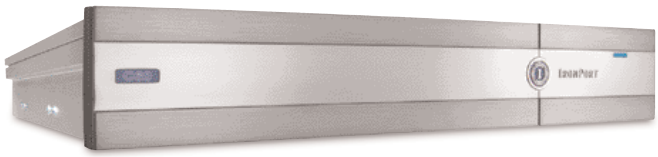
IronPort C-Series **Virus Outbreak Filters**



IronPort C-Series

Powering and Protecting Business Email

The IronPort C-Series™ email security appliance is built on IronPort's revolutionary MTA platform. It incorporates email threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters.™ Additional capabilities include: the IronPort content scanning engine, anti-spam and anti-virus technology.

IronPort Virus Outbreak Filters

A high-performance preventive security system protects your network from infections.

IronPort email security appliances intelligently quarantine suspicious mail during the earliest stage of a virus outbreak.

IronPort Virus Outbreak Filters act to provide a critical first layer of defense against new outbreaks. The IronPort email security appliances perform a threat assessment of inbound and outbound messages. The assessment returns a virus score that triggers an automated response. Suspicious messages are quarantined temporarily and re-scanned through the traditional reactive anti-virus solutions once signature updates are in place.

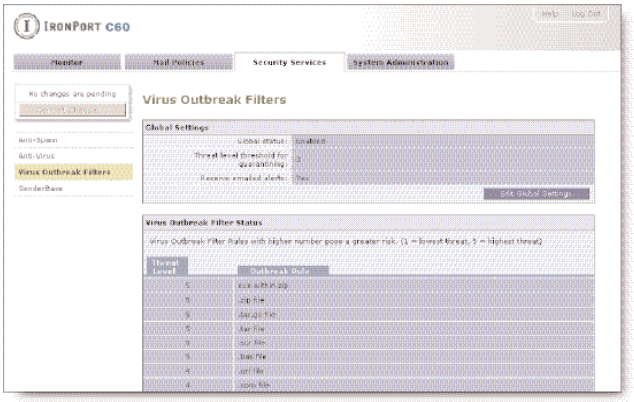
Detect New Virus Outbreaks in Real-time

New virus outbreaks are detected in real-time, hours before signatures used by reactive anti-virus solutions are updated. Detection is based on SenderBase,™ the world's largest email traffic monitoring network. Today, SenderBase captures data from over 50,000 contributing organizations and has a view into a remarkable 25% of the world's email traffic. IronPort's detection technology uses historical SenderBase data to create a statistical view of normal global traffic patterns. Realtime data from the global SenderBase network is compared and correlated with the baseline, to identify anomalies that are proven predictors of an outbreak. The IronPort Threat Operations Center (TOC) publishes rules which are used by the appliance to determine the threat level and quarantine suspicious email.

Ensure and Automate, Tailored Response

The IronPort email security appliances dynamically apply policies based on the threat level. When the threat level is elevated mail is automatically filtered and suspicious messages are quarantined. Immediate and automated response to new outbreaks provides protection until up-dated signatures are in place. At that point, mail is released and re-scanned through the traditional anti-virus filters.

Administrators can set policies based on their specific needs. The Web-based administration tool in the IronPort appliance lets administrators easily configure policy parameters, as well as view, search, test, and selectively release quarantined messages.



Unprecedented visibility and control. *The integrated Web-based user interface enables realtime and historical visibility plus the ability to configure policies, search, and selectively release quarantined messages.*

Build a Defense in Depth

IronPort Virus Outbreak Filters complement traditional anti-virus solutions. Virus Outbreak Filters detect and react to new threats in real-time to provide a critical first line of defense, preventing infections during the initial stages of a new outbreak. Reactive anti-virus solutions continue to play a critical role, accurately scanning for known viruses and cleaning, stripping or deleting email once updated signatures are in place.

IRONPORT™

IronPort Systems, Inc. 1100 Grundy Lane, Suite 100 San Bruno, California 94066 **tel** 650.989.6500 **fax** 650.989.6543 **email** info@ironport.com **web** www.ironport.com

Copyright © 2004 IronPort Systems, Inc. All rights reserved. IronPort, IronPort C-Series, Reputation Filters, Virus Outbreak Filters, SenderBase, and AsyncOS are trademarks of IronPort Systems, Inc. All other trademarks are the property of their respective owners. Specifications are subject to change without notice. P/N 435-0018 9/28