
HAFS
Distributeur à valeur ajoutée
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 intellligentes
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	Cloud Adoption	Extended Endpoints
• Exponential Increase of Traffic • New business apps/upgrades • Access from anywhere	• Private/Hybrid deployment • SaaS apps • Serverless computing • Containers	• 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

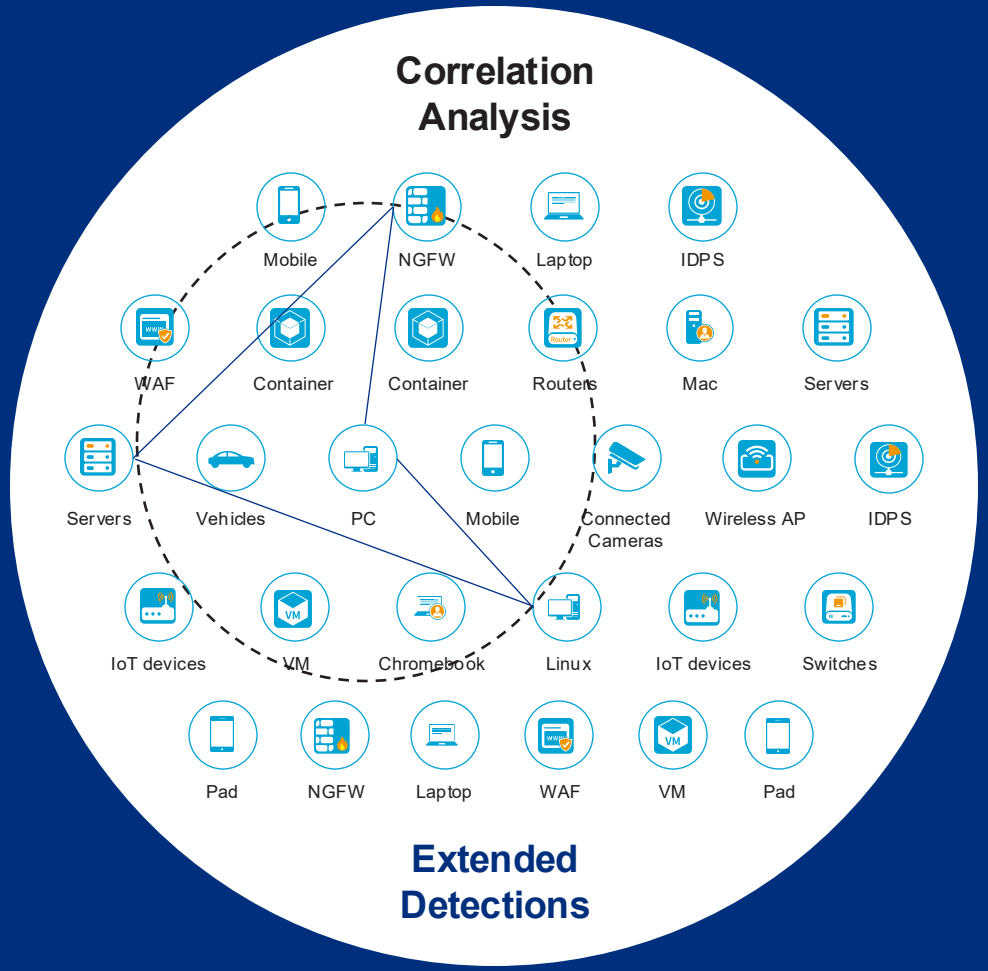
What Do Customers Need?

Comprehensive Data Collection

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

Full visibility

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



Threat Hunting and Analysis

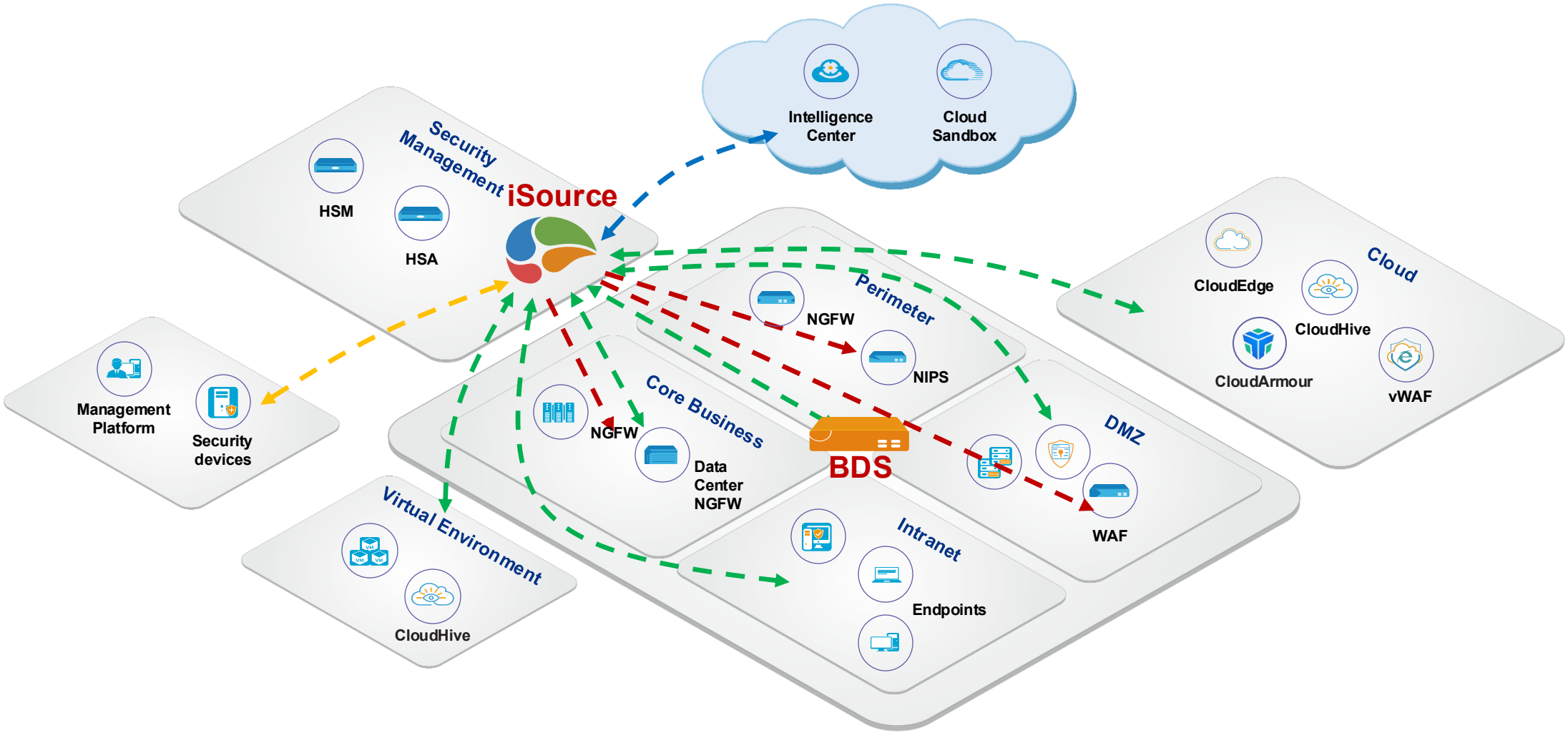
- Threat detection
- Behavior analysis
- Correlation analysis
- Root cause and attack source analysis
- …

