

Hillstone iSource Product Introduction



Integrative Cyber
Security

Agenda

Business Problem

Introduction of Hillstone iSource

Product Models & Ordering Info

Deployment Scenarios & Use Cases

Case Studies

Business Problem

New IT Trends Brings New Challenges



Digital Transformation

- Exponential Increase of Traffic
- New business apps/upgrades
- Access from anywhere



Cloud Adoption

- Private/Hybrid deployment
- SaaS apps
- Serverless computing
- Containers



Extended Endpoints

- IoT devices
- Mobile devices
- Connected vehicles

Increased traffic, new services and new devices will introduce new security threats and vulnerabilities

Key Problems In Security Operation

- Tons of Logs

- Security Information Silos

- Separated investigations

- False positives

- Long lead time of investigation

- Imperceptible threats

- Overloaded Alerts

- Slow incident responses

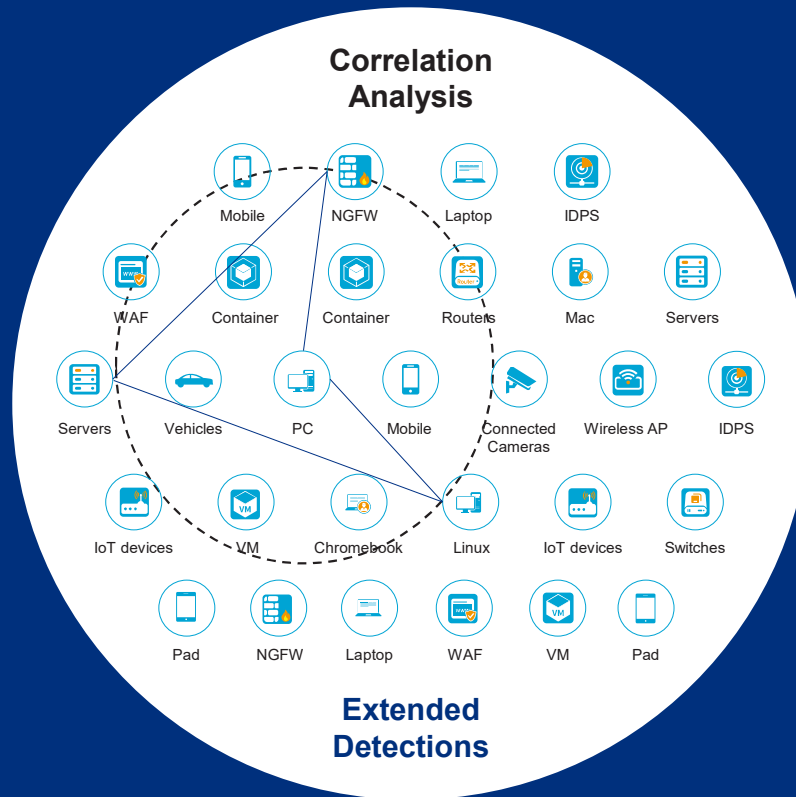
What Do Customers Need?

Comprehensive Data Collection

- Syslog
- Telemetry
- Metadata
- Threat Intelligence
- Vulnerability reports
- ...

Full visibility

- Endpoints/Servers
- Network/Cloud
- Apps/Services
- Evidence
- ...



Threat Hunting and Analysis

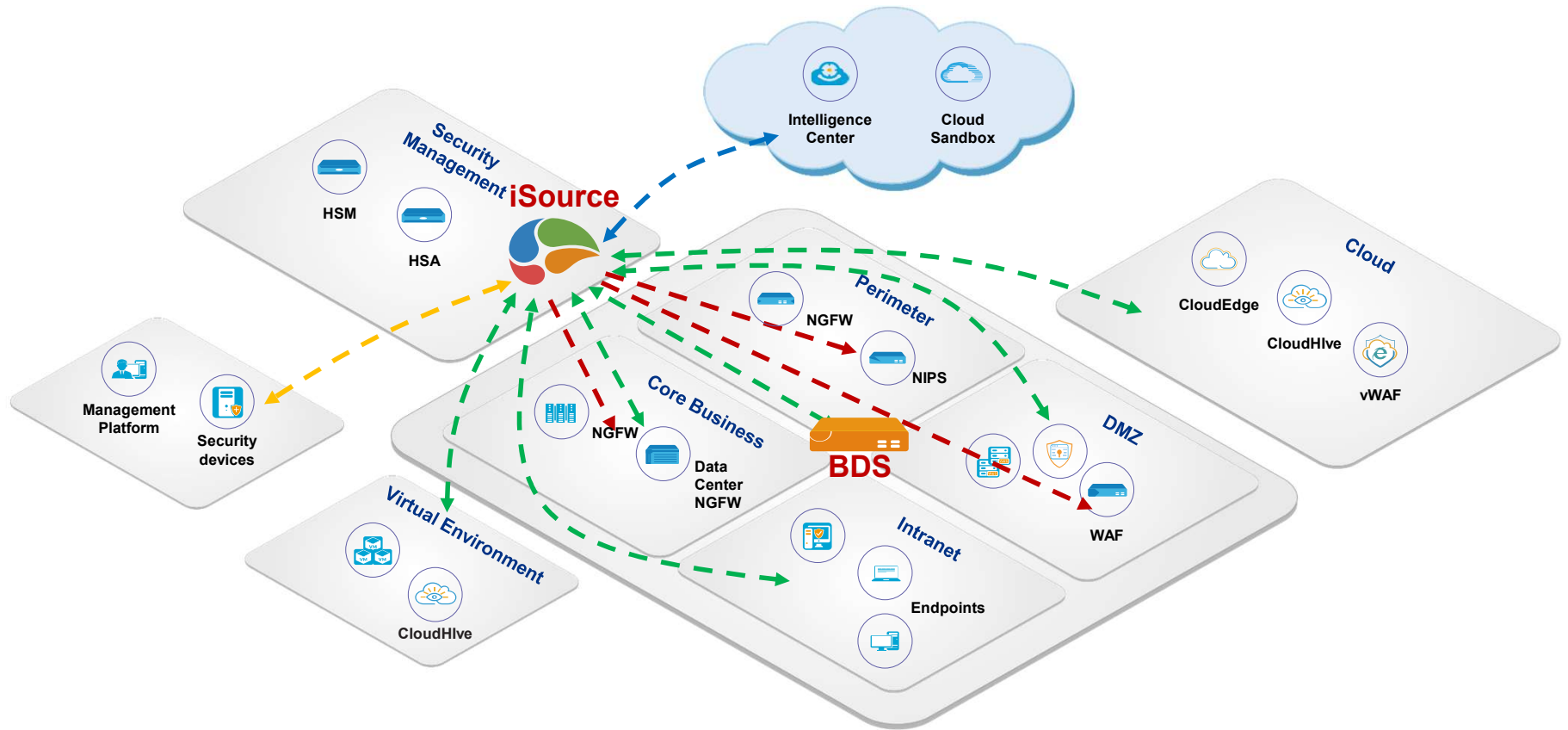
- Threat detection
- Behavior analysis
- Correlation analysis
- Root cause and attack source analysis
- ...

Automated Response

- Auto log aggregation
- Playbook driven response
- Auto response enforcement
- Efficient case management
- ...

Introduction of Hillstone iSource

Hillstone XDR Solution Overview



←-----→ Intelligence Sharing

-----> Logs/Metadata

-----> Responses

iSource Feature Highlights



01 Complete Data Collection & Full Visibility

- Granular data collection
- Full screen dashboard with rich security information

02 Asset Discovery and Management

- Auto discovery of assets
- Asset-based threat management

03 AI powered Threat Detection & Analysis

- Abnormal behavior analysis
- Correlation analysis
- Advanced threat detection
- Threat intelligence interaction

04 Investigation

- Threat analysis via SPL language based log search
- Threat insight: displays interconnectivity between assets to pinpoint the source of attack
- Threat hunting

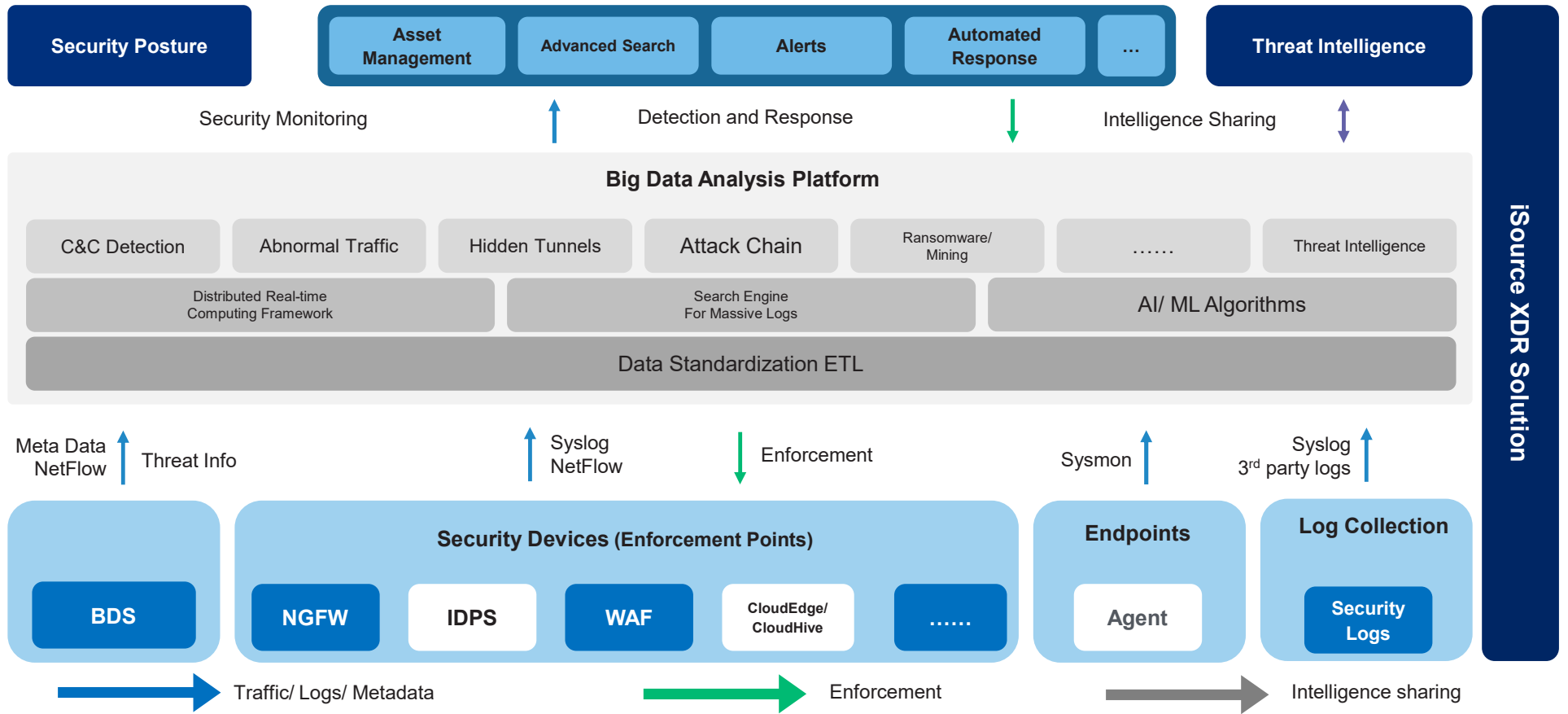
05 Automated Orchestration and Response

- Playbook driven orchestration
- Auto responses over enforcement points(integrated security devices)

