October 14, 2013

Fortinet Expands Virtual Security Ecosystem: Supports Windows Server Hyper-V and KVM in Addition to VMware and Citrix

Company Now Provides Industry's Most Comprehensive Virtualized Security Solutions

SUNNYVALE, CA -- (Marketwired) -- 10/14/13 -- Fortinet® (NASDAQ: FTNT) -- a global leader in high-performance network security -- today announced an expansion of its virtual security ecosystem that now supports Microsoft's Windows Server Hyper-V as well as the Kernel-based Virtual Machine (KVM) virtualization infrastructure. Designed for data centers, MSSPs, cloud service providers and enterprises building out private cloud infrastructures, Fortinet's virtual security ecosystem delivers critical security services between virtual machine instances. In addition, it uniquely delivers centralized management of virtualized and physical infrastructures through a "single pane of glass" approach to management.

Today's announcement comes on the heels of news Fortinet made at VMworld in August. There, the company demonstrated a proof-of-concept integration with VMware's recently announced NSX network virtualization platform that delivers security policy enforcement of communication across and between physical and logical workloads.

In September, Fortinet announced its FortiGate-VM virtual appliance received Common Criteria EAL 4+ certification for its intrusion detection, application firewall and general firewall performance. EAL 4+ is the highest level of certification a network security vendor can receive in the category of network firewall.

By adding support for Windows Server Hyper-V and KVM on top of its existing support for VMware, Citrix XenServer and Open Source Xen virtualization technologies, Fortinet now delivers the industry's most comprehensive range of security solutions for virtualized infrastructures.

"Windows Server includes powerful functionality that helps our customers transform their IT operations to reduce costs and deliver a new level of business value," said Brian Hillger, Director, Server and Tools Marketing at Microsoft. "With Windows Server and Fortinet's security ecosystem, our joint customers can deploy an industry-leading solution with confidence that their virtualized infrastructures are more secure."

Comprehensive Virtualized Security Solutions

Fortinet's virtual security ecosystem delivers VMware and Windows Server Hyper-V support for its FortiGate-VM, FortiAnalyzer-VM and FortiManager-VM virtual appliances and adds KVM support for its FortiGate-VM virtual appliance.

FortiGate-VM provides consolidated, multi-threat security in a virtual form factor and is available in five virtual appliance models. Each FortiGate virtual appliance offers protection from a broad array of threats with support for all of the security and networking services offered by the FortiOS 5 operating system.

FortiAnalyzer-VM securely aggregates log data from Fortinet physical and virtual appliances and other syslog-compatible devices. Using a comprehensive suite of easily customized reports, users can filter, review and mine records, including traffic, event, virus, attack, Web content and email data, to determine an organization's security stance and helps assure regulatory compliance.

FortiManager-VM delivers a centralized management system that serves as the command and control for Fortinet infrastructure, offering the same powerful network security management features as its hardware-based version. Fortinet virtual appliances enable customers to deploy a mix of physical and virtual appliances, operating together to enforce a common set of policies, and managed from a centralized FortiManager platform.

With today's announcement, Fortinet is also introducing FortiCache-VM to its virtual security ecosystem and Citrix XenServer and Open Source Xen support for the FortiWeb-VM virtual appliance family.

FortiCache-VM offers high performance Web caching to address bandwidth saturation, high latency, and poor performance caused by caching popular Internet content locally for carriers, service providers, enterprises and educational networks. FortiCache physical and virtual appliances reduce the cost and impact of cached content on the network or in the cloud, while increasing performance and end-user satisfaction by improving the speed of delivery of popular repeated content.

FortiWeb-VM provides specialized, layered application threat protection for medium and large enterprises, application service providers and SaaS providers. FortiWeb Web application firewalls protect Web-based applications and Internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against malicious sources, application layer DoS attacks and sophisticated threats like SQL injection and Cross-site scripting, FortiWeb physical and virtual appliances help to prevent identity theft, financial fraud and denial of service. They deliver the technology enterprises need to monitor and enforce government regulations, industry best practices and internal policies.

"Data center customers, enterprises and MSPs building public and private cloud infrastructures now have a lot of choices when it comes to deploying virtualization platforms," said Chris Rodriguez, senior industry analyst for Frost & Sullivan. "In addition to VMware, Microsoft and Citrix, open source alternatives such as KVM have emerged. But this flexibility creates significant challenges when it comes to securing these environments. By adding support for Windows Server Hyper-V and KVM, along with support for Citrix and VMware, Fortinet now provides security support for the largest number of hypervisor platforms on the market today. And this gives customers assurances that whichever virtualization platform they choose, a comprehensive security offering is available for their virtualized infrastructure of choice."

"Our cloud customers demand a number of secure options for their virtualized infrastructures depending on the type of cloud they're deploying, and Fortinet offers the breadth and depth of network security virtual machines they require," said Chris Ward, GreenPages-LogicsOne CTO. "It is critically important to us that we can rely on Fortinet to support the different hypervisors."

Examining the Fortinet Virtual Security Ecosystem

Fortinet's virtual appliances can be provisioned rapidly and easily scale to protect intra-virtual machine communications by implementing critical security controls within virtual infrastructures. This enables customers to mitigate potentially harmful blind spots and increase policy compliance.

"As more companies build out public and private cloud infrastructures, all too often the selection of which virtualization platform to use is made independent of a security solution," said John Maddison, vice president of marketing for Fortinet. "That's why the addition of our support for Windows Server Hyper-V and KVM virtualization technologies is so significant. Now, customers can rest assured that their virtualization platform of choice -- regardless of vendor -- can be secured by Fortinet's virtual security ecosystem that supports the industry's broadest range of hypervisors."

Fortinet virtual machines currently support the industry leading hypervisors referenced in the accompanying image.

Additional Resources:
For more information on Fortinet's virtual security platform, please visit: http://www.fortinet.com/solutions/virtual_security.html.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a 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 2012 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

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