



**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 Networks cooperate overview



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

Global Presence Across 60+ Countries



 Hillstone Regional Offices

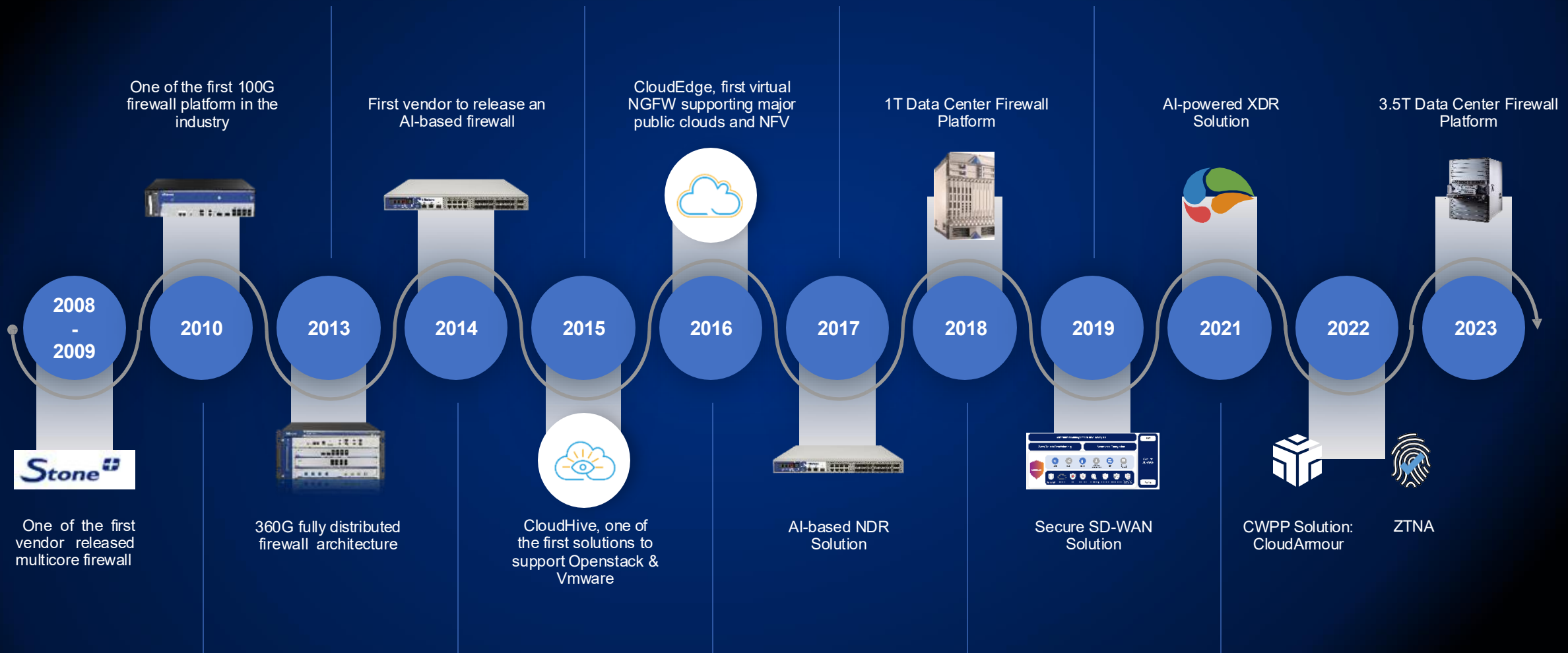
 Hillstone Customer Territories

Business Snapshot



<p>2006 Founded by NetScreen Veterans</p>	<p>340+ Core Patents (authorized/pending)</p>	<p>280K+ Hardware Devices Shipped</p>
<p>26,000+ Customers</p>	<p>100+ Fortune 500 Customers</p>	<p>60+ Countries</p>
<p>2000+ Employees Worldwide</p>	<p>30%+ Employees in R&D</p>	<p>3 R&D Centers in US & China</p>

Over a Decade of Continuous Innovation





A Visionary in the Gartner Magic Quadrant for Network Firewalls

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

4 Consecutive Years of **Customers' Choice** in the Gartner Peer Insights Voice of the Customer for Network Firewalls

Strong Performer in the 2023 Gartner Peer Insights Voice of the Customer for Network Detection and Response



Centralized Security Analytics, Management and Operations



isource

Hillstone Security Operation Platform



HSM/vHSM

Hillstone Security Management Platform



HSA/vHSA

Hillstone Security Audit Platform



CloudView

Cloud Security Monitoring & Analytics

EDGE PROTECTION



A-Series
Next-Gen Firewall (NGFW)



x-Series
Data Center NGFW



S-Series
Network intrusion
Prevention System (NIPS)

CLOUD PROTECTION



CloudArmour
Cloud Workload Protection Platform



CloudHive
Micro-segmentation Solution



CloudEdge
Virtual NGFW Solution

SERVER PROTECTION



I-Series
Server Breach
Detection System
(sBDS)

APPLICATION PROTECTION



AX-Series
Application Delivery
Controller (ADC)



W-Series
Web Application
Firewall (vWAF)



SD-WAN



ZTNA



Micro-Segmentation



CWPP



NDR



XDR

A Future-Ready NGFW

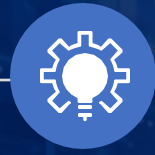
A Future-Ready NGFW



A-Series with Advance Hardware Architecture



**High
Performance**



**Excellent
Expansion
Capability**



**Advanced
Threat
Protection**



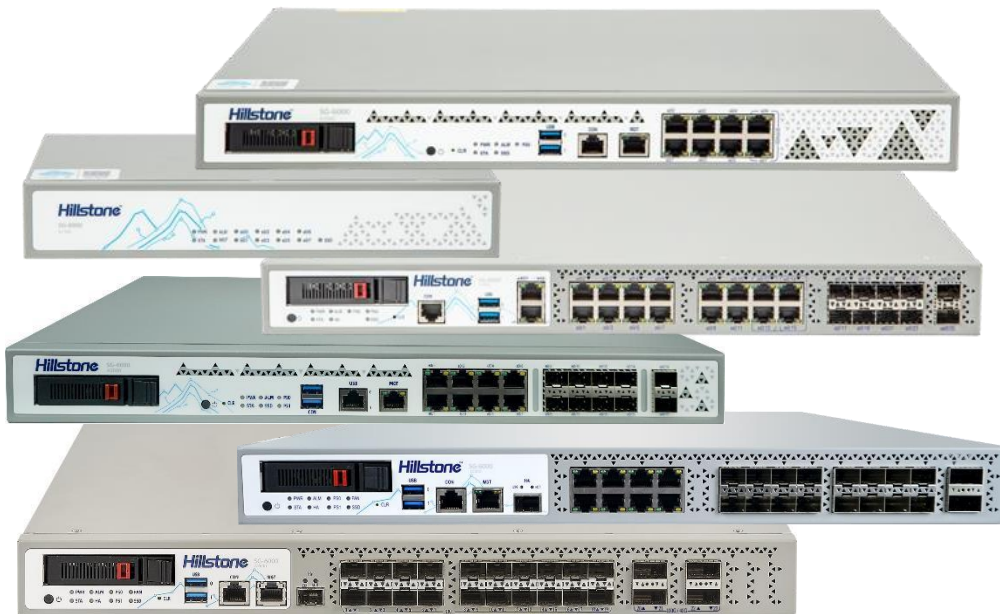
**Smart Policy
Operation**



**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



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 guarantees high 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.



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 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	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	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)	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 (4 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	4 * QSFP28 (or 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP	4 * QSFP28 (or 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP		
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	4G Dongle	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	2	1	1	1	1	1	1	1	1	1	1	1	1	
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-8GE-IN IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-F-8GE-IN IOC-A-4SFP+-IN IOC-A-4SFP+-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SMM-BE-IN
USB	1 x USB2.0	1 x USB2.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	2 x USB3.0	

Better Analytics and Visibility with Increased



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

- ▶ 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**



Hard Drive
(256GB to 1.92TB)
Optional

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**



**Advanced
Threat
Protection**



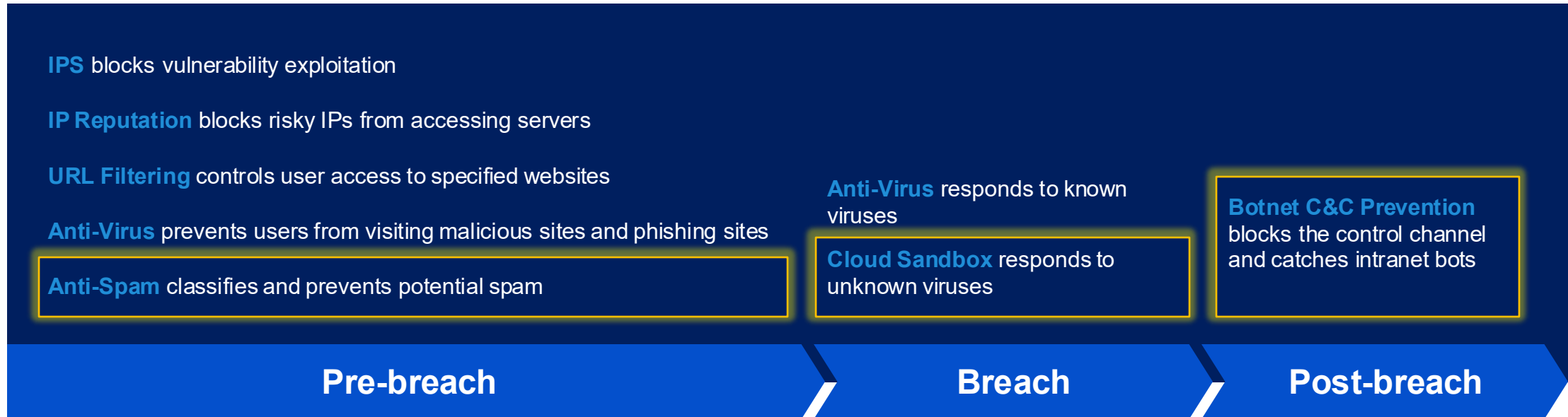
**Smart Policy
Operation**



**Multiple
Deployment
Scenarios**

Interface & Storage

Advanced Threat Protection for Known and Unknown Malware



Intrusion Prevention



IP Reputation



Anti-Spam



Anti-Virus



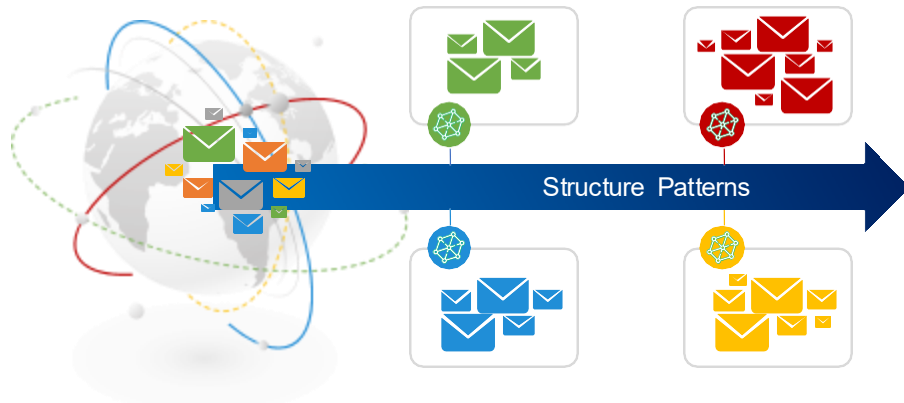
Cloud Sandbox



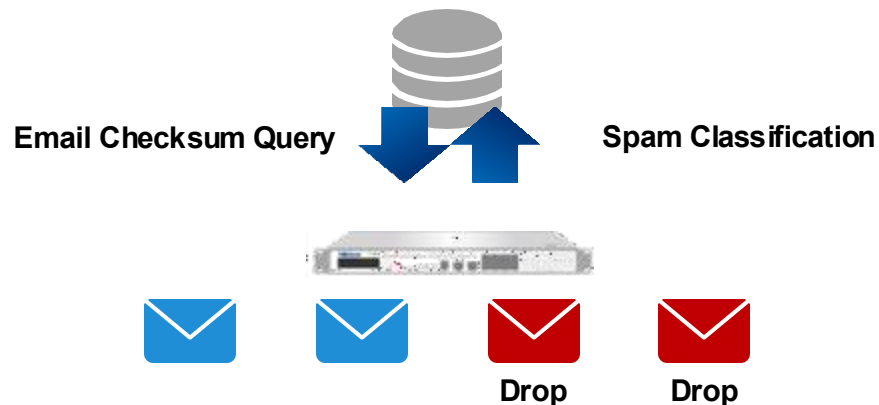
Botnet C2 Prevention

Anti-Spam for Real-time Spam Classification and Prevention

Global Spam Collection (Partner)



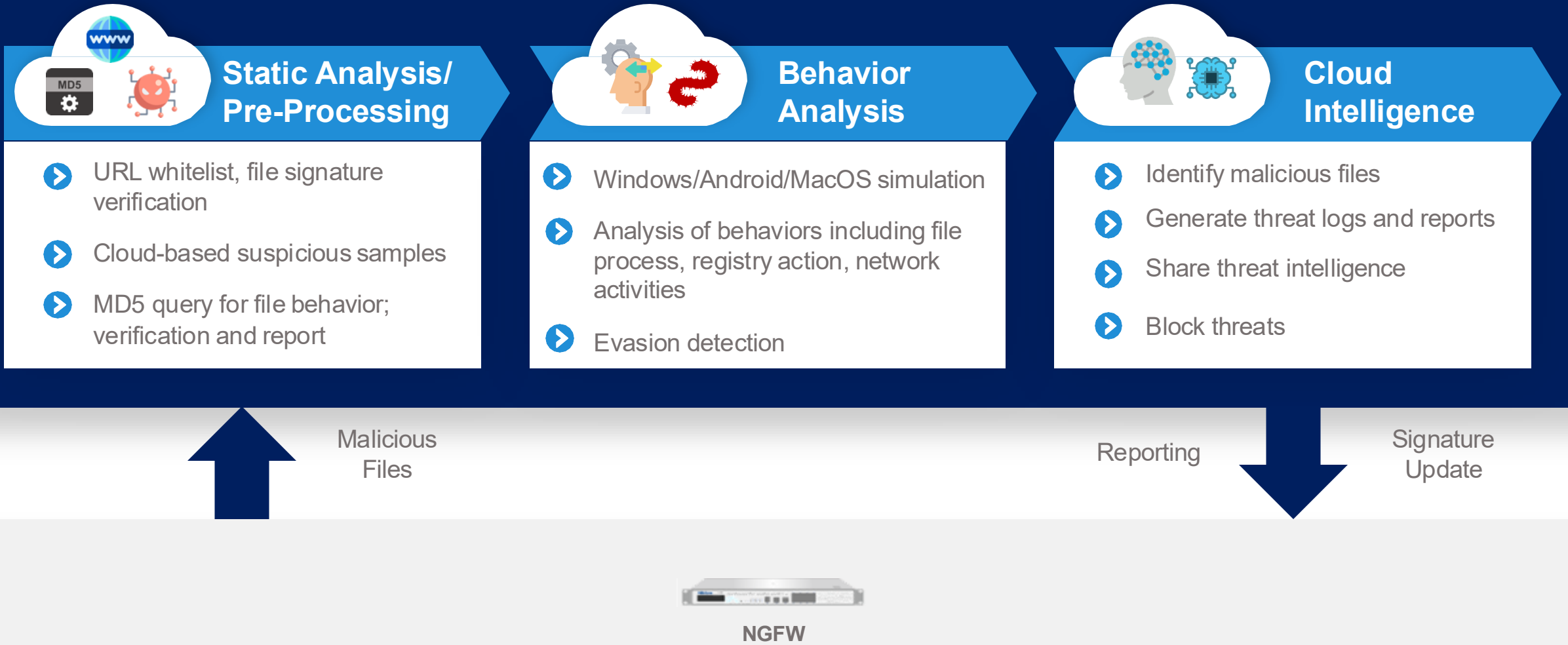
Cloud-Based Spam Database



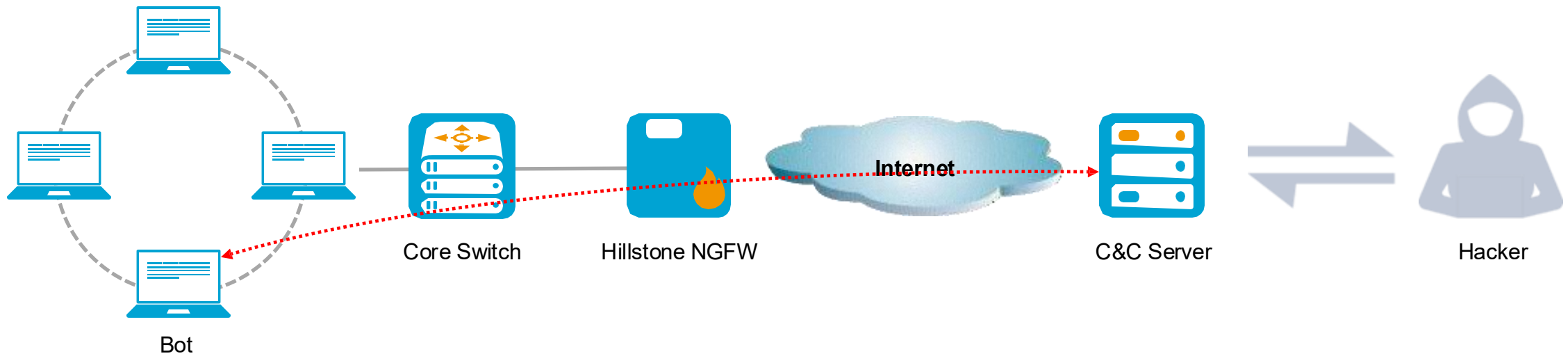
Key Features

- **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 and POP3 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



Complete Botnet C&C Prevention



**C2 Address
Database**

**DNS Sinkhole
Detection**

**DNS Tunnel
Detection**

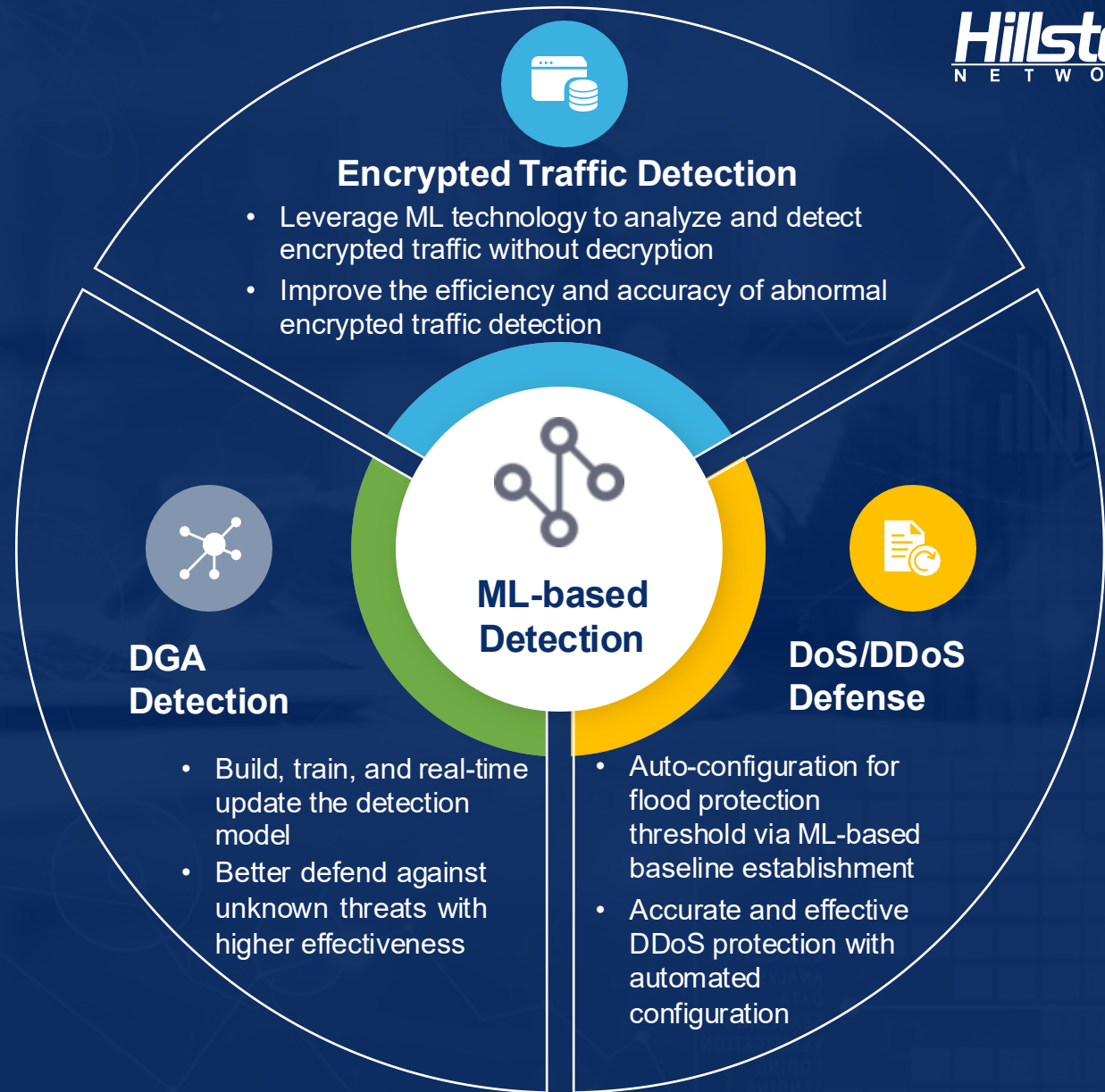
**DGA Domain
Detection**

ML-based Intelligent Threat Detection and Protection

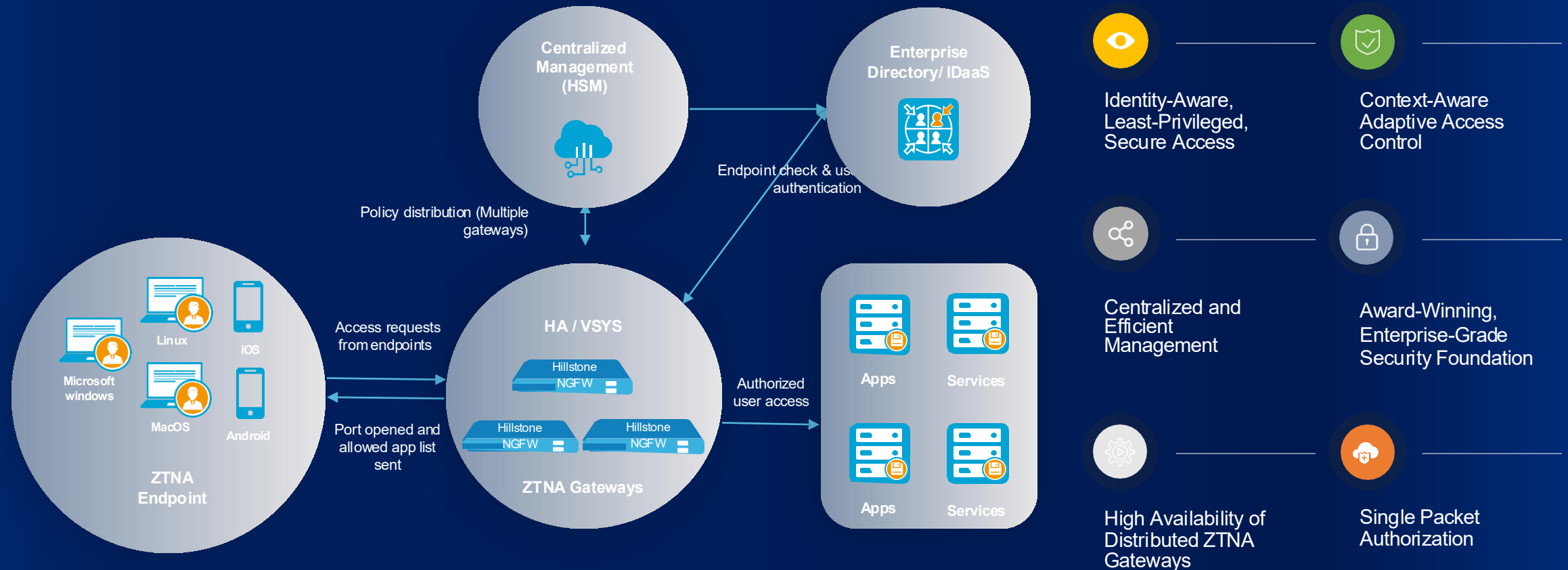
Encrypted Traffic Detection

DoS/DDoS Defense

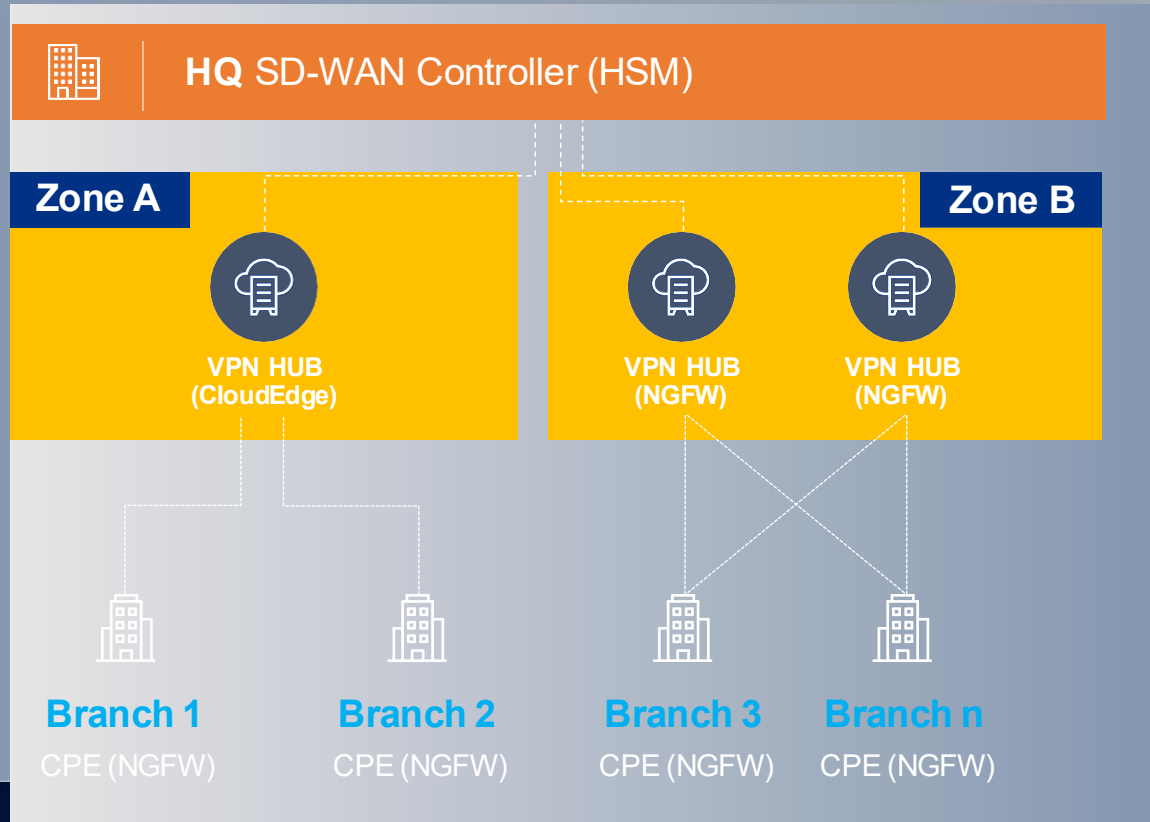
DGA Detection



ZTNA: Enabling Precise Enforcement of Nuanced Privileges



Secure SD-WAN for Distributed Enterprises



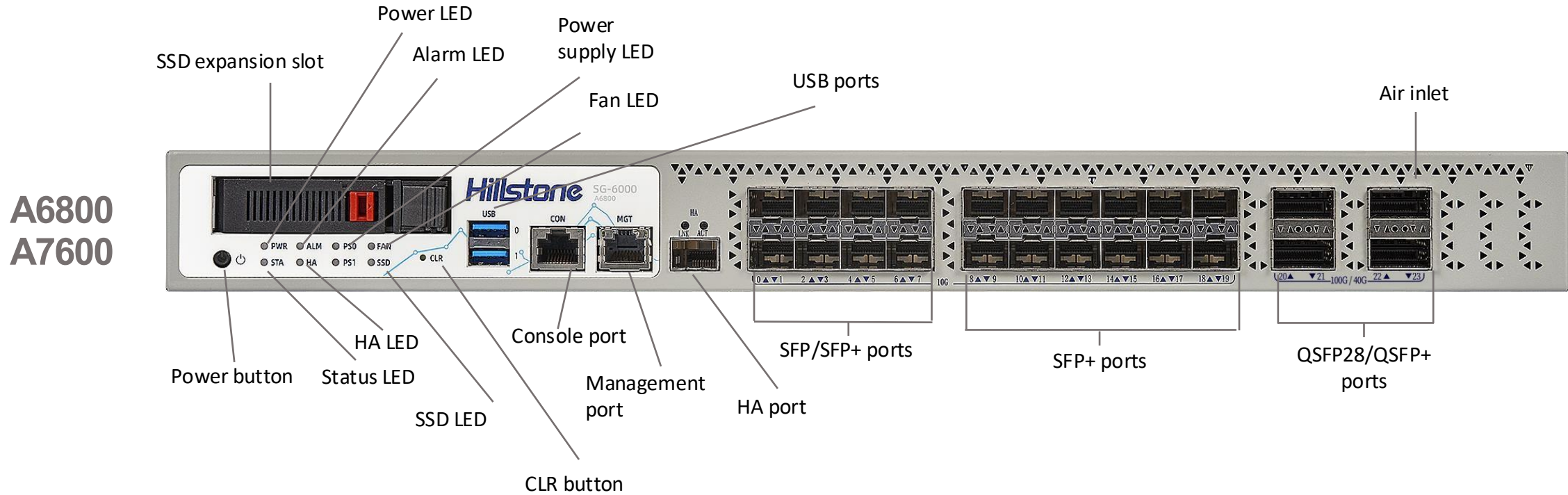
Centralized management with zero-touch provisioning at the edge

VPN over multiple links with intelligent routing

Seamless and comprehensive encryption

Award-winning enterprise-grade security foundation

A6800 / A7600 Front Panel



2

Hillstone NIPS Value Proposition

Hillstone NIPS – A Comprehensive Network Intrusion Prevention System



New Hardware Platform

01 Complete Network Threat Detection and Defense

02 Advanced Threat Protection Throughout the Threat Lifecycle

06 Easy Deployment with Minimum Network Interruption

03 Better Understanding with Rich and Granular Reporting

05 Simplified and Centralized Management for Efficient Security Operation

04 High Reliability to Ensure Reliable Operation of the Network



Context-Aware Detection



User awareness

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



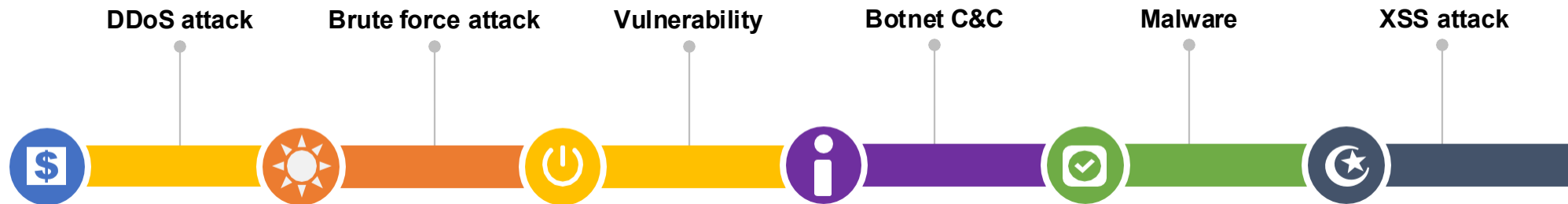
Application awareness

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



Risk awareness

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

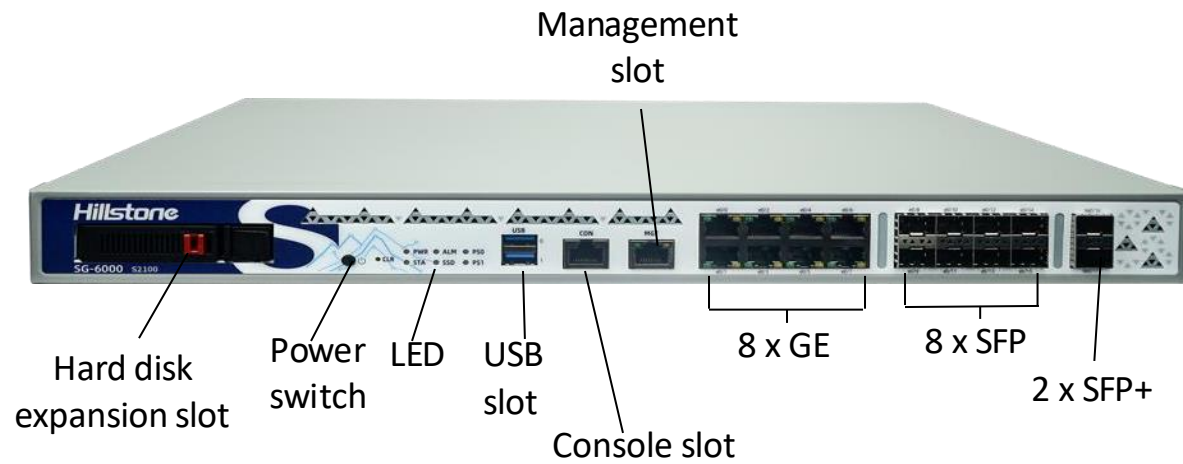


Nearly 10,000 intrusion rules and tens of millions of virus signature database to detect and prevent different attacks

Hillstone NIPS Portfolio



Front View



Back View



Introduction of Hillstone WAF

Hillstone Web Application Firewall Overview

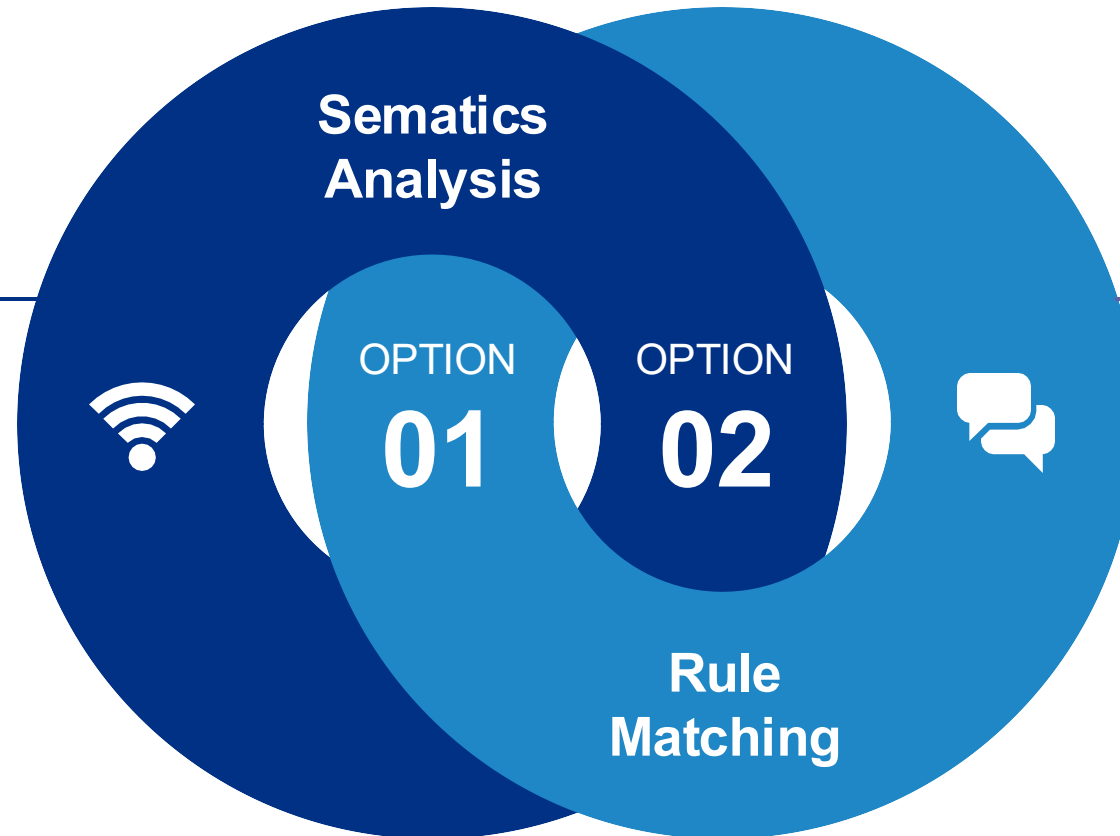


Dual Detection Engine - Semantics Analysis + Rule Matching

Dual Detection Engine

Semantic Analysis

- XSS Semantics Detection
- SQL Injection Detection
- Recursive Decoding



30% decrease in false positive

Rule Matching

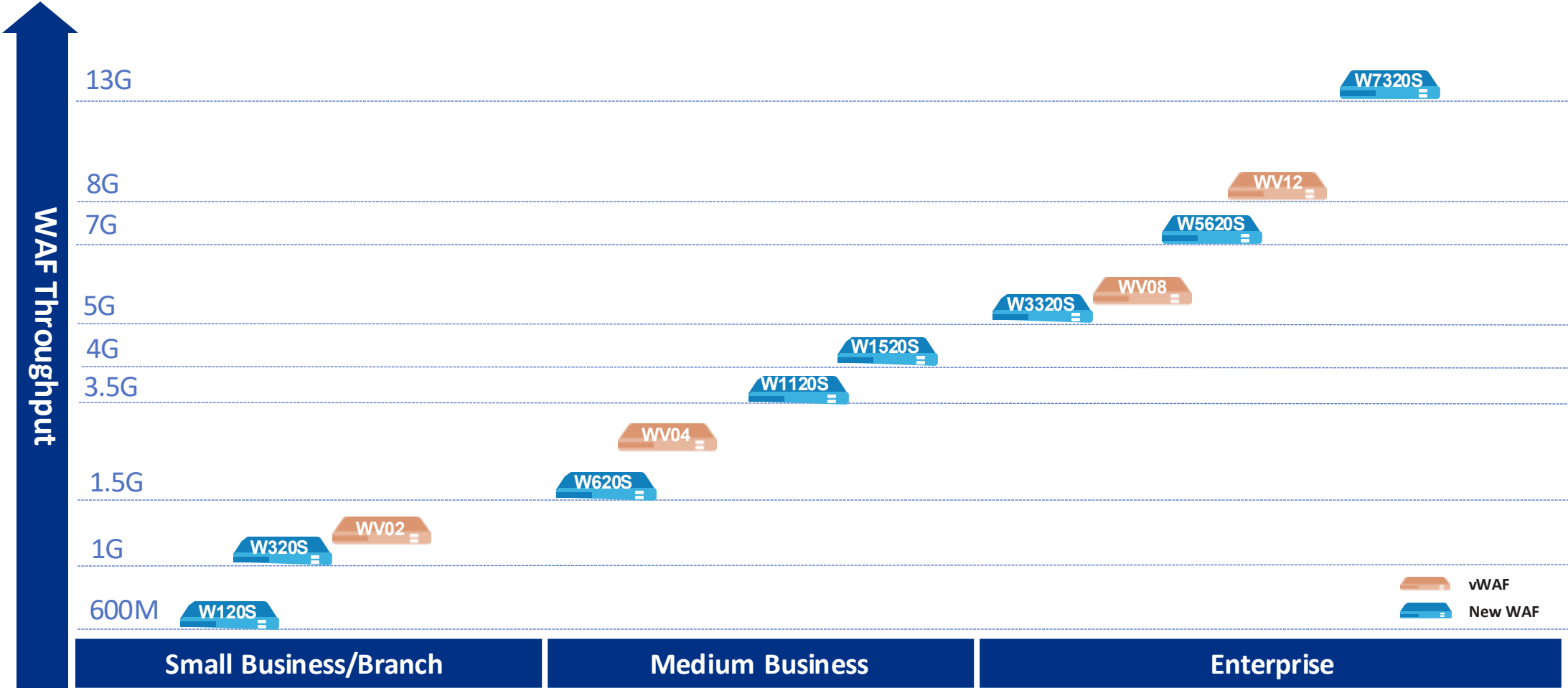
- Regular Expression
- False positive Remediation
- Recursive Decoding

Full-screen Dashborad for Security Posture

Web Application Security Monitoring



Hillstone W-Series Web Application Firewall Portfolio



WAF Hardware Appliance Feature Highlights

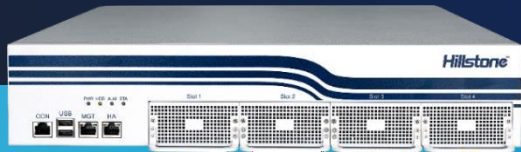
High performance application layer throughput

1. Multiple models covering extensive scenarios
Hardware HTTP throughput: 600Mbps~13 Gbps
2. Flexible interface expansion options
3. SSL hardware acceleration
4. High-density interface with 1U form factor
High-end model fixed I/O Ports : 2 x QSFP+, 16 x SFP+, 8 x GE(including 4 bypass pair)



Hillstone ADC Value Proposition

Hillstone Application Delivery Controller



Hillstone ADC

the Advanced Application Delivery Service



Load Balancing

Server Load Balancing

Link Load Balancing

Global Server Load Balancing

Access Acceleration

Website Acceleration

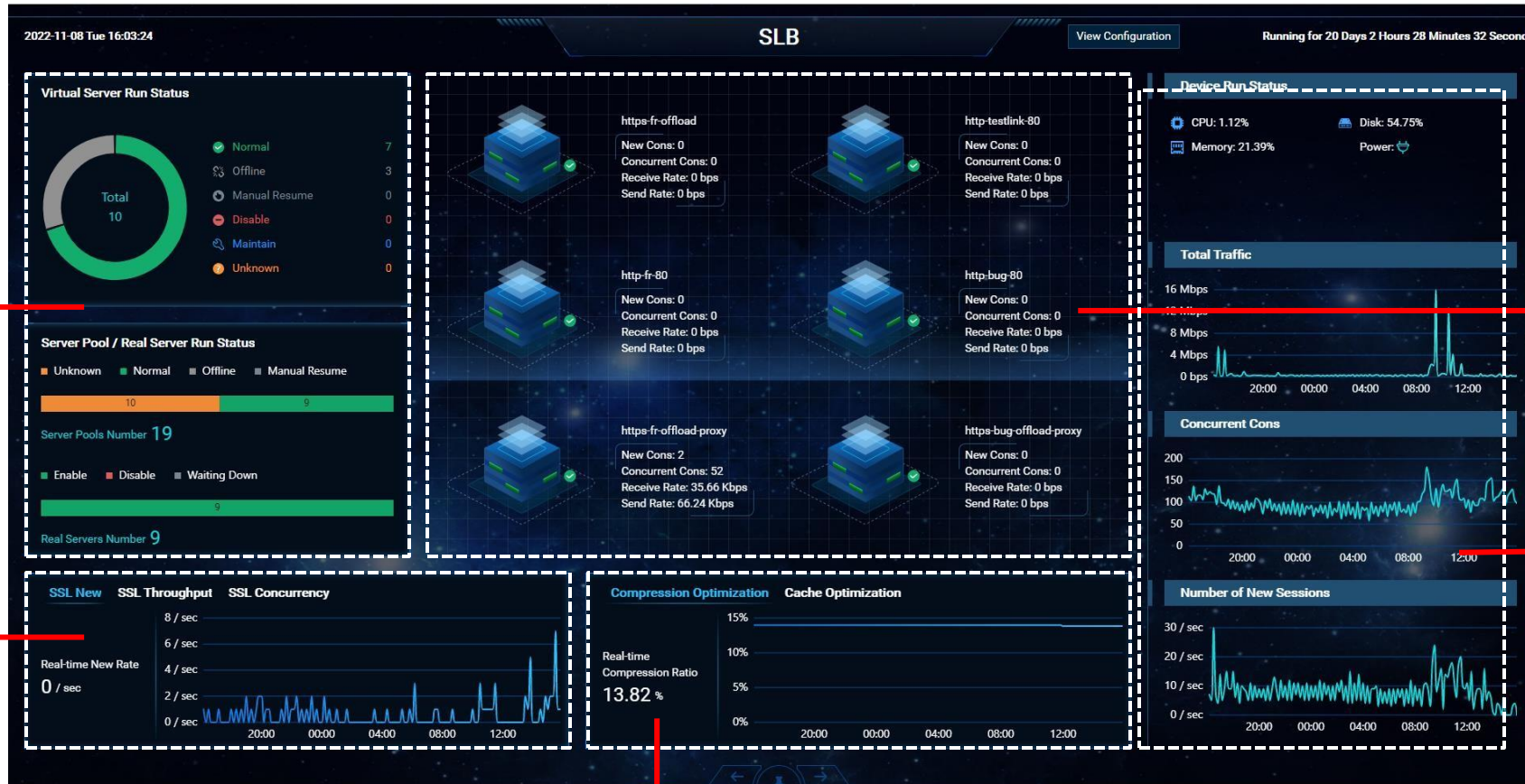
Application Acceleration

Business Transformation

HTTPS Transformation

IPv6 Migration

Full-Screen Dashboard for SLB



Server operation status

Web server status

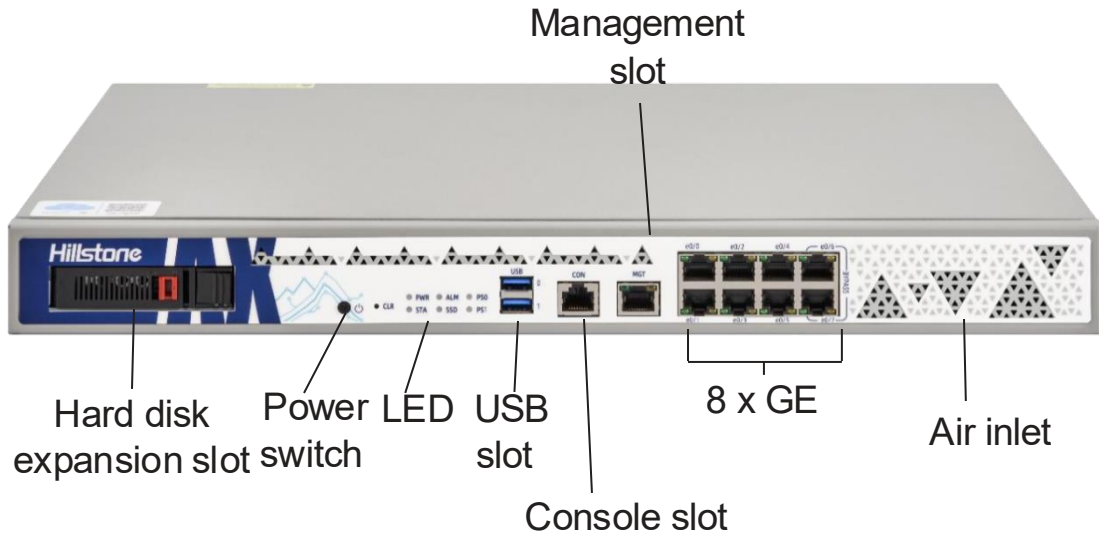
SSL status

Basic device information

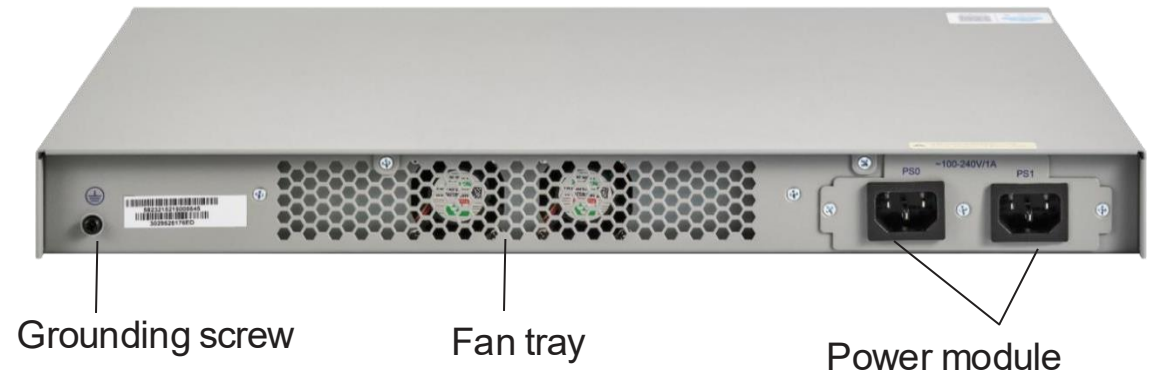
Compression and cache

AX120S-IN

Front View



Back View



Hillstone Breach Detection System (BDS) I-Series

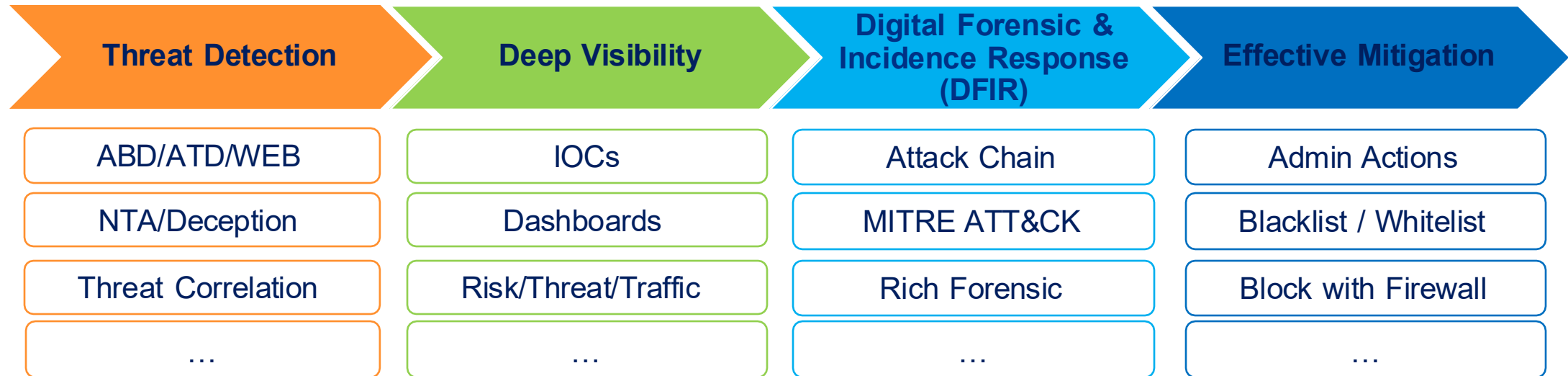


Integrative Cyber
Security

Hillstone NDR Product BDS



Hillstone NDR product detects and responds to Advanced Network Threats

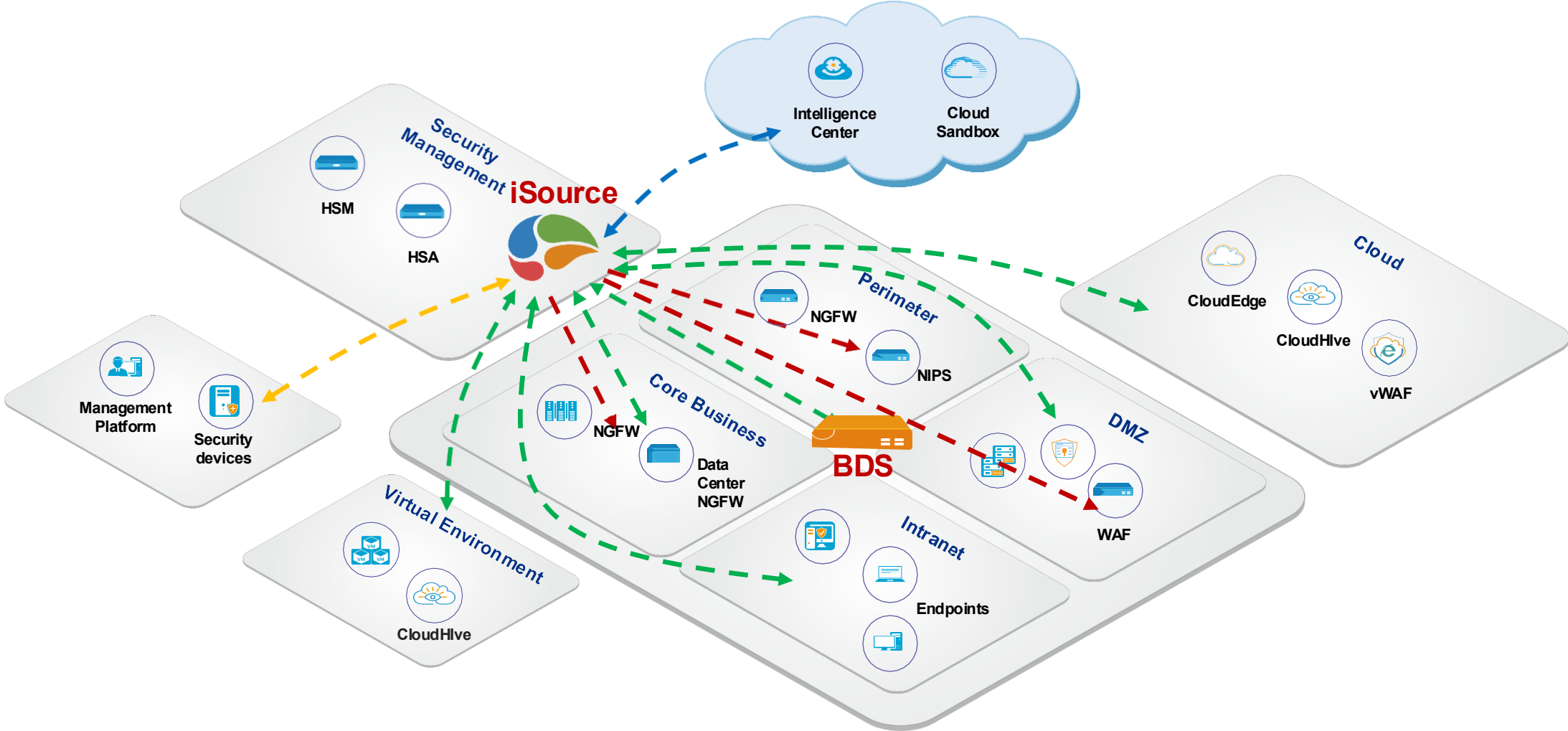


Visibility: Intranet Risk Monitoring Projection



Introduction of Hillstone iSource

Hillstone XDR Solution Overview



←--- Intelligence Sharing

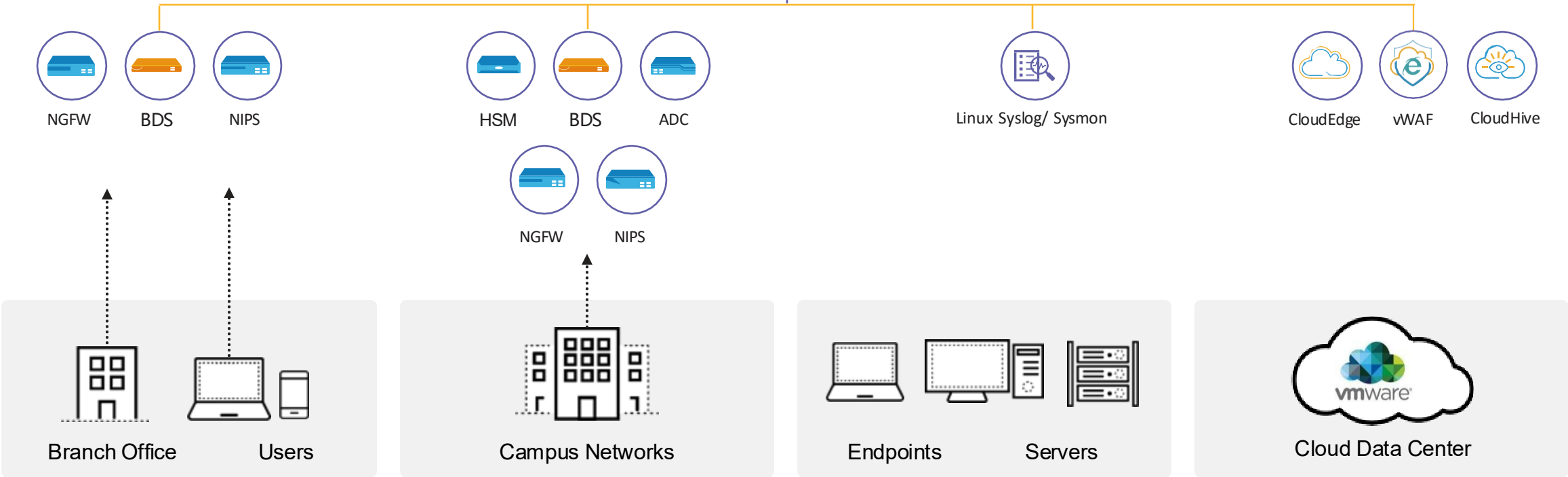
--- Logs/Metadata

--- Responses

Complete Data Collection Across The Environment



- Metadata
- Netflow
- Parsed logs from 3rd party
- Syslogs
- Sysmon
- Vulnerability reports



iSource Feature Highlights

01 Complete Data Collection & Full Visibility

- Granular data collection
- Full screen dashboard with rich security information

02 Asset Discovery and Management

- Auto discovery of assets
- Asset-based threat management

03 AI powered Threat Detection & Analysis

- Abnormal behavior analysis
- Correlation analysis
- Advanced threat detection
- Threat intelligence interaction

04 Investigation

- Threat analysis via SPL language based log search
- Threat insight: displays interconnectivity between assets to pinpoint the source of attack
- Threat hunting

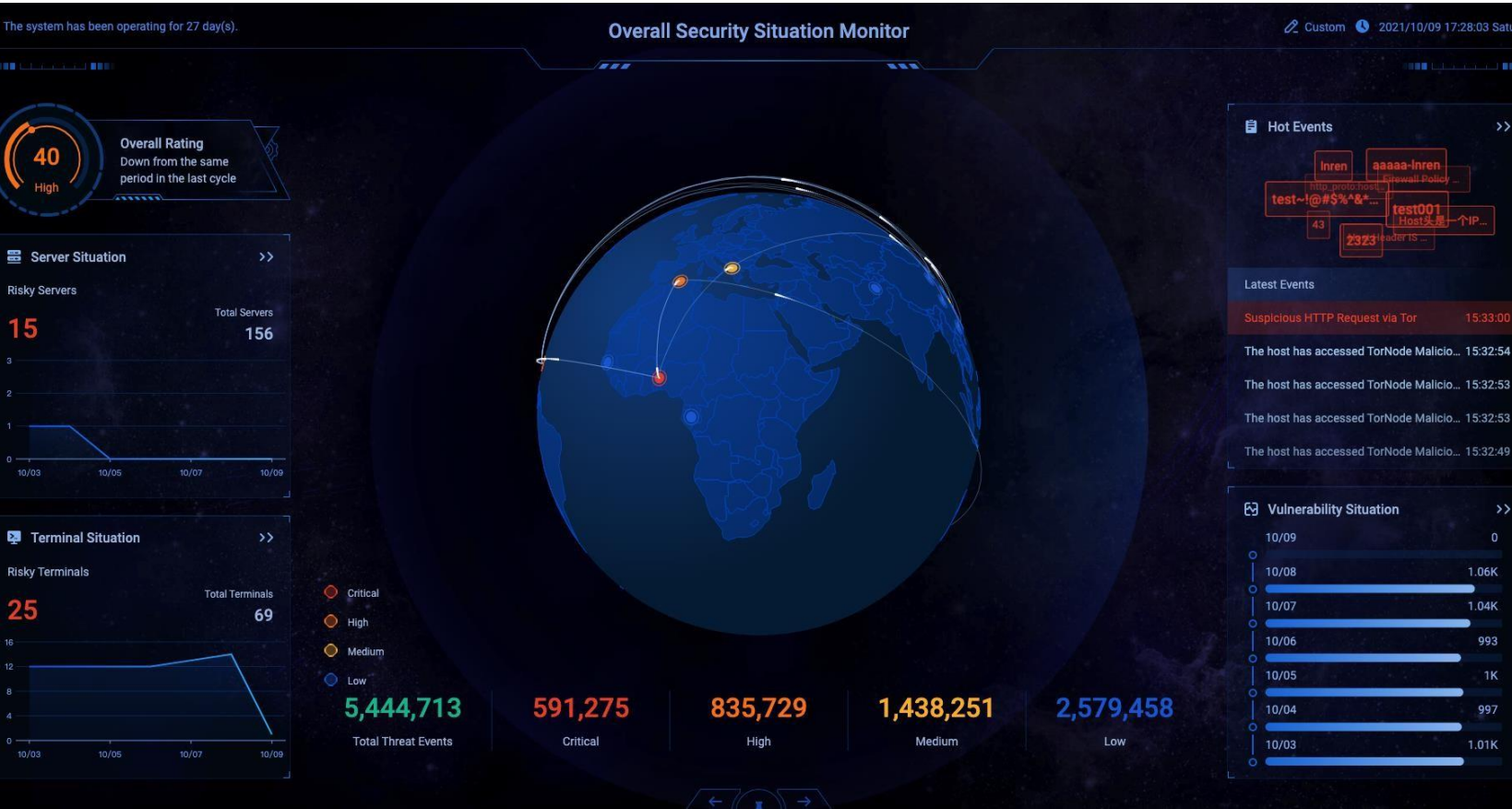
05 Automated Orchestration and Response

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

06 Open Platform with High scalability

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

Full-screen Monitoring Dashboards



Security Overview Dashboard

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

Full-screen Monitoring Dashboards

External Attacks Monitoring

External Attack Situation Monitor

Custom 2021/10/09 17:29:40 Saturday

Attack Event Severity Distribution



Killchain Stage Distribution



TOP5 Attacker IPs

1	1.1.1.61 Australia	615,842Times
2	10.182.191.124 Unknown Location	20,386Times
3	10.182.139.97 Unknown Location	16,989Times
4	10.182.138.221 Unknown Location	16,976Times
5	10.88.25.200 Unknown Location	15,009Times



Attack Event Trendline



TOP5 Attacker Locations

1	Australia	615,842Times
2	China	40Times

TOP5 Attacks Suffered

Asset	Area	Count
1	空去过	616,192Times
2	10.88.7.10	199,163Times
3	10.181.70.120	15,014Times
4	10.160.31.231	10,754Times
5	10.192.5.17	976Times

Full-screen Monitoring Dashboards

Threat Events Monitoring

Threat Event Situation Monitor

Custom 2021/10/09 17:32:55 Saturday

Critical
591,275

High
835,729

Medium
1,438,251

Low
2,579,458

Hot Threat Events



Threat Situation in Last 7 Days



Statistics by Type



Total Threat Events

5,444,713

External-to-Internal	15%	842,770
Internal-to-Internal	2%	107,566
Internal-to-External	0%	15,717
Others	83%	4,478,660

Inren

Attacks
538,515

Affected Areas
2

Affected Servers
1

Affected Terminals
4

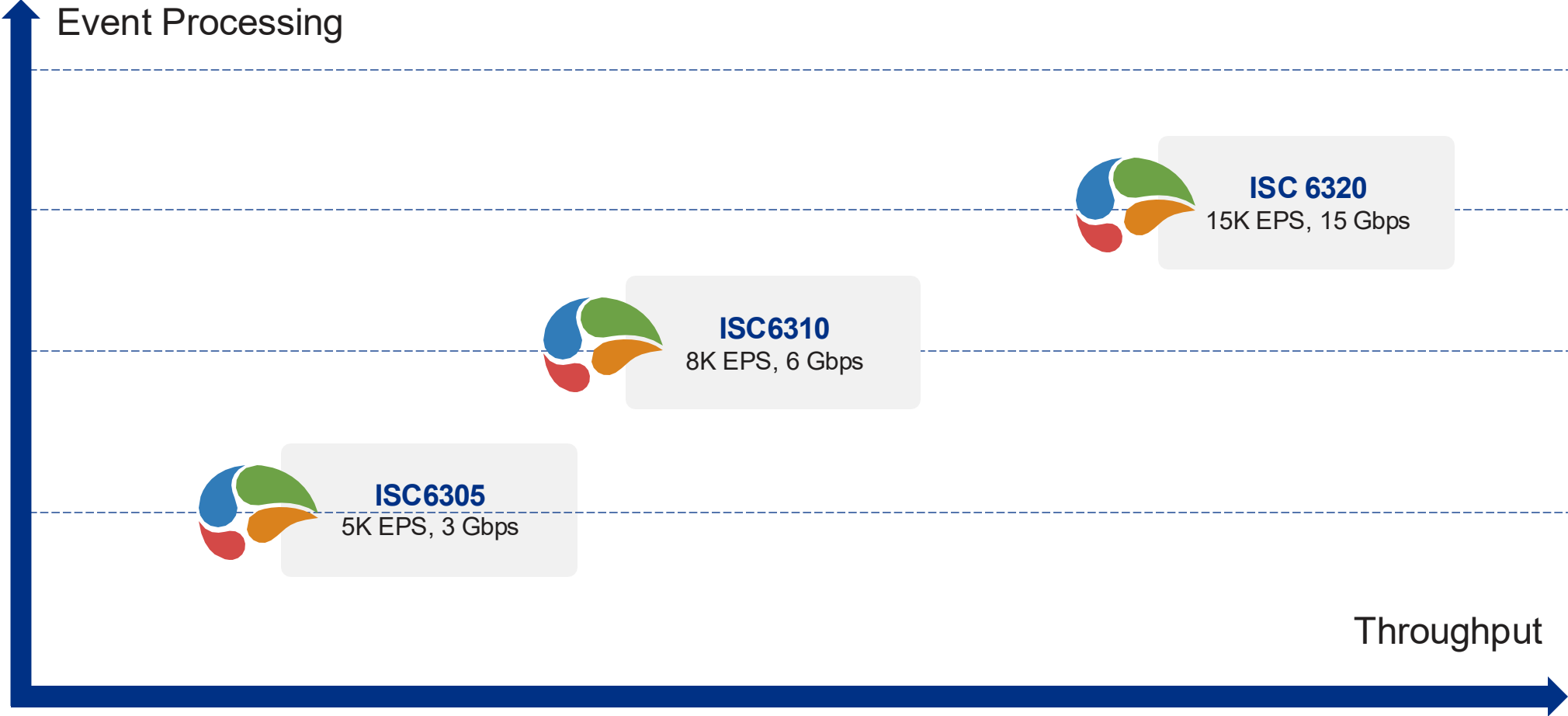
Latest Threat Events

Attack Time	Source IP	Destination IP	Source Area/Geo Location	Destination Area/Geo Location	Severity
2021/09/22 17:05:36	10.182.0.1	10.182.243.160	-	-	Medium
2021/09/22 17:05:06	10.182.0.1	10.182.243.160	-	-	Medium
2021/09/22 17:04:43	10.182.55.116	224.0.0.251	-	-	Medium
2021/09/22 17:04:41	10.182.243.80	239.255.255.250	-	-	Medium
2021/09/22 17:04:36	10.182.0.1	10.182.243.160	-	-	Medium

Threat Event Ranking

Name	Attacks
1 test~!@#%&*(*)_+{} :~<?/\	547,320
2 Inren	538,515
3 aaaaa-Inren	507,366
4 test001	489,052
5 2323	457,258
6 43	446,617
7 http_proto:host_with_ip_address	306,725
8 Firewall Policy Violation	209,323
9 Host头是一个IPv4或者IPv6地址	205,664
10 Host Header IS A IPv4 or IPv6 Addr...	205,479

Hillstone iSource Product Portfolio



iSource is offered as a software package

These 3 different models offer different performances and require different hardware configuration

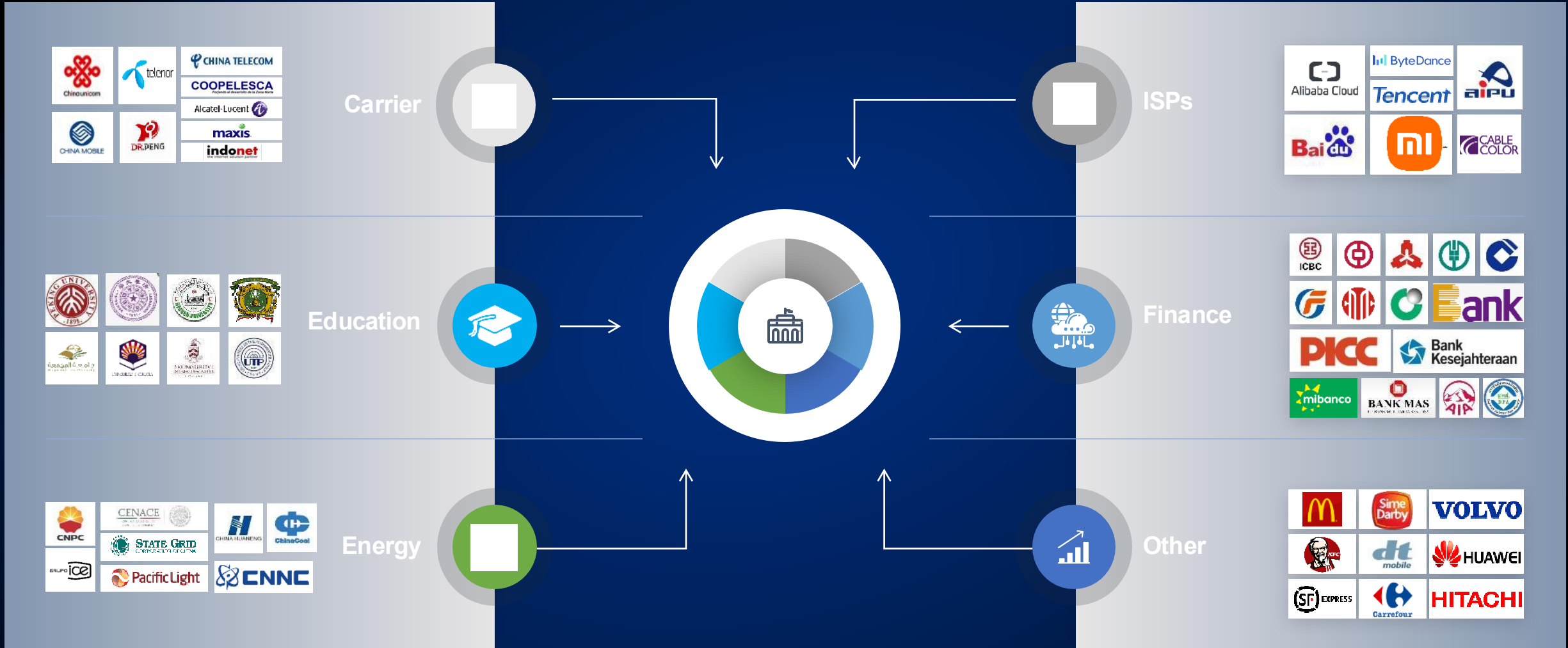
iSource Software Package Format



iSource supports installation in the following environments

Environment	Version	Software Image Format
VMware EXSi	EXSi V6.7	VMDK OVA
Linux	CentOS7	QCOW2
Windows	Windows 10	VHD

More Than 26,000 Customers from All Verticals



Global Technology Certification and Validation





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

