



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



EXPERTISE

Des solutions adaptées
à chaque environnement



CONFIANCE

Un partenaire fiable
à vos côtés



PERFORMANCE

Des infrastructures
sécurisées et évolutives



SUPPORT

Un accompagnement
technique de qualité

HAFS
Distributeur à valeur ajoutée

Des solutions IT innovantes pour
un monde connecté et sécurisé



**WIRELESS
RADIO**

Connectivité sans fil
haute performance



**RÉSEAUX &
SÉCURITÉ IT**

Des réseaux fiables
et sécurisés



**VIRTUALISATION
CLOUD**

Des solutions Cloud
flexibles et évolutives



CYBERSECURITY

Protéger vos données
et vos systèmes



**VIDÉO
PROTECTION**

Solutions de vidéosurveillance
intelligentes



**HCI STOCKAGE
SAUVEGARDE**

Stockage, sauvegarde
et haute disponibilité

SOLUTIONS IT

CYBERSÉCURITÉ

CLOUD

INFRASTRUCTURE RÉSEAU

STOCKAGE

PROTECTION

Hillstone Breach Detection System (BDS) I-Series



Integrative Cybersecurity
Visionary. **AI-powered.** **Accessible.**

Agenda

Today's Intranet Security Reality

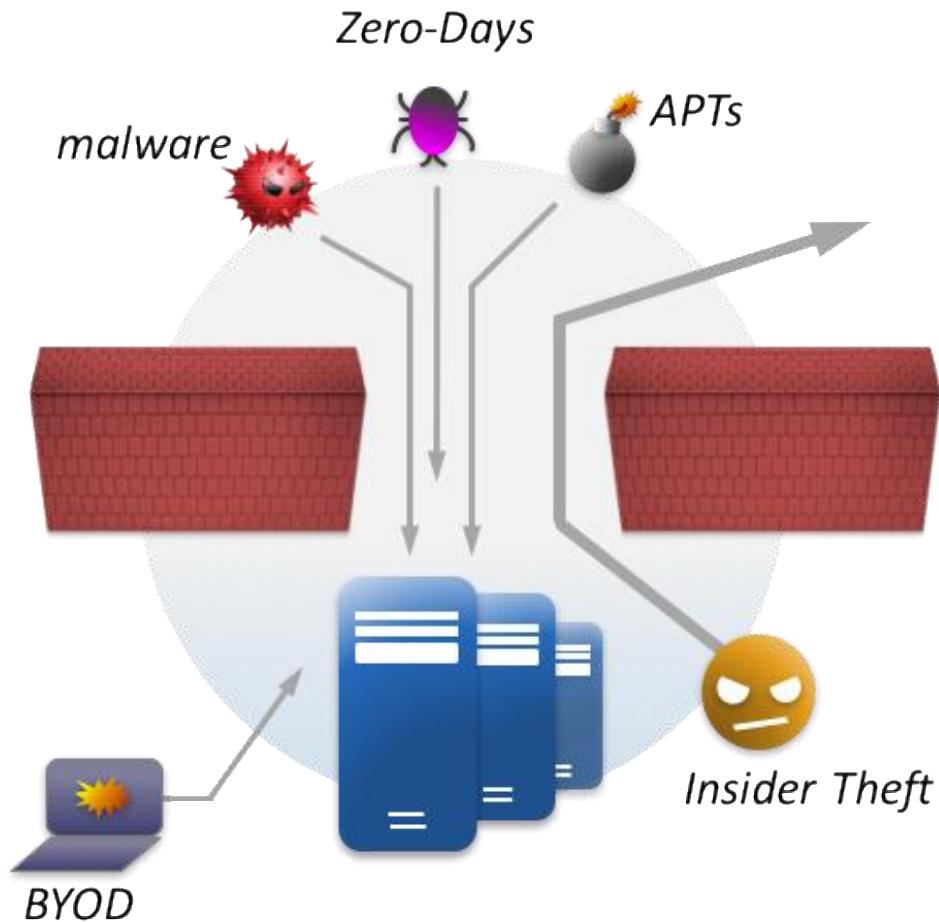
Hillstone BDS Value Proposition

Hillstone BDS Portfolio

Deployment Scenarios & Case Studies

Today's Intranet Security Reality

Internal Network Breaches Occur at an Alarming Rate



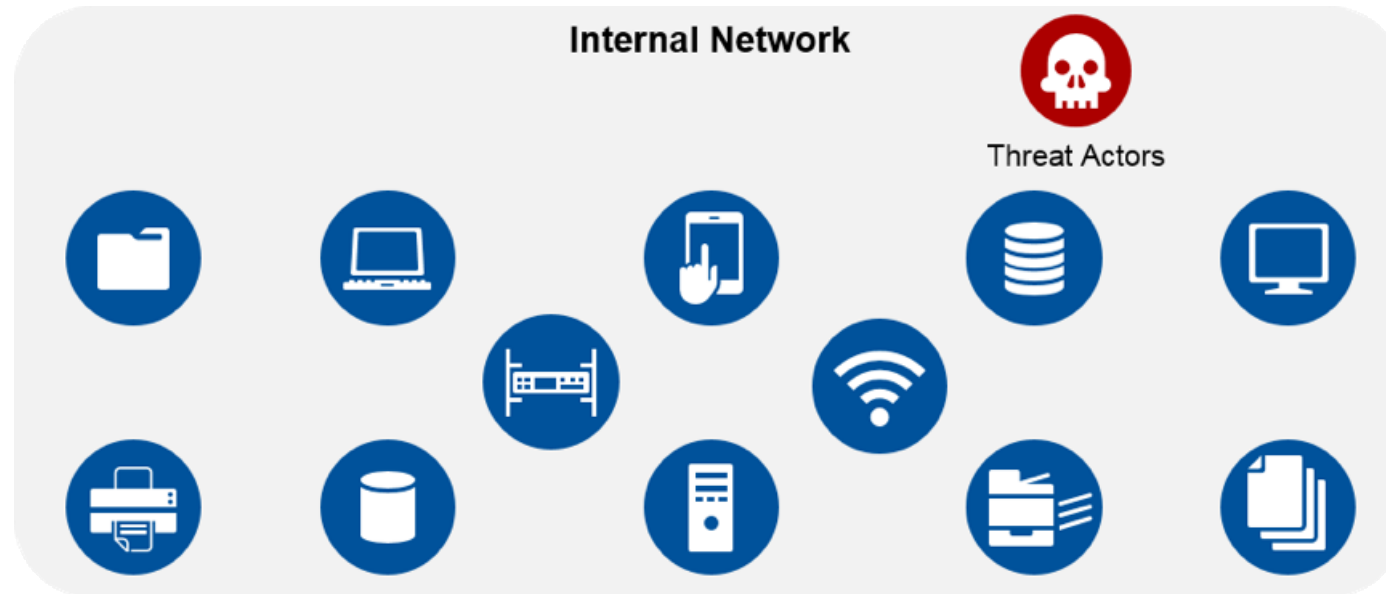
Traditional signature defenses can only stop old “**amateur**” attacks

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

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

– Verizon 2015 DBIR

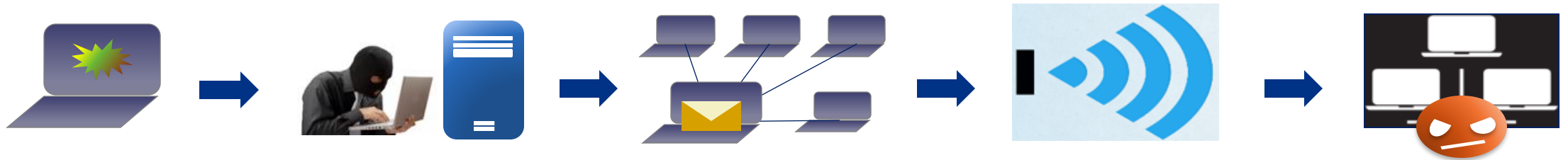
Threat Spreads Easily in Flat Internal Networks...



“...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 BDS Value Proposition

Hillstone NDR Product BDS



Hillstone NDR product BDS detects and responds to Advanced Network Threats

Threat Detection	Deep Visibility	Digital Forensics & Incident Response(DFIR)	Effective Mitigation
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

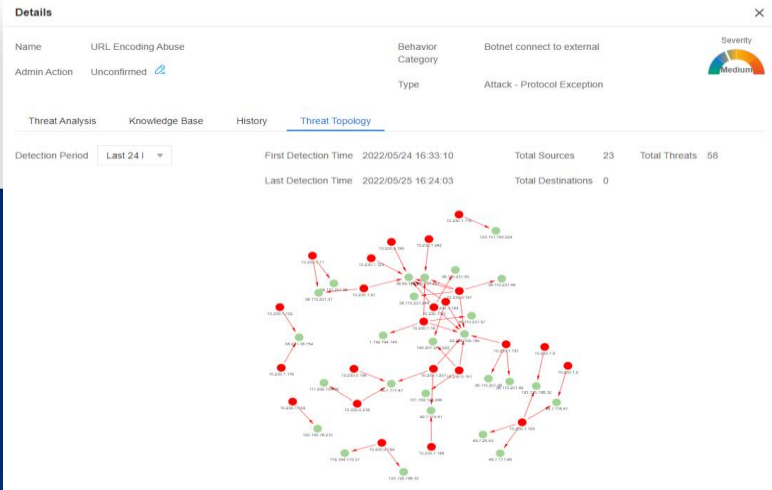
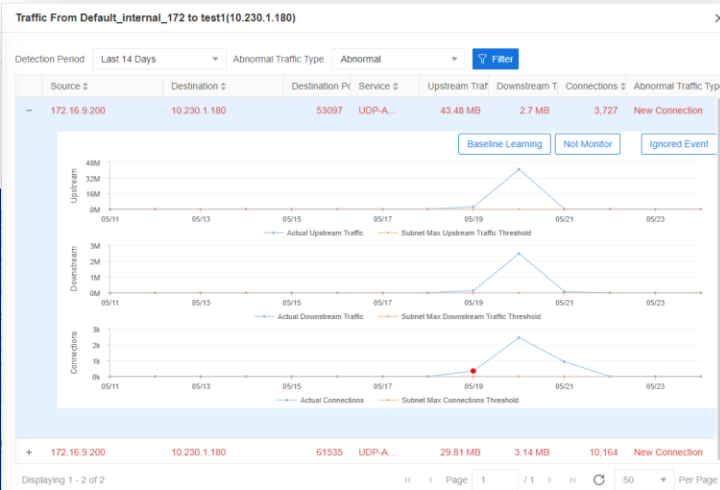
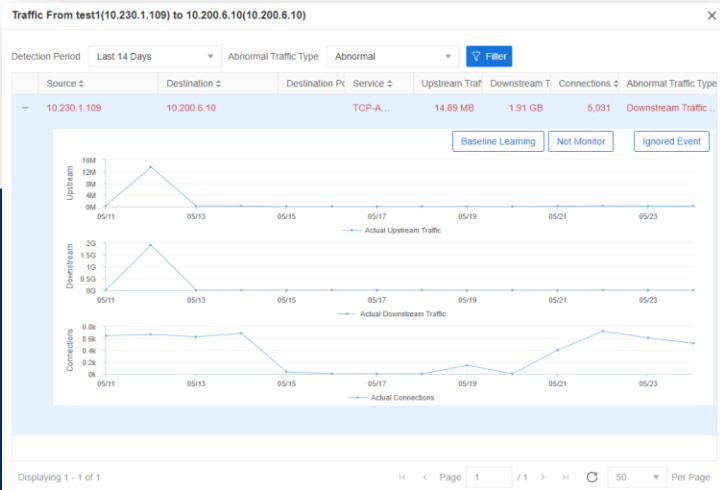


Learn and Establish Normal Traffic Baseline and Threshold

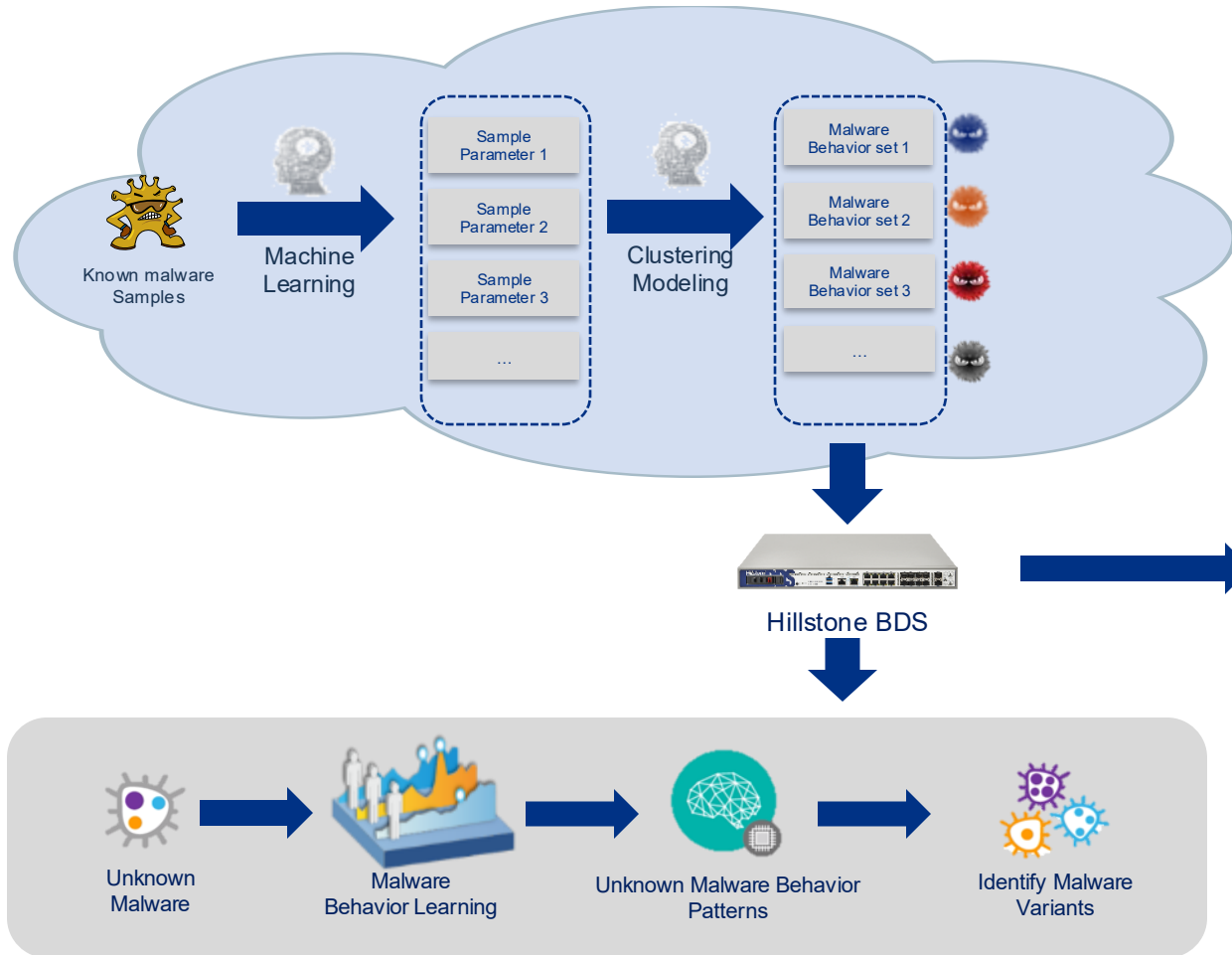
Detect Traffic Trend and Identify Abnormal Traffic Behaviors

