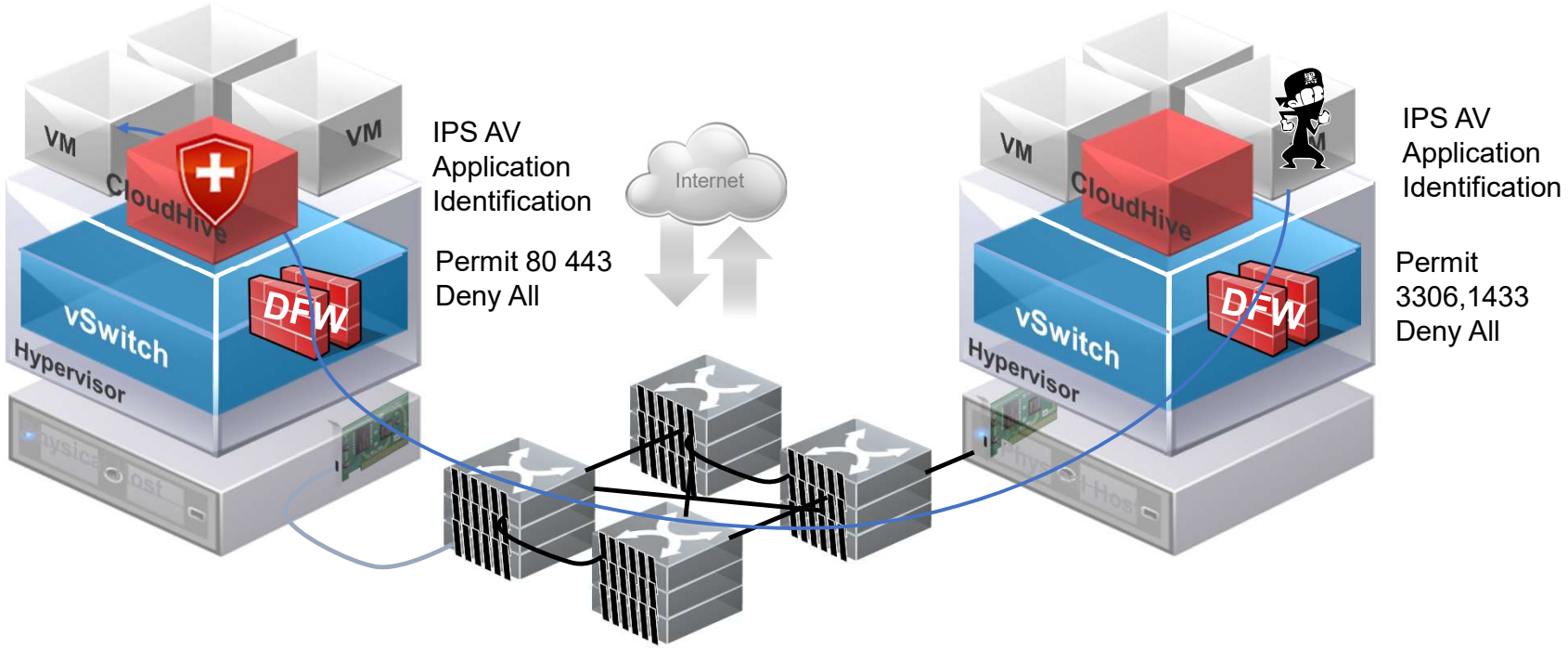
http://192.168.1.1/showdetail.asp?id=49 and 1=1

http://192.168.1.1/showdetail.asp?id=49 and 1=1

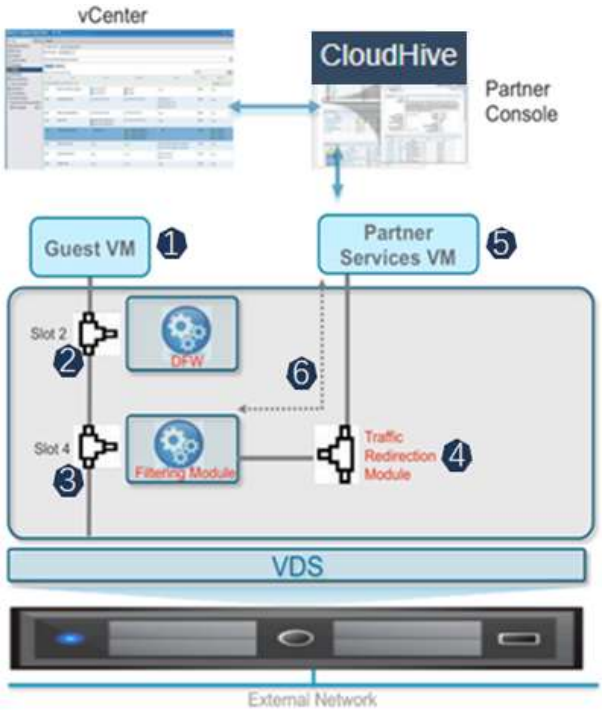


CloudHive+DFW Intranet Protection

http://192.168.1.1/showdetail.asp?id=49 and 1=1



How VMware NSX Redirects Traffic



① VM sends the packet

② Distributed FW module checks the policy; if permitted, the traffic goes to the redirect module

③ Redirection module forwards the traffic

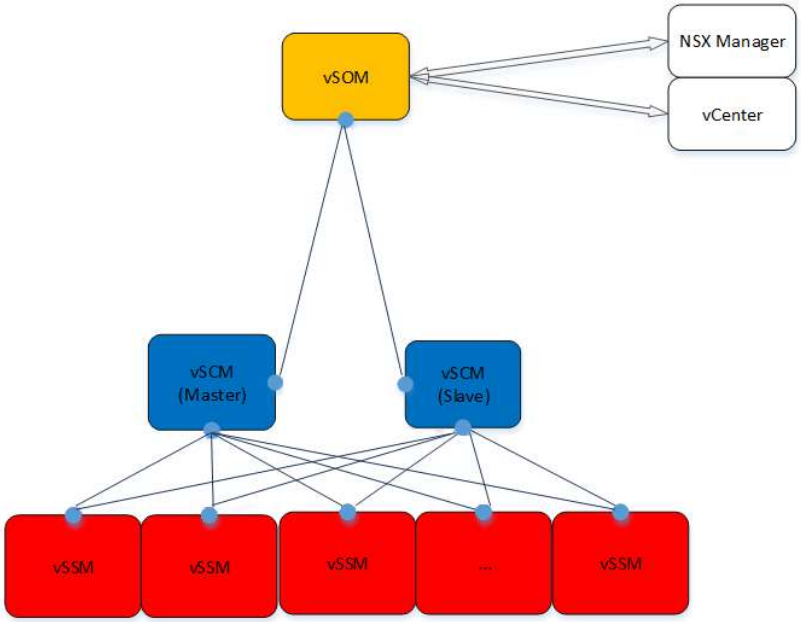
④ Redirect the traffic to thirty-party security service VM (shared memory copy）

⑤ Thirty-party security service VM checks policy permit or denies it

⑥ If permitted, the traffic will route to redirection module

NSX’s traffic redirection is not network based

CloudHive Architecture and Components



Service Manager

vSOM virtual Security Orchestration Module, as part of Service Manager. Interact with vCenter and NSX Manager

Security Service VM

vSCM virtual Service Center Module, serve as central data synchronization point for service VMs. Manage security service VMs for configuration and status monitoring

vSSM virtual Security Service Module, service VM, Provide application security services

vSCM and vSSM need to connect to the same VDS PG, or be reachable to each other via IP address, for the immediate effect of policies and logs.

