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	Cloud Adoption	Extended Endpoints
• Exponential Increase of Traffic	• Private/Hybrid deployment	• IoT devices
• New business apps/upgrades	• SaaS apps	• Mobile devices
• Access from anywhere	• Serverless computing	• Connected vehicles
	• Containers	

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

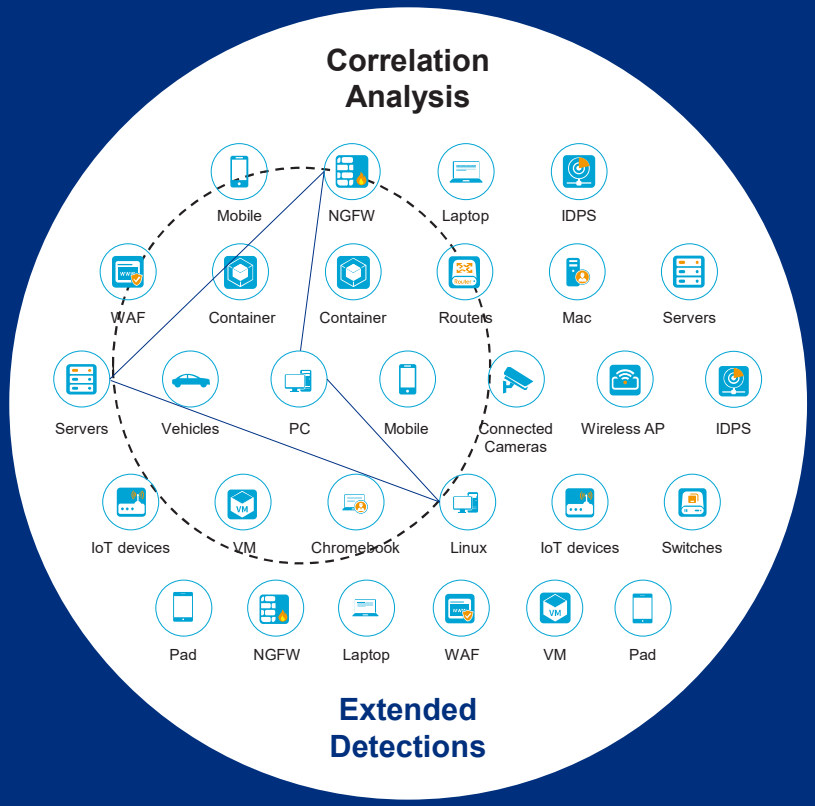
What Do Customers Need?

Comprehensive Data Collection

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

Full visibility

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



Threat Hunting and Analysis

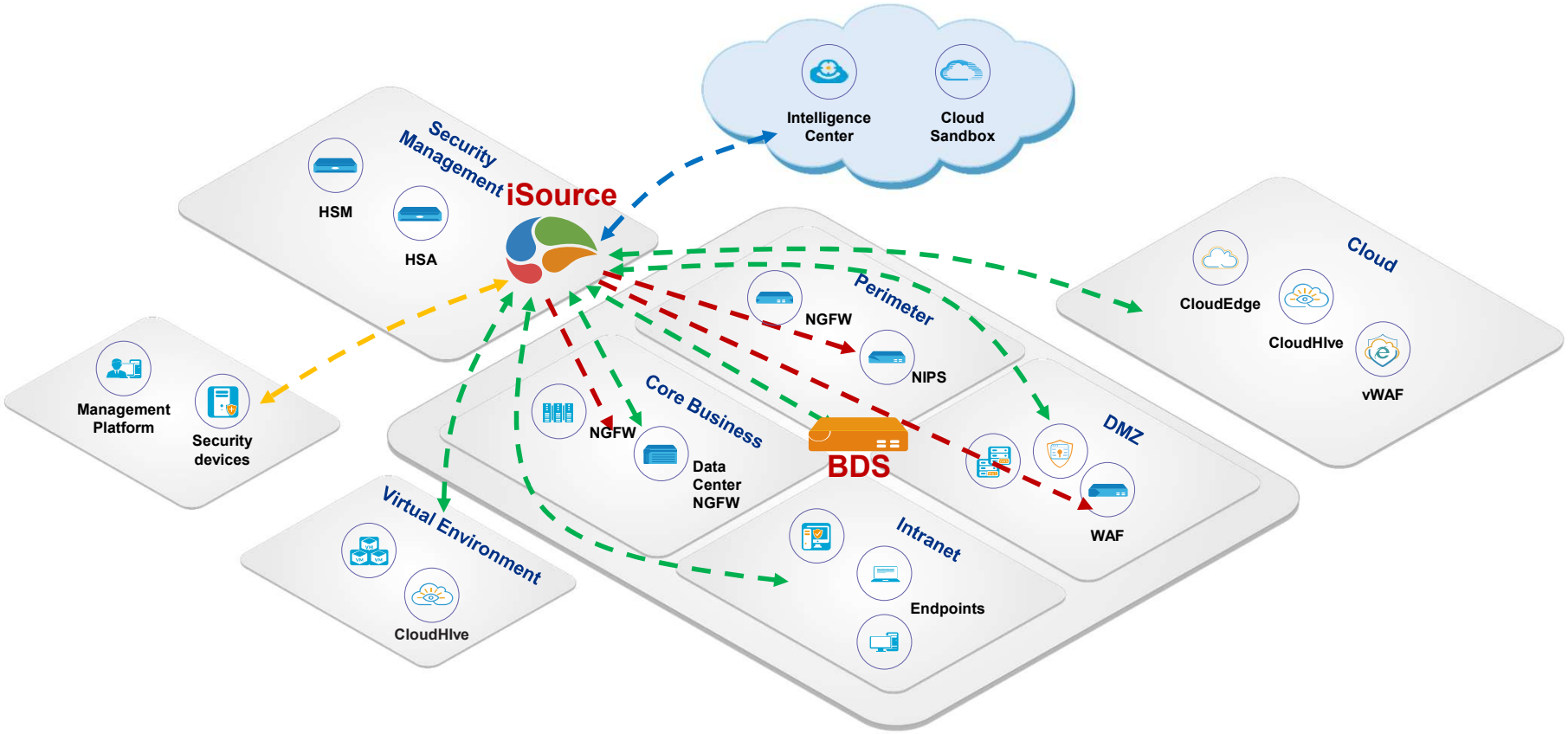
- Threat detection
- Behavior analysis
- Correlation analysis
- Root cause and attack source analysis
- …