Automated Response

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

Introduction of Hillstone iSource

Hillstone XDR Solution Overview



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

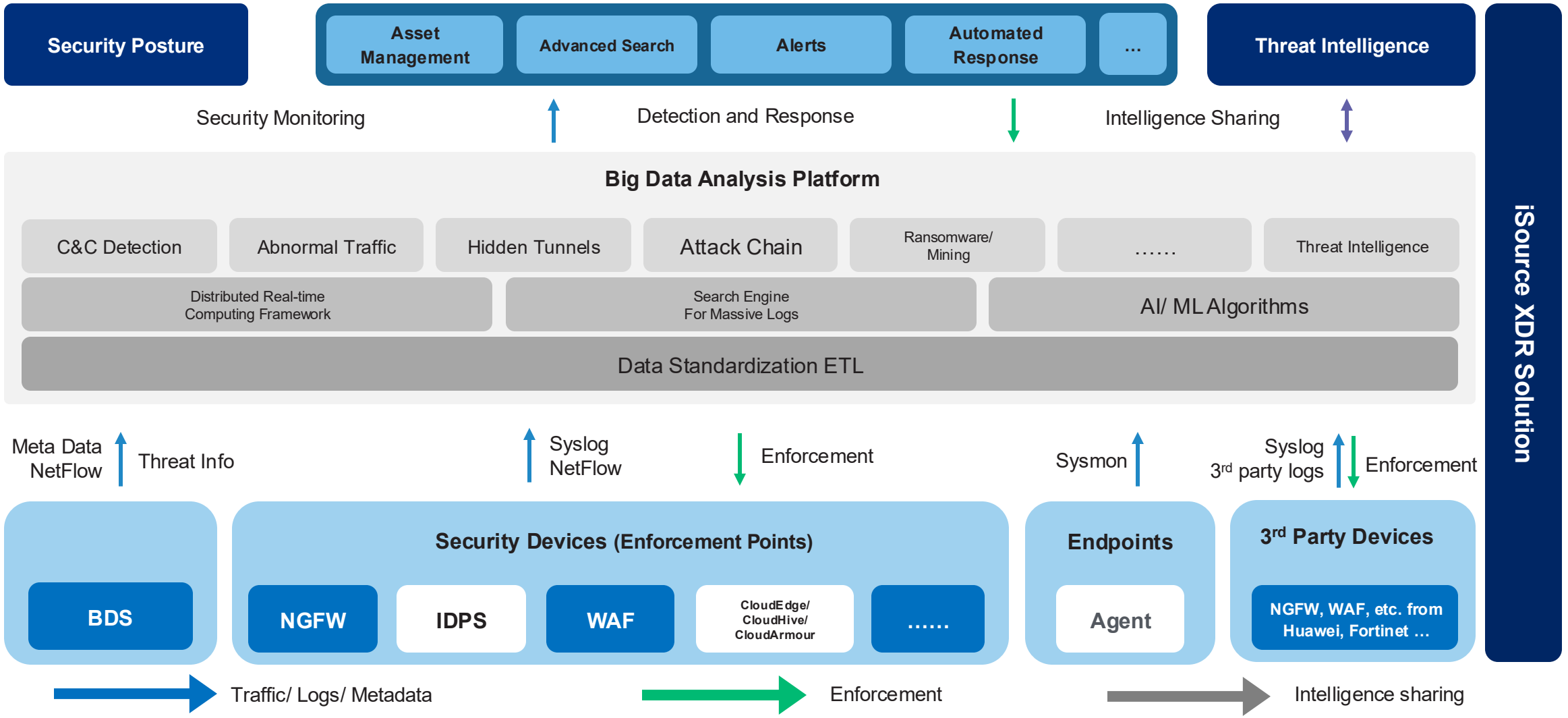
05 Automated Orchestration and Response

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

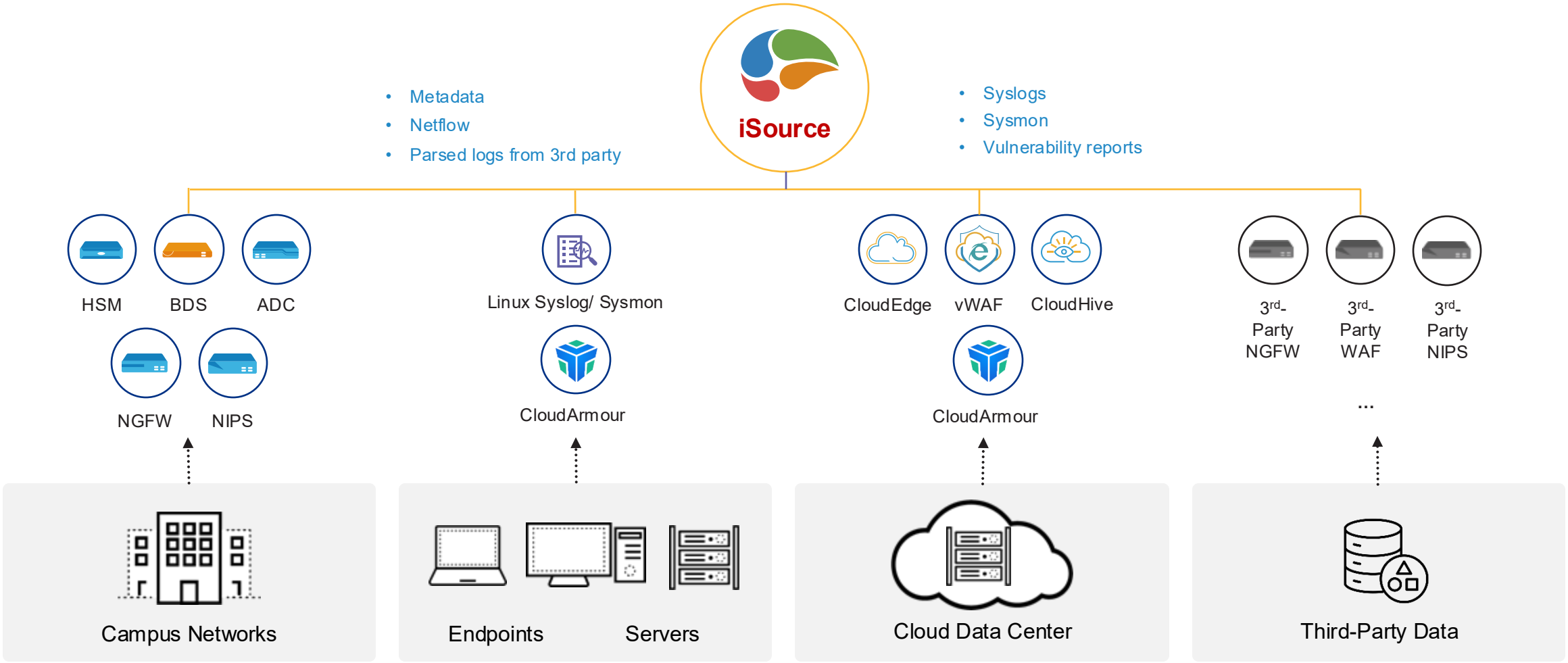
06 Open Platform with High scalability

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

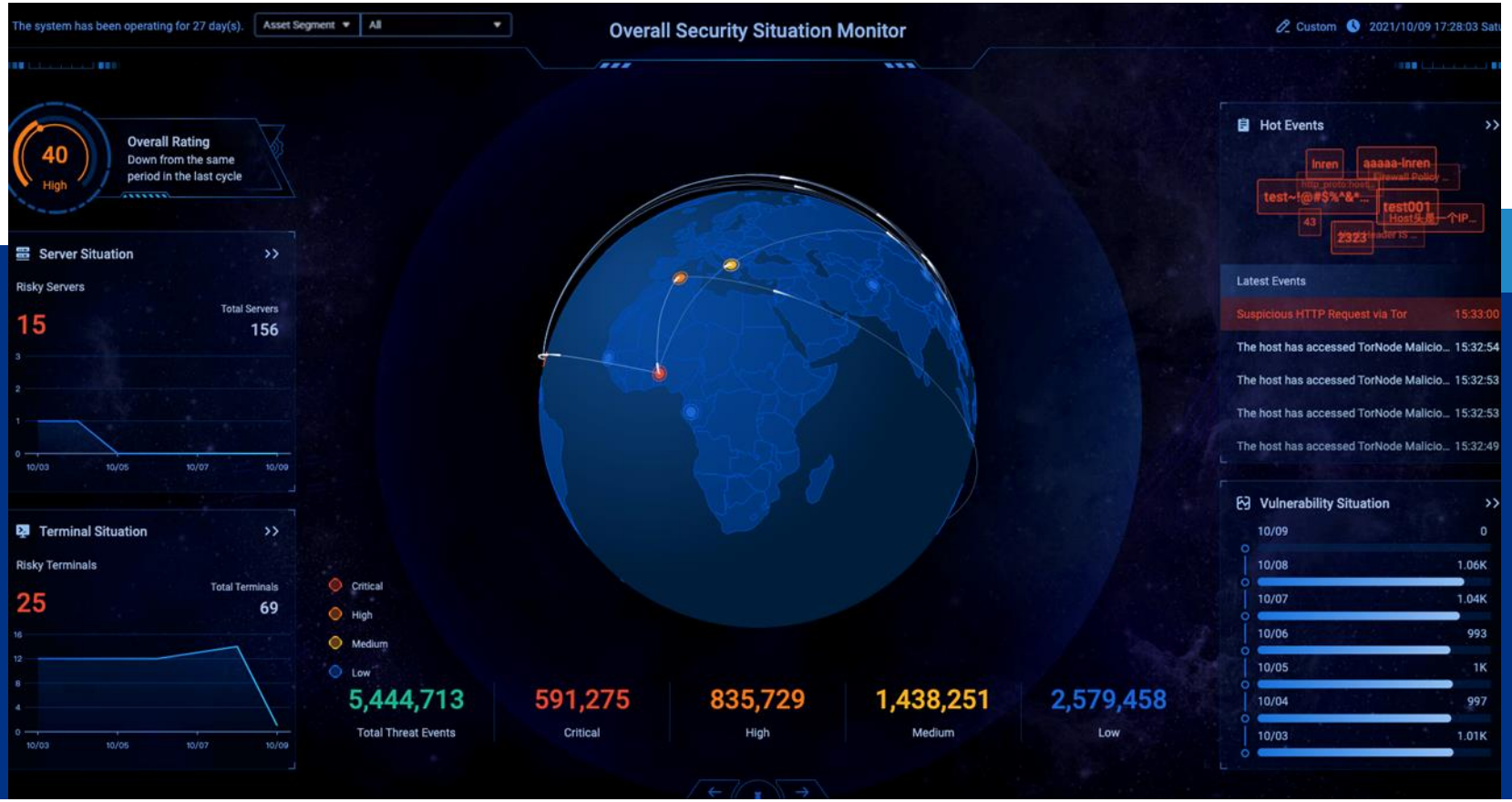
iSource: XDR Solution Architecture



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

Full-screen Monitoring Dashboards

Hillstone NETWORKS

Server Monitoring

Full-screen Monitoring Dashboards

Endpoints Monitoring

Full-screen Monitoring Dashboards

Threat Events Monitoring

Full-screen Monitoring Dashboards

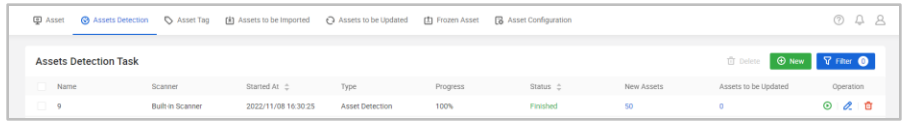
Vulnerability Monitoring

Full-screen Monitoring Dashboards

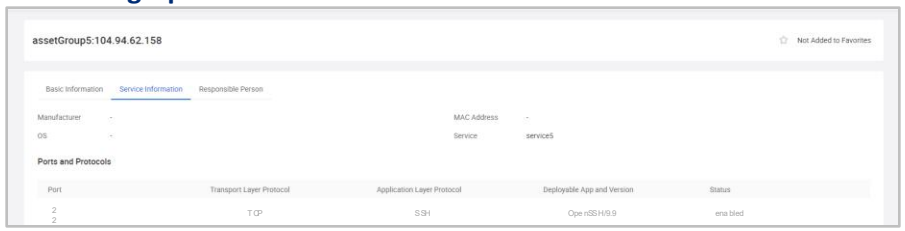
Area Monitoring

Asset Discovery and Management

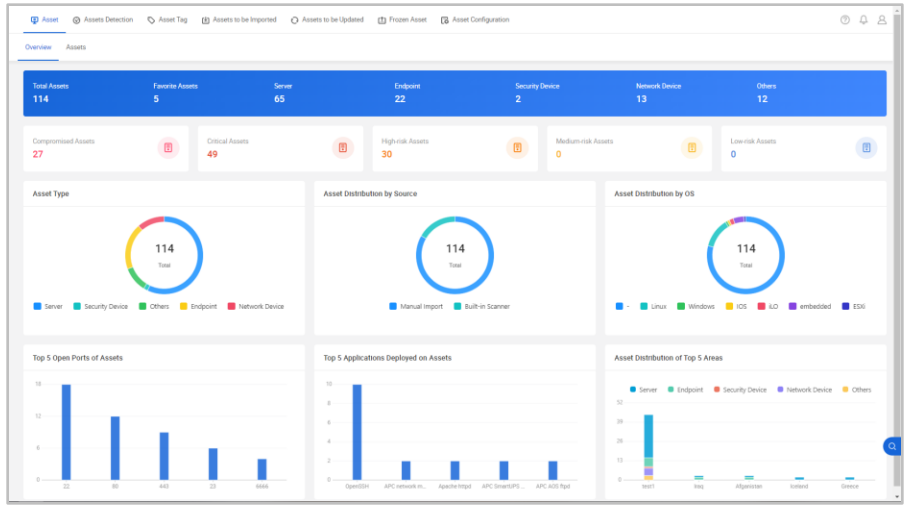
Asset Detection

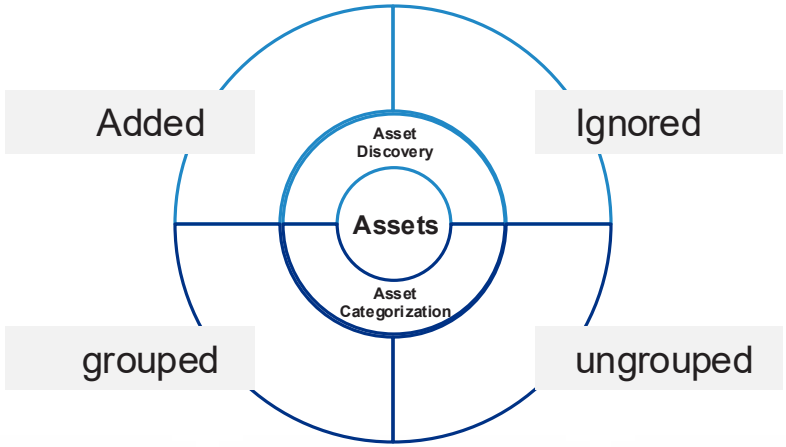


Device Fingerprint



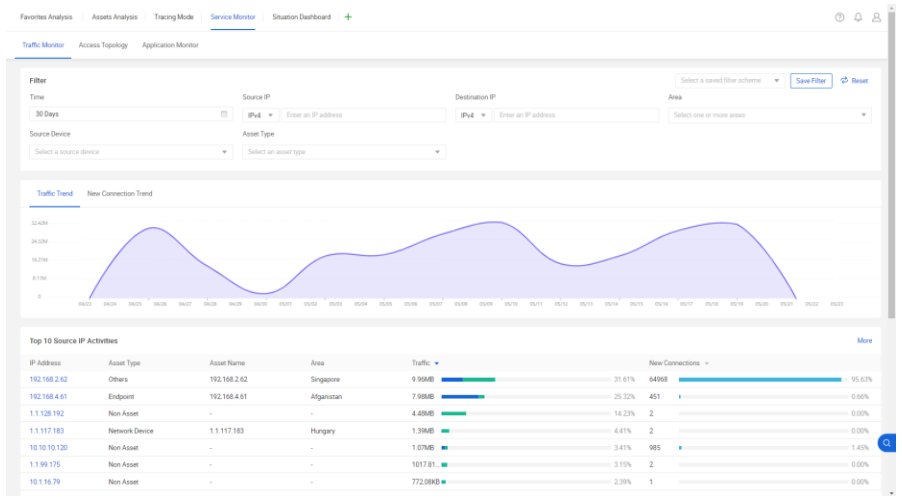
Asset Overview





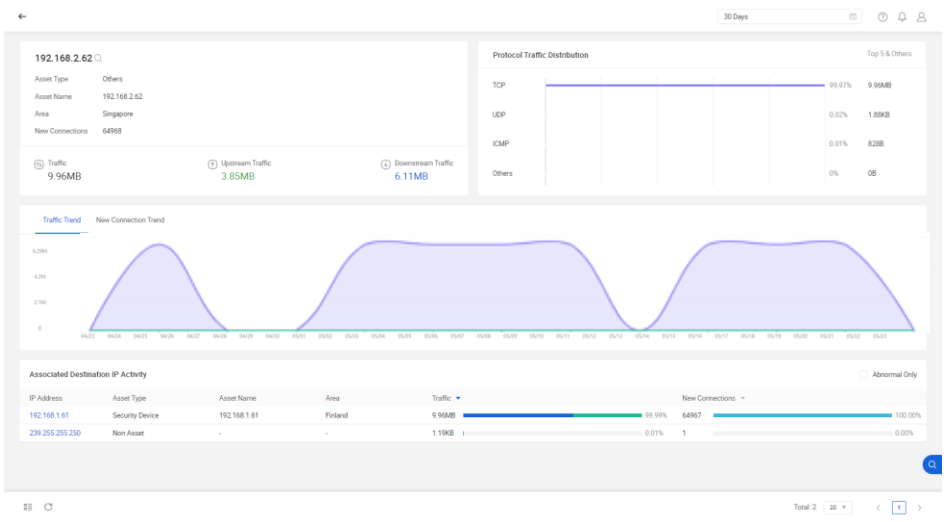
Asset Discovery	Grouping	Lifecycle Management
Discover assets via: • Traffic • Logs • Threat events • Vulnerability report • Manual import • Active scan	**Grouping as:** • Servers • Endpoints • Network devices • Security devices • IoT devices • Others	• Asset export • Template based import • Asset offboarding