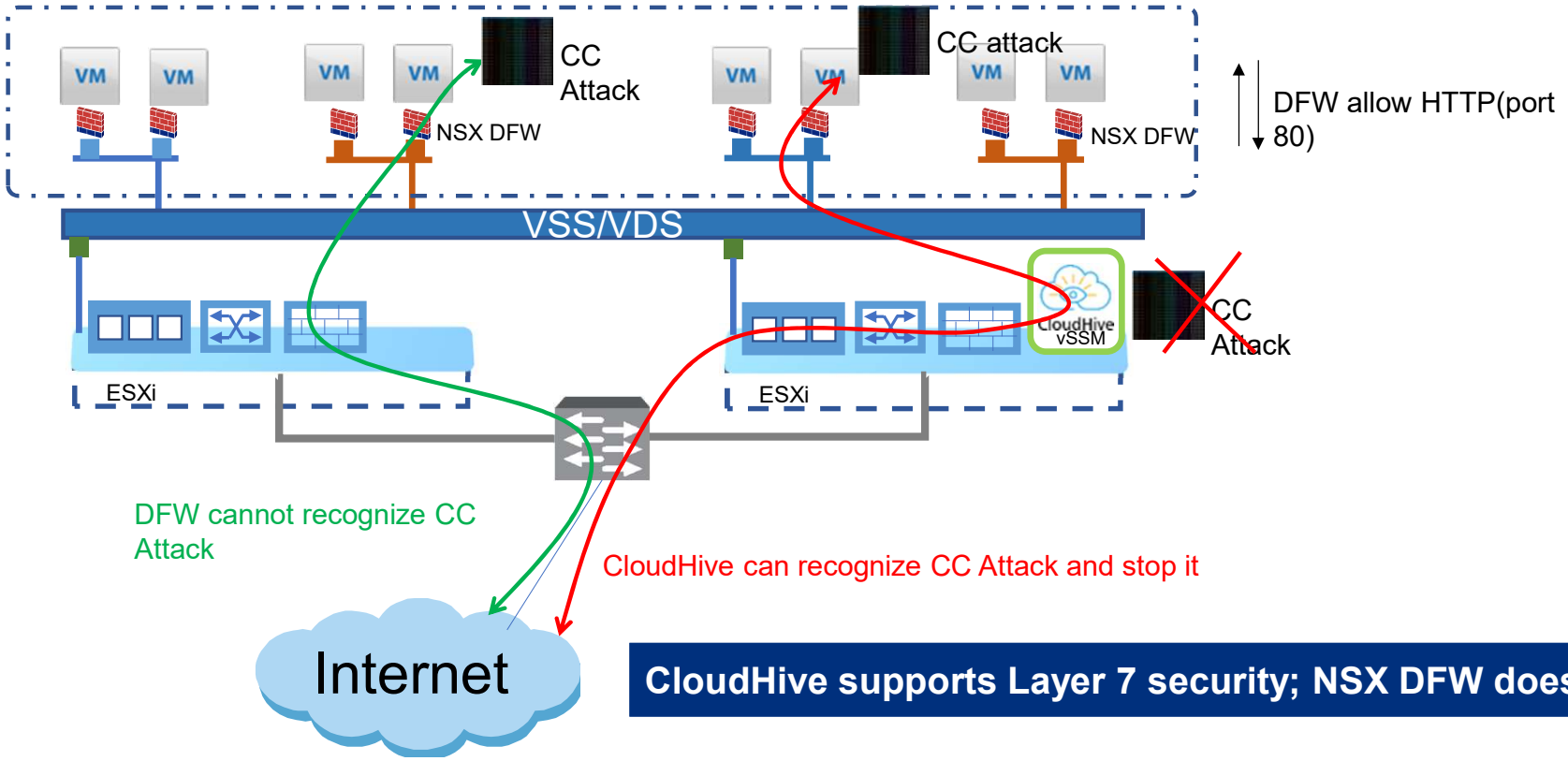
We are unique; not just vFWs + centralized MGT.

Installation and Configuration Process

1. Import SG6000-CloudHive-NSX-vSOM-2.5.1.ova image; start instance and configure management address.
2. Visit vSOM management interface via browser first, and then install according to prompts. Then, initiate CloudHive.
3. Deploy CloudHive security service for cluster through NSX Manager.
4. Visit CloudHive management interface via browser, and check the status of security service.
5. Configure security groups in the NSX Manager.
6. Configure the distributed firewall policy for security groups in the NSX Manager.
7. Configure the corresponding firewall policies for security groups in the CloudHive Web UI.
8. Configure the redirect policy for security groups in the NSX Manager.

