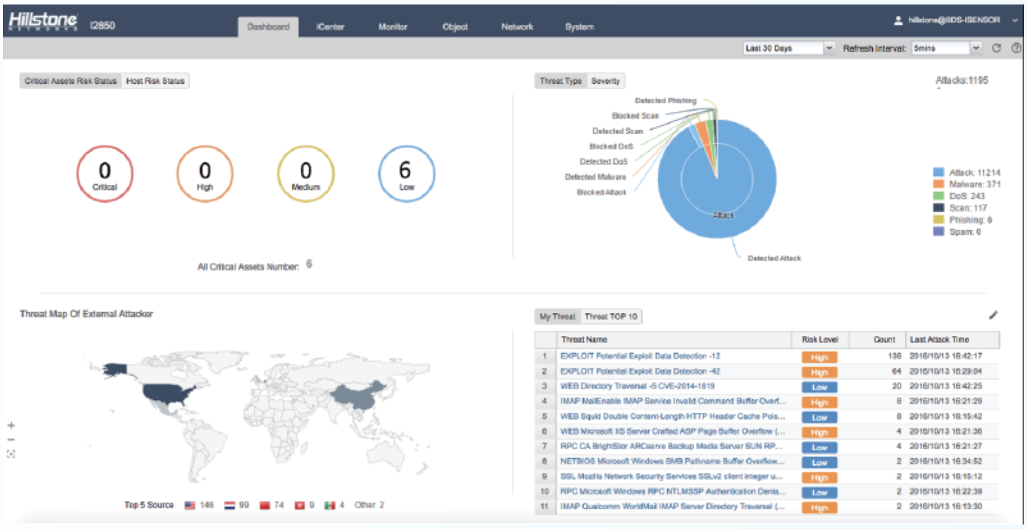
Hillstone I-Series
Server Breach Detection System(sBDS)

I-2850

The Hillstone sBDS solution is a key component of Hillstone’ s Intranet security portfolio, protecting critical assets such as servers, and leveraging Hillstone’ s unique behavior-based threat detection technology to detect compromised hosts and threats within the intranet. Deployed in front of critical servers, Hillstone sBDS monitors server behavior and establishes a behavioral baseline. When the pattern changes, the advanced behavior detection engine alerts the other parallel engines of the event, where it is quickly pinpointed, characterized, and the IT security team is notified of the action with all of the pertinent information. The Hillstone sBDS solution is often tapped into an enterprise internal network traffic, and complement existing perimeter protection, such as Next-Generation Firewall (NGFW) and Network Intrusion Prevention System (NIPS).

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 sBDS consists of multiple detection engines focused on different aspects of post-breach threat detection, including advanced malware detection based on patented machine learning algorithms; abnormal behavior detection engines; malicious files identification via cloud sandbox service, as well as traditional intrusion detection and virus scanning engines. Hillstone’s threat correlation engine analyzes the details of the relationships of each individual suspicious threat event as well as other contextual information within the network, in order to connect the dots and provide accurate and effective malware and attack detection with high confidence levels.

