December 15, 2009

FireEye Expands Federal Market Presence to Help Government Agencies Combat Targeted Malware Attacks and Cyber Criminal Activities

Company Appoints Proven Veteran Gene Skiba as Vice President of Federal Sector, Establishes Local Beltway Office

Milpitas, Califorinia and Herndon, Virgina - Dec 15, 2009 – FireEye, Inc., the leader in modern malware protection systems, today extended its efforts to help the U.S. Federal government address global cyber warfare, targeted malware attacks, and cyber security threats, appointing Gene Skiba as vice president, federal sector, and opening a new office in the Washington Beltway. Skiba, a seasoned federal sales veteran, is responsible for defining and executing the sales strategy for FireEye's malware protection systems within the public sector, military/defense and intelligence markets.

Skiba has more than 15 years of experience in telecommunications, networking and security. Prior to joining FireEye, Skiba served as the vice president of the U.S. Public Sector at BlueCat Networks, where he established a Federal sales strategy that included distribution and channel programs to support Federal business. Before BlueCat, Skiba was vice president of U.S. government sales and operations at F5 Networks where he implemented a sales strategy aligned closely with independent software vendors (ISVs) and solutions partners. Prior to F5 Networks, Skiba held various senior level positions at eEye Digital Security, within government and international sales at Nortel Networks and Alteon Websystem (acquired by Nortel).

"Our nation's cyber security is vulnerable to global cyber criminal and cyber espionage threats, as well as targeted malware-based cyber attacks that increasingly pose a danger to our critical infrastructure," said Skiba. "FireEye's unique technology fills the security gaps left by existing security solutions. The continued adoption of FireEye's technology throughout the federal market and In-Q-Tel's recent investment in FireEye is strong validation of the market opportunity for FireEye's solutions."

National cyber security remains a high priority for the U.S. government, customers and partners. Recently, the GAO's Homeland Security and Justice Team noted several cyber security challenges the Department of Homeland Security should tackle. Three of these challenges included bolstering cyber analysis and warning capabilities, improving cyber security of infrastructure control systems and addressing cyber crime. Modern malware is at the heart of these threats. Modern malware exploits the popularity of browser-based (Web 2.0) applications, mobile computing and social networking to infiltrate enterprise, government and consumer systems on a massive scale. Malicious software (malware) is commonly embedded into user-generated content websites, PDFs, online search ads and high-traffic Web applications to take over computer systems and build "callback channels" out of infiltrated networks. The fusion of Web-borne, targeted malware with advanced intrusion and data theft payloads readily bypass traditional network security and are used to exfiltrate confidential data and resources.

FireEye provides federal, state and local agencies with a valuable combination of next-generation malware protection and extensive security research that enhances cyber security infrastructure. FireEye's solution fills the security gaps left by existing security products to protect against targeted attacks and cyber criminal and cyber espionage activities that seek to steal, compromise, alter, or completely destroy sensitive information. FireEye has advanced modern malware analysis through the unique FireEye Analysis and Control Technology, and continues to push the envelope in the development of products and security research services to serve the broader public and private sectors.

"Cyber crime and cyber espionage have no barriers - they span companies, countries and continents," said Ashar Aziz, CEO, FireEye, Inc. "FireEye's cyber security appliances and Malware Analysis & Exchange (MAX) network service offers customers the first complete global and local malware protection system to precisely identify, understand, and stop targeted malware attacks and botnets. FireEye's security architecture also offers the federal government an extensible security platform as cyber crime and cyber espionage move to new attack vectors. Through this expansion, we are adding significant resources to address the growing targeted malware and botnet threat to consumers, enterprises and government agencies alike."

For the latest updates on malware and botnet research, visit the FireEye Malware Intelligence Lab's blog at http://blog.fireeye.com/, or follow the company on twitter at http://twitter.com/fireeye

About FireEye, Inc.

FireEye, Inc. is the leader in malware protection systems, enabling organizations to protect critical infrastructure, intellectual property, and networks against Web malware and botnet infiltration. The FireEye Malware Protection System is a next-generation malware analysis platform featuring the network use of transparent virtual machines to uncover zero-day malware, botnets, and targeted attacks that circumvent today's technologies such as intrusion prevention systems, antivirus, and URL filters. By essentially eliminating false positives, FireEye re-defines effective network security. The company is backed by Sequoia Capital, Norwest Venture Partners, JAFCO, SVB Capital, DAG Ventures, and Juniper Networks. For more information, contact (408) 321-6300 or email: info@fireeye.com. Visit us at www.FireEye.com.

###