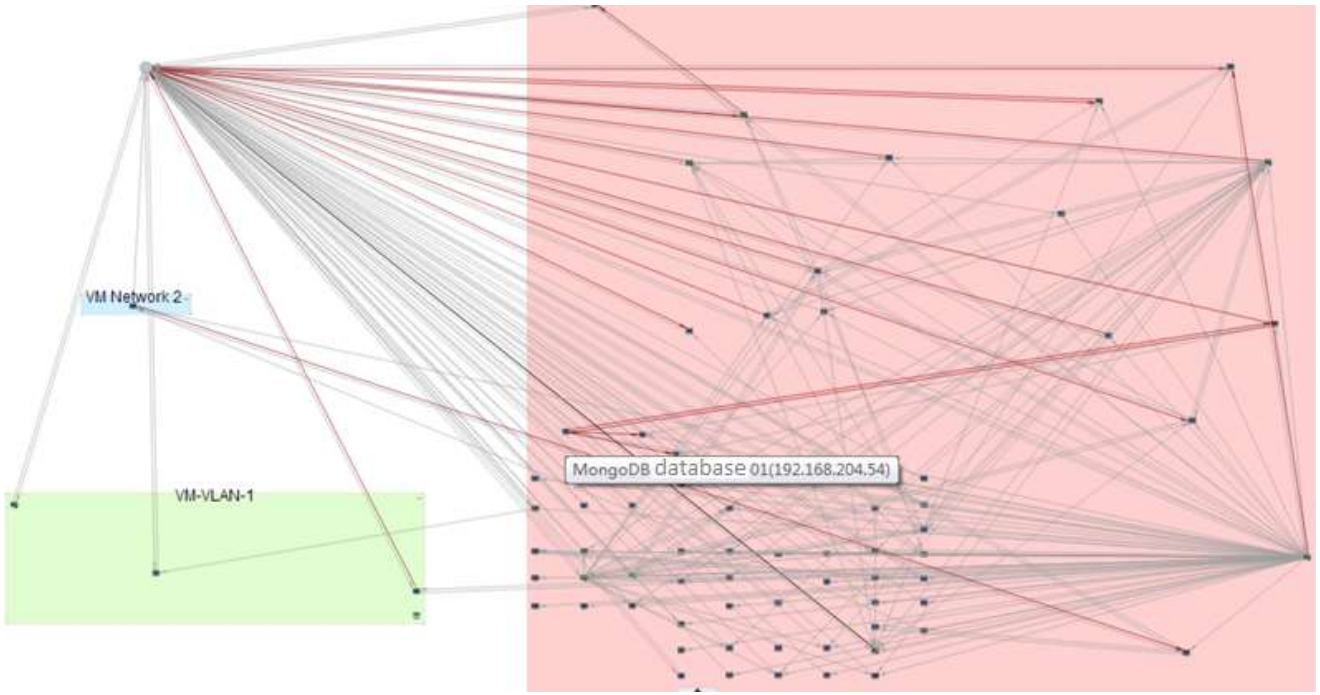
Traffic redirect policies are configured by NSX.

Relationship Between NSX DFW and CloudHive



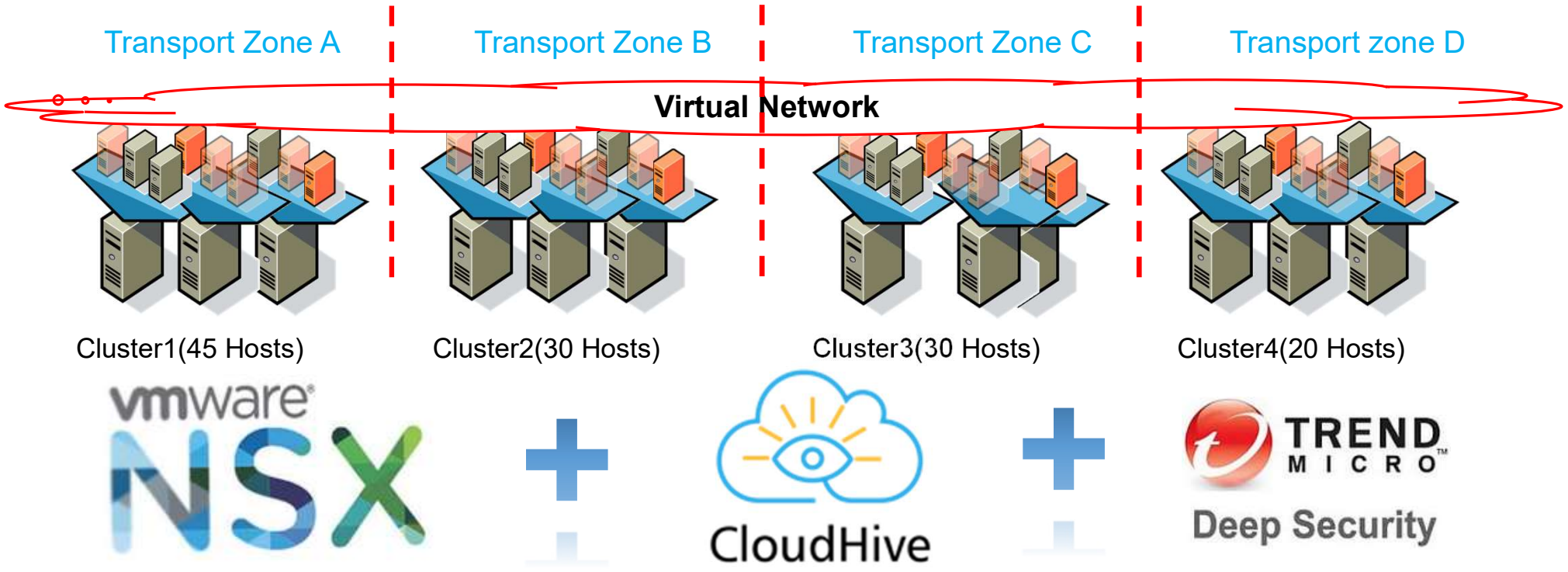
CloudHive supports Layer 7 security; NSX DFW does not.

Hillstone CloudHive DC Visibility Capability



Visibility of the traffic applications and threats between VMs and Networks.

Use Case: A Province Smart City Project



We are different, DS focuses on host-based AV, CloudHive focuses on network security.

Hillstone CloudHive Portfolio

CloudHive Components

Module	Definition	Function	Description	Deployment
vSOM	virtual Security Orchestration Module	Integrates with third-party CMP, manages service lifecycle	Management Plane: • Manages the lifecycle of the CloudHive system (System installation, stopping, deleting etc.) • CMP connects with vSOM (Web UI/CLI/ North interface)	One CloudHive system deploys a single vSOM; it supports HA, and can be installed on any physical server
vSCM	virtual Security Control Module	Centralized management and configuration for all vSSMs	Control Plane: • Security policy configuration • Manages the lifecycle of the vSSMs (Monitors starting and stopping of VMs) • Collects logs/data	One CloudHive system deploys two vSCMs in HA mode; they must be installed on two different physical servers
vSSM	virtual Security Service Module	Provides FW, IPS, AV, APPID, AD and more services	Security policy query (Slow path) • Distributed storage for session status (Session) • Packet forwarding based on session (Fast path) • Security Service (L2-L7)	Each physical server must be installed with a vSSM; supports up to 200 vSSMs
vDSM	virtual Data Service Module	High speed log forwarding	Forward log from vSSM and vSCM modules to 3rd party log servers	One CloudHive system can deploy 1 or multiple vDSM depends on log volume

CloudHive Performance

Specification	Single vSSM 02 (1 * vSSM 02)	Maximum Extension (200 * vSSM 02)	Single vSSM 04 (1 * vSSM 04)	Maximum Extension (200 * vSSM 04)
Firewall Throughput (Max)	5 Gbps	1 Tbps	5 Gbps	1 Tbps
Max Concurrent Sessions	1.7 Million	340 Million	3.4 Million	680 Million
New sessions/sec (HTTP)	30,000	6 Million	50,000	10 Million
IPS Throughput	1.5 Gbps	300 Gbps	5 Gbps	1 Tbps
AV Throughput	1.5 Gbps	300 Gbps	5 Gbps	1 Tbps

- vDSM: Max. performance is 200K PPS, 1 vDSM can support up to 7 vSSMs' log forwarding requirement.

