



POWERFUL MALWARE  
PROTECTION ENABLES  
THE INDUSTRY'S MOST  
COMPREHENSIVE  
PERIMETER DEFENSE

## IronPort S-Series Web Security Appliances

### OVERVIEW

#### SECURE AND CONTROL WEB TRAFFIC WITH THE INDUSTRY'S LEADING WEB SECURITY APPLIANCE

Web traffic is now a major threat distribution vector, with clear and present risks. Existing gateway defenses are proving to be inadequate against a variety of Web-based malware, leaving corporate networks exposed to the inherent danger posed by these threats. According to industry estimates, approximately 75 percent of corporate PCs are infected with spyware, yet less than 10 percent of corporations have deployed perimeter malware defenses. The speed, variety and maliciousness of Web-based malware attacks highlight the importance of a robust, secure platform to protect the enterprise network perimeter from such threats.

Existing gateway defenses are proving to be inadequate against a variety of Web-based malware. Only the *IronPort S-Series* Web security appliance provides a single platform solution to enable the industry's most powerful protection and control.



In addition to the security risks introduced by Web-based malware and spyware, Web traffic also exposes an organization to compliance and productivity risks introduced by inappropriate usage of the Web within an organization.

The *IronPort S-Series Web Security Appliance* is the industry's first and only Web security appliance to combine traditional URL filtering, reputation filtering and malware filtering on a single platform to address these risks. By combining these innovative technologies, the *IronPort S-Series* helps organizations address the growing challenges of both securing and controlling Web traffic.

Customers enjoy low Total Cost of Ownership (TCO), as these powerful applications are integrated and managed on a single appliance. Robust management and reporting tools deliver ease of administration, flexibility and control, and complete visibility into policy-related and threat-related activities.



## FEATURES

### INNOVATIVE SECURITY PLATFORM DELIVERS INDUSTRY-LEADING PERFORMANCE AND ACURACY

*IronPort S-Series* appliances help enterprises secure and control Web traffic by combining a secure application proxy for Web traffic, a Layer 4 (L4) Traffic Monitor, and the *IronPort Dynamic Vectoring and Streaming (DVS) engine™* — a sophisticated scanning and vectoring engine that has been designed from the ground up to address the unique challenges posed by scanning Web transactions and objects. This provides a powerful Web security platform, optimized for performance and efficacy.

**A fast Web proxy** provides control over all Web traffic and allows for deep content analysis, which is critical to accurately detect devious and rapidly mutating Web-based malware. The industry's first implementation of reputation-based caching enables fast delivery of safe objects and content to the end-user. Powered by *AsyncOS™*, IronPort's proprietary operating system, the Web proxy easily ensures high performance and throughput for even the largest of networks.

**An integrated Layer 4 (L4) Traffic Monitor** scans all ports at wire speed, detecting and blocking spyware “phone-home” activity. By tracking all 65,535 network ports, the L4 Traffic Monitor effectively stops malware that attempts to bypass Port 80 and also prevents rogue P2P- and IRC-related activity.

**IronPort's DVS Engine** employs sophisticated object parsing and vectoring techniques, along with stream scanning and verdict caching, resulting in up to ten times the scanning throughput of first-generation solutions.

### MULTI-LAYER, MULTI-VENDOR DEFENSE-IN-DEPTH

**IronPort URL Filters™** offer the broadest reach and the highest accuracy rate in controlling Web content. These filters compare users' Web traffic requests against administrator-set policies for 52 pre-defined (and an unlimited number of custom) categories, easily addressing acceptable use policy concerns.

With a database that contains more than 20 million sites (corresponding to over 3 billion webpages) and global coverage across 70 languages and 200 countries, *IronPort URL Filters* offer industry-leading coverage and accuracy against Web traffic requests.

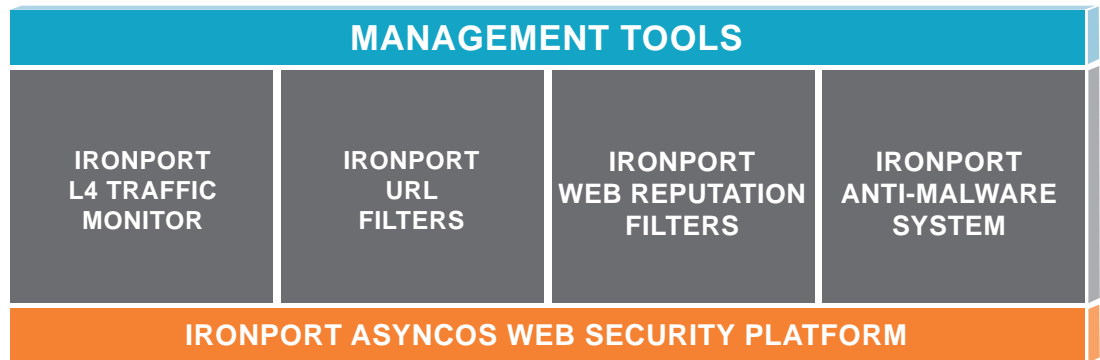
**The industry's first Web reputation filters** provide a powerful outer layer of defense. Leveraging *SenderBase®*, *IronPort Web Reputation Filters™* analyze over 50 different Web traffic and network-related parameters to accurately evaluate a URL's trustworthiness. Sophisticated security modeling techniques are used to individually weigh each parameter and generate a single score on a scale of -10 to +10. Administrator configured policies are dynamically applied, based on reputation scores.

**The industry-leading IronPort Anti-Malware System™** leverages the *IronPort DVS engine* and multiple verdict engines (the first from Webroot), to provide best-of-breed protection against the widest variety of Web-based threats. These threats can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and keyloggers.



**FEATURES**  
(CONTINUED)

**Power at the Perimeter:**  
The *IronPort S-Series* combines revolutionary technologies to provide multi-layered Web security on a single appliance.



**The IronPort DVS engine** was built to provide an integrated single-appliance solution matching against multiple signature types from different vendors. The first set comes from Webroot, an industry-leading anti-malware company. Webroot’s Threat Research team is backed by Phileas, the first automated spyware detection system, which identifies existing and new threats by intelligently scanning millions of sites daily. *IronPort S-Series* appliances are the first to include Webroot’s award-winning technology at the gateway perimeter to keep these threats from entering the network.

**COMPREHENSIVE MANAGEMENT AND REPORTING CAPABILITIES**

**IronPort Web Security Manager™** enables unified policy creation for all filtering services on the appliance and provides

granular options for the enterprise based on authenticated or non-authenticated users.

Administrators manage all Web access policies (including those for URL filtering, reputation filtering and malware filtering) from a single location. Administrators create and manage groups and users for all filtering services on the appliance.

**IronPort Web Security Monitor™** provides valuable insight into overall Web activity, as well as threat identification and prevention, within corporate networks. These on-box and off-box reports are designed to provide actionable information as well as historical trends. Enhanced reporting provides enterprises visibility into policy violations and security violations.

**Web Filtering Policies**

Order	Group	Applications	URL Categories	Objects	Anti-Malware	Delete
1	QA	Block: FTP Block: User Agents	Block: 52 Monitors: 2 Allow: 0	Block: 256 Mb	(global policy)	🗑️
2	Engineering	Block: User Agents	Block: 80 Monitors: 2 Allow: 2	Block: No Max Size Block: Object Types Block: File Types	(disabled)	🗑️
3	Marketing	(disabled)	Block: 60 Monitors: 2 Allow: 2	Block: No Max Size Block: Object Types	Block: 11 Monitors: 2	🗑️
4	Dev	(global policy)	Block: 50 Monitors: 2 Allow: 2	Block: No Max Size	(global policy)	🗑️
	Global Policy	Block: FTP, HTTPS Allow: HTTP Block: User Agents Allow: Ports 443, 21	Block: 48 Monitors: 8 Allow: 0	Block: 256 Mb Block: Object Types Block: File Types	Block: 13 Monitors: 0	

Key: Global Disabled  
? Authentication

**Group by LDAP, AD, Network**

- Block FTP
- Allow Media files
- Allow all URL categories
- Block executables
- Block gambling sites
- Block all malware
- Allow Skype
- Monitor all traffic
- Allow executables
- Allow all applications



**FEATURES**  
(CONTINUED)

The *IronPort S-Series*' sophisticated reporting tools yield a complete real-time and historical view of Web traffic, as well as threat activity and prevention — providing unprecedented security insight.



**Multiple deployment modes** enable flexibility within a corporate network. Deployment modes include deployment as an explicit forward proxy for the network or transparent deployment off an L4 switch or a WCCP router within the network. The *IronPort S-Series* appliance can be configured as a standalone proxy or to co-exist with other proxies.

**An SNMP Enterprise MIB** facilitates hands-off monitoring and alerting for key system metrics including hardware, performance and availability. A comprehensive enterprise class alert engine ensures oversight for all system parameters – including hardware, security, performance and availability.

**Integrated authentication** via standard directories (such as LDAP or Active Directory) and the ability to implement multiple

authentication schemes (such as NTLM or Basic) lets enterprises deploy the *IronPort S-Series* seamlessly, while taking advantage of pre-existing authentication and access control policies within their networks.

**Extensive logging** allows enterprises to keep track of all Web traffic, benign and malware-related. Standard log formats include Apache, Squid or Squid-detailed—along with the ability to specify custom log formats, consistent with enterprise logging policies. Administrators can enable or disable log subscriptions or set log subscriptions, or set log rollover and size limits, based on log types.



## BENEFITS

### Single Appliance Security and Control

*IronPort S-Series* offers a single appliance solution to secure and control the three greatest Web traffic risks facing enterprise networks: security risks, resource risks and compliance risks.

**Mitigate Malware Risks and Costs** With malware infecting up to 75 percent of corporate desktops, there is considerable overhead around managing infected desktops, ensuring minimal downtime to the end-user and minimizing the risk of information leakage.

By stopping these threats at the network perimeter with the *IronPort S-Series*, enterprises can significantly reduce the administrative costs, prevent attacker “phone-home” activity on networks, reduce support calls, enhance worker productivity and also eliminate the business exposure that accompanies these threats.

**Complete, Accurate Protection** IronPort® designed the *IronPort S-Series* appliances from the ground up to address the broadest range of Web-based malware threats. A multi-layered defense that includes *IronPort URL Filters*, *IronPort Web Reputation Filters*, and multiple types of malware signatures within *IronPort’s DVS engine*, ensures industry-leading accuracy.

The *IronPort S-Series’* multi-layered protection is based on a deep content application-layer inspection, as well as network-layer pattern detection, checking both inbound and outbound activities. These innovations result in the *IronPort S-Series* appliances protecting with the industry’s most accurate anti-malware solution.

### Implement Acceptable Use Policies (AUP)

By implementing acceptable use Web policies, enterprises have the opportunity to monitor activities, but also generate awareness and increase education as to the risks being avoided with policies. Enterprises can increase the amount of time employees work on business-oriented activities, reducing misuse of enterprise networks and bandwidth.

**Comprehensive Visibility** The *IronPort S-Series* appliances deliver real-time and historical security information, enabling administrators to quickly understand Web traffic activity. Real-time reports let administrators identify and track issues such as policy violations and security violations as they occur. Historical reports allow administrators to identify trends and report on efficacy and ROI.

**Enterprise-Scale Performance** Real-time scanning of Web traffic has been traditionally plagued by poor performance and high latency. Consequently, enterprises have shied away from deploying signature-based protection at the HTTP layer. *IronPort S-Series* appliances scale to meet the unique scanning needs of Web traffic, thereby ensuring that the end-user experience is maintained. IronPort’s performance focus (with technical innovations in *AsyncOS*, which includes TCP connection management, reputation-based caching and adaptive object storage) ensures a platform that can address the capacity requirements of even the largest of enterprises.

**Low Total Cost of Ownership** Legacy ICAP-based solutions typically require multiple appliances or servers to address securing and controlling Web traffic against security,



**BENEFITS**  
(CONTINUED)

resource and compliance risks. Unlike other solutions, the *IronPort S-Series* provides a single platform that contains a complete, in-depth defense — along with all the necessary management tools — significantly reducing initial and ongoing TCO.

and management with an intuitive graphical user interface, support for automated updates, and comprehensive monitoring and alerting. The solution is also easy to deploy and configure to match corporate-specific policies.

**Reduced Administrative Overhead** Designed to minimize administrative overhead, the *IronPort S-Series* appliances offer easy setup

**PRODUCT LINE**

**-sizing up your web security solution**

IronPort Systems provides industry-leading Web security appliances for organizations of all sizes.

<b>IronPort S650</b>	Designed to meet the needs of the most demanding networks in the world. Suggested for organizations above 5000 users.
<b>IronPort S350</b>	Suggested for organizations up to 5000 users.

**SPECS**  
(MODEL DEPENDENT)

**CHASSIS / PROCESSOR**

Form Factor	19" Rack-Mountable, 2U rack height
Dimensions	3.5" (h) x 19" (w) x 29" (d)
CPU	2x Dual Core Intel Xeon 5140, 4 MB Cache
Memory	4 GB
Power Supplies	Hot-plug redundant, 750 watts, 100/240 volts

**STORAGE**

RAID	RAID 10 configuration, battery-backed 256MB cache
Drives	Six hot-swappable, 146 GB SAS Drives, 876 GB Total

**CONNECTIVITY**

Ethernet	6x Gigabit NICs, RJ-45
Serial	1x RS-232 (DB-9) Serial Port

**INTERFACES/CONFIGURATION**

Web Interface	Accessible by HTTP or HTTPS
Command Line Interface	Accessible via SSH or Telnet; Configuration Wizard or command-based
File Transfer	SCP, FTP or SYSLOG
Configuration Files	XML-based configuration files



## SUMMARY

### THE ULTIMATE WEB SECURITY SYSTEM

The challenges of securing and controlling enterprise Web traffic is continually growing and changing. The security risk is real, with Web-based malware a rapidly growing threat that is responsible for significant corporate downtime, productivity losses and major strains on IT resources. Enterprises need control to understand when, where and how their employees are using the Web. Additionally, an enterprise runs the risk of violating compliance and data privacy regulations if their networks become compromised. The legal exposure as a result of these violations comes at a significant cost. Malware infections also risk exposing an organization's business-critical data and intellectual property assets.

The best place to control and protect against these risks posed by Web traffic is right at the gateway. Combining Web traffic policies with deep application content inspection, through a Web proxy and Layer 4 Traffic Monitor, allows enterprises to ensure breadth of coverage within their networks. *IronPort Web Reputation Filters* and multiple malware signatures from Webroot, integrated within IronPort's *DVS Engine* and *IronPort URL Filters*, provide industry-leading accuracy against suspicious Web traffic. With threats becoming more complex and sophisticated, *IronPort S-Series* offer the industry's most comprehensive Web security solution — while also ensuring enterprise-class performance.

## CONTACT US



### TAMIL NADU:

**Dynamic Computer Services**  
Head Office:  
"Sun Flower" # 355 Lloyds Road  
Gopalapuram, Chennai - 600086  
State of Tamil Nadu, INDIA

Phone: (044).2811.3070  
Mobile Phone: +91.98408.65098  
Fax: (044).2811.3073

### KARNATAKA:

**Dynamic Computer Services**  
Regional Office:  
# 57, 17th "A" Main, HAL II Stage  
Bangalore - 560008  
State of Karnataka, INDIA

Phone: (080).2526.3594  
Mobile Phone: +91.98408.65098  
Fax: (080).2526.0315

Sales: info@dynamicgroup.in  
Support: support@dynamicgroup.in

www.dynamicgroup.in

## HOW TO GET STARTED WITH IRONPORT

IronPort sales representatives, channel partners and sales engineers are ready to help evaluate how IronPort products can make your corporate network infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from IronPort's industry-leading products, please call 650-989-6530 or visit us on the Web at [www.ironport.com/leader](http://www.ironport.com/leader)



### IronPort Systems, Inc.

950 Elm Avenue, San Bruno, CA 94066  
TEL 650.989.6500 FAX 650.989.6543  
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use — providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

Copyright © 2007 IronPort Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of IronPort Systems, Inc. All other trademarks are the property of IronPort Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, IronPort does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 435-0120-3 2/07

