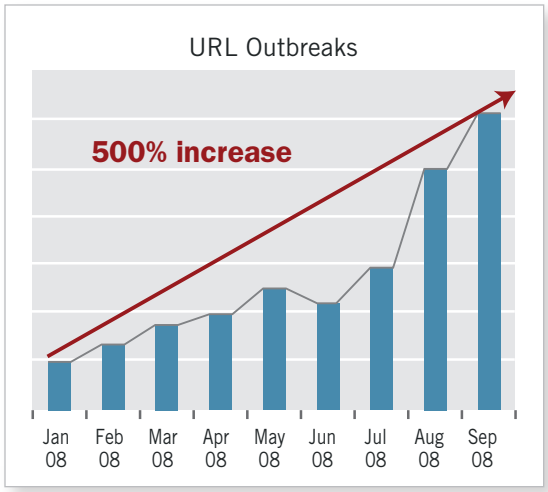
IRONPORT S-SERIES

THE INDUSTRY'S FIRST WEB REPUTATION FILTERS PROVIDE A POWERFUL DEFENSE AGAINST MALWARE

IronPort Web Reputation Filters

OVERVIEW

IronPort Web Reputation Filters™ are designed to combat the increasingly prevalent and dynamic nature of malware. Today's threats are no longer found as an email attachment. Instead, they are well orchestrated – utilizing social engineering techniques that mirror and target legitimate websites. According to IronPort's Threat Operations Center, exploited websites are responsible for more than 87 percent of all Web-based threats today. Malware writers are now targeting well-known, trusted websites. An unsuspecting users credit card number can be worth up to one hundred dollars to a threat writer.



IronPort's Threat Operations Center has observed a significant increase in URLs hosting new malware, for which no signatures are available. Existing malware defenses are proving to be inadequate against these threats.

One of the fastest growing vectors for distributing these Web-based threats is through compromised hosts (known as botsites) that follow instructions from a command-and-control network (known as botnets). Spreading through recruiting emails and webpage spam, malicious botsites self-propagate through their own established peer-to-peer networks. These botnet/botsite systems represent an intelligent malware distribution platform that is reusable and self-defending.

As the first line of malware defense, *IronPort Web Reputation Filters* analyze more than 5 billion Web transactions daily – blocking up to 70 percent of malware at the connection level, prior to signature scanning. By leveraging its global footprint of URL traffic data IronPort's Web reputation system is able to offer an industry-leading 60 percent higher malware catch rate than traditional signature scanners.

IronPort Web Reputation Filters examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains. This gives these IronPort® a unique advantage over vendors that reduce Web reputation to a simple URL filtering category. *IronPort Web Reputation Filters* are the industry's only reputation system to include exploit filtering, botsite defense and URL outbreak detection – protecting users from known and unknown exploits (including adware, Trojans, system monitors, keyloggers, malicious/ tracking cookies, browser hijackers, browser helper objects and phishing attacks) delivered through cross-sight scripting (XSS), cross-sight request forgery, SQL injections or invisible iFrames.

As the industry's first and best Web reputation filtering system, *IronPort Web Reputation Filters* provide a powerful outer layer of malware defense at the network perimeter.

FEATURES

IronPort Web Reputation Filters intelligently apply Web security policies based on a requested URL's reputation. This prevents malicious Web traffic from even entering the network, while allowing legitimate Web requests to flow unobstructed.

ACCURATE REPUTATION SCORES

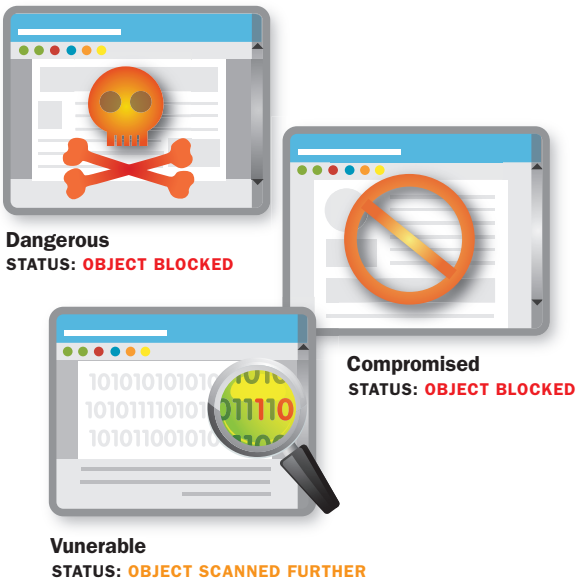
IronPort's SenderBase® Network is the world's first and largest Web and email traffic monitoring system. *SenderBase* collects data from more than 100,000 networks around the world, ten times more than competing reputation monitoring systems. By tracking a broad set of over 150 Web- and email-related parameters, *IronPort's SenderBase* supports very accurate conclusions about any given URL or IP address. Parameters examined to determine URL reputation include: domain registration information, use of dynamic IPs, traffic volumes, patterns in the URL being requested, as well as the use of behavior-based scanners. IronPort's Web reputation technology leverages real-time cloud scanning, powered by *SenderBase*, to find and block access to compromised websites before malware can become operational. The breadth of data available to IronPort through the *SenderBase Network* allows virtually every active URL and IP address on the Internet to receive a Web reputation score. By comparison, even the best URL filtering technologies from other vendors have scored only 15 percent of webpages.

