October 12, 2015

Fortinet Delivers Advanced Cybersecurity to Software-Defined Data Centers

Fortinet's FortiGate VMX With VMware NSX Enables Automated Policy-Driven Network Segmentation for the Data Center

SUNNYVALE, CA -- (Marketwired) -- 10/12/15 -- Fortinet® (NASDAQ: FTNT) -- the global leader in high-performance cybersecurity solutions, today announced their FortiGate VMX next-generation and internal segmentation firewall (NGFW/ISFW). The FortiGate VMX with the VMware NSX® network virtualization platform enables organizations to automate advanced cybersecurity in the Software-Defined Data Center (SDDC).

Advanced Security for Dynamic Data Centers

Working in collaboration with VMware, Fortinet developed the FortiGate VMX to fully leverage the capabilities of the VMware NSX network virtualization platform, enabling customers to automate the insertion, deployment and orchestration of FortiGate VMX for threat protection inside their data center environments.

"NTT Com Security has been working closely with our clients and industry leaders like Fortinet to leverage the security benefits of network virtualization," said Dave Polton, chief technology architect at NTT Com Security. "Bringing cloud and security technologies together with the VMware vSphere and VMware NSX platforms enables our clients to benefit from greater security and efficiency as we transition them to a fully Software-Defined Data Centre (SDDC), while empowering our customers with even better levels of managed service."

Policy Driven Network Segmentation

Recent high-profile security breaches have highlighted the need for security solutions that expand beyond the traditional edge defense strategies and segment networks internally, avoiding the rapid spread of threats once inside the data center. VMware brings an SDDC approach to network security with micro-segmentation, isolating communications across unrelated networks, controlling the communications within a network and integrating with advanced security services like Fortinet's Internal Segmentation Firewalls (ISFW).

The native security capabilities of VMware NSX, including micro-segmentation, distributed firewalling and security operations automation, enable policy-based segmentation of network traffic and threat protection at the workload level controls for East-West traffic. The NSX distributed service framework enables dynamic insertion of Fortinet's ISFW/NGFW technologies using Fortinet's Network Security Function Virtualization (NSFV) feature. Based on Virtual Domain (VDOM) technologies, a multi-tenant system can be defined with different security policies enabled. This granular approach enables service providers and larger enterprises to set up per-customer or per-business unit security policies. Fortinet also provides high-speed, north-south network security appliances, providing a holistic data center solution under a single policy model.

"Fortinet has been working closely with VMware to arm customers with the same level of cybersecurity inside the data center as they do at the perimeter. FortiGate VMX demonstrates our commitment to the VMware partnership and ecosystem," said John Maddison, vice president of products and solutions at Fortinet.

About Fortinet

Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments -- be it virtualized/cloud or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at http://www.fortinet.com, the Fortinet Blog or FortiGuard Labs.

or trademarks of VMware, Inc. in the United States and other jurisdictions. 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 contains forward-looking statements that involve uncertainties and assumptions, such as statements regarding product releases. 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
Sandra Wheatley
Fortinet, Inc.
408-391-9408
swheatley@fortinet.com

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

Analyst Contact
Ron Davis
Fortinet, Inc.
415-806-9892
rdavis@fortinet.com

Source: Fortinet

News Provided by Acquire Media