

February 24, 2014

Fortinet Upgrades and Extends Next-Generation Firewall (NGFW) With Authentication and Advanced Threat Protection

New Software and Hardware Releases Improve Class-Leading Performance and Security

SUNNYVALE, CA -- (Marketwired) -- 02/24/14 -- [Fortinet®](#) (NASDAQ: FTNT) -- a world leader in [high-performance network security](#) -- today announced a significant update to the company's [FortiOS](#) network security operating system, along with new releases for integrated reporting, advanced threat protection (APT) and strong authentication. These releases demonstrate Fortinet's vision of extending the [next-generation firewall](#) (NGFW) to address the challenges facing today's enterprises including increasingly complex cyber threats. As a result, Fortinet's [FortiGate®](#) appliances, which routinely deliver five times faster performance than competitive offerings, will deliver even greater performance and more security.

The FortiOS Advantage

FortiOS 5 is the operating system foundation for the FortiGate platform and offers a broad range of world class security capabilities and configuration options. Announced today, FortiOS 5 now delivers:

- Significantly faster SSL inspection
- Richer reporting with even more out-of-the-box reports and drill down capability from FortiAnalyzer
- Tighter integration with FortiAuthenticator and FortiSandbox for seamless Strong Authentication and Advanced Threat Protection

"Security leaders must address threats from rising SSL traffic," wrote Jeremy D'hoinne and Adam Hils, Research Directors with Gartner.¹ They go on to write, "Less than 20% of organizations with a firewall, an intrusion prevention system (IPS) or a unified threat management (UTM) appliance decrypt inbound or outbound SSL traffic. Gartner believes that, in 2017, more than half of the network attacks targeting enterprises will use encrypted traffic to bypass controls, up from less than 5% today."

"Enterprises today are clamoring for improved network visibility that includes deeper packet inspection and granular control over network access, traffic, content and use, and they want it without introducing bottlenecks into the real-world traffic flow," said John Maddison, vice president of marketing for Fortinet. "Today, Fortinet extends that capability with advanced threat protection and authentication, all from a single vendor and all orchestrated through a single management console."

Richer Reporting and Analysis from FortiAnalyzer

Today, the company released a FortiAnalyzer 5 update and announced the upcoming [FortiAnalyzer-3500E](#). Software enhancements include a wider selection of prebuilt reports and greater drilldown capabilities for better visibility into network behavior and tighter integration with the company's FortiGate platform. In addition, the new FortiAnalyzer-3500E will feature 24 TB (upgradable to 48 TB) of storage to meet the requirements of high volume enterprises.

Seamless Strong Authentication

The company also announced the enterprise-grade [FortiAuthenticator-1000D](#), which provides multiple methods of authentication, including hardware, software, email and SMS tokens to help enterprises move to a stronger, user-based authentication model in an increasingly BYOD world. The new appliance supports up to 10,000 users and integrates seamlessly with FortiGate appliances.

Advanced Threat Protection Together with FortiSandbox

Today's threat landscape includes increasingly sophisticated, highly targeted attacks (or advanced persistent threats) designed specifically to breach an individual or small set of organizations. Use of traditional FortiGate NGFW technologies -- firewall segmentation, IPS and antimalware strong in proactive detection, malicious application and Website filtering, Command and Control blocking, SSL Inspection and more -- have a role to play in hardening defenses. However, at some point a really determined attacker is likely to get through, and even a single compromise can be costly. Many organizations are looking at advanced or specialty threat detection solutions, including sandboxing, to complement traditional defenses and speed identification and response.

To help Fortinet customers meet this challenge, Fortinet has announced the new [FortiSandbox-1000D](#). Its unique dual-level sandbox along with proactive pre-filtering, dynamic threat intelligence and rich reporting are effective in detecting highly targeted attacks. And its consolidated approach to covering all protocols and functions in one appliance together with its ability to deploy stand-alone or as an integrated extension of FortiGate and [FortiMail](#) appliances, reduce cost and complexity. Finally, the new FortiSandbox-1000D (and previously released [FortiSandbox-3000D](#)) now run software version 1.2, which features

enhanced instrumentation to better deal with increasing virtual machine (VM) evasion techniques, an updated assessment engine to increase detection rates and new call-back detection to identify outbound communications both in the sandbox and on the wire.

Availability

The FortiOS 5/FortiAnalyzer 5 updates are available now. FortiAnalyzer-3500E is expected in the second quarter of this year. FortiAuthenticator-1000D is available now. The FortiSandbox 1.2 software update is available now for FortiSandbox-3000D customers, and the FortiSandbox-1000D is expected to ship in the second quarter of this year.

¹ = Gartner, Security Leaders Must Address Threats From Rising SSL Traffic, Jeremy D'Hoinne, Adam Hills, December 9, 2013.

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.

Copyright © 2013 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, including statements regarding product releases and functionality. 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 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
mbspolver@fortinet.com

Source: Fortinet

News Provided by Acquire Media