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

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

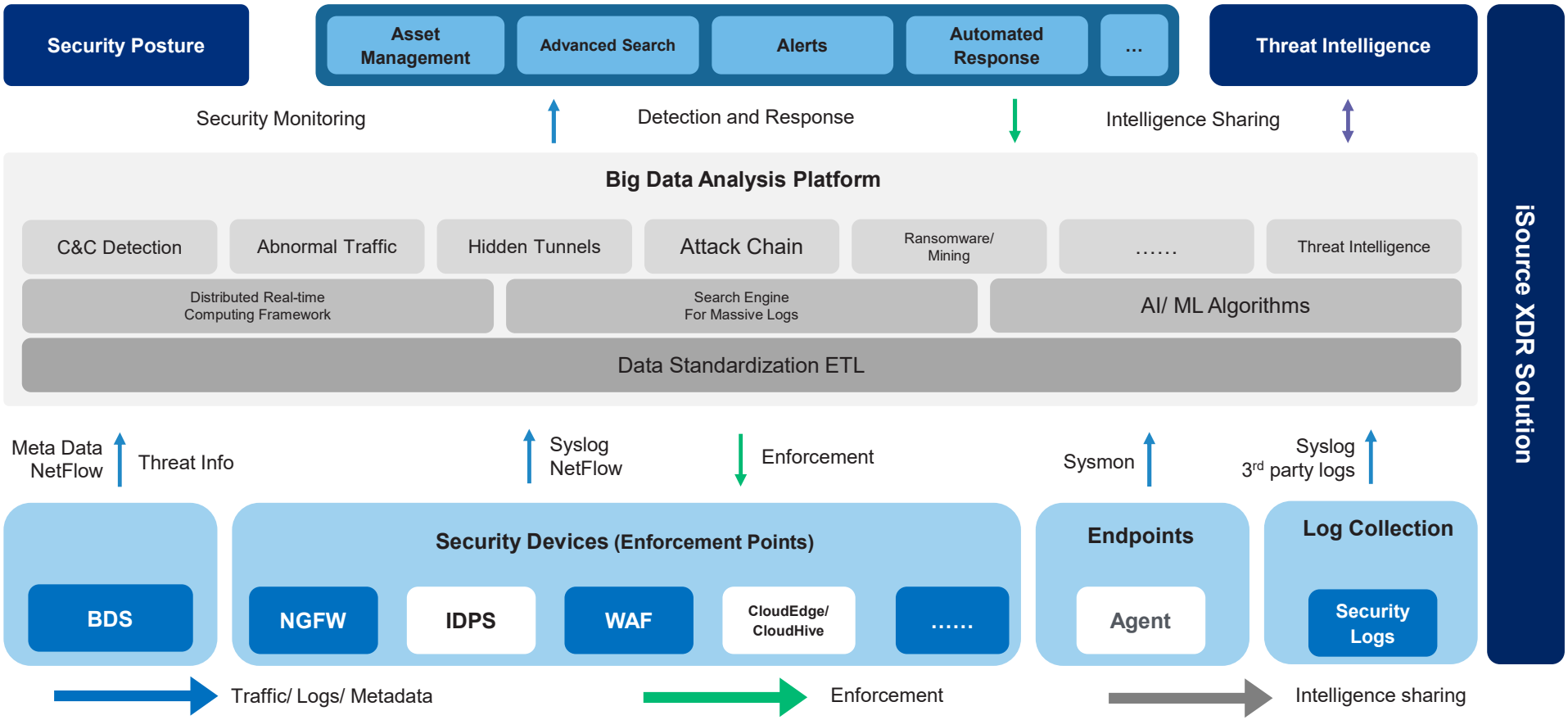
05 Automated Orchestration and Response

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

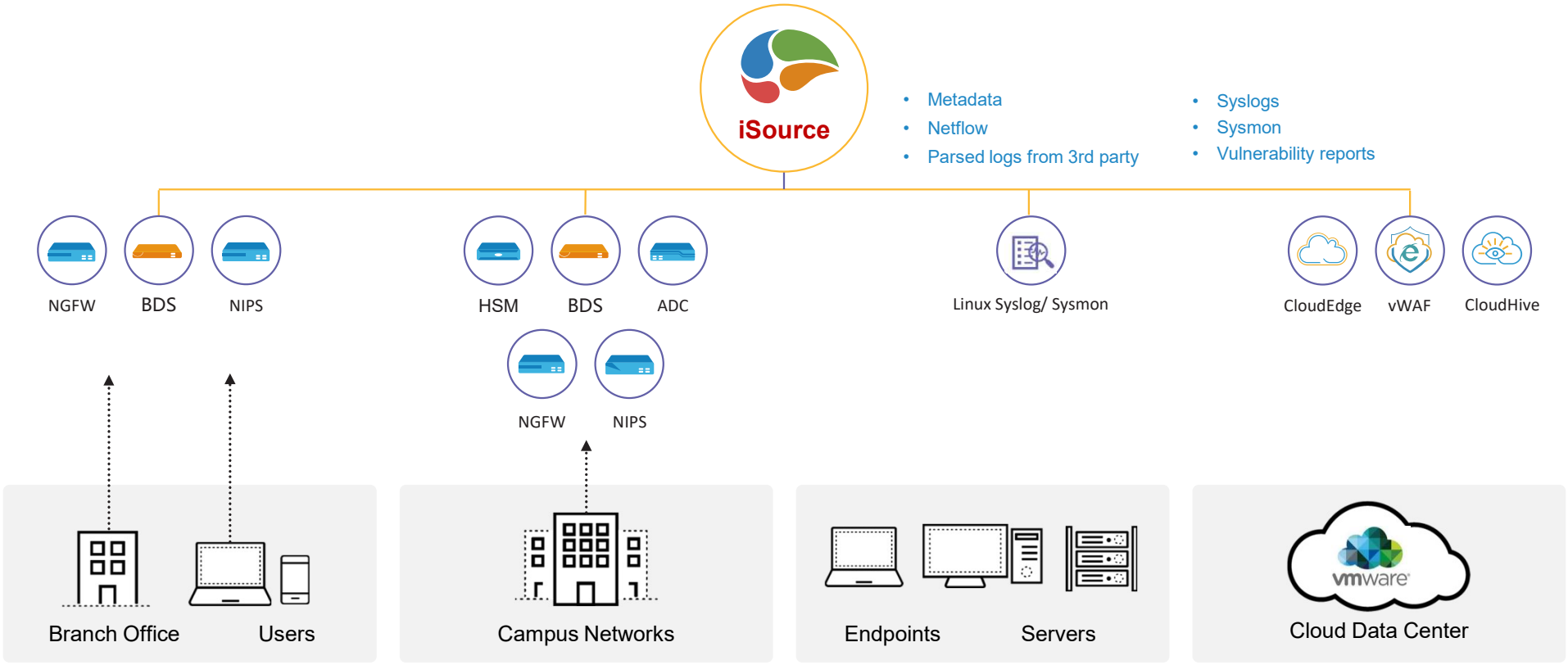
06 Open Platform with High scalability

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

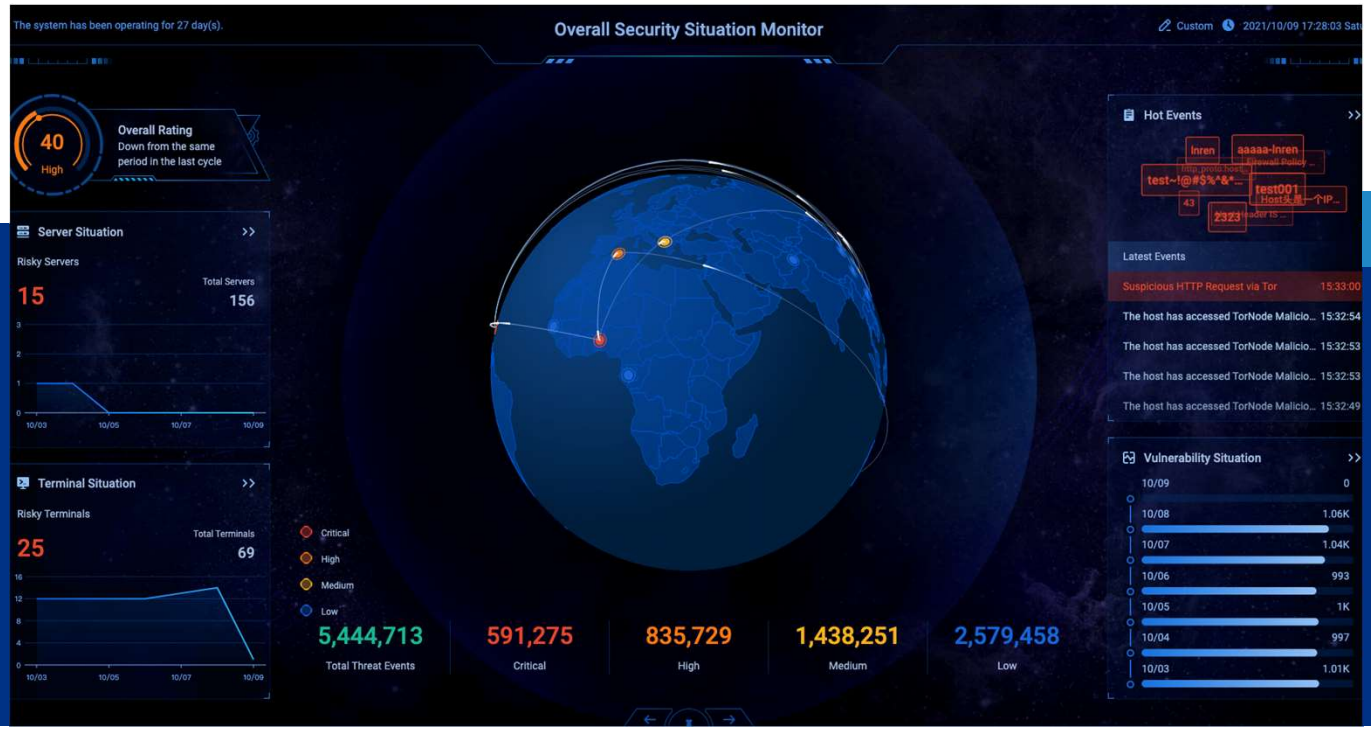
iSource: XDR Solution Architecture



Complete Data Collection Across The Environment



Full-screen Monitoring Dashboards

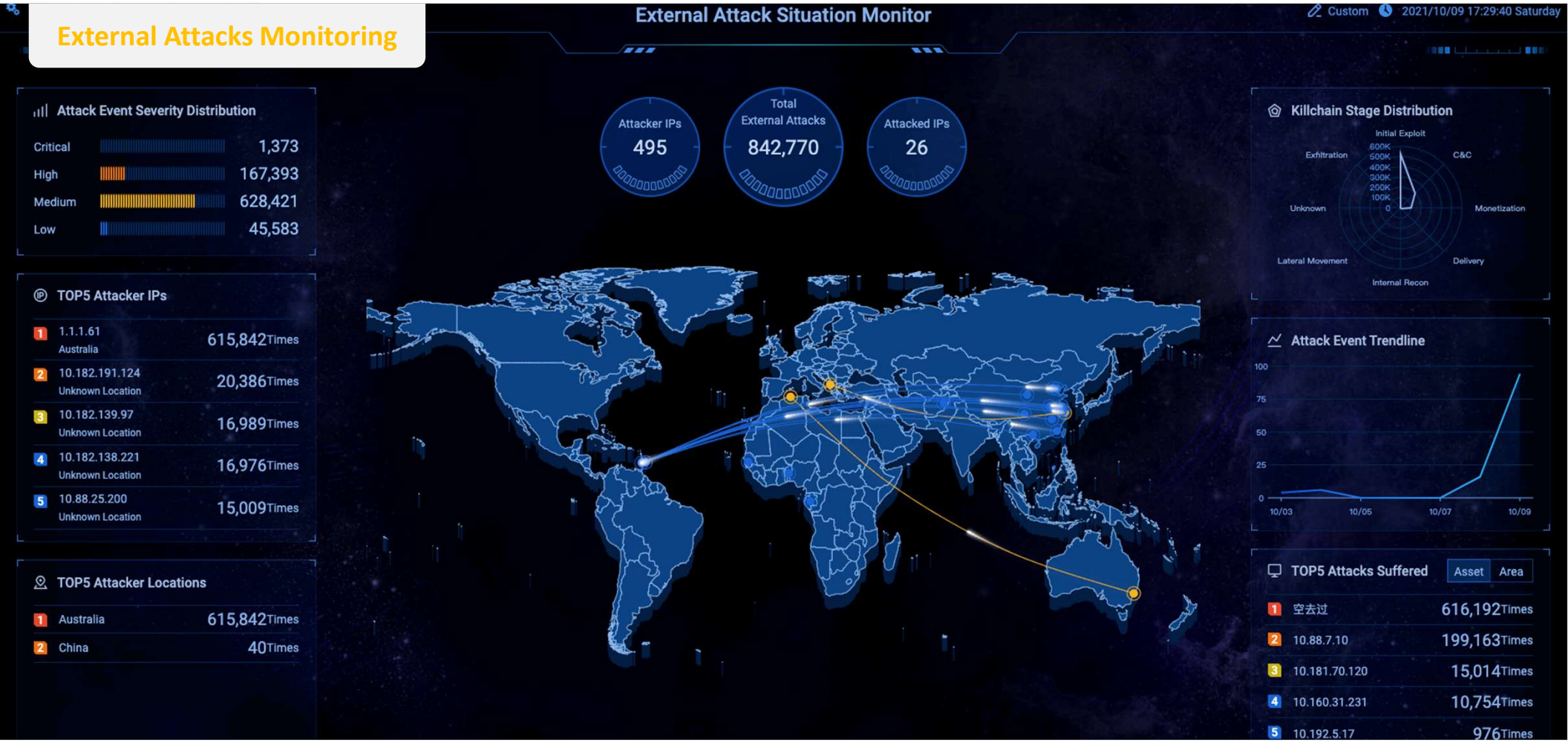


Security Overview Dashboard

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

Full-screen Monitoring Dashboards

External Attacks Monitoring



Full-screen Monitoring Dashboards

Server Monitoring

Full-screen Monitoring Dashboards

Hillstone NETWORKS

Endpoints Monitoring

Full-screen Monitoring Dashboards

Hillstone NETWORKS

Threat Events Monitoring

Full-screen Monitoring Dashboards

Hillstone NETWORKS

Vulnerability Monitoring

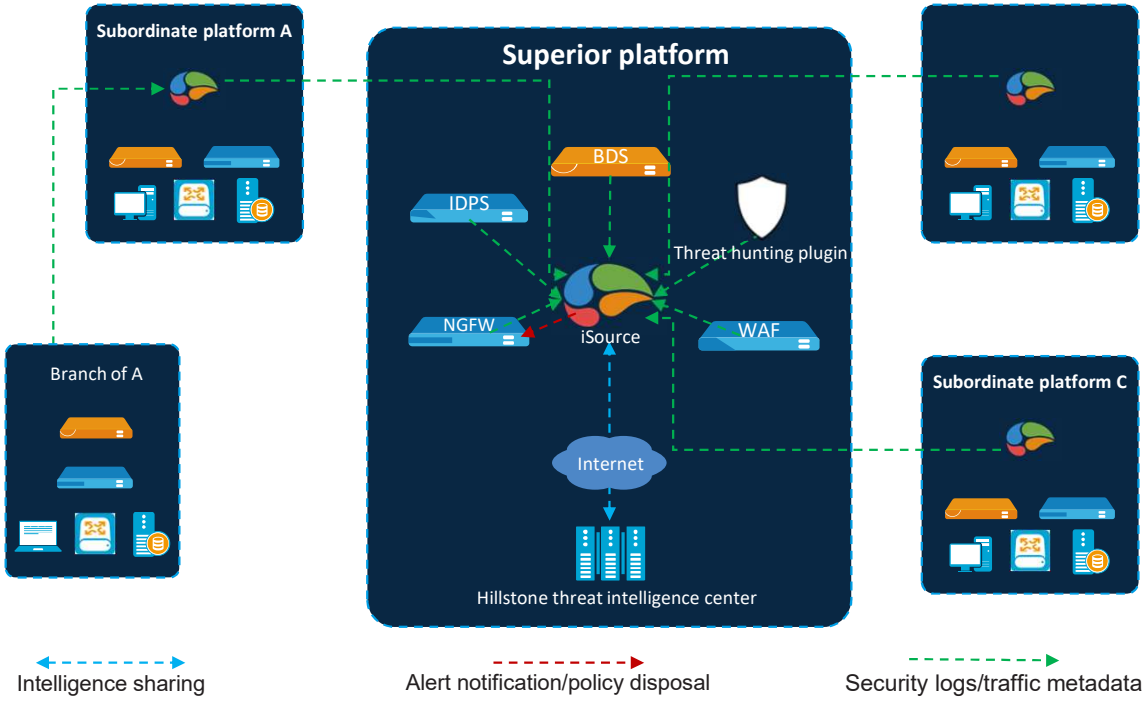