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

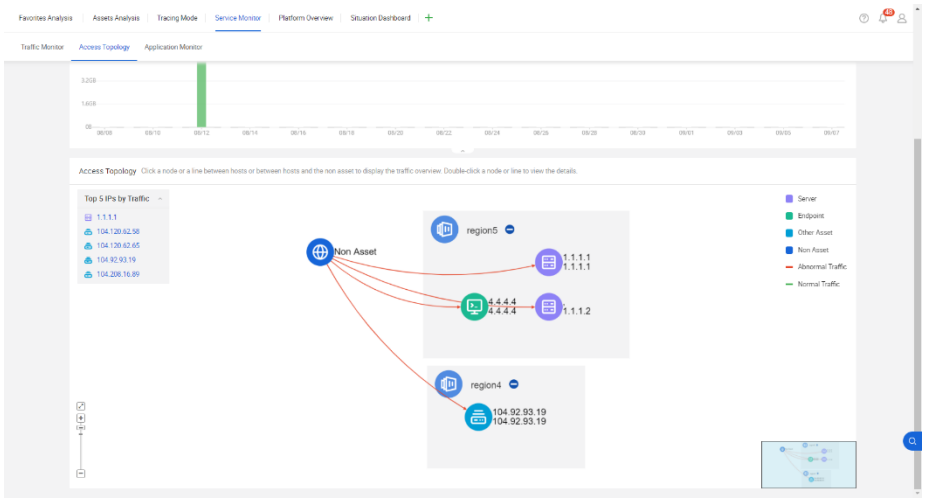
Collect traffic data from the netflow and metadata of BDS