Monitor Normal and Abnormal Traffic for each server/host

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



Detection: Advanced Threat Detection (ATD)



Unknown Malware Detected by ATD

Threat Severity

Details

Name	Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain	Behavior Category	Botnet connect to external	Severity	Critical
Admin Action	Unconfirmed	Type	Malware - Trojan		

[Threat Analysis](#) | Knowledge Base | MITRE ATT&CK® Tactic Details | ATT&CK® Technique Details | History | Threat

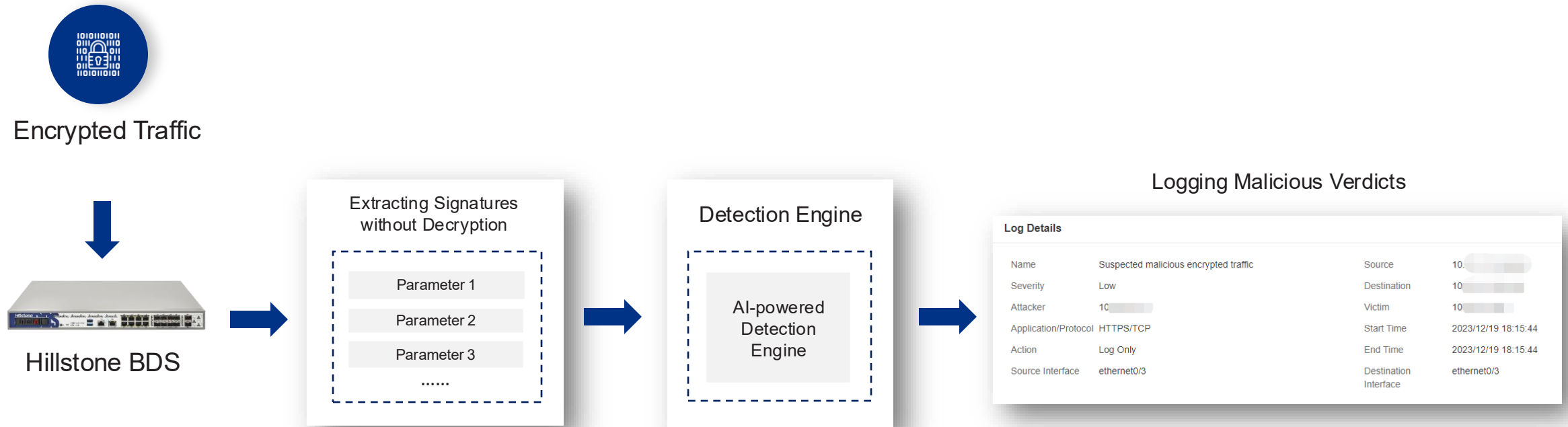
Application/Protocol DNS/UDP

Source		Destination	
Endpoint Name/IP	192.168.1.37	Endpoint Name/IP	8.8.8.8
Port	53608	Port	53
Interface	ethernet0/1	Interface	ethernet0/1
Zone	tap-bds	Zone	tap-bds

Action Log Only

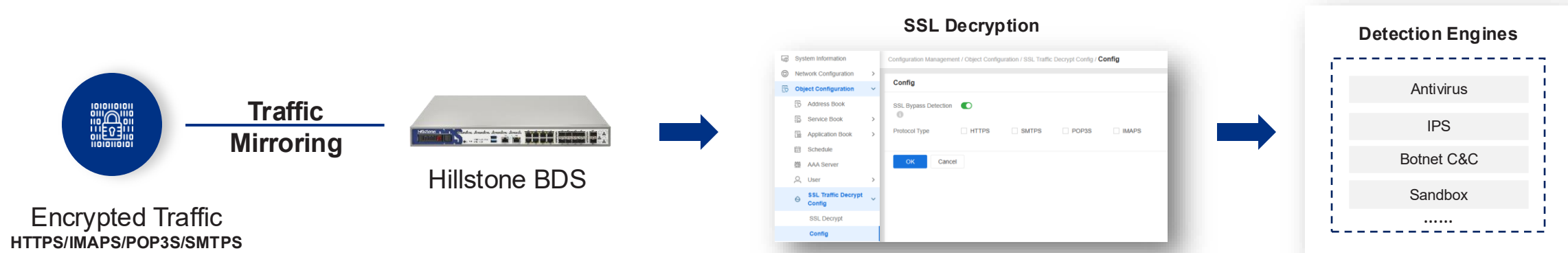
Known Malware Information

Detection: Abnormal Encrypted Traffic Detection



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

WAF rules
Utilizing OWASP ModSecurity Core Rule Set (CRS) 3.3



Detect and analyze threats for WEB servers and applications

WEB Attacks Detection

DDoS Attack

Injection Attack

Cross-site Attack

Abnormal HTTP

Special Vulnerability Attack

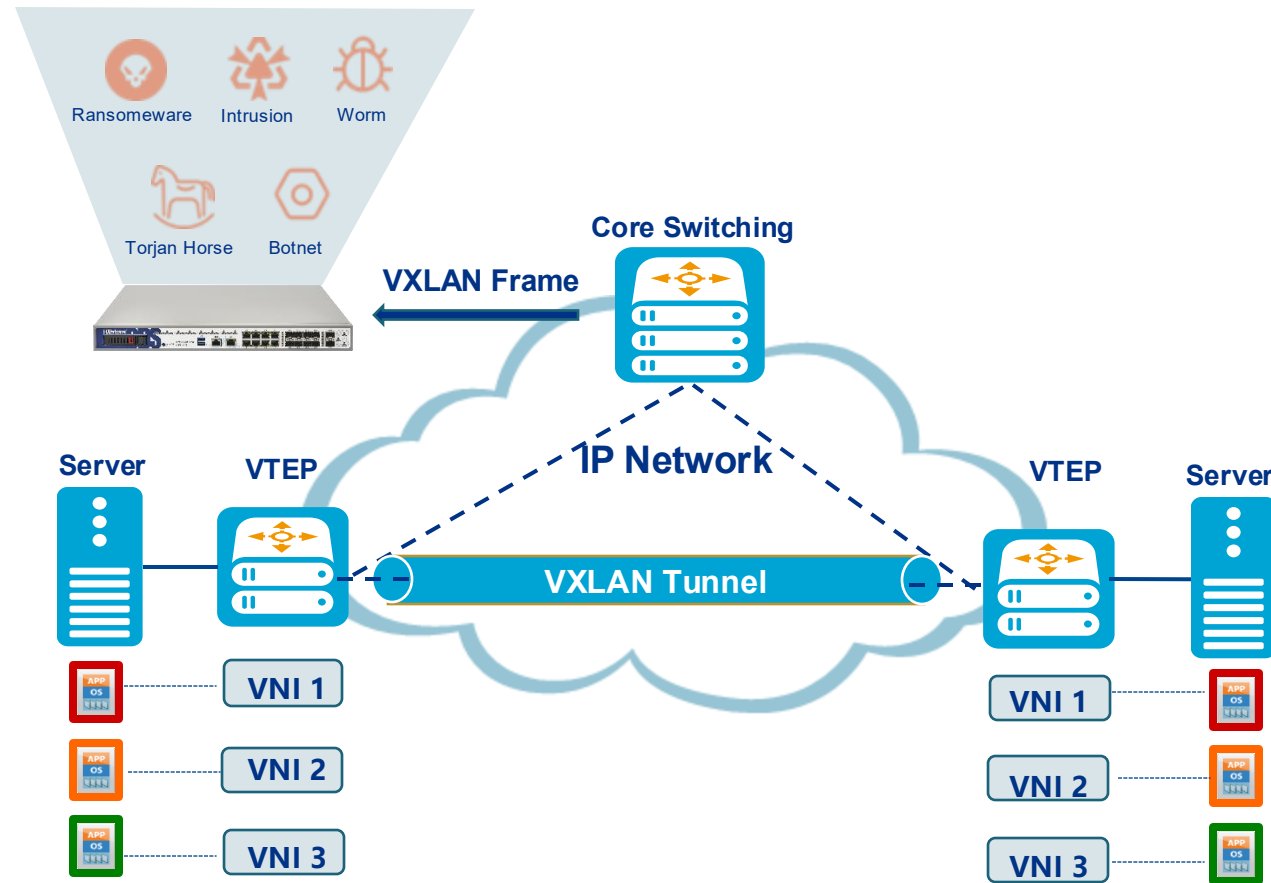
Information Leakage

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

Details

Name: Unauthorized HTTP access | Behavior Category: Botnet connect to external | Severity: Critical

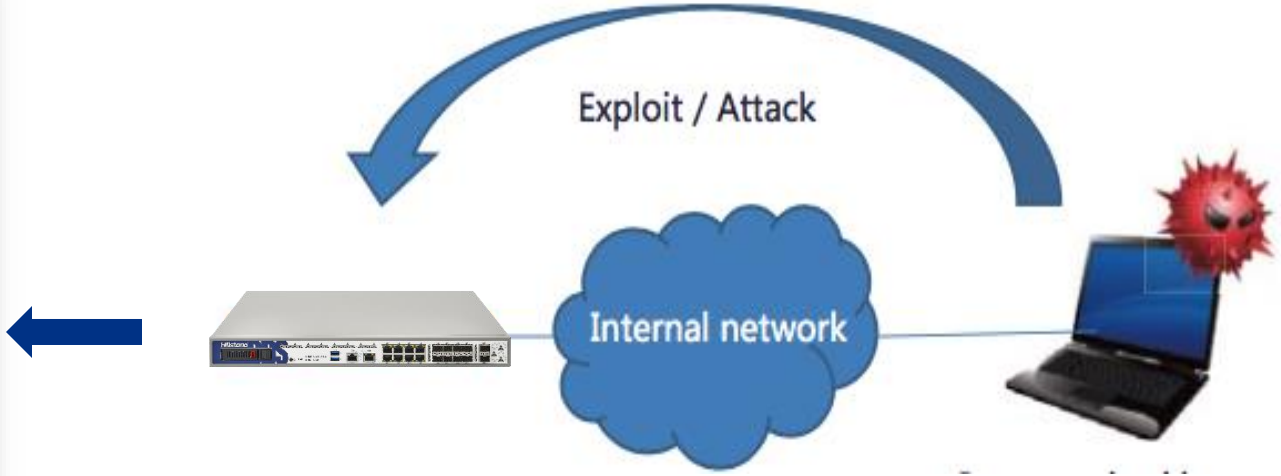
Admin Action: Unconfirmed | Type: Malware - Trojan

Application/Protocol: DNS/UDP

Source	Destination
Endpoint Name/IP: 192.168.1.37	Endpoint Name/IP: 8.8.8.8
Port: 53608	Port: 53
Interface: ethernet0/1	Interface: ethernet0/1
Zone: Deception	Zone: Deception

Action: Log Only
Start Time: 2023/04/21 07:57:08
End Time: 2023/04/21 07:57:28
Attacks: 1
Duration: 10seconds
Profile: predef_1