Full-screen Monitoring Dashboards

Hillstone NETWORKS

Area Monitoring

Hierarchical Management

Hierarchical Management



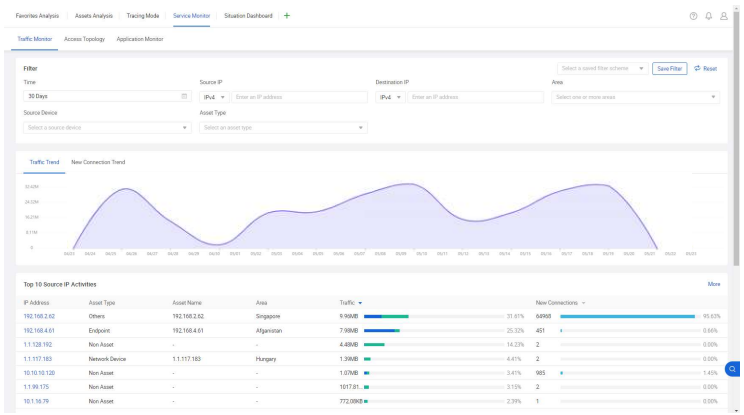
Hierarchical Management Monitoring Dashboard

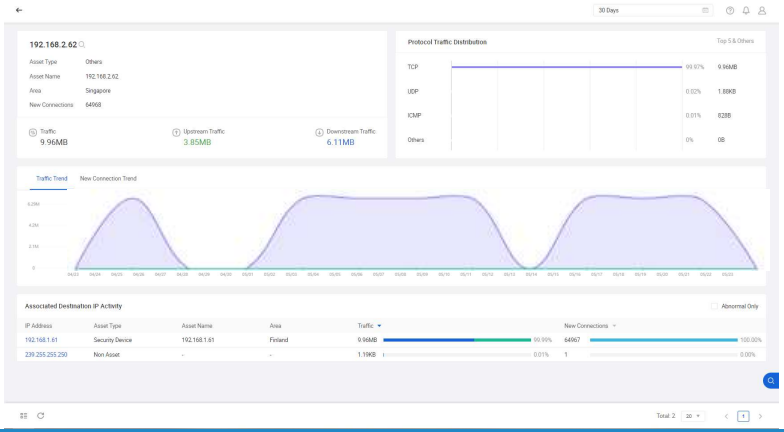
Aggregated Security Posture Across All Platforms

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

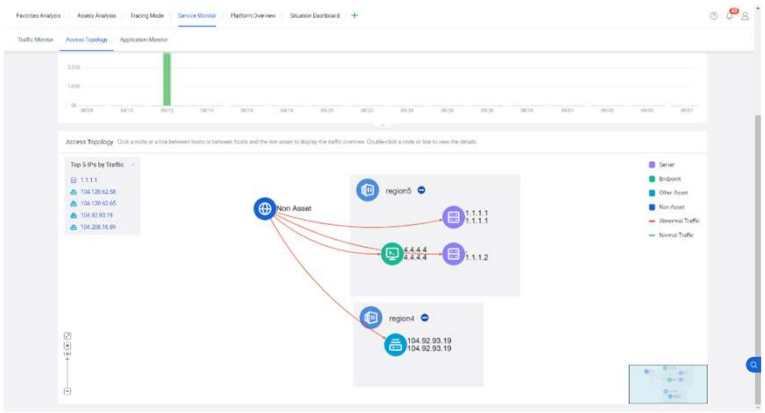
Collect traffic data from the netflow and metadata of BDS

Traffic monitoring enables security analyst to detect network anomalies

Traffic Insight

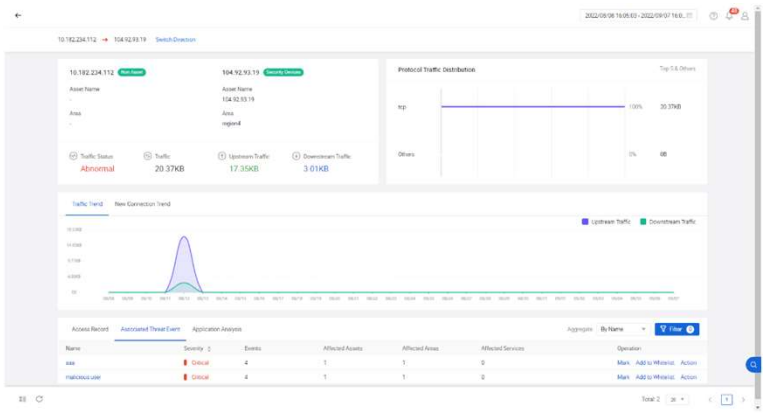
Traffic Insight Topology

- 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:

Visulized 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

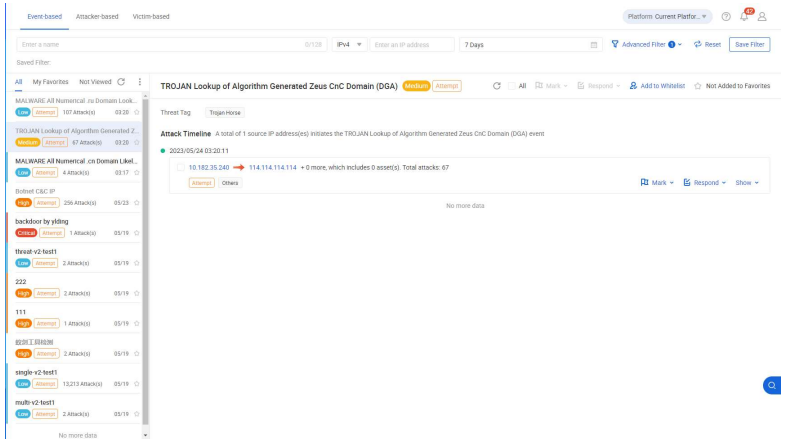
Threat Aggregation

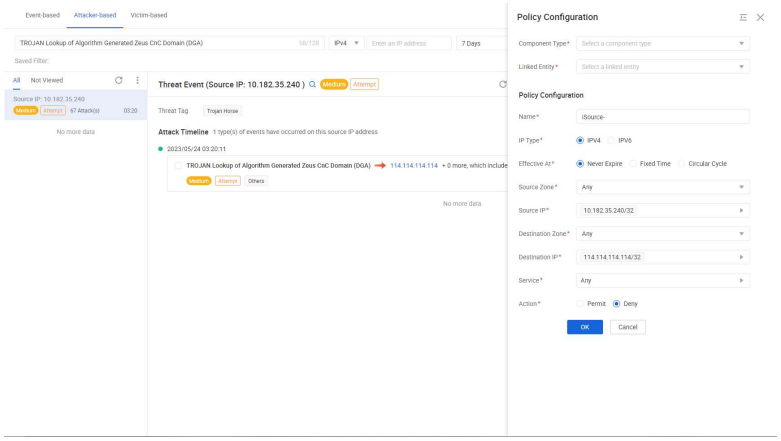
Threat Aggregation

- 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

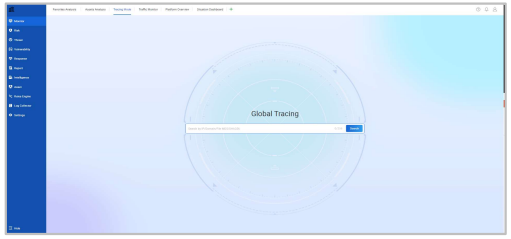
- Support batch marking and remediation of the aggregated threat events
- Remediation includes policy configuration and IP block configuration