Traffic monitoring enables security analyst to detect network anomalies

Traffic Insight

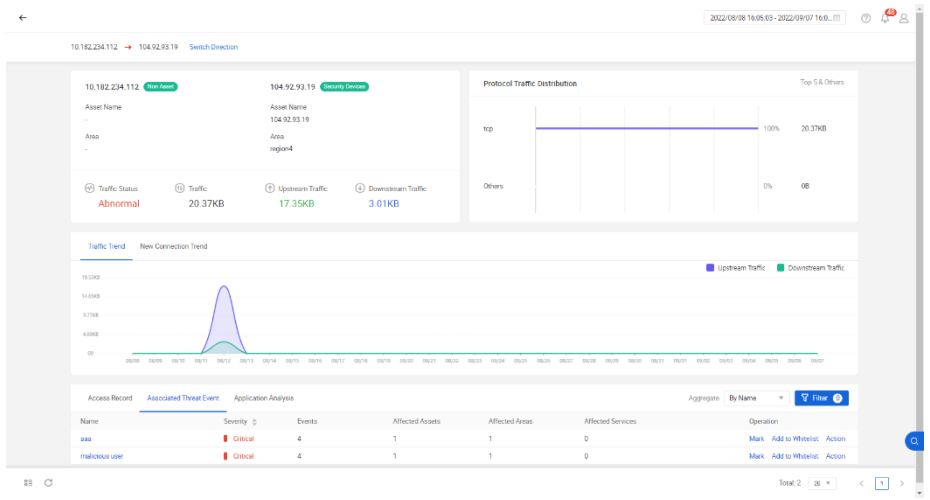
Traffic Insight Topology

- 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



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

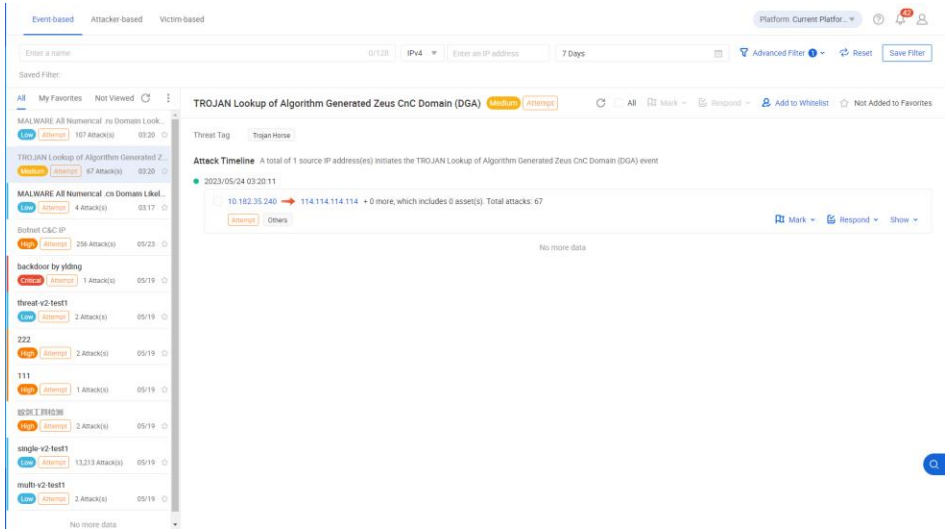
Advanced Mode

- Log-based correlation
- Event-based correlation

Threat Aggregation

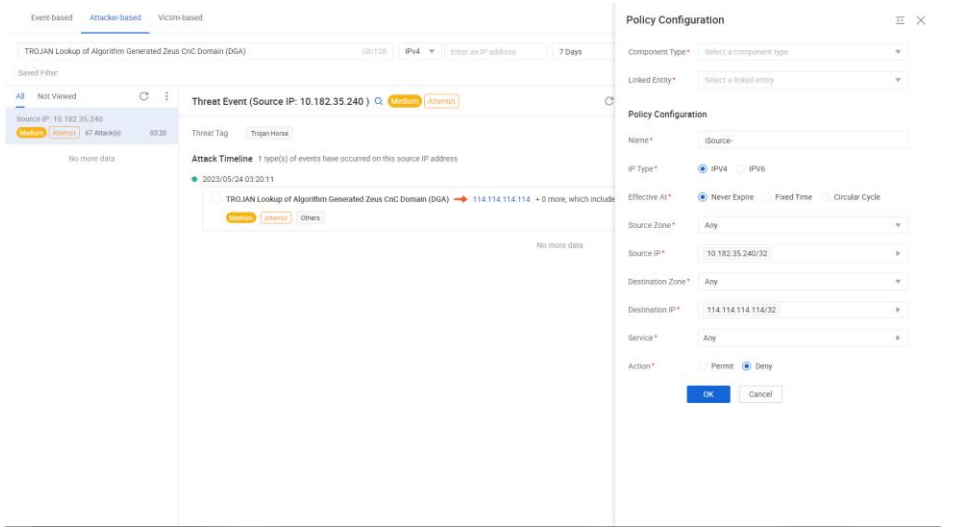
Threat Aggregation

- 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

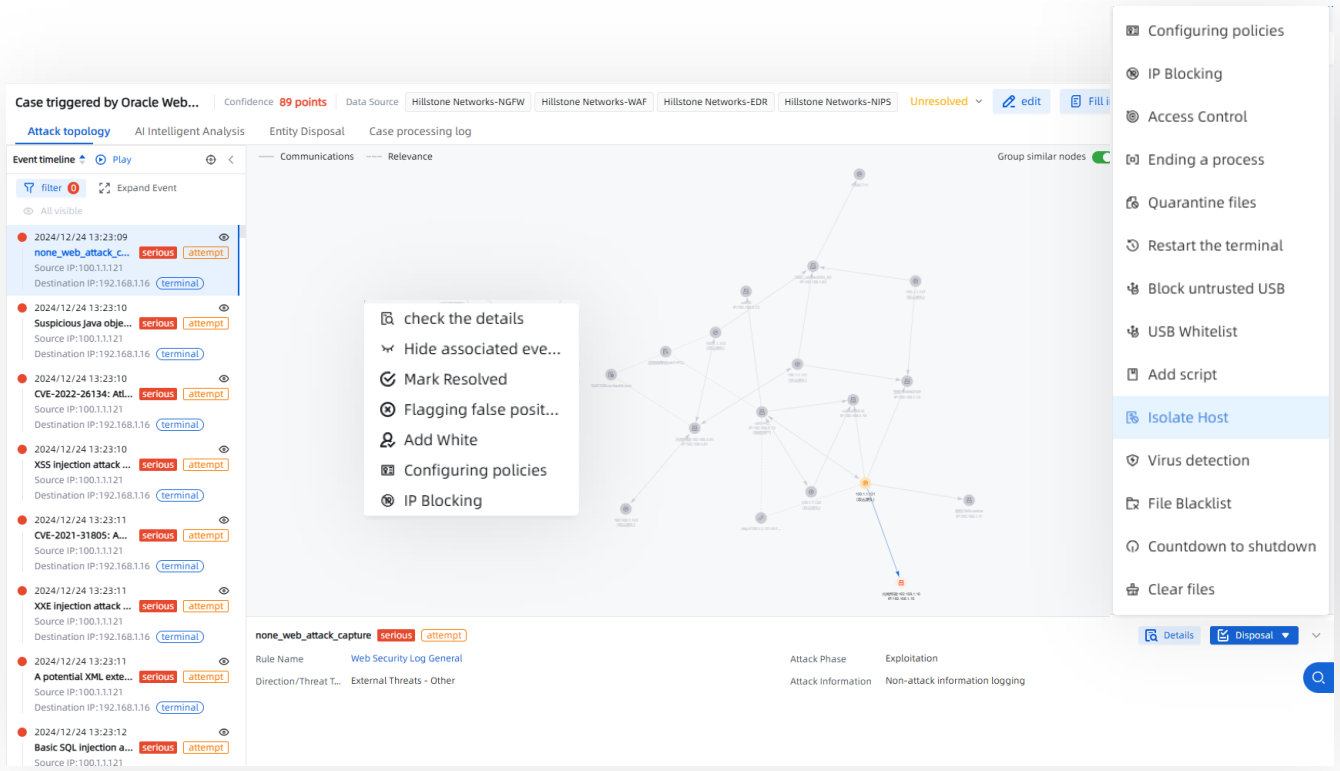


Aggregated Response

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



Incident Investigation



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

Risk Management

Asset Centric Risk Management

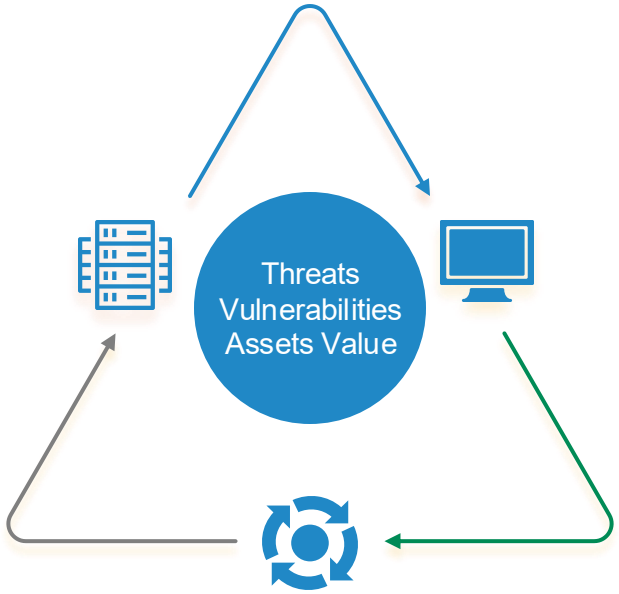
Server Risks

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

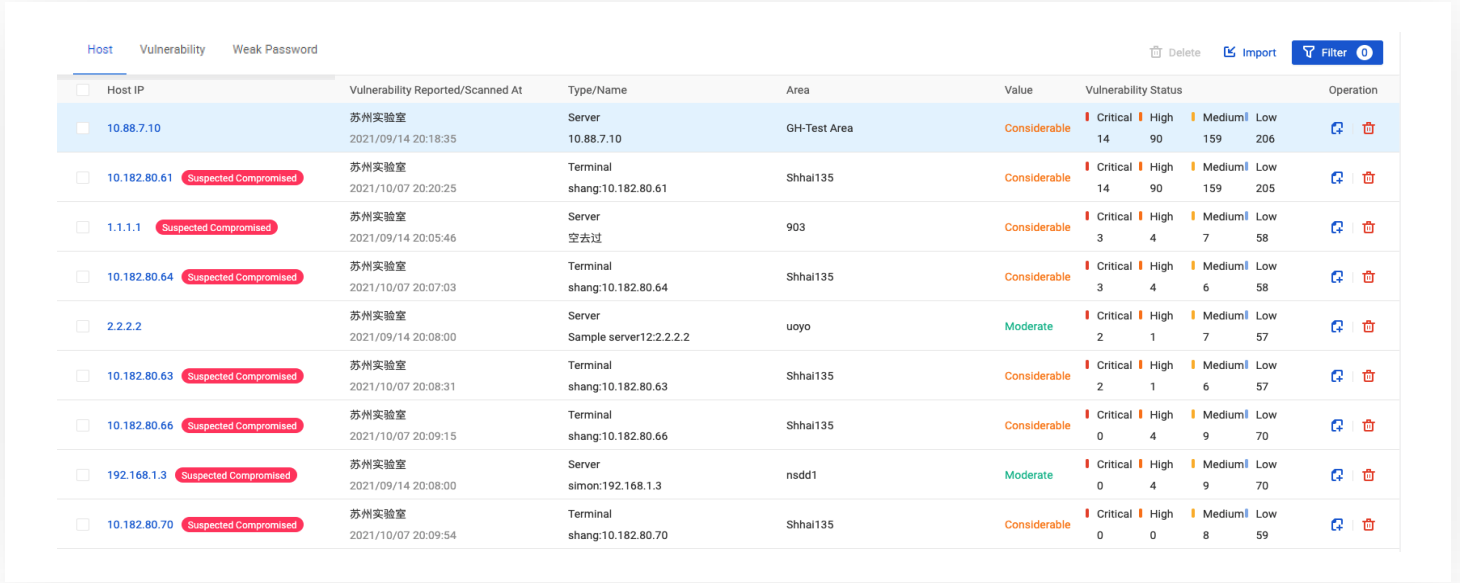
Endpoint(s) risk details

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

Vulnerability Analysis

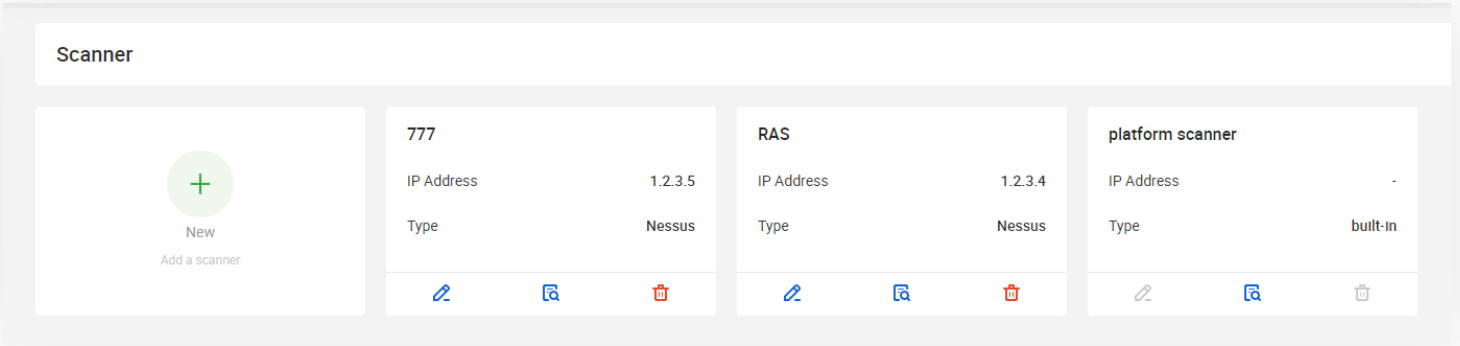
Vulnerability Visualization

- 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



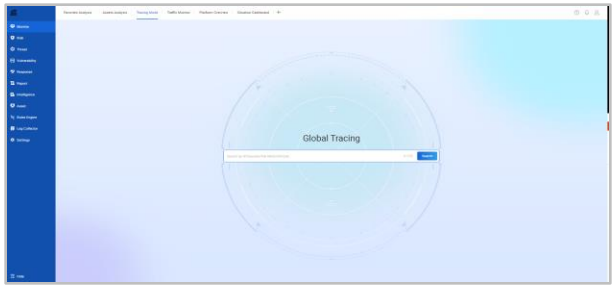
Scanner Management

- 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)

