August 20, 2012

Fortinet(R) Further Enhances Its Bring-Your-Own-Device (BYOD) Network Security Solution With New Mobile Clients

New Versions of FortiClient™ for Android and iOS Platforms Now Available as Part of End-to-End Security Solution

SUNNYVALE, CA -- (Marketwire) -- 08/20/12 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today announced key enhancements to address the numerous challenges surrounding network, data and device security posed by the Bring Your Own Device (BYOD) phenomenon wherein end users are bringing their own smartphone and tablet devices to their work environments. As part of its broad strategy to apply effective security measures for BYOD environments, Fortinet is introducing new versions of its FortiClient application for iOS and Android platforms that are downloadable from the iTunes store at: http://itunes.apple.com/us/app/forticlient/id525600370?mt=8.

And on Google Play at:
https://play.google.com/store/apps/details?id=com.fortinet.forticlient&hl=en

The FortiClient application for Android platforms allows for both SSL tunnel mode and IPSec VPN connections to FortiGate appliances. The end user connection is fully encrypted and all traffic is sent over a secure tunnel. The updated FortiClient application for iOSdevices provides Web-mode SSL VPN functionality and has been modified for the iPad platform.

Fortinet's comprehensive BYOD security strategy, which is designed to protect organizations by authenticating devices, controlling user behavior in the network and restricting data access rights, is built around a combination of six key differentiating capabilities:

- A wide range of high-performance deployment options supporting LAN and WAN connectivity centered around the FortiGate family of appliances
- The lack of 'per-user' or 'per-seat' licensing means that customers can add new devices to their network without incurring additional license fees. This feature becomes critical as the number of devices attached to the network can double or even triple due to users bringing their smartphones and tablets to work
- Centralized "single pane of glass" management
- Integrated wireless controllers in all FortiGate appliances for improved application and user visibility and control, rogue access point detection, guest access and bandwidth management
- Built-in Wi-Fi for secure LAN deployments on certain FortiGate models reduces the need for a separate wireless access point
- Mobile VPN clients and interoperable soft-tokens for two-factor authentication

The Scope of the BYOD Security Challenge
In a recent global survey of Gen-Y BYOD users conducted by Fortinet in fifteen countries -- including the U.S., western Europe, the Middle East and Southeast Asia -- 42 percent of respondents believe potential data loss and exposure to malicious IT threats are the dominant risks posed by BYOD to their organization. Despite these concerns, more than a third of respondents admitted they have or would contravene a corporate policy banning the use of personally owned devices for work purposes.

Traditional Approaches Falling Short
While the security challenges associated with mobile devices are not necessarily new, BYOD environments make it difficult for organizations to enforce corporate security policies. The broad scope of Fortinet's security solution, including application control, next generation firewall, intrusion prevention, antimalware, antispam and data leak prevention helps organizations ensure that information flowing to and from mobile devices is protected on both the LAN and WAN.

Fortinet's Approach to the BYOD Security Challenge
As a network-based solution, Fortinet supports a variety of approaches to smartphone and tablet security. This includes support for Mobile Device Management (MDM), Virtual Desktop and third party VPN clients.

"While mobile devices have tremendous potential for enhancing productivity, the challenge for organizations today is to provide the same level of security regardless of the device or location of the user," said Kevin Flynn, senior product manager at Fortinet. "We're helping organizations of all sizes -- from SMBs to large enterprises -- deploy a robust BYOD security infrastructure that uniquely combines integrated wireless functions, embedded security technologies and simple, cost-effective licensing."

Availability
The free FortiClient applications for iOS and Android platforms are available for download now. IPSec functionality on the Android client is expected to be available on Monday, September 3.

Follow Fortinet Online: Subscribe to threat landscape reports: http://blog.fortinet.com/feed/; Twitter at: www.twitter.com/fortinet; Facebook at: www.facebook.com/fortinet; YouTube at: http://www.youtube.com/user/SecureNetworks

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2011 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

Fortinet has not independently verified statements or certifications herein attributed to third parties, and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release may contain forward-looking statements that involve uncertainties and assumptions. Changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

Media Contact:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media