



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 SYSTEMSTM Expands Email Threat Operations Center, Launches Email Security Report Website

Powered by IronPort SenderBase, the Industry's First and Largest Email Traffic Monitoring Network

SAN BRUNO, Calif., — February 14, 2005 – IronPort, the market share leader in email security, today announced the expansion of its Threat Operations Center (TOC) and launched the Threat Operations Center Report, a website which offers an unprecedented view into global email activity. IronPort TOC analysts use sophisticated tools to review complex real-time and historical traffic patterns, analyze anomalies to uncover new threats, and track email traffic trends. Automatically generated alerts are verified and updates are issued to IronPort's email security appliances on a constant, rapid basis successfully countering threats, such as new virus outbreaks. TOC tools are powered by a series of proprietary algorithms that process data from IronPort's SenderBaseTM, the world's first and largest email traffic monitoring network. The TOC Report can be found at <http://www.ironport.com/toc>.

IronPort's Threat Operations Center is a 7x24x365 global operation that provides oversight to IronPort's automated security services. The TOC technical staff is fluent in more than 32 languages and has operators in London, Beijing and San Francisco. IronPort's TOC is the command and control center for IronPort's unique preventive security services which can stop viruses 8 hours before traditional anti-virus signatures are available and stop 75% of incoming spam at the connection level before the message has even been accepted. These security services are built-in to IronPort's industry leading email security appliances. 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.

It Starts with SenderBase Reputation Service

The traditional approach to network security is to look for "signatures" in the content of incoming data to identify harmful code. Before beginning the costly and sometimes inaccurate process of scanning the content of a message for signatures, a reputation service asks the simple but powerful question: "What do we know about the sender?" By examining traffic patterns over time, an effective reputation system can stop threats before signatures are even available.

The industry is rapidly realizing that a reputation service is the critical first line of defense for any network. Since IronPort launched SenderBase, the world's first reputation service, more than 3 years ago—nearly all other enterprise-class vendors have followed. But the key to an effective reputation service lies in the quantity, quality, and breadth of data in the underlying database. IronPort's SenderBase dominates the industry, collecting data from more than 75,000 participating networks, ten times more than any competing service. These networks include the largest ISPs in the world such as China Telecom, Tiscali in Europe, and 6 of the 10 largest ISPs in the US. The SenderBase network also captures data from small ISPs and corporations in every corner of the globe, providing a large and diverse sample of Internet traffic patterns.

From this large network, SenderBase captures a broad set of data for any given sender-- including global volume of mail being sent, whether the sender accepts mail in return, the country of origin - more than 50 different parameters in total. With nearly 3 years of operating experience, the technicians at IronPort's TOC have realized that not all data is created equal. IronPort has developed a data quality engine that correlates the many diverse data streams with known benchmarks and assigns an appropriate statistical weighting to account for data quality fluctuations. The result of this is that SenderBase provides highly accurate and granular data that allows IronPort to identify the tactics of zombie computers, virus outbreaks, and "phishing" attacks more accurately and more rapidly than any other source.

Contributing to the Internet Community

SenderBase's widespread adoption is fueled in part by IronPort's willingness to share critical security data with the entire Internet community. IronPort licenses SenderBase data to select ISPs and open-source software products, spreading the reach of SenderBase and at the same time increasing its data quality. Senderbase data can be accessed at www.senderbase.org.

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>.

###