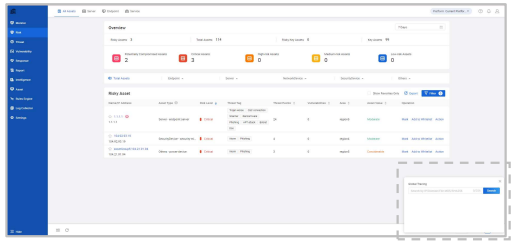


Forensics

Global Search



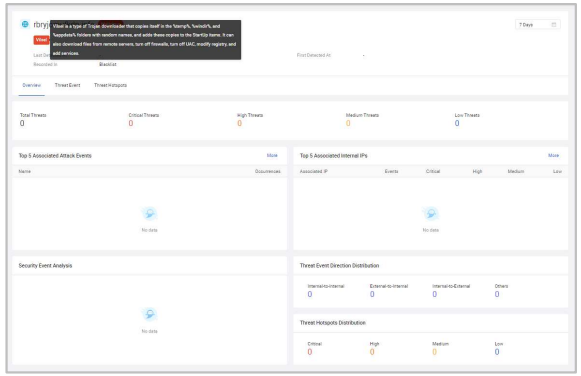
Primary entry



Quick entry

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

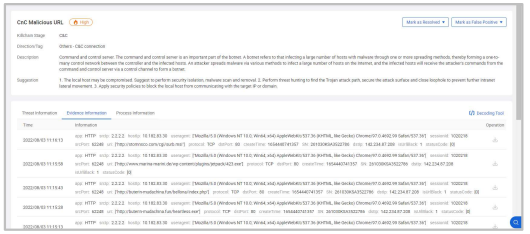
Info Display



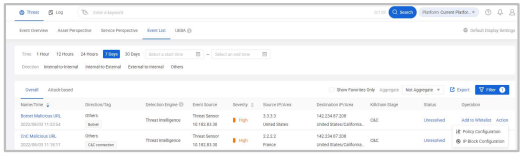
Info display

- 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



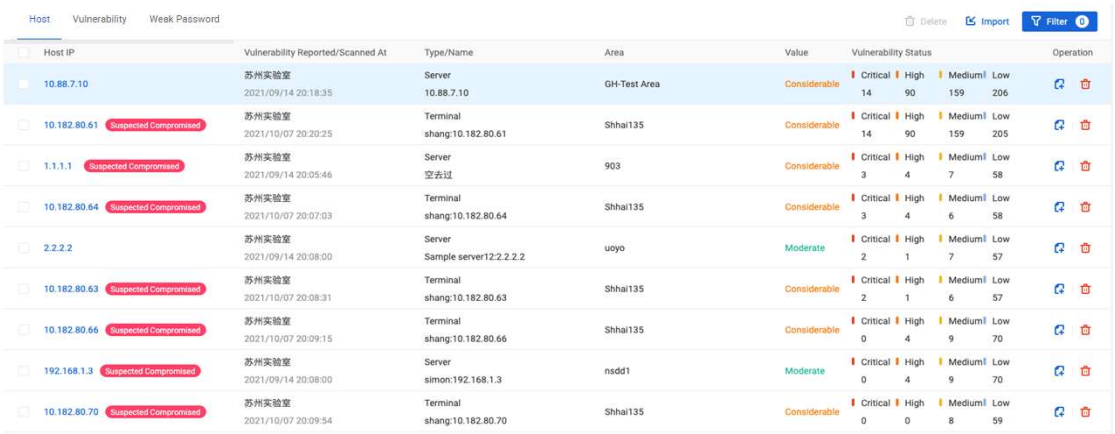
Incident Response

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

Vulnerability Analysis

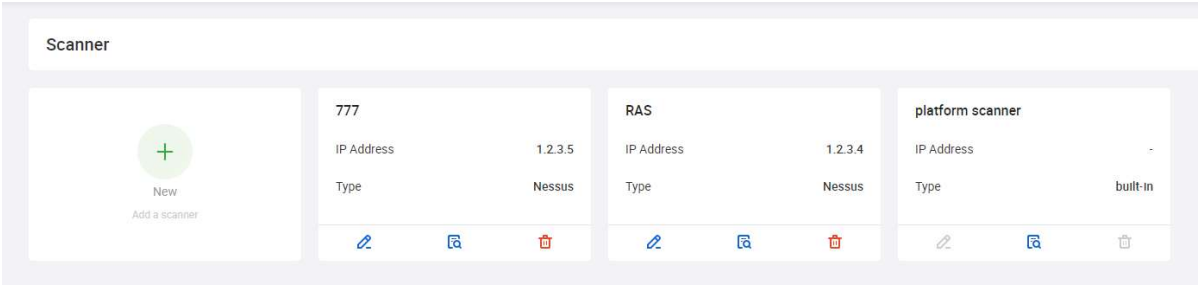
Vulnerability Visualization

- 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

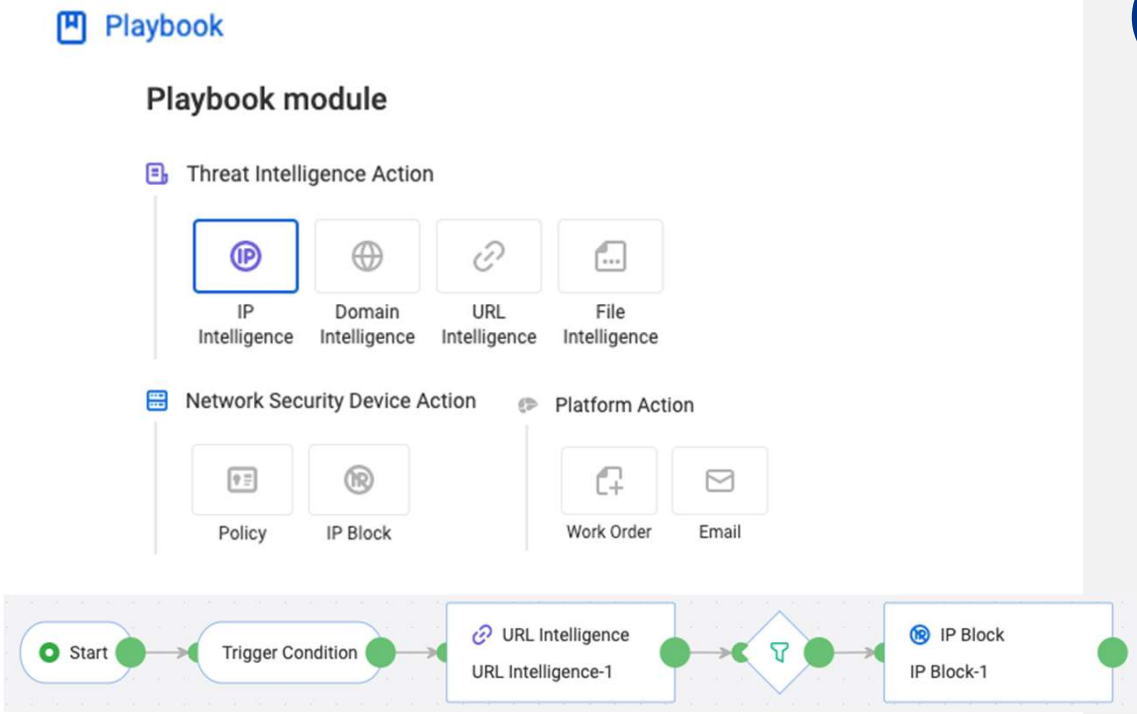


Scanner Management

- 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)



