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 Network Intrusion Prevention System (NIPS) S-Series

Integrative Cybersecurity

Visionary. AI-powered. Accessible.

Agenda

- Business Problem
- Hillstone NIPS Value Proposition
- Hillstone NIPS Portfolio
- Deployment Scenarios & Winning Cases

1 Business Problem

High-risk Vulnerabilities Emerge Explosively

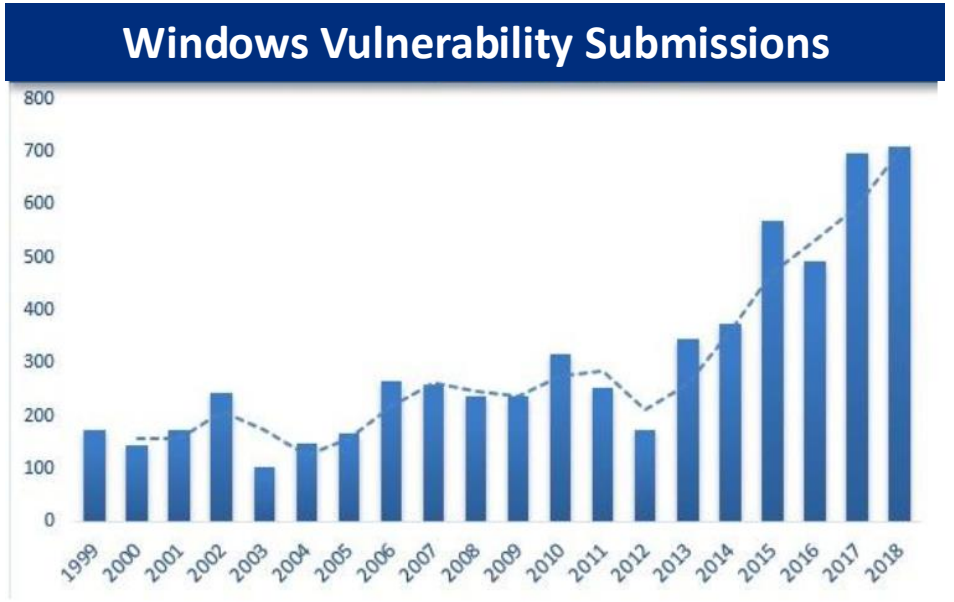
Heartbleed Bug

Shellshock Bash Vulnerability

Java Deserialization Vulnerability

IIS 7 HTTP.sys

Redis Unauthorized Access Vulnerability



The number of vulnerabilities submitted for the Windows operating system has entered an explosive growth trend

IDPS is Even More Relevant in Today's Network Security Landscape

- Dedicated IDPS
- Layered defense
- High performance levels with sustained throughput
- For internal network segmentation
- IDPS solution from different vendor

- 85% of new stand-alone IDPSs will be in data centers (cloud or on-premises).
- More than 40% of new IDPS deployments are not on the perimeter. Gartner believes that, by YE21, 80% of new stand-alone IDPSs will be deployed for internal use cases, up from about 40% in 2018

Market Guide for Intrusion Detection and Prevention Systems | 1 July 2019

Stand-alone IDPS solutions are ideal when you need improved blocking and performance

When Do You Use an IDPS Versus an NGFW?

Intrusion Detection and Prevention System

- When Best-of-Breed protection is desired
- When different staff manage the IPS from the firewalls
- When high-performance throughput is required
- To enable network segmentation on parts of the internal network
- As an IDS solution on parts of the internal network

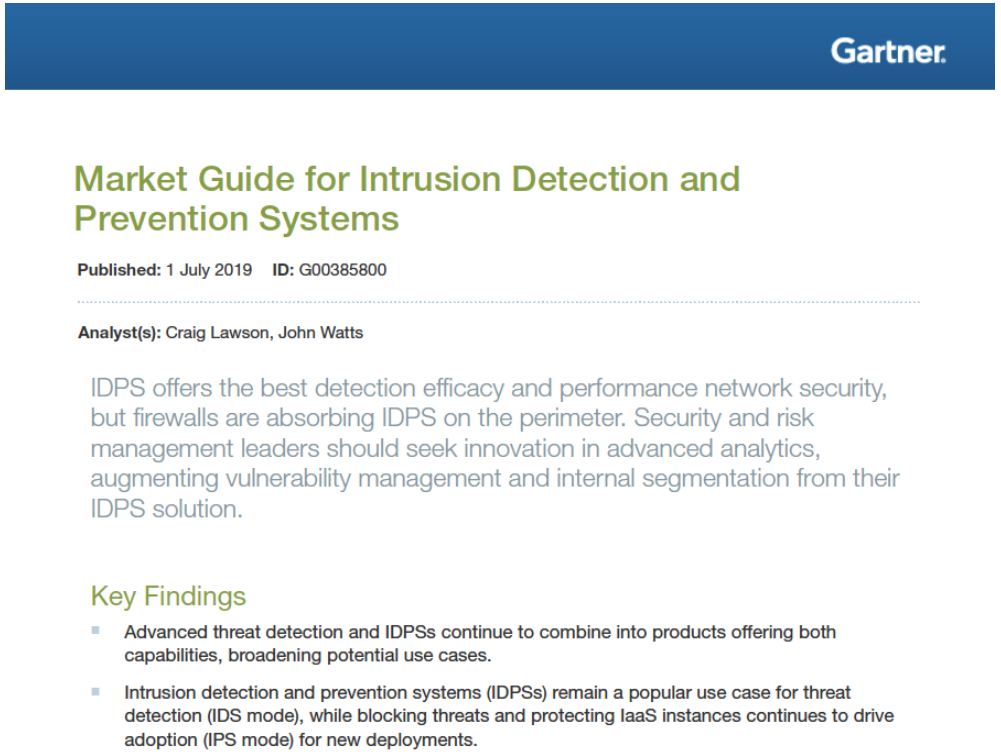
Next-Generation Firewall

- When a single view of network threats is required
- When performance and throughput is not a priority
- When application awareness is required (traffic visibility and control)
- When malware monitoring is a requirement
- When user identity awareness is required

2

Hillstone NIPS Value Proposition

Hillstone is Representative Vendor in Gartner Market Guide for Intrusion Detection and Prevention Systems



Gartner.

Market Guide for Intrusion Detection and Prevention Systems

Published: 1 July 2019 **ID:** G00385800

Analyst(s): Craig Lawson, John Watts

IDPS offers the best detection efficacy and performance network security, but firewalls are absorbing IDPS on the perimeter. Security and risk management leaders should seek innovation in advanced analytics, augmenting vulnerability management and internal segmentation from their IDPS solution.

Key Findings

- Advanced threat detection and IDPSs continue to combine into products offering both capabilities, broadening potential use cases.
- Intrusion detection and prevention systems (IDPSs) remain a popular use case for threat detection (IDS mode), while blocking threats and protecting IaaS instances continues to drive adoption (IPS mode) for new deployments.

"ABD is Hillstone's analytics approach that does network baselining, looking for abnormal behavior.

The sandbox is also interesting for the IDPS market because it allows for "fuzzy" malware behavior signatures to be used to help convict new iterations of existing families of malware."

Source: Gartner (July 2019)

Hillstone NIPS – A Comprehensive Network Intrusion Prevention System

New Hardware Platform

01 Complete Network Threat Detection and Defense

06 Easy Deployment with Minimum Network Interruption

05 Simplified and Centralized Management for Efficient Security Operation

02 Advanced Threat Protection Throughout the Threat Lifecycle

03 Better Understanding with Rich and Granular Reporting

04 High Reliability to Ensure Reliable Operation of the Network

High Performance of SSL Encrypted Traffic

Improved hardware acceleration capability of SSL decryption

- HTTPS traffic increasing
- New attacking methods
- Key security requirements

NIPS provide comprehensive threat protection to SSL encrypted traffic through built-in encryption/decryption module

Lower cost

With SSL decryption hardware acceleration capability

Security and visibility

Provide detection of systems, applications, malware and clients

Massive Processing Guarantee

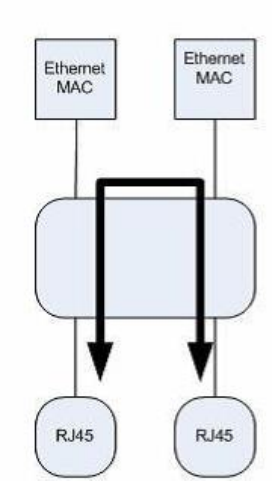
High performance application layer throughput

01 High-density interface
S5500-IN comes with 8×GE (4 pairs of bypass) + 16×SFP+ + 2 x QSFP+ fixed I/O Ports

02 Most models support expansion slot

03 Support optical/electrical interface hardware bypass

04 Built-in large-capacity storage, storage can be expanded on demand



Fully support bypass, guarantee the business continuity in serial deployment

Context-Aware Detection

User awareness

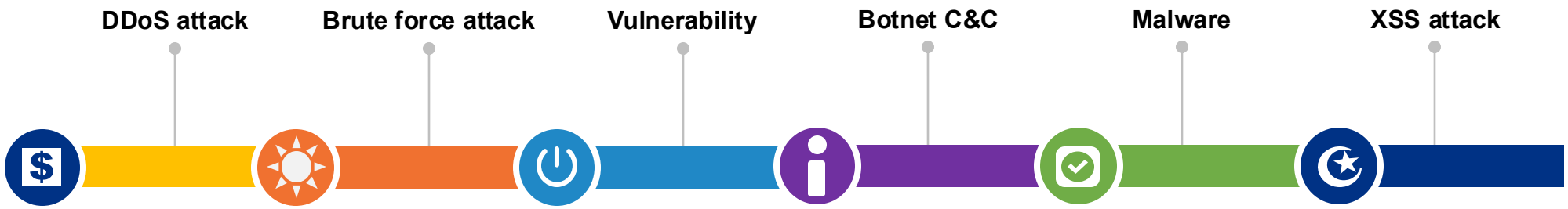
Accurately identify defined and undefined users, and analyze user traffic and concurrent connections

Application awareness

Accurately identify 3000+ network applications, hundreds of mobile/cloud applications, including applications with SSL encrypted traffic

Risk awareness

Provide multi-dimensional information including risk level, known vulnerabilities, large bandwidth consumption, file transfer behavior



Nearly 10,000 intrusion rules and tens of millions of virus signature database to detect and prevent different attacks

Advanced Threat Protection Throughout the Threat Lifecycle

Hot Threat Intelligence Proactively avoid threats

IPS blocks vulnerability exploitation

IP Reputation blocks risky IPs from accessing servers

URL Filtering controls user access to specified websites

Anti-Virus prevents users from visiting malicious sites and phishing sites

Anti-Spam classifies and prevents potential spams

Anti-Virus responds to known viruses

Cloud Sandbox responds to unknown viruses

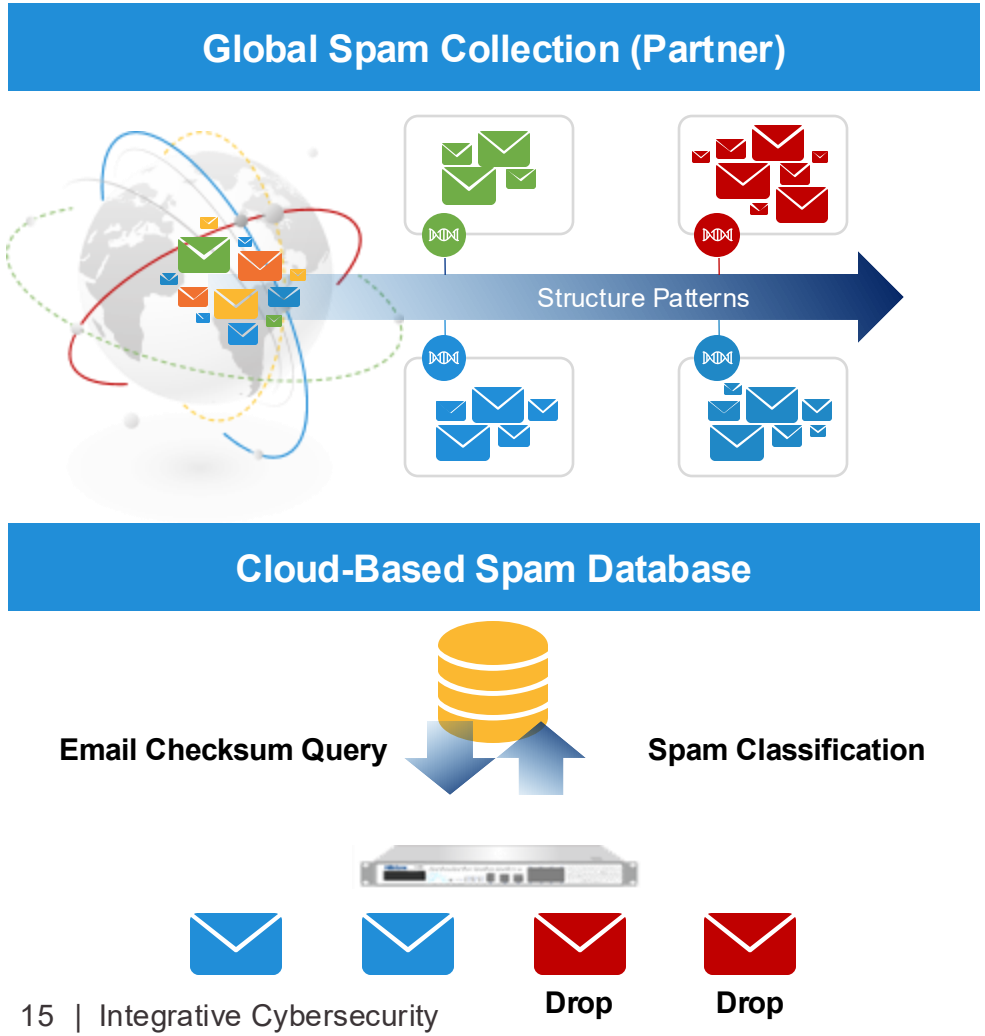
Botnet C&C Prevention blocks the control channel and catches intranet bots

Pre-breach → **Breach** → **Post-breach**

Intrusion Prevention | **IP Reputation** | **URL Filtering** | **Anti-Spam** | **Anti-Virus** | **Cloud Sandbox** | **Botnet C2 Prevention**

Works in conjunction with Hillstone NGFW

Anti-Spam for Real-time Spam Classification and Prevention

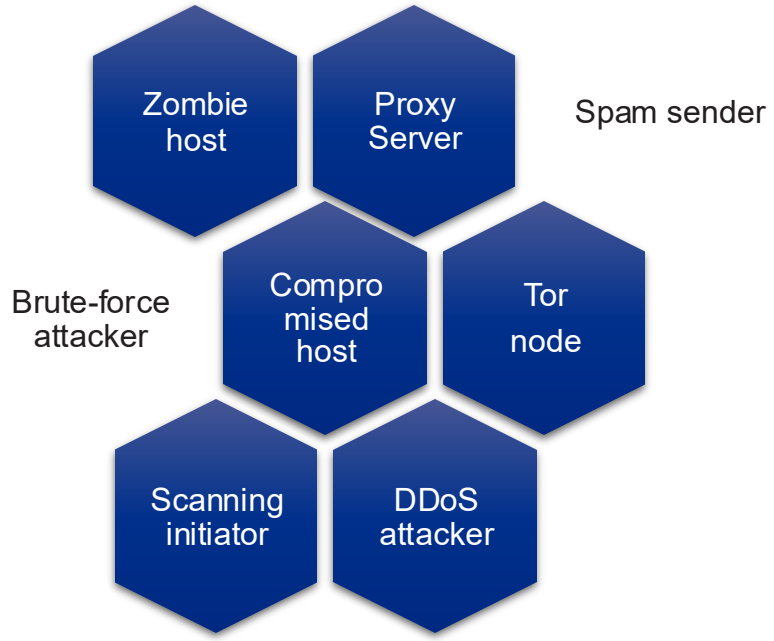


Key Features

- **Real-time Spam Classification and Prevention**
- Supported Spam classification: Confirmed Spam, Suspected Spam, Bulk Spam, Valid Bulk
- **Support encrypted traffic spam detection**
- Regardless of the language, format, or content of the message
- Works on both SMTP and POP3 email protocols
- Inbound and outbound detection
- White lists to allow emails from trusted domain

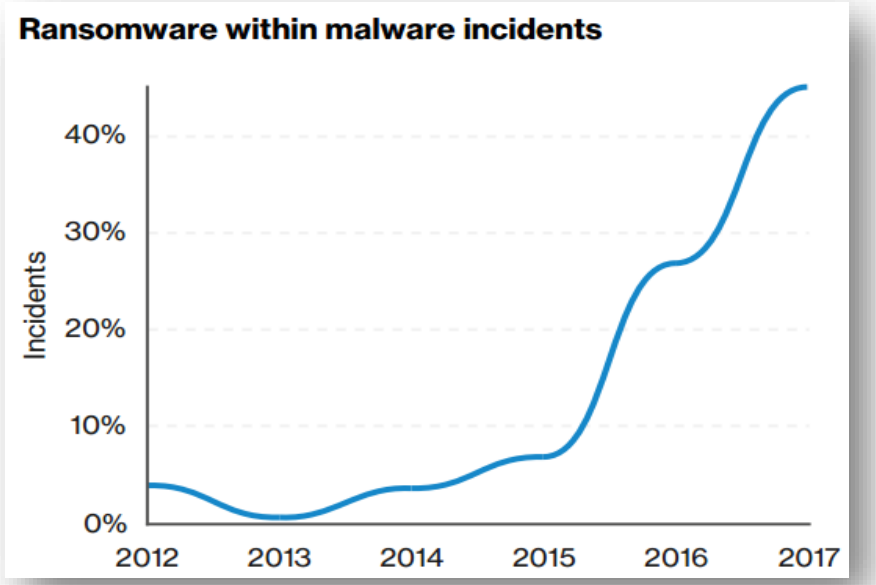
IP Reputation – Multiple Risk IP Identification and Blocking

- IP Threat Intelligence: record all types of risky IP traffic logs and block risky IP access to the intranet
- Multiple risk IP identification: zombie hosts, spammers, etc.
- Update IP reputation signatures every hour to get the latest features of IP threat intelligence



Virus Filtering Service – Effectively Detects and Blocks Ransomware

- **Efficient flow detection engine:** performance of single device protection against virus up to 24Gbps
- **Tens of millions of virus signatures:** daily real-time update to effectively detect and block all types of malware
- **Effective ransomware protection :** effectively detect and block the spread of malware and ransomware, filter and block virus of files transferred with SMB protocol when resuming from breakpoint



Ransomware events are growing rapidly; protection measures against viruses are essential

Cloud Sandbox for Malicious File Detection and Prevention

Static Analysis/ Pre-Processing

- URL whitelist, file signature verification
- Cloud-based suspicious samples
- MD5 query for file behavior; verification and report

Behavioral Analysis

- Windows/Android/MacOS simulation
- Behavioral analysis to file process, Registry action, network behavior
- Evasion detection

Cloud Intelligence

- Identify malicious files
- Generate threat log and report
- Share threat intelligence
- Block threats

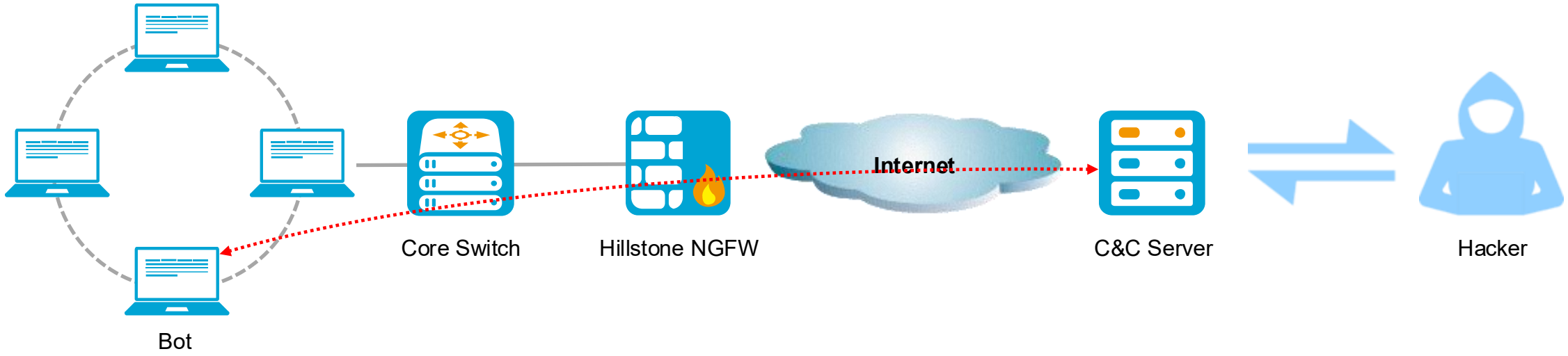
Malicious Files

Reporting

Signature Update

NGFW

Complete Botnet C&C Prevention



C2 Address Database

DNS Sinkhole Detection

DNS Tunnel Detection

DGA Domain Detection

AI Technology Enables Intelligent and Efficient Threat Protection

Encrypted Traffic Detection

- Leverage AI technology to analyze and detect encrypted traffic without decryption

Improve the efficiency and accuracy of abnormal encrypted traffic detection

Intelligent Anti-DDoS

- Auto-configuration for flood protection threshold via ML-based baseline establishment

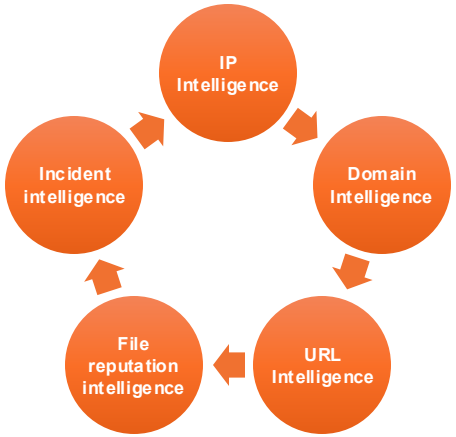
Accurate and effective DDoS protection with automated configuration

Domain Generation Algorithm (DGA) Detection

- Build, train, and real-time update the detection model

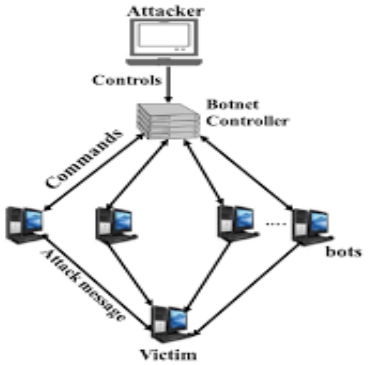
Better defend against unknown threats with higher effectiveness

Unknown Threat Mitigation



Internal intelligence: FW, IPS, WAF, cloud sandbox, traffic collection, CloudView

External intelligence: business intelligence, open source intelligence



Rich threat intelligence data

Prevention in advance

Before attack:

Hot threat intelligence is actively pushed to prevent threats in advance.

Multi-source intelligence integration

Continuous Enablement

In attack:

Enabling security device to improve threat detection capabilities.

Intelligence based threat mitigation

Minimization of threat

After attack:

Under the help from the intelligence, the NIPS could detect the compromised hosts and help mitigate the threat.

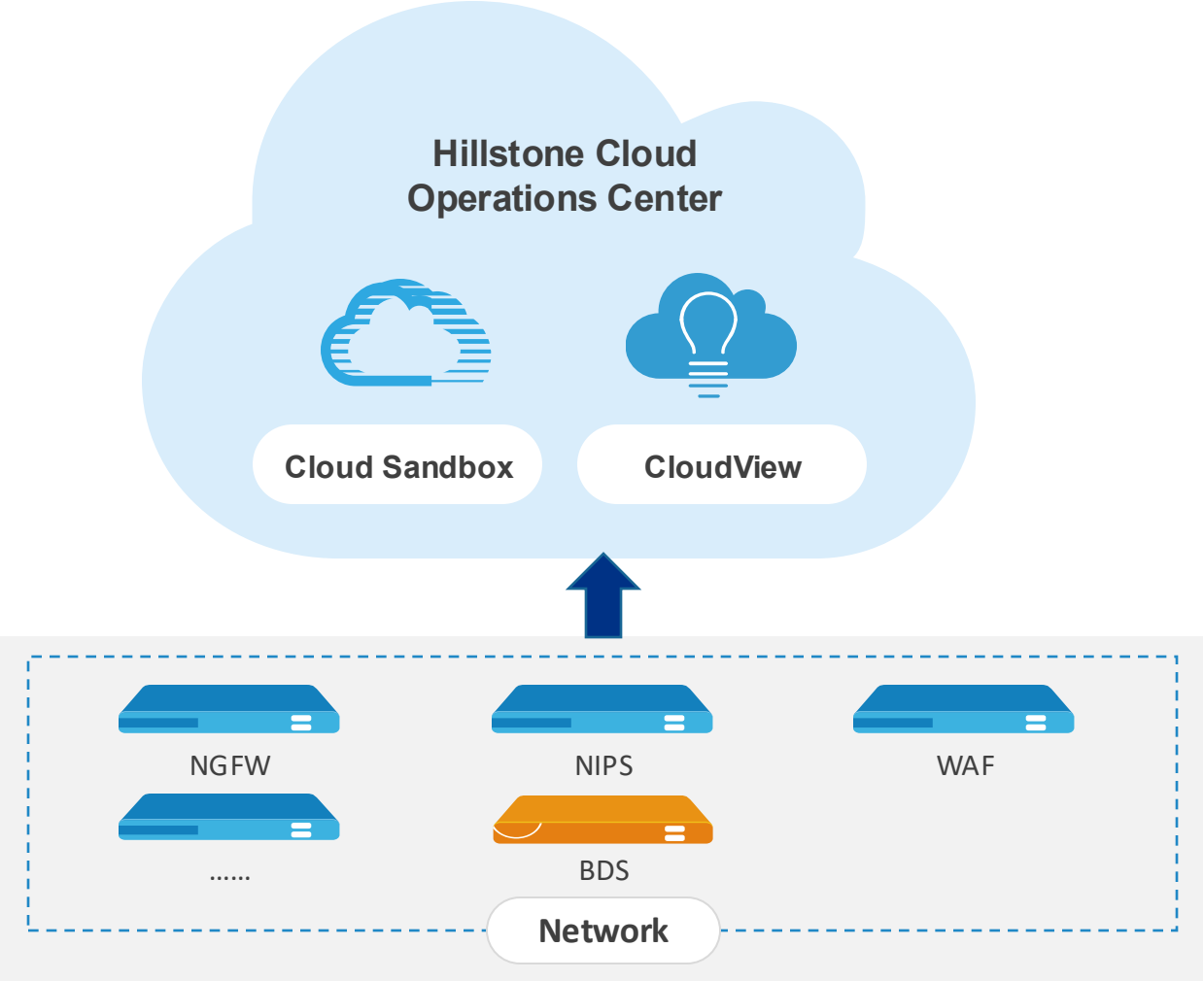
Cloud-Based Intelligence Interaction

Support linkage with Hillstone's firewall, CloudView, HSM, HSA

01 **Hot threat monitoring**

02 **Incident handling**

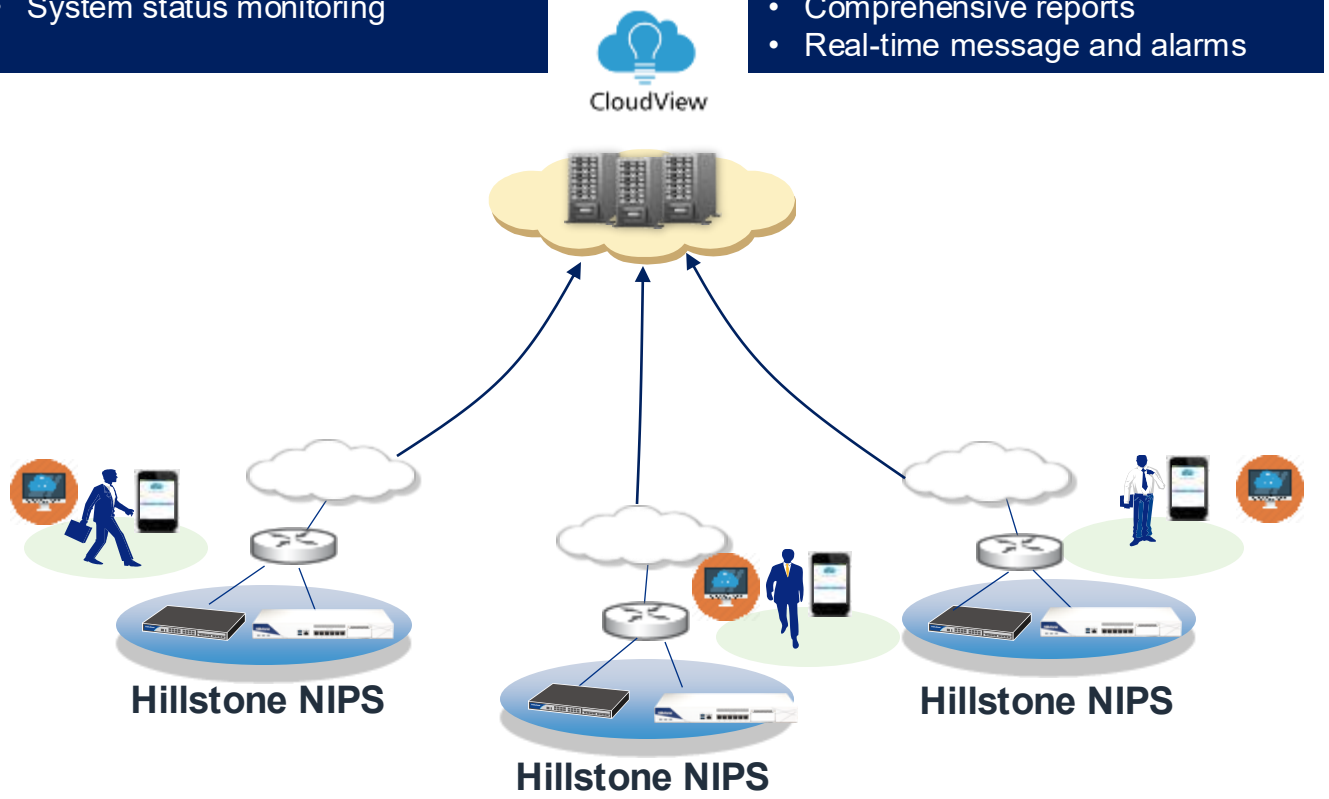
03 **Signature update**



Cloud-Based Security Monitoring & Analytics

Centralized Threat Monitoring
- Threat monitoring
- System status monitoring

Threat Analysis and Alarm
- Threat and event logs
- Comprehensive reports
- Real-time message and alarms



Real-time Monitoring

- 24/7 monitoring and alerts
- Threat analysis and reports
- Mobile/web access

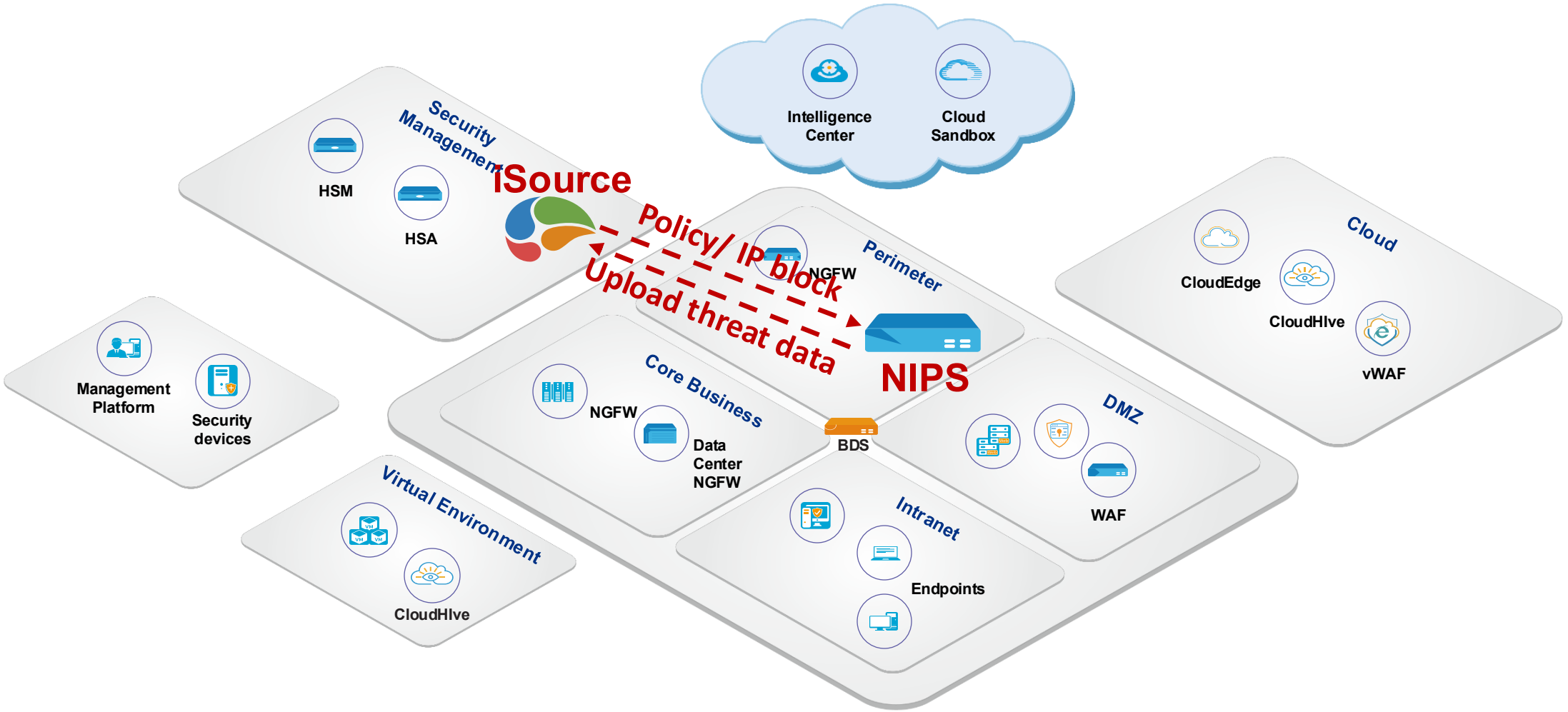
Ease of Deployment

- No deployment required
- No maintenance
- Easy and instant subscription

Low/Flexible Investment Options

- Free to initiate (Includes essential features)
- Pay to subscribe (For advanced features, Professional Version)
- Security as a Service (SaaS)

Integration with Hillstone XDR



NIPS uploads threat data (threat event / forensic Pcap) to iSource, strengthening correlative threat analysis

Better Understanding with Rich and Granular Reporting

IPS Reporting System

Network Traffic Analysis
The health status of traffic

Application and Risk Assessment
Application status and risk of the core assets

System Operating Status
Display of system hardware and computing resources

Security Risk Overview
Comprehensive display of the security risks and their importance

Threat Assessment
Attacks and abnormal behavior

Reports based on User Profile

Management/C-levels, Application Owners, Network Security Administrators

High Reliability to Ensure Reliable Operation of the Network

Reliable system
Safe and stable operating system, Hillstone StoneOS

Reduce hardware failures with reliable components
Stable hard drive
Redundant power supply

Stable device with real-time device status monitoring
Monitors CPU/memory utilization, processes, Network port status, Threat information, etc.

