



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

IronPort Anti-Malware System

OVERVIEW

The malware threat is real and the resulting costs are substantial. Web-based malware is wreaking havoc on corporations, with IDC estimating that 80 percent of corporate desktops are currently and unknowingly infected by spyware. Spyware and other 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 perfor-

mance scanning engine, with best-of-breed signature-based verdict engines to provide a powerful, fully integrated anti-malware defense. As the second layer of defense on the *IronPort S-Series*™, the *IronPort Anti-Malware System* rapidly scans Web content as it is downloaded against malware signatures – eliminating the broadest range of known and emerging Web-based threats. By preventing Web-based malware from entering the corporate network, the *IronPort Anti-Malware System* reduces infections and desktop clean up costs.

FEATURES

INDUSTRY-LEADING 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 and more.

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

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

THE BROADEST RANGE OF SIGNATURES

Webroot's signature-based verdict engine is currently incorporated into the *IronPort Anti-Malware System*. Webroot consistently receives top ratings and recommendations by respected third-party media and product reviewers. Unmatched in terms of size and breadth, Webroot provides a full range of signatures — protecting against adware, tracking cookies, browser hijackers, phishing, pharming attacks and more to identify sig-



FEATURES (CONTINUED)

nificantly more malicious forms of malware such as Trojans, system monitors, keyloggers and other threats.

An in-house Threat Research team and Phileas, the industry's first automated research system, power Webroot's signature-based verdict engine. Architected for performance, Phileas proactively scours millions of sites daily to discover malware faster and more efficiently than any other method. Backed by Phileas, the Threat Research team rapidly builds new definitions and updates the verdict engine to provide the best and most up-to-date protection.

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".

Point-and-click functionality is also provided by the *IronPort Web Security Manager*™ to enable/disable the service, select deployment modes, set thresholds, select granular malware categories and actions by verdict type, configure automated updates and more. The *IronPort Anti-Malware System* is the only

solution to offer customers distinct settings for "known" and "suspect" malware. Automated, timely and secure updates are provided via HTTP.

REAL-TIME MONITORING AND COMPREHENSIVE REPORTING

Real-time visibility into trouble spots in a network's Web traffic requests are delivered 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.

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 *IronPort Anti-Malware 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 *IronPort Anti-Malware System* combines the rapid parsing and vectoring capabilities of the *IronPort DVS engine* with the extensive and accurate Webroot signature-based verdict engine. Webroot relies on

next generation, automated research technologies to proactively identify new threats, enabling the in-house Threat Research team 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 up-to-date protection.



BENEFITS
(CONTINUED)

Protects 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 adware, Trojans, system monitors, keyloggers, 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 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 other products, the *IronPort Anti-Malware System* is delivered as a high-performance, single appliance solution.

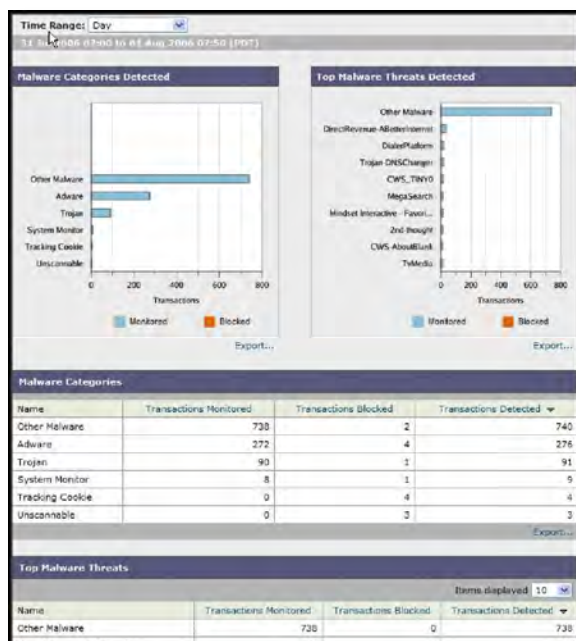
FIGURE 1.

IronPort Web Security Manager provides an easy-to-use interface for configuring the *IronPort Anti-Malware System*.



FIGURE 2.

Powerful, security-focused reports provide detailed information on malware.



SUMMARY

The strong perimeter defense provided by the *IronPort Anti-Malware System* prevents client infections and greatly reduces client cleanup costs. As part of the *IronPort S-Series* appliance, this defense-in-depth solution combines unmatched accuracy and exceptional performance to deliver a powerful defense 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 email 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



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 the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.

Copyright © 2006 IronPort Systems, Inc. All rights reserved. IronPort and SenderBase are registered trademarks of IronPort Systems, Inc. All other trademarks are the property of IronPort Systems, Inc. or their respective owners. Specifications are subject to change without notice. P/N 435-0217-1 9/06