DYNAMIC PROTECTION

Exploit Filtering zeros in on the latest network security threat: trusted websites that have been compromised to deliver Trojans or phishing attacks through techniques such as cross-site scripting (XSS), SQL injections and invisible iFrames. IronPort's Exploit Filtering technology groups compromised websites into three risk levels:

- Dangerous – These sites are actively serving malware or have malicious scripts injected into the site and are immediately blocked.
- Compromised – These sites have malicious scripts present, but they have not been activated by the bot network's command and control servers. These sites, too, are blocked by default.
- Vulnerable – These sites are at put on a "risk watch" and actively monitored by IronPort's Threat Operations Center because they are susceptible to attack or have been linked to malware distribution in the past.

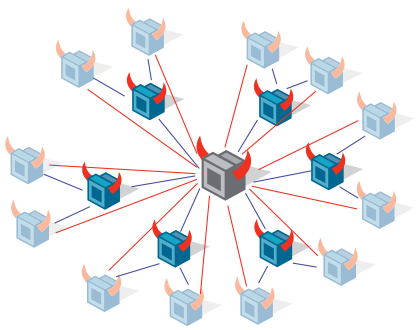
Exploit Filtering



With the addition of Exploit Filtering, IronPort offers uncompromised protection against the biggest invisible threats on the Web: the transparent passing of malware through legitimate websites.

FEATURES (continued)

Industry estimates point to at least 7 percent of computers connected to the Internet (75 to 100 million machines) being a part of some botnet/ botsite system.



A single Botnet can spawn thousands of malware-laden Botsites in just a few hours.

Botsite Defense utilizes next generation threat assessment techniques on all content fetched by the browser – giving *IronPort Web Reputation Filters* the ability to detect and block botsites based on certain characteristics they exhibit. Looking at the content's origin, *IronPort's Botsite Defense* leverages security-modeling techniques to provide dynamic protection against threats that target legitimate websites.

URL Outbreak Detection is designed to identify and defend against URLs that have no reputation or signature, which are typically hosted on a botsite and controlled by a botnet. Leveraging *IronPort's SenderBase*, URL Outbreak Detection is able to identify virus outbreaks on average 13 hours before traditional anti-virus solutions – providing *IronPort Web Reputation Filters* "always on" detection when tracking the infrastructure behind malware attacks, then adjusting to rapidly block them. URL Outbreak Detection closes the window of vulnerability on zero-day threats.

COMPREHENSIVE MANAGEMENT

Web-based administration makes it simple to manage Web security policies. Administrators easily update and adjust policies to meet the varied needs of the global enterprise. Administrators also control the aggressiveness of the system by adjusting the thresholds for "block", "allow" and "scan".

Automatic updates are pushed to each *IronPort S-Series*™ appliance on a regular basis. Once the appliance is configured, scores are dynamically updated based on the latest threat data from *SenderBase*. This eliminates the need for any ongoing management of *IronPort Web Reputation Filters*.

Comprehensive reporting and alerts deliver complete real-time visibility into trouble spots in a network's HTTP traffic requests. Reports provide actionable information (such as a list of top clients infected) as well as historical trends.

BENEFITS

Superior protection against Web-based malware IronPort's multi-layer, defense-in-depth solution provides a significantly higher malware catch- rate over existing, single layer solutions. The breadth and depth of *SenderBase* data allows *IronPort Web Reputation Filters* to stop both known and emerging threats. This results in a malware catch-rate significantly greater than traditional URL filters, which are not effective in identifying these threats because they rely on manual classification techniques and enable infected sites to hide behind generic classifications, such as shopping, finance, entertainment or news.

Lower costs *IronPort Web Reputation Filters* are the only Web security solution to categorize both high reputation and low reputation webpages. Most Web traffic is to malware-free websites, allowing *IronPort Web Reputation Filters* to quickly offload this traffic from the scanning engine — saving system resources and lowering ownership costs.

BENEFITS (continued)

Complete administrative control *IronPort Web Reputation Filters* give administrators significant control and flexibility. This unique solution allows different security policies to be implemented, based on different Web reputation scoring ranges.

No administrator maintenance required Managing policies can be time-consuming, frustrating for both administrators and users, and difficult to do accurately. *IronPort Web Reputation Filters* adjust scores automatically as *SenderBase* gathers new data. The administrator only needs to configure desired policies, and IronPort does the rest.

SUMMARY

IronPort first introduced the concept of reputation filtering over five years ago. Since then, the *IronPort SenderBase Network* has grown to be the industry's largest Web and email traffic monitoring system. As the first line of defense against malware, *IronPort Web Reputation Filters* provide customers with the critical security features necessary, exploit filtering, botsite defense and URL outbreak detection, to safeguard their networks from dynamic Web-based attacks, without interrupting daily business communications. With extremely high accuracy and near-zero latency for customers, *IronPort Web Reputation Filters* on the *IronPort S-Series* Web security appliance provide the most comprehensive Web security solution available.

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

IronPort Systems, now part of Cisco, 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.

IronPort is now part of Cisco.