Automated Security Orchestration

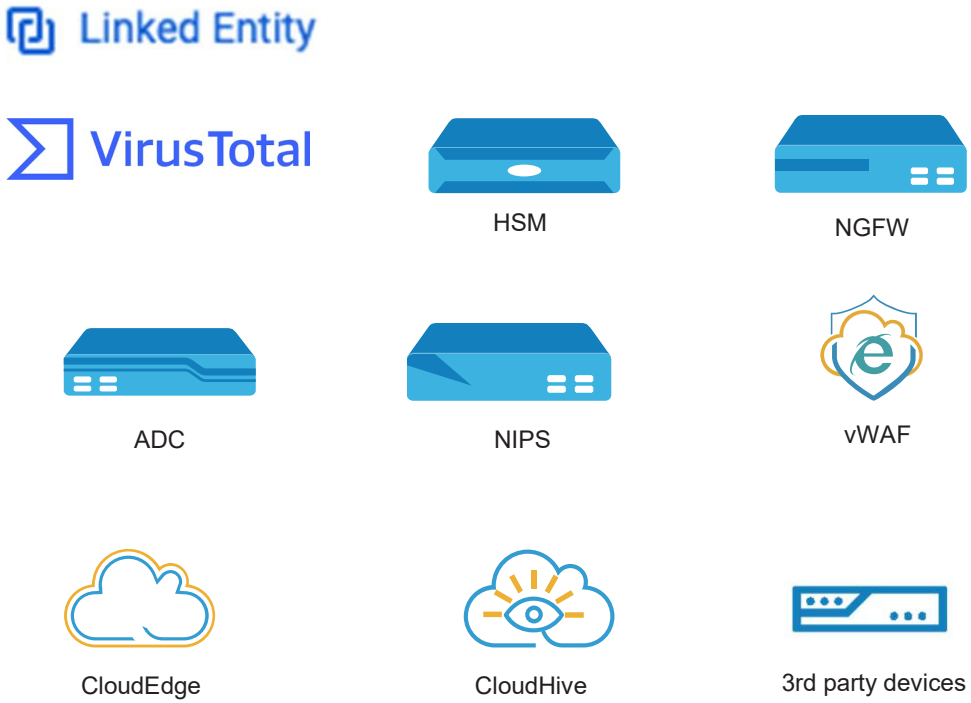


Automated Orchestration

- 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

Threat Responses – Integrated Devices

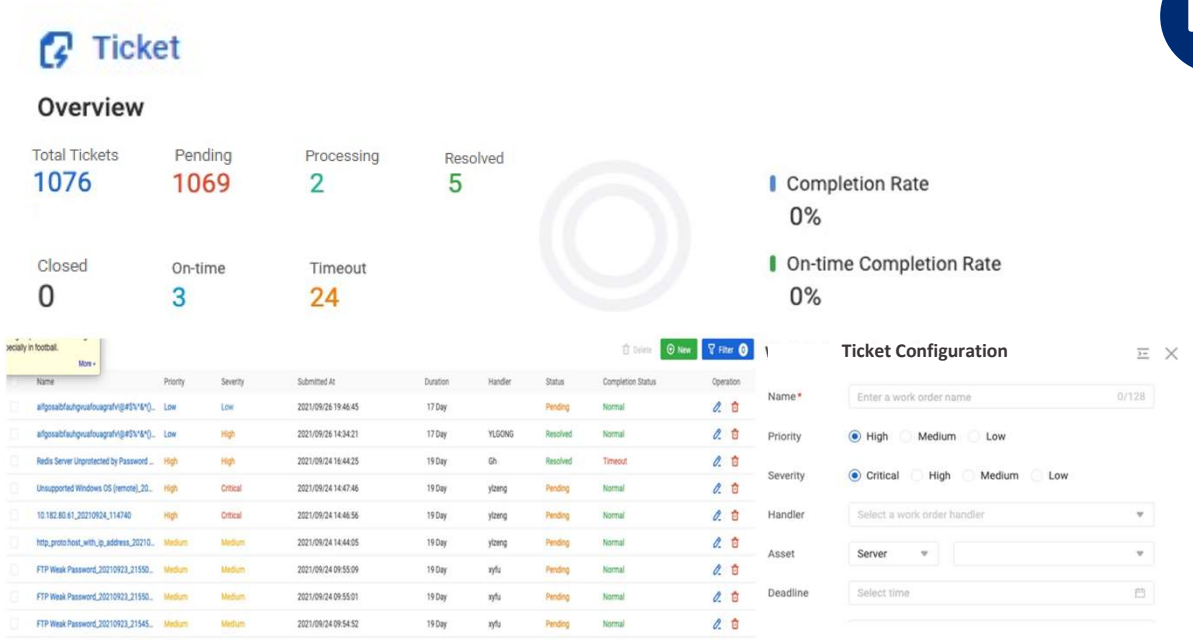
Hillstone NETWORKS



Integrated Devices

- Register integrated products
- Interact with intellgence 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



Case Management

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

Risk Management

Asset Centric Risk Management

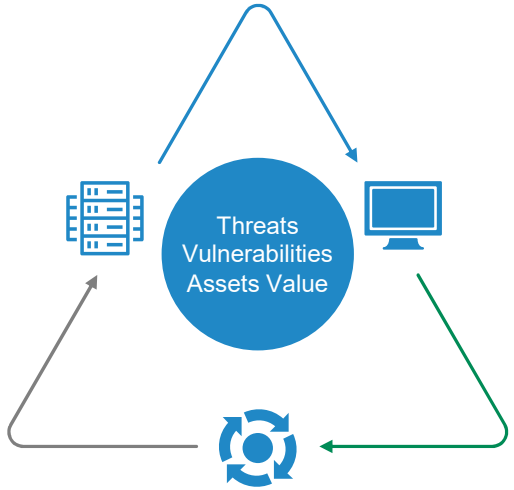
Server Risks

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

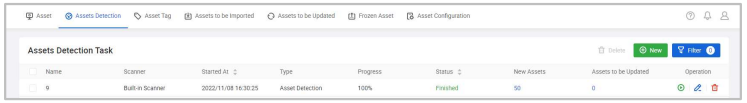
- Total risks/distributions/trends
- Threat distribution/trends
- Vulnerability distribution/trends

Endpoint(s) risk details

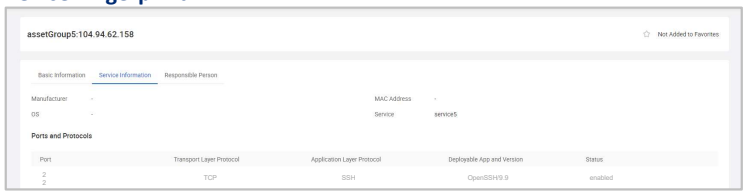
- Risk reports
- Vulnerabilities
- Threat events
- Report of compromised assets

Assets Management

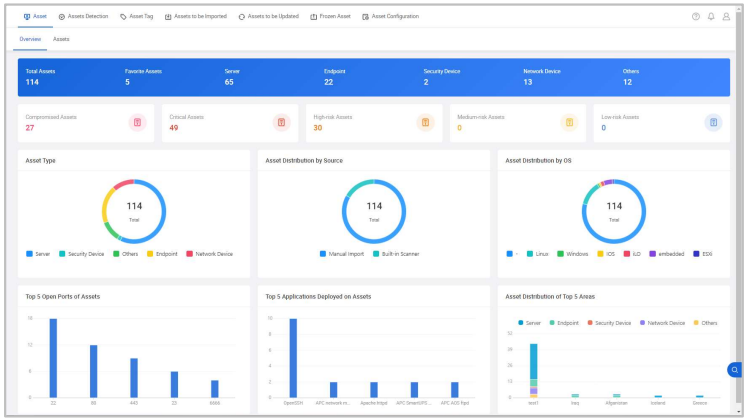
Asset Detection

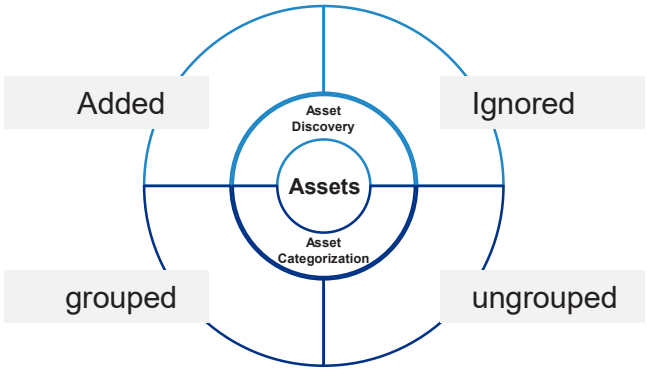


Device Fingerprint



Asset Overview

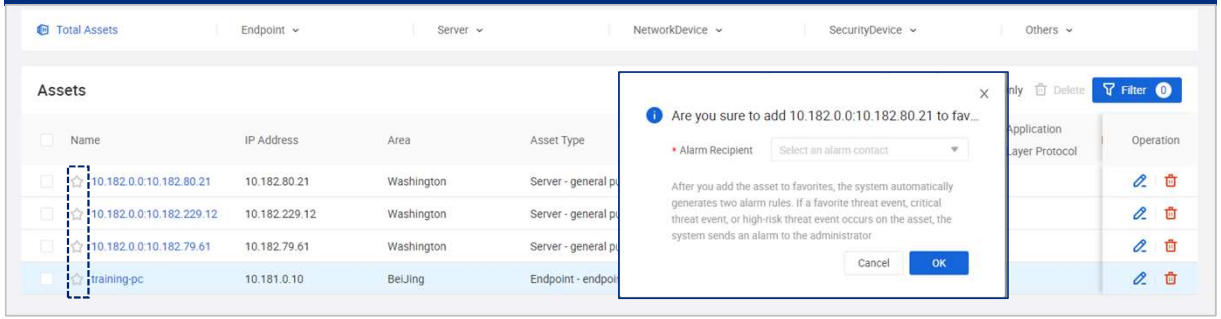




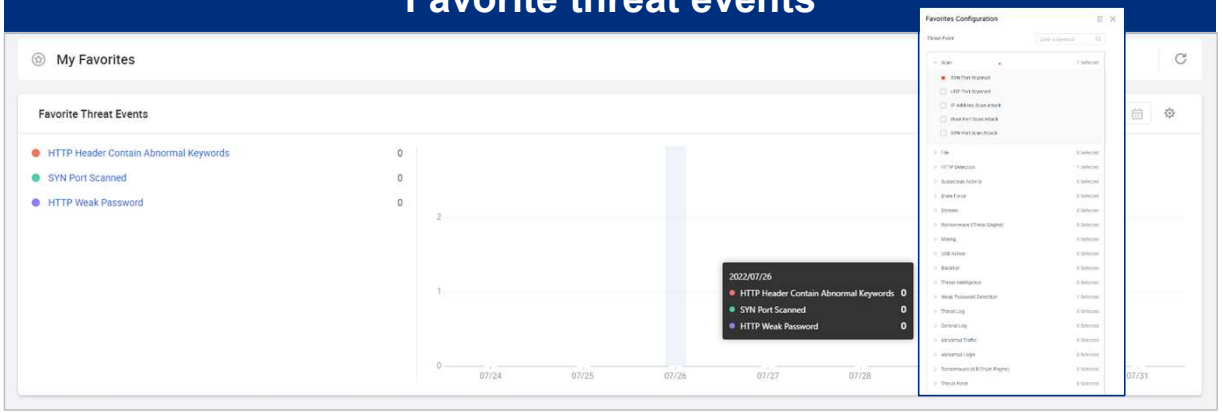
Asset Discovery	Grouping	Lifecycle Management
Discover assets via: • Traffic • Logs • Threat events • Vulnerability report • Manual import • Active scan	**Grouping as:** • Servers • Endpoints • Network devices • Security devices • Others	• Asset export • Template based import • Asset offboarding