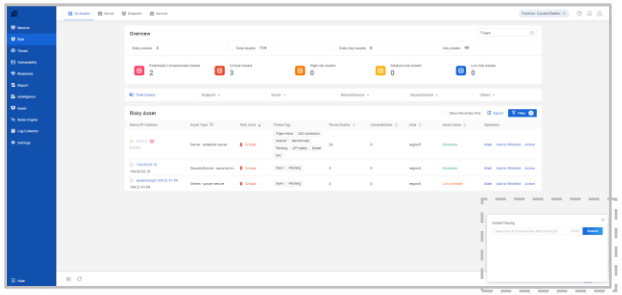


Threat Forensics

Global Search



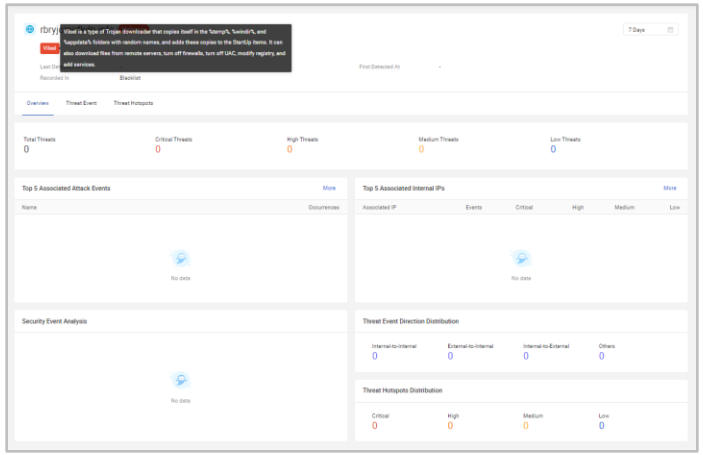
Primary entry



Quick entry

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

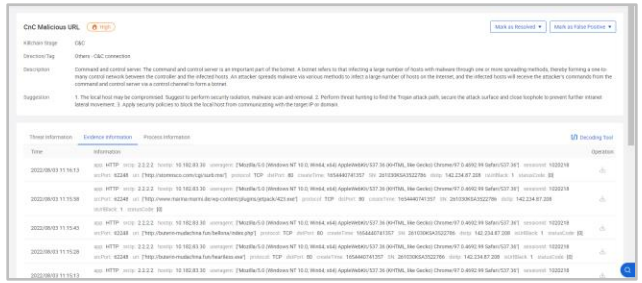
Info Display



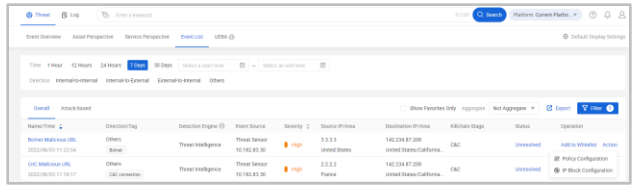
Info display

- 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



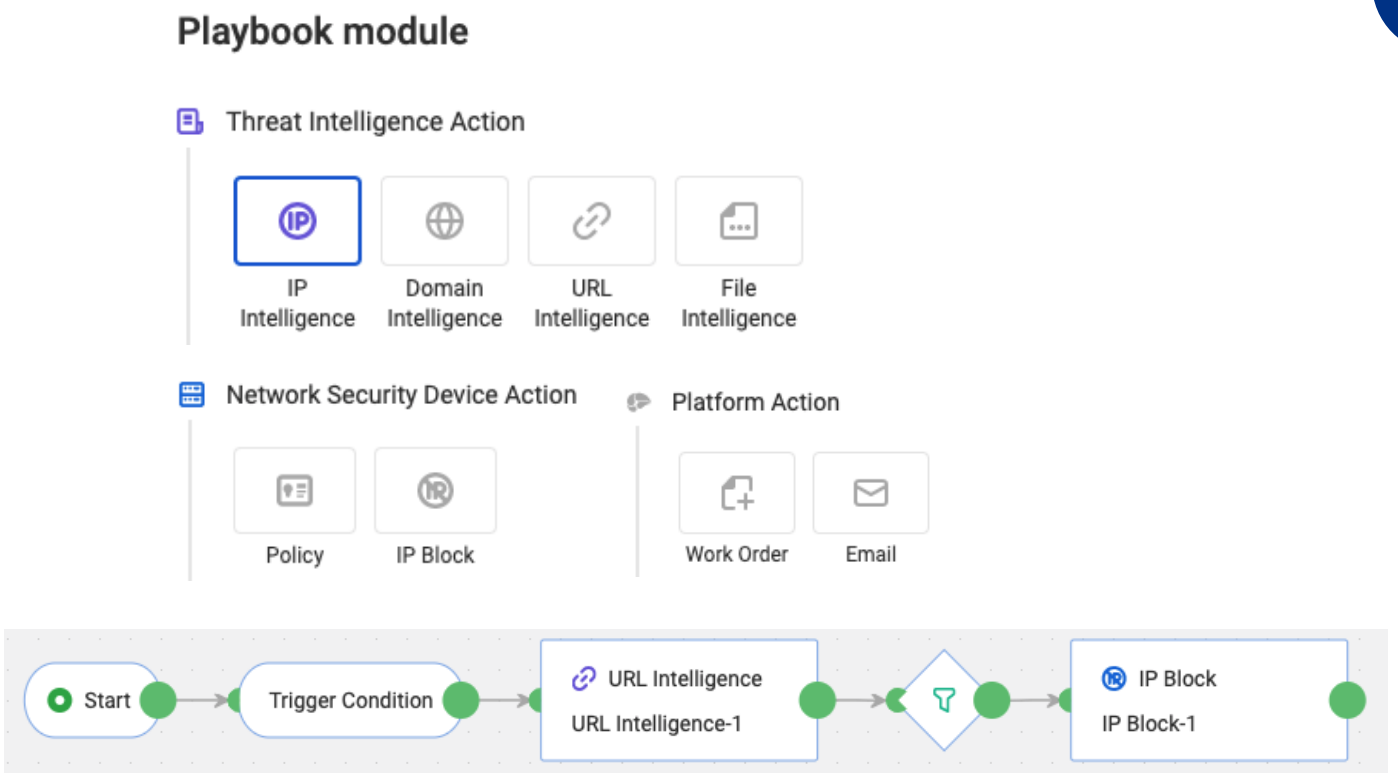
Evidence Information



Incident Response

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

Automated Security Orchestration



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

Incident Response – Integrated Devices


HSM


NGFW


ADC


NIPS


vWAF


CloudEdge


CloudHive

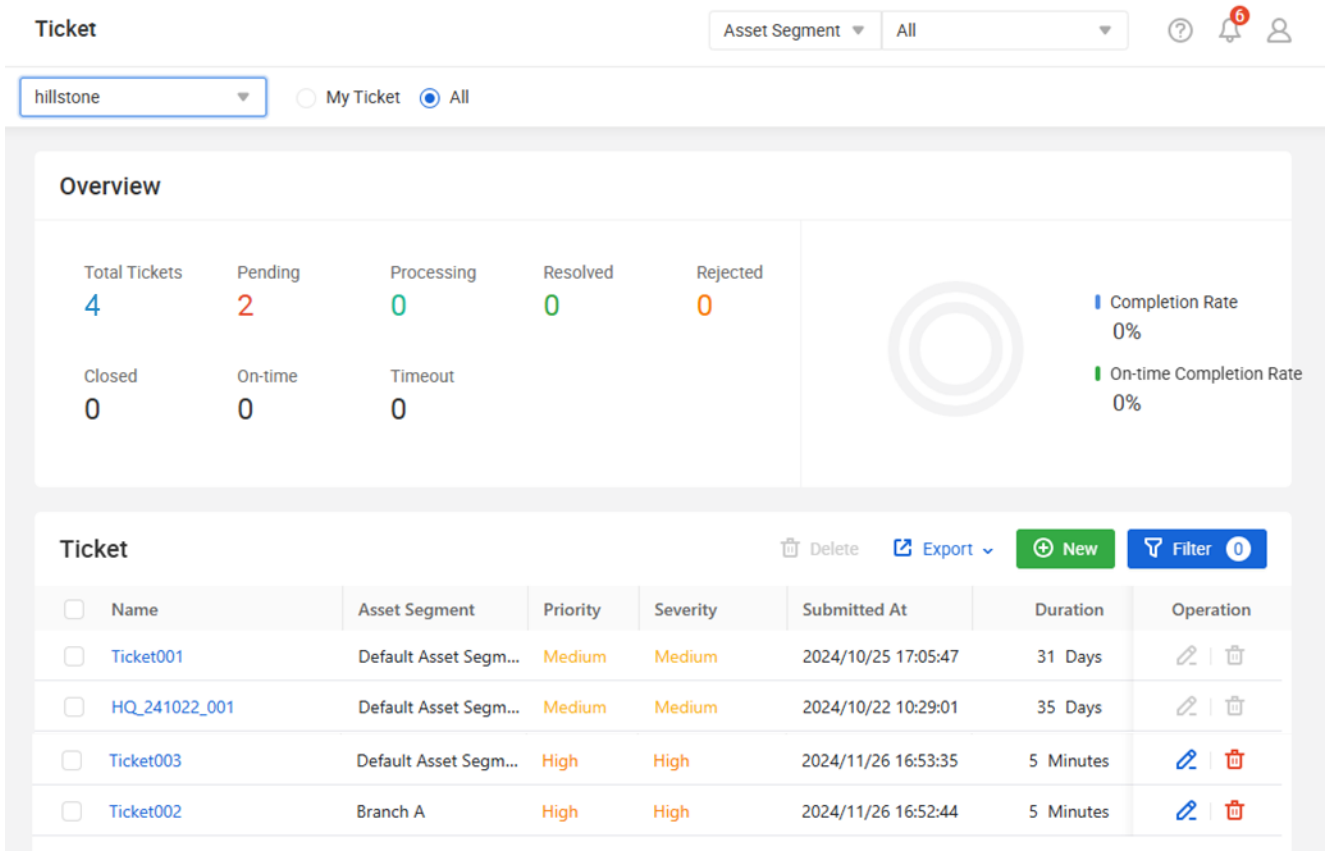

CloudArmour


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

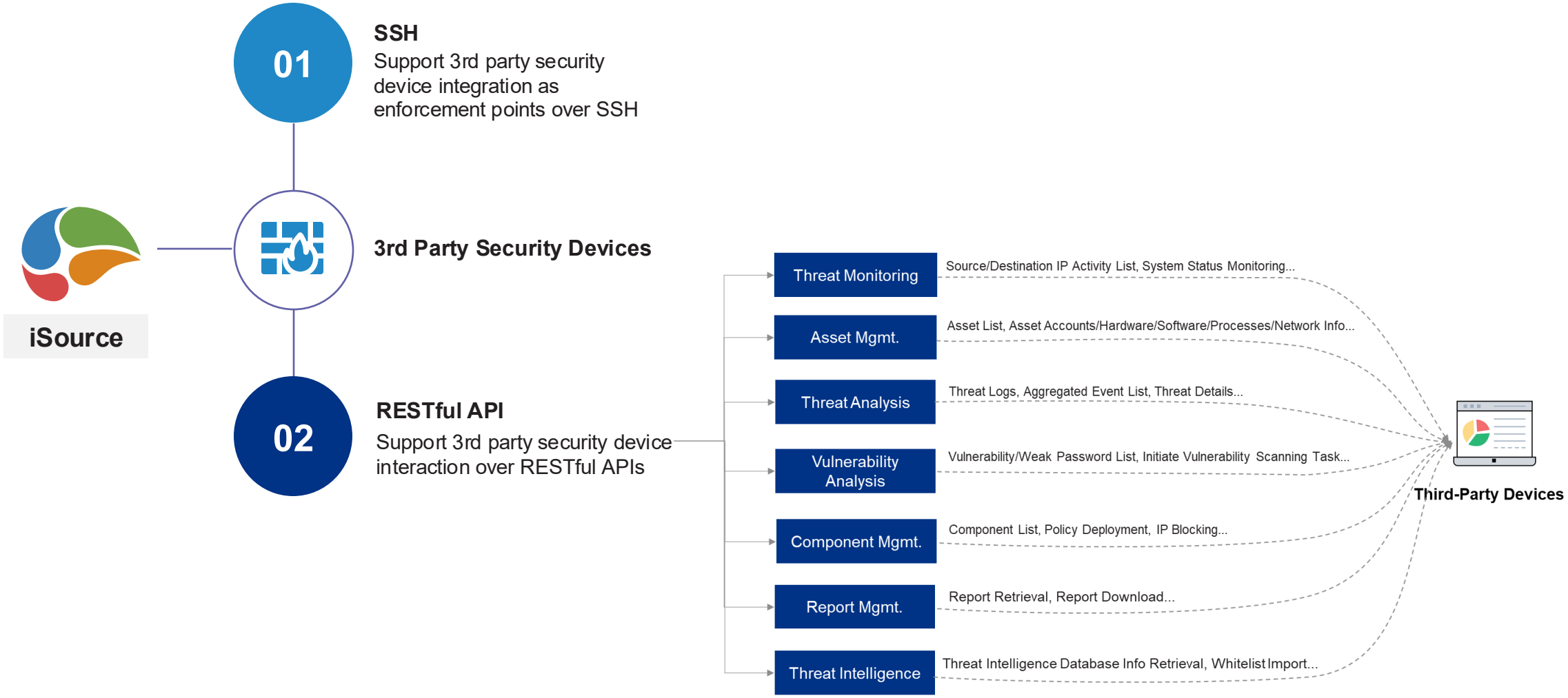
Incident Response – Ticket Management



Ticket Management

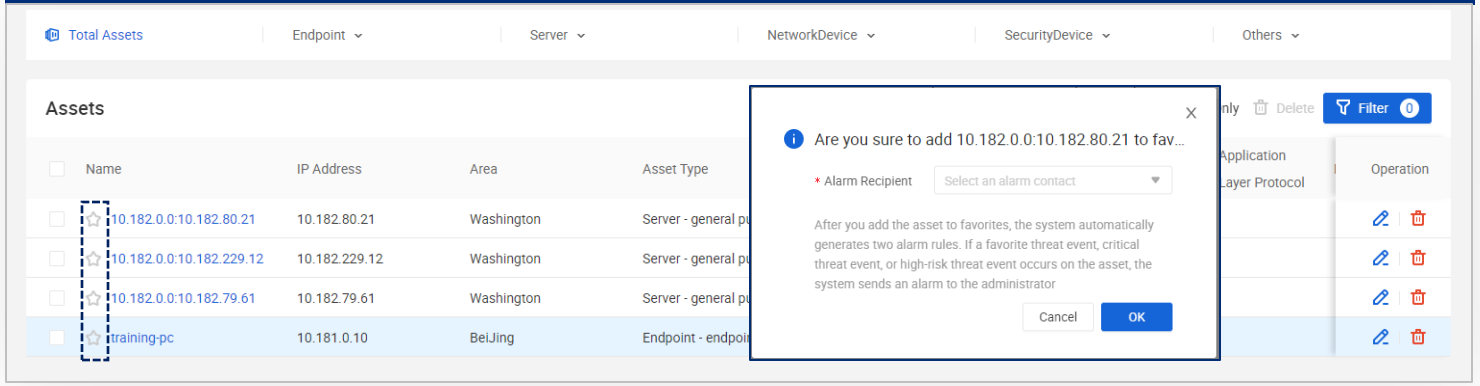
- Ticket delegation and handling across roles
- Role-based ticket visibility
- Ticket status updates
- Ticket operation logs

