



**VOTRE PARTENAIRE
TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT
SÉCURISÉES ET PERFORMANTES**



EXPERTISE

Des solutions adaptées
à chaque environnement



CONFIANCE

Un partenaire fiable
à vos côtés



PERFORMANCE

Des infrastructures
sécurisées et évolutives



SUPPORT

Un accompagnement
technique de qualité



HAFS

Distributeur à valeur ajoutée

Des solutions IT innovantes pour
un monde connecté et sécurisé



**WIRELESS
RADIO**

Connectivité sans fil
haute performance



**RÉSEAUX &
SÉCURITÉ IT**

Des réseaux fiables
et sécurisés



**VIRTUALISATION
CLOUD**

Des solutions Cloud
flexibles et évolutives



CYBERSECURITY

Protéger vos données
et vos systèmes



**VIDÉO
PROTECTION**

Solutions de vidéosurveillance
intelligentes



**HCI STOCKAGE
SAUVEGARDE**

Stockage, sauvegarde
et haute disponibilité

SOLUTIONS IT

CYBERSÉCURITÉ

CLOUD

INFRASTRUCTURE RÉSEAU

STOCKAGE

PROTECTION

Hillstone iSource Product Introduction



Integrative Cybersecurity
Visionary. AI-powered. Accessible.

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

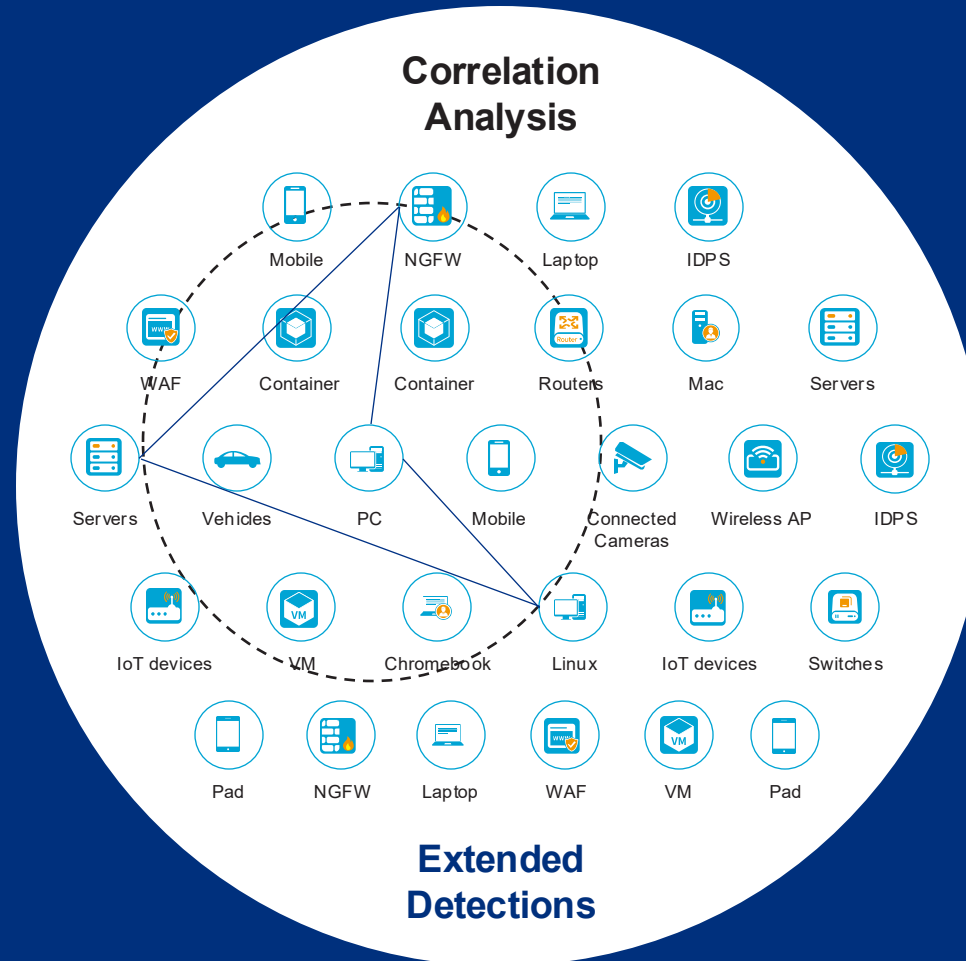
What Do Customers Need?

Comprehensive Data Collection

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

Full visibility

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



Threat Hunting and Analysis

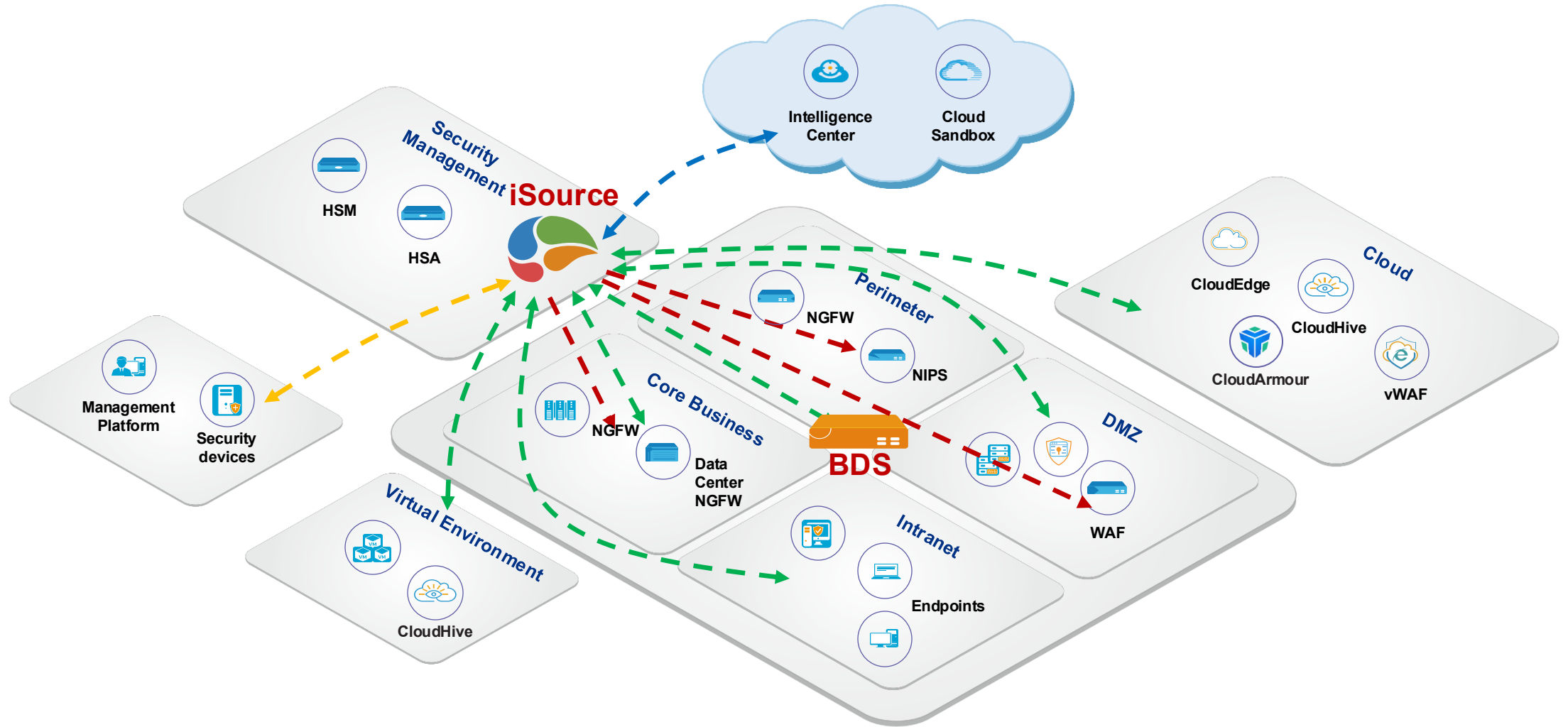
- Threat detection
- Behavior analysis
- Correlation analysis
- Root cause and attack source analysis
- ...

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
- IoT asset discovery

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

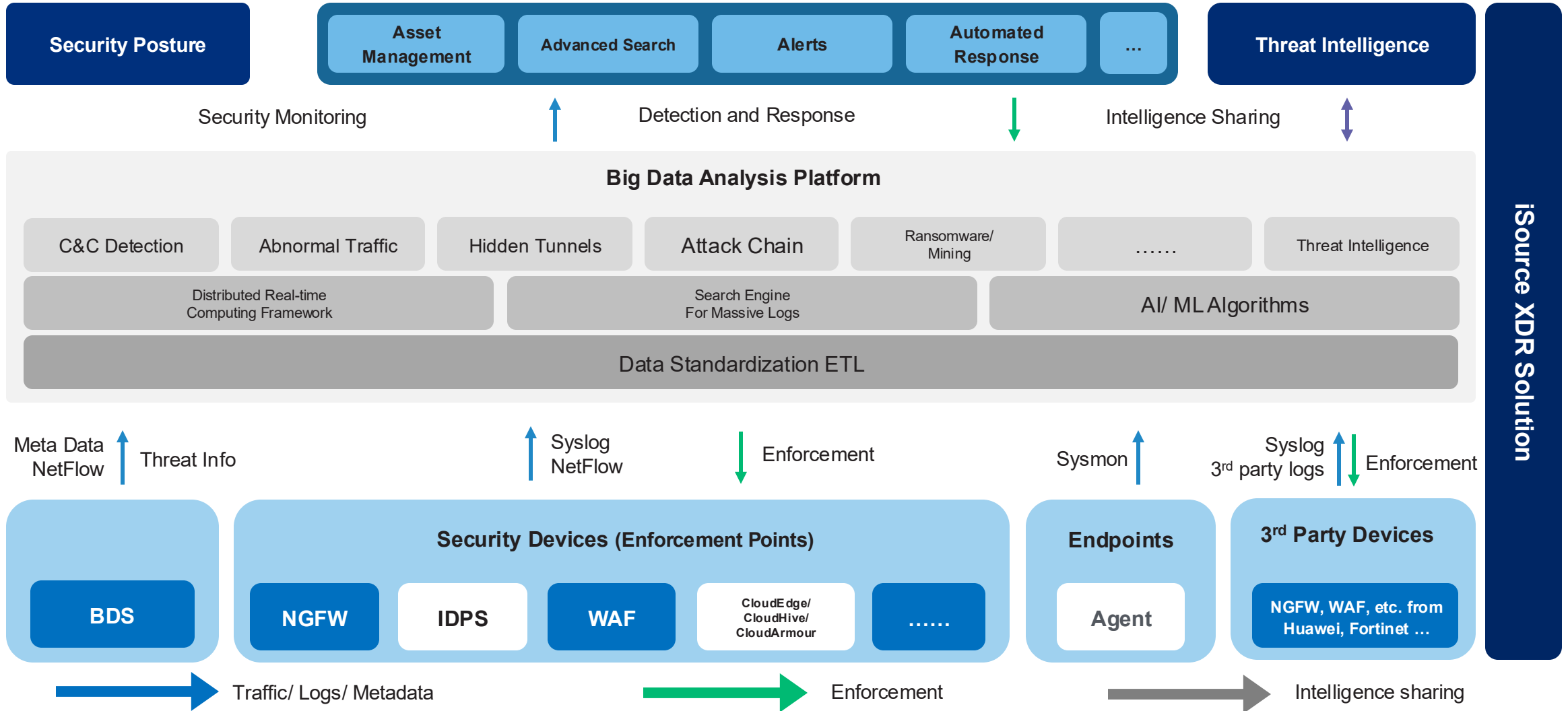
- Playbook driven orchestration
- Auto responses over enforcement points (integrated security devices)

