



## Blue Coat Implements Dynamic Link Analysis in WebPulse Service to Analyze and Assess Risk of Dynamic Web Content

*Dynamic Link Analysis Provides Next Generation Protection Against Malware Delivered through Web Links*

**SUNNYVALE, Calif., April 13, 2009**—Blue Coat Systems, Inc. (Nasdaq: BCSI), the technology leader in Application Delivery Networking, today announced that it has implemented Dynamic Link Analysis in the Blue Coat® WebPulse™ cloud-based community watch service. Dynamic Link Analysis incorporates the latest advances in protection against a rapidly expanding category of threats that relies upon dynamic Web links to spread malware and malicious content.

Dynamic Link Analysis within the Blue Coat Web-Pulse service combines URL filtering and anti-malware techniques to protect users against Web-based threats that utilize dynamic links. Frequently injected into popular and trusted web sites, these dynamic links connect through relay servers to hosts of malware downloads. Dynamic Link Analysis includes the following four components:

- **Cloud-Connected Community** that unites a broad and diverse user population to provide protection in numbers.
- **Real-Time Input** from the user community that includes new Web links and content that have not been rated.
- **Immediate Threat Assessment** that detects malware, phishing and malicious content through multiple analysis techniques, including ratings-based categorization, threat engines, machine analysis and human raters.
- **Cloud-Based Ratings Updates** on new Web content that immediately protect all members of the community from malware and malicious content without the burden of database downloads.

“Malware continues to migrate to the Web, the always changing content poses a significant security risk and the threat cycle is being rapidly compressed,” said Christian Christiansen, IDC’s vice president of security products & services. “To combat this trend, businesses should consider proactive security strategies that incorporate the control capabilities of URL filtering and detection capabilities of anti-malware analysis. Both these elements should function in a real-time environment to successfully protect against rapidly evolving Web-based threats.”

### Dynamic Web Content Requires Dynamic Security

The transition from Web 1.0 to Web 2.0 has been driven by dynamic content, where multiple changing components, such as advertisements, news feeds, photos, videos or reference links to other content, and their corresponding URLs, are part of a single Web page experience. In this environment, iFrame or SQL attacks inject links into popular Web sites that lead to relay servers and eventually hosts of malware downloads. Popular search engine terms are also targeted, providing results into link farms that lead to Web threats. In today’s world of dynamic Web content, static, first generation URL databases that update infrequently are ineffective as a defense layer.

Dynamic Link Analysis leverages a broad and diverse user community to profile more Web content and apply more defenses than a single user could maintain. Real-time inputs from this community into the WebPulse service, as well as cloud-based analysis and updates, protect users from dynamic links to malware or other malicious content.

“The emergence of malware that preys upon people’s trust in legitimate Web sites and utilizes the Web as a tool for spreading malicious content in a viral manner underscores the requirement for proactive layers of defense,” said Mikko Valimaki, chief scientist at Blue Coat Systems. “WebPulse implements Dynamic Link Analysis to provide the real-time community watch environment with continuous inputs, assessments and cloud protection that businesses require to keep pace with today’s rapidly evolving threat landscape.”

### **Immediate Protection through WebPulse Community Watch**

The Blue Coat WebPulse community watch service builds a comprehensive profile of Web content with real-time inputs from both businesses and consumers to protect users from new and evolving malware and malicious content. More than 54 million users of BlueCoat® WebFilter and ProxyClient® enterprise products as well as users of K9® Web Protection, Blue Coat’s free software for consumers, send more than one billion requests to the WebPulse service weekly.

The Blue Coat WebPulse service leverages multiple threat engines in addition to machine analysis and human raters. Utilizing these analysis tools, the service provides immediate updates to the WebPulse database to protect all remote users and Web gateways against known and new malicious content, compressing the analysis cycle for dynamic links and Web content.

### **About Blue Coat Systems**

Blue Coat Systems is the technology leader in Application Delivery Networking. Blue Coat offers an Application Delivery Network Infrastructure that provides the visibility, acceleration and security required to optimize and secure the flow of information to any user, on any network, anywhere. This application intelligence enables enterprises to tightly align network investments with business requirements, speed decision making and secure business applications for long-term competitive advantage.

*FORWARD LOOKING STATEMENTS: The statements contained in this press release that are not purely historical are forward-looking statements, including statements regarding Blue Coat Systems’ expectations, beliefs, intentions or strategies regarding the future, and including statements regarding the capabilities and expected performance of Blue Coat Systems’ products. All forward-looking statements included in this press release are based upon information available to Blue Coat Systems as of the date hereof, and Blue Coat Systems assumes no obligation to update any such forward-looking statements. Forward-looking statements involve risks and uncertainties, which could cause actual results to differ materially from those projected. These and other risks relating to Blue Coat Systems’ business are set forth in Blue Coat Systems’ Form 10-Q for the quarter ended January 31, 2009 and Form 10-K for the year ended April 30, 2008, filed with the Securities and Exchange Commission.*

### **About GEOBRIDGE**

Since 1997, GEOBRIDGE (www.GEOBRIDGE.net) has been providing information security solutions to global clients. Today our client list includes Fortune 500 companies, financial institutions, health care, government agencies and defense clients across North America and internationally. GEOBRIDGE helps clients mitigate risk and realize significant value from their IT investments while allowing clients to focus on the growth and profitability of their company. Our team provides solutions, integration services and consultancy in the areas of encryption, network security, identity management, transaction security, and compliance. Due to the increased needs for compliance with internal governance, and external legal and regulatory requirements, we have expanded our compliance and security best-practices offerings to address information assurance. GEOBRIDGE is a Qualified Security Assessor company (QSAC) certified by the Payment Card Industry (PCI) and a TG-3 Assessor recognized by the Electronic Funds Transfer (EFT) networks.