Press Release

Media Contact:

Amber Dale
amber@chatterboxpre.com
+971 50 792 2652

IT Leaders Reveal Harsh Realities of Protecting Businesses in Fortinet Global Survey

Enterprise Security Decisions Reach Board Level and Take Primary Consideration Among Business Initiatives

Dubai, UAE, November 2, 2014 - Ninety percent of CIOs and CTOs believe the job of keeping their enterprise protected is becoming more challenging according to new research from Fortinet® (NASDAQ: FTNT), a global leader in high-performance network security. Serious boardroom pressure to keep the enterprise secure has jumped almost one-third in the last 12 months, making security paramount and a primary consideration over other business initiatives. This and other findings come from an independent survey commissioned by Fortinet of over 1,600 enterprise IT decision makers (ITDMs), largely from 500+ employee organizations around the world. All respondents were sourced from independent market research company Lightspeed GMI's online panel.

Survey highlights include:

- Among IT decision makers recording the highest boardroom pressure, 63 percent admit abandoning or delaying at least one new business initiative because of IT security concerns.
- The increasing frequency and complexity of threats (88 percent) and the new demands of emerging technology like the Internet of Things (IoT) and biometrics (88 percent) pose the biggest challenge to ITDMs to keep their organizations secure.
- The majority of ITDMs have been provoked into action by rising data privacy concerns (90 percent) and securing big data initiatives (89 percent); in the majority of cases this means new IT security investment.

Boards Prioritize Security

The growing awareness of IT security within the boardroom – and its resulting pressure and involvement – was cited as a major contributor to making the IT security job more difficult, with three-quarters rating awareness of senior management as 'high' or 'very high' today, up from barely 50 percent one year prior. The survey also unveils that a total of 53 percent of all ITDMs surveyed have slowed down or cancelled a new application, service or other initiative because of cyber-security fears. The figure is 63 percent among those reporting a very high level of boardroom pressure and scrutiny around IT security. Mobility related applications and strategies are the biggest sticking points, with cloud also scoring high.

Security Concerns Rise with Emerging Technology

The rising volume/complexity of advanced persistent threats (APT), DDoS attacks and other cyber threats, and the demands of emerging technology trends like Internet-of-Things and biometrics, are the most prevalent drivers making ITDMs' jobs more challenging. There is a big expectation across industry sectors for biometrics to arrive very soon, with 46 percent claiming the technology has already landed or will do so in the next 12 months. Two-thirds say they already have the tools to ensure it can be managed securely. Of the third that doesn't feel prepared today, one-third of those believe they will struggle to secure biometrics in the future as well.

Data Privacy & Big Data Security Drive Increased Spending

The high profile issues surrounding data privacy are provoking action, with 90 percent of ITDMs planning to change their outlook on IT security strategy in response. Of these, 56 percent are inclined to invest more money and resources to address the challenge, with 44 percent preferring instead to rethink existing strategy.

Meanwhile 'Big Data' and data analytics was cited by 89 percent of respondents as a change driver for IT security strategy, with 50 percent of these planning investments.

Industry sectors with the highest predisposition to invest in IT security were financial services (53 percent) and telecoms/technology (59 percent). The research also indicated organizations of greatest size have the greatest tendency to invest.

When asked if they had been provided with sufficient human and financial resources for IT security in the last 12 months, four-out-of-five ITDMs said yes. A total of 83 percent feel they will also have sufficient resources in the next 12 months. Most industry sectors carried this trend, for example with public sector going from 74 to 77 percent and retail from 80 to 81 percent. Financial services sector ITDMs feel best equipped (87 percent for the next 12 months), though their trend is downward (89 percent for the past 12 months).

Findings Show Need for Cyber Resilience

"With IT security on the boardroom agenda, this and other challenges are clearly adding weight onto the shoulders of senior IT professionals and questioning the ability of some organizations to exploit innovation while remaining secure," said John Maddison, vice president of marketing products, at Fortinet. "These organizations must act now to address the impact of the growing threat environment and increased scrutiny on IT security, re-evaluating their goals to ensure they strike the right balance and achieve resilience in the face of cyber threats."

The good news is that many are positive and feeling well equipped with human and financial resources for the IT security challenges that lie ahead. However, to do so points toward intelligent new strategies and more investment in security technologies."

-ends-

Note to Editors

The Fortinet Security Census 2014 was a research exercise undertaken on behalf of Fortinet by independent market research company Lightspeed GMI. The survey involved 1,610 qualified IT decision makers – predominantly CIOs, CTOs, IT Directors and Heads of IT – largely from organizations larger than 500 employees.*

15 countries participated in the survey: Australia, Brazil, Canada, China, Colombia, France, Germany, India, Italy, Japan, Korea, Mexico, Spain, UK and USA.

*8% of respondents came from organizations in the 100 to 500-employee bracket.

About Fortinet

Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com.

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, Fortinet reserves the right to, and may, change its plans at any time without notice in its sole and absolute discretion, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions, such as statements regarding Fortinet's intentions related to its current and future activities in Singapore. Changes of circumstances, a change of plans in Fortinet's sole and absolute discretion, 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.