High reliable networking
Supports AP / AA mode

Bypass deployment guarantees business continuity
Provides default bypass pairs
Supports expansion of bypass interfaces

Efficient Security Operation: Smart Policy Operation

Automated User Policy Deployment
Radius Dynamic Authorization
Automatically issue user policy via CoA message

Policy Redundancy Check
Discover redundant policies for deletion

Policy Analysis
Adjust the policies by observing the hit counts and hit trends

Policy Group
Efficient policy management based on business requirement

Aggregate Policy
A set of policies act as one single policy

Policy Assistant
Refine a general policy into detailed policy

Easy Deployment

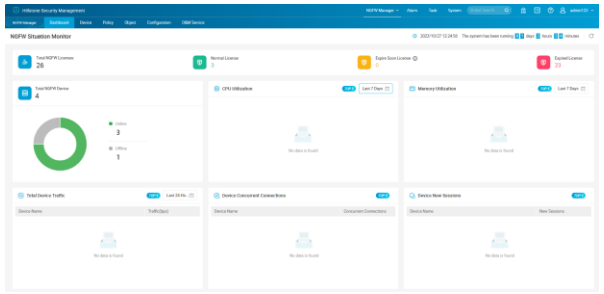
Rapid Launch of New Services

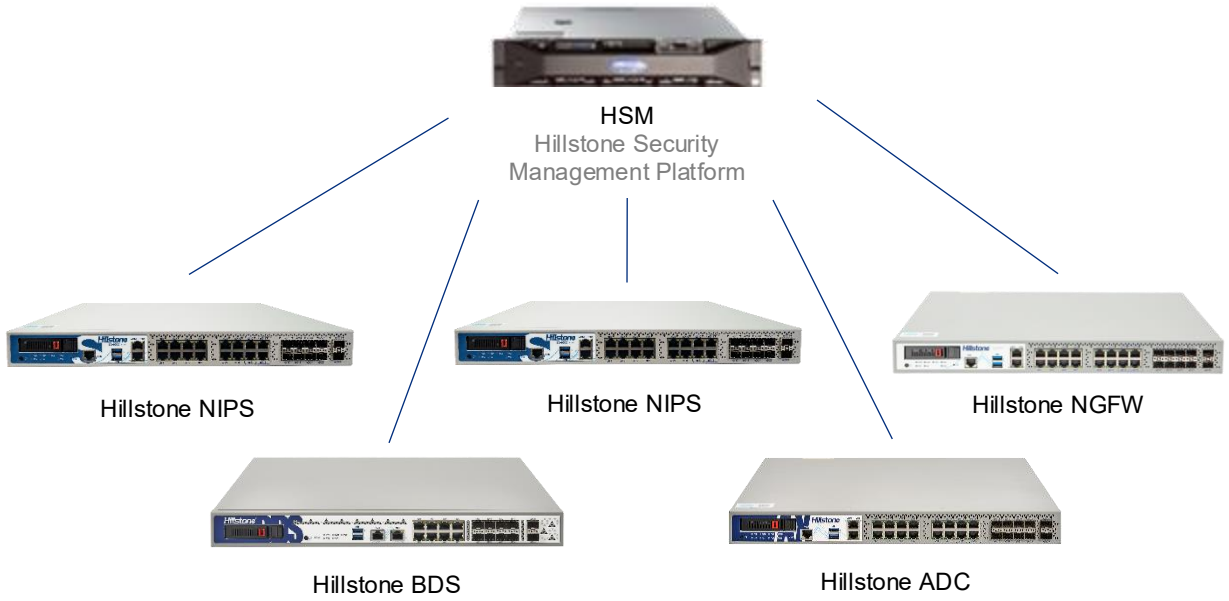
Dynamic Policy Adjustment

Increased Efficiency & Reduced Overhead

Efficient Security Operation: Simplified and Centralized Management Platform

Intuitive management interface





- *NIPS can be managed by HSM hardware appliance and virtual appliance (vHSM)*
- *Support NIPS device registration management via HSM/vHSM*
- *Support NIPS image upgrade via HSM/vHSM*
- *Support NIPS configuration, monitoring and reporting, NIPS signature online/offline update*

Support RESTful API

Easy Deployment with Minimum Network Interruption

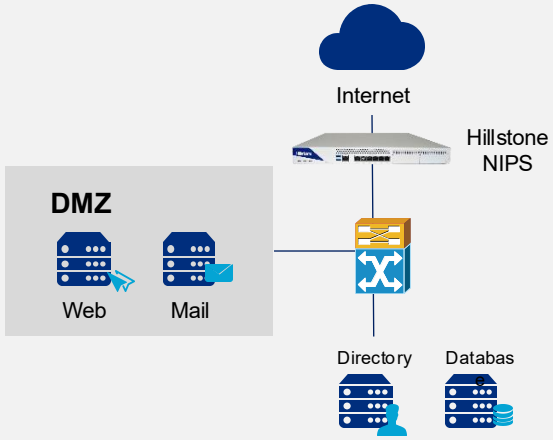
Plug-and-play with three easy steps:

- Connect the line
- Select the mode
- Bundle the policy as applicable

Minimum network disruption

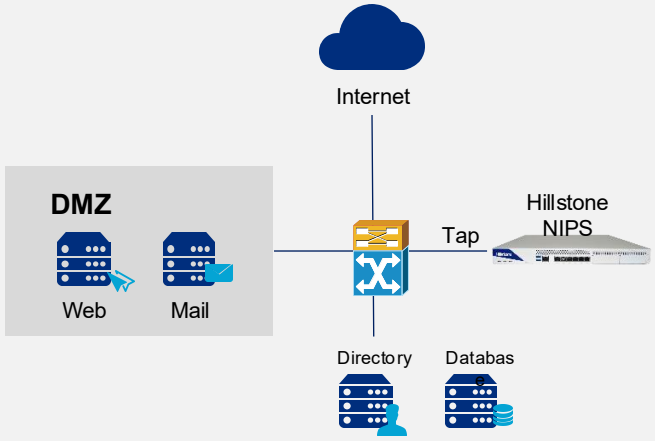
- No network topology change
- No network configuration needed
- No network traffic interruption

Support VSYS



Inline Mode: Blocking/monitoring

- Real time monitoring and blocking
- L2 transparent or L3 routing
- Two ports requirement



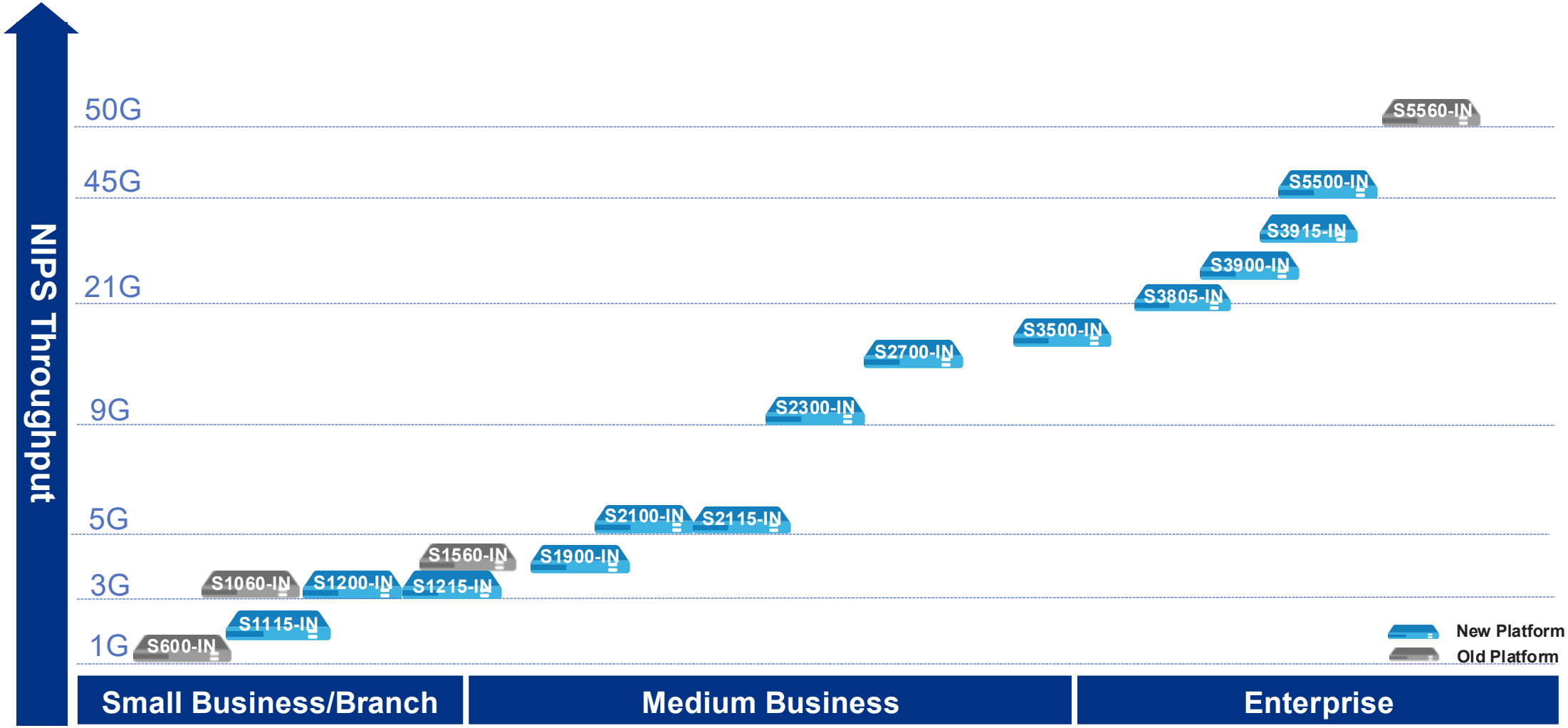
Passive Mode: Monitoring Only

- Real time monitoring and alerts
- Mirroring/TAP
- One port requirement

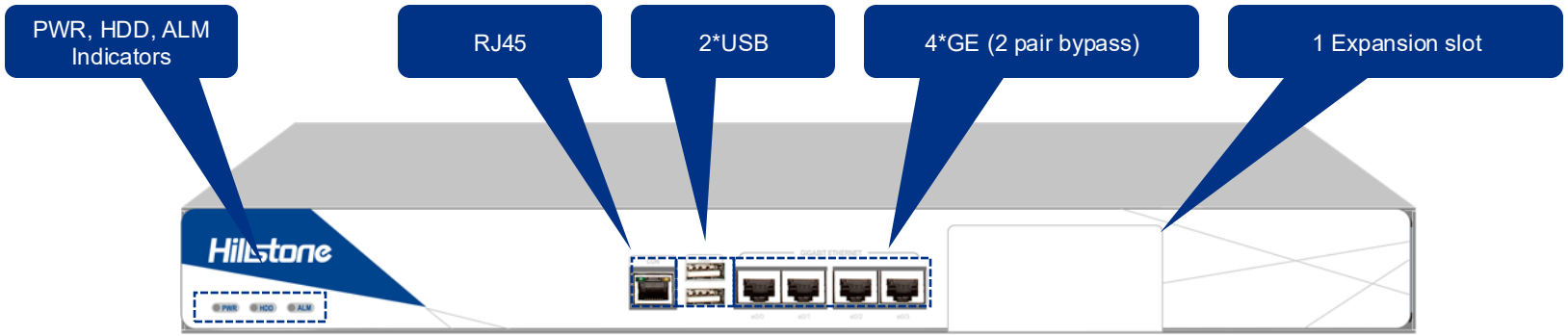
3

Hillstone NIPS Portfolio

Hillstone NIPS Portfolio



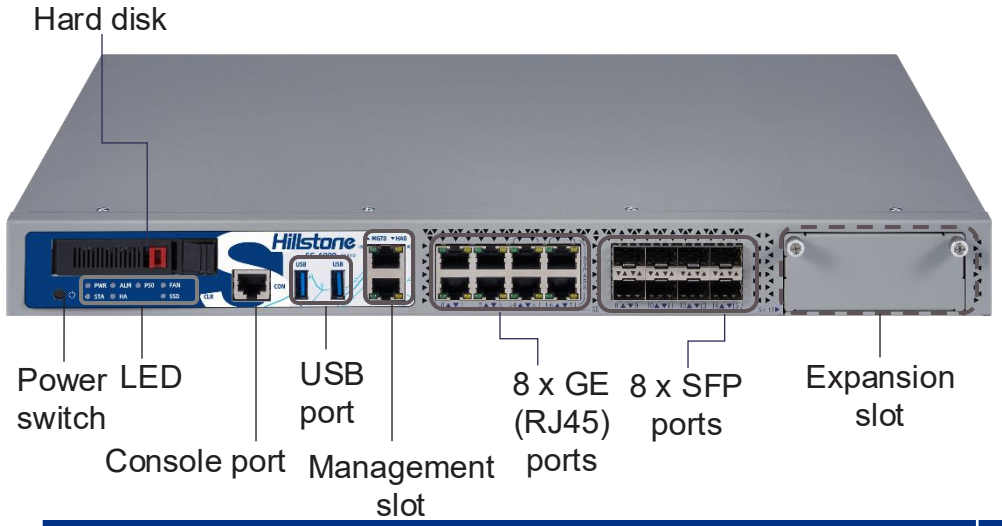
S600/S1060/S1560



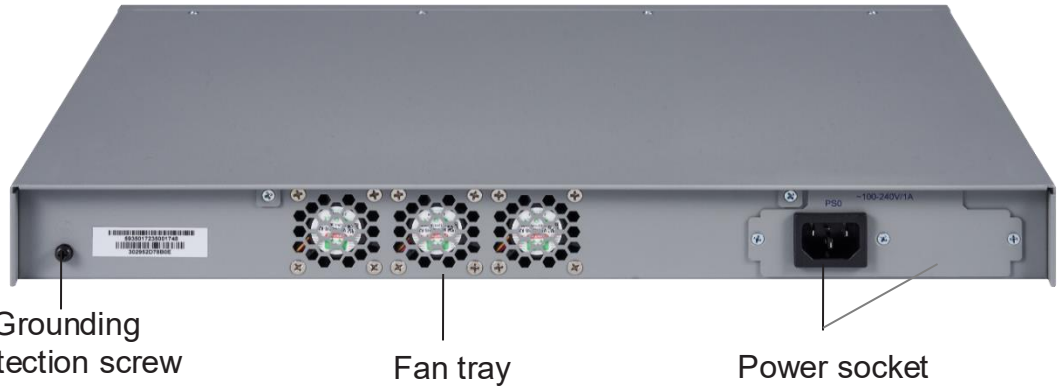
Model	S600-IN	S1060-IN	S1560-IN
NIPS throughput	1 Gbps	3 Gbps	4 Gbps
IPS throughput(realworld, IPS on)	0.9 Gbps	0.9 Gbps	1.4 Gbps
Maximum Concurrent Connections (TCP)	1 Million/ 2 Million (AEL)	1 Million/ 2 Million (AEL)	1 Million/ 2 Million (AEL)
New connections per second (HTTP)	12,000	25,000	30,000
StoneShield	N/A	N/A	Yes
Storage	960 GB HDD	960 GB HDD	960 GB HDD
Form factor	1 U	1 U	1 U
Management Ports	2 x USB Port , 1× Console Port	2 x USB Port , 1× Console Port	2 x USB Port , 1× Console Port
Fixed I/O Ports	4 x GE (including 2 pairs Bypass port)	4 x GE (including 2 pairs Bypass port)	4 x GE (including 2 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP-L-IN, IOC-S-4GE-B-IN	IOC-S-4SFP-L-IN, IOC-S-4GE-B-IN	IOC-S-4SFP-L-IN, IOC-S-4GE-B-IN
Bypass Ports (Default / Max.)	4 / 8	4 / 8	4 / 8
Power Supply	AC 100-240 V 50 / 60 Hz	AC 100-240 V 50 / 60 Hz	AC 100-240 V 50 / 60 Hz
Maximum Power Consumption	60W 1 x AC power supply	60W 1 x AC power supply	60W 1 x AC power supply

S1115

Front View



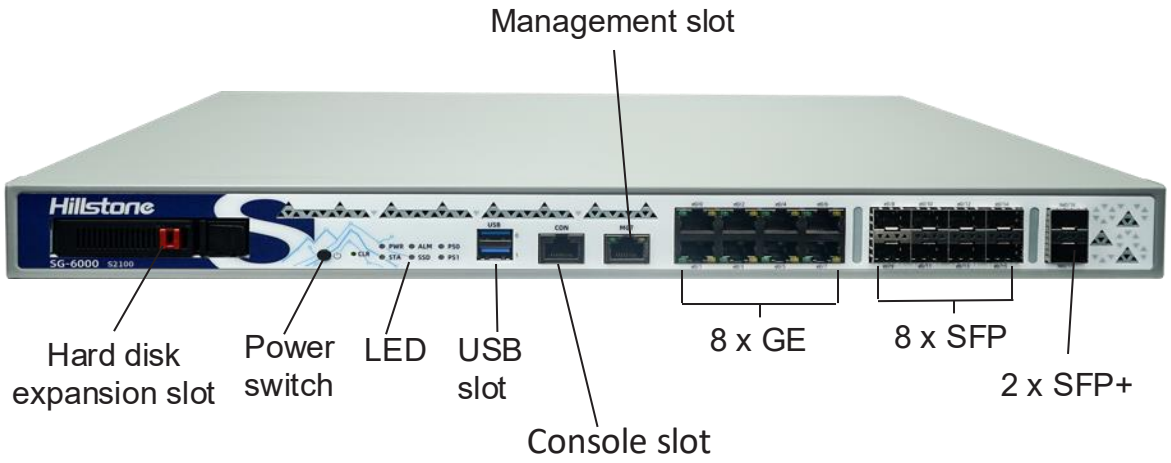
Back View



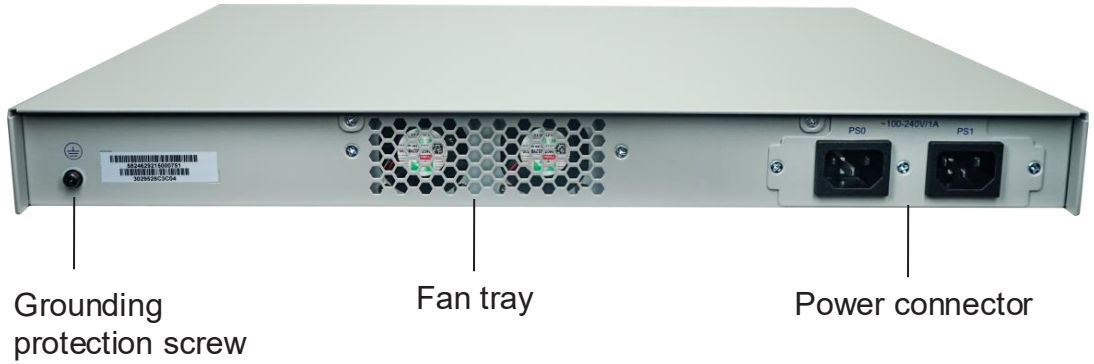
Model	S1115-IN
IPS throughput (HTTP)	2 Gbps
IPS throughput (realworld, IPS on)	1.5 Gbps
Maximum Concurrent Connections (TCP)	1.2 Million
New connections per second (HTTP)	30,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB port, 1 × MGT port, 1 x Console port, 1 x HA
Fixed I/O Ports	8 × GE (including 2 pairs Bypass port), 8 × SFP
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-F-4SFP+-A-IN, IOC-S-F-8SFP+-A-IN, IOC-S-F-8GE-B-A-IN
Bypass Ports (Default / Max.)	4/12
Power Supply	AC: 100-240V 50 / 60 Hz
Maximum Power Consumption	60W 1 x AC power supply 2 x AC power supply

S1200

Front View



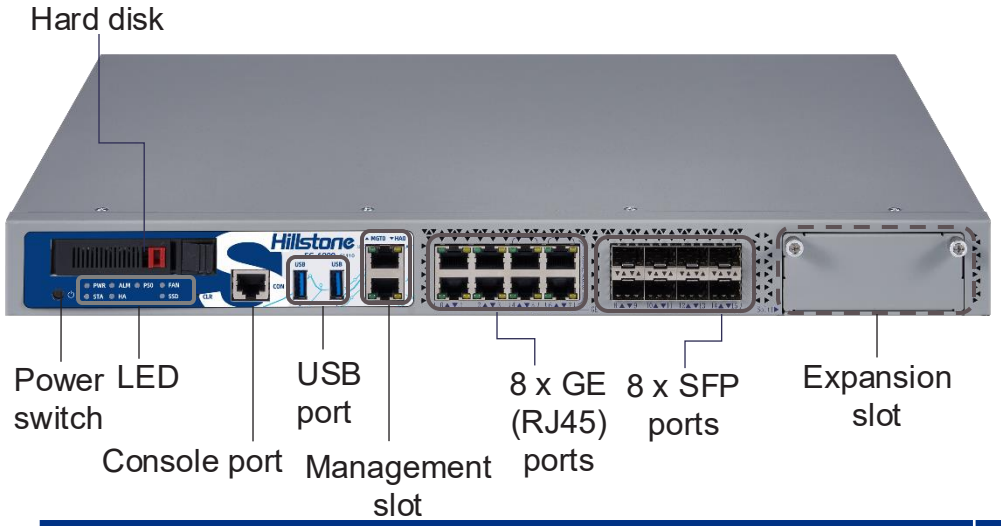
Back View



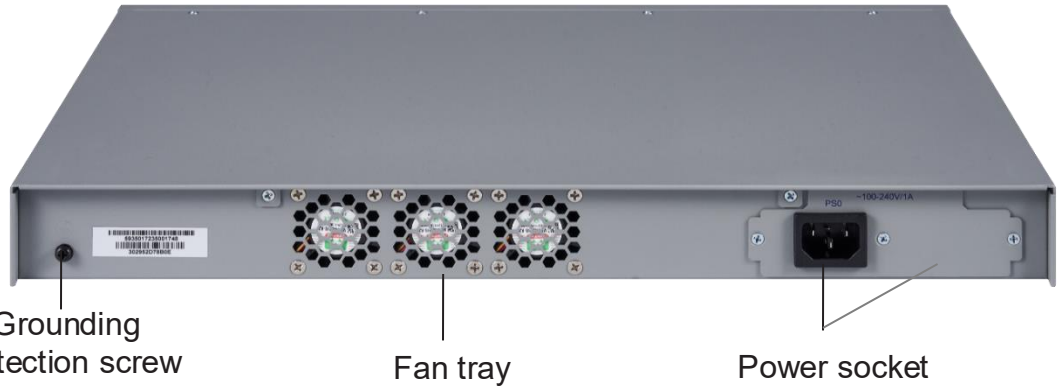
Model	S1200-IN
IPS throughput （HTTP）	3 Gbps
IPS throughput (realworld, IPS on)	1.8 Gbps
Maximum Concurrent Connections (TCP)	1.2 Million
New connections per second (HTTP)	40,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB Port , 1× Console Port, 1 MGT Port
Fixed I/O Ports	2x SFP+, 8x SFP, 8x GE
Available Slots for Expansion Modules	N/A
Expansion Module Option	N/A
Bypass Ports (Default / Max.)	N/A
Power Supply	AC: 100-240V 50 / 60 Hz
Maximum Power Consumption	50W 1 x AC power supply 2 x AC power supply

S1215

Front View



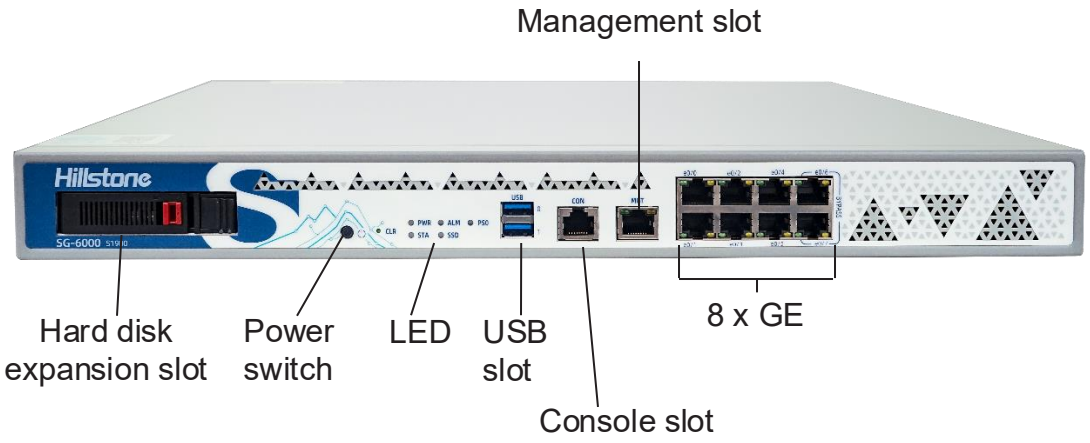
Back View



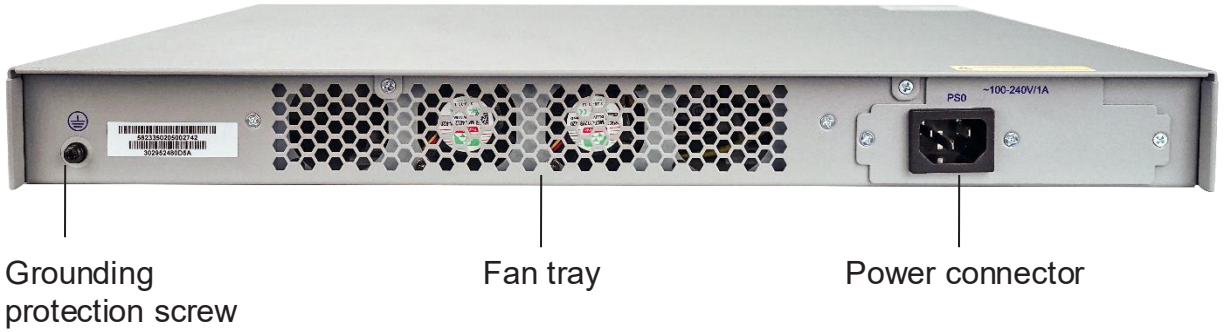
Model	S1215-IN
IPS throughput （HTTP）	3 Gbps
IPS throughput (realworld, IPS on)	1.8 Gbps
Maximum Concurrent Connections (TCP)	1.2 Million
New connections per second (HTTP)	40,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB port, 1 × MGT port, 1 x Console port, 1 x HA
Fixed I/O Ports	8 × GE (including 2 pairs Bypass port), 8 × SFP
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-F-4SFP+-A-IN, IOC-S-F-8SFP+-A-IN, IOC-S-F-8GE-B-A-IN
Bypass Ports (Default / Max.)	4/12
Power Supply	AC: 100-240 V 50 / 60 Hz
Maximum Power Consumption	60W 1 x AC power supply 2 x AC power supply