06

Open Platform with High scalability

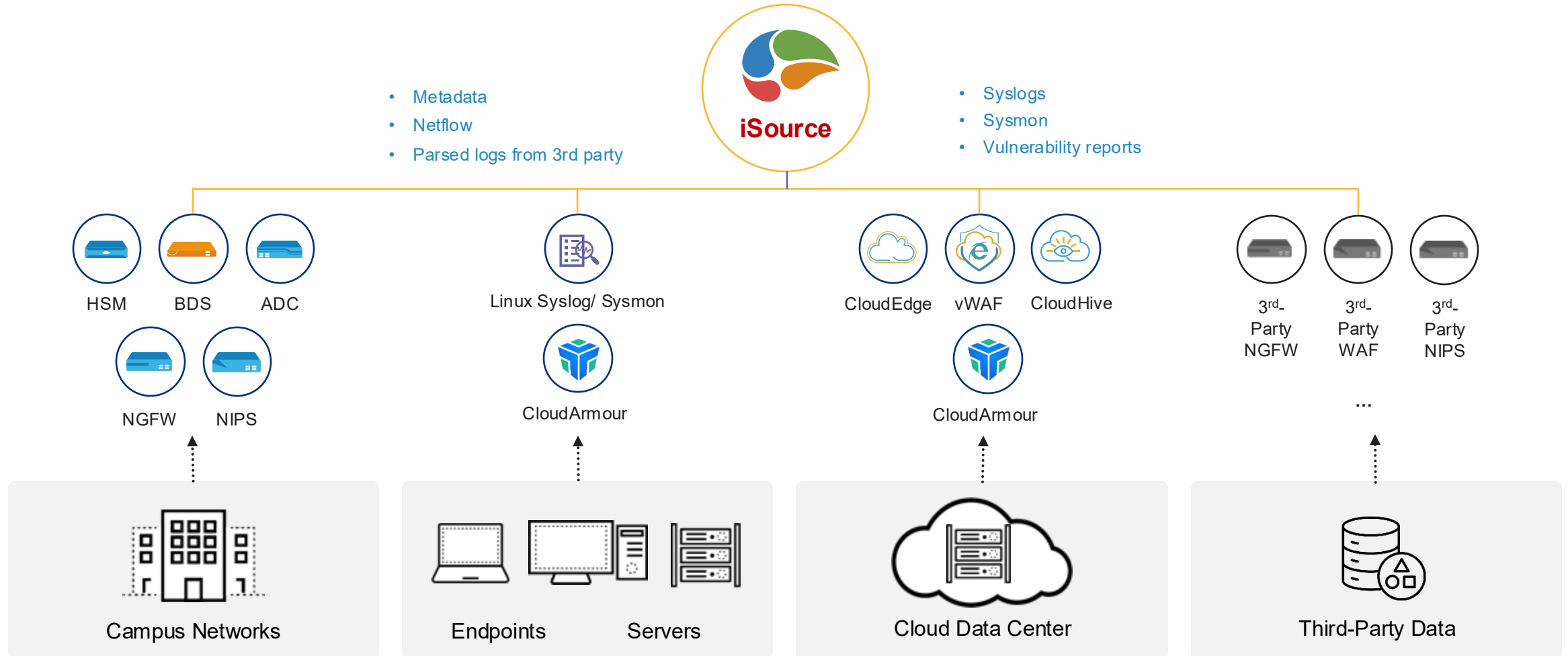
- Support 3rd party logs
- Support 3rd party security device integration
- Support clustering for scalability

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



Killchain Stage 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



Attack Event Trendline



TOP5 Attacker Locations

1	Australia	615,842Times
2	China	40Times

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 Threat Event

Total Threat Events: **926,168**

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

Date	Threat Events
10/06	0
10/08	0
10/10	1
10/11	9
10/12	2

Server Security Status Distribution

14 Risky Servers

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

Risk Status

Critical

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

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 Vulnerability

Total Vulnerabilities: **735**

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

Date	Vulnerabilities
10/06	0
10/08	0
10/10	0
10/11	3
10/12	0

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**



Terminal Threat Event

Total Threat Events **34,935**

● Critical ● High ● Medium ● Low

Terminal Security Status Distribution

25 Risky Terminals

Critical	36%	9
High	48%	12
Medium	12%	3
Low	4%	1

Risk Status

Critical

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

TOP5 Threat Events

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

Terminal Vulnerability

Total Vulnerabilities **1,063**

● Critical ● High ● Medium ● Low

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

Hot Threat Events



Threat Situation in Last 7 Days



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

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

Threat Event Ranking

Name	Attacks
1 test~!@#%*&*()_+{} :~<?/\	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

Full-screen Monitoring Dashboards

Vulnerability Monitoring

Vulnerability Situation Monitor

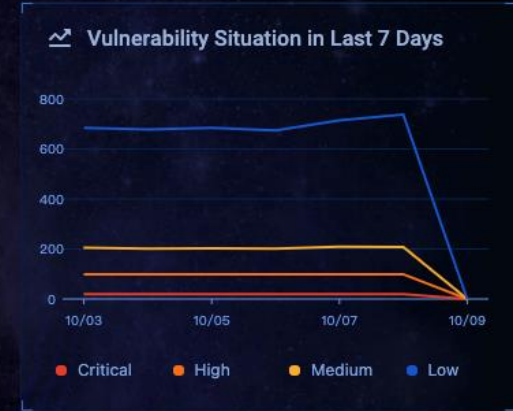
Custom 2021/10/09 17:34:21 Saturday

Total Hosts
225

Vulnerable Host
19

TOP5 Vulnerabilities by Type

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



Vulnerability Ranking

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

Vulnerable Host Ranking

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

Full-screen Monitoring Dashboards

Area Monitoring

Area Situation Monitor

Custom 2021/10/12 16:17:26 Tuesday

Area Map Display



uoyo

Servers **2**

Total Hosts **2**

Terminals **0**

Normal Servers	50.00%	1	Normal Terminals	0%	0
Risky Servers	50.00%	1	Risky Terminals	0%	0

Threat Event Ranking

Name	Attacks
1 Suspicious LDAP Activity	167
2 jintianshigehaarizhijintianshigeaarizh...	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 Shhai135	High
5 GH-Test Area	High

Asset Discovery and Management

Asset Detection

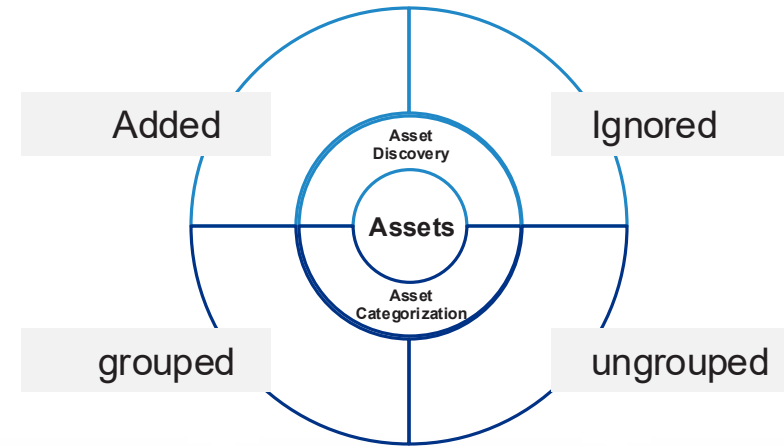
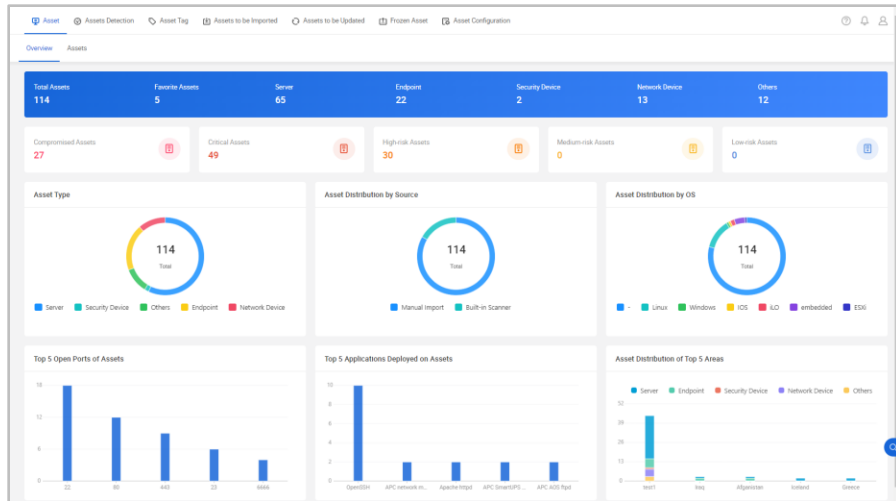
Name	Scanner	Started At	Type	Progress	Status	New Assets	Assets to be Updated	Operation
9	Built-in Scanner	2022/11/08 16:30:25	Asset Detection	100%	Finished	50	0	

Device Fingerprint

assetGroup5:104.94.62.158

Port	Transport Layer Protocol	Application Layer Protocol	Deployable App and Version	Status
22	TCP	SSH	OpenSSH/9.0	enabled

Asset Overview



Asset Discovery

Discover assets via:

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

Grouping

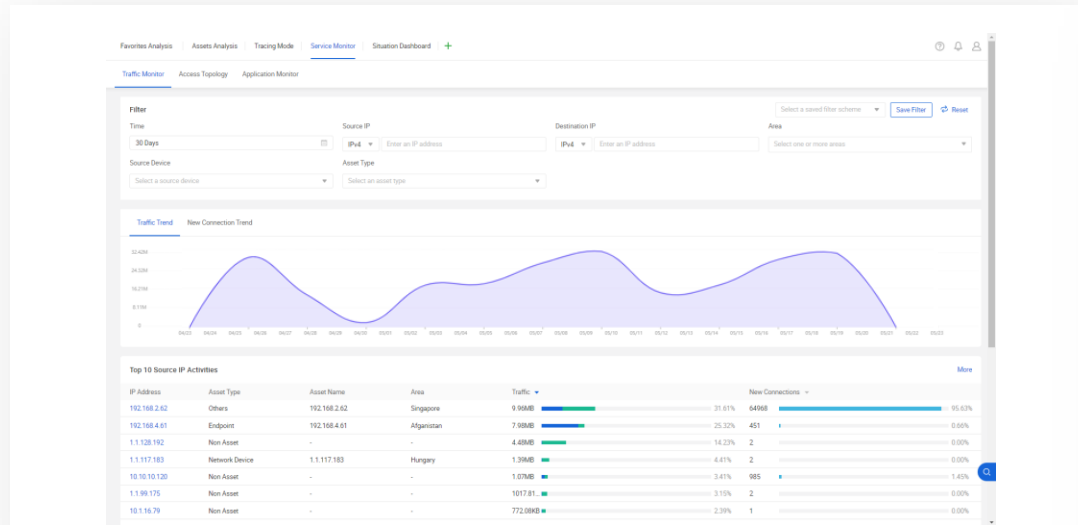
Grouping as:

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

Lifecycle Management

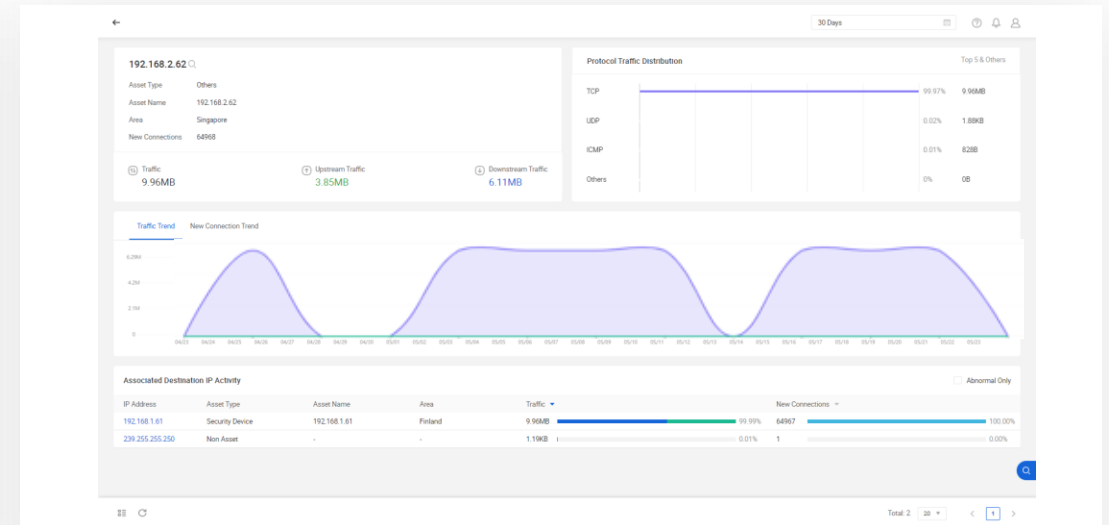
- Asset export
- Template based import
- Asset offboarding

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

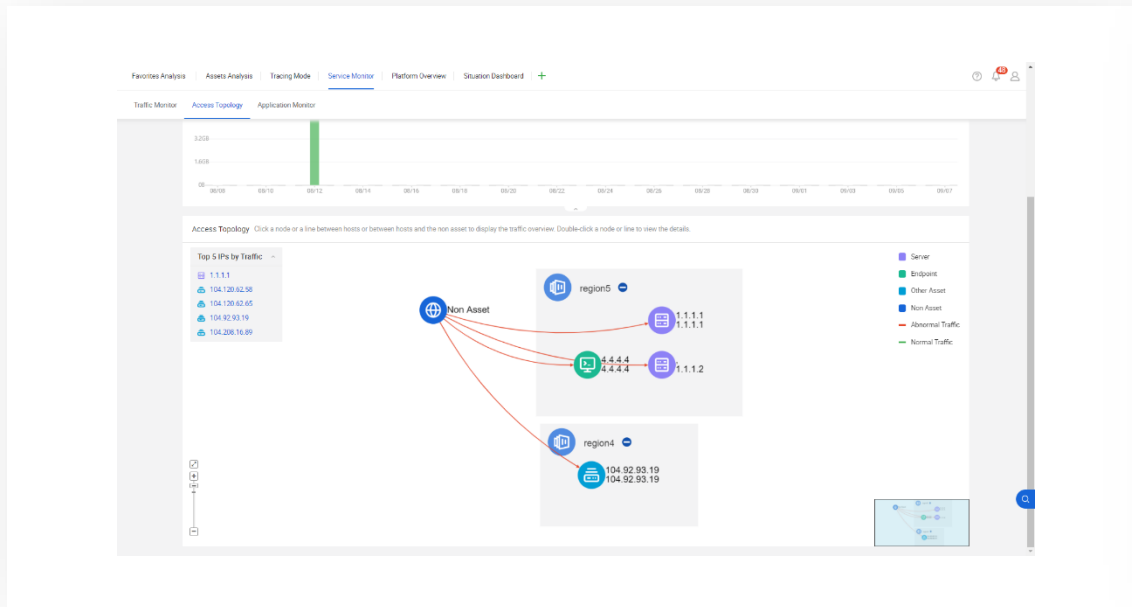
Collect traffic data from the netflow and metadata of BDS

Traffic monitoring enables security analyst to detect network anomalies

Traffic Insight

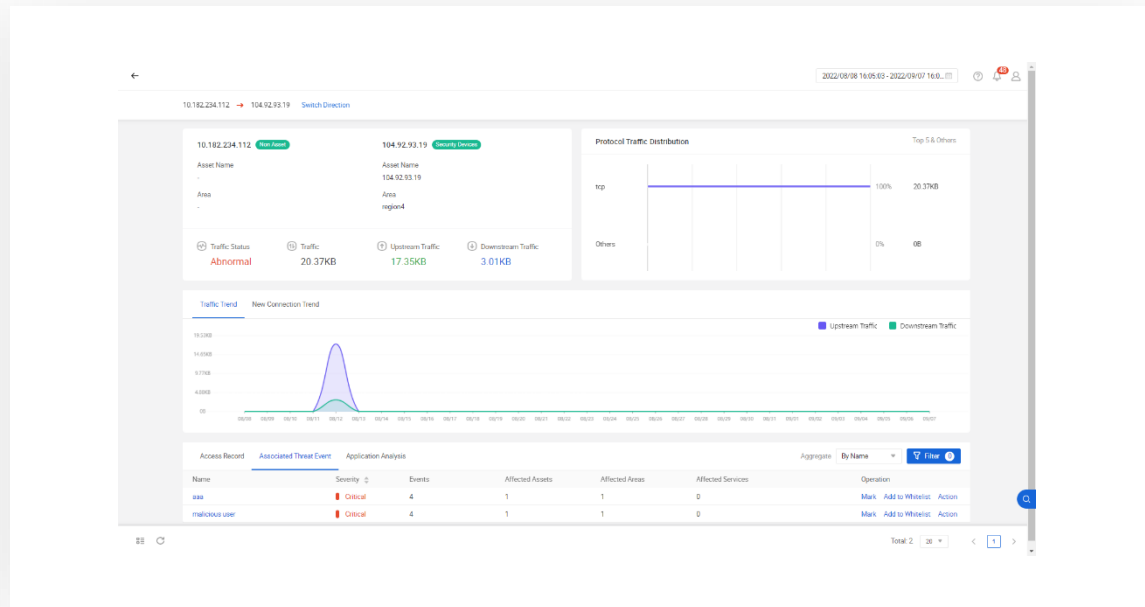
Traffic Insight Topology

- 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



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

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

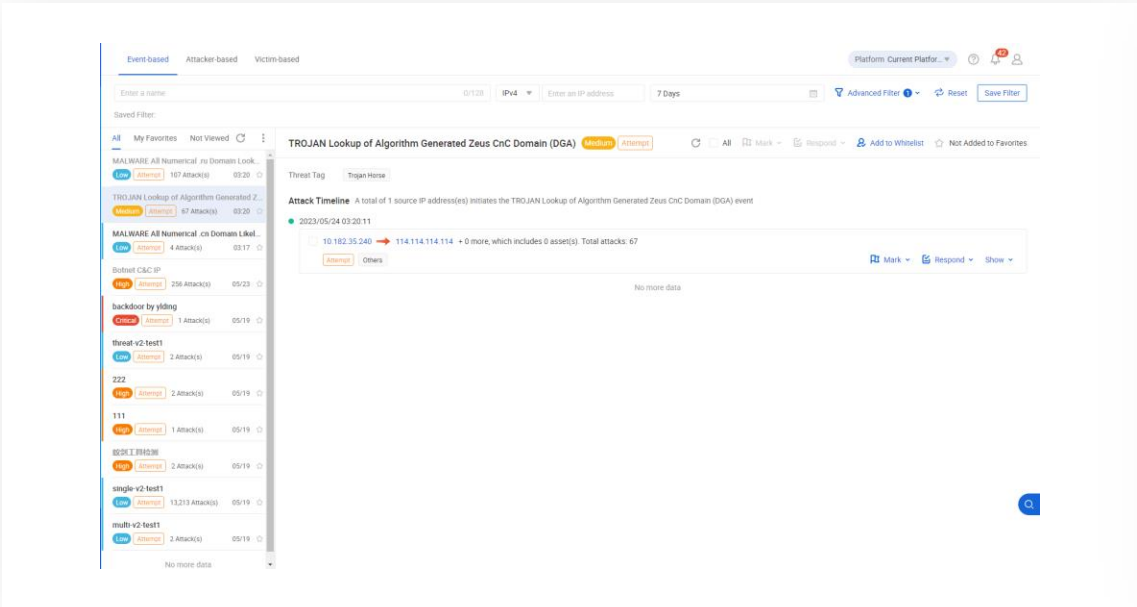
Advanced Mode

- Log-based correlation
- Event-based correlation

Threat Aggregation

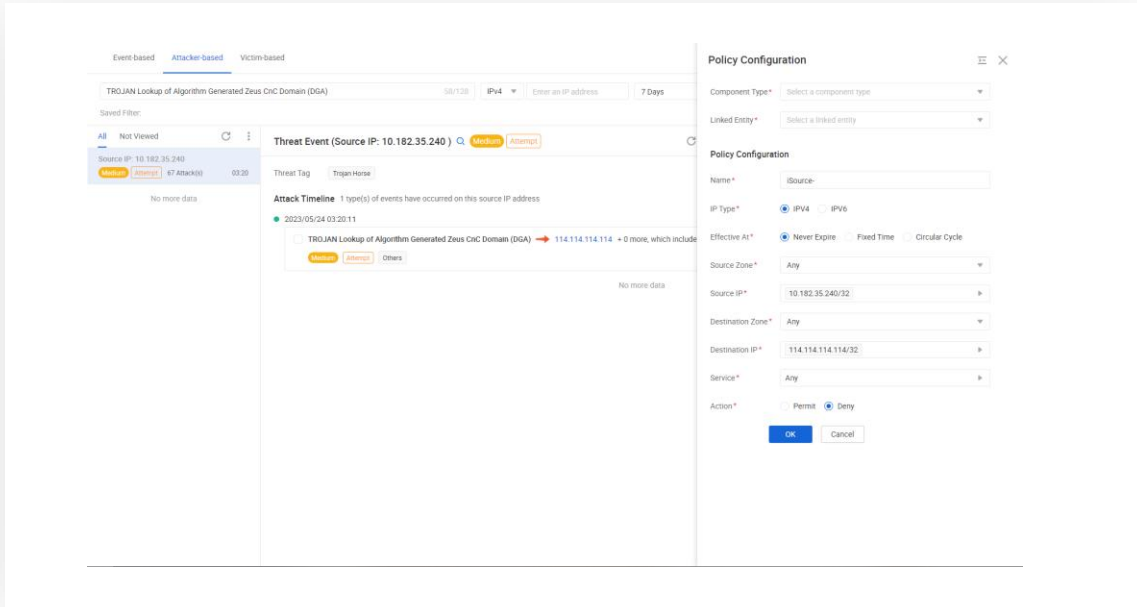
Threat Aggregation

- 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



Incident Investigation

The screenshot displays the Hillstone Networks incident investigation interface. At the top, a case titled "Case triggered by Oracle Web..." is shown with a confidence of 89 points and a status of "Unresolved". The interface is divided into several sections:

- Event timeline:** A list of events on the left side, including "none_web_attack_c...", "Suspicious java obje...", "CVE-2022-26134: A...", "XSS injection attack...", "CVE-2021-31805: A...", "XXE injection attack...", "A potential XML exte...", and "Basic SQL injection a...". Each event includes a timestamp, source and destination IP addresses, and severity levels like "serious" and "attempt".
- Network topology:** A central diagram showing a network of nodes and connections, with a "Group similar nodes" toggle.
- Actions menu:** A dropdown menu on the right side listing various actions such as "Configuring policies", "IP Blocking", "Access Control", "Ending a process", "Quarantine files", "Restart the terminal", "Block untrusted USB", "USB Whitelist", "Add script", "Isolate Host", "Virus detection", "File Blacklist", "Countdown to shutdown", and "Clear files".
- Details panel:** A panel at the bottom showing details for a specific rule, "none_web_attack_capture", with fields for "Rule Name", "Attack Phase", and "Direction/Threat T...".