Third-Party Device Integration

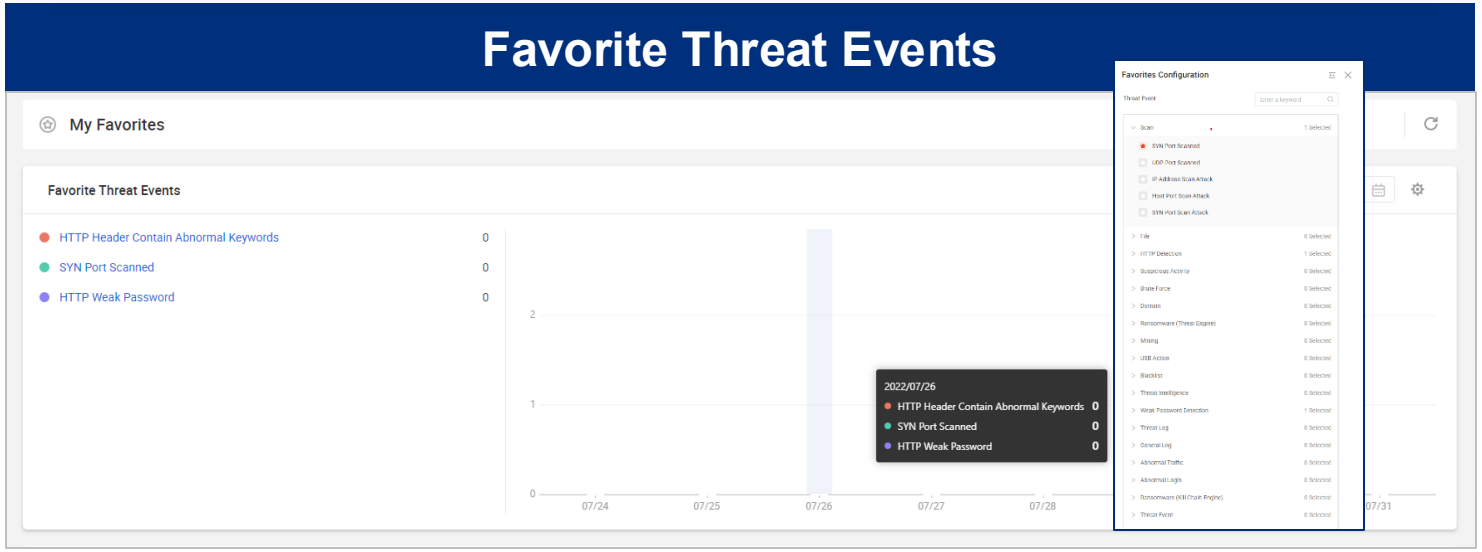


Favorite Asset and Threat Event Management

Favorite Assets



Favorite Threat Events



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 Posture

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

Agile Key Threat Management

Weak Password Breaches

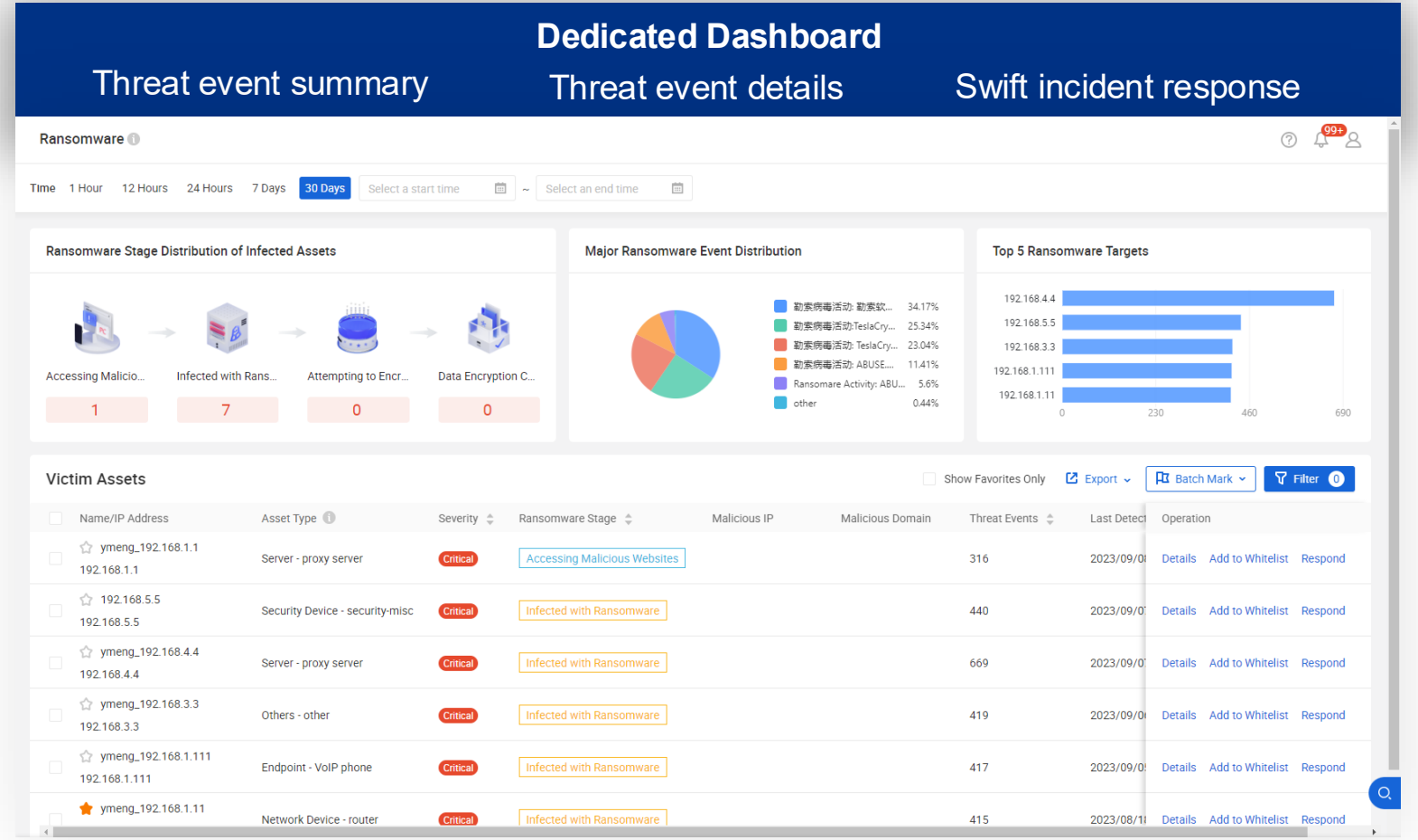
Mining Attacks

Ransomware Attacks

Favorite Assets/Threats

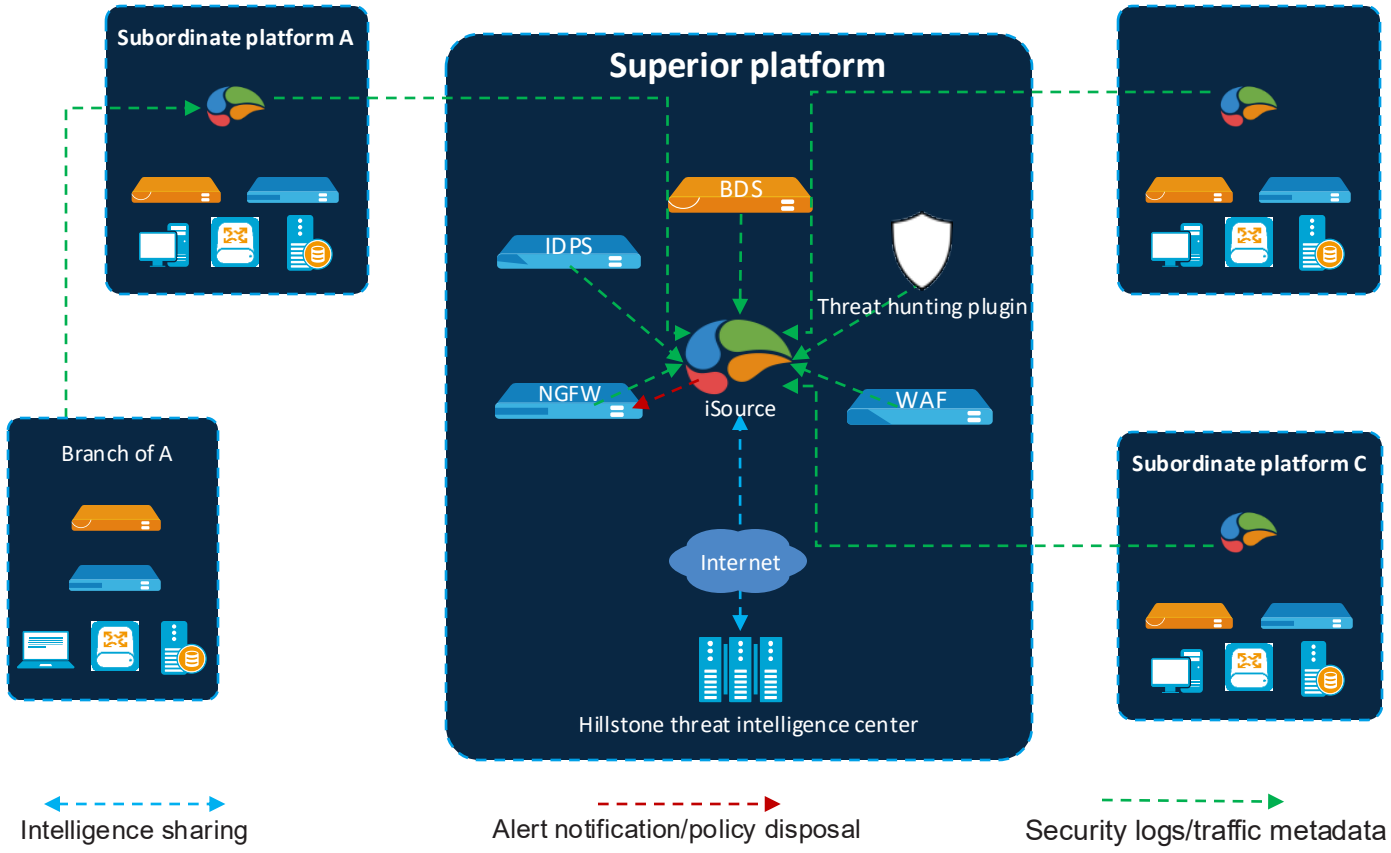
Dedicated Dashboard

Threat event summary | Threat event details | Swift incident response



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

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

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
  - GROK
  - Key-Value
  - JSON
  - JsonPath
- 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

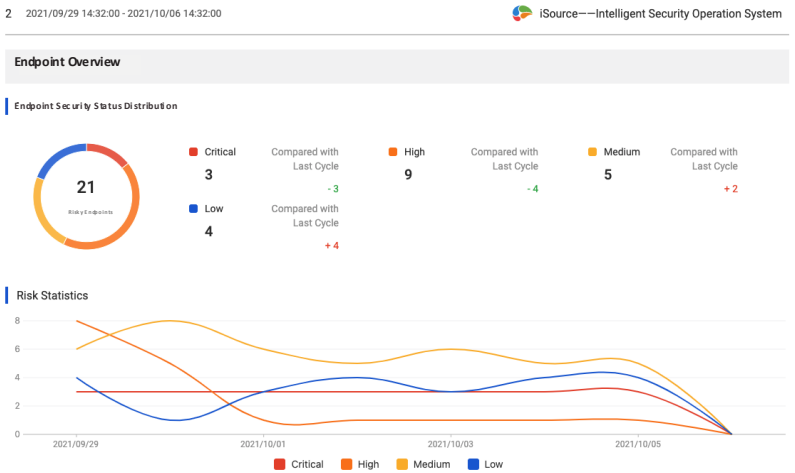
- List all reports
- Support live view
- Support export report in PDF
- Support manual export for customizable queries

Report Task

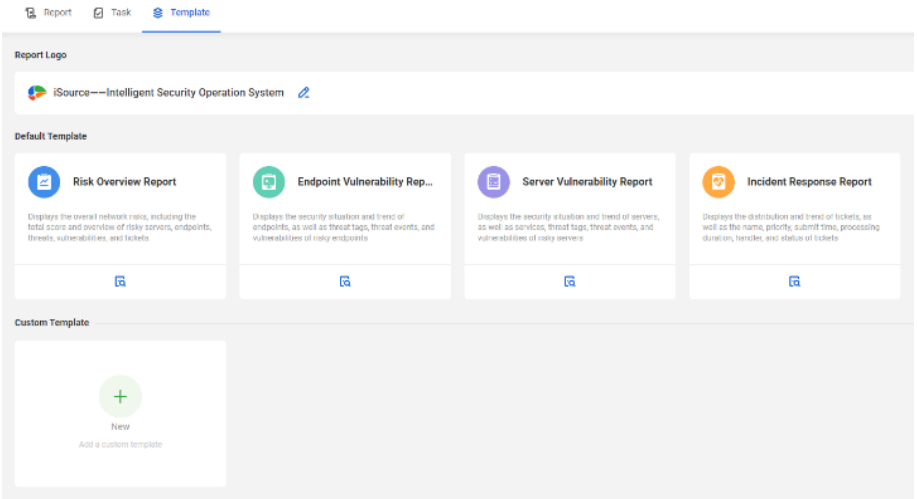
- Generate reports periodically (daily/weekly/monthly)
- Overview or detailed reports

Report Template

- Multiple pre-defined templates
- Customizable templates

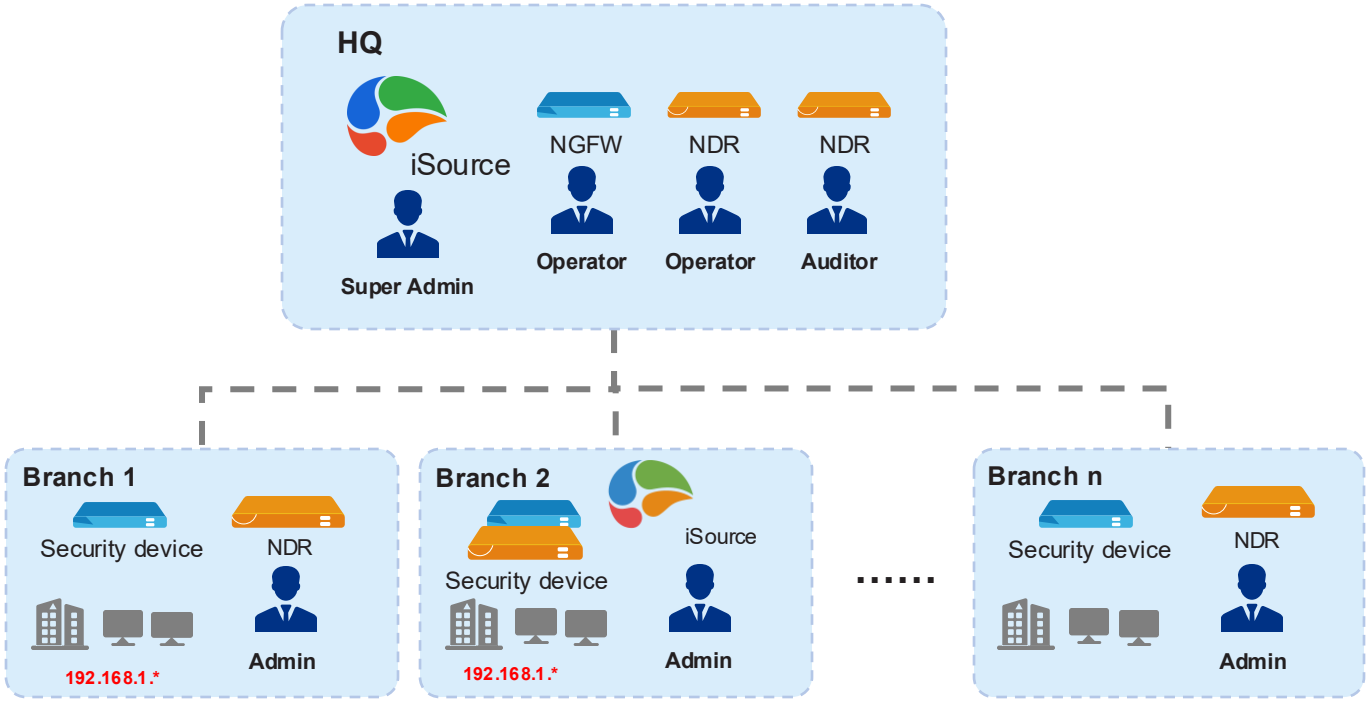


A page of summary report



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

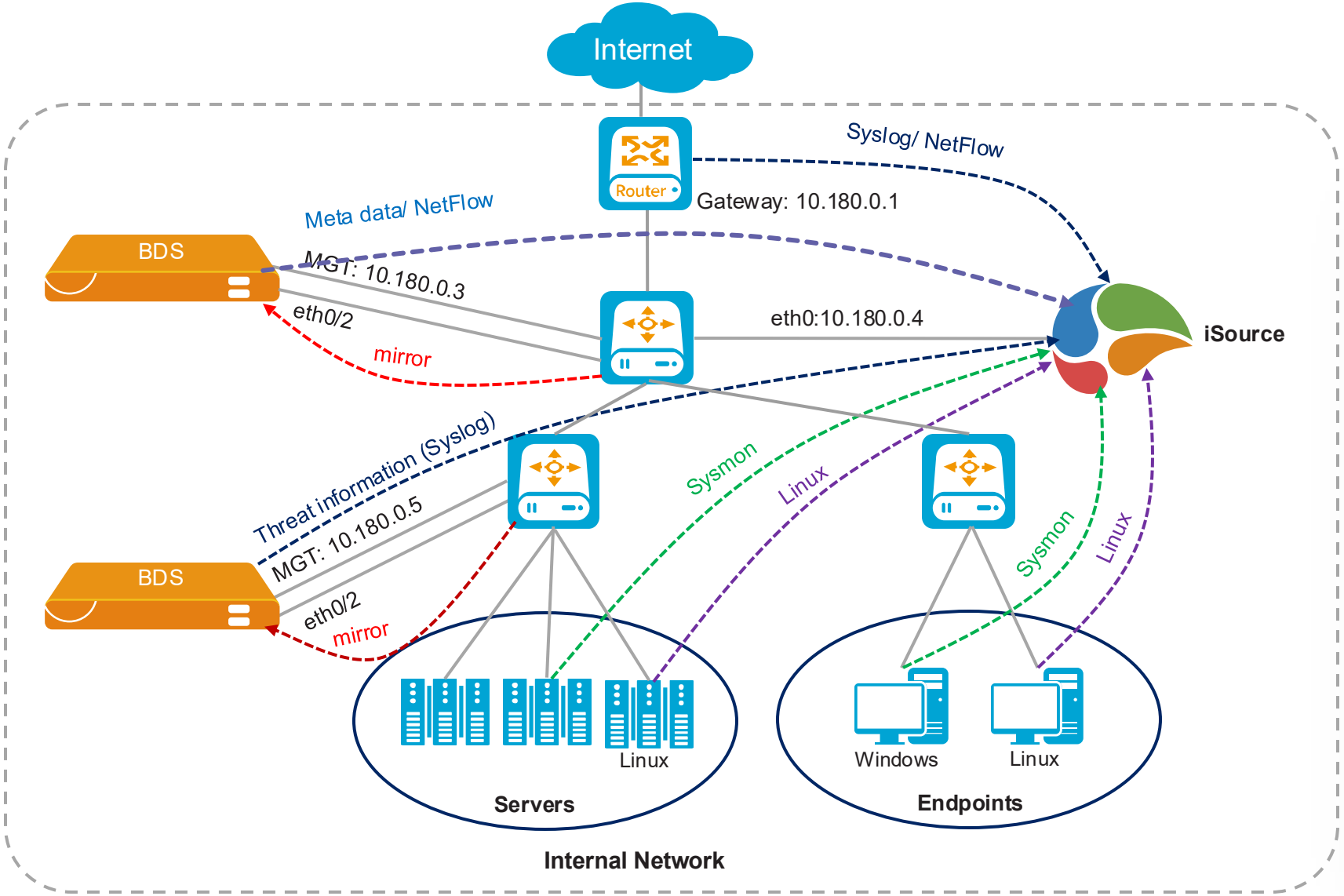
Models		SG-6000-ISC6305	SG-6000-ISC6310	SG-6000-ISC6320
Performance	Throughput	3Gbps	6Gbps	15Gbps
	Event Processing	5000EPS	8000EPS	15000EPS
Minimum Hardware Configuration	CPU	20 cores (64bits)	24 cores (64bits)	48 cores (64bits)
	Memory	128G	128G	256G
	HDD		1TB	

iSource Ordering Guide

Category	SKU	Definition	Term
Base System	• 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	• 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