S1900

Front View



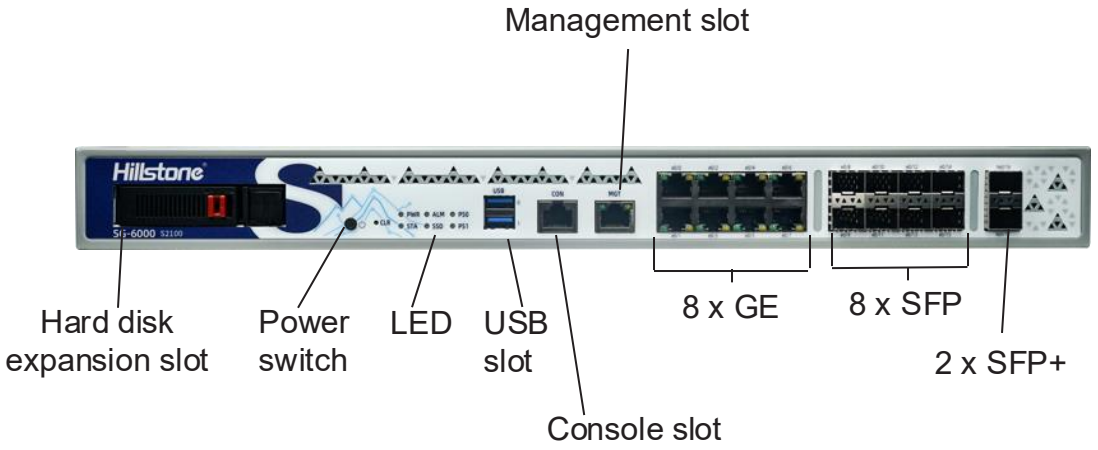
Back View



Model	S1900-IN
IPS throughput （HTTP）	3.8 Gbps
IPS throughput (realworld, IPS on)	2 Gbps
Maximum Concurrent Connections (TCP)	1.2 Million
New connections per second (HTTP)	60,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB Port , 1× Console Port, 1 MGT Port
Fixed I/O Ports	8x GE (including 1 pair Bypass port)
Available Slots for Expansion Modules	N/A
Expansion Module Option	N/A
Bypass Ports (Default / Max.)	2 / 2
Power Supply	DC: -36~ -72 V; AC: 100-240 V 50 / 60 Hz
Maximum Power Consumption	50W　1 x AC power supply　2 x AC power supply

S2100

Front View

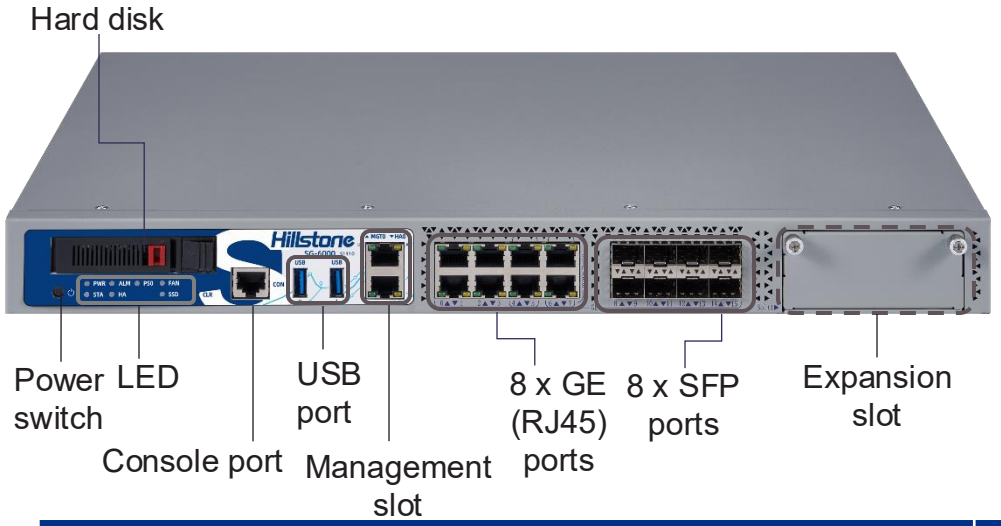


Back View

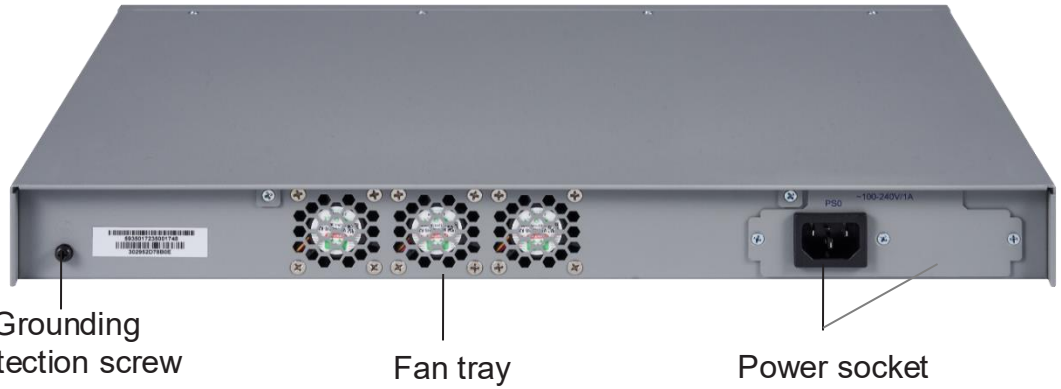
Model	S2100-IN
IPS throughput （HTTP）	5 Gbps
IPS throughput (realworld, IPS on)	2.4 Gbps
Maximum Concurrent Connections (TCP)	1.2 Million
New connections per second (HTTP)	60,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB Port , 1× Console Port, 1 MGT Port
Fixed I/O Ports	2× SFP+, 8 × SFP, 8 × GE
Available Slots for Expansion Modules	N/A
Expansion Module Option	N/A
Bypass Ports (Default / Max.)	N/A
Power Supply	AC: 100-240 V 50 / 60 Hz
Maximum Power Consumption	50W 1 x AC power supply 2 x AC power supply

S2115

Front View



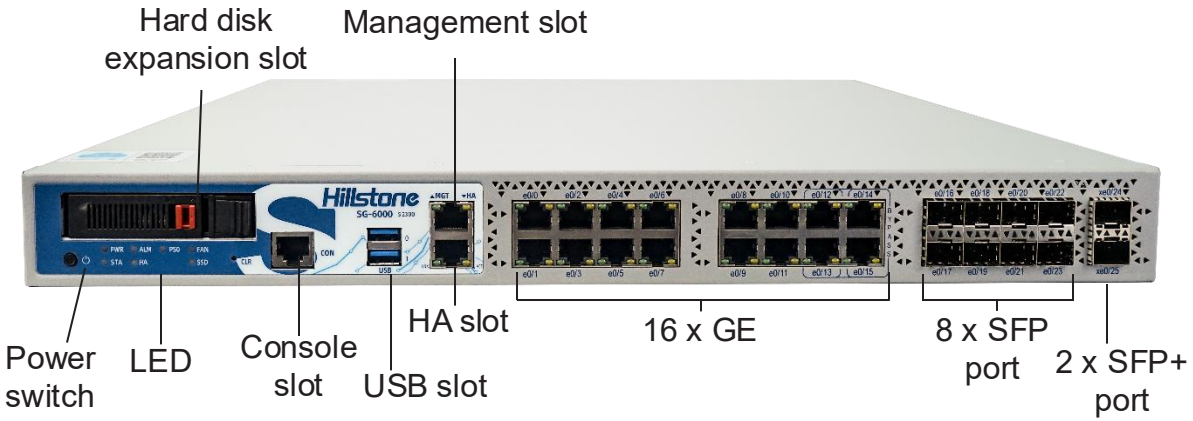
Back View



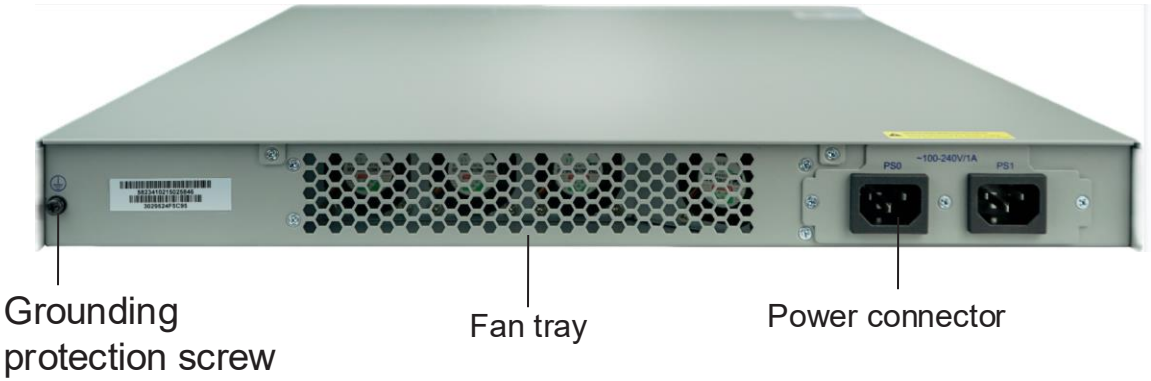
Model	S2115-IN
IPS throughput （HTTP）	5 Gbps
IPS throughput (realworld, IPS on)	2.4 Gbps
Maximum Concurrent Connections (TCP)	1.2 Million
New connections per second (HTTP)	60,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB port, 1 × MGT port, 1 x Console port, 1 x HA
Fixed I/O Ports	8 × GE (including 2 pairs Bypass port), 8 × SFP
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-F-4SFP+-A-IN, IOC-S-F-8SFP+-A-IN, IOC-S-F-8GE-B-A-IN
Bypass Ports (Default / Max.)	4/12
Power Supply	AC: 100-240 V 50 / 60 Hz
Maximum Power Consumption	60W 1 x AC power supply 2 x AC power supply

S2300

Front View



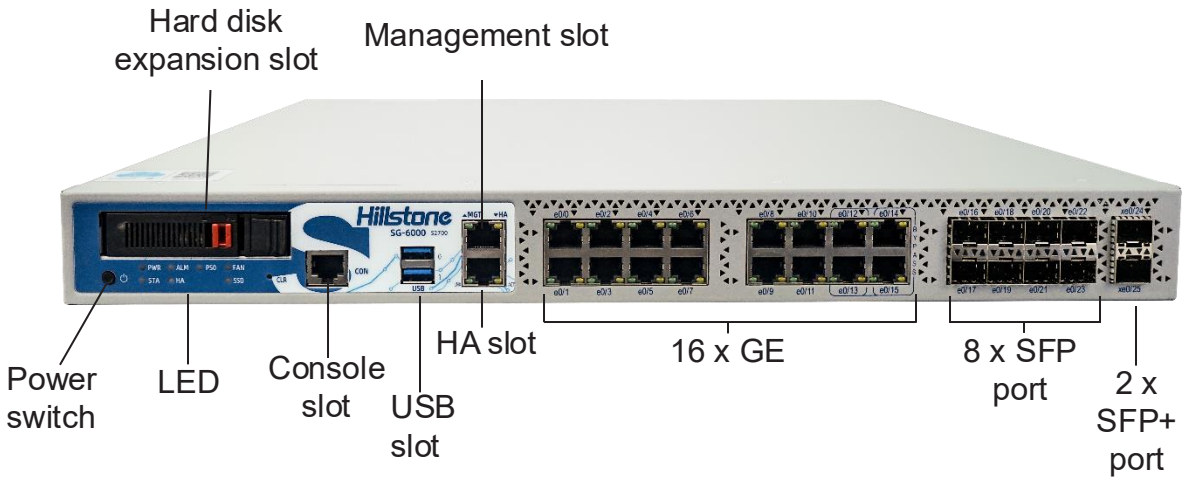
Back View



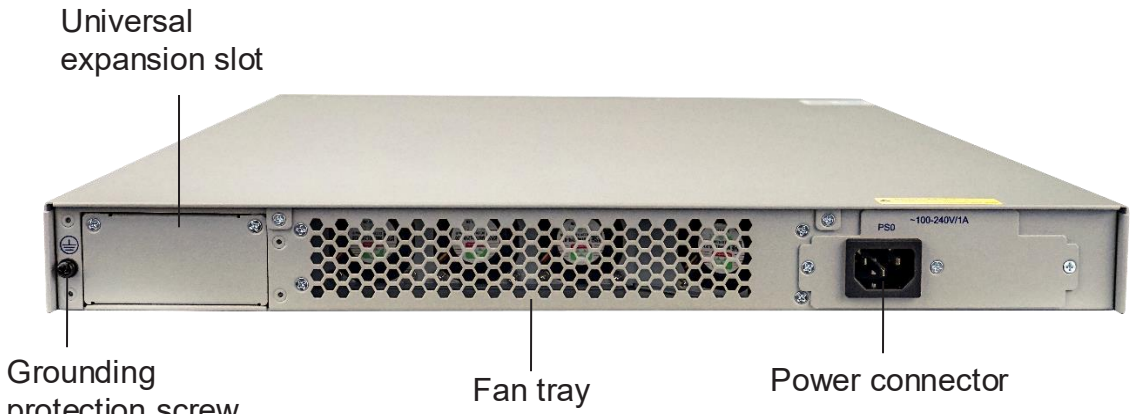
Model	S2300-IN
IPS throughput （HTTP）	9 Gbps
IPS throughput (realworld, IPS on)	2.4 Gbps
Maximum Concurrent Connections (TCP)	3 Million
New connections per second (HTTP)	60,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB 3.0 Port , 1× Console Port, 1 MGT Port, 1 HA Port
Fixed I/O Ports	2× SFP+, 8 × SFP, 16 × GE(including 2 pairs Bypass port)
Available Slots for Expansion Modules	N/A
Expansion Module Option	N/A
Bypass Ports (Default / Max.)	4 / 4
Power Supply	AC: 100-240 V 50 / 60 Hz
Maximum Power Consumption	100W 1 x AC power supply 2 x AC power supply

S2700

Front View



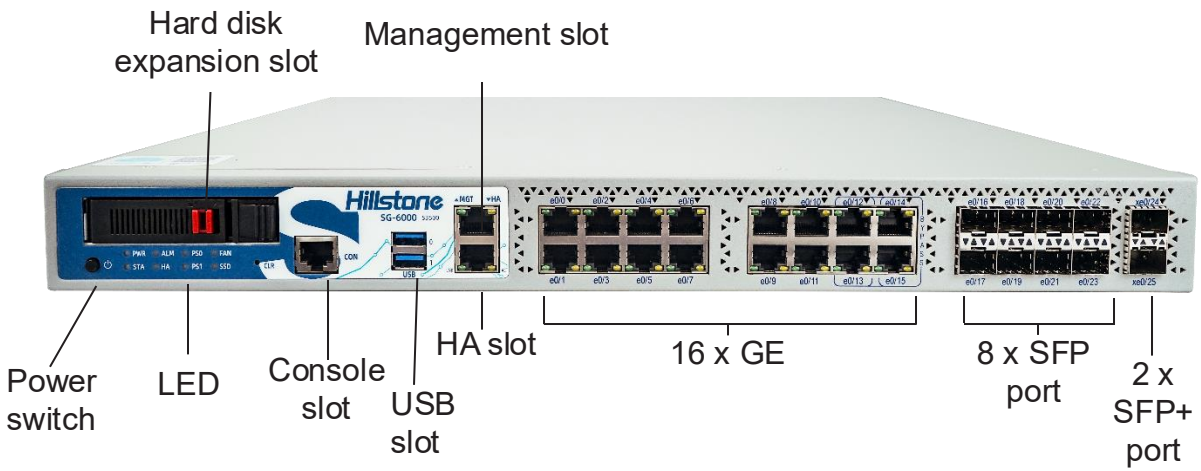
Back View



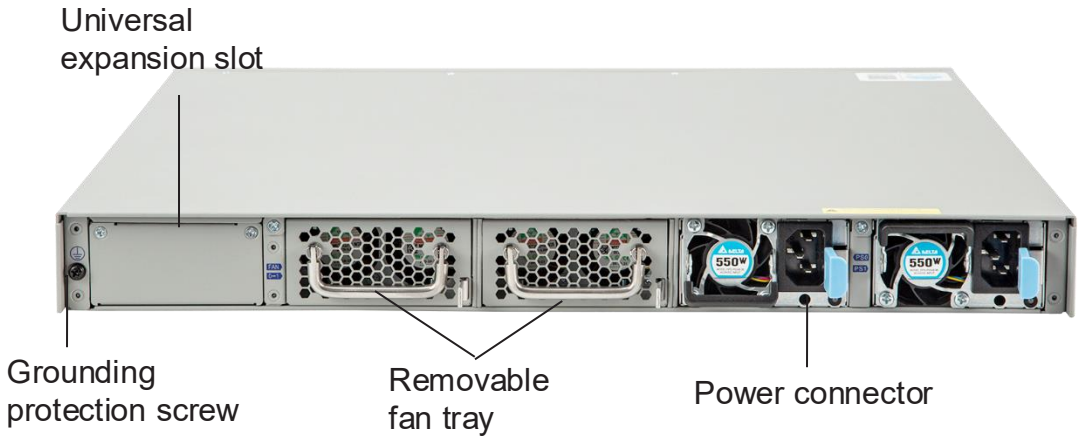
Model	S2700-IN
IPS throughput （HTTP）	11 Gbps
IPS throughput (realworld, IPS on)	2.4 Gbps
Maximum Concurrent Connections (TCP)	6 Million
New connections per second (HTTP)	60,000
Storage	480 GB SSD
Form factor	1 U
Management Ports	2 x USB 3.0 Port , 1× Console Port, 1 x MGT Port, 1x HA Port
Fixed I/O Ports	2 x SFP+, 8 x SFP, 16 x GE (including 2 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN
Bypass Ports (Default / Max.)	4 / 4
Power Supply	DC: -36~ -72 V; AC 100-240 V 50 / 60 Hz
Maximum Power Consumption	100W 1 x AC power supply 2 x AC power supply

S3500

Front View



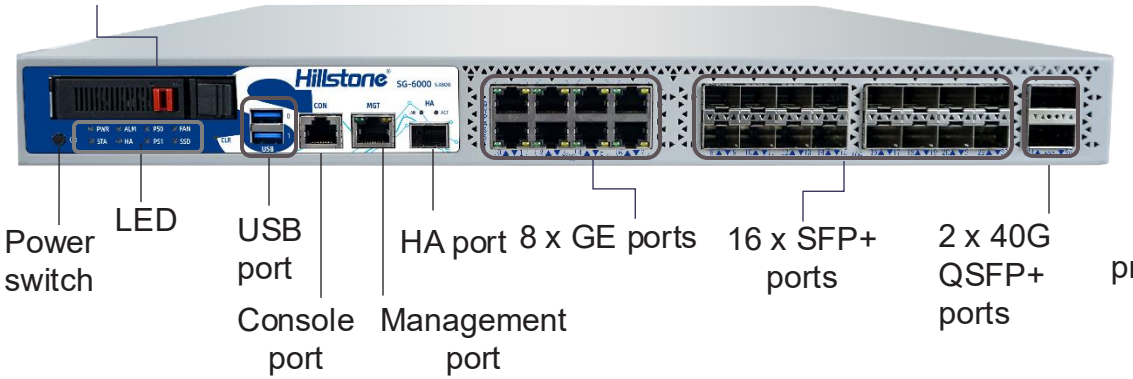
Back View



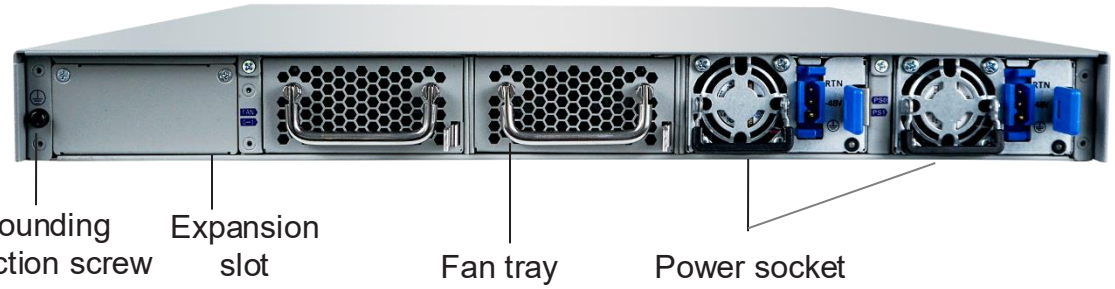
Model	S3500-IN
IPS throughput （HTTP）	15 Gbps
IPS throughput (realworld, IPS on)	4.5 Gbps
Maximum Concurrent Connections (TCP)	8 Million
New connections per second (HTTP)	140,000
Storage	960 GB SSD
Form factor	1 U
Management Ports	2 x USB 3.0 Port , 1× Console Port, 1 x MGT Port, 1x HA Port
Fixed I/O Ports	2 x SFP+, 8 x SFP, 16 x GE (including 2 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN
Bypass Ports (Default / Max.)	4 / 4
Power Supply	DC: -36~ -72 V; AC: 100-240 V 50 / 60 Hz
Maximum Power Consumption	100W 2 x AC power supply 2 x DC power supply

S3805/S3915

Front View



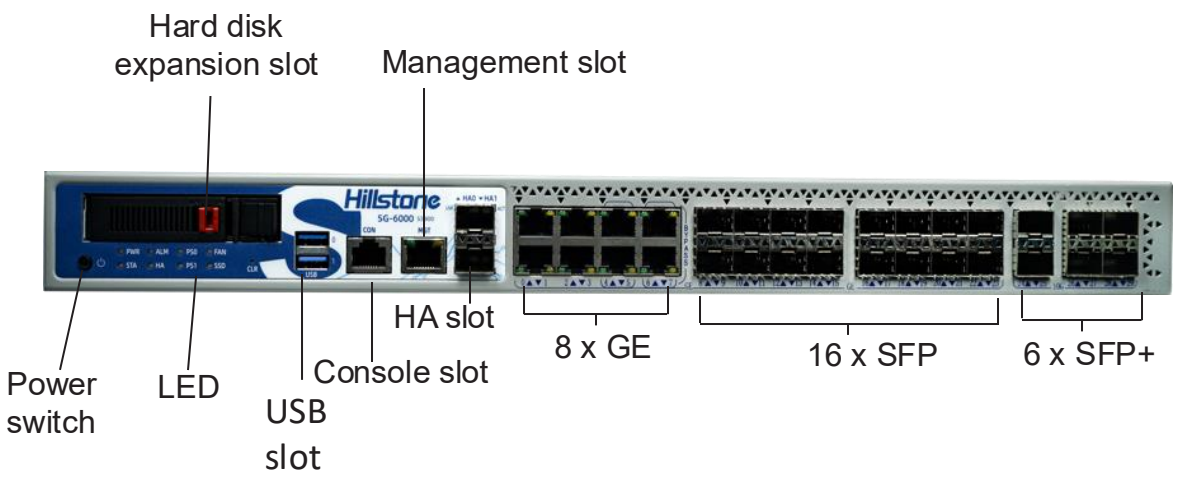
Back View



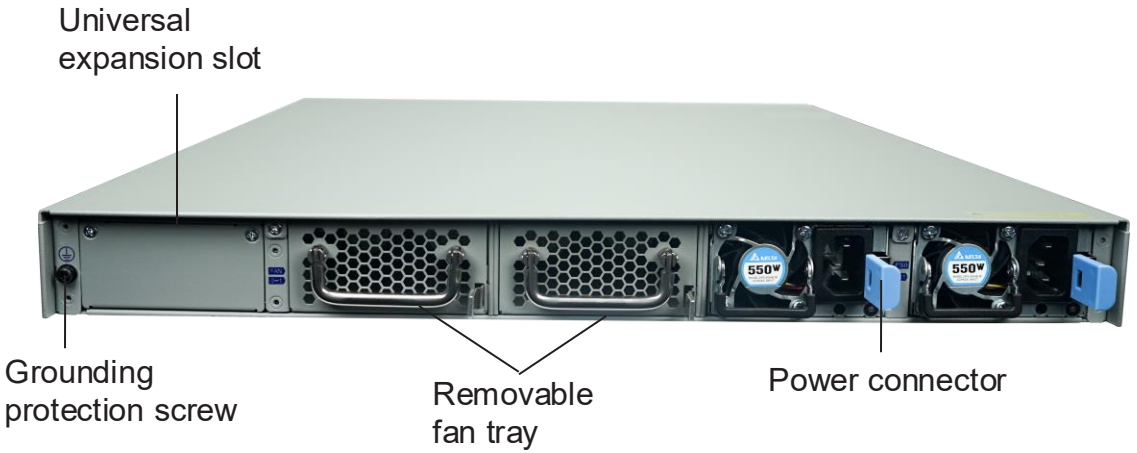
Model	S3805-IN	S3915-IN
IPS throughput （HTTP）	20 Gbps	30 Gbps
IPS throughput (realworld, IPS on)	10 Gbps	14 Gbps
Maximum Concurrent Connections (TCP)	12M	15M
New connections per second (HTTP)	250,000	380,000
Storage	960 GB SSD	960 GB SSD
Form factor	1 U	1 U
Management Ports	2 x USB Port, 1 × MGT port, 1 x Console Port , 1 HA port	2 x USB Port, 1 × MGT port, 1 x Console Port , 1 HA port
Fixed I/O Ports	2 × QSFP+, 16 × SFP+, 8 x GE (including 4 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 x GE (including 4 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN
Bypass Ports (Default / Max.)	8/8	8/8
Power Supply	DC: -36~ -72 V; AC: 100-240 V 50 / 60 Hz	DC: -36~ -72 V; AC: 100-240 V 50 / 60 Hz
Maximum Power Consumption	280W 2 x AC power supply 2 x DC power supply	280W 2 x AC power supply 2 x DC power supply

S3900

Front View



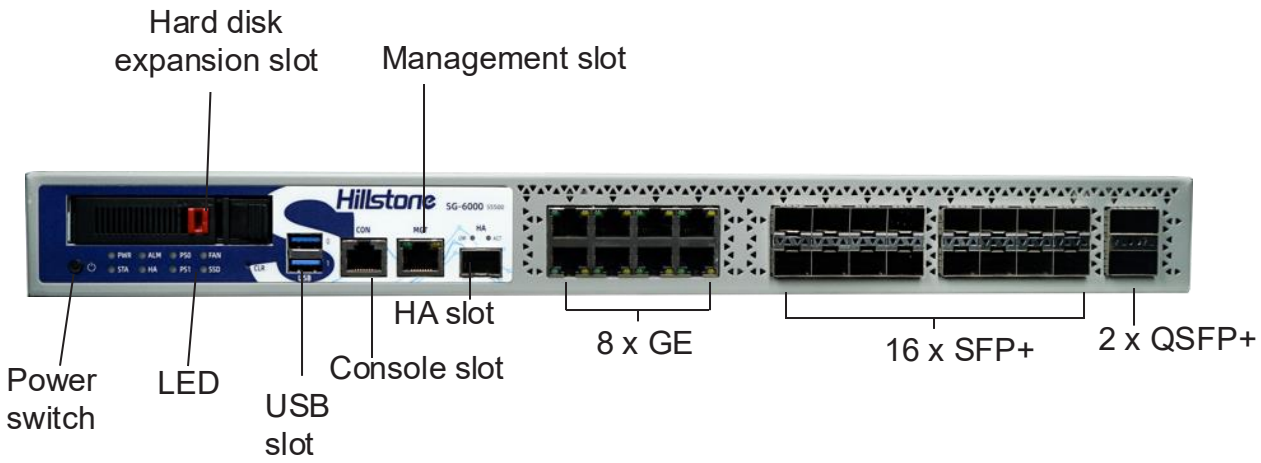
Back View



Model	S3900-IN
IPS throughput （HTTP）	25 Gbps
IPS throughput (realworld, IPS on)	14 Gbps
Maximum Concurrent Connections (TCP)	12 Million
New connections per second (HTTP)	380,000
Storage	960 GB SSD
Form factor	1 U
Management Ports	2 x USB 3.0 Port , 1× Console Port, 1 x MGT Port, 2 x HA Port (SFP+)
Fixed I/O Ports	6 × SFP+, 16 × SFP, 8 × GE (including 2 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN
Bypass Ports (Default / Max.)	4 / 4
Power Supply	DC: -36~ -72 V; AC 100-240 V 50 / 60 Hz
Maximum Power Consumption	280W 2 x AC power supply 2 x DC power supply

S5500

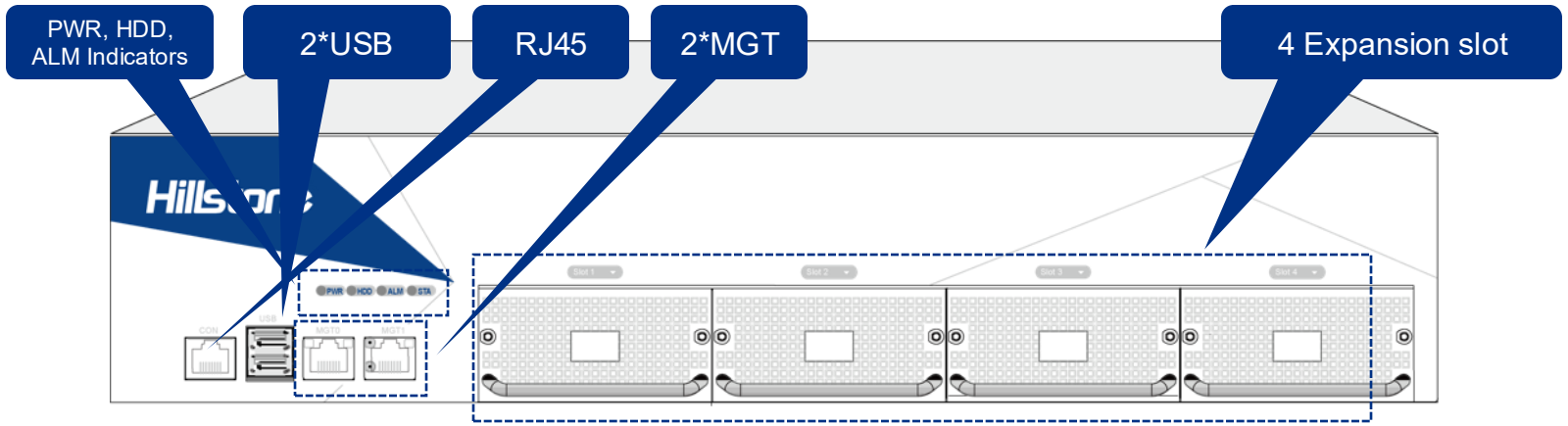
Front View



Back View

Model	S5500-IN
IPS throughput （HTTP）	45 Gbps
IPS throughput (realworld, IPS on)	25 Gbps
Maximum Concurrent Connections (TCP)	24 Million
New connections per second (HTTP)	550,000
Storage	960 GB SSD
Form factor	1 U
Management Ports	2 x USB 3.0 Port , 1× Console Port, 1 x MGT Port, 1 x HA Port (SFP+)
Fixed I/O Ports	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN
Bypass Ports (Default / Max.)	8 / 8
Power Supply	DC: -36~ -72 V; AC 100-240 V 50 / 60 Hz
Maximum Power Consumption	320W 2 x AC power supply 2 x DC power supply

S5560



Model	S5560-IN
NIPS throughput	50 Gbps
IPS throughput (realworld, IPS on)	31.4 Gbps
Maximum Concurrent Connections (TCP)	8 Million / 10 Million (with AEL)
New connections per second (HTTP)	700,000
StoneShield	Yes
Storage	960 GB HDD
Form factor	2 U
Management Ports	2 x USB Port , 2 x GE MGT, 1× Console Port
Fixed I/O Ports	N/A
Available Slots for Expansion Modules	4 x Generic Slot
Expansion Module Option	IOC-S-4GE-B-H-IN, IOC-S-4SFP-IN,IOC-S-8GE-B-H-IN, IOC-S-8SFP-H-IN,IOC-S-4GE-4SFP-H-IN,IOC-S-2SFP+-H-IN, IOC-S-4SFP+-H-IN, IOC-S-4SFP-B-H-IN, IOC-S-2SFP+-B-H-IN
Bypass Ports (Default / Max.)	0 / 32
Power Supply	AC 100-240 V 50 / 60 Hz
Maximum Power Consumption	350W 2 x AC power supply