System Resource Requirement

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 02 (Standard)	Virtual Security Service Module	2*vCPU, 6GB Memory, 5GB Hard Disk	200 Max.
vSSM 04 (Advanced)		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 Service Module	2*vCPU, 6GB Memory, 5GB Hard Disk	Optional, multiple mode supported

Virtualization Support

CMP	VMware	FusionCompute
CMP	vCenter 5.5/6.0/6.5/6.7/7.0	6.5.1 or above (only Security mode supported)
Hypervisor	ESXi	KVM
Required Components	vCenter (VSS or VDS or NSX 6.2/6.3/6.4)	VRM
Interactive Mode	vCenter Mgt API	FunsionCompute Mgt API
Restful API	Supported	Supported

CloudHive SKUs

Perpetual Mode		Subscription Mode	
CloudH-vSSM-BP-IN	CloudHive vSSM Perpetual License Essential Package (4*CPU perpetual license, vSSM by demand, 1*vSOM, 2*vSCM, without service）	CloudH-vSSM-BS-IN-12	CloudHive subscription license Essential package (4*CPU 1 year subscription license, vSSM by demand, 1*vSOM, 2*vSCM, 1-year software upgrade and maintenance service)
CloudH-vSSM-EP-IN	CloudHive vSSM Perpetual License Expansion Package (1*CPU perpetual license without service)	CloudH-vSSM-SS-IN-12	CloudHive vSSM expansion package (1*CPU subscription license, 1-year software upgrade and maintenance service)
CloudH-vSSM04-BP-IN	CloudHive vSSM Perpetual License Essential Package (vSSM04 4*CPU perpetual license, 1*vSOM, 2*vSCM, vDSM, without service）	CloudH-vSSM04-BS-IN-12	CloudHive subscription license Essential package (vSSM04 4*CPU 1 year subcription license, 1*vSOM, 2*vSCM, vDSM, 1-year software upgrade and maintenance service)
CloudH-vSSM04-EP-IN	CloudHive vSSM Perpetual License Expansion Package (vSSM04 1*CPU perpetual license without service)	CloudH-vSSM04-SS-IN-12	CloudHive vSSM expansion package (vSSM04 1*CPU subsription license, 1-year software upgrade and maintenace service)
SPM-SP-IN	CloudHive service performance monitor license (1*CPU perpetual license)	SPM-SS-IN-12	CloudHive 1-year service performance monitor license (1*CPU subscription license, 1-year software upgrade and maintenace service)
CloudH-vSSM-SP-IN-12	1*CPU 1-year software upgrade and maintenance service	N/A	
CloudH-vSSM-SP-IN-24	1*CPU 2-year software upgrade and maintenance service		
CloudH-vSSM-SP-IN-36	1*CPU 3-year software upgrade and maintenance service		
IPS-SP-IN-12	CloudHive vSSM 1-year IPS license with signature upgrade service	IPS-SS-IN-12	CloudHive vSSM 1-year IPS license with signature upgrade service
IPS-SP-IN-24	CloudHive vSSM 2-year IPS license with signature upgrade service		
IPS-SP-IN-36	CloudHive vSSM 3-year IPS license with signature upgrade service		
AV-SP-IN-12	CloudHive vSSM 1-year AV license with signature upgrade service	AV-SS-IN-12	CloudHive vSSM 1-year AV license with signature upgrade service
AV-SP-IN-24	CloudHive vSSM 2-year AV license with signature upgrade service		
AV-SP-IN-36	CloudHive vSSM 3-year AV license with signature upgrade service		
URL-SP-IN-12	CloudHive vSSM 1-year URL license with signature upgrade service	URL-SS-IN-12	CloudHive vSSM 1-year URL license with signature upgrade service
URL-SP-IN-24	CloudHive vSSM 2-year URL license with signature upgrade service		
URL-SP-IN-36	CloudHive vSSM 3-year URL license with signature upgrade service		

How to Buy CloudHive

Example A: 2*2-CPU Servers requiring vSSM02, 1 year CloudHive Service only

	Basic Package	Service
Perpetual Mode	1*CloudH-vSSM-BP-IN	4*CloudH-vSSM-SP-IN-12
Subscription Mode	1*CloudH-vSSM-BS-IN-12	/

Example B: 5*2-CPU Servers requiring vSSM02, 1 year CloudHive Service with IPS and AV Subscription

	Basic Package	Extension Package	Service	IPS	AV
Perpetual Mode	1*CloudH-vSSM-BP-IN	6*CloudH-vSSM-EP-IN	10*CloudH-vSSM-SP-IN-12	10*IPS-SP-IN-12	10*AV-SP-IN-12
Subscription Mode	1*CloudH-vSSM-BS-IN-12	6*CloudH-vSSM-SS-IN-12	/	10*IPS-SS-IN-12	10*AV-SS-IN-12

Note: CloudHive basic Package SKU support 4 CPU by default

How to Buy CloudHive

Example A: 2*2-CPU Servers requiring vSSM04, 1 year CloudHive Service only

	Basic Package	Service
Perpetual Mode	1*CloudH-vSSM04-BP-IN	4*CloudH-vSSM-SP-IN-12
Subscription Mode	1*CloudH-vSSM04-BS-IN-12	/

Example B: 5*2-CPU Servers requiring vSSM04, 1 year CloudHive Service with IPS and URL Subscription

	Basic Package	Extension Package	Service	IPS	URL
Perpetual Mode	1*CloudH-vSSM04-BP-IN	6*CloudH-vSSM04-EP-IN	10*CloudH-vSSM-SP-IN-12	10*IPS-SP-IN-12	10*URL-SP-IN-12
Subscription Mode	1*CloudH-vSSM04-BS-IN-12	6*CloudH-vSSM04-SS-IN-12	/	10*IPS-SS-IN-12	10*URL-SS-IN-12