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

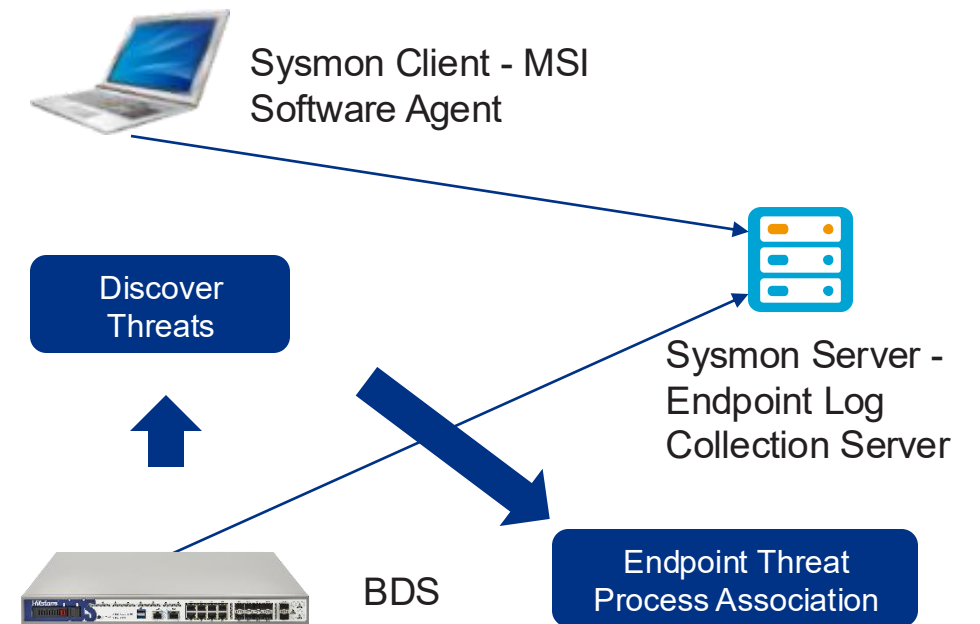
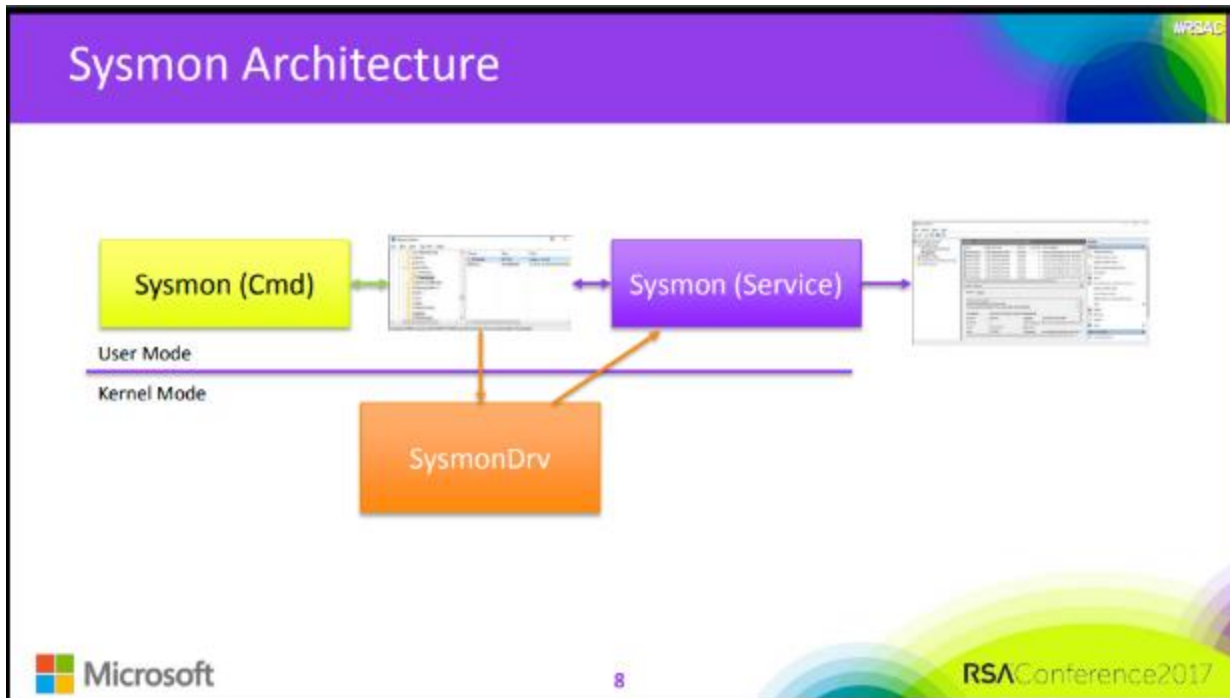
- MD5 file hash-based
- Support all files
- Use Case: Known virus detection



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

Details [Close]

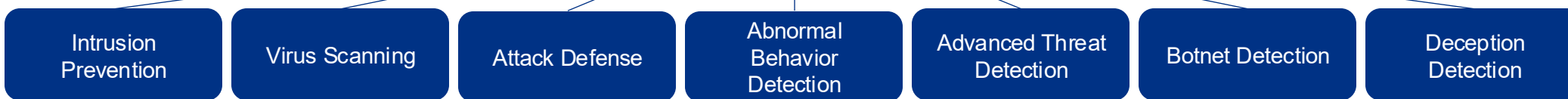
Name: Ransomare Activity: TeslaCrypt/AlphaCrypt Variant .onion Proxy Domain Info Behavior Category: Botnet connect to external Severity: Critical

Admin Action: Unconfirmed Link Type: Malware - Trojan

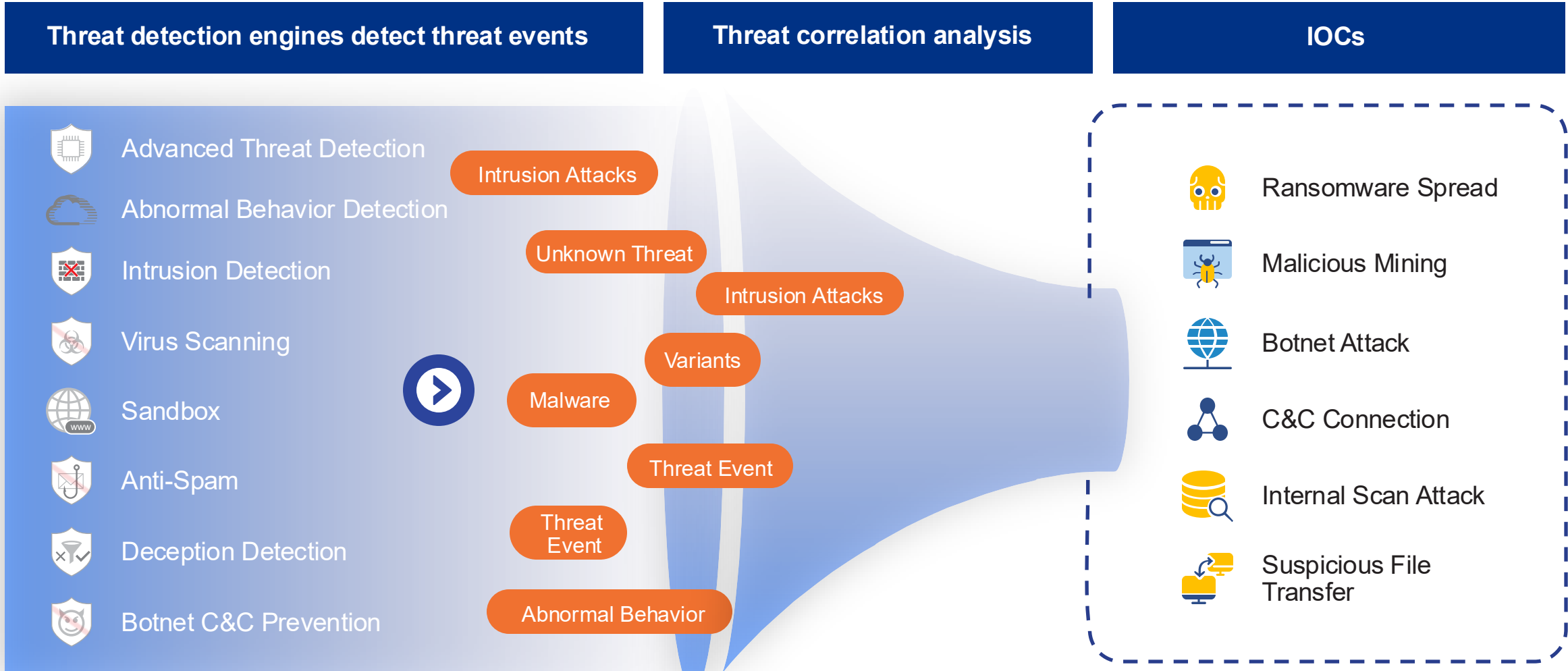
Threat Analysis Knowledge Base MITRE ATT&CK[®] Tactic Details ATT&CK[®] Technique Details **History** Threat Topology

	Source	Source Zone	Source Interface	Destination	Destination Zone	Detected at
1	192.168.1.37	tap-bds	ethernet0/1	8.8.8.8	tap-bds	2023/04/21 07:57:28

Threat Correlation Analytics



Visibility: Indicator of Compromises (IOCs) Threats



Visibility: Global View of Intranet Threat

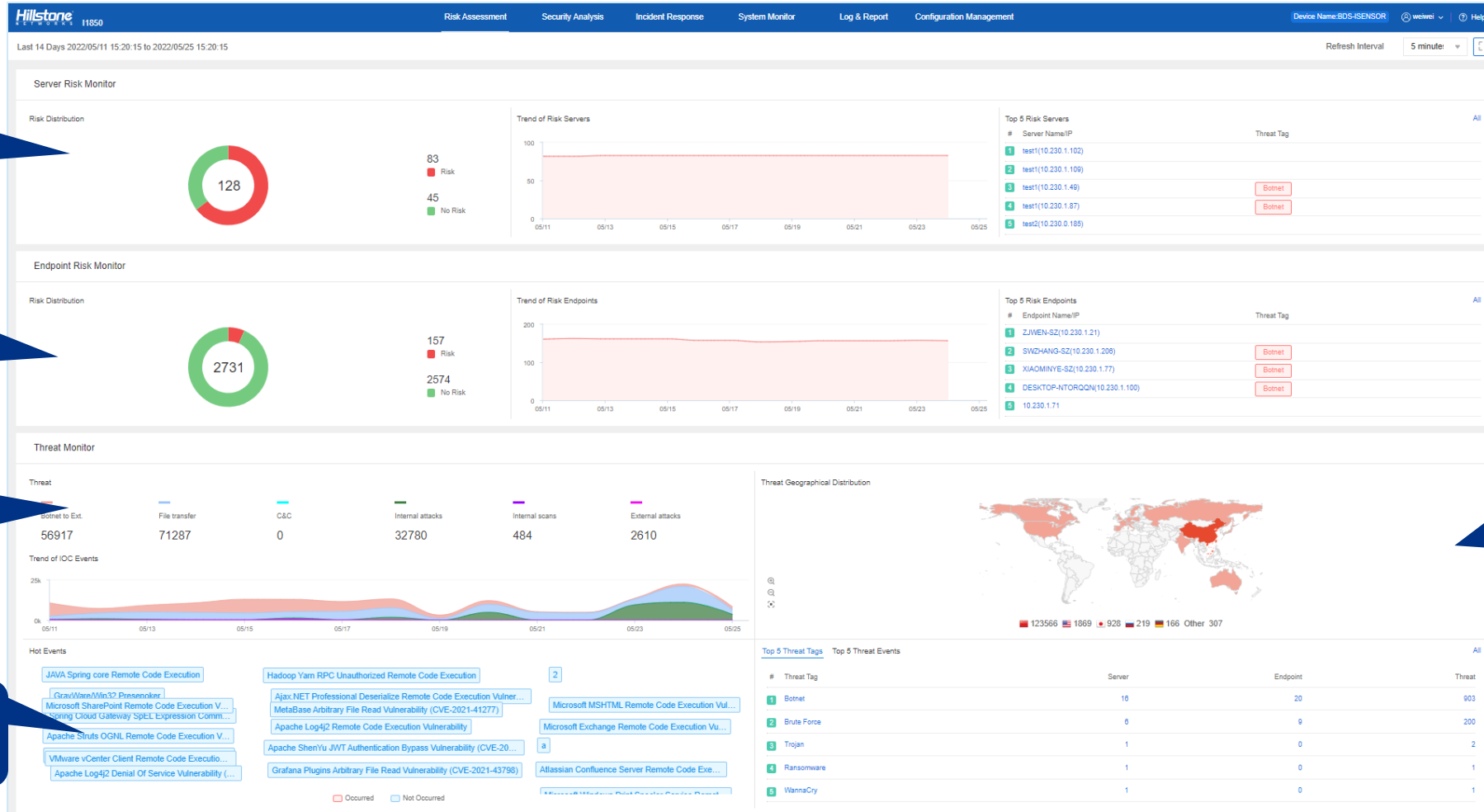
Overview of Critical Servers and risk level

Overview of internal host and risk level

Threat type, statistic, historical distribution etc.