Expansion Modules (1)

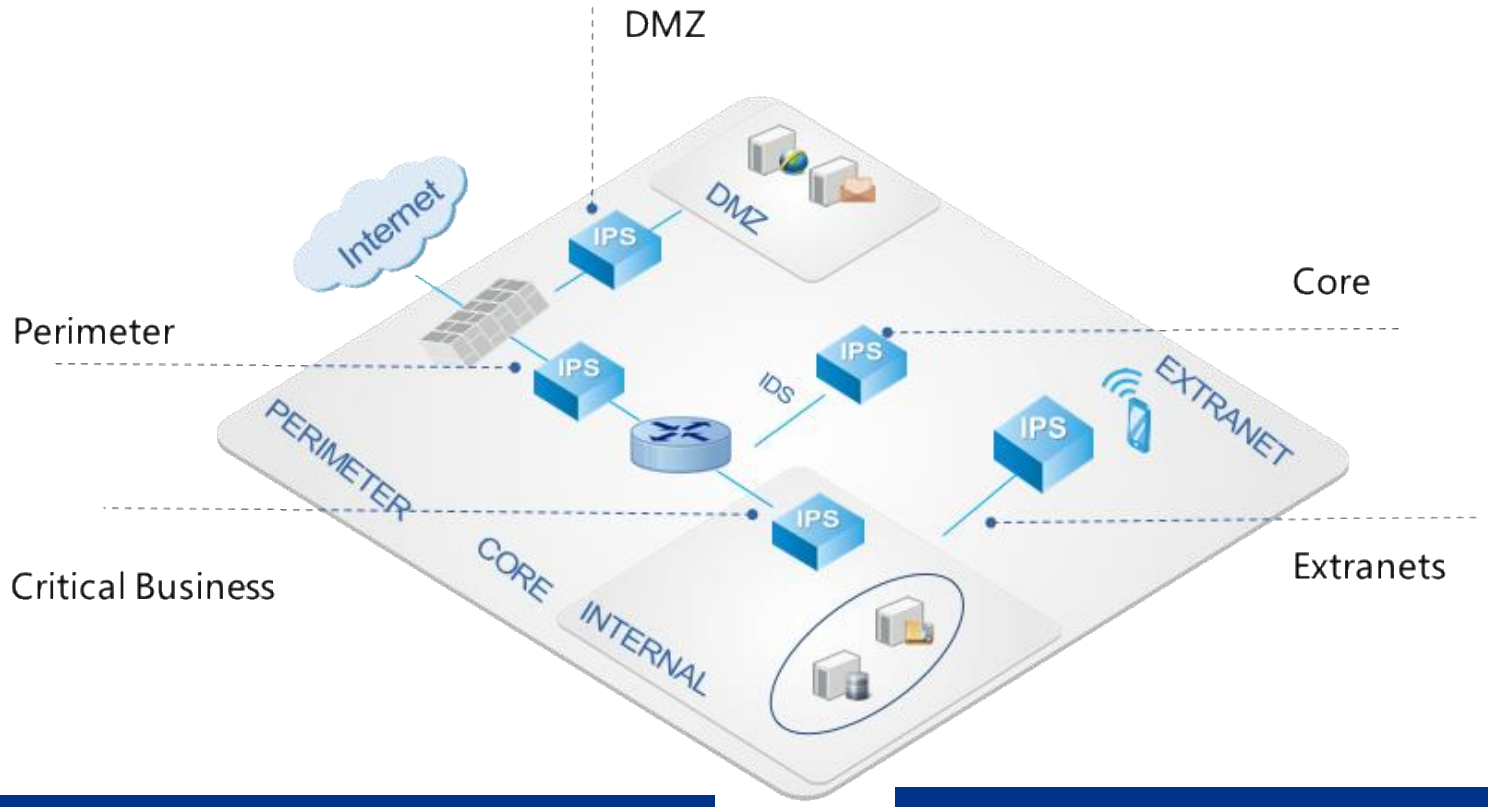
Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN	IOC-S-F-4SFP+-A-IN	IOC-S-F-8SFP+-A-IN	IOC-S-F-8GE-B-A-IN	IOC-S-4SFP+-A-IN	IOC-S-2MM-BE-A-IN	IOC-S-2SM-BE-A-IN	IOC-S-2QSFP+-A-IN
I/O Ports	4 x SFP Ports	4 x GE Bypass Ports	4 x SFP+ Ports (for Front Panel)	8 x SFP+ ports (for Front Panel)	8 x GE, including 4 bypass pairs (for Front Panel)	4 × SFP+, SFP+ module not included	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)	2 × QSFP+
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U	1U	1U	1U	1U	1U	1U
Weight	0.22 lb (0.1 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.62 lb (0.28 kg)	0.6 lb (0.27 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)
Applicable Models	S600-IN S1060-IN S1560-IN		S1115-IN S1215-IN S2115-IN			S2700-IN S3500-IN S3900-IN S3805 S3915 S5500-IN			

Expansion Modules (2)

Module	IOC-S-4GE-B-H-IN	IOC-S-4SFP-H-IN	IOC-S-8GE-B-H-IN	IOC-S-8SFP-H-IN	IOC-S-4GE-4SFP-H-IN	IOC-S-2SFP+-H-IN	IOC-S-4SFP+-H-IN	IOC-S-4SFP-B-H-IN	IOC-S-2SFP+-B-H-IN
I/O Ports	4 x GE Bypass Ports	4 x SFP Ports	8 x GE Bypass Ports	8 x SFP Ports	4 x GE and 4 x SFP Ports	2 x SFP+ Ports	4 x SFP+ Ports	4 x SFP Bypass ports	2 x SFP+ Bypass ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.33 lb (0.15 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.33 lb (0.15 kg)	0.44 lb (0.2 kg)	0.88 lb (0.4 kg)	0.88 lb (0.4 kg)
Applicable Models	S5560-IN								

4 Deployment Scenarios & Winning Cases

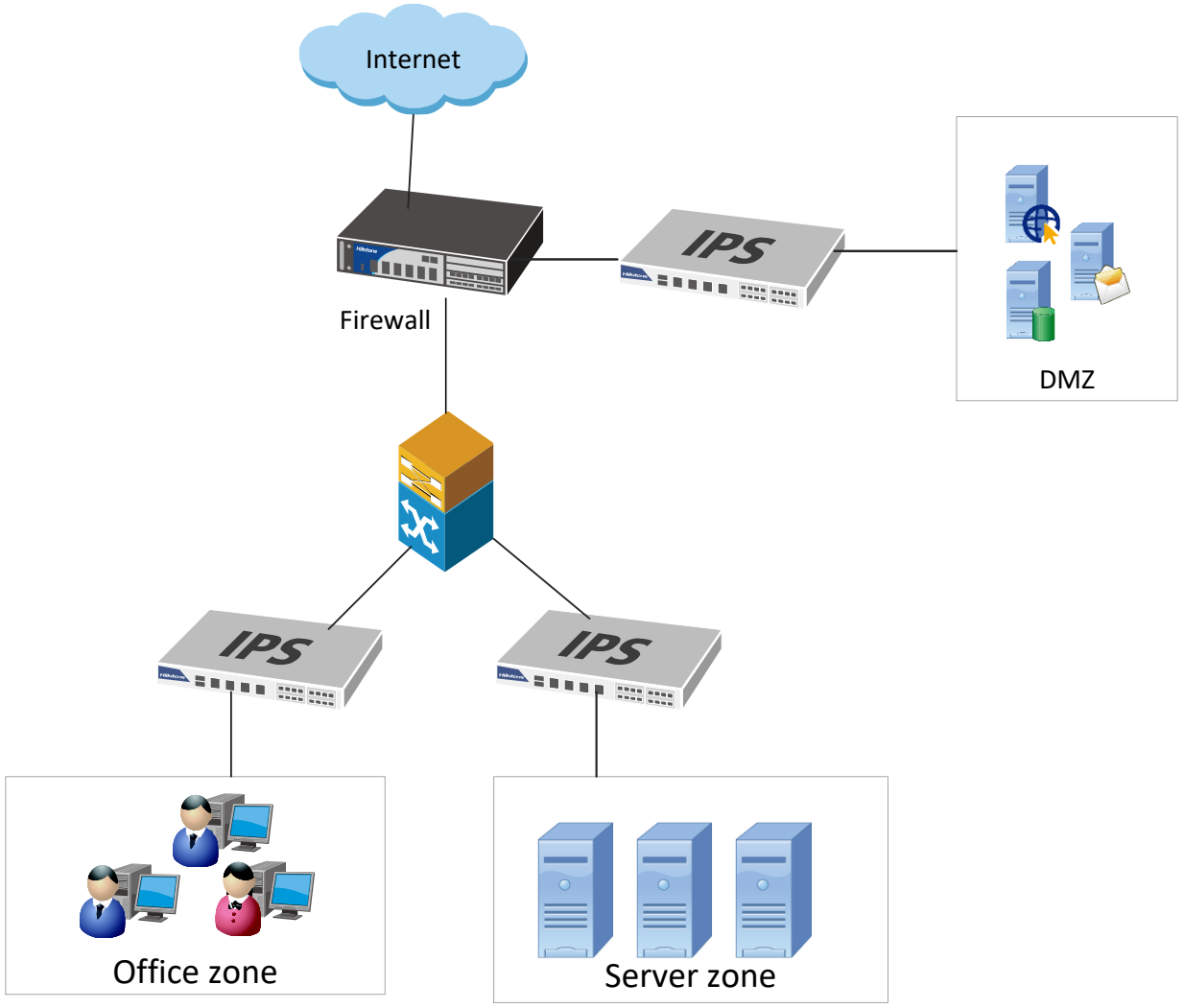
Deployment Scenarios



Customers: Government, Financial Sectors, Enterprises customers who need standalone IPS/IDS appliance for better protection/internal network segmentation/Threat monitoring etc.

Deployment Scenarios: inline deployment after perimeter firewall, DMZ/Internal network/Remote access segmentation, Tapping mode by core switch/access switch for threat monitoring/detection

S-Series Deployment in Enterprises



Requirements

- Protection against sophisticated attacks
- Insight into network environment

Solutions

- Strong defensive capabilities
- Deep visibility from L2 – L7
- Unknown threat detection
- Automated analysis and mitigation

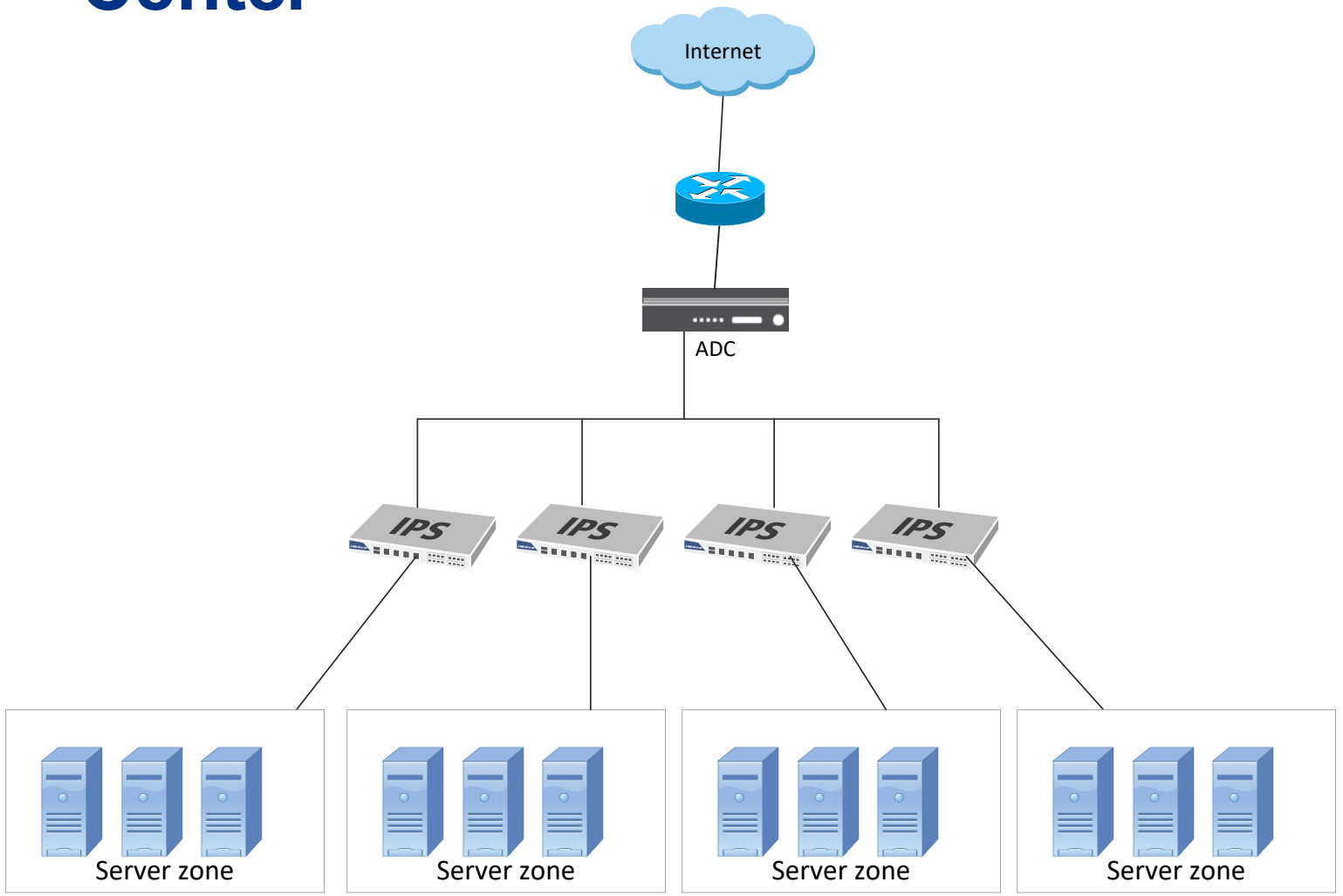
Products

- S Series

Market

- Education
- Enterprises
- Government

S-Series Deployment in Service Provider/Data Center



Requirements

- Protection against sophisticated attacks
- High performance

Solutions

- Integrate with ADC
- Strong defensive capabilities
- Deep visibility from L2 – L7
- Unknown threat detection
- Automated analysis and mitigation

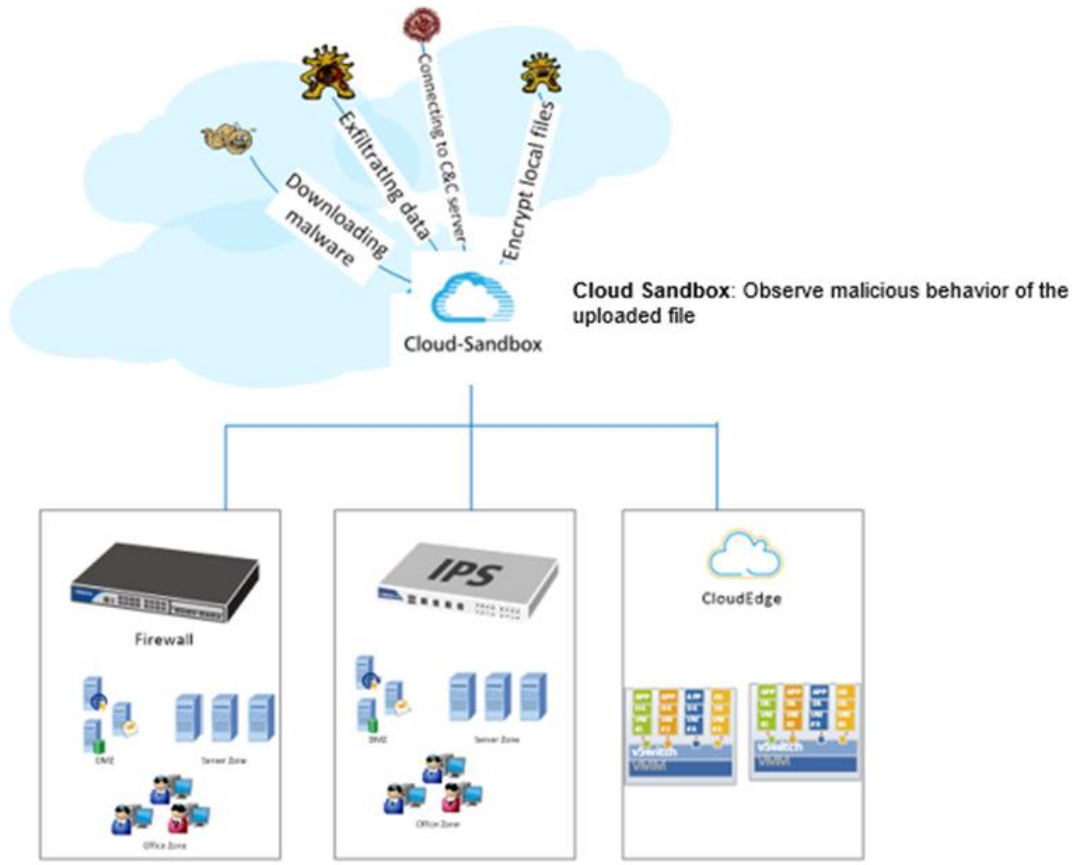
Products

- S-Series

Market

- Service Provider
- Data Center

Using Cloud Sandbox to Detect Advanced Threats



Requirements

- Protection against advanced threats

Solutions

- Static and dynamic analysis
- Unknown threat detection

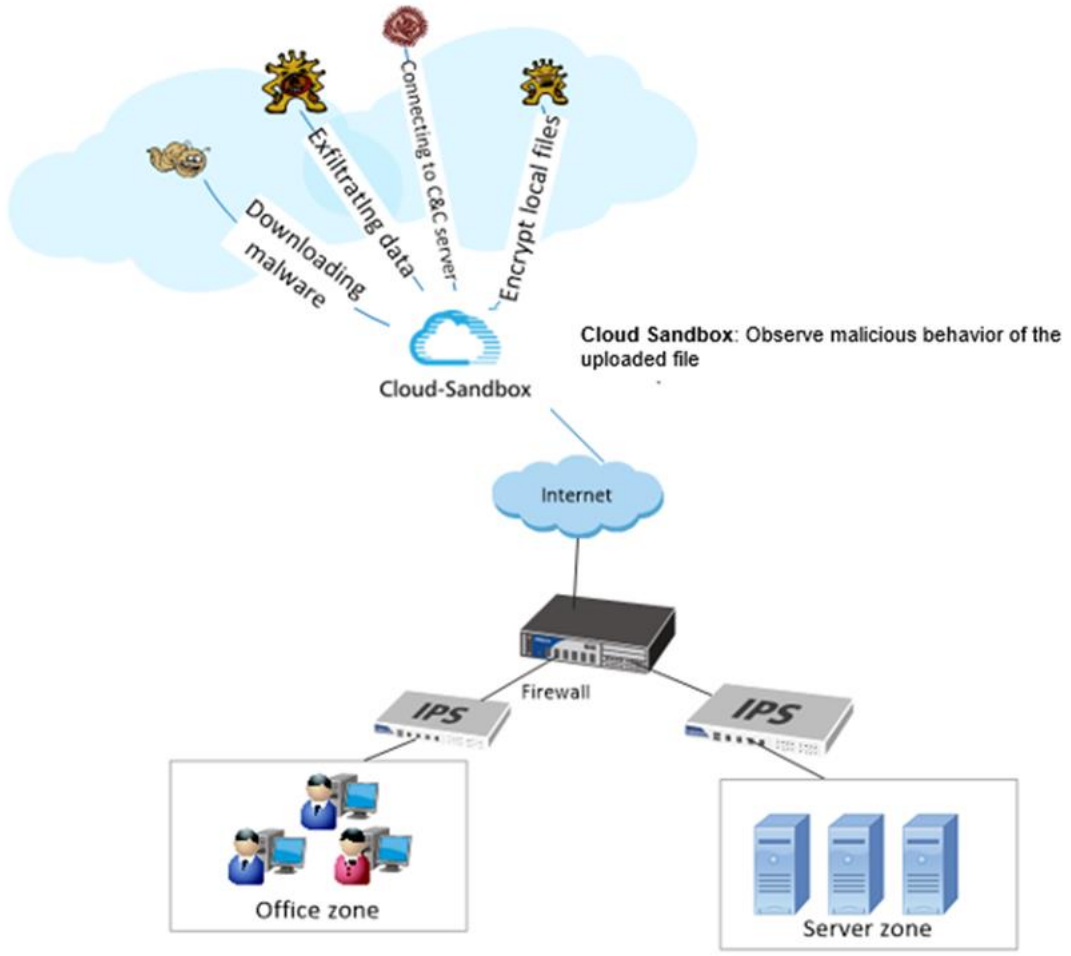
Products

- E/T Series with Sandbox enabled
- S-Series with Sandbox enabled
- CloudEdge with Sandbox enabled

Market

- Education
- Enterprises
- Government
- Finance

Solution Against Ransomware



Requirements

- Protection against ransomware

Solutions

- Antivirus against known ransomwares, 10,000,000+ signatures. In breaching stage.
- Sandbox against unknown ransomwares. In breaching stage.
- C&C server detection based on behavior analysis. In post-breaching stage.
- Abnormal behavior analysis in post-breaching stage.

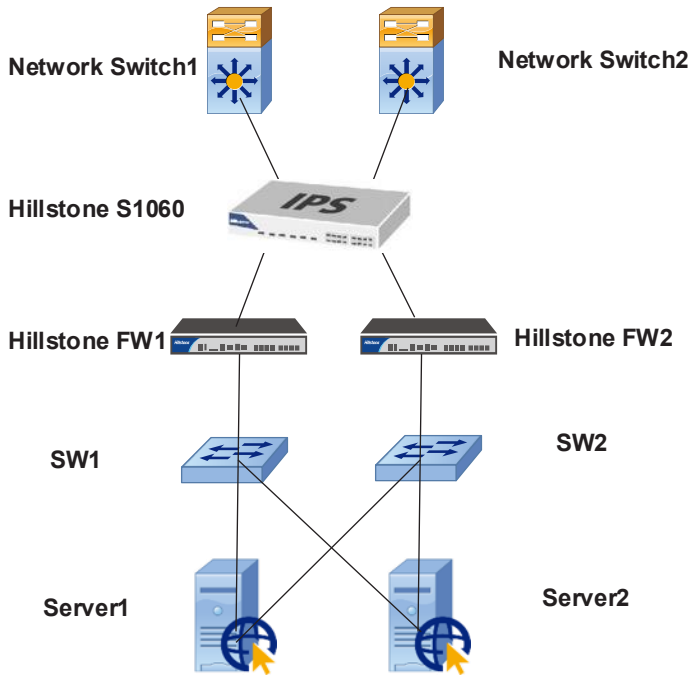
Products

- S/T Series with AV, Sandbox, StoneShield
- E-Series/CloudEdge with AV, Sandbox

Market

- Education
- Enterprises
- Government
- Finance

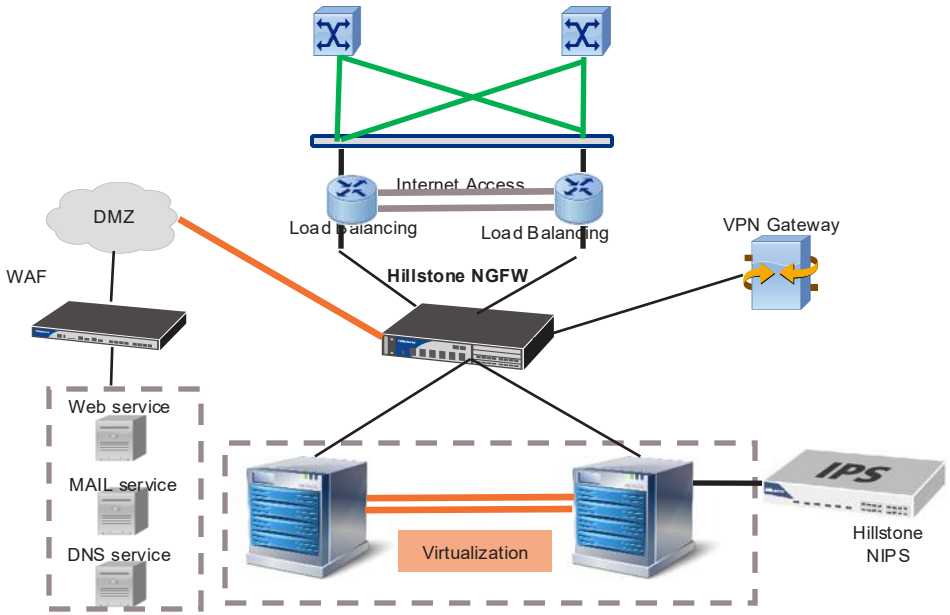
Winning Case 1: Protect Critical Business for a Commercial Bank



Hillstone NIPS Offerings and Benefits

- Inline deployment in transparent mode, between core switch and critical servers (SMBs business) in Tier 1 branch network, with the objective to detect and block attacks in real-time.
- Business availability and continuity for SMB customers have enhanced significantly after the deployment
- Two pairs of bypass interfaces ensure network connection even in the face of power outages.
- Expansion capability protects customer investment during network upgrades.

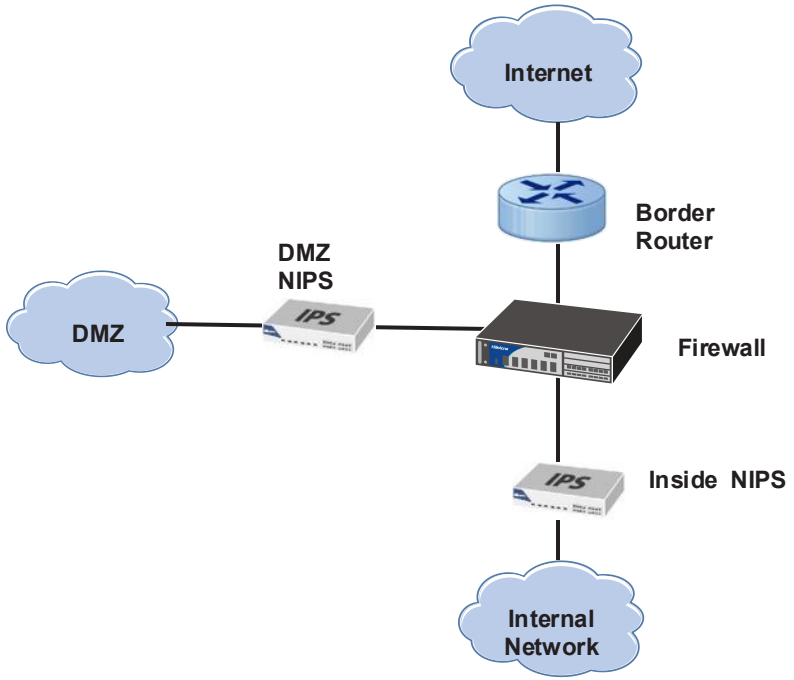
Winning Case 2: Protect a National Supercomputing Center



Hillstone NIPS Offerings and Benefits

- The complete solution includes the Hillstone high-end E-Series NGFW and NIPS solution, providing a 360 degree protection to the supercomputing center's internal network and business servers.
- The Hillstone NGFW is deployed as an internet gateway, with the Hillstone NIPS deployed in tapping mode in the business server zones, continuously detecting threats and protocol abnormality in real-time.
- After being in production for one year, the system has detected and prevented several large-scale worm, injection and C&C attacks, which ensured network connectivity and business continuity for the customer.

Winning Case 3:
Protect DMZ for a Local Government Agency



Hillstone NIPS Offerings and Benefits

- Deployed inline between DMZ and the internet to detect and block threats real-time
- Meets compliance requirement from the government
- Prevents public information leakage, and ensures public service continuity

NIPS Customers

Royal Thai Armed Forces
Government
Thailand, SEA, S2160

Perusahaan Listrik Negara
Energy
Indonesia, SEA, S1560

People's Government of
Shandong Province
Government
China, S1060, S2060

Shanghai Ministration of Civil
Service
Government
China, S2560, S3560

Huaxia Bank
Finance
China, S2160

China Guodian
Energy
China, S1060

Bank of Tibet
Finance
China, S1060, S3860

China Telecom
Internet Carrier
China, S3560

Anhui University of Finance &
Economics
Education
China, S1560

Sunshine Insurance Group
Finance
China, S1060

Nanjing University
Education
China, S2060

Caitong Fund
Finance
China, S2060

Changjiang Daily
Media
China, S2160

Hillstone Network Detection and Response (NDR) Solution

Integrative Cybersecurity

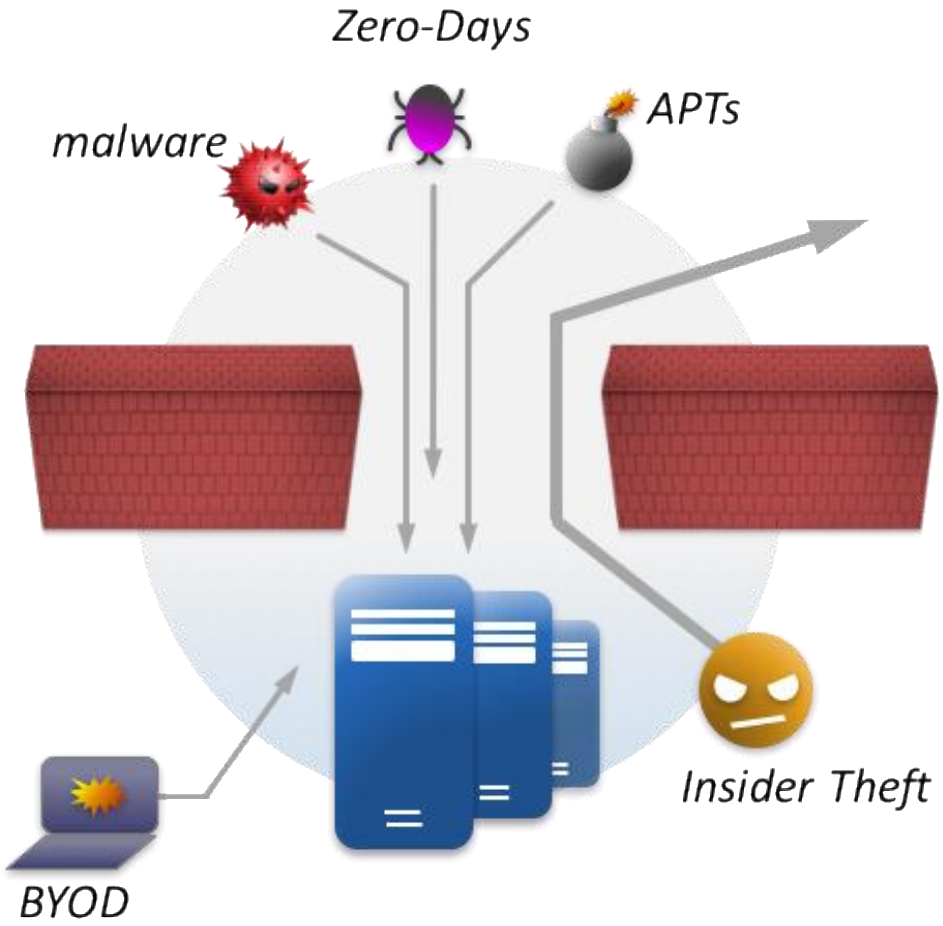
Visionary. AI-powered. Accessible.