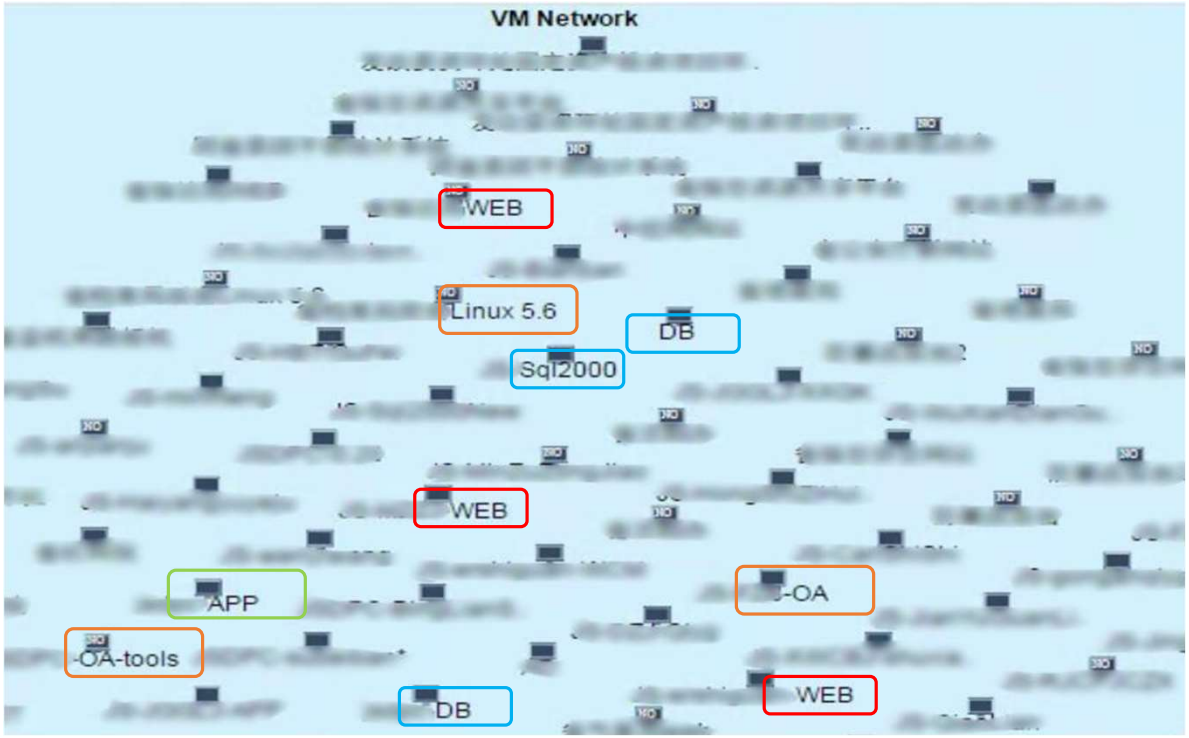
Note: CloudHive basic Package SKU support 4 CPU by default

Deployment Scenarios & Winning Cases

Customer References

20,000+ CPUs Serve Customers

Use Case: Secure the Cloud for a Local Government



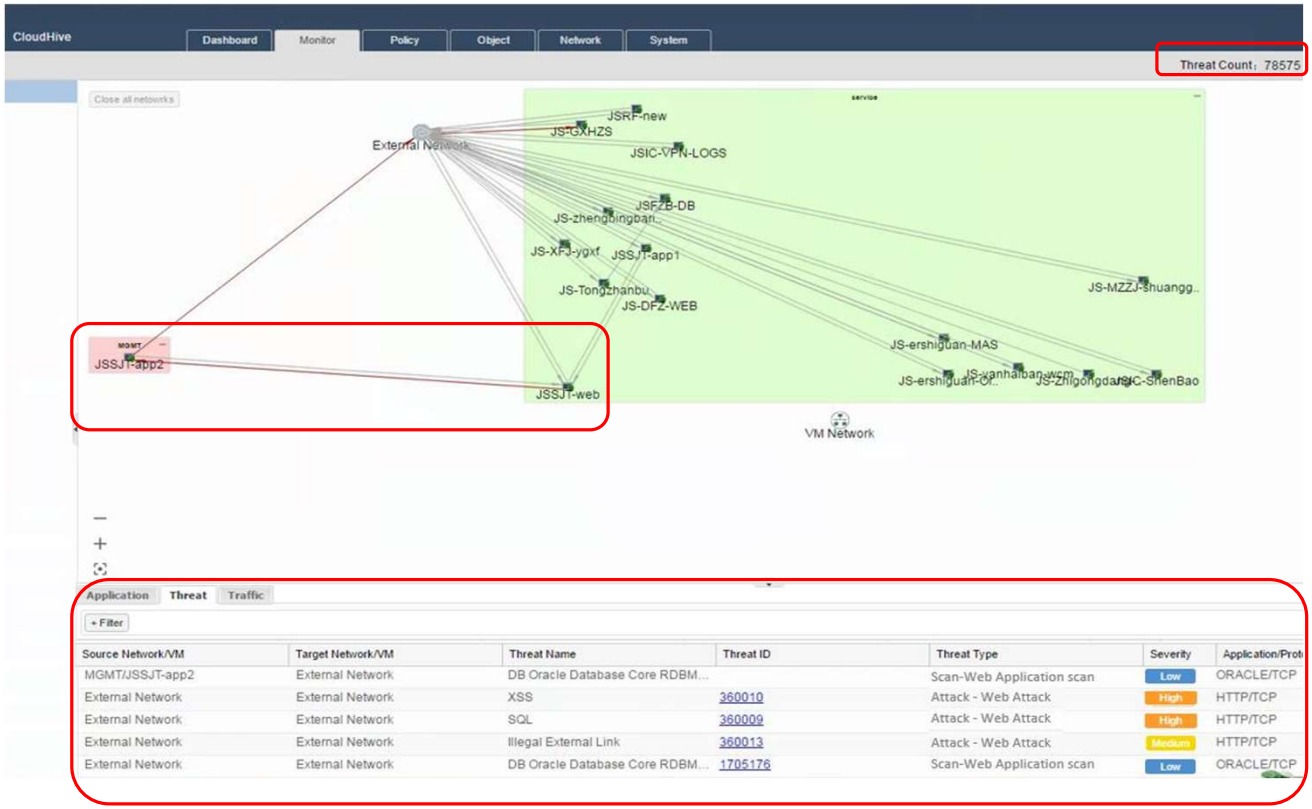
Reality: All the VMs are in the same L2 network without any segmentation

- Different tenants: Investment, weather bureau; law enforcement etc.
- Different functions: Web,. App, DB, Admin etc.
- Different business priority and security classification.

Challenges: One point breach can compromise the entire virtual network

- Create VLAN for different users/apps through vCenter need configuration on firewall, switch and router: **Time consuming with limited security effect.**
- Admin can only scale business within the same L2 network: **Zero trust inside the cloud**

Use Case: Secure the Cloud for a Local Government



CloudHive Solution Benefits:

No interruption with Easy scalability

- No network configuration
- No VM configuration
- Business continuity

VM level Segmentation with deep visibility

- Segmentation between each VM
- L2-L7 security service
- VM level threat, application, traffic visualization.