06 Open Platform with High scalability

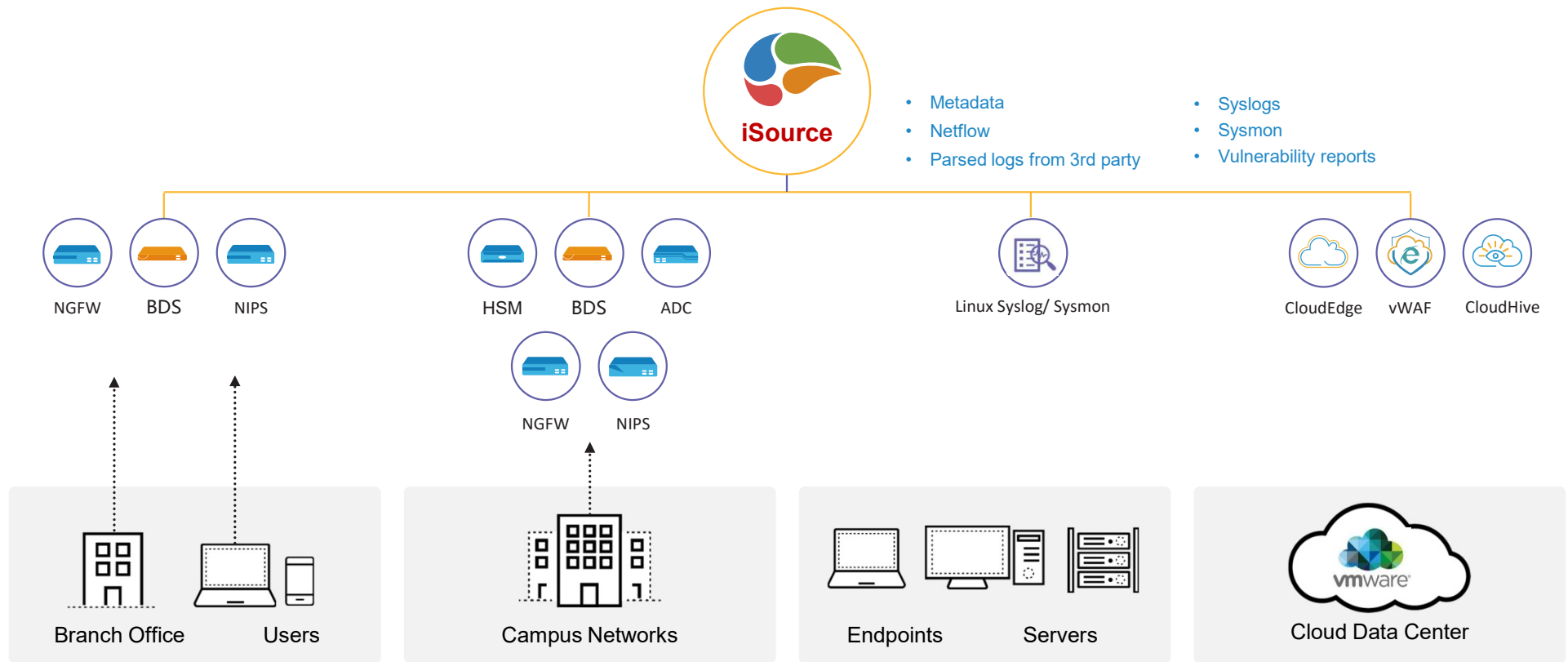
- Support 3rd party logs
- Support 3rd part security device integration
- Suupport clustering for scalability

iSource: XDR Solution Architecture



iSource XDR Solution

Complete Data Collection Across The Environment



Full-screen Monitoring Dashboards



Security Overview Dashboard

- Multiple Full-screen Dashboards
- Rich Data
- Custom Dashboard Title
- Auto Rotation

Full-screen Monitoring Dashboards

External Attacks Monitoring

External Attack Situation Monitor

Custom 2021/10/09 17:29:40 Saturday

Attack Event Severity Distribution



TOP5 Attacker IPs

1	1.1.1.61 Australia	615,842Times
2	10.182.191.124 Unknown Location	20,386Times
3	10.182.139.97 Unknown Location	16,989Times
4	10.182.138.221 Unknown Location	16,976Times
5	10.88.25.200 Unknown Location	15,009Times

TOP5 Attacker Locations

1	Australia	615,842Times
2	China	40Times



Killchain Stage Distribution



Attack Event Trendline



TOP5 Attacks Suffered

	Asset	Area
1	空去过	616,192Times
2	10.88.7.10	199,163Times
3	10.181.70.120	15,014Times
4	10.160.31.231	10,754Times
5	10.192.5.17	976Times

Full-screen Monitoring Dashboards

Server Monitoring

Server Situation Monitor

Custom 2021/10/12 16:14:28 Tuesday

Total Servers
151

Risky Servers
14

Important Servers
121

Important Risky Servers
6

Server Security Status Distribution

14 Risky Servers

Critical	29%	4
High	64%	9
Medium	7%	1
Low	0%	0



Risk Status

Critical

- Threat Events: 196,453
- Vulnerabilities: 469
- Asset Value: Considerable

TOP5 Threat Events

Name	Severity	Events	Unresolved Events
DNS Domain is Generated by DGA	High	130,046	130,046
DNS Protocol Abuse	Low	16,141	16,140
Suspicious DNS Tunnel Data Transfer	High	15,896	12,759
TTL in DNS Message is 0	Low	8,716	8,716
The host has accessed Trojan Malicious Dom...	High	4,428	4,428

Server Threat Event

Total Threat Events: 926,168

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Blue)

Server Vulnerability

Total Vulnerabilities: 735

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Blue)

Full-screen Monitoring Dashboards

Endpoints Monitoring

Terminal Situation Monitor

Custom 2021/10/12 16:15:41 Tuesday

- Total Terminals **69**
- Risky Terminals **25**
- Important Terminals **27**
- Important Risky Terminals **21**



Risk Status

Critical

- Threat Events: **282**
- Vulnerabilities: **67**
- Asset Value: **Considerable**

Name	Severity	Events	Unresolved Events
2323	Low	47	47
43	Low	47	47
aaaaa-lnren	Low	47	47
lnren	Medium	47	47
test001	Low	47	47



Full-screen Monitoring Dashboards

Threat Events Monitoring

Threat Event Situation Monitor

Custom 2021/10/09 17:32:55 Saturday

Critical
591,275
High
835,729
Medium
1,438,251
Low
2,579,458

Statistics by Type



Total Threat Events
5,444,713

External-to-Internal	15%	842,770
Internal-to-Internal	2%	107,566
Internal-to-External	0%	15,717
Others	83%	4,478,660

Hot Threat Events



Threat Situation in Last 7 Days



Threat Event Ranking

Name	Attacks
1 test~!@#\$\$%^&*()+0 []:~><?/\	547,320
2 Inren	538,515
3 aaaaa-Inren	507,366
4 test001	489,052
5 2323	457,258
6 43	446,617
7 http_proto:host_with_ip_address	306,725
8 Firewall Policy Violation	209,323
9 Host头是一个IPv4或者IPv6地址	205,664
10 Host Header IS A IPv4 or IPv6 Addr...	205,479

Inren

Attacks **538,515** Affected Areas **2** Affected Servers **1** Affected Terminals **4**

Latest Threat Events

Attack Time	Source IP	Destination IP	Source Area/Geo Location	Destination Area/Geo Location	Severity
2021/09/22 17:05:36	10.182.0.1	10.182.243.160	-	-	Medium
2021/09/22 17:05:06	10.182.0.1	10.182.243.160	-	-	Medium
2021/09/22 17:04:43	10.182.55.116	224.0.0.251	-	-	Medium
2021/09/22 17:04:41	10.182.243.80	239.255.255.250	-	-	Medium
2021/09/22 17:04:36	10.182.0.1	10.182.243.160	-	-	Medium

Full-screen Monitoring Dashboards

Vulnerability Monitoring

Vulnerability Situation Monitor

Custom 2021/10/09 17:34:21 Saturday

Total Hosts
225

Vulnerable Host
19

TOP5 Vulnerabilities by Type

Type	Percentage	Quantity
others	78.1%	1,285
Port scanners	9.9%	163
Denial Of Service	6.1%	100
Obtain Information	3.8%	63
Bypass a restriction or similar	2.1%	34



Vulnerable Host Ranking

Rank	Host IP	Vulnerability Report Name	Scanning Time	Critical	High	Medium	Low
1	10.88.7.10	苏州实验室	2021/09/14 20:18:35	14	90	159	206
2	10.182.80.61	苏州实验室	2021/10/08 20:20:24	14	90	159	205
3	1.1.1.1	苏州实验室	2021/09/14 20:05:46	3	4	7	58
4	10.182.80.64	苏州实验室	2021/10/08 20:06:00	3	4	6	58
5	2.2.2.2	苏州实验室	2021/09/14 20:08:00	2	1	7	57

Vulnerability Ranking

Rank	Name	Quantity
1	Nessus SYN scanner	120
2	Service Detection	86
3	DCE Services Enumeration	77
4	Netstat Portscanner (SSH)	46
5	Remote listeners enumeration (Linux / AI...	39
6	HyperText Transfer Protocol (HTTP) Infor...	36
7	SSL / TLS Versions Supported	24
8	SSL Certificate Information	24
9	SSL Certificate Cannot Be Trusted	24
10	SSL Cipher Suites Supported	23

Full-screen Monitoring Dashboards

Area Monitoring

Area Situation Monitor

Area Map Display

Shhal135

test3

uoyo

ee

GH-Test Area

uoyo



Servers

2



Total Hosts

2

Terminals

0



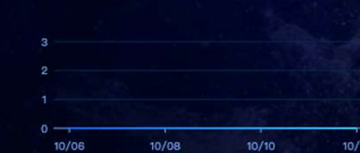
Threat Event Ranking

Name	Attacks
1 Suspicious LDAP Activity	167
2 jintianshigeaorizhijintianshigeaorizh...	8
3 Suspicious IRC Activity	8
4 ylzengtest	1

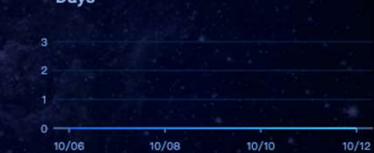
Vulnerability Ranking

Name	Quantity
1 Nessus SYN scanner	11
2 DCE Services Enumeration	7
3 Service Detection	3
4 Microsoft Windows SMB Service Dete...	2
5 Microsoft Windows SMB NativeLanMa...	1

Threat Situation in Last 7 Days



Vulnerability Situation in Last 7 Days



Total Areas

31

Risky Areas

12

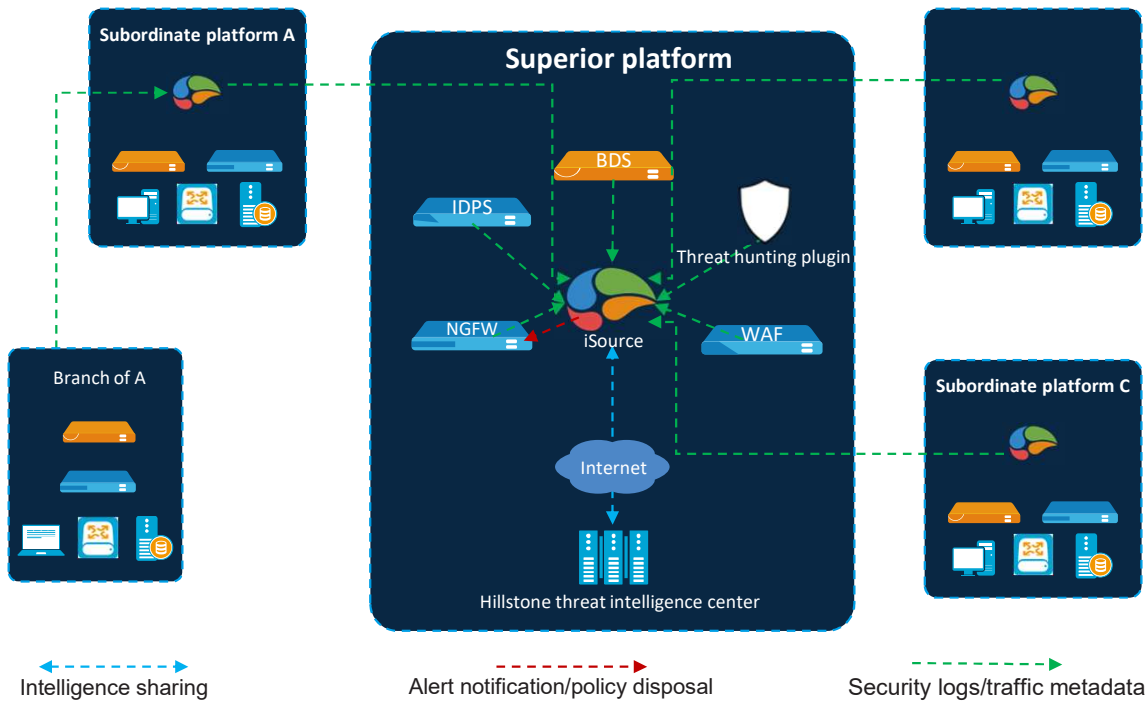
TOP5 Risky Areas

- 1 ee High
- 2 uoyo High
- 3 test3 High
- 4 Shhal135 High
- 5 GH-Test Area High



Hierarchical Management

Hierarchical Management



Hierarchical Management Monitoring Dashboard



Aggregated Security Posture Across All Platforms

Presents assets, threat events and other security posture information from all subordinate platforms as well as superior platform

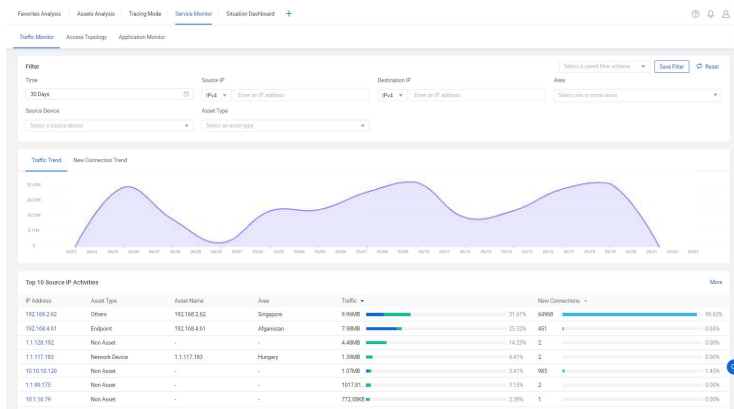
Aggregated Security Posture Monitoring Dashboard

Tiered Analysis from Different Perspectives

Efficient Data Synchronization

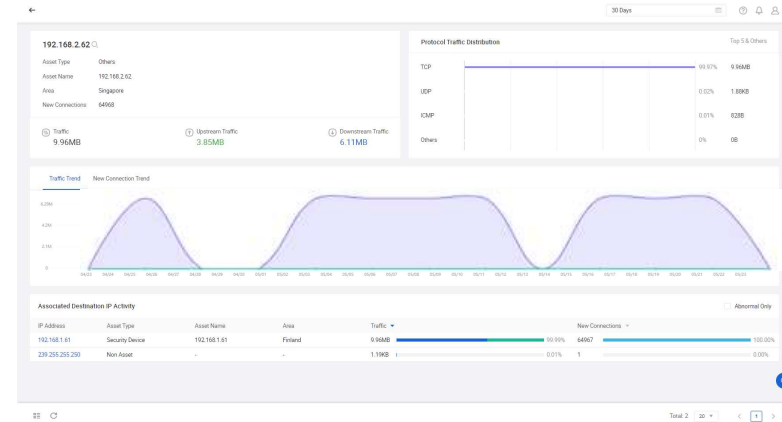
Zero Pressure on Superior Platform

Traffic Monitoring



Traffic Monitoring Overview

IP address of Top 10 Traffic /Traffic Trends



Traffic Monitoring per Individual IP

Total traffic/Traffic trends/Protocol Traffic Distribution/Associated Destination IP Activity

Collect traffic data from the netflow and metadata of BDS

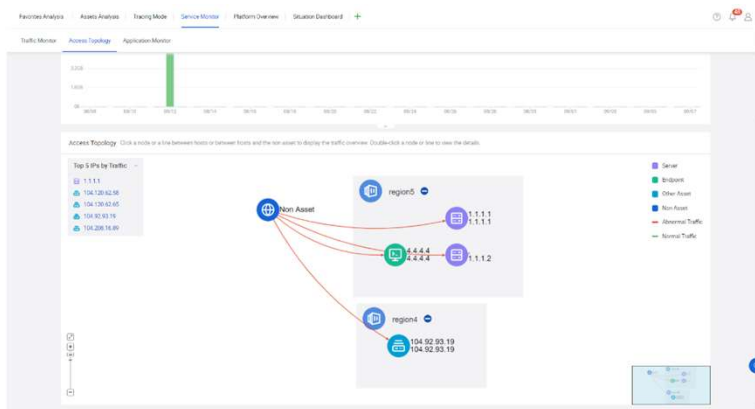
Traffic monitoring enables security analyst to detect network anomalies

Traffic Insight



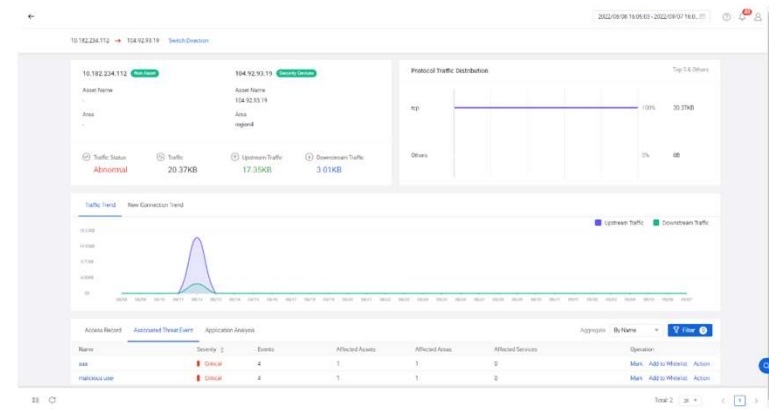
Traffic Insight Topology

- Support establishing the insight topology of network flow by collecting and analyzing the traffic
- Support visual inspection of abnormal traffic
- Support traffic baseline learning
- Support application identification in traffic



Associated Threat Event

- Support directing to the associated threat event
- Support threat information view and policy distribution



Threat Management



Visibility

Responses

Forensics

Threat Events

Comprehensive statistics for a single asset:

- Attack chain stage distribution
- Threat/ attacks trend

Present a threat with rich detail:

Threat information/MITRE ATT&CK/
PCAP/Process information/Original alert list

Threat insights:

Visualized relationship among assets

Threat Analysis

Machine Learning

Rule based detection

Threat Intelligence

Behavior Analysis

Correlation Analysis

Statistical Analysis

Threat Log

Five types of logs:

- Syslog
- Netflow
- Sysmon
- Linux
- MetaData

Advance log searching: SPL based

Support searching by:

- Key-value pair
- Regex
- Nested conditions
- Fuzzy matching

Rich decoding types:

- URL
- Base64
- Unicode
- UTF-8
- HEX
- ...

Traffic

Logs

Assets

Vulnerabilities

Users

Intelligence

Advanced Threat Analysis

Machine Learning & Statistics



Rule-based Detection

Multiple Detection Engines

- Scan
- File
- HTTP Detection
- Suspicious Protocol
- Brute Force
- Domain
- Ransom
- Mining
- USB Action
- Blocked Access
- Weak Password Detection



Behavior Analysis

Abnormal Traffic Detection

- Netflow data from BDS or NGFW
- Machine learning based traffic modeling
- Model self tuning
- Threats are registered when behavior or entity is beyond threshold baseline of normality



Correlation Analysis

Simple Mode

- Threat logs
- General logs
- Attack chain analysis: Customizable based on threat events

Advanced Mode

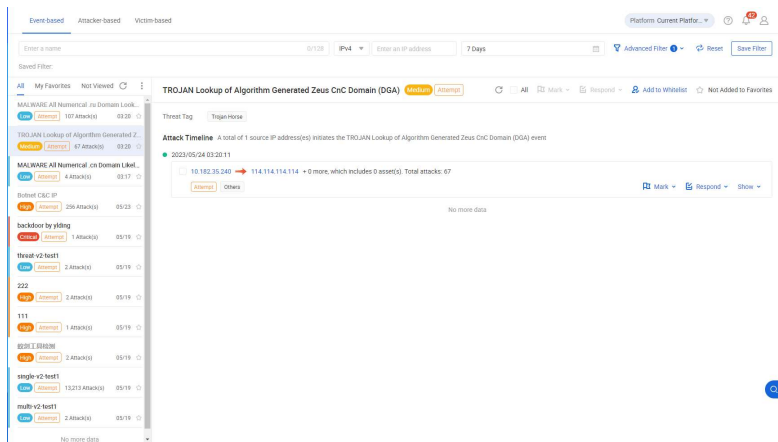
- Log-based correlation
- Event-based correlation

Threat Aggregation



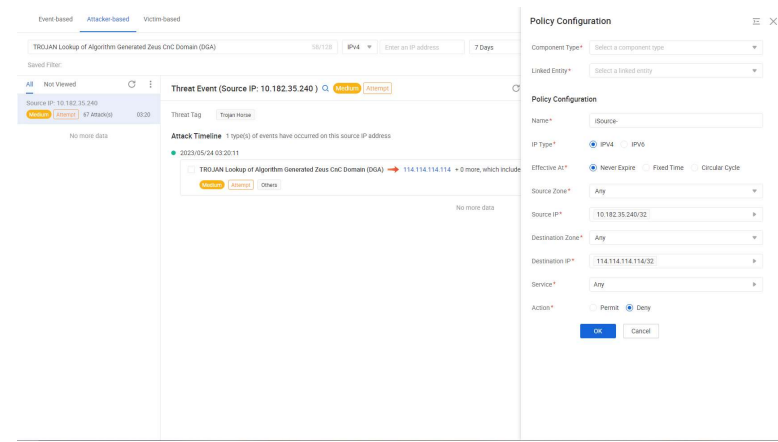
Threat Aggregation

- Aggregates threat events by: threat name, threat type, attack success status, etc.
- Aggregated analysis from: event, attacker, victim investigation
- Support secondary aggregation of threat events with identical names and source/destination IP addresses

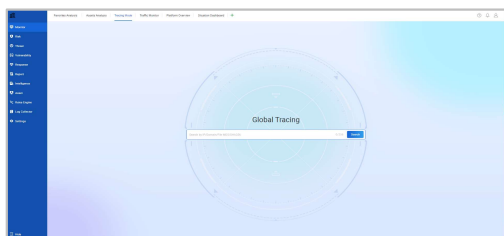


Aggregated Response

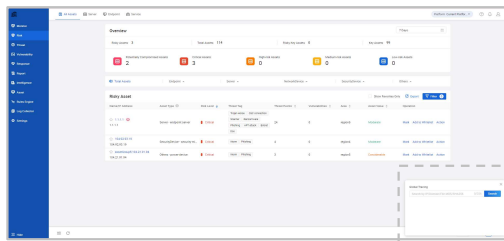
- Support batch marking and remediation of the aggregated threat events
- Remediation includes policy configuration and IP block configuration



Global Search



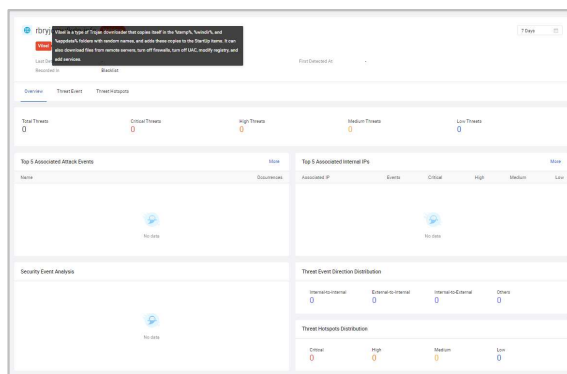
Primary entry



Quick entry

- Search via IP/domain names/URL/file MD5
- Record recent search history
- Quick entry from all pages

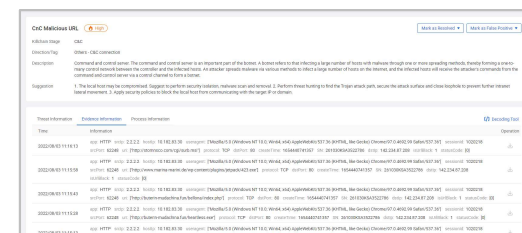
Info Display



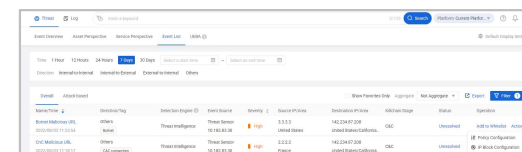
Info display

- Forensics overview, including relevant threat family information, threat/vulnerability trends, kill-chain stage etc.
- Correlate threat events, vulnerability events, traffic monitoring and hotspot intelligence to achieve one-step global search.

Incident Response



Evidence Information



Incident Response

- Support viewing/decoding /exporting/ saving event evidence information.
- Support marking threats as false positives, adding to whitelists, etc.

Vulnerability Analysis

Vulnerability Visualization

- Display statistical and detailed information about the vulnerabilities
- Support filtering by: host IP, report name, scan time, total vulnerabilities/ vulnerability name/ type/ level, and protocol
- Support auto scanning and manual import of vulnerability reports

Host IP	Vulnerability Reported/Scanned At	Type/Name	Area	Value	Vulnerability Status	Operation
10.88.7.10	苏州实验室 2021/09/14 20:18:35	Server 10.88.7.10	GH-Test Area	Considerable	Critical: 14, High: 90, Medium: 159, Low: 206	[Refresh] [Delete]
10.182.80.61	苏州实验室 2021/10/07 20:20:25	Terminal shang:10.182.80.61	Shhai135	Considerable	Critical: 14, High: 90, Medium: 159, Low: 205	[Refresh] [Delete]
1.1.1.1	苏州实验室 2021/09/14 20:05:46	Server 空去过	903	Considerable	Critical: 3, High: 4, Medium: 7, Low: 58	[Refresh] [Delete]
10.182.80.64	苏州实验室 2021/10/07 20:07:03	Terminal shang:10.182.80.64	Shhai135	Considerable	Critical: 3, High: 4, Medium: 6, Low: 58	[Refresh] [Delete]
2.2.2.2	苏州实验室 2021/09/14 20:08:00	Server Sample server12.2.2.2.2	uoyo	Moderate	Critical: 2, High: 1, Medium: 7, Low: 57	[Refresh] [Delete]
10.182.80.63	苏州实验室 2021/10/07 20:08:31	Terminal shang:10.182.80.63	Shhai135	Considerable	Critical: 2, High: 1, Medium: 6, Low: 57	[Refresh] [Delete]
10.182.80.66	苏州实验室 2021/10/07 20:09:15	Terminal shang:10.182.80.66	Shhai135	Considerable	Critical: 0, High: 4, Medium: 9, Low: 70	[Refresh] [Delete]
192.168.1.3	苏州实验室 2021/09/14 20:08:00	Server simon:192.168.1.3	nsdd1	Moderate	Critical: 0, High: 4, Medium: 9, Low: 70	[Refresh] [Delete]
10.182.80.70	苏州实验室 2021/10/07 20:09:54	Terminal shang:10.182.80.70	Shhai135	Considerable	Critical: 0, High: 0, Medium: 8, Low: 59	[Refresh] [Delete]

Scanner Management

- Support built-in scanner
- Support Nessus scanner to generate reports automatically
- Periodical scanning task configuration (daily, weekly, monthly)
- Support manually import Nessus report (.nessus files)

Scanner

<p>New Add a scanner</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td colspan="2">777</td></tr> <tr><td>IP Address</td><td>1.2.3.5</td></tr> <tr><td>Type</td><td>Nessus</td></tr> <tr><td colspan="2" style="text-align: right;">[Refresh] [Delete]</td></tr> </table>	777		IP Address	1.2.3.5	Type	Nessus	[Refresh] [Delete]		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td colspan="2">RAS</td></tr> <tr><td>IP Address</td><td>1.2.3.4</td></tr> <tr><td>Type</td><td>Nessus</td></tr> <tr><td colspan="2" style="text-align: right;">[Refresh] [Delete]</td></tr> </table>	RAS		IP Address	1.2.3.4	Type	Nessus	[Refresh] [Delete]		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td colspan="2">platform scanner</td></tr> <tr><td>IP Address</td><td>-</td></tr> <tr><td>Type</td><td>built-in</td></tr> <tr><td colspan="2" style="text-align: right;">[Refresh] [Delete]</td></tr> </table>	platform scanner		IP Address	-	Type	built-in	[Refresh] [Delete]	
777																											
IP Address	1.2.3.5																										
Type	Nessus																										
[Refresh] [Delete]																											
RAS																											
IP Address	1.2.3.4																										
Type	Nessus																										
[Refresh] [Delete]																											
platform scanner																											
IP Address	-																										
Type	built-in																										
[Refresh] [Delete]																											

Automated Security Orchestration

Playbook

Playbook module

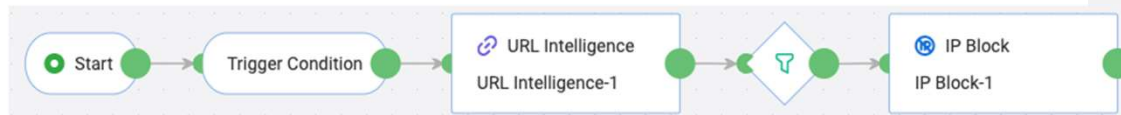
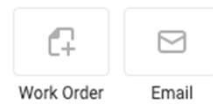
Threat Intelligence Action



Network Security Device Action



Platform Action



Automated Orchestration

- Playbook/template-based automation
- Playbook defines the threat event triggering condition, threat intelligence query, conditions to response and actions of response.
- Drag and drop to edit the playbook
- Predefined playbook templates:
 - Crypto mining
 - Ransomware
 - Brute force
 - Weak password

Threat Responses – Integrated Devices

 Linked Entity

 VirusTotal



ADC



CloudEdge



HSM



NIPS



CloudHive



NGFW



vWAF



3rd party devices



Integrated Devices

- Register integrated products
- Interact with intelligence center
- Perform actions as a response with integrated products by:
 - deploying polices
 - blocking addresses
- Action defined via template or via manual configurations
- Support 3rd party security devices over RESTful APIs or SSH to mitigate vendor lock-in inconveniences

Threat Responses – Case Management

Ticket

Overview

Total Tickets: **1076** | Pending: **1069** | Processing: **2** | Resolved: **5**

Closed: **0** | On-time: **3** | Timeout: **24**

Completion Rate: **0%**
On-time Completion Rate: **0%**

Name	Priority	Severity	Submitted At	Duration	Handler	Status	Completion Status	Operation
allgsabfahgusouagprv#@3v*4^...	Low	Low	2021/09/26 19:46:45	17 Day		Pending	Normal	
allgsabfahgusouagprv#@3v*4^...	Low	High	2021/09/26 14:34:21	17 Day	YUGONG	Resolved	Normal	
Redis Server Unprotected by Password...	High	High	2021/09/24 16:44:25	19 Day	Gh	Resolved	Timeout	
Unsupported Windows OS (remote_20...	High	Critical	2021/09/24 14:47:46	19 Day	yzeng	Pending	Normal	
10.182.80.61_20210924_114740	High	Critical	2021/09/24 14:46:56	19 Day	yzeng	Pending	Normal	
http_protohost_w0_ip_address_20210...	Medium	Medium	2021/09/24 14:44:05	19 Day	yzeng	Pending	Normal	
FTP Weak Password_20210923_21550...	Medium	Medium	2021/09/24 09:55:09	19 Day	xyfu	Pending	Normal	
FTP Weak Password_20210923_21550...	Medium	Medium	2021/09/24 09:55:01	19 Day	xyfu	Pending	Normal	
FTP Weak Password_20210923_21545...	Medium	Medium	2021/09/24 09:54:52	19 Day	xyfu	Pending	Normal	

Ticket Configuration

Name*: 0/128

Priority: High Medium Low

Severity: Critical High Medium Low

Handler:

Asset:

Deadline:



Case Management

- Assign tasks to follow up
- Status updates
- Recommended solution

Asset Centric Risk Management

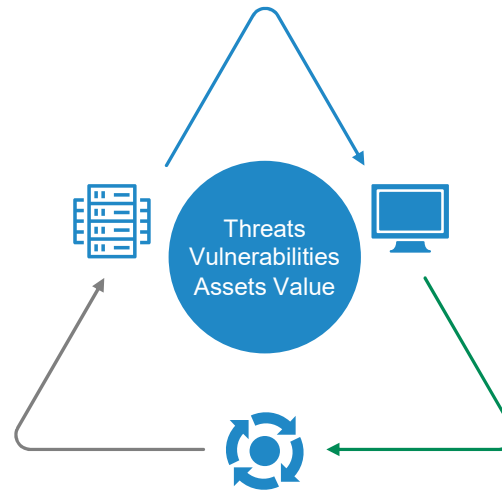
Server Risks

Server risk overview

- Total risks/distributions/trends
- Threat distribution/trends
- Vulnerabilities distribution/ trend

Server(s) risk details

- Risk reports
- Vulnerabilities
- Threat events
- Report of compromised assets



Service Risks

- Service risk overview
- Service risk details

Endpoint Risks

Endpoint risk overview

- Total risks/distributions/trends
- Threat distribution/trends
- Vulnerability distribution/trends

Endpoint(s) risk details

- Risk reports
- Vulnerabilities
- Threat events
- Report of compromised assets

Assets Management

Asset Detection

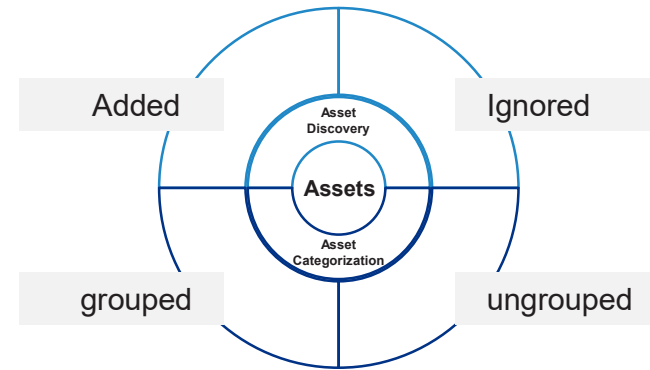
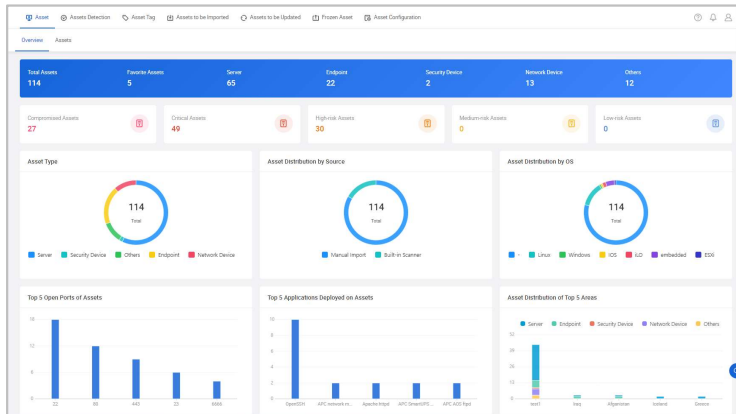
Name	Scanner	Started At	Type	Progress	Status	New Assets	Assets to be Updated	Operation
9	Built-in Scanner	2022/11/03 16:30:25	Asset Detection	100%	Finished	90	0	

Device Fingerprint

Basic Information		Service Information		Responsible Person	
Manufacturer	-	MAC Address	-	-	-
OS	-	Service	services	-	-

Port	Transport Layer Protocol	Application Layer Protocol	Deployable App and Version	Status
2	TCP	SSH	OpenSSH 8.9	enabled

Asset Overview



Asset Discovery

Discover assets via:

- Traffic
- Logs
- Threat events
- Vulnerability report
- Manual import
- Active scan

Grouping

Grouping as:

- Servers
- Endpoints
- Network devices
- Security devices
- Others

Lifecycle Management

- Asset export
- Template based import
- Asset offboarding

Favorite Asset and Threat Event Management

Favorite Assets

Total Assets | Endpoint | Server | NetworkDevice | SecurityDevice | Others

Name	IP Address	Area	Asset Type
10.182.0.0:10.182.80.21	10.182.80.21	Washington	Server - general p...
10.182.0.0:10.182.229.12	10.182.229.12	Washington	Server - general p...
10.182.0.0:10.182.79.61	10.182.79.61	Washington	Server - general p...
training-pc	10.181.0.10	BeiJing	Endpoint - endpo...

Are you sure to add 10.182.0.0:10.182.80.21 to fav...

Alarm Recipient: Select an alarm contact

After you add the asset to favorites, the system automatically generates two alarm rules. If a favorite threat event, critical threat event, or high-risk threat event occurs on the asset, the system sends an alarm to the administrator

Cancel OK

Favorites Function

Provide extra attention and independent analysis to assets/threat events customer marked as favorites.

Various Alert Rules

iSource automatically correlates favorite events and assets to generate corresponding alert rules. Users can also configure independent alert rules for favorite assets.

Favorite threat events

My Favorites

Favorite Threat Events

- HTTP Header Contain Abnormal Keywords: 0
- SYN Port Scanned: 0
- HTTP Weak Password: 0

Favorite Configuration

- Web/Http Scanned
- Web/Port Scanned
- IP Address Scan Check
- Host Port Scan Check
- Web/Port Scan Check
- Web/Port Scan Check
- File
- HTTP Detection
- Subspace History
- Sniff Force
- Device
- Networkmap Other Logset
- Sniff
- Web/Http
- Blacklist
- Threat Intelligence
- Weak Password Detection
- Threat Log
- General Log
- Advanced Traffic
- Advanced Log
- Government Risk/Trust Region
- Threat Base

Favorite Posture

- Support filtering favorite threat events on threat event list
- Support filtering favorite assets on asset list

Intelligence Management

Hotspot Intelligence

- CVE threat Intelligence notification supports intelligence search by
 - IP
 - File
 - Domain
 - URL
 - Name
 - CVEID
 - CNNVD
 - Threat tag
- Support asset check by opening a case directly from a new intelligence tab

Hillstone Intelligence Database

- Hillstone Intelligence Databases:
 - Domain
 - IP
 - Vulnerability
 - MITRE ATT&CK®
 - Abnormal Behavior
 - Honeypot
 - Intrusion detection
 - Malicious code
 - Geo-location
 - Web Attack Detection
 - Malware Behavior
- Updates periodically or on-demand
- Supports online or offline update

Allow/Block List

- Customizable access list:
 - DNS allow list
 - File allow list
 - DNS block list
 - Malicious code block list
 - IP block list

Log Management

Log Parse

- 3rd party log integration
- Predefined parsing template
- Custom parse configuration
- Support parsing:
 - Grok
 - Key-Value
 - JSON

Log Source

- Trusted log sources
- Ensure the system security

Log Storage

- Storage availability
- Log backup configuration
- Log restoration

Log Device

- List Sysmon host
- Auto updated

Log Server

- External Log servers that iSource will send the followings to:
- Collected logs
 - Detected threat events

Report Management



Report Overview

- List all reports
- Support live view
- Support export report in PDF
- Support manual export for customizable queries



Report Task

- Generate reports periodically (daily/weekly/monthly)
- Overview or detailed reports

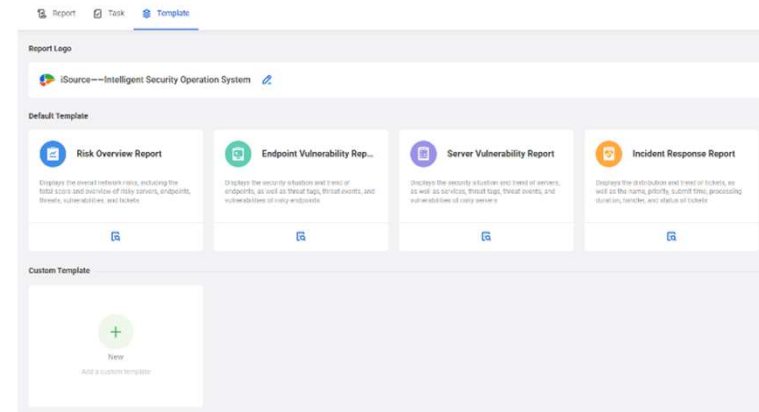


Report Template

- Multiple pre-defined templates
- Customizable templates



A page of summary report

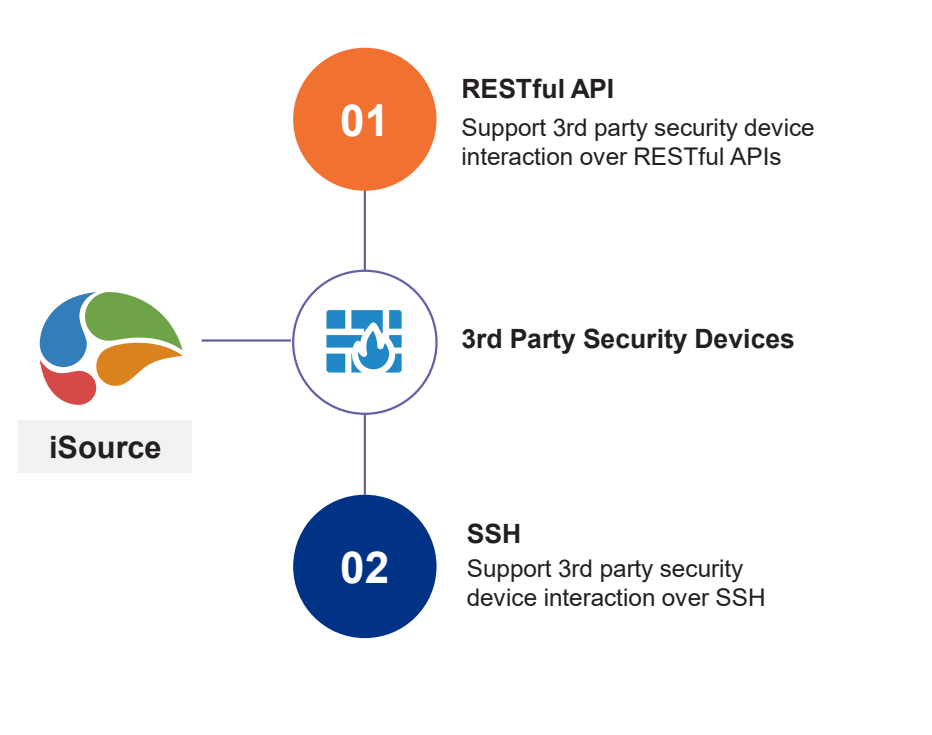
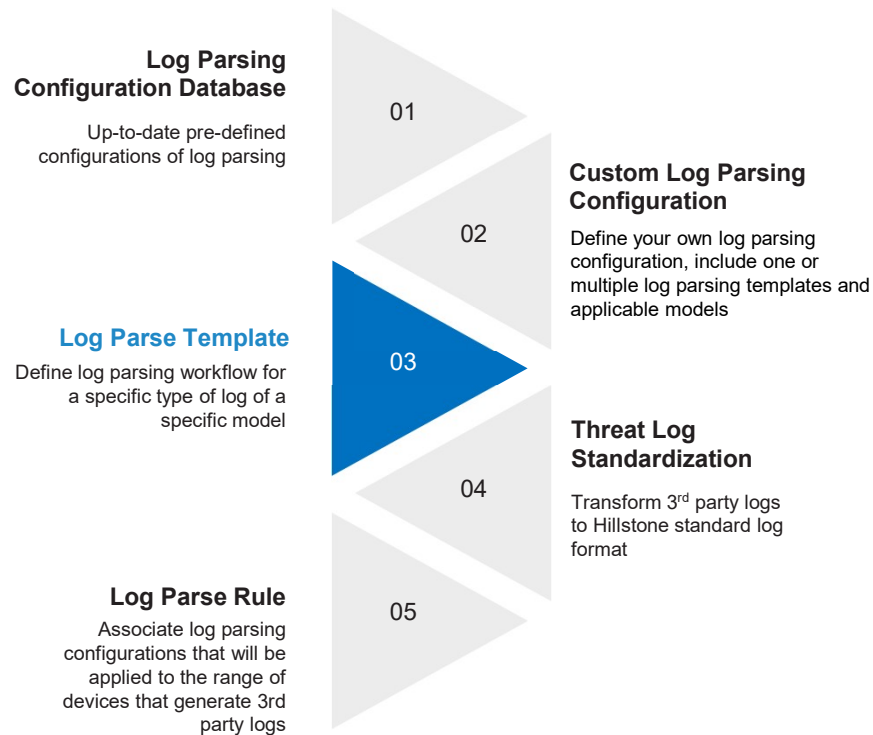


Rich report templates

XDR Eco-System

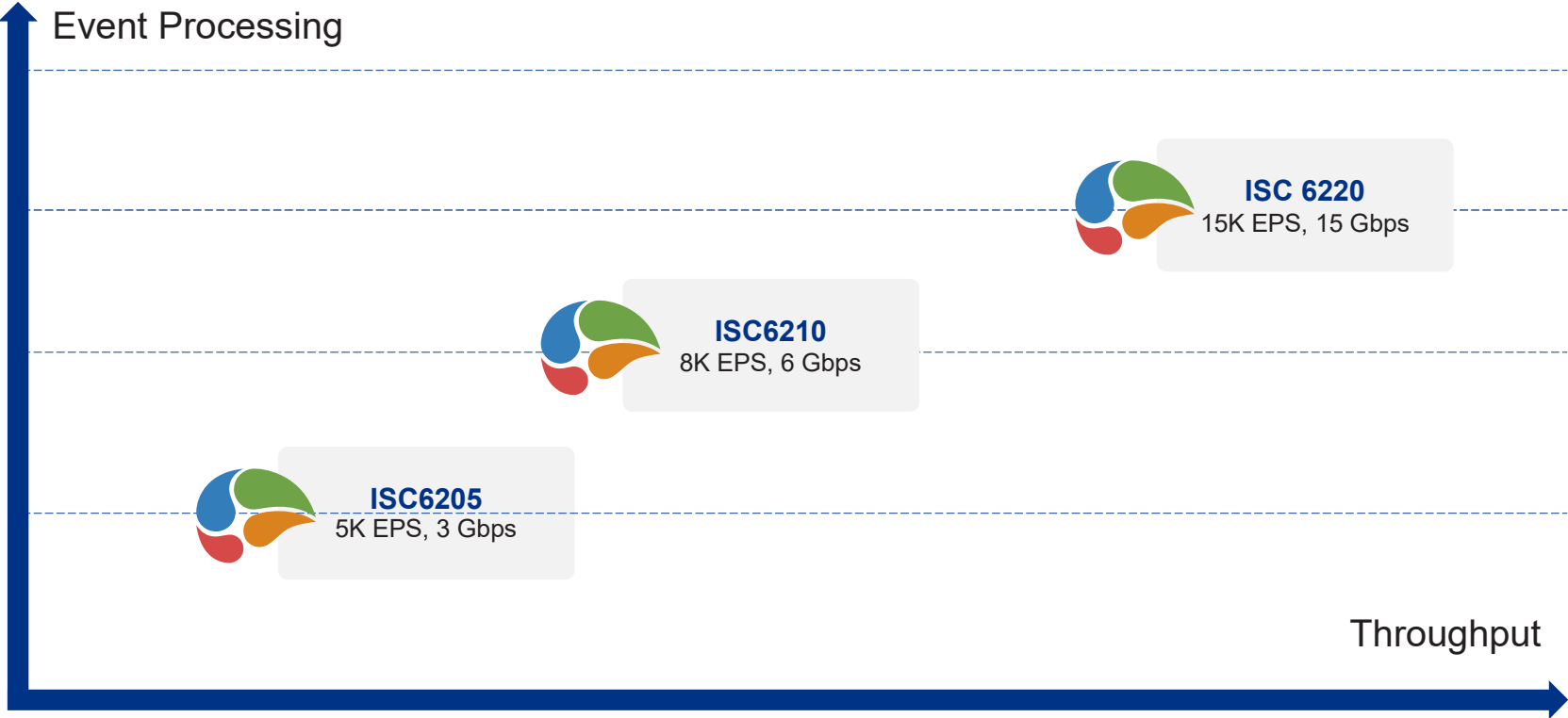
3rd Party Log Integration

3rd Party Product Integration (Enforcement Point)



Product Models & Ordering Info

Hillstone iSource Product Portfolio



iSource is offered as a software package

These 3 different models offer different performances and require different hardware configuration

iSource Software Package Format



iSource supports installation in the following environments

Environment	Version	Software Image Format
VMware EXSi	EXSi V6.7	VMDK OVA
Linux	CentOS7	QCOW2
Windows	Windows 10	VHD

Hillstone iSource Specification



Models	SG-6000-ISC6205	SG-6000-ISC6210	SG-6000-ISC6220	
Performance	Throughput	3Gbps	6Gbps	15Gbps
	Event Processing	5000EPS	8000EPS	15000EPS
Minimum Hardware Configuration	CPU	20 cores (64bits)	24 cores (64bits)	48 cores (64bits)
	Memory	128G	128G	256G

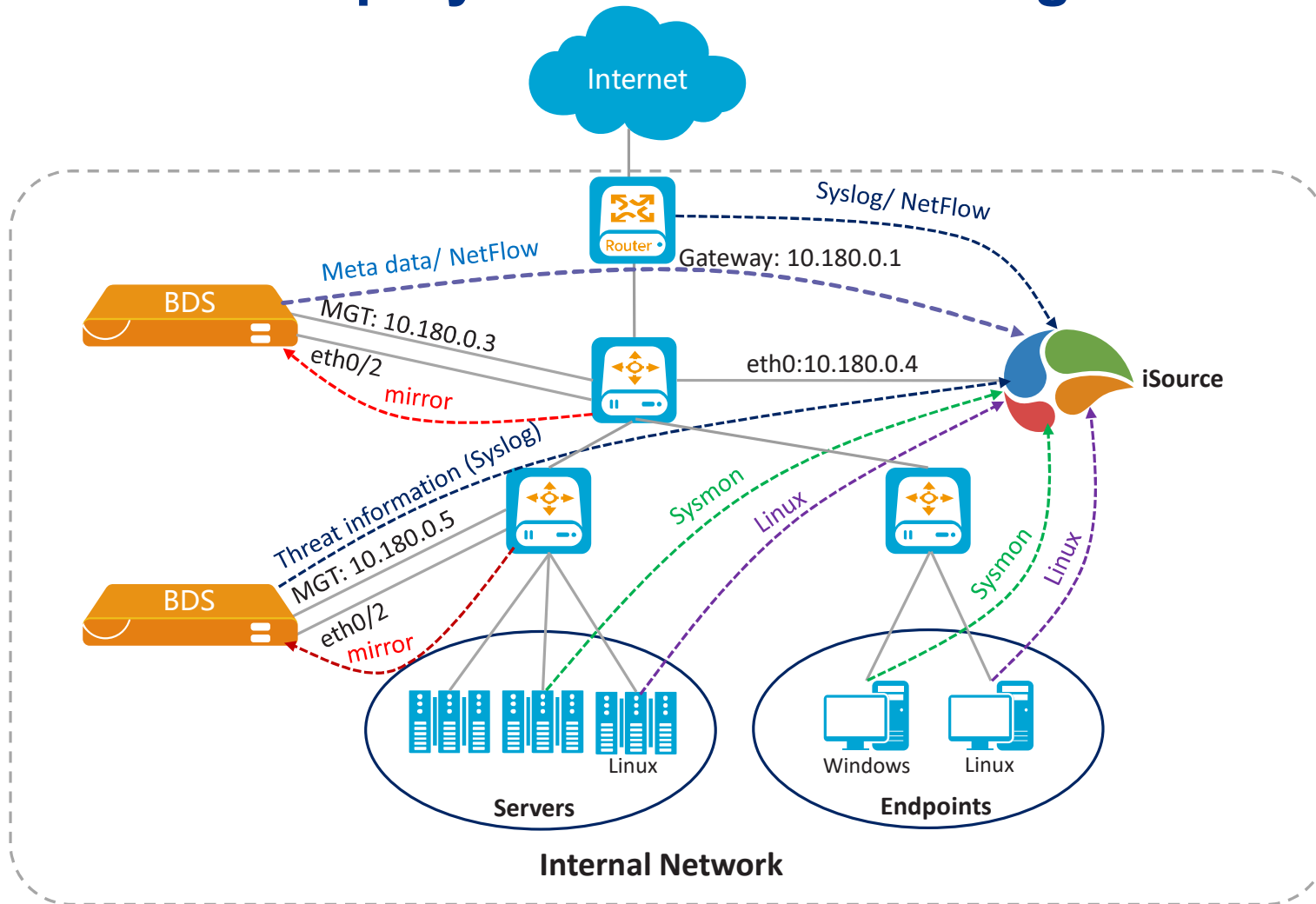
iSource Ordering Guide



Category	SKU	Definition
Base System	SG-6000-ISC6205-BP-IN	iSource ISC6205 Base System
	SG-6000-ISC6210-BP-IN	iSource ISC6210 Base System
	SG-6000-ISC6220-BP-IN	iSource ISC6220 Base System
Software Maintenance Service	SG-6000-ISC6205-SP-IN12	iSource ISC6205 1 Year Software Maintenance Service
	SG-6000-ISC6210-SP-IN12	iSource ISC6210 1 Year Software Maintenance Service
	SG-6000-ISC6220-SP-IN12	iSource ISC6220 1 Year Software Maintenance Service

Deployment Scenarios & Use Cases

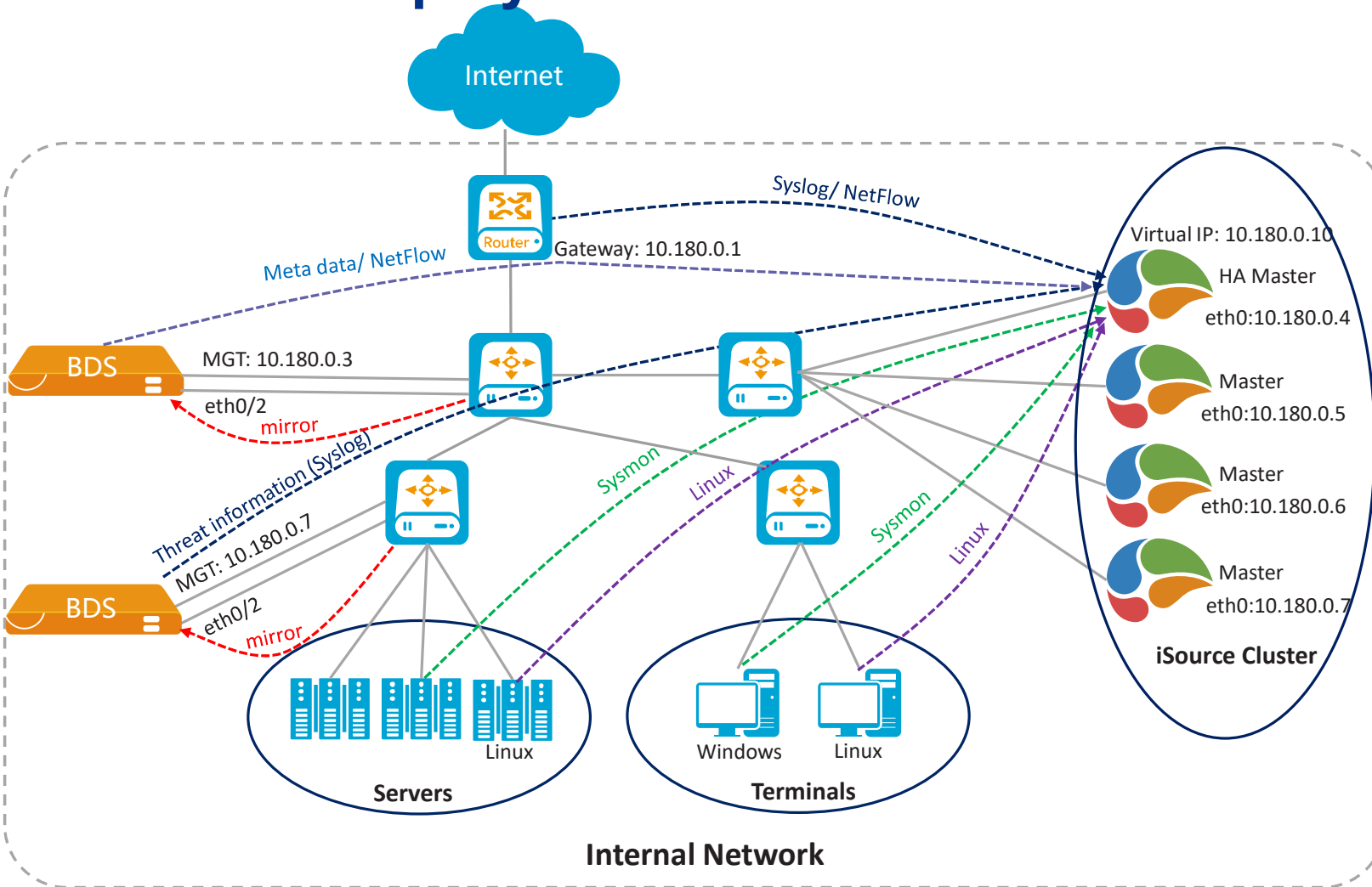
iSource Deployment Scenario- Single Node



Single Node Deployment

- BDS as a network sensor in TAP mode
- iSource deployment has little impact on the existing network environment
- Economic solution

iSource Deployment Scenario- Cluster



Cluster Deployment

- BDS as a network sensor in TAP mode
- Cluster up to 5 nodes
- iSource deployment has little impact on the existing network environment
- Highly scalable solution

Use Case- Ransomware Solution



源IP地址	目的IP地址	源端口	目的端口	协议	操作
10.180.134.220	10.180.192.200	52108	445	SMB	允许
10.180.192.200	10.180.134.220	445	52108	SMB	允许

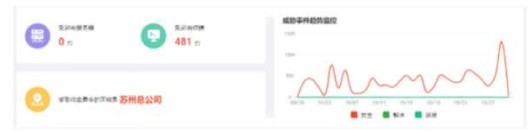
Multiple alters for remote code execution via RDP on Microsoft Server Message Block 1.0 (SMBv1) server

- 01 A server in internal subnet A was cracked by the brute force scanner from hacker when it was working as Internet NAT device during operation. Then, it worked as a jump server to attack the rest of the network and other domains.
- 02 The domain controller server of domain B was then compromised because of a weak password. All the credentials were compromised.
- 03 All the servers in domain B were logged into centrally and executed the ransomware.
- 04 Eliminates anti-virus software using PC Hunter.



开始时间	结束时间	应用/协议	目的
2020/10/29 01:00:17	2020/10/29 01:05:17	NETBIOS	目的地址: 10.180.134.220
			端口: 445
			目的地址区域: 苏州总公司

The Source IP of the attack is an internal host. It has been affected by 'eternal blue' ransomware after investigation, and is being spread.



- Response includes:**
- 01 Close port 445 and deny the bilateral data request
 - 02 Discover and analyze the compromised hosts and take them offline
 - 03 Install MS17-010 patch to all internal hosts
 - 04 Collect relevant data to build a solution in the future.

```

time: 2020/10/29 01:09:06
type: Message
severity: Critical
sourceName: 2307001130001321
srcIp: 10.180.192.200
dstIp: 10.180.134.220
subCategory: Web Attack
protectionType: 0
hostIp: 10.180.81.3
srcPort: 445
dstPort: 445
protocol: SMB
threatName: SMB Doublepulsar Remote Code Execution (CVE-2017-0143)
action: pcas, log-only
msg: 10.180.134.220 -> 10.180.192.200:445 [SMB]
message: Threat[IPS]: CRITICAL! From 10.180.192.200 [SMB] to 10.180.134.220 [SMB], threat name: SMB Doublepulsar Remote Code Execution (CVE-2017-0143), threat type: Attack, threat subtype: Web Attack, App/Protocol: NETBIOS, action: pcas, logonly, defender: IPS, signature: D_11605802_profile_vR_piling_threat.severity: High, policy: 1
    
```

Use Case– Crypto-mining

- As the value of digital currency continues to rise, stealing the computing power of a user's computer processor for mining has become one of the main threats in the online world.
- Education is the industry most heavily impacted by crypto-mining and Trojan horse attacks



Crypto-mining Trojan horses were found in multiple servers in a customer who deployed iSource in their environment. The compromised servers were sending a large amount of data to the mining pool frequently.

挖矿进程行为 历史记录 筛选

攻击阶段: 命令控制
 方向/威胁标签: 横向威胁, C&C连接(通信和指挥控制)

相关信息: 比特币 (BTC)、门罗币 (XMR) 等虚拟货币, 通过“挖矿”产生, 所谓“挖矿”实际上是利用计算机进行复杂的数学计算, 虚拟货币可用于互联网金融, 也可作为一种新型货币在现实世界中直接使用。由于虚拟货币带来的经济利益驱动, 挖矿有着日益成为黑客和勒索病毒勒索的方式之一, 黑客利用挖矿病毒, 使个人计算机或服务器成为矿机, 运行复杂的运算, 从而获取虚拟货币, 牟取暴利。“挖矿”会导致计算机的运算被占用, 比如主机CPU占用率高, 造成可用空间有限, 主要造成性能问题, 严重影响正常的业务, 检测到主机与挖矿服务器进行通信的流量, 表明主机很有可能感染了挖矿病毒, 正在尝试与矿池建立连接。

处置建议: 1. 建议用户检查内网主机是否主动安装过网络资源挖掘软件, 用户不知情的情况下安装了挖矿软件表明该主机可能已经沦为僵尸主机, 请考虑立即卸载挖矿软件并运行主机杀毒软件进行排查。2. 加强安全管理, 不要点击来源不明的邮件中的链接或附件, 不要在网站随意下载软件, 3. 及时安装安全软件并开启病毒库, 定期查杀病毒, 保持及时补丁, 4. 及时更新Windows安全补丁及Web漏洞补丁。

威胁情报 威胁信息 进程信息

开始时间: 2020/11/11 13:36:14
 威胁名称: 挖矿进程行为
 域名: server9.sources.com
 DNS服务器: 10.0.0.10

IP地址: 10.0.0.110
 端口: 50369
 源地址区域: 欧洲

进程名: 挖矿
 IP地址: 10.0.0.10
 端口: 53
 目的地址区域: 欧洲

名称/时间	方向/威胁标签	所属引擎	来源	攻击	源IP地址区域	目的IP地址区域	状态	操作
挖矿进程行为 2020/11/11 13:36:14	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/11 13:35:49	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/11 02:22:16	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/11 08:52:13	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 20:49:09	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 20:49:08	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 20:49:05	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 20:49:05	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 20:49:04	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 19:25:33	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 17:24:20	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗
挖矿进程行为 2020/11/10 17:24:14	横向威胁 C&C连接 虚拟货币挖矿	挖矿类	挖矿	高危	10.0.0.110	203.107.1.1	未解决	🔗

Use Case– Closed Loop Response

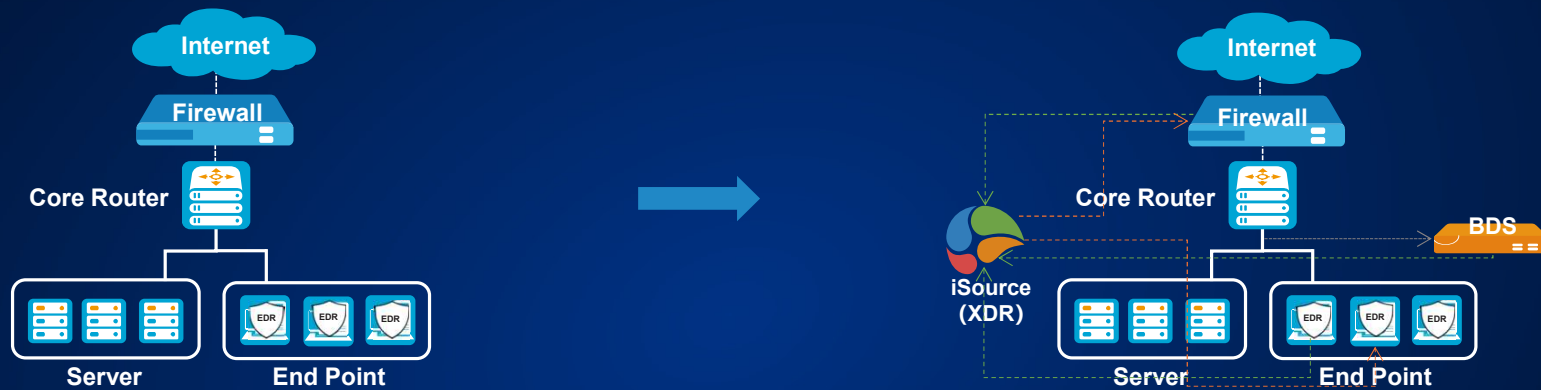
Evidence
Source of attack, the context, the logical relation among security events.
Source of attacks
Total attackers and its distribution
Fingerprint
The fingerprint of attack tools
Characteristics
Attack event, request, target, path, content etc.
Interactive Response
Interactive response based on the security orchestration:
<ol style="list-style-type: none"> 1. Add the source IP of the attack to the blocked list 2. Quarantine the malicious program by interacting with the installed agent on the servers



Incident Alert
A group of backdoor attack alerts with extremely similar behaviors appeared. The target of the attack was a hospital website, and each attack source only appeared once during the period.
Correlation Analysis
Attack source analysis, attack fingerprint analysis, attack feature analysis, attack target analysis, association of the attacker's behavior with threat intelligence.
<ol style="list-style-type: none"> 1. The attack source has botnets, credential-stuffing, etc.; 2. The fingerprint feature of the attack source is an IoT device 3. The attack source is a controlled IoT botnet whose IP is located in Hong Kong: XX.XX.XX.*
Alerts & Notification
Alert and Notification
<ol style="list-style-type: none"> 1. Send alerts through iSource and over Email 2. Create a case and assign to security operators

Case Studies

Protect Critical Business for A National Bank



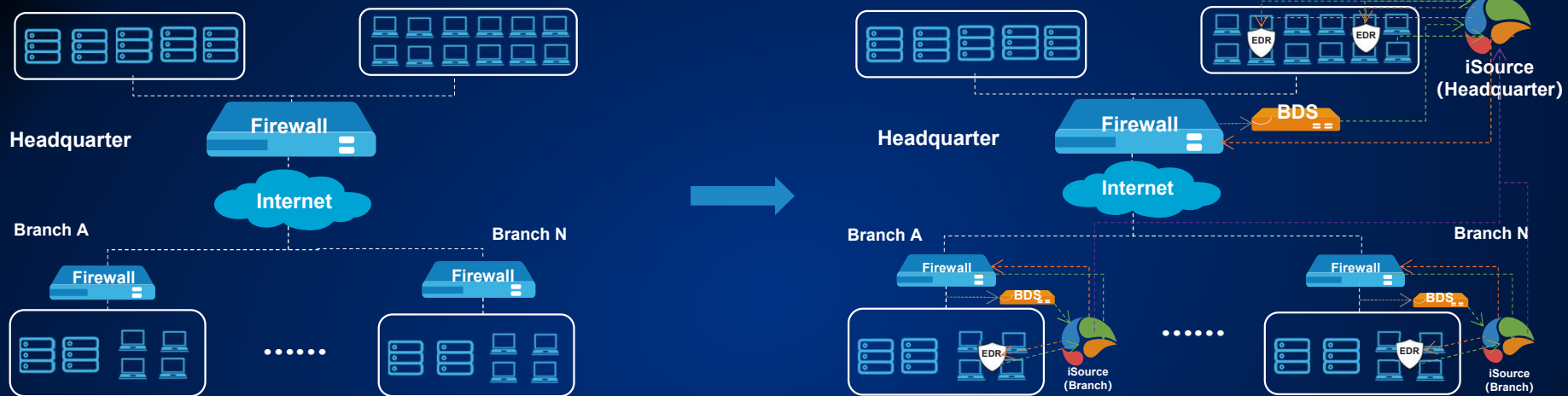
Customer Pain Points

- The customer had perimeter security devices in place, but they faced difficulties in effectively analyzing and mitigating threats within their Intranet environment;
- Although the firewall could detect threats that breached the perimeter, the dynamically assigned IP addresses of endpoints through DHCP made it challenging to identify and locate risky endpoints.

Hillstone Solutions

- Hillstone BDS(Breach Detection System) was employed to mirror network traffic, actively scanning for threats within the intranet. It captured relevant asset information, threat logs, metadata, and netflow data, which were then forwarded to the iSource platform for further analysis;
- EDR was deployed on endpoints to collect asset information and threat logs, which enabled iSource to conduct baseline inspection, antivirus scans, and other necessary assessments on the endpoint data;
- Hillstone iSource efficiently detected and responded to hidden and sophisticated threats by correlating data from firewalls, BDS, and EDR, and utilizing its automated incident response capabilities.

Protect Branch Security for A Service Provider



Customer Pain Points

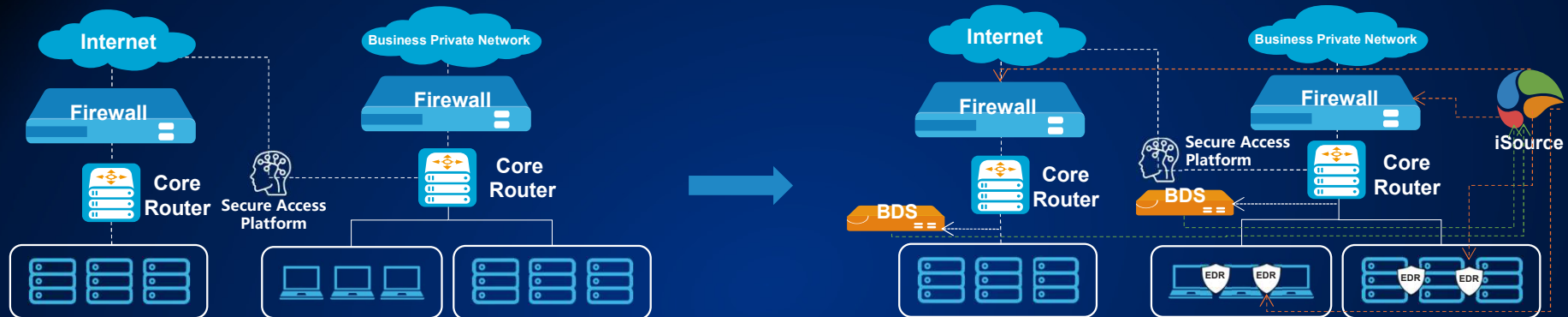
- The customer, with a large organizational structure, required unified supervision of multiple subordinate organizations;
- Despite having perimeter security devices in place at both headquarters and branches, there was a lack of capability to analyze and mitigate threats within the Intranet;
- The customer also faced challenges in locating risky hosts due to the complexity of the network environment.

Hillstone Solutions

- Hillstone iSource XDR solution offered hierarchical management for multiple branches, enabling comprehensive supervision. The iSource platform at headquarters provided a centralized view of the organization's security posture;
- Hillstone iSource XDR solution correlated data from BDS and EDR to effectively detect threats within the Intranet;
- Integration of firewall and EDR devices across subordinate platforms, along with automated orchestration capability, enabled a closed-loop response. This facilitated the efficient identification of attack sources, thereby enhancing the organization's overall security posture.

© 2023 Hillstone Networks | All Rights Reserved.

Streamline Security Operation for A Government Agency



Customer Pain Points

- Customer relied on passive threat prevention for their business operations;
- Manual analysis of large number of security logs was required;
- Incident response involved multiple devices/systems;
- Heavy workload and low efficiency in incident response.

Hillstone Solutions

- Hillstone iSource XDR solution was deployed at the government agency, which integrated various security tools including NGFW and BDS, enabling unified visibility of security posture across networks, servers, and endpoints;
- It utilized pre-defined playbooks for automated incident response actions;
- It also provided advanced ML-driven analytics and detection for rapid threat detection and remediation.



Integrative
Cyber
Security

Hillstone
NETWORKS

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