Favorite Asset and Threat Event Management

Favorite Assets



Favorite threat events



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 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

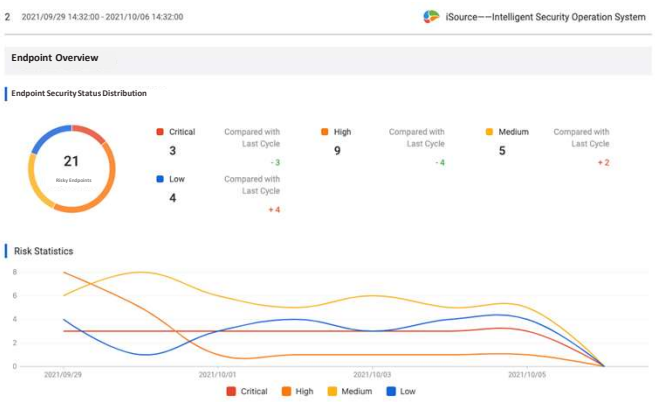
- List all reports
- Support live view
- Support export report in PDF
- Support manual export for customizable queries

Report Task

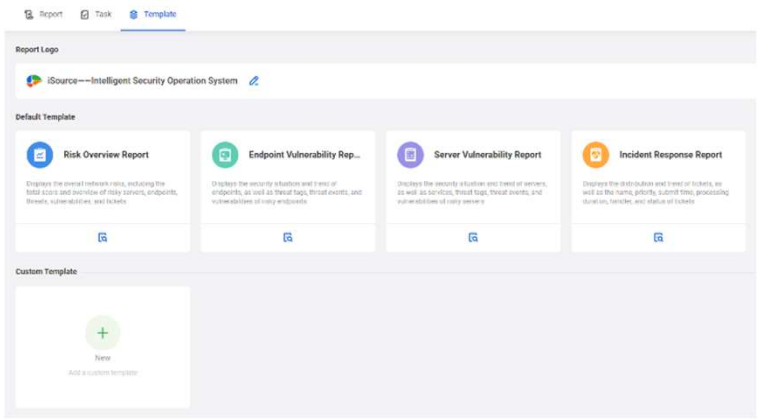
- Generate reports periodically (daily/weekly/monthly)
- Overview or detailed reports

Report Template

- Multiple pre-defined templates
- Customizable templates



A page of summary report



Rich report templates

XDR Eco-System

3rd Party Log Integration

Log Parsing Configuration Database

Up-to-date pre-defined configurations of log parsing

01

02

Custom Log Parsing Configuration

Define your own log parsing configuration, include one or multiple log parsing templates and applicable models

Log Parse Template

Define log parsing workflow for a specific type of log of a specific model

03

04

Threat Log Standardization

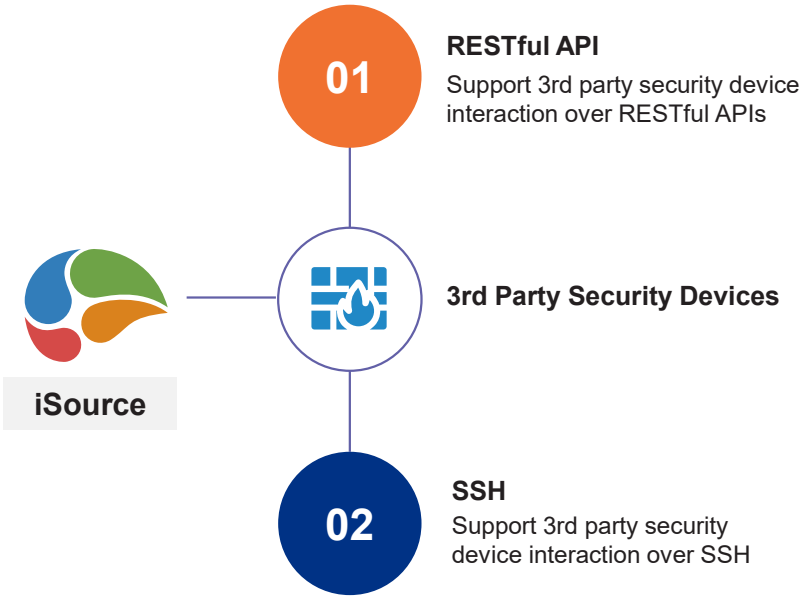
Transform 3rd party logs to Hillstone standard log format

Log Parse Rule

Associate log parsing configurations that will be applied to the range of devices that generate 3rd party logs