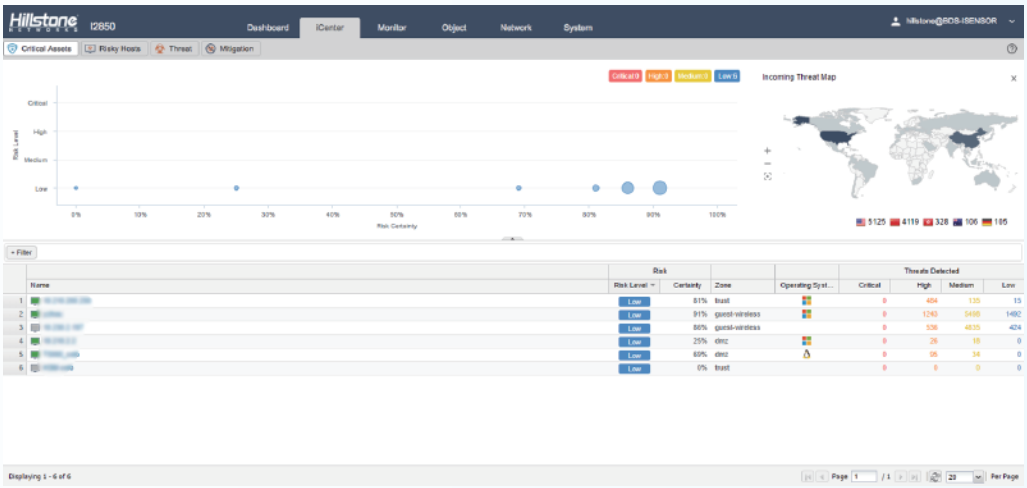


	Threat Name	Risk Level	Count	Last Attack Time
1	EXPLOIT Potential Exploit Data Detection -12	High	136	2016/10/13 16:42:17
2	EXPLOIT Potential Exploit Data Detection -42	High	64	2016/10/13 16:29:04
3	WEB Directory Traversal -5 CVE-2014-1619	Low	20	2016/10/13 16:42:25
4	IMAP MailEnable IMAP Service Invalid Command Buffer Overf...	High	8	2016/10/13 16:21:29
5	WEB Squid Double Content-Length HTTP Header Cache Pois...	Low	8	2016/10/13 16:15:42
6	WEB Microsoft IIS Server Crafted ASP Page Buffer Overflow (...	High	4	2016/10/13 16:21:36
7	RPC CA BrightStor ARCserve Backup Media Server SUN RP...	Low	4	2016/10/13 16:21:27
8	NETBIOS Microsoft Windows SMB Pathname Buffer Overflow...	Low	2	2016/10/13 16:34:52
9	SSL Mozilla Network Security Services SSLv2 client integer u...	High	2	2016/10/13 16:15:12
10	RPC Microsoft Windows RPC NTLMSSP Authentication Denia...	Low	2	2016/10/13 16:22:39
11	IMAP Qualcomm WorldMail IMAP Server Directory Traversal (...	High	2	2016/10/13 16:13:30

Figure 1. Hillstone sBDS I-2850 Dashboard

Real-time risk monitoring for internal networks and critical assets

As network boundaries have become more blurred with the adoption of cloud platforms and Bring Your Own Device (BYOD) in the workplace, enterprise network assets have become more vulnerable, especially those defined as “Critical Assets.” Critical assets include servers, network and storages devices that are critical to business operations, and which also happen to be the priority targets for hackers. Because of this, critical assets need more granular monitoring than non-critical assets. HIllstone sBDS allows admins to define critical assets based on their business operation priority, inspect all traffic that pass through the assets with advanced threat detection functions, and show risk and threat details for each critical asset.



	Name	Risk Level	Certainty	Zone	Operating Syst...	Critical	High	Medium	Low
1	[redacted]	Low	81%	trust		0	484	135	15
2	[redacted]	Low	91%	guest-wireless		0	1240	5498	1492
3	[redacted]	Low	86%	guest-wireless		0	536	4835	424
4	[redacted]	Low	25%	dmz		0	26	18	0
5	[redacted]	Low	69%	dmz		0	95	34	0
6	[redacted]	Low	0%	trust		0	0	0	0

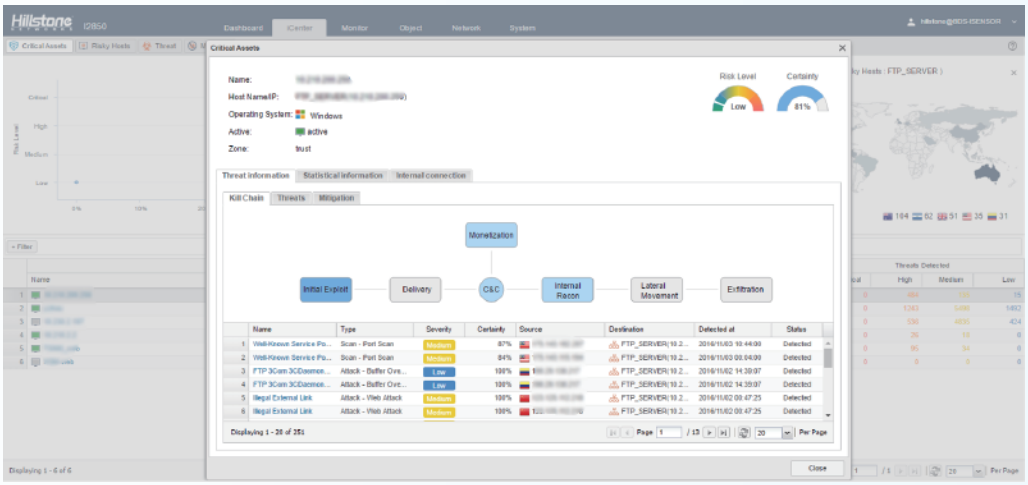
Displaying 1 - 6 of 6

Page 1 / 1 | 20 | Per Page

Figure 2. Threat Detection for Critical Assets

Full life cycle threat visibility and insight through the cyber kill chain

Sophisticated attackers use various methods that include exploiting zero day vulnerabilities, using modified malware, customizing threat tools, employing anti-sandboxing techniques to escape perimeter detection. However, with Hillstone – beyond just detecting the threat – BDS maps the threat events to the cyber kill chain (CKC) model and provides deep insights into the post-breach threat attack path inside the compromised network. Security administrators can understand more about each stage of the attack and take proper action to stop exfiltration of sensitive data from the internal network.



Name: [redacted]

Host Name/IP: [redacted]

Operating System: Windows

Active: active

Zone: trust

	Name	Type	Severity	Certainty	Source	Destination	Detected at	Status
1	Well-Known Service Po...	Scan - Port Scan	Medium	87%	[redacted]	FTP_SERVER(10.2...	2016/11/03 10:44:00	Detected
2	Well-Known Service Po...	Scan - Port Scan	Medium	84%	[redacted]	FTP_SERVER(10.2...	2016/11/03 00:04:00	Detected
3	FTP 3Com 3CDaemon...	Attack - Buffer Ove...	Low	100%	[redacted]	FTP_SERVER(10.2...	2016/11/02 14:39:07	Detected
4	FTP 3Com 3CDaemon...	Attack - Buffer Ove...	Low	100%	[redacted]	FTP_SERVER(10.2...	2016/11/02 14:39:07	Detected
5	Illegal External Link	Attack - Web Attack	Medium	100%	[redacted]	FTP_SERVER(10.2...	2016/11/02 00:47:25	Detected
6	Illegal External Link	Attack - Web Attack	Medium	100%	[redacted]	FTP_SERVER(10.2...	2016/11/02 00:47:25	Detected

Displaying 1 - 20 of 251

Page 1 / 13 | 20 | Per Page

Figure 3. Kill Chain mapping of post-breach threats

Deployment Scenario

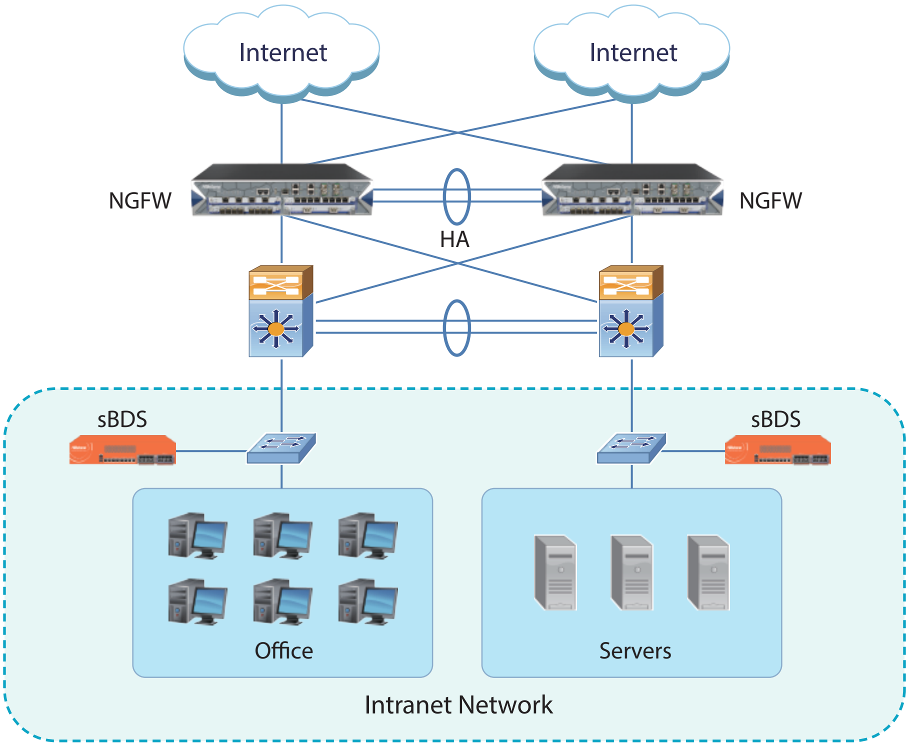


Figure 4. Hillstone sBDS deployment scenarios

Core Features

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

Advanced Threat Detection

- Behavior-based advanced malware detection
- Detection of More than 2000 known and unknown malware families including Virus, Worm, Trojan, Overflow etc
- Real-time, online, malware behavior model database update

Abnormal Behavior Detection

- Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM, SSH/FTP weak password
- Detection of DDoS including Flood, Sockstress, zip of death, reflect, DNS query, SSL and application DDoS
- Supports inspection of encrypted tunneling traffic for unknown applications
- Real-time, online, abnormal behavior model database update

Intrusion Detection

- 8000+ 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, etc
- Support for buffer overflow, SQL injection and cross-site scripting attack detection

Virus Scan

- 4 Million virus signature database
- Online real-time updates
- Compressed file scans

Application identification

- Over 3000 applications, including IM, p2p, email, 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

Monitoring

- Dynamic, real-time dashboard status and drill-in monitoring widgets

- Overview of internal network risk status, including 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 host, including risk level, risk certainty, attack geo-location, kill chain mapping and other statistical information
- Visual details of network threat events, including name, type, threat severity and certainty, threat analysis, knowledge base and history

Logs & Reporting

- Three predefined reports: Security, Flow and System reports
- Support user defined reporting
- Reports can be exported in PDF via Email and FTP
- Logs, including events, networks, threats, and configuration logs
- Logs can be exported via Syslog or Email

Administration

- 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

Product Specification

Model	I-2850
Breach Detection Throughput[1]	2Gbps
Maximum Concurrent Connections (HTTP)[2]	1.5 Million
New Sessions/s (HTTP)[3]	20,000
Form Factor	1 U
Storage	1T HDD
Management Ports	2 x USB Port, 1 x RJ45 port, 2 x MGT
Fixed I/O Ports	4 x GE
Available Slots for Extension Modules	1 x Generic Slot
Expansion Module Option	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-2SFP+, IOC-S-4SFP+
Power Supply	AC 100-240V 50/60Hz
Maximum Power Consumption	250 W
Dimension (W×D×H, mm)	16.9 x 11.8 x 1.7 in (430 x 300 x 44mm)
Weight	15.4 lb (7 kg)
Temperature	32-104 F (0-40°C)
Relative Humidity	5-85% (no dew)

Module Options

Module	IOC-S-4GE-B	IOC-S-4SFP	IOC-S-8GE-B	IOC-S-8SFP	IOC-S-4GE-4SFP	IOC-S-2SFP+	IOC-S-4SFP+
I/O Ports	4 x GE Bypass Ports	4 x SFP Ports	8 x GE Bypass Ports	8xSFP	4XFP Extension Module	8SFP+ Extension Module	4GE PoE Extension Module
Dimension	1U	1U	1U	1U	1U	1U	1U
Weight	0.33 lb (0.15kg)	0.33 lb (0.15kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.33 lb (0.15kg)	0.44 lb (0.2kg)

NOTES:(1) Breach Detection Throughput is obtained under bi-direction HTTP traffic detection with all threat detection features enabled. (2) Maximum Concurrent Connections are obtained under HTTP traffic. (3) New Sessions are obtained under HTTP traffic.