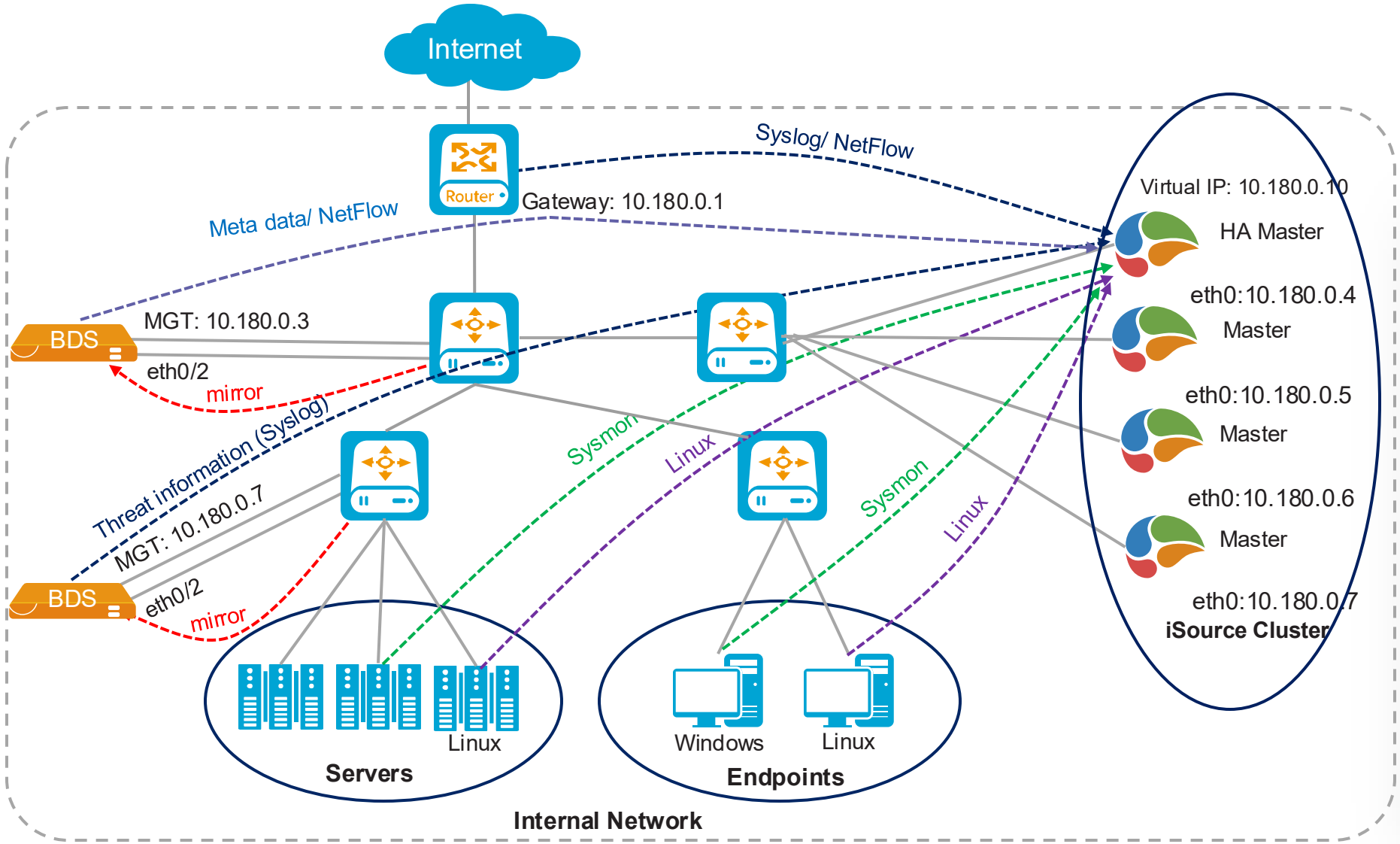
iSource Deployment Scenario- Single Node



Single Node Deployment

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

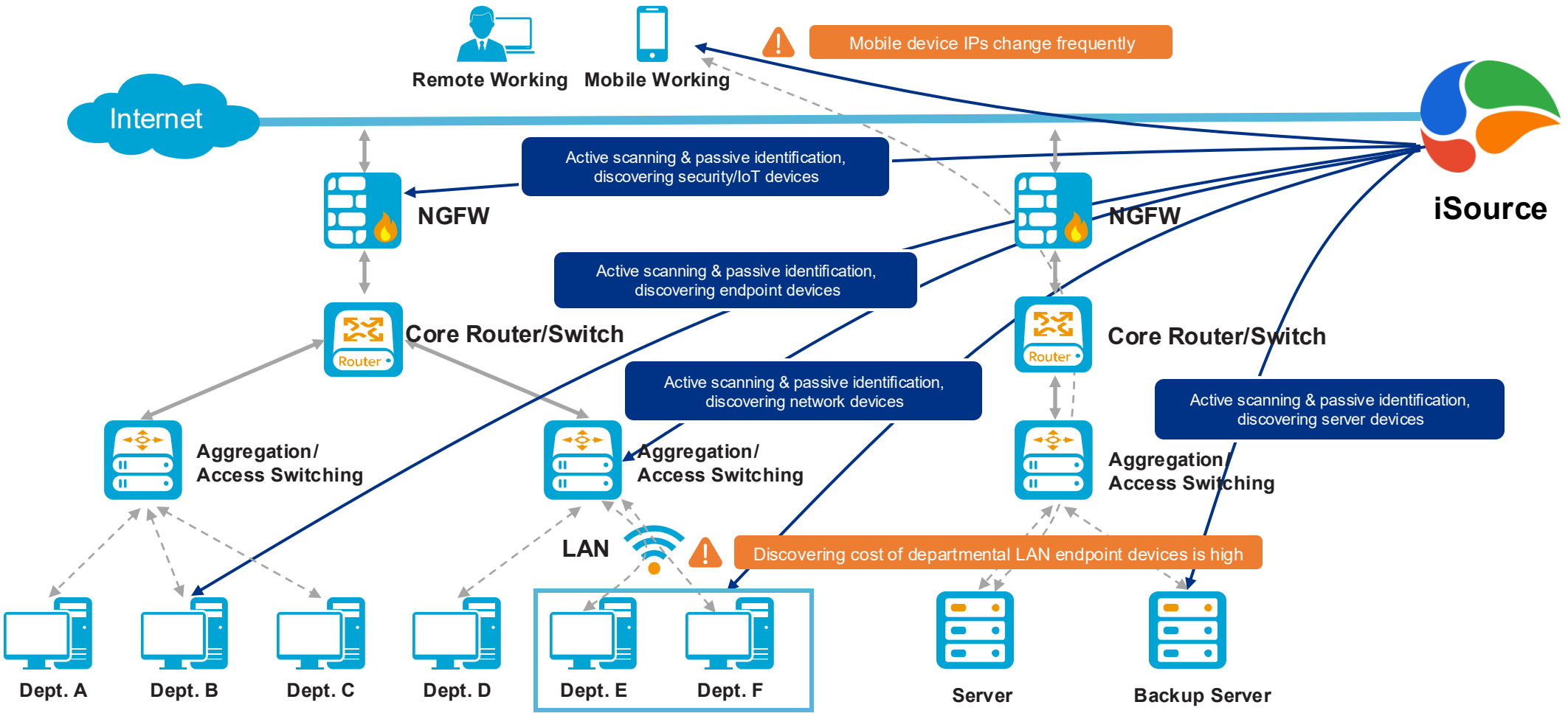
iSource Deployment Scenario- Cluster



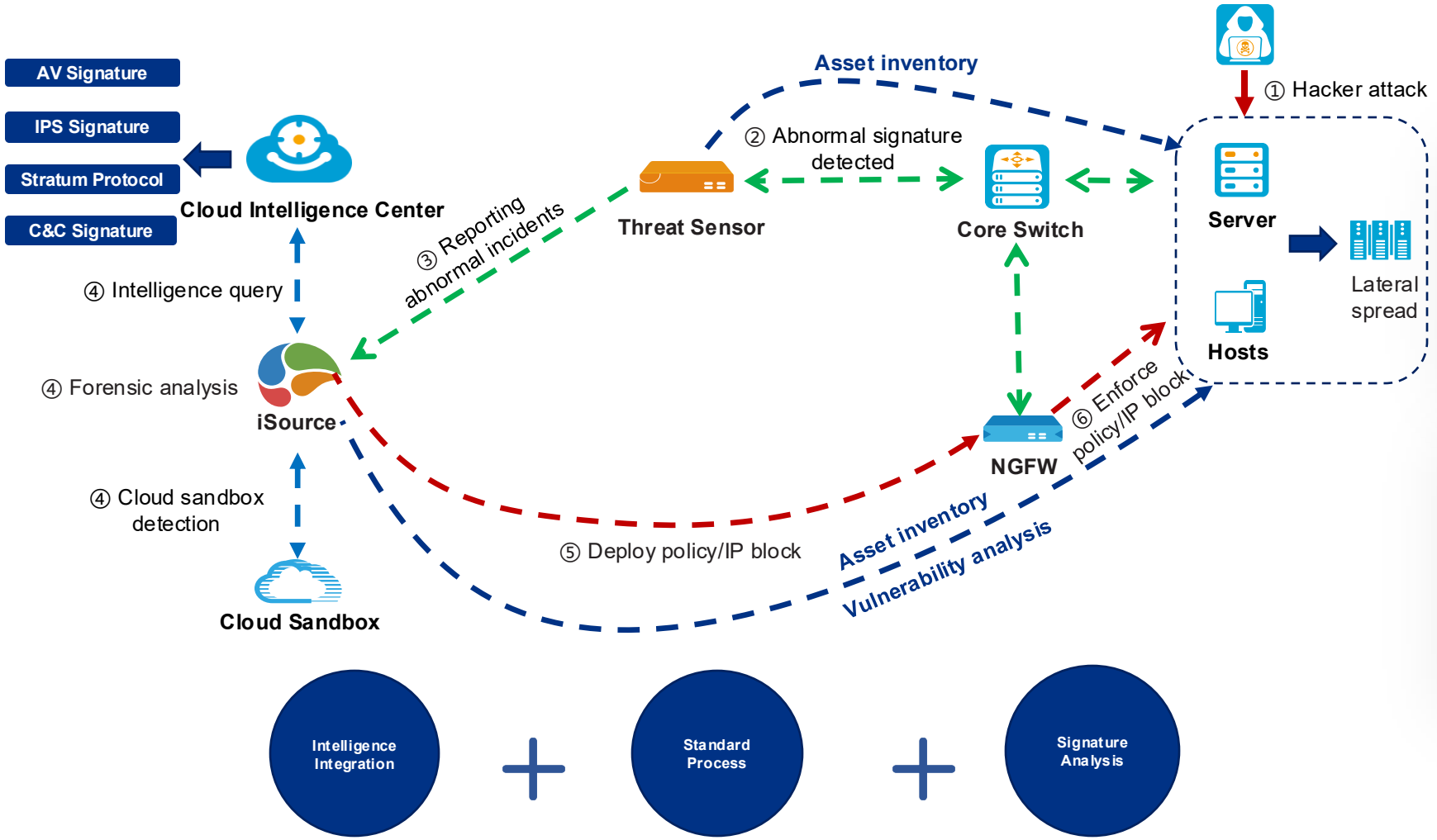
Cluster Deployment

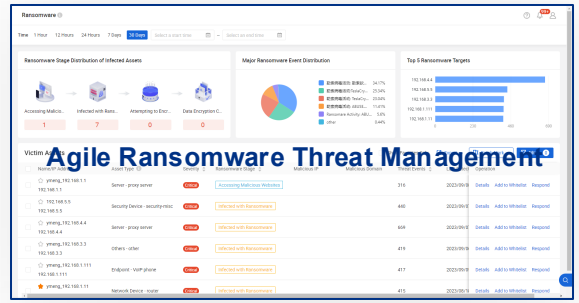
- BDS as a network sensor in TAP mode
- Cluster up to 5 nodes
- iSource deployment has little impact on the existing network environment
- Highly scalable solution