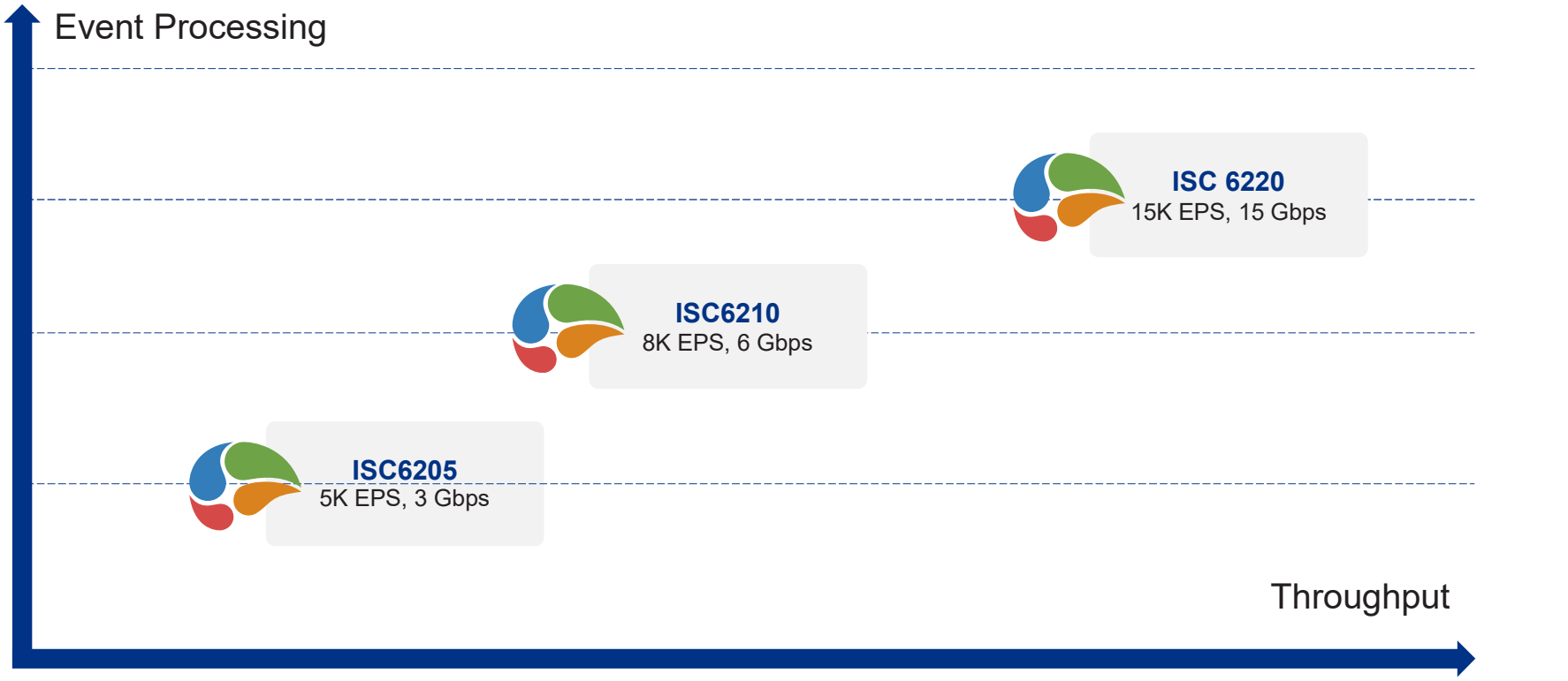
05

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

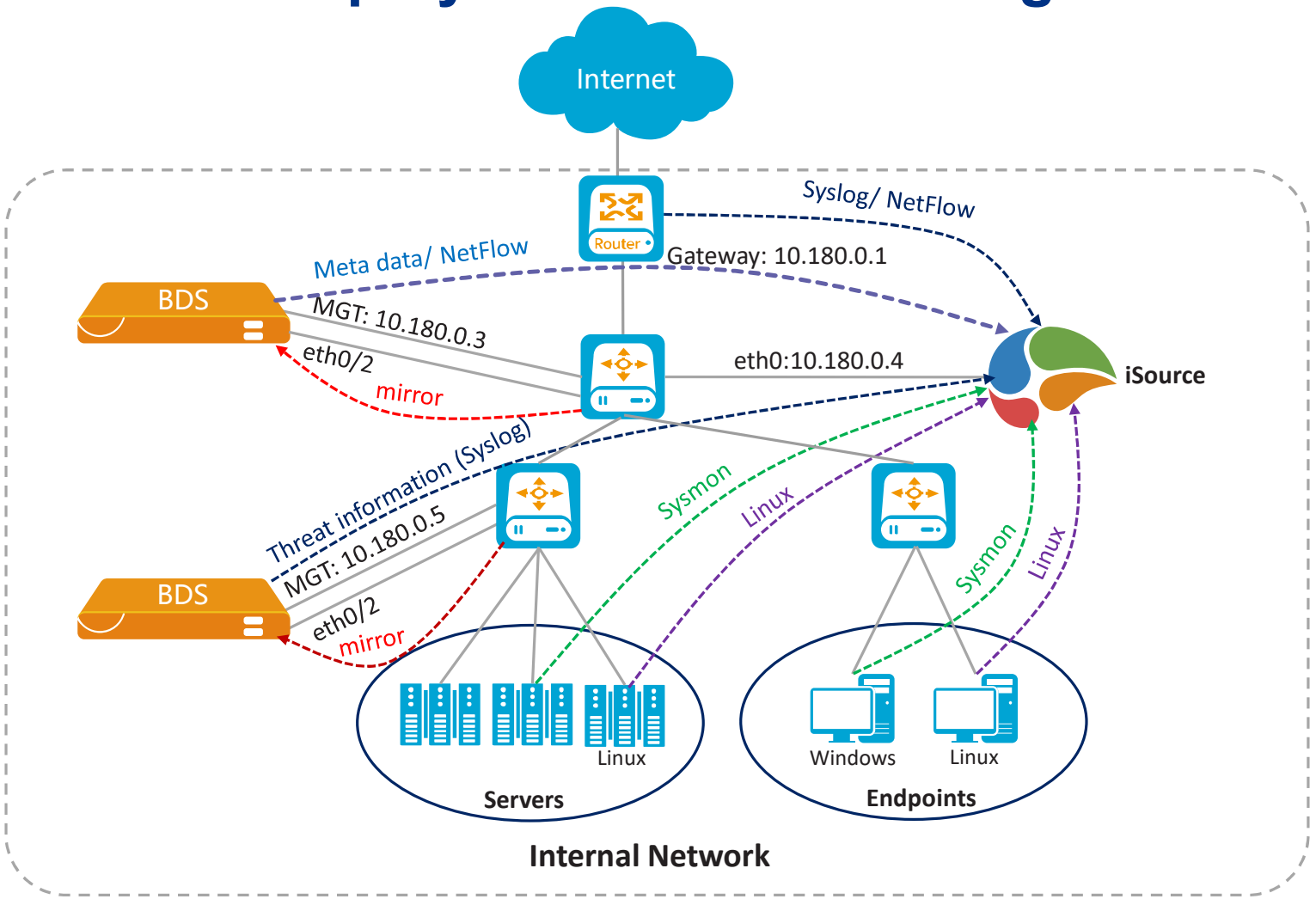
Models		SG-6000-ISC6205	SG-6000-ISC6210	SG-6000-ISC6220
Performance	Throughput	3Gbps	6Gbps	15Gbps
	Event Processing	5000EPS	8000EPS	15000EPS
Minimum Hardware Configuration	CPU	20 cores (64bits)	24 cores (64bits)	48 cores (64bits)
	Memory	128G	128G	256G

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

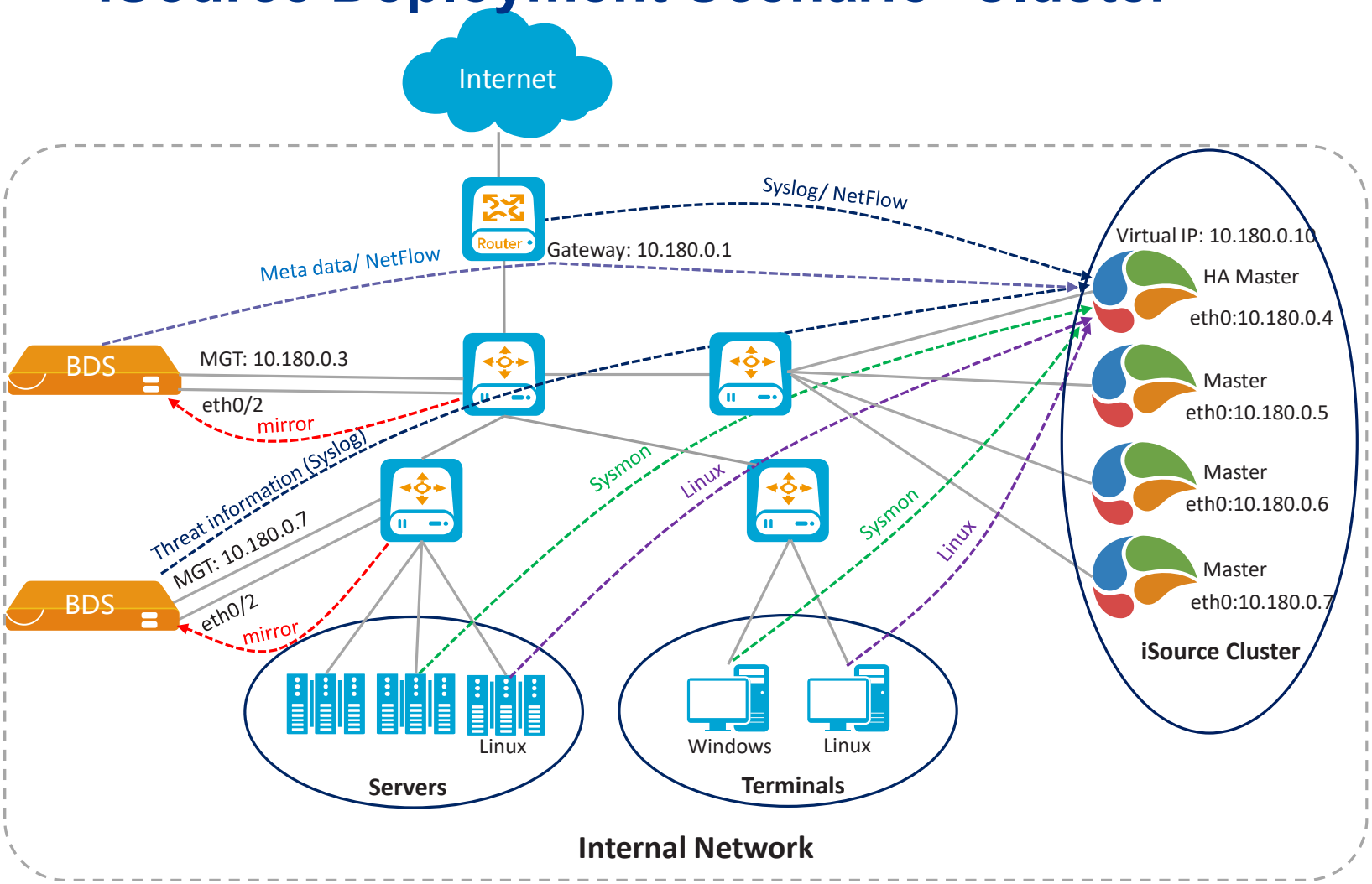
iSource Deployment Scenario- Single Node



Single Node Deployment

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

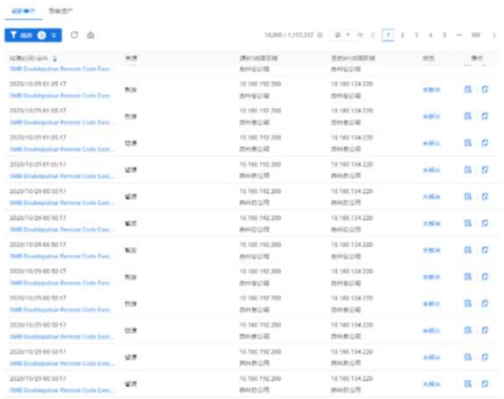
iSource Deployment Scenario- Cluster



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



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.

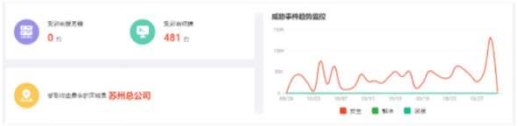
02 The domain controller server of domain B was then compromised because ofa weak password. All the credentials were compromised.

03 All the servers in domain B were logged into centrally and executed the ransomware.

04 Eliminates anti-virus software using PC Hunter.

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

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

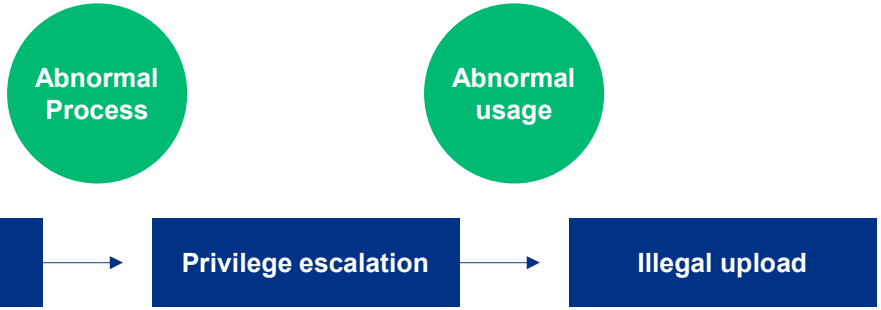
02 Discover and analyze the compromised hosts and take them offline

03 Install MS17-010 patch to all internal hosts

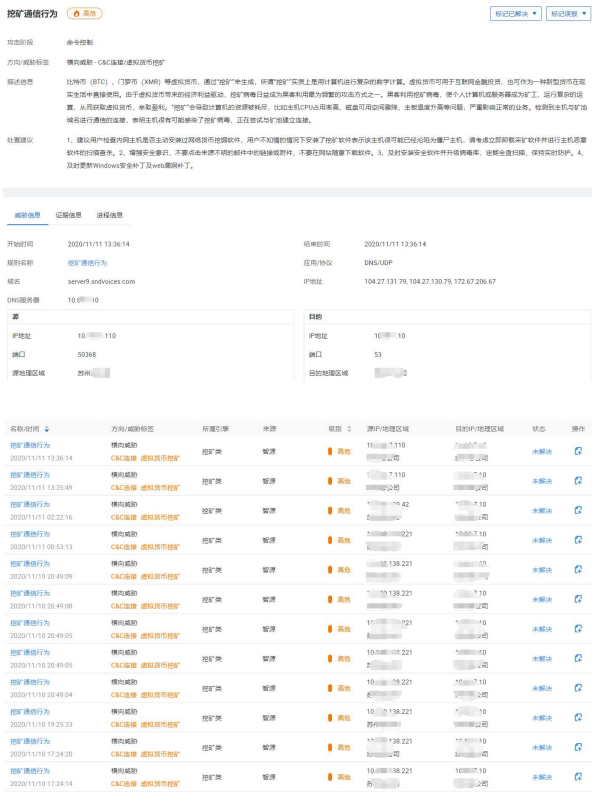
04 Collect relevant data to build a solution in the future.

