FOR IMMEDIATE RELEASE

BT ETHICAL HACKING CENTER TESTING CONFIRMS FN CONNECT SECURE CLIENT AGENT STOPS ALL COMMON DESKTOP END-USER COMPUTER ATTACKS

The Third in a Series of Independent Tests Demonstrates the Effectiveness of Federated Networks' Breakthrough Cyber Security Technology Against Spyware and Other Malicious Desktop Threats

TORONTO, Ontario February 1, 2011–Federated Networks today announced that the BT Ethical Hacking Center was unable to compromise end users protected by Federated Networks FN Connect Secure Client Agent. During a recent round of testing, ethical hackers failed to log keystrokes, capture screens or successfully execute man-in-the-browser and a variety of other attacks against clients running the Federated Networks software. Earlier testing by BT validated the efficacy of the FN ASL protocol, which thwarts common network vulnerabilities, such as phishing and man-in-the-middle attacks as well as the FN Connect Secure Web Application Gateway's elimination of common security vulnerabilities inherent in web applications, such as the Open Web Application Security Project (OWASP) 2010 Top 10 web-based vulnerabilities.

To validate the effectiveness of its solution, FN provided BT with a blank slate in selecting the "best-of-the-best" known malware attacks and tools, a formidable arsenal to say the least, augmented for completeness and comparison at FN's request with certain tools utilized by FN's competitors in assessing the veracity of their solutions. In summary, none of hacking tools or methods were able to steal user data – a copy of the full report is available here.

It is well understood within the security community and growingly by end user's that existing solutions, particularly those provided by the "anti-vendors" fall appallingly short of providing comprehensive threat mitigation against increasingly sophisticated malware. "It's pretty clear that the bad guys are better at getting malware onto your computer than the anti-vendors are at keeping it off", said David Lowenstein, FN's CEO "the sterilization approach didn't work for Howard Hughes and its not working in cyber-security either."

FN has taken radically different approach whereby FN's technology effectively "immunizes" a User's system form the payloads or effect of identity, data, or content theft oriented malware. More specifically, FN's Acute Threat Model not only assumes that some form of malware will make its way onto a User's computer, but rather that all of the most potent variants of known malware are on the computer at once, operated combinatorially by an expert, on a completely compromised host, assuming the worst of all conditions of the host environment:

i. The OS has not been patched
ii. The OS passwords have been compromised
iii. The User's browser is not patched, security settings are at their lowest and the User could be running the oldest versions of the browser software (i.e. IE6 vs. IE8)

and even under these admittedly extreme assumptions of the FN Acute Threat Model, User data and content must be kept secure.

"We are very pleased to report that BT has validated in this assessment our contention that there are no known generic threats or tools that can compromise FN protected user data," said Risu Na, Chief Technology Officer at Federated Networks. "Obviously this is an important outcome for all enterprises and end users in the war on f identity ,data or content theft , for our solution provably mitigates all current, best-of-breed keyloggers, screen capture and man-in-the-browser (M-I-B) threats. Importantly, these same technologies that now protect login and ecommerce also protect all of user or company communications, including email, IM and social networking applications."

Detailed reports outlining each of the three testing sequences performed by BT, including the current FN client/desktop security testing as well as the previous testing of FN Connect Secure Web Application Gateway and the FN ASL protocol, are available here. Also available on the Federated Networks website is more technical information about the company's products, solutions and technology.

The FN Connect Secure Client is a key part of The FN Connect Securely™ Framework, which provides the foundational infrastructure for securing planned Internet initiatives, such as secure e-statements and e-billing, e-voting, e-currency and e-health applications. Additionally, the company's technologies significantly strengthen military mission critical command and control IT infrastructure including solving several of the U.S. military's most challenging cyber security challenges, as outlined by the INFOSEC Research Council's "Hard Problems List", while meeting the stringent secure coding requirements of the Joint Strike Fighter(JDF) plane, as well as the quality and maintainability metrics outlined by NASA for the coding of space shuttle software.

About Federated Networks
Federated Networks enables consumers, corporations and government to Connect Securely™ to all things digital. The FN Connect Securely™ Architecture seamlessly and comprehensively protects content and communications against networked software's most pervasive threat vectors. Federated Networks' breakthrough cloud native, zero-knowledge protocol guards against identity theft and data compromise of any kind, whether it resides on social networks or secure servers. Establishing the new standard for cyber confidence, Federated Networks enables user centric control of the security and access rights of personal information and data. Founded in 2005, Federated Networks is privately held and headquartered in Toronto, Ontario. For more information please visit http://www.federatednetworks.com.

About BT Managed Security Solutions Group
As the authority on enterprise security, BT's Managed Security Solutions Group combines managed security services portfolio with an Ethical Hacking Center of Excellence, offering its customers the only Human Computer Interface extended end-to-end security solutions in the industry. BT has been offering security services to the Fortune 1000 since 1991 and has performed thousands of Ethical Hacking assignments on a variety of systems and applications, including network infrastructure, online banking and trading and ecommerce. BT's Ethical Hacking (EH) services enable customers to protect their networks, information assets, and corporate reputations by identifying vulnerabilities before they can be exploited.

Contacts:

David Lowenstein, Federated Networks
905-361-2834
Dave@FederatedNetworks.com

Shweta Agarwal, Schwartz Communications
781-684-0770
federatednetworks@schwartz-pr.com