Hot events that need attention

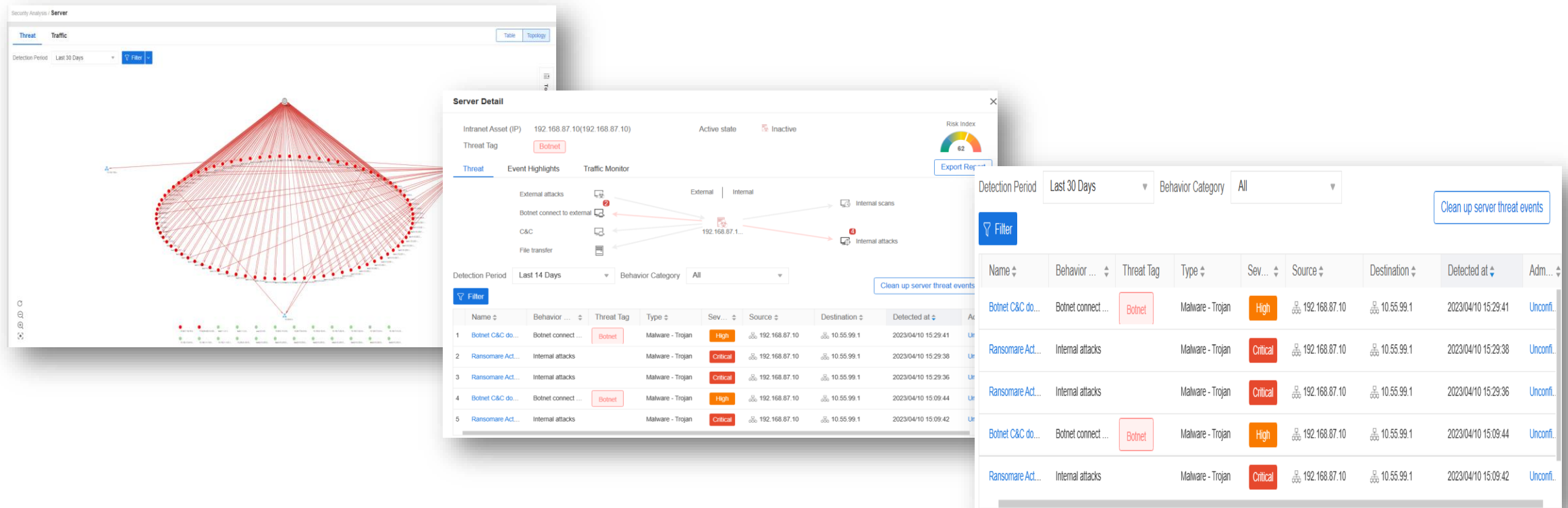
Geo-location threat distribution and top threat



Visibility: Intranet Risk Monitoring Dashboard

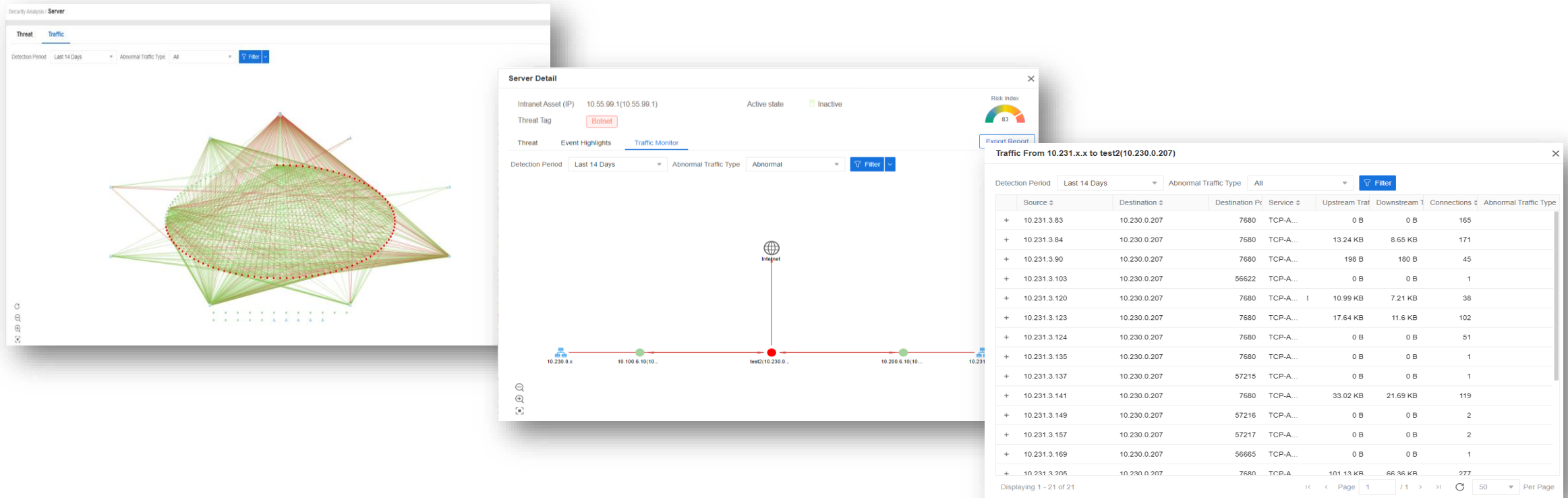


Visibility: Server Threat Monitoring



- 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

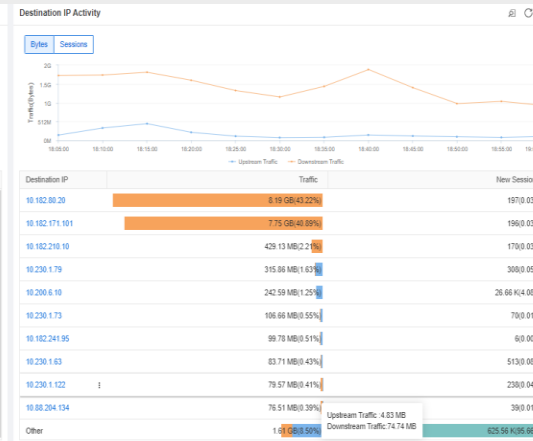
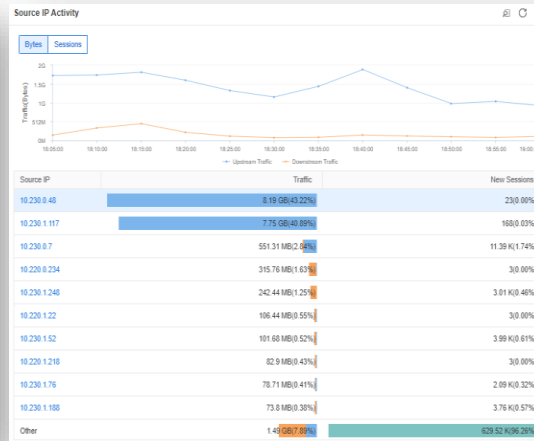
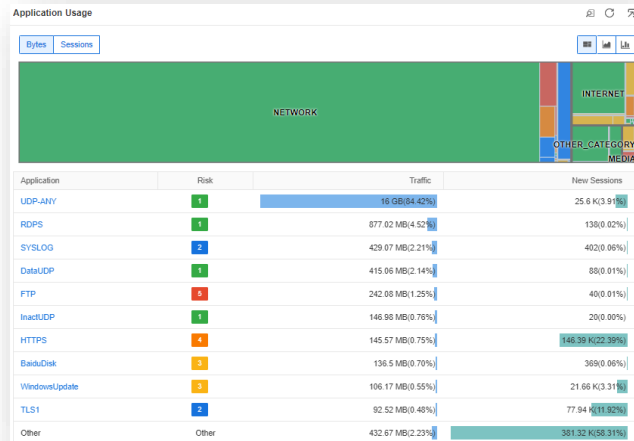
Visibility: Threat Topology

The image displays three overlapping screenshots from a security dashboard. The top-left screenshot shows 'Details' for a threat named 'Ransomare Activity: TeslaCrypt/AlphaCrypt Variant'. It includes fields for Name, Behavior Category (Botnet connect to external), Admin Action (Unconfirmed), and Type (Malware - Trojan). A severity gauge indicates 'Critical'. The top-right screenshot shows 'Details' for a threat named 'illegal downloading', with Behavior Category 'File transfer' and Type 'Attack - Suspicious File Operation'. A severity gauge indicates 'High'. The bottom screenshot shows 'Endpoint Detail' for IP 192.168.1.37, featuring a threat topology diagram and a table of events. The topology diagram shows a central node (192.168.1.37) connected to various external and internal assets. The event table lists five instances of 'Ransomare Act...' with 'Botnet connect...' behavior, all classified as 'Malware - Trojan' with a 'Critical' severity.

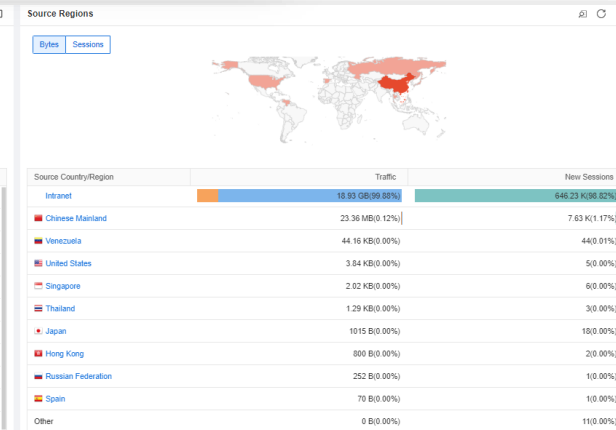
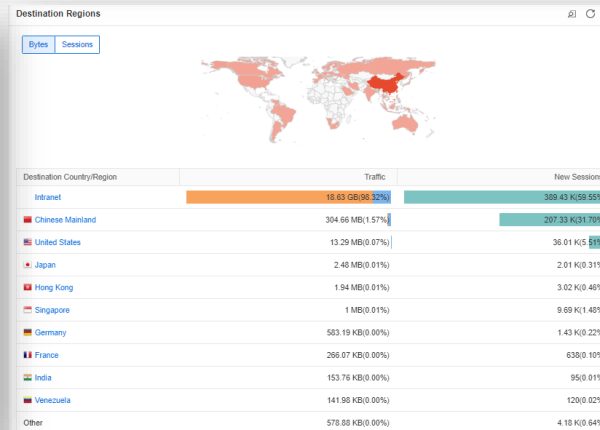
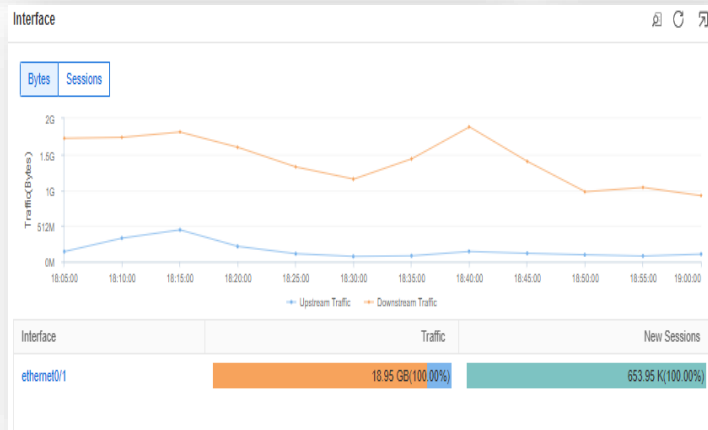
Name	Behavior	Threat Tag	Type	Sev	Source	Destination	Detected at	Adm
1 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/21 07:57:28	Unconfi...
2 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:15:36	Unconfi...
3 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:15:26	Unconfi...
4 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/18 16:14:22	Unconfi...
5 Ransomare Act...	Botnet connect ...		Malware - Trojan	Critical	192.168.1.37	8.8.8.8	2023/04/15 13:37:18	Unconfi...

- 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

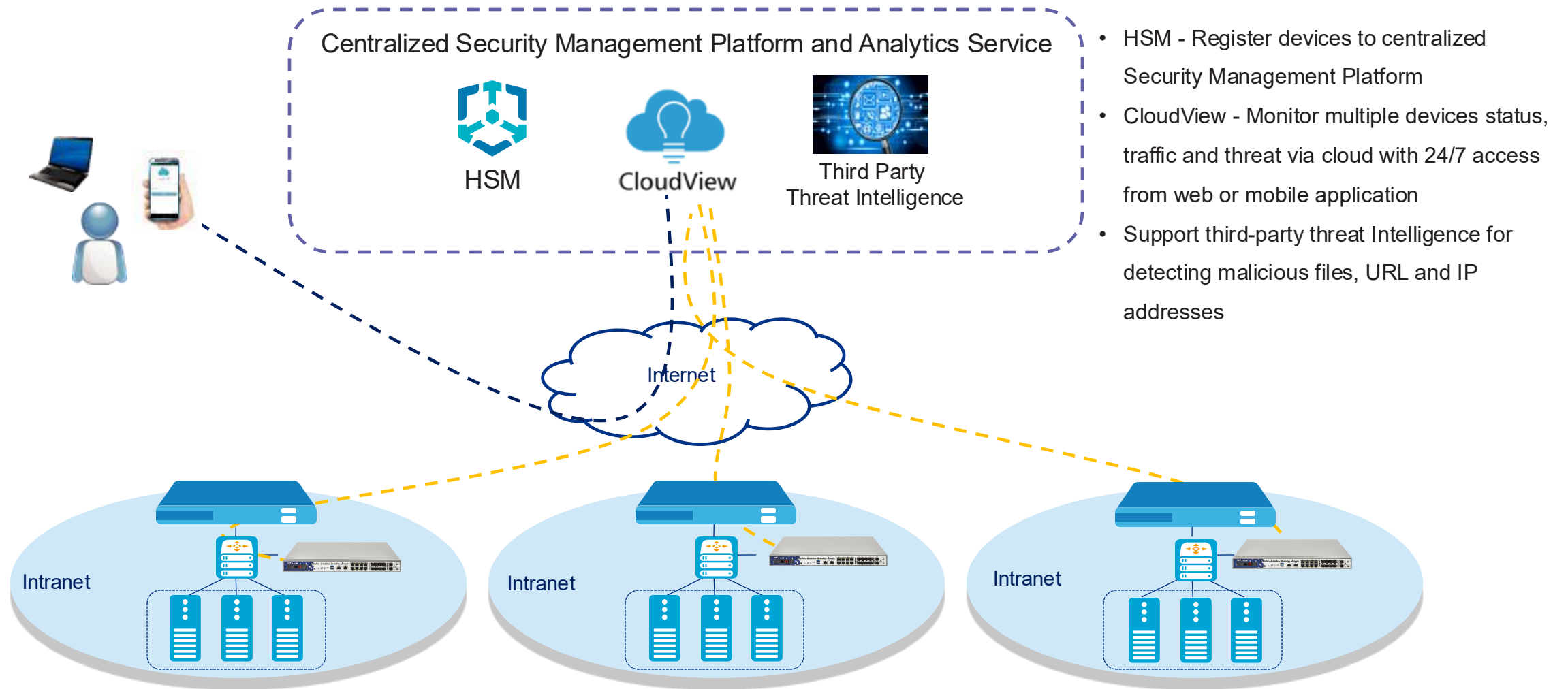
Visibility: Intranet Application Analysis



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



Visibility: Centralized Security Management



DFIR: Rich Forensics Enables Risk Assessment

Details

Name: Ransomware Activity: TeslaCrypt/AlphaCrypt Variant
onion Proxy Domain

Behavior Category: Botnet connect to external

Admin Action: Unconfirmed

Type: Malware - Trojan

Severity: Critical

Threat Analysis | Knowledge Base | MITRE ATT&CK[®] Tactic Details | ATT&CK[®] Technique Details | History | Threat Topology

Release Date: 2020-12-14

Name: Ransomware Activity: TeslaCrypt/AlphaCrypt Variant_onion Proxy Domain

Severity: Critical

Bug ID:

CVE ID:

CNNVD ID:

Description: Ransomware virus uses various encryption algorithms to encrypt the file. The infected person can't decrypt the file without decrypted private key.