Incident Investigation

Incidents Auto-Creation & Overview

- **Incident auto-creation:** Correlates alerts from multiple products into a single incident using predefined or custom rules
- **Incident merging:** continuously identifies and merges related incidents and alerts into a comprehensive incident
- **Attack story:** provides a detailed narrative of the attack's origin, progression, and scope

Incident Management

- **Incident resolution:** implements mitigation actions on entities (assets, IPs, domains, files, processes); logs activities, insights, and conclusions
- **Incident export:** enables exporting of incident lists for offline analysis at any time

Asset Centric Risk Management

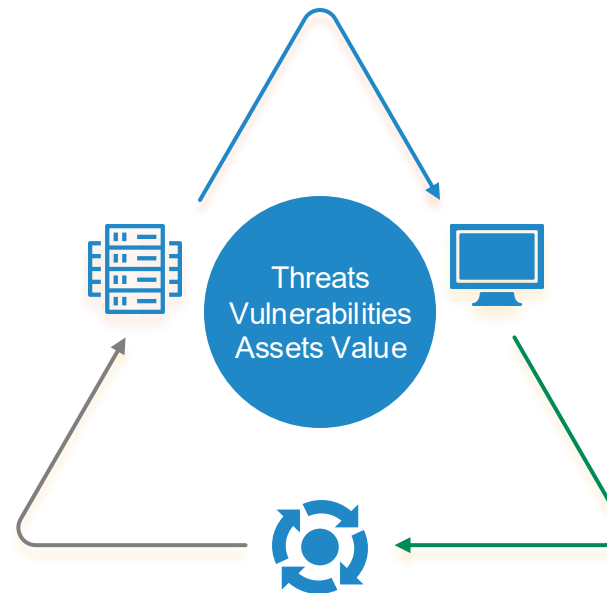
Server Risks

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

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 Suspected Compromised	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 Suspected Compromised	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 Suspected Compromised	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 Suspected Compromised	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 Suspected Compromised	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 Suspected Compromised	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 Suspected Compromised	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 style="text-align: center; margin: 5px 0;">New Add a scanner</p>	<p>777</p> <p>IP Address: 1.2.3.5</p> <p>Type: Nessus</p> <p style="text-align: right;">[Edit] [Refresh] [Delete]</p>	<p>RAS</p> <p>IP Address: 1.2.3.4</p> <p>Type: Nessus</p> <p style="text-align: right;">[Edit] [Refresh] [Delete]</p>	<p>platform scanner</p> <p>IP Address: -</p> <p>Type: built-in</p> <p style="text-align: right;">[Edit] [Refresh] [Delete]</p>
-------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------

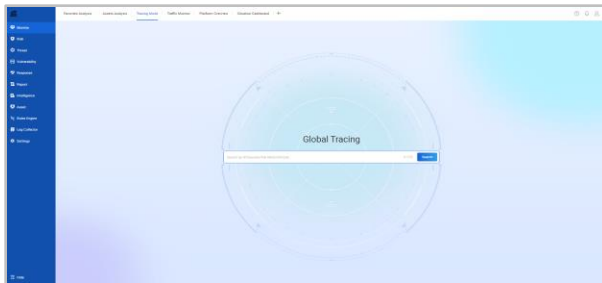
Threat Forensics



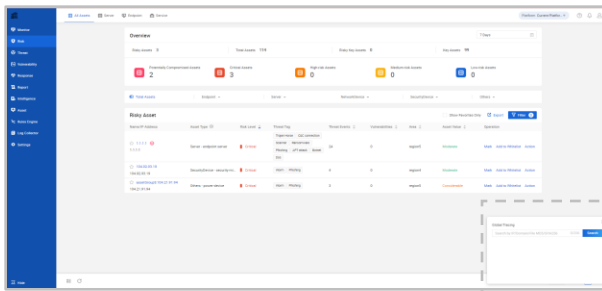
Global Search

Info Display

Incident Response

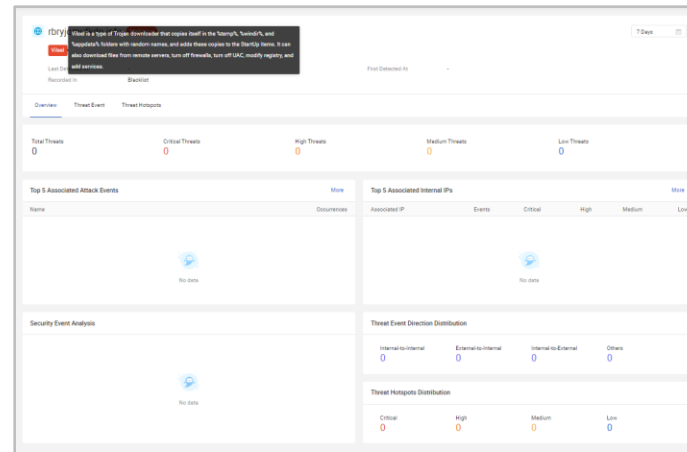


Primary entry



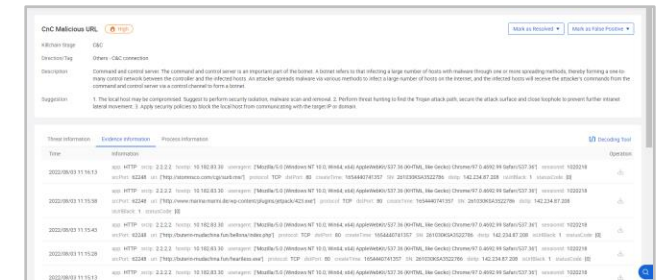
Quick entry

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

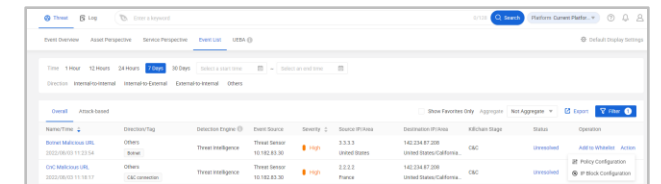


Info display

- 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.



Evidence Information



Incident Response

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

Automated Security Orchestration



Automated Orchestration

Playbook module

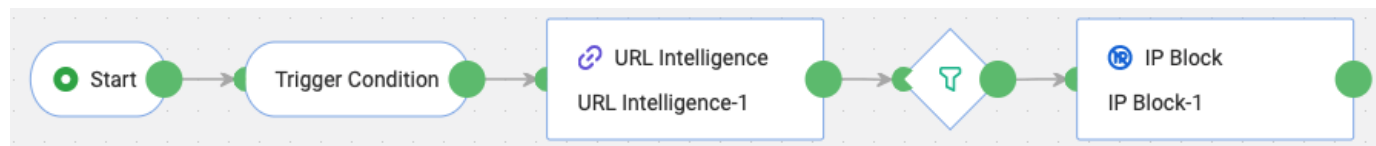
Threat Intelligence Action



Network Security Device Action



Platform Action



- 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

Incident Response – Integrated Devices



HSM



NGFW



ADC



NIPS



vWAF



CloudEdge



CloudHive



CloudArmour



3rd party devices



Integrated Devices

- Register integrated products
- Interact with intelligence center
- Perform actions as a response with integrated products by:
 - deploying policies
 - blocking addresses
 - process termination/host isolation/ file removal (CloudArmour)
- Action defined via template or via manual configurations
- Support 3rd party security devices over RESTful APIs or SSH to mitigate vendor lock-in inconveniences

Incident Response – Ticket Management



Ticket Management

- Ticket delegation and handling across roles
- Role-based ticket visibility
- Ticket status updates
- Ticket operation logs

Ticket Asset Segment All

hillstone My Ticket All

Overview

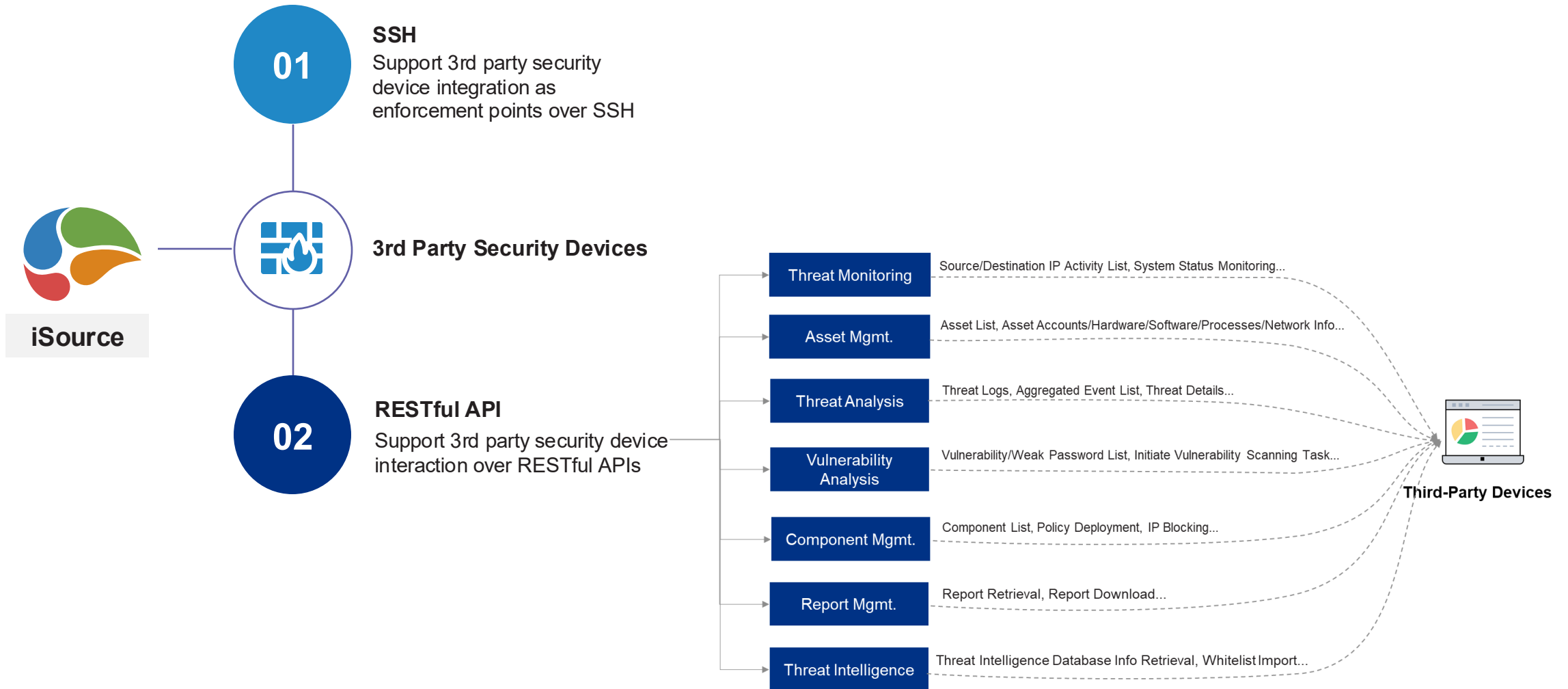
Total Tickets	Pending	Processing	Resolved	Rejected	Completion Rate 0%
4	2	0	0	0	
Closed	On-time	Timeout	On-time Completion Rate 0%		
0	0	0			

