



# PRESS RELEASE

---

## FOR IMMEDIATE RELEASE

CONTACT: LIZ LANDIS  
IRONPORT SYSTEMS  
415.828.4801 MOBILE  
LLANDIS@IRONPORT.COM

BROOKE CHILEN  
BITE COMMUNICATIONS FOR IRONPORT SYSTEMS  
415.365.0397 DIRECT  
BROOKE.CHILEN@BITEPR.COM

## **IRONPORT SYSTEMS™ Virus Outbreak Filters™ Detect Viruses Faster Than Any Other Technology in the World**

***IronPort Identifies and Quarantines Viruses up to 27 Hours Before Signatures Are Available from Traditional Anti-Virus Vendors***

**SAN BRUNO, Calif. —March 1, 2005** – IronPort Systems, the market share leader in email security, today announced that IronPort Virus Outbreak Filters has established itself as the world's leading preventive anti-virus technology. Integrated into the IronPort C-Series email security product line, Virus Outbreak Filters are a preventive security solution; a proactive, critical first layer of defense that protects networks from infections during the critical initial stages of a virus outbreak. Analyzing global data from SenderBase™, the industry's largest email traffic monitoring network, Virus Outbreak Filters detect viruses in real-time as they begin to propagate— up to 27 hours before signatures from reactive anti-virus vendors are published. Suspect email is temporarily quarantined and re-scanned through traditional anti-virus solutions once signature updates are in place.

### **Protecting Assets and Eliminating Costs**

IronPort Virus Outbreak Filters protect corporate assets by safeguarding networks from malicious viruses, allowing corporations to defend against new outbreaks before they escalate into damaging and costly incidents. With an estimated clean-up cost per virus of \$200 per user, IronPort saves its customers millions of dollars every time there is a virus outbreak.

### **Traditional Anti-Virus Solutions vs. IronPort Outbreak Filters**

Most anti-virus defenses rely almost entirely on signature-based filters that look for patterns in data streams, and stop messages that match known viruses. This makes them vulnerable to finite reaction times that can vary from hours to days depending on the complexity of the virus. During that “vulnerability window”, a modern virus can propagate globally, bringing email infrastructure to a halt. Using SenderBase, the IronPort Threat Operation Center analyzes global patterns in real-time to detect anomalies that are proven predictors of a new virus outbreak. Automatically generated alerts are quickly verified and updates issued to IronPort's email security appliances.

## **IronPort Detects Viruses Ahead of the Game—Three Case Studies**

### **MyDoom.BB**

IronPort Virus Outbreak Filters were able to detect W32.MyDoom.BB@mm- a MyDoom variant that is polymorphic in nature, on February 15, 2005 at 18:08 (GMT). The first signature became available on February 16, 2005 at 21:57 (GMT). IronPort lead-time: +27 hours.

### **Sober.J**

IronPort Virus Outbreak Filters were able to detect W32.Sober.J@mm on January 30, 2005 at 23:01 (GMT), ahead of all major AV signatures and alerts. The first major AV alert was issued on January 31, 2005 at 09:21 (GMT). IronPort lead-time: +10 hours.

### **Goldun-H**

IronPort Virus Outbreak Filters were able to detect TROJ/Goldun-H, on February 15, 2005 at 23:04 (GMT). The first major AV alert was issued on February 16, 2005 at 03:12 (GMT). IronPort lead-time: +4 hours.

"IronPort appliances are at work protecting the email systems of the world's largest corporations and networks, including more than 50% of the world's largest ISP, technology, and media companies," said Scott Weiss, CEO of IronPort Systems. "Prior to the development of IronPort's Virus Outbreak Filters, these customers would take dramatic steps such as halting all inbound mail until the virus defenses were in place. Now, IronPort's Virus Outbreak Filters are detecting new outbreaks as they happen and dynamically triggering policies to protect networks until updated signatures are deployed."

### **Track the Threat Level**

Virus Outbreak Filters data is tracked at the IronPort Threat Operations Center (TOC). Analysis from the TOC can be found on the IronPort TOC Report (<http://www.ironport.com/toc>), a website which offers an unprecedented view into global email activity.

### **ABOUT IRONPORT SYSTEMS**

IronPort Systems is the leading email security provider for organizations ranging from small businesses to the Global 2000. The company has developed a family of email security appliances, the IronPort C-Series™, that offer breakthrough performance, unprecedented ease of use and reduced total cost of ownership. IronPort is driving new standards and providing innovative products for those faced with the monumental task of managing, protecting, and growing mission-critical email systems. For more information on IronPort products and services, visit: <http://www.ironport.com>.