Agenda

- Today’s Intranet Security Reality
- Hillstone NDR Value Proposition
- Hillstone NDR Product Portfolio
- Deployment Scenarios & Case Studies

Today’s Intranet Security Reality

Internal Network Breaches Occur at an Alarming Rate



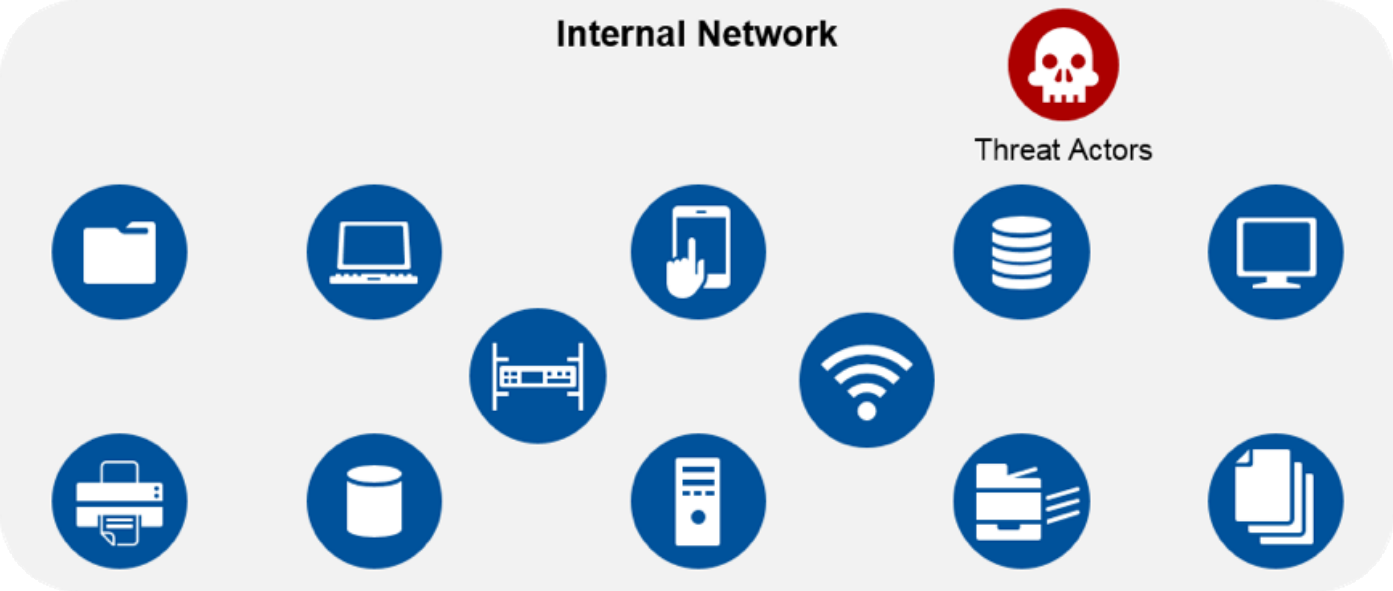
Traditional signature defenses can only stop old "**amateur**" attacks

New, **sophisticated** attacks breach every network.

"*In 60% of cases, attackers are able to compromise an organization within **minutes**.*"

– Verizon 2015 DBIR

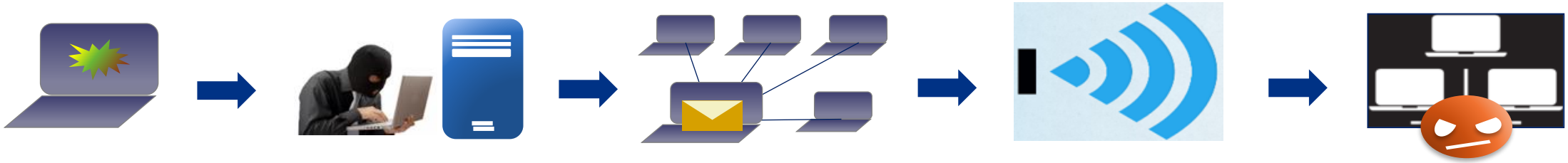
Threat Spreads Easily in Flat Internal Networks…



"…regardless of their motivation, should adversaries gain a foothold on your internal network, they can pivot through and access anything on your internal network. This is a primary reason modern breaches are so devastating in terms of the amount of data lost and the dwell time spent on an organization's network before being discovered. As a result, lateral movement detection/prevention has become an area of considerable focus"

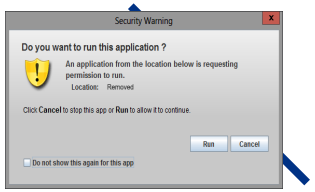
-Source: Gartner (September 2016)

Interrupts Critical Servers and Business Continuity



- Phishing occurs when staff surf the internet
- C&C
- Hacker completely controls the host
- Fake internal email and attachment propagates damage internally
- More hosts are compromised
- Host loses control
- Launches DDoS from inside
- Results in server, firewall break-down
- Ultimately, network and business are down

Breaches Sensitive Data Through Compromised Host



- Phishing occurs when staff surf the internet

- Inject malware with fake or expired antivirus software signatures

- Antivirus software fails to detect malware
- Malware is executed

- C&C
- Downloads PE file
- Hacker completely controls the host

- Database server is breached through the compromised host

Hillstone NDR Value Proposition

Hillstone NDR Product BDS

Hillstone NDR product BDS detects and responds to Advanced Network Threats

Threat Detection	Deep Visibility	Digital Forensics Analysis	Effective Response
ABD/ATD/WEB	IOCs	Attack Chain	Admin Actions
NTA/Deception	Dashboards	MITRE ATT&CK	Blacklist / Whitelist
Threat Correlation	Risk/Threat/Traffic	Rich Forensics	Block with Firewall
…	…	…	…

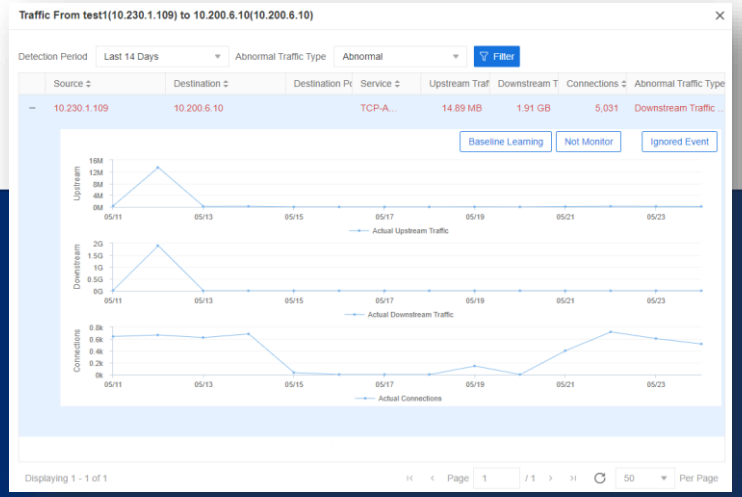
ML-based Analytics for Abnormal Behaviors

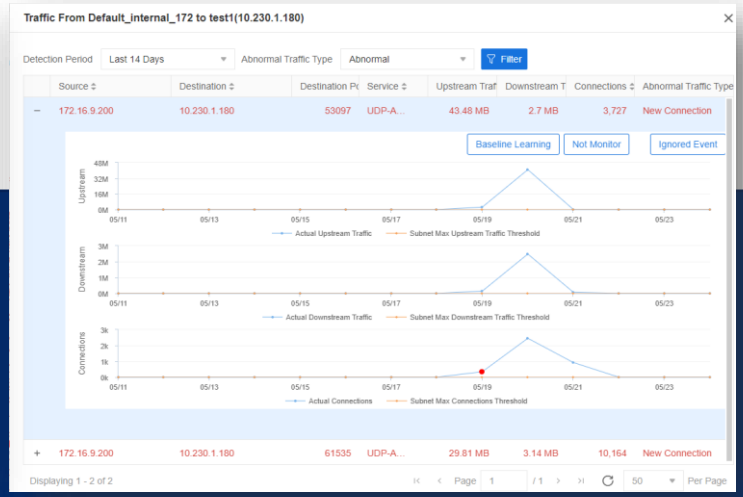
Learn and Establish Normal Traffic Baseline and Threshold

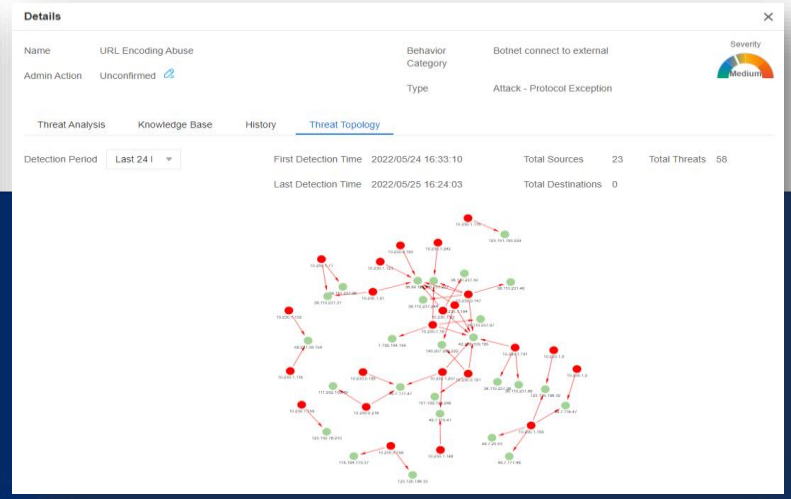
Detect Traffic Trend and Identify Abnormal Traffic Behaviors

Monitor Normal and Abnormal Traffic for each server/host

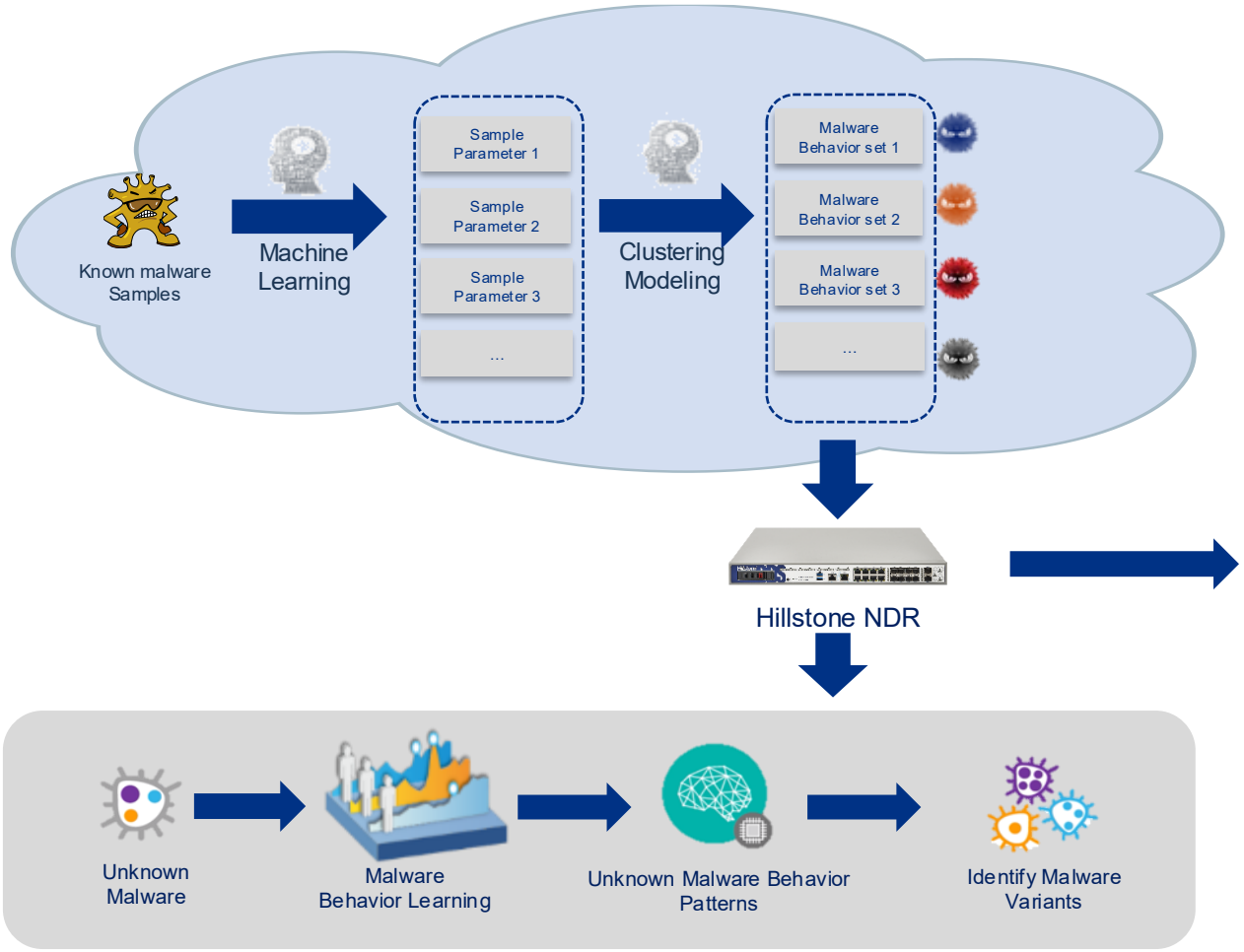
ML-based behavior analytics for URL, UEBA, threat correlations etc.







Detection: Advanced Threat Detection (ATD)



Detection: Abnormal Encrypted Traffic Detection

Encrypted Traffic

Hillstone NDR

Extracting Signatures without Decryption

- Parameter 1
- Parameter 2
- Parameter 3
- .....

Detection Engine

AI-powered Detection Engine

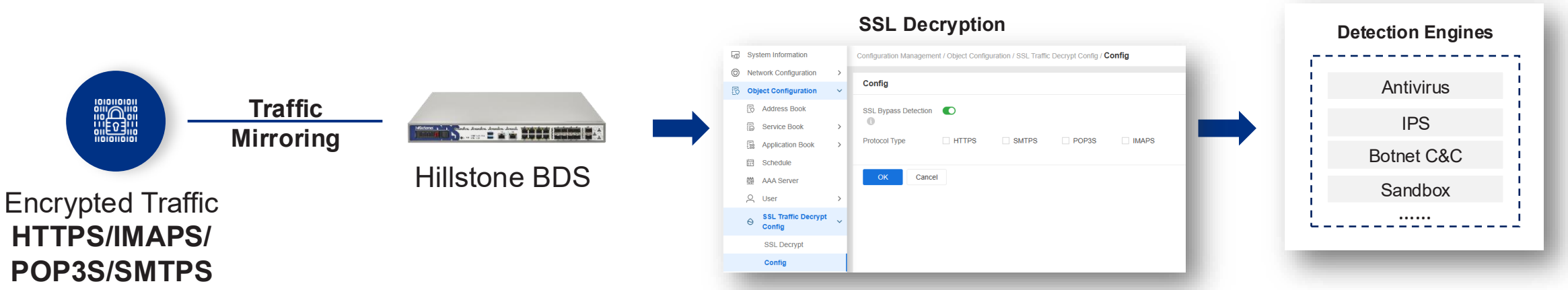
Logging Malicious Verdicts

Log Details

Name	Suspected malicious encrypted traffic	Source	10.
Severity	Low	Destination	10
Attacker	10	Victim	10
Application/Protocol	HTTPS/TCP	Start Time	2023/12/19 18:15:44
Action	Log Only	End Time	2023/12/19 18:15:44
Source Interface	ethernet0/3	Destination Interface	ethernet0/3

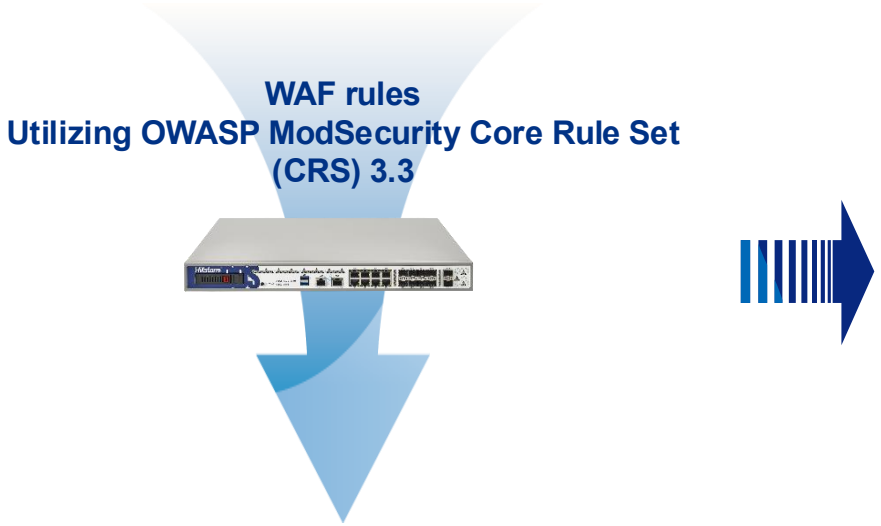
Leverage AI-powered technology to detect abnormal encrypted traffic without decryption

Detection: Threat Detection for Encrypted Traffic with SSL Decryption in TAP Mode



Comprehensive Threat Detection for Encrypted Traffic with SSL Decryption in TAP Mode

Detection: WEB Attacks Detection

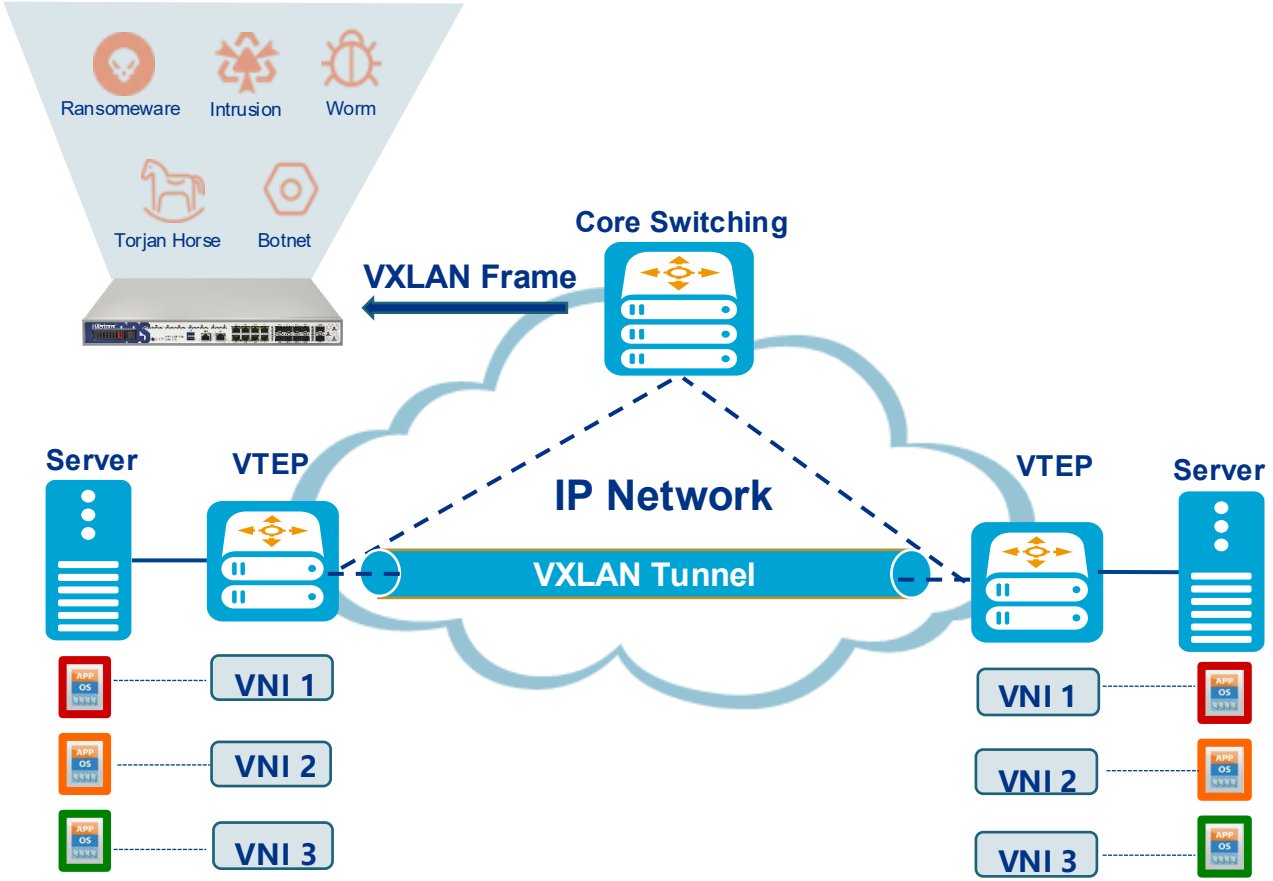


Detect and analyze threats for WEB servers and applications

WEB Attacks Detection

DDoS Attack	Injection Attack
Cross-site Attack	
Abnormal HTTP	Special Vulnerability Attack
Information Leakage	Malicious Software
Illegal Access to Resources	Malicious Network Scanning

Detection: VxLAN Frame Detection

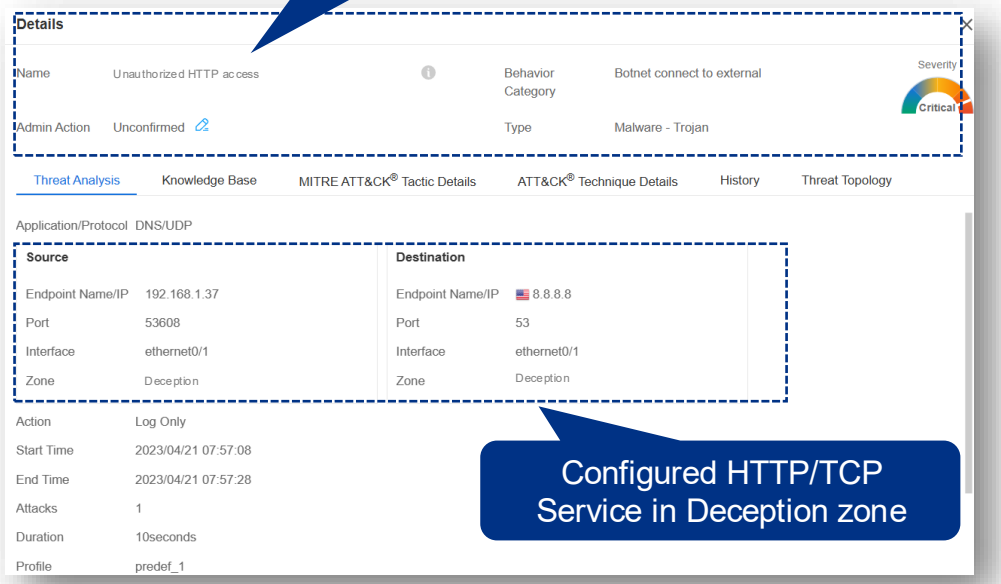


Detect VXLAN frame with UDP port 4789 as the destination port

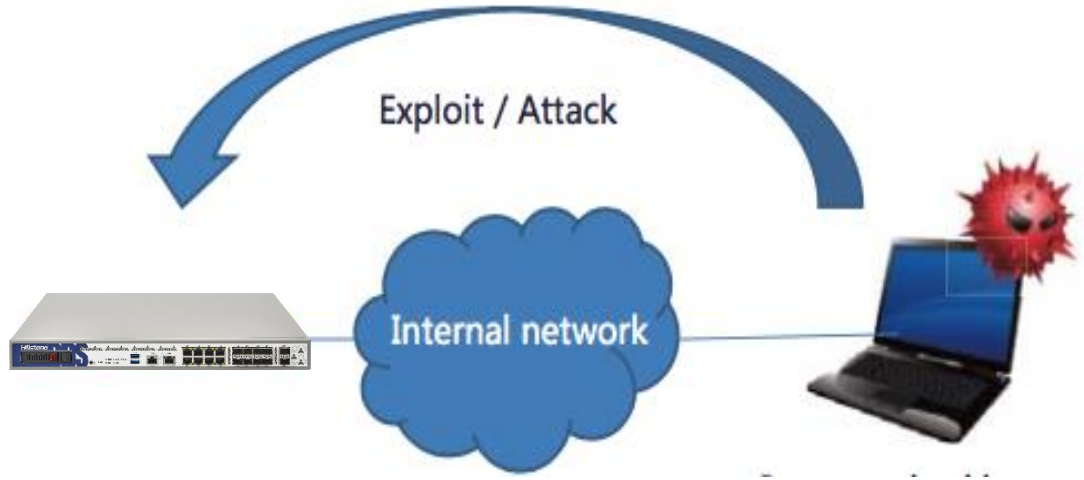
Do NOT detect non-VXLAN traffic whose destination port is UDP 4789

Detection: Deception Technology

Unauthorized HTTP access detected by Deception engine



Configured HTTP/TCP Service in Deception zone



Simulate services in Deception zone, when a hacker visits these services, the attack will be detected

Detection: Dual Antivirus Detection Engine

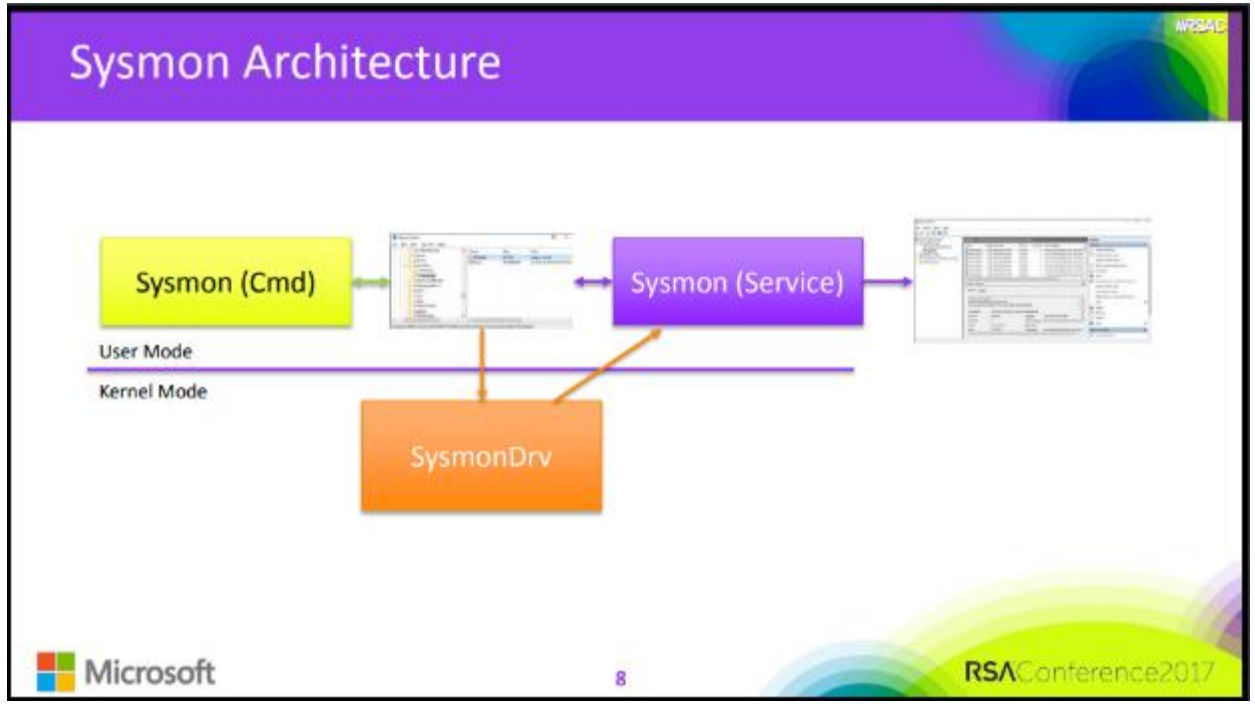
Hash-Based Detection

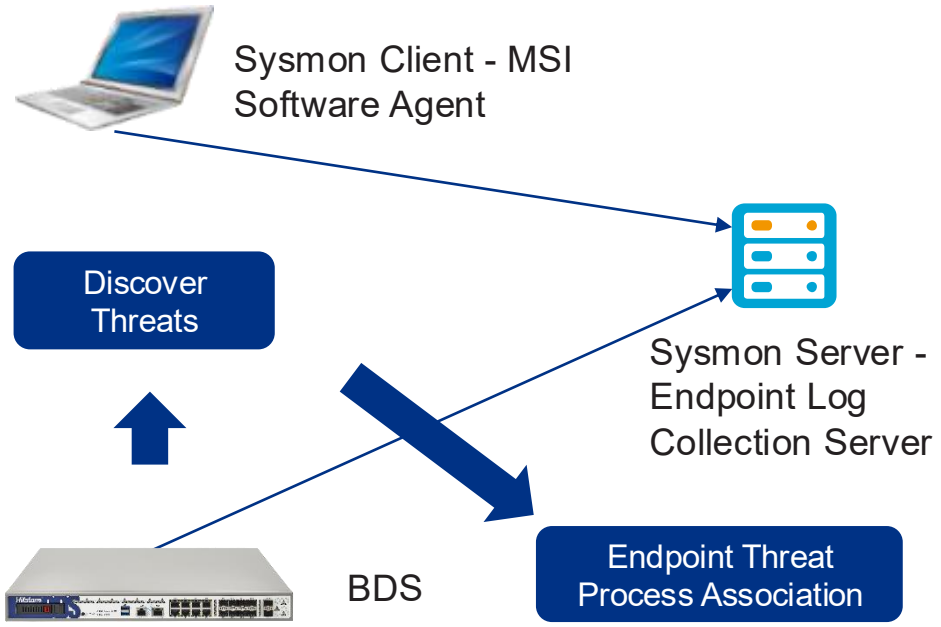
- MD5 file hash-based
- Support all files
- Use Case: Known virus detection

