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

Introducing the Hillstone Future-Ready A-Series Next Generation Firewall

Integrative Cybersecurity

Visionary. AI-powered. Accessible.

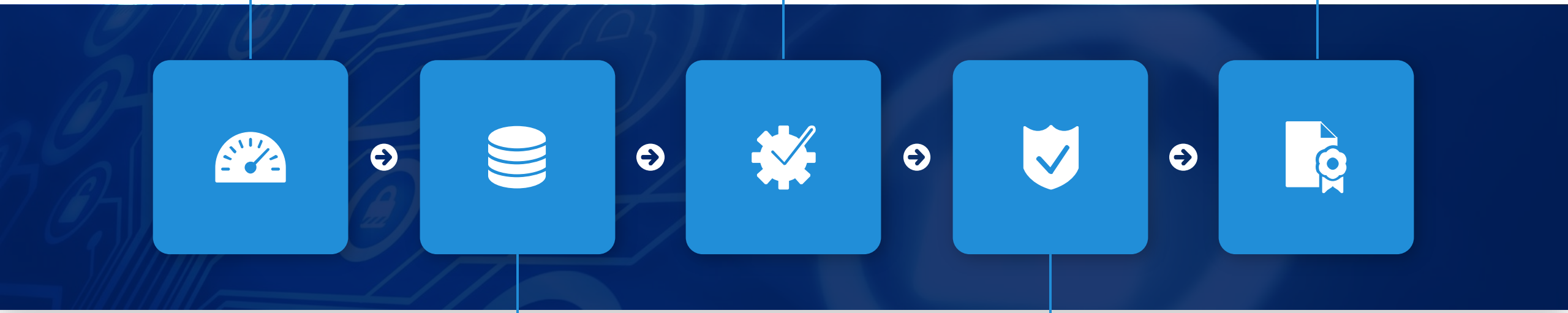
What's the New Reality for NGFW?

What's the New Reality for NGFW?

Performance becomes a bottleneck

Devices have to be more compact

Policy overload creates risk and complexity



Storage space limits analytical capability

Security landscape is constantly changing dramatically

A Future-Ready NGFW

A Future-Ready NGFW

Hillstone NETWORKS

A-Series with Advance Hardware Architecture

- High Performance
- Excellent Expansion Capability
- Advanced Threat Protection
- Smart Policy Operation
- Multiple Deployment Scenarios

The Hillstone A-Series: An Overview

Product name:
SG-6000-A-Series NGFW

Product Highlights

- Built on a new generation of firewall hardware architecture.
- Excellent application security protection performance, high-density ports, large-capacity local and optional expansion storage, at a better TCO.
- Based on Hillstone innovative operating system, StoneOS.
- Hillstone's evolution in AI will continue to provide robust advanced threat detection in the future.

A Future-Ready NGFW - Extraordinary Performance Based on Advanced Hardware Architecture

Hillstone NETWORKS

A-Series with Advance Hardware Architecture

- **High Performance**
- **Excellent Expansion Capability**
- **Advanced Threat Protection**
- **Smart Policy Operation**
- **Multiple Deployment Scenarios**

Advanced NGFW Hardware Architecture

Powerful computing foundation guarantees high performance

Friendly software ecology for third-party integration

SSL decryption hardware acceleration capability: alleviates CPU intensive tasks from servers

Hillstone proprietary hardware acceleration engine: significantly improves packet fast forwarding capability by offloading traffic from CPU

High-density interfaces, and front and rear-end air ventilation in compact design

Note: the SSL decryption hardware acceleration capability will be available via software upgrade in phase 2. A200(W)-IN series do NOT support hardware acceleration; the Hillstone proprietary hardware acceleration engine is only available for A6800-IN and A7600-IN.

Outstanding Hardware Design

SSL Decryption Hardware Acceleration

- Free up more CPU resources
- Defend against the threats of encrypted traffic with strong decryption capability

Compact Design

- Small size, energy-saving: Desktop or 1RU rackmount model
- Possess high-density interfaces and power modules in all 1RU rackmount models

Front and Rear-end Air Ventilation

- Improve heat-dissipation capability
- Meet the heat-dissipating requirement of data center rack
- Maintain good performance

Hillstone Proprietary Hardware Acceleration Engine

High Throughput

- Enable high-end models to cover the throughput requirements of high-traffic scenarios

Fast Packet Forwarding

- Free up CPU by offloading IPv4/IPv6 traffic, to process comprehensive security services

CPU Offload

- Ultra-low latency in packet forwarding within a few microseconds, fully meet the needs of latency-sensitive scenarios

High Performance Highlights & Values

High Firewall Throughput

- High firewall throughput up to **280 Gbps**

Meet the high-traffic needs in scenarios like data centers

High Application-Layer Performance

- High IPS throughput up to **70 Gbps** with 2QSFP+ module
- High level of concurrent sessions up to **42 Million**

Meet real-world network security needs

Powerful Fast-forward Capability

- Ultra-low latency in packet forwarding within a few **microseconds**

Meet the requirements of latency-sensitive scenarios

A Future-Ready NGFW - Excellent Expansion Capability

A-Series with Advance Hardware Architecture

- High Performance
- Excellent Expansion Capability
  - *Interface & Storage*
- Advanced Threat Protection
- Smart Policy Operation
- Multiple Deployment Scenarios

Excellent Access Capability with Advanced Interface

Interface Highlights

- Large amount of fixed, high-speed I/O ports (high-density up to 4 QSFP28)
- A2715-IN/A2815-IN/A3615-IN/A3700-IN/A3800-IN/A3815-IN/A5K-IN/A6800-IN/A7600-IN models support expansion
- Native bypass pairs in A1100-IN/A2K-IN/A3K-IN/A5K-IN rackmount models
- All rackmount models provide two USB3.0 interfaces

Benefits

- NGFW can also act as a switch and router; fast data rate support
- Throughput increase by adding expansion module : A3700-IN/A3800-IN: 20 Gbps -> 30 Gbps, A5100-IN/A5155-IN: 25 Gbps -> 50 Gbps, A5200-IN/A5255-IN: 32 Gbps -> 65 Gbps, A5500-IN/A5555-IN: 40 Gbps -> 80 Gbps, A5600: 60 Gbps -> 85 Gbps, A5800-IN: 80 Gbps -> 95 Gbps, A7600: 280 Gbps -> 320 Gbps
- Bypass capability ensures business continuity
- 4G access capability

Value

- Cost Savings
- Increased Performance
- High Availability
- Future Ready

Platform	A200-IN	A200W-IN	A1000-IN	A1100-IN	A2000-IN	A2600-IN	A2700-IN	A2715-IN	A2800-IN	A2815-IN	A3000-IN	A3600-IN	A3615-IN
Fixed I/O Ports	5 * GE, 1 * SFP	5 * GE, 1 * SFP	4 * GE	8 * GE(RJ45) (1 bypass pair)	8 * GE(RJ45) (1 bypass pair)	8 * GE(RJ45) (1 bypass pair)	2 * SFP+ 8 * SFP 8 * GE	8 * SFP, 8 * GE (2 bypass pairs)	2 * SFP+ 8 * SFP 8 * GE	8 * SFP, 8 * GE (2 bypass pairs)	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	8 * SFP, 8 * GE (2 bypass pairs)
Wi-Fi/ 4G Dongle	4G Dongle	IEEE802.11 a/b/g/n/ac, 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
Expansion Slots	-	-	-	-	-	-	-	1	-	1	-	-	2
Expansion Module Option	-	-	-	-	-	-	-	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN	-	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN	-	-	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN IOC-A-4SFP+-IN IOC-A-2QSFP+-IN IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN
USB	1 × USB2.0	1 × USB2.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0

Platform	A3700-IN	A3800-IN	A3815-IN	A5100-IN	A5155-IN	A5200-IN	A5255-IN	A5500-IN	A5555-IN	A5600-IN	A5800-IN	A6800-IN	A7600-IN
Fixed I/O Ports	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	8 * SFP, 8 * GE (2 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE （2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE （2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE （2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE(RJ45) (4 bypass pairs)	4 * QSFP28 (or 2 * QSFP+, 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP	4 * QSFP28 (or 2 * QSFP+, 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP
Wi-Fi/ 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	N/A	N/A
Expansion Slots	1	1	2	1	1	1	1	1	1	1	1	1	1
Expansion Module Option	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN IOC-A-4SFP+-IN IOC-A-2QSFP+-IN IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN
USB	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0

Better Analytics and Visibility with Increased Storage

Hillstone NETWORKS

eMMC (4/8/64GB)
Standard

- Store configuration files, signature databases, images, etc.
- Store network/event/configuration logs, reports
- Cloud Sandbox logs or threat logs should be sent to HSM, HSA or CloudView for longer term storage
- The storage size of each module is specified by the system and cannot be configured

eMMC (8/64GB)
Standard

+

Hard Drive (256GB to 1.92TB)
Optional

- eMMC stores:
  - configuration files, signature databases, images, etc.
- Hard drive stores:
  - Network/event/configuration/threat/cloud sandbox logs (up to 6 months)
  - More comprehensive reports
- More analytics capability, including IPS threat packet capture
- The storage size of each module is specified by the system by default, and it can be configured

Platform	A200-IN	A200W-IN	A1000-IN	A1100-IN	A2000-IN	A2600-IN	A2700-IN	A2715-IN	A2800-IN	A2815-IN	A3000-IN	A3600-IN	A3615-IN	A3700-IN	A3800-IN	A3815-IN	A5100-IN	A5155-IN	A5200-IN	A5255-IN	A5500-IN	A5555-IN	A5600-IN	A5800-IN	A6800-IN	A7600-IN
Local Storage	4 GB	4 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB
Expansion Storage Options	0	0	256 GB SSD	256 GB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD

A Future-Ready NGFW - Advanced Threat Protection

A-Series with Advance Hardware Architecture

- High Performance
- Excellent Expansion Capability
  - *Interface & Storage*
- **Advanced Threat Protection**
- Smart Policy Operation
- Multiple Deployment Scenarios

Advanced Threat Protection for Known and Unknown Malware

IPS blocks vulnerability exploitation

IP Reputation blocks risky IPs from accessing servers

URL Filtering controls user access to specified websites

Anti-Virus filters viruses in files of different types and over different protocols

Anti-Spam classifies and prevents potential spam

Anti-Virus responds to known viruses

Cloud Sandbox responds to unknown viruses

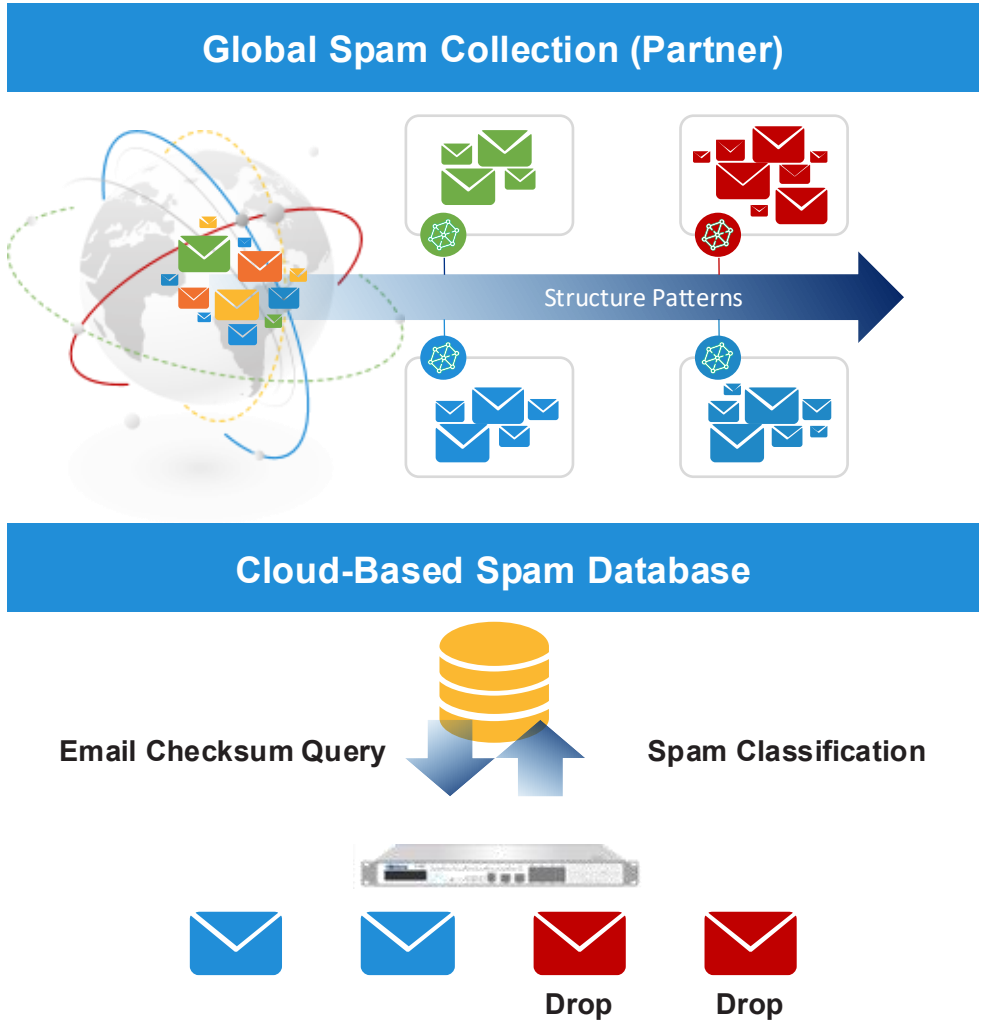
Botnet C&C Prevention blocks the control channel and catches intranet bots

Pre-breach | **Breach** | **Post-breach**

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

Application Control

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
- **Supports encrypted traffic spam detection**
- Works on both SMTP(S) and POP3(S) email protocols
- Inbound and outbound detection
- Whitelisting permits emails from trusted domains
- Support multiple languages, formats, or content of the message

Cloud Sandbox for Malicious File Detection and Prevention

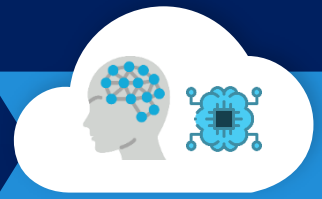
Static Analysis/ Pre-Processing

- URL whitelist, file signature verification
- Cloud-based suspicious samples

MD5 query for file behavior; verification and report

Behavior Analysis

- Android/Linux simulation
- Analysis of behaviors including file process, registry action, network activities
- Evasion detection



Cloud Intelligence

- Identify malicious files
- Generate threat logs and reports
- Share threat intelligence
- Block threats

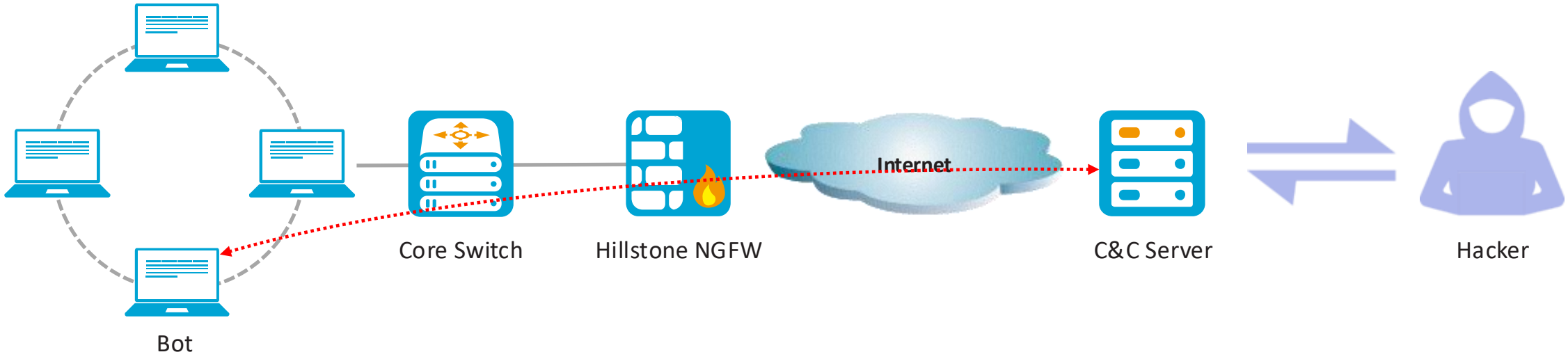
Malicious Files

Reporting

Signature Update

NGFW

Complete Botnet C&C Prevention



C2 Address Database

DNS Sinkhole

DNS Tunnel Detection

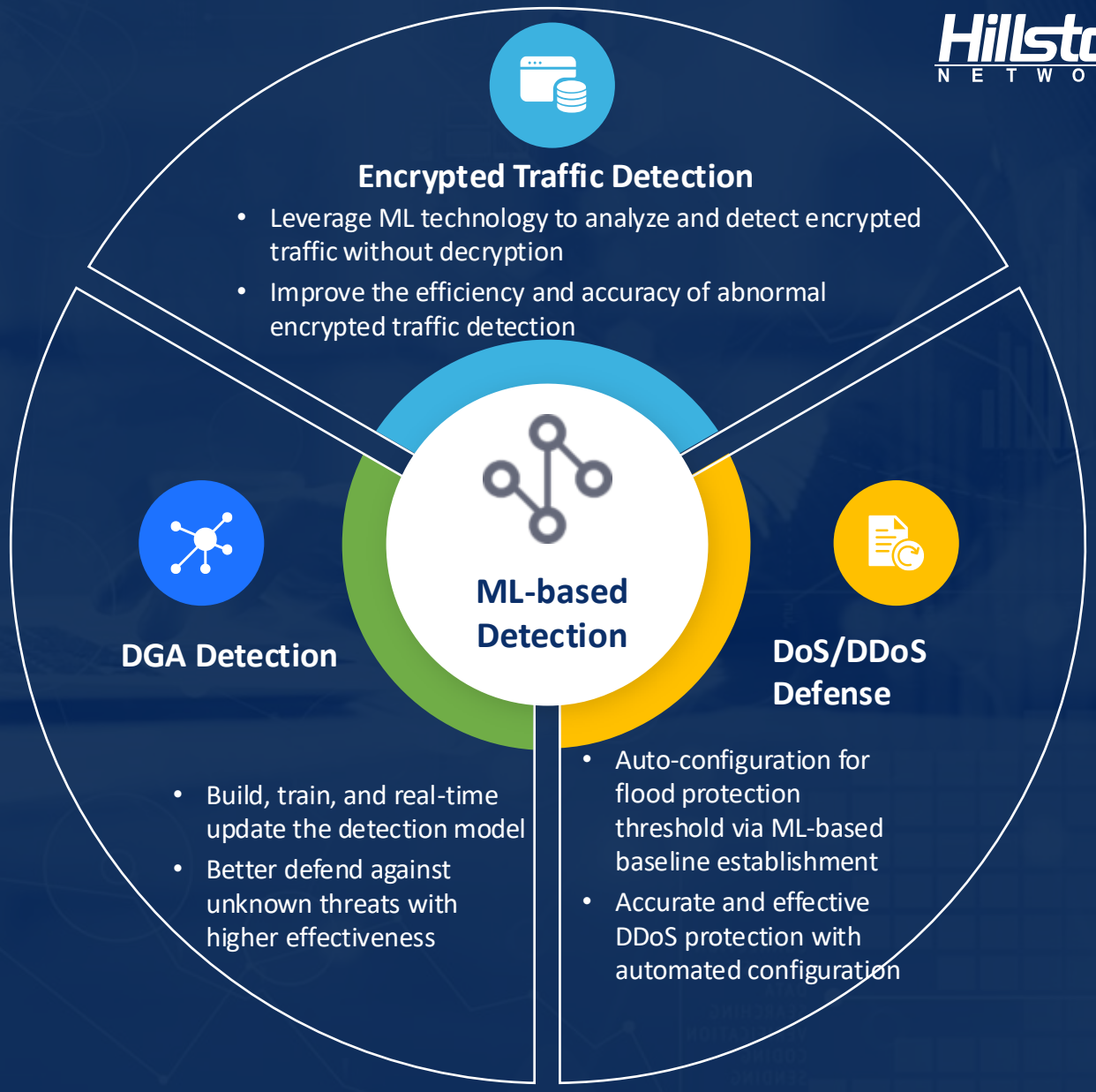
DGA Domain Detection

ML-based Intelligent Treat Detection and Protection

Encrypted Traffic Detection

DoS/DDoS Defense

DGA Detection



A Future-Ready NGFW - Smart Policy Operation

A-Series with Advance Hardware Architecture

- High Performance
- Excellent Expansion Capability
- Advanced Threat Protection
- **Smart Policy Operation**
- Multiple Deployment Scenarios

Smart Policy Operation

Automated User Policy Deployment

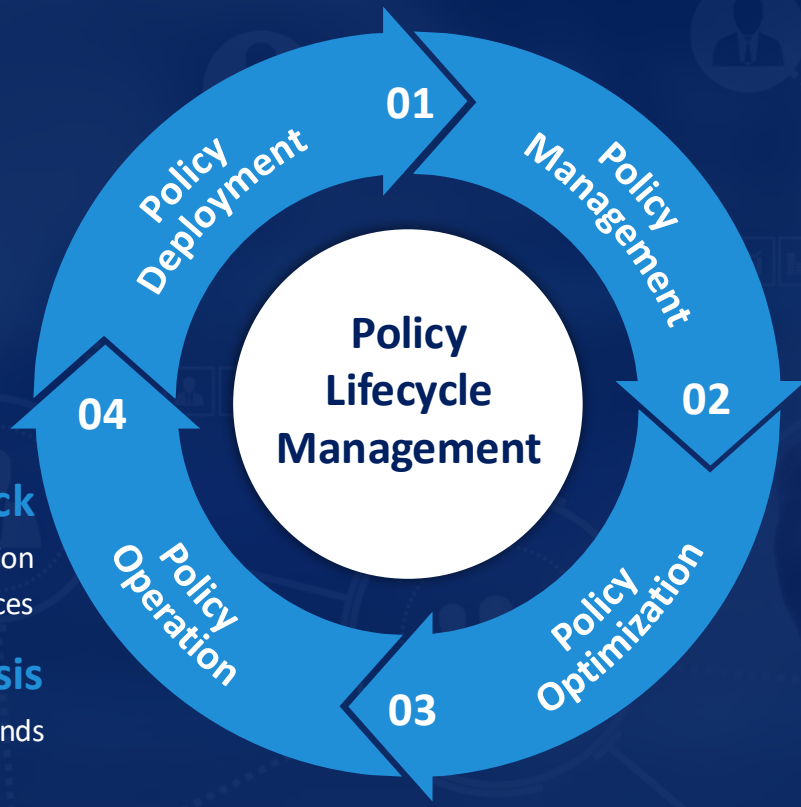
- Radius Dynamic Authorization
- Automatically issue user policy via CoA message

Policy Redundancy Check

- Discover redundant or conflict FW/NAT policies for deletion
- Provide detailed insights and remediation advices

Policy Analysis

Adjust policies by observing hit counts and hit trends



Policy Group

Efficient policy management based on business requirements

Aggregate Policy

Combining a set of individualized policies into one unified policy

Millions of Mini Policy

Ensures consistent policy enforcement on all firewall security features with extreme scalability

Policy Assistant

Generate and refine granular policies based on traffic patterns

Easy Deployment

Rapid Launch of New Services

Dynamic Policy Adjustment

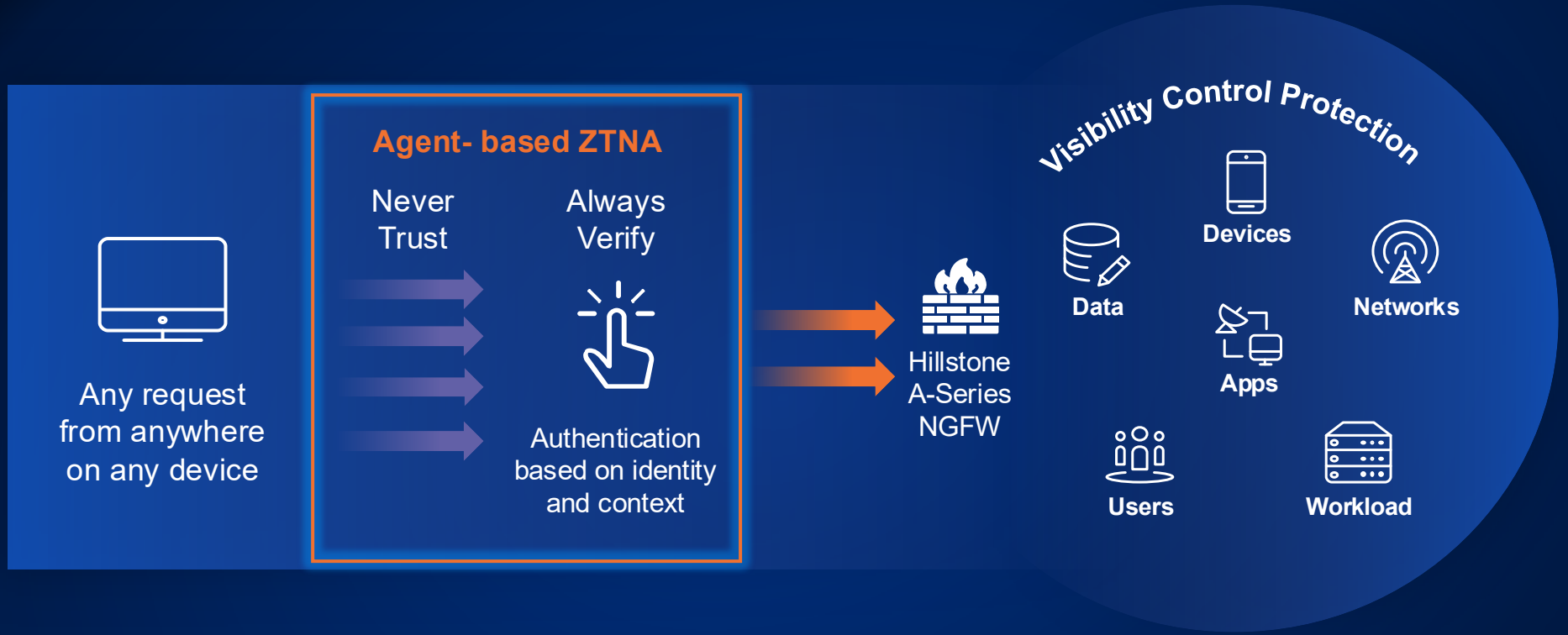
Increased Efficiency & Reduced Overhead

A Future-Ready NGFW - Multiple Deployment Scenarios

A-Series with Advance Hardware Architecture

- High Performance
- Excellent Expansion Capability
- Advanced Threat Protection
- Smart Policy Operation
- Multiple Deployment Scenarios

