



A HIGH PERFORMANCE SOLUTION THAT ACCURATELY DETECTS AND BLOCKS A BROAD RANGE OF WEB-BASED MALWARE.

## IronPort Anti-Malware System

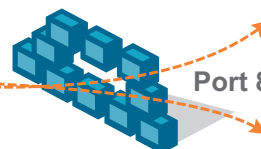
### OVERVIEW

The threat of malware is a very real and costly problem most companies face today. IDC estimates that 75 percent of corporate desktops are currently, and unknowingly, infected with spyware. Spyware and other types of malware can result in loss of confidential information, system and network downtime, reduced employee productivity and escalating customer support costs.

The *IronPort Anti-Malware System™* uniquely combines the *IronPort Dynamic Vectoring and Streaming (DVS) engine™*, a high performance scanning engine, with best-of-breed signature-based verdict engines to provide a powerful, fully integrated anti-malware

Web traffic has become 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.

- Adware
- System Monitors
- Phishing
- Pharming
- Browser Hijackers
- Keyloggers
- Trojans
- and more*



defense. As the second layer of defense on the *IronPort S-Series™* Web security appliance, the *IronPort Anti-Malware System* rapidly scans Web content as it is downloaded against malware and virus signatures — eliminating the broadest range of known and emerging Web-based threats. Web security technology is a critical element in securing and controlling the network. By preventing Web-based malware from entering the corporate network, *IronPort Anti-Malware System* reduces infections and desktop clean up costs.

### FEATURES

#### INDUSTRY-LEADING ACCURACY AND PERFORMANCE

The **IronPort Anti-Malware System** is optimized for exceptional performance integrated into a single appliance solution. IronPort® built the system to be fast and accurate, relying on a less computationally-intensive single scan to evaluate for multiple

threats including a broad range of malware, phishing, pharming, malicious rootkits and more. With the industry's largest malware signature database located at the gateway, the *IronPort Anti-Malware System* provides enterprises with industry-leading protection against these threats.



## FEATURES (CONTINUED)

**IronPort’s powerful DVS engine** employs rapid object parsing and vectoring techniques, along with stream scanning, early exit algorithms and reputation-based caching. This results in an unparalleled increase in scanning throughput over existing first-generation ICAP-based solutions.

The *IronPort Anti-Malware System* is designed to support verdict engines from multiple vendors, which maximizes efficacy.

**Broad threat categorization** identifies new and more sophisticated security threats, both on the request side and response side. The *IronPort Anti-Malware System* conducts deep archive scanning to detect viruses and malware obfuscated within archive packages. It also detects rootkits — hidden malicious software that provides root-level access to, and control over, a computer without its owner’s knowledge.

**Block threats at the corporate gateway** to prevent infection and reduce clean-up costs. By stopping threats before they enter the network, the *IronPort Anti-Malware System* prevents initial and ongoing damage.

## THE BROADEST RANGE OF SIGNATURES

**Scanning engines from Webroot and McAfee** are fully integrated into the *IronPort Anti-Malware System*. These two industry-leading solutions allow you to scan for Web-based threats in parallel, providing superior protection and performance.

The Webroot scanning engine, backed by a threat research team at Webroot, performs both request- and response-side scans. Efficacy and coverage are strengthened by Phileas (the first automated spyware detection system), which identifies existing and new threats by intelligently scanning millions of sites daily.

The McAfee scanning engine is backed by Avert Labs, the world’s top threat research center. The McAfee database includes both virus and malware signatures and can be configured to perform both signature-based and heuristics-based scanning.

**The largest variety of threat categories** for a Web gateway provide the *IronPort Anti-Malware System* with granular visibility into threat activity and specialized policy creation. Sixteen threat categories provide the enterprise with significant control to manage and balance risk management versus users needs.

Scanning engines from Webroot and McAfee are fully integrated into the *IronPort Anti-Malware System*.

