iNFOTECT

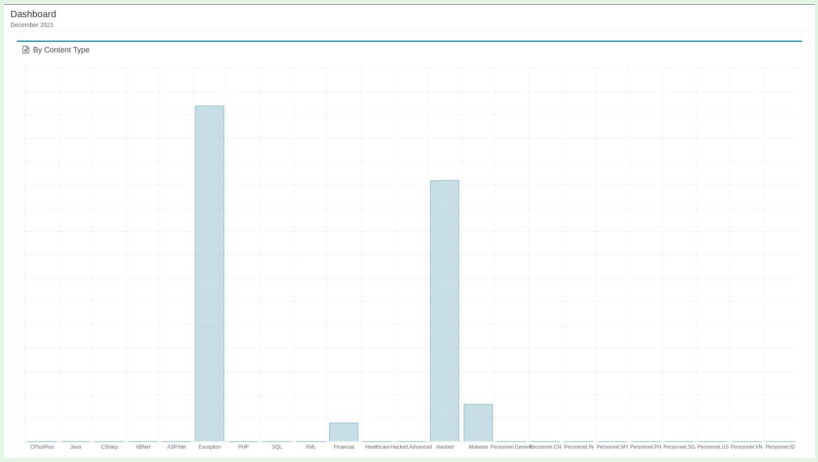
iNSIGHT FOR WEB SERVER

IWS Series 5300 /5200 /5100 Data Sheet

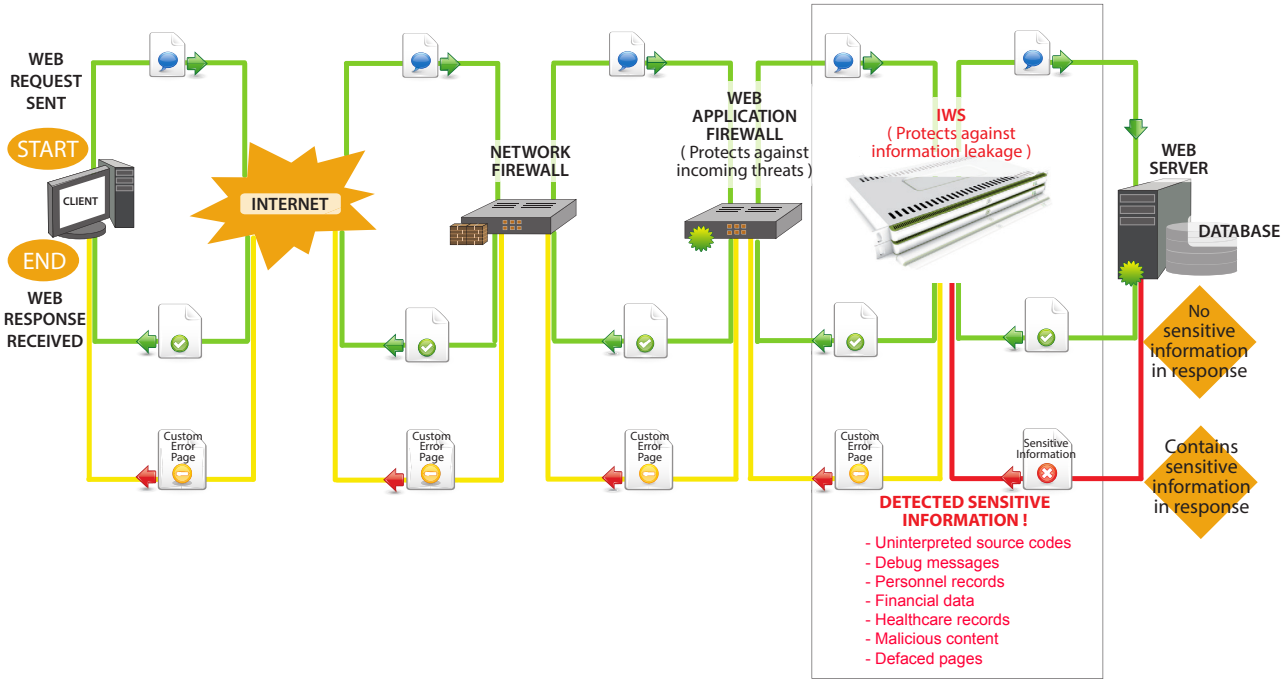
iNSIGHT For Web Server (“IWS”)

is an Outbound Security appliance for cloud and web services, built on patented technologies. IWS complements your existing network security peripherals by offering outbound protection for your cloud and web services.

iNSIGHT For Web Server ("IWS") provides real-time detection and prevention capabilities to protect against information leakage and malware propagation via outgoing web server traffic.



HOW IWS WORKS



Protection Against These Outbound Risks for Cloud and Web Services:

Compromised Web Servers
Web servers infected by computer worm, Trojan horse or virus can cause information to be leaked out.

Vulnerabilities In Web Applications
Poorly written applications can result in more information than necessary being shown.

Server Errors
Malfunctioned or misconfigured web servers can display too much information.

Sensitive Information Left On Web Servers
Backup copies of source code, SQL files, CSV files containing customer records can be left on web servers.

Disclosure Of Website Defacement
Defaced web pages can be prevented from being displayed to the public.

Transmission of Malware
Compromised websites can trick innocent web visitors into clicking malicious links.

BETTER COMPLIANCE FOR REGULATIONS

1	European Union Data Protection Directive - Security Safeguards Principle 11
2	Sarbanes-Oxley Act (2002)
3	HIPAA (1996)
4	Gramm-Leach Bliley Act (GLBA)
5	California SB 1386 (2003)
6	Japan's Personal Information Protection Act
7	UK's Data Protection Act
8	Singapore's & Malaysia's Data Protection Act

BETTER PROTECTION FOR WEB APPLICATIONS

A2	**Injection Flaws** IWS can protect against SELECT SQL injection flaws which may result in leakage of sensitive information stored in databases.
A4	**Insecure Direct Object Reference** IWS can protect against unwanted direct object references, such as a file, directory, database record, or key, as a URL or form parameter.
A6	**Information Leakage And Improper Error Handling** IWS can protect against application loopholes that unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems.
A8	**Insecure Cryptographic Storage** IWS can protect against leakages of information, such as credit card numbers, if not properly encrypted or masked.
A10	**Failure To Restrict URL Access** IWS can protect against leakages of information through unwanted direct URL accesses by hackers.

Based on Open Web Application Security Project (OWASP) Top 10 items: *http://www.owasp.org/index.php/Top_10_2007*

MAXIMUM SECURITY WITH HIGH PERFORMANCE

1	Web proxy cache reduces frequency of scanning and analysing identical non-sensitive server responses
2	Multi-threaded processing
3	Bypass lower-risk CSS, image, multimedia, Flash files and whitelisted request URLs
4	No need to scan entire file content in order to detect sensitive information

HIGH ACCURACY USING PATENTED TECHNOLOGIES

1	**Content Dissection Reduces False Negatives** IWS dissects HTTP responses from web servers into chunks for further analysis. This prevents IWS from being misled by small amounts of sensitive data hidden among large amounts of non-sensitive data.
2	**Use Of Highly Accurate Proprietary Content Identifiers** Many man hours are invested by our R&D team in analysis and selection of proprietary identifiers for each content type – source code, personnel, financial and medical. For instance , IWS has overcome the challenge of identifying source code from normal English text messages though both are written in English.
3	**Materiality-based Algorithm Reduces False Positives** IWS is able to assess the context and decide whether the detected sensitive data is material enough to warrant further attention. For instance, a single occurrence of source code identifier may not be material enough to warrant attention, but a single occurrence of personnel ID may be one too many and deserves further attention.

	IWS 5300 Series	IWS 5200 Series		IWS 5100 Series	
	5350	5255	5250	5155	5150
Capabilities					
Inline Interception	Yes	Yes	Yes	Yes	Yes
Out-of-band Monitoring	Yes	Yes	Yes	Yes	Yes
Source Code Detection	Yes	Yes	Yes	Yes	Yes
Personnel Info Detection	Yes	Yes	Yes	Yes	Yes
Financial Info Detection	Yes	Yes	Yes	Yes	Yes
Medical Info Detection	Yes	Yes	Yes	Yes	Yes
Malware Containment	Yes (Optional add-on)	Yes (Optional add-on)		Yes (Optional add-on)	
High Availability	Yes	Yes	Yes	Yes	Yes
Load Balancing	Yes	Yes	Yes	Yes	Yes
Custom Editor	Yes	Yes	Yes	Yes	Yes
Protocol Support					
HTTP	Yes	Yes	Yes	Yes	Yes
Performance					
Maximum Throughput*	7Gbps (fiber)	1.4Gbps (fiber)	700Mbps	350Mbps	70Mbps
Bundled Host Licenses	Unlimited	Up to 5	Up to 5	Up to 2	Up to 2
Physical					
Form Factor	4U	1U	1U	1U	1U
Dimensions	Height: 6.8"(17.26 cm) Width: 19" (48.3 cm) Depth: 31.59" (80.23 cm)	Height: 1.7" (4.28 cm) Width: 19" (48.3 cm) Depth: 23.9" (60.7 cm)		Height: 1.7" (4.28 cm) Width: 19" (48.3 cm) Depth: 23.9" (60.7 cm)	
Weight	130.0 lbs (59 kg)	44.09 lbs (20 kg)		44.09 lbs (20 kg)	
Architecture					
CPU	96 Cores	22 Cores	16 Cores	12 Cores	8 Cores
Interfaces					
Ethernet	2 x 10 Gbps (fiber) 4 x 1Gbps	2 x 10Gbps (fiber) 4 x 1Gbps	6 x 1Gbps	4 x 1Gbps	4 x 1Gbps
Environmental					
AC Power	2 x 1100W Dual redundant, Hot-Swappable Power Supply	2 x 550W Dual redundant, Hot-Swappable Power Supply		2 x 550W Dual redundant, Hot-Swappable Power Supply	
Operating Temperature	5° to 32°C (41° to 90°F)	5° to 31°C (41° to 88°F)		5° to 35°C (41° to 95°F)	

*for inline HTTP protection mode only
For inline HTTPS protection mode, throughput is 20% of maximum throughput.

CONTACT US | INFOTECT SECURITY PTE LTD

Address: 11 Irving Place, #07-01 Tai Seng Point Singapore 369551

Main Line: (65) 6242-6478

Email: enquiry@infotectsecurity.com

www.infotectsecurity.com