June 19, 2012

Fortinet(R) Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems

Over 1-in-3 Respondents Would Contravene Company Policy Banning the Use of Personal Devices at Work or for Work Purposes

SUNNYVALE, CA -- (Marketwire) -- 06/19/12 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- has conducted a global survey that reveals the extent of the challenge posed to corporate IT systems by first generation Bring Your Own Device (BYOD) users; people entering the workplace with an expectation to use their own devices. The survey describes the degree to which security is widely given low consideration by Gen-Y employees using their own devices, including the disturbing fact that more than 1-in-3 employees would contravene a company's security policy that forbids them to use their personal devices at work or for work purposes. Overall, the findings underscore the urgency with which enterprises should develop security strategies to successfully secure and manage BYOD activity.

The survey, conducted in 15 territories* during May/June 2012, asked over 3,800 active employees in their twenties about their perspectives on BYOD, its impact on their work environment and their approach to personal and corporate IT security.

Strong Dependence on Personal Communications Means BYOD is Here to Stay
Within the demographic of the survey, which represents tomorrow's management and decision makers, BYOD is confirmed as a mainstream activity. Nearly three quarters (74%) of respondents across all territories already regularly engage in the practice. More importantly, 55% of respondents view using their device at work as a 'right' rather than a 'privilege.'

From a user perspective, the primary driver of the BYOD practice is that individuals can constantly access their preferred applications, especially social media and private communications. The dependence on personal communications is strong with 35% of respondents admitting they could not go a day without accessing social networks and 47% unable to last a day without SMS.

Lax Consideration of Business Risks Means Workers Contravene Corporate Policy
The first generation of BYOD workers understand the risks posed by BYOD to their organization. 42% of the survey sample actually believe potential data loss and exposure to malicious IT threats to be the dominant risk. Yet, worryingly for IT departments, this risk awareness does not prevent those workers from bypassing corporate policies. In fact, more than a third of respondents (36%) admitted they have or would contravene a corporate policy banning the use of personally-owned devices for work purposes. Of the 15 countries surveyed, the figure is highest in India where 66% admitted they have or would contravene policy.

When asked about policies banning the use of non-approved applications, the figure remains approximately the same, with 30% of all respondents admitting they have or would contravene policy. The risk to organizations from non-approved applications looks set to grow. Indeed, 69% of respondents confirmed they are interested in Bring Your Own Application (BYOA) -- where users create and use their own custom applications at work.

The survey also hinted at the resistance organizations might face with regards to implementing security on an employee's device. The majority (66%) of respondents consider themselves -- not the company -- to be responsible for the security of the personal devices they use for work purposes. This is three times the number who believes responsibility ultimately rests with their employer (22%).

"The survey clearly reveals the great challenge faced by organizations to reconcile security and BYOD," said Patrice Perche, international vice president of International Sales &Support for Fortinet. "While users want and expect to use their own devices for work, mostly for personal convenience, they do not want to hand over responsibility for security on their own devices to the organization. Within such an environment, organizations must regain control of their IT infrastructure by strongly securing both inbound and outbound access to the corporate network and not just implement mobile device management or 'MDM.' Organizations cannot rely on a single technology to address the security challenges of BYOD. The most effective network security strategy requires granular control over users and applications, not just devices."

Note for Editors
The Fortinet Internet Security Census 2012 was a research exercise undertaken between May 31 - June 12, 2012 on behalf of Fortinet by independent market research company Vision Critical. The survey involved 3,872 university graduate level individuals aged 20 to 29 and in full time employment, who own their own smartphone, tablet or laptop.

*15 territories participated in the survey: USA, UK, France, Germany, Italy, Spain, Poland, UAE, India, South Korea, China, Singapore, Taiwan, Japan and Hong Kong.

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

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contact:

Rick Popko

Fortinet

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media