Ticket

Delete Export New Filter 0

Name	Asset Segment	Priority	Severity	Submitted At	Duration	Operation
<input type="checkbox"/> Ticket001	Default Asset Segm...	Medium	Medium	2024/10/25 17:05:47	31 Days	
<input type="checkbox"/> HQ_241022_001	Default Asset Segm...	Medium	Medium	2024/10/22 10:29:01	35 Days	
<input type="checkbox"/> Ticket003	Default Asset Segm...	High	High	2024/11/26 16:53:35	5 Minutes	
<input type="checkbox"/> Ticket002	Branch A	High	High	2024/11/26 16:52:44	5 Minutes	

Third-Party Device Integration



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 - endpoi...

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 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
- SYN Port Scanned
- HTTP Weak Password

Threat Posture Configuration

- Scan
 - SYN Port Scanned
 - UDP Port Scanned
 - IP Address Scan Attack
 - Host Port Scan Attack
 - SYN Port Scan Attack
- File
- HTTP Detection
- Suspicious Activity
- State Force
- Domains
- Personware (Threat Engine)
- Mining
- USB Access
- Bluetooth
- Threat Intelligence
- Weak Password Detection
- Threat Log
- General Log
- Abnormal Traffic
- Abnormal Logs
- Personware (Off-Chain Engine)
- Threat Posture

Favorite Posture

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

Agile Key Threat Management

Weak Password Breaches

Mining Attacks

Ransomware Attacks

Favorite Assets/Threats

Dedicated Dashboard

Threat event summary
Threat event details
Swift incident response

Ransomware 99+

Time: 1 Hour | 12 Hours | 24 Hours | 7 Days | **30 Days** | Select a start time | Select an end time

Ransomware Stage Distribution of Infected Assets

Major Ransomware Event Distribution

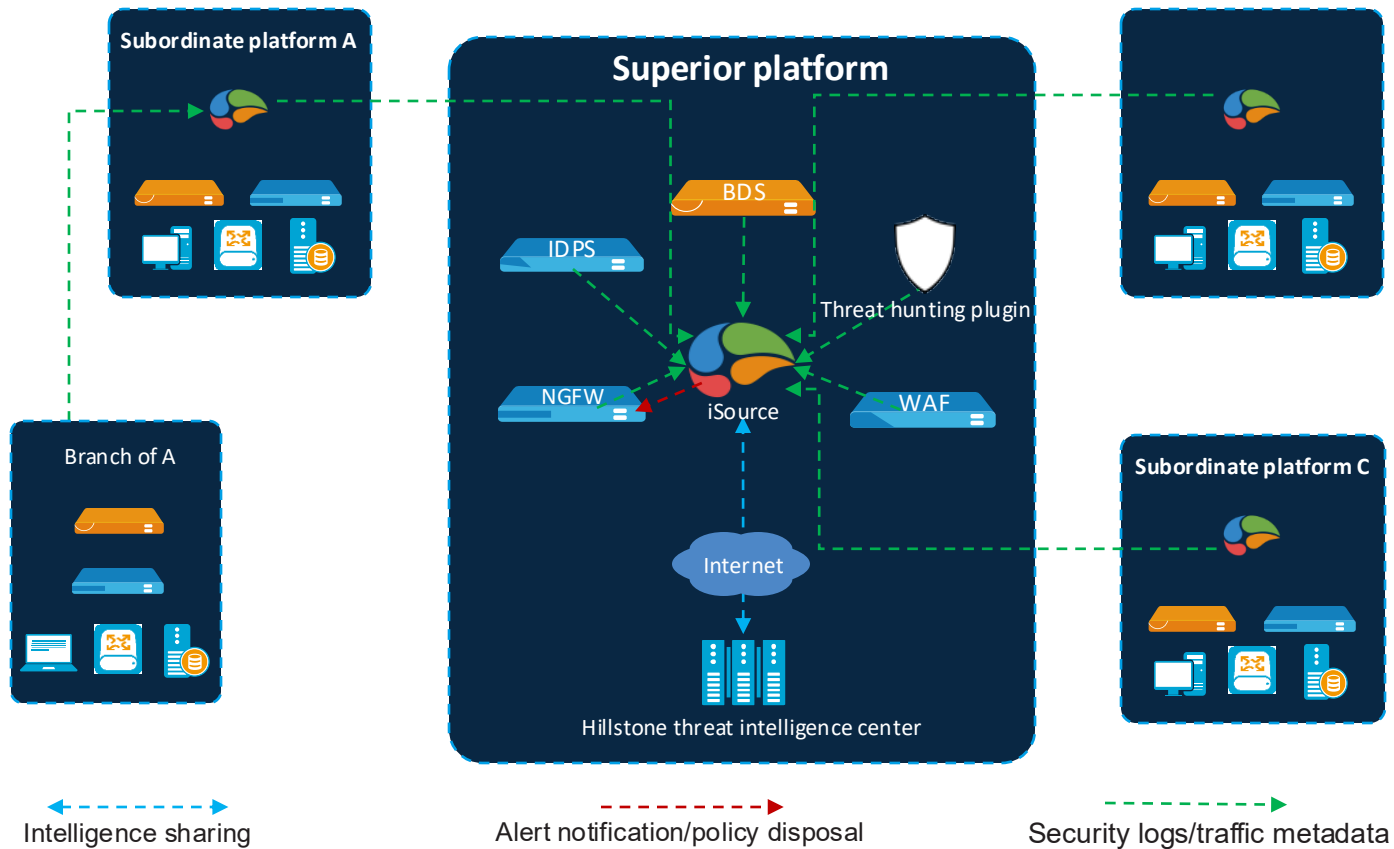
Top 5 Ransomware Targets

Victim Assets Show Favorites Only | Export | Batch Mark | Filter 0

Name/IP Address	Asset Type	Severity	Ransomware Stage	Malicious IP	Malicious Domain	Threat Events	Last Detect	Operation
ymeng_192.168.1.1 192.168.1.1	Server - proxy server	Critical	Accessing Malicious Websites			316	2023/09/01	Details Add to Whitelist Respond
192.168.5.5 192.168.5.5	Security Device - security-misc	Critical	Infected with Ransomware			440	2023/09/01	Details Add to Whitelist Respond
ymeng_192.168.4.4 192.168.4.4	Server - proxy server	Critical	Infected with Ransomware			669	2023/09/01	Details Add to Whitelist Respond
ymeng_192.168.3.3 192.168.3.3	Others - other	Critical	Infected with Ransomware			419	2023/09/01	Details Add to Whitelist Respond
ymeng_192.168.1.111 192.168.1.111	Endpoint - VoIP phone	Critical	Infected with Ransomware			417	2023/09/01	Details Add to Whitelist Respond
ymeng_192.168.1.11	Network Device - router	Critical	Infected with Ransomware			415	2023/08/11	Details Add to Whitelist Respond

Hierarchical Management

Hierarchical Management



Hierarchical Management Monitoring Dashboard



Aggregated Security Posture Across All Platforms

Presents assets, threat events and other security posture 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

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

Connection Protocols

- Built-in mainstream connection protocols:
 - TCP
 - UDP
 - Kafka
 - JDBC
 - Beats
- Support the integration of custom protocols via plugins

Parsing Templates

- Built-in parser for mainstream data formats:
 - AVRO
 - JSON
 - GROK
 - JsonPath
 - Key-Value
- Support the integration of custom data formats via plugins
- Custom parsing templates
- Support online/offline upgrade

Log Storage

- Storage availability with retention period of up to 1800 days
- Log backup configuration
- Log restoration
- Log history query

Log Server

- External Log servers that iSource will send the followings to:
 - Collected logs
 - Detected threat events
- Protocols support:
 - HTTPS API
 - FTP

Report Management

Report Overview

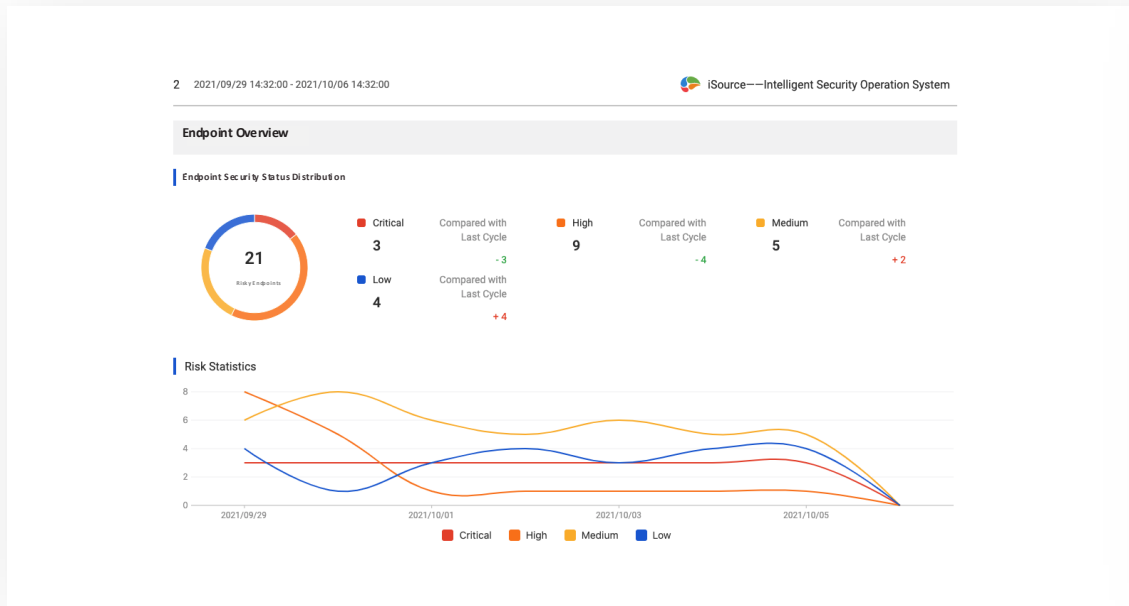
- List all reports
- Support live view
- Support export report in PDF
- Support manual export for customizable queries