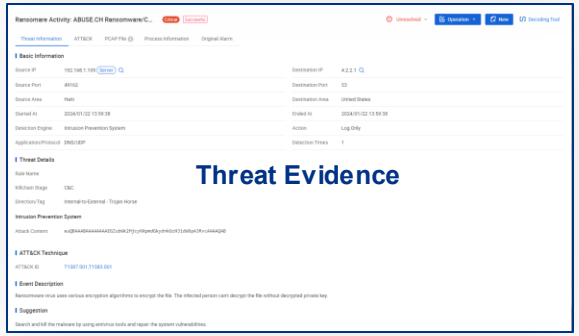
Use Case - Unified Asset Management



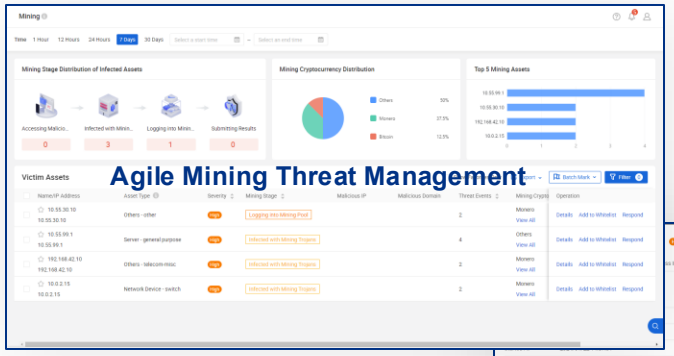
Use Case - Ransomware Solution

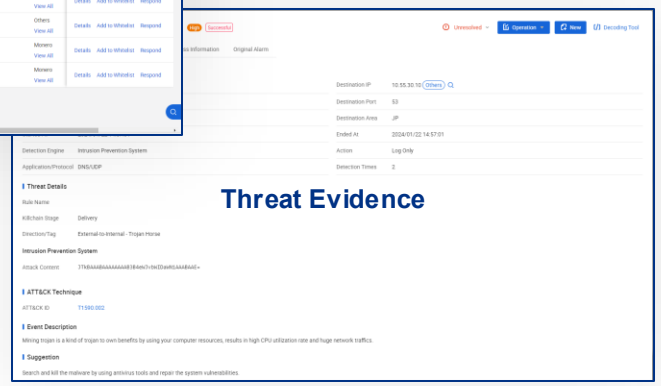


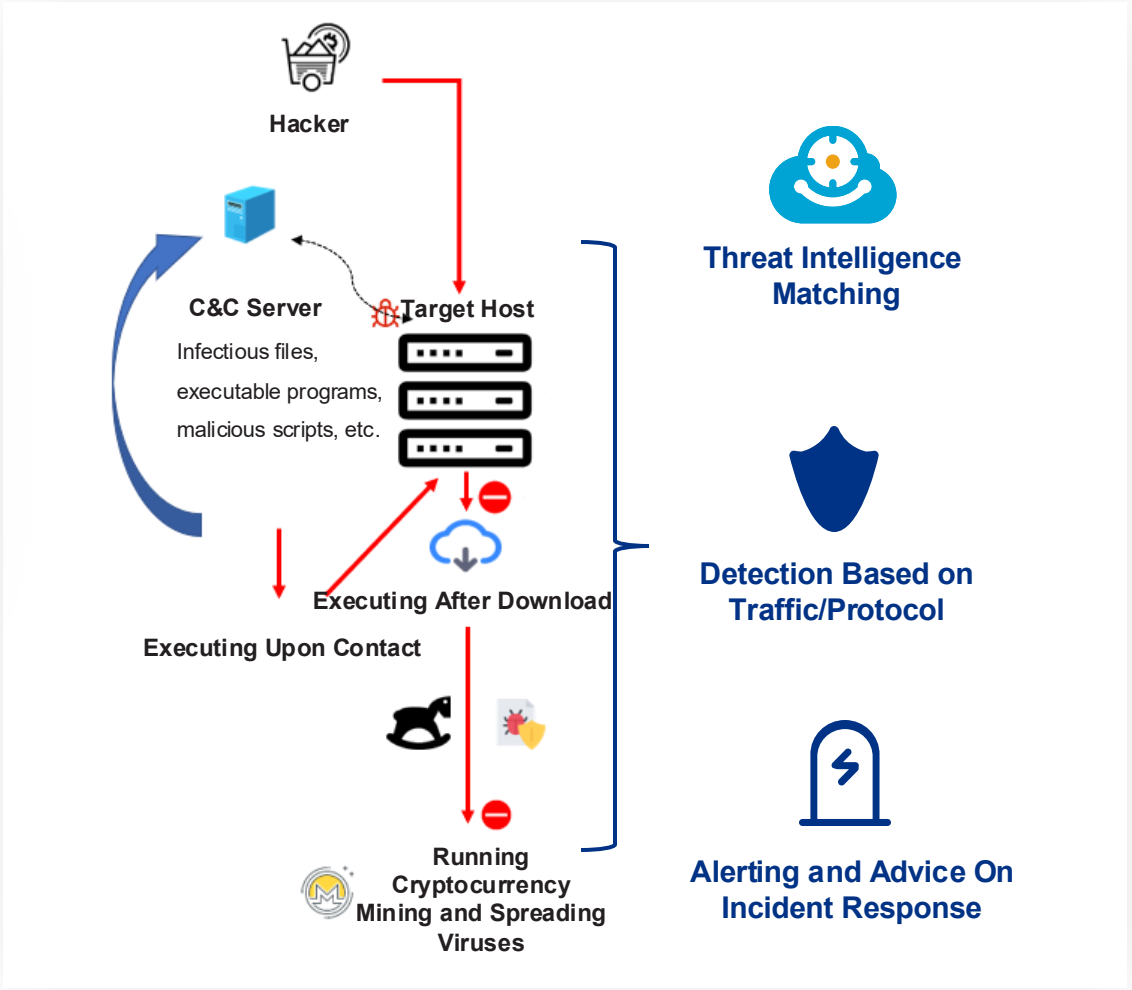




Use Case - Cryptomining Solution





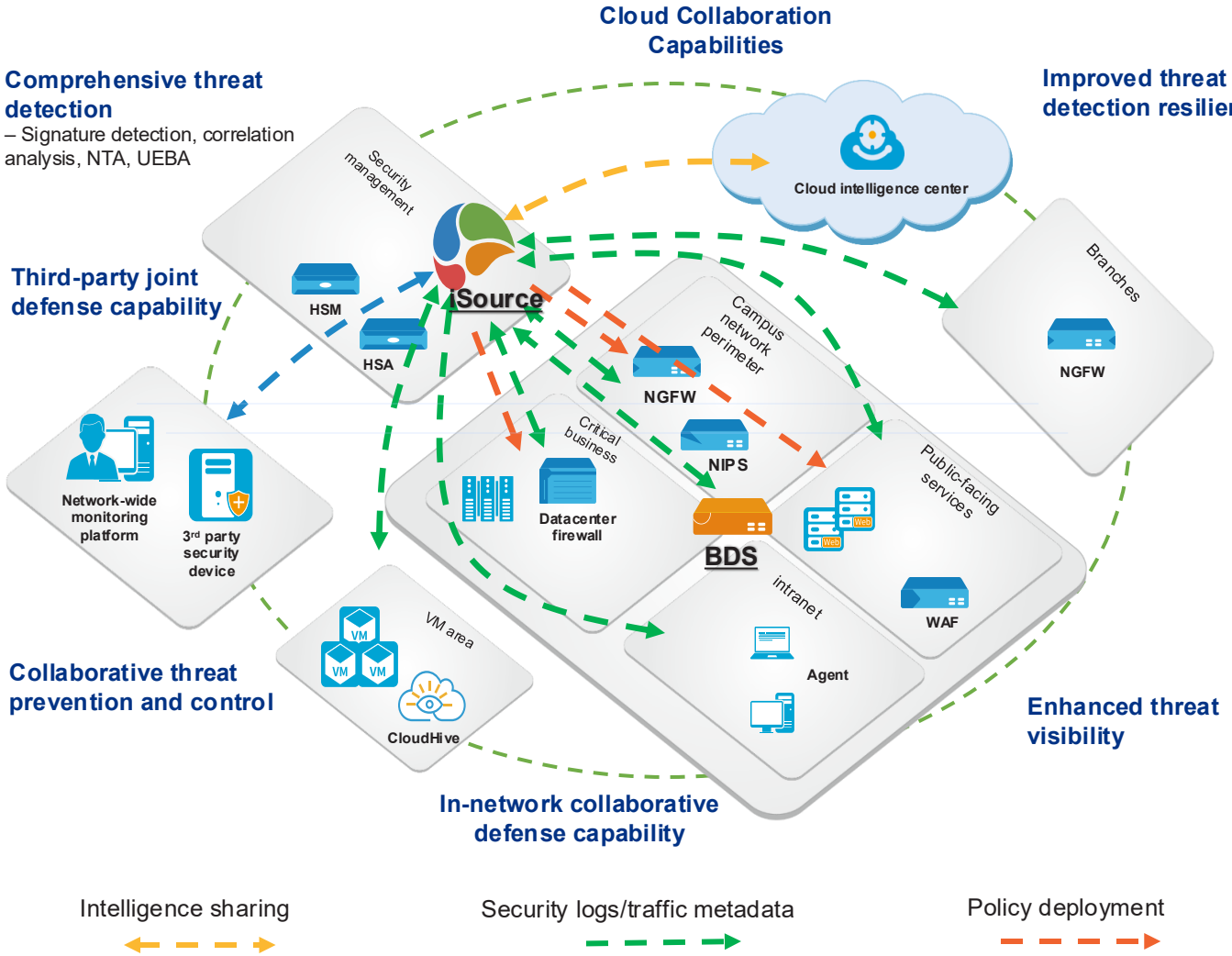


Abnormal process

Abnormal usage

Abnormal login → Privilege escalation → Illegal upload

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

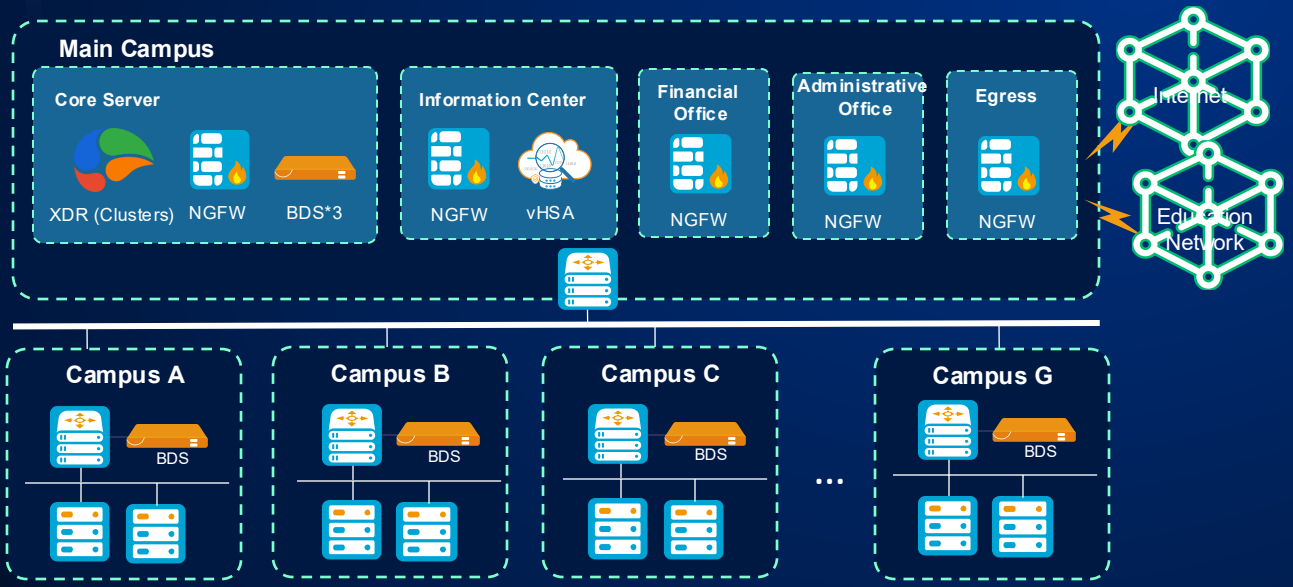
Case Studies

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

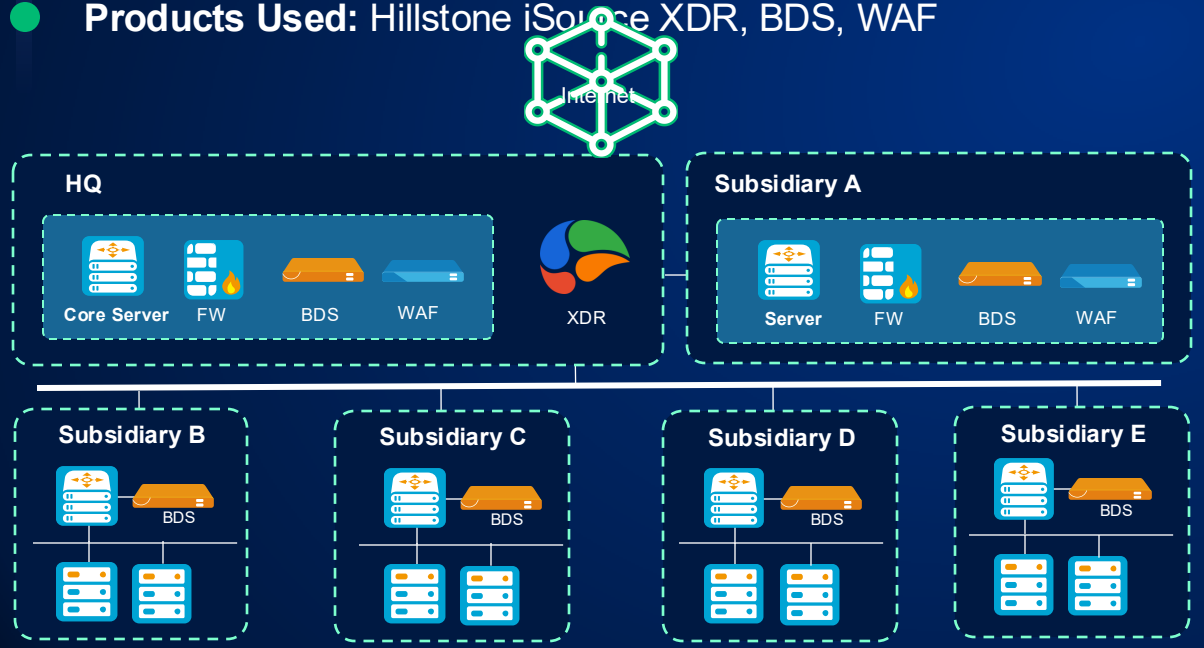
- Hillstone iSource XDR delivers centralized threat visibility across endpoints, networks, and cloud environments, detecting cryptomining, malicious outbound connections, and other hidden threats.
- It ensures consistent security across departments, preventing silos.
- It automates routine tasks and 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

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY Vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision