

# Overview

## IRONPORT Web Security Monitor

INSTANTLY ASSESS AND  
PROTECT AGAINST A RANGE  
OF WEB SECURITY THREATS.

### OVERVIEW

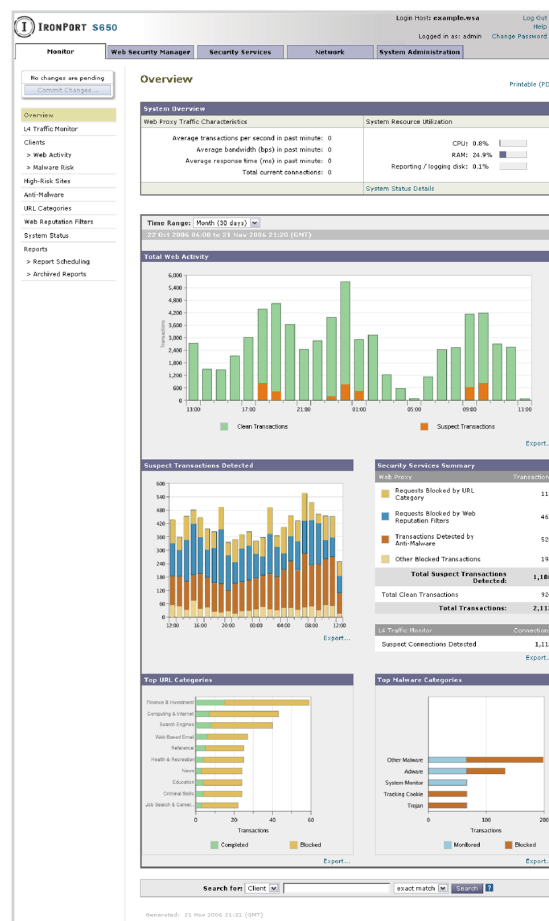
Securing and controlling your network to maximize employee and network resource utilization while protecting against a broad range of spyware and other Web-based malware requires a robust and secure Web security platform, capable of providing accurate information and constant feedback. *IronPort S-Series*™ Web security appliances incorporate real-time monitoring and reporting capabilities — providing administrators with unprecedented visibility into their Web security infrastructures.

*IronPort Web Security Monitor*™ is a real-time threat monitoring and reporting system, integrated into every IronPort Web security appliance. The system tracks all network traffic to provide a single location from which to identify a broad range of Web security threats and monitor all Web traffic.

### FEATURES

*IronPort Web Security Monitor's* intuitive graphical user interface enables real-time and historical visibility into your Web traffic.

### HOLISTIC VIEW OF WEB SECURITY STATUS



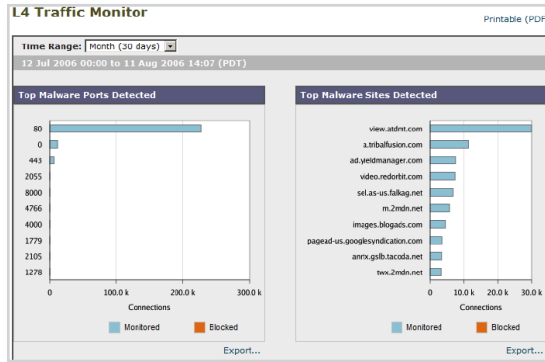
An easy to understand system overview report profiles all Web transactions, instantly identifies top threats, and displays an at-a-glance indication of the current operating state of each IronPort® appliance, including an “infected user” counter. Easily demonstrate Return on Investment (ROI) by reviewing how Web transactions within a network get filtered by *IronPort Web Reputation Filters*™, the *IronPort Anti-Malware System*™ and *IronPort URL Filters*™.



**FEATURES**  
(CONTINUED)

Top-level graphs highlight key data points, and detailed information is available in tabular format.

**Layer 4 Traffic Monitor** information helps you identify compromised network ports and detect malware “phone home” activity that attempts to bypass Port 80. Reports assist administrators in correlating malware categories and infected clients with specific malware threats.