Ease of management

- Flexible policy configuration based on business requirement and security features.

Use Cases

- **Use Case 1: Cloud Security**
- Use Case 2: Cloud Compliance Audit
- Use Case 3: Value-added Safety with SDN
- Use Case 4: Cloud Value-added Service

Large Power Company

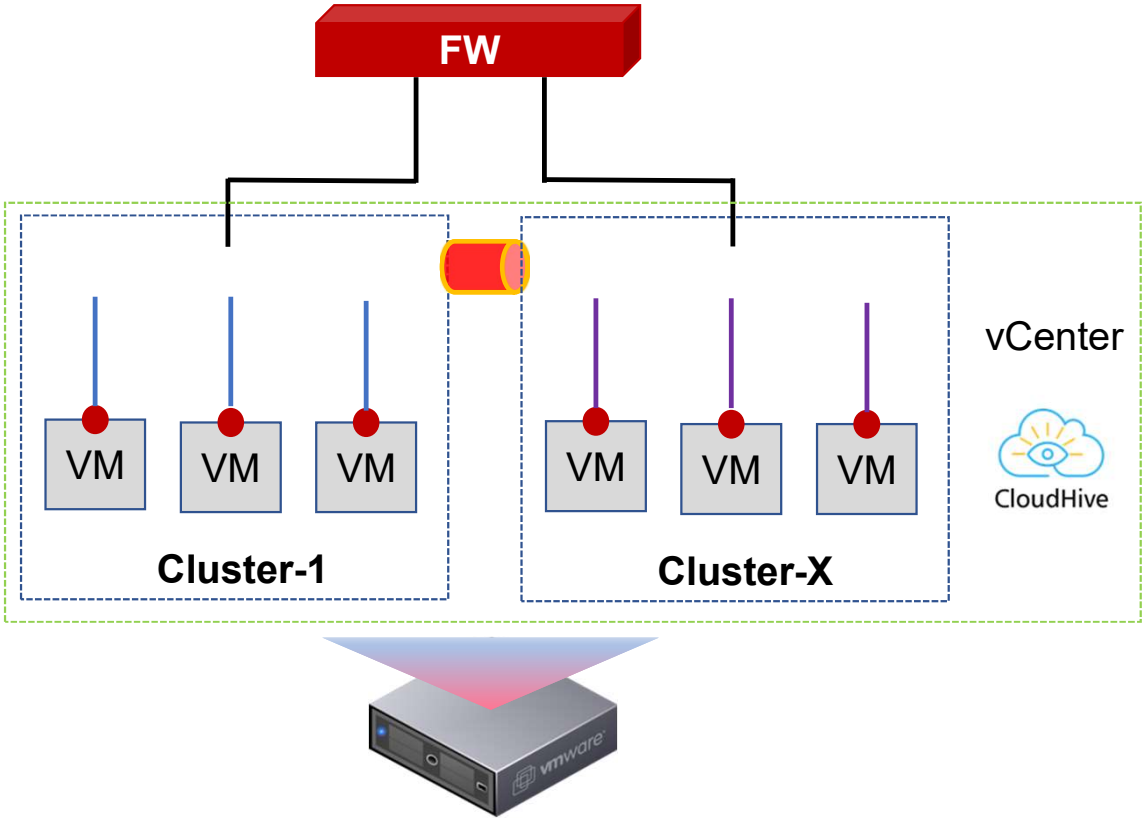
Customer: Network Security Department

System and Solution :

- VMware based virtualization environment
- 1*vCenter, 1&DC, 18 &Cluster
- 1*VDS, communication between different port groups need go through L3 router
- vNetwork Card for each VM, management and business share the same network
- Deployed 1*CloudHive to protect the online electricity payment system

Customer Value :

- Protect critical business applications running in the Cloud



National Commercial Bank

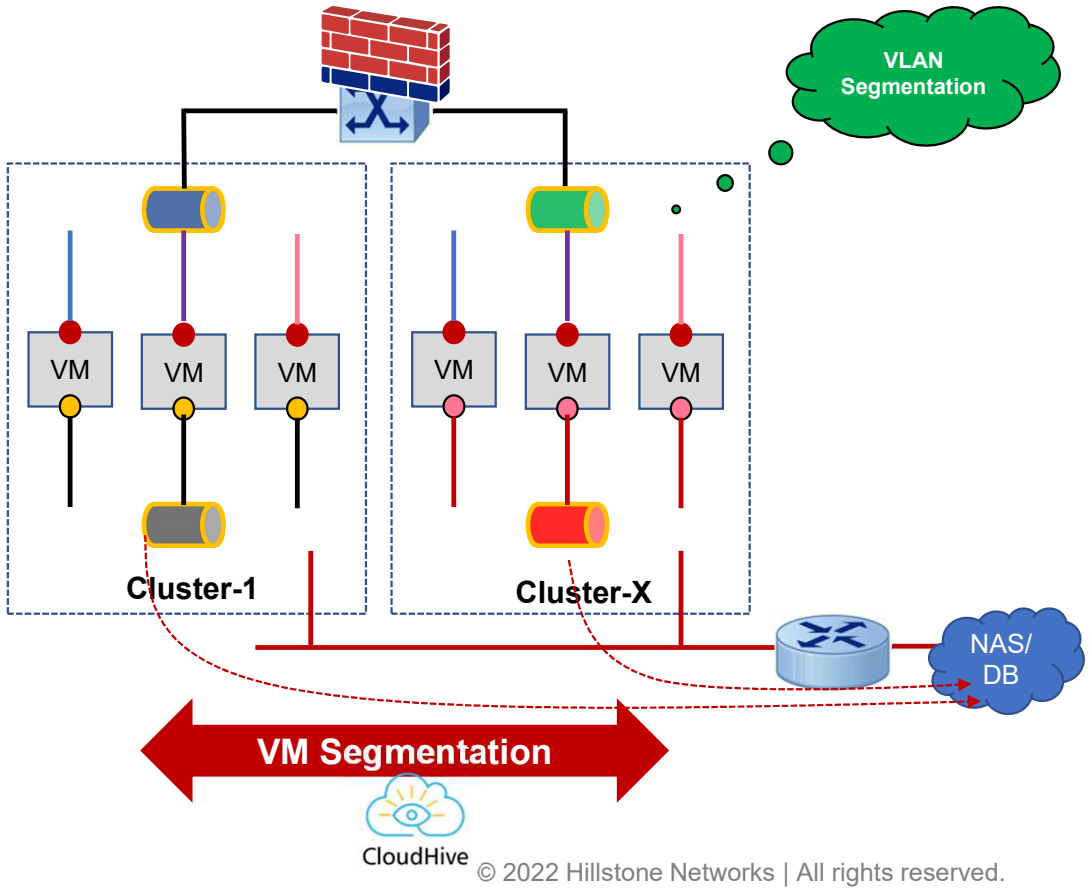
Customer: IT System Department

System & Solution:

- VMware based virtualization environment
- 1*vCenter, 1*DC, multiple Cluster
- Dedicated VDS for each Cluster, communication needed between Clusters
- Virtual network card for each VM
- Separation of External business network and storage network
- External business network is protected by VLAN+Firewall
- Storage network is protected by Hillstone CloudHive

Customer Value :

- Protect storage network as needed.
- Segmented VMs can communicate via the storage network



Fortune 500 Telco

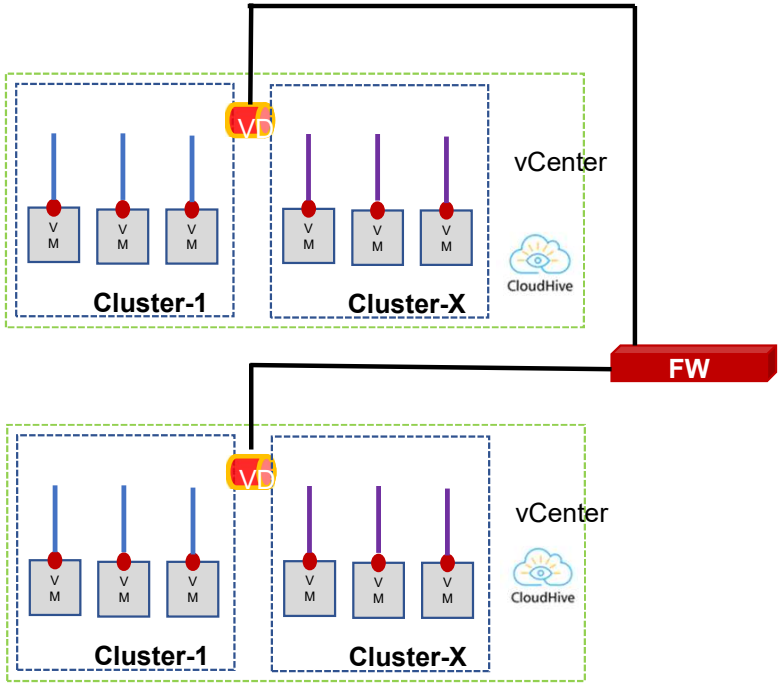
Customer: Network Operation Center

System & Solution:

- VMware based virtualization environment
- Run several Telco business applications
- Deployed Hillstone NGFW in perimeter for N-S protection
- Deployed 2*CloudHive under 2*vCenter in Phase I to secure E-W traffic, monitor and protect key application system

Customer value:

- Visibility of East-West traffic and threat inside the cloud
- Segment and protect key business applications to ensure business continuity
- Incident forensics and audit



Use Cases

- Use Case 1: Cloud Security
- **Use Case 2: Cloud Compliance Audit**
- Use Case 3: Value-added Safety with SDN
- Use Case 4: Cloud Value-added Service

Cloud Compliance Audit for a Government Agency

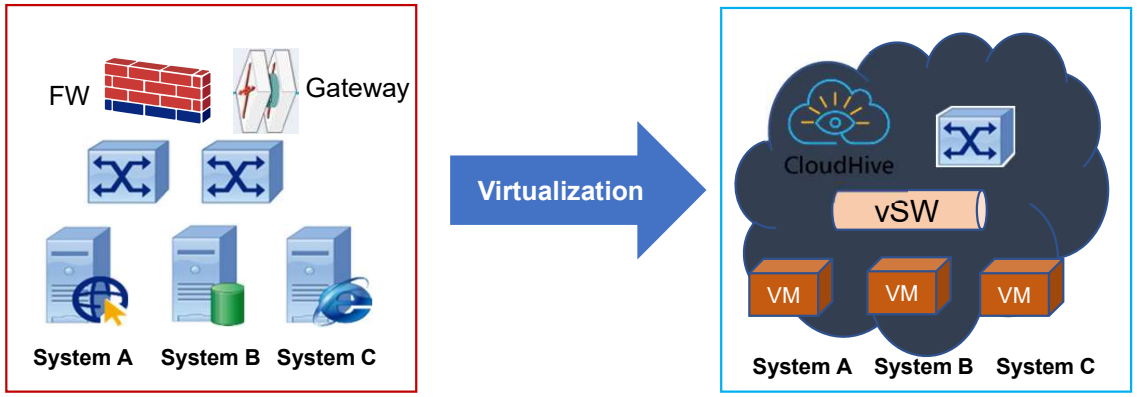
Physical Security

- Server
- Switch
- Gateway/Firewall

Bureau of Statistics

CloudHive

- VM level visibility
- VM level security
- Log and audit



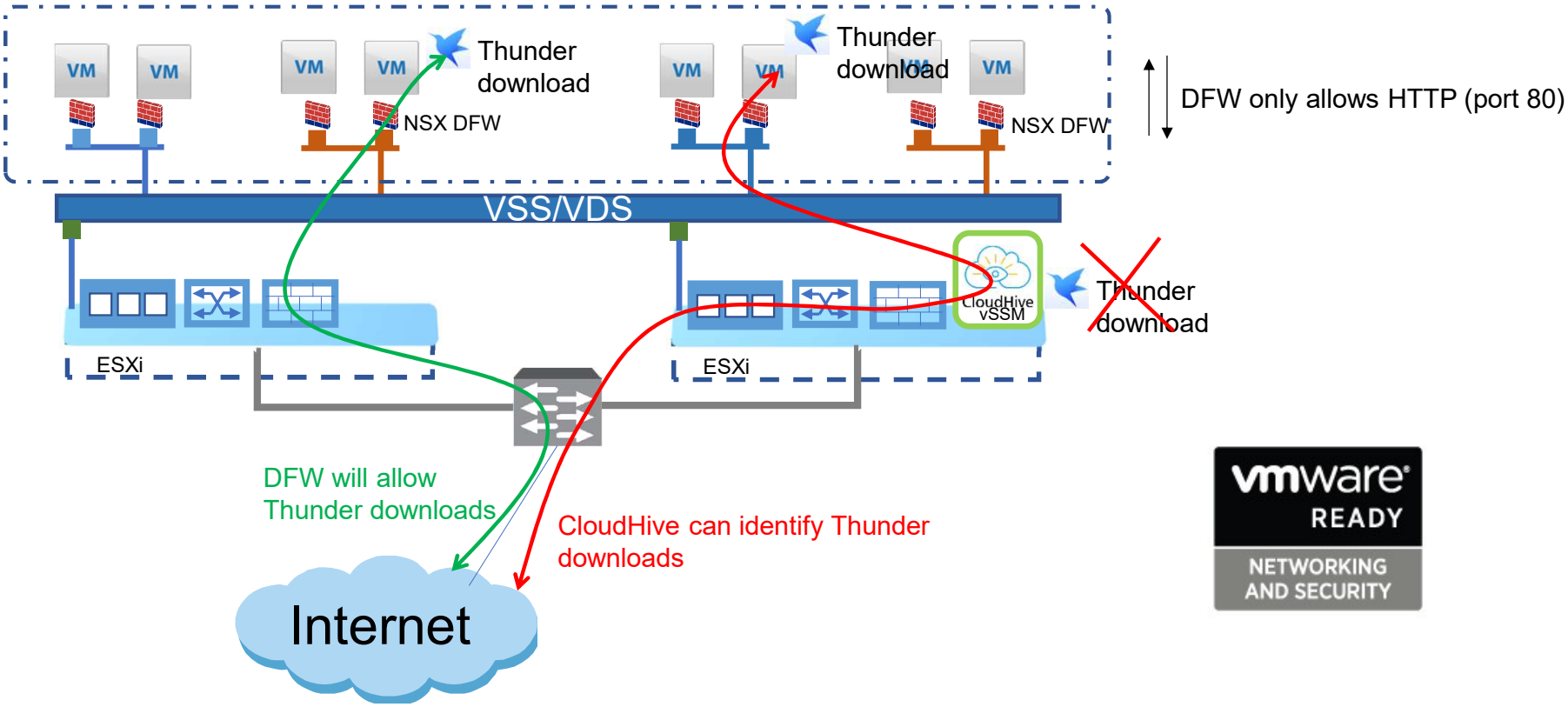
Value Proposition:

Meet compliance and audit requirements, accelerate the process of moving customers' applications to the Cloud

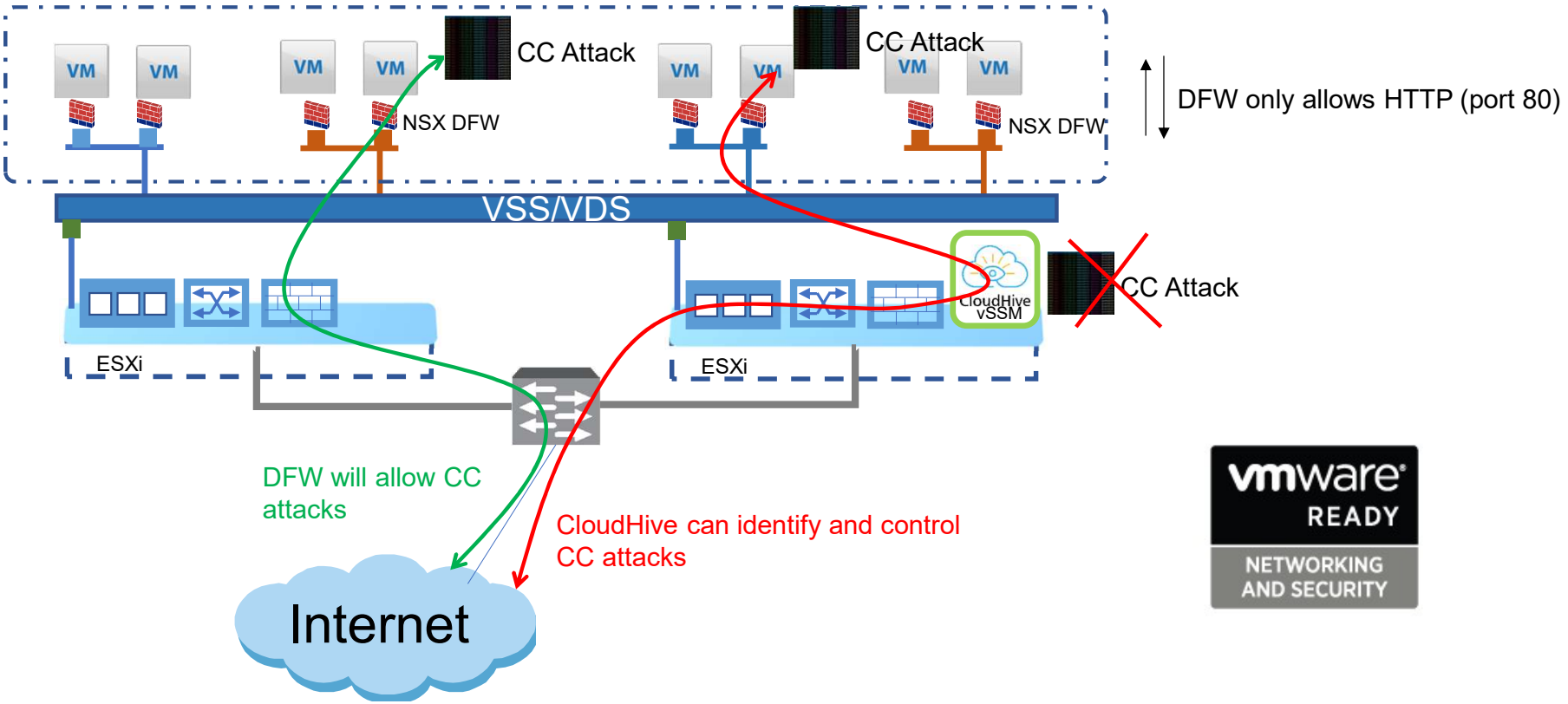
Use Cases

- Use Case 1: Cloud Security
- Use Case 2: Cloud Compliance Audit
- **Use Case 3: Value-added Safety with SDN**
- Use Case 4: Cloud Value-added Service

University – Non-Compliance Application Identification Control with NSX DFW



IDC - CC Attack Recognition Control with NSX DFW



Use Cases

- Use Case 1: Cloud Security
- Use Case 2: Cloud Compliance Audit
- Use Case 3: Value-added Safety with SDN
- **Use Case 4: Cloud Value-added Service**

Value-Added Service for Cloud Service Providers

Local Government E-Government Cloud

- VMware Based Virtualized Cloud, running environment service and system
- 1*vCenter，2*DC，1*Cluster for each DC
- Integration with CloudHive
- Operated and Management by Inspur

Regional Cloud Computing Center

- VMware Based Virtualized Cloud, running public information service system
- 1*vCenter，1*DC，3*Cluster
- Integrated with CloudHive
- Operated by a CSP

Value Proposition

The integration with CloudHive provides the customer a comprehensive virtualization solution with security services, and enhanced competitive advantage for the CSPs

Security that Works!

+1 408 508 6750
inquiry@hillstonenet.com
5201 Great America Pkwy, #420
Santa Clara, CA 95054
www.hillstonenet.com

Hillstone NETWORKS