Ironport DVS Anti-Malware Settings		
<input checked="" type="checkbox"/> Enable Suspect User Agent Scanning	<input checked="" type="checkbox"/> Enable Webroot	<input checked="" type="checkbox"/> Enable McAfee
<b>Malware Categories</b>	Monitor ☺	Block ☹
	Select all	Select all
☺ Adware	<input checked="" type="checkbox"/>	
☹ Browser Helper Object		<input checked="" type="checkbox"/>
☹ Commercial System Monitor		<input checked="" type="checkbox"/>
☹ Dialer		<input checked="" type="checkbox"/>
☹ Hijacker		<input checked="" type="checkbox"/>
☹ Phishing URL		<input checked="" type="checkbox"/>
☹ System Monitor		<input checked="" type="checkbox"/>
☹ Trojan Downloader		<input checked="" type="checkbox"/>
☹ Trojan Horse		<input checked="" type="checkbox"/>
☹ Trojan Phisher		<input checked="" type="checkbox"/>
☹ Virus		<input checked="" type="checkbox"/>
☹ Worm		<input checked="" type="checkbox"/>
☹ Other Malware <small>(May include Worms, Trojans and other dangerous forms of malware.)</small>		<input checked="" type="checkbox"/>
<b>Other Categories</b>	Monitor ☺	Block ☹
	Select all	Select all
☹ Encrypted File		<input checked="" type="checkbox"/>
☹ Suspect User Agents		<input checked="" type="checkbox"/>
☹ Unscannable		<input checked="" type="checkbox"/>



**FEATURES**  
(CONTINUED)**POWERFUL MANAGEMENT CAPABILITIES**

A **Web-based GUI** provides unprecedented control for initial configuration and ongoing management. The comprehensive, easy-to-use *IronPort Anti-Malware System* deploys in multiple modes, including “monitor only” or “monitor and block”.

**Malware categories and actions by verdict type** are managed within *IronPort Web Security Manager*<sup>™</sup>. Administrators create and easily manage custom anti-malware policies. Administrators enable or disable malware filtering on a per-user/per-group basis. The *IronPort Anti-Malware System* is the only solution to offer customers distinct settings for “known” and “suspect” malware and allow enterprises to set their own custom thresholds for malware-positive verdicts.

**Point-and-click functionality** is also provided by *IronPort Web Security Manager* to enable/disable the service, select deployment modes, set thresholds, configure automated updates and more. Automated, timely and secure updates, which can be scheduled for as frequently as every five minutes, ensure coverage against the latest emerging virus and malware threats.

**REAL-TIME MONITORING AND COMPREHENSIVE REPORTING**

**Real-time visibility** into trouble spots in a network’s Web traffic requests are provided by the *IronPort Anti-Malware System*. Reports include top malware sites detected, malware threats and categories identified/ blocked and others. In addition, the reports provide actionable information, such as a list of top clients infected, as well as historical trends. Through *IronPort Web Security Manager*, administrators have comprehensive visibility and the ability to correlate malware activity with clients.

A **sophisticated alert engine**, which is included with every *IronPort S-Series* appliance, also benefits the *IronPort Anti-Malware System*. Administrators can set up individual alert subscriptions for the system, based on severity levels. Alerts are calibrated in three categories: informational, warning and critical. This provides administrators with clear visibility into the application and enables them to take appropriate and timely action, if required.

**BENEFITS****Highest Accuracy and Lowest Latency**

Optimized for accuracy and performance, the *IronPort Anti-Malware System* ensures industry-leading efficacy, without any perceptible change to the end-user experience. The system combines the rapid parsing and vectoring capabilities of the *IronPort DVS engine* with the extensive and accurate signature-based verdict engines, Webroot and McAfee. Both engines rely on next generation, automated research technologies to proactively identify new threats, enabling their in-house threat research teams to rapidly develop and test signatures for new threats – before they infect corporate networks.

The *IronPort Anti-Malware System* is updated in real time to ensure the most current protection available.

**Protection Against the Broadest Range of Web-based Malware** The *IronPort Anti-Malware System* quickly and accurately detects and blocks a full range of known and emerging threats, including viruses, adware, Trojans, system monitors, keyloggers, root-kits, malicious/tracking cookies, browser hijackers, browser helper objects, phishing and more.