AI-Powered Detection

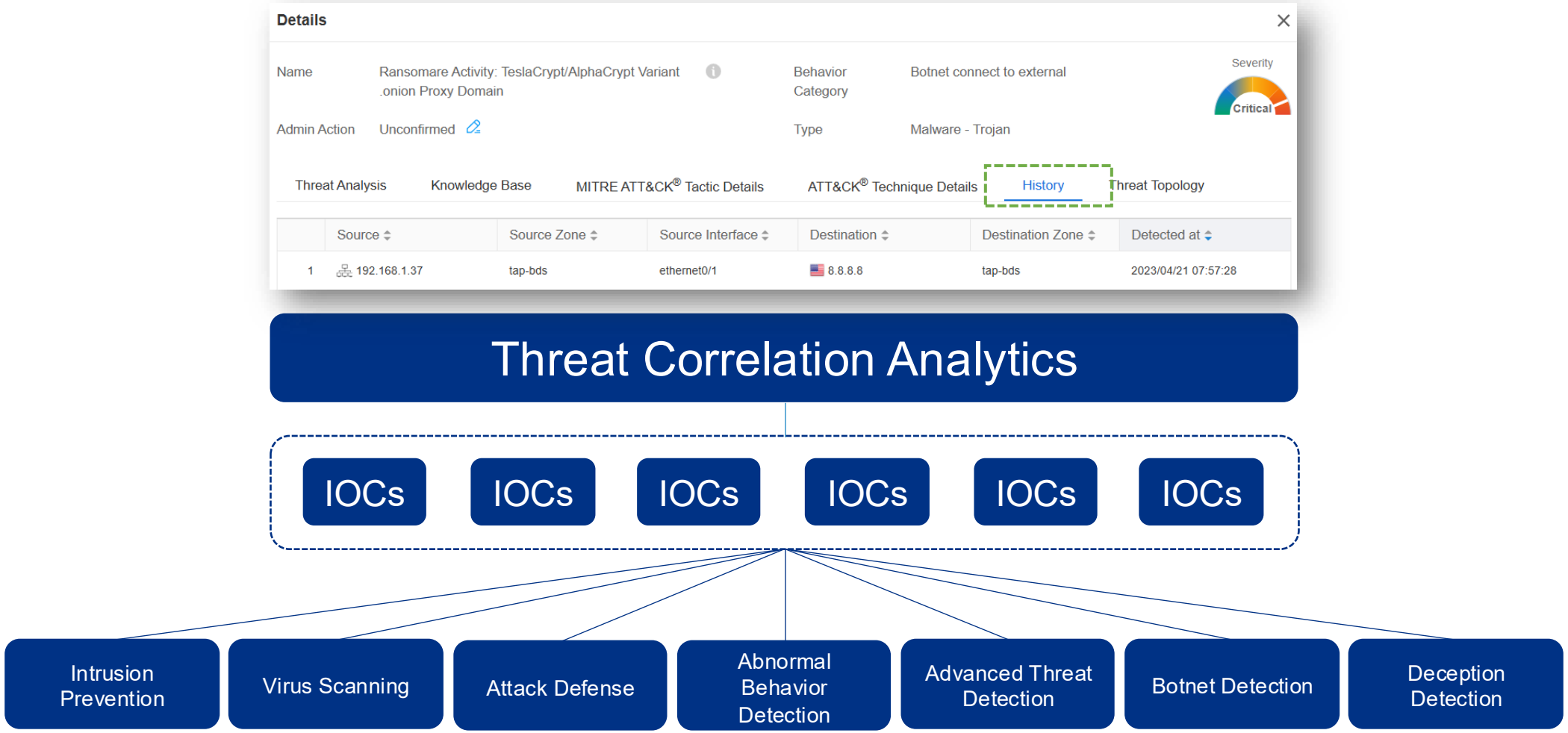
- File characteristics analysis
- Support PE/PDF/Office/ELF files
- Use Case: Unknown/variant viruses detection

Detection: Sysmon Endpoint Service Integration



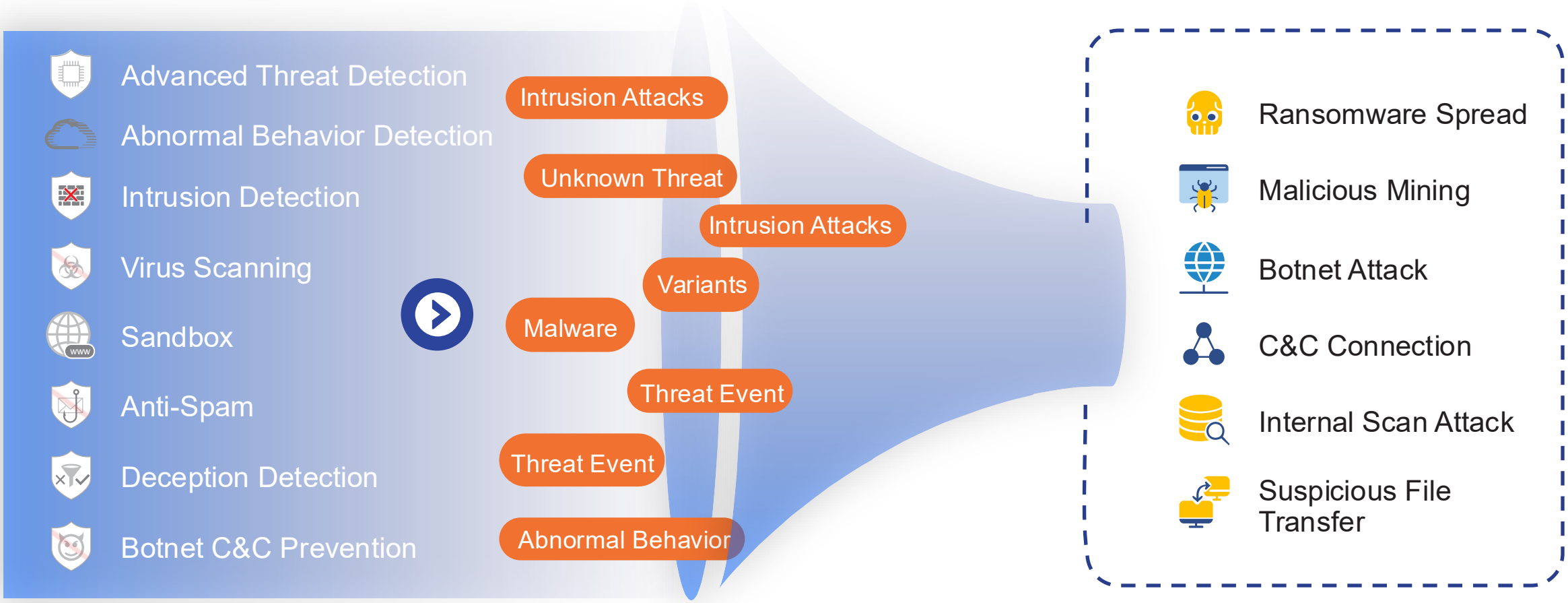


Detection: Detection Efficacy and Lower False Positive



Visibility: Indicator of Compromises (IOCs) Threats

Threat detection engines detect threat events	Threat correlation analysis	IOCs



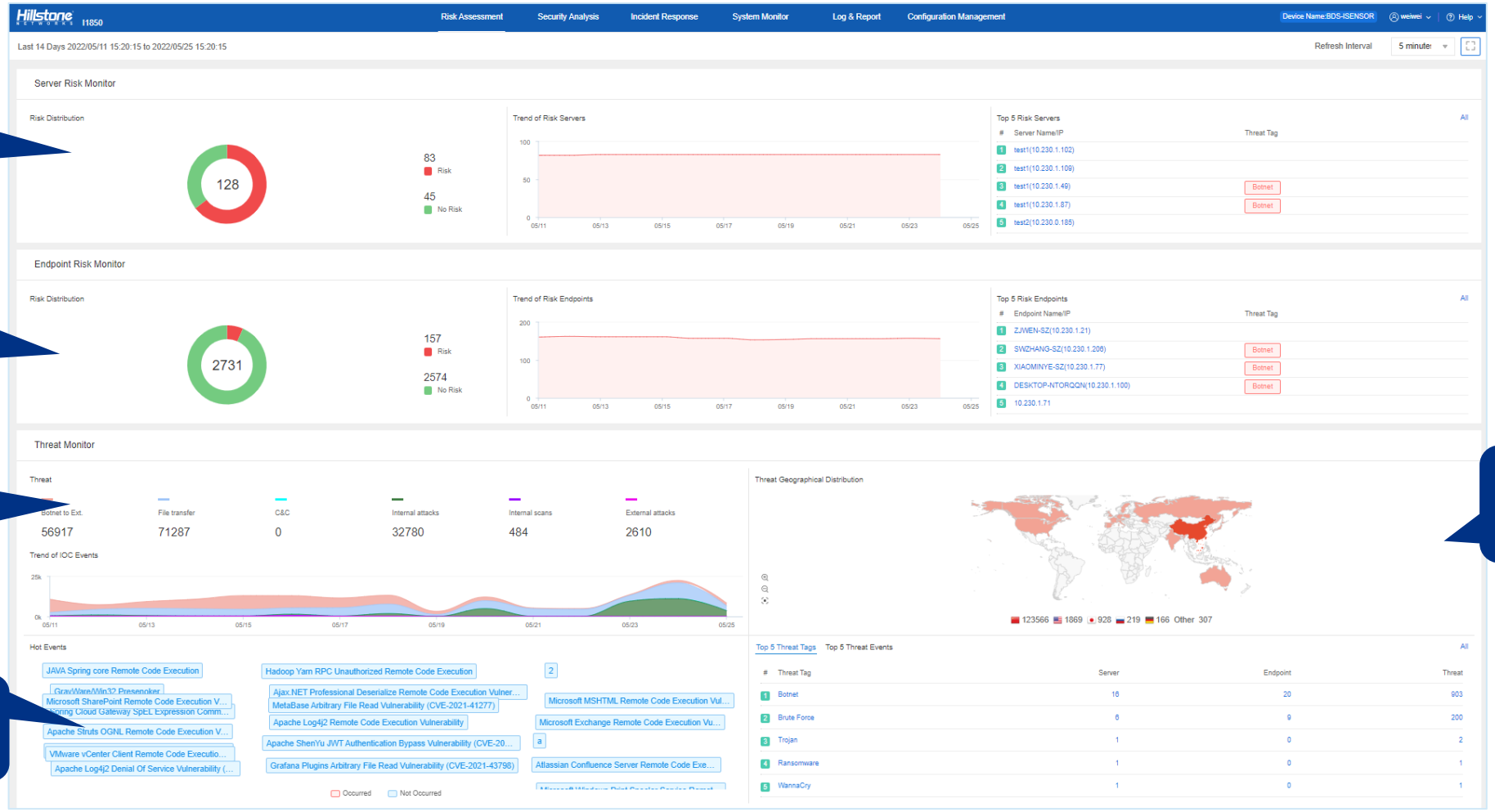
Visibility: Global View of Intranet Threat

Overview of Critical Servers and risk level

Overview of internal host and risk level

Threat type, statistic, historical distribution etc.

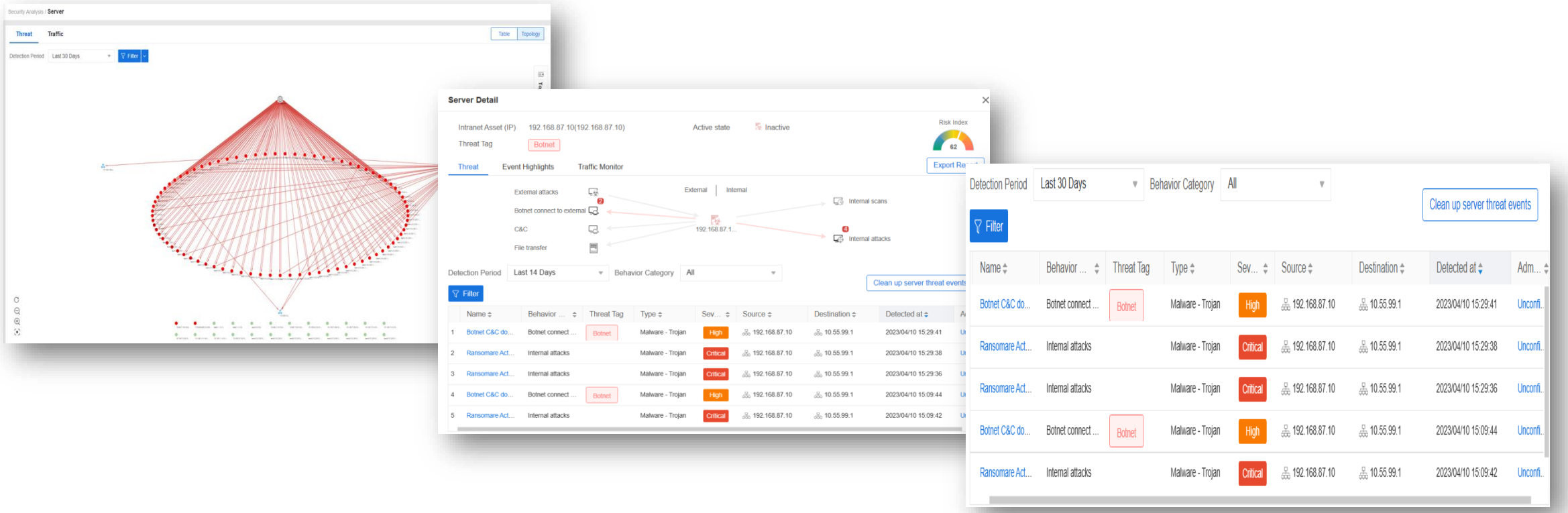
Hot events that need attention



Geo-location threat distribution and top threat

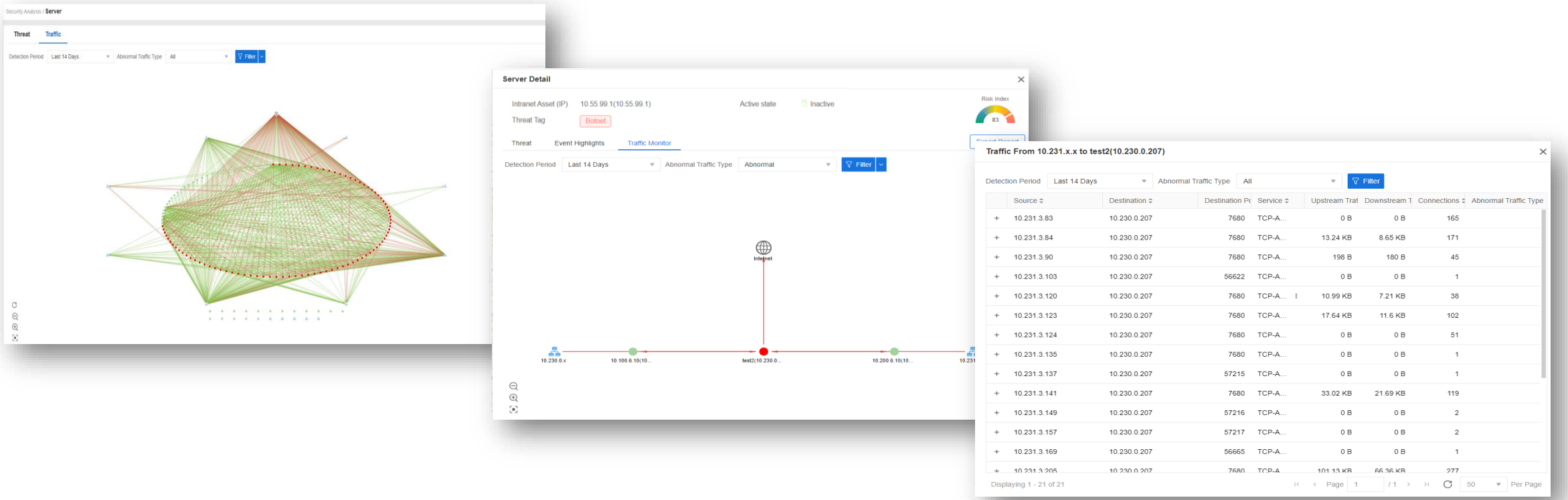
Visibility: Intranet Risk Monitoring Dashboard

Visibility: Server Threat Monitoring



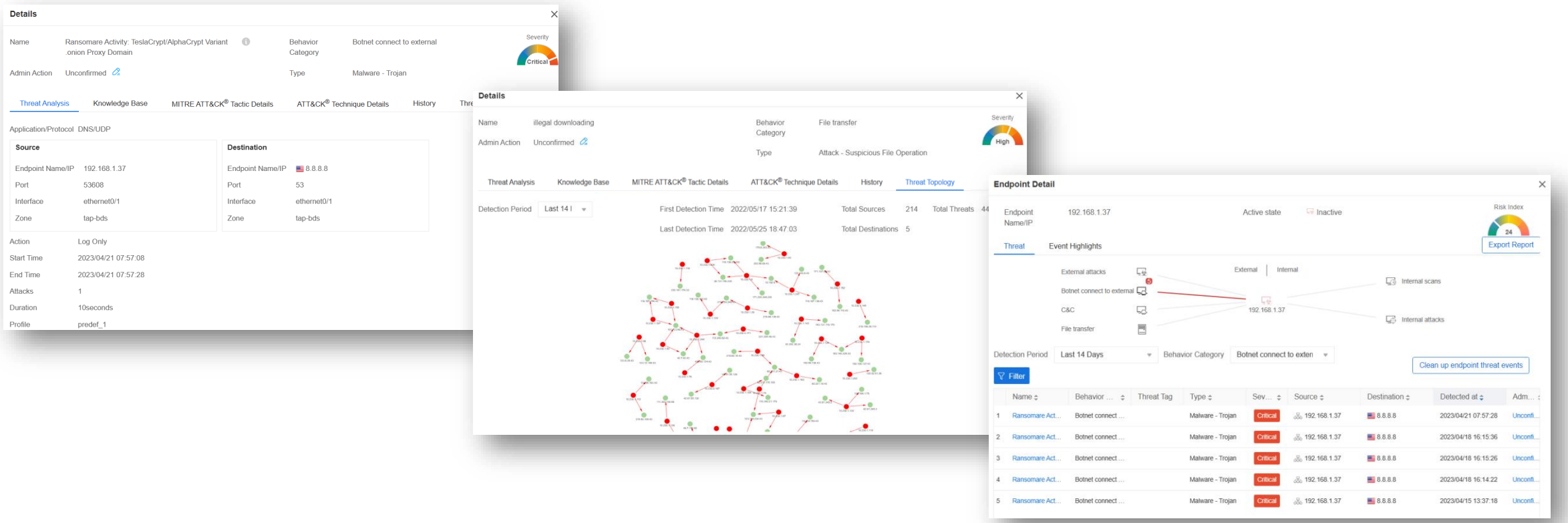
- Server threat topology for intranet servers: attack direction, severity, relationships
- Threat analysis for individual server: 6 types of attack chain
- Threat events list

Visibility: Server Traffic Monitoring



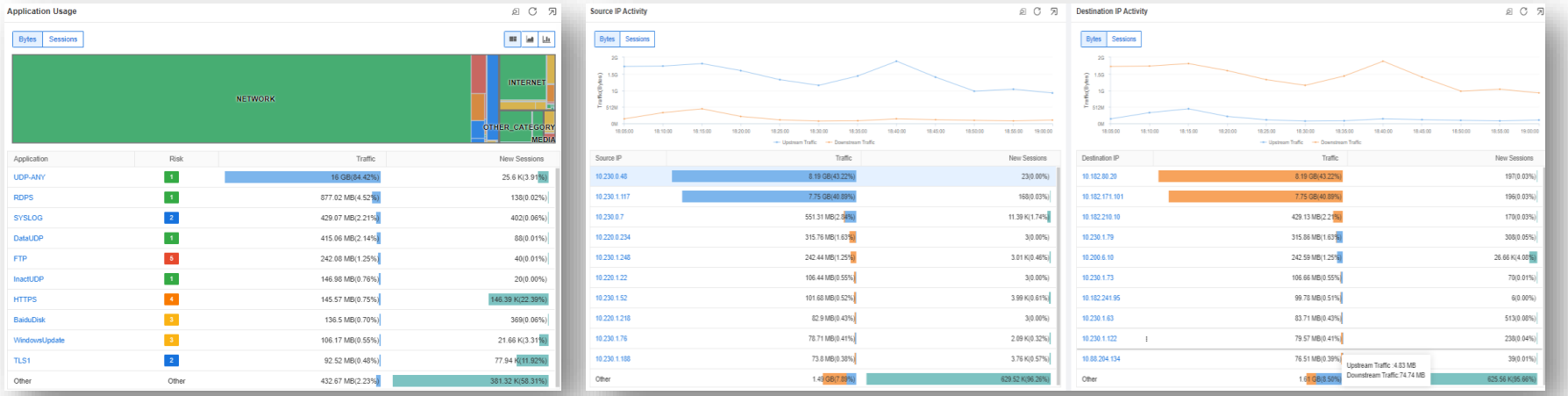
- Server traffic topology for all intranet servers: all traffic relations among all intranet servers
- Server traffic diagram for individual server: traffic in/out of an individual server
- Traffic activity list: all traffic activities between servers

Visibility: Threat Topology

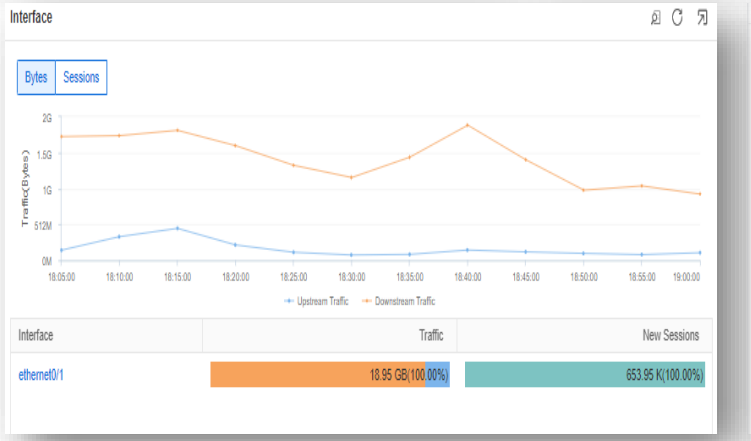


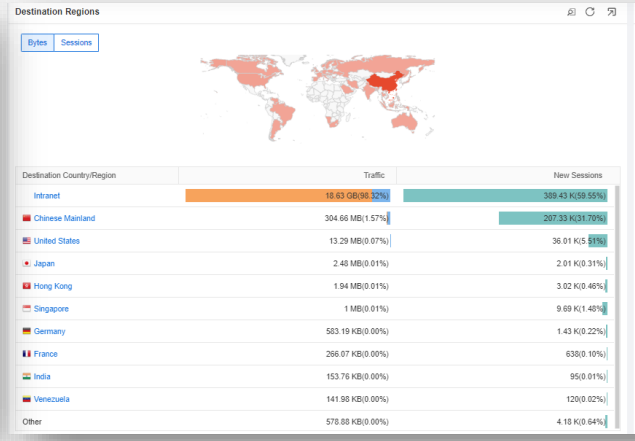
- Details of a threat
- Threat topology that shows the interactions between assets involved in this threat event
- View of the detailed activities of a specific IP in this threat topology

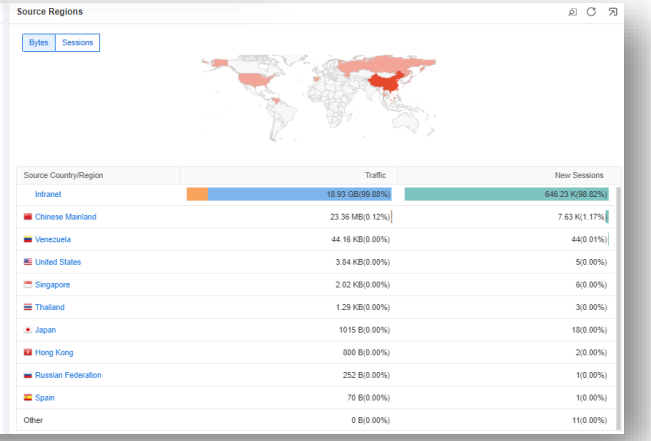
Visibility: Intranet Application Analysis



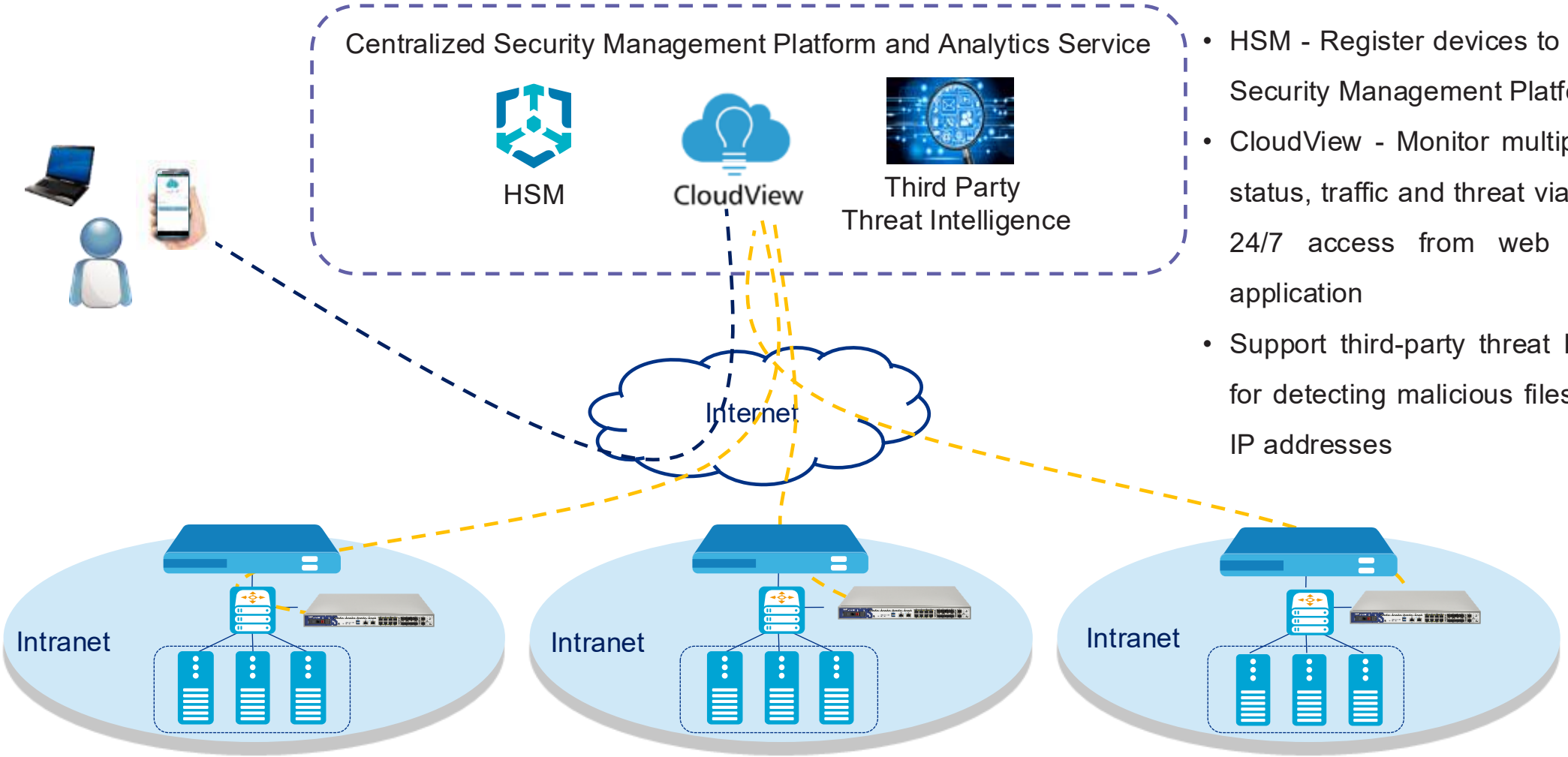
- Application Usage/Ranking
- Source/Destination IP traffic ranking
- Interface Traffic Ranking
- Threat Geo-location





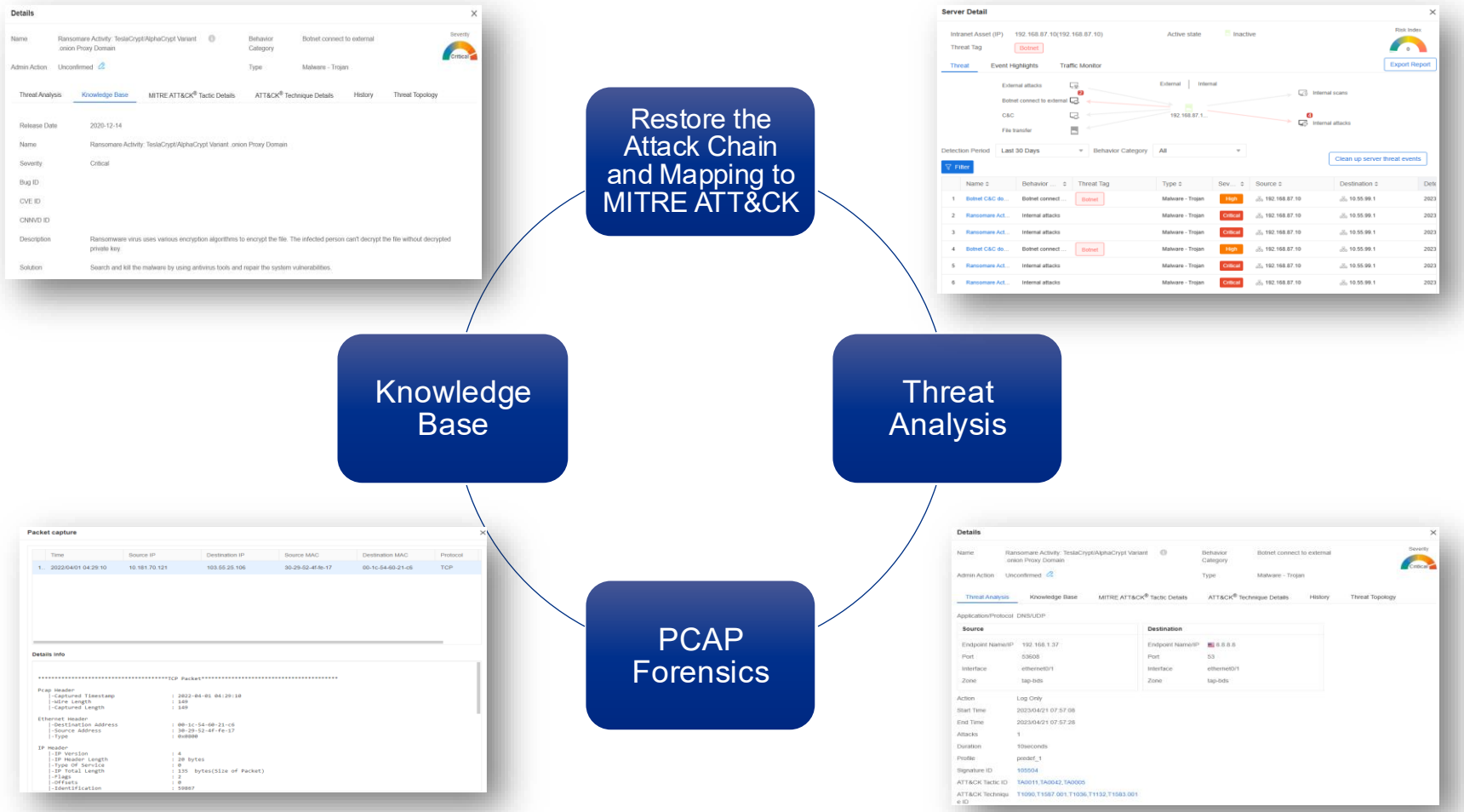


Visibility: Centralized Security Management



- HSM - Register devices to centralized Security Management Platform
- CloudView - Monitor multiple devices status, traffic and threat via cloud with 24/7 access from web or mobile application
- Support third-party threat Intelligence for detecting malicious files, URL and IP addresses

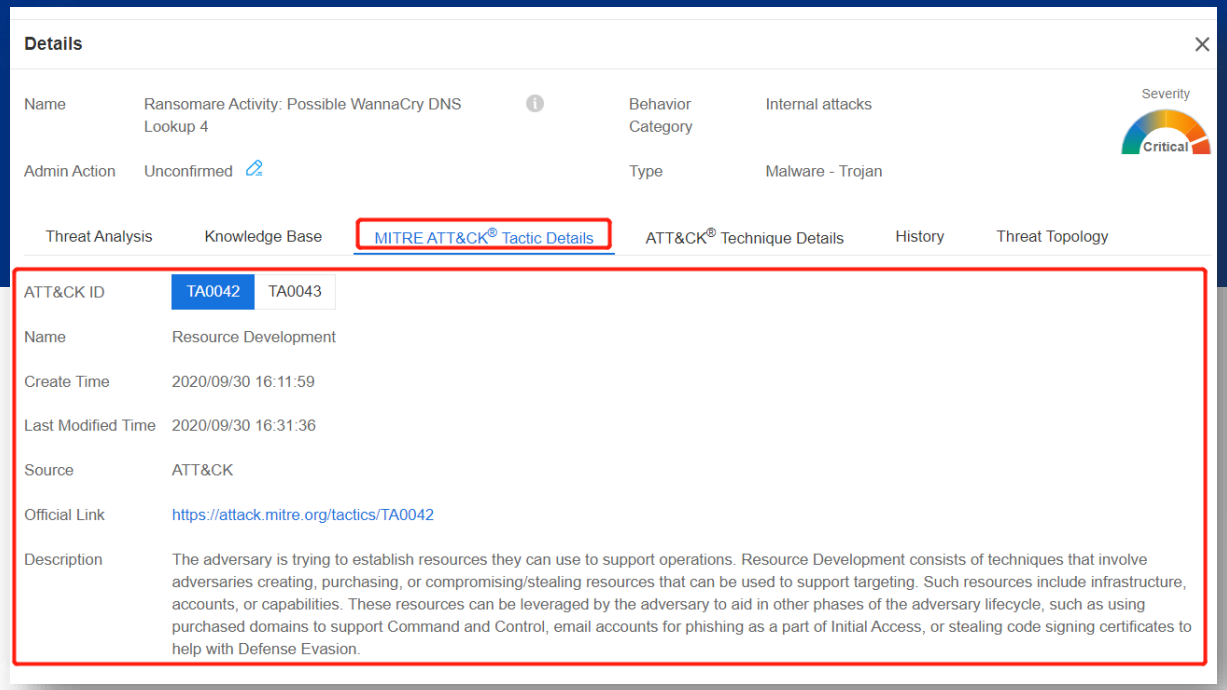
Digital Forensics Analysis: Rich Forensics Enables Risk Assessment



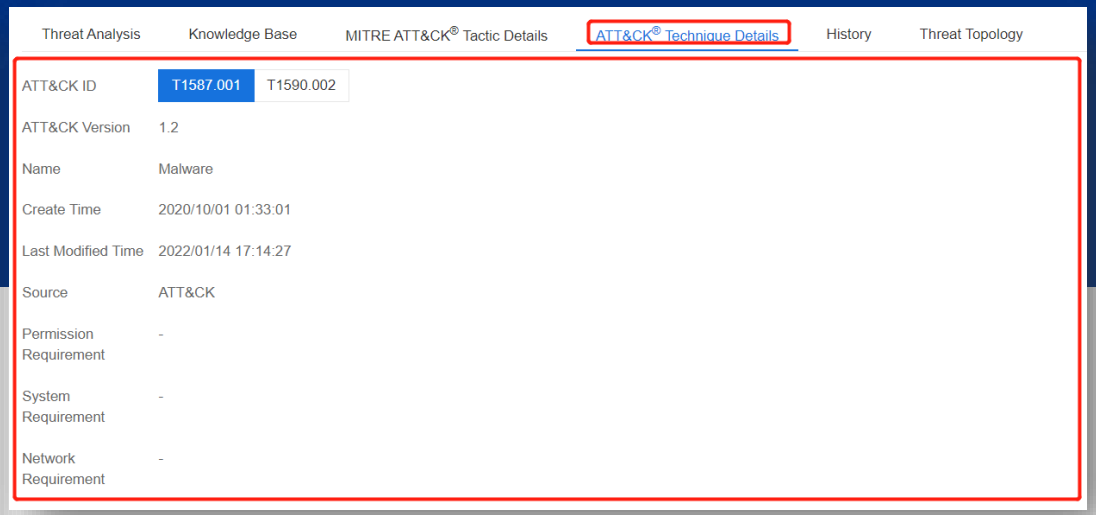
Digital Forensics Analysis: MITRE ATT&CK Framework Mapping

MITRE ATT&CK®

Stands for Adversarial Tactics, Techniques, and Common Knowledge, is a globally recognized framework developed by the MITRE Corporation to classify and describe the potential threat behaviors.