Solution: Search and kill the malware by using antivirus tools and repair the system vulnerabilities.

Server Detail

Intranet Asset (IP): 192.168.87.10(192.168.87.10) Active state: Inactive

Threat Tag: Botnet

Risk Index: 0

Threat | Event Highlights | Traffic Monitor

External attacks, Botnet connect to external, C&C, File transfer

Detection Period: Last 30 Days | Behavior Category: All

Name	Behavior	Threat Tag	Type	Sev.	Source	Destination	Date
Botnet C&C de...	Botnet connect...	Botnet	Malware - Trojan	High	192.168.87.10	10.55.99.1	2023
Ransomware Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023
Ransomware Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023
Botnet C&C de...	Botnet connect...	Botnet	Malware - Trojan	High	192.168.87.10	10.55.99.1	2023
Ransomware Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023
Ransomware Act...	Internal attacks		Malware - Trojan	Critical	192.168.87.10	10.55.99.1	2023

Restore the Attack Chain and Mapping to MITRE ATT&CK

Knowledge Base

Threat Analysis

PCAP Forensics

Packet capture

Time	Source IP	Destination IP	Source MAC	Destination MAC	Protocol
1. 2023/04/01 04:29:10	10.181.70.121	103.55.25.106	30-29-52-4f-fe-17	00-1c-54-60-21-c6	TCP

Details info

.....TCP Packet.....

Pcap Header
- Captured Timestamp: 2023-04-01 04:29:10
- Wire Length: 149
- Captured Length: 149

Ethernet Header
- Destination Address: 00-1c-54-60-21-c6
- Source Address: 30-29-52-4f-fe-17
- Type: 0x0000

IP Header
- IP Version: 4
- IP Header Length: 20 bytes
- Type Of Service: 0
- IP Total Length: 135 bytes (Size of Packet)
- Flags: 2
- Offsets: 0
- Identification: 59867

Details

Name: Ransomware Activity: TeslaCrypt/AlphaCrypt Variant
onion Proxy Domain

Behavior Category: Botnet connect to external

Admin Action: Unconfirmed

Type: Malware - Trojan

Severity: Critical

Threat Analysis | Knowledge Base | MITRE ATT&CK[®] Tactic Details | ATT&CK[®] Technique Details | History | Threat Topology

Application/Protocol: DNS/UDP

Source	Destination
Endpoint Name/IP: 192.168.1.37 Port: 53608 Interface: ethernet0/1 Zone: tap-bds	Endpoint Name/IP: 8.8.8.8 Port: 53 Interface: ethernet0/1 Zone: tap-bds

Action: Log Only

Start Time: 2023/04/21 07:57:08

End Time: 2023/04/21 07:57:28

Attacks: 1

Duration: 10seconds

Profile: predef_1

Signature ID: 100504

ATT&CK Tactic ID: TA0011,TA0042,TA0005

ATT&CK Technique ID: T1090,T1587.001,T1036,T1132,T1583.001

DFIR: 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.

The screenshot shows the 'Details' view for the MITRE ATT&CK tactic TA0042. The interface includes a top navigation bar with tabs for Threat Analysis, Knowledge Base, MITRE ATT&CK[®] Tactic Details (selected), ATT&CK[®] Technique Details, History, and Threat Topology. The main content area displays the following information:

Name	Ransomare Activity: Possible WannaCry DNS Lookup 4	Behavior Category	Internal attacks	Severity	Critical
Admin Action	Unconfirmed	Type	Malware - Trojan		

Below the main content, there is a secondary navigation bar with tabs for Threat Analysis, Knowledge Base, MITRE ATT&CK[®] Tactic Details (selected), ATT&CK[®] Technique Details, History, and Threat Topology. The main content area displays the following information:

ATT&CK ID	TA0042	TA0043
Name	Resource Development	
Create Time	2020/09/30 16:11:59	
Last Modified Time	2020/09/30 16:31:36	
Source	ATT&CK	
Official Link	https://attack.mitre.org/tactics/TA0042	
Description	The adversary is trying to establish resources they can use to support operations. Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.	

ATT&CK tactic details of threat events

The screenshot shows the 'ATT&CK[®] Technique Details' view for T1587.001. The interface includes a top navigation bar with tabs for Threat Analysis, Knowledge Base, MITRE ATT&CK[®] Tactic Details, ATT&CK[®] Technique Details (selected), History, and Threat Topology. The main content area displays the following information:

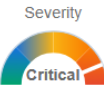
ATT&CK ID	T1587.001	T1590.002
ATT&CK Version	1.2	
Name	Malware	
Create Time	2020/10/01 01:33:01	
Last Modified Time	2022/01/14 17:14:27	
Source	ATT&CK	
Permission Requirement	-	
System Requirement	-	
Network Requirement	-	

ATT&CK technique details of threat events

DFIR: Threat Behavior Details

















Details ✕

Name Ransomare Activity: TeslaCrypt/AlphaCrypt Variant ⓘ
.onion Proxy Domain Behavior Botnet connect to external Category 

Admin Action Unconfirmed [🔗](#) Type Malware - Trojan

Threat Analysis Knowledge Base MITRE ATT&CK® Tactic Details ATT&CK® Technique Details History Threat Topology

	Source ⇅	Source Zone ⇅	Source Interface ⇅	Destination ⇅	Destination Zone ⇅	Detected at ⇅
1	 192.168.1.37	tap-bds	ethernet0/1	 8.8.8.8	tap-bds	2023/04/21 07:57:28
2	 192.168.1.37	tap-bds	ethernet0/1	 8.8.8.8	tap-bds	2023/04/18 16:15:36
3	 192.168.1.37	tap-bds	ethernet0/1	 8.8.8.8	tap-bds	2023/04/18 16:15:26
4	 192.168.1.37	tap-bds	ethernet0/1	 8.8.8.8	tap-bds	2023/04/18 16:14:22
5	 192.168.1.37	tap-bds	ethernet0/1	 8.8.8.8	tap-bds	2023/04/15 13:37:18
6	 192.168.1.37	tap-bds	ethernet0/1	 8.8.8.8	tap-bds	2023/04/10 15:29:41
7	 192.168.1.37	tap-bds	ethernet0/1	 8.8.8.8	tap-bds	2023/04/10 15:09:35

Displaying 1 - 7 of 7 ⏪ < Page 1 / 1 > ⏩ ↻ 50 Per Page

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

Mitigation: Mitigate/Block Attacks in Conjunction with NGFW/NIPS



Hillstone BDS



Hillstone NGFW



Hillstone NIPS

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



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

Mitigation: Detect and Respond to Threats and Attacks with Integration of iSource



Under the scenario of integrating with iSource:

- BDS uploads data* (threat log/ evidential packets/ metadata/ netflow) to iSource
- BDS can perform active assets scanning task delivered by iSource, and uploads the results to iSource
- 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 iSource V2.0R4-R8; Threat log, evidential packets, and netflow can be uploaded to iSource V2.0R9 or later

Report: Host Risk Assessment

Server Detail

Intranet Asset (IP) 192.168.87.10(192.168.87.10) Active state Inactive Risk Index 48 [Export Report](#)

Threat Tag Botnet

[Threat](#) [Event Highlights](#) [Traffic Monitor](#)

Endpoint Detail

Endpoint Name/IP 192.168.1.37 Active state Inactive Risk Index 24 [Export Report](#)

[Threat](#) [Event Highlights](#)

[test1(10.230.1.165)]
Server Security Assessment Report
Period : 2022-05-11 19:39:23 - 2022-05-25 19:39:23
Created at : 2022-05-25 19:39:24

1. Security Assessment

1.1 Overview of Security Assessment

The risk index of server test1(10.230.1.165) is 48. The server is at low risk level. The following lists the threat behaviors detected on the server:

Threat Behavior	Frequency
The server tries to connect to the C&C server	0
The server conducts an internal network attack	0
The server performs an internal network scans	0
The server is involved in botnet activities	10
The server tries to transmit suspicious files	238
The server downloads malware	2

1.The server is at low risk level.No threat event of high reliability is detected.
The threat event of low reliability listed in the second section may be normal. Please check whether it's a real threat.
2.According to historical traffic statistics, the network traffic of the server is found abnormal. For details, refer to the third section.
It is necessary to note that the abnormal traffic of the server may have the following potential risks:
1) Threat Spread Risk: The malware, viruses and malicious plug-ins may exploit new connections with small traffic to spread threats.
2) Data Leakage Risk: The latest malware may leak sensitive data to the external with normal traffic.
3) Bandwidth Consumption Risk: The large number of abnormal traffic may cause bandwidth consumption, which will affect server performance.

2. Threat Event

2.1 Typical Threat Events

No data to display

3. Abnormal Traffic

The following lists the abnormal traffic of the server:

3.1 Traffic From Client To Server

Source Address	Service/Port	Upstream Traffic	Downstream Traffic	Connections	Anomaly Reason
10.231.3.225	TCP-4444(7480)	26.55KB	2.12MB	866	New Connection
101.226.232.201	HTTP(80)	55.37KB	2.68MB	13	New Connection
10.182.142.116	SSH(22)	110.49MB	1.93MB	1	New Connection
10.182.142.81	SSH(22)	1.77MB	55.64MB	5	New Connection
10.88.15.114	TCP-4444(7480)	76.62KB	1.91MB	20	New Connection

3.2 Traffic From Server

Destination Address	Service/Port	Upstream Traffic	Downstream Traffic	Connections	Anomaly Reason
10.231.3.225	TCP-4444(7480)	26.55KB	2.12MB	866	New Connection
101.226.232.201	HTTP(80)	55.37KB	2.68MB	13	New Connection
10.182.142.116	SSH(22)	110.49MB	1.93MB	1	New Connection
10.182.142.81	SSH(22)	1.77MB	55.64MB	5	New Connection
10.88.15.114	TCP-4444(7480)	76.62KB	1.91MB	20	New Connection

Anomaly Info :

- #1: Latest Abnormal Traffic Info : 2022-05-24 12:00:00 New Connection
- #2: Latest Abnormal Traffic Info : 2022-05-24 17:00:00 New Connection
- #3: Latest Abnormal Traffic Info : 2022-05-24 10:00:00 New Connection
- #4: Latest Abnormal Traffic Info : 2022-05-24 11:00:00 New Connection
- #5: Latest Abnormal Traffic Info : 2022-05-24 12:00:00 New Connection

3.3 Analysis and Recommendations

The following analyzes the reason of abnormal traffic and offers related recommendations:

- *New Connection**
An unknown new connection was detected. Please check whether there is a new network service or whether the connection is conducted by malware.
- *Upstream Traffic Exceeds Threshold**
The upstream traffic of certain connection exceeded the threshold. Please check whether the upstream traffic is normal or whether the malware conducted content leakage.
- *Downstream Traffic Exceeds Threshold**
The downstream traffic of certain connection exceeded the threshold. Please check whether the downstream traffic is normal or whether the malware conducted content download.
- *Connections Exceeds Threshold**
The number of connections exceeded the threshold. Please check whether the connection frequency is normal or whether the number of connections conducted by the malware exceeded the threshold.

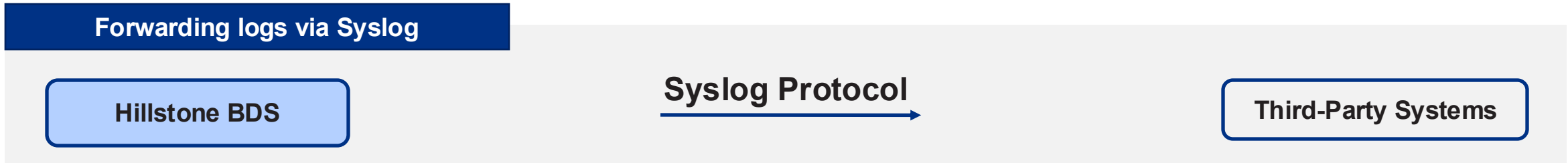
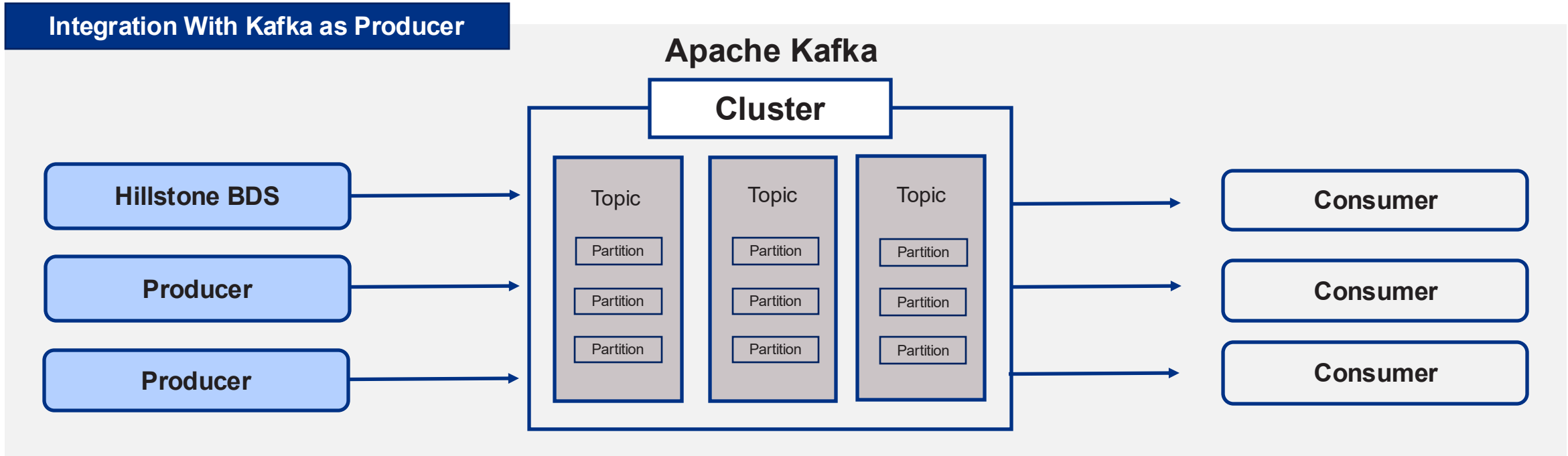
On the risk server or risk endpoint page, the threat and traffic information matching the current interface filtering conditions are exported. A PDF report is generated, which includes the following information:

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

Closed Cycle: Network Detection and Response

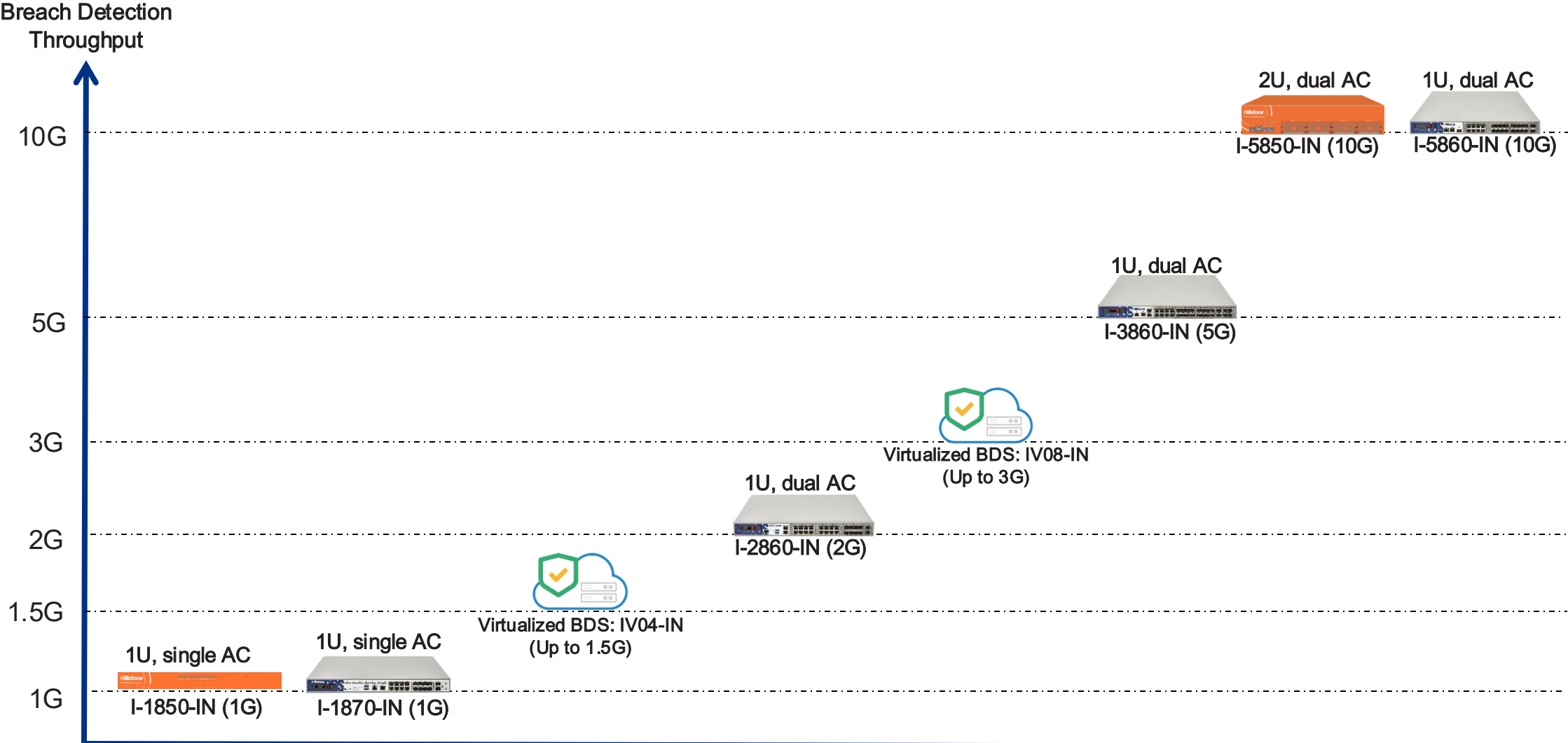


Third-Party Integration

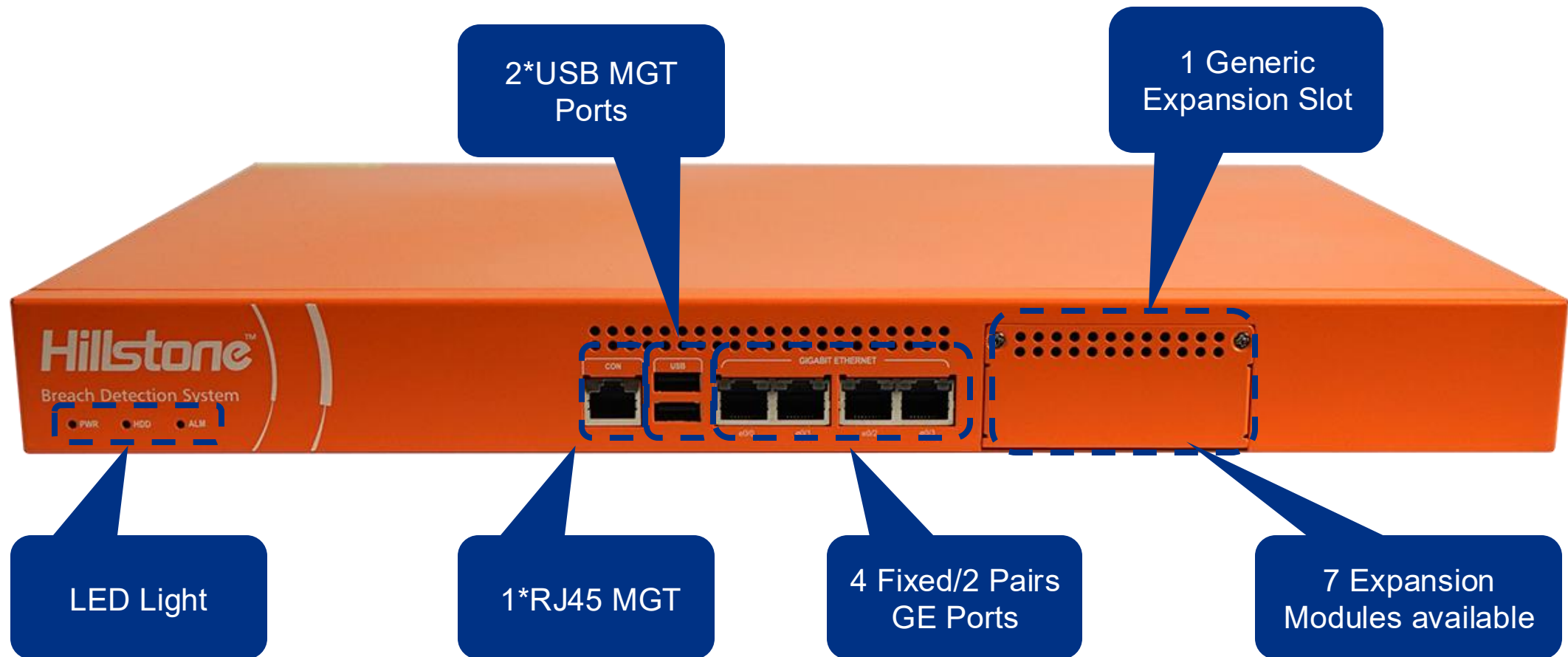


Hillstone BDS Portfolio

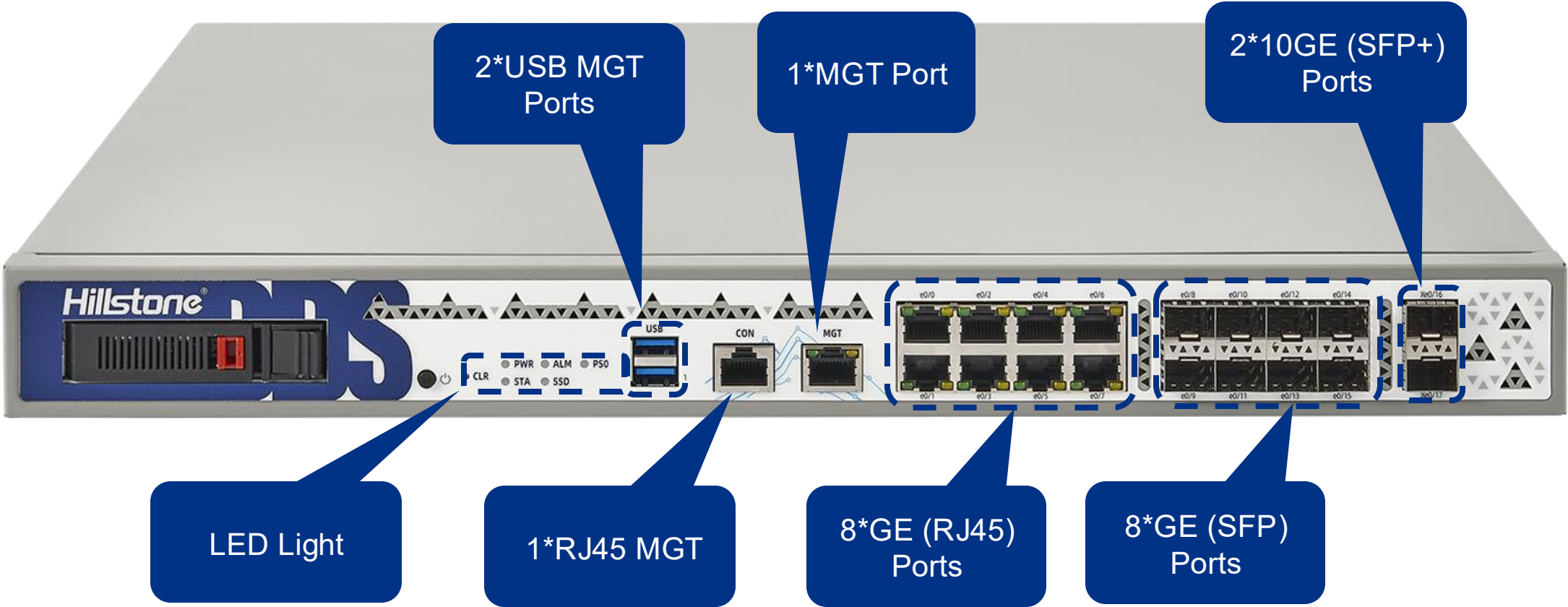
BDS Product Portfolio



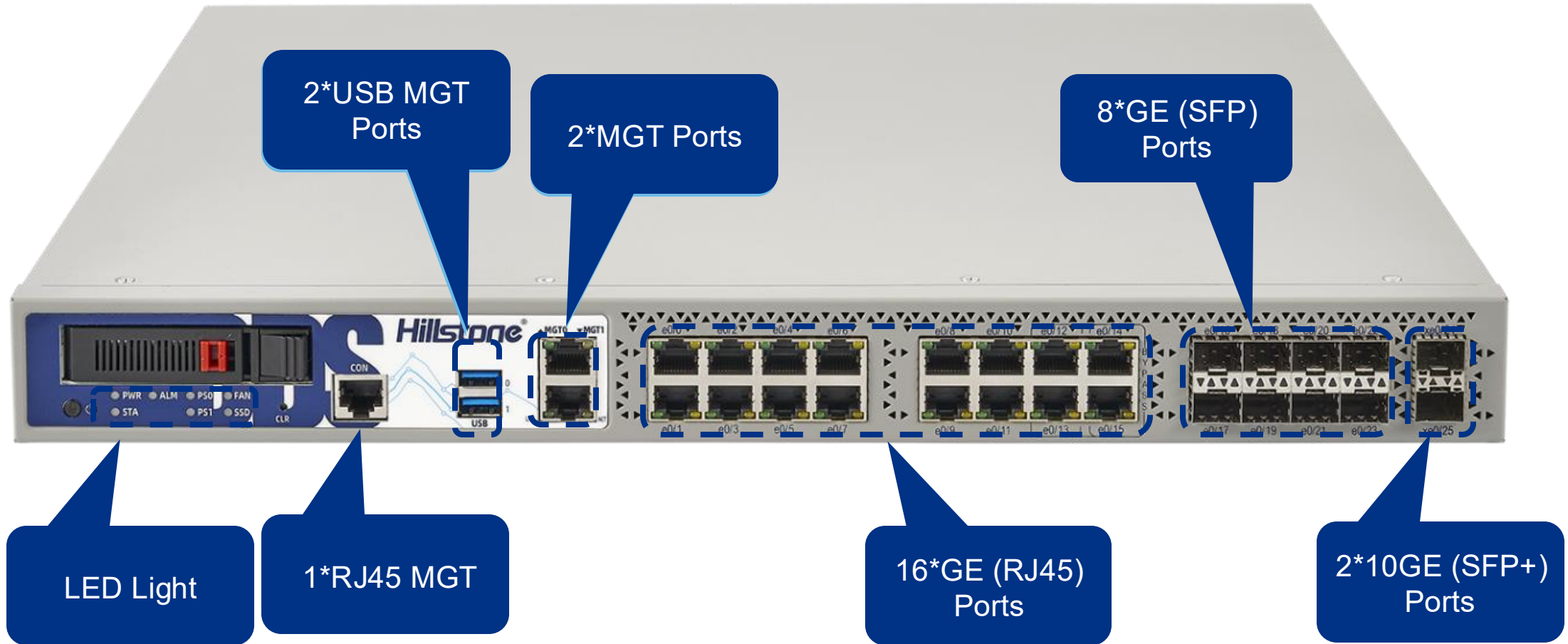
I-1850 Hardware Specification



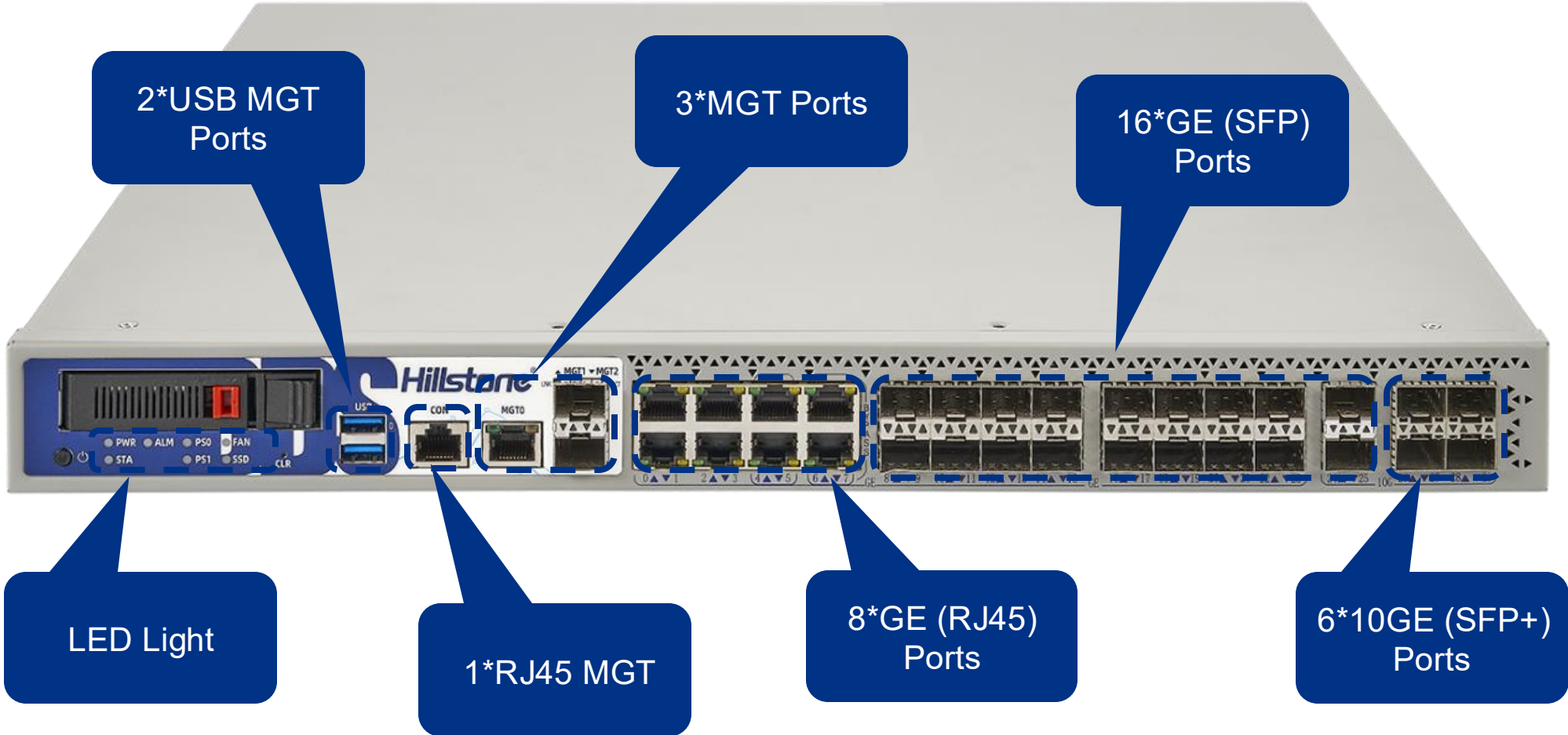
I-1870 Hardware Specification



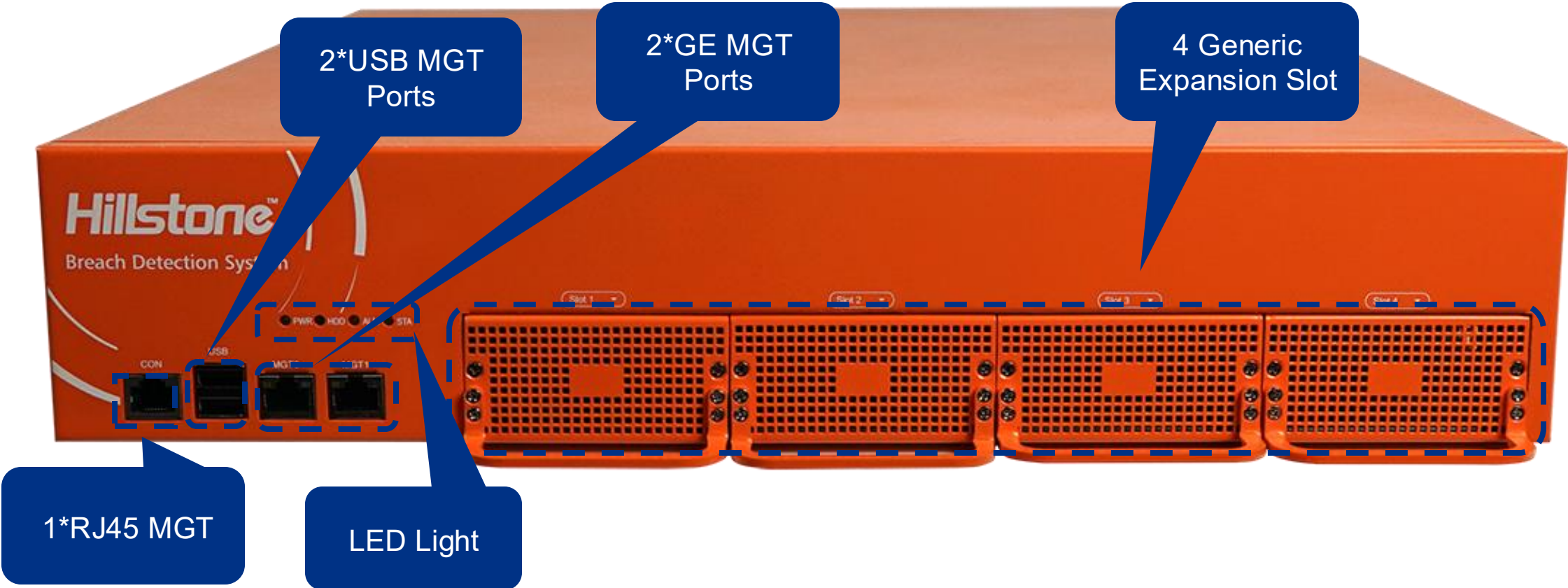
I-2860 Hardware Specification



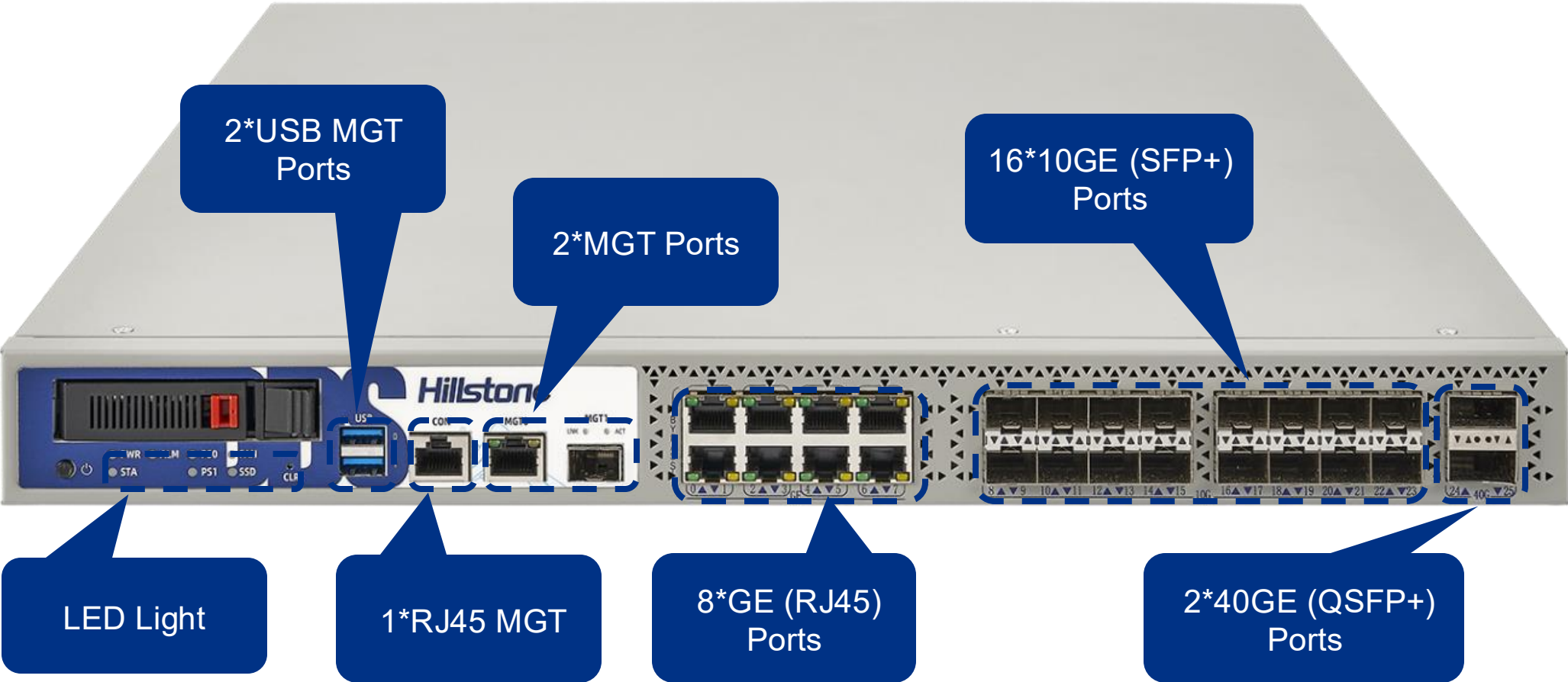
I-3860 Hardware Specification



I-5850 Hardware Specification



I-5860 Hardware Specification



BDS 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	2x10GE (SFP+) 8 x GE (SFP) 8 x GE (RJ45)	2x10GE (SFP+) 8 x GE (SFP) 16 x GE (RJ45)	6x10GE (SFP+) 16xGE (SFP) 8xGE (RJ45)	N/A	8xGE (RJ45) 16x10GE (SFP+) 2x40GE (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 BDS 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	

* 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

- 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.

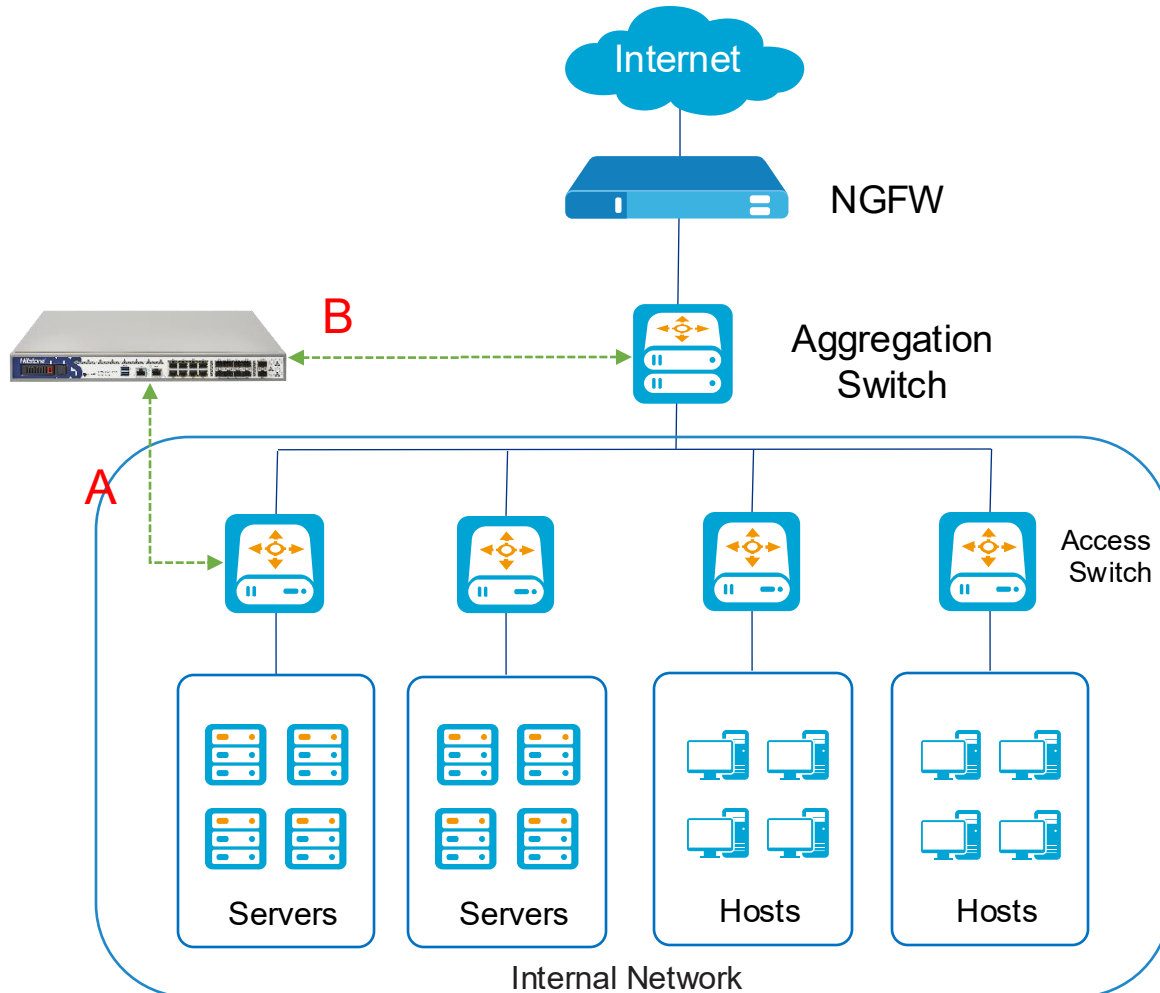
Two installation methods are available:

- 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

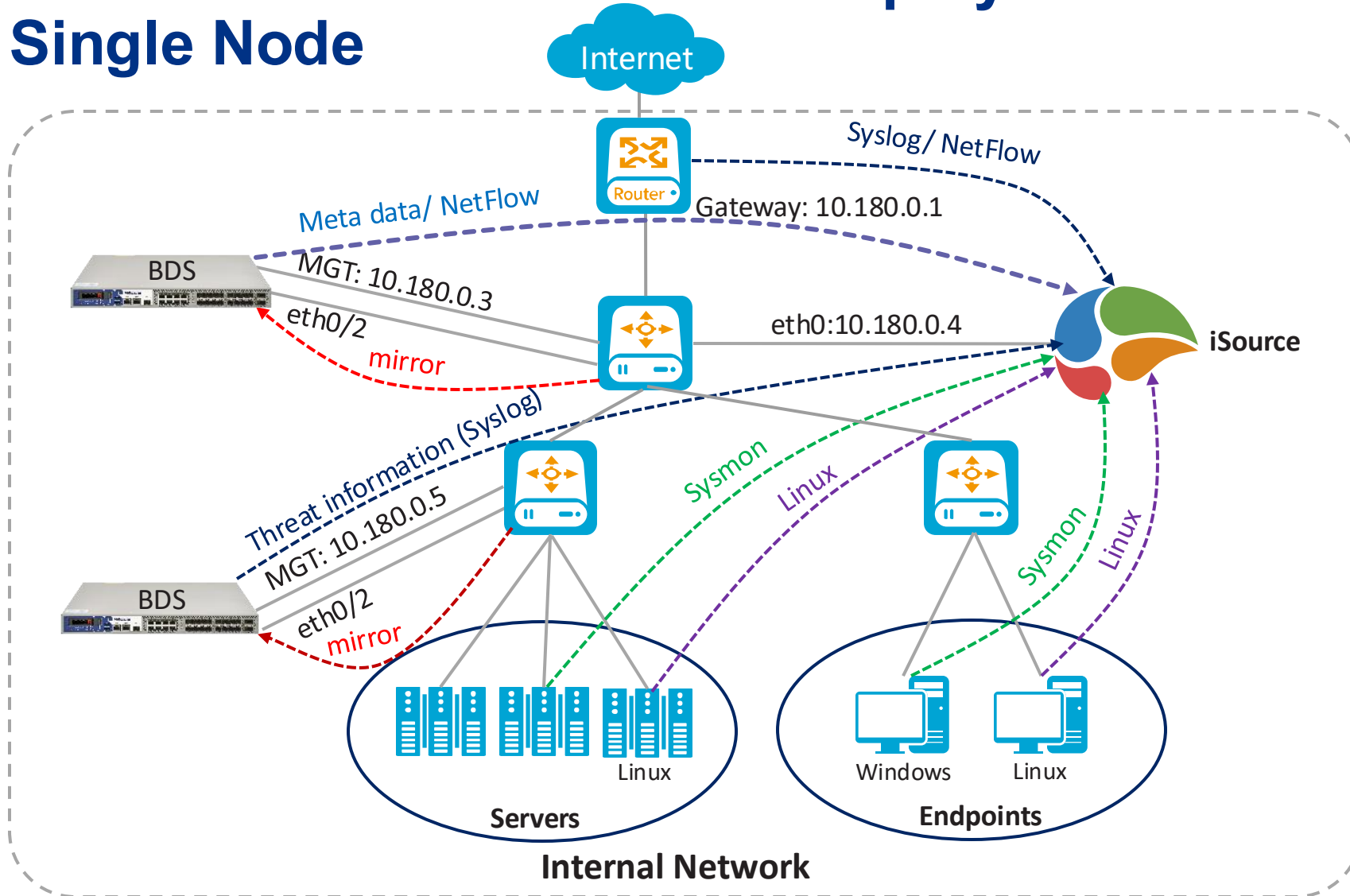
- Monitor traffic between servers within the same segment; servers in different segments; server and internet; servers and other hosts.

- **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

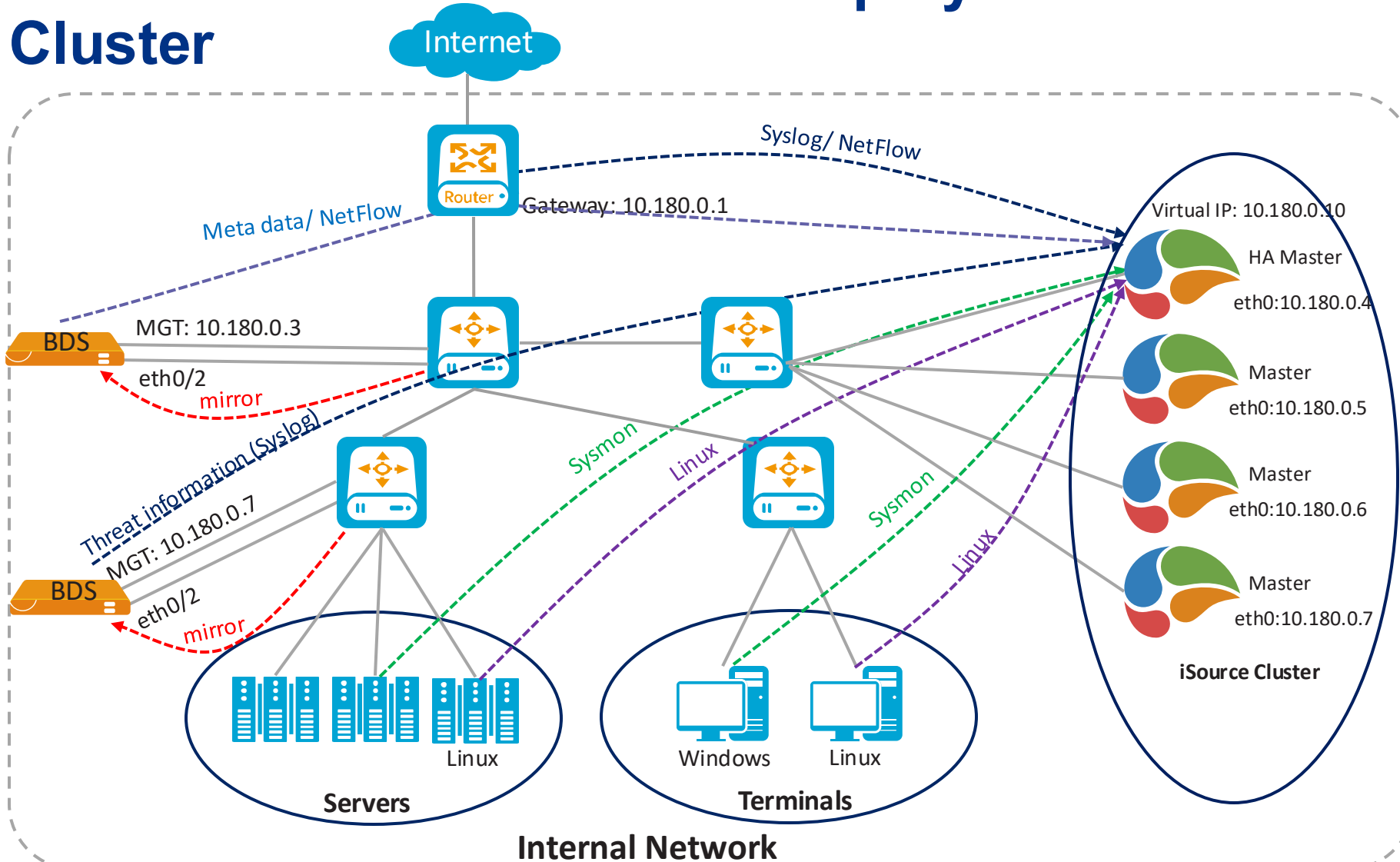
Hillstone BDS and iSource Deployment Scenario- Single Node



Single Node Deployment

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

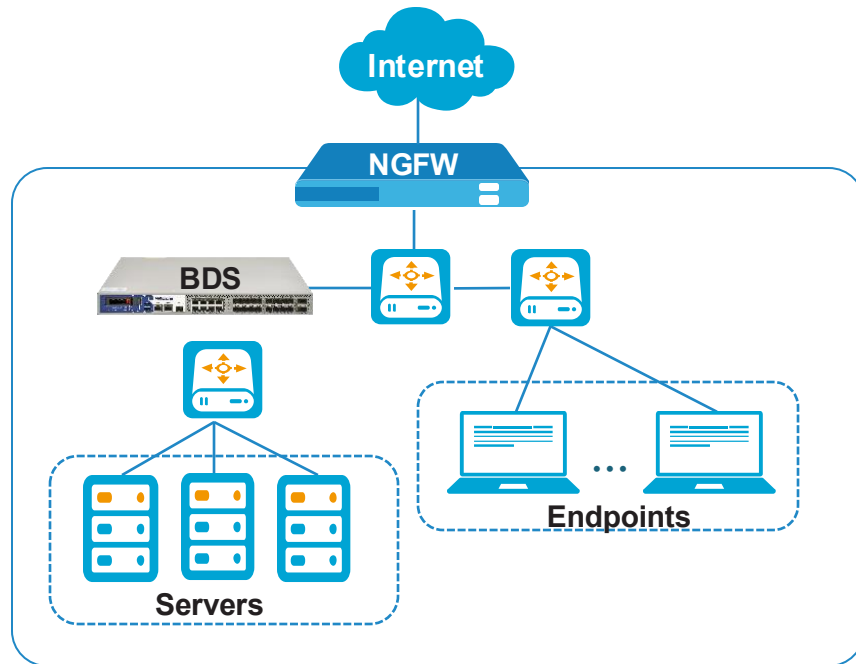
Hillstone BDS and iSource Deployment Scenario-Cluster



Cluster Deployment

- BDS deployed in TAP mode
- Cluster up to 5 nodes
- iSource 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 BDS 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 BDS 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



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.

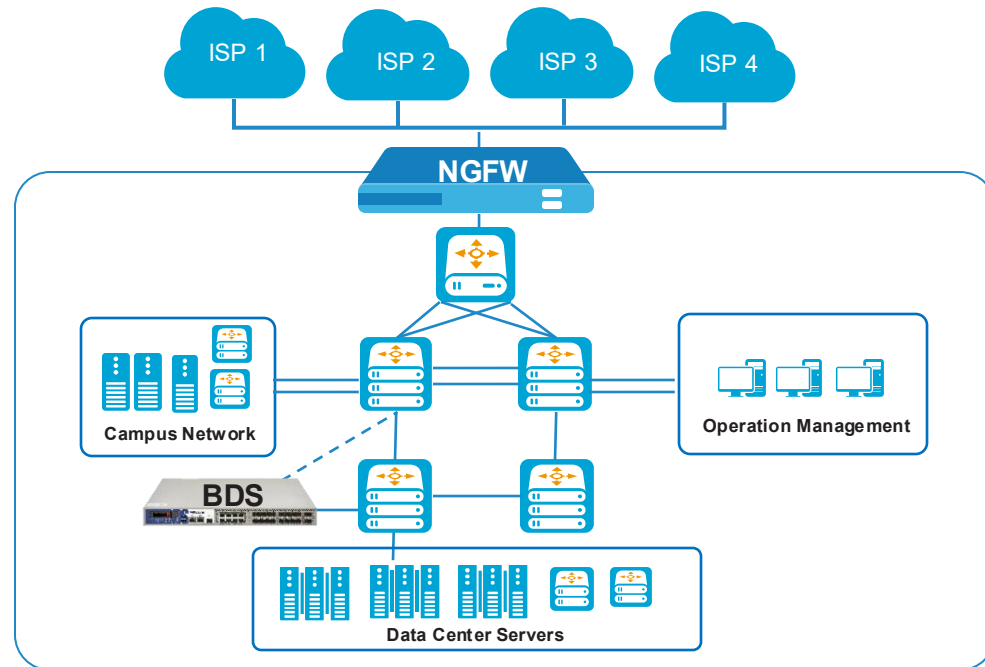
Hillstone Solution

- 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.

Customer Profile:

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

Case Study 4: Protect Critical Servers for a Large University



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.

Customer Profile

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

Customer References



Computer Network Information Center
Government,
China



China Telecom
ISP,
China



Datatell
Communication,
Costa Rica



Shaanxi Regional Electric Power
Group
Energy,
China



Gobierno Regional De Amazonas
Government,
Peru



Woori Bank
Finance,
S.Korea



Bangkok Metropolitan Administration
Government,
Thailand



Camel
Manufacturing,
China



Sichuan Railway Industry Investment Group
Finance,
China



Credimatic
Finance,
Ecuador



Xiangnan University
Education,
China



Nanjing City Vocational College
Education,
China



Jiangsu Agri-animal Husbandry
Vocational College
Education,
China



Changchun Institute of Technology
Education,
China



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