**Near-Zero Administrative Overhead** The *IronPort S-Series*’ easy-to-use, Web-based GUI makes initial configuration and set up simple. The *IronPort Anti-Malware*



**BENEFITS**  
(CONTINUED)

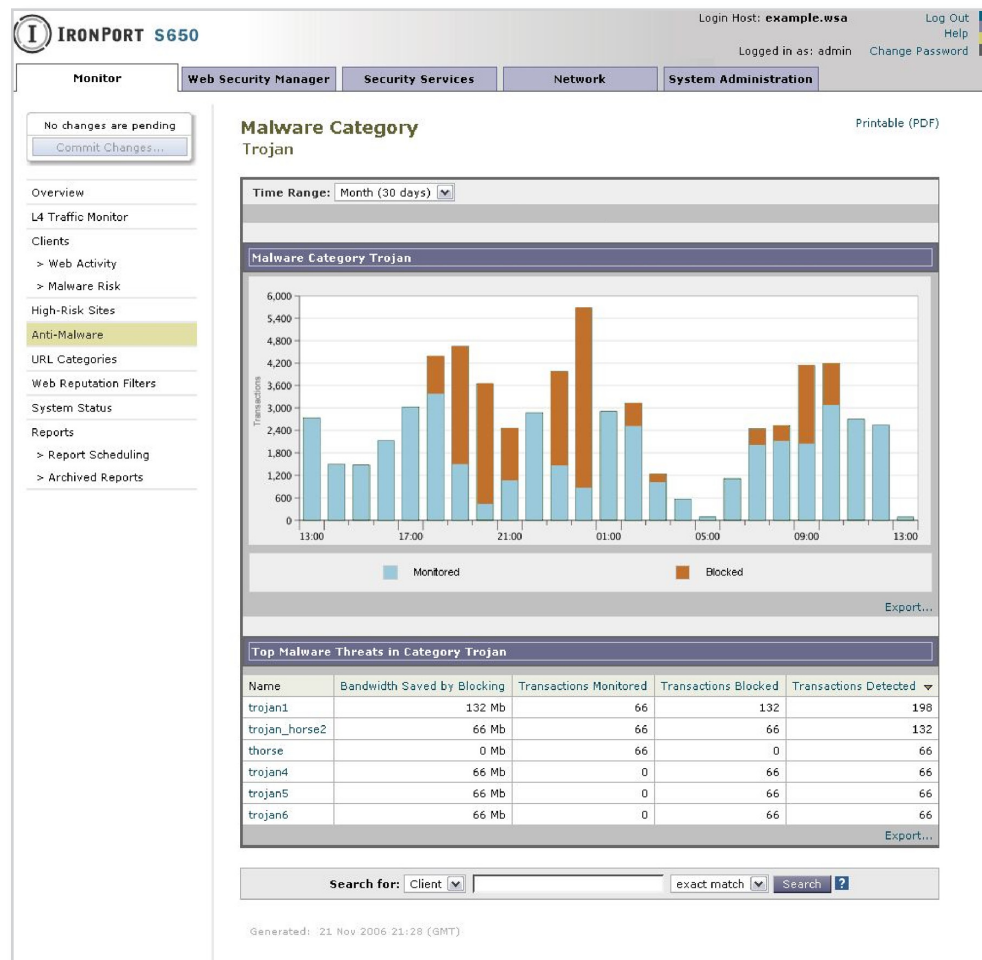
System's scanning accuracy drives customer support calls and expensive desktop clean up operations to zero. Automated, timely and secure updates eliminate the need for ongoing manual tuning and maintenance to catch new and emerging threats.

**Comprehensive Visibility** While the *IronPort Anti-Malware System* controls the malware threat to a corporate environment, administrators and executive management may require information to better understand ever-evolving corporate threats. The *IronPort Anti-Malware System's* comprehensive reporting gives administrators powerful

insight into threats monitored or blocked, as well as the presence of infected clients. This reporting functionality also allows for a better view of user actions, providing data to help drive additional policies to further protect the network and corporate desktops.

**Low Total Cost of Ownership** First-generation, ICAP-based anti-malware solutions require ownership and administration of multiple servers. Unlike these products, the *IronPort Anti-Malware System* is delivered as a high-performance, single appliance solution.

Powerful, security-focused reports provide detailed information on malware including client correlation and trend data.



## SUMMARY

The strong perimeter defense provided by the *IronPort Anti-Malware System* prevents client infections and greatly reduces clean up costs. As an important part of the *IronPort S-Series* appliance, this defense-in-depth solution combines unmatched accuracy and exceptional performance to deliver powerful protection with no perceptible change to the end-user experience.

## 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, California 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, a Cisco business unit, 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 © 2000-2007 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco 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 435-0217-3 10/07

IronPort is now  
part of Cisco.