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.



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

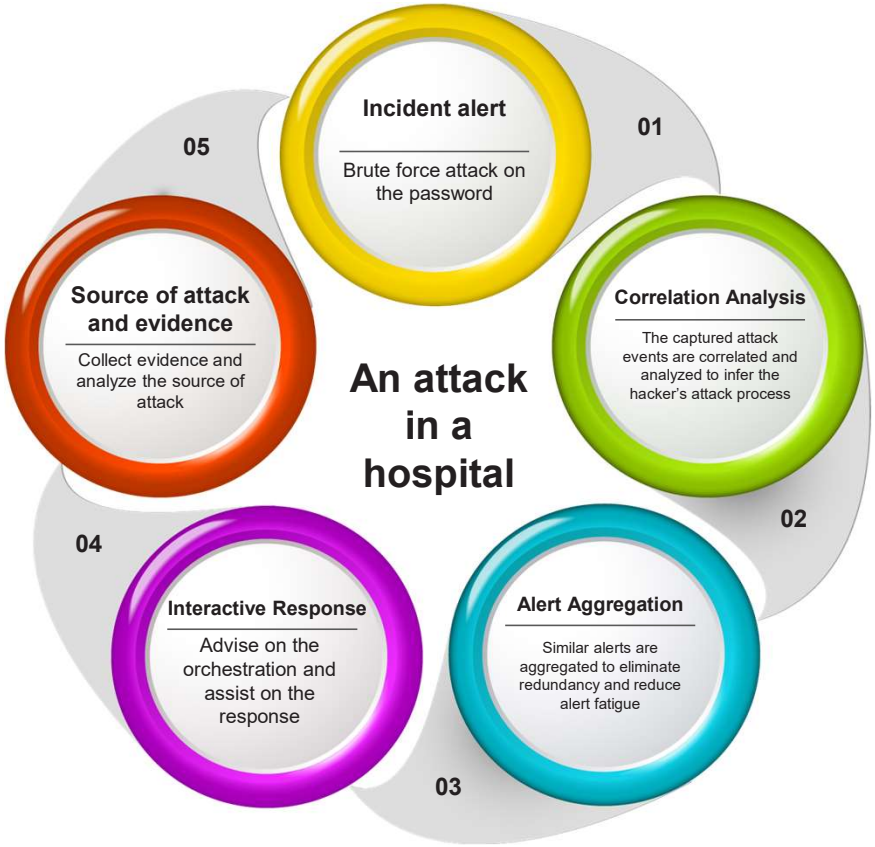
Characteristics

Attack event, request, target, path, content etc.

Interactive Response

Interactive response based on the security orchestration:

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.

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.*

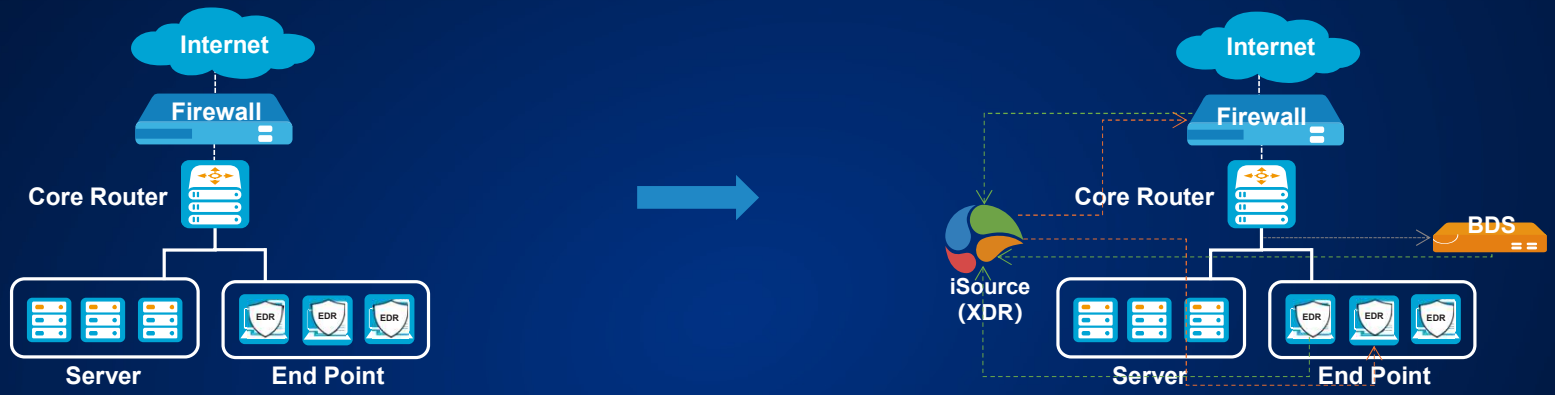
Alerts & Notification

Alert and Notification

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



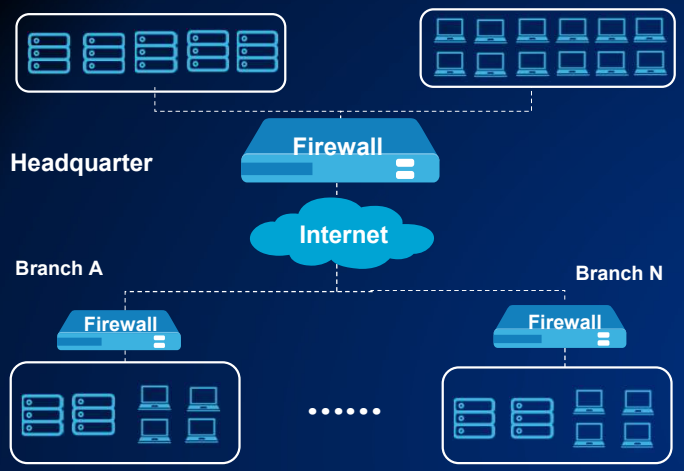
Customer Pain Points

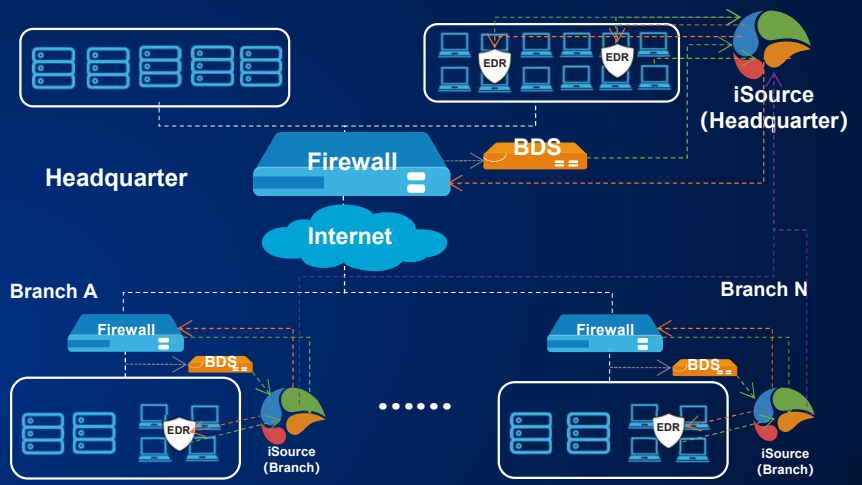
- The customer had perimeter security devices in place, but they faced difficulties in effectively analyzing and mitigating threats within their Intranet environment;
- Although the firewall could detect threats that breached the perimeter, the dynamically assigned IP addresses of endpoints through DHCP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





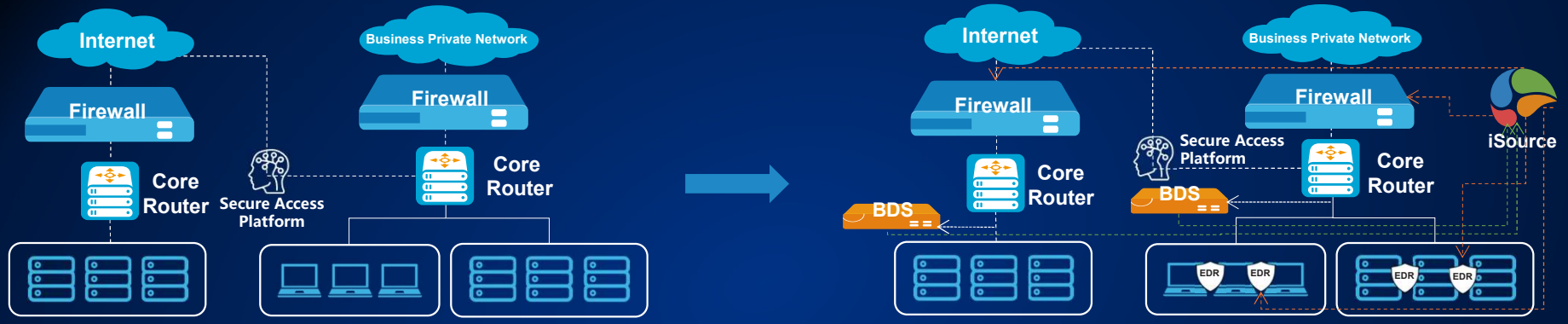
Customer Pain Points

- 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.

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.

Hillstone NETWORKS

Integrative
Cyber
Security

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