Report Task

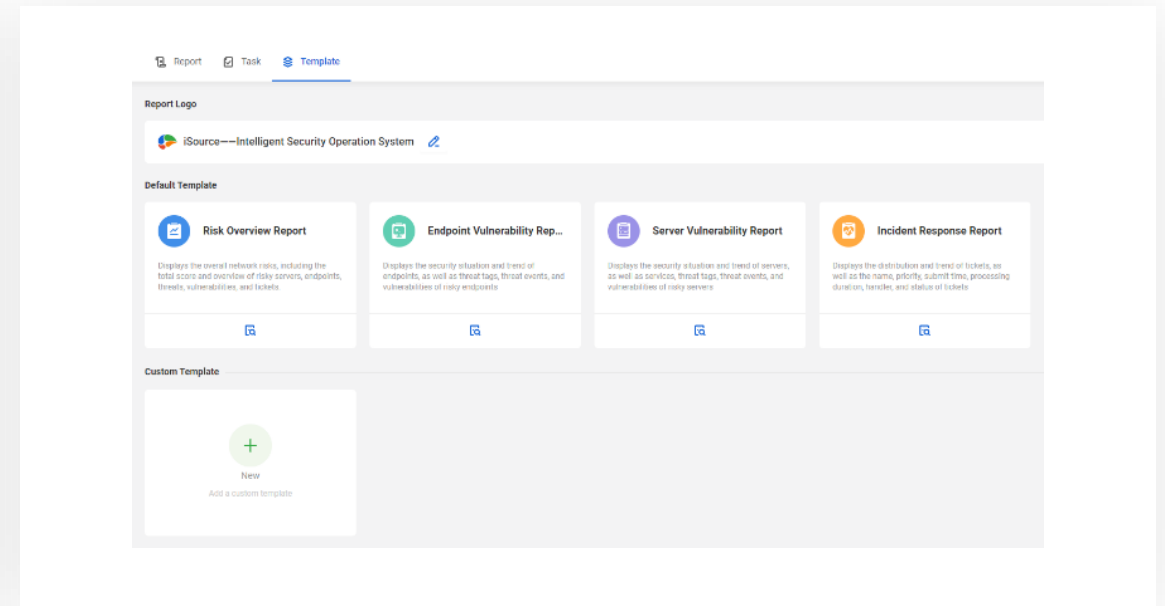
- Generate reports periodically (daily/weekly/monthly)
- Overview or detailed reports

Report Template

- Multiple pre-defined templates
- Customizable templates

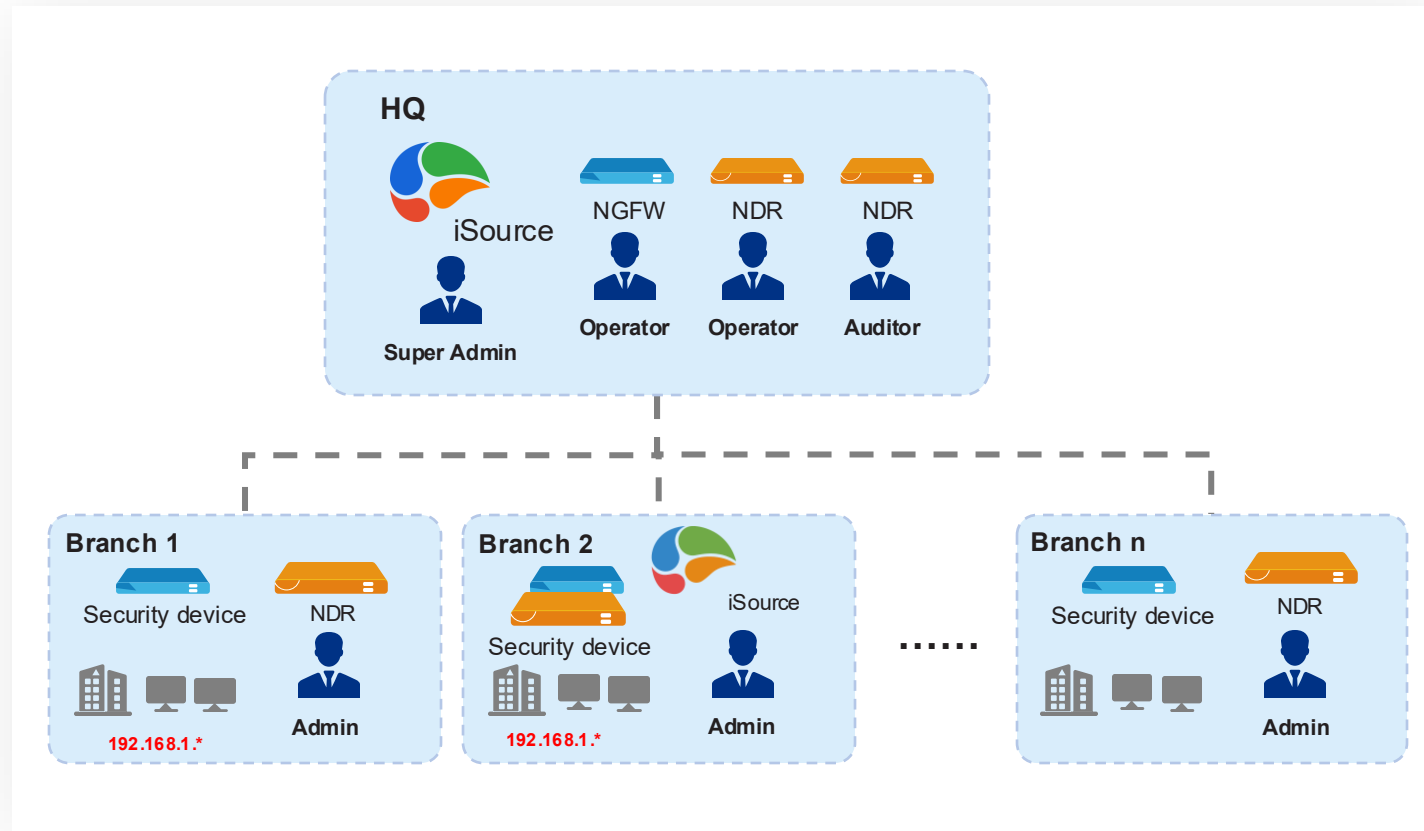


A page of summary report



Rich report templates

Role-Based Privilege Management



Role-Based Privilege Management

Roles

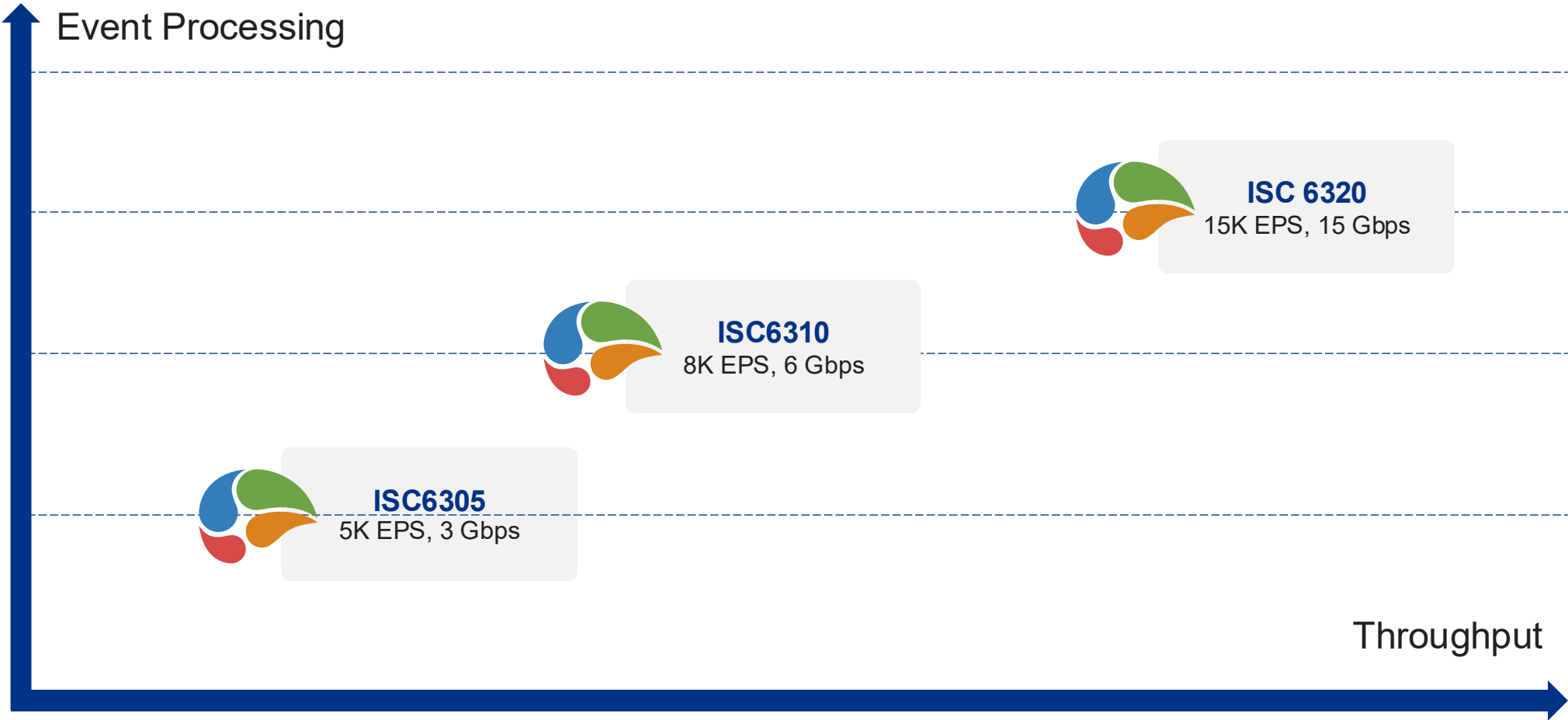
- **Super Admin:** Full access to all data and features
- **Admin:** Full access to data and features within a specific branch
- **Operator:** Access to all data and features except permission settings and system logs
- **Auditor:** Access to data and system logs
- **Operator (Read-Only):** View-only access to data and features

Privileges

- Assign roles with feature-specific access
- Assign roles with data-specific access

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-ISC6305	SG-6000-ISC6310	SG-6000-ISC6320
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
	HDD		1TB	

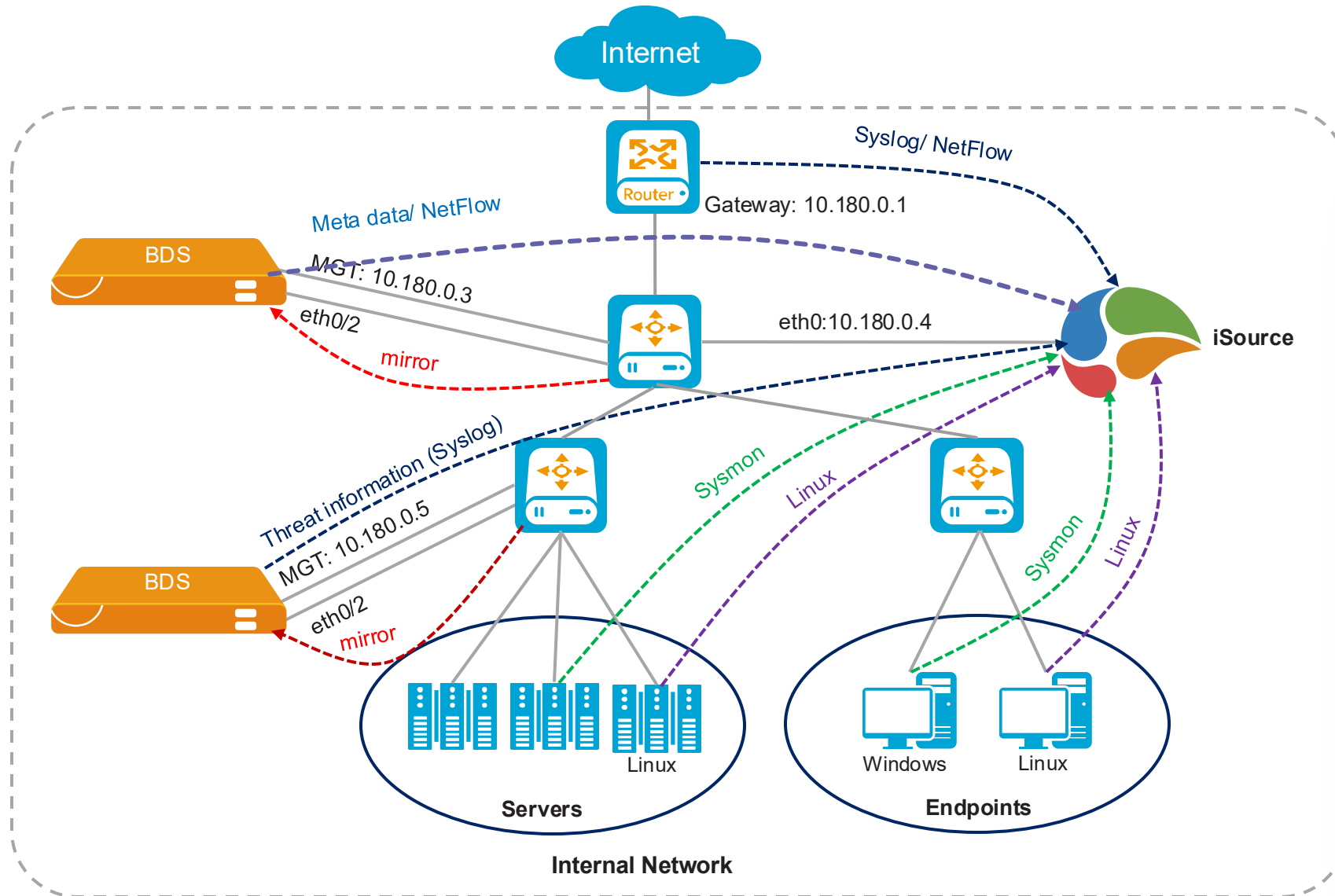
iSource Ordering Guide



Category	SKU	Definition	Term
Base System	<ul style="list-style-type: none"> SG-6000-ISC6305-SW-IN-yy SG-6000-ISC6310-SW-IN-yy SG-6000-ISC6320-SW-IN-yy 	iSource ISC6305/ISC6310/ISC6320 base system with with software upgrade and remote support	1-5 yrs. (yy:12/24/36/48/60)
Base QSystem Renewal Service	<ul style="list-style-type: none"> SGSV-ISC6305-SW-IN-zz-U SGSV-ISC6310-SW-IN-zz-U SGSV-ISC6320-SW-IN-zz-U 	Renewal service for iSource ISC6305/ISC6310/ISC6320 base system, including software upgrade and remote support	1-3 yrs. (zz:12/24/36)

Deployment Scenarios & Use Cases

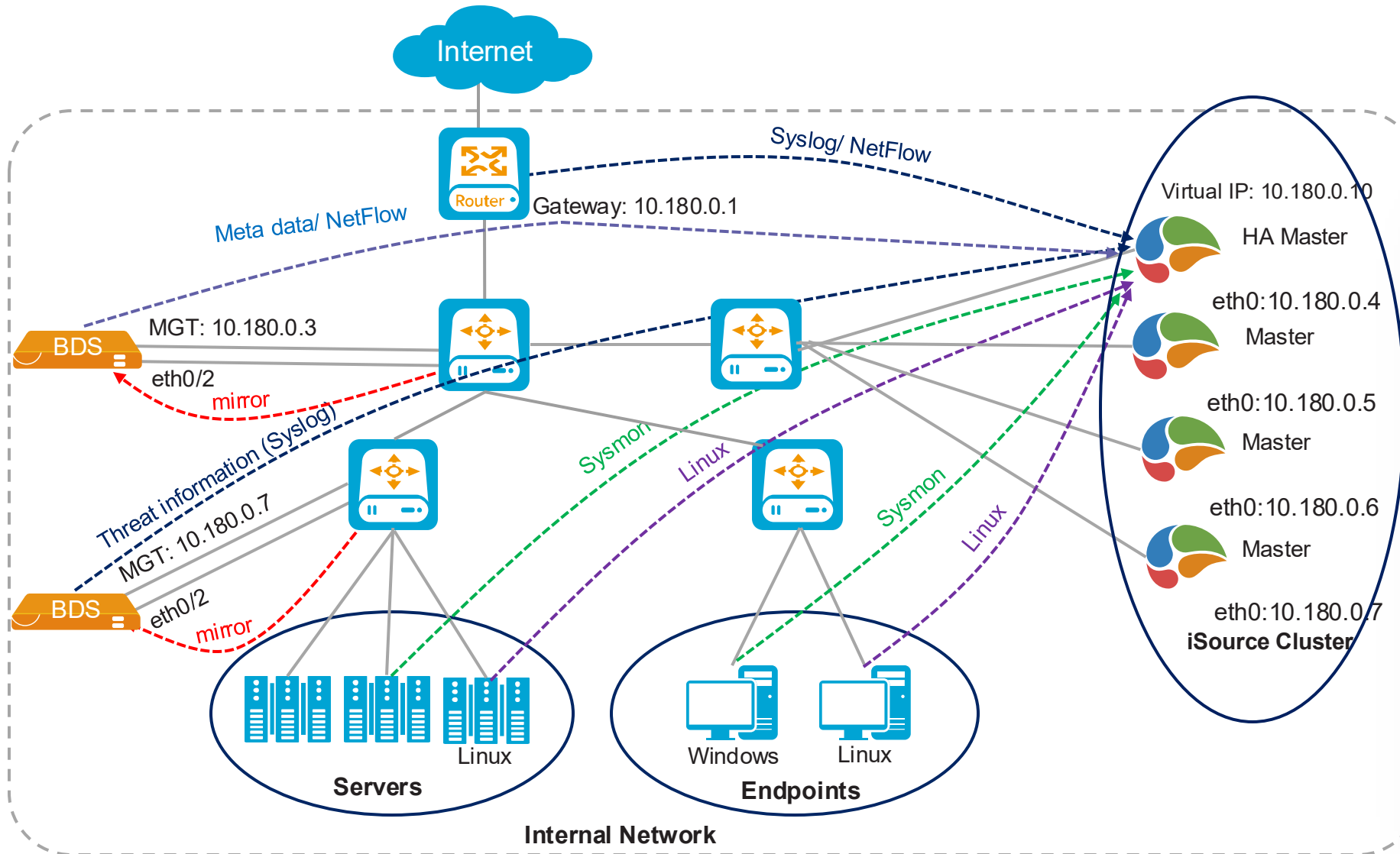
iSource Deployment Scenario- Single Node



Single Node Deployment

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

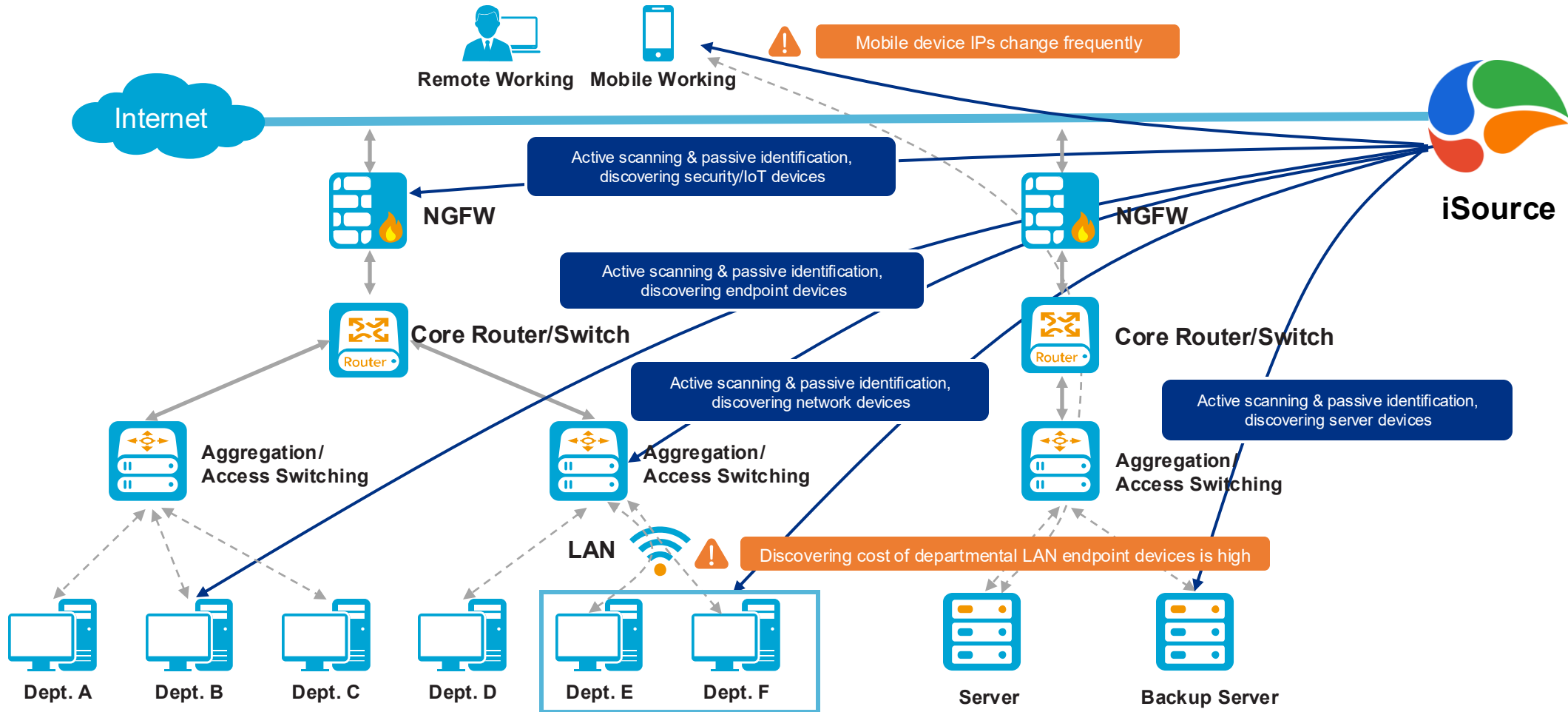
iSource Deployment Scenario- Cluster



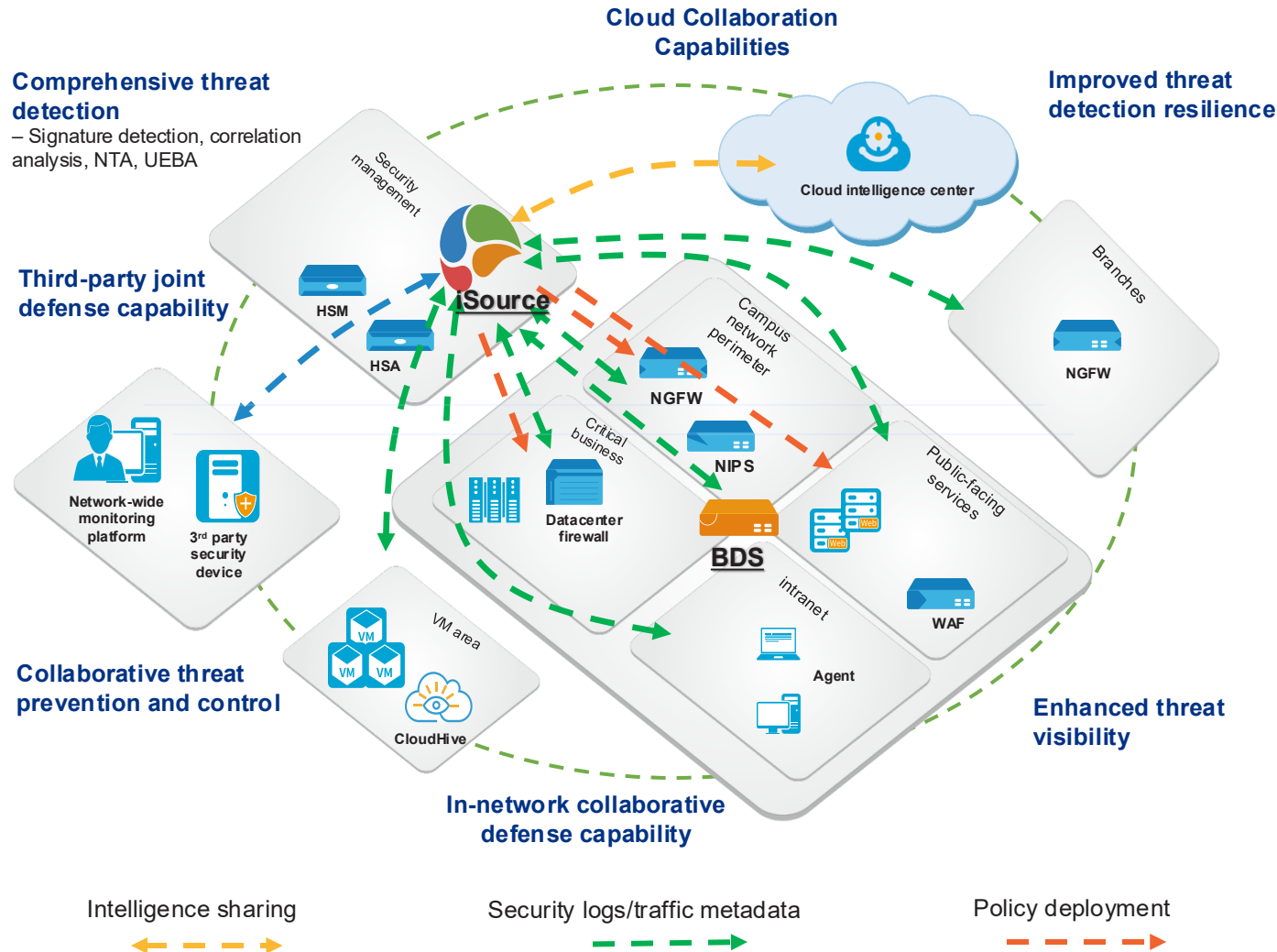
Cluster Deployment

- 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 - Unified Asset Management



Use Case - Security Operations



01 Unified data collection with full threat visibility

02 Advanced AI/ML-driven security detection and analytics

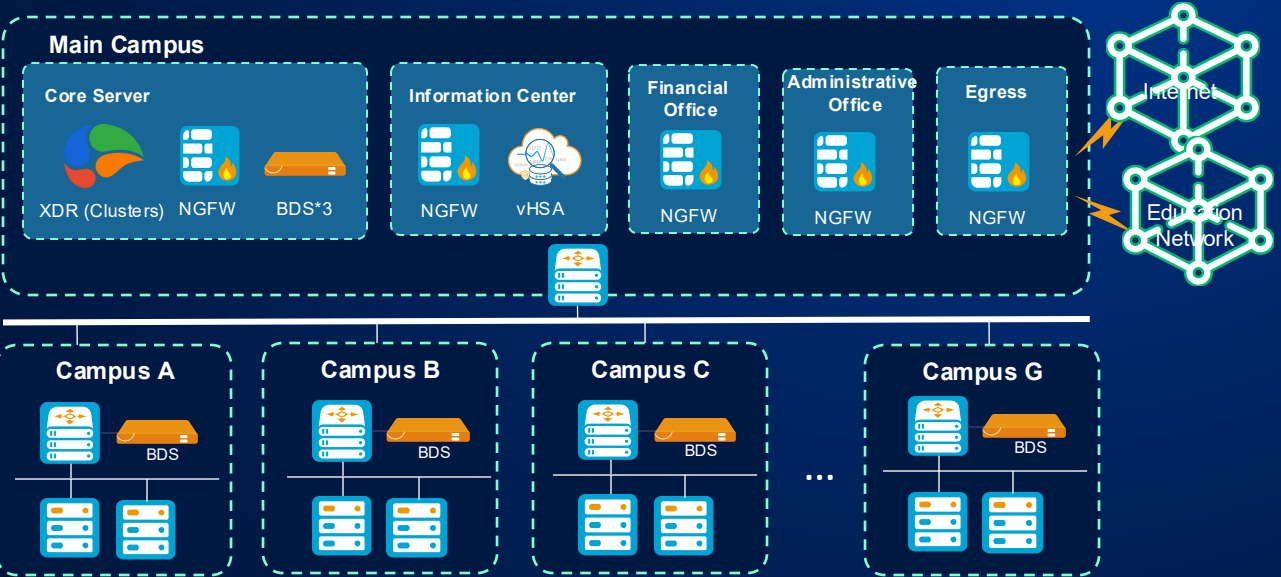
03 Automated security orchestration and cohesive response

Case Studies

Streamline Security Operations for A Prestigious University



- Overview:** Established in 1946, the university is a prominent comprehensive institution directly managed under the Ministry of Education in China.
- Size:** The university has eight campuses, with a student body of over 70,000 and more than 6,000 faculty members.
- Products Used:** Hillstone iSource XDR, vHSA, BDS, NGFW



Customer Pain Points

- Frequent undetected cryptomining and malicious outbound connections due to lack of unified threat visibility
- Difficulty in aligning diverse security policies across departments without centralized management
- Overburdened security operations leading to inefficiencies and missed threats



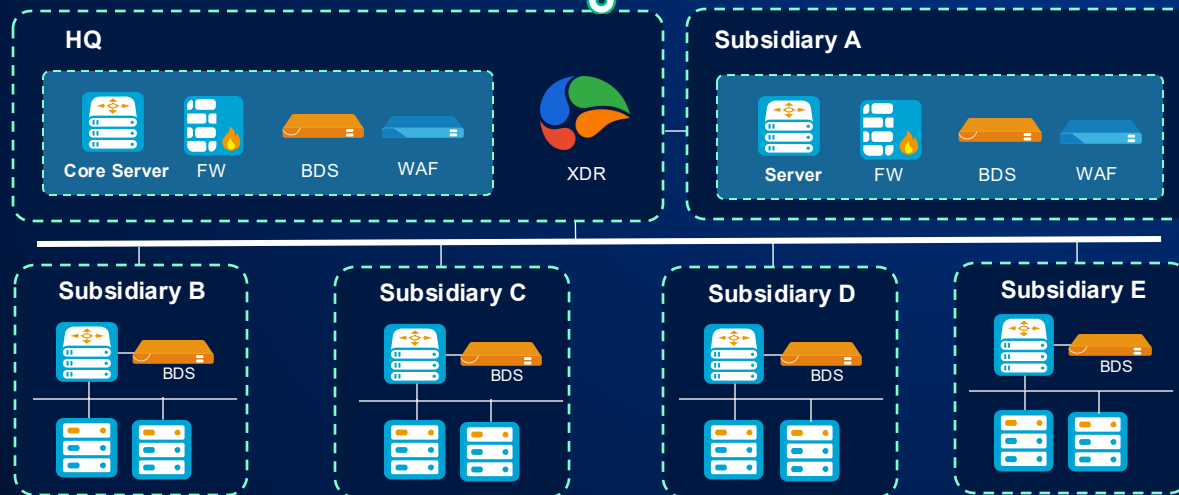
Hillstone Solutions

- Hillstone iSource XDR delivers centralized threat visibility across endpoints, networks, and cloud environments, detecting cryptomining, malicious outbound connections, and other hidden threats.
- It ensures consistent security across departments, preventing silos.
- It automates routine tasks and prioritizes threats based on risk, helping security teams focus on the most critical issues.

Streamline Security Operations for A Large Automotive Manufacturer



- **Overview:** Founded in 1947, the **car manufacturer** is a large Chinese enterprise engaged in automotive R&D, manufacturing, and sales, ranked among the **top 100 most valuable automotive brands globally**.
- **Size:** The company comprises **37 primary subsidiaries**, 50+ dealers, 390+ overseas sales points, and 270+ overseas service stations.
- **Products Used:** Hillstone iSource XDR, BDS, WAF



Customer Pain Points

- The company and its subsidiaries use **separate security devices**, lacking unified threat management and visibility
- Difficulty in **pinpointing critical issues** leads to missed detections and delayed responses
- **Overburdened security operations** leading to inefficiencies and increased risks



Hillstone Solutions

- Hillstone iSource XDR **consolidates data from all security devices** into a single system, enhancing visibility and threat management
- It employs **advanced analytics** to quickly identify and **prioritize critical issues**, enabling faster response and mitigation
- It offers **automated workflows and response playbooks** to accelerate incident handling and reduce response times



Département Commercial
WCA

 **HAFS**
Distributeur à valeur ajoutée **WCA**

Vous accompagne



www.hafs-networks.com
Visitez notre site web



sales-ci@hafs-networks.com
Envoyez-nous un e-mail



(+225) 07 69 32 13 55
Contact commercial 1



(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

