FORTINET

Rural Wisconsin Healthcare Cooperative Engages Fortinet to Help With Compliance

Network of Hospitals Protected From Excess Spam and Malicious Attacks With FortiMail and FortiGate Appliances

SUNNYVALE, CA -- (MARKET WIRE) -- 04/04/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced that Rural Wisconsin Healthcare Cooperative (RWHC) has deployed Fortinet appliances throughout its core network which hosts various applications for many of its 35 member hospitals and clinics as well as throughout its Information Technology Network which consists of four hospitals joining forces to share Electronic Health Records (EHR) resources. The Fortinet appliances are being used to help reduce the amount of spam hitting the network and to help enable the healthcare provider to better protect the network of Critical Access hospitals in an economically viable manner.

Previously using a Cisco-based solution, the IT team at RWHC turned to trusted partner, Digicorp, an industry leader in computer networking, computer security, video teleconferencing and IP video surveillance. Together, Fortinet appliances were selected to help RWHC with compliance with Federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) as well as to help with certain requirements of the Rural Health Care Pilot Program (RHCPP). The Cisco solution did not meet all RWHC Information Technology Network needs in a single termination point.

RWHC
The rural Wide Area Network (WAN) initiative connects a number of hospitals to services provided by RWHC and third-party providers and the IT team at RWHC is responsible for managing the core network. Deployed in the network are FortiGate®-310B appliances, FortiGate-200B appliances and FortiGate-30B appliances located at different hospitals and clinics. The appliances are helping to provide antivirus and intrusion prevention protection as well as firewall protection and various VPN services.

Also deployed throughout the RWHC network are FortiMail™ appliances. The appliances are helping to protect eight differen email domains consisting of roughly 2,000 employee email addresses. Prior to the FortiMail deployment, the IT staff were seeing more than 200,000 emails a day passing through the network. Since the deployment, that number has dropped to 35,000 -- a direct result of spam being blocked before it enters the RWHC network.

Rural Wisconsin Health Cooperative Information Technology Network (RWHCITN)
The second deployment is the RWHCITN Wide Area Network (funded by the RHCPP) which consists of four hospitals. The primary goals of the RWHCITN are (1) to provide high speed, redundant WAN connectivity for facilities participating in a RWHC Shared EHR initiative, (2) to use technology to achieve CMS-mandated "Meaningful Use" and (3) to implement WAN security and reporting features. By sharing resources, the hospitals will reduce medication errors, facilitate the practice of evidence-based medicine and improve care quality.

Located at the Tomah Memorial Hospital, Memorial Hospital of Lafayette County, St. Joseph's Community Health Services and Boscobel Area Health Care are an active/passive pair of FortiGate-200B appliances. The Fortinet solution is helping to