IRONPORT

IRONPORT SECURITY MODULES

ACCURATELY PROTECTING AGAINST THE BROADEST RANGE OF THREATS.

IronPort Anti-Spam

OVERVIEW

As threat writers use constantly evolving techniques to penetrate companies' existing defenses, email threats have expanded beyond simple nuisance spam. *IronPort Anti-Spam*™ combines best-of-breed conventional techniques with IronPort's breakthrough context-sensitive detection technology, to eliminate the broadest range of known and emerging email threats.

FEATURES

A POWERFUL OUTER LAYER OF DEFENSE

Reputation Filtering— a technique pioneered by IronPort– provides a powerful outer layer of spam defense. *IronPort Reputation Filters*™ deliver unmatched efficacy, accurately stopping up to 80% of incoming spam at the connection level. IronPort® appliances also support a unique rate limiting capability, which intelligently slows down suspicious senders—greatly reducing the spam, without the risk of false positives.

ACCURACY WITH CONTEXT-BASED SCORING

IronPort Anti-Spam utilizes the industry's most innovative approach to threat detection. In addition to reviewing sender reputation, IronPort's unique *Context Adaptive Scanning Engine*™ *(CASE)* examines the complete context of a message, including:

- content
- methods of message construction
- reputation of the sender

When the *CASE* score is combined with sender reputation, the end result is more accurate than traditional spam filtering techniques.

IronPort's Web Reputation technology measures the behavior and traffic patterns of a website to assess its trustworthiness. *IronPort's CASE* technology determines the reputation of any URL within a message body, so that a more accurate analysis of the messages can be performed. This enables IronPort to immediately protect *IronPort Anti-Spam* users from spam, phishing, and spyware threats distributed over email.

FEATURES (CONTINUED)

AUTOMATIC UPDATES AND COMPREHENSIVE CONTROLS

Automatic, timely and secure rule updates eliminate the need for ongoing manual tuning and maintenance to catch emerging threats. The IronPort update service ensures that IronPort appliances are running the most up-to-date engine.

Administrators can easily configure the service at a global level and leverage IronPort's powerful *Email Security Manager*™ to set user and group specific policies.

End-users directly access the IronPort Spam Quarantine to check and manage messages, or review email digests that are sent to them periodically. A powerful spam reporting plug-in for Microsoft Outlook allows users to send missed spam directly to *IronPort's Threat Operation Center* for review.

REAL-TIME MONITORING AND CENTRALIZED REPORTING

Mail Flow Monitor™ delivers complete real-time visibility into who is sending you email, and alerts administrators of suspicious traffic — allowing them to take immediate action.

Mail Flow Central™ allows you to find the status of any message that has traversed your infrastructure. With this centralized reporting tool, administrators and support staff can quickly answer end-user inquiries such as, "What happened to my email?".

FAST, ACCURATE DETECTION

IronPort's 24x7 Threat Operation Center (TOC) leverages extensive technology and infrastructure to ensure efficacy. TOC analysts speak over 32 languages and have powerful tools to maintain a massive email corpus, manage a knowledge-base of latest trends, publish real-time rule updates to ensure that new spam attacks can be blocked as soon as they start, and provide closed loop verification of customer reports.

Jan Mak, Manager of the *IronPort Threat Operations Center (TOC)*

BENEFITS

Eliminates the Broadest Range of Email Threats *IronPort Anti-Spam* addresses a full range of known threats including spam, phishing, and zombie attacks, as well as hard-to-detect low volume, short-lived email threats such as “419” scams. In addition, *IronPort Anti-Spam* identifies new and evolving blended threats such as spam attacks distributing malicious content through a download URL or an executable.

Provides Highest Accuracy The key to efficacy is data captured by IronPort’s *SenderBase*®, the world’s first, largest and most accurate traffic monitoring network. In addition to the best technology, *IronPort Anti-Spam* is backed by an interdisciplinary team of experts with backgrounds in email security, machine learning, and human genomics. As a leader in preventive threat detection techniques, IronPort’s security experts constantly innovate to stay ahead of emerging threats. *IronPort Anti-Spam* is integrated with *IronPort’s Threat Operations Center*, which ensures the highest level of accuracy and responsiveness.

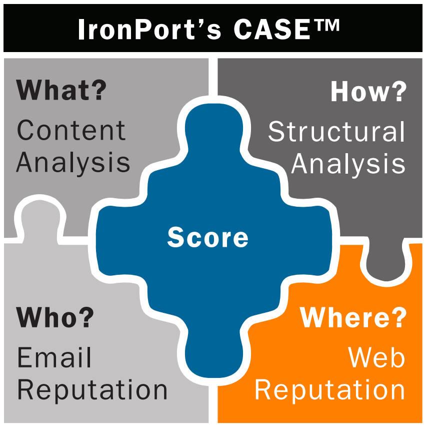
Enables Ease of Use and “Zero Administration” IronPort’s automatic, timely and secure rule updates eliminate the need for ongoing manual tuning and maintenance to catch emerging threats. This time savings, combined with comprehensive reporting, gives administrators powerful insight into their email traffic.

Adds A Global Solution In addition to locale-specific, content-aware threat detection techniques, *IronPort Anti-Spam* leverages globally representative SMTP and HTTP content-agnostic data – contributed by over 100,000 ISPs, universities and corporations throughout the Americas, Europe, and Asia.

Delivers Industry-Leading Performance IronPort’s spam filtering technologies deliver industry-leading performance based on real-world mail streams. This is made possible by *IronPort Reputation Filters*, which decrease email bandwidth consumption by as much as 80%, greatly improving system efficiency by reducing the number of messages that need to be processed. In addition, *IronPort’s CASE* technology uniquely performs multiple evaluations simultaneously, during a single message scan, eliminating unnecessary computational overhead.

FIGURE 1. IRONPORT ANTI-SPAM ADVANTAGE: LEADING WORLDWIDE EFFICACY

IronPort’s CASE technology uses advanced machine learning techniques to emulate the logic used by a human that is evaluating the legitimacy of a message. A human reader, as well as the CASE, asks these four basic questions.



- Optimized to stop blended threats
- Delivers industry-leading efficacy
  - Full contextual analysis minimizes false positives
  - 100,000+ attributes
  - 24x7 Threat Operation Center
- Offers a global solution
  - Content-specific & agnostic attributes
  - Global SenderBase Network

SUMMARY

THE NEW ANTI-SPAM SOLUTION

With email threats on the rise, and threat writers constantly evolving spamming techniques to penetrate companies' existing defenses, a multi-layered spam defense provides companies with the most secure protection. Utilizing both best-of-breed conventional techniques and IronPort's revolutionary context-sensitive detection technology, that even filters the URL within a message body, *IronPort Anti-Spam* eliminates the broadest range of known and emerging email threats.

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®

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.

IronPort Anti-Spam
04/06
DOC RELEASE