FORTINET.

May 15, 2014

Custom Technology Adoption Profile Survey Reveals Recent Security Breaches Among Top Purchasing Drivers for Next-Generation Firewalls (NGFW)

Current and Quantitative Results From Enterprise Security Peers Highlight NGFW Purchasing Plans, Requirements and More

SUNNYVALE, Calif., May 15, 2014 – Fortinet® (NASDAQ: FTNT), a global leader in High-Performance Network Security, today published the results of a new commissioned survey conducted by Forrester Consulting that reveals the purchasing plans, drivers and requirements enterprise network security professionals are considering when evaluating a next-generation firewall (NGFW). The Forrester Technology Adoption Profile Study, "Firms Turn to Next-Generation Firewalls to Tackle Evolving IT Threats," takes a current and qualitative look at the NGFW landscape and provides insights directly from security peers. The survey sample consisted of 229 network security professionals from organizations with 1,000 or more employees in the US, Canada, UK, France and Germany. And survey respondents were involved with IT security investment decision-making and were at the manager level or higher.

NGFW Adoption Drivers
When asked what the key drivers were for their current or planned next-generation firewall project, survey respondents said, "Expanding/re-architecting infrastructure" (56%), "Recent security breaches that we've seen in the news" (54%) and, perhaps most surprising, "Recent security breach within our own organization" (44%).

The above results help to explain the key requirements expected in an NGFW today. In ranking the top 5 features when selecting a next-generation firewall system," 71% of the respondents selected "Advanced threat capability (i.e. sandbox).". This was closely followed by stateful firewall at 70%. Antivirus (67%), Authentication (65%) and SSL (62%) rounded out the list.

"What security teams want are integrated controls that can scale and change as threats constantly mutate. Hence we see the irreversible trend toward NGFW dominance in the security gateway market," the study concludes. "Today, customers want NGFWs that do more than firewalling and IPS/app control; they want gateways that fight advanced threats like zero-day malware and respond to new cybercriminal tactics such as encrypting payloads or stolen data inside of an SSL tunnel."

With that in mind, when respondents were asked to rank their top decision criteria when selecting a next-generation firewall system, security effectiveness was far and away the top response, with 63% ranking it in the top three. This was followed by product performance (throughput, latency, reliability) at 41% and compatibility with current infrastructure at 39%. Of note, trusted provider/brand was cited in the top three only 25% of the time and reporting/visibility only 14% of the time.

"Today organizations are tired of security vendor marketing, focusing instead on a product's quantified ability to do the job," said John Maddison, VP of Marketing at Fortinet, "This is why Fortinet advocates third-party, real-world effectiveness and performance testing and participates in so many tests performed by credible test houses like NSS Labs, Virus Bulletin, Ixia and more. We encourage all organizations to test products in their own environments under production workloads or, barring that, to at least evaluate credible, third-party tests before making a strategic or important buying decision."

The complete survey study can be downloaded at http://www.fortinet.com/resource_center/whitepapers/forrester-survey-report-ngfw-purchasing.html.

Live Webinar
Please join our live **webinar**, "Peer Perspective: Top Drivers, Requirements and Selection Criteria for NGFWs" on Friday, June 6th, at 9:30am. Guest speaker John Kindervag, vice president and principal analyst for Forrester Research, will discuss the survey's findings and what they mean in more detail. Register at
https://attendee.gotowebinar.com/register/4877555985008501762

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.

and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiAP, FortiDB, FortiVoice and FortiWeb. Other trademarks belong to their respective owners. 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. Changes of circumstances, product release delays, changes in product plans and 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 prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements. 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 forward-looking statements.
FTNT-O

Media Contact:
Rick Popko
Fortinet, Inc.
408-486-7853
rpopko@fortinet.com

Investor Contact:
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Source: Fortinet

News Provided by Acquire Media