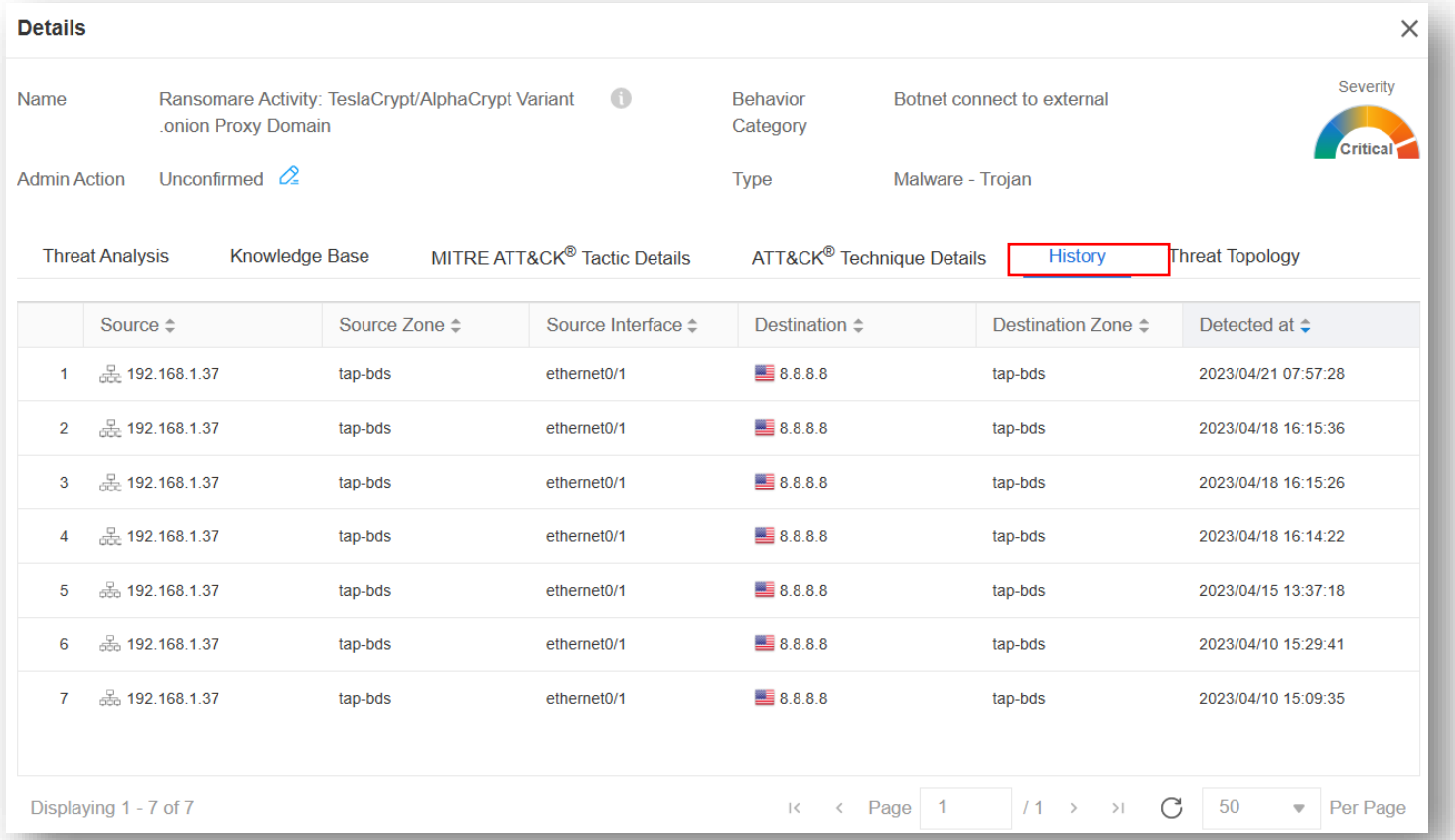


ATT&CK tactic details of threat events



ATT&CK technique details of threat events

Digital Forensics Analysis: Threat Behavior Details



Information tracking for threat events:

- IP, port scanning
- Brute-force cracking of common services such as FTP, LDAP, and MySQL
- Abnormal HTTP access response
- C&C connection

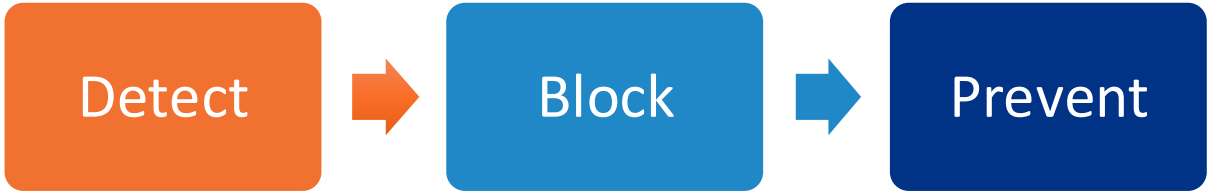
Response: Mitigate Attacks with Hillstone & Third-party Security Devices

Hillstone NDR

Hillstone NGFW/NIPS

Third-party NGFW

- Detect and identify threat
- Configure linkage with Hillstone NGFW/NIPS or third-party NGFW
- Add the confirmed attacks to block list



- Linked with Hillstone NDR
- Synchronize block list from Hillstone NDR
- Block the attacks

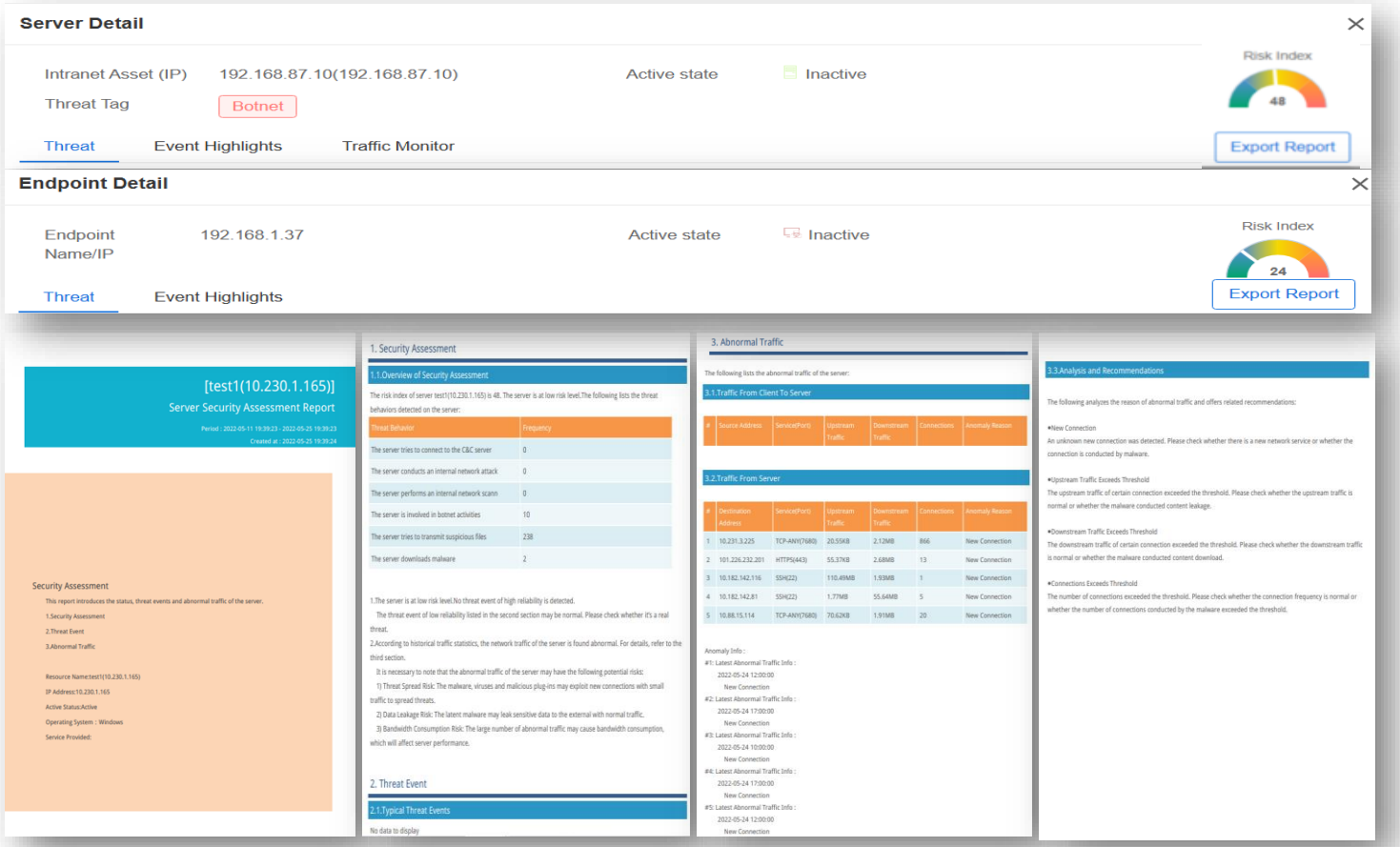
Response: Detect and Respond to Threats with Hillstone XDR

Under the scenario of integrating with Hillstone XDR:

- NDR uploads data* (threat log/ evidential packets/ metadata/ netflow) to XDR
- NDR can perform active assets scanning task delivered by XDR, and uploads the results to XDR
- Support various types of detection and analysis for advance threats and attacks, including signature based detection, correlation analysis, NTA, etc.
- Provide full visibility and automated response to the integrated security products like NGFWs

*Note: Threat log, metadata, and netflow can be uploaded to iSouce V2.0R4-R8; Threat log, evidential packets, and netflow can be uploaded to iSource V2.0R9 or later

Report: Host Risk Assessment

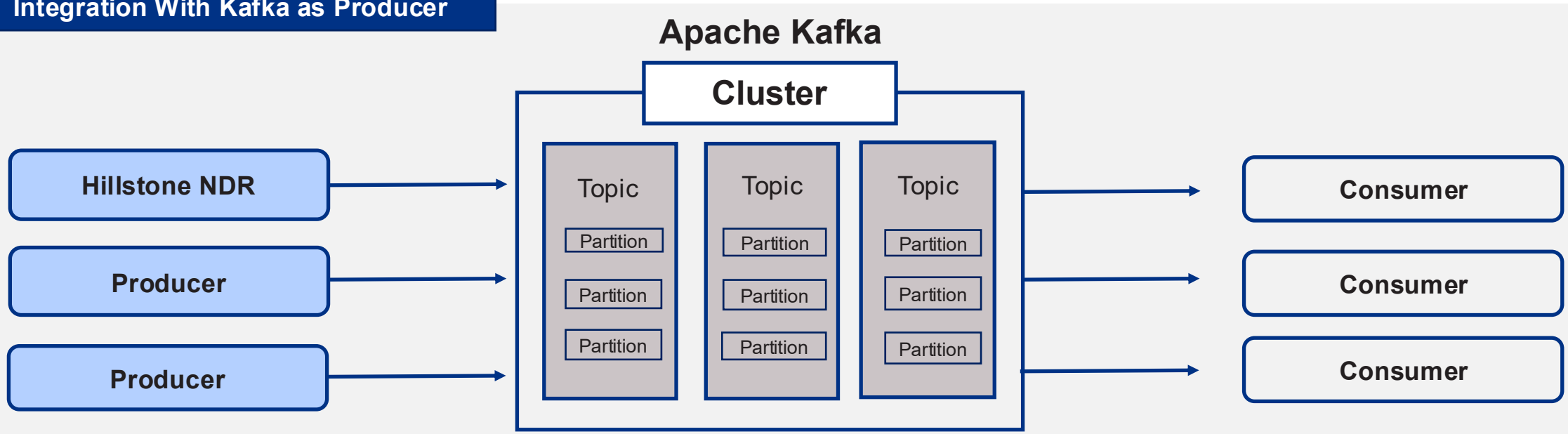


On the risk server or risk endpoint page, the threat and traffic information matching the current interface filtering conditions are exported. A PDF report is generated, which includes the following information:

- Server/endpoint information
- Security status assessment
- Threat event
- Abnormal traffic
- Analytical and disposal recommendations

Third-Party Integration

Integration With Kafka as Producer

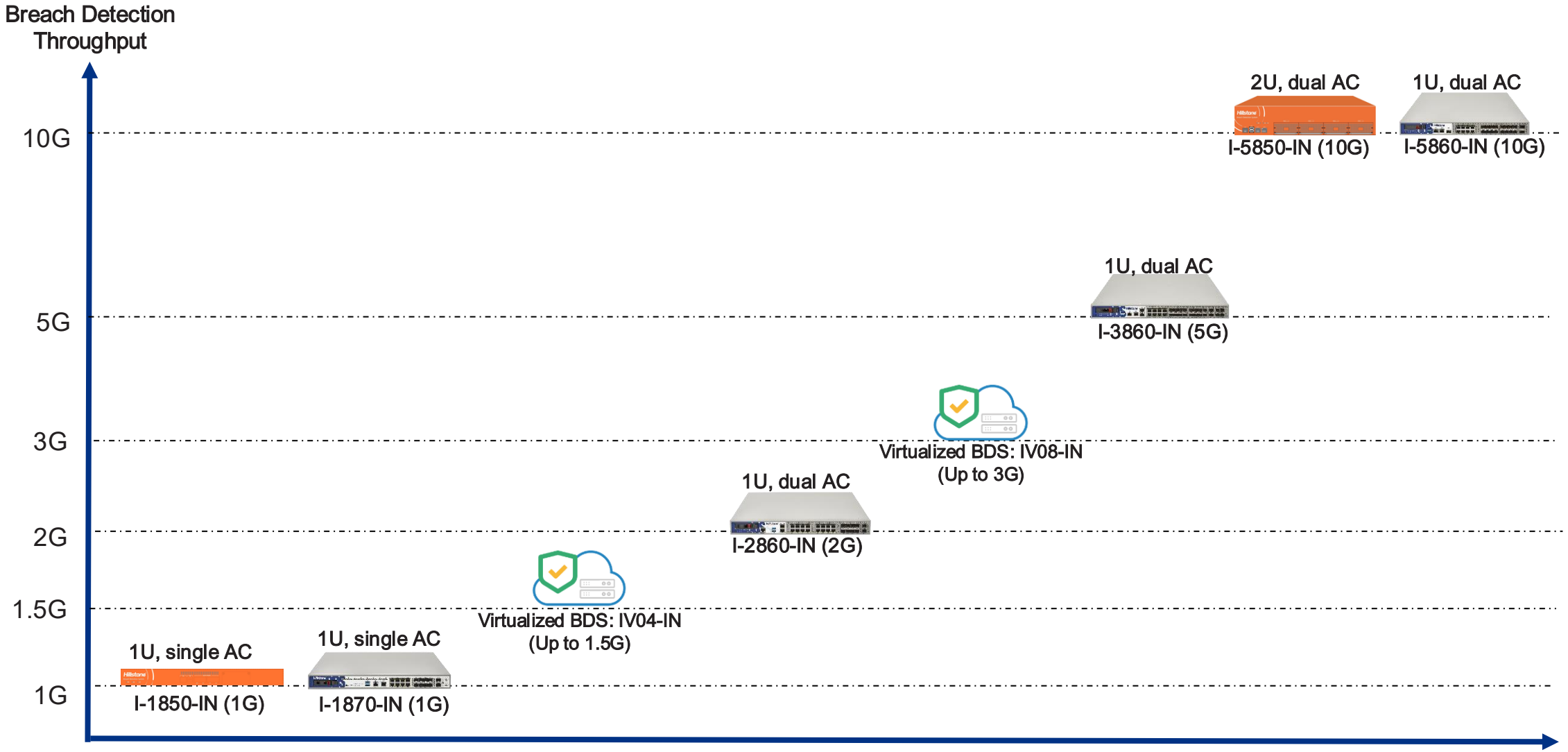


Forwarding logs via Syslog

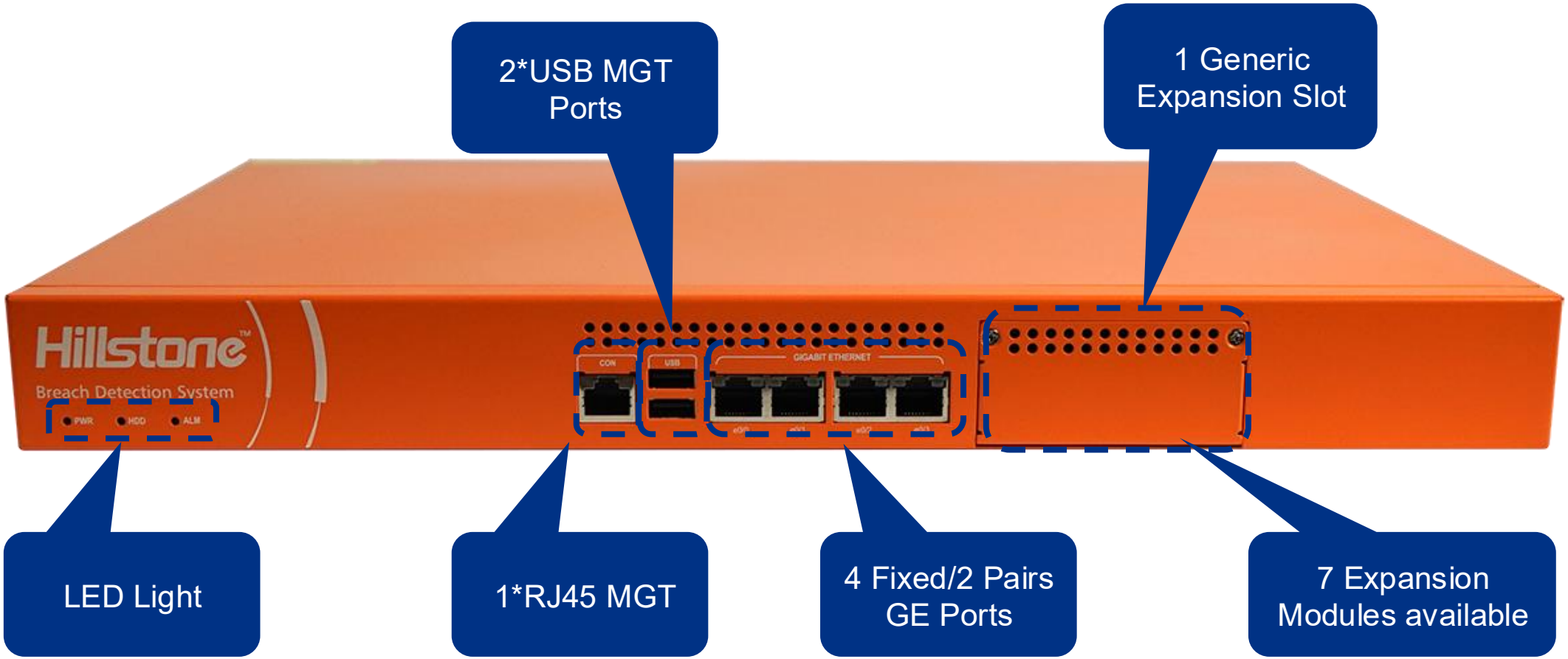
Closed Cycle: Network Detection and Response

