



February 3, 2015

Fortinet Joins the VMware NSX Partner Ecosystem to Further Advance Security for the Software-Defined Data Center

Fortinet Unveils the New FortiGate-VMX Firewall Engineered for VMware Virtualization Solutions

SAN FRANCISCO, CA -- (Marketwired) -- 02/03/15 -- **VMware 2015 Partner Exchange** - Fortinet® (NASDAQ: FTNT) - a global leader in high-performance cyber security solutions, today announced that the company has joined the VMware NSX™ partner ecosystem. Committed to providing leading security solutions for virtualization, Fortinet also revealed its new FortiGate-VMX firewall appliance, which will enable greater security for customers within agile, elastic software-defined data centers based on VMware vSphere® and VMware NSX virtualization platforms.

Fortinet is proud to be the Silver sponsor for the 2015 VMware Partner Exchange. To test drive the FortiGate-VMX and get more information about FortiGate-VMX, please visit Moscone West Booth #701.

Security for Virtual and Physical Worlds

Rapid industry adoption of cloud and virtual infrastructure has created a need for transforming the way security is applied in the data center. With Fortinet's new VMX solution, VMware vSphere and VMware NSX customers will be able to leverage Fortinet's leading approach to security, which automates the orchestration of network security with seamless centralized management across physical and virtual domains.

"The SDDC promises a highly automated, easily managed platform that embraces and secures all applications, for fast, safe deployment across data centers, clouds and mobile devices," said Mary Yang, vice president of business development at Fortinet. "Fortinet and VMware are uniquely positioned to deliver on this promise, providing the highest levels of security in virtualized environments."

FortiGate-VMX, Securing Data Centers in Transition

Today's data center is rapidly changing in response to cloud, big data, software and infrastructure-as-a-service. Software Defined Networking and Software Defined Data Centers are also creating very dynamic environments which challenge the status quo of how network services are delivered.

In many data center environments, hardware security appliances are deployed at the aggregation layer and can only see "north-south" traffic passing through the physical network. Conversely, inter-VM traffic (i.e. "east-west" traffic) does not leave the virtual switch in the virtual host, and network virtualization and software-defined architectures further exacerbate the volume of virtual traffic.

To address these challenges, the FortiGate-VMX solution interoperates with VMware virtualization solutions in the SDDC, providing API integration that gives customers greater visibility and control of virtual network traffic regardless of network topology. In addition, orchestration with VMware's platform allows for automatic protection of new workloads. Key FortiGate-VMX features include:

- Current interoperability with VMware vSphere and vCloud Suite®
- Future interoperability with VMware NSX
- Centralized management across FortiGate-VMX security appliances
- Visibility into all vSphere virtual network traffic
- Auto-deployment and provisioning FortiGate-VMX elastically to new ESXi hosts
- Instant-on protection of new VM workloads
- Ability to retain session-state across vMotion® live migration events
- Object-based protection rules that follow VM's across IP or MAC address changes

"Purpose-built virtual security appliances will be increasingly used alongside hardware appliances to secure enterprise data centers, which are becoming increasingly dynamic due to rapid adoption of server virtualization and SDN," said Jeff Wilson, Principal Analyst, Security for Infonetics. "Fortinet is doing well in enterprise data centers, with a string of new customer wins and highly competitive hardware price-to-performance; this success will be bolstered by virtual appliance integration with VMware's virtualization and SDDC platform."

Availability:

The FortiGate-VMX firewall appliance will be available in March of this year.

For more information, visit:

Fortinet FortiGate-VMX Product Page

<http://www.fortinet.com/products/fortigate/vmware-virtual-appliance.html>

Fortinet FortiGate-VMX Solution Guide

http://www.fortinet.com/resource_center/solution_briefs/sdn-security-for-vmware-data-center-environments.html

VMware NSX

<http://www.vmware.com/products/nsx/resources>

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](#)

Copyright © 2015 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks 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 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

Andrea Cousens

Fortinet, Inc.

310-270-8903

[Email contact](#)

Dan Mellinger

Fortinet, Inc.

415-572-0216

[Email contact](#)

Source: Fortinet

News Provided by Acquire Media