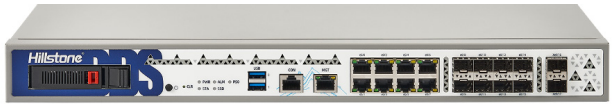
Hillstone I-Series

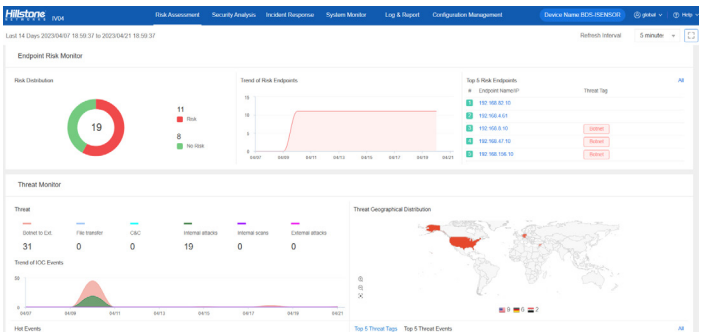
Breach Detection System (BDS)




The Hillstone Network detection and response (NDR) product Breach Detection System (BDS) adopts multiple threat detection technologies that include traditional signature-based or rule-based technology and large-scale threat intelligence data modeling, as well as machine learning-based user behavior analysis. The system provides an ideal solution for detecting advanced threats, including ransomware and crypto-mining malware, and protecting high-value critical servers and sensitive data from being leaked or stolen. Together with deep threat hunting analytical capabilities and visibility, Hillstone BDS provides security admins the effective means to detect IOCs (Indicators of Compromise) events, locate risky hosts and servers, and restore the attack chain. Moreover, it conducts threat and attack mitigation with the conjunction of NGFW, as well as with the integration of Hillstone XDR system iSource. The Hillstone NDR product BDS brings an effective and comprehensive solution to detect and respond to different breeds of network attacks and threats in an enterprise's assets.

Product Highlights

Comprehensive Threat Correlation Analytics for Advanced Threat Detection



Cyber attackers have become ever more sophisticated, using targeted, persistent, stealthy and multi-phased attacks, which can easily evade perimeter detection. Hillstone BDS consists of multiple detection engines focused on different aspects of post-breach threat detection, including advanced malware detection (ATD), abnormal behavior detection (ABD), as well as traditional intrusion detection and virus scanning engines. Hillstone's threat correlation platform analyzes the details of the relationships of each individual suspicious threat event as well as other contextual information within the network, to connect the dots and provide accurate and effective malware and attack detection with high confidence levels.

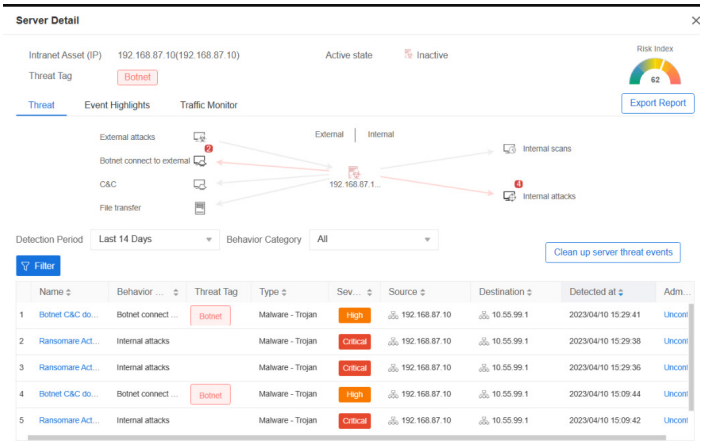
Product Highlights (Continued)

Real-time Threat Monitoring for Critical Servers and Hosts

The Hillstone BDS platform focuses on protecting critical servers within the intranet, detecting unknown and near 0-day threat attacks and finding abnormal network and application level activities of server and host machines. Once a threat or an abnormal behavior is detected, Hillstone BDS will perform threat or behavioral analysis and use topology-based graphic presentations to provide extensive visibility into the threat details and behavioral abnormalities. This gives security admins unprecedented insights into the attack progress, traffic trending in each direction, as well as the entire network risk assessment.

Complete Indicator of Compromises and Cyber Attack Chain

IOCs events are threat events detected during the post breach attack. They are identified among large numbers of the threat attacks in the network that are directly associated with the protected server or host. IOCs are typically seen as threat activities with higher risk and with a high confidence level that a server or host is being compromised and that poses a potentially bigger threat to the critical assets within the corporate network. To effectively detect IOCs and perform deep threat detection on these IOCs is critical in throttling the goal of stealing important data from critical assets, and preventing a threat attack from further spreading within the network. Hillstone BDS drills down and surfaces more threat analysis and intelligence on these IOC events, reconstructing the attack chain based on these IOCs and correlating other threat events associated with these IOCs within time and space spectrums.



Rich Forensic Information and Preemptive Mitigation

The Hillstone BDS platform conducts threat mitigation with conjunction of Hillstone A-Series NGFW, E-Series NGFW, and X-Series data center NGFW devices, which are positioned at the network perimeter. After the security admin or network operators analyze and validate threat alerts, they can add threat elements such as IP addresses, type of threats etc., to the blacklist or security policies, and then synchronize them to the Hillstone firewalls so that future attacks from the same breeds or malware family can be blocked at the network perimeter. This prevents future attacks from spreading to broader network territories.

Features

Abnormal Behavior Detection
- Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM
- Detect DDoS including Flood, Sockstress, zip of death, reflect, DNS query, SSL and application DDoS
- Support inspection of encrypted tunneling traffic for unknown applications
- Real-time, online, abnormal behavior model database update
- Support the detection of RDP/VNC/SMB/SSH/FTP brute force attack, TOR based suspicious HTTP requests

Advanced Threat Detection
- Behavior-based advanced malware detection
- Detect more than 2,000 known and unknown malware families including Virus, Worm, Trojan, Overflow etc
- Real-time, online, malware behavior model database update
- Detect major ransomware and cryptomining malware

Threat Correlation Analytics
- Correlation among unknown threats, abnormal behavior and application behavior to discover potential threat or attacks
- Multi-dimension correlation rules, automatic daily update from the cloud

Deception Threat Detection
- Local deception engine with regular deception models update
- Simulate to Web, Doc or Database Servers, support protocols including FTP, HTTP, MYSQL, SSH and TELNET

Intrusion Detection
- 30,000+ signatures, protocol anomaly detection and rate-based detection
- Custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- Over 20 types of protocols anomaly detection, including HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS, VxLAN, MPLS, etc
- Support for buffer overflow, SQL injection and cross-site scripting attack detection
- Support weak password detection for protocols of FTP/HTTP/SMTP/POP3/IMAP/TELNET

Virus Scan
- Over 13 million virus signature database and online real-time update
- Support compressed file scan

Anti-Spam
- Real-time spam classification and prevention
- Confirmed Spam, Suspected Spam, Bulk Spam, Valid Bulk
- Protection regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Whitelists to allow emails from trusted domain/email addresses

Cloud-Sandbox
- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP, SMTP, POP3, IMAP4 and FTP
- Support file types including PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP
- Provide complete behavior analysis report for malicious files
- Global threat intelligence sharing, real-time threat blocking
- Multiple static detection engines quickly filter normal files and known threats
- Unknown threat visualization based on logs, reports, monitoring information, file behavior reports

Botnet C&C Detection
- Discover intranet botnet host by monitoring C&C connections
- Detect C&C IP and domain name in TCP, HTTP and DNS traffic
- Automatically update the botnet C&C defense signature library

Attack Detection
- Abnormal protocol attack detection
- DoS/DDoS detection, including SYN Flood, DNS Query Flood
- ARP attack detection
- Support WEB attack detection based on WAF rules for abnormal HTTP protocol, DDoS attack, injection attack, cross-site attack, special vulnerability attack, information leakage, detection access, malicious software, illegal access to resources
- WEB detection function whitelist

Application Identification
- Over 4,000 applications, including IM, p2p, file transfer, email, online games, media streaming, etc
- Multi-dimension application statistic based on zones, interface, location, user, and IP address
- Support for Android, IOS mobile applications

Threat Mitigation
- Admin actions to change threat events status, open, false positive, fixed, ignore, confirmed
- One-click cleanup of server/computer threat and reevaluation of host security
- Threat events whitelist, including threat name, source/destination IP, hit count etc.
- Conjunction with Hillstone firewall platforms to block threat
- Sysmon endpoint service integration
- Threat hunting
- Support MITRE ATT&CK framework mapping

ARP Spoofing Detection
- Prevent ARP spoofing by IP-MAC binding and APR packet inspection

Monitoring
- Dynamic, real-time dashboard status and drill-in monitoring widgets
- Intranet risk monitoring projection
- Overview of internal network risk status, including TOP5 risk server/computer list and threat trends, critical assets risk status, host risk status, threat severity and type, external attack geo-locations, etc
- Visual details of threat status for critical assets and other risky hosts, including risk level, risk certainty, attack geo-location, attack chain uncovering and other statistical information
- Support active scanning for assets. The scanning results can be uploaded to iSource
- Visual details of network threat events, including threat analysis, knowledge base, MITRE ATT&CK tactic details, MITRE ATT&CK technique details, history and topology
- Send alarm via Email and Trap
- Cloud-based threat intelligence push service

Logs & Reporting
- Three predefined reports: Security, Flow and System reports
- Support user defined reporting
- Reports can be exported in PDF, Word and HTML format via Email and FTP
- Logs, including events, networks, threats, and configuration logs
- Logs can be exported via Syslog or Email
- Support AV log aggregation and Botnet log aggregation
- Host risk assessment

Administration
- Monitoring internal network hosts and servers, identifying name, operation system, browser, type, and network threat statistic record
- Management access: HTTP/HTTPS, SSH, telnet, console
- Device condition alerts, including CPU usage, memory usage, disc usage, new session and concurrent sessions, interface bandwidth, chassis temperature and CPU temperature
- Alerts based on application bandwidth and new connection
- Support for three types of alerts: email, text message, trap
- Language support: English

Centralized Management
- Register devices to Hillstone Security Management Platform (HSM)
- Monitor multiple devices status, traffic and threat via cloud with 24/7 access from web or mobile application (CloudView)
- Upload threat logs, evidential packets, NetFlow, metadata to iSource for threat analysis
- Support third-party threat Intelligence for detecting malicious files, URL and IP addresses

Features

RESTful APIs

- Support standard RESTful APIs for accessing hardware/system/threat event information
- Seamless integration with 3rd party network management system

Specifications

	I-1850-IN	I-1870-IN	I-2860-IN
			
Breach Detection Throughput [1]	1 Gbps	1 Gbps	2 Gbps
New Sessions/s [2]	20,700	32,000	75,000
Maximum Concurrent Sessions [2]	750,000	750,000	1.5 Million
Form Factor	1 U	1 U	1 U
Storage	1T HDD	1T SSD	1T 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
Fixed I/O Ports	4 x GE	2 × SFP+ 8 × SFP 8 × GE	2 × SFP+ 8 × SFP 16 × GE
Available Slots for Expansion Modules	1 x Generic Slot	0	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP-L-IN	N/A	IOC-A-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	60W, Single AC	50W, Single AC	100W, Dual AC Redundant
Dimension (W×D×H, mm)	16.9 x 11.8 x 1.7 in (430 x 300 x 44mm)	17.2 x 12.6 x 1.7 in (436 x 320 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Weight	8.8lb (4 kg)	9 lb (4.1 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)
Relative Humidity	5-85% (no dew)	10-95% (no dew)	10-95% (no dew)

	I-3860-IN	I-5850-IN	I-5860-IN
			
Breach Detection Throughput [1]	5 Gbps	10 Gbps	10 Gbps
New Sessions/s [2]	210,000	250,000	500,000
Maximum Concurrent Sessions [2]	3 Million	6 Million	6 Million
Form Factor	1 U	2 U	1 U
Storage	1T SSD	1T HDD	2T SSD
Management Ports	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	6 × SFP+ 16 × SFP 8 × GE	N/A	2 × QSFP+ 16 × SFP+ 8 × GE
Available Slots for Expansion Modules	1 x Generic Slot	4 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-A-4SFP+-IN	IOC-BDS-8GE-H-IN, IOC-BDS-8SFP-H-IN, IOC-BDS-4SFP+-H-IN	IOC-A-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100 -240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	289W, Dual AC Redundant	350W, Dual AC Redundant	382W, Dual AC Redundant
Dimension (W×D×H, mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	16.9 x 19.7 x 3.5 in (430 x 500 x 88mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Weight	22.5 lb (10.2 kg)	26.5 lb (12 kg)	22.5 lb (10.2 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	5-85% (no dew)	10-95% (no dew)

Specification and Minimum Hardware Configuration

	IV04-IN	IV08-IN
Breach Detection Throughput [3]	Up to 1.5 Gbps	Up to 3 Gbps
CPU Support (Min.)	4 Core	8 Core
Memory (Min.)	8G	16G
Storage (Min.)	100G	100G
System Requirement	KVM / Vmware ESXi version 6.5 or above	KVM / Vmware ESXi version 6.5 or above

Network Interface Card Supported

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

Module Options

Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN
I/O Ports	4 x SFP Ports	4 x GE Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.22 lb (0.1 kg)	0.33 lb (0.15 kg)

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

Recommended Sysmon Configuration

Specification	Sysmon Server	Sysmon Client
CPU	4 Core	\
Memory	16G	1G
Storage	1T HDD, extendable	40G HDD
Installation Package	OVF Mirror	MSI Service Program
System Requirement	VMware ESXi	Windows 7 / Windows Server 2008 or above

NOTES:

(1) Breach detection throughput is obtained under bi-direction HTTP traffic detection with all threat detection features enabled;

(2) The data is obtained when the WEB attack detection function is turned off. Performance may vary if it's turned on;

(3) The breach detection throughput data is depends on the hardware configuration;

Version:EX-08.01-BDS-V3.7-0523-EN-01