Hillstone NDR Product Portfolio

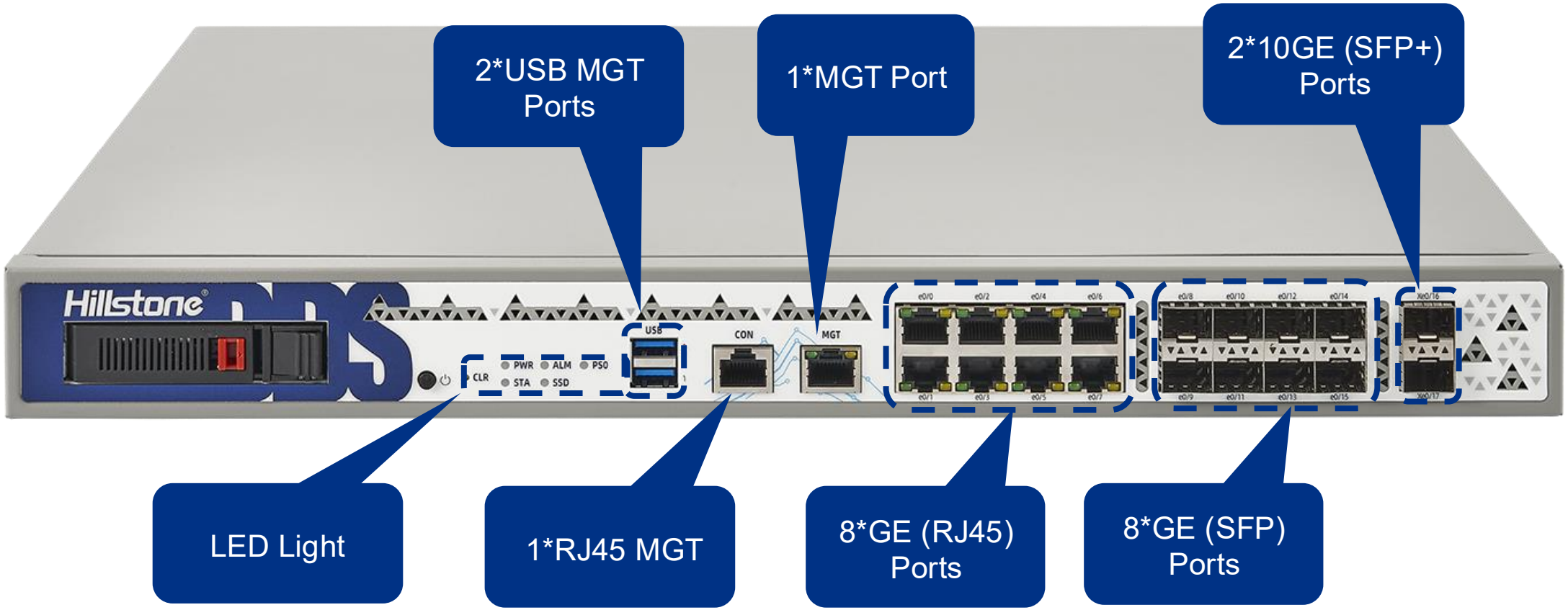
Hillstone NDR Product Portfolio



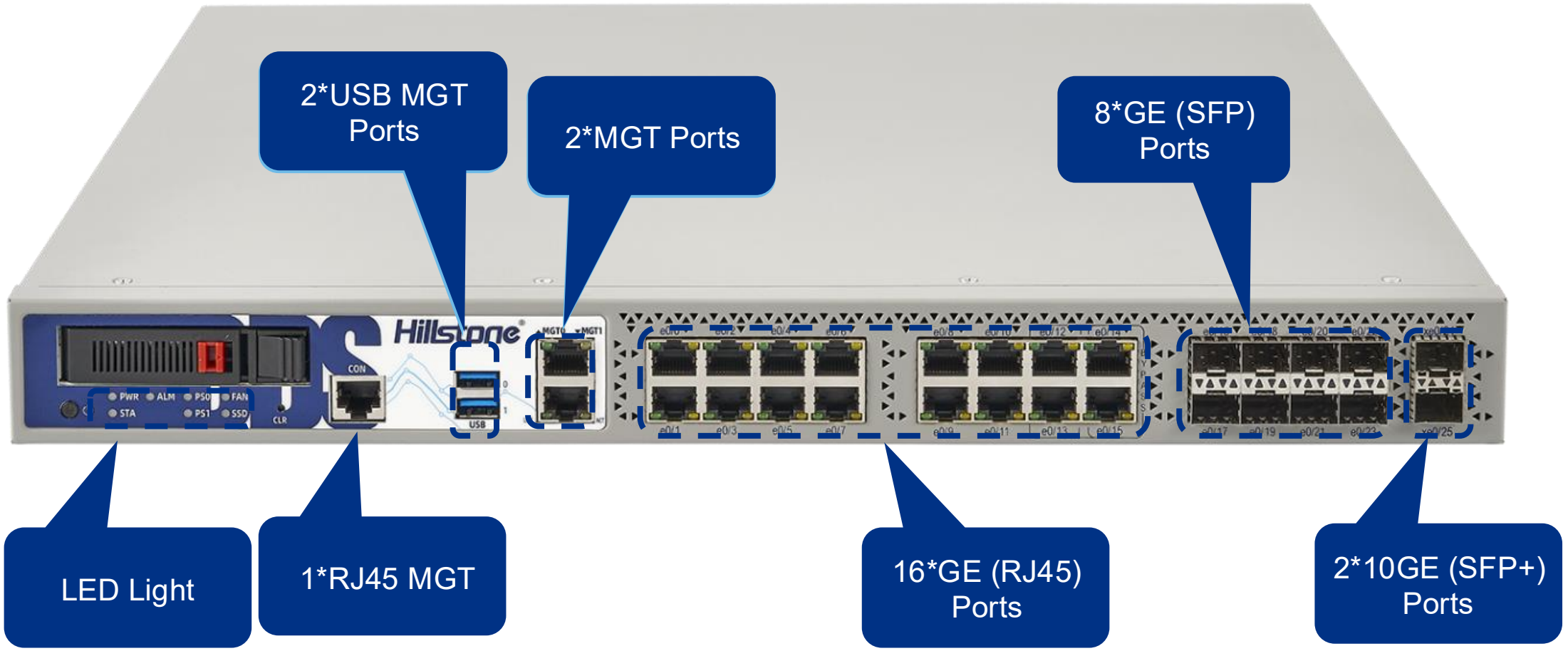
I-1850 Hardware Specification



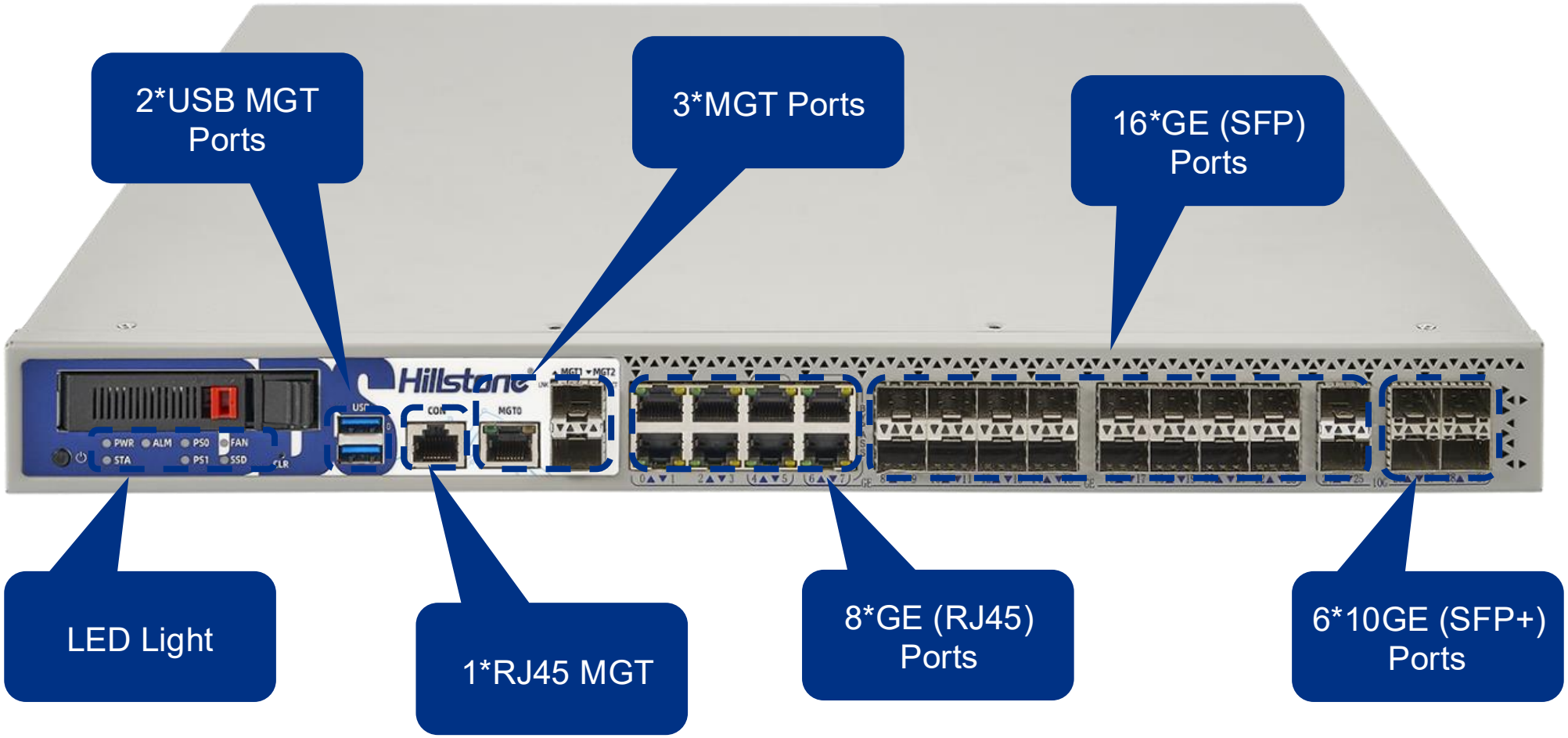
I-1870 Hardware Specification



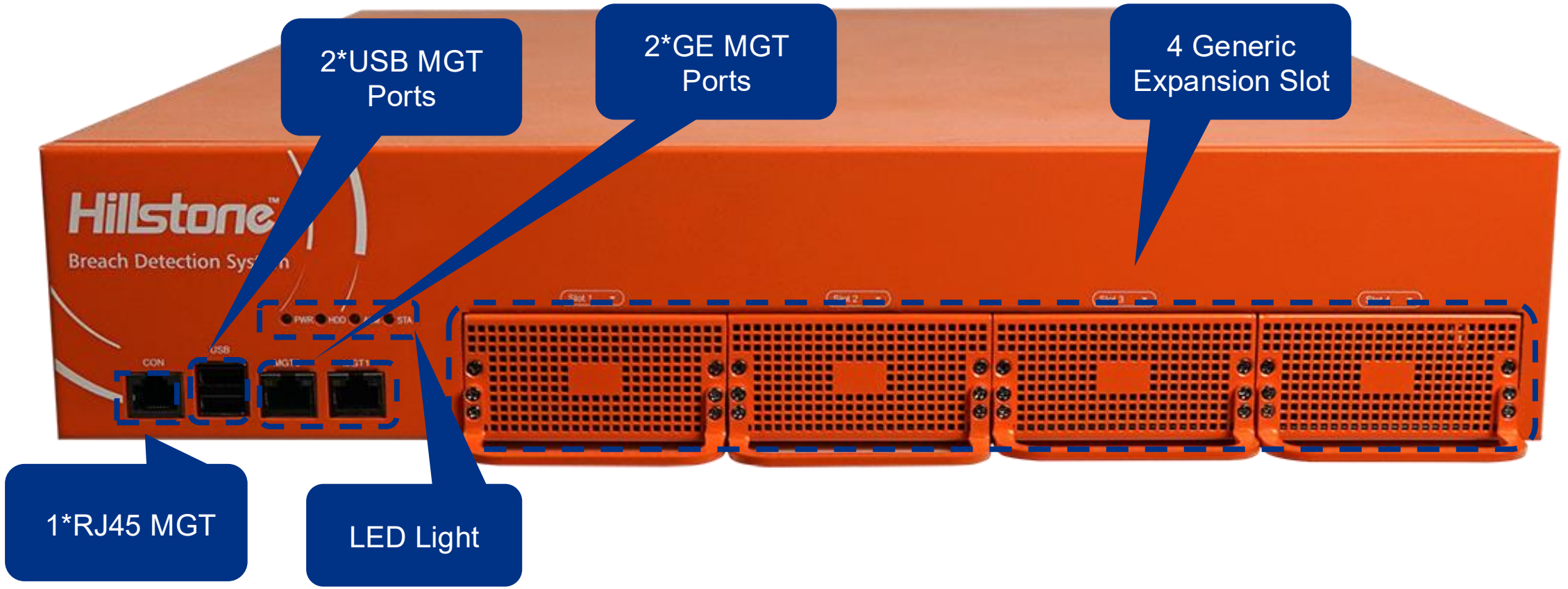
I-2860 Hardware Specification



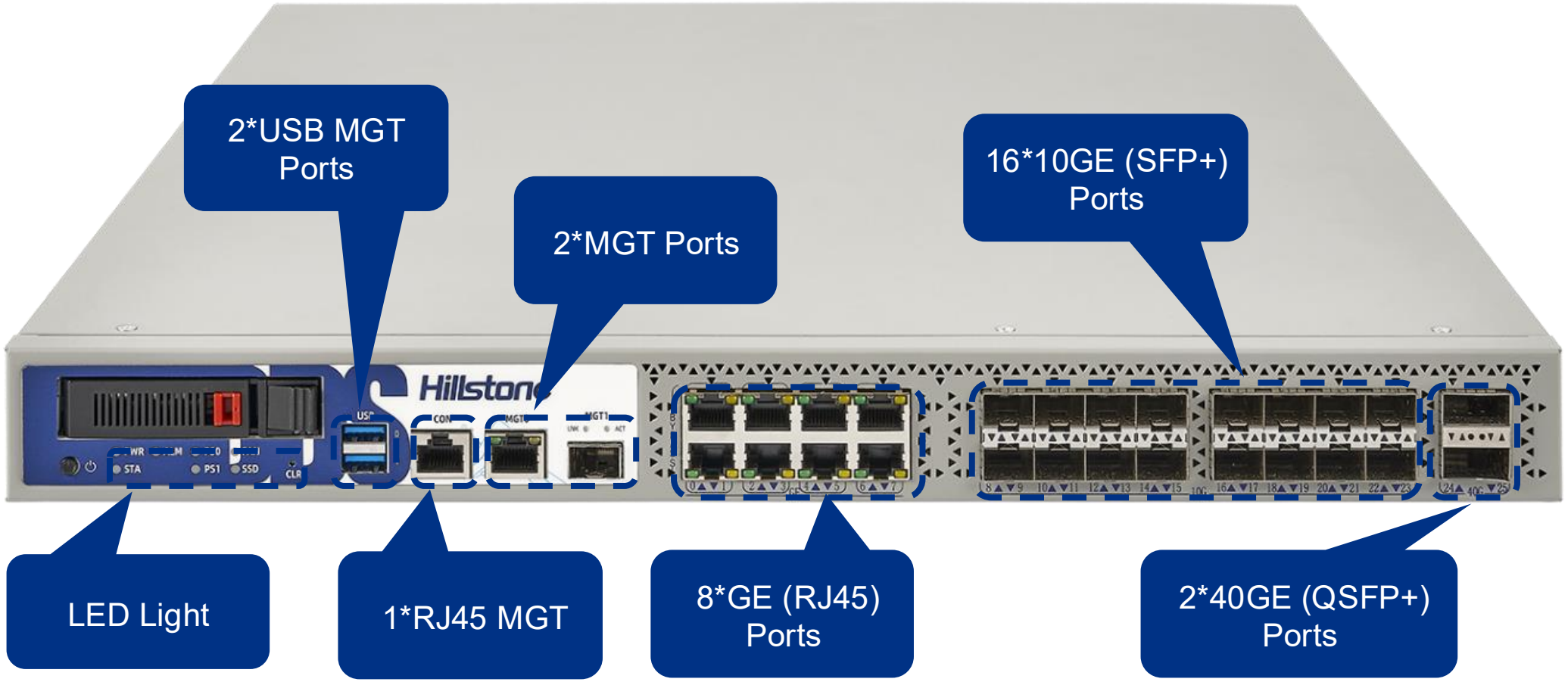
I-3860 Hardware Specification



I-5850 Hardware Specification



I-5860 Hardware Specification



NDR Hardware Specification

Model	I-1850-IN	I-1870-IN	I-2860-IN	I-3860-IN	I-5850-IN	I-5860-IN
Breach Detection Throughput	1 Gbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps	10 Gbps
New Sessions/s	20,700	32,000	75,000	210,000	250,000	500,000
Maximum Concurrent Sessions	750,000	750,000	1,500,000	3,000,000	6,000,000	6,000,000
Form Factor	1 U	1 U	1 U	1 U	2 U	1 U
Storage	1T HDD	1T SSD	1T SSD	1T SSD	1T HDD	2T SSD
Management Ports	2 x USB port 1 x RJ45 port	2 x USB port 1 x RJ45 port 1 x MGT	2 x USB port 1 x RJ45 port 2 x MGT	2 x USB port 1 x RJ45 port 3 x MGT	2 x USB port 1 x RJ45 port 2 x MGT	2 x USB port 1 x RJ45 port 2 x MGT
Fixed I/O Ports	4 (2 Pairs) GE ports	2×10GE (SFP+) 8 × GE (SFP) 8 × GE (RJ45)	2×10GE (SFP+) 8 × GE (SFP) 16 × GE (RJ45)	6×10GE (SFP+) 16×GE (SFP) 8×GE (RJ45)	N/A	8×GE (RJ45) 16×10GE (SFP+) 2×40GE (QSFP+)
Available Slots for Expansion Modules	1	N/A	1	1	4	1
Expansion Module Option	IOC-S-4SFP-L-IN	N/A	IOC-A-4SFP+-IN	IOC-A-4SFP+-IN	IOC-BDS-8GE-H-IN, IOC-BDS-8SFP-H-IN, IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN

Virtualized Product Specification & Configuration

Specification and minimum hardware configuration:

Model	IV04-IN	IV08-IN
Breach Detection Throughput *	Up to 1.5 Gbps	Up to 3 Gbps
CPU Support	4 Core	8 Core
Memory	8G	16G
Storage	100G	100G
System Requirement	KVM / Vmware ESXi version 6.5 or above	
Public Cloud Support	Alibaba Cloud / Tencent Cloud	

* The breach detection throughput data depends on the hardware configuration

Network interface card supported:

	SR-IOV	All NICs except SR-IOV
KVM	√ (only SR-IOV X710 can be supported)	√
VMware	×	√

Expansion Modules

Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN	IOC-BDS-8GE-H-IN	IOC-BDS-8SFP-H-IN	IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN
I/O Ports	4 x SFP Ports	4 x GE Ports	8 x GE Ports	8 x SFP Ports	4 x SFP+ Ports	4 x SFP+, SFP+ module not included
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U
Weight	0.22. lb (0.1 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)	0.44 lb (0.2 kg)	2.09 lb (0.96 kg)

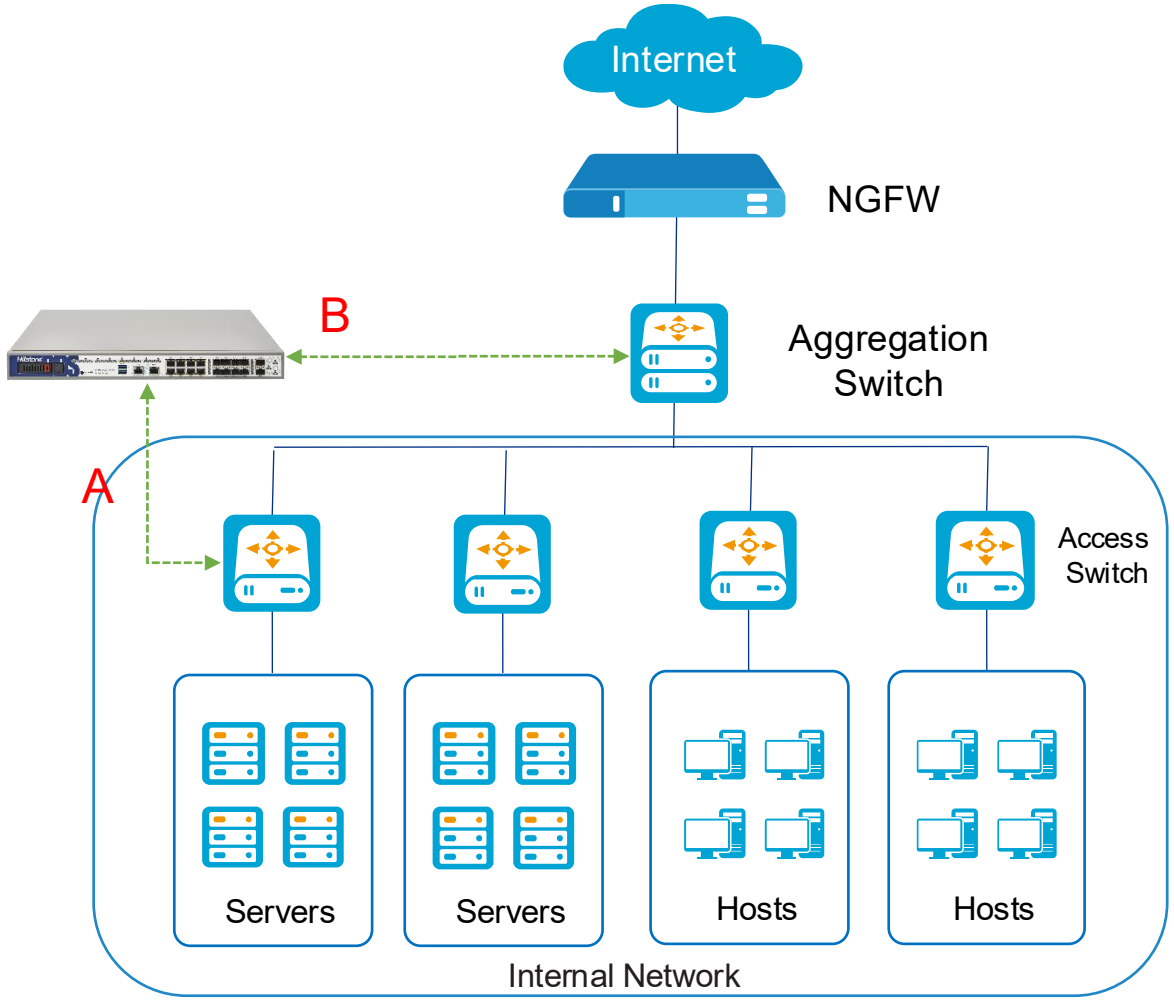
Sysmon Configuration

Specification	Sysmon Server	Sysmon Client
CPU	core*4	\
Memory	16G	1G
Storage	1T HDD, extendable	40G HDD
Installation Package	OVF Mirror	MSI Service Program
Software	VMware ESXi	Windows 7 / Windows Server 2007 or above
Others	• The default configuration supports log storage of 1000 PCs. • Sysmon server stores up to 90 days of data. Data will be automatically deleted (cleaned up) after 90 days. When the disk (/data) usage exceeds 85%, the system will automatically delete the oldest data. • Sysmon Server system has enabled the Log Receiving Service (Logstash) and the Query service (Elasticsearch), using ports 5044 and 9200 respectively.	Two installation methods are available: • direct installation by user • batch installation via Windows Active Directory domain distribution software

- Sysmon Client - Installed on user's computer; used to record the process creation and termination initiated by the computer, as well as network connection information; send the information to the Sysmon Server.
- Sysmon Server - Receive and store the process information log sent by the client software for BDS device query and display.

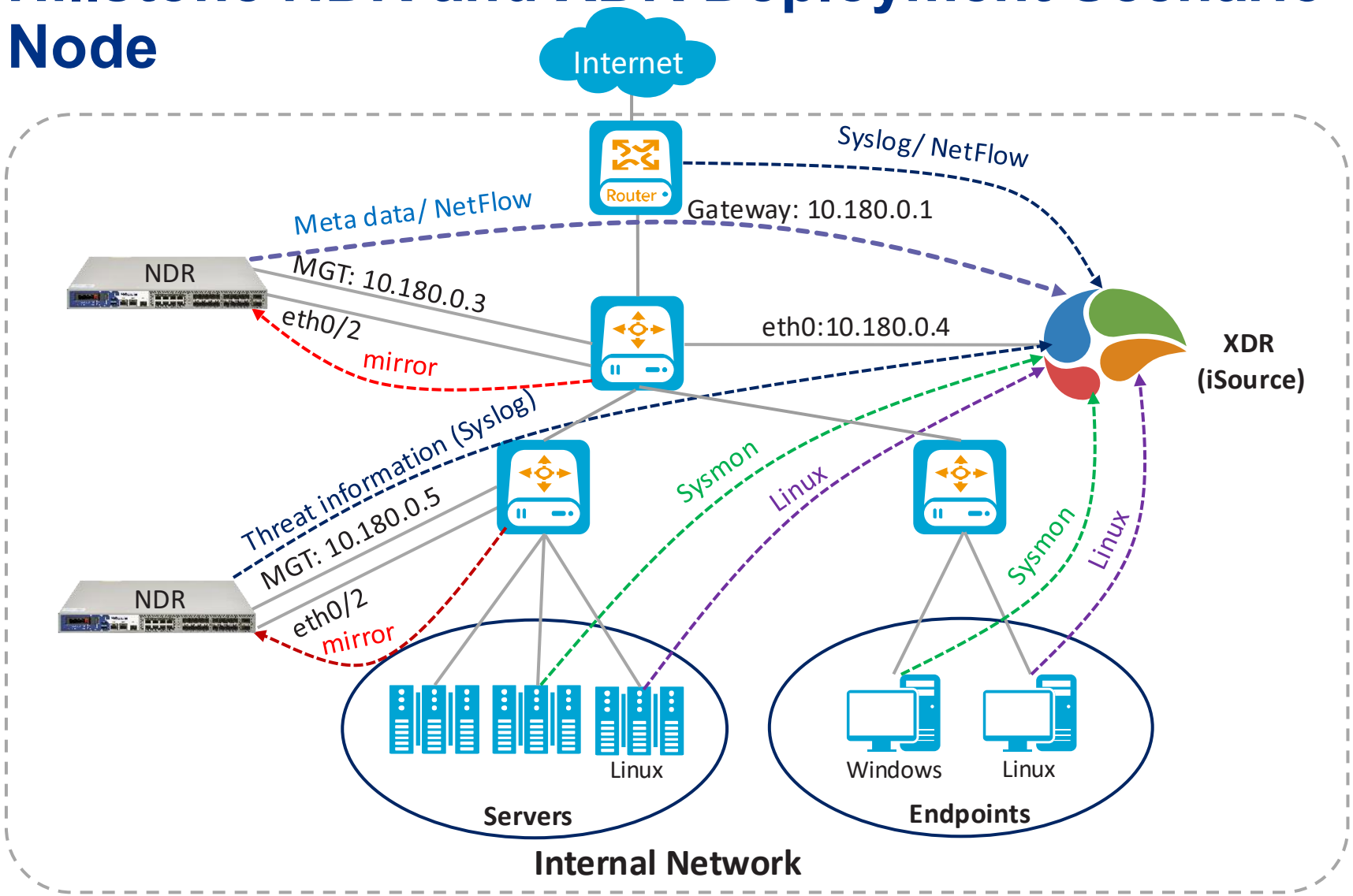
Deployment Scenarios & Case Studies

Hillstone NDR Deployment Scenarios- BDS and NGFW



- ***Scenario A:*** *Access Switch connecting to servers or server groups*
  - Monitor traffic between servers within the same segment; servers in different segments; server and internet; servers and other hosts.
- ***Scenario B:*** *Aggregation switch between Access Switches*
  - Monitor traffic between servers in different segments; servers and internet; servers and other hosts; hosts and internet.
- ***Scenario C:*** *Combination of the above scenarios*

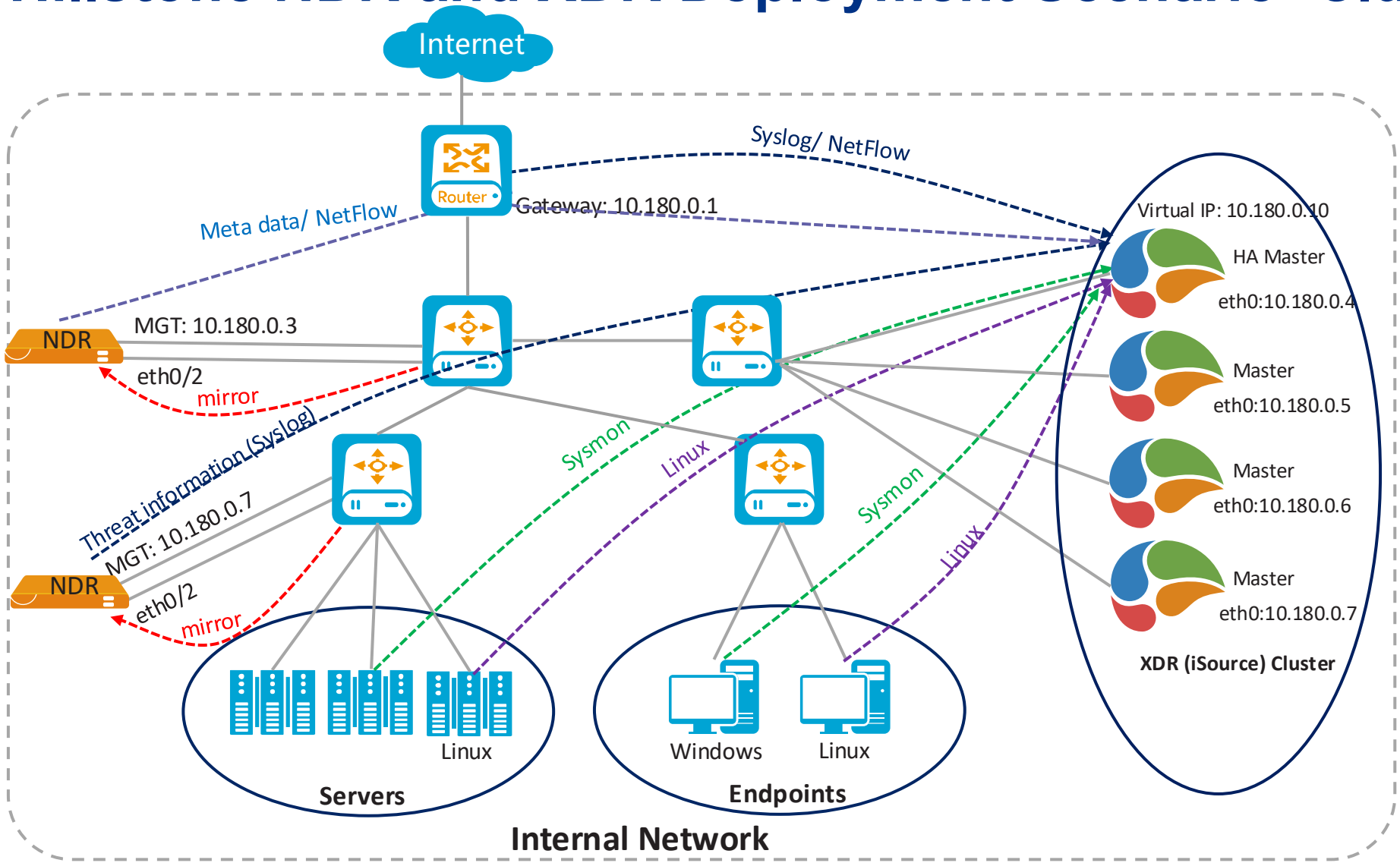
Hillstone NDR and XDR Deployment Scenario- Single Node



Single Node Deployment

- NDR deployed in TAP mode
- XDR deployment has little impact on the existing network environment
- Economic solution

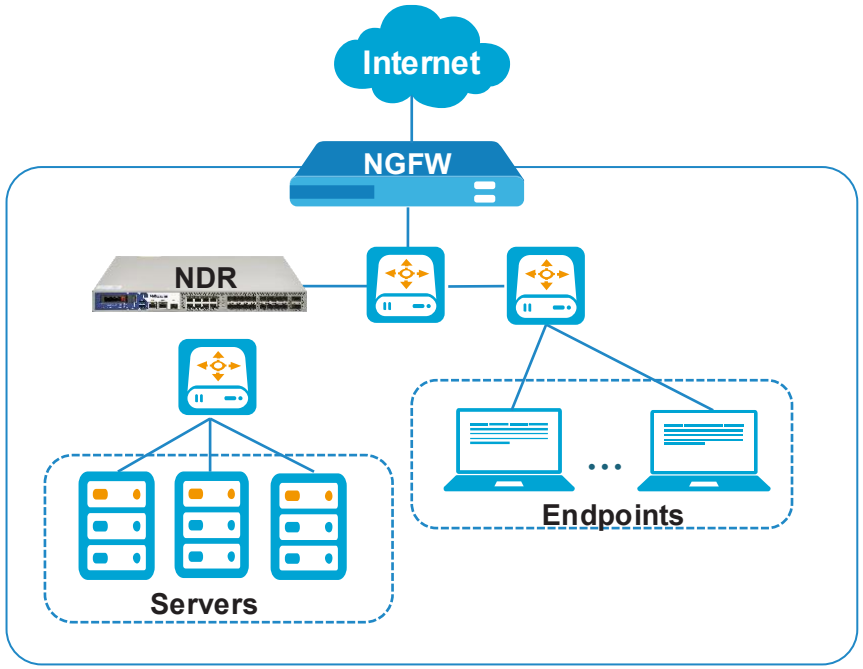
Hillstone NDR and XDR Deployment Scenario- Cluster



Cluster Deployment

- NDR deployed in TAP mode
- Cluster up to 5 nodes
- XDR deployment has little impact on the existing network environment
- Highly scalable solution

Case Study 1: Protect Critical Information for Large University



Customer Profile

- A large private university with an enrollment of more than 10,000 students, located in South America

Challenges

- There are significant number of users connecting or accessing the networks from various devices, often compromising the perimeter security, and generating breaches that could put critical information at risk.
- The potential cyber attacks could impact business continuity, halting access to University web properties.

Hillstone Solution

- The customer deployed Hillstone NDR in conjunction with Hillstone T-Series intelligent next generation firewalls (iNGFW).
- The intelligence security features of Hillstone BDS and iNGFW – ML-based detection of behavior and threats, helped achieve detection and prevention from the perimeter to the internal network.
- A critical attack was detected by this solution deployed, which would have caused an enormous breach in internal services, as well as compromised data.

Case Study 2: Secure Critical Assets for A Regional Government in Latam

Customer Profile

- A regional government with administrative, political and economic autonomy in South America

Challenges

- Organizations constantly conduct operations and procedures online, managing a massive flow of information as well as money. There is a great need to protect these information and assets due to the ever growing wave of cyber-attacks in the world.
- The customer needs to minimize the threat to the services it provides, as well as to guarantee the availability of the applications used by the personnel.

Hillstone Solution

- The customer deployed Hillstone NDR to fully protect their internal network. It can effectively identify advanced threats that lurk within an internal network, and affected from BYOD (bring your own device) of the organization employees.
- The deployed solution protected the customer from threats by detecting the use of devices and access to data that appear abnormal in their network. And also allowed the customer to adopt measures to avoid attacks.

Case Study 3: Detect Locky Ransomware for a Pharmaceutical Company

Customer Profile:

- A large Pharmaceutical Company has 2000+ employees in 5 countries

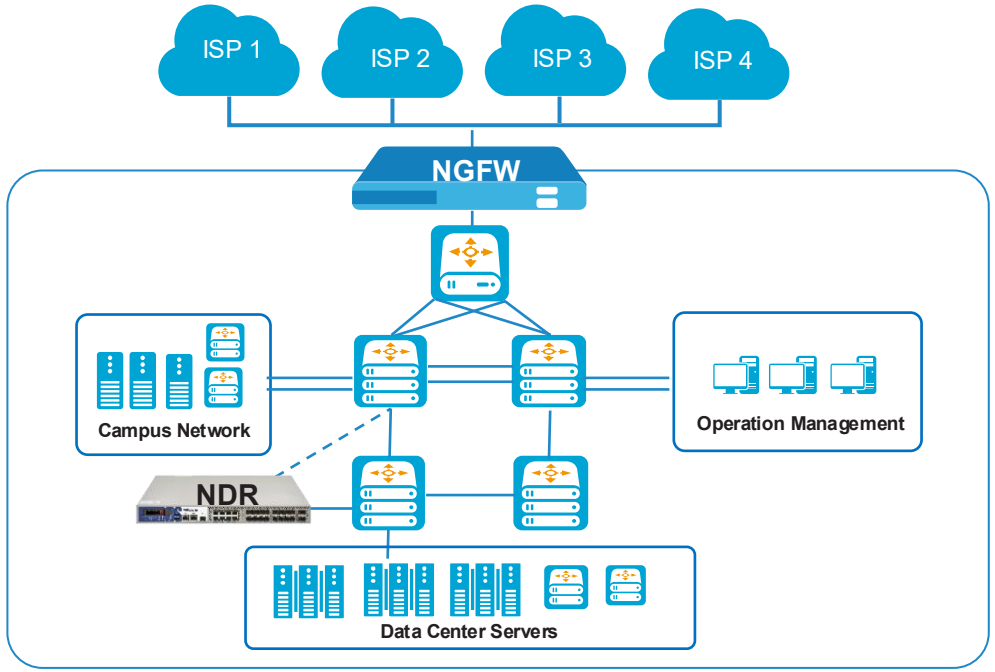
Challenges

- The customer deployed viable security solutions including firewall/IPS/Antivirus solutions, but they couldn't detect the ransomware variants in early stage and protect their servers from being locked.
- The customer was also trying to hire security professionals to disinfect their locked systems. but the process takes days, at a much higher cost even than the ransom.

Hillstone Solution

- Customer deployed Hillstone NDR product in front of servers area, in Tapping mode by access switch, along with Hillstone NGFW and IPS in the network exit.
- Hillstone NDR product leverage its layered detection engines (ABD/ATD/IPS/AV) to detect and identify the Locky ransomware and other advanced attack and alarm the IT team to take promptly actions to block these blocks.

Case Study 4:
Protect Critical Servers for a Large University



Customer Profile

- A top university with 25,000 students accessing the campus network and resource

Challenges

- Can't identify and detect the compromised internal host
- No dedicate solution for critical servers in the data center
- The current NGFW and IPS couldn't detect advanced unknown threat

Hillstone Solution

- Hillstone's NDR solution is designed to detect internal threats and sophisticated attacks that bypass traditional perimeter defense.
- By focusing on high-risk assets and providing granular control, Hillstone ensures that the most valuable data is protected against both external and internal threats.
- Hillstone's NDR solution offers continuous monitoring, detection of threats, and the ability to respond to security incidents effectively.

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 V vade | CyberShield

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