Zero Trust Network Access (ZTNA) Solution



Zero Trust

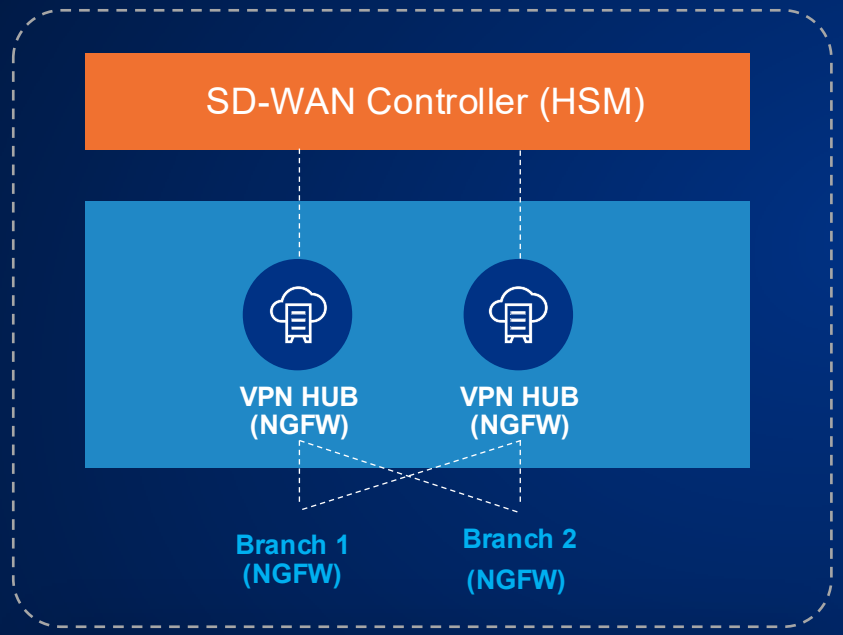
Highlights

- Identity-Based, Least-Privileged Secure Access
- Context-Aware, Adaptive Access Control
- Centralized and Efficient Management
- Award-Winning Enterprise-Grade Security Foundation

NGFW Fits into Hillstone Solutions

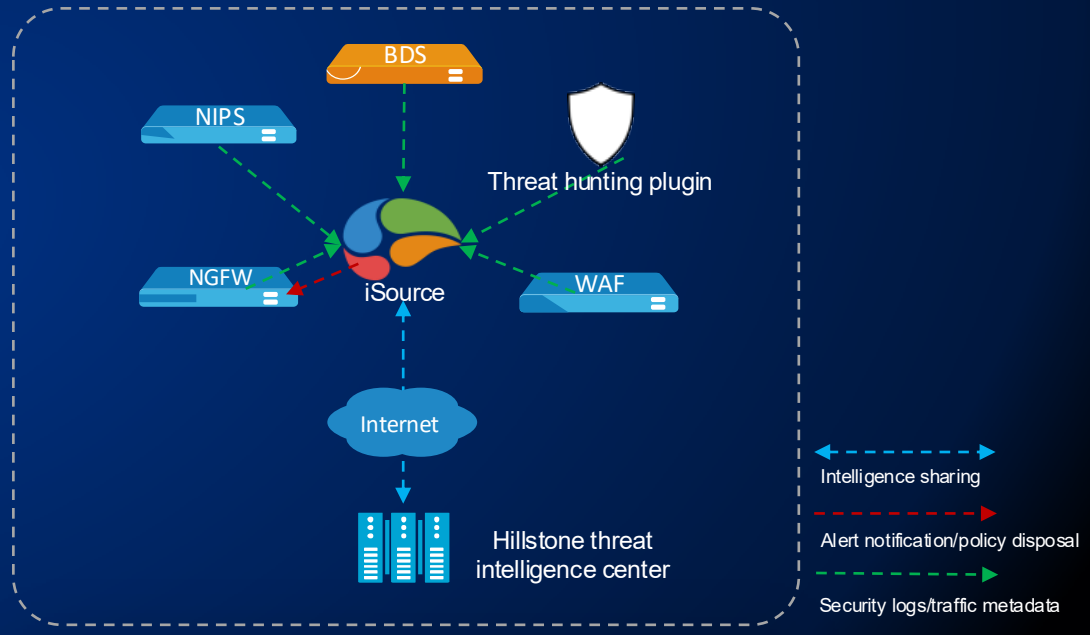
The integration of NGFW and other Hillstone security products enables multiple Hillstone solutions

SD-WAN solution



- Efficient centralized management for multiple NGFW

XDR solution



- Promote joint protection against new types of attacks through integration with iSource and deployment in XDR solution

Enable Multiple Use Cases with High Performance

Network Edge

- Powerful network security capabilities to defend against more advanced threats
- Expedited execution of various security services with strong CPU power

Data Center

- High throughput to handle massive volumes of traffic in data center
- Twin-mode HA maintains high reliability of data center communication

SD-WAN

- High security performance of built-in NGFW brings faster, lower-cost and secure local internet connections at remote location

Remote Access with ZTNA

- Context and identity-aware, and least-privileged secure access control guarantee the security and effectiveness for the remote access

Fast, Effective, Efficient Future-Ready Security Protection with Hillstone A-Series NGFW

FAST

High Security Performance

Leading application layer performance meets real network security needs

EFFECTIVE

Complete Advanced Threat Detection and Prevention

Protect against known and unknown threats

EFFICIENT

Smart and Automated Operation

Security operations made easy

FUTURE

Expansion as Needed

High-density ports ensure excellent access capability

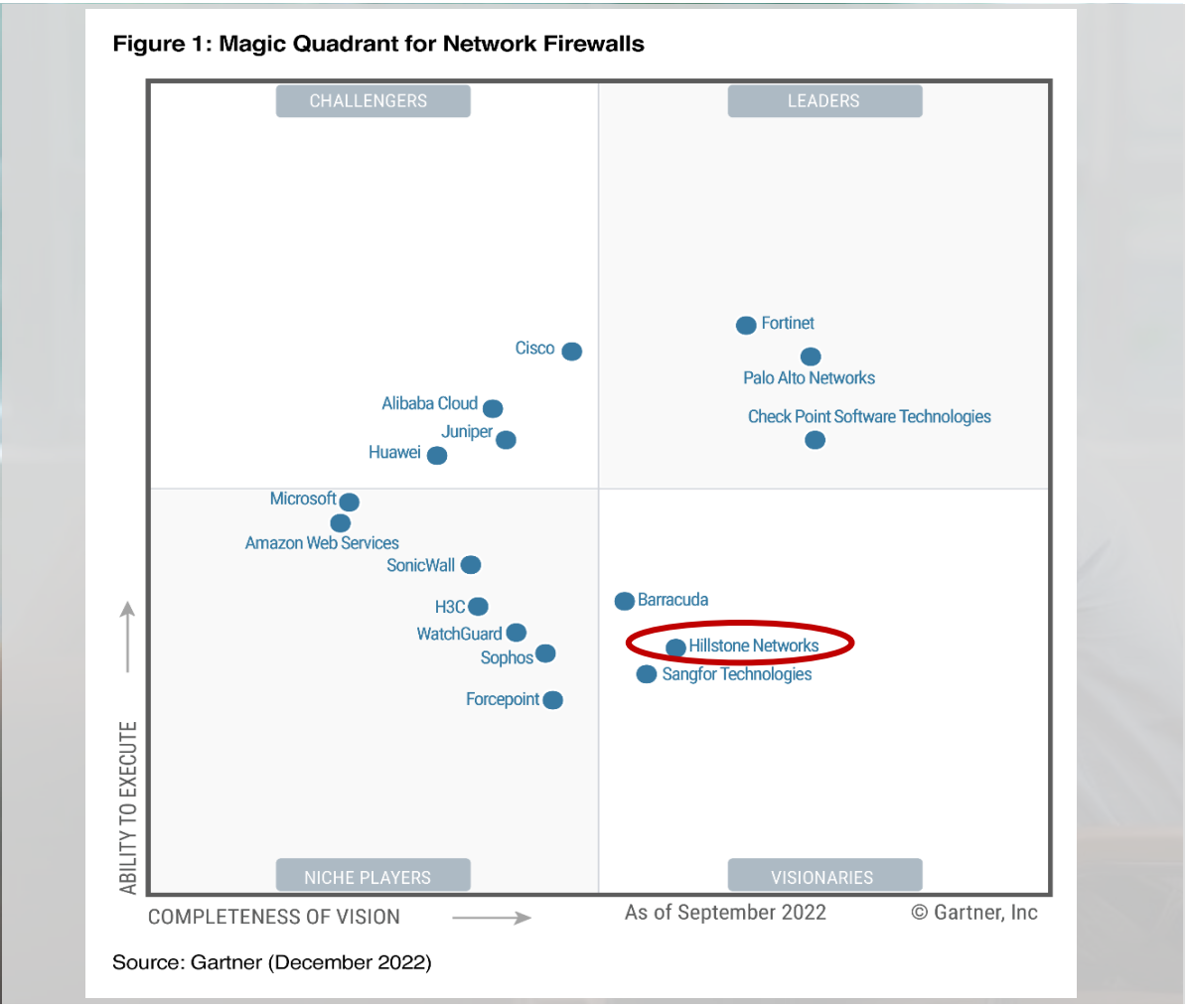
Large storage options allow for deeper analytics and better visibility

EXTENSION

Multiple Solutions and Deployment Scenarios

Enables multiple Hillstone solutions and deployments scenarios with high performance

Hillstone Networks is Your Trusted Security Partner



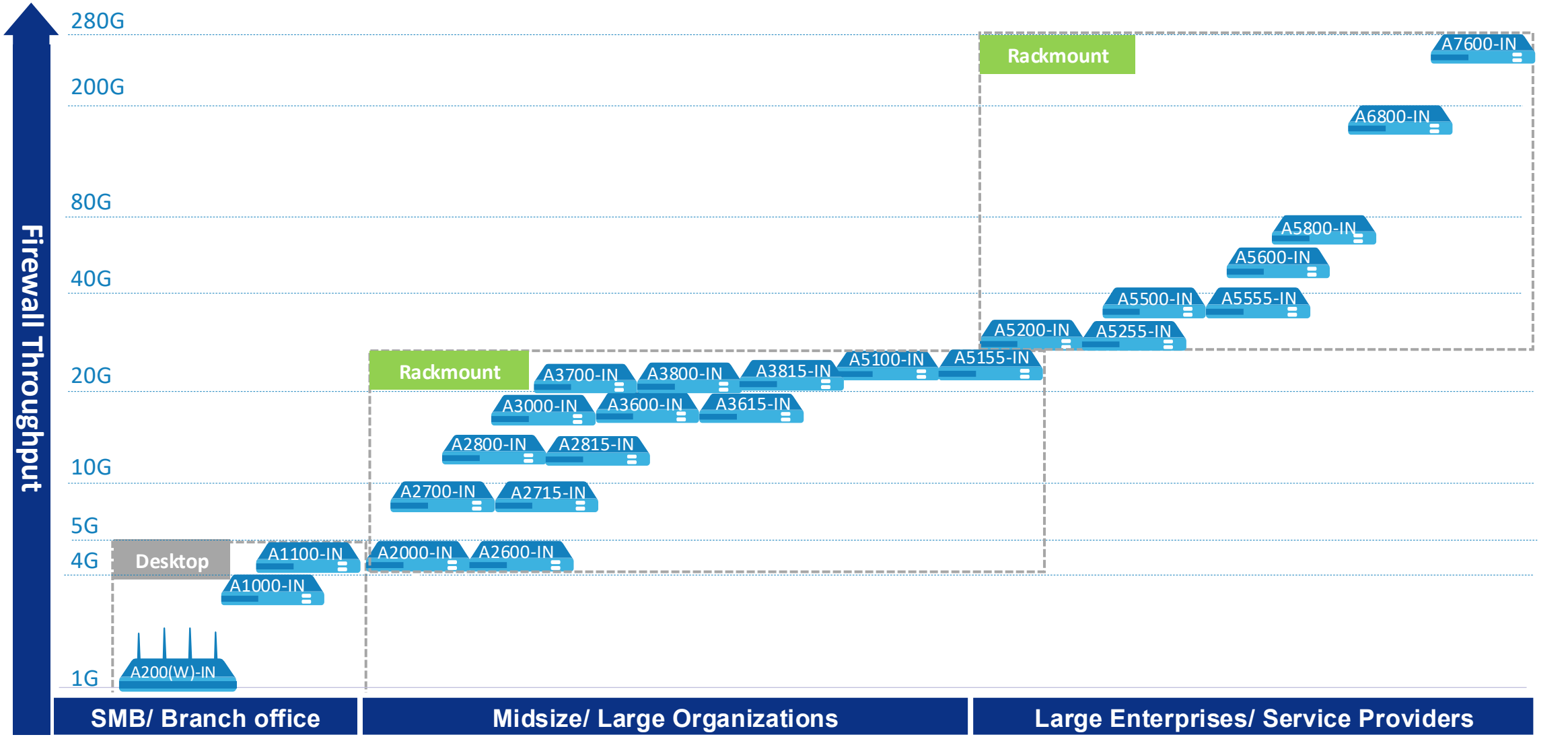
Gartner

A Visionary in the Gartner Magic Quadrant for Network Firewalls

9 Consecutive Years *in Gartner Magic Quadrant for Network Firewalls*

The Product Introduction

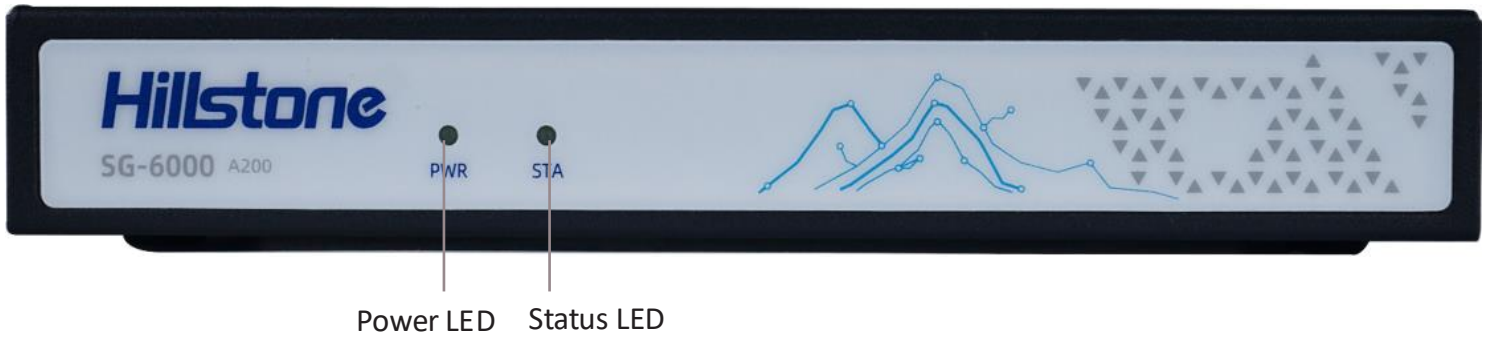
A-Series Product Positioning

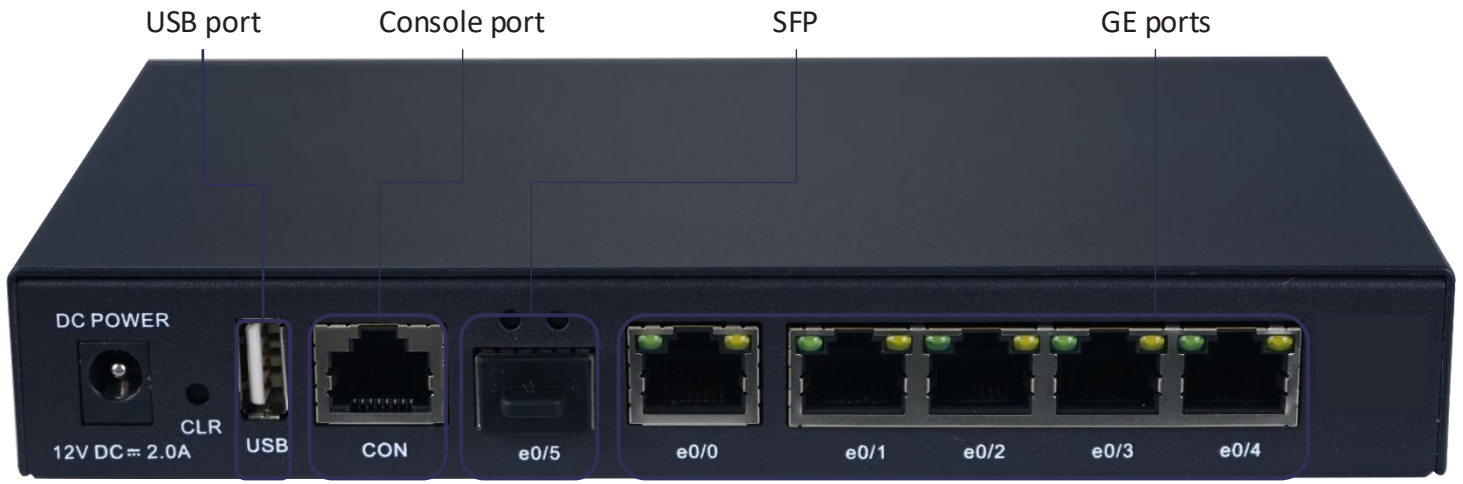


The Hillstone A-Series NGFW: Specifications

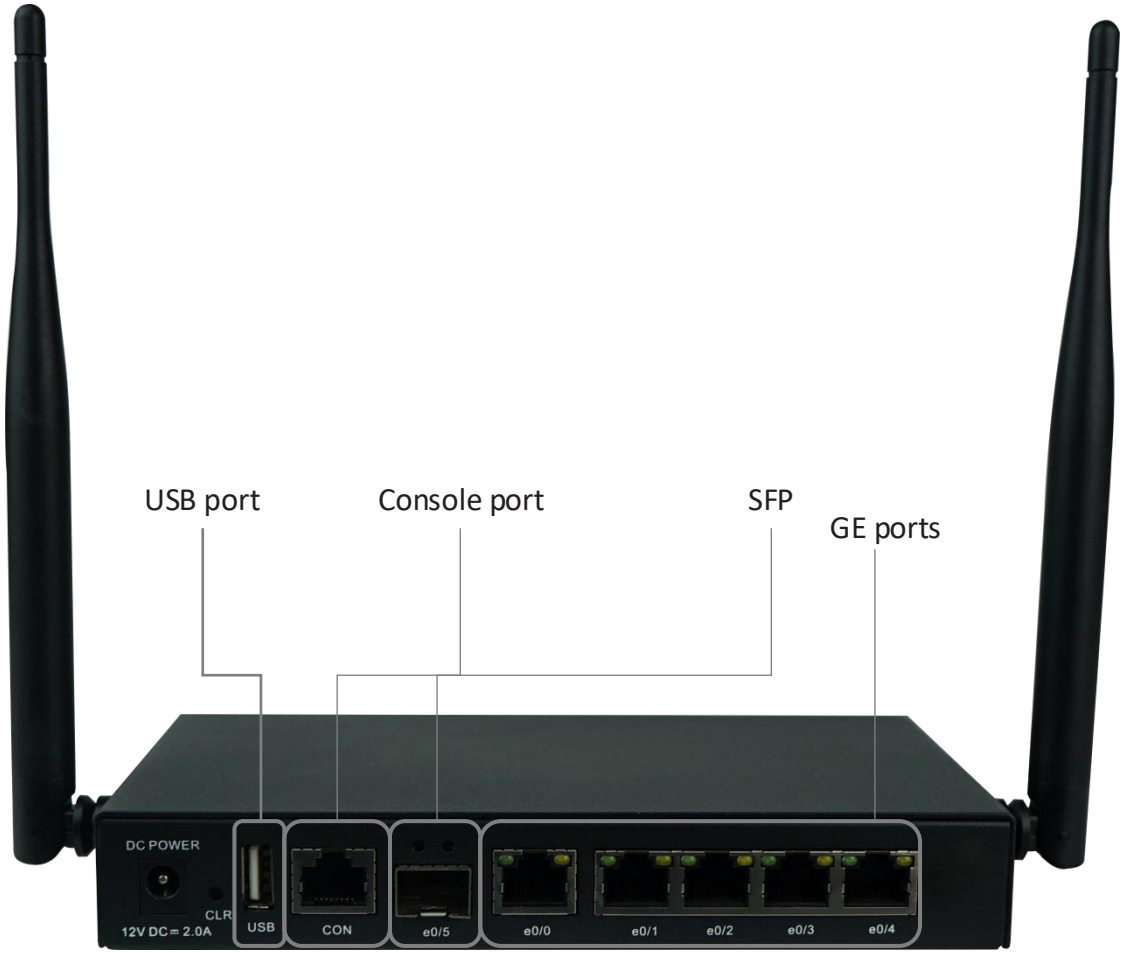
	Desktop			
	SG-6000-A200-IN	SG-6000-A200W-IN	SG-6000-A1000-IN	SG-6000-A1100-IN
Firewall Throughput	1 Gbps	1 Gbps	4 Gbps	5 Gbps
Maximum Concurrent Sessions	450,000	450,000	450,000	450,000
New Sessions/s	14,000	14,000	48,000	48,000
IPS Throughput	610 Mbps	610 Mbps	3 Gbps	2.8 Gbps
NGFW Throughput	400 Mbps	400 Mbps	1.5 Gbps	1.7 Gbps
Threat Protection Throughput	200 Mbps	200 Mbps	800 Mbps	800 Mbps
AV Throughput	550 Mbps	550 Mbps	1.8 Gbps	1.8 Gbps
IPsec VPN Throughput	590 Mbps	590 Mbps	2.5 Gbps	2.7 Gbps
Virtual Systems (Default/Max)	N/A	N/A	N/A	N/A
SSL VPN User Number	128	128	128	128
IPsec Tunnel Number	2,000	2,000	2,000	2,000
Management Ports	1 * Console Port, 1 * USB 2.0 Port	1 * Console Port, 1 x USB 2.0 Port	1 * Console Port, 2 * USB3.0 Ports	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45)
Fixed I/O Ports	1 * SFP, 5 * GE	1 * SFP, 5 * GE	4 * GE	8 * GE (including 1 bypass pair)
Wi-Fi/ 4G Dongle	4G Dongle	IEEE802.11a/b/g/n/ac, 4G Dongle	4G Dongle	4G Dongle
Available Slots for Expansion Modules	N/A	N/A	NA	NA
Expansion Module Option	N/A	N/A	NA	NA
Twin-mode HA	N/A	N/A	NA	NA
Local Storage	4 GB	4 GB	8 GB	8 GB
Expansion Storage Options	N/A	N/A	256 GB SSD	256 GB SSD
Power Specification	24W, Single AC (default)	24W, Single AC (default)	36W, Single AC	65W, Single AC
Power Supply	AC 100-240V, 50/60 Hz	AC 100-240V, 50/60 Hz	AC 100-240V, 50/60 Hz	AC 100-240V, 50/60 Hz
Form Factor	Desktop	Desktop	Desktop	Desktop
Weight	2.2 lb (0.6 kg)	2.2 lb (0.6 kg)	3.1 lb (1.4 kg)	3.1 lb (1.4 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

A200 Front and Rear Panel

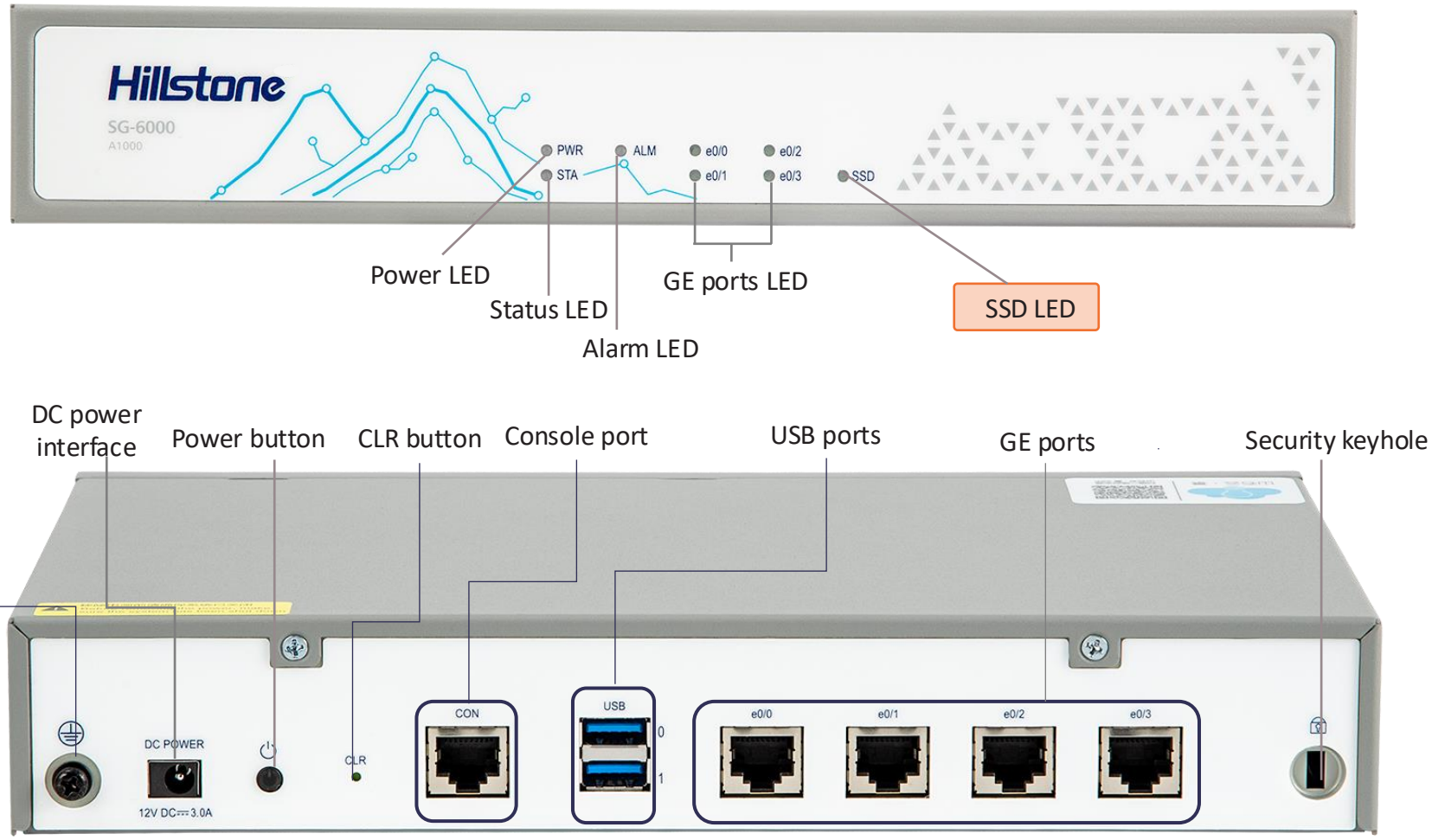




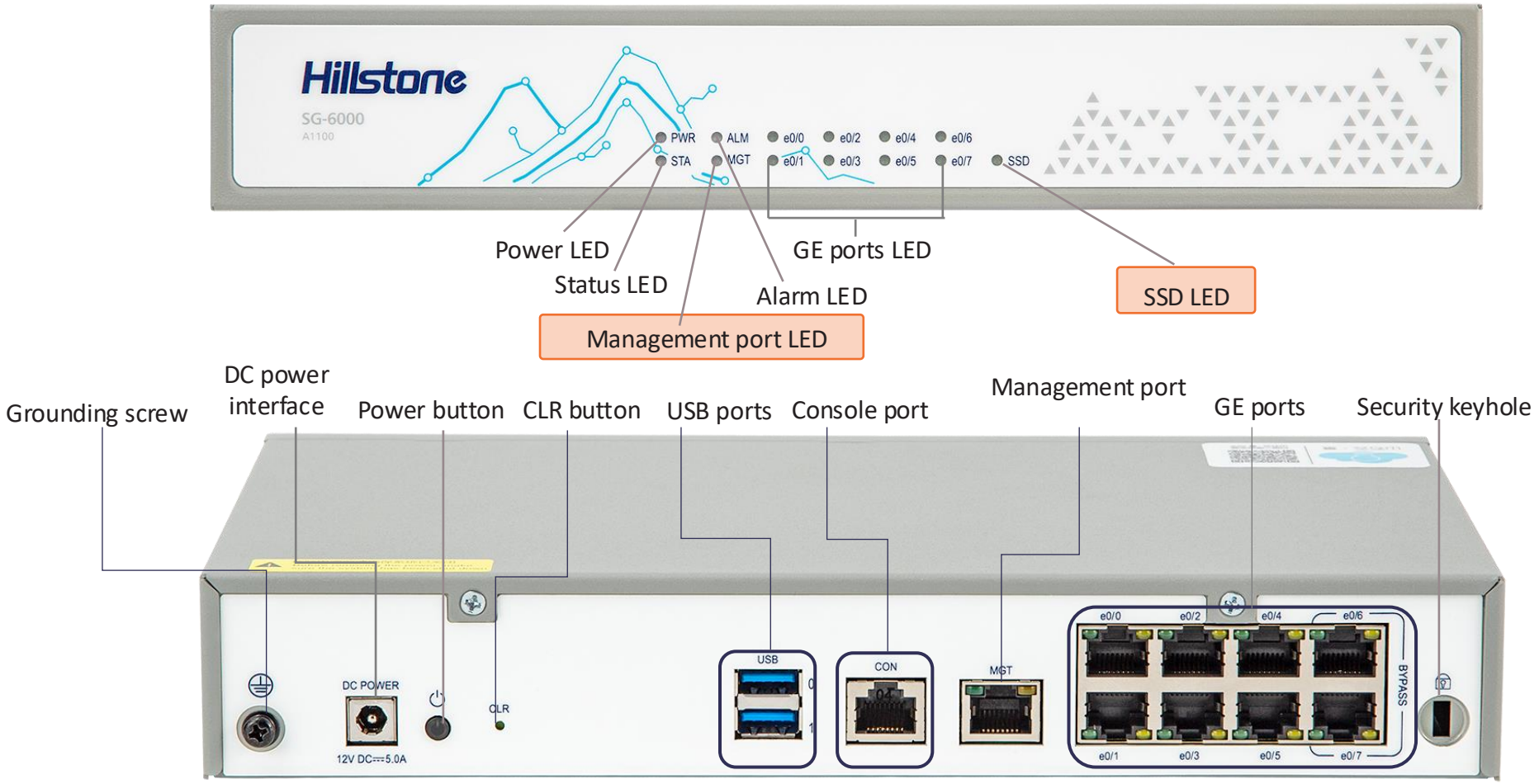
A200W Front and Rear Panel



A1000 Front and Rear Panel



A1100 Front and Rear Panel

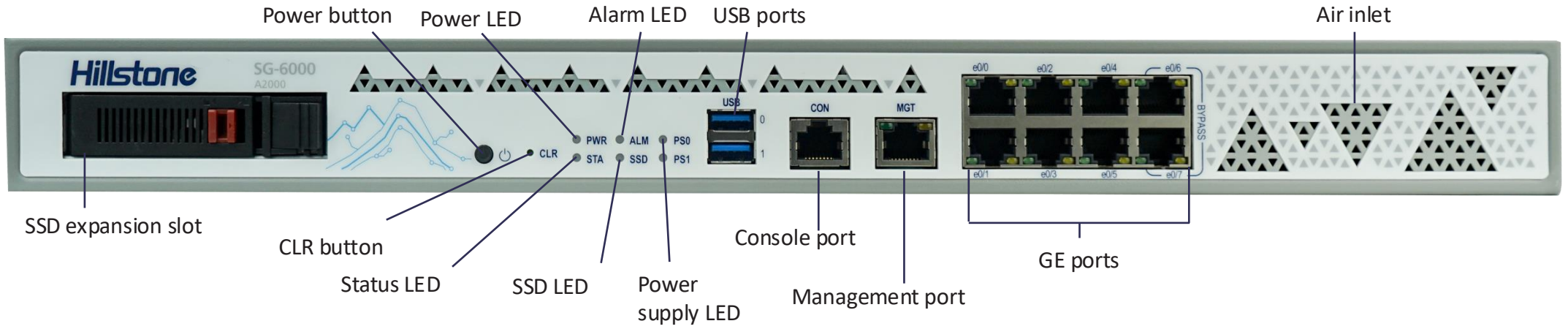


The Hillstone A-Series NGFW: Specifications

	Rackmount					
	SG-6000-A2000-IN	SG-6000-A2600-IN	SG-6000-A2700-IN	SG-6000-A2715-IN	SG-6000-A2800-IN	SG-6000-A2815-IN
Firewall Throughput	5 Gbps	5 Gbps	10 Gbps	10 Gbps	16 Gbps	16 Gbps
Maximum Concurrent Sessions	1.5 Million	1.85 Million	2.2 Million	2.2 Million	2.4 Million	2.4 Million
New Sessions/s	48,000	120,000	130,000	130,000	130,000	130,000
IPS Throughput	3Gbps	3.5 Gbps	8 Gbps	9 Gbps	10 Gbps	9 Gbps
NGFW Throughput	1.7 Gbps	3 Gbps	5 Gbps	6 Gbps	6.5 Gbps	6.5 Gbps
Threat Protection Throughput	1 Gbps	2.5 Gbps	3 Gbps	3 Gbps	3 Gbps	2.8 Gbps
AV Throughput	2 Gbps	3 Gbps	5 Gbps	6 Gbps	6.5 Gbps	6.5 Gbps
IPsec VPN Throughput	3 Gbps	3 Gbps	5 Gbps	5.2 Gbps	6 Gbps	5.3 Gbps
Virtual Systems (Default/Max)	1/5	1/5	1/5	1/5	1/5	1/5
SSL VPN User Number	1,000	2,000	4,000	4,000	4,000	4,000
IPsec Tunnel Number	4,000	6,000	6,000	6,000	6,000	6,000
Management Ports	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port（RJ45）	1 * Console Port, 2 * USB3.0 Ports, 1 * HA Port (RJ45), 1 * MGT Port（RJ45）	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port（RJ45）	1 * Console Port, 2 * USB3.0 Ports, 1 * HA Port (RJ45), 1 * MGT Port（RJ45）
Fixed I/O Ports	8 * GE (including 1 bypass pair)	8 * GE (including 1 bypass pair)	2 * SFP+ 8 * SFP 8 * GE	8 * SFP 8 * GE (including 2 bypass pairs)	2 * SFP+ 8 * SFP 8 * GE	8 * SFP 8 * GE (including 2 bypass pairs)
Wi-Fi/ 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
Available Slots for Expansion Modules	N/A	N/A	N/A	1	N/A	1
Expansion Module Option	N/A	N/A	N/A	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN	N/A	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN
Twin-mode HA	N/A	N/A	N/A	Yes	N/A	Yes
Local Storage	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	60W, Single AC (default), Dual AC (optional)	60W, Single AC (default), Dual AC (optional)	60W, Single AC (default), Dual AC (optional)	60W, Single AC (default), Dual AC (optional)	60W, Single AC (default), Dual AC (optional)	150W, Single AC (default), Dual AC (optional)
Power Supply	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Weight	8.6 lb (3.9 kg)	8.6 lb (3.9 kg)	9 bl (4.1 kg)	10.0 lb (4.55 kg)	9 bl (4.1 kg)	10.0 lb (4.55 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	0°C~40°C	0°C~40°C	0°C~40°C	0°C~40°C
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

A2000 / A2600 Front Panel

A2000
A2600

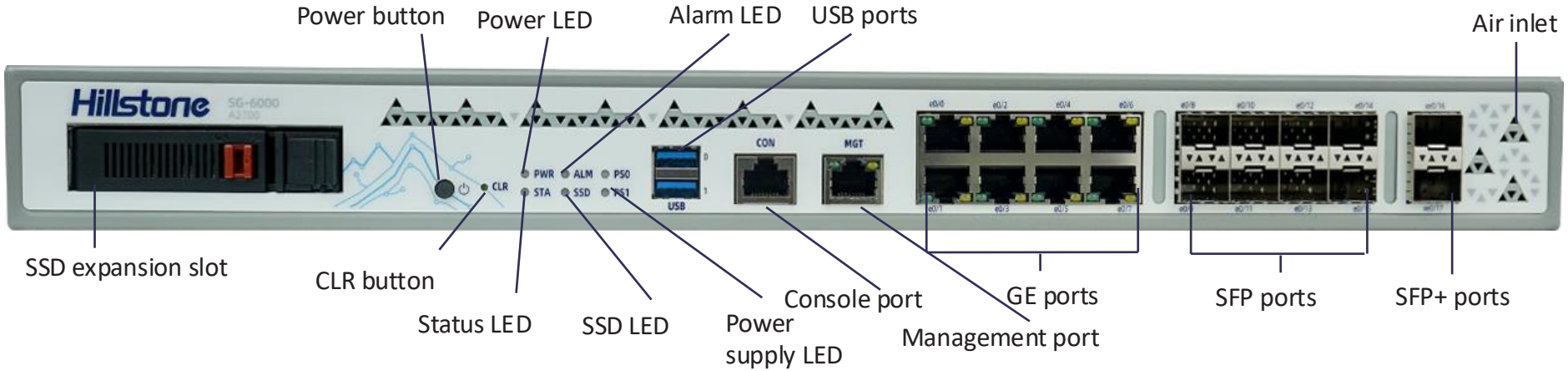


A2000 / A2600 Rear Panel

A2000
A2600

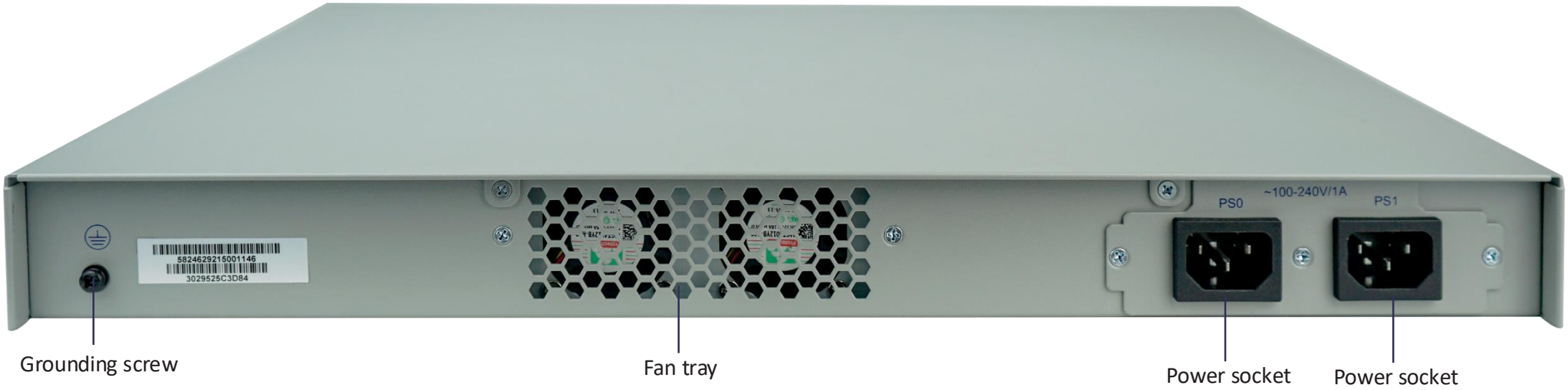
A2700 / A2800 Front Panel

A2700
A2800

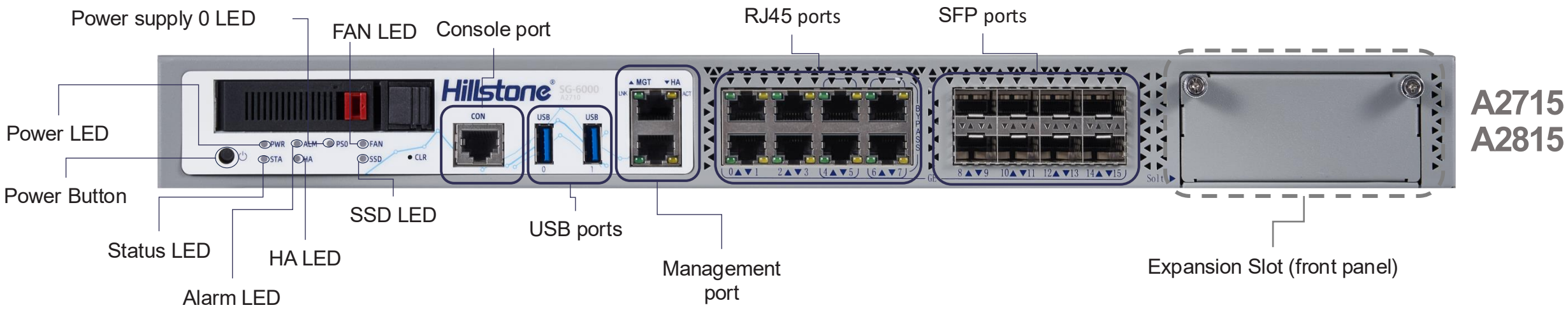


A2700 / A2800 Rear Panel

A2700
A2800

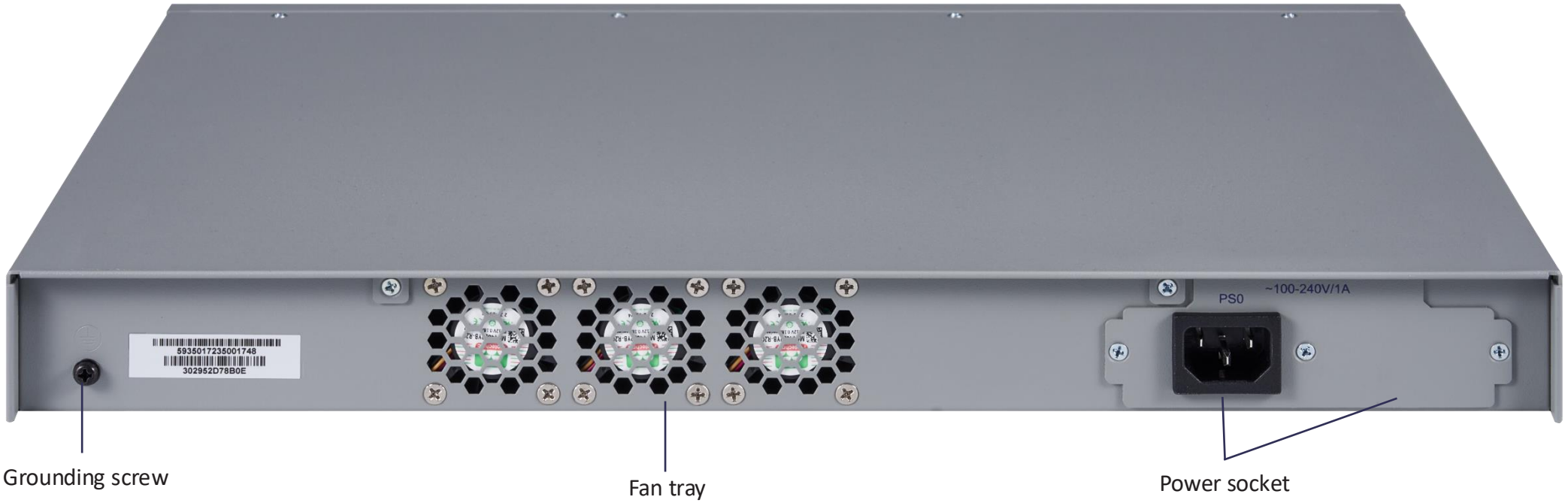


A2715 / A2815 Front Panel



A2715 / A2815 Rear Panel

A2715
A2815



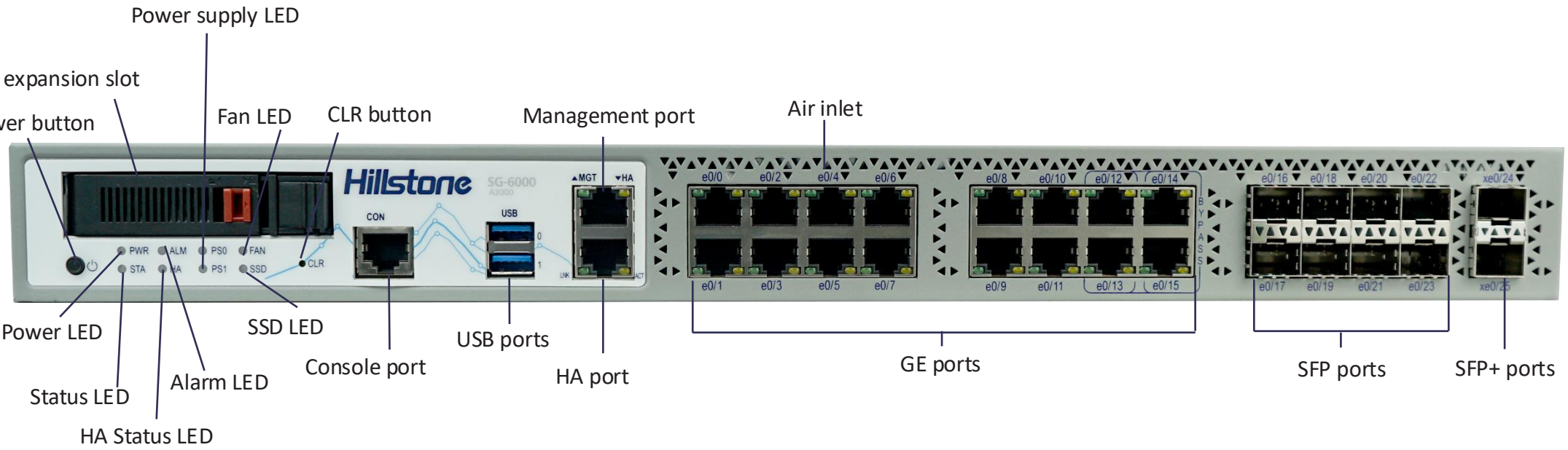
The Hillstone A-Series NGFW: Specifications

Hillstone NETWORKS

	Rackmount					
	SG-6000-A3000-IN	SG-6000-A3600-IN	SG-6000-A3615-IN	SG-6000-A3700-IN	SG-6000-A3800-IN	SG-6000-A3815-IN
Firewall Throughput	20 Gbps	20 Gbps	20 Gbps	20/30 Gbps	20/30 Gbps	20 Gbps
Maximum Concurrent Sessions	3 Million	4.5 Million	4.5 Million	7 Million	8 Million	8 Million
New Sessions/s	135,000	135,000	135,000	140,000	310,000	310,000
IPS Throughput	10 Gbps	10 Gbps	11 Gbps	11 Gbps	16 Gbps	14 Gbps
NGFW Throughput	5.5 Gbps	5.5 Gbps	6.5 Gbps	6.5 Gbps	12 Gbps	13 Gbps
Threat Protection Throughput	3 Gbps	3 Gbps	3 Gbps	3.1 Gbps	6 Gbps	6.5 Gbps
AV Throughput	5 Gbps	5 Gbps	6.5 Gbps	6.5 Gbps	12 Gbps	11 Gbps
IPsec VPN Throughput	6 Gbps	6 Gbps	6 Gbps	6 Gbps	12 Gbps	12 Gbps
Virtual Systems (Default/Max)	1/50	1/100	1/100	1/250	1/250	1/250
SSL VPN User Number	4,000	8,000	8,000	10,000	10,000	10,000
IPsec Tunnel Number	8,000	10,000	10,000	20,000	20,000	20,000
Management Ports	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA Port (RJ45)
Fixed I/O Ports	2 * SFP+, 8 * SFP, 16 * GE (including 2 bypass pairs)	2 * SFP+, 8 * SFP, 16 * GE (including 2 bypass pairs)	8 * SFP, 8 * GE (including 2 bypass pairs)	2 * SFP+, 8 * SFP, 16 * GE (including 2 bypass pairs)	2 * SFP+, 8 * SFP, 16 * GE (including 2 bypass pairs)	8 * SFP, 8 * GE (including 2 bypass pairs)
Wi-Fi/ 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
Available Slots for Expansion Modules	N/A	N/A	2	1	1	2
Expansion Module Option	N/A	N/A	IOC-A-F-4SFP+-IN, IOC-A-F-8SFP+-IN, IOC-A-F-8GE-IN, IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-F-4SFP+-IN, IOC-A-F-8SFP+-IN, IOC-A-F-8GE-IN, IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN
Twin-mode HA	Yes	Yes	Yes	Yes	Yes	Yes
Local Storage	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	150W, Single AC (default), Dual AC (optional)	150W, Single AC (default), Dual AC (optional)	150W, Single AC (default), Dual AC (optional)	150W, Single AC (default), Dual AC (optional)	550W, Dual AC (default), Dual DC (optional), hot swappable power	550W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz	AC 100-240 V, 50/60 Hz
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Weight	13.2 lb (6 kg)	13.2 lb (6 kg)	13.7 lb (6.2 kg)	13.4 lb (6.1 kg)	15 lb (6.8 kg)	19.8 lb (8.98 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

A3000 / A3600 / A3700 / A3800 Front Panel

A3000
A3600
A3700
A3800



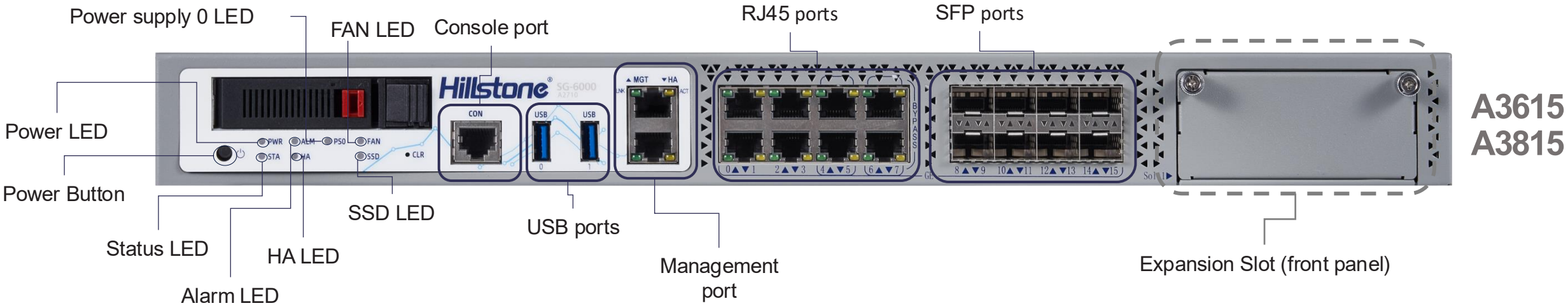
A3000 / A3600 / A3700 / A3800 Rear Panel

A3000
A3600

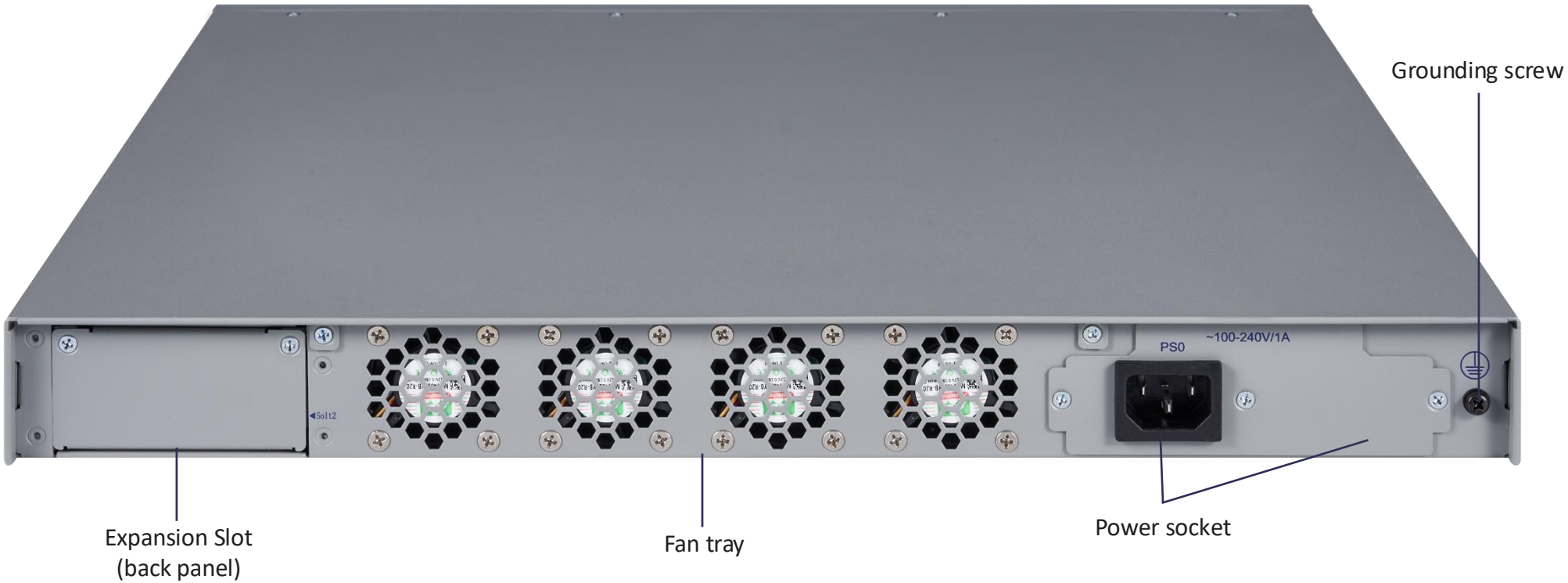
A3700

A3800

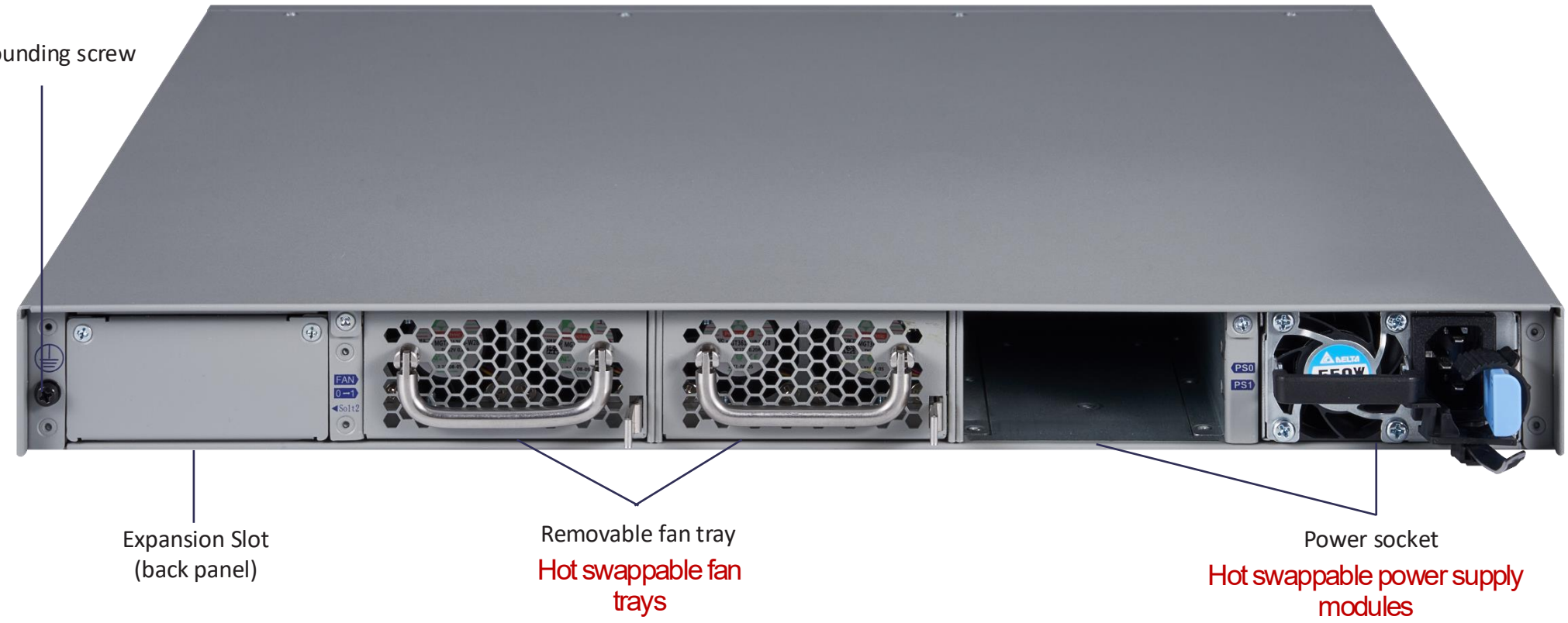
A3615 / A3815 Front Panel



A3615 Rear Panel



A3815 Rear Panel

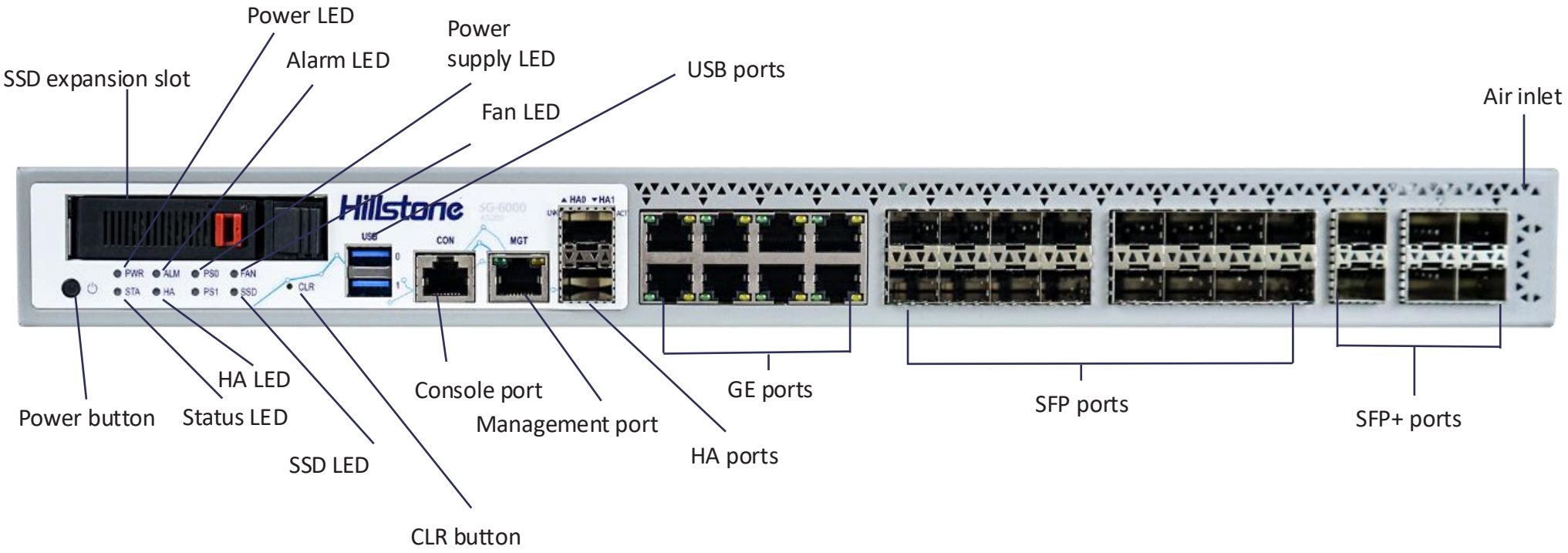


The Hillstone A-Series NGFW: Specifications

	Rackmount							
	SG-6000-A5100-IN	SG-6000-A5155-IN	SG-6000-A5200-IN	SG-6000-A5255-IN	SG-6000-A5500-IN	SG-6000-A5555-IN	SG-6000-A5600-IN	SG-6000-A5800-IN
Firewall Throughput (without/with expansion module)	25/50 Gbps	25/50 Gbps	32/65 Gbps	32/65 Gbps	40/80 Gbps	40/80 Gbps	60/85 Gbps	80/95 Gbps
Maximum Concurrent Sessions	9 Million	9 Million	15 Million	15 Million	18 Million	18 Million	25 Million	30 Million
New Sessions/s	480,000	490,000	600,000	650,000	700,000	700,000	900,000	1,000,000
IPS Throughput	20/30 Gbps	21/30 Gbps	25/35 Gbps	27/40 Gbps	35/45 Gbps	35/50 Gbps	45/65 Gbps	50 Gbps
NGFW Throughput	20 Gbps	20 Gbps	25 Gbps	25 Gbps	30 Gbps	30 Gbps	40 Gbps	50 Gbps
Threat Protection Throughput	12 Gbps	12 Gbps	14 Gbps	15 Gbps	17 Gbps	17 Gbps	25 Gbps	25 Gbps
AV Throughput	15 Gbps	15 Gbps	20 Gbps	25 Gbps	30 Gbps	29 Gbps	35 Gbps	35 Gbps
IPsec VPN Throughput	15 Gbps	18 Gbps	25 Gbps	25 Gbps	30 Gbps	30 Gbps	40 Gbps	45 Gbps
Virtual Systems (Default/Max)	1/250	1/250	1/250	1/250	1/250	1/250	1/500	1/500
SSL VPN User Number	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000
IPsec Tunnel Number	20,000	20,000	20,000	20,000	20,000	20,000	20,000	20,000
Management Ports	1 * Console Port, 2 * USB3.0 Ports, 2 * HA Ports (SFP+), 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * HA port (SFP), 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 2 * HA Ports (SFP+), 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * HA port (SFP), 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 2 * HA Ports (SFP+), 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * HA port (SFP), 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * HA Port (SFP), 1 * MGT Port (RJ45)	1 * Console Port, 2 * USB3.0 Ports, 1 * HA Port (SFP), 1 * MGT Port (RJ45)
Fixed I/O Ports	6 * SFP+, 16 * SFP, 8 * GE (including 2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (including 4 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE (including 2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (including 4 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE (including 2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (including 4 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (including 4 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (including 4 bypass pairs)
Wi-Fi/ 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle
Available Slots for Expansion Modules	1	1	1	1	1	1	1	1
Expansion Module Option	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN
Twin-mode HA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local Storage	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Weight	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

A5100 / A5200 / A5500 Front Panel

A5100
A5200
A5500



A5100 / A5200 / A5500 Rear Panel

A5100
A5200
A5500

Grounding screw

General expansion slot

Removable fan tray

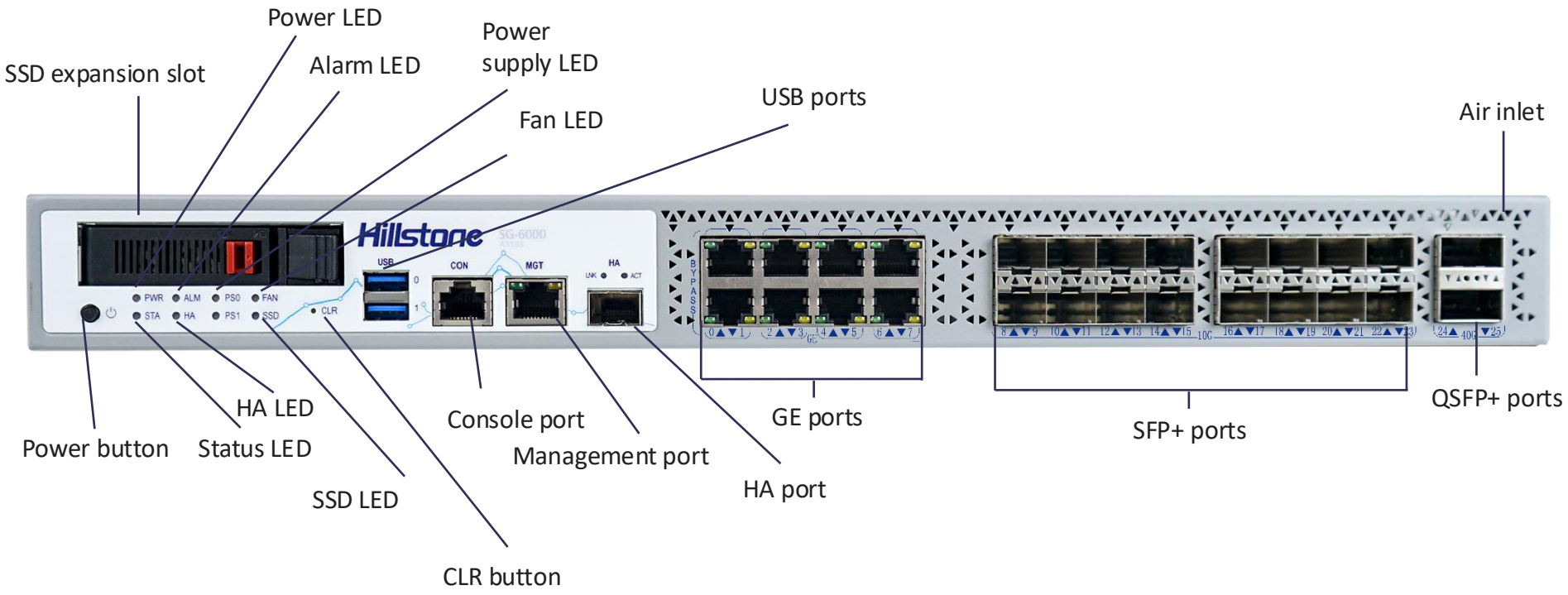
Hot swappable fan trays

Power socket

Hot swappable power supply modules

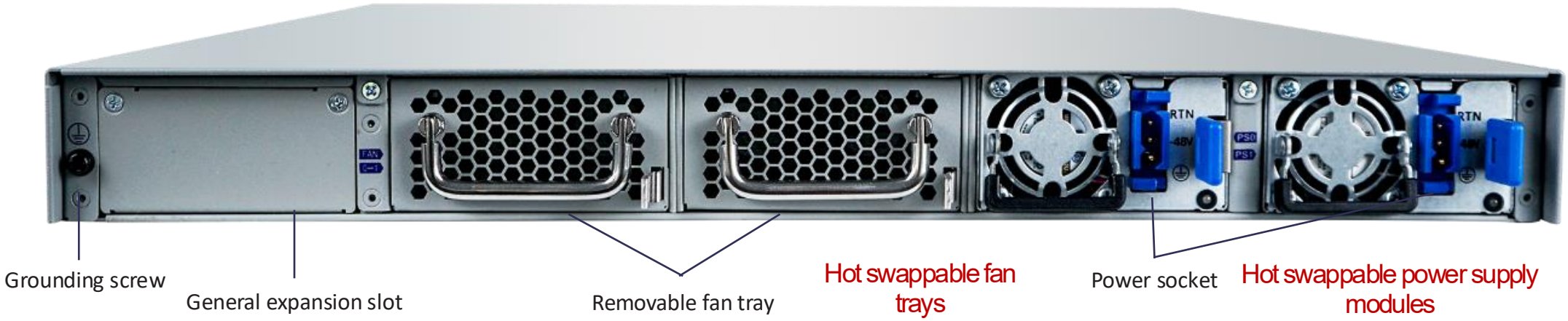
A5155 / A5255 / A5555 / A5600 / A5800 Front Panel

A5155
A5255
A5555
A5600
A5800



A5155 / A5255 / A5555 / A5600 / A5800 Rear Panel

A5155
A5255
A5555
A5600
A5800

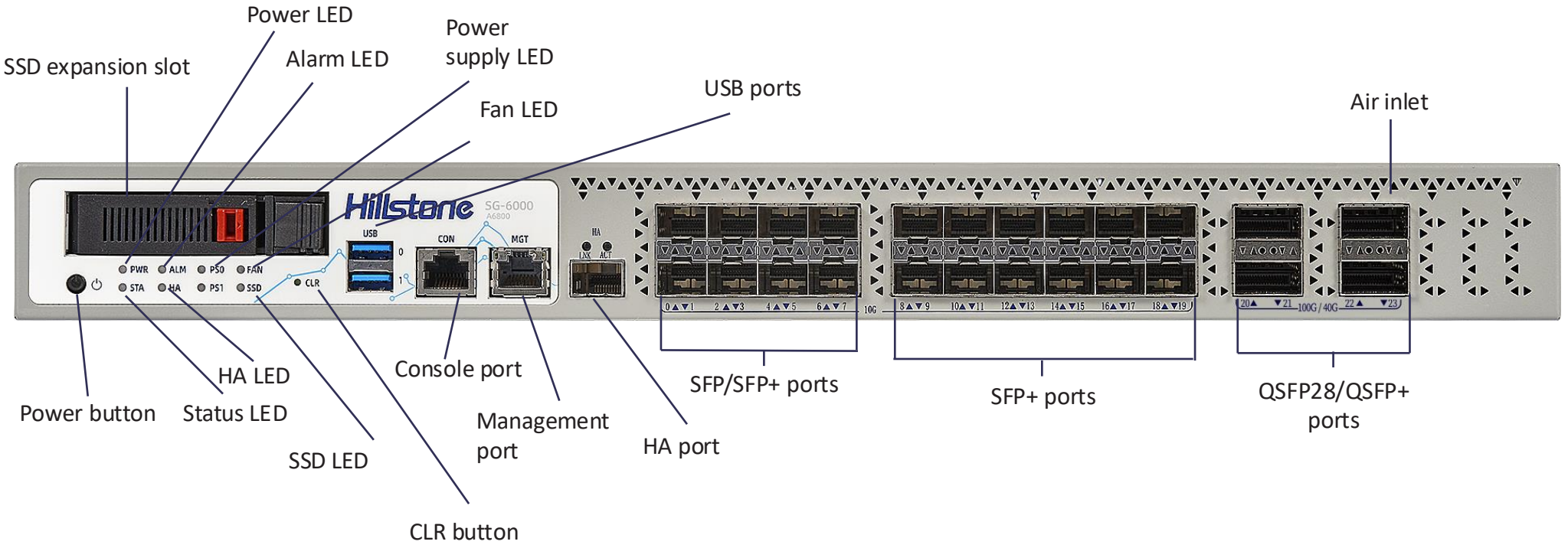


The Hillstone A-Series NGFW: Specifications

	Rackmount	
	SG-6000-A6800-IN	SG-6000-A7600-IN
Firewall Throughput (without/with expansion module)	200 Gbps	280/320 Gbps
Maximum Concurrent Sessions	35 Million	42 Million
New Sessions/s	900,000	900,000
IPS Throughput	80 Gbps	80 Gbps
NGFW Throughput	80 Gbps	80 Gbps
Threat Protection Throughput	30 Gbps	30 Gbps
AV Throughput	45 Gbps	45 Gbps
IPsec VPN Throughput	45 Gbps	45 Gbps
Virtual Systems (Default/Max)	1/500	1/500
SSL VPN User Number	10,000	10,000
IPsec Tunnel Number	20,000	20,000
Management Ports	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA port (SFP)	1 * Console Port, 2 * USB3.0 Ports, 1 * MGT Port (RJ45), 1 * HA port (SFP)
Fixed I/O Ports	4 * QSFP28 (or 2 * QSFP+, 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP	4 * QSFP28 (or 2 * QSFP+, 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP
Wi-Fi/ 4G Dongle	N/A	N/A
Available Slots for Expansion Modules	1	1
Expansion Module Option	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN
Twin-mode HA	Yes	Yes
Local Storage	64 GB	64 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	550W, Dual AC (default), Dual DC (optional)	550W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240 V, 50/60 Hz DC -36~-72 V	AC 100-240 V, 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U
Weight	20.3 lb (9.2 kg)	20.3 lb (9.2 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing

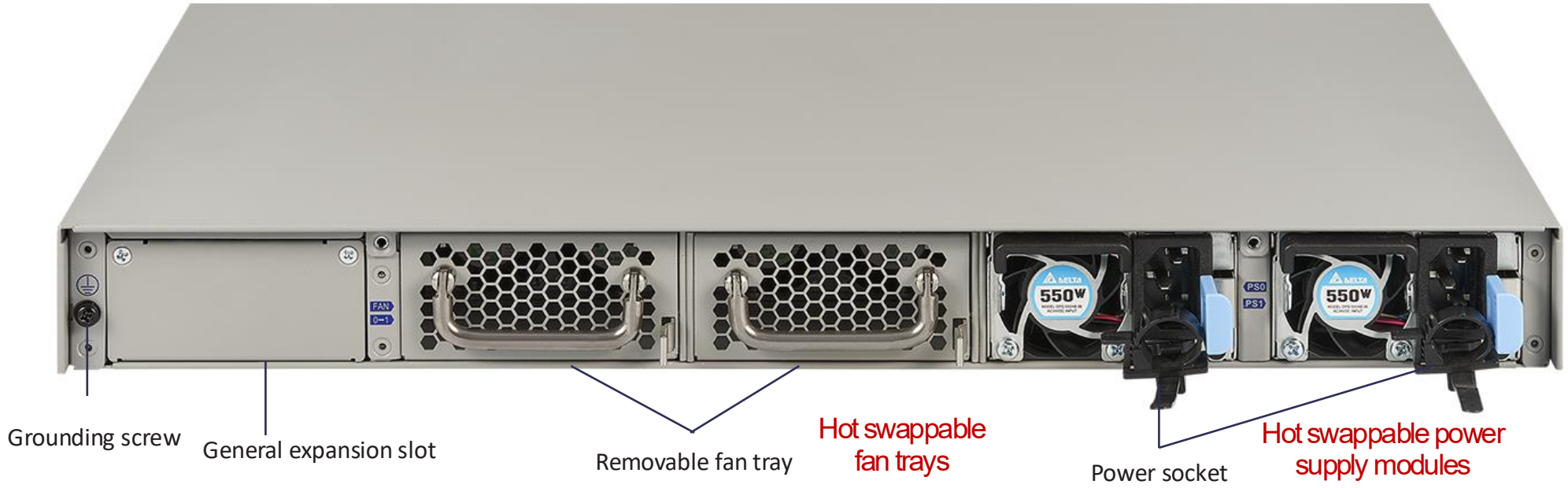
A6800 / A7600 Front Panel

A6800
A7600



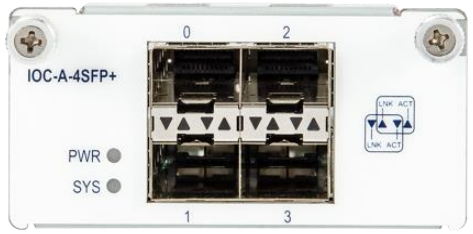
A6800 / A7600 Rear Panel

A6800
A7600



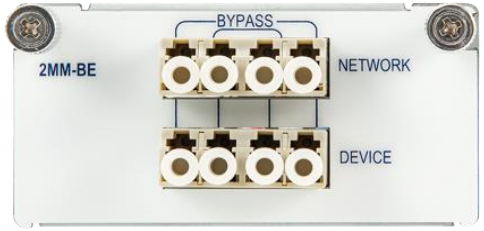
Expansion Modules

IOC-A-4SFP+-IN



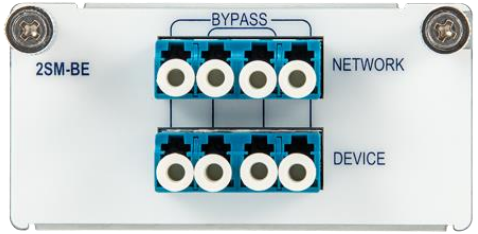
4SFP+ expansion module for rear panel (adaptive to SFP module)

IOC-A-2MM-BE-IN



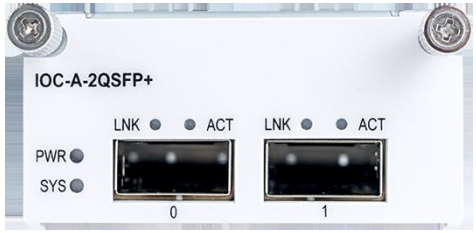
Multi-mode bypass expansion module for rear panel

IOC-A-2SM-BE-IN



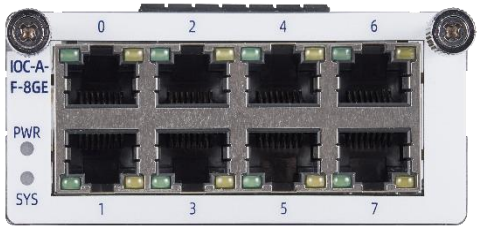
Single-mode bypass expansion module for rear panel

IOC-A-2QSFP+-IN



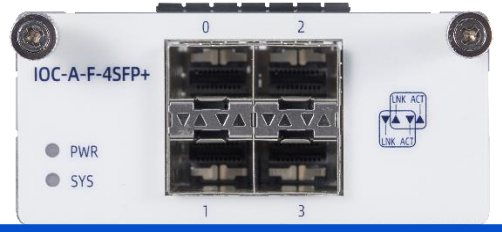
2QSFP+ expansion module for rear panel

IOC-A-F-8GE-IN



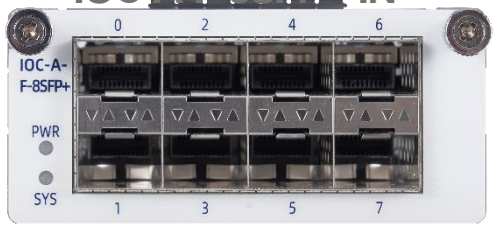
8GE (including 4 bypass pairs) expansion module for front panel

IOC-A-F-4SFP+-IN



4SFP+ expansion module for front panel

IOC-A-F-8SFP+-IN



8SFP+ expansion module for front panel

Expansion SSD: Images

256 GB SSD
For A1000, A1100

480 GB / 960 GB / 1.92 TB SSD
For A2000, A2600, A2700, A2715, A2800, A2815, A3000, A3600, A3615, A3700, A3800, A3815, A5100, A5155, A5200, A5255, A5500, A5555, A5600, A5800, A6800, A7600

Hillstone Network Detection and Response (NDR) Solution

Integrative Cybersecurity

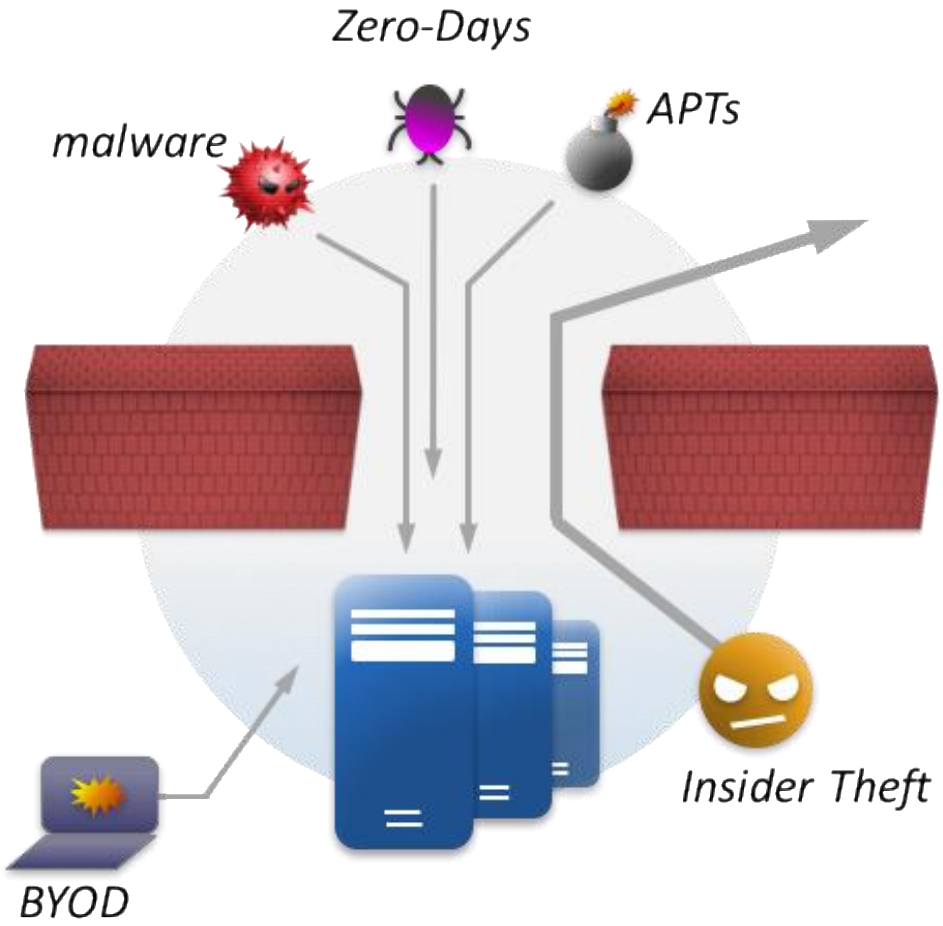
Visionary. AI-powered. Accessible.

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



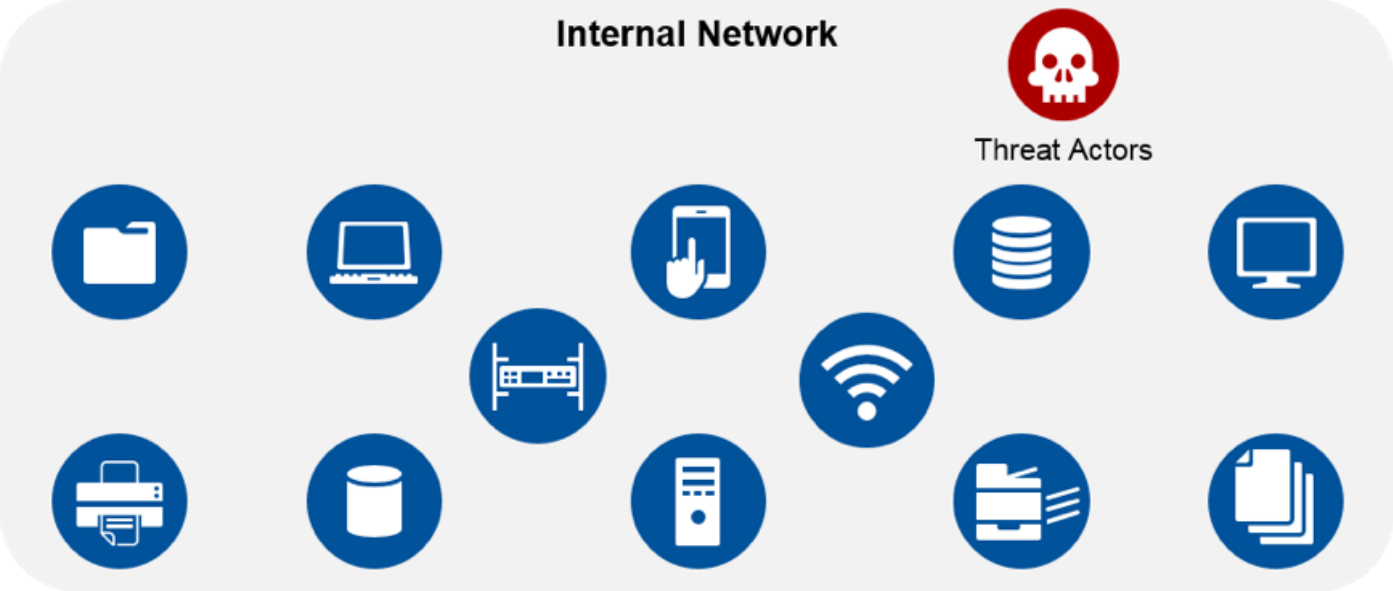
Traditional signature defenses can only stop old "**amateur**" attacks

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

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

– Verizon 2015 DBIR

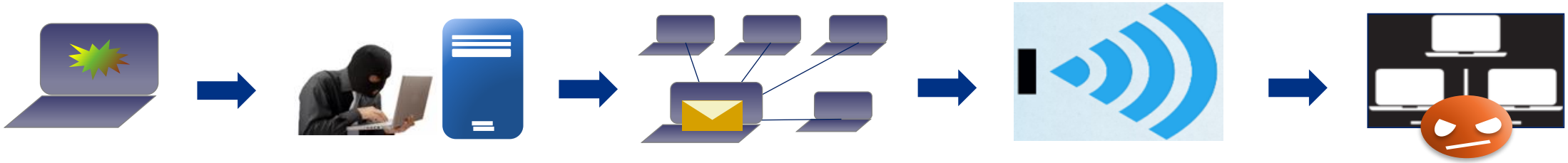
Threat Spreads Easily in Flat Internal Networks…



"…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"

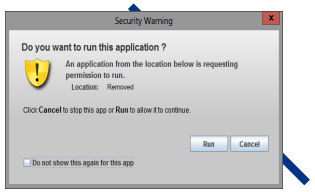
-Source: Gartner (September 2016)

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
…	…	…	…

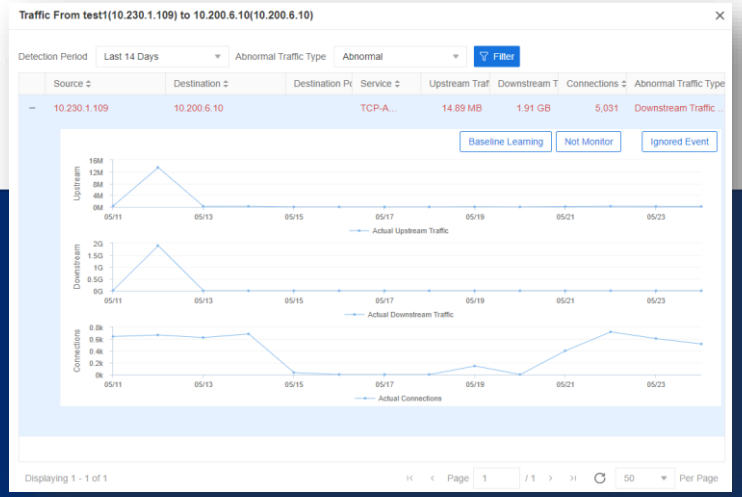
ML-based Analytics for Abnormal Behaviors

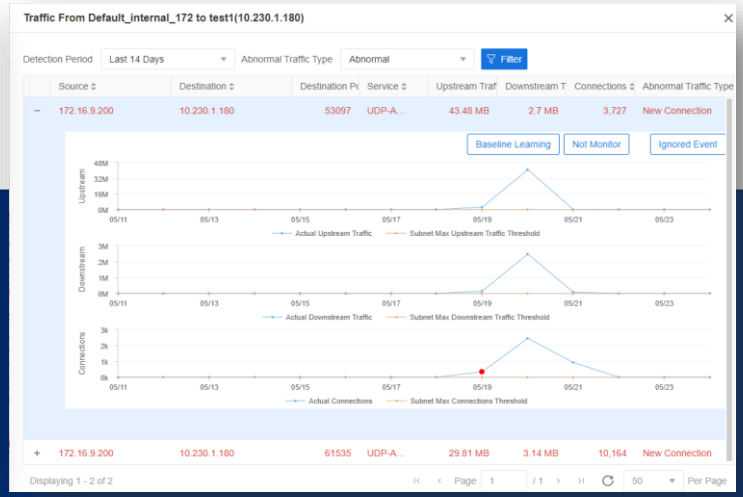
Learn and Establish Normal Traffic Baseline and Threshold

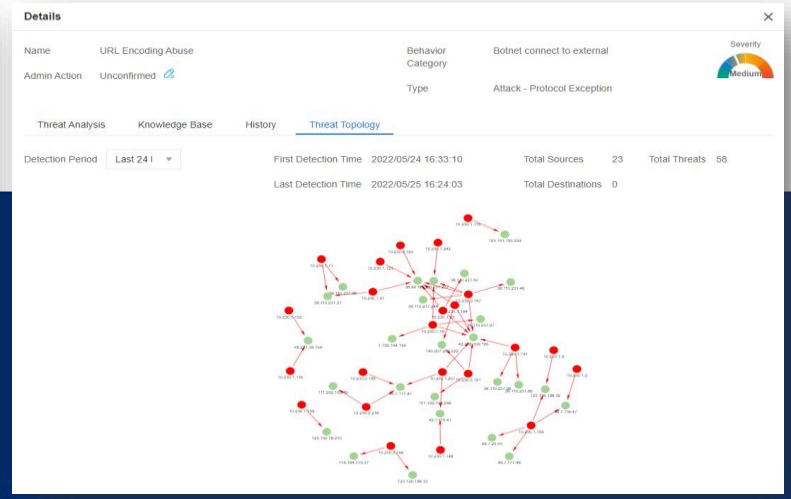
Detect Traffic Trend and Identify Abnormal Traffic Behaviors

Monitor Normal and Abnormal Traffic for each server/host

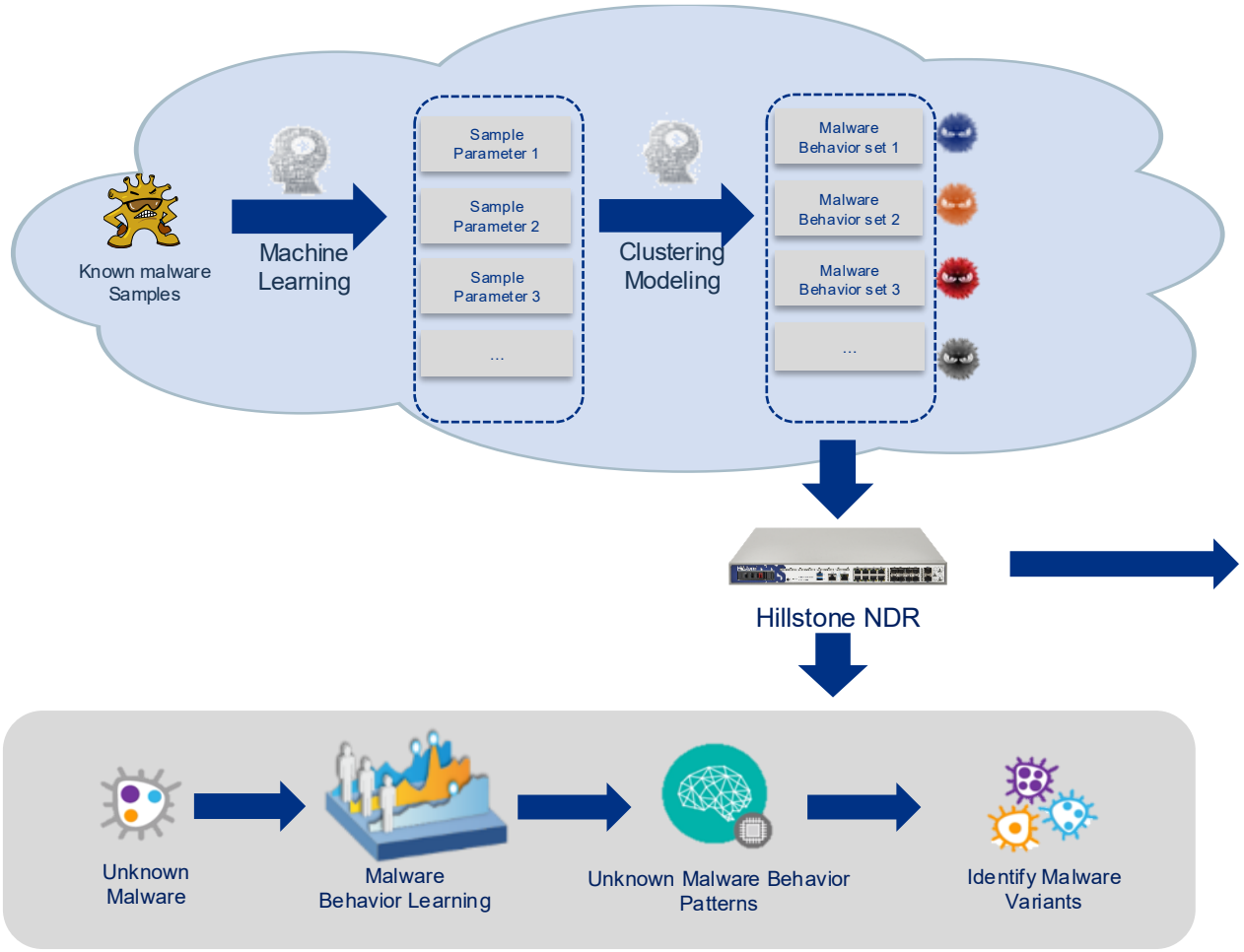
ML-based behavior analytics for URL, UEBA, threat correlations etc.







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

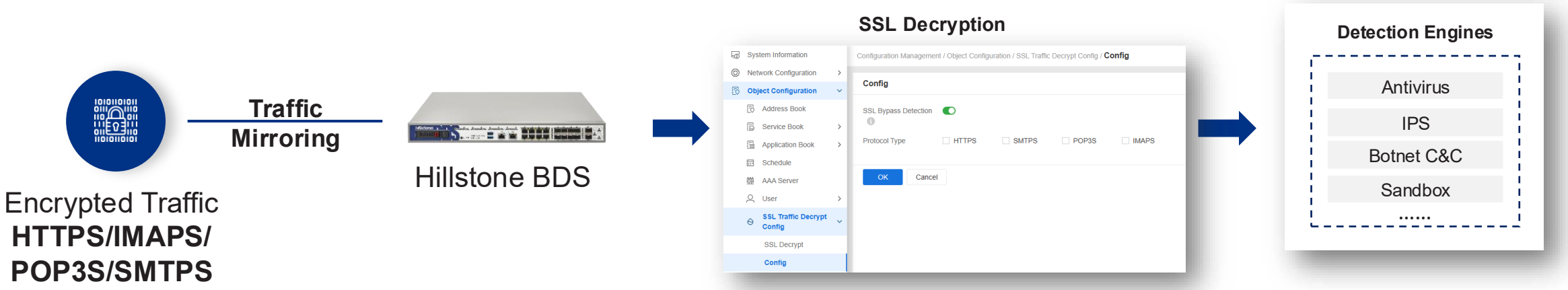
Logging Malicious Verdicts

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

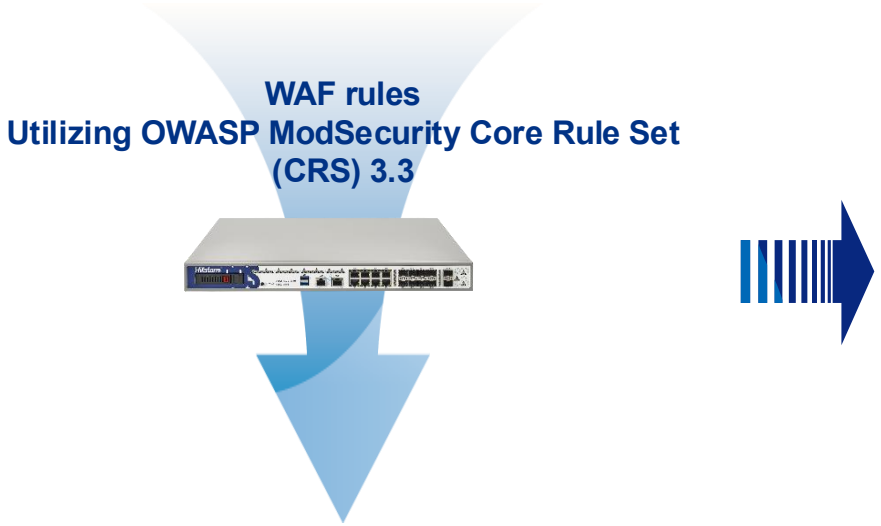
Leverage AI-powered technology to detect abnormal encrypted traffic without decryption

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

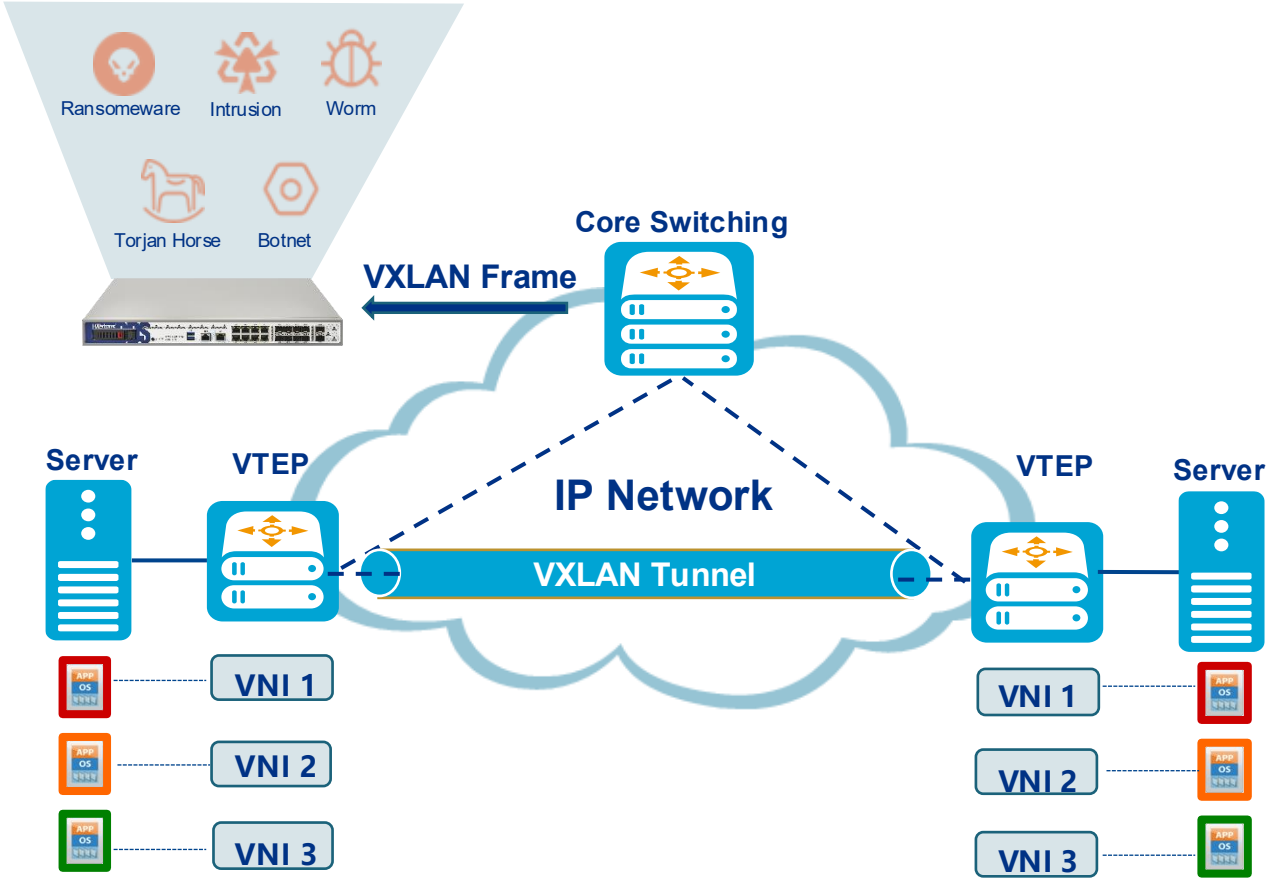


Detect and analyze threats for WEB servers and applications

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

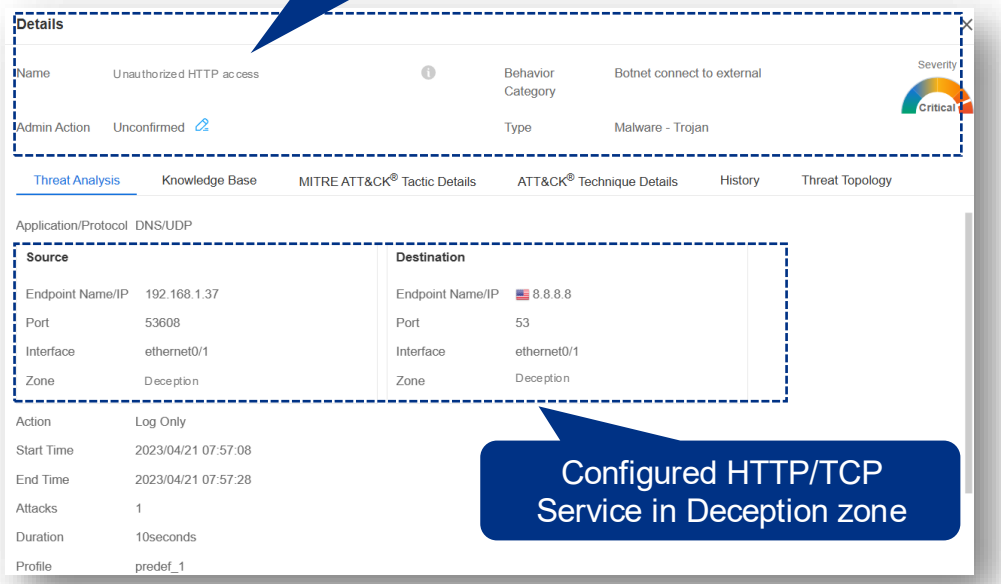


Detect VXLAN frame with UDP port 4789 as the destination port

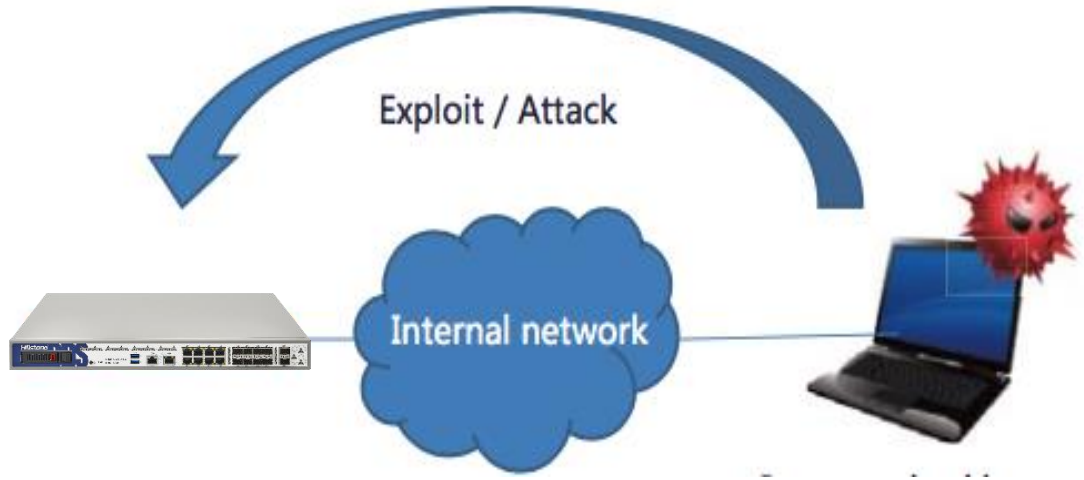
Do NOT detect non-VXLAN traffic whose destination port is UDP 4789

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

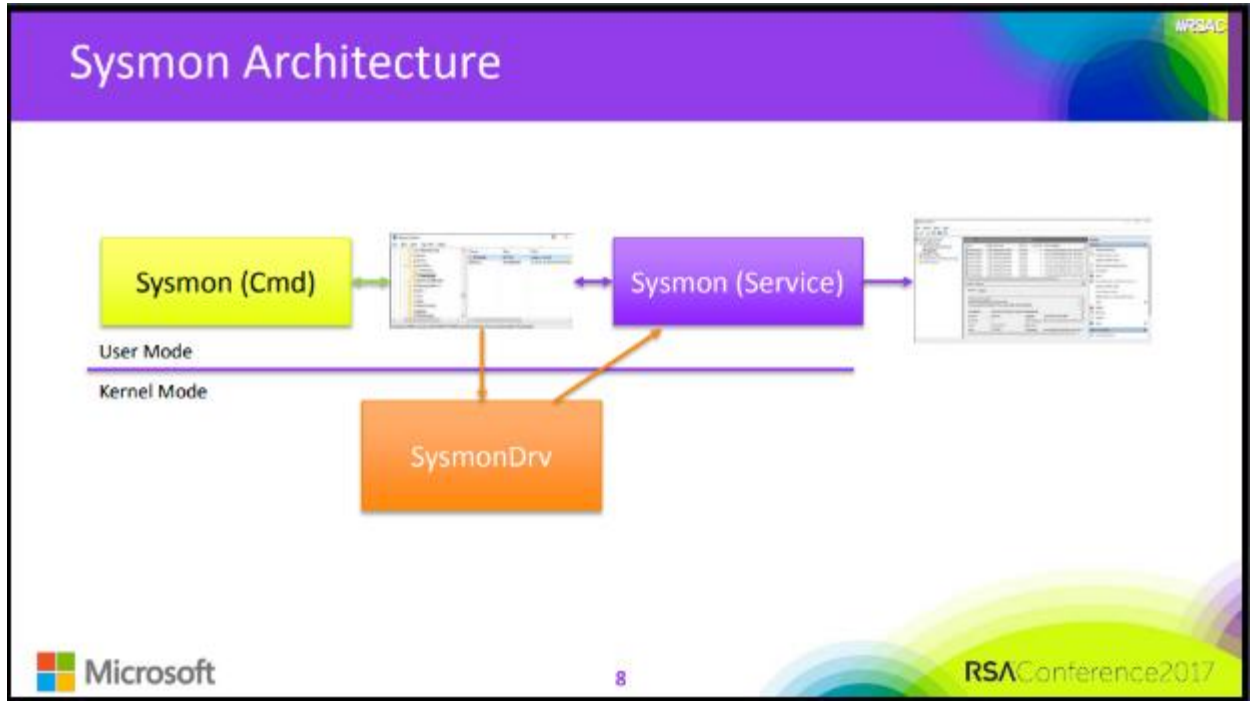
Hash-Based Detection

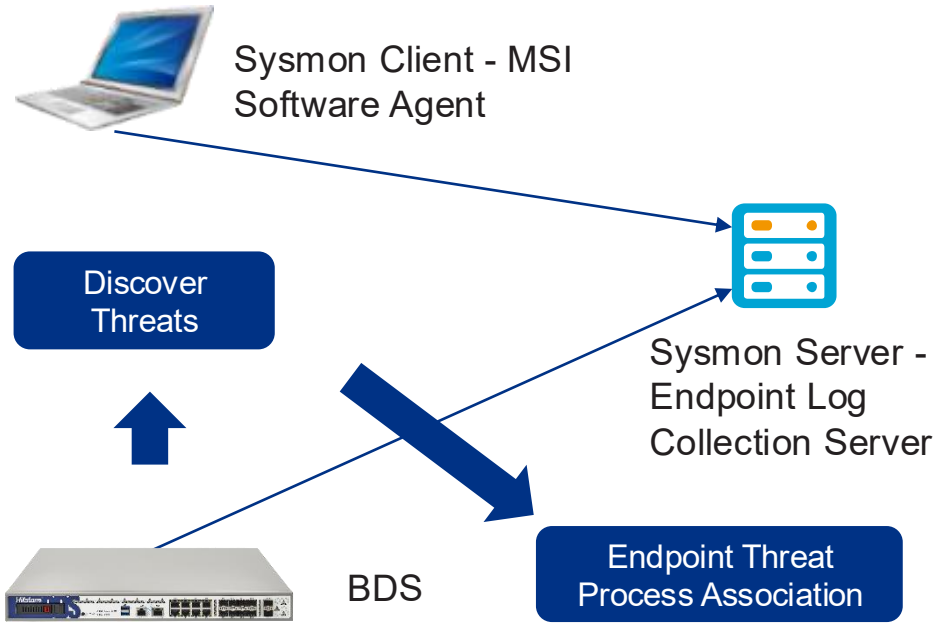
- MD5 file hash-based
- Support all files
- Use Case: Known virus detection

AI-Powered Detection

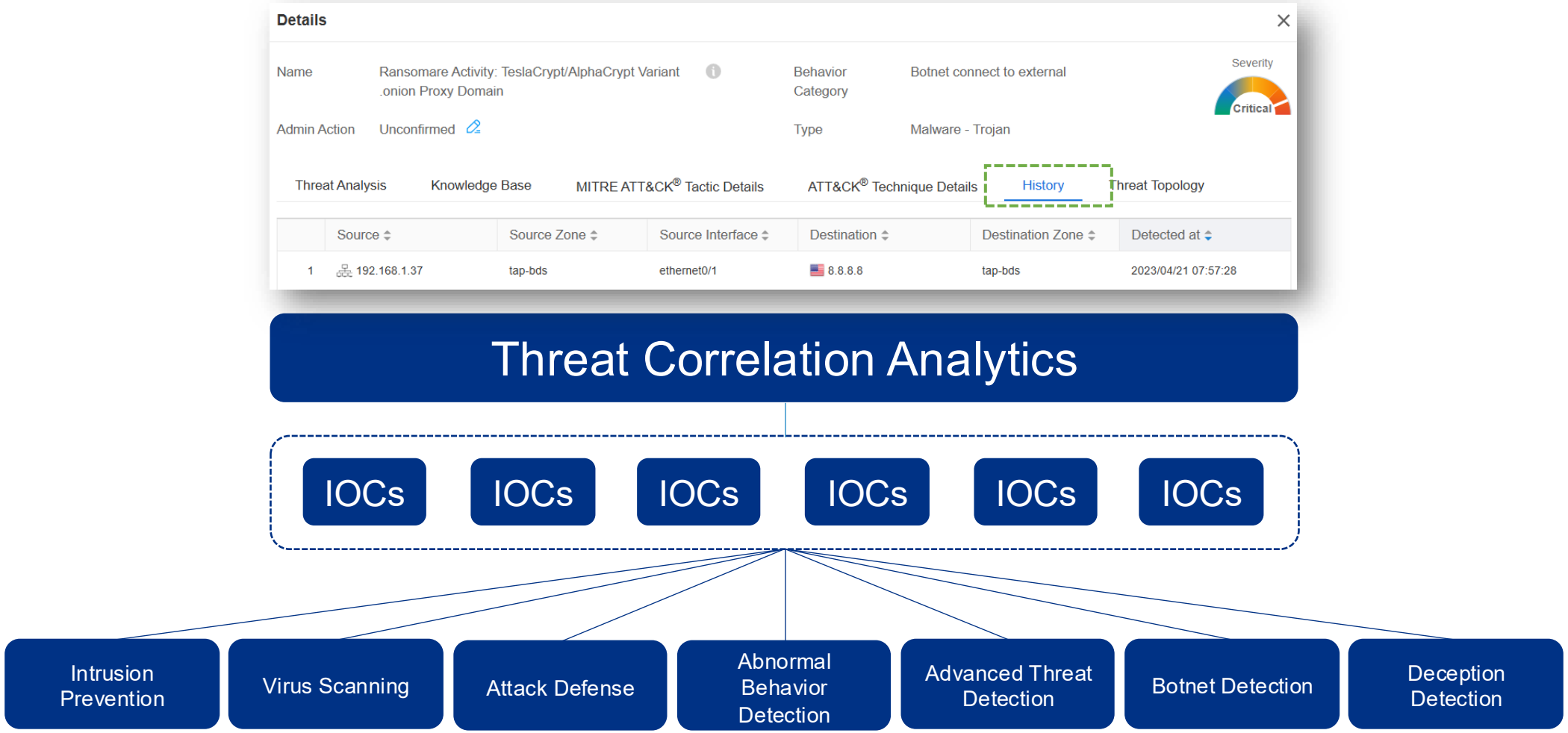
- File characteristics analysis
- Support PE/PDF/Office/ELF files
- Use Case: Unknown/variant viruses detection

Detection: Sysmon Endpoint Service Integration



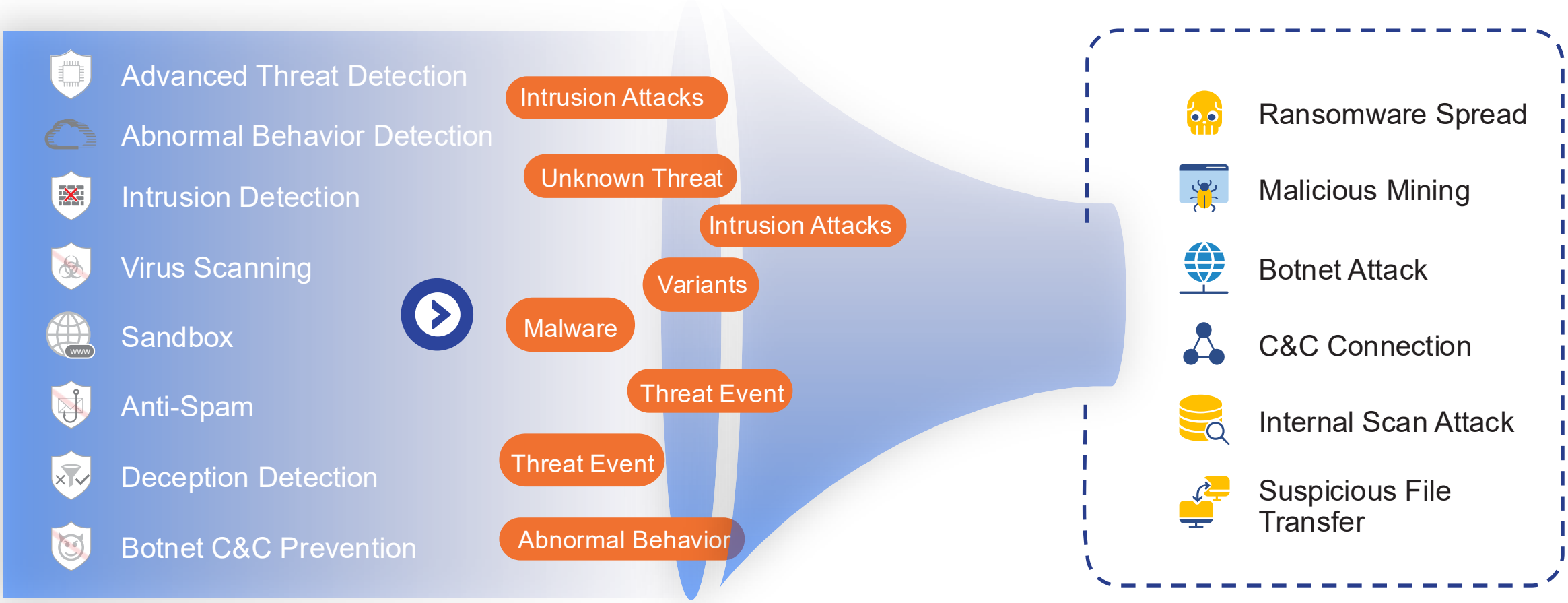


Detection: Detection Efficacy and Lower False Positive



Visibility: Indicator of Compromises (IOCs) Threats

Threat detection engines detect threat events	Threat correlation analysis	IOCs



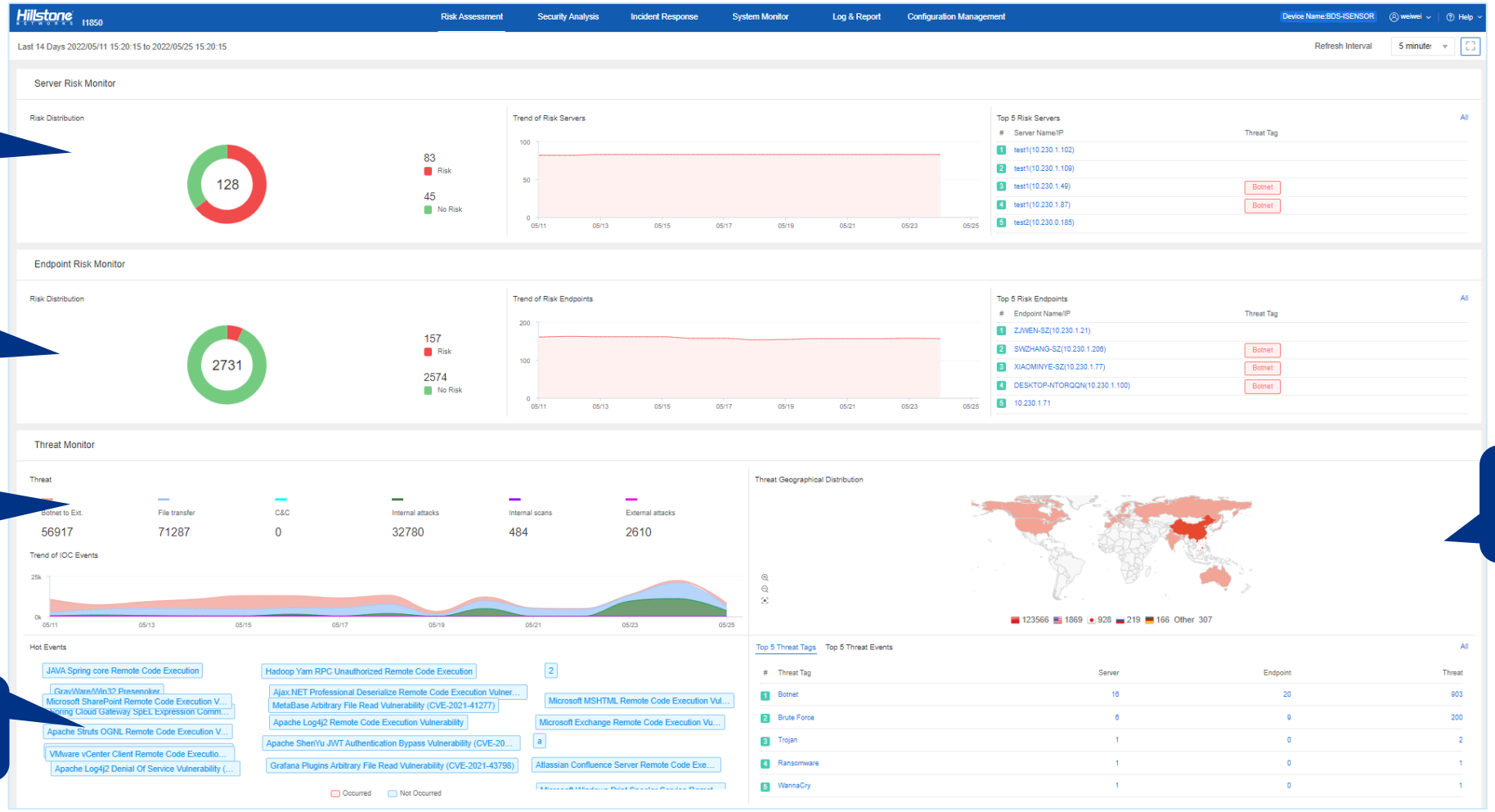
Visibility: Global View of Intranet Threat

Overview of Critical Servers and risk level

Overview of internal host and risk level

Threat type, statistic, historical distribution etc.

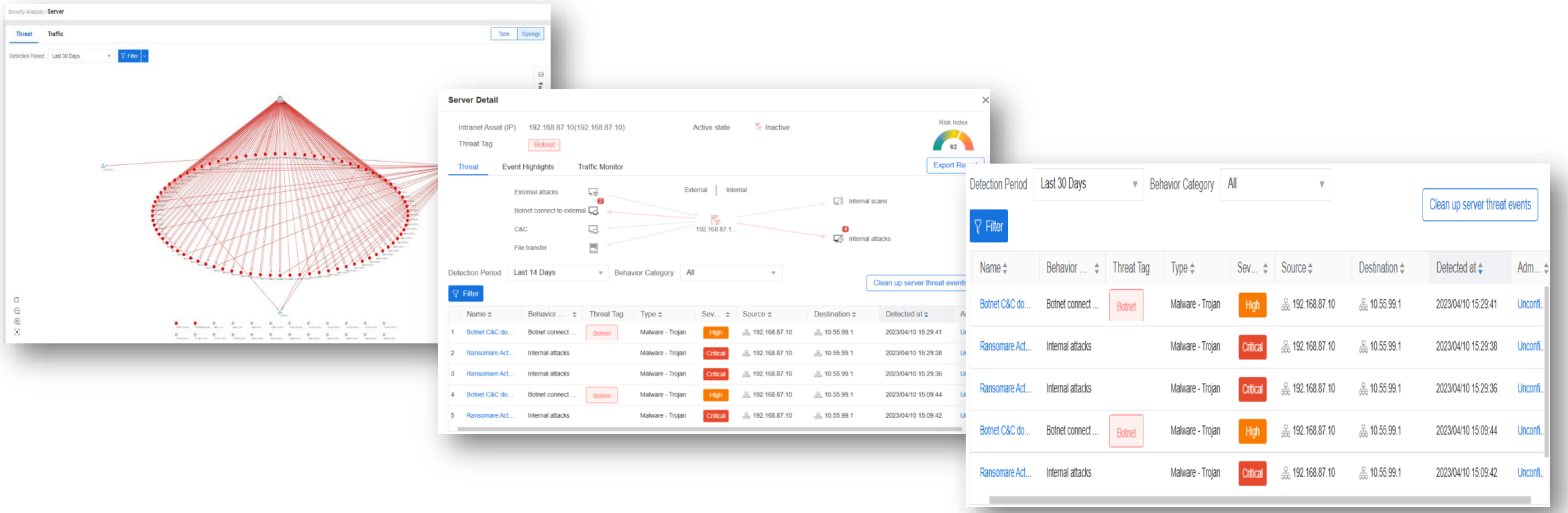
Hot events that need attention



Geo-location threat distribution and top threat

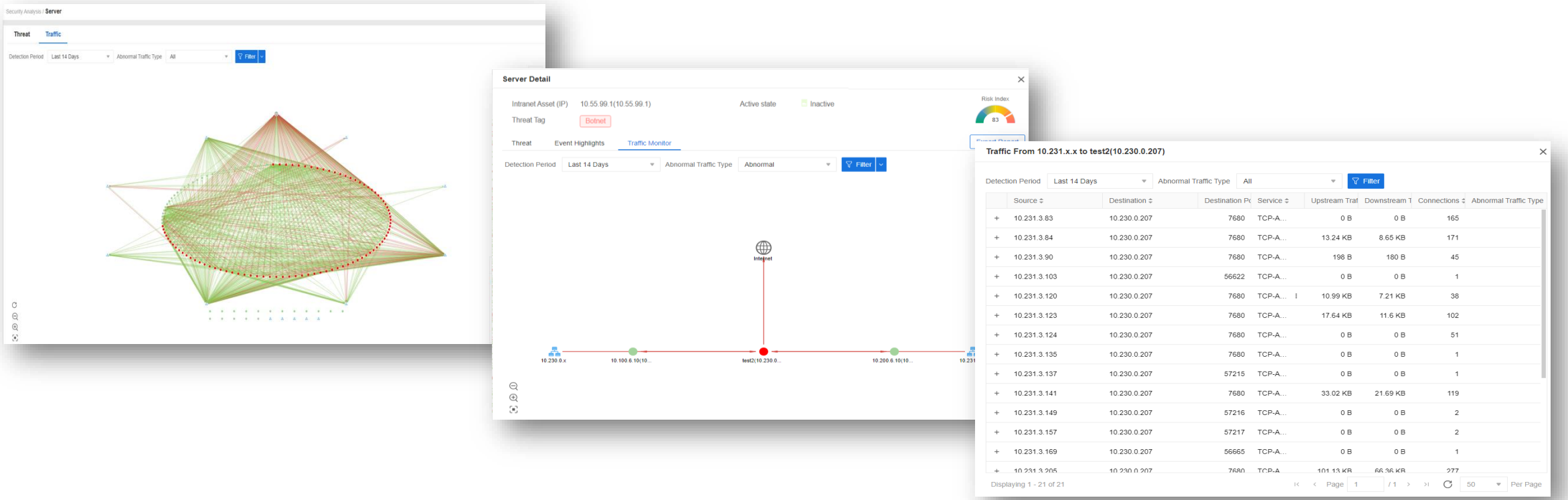
Visibility: Intranet Risk Monitoring Dashboard

Visibility: Server Threat Monitoring



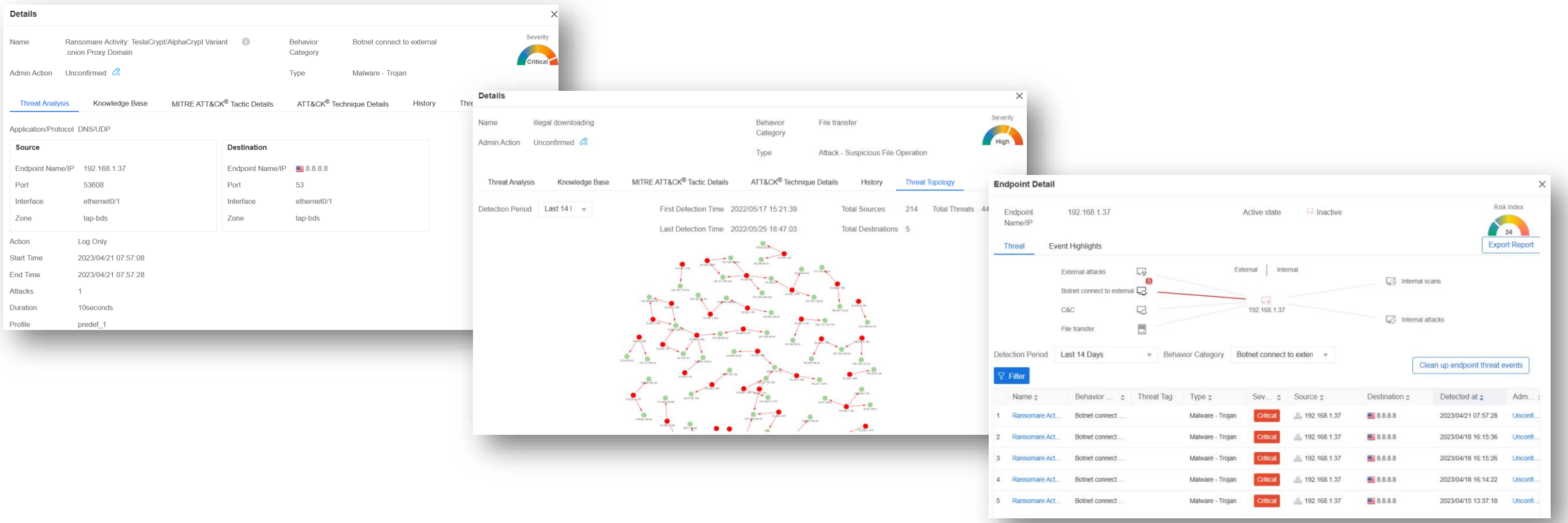
- Server threat topology for intranet servers: attack direction, severity, relationships
- Threat analysis for individual server: 6 types of attack chain
- Threat events list

Visibility: Server Traffic Monitoring



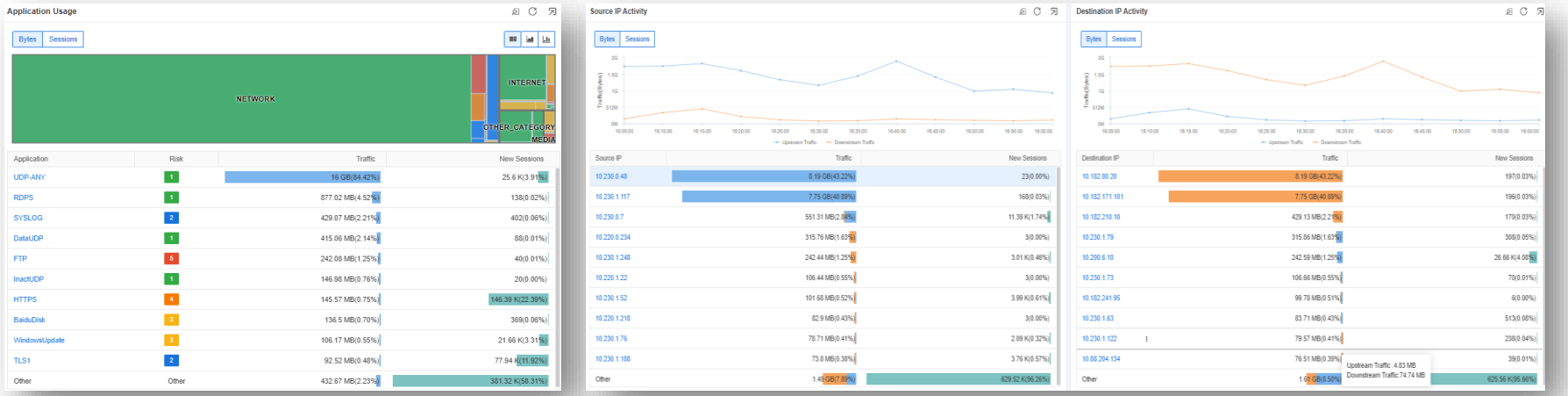
- Server traffic topology for all intranet servers: all traffic relations among all intranet servers
- Server traffic diagram for individual server: traffic in/out of an individual server
- Traffic activity list: all traffic activities between servers

Visibility: Threat Topology

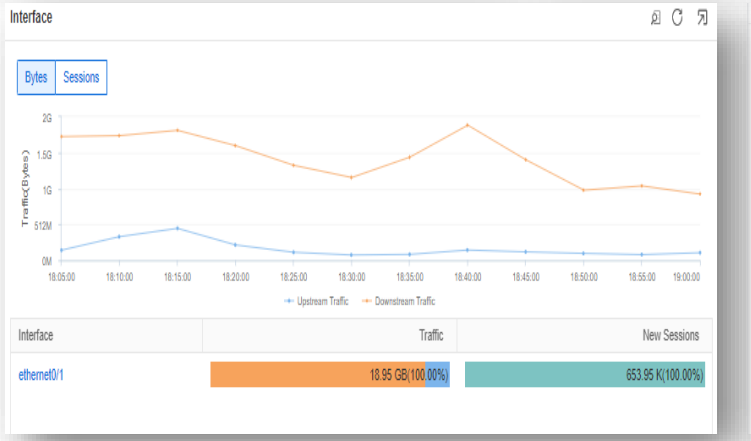


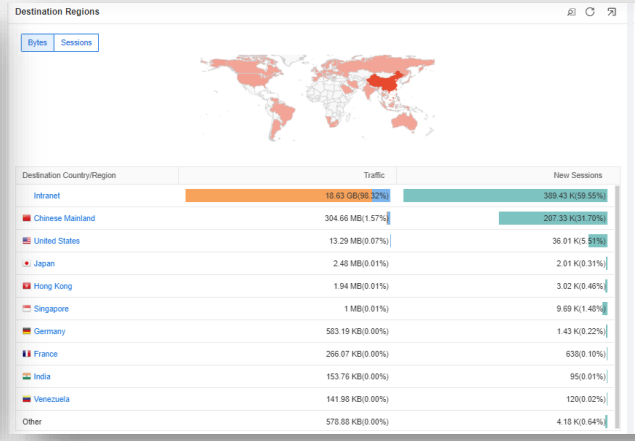
- Details of a threat
- Threat topology that shows the interactions between assets involved in this threat event
- View of the detailed activities of a specific IP in this threat topology

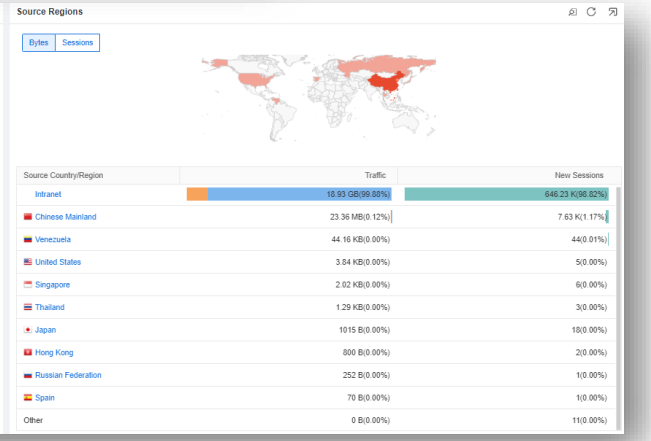
Visibility: Intranet Application Analysis



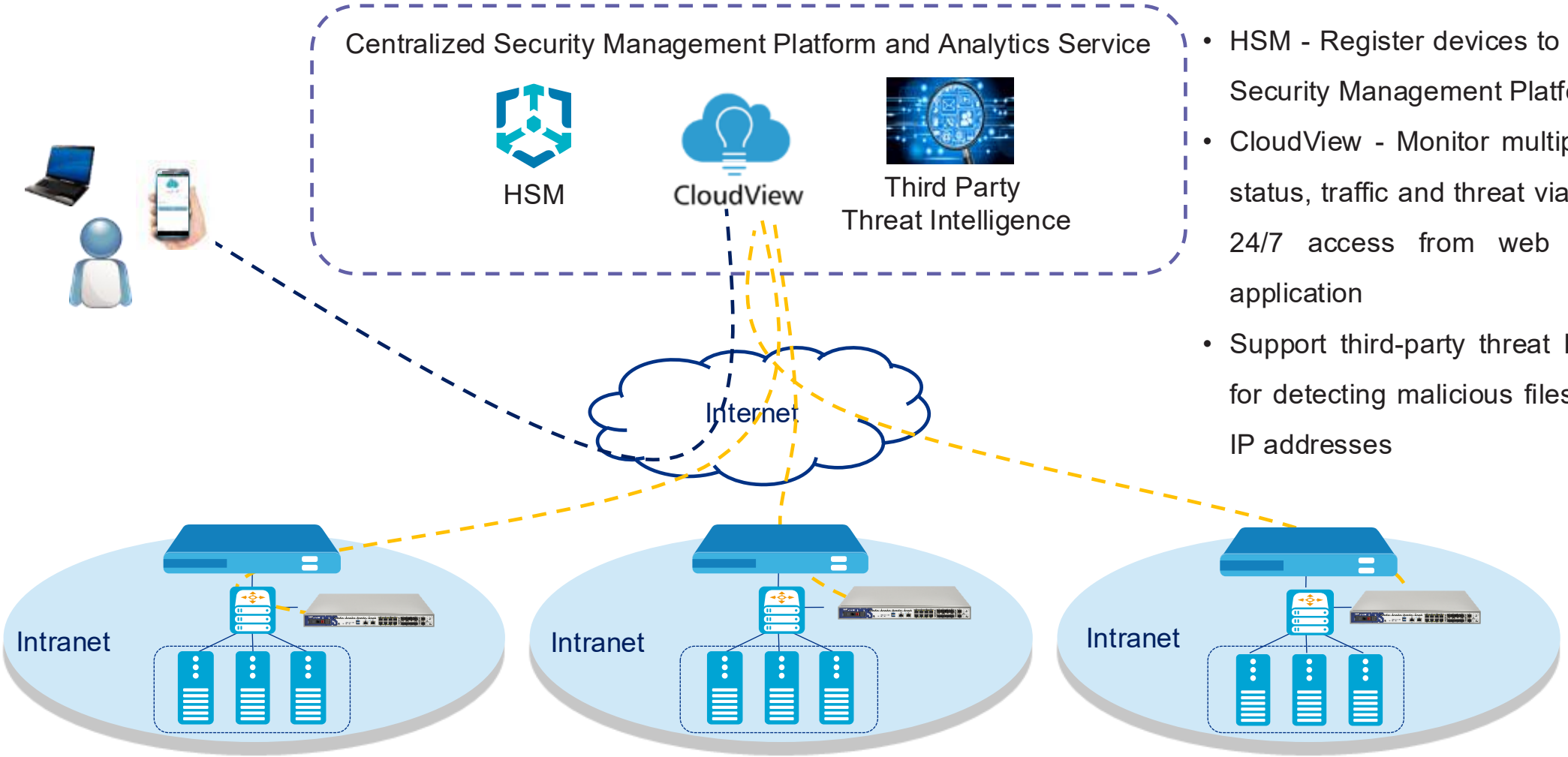
- Application Usage/Ranking
- Source/Destination IP traffic ranking
- Interface Traffic Ranking
- Threat Geo-location





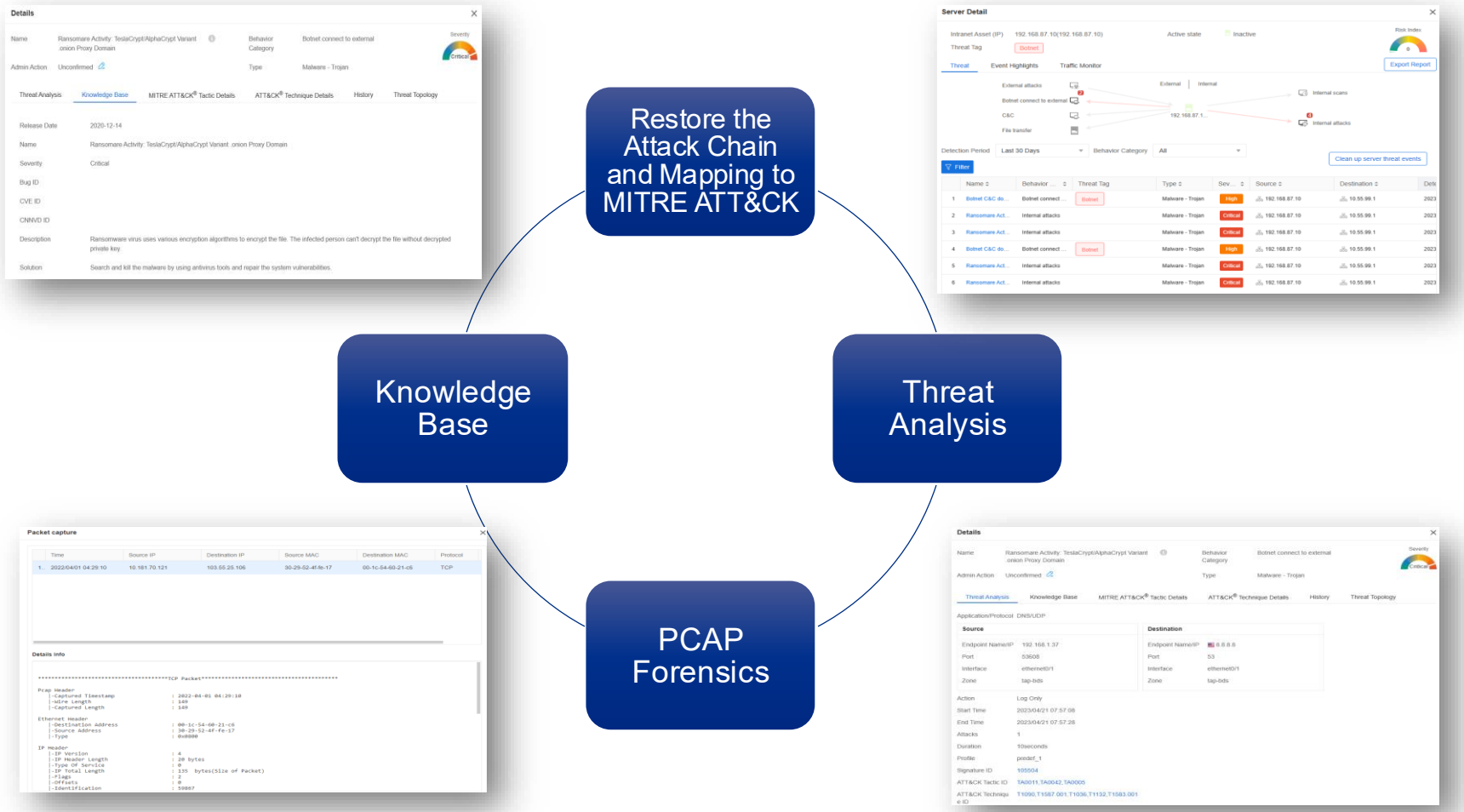


Visibility: Centralized Security Management



- 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

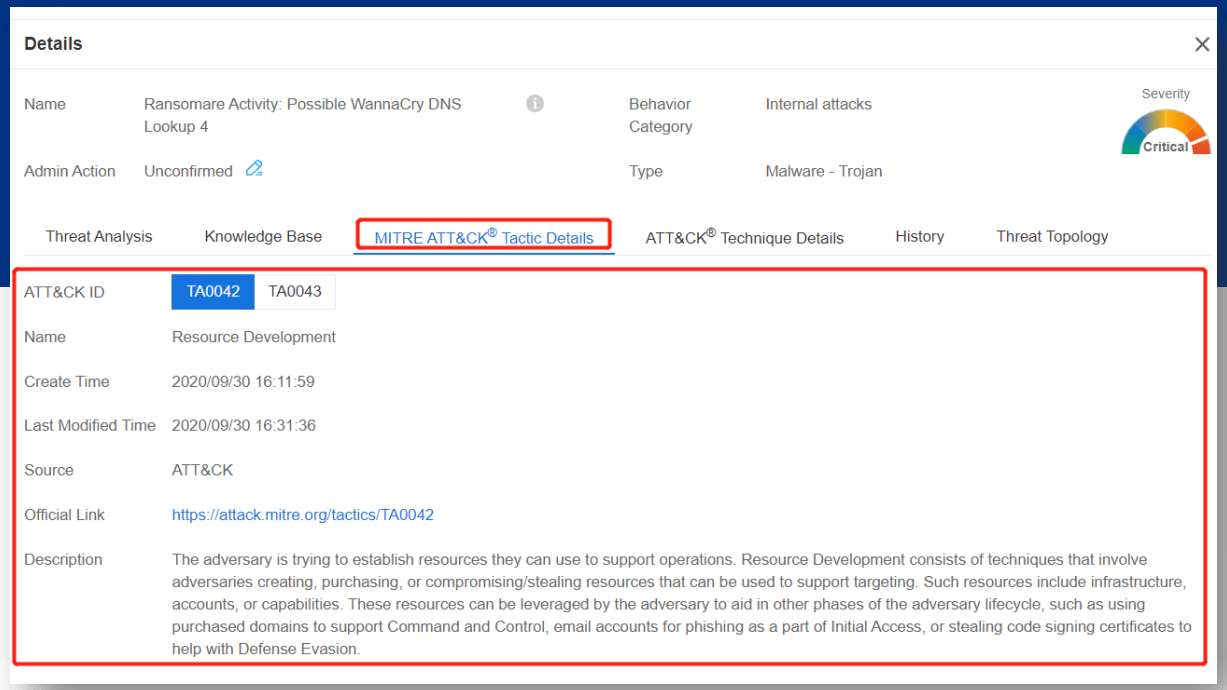
Digital Forensics Analysis: Rich Forensics Enables Risk Assessment



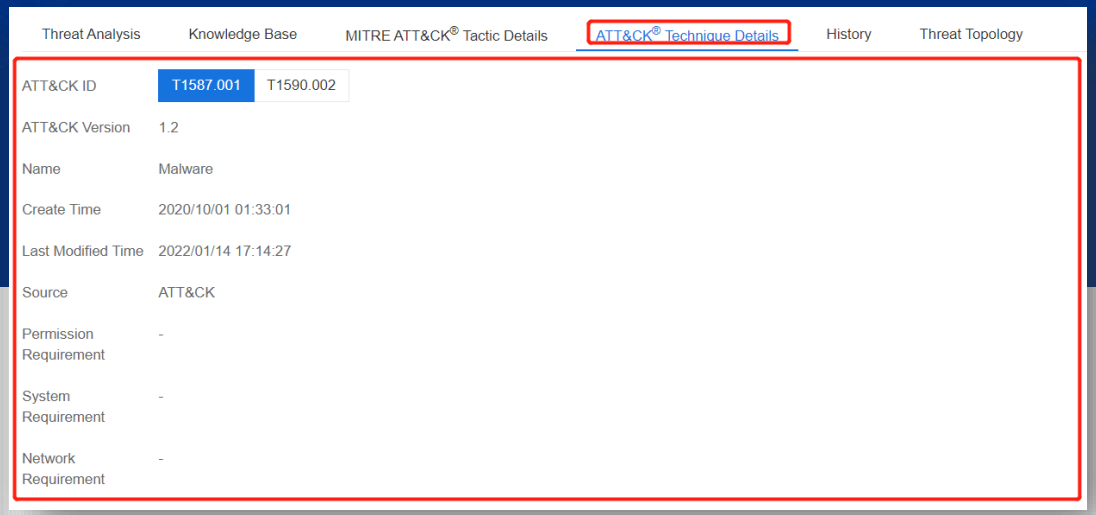
Digital Forensics Analysis: MITRE ATT&CK Framework Mapping

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.

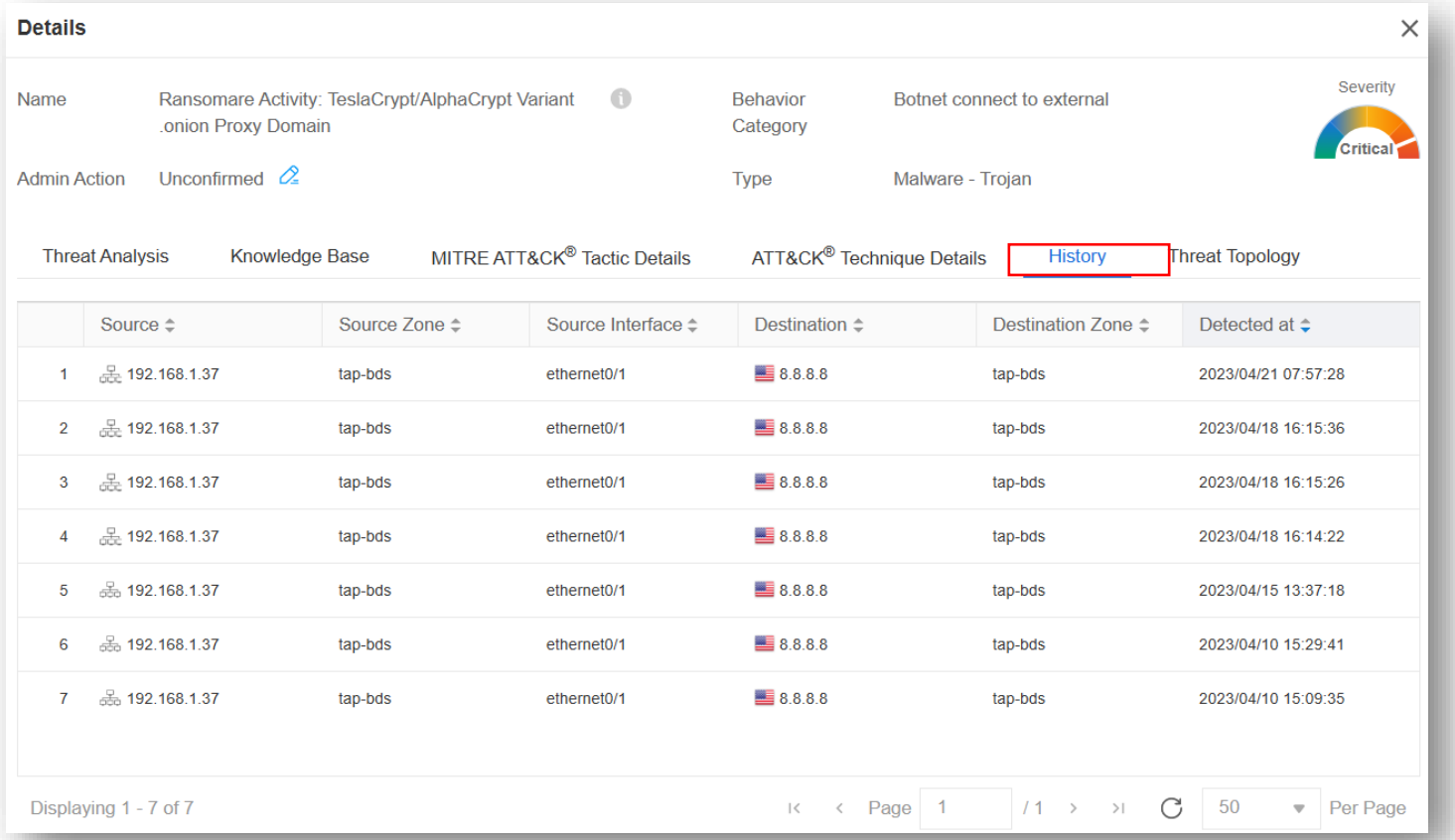


ATT&CK tactic details of threat events



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

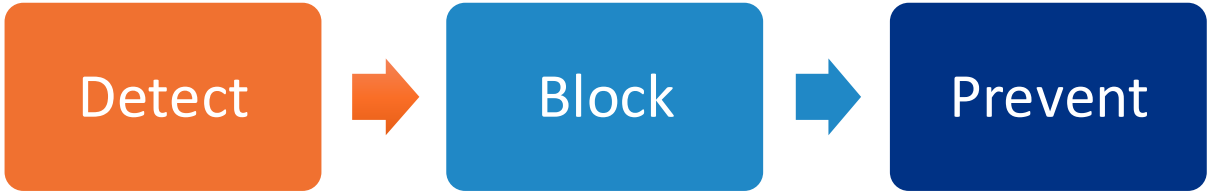
Response: Mitigate Attacks with Hillstone & Third-party Security Devices

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

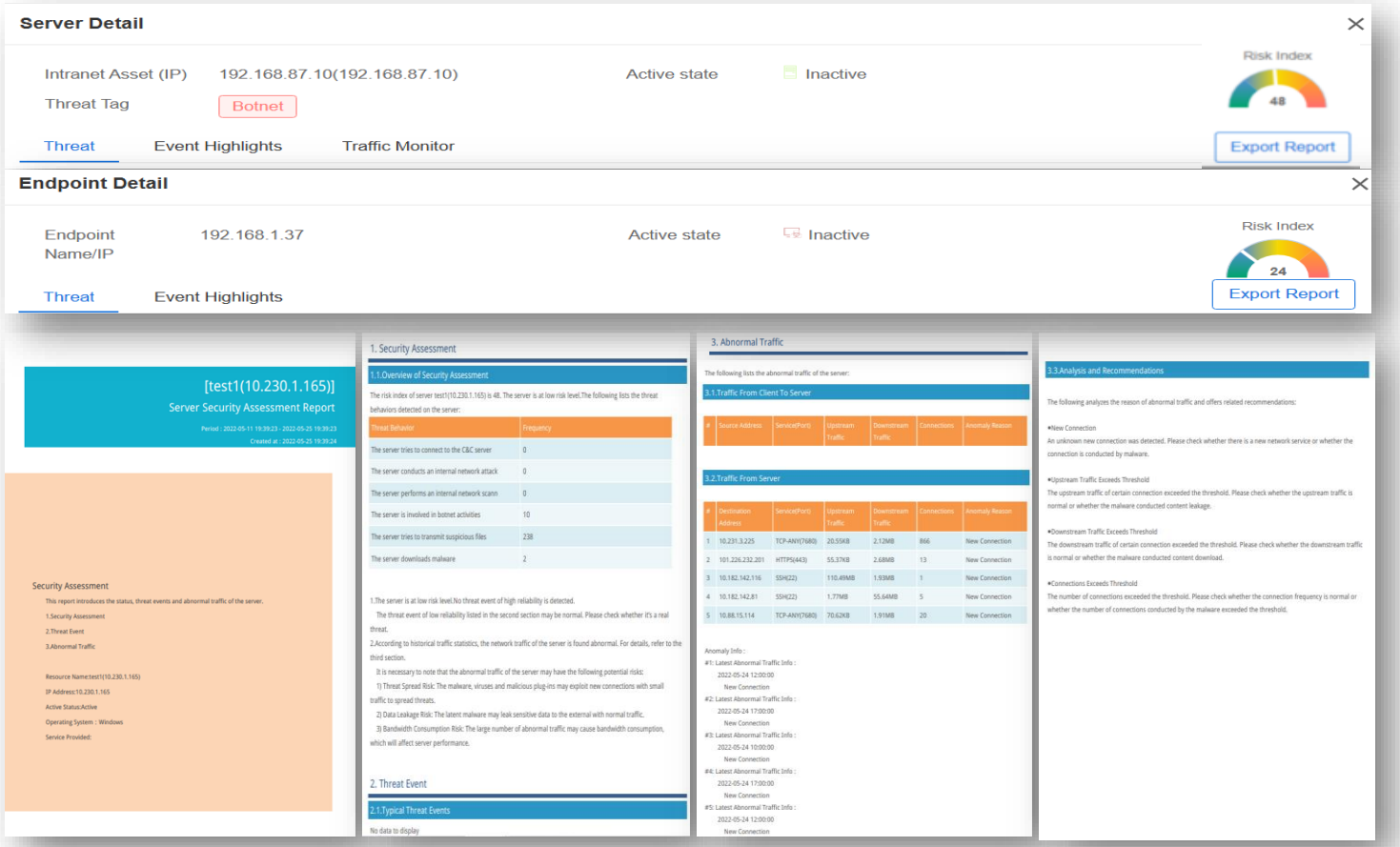
Response: Detect and Respond to Threats with Hillstone XDR

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

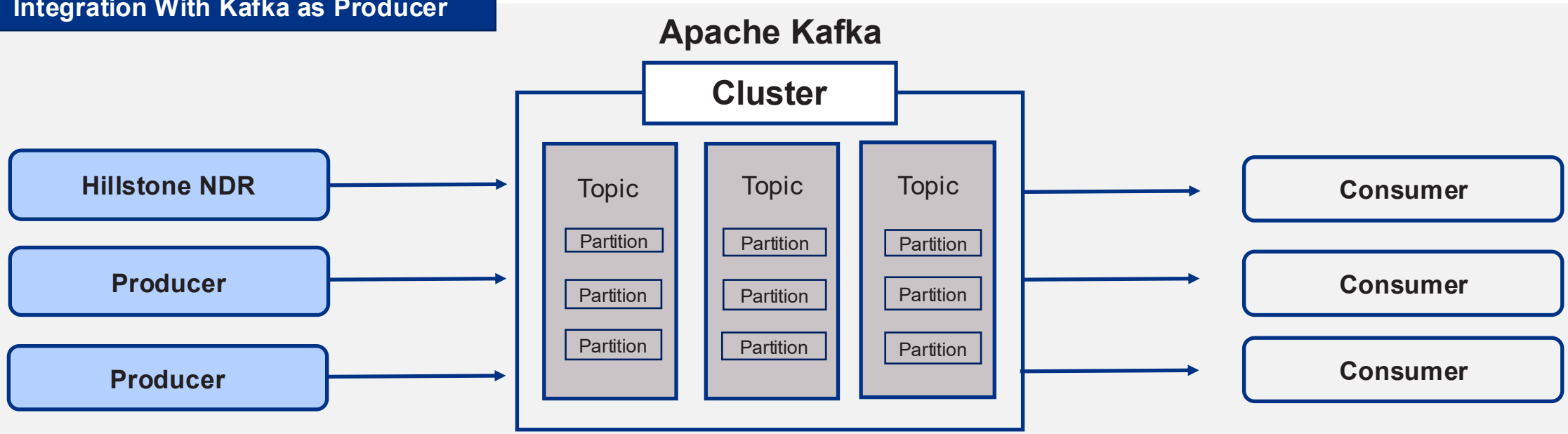


On the risk server or risk endpoint page, the threat and traffic information matching the current interface filtering conditions are exported. A PDF report is generated, which includes the following information:

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

Third-Party Integration

Integration With Kafka as Producer

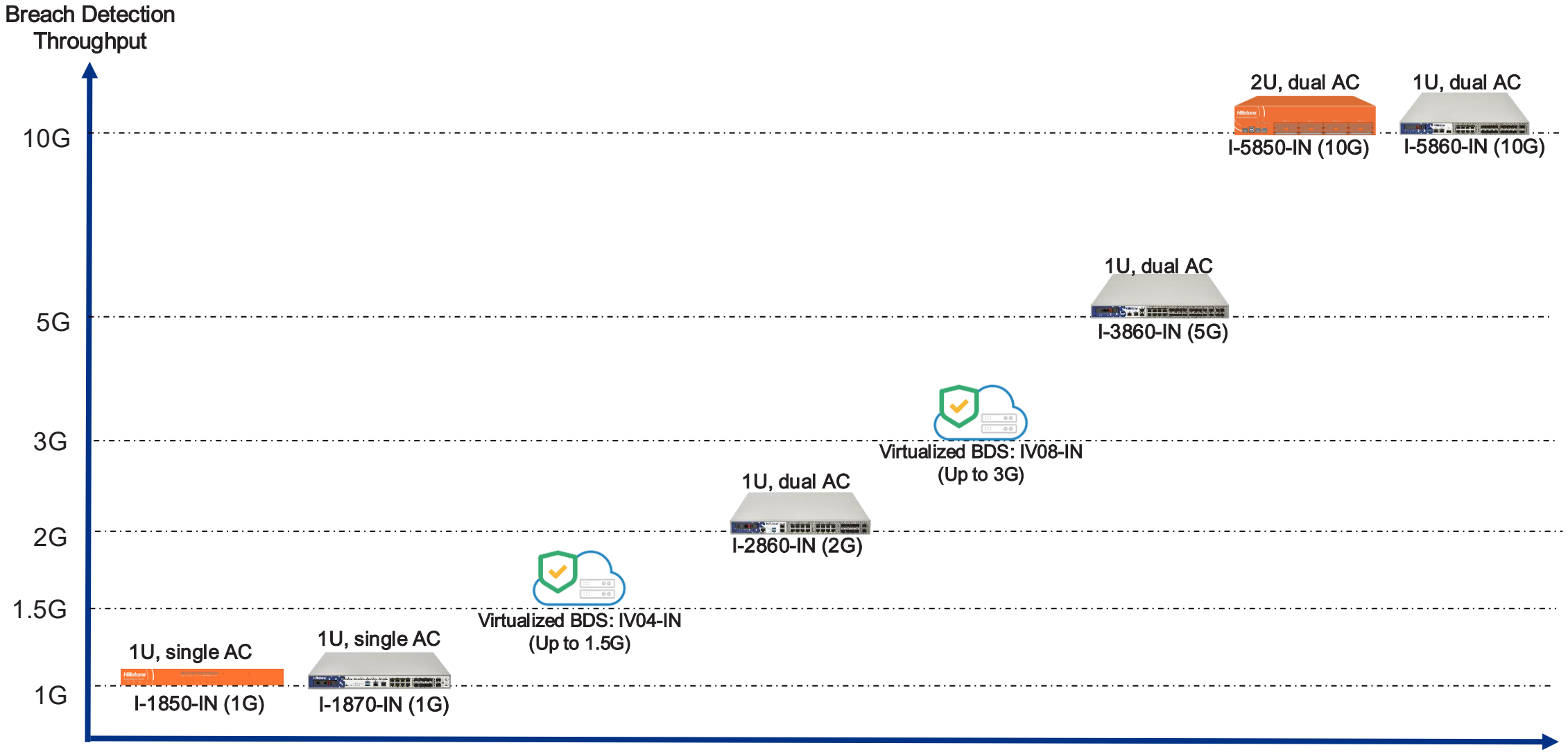


Forwarding logs via Syslog

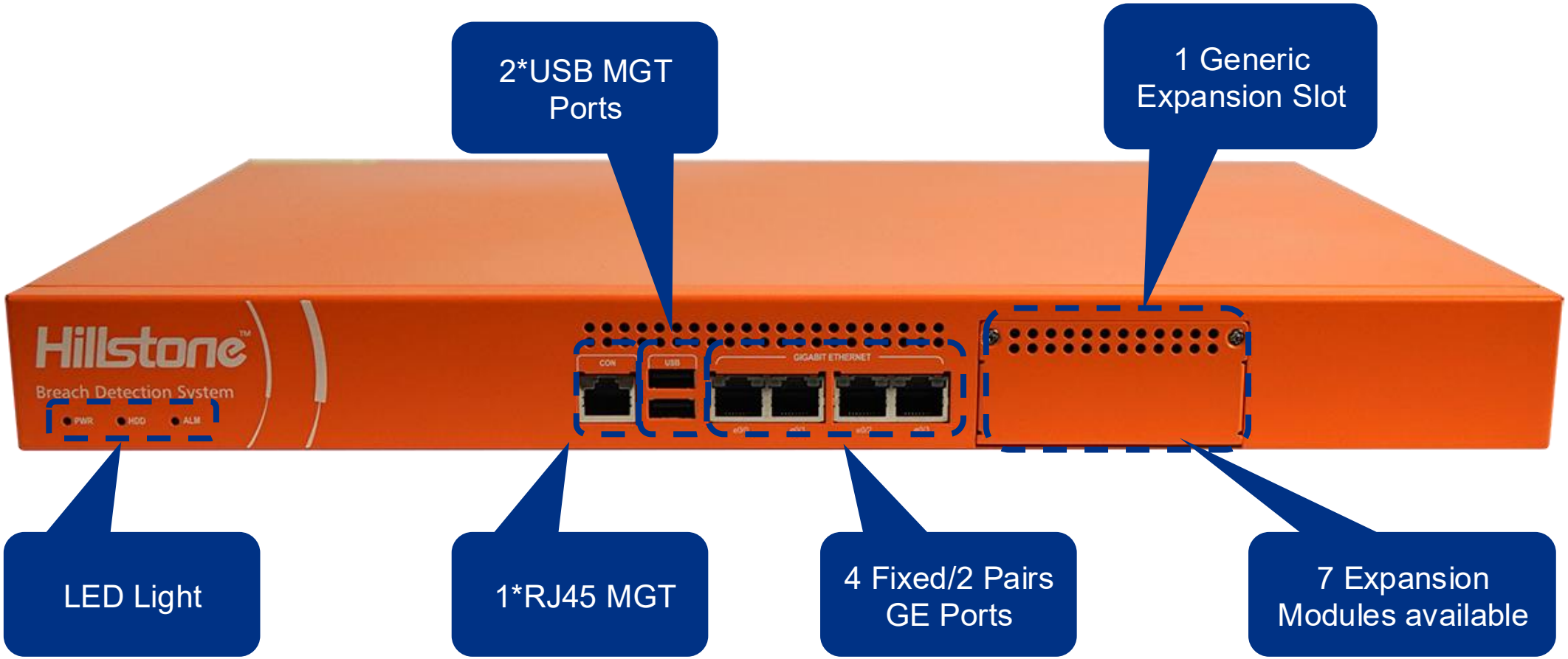
Closed Cycle: Network Detection and Response

Hillstone NDR Product Portfolio

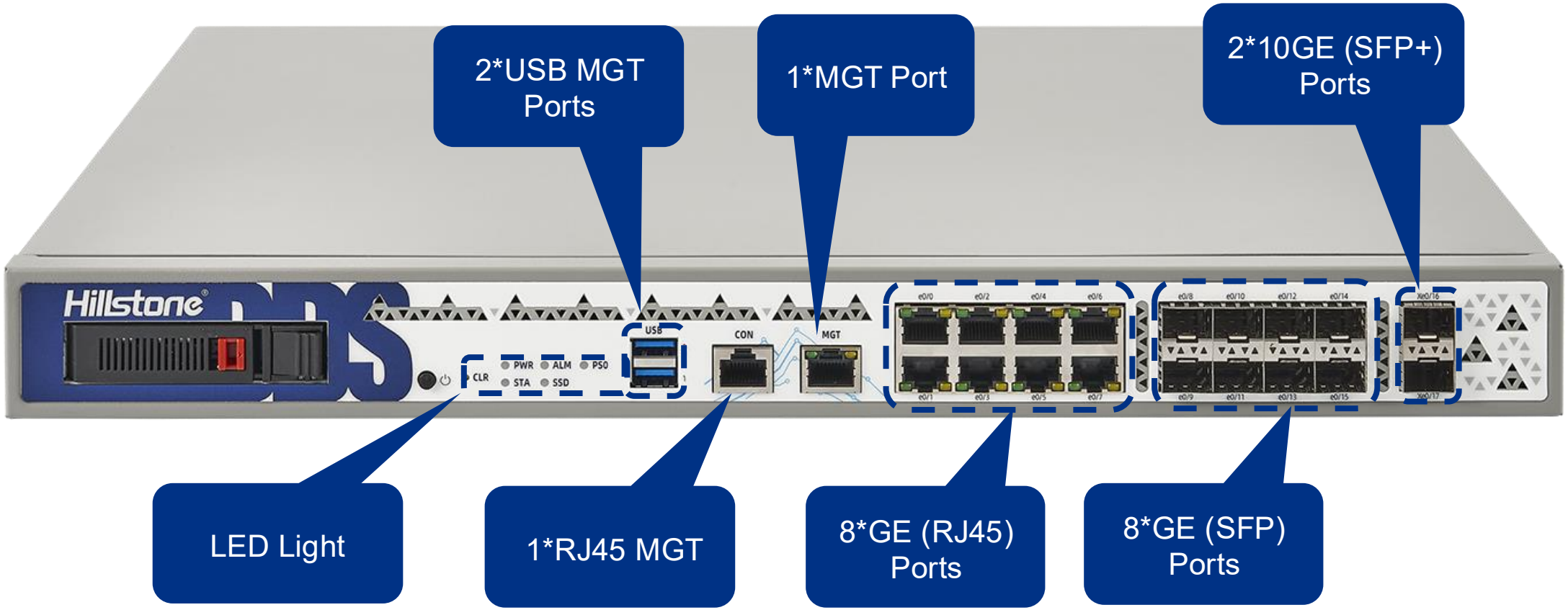
Hillstone NDR Product Portfolio



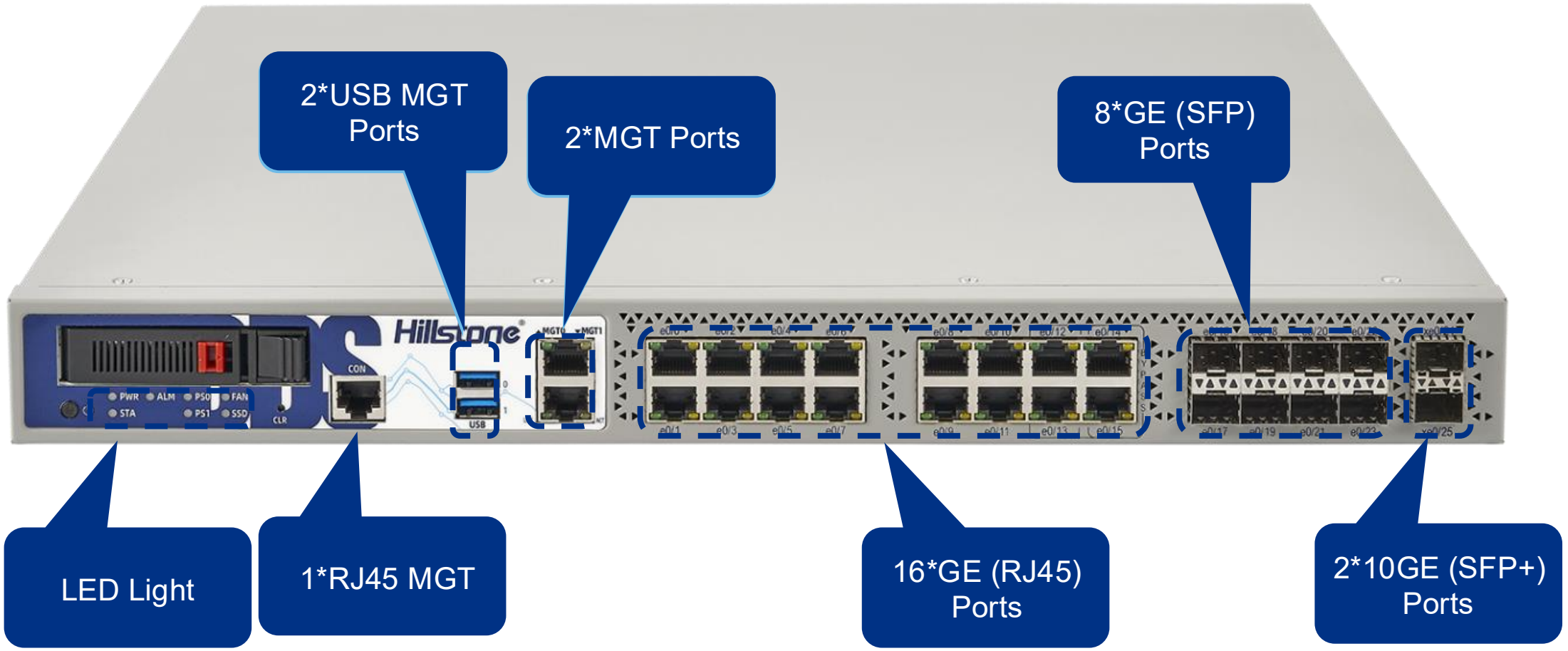
I-1850 Hardware Specification



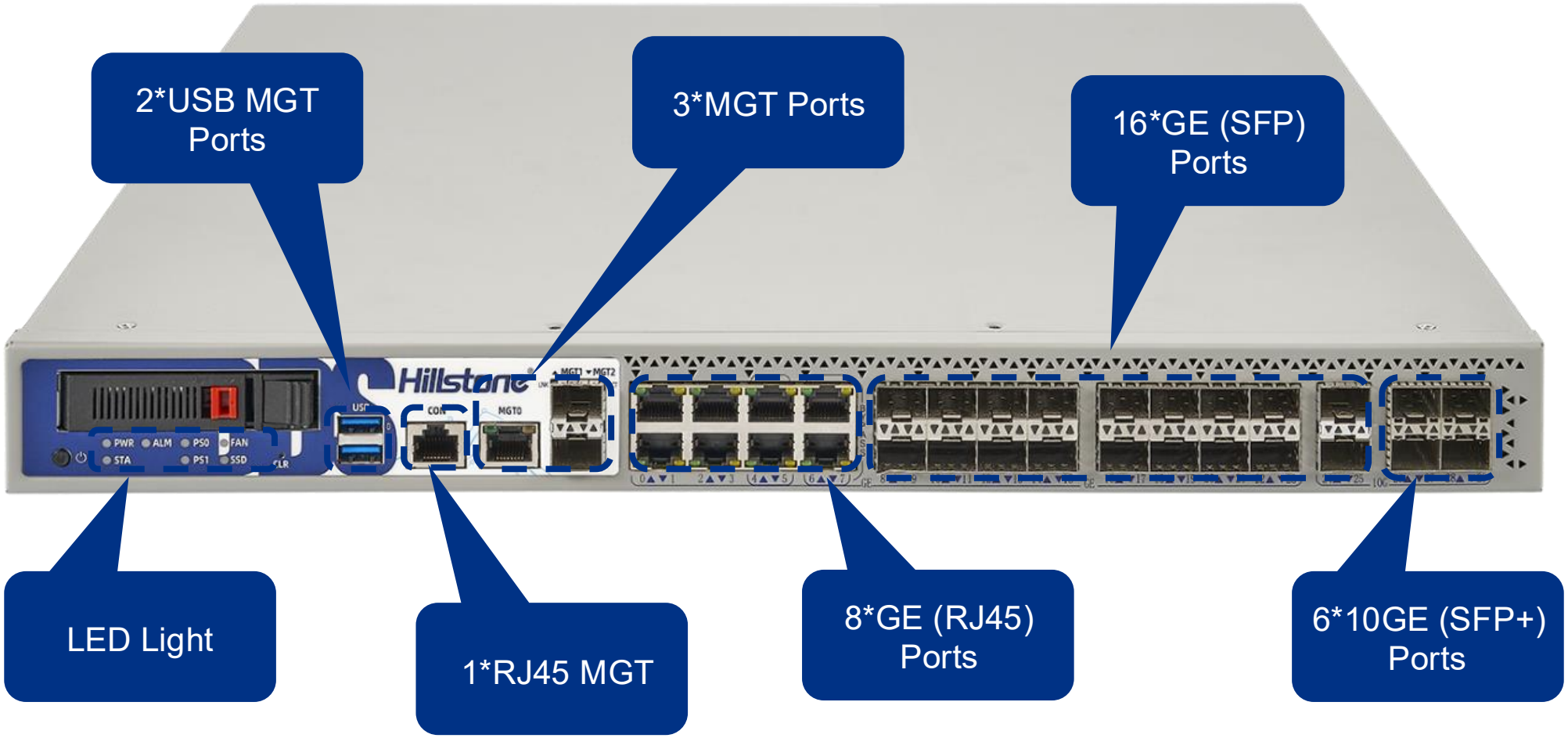
I-1870 Hardware Specification



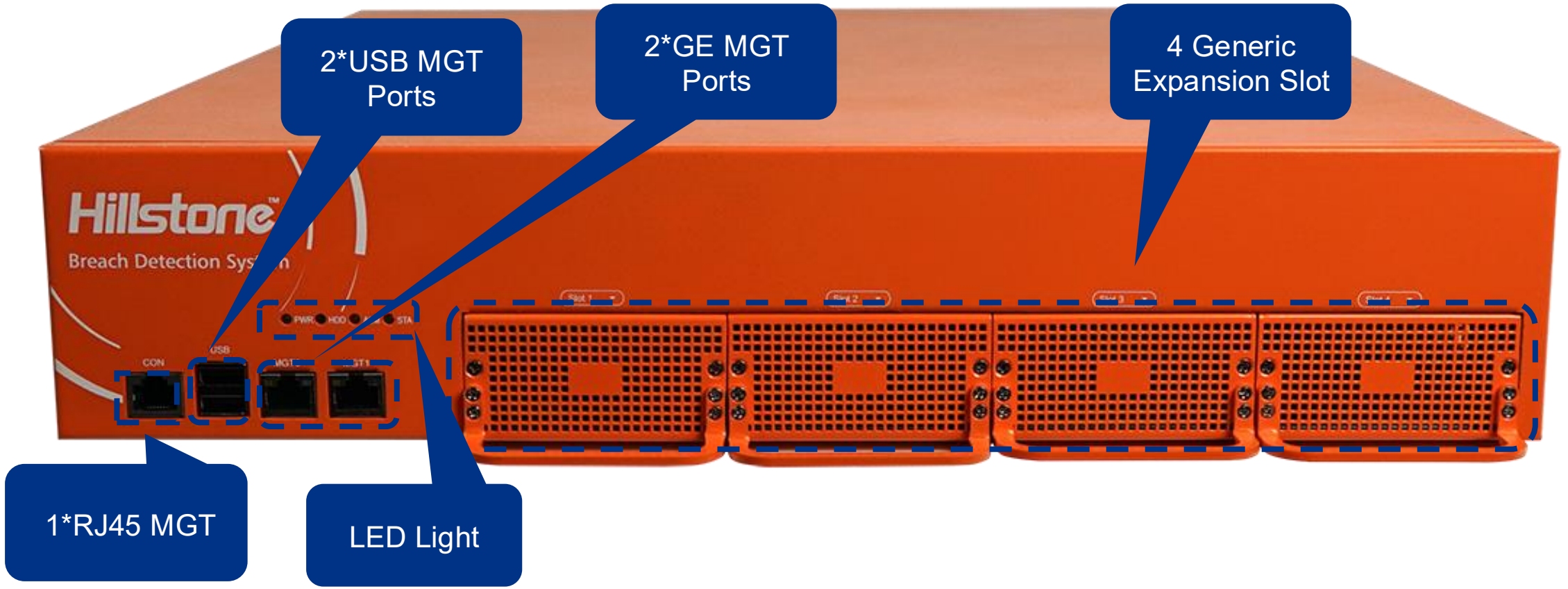
I-2860 Hardware Specification



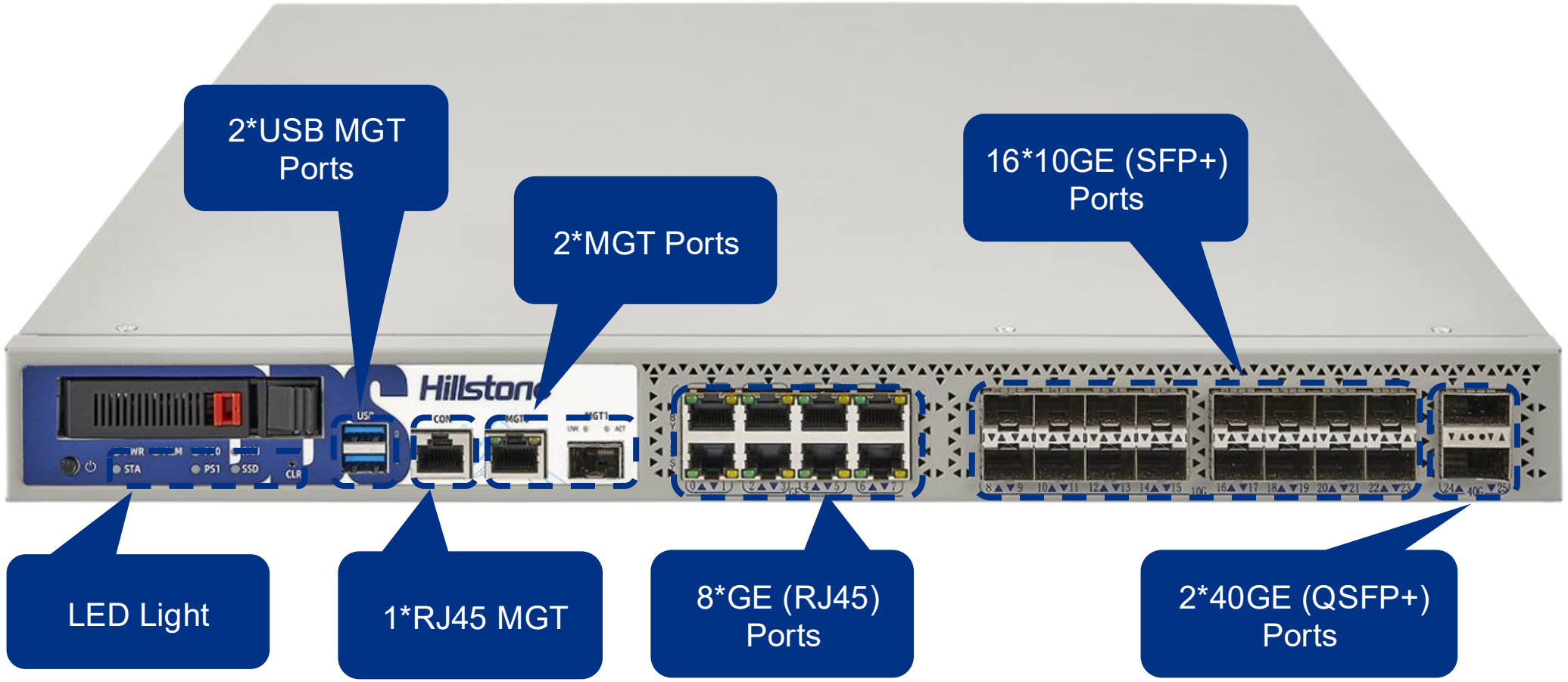
I-3860 Hardware Specification



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)

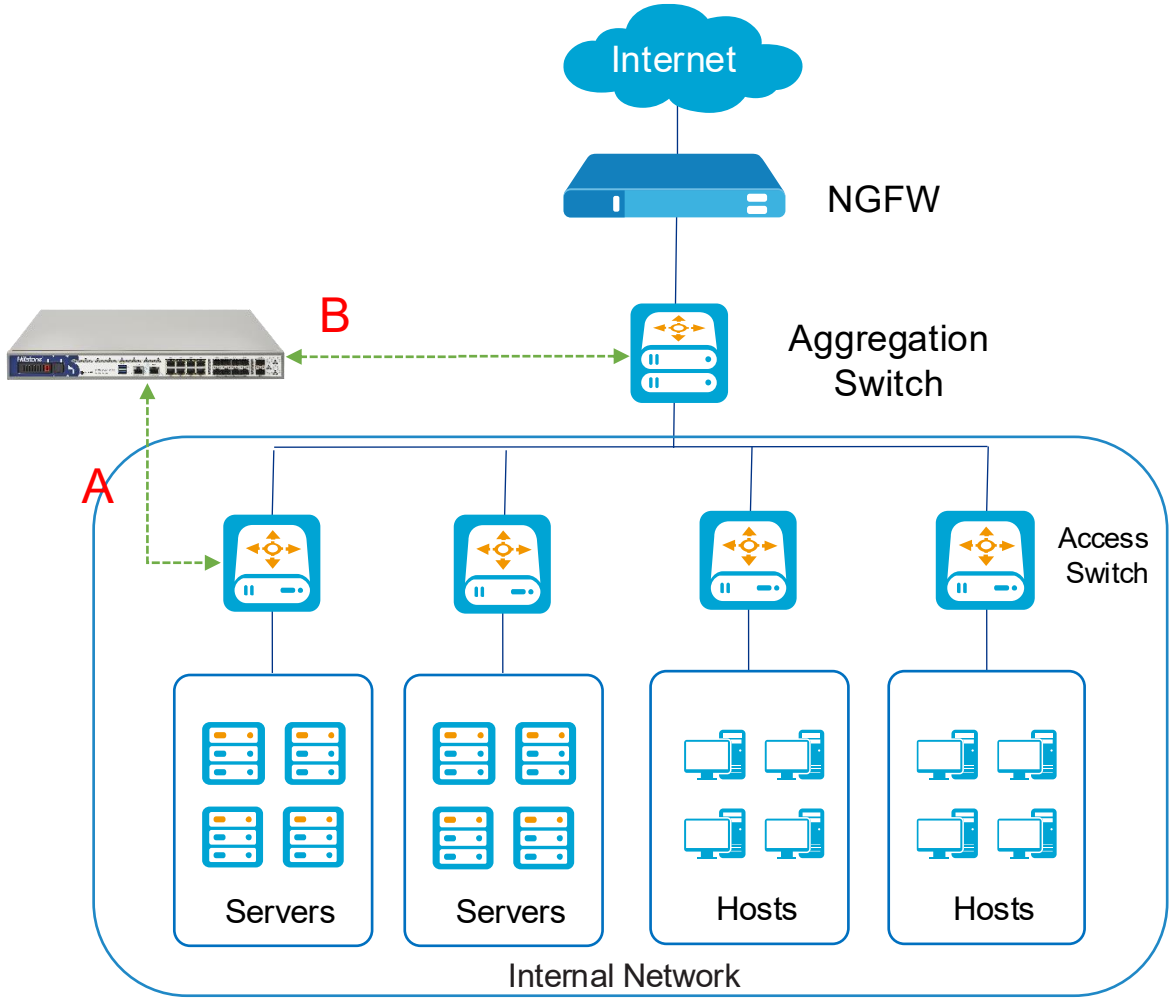
Sysmon Configuration

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.

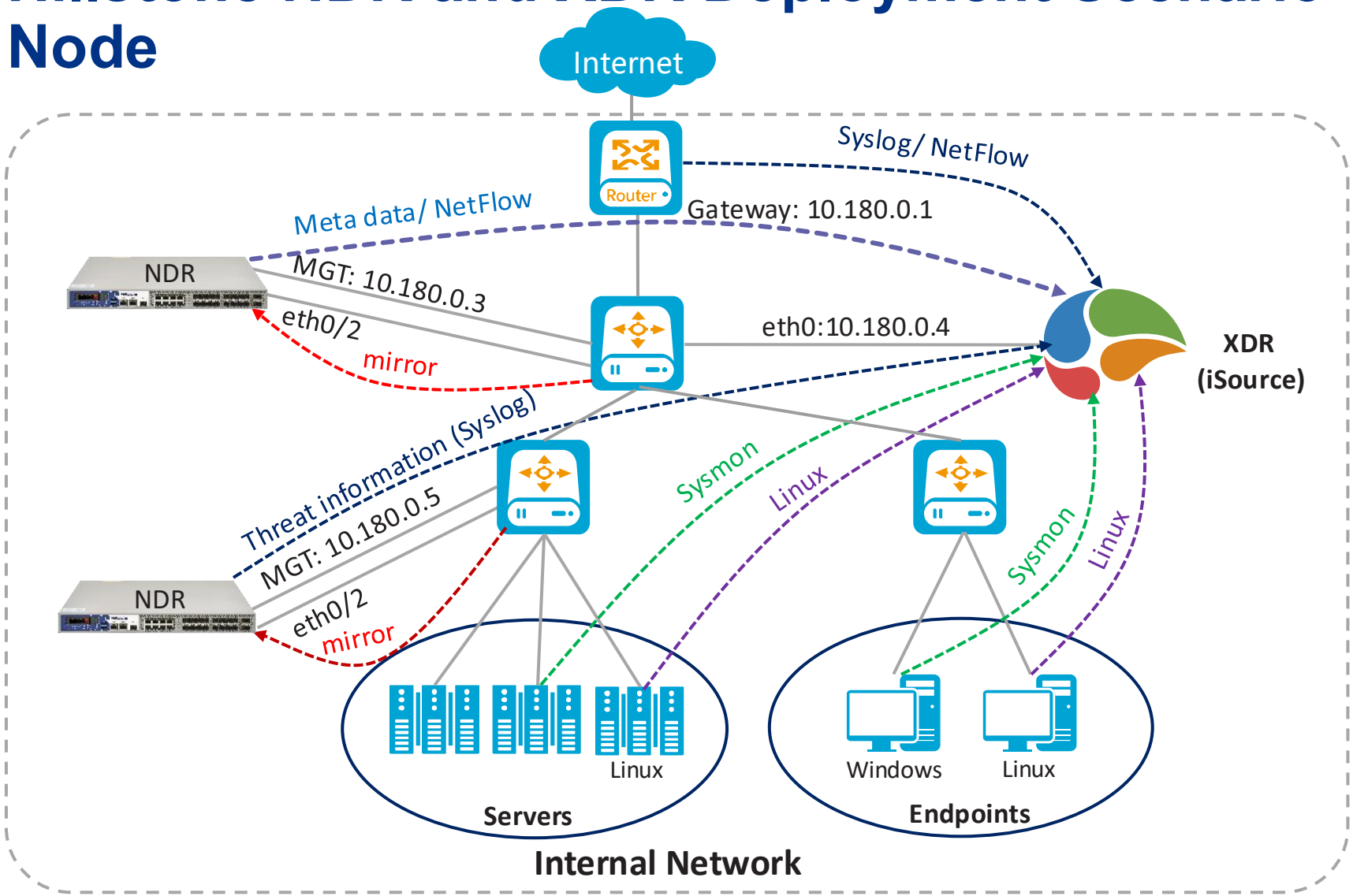
Deployment Scenarios & Case Studies

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*

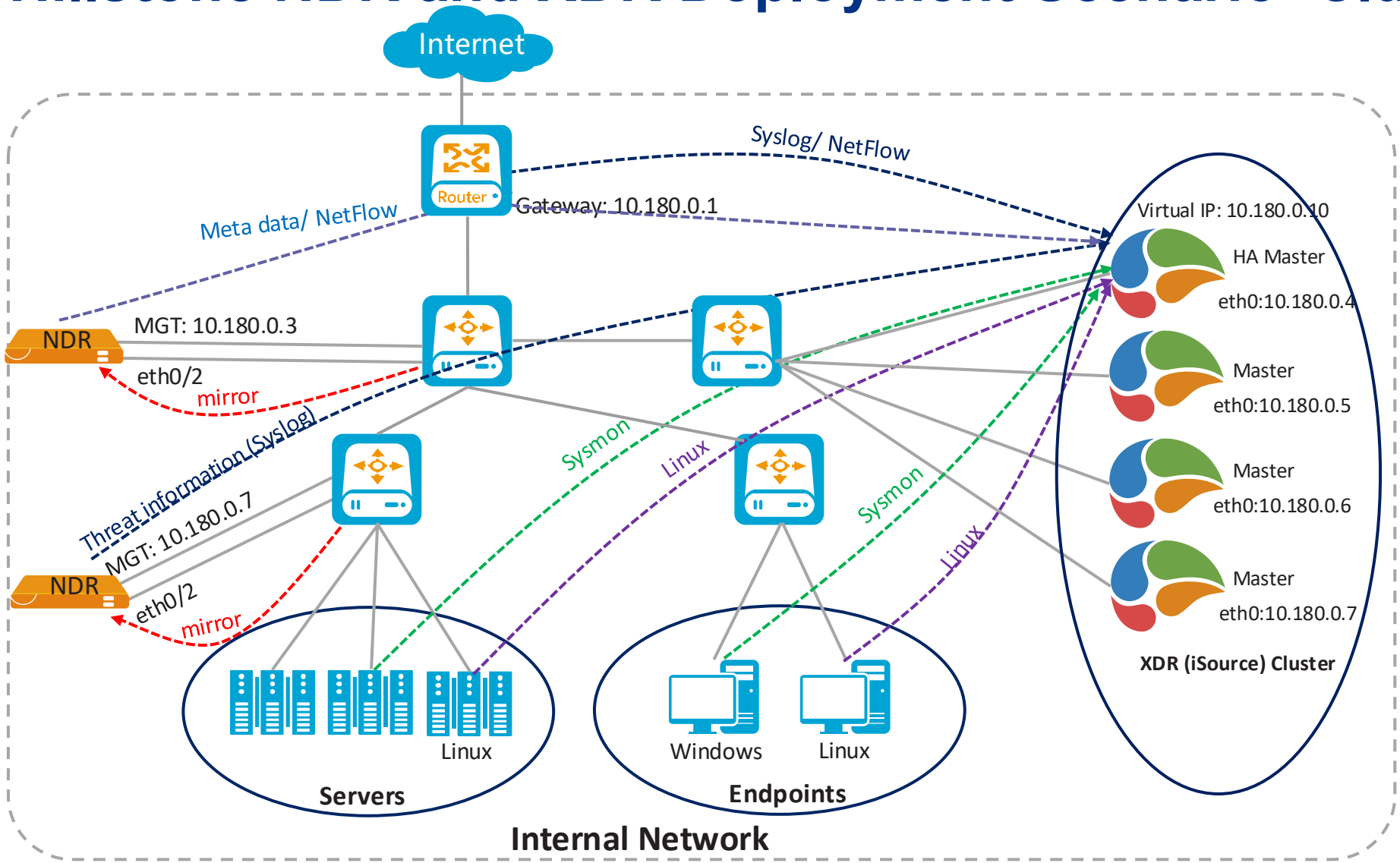
Hillstone NDR and XDR Deployment Scenario- Single Node



Single Node Deployment

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

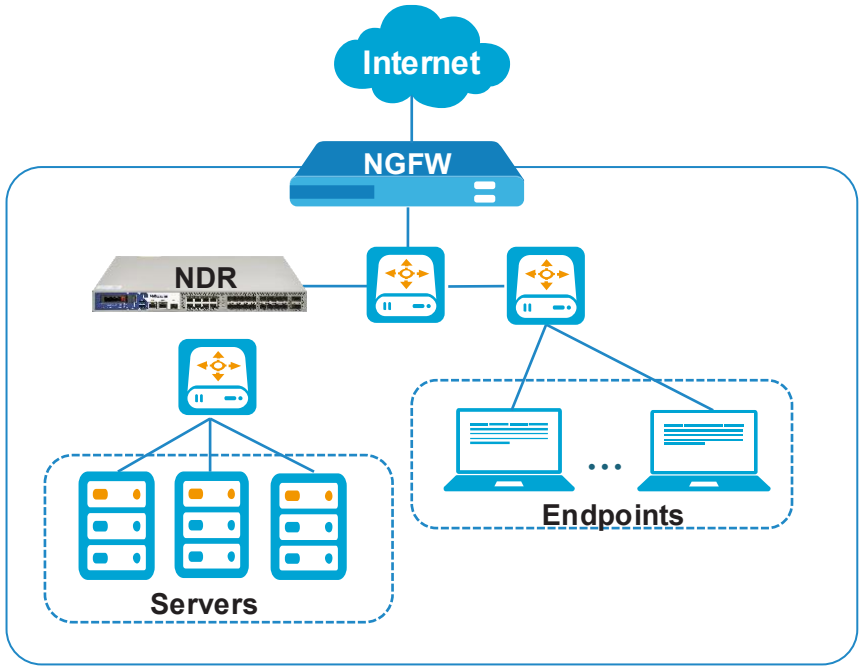
Hillstone NDR and XDR Deployment Scenario- Cluster



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

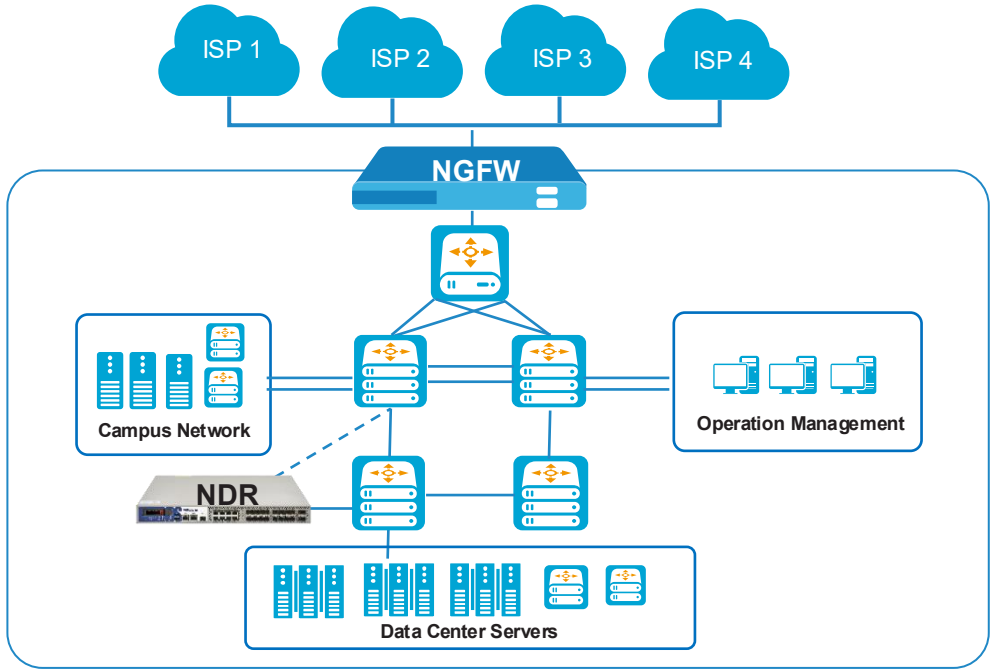
Challenges

- 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