F⊖RTINET.

February 1, 2017

Fortinet FortiGate Enterprise Firewalls Approved by Defense Department's Top Cybersecurity Authority as a Solution for Classified Networks

FortiGate Firewalls Running FortiOS 5.4.2 Meet Stringent Federal Standards; Approved for Commercial Solutions for Classified (CSfC) Components List

SUNNYVALE, Calif., Feb. 01, 2017 (GLOBE NEWSWIRE) --

Philip Quade, chief information security officer, Fortinet
"US Federal customers require the industry's most advanced commercial technologies to deliver the best security for their networks. Fortinet's flagship product has been approved by the Defense Department's top cybersecurity authority as a solution for classified environments, validating that Fortinet delivers the performance and scale government organizations need for a complete security assurance solution."

News Summary
Fortinet® (NASDAQ:FTNT), the global leader in high-performance cybersecurity solutions, today announced that its FortiGate Enterprise Firewall has been added to the Commercial Solutions for Classified Programs (CSfC) approved Components List. Being validated against the Common Criteria Protection Profiles demonstrates Fortinet's commitment to deliver high-performance, scalable security solutions that are designed to protect highly-sensitive government and critical infrastructure data.

- Fortinet demonstrates commitment to deliver the highest caliber of network security solutions to protect classified government and critical infrastructure data.
- FortiGate Enterprise Firewalls running FortiOS 5.4.2 are being validated against three NIAP Protection Profiles relevant to the FortiGate under the rigorous U.S. implementation of the Common Criteria: Collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 1.0; Extended Package - VPN Gateway, Version 2.0; and Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.1.
- The CSfC Program has been established to enable commercial products to be used in layered solutions protecting classified Federal government data. This will provide the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.

Fortinet's U.S. Federal Agency security solution is ideally suited to protect agencies within the intelligence community and the Department of Defense, as well as civilian agencies. The Fortinet Security Fabric protects classified and unclassified Federal systems used by 12 of 15 cabinet-level agencies and by numerous independent executive agencies. These platforms make use of our USG products that are specially configured for the Federal market. They comply with Federal certification requirements including the National Institute of Standards and Technology FIPS 140-2 certification, National Information Assurance Partnership Common Criteria certification, and the Department of Defense Unified Capabilities certification.

Additional Resources

- Please visit https://www.fortinet.com for more details about the Fortinet Security Fabric for government organizations.
- Follow Fortinet on Twitter, LinkedIn, and Facebook.
- Join the conversation on the Fortinet blog.

About Fortinet
Fortinet (NASDAQ:FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 290,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

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, FortiCloud, 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 technology and functionality releases and release times. Changes of circumstances, product release delays or product priority or roadmap changes, 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.

Media Contact:

Darlene Gannon

Fortinet, Inc.

408.235.7700

pr@fortinet.com

Investor Contact:

Sandra Wheatley

Fortinet, Inc.

408-391-9408

swheatley@fortinet.com

Investor Contact:

Ron Davis

Fortinet, Inc.

408-486-7837

rdavis@fortinet.com

Source: Fortinet, Inc.

News Provided by Acquire Media