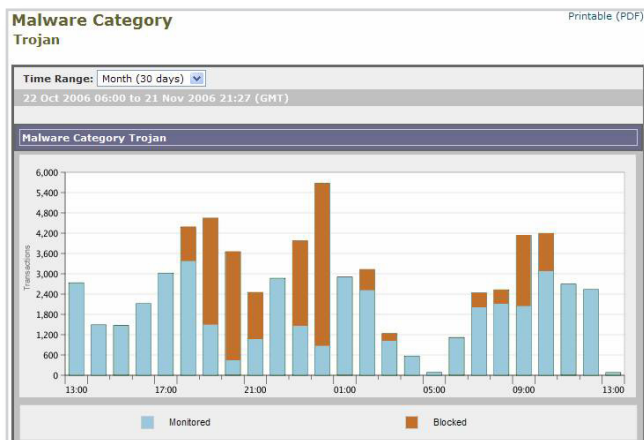
**End-user reports** highlight users browsing sites by category. Identify the top Internet users on the network, know how frequently users are trying to access blocked sites, and who those users are. Ensure system uptime with proactive management of risky behavior, and targeted cleanup activities for infected machines. Reports also detail bandwidth used and bandwidth saved (based on blocked transactions) per client.

Track end-user browsing patterns and instantly identify systems infected with malware using the Client Activity report.



**Detailed, system-wide malware reports** identify the top malware categories as well as specific instances of malware detected on your network. Assess the security of your network against high profile threats and develop policies to manage the top malware risks.

Web Security Monitor's Anti-Malware report provides comprehensive visibility into malware threats on your network.

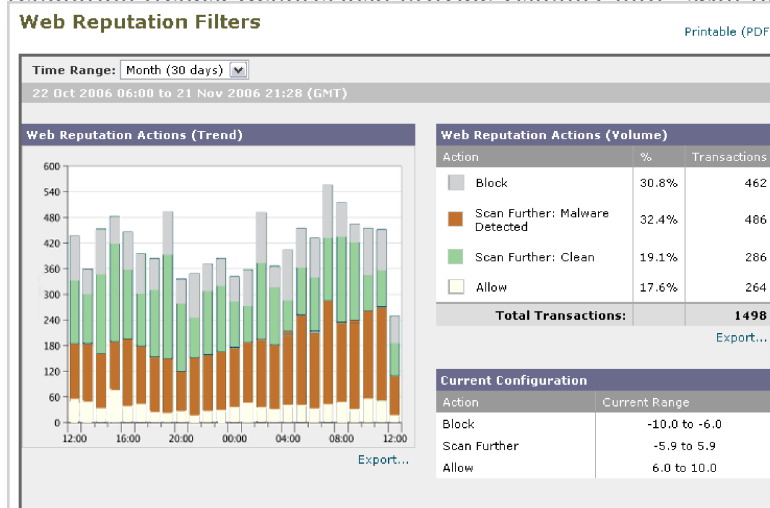


**FEATURES**

(CONTINUED)

**Web reputation data, powered by the IronPort SenderBase® Network,** shows how much Web traffic and which sites were blocked by reputation and provides key insight into Web reputation trends. Reports also provide visibility into “scan further” verdicts.

By integrating SenderBase data, IronPort Web Security Monitor accurately assesses the threat level of every Web request.



**Detailed, system-wide Web traffic reports** identify the top URL categories requested and blocked. Review actual Web activity against corporate appropriate use policies. Develop education and awareness activities to improve resource utilization.

Overall Web traffic reports allow organizations to keep track of policy and security violations.

**Top Clients** Items displayed 10

Summary **All**

User ID / Client IP Address	Bandwidth		Web Transactions						
	Bandwidth Saved by Blocking	Bandwidth Used	Blocked by URL Category	Blocked by Web Reputation	Blocked by Anti-Malware	Other Blocked Transactions	Total High-Risk Transactions Blocked	Transactions Completed	Total Transactions
jdoe	2500 Mb	222 Mb	5	5	10	5	25	2475	2500
rsrinivasan	2100 Mb	111 Mb	0	0	10	11	21	2079	2100
jsmith	160 Mb	99 Mb	1	1	13	1	16	144	160
auser	150 Mb	111 Mb	0	15	0	0	15	135	150
10.251.23.235	120 Mb	11 Mb	0	12	0	0	12	108	120
buser	100 Mb	11 Mb	0	10	0	0	10	90	100
buser2	100 Mb	11 Mb	0	10	0	0	10	90	100
cuser	90 Mb	22 Mb	0	9	0	0	9	81	90
duser	4 Mb	1 Mb	0	4	0	0	4	0	4
euser3	3 Mb	2 Mb	0	3	0	0	3	0	3

Export...

Search for: Client  exact match Search ?

Generated: 21 Nov 2006 10:25 (GMT -0000)

**Per category analysis** allows administrators to understand a specific URL category, while per website analysis allows administrators to review the top sites users access and identify top



**FEATURES**  
(CONTINUED)

**POWERFUL REPORTING ENGINE**

**PDF snapshots** allow you to capture the current view of a report in an Adobe Portable Document Format (PDF) file. Save or print the file for easy future reference.

**Regularly scheduled reports** can be configured for delivery over email or archived to the local system in PDF format. All real-time reports are available for periodic scheduled delivery.

Easily schedule reports for delivery on a daily, weekly or monthly basis.

**Report Settings**

Run This Report...

**Report Type**

Type: Anti-Malware

Title: Anti-Malware Monthly Report

Time Range To Include: Previous calendar month

**Report Options**

Number of Rows: Include top 20

**Scheduling and Delivery**

Schedule:  Daily At time: 01 : 00  
 Weekly on Monday  
 Monthly (on first day of month)

Email to: admin@mydomain.com  
Separate multiple addresses with commas. Leave blank for archive only.

**On-demand report generation** provides instant, ad hoc access to reporting data on your appliances. Dig deeper into a particular security incident by viewing all reports for a specific timeframe.

**Download reporting data** in CSV format for easy integration with existing monitoring solutions. Simply click the 'Export' links in the GUI or create automated scripts to export the reporting data from the *IronPort S-Series* appliances.

**Convenient search functionality** is available across all reporting pages, allowing administrators to quickly pinpoint specific websites, users or IP address.

Ad hoc reports allow you to instantly access historical reporting data on your appliance.

**Generate Report**

Report Type: L4 Traffic Monitor

Title: L4 Traffic Monitor

Time Range To Include: Custom date range : 27 Jul 2006 through 17 Aug 2006  
Data available from 23 Jul 2006 to 22 Aug 2006.

**Report Options**

Number of Rows: Include top 20

**Delivery Options:**

Archive

Email now to recipients: admin@mydomain.com

<< Back to Scheduled Reports View This Report... Deliver This Report...



### BENEFITS

**Reduce Administrative Overhead** Simple, easy-to-understand, real-time reports allow you to instantly assess the overall health of your network security. You no longer need to search through and post-process logs from multiple systems on your network. Quickly answer requests for detailed reports about Web browsing activities for a specific user.

**Integrate with Existing Solutions** All reporting data is available in industry-standard CSV format. Protect your investment in enterprise reporting solutions by simply importing Web security data from IronPort appliances.

**Enhance Network Security** *IronPort Web Security Monitor* provides a holistic view into the spyware and other Web-based threats in your network, enabling you to make critical security decisions. Defend your users against dangerous threats, and protect your business from critical downtime and lost opportunities.

**Improve and Facilitate Acceptable Use Policy** *IronPort Web Security Monitor* provides detailed view into Web traffic patterns, by Web category, website and client, enabling you to make critical policy decisions that effect both network security and employee productivity. IronPort helps guard against compliance risks to keep your network safe.

**Plan Targeted Cleanup Activities** Reports from the Layer 4 Traffic Monitor help you quickly identify potentially compromised hosts on your network. These actionable reports allow you to minimize the time wasted on forensics and focus your efforts on cleaning up infected hosts.

**Measurable Return on Investment** See exactly why IronPort provides the most effective Web security solutions in the industry. Information about each element of IronPort's unique multi-layer, multi-vendor malware protection is readily available. Easily scheduled ROI reports are automatically delivered for management review. Reports identify how many HTTP requests were blocked by URL filtering and provide detailed information on browsing trends by URL categories, such as top hits and top categories blocked.

---

**PRODUCT LINE** *IronPort Web Security Monitor* is available on all *IronPort S-Series* appliances.



## SUMMARY

### UNPRECEDENTED INSIGHT INTO WEB SECURITY THREATS

*IronPort Web Security Monitor* provides complete, real-time visibility into your Web traffic. This information helps administrators make critical network security decisions as well as proactively take actions to eliminate existing network threats. Scheduled reports reduce administrative overhead and reinforce the ROI of the IronPort appliances. With fully integrated data from the *IronPort SenderBase Network*, and the ability to instantly detect and respond to malware trends, *IronPort Web Security Monitor* gives you the power to know, act, control and protect.

## CONTACT US

### HOW TO GET STARTED WITH IRONPORT

IronPort sales representatives, channel partners, and support engineers are ready to help you evaluate how IronPort products can make your 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](mailto:info@ironport.com) WEB [www.ironport.com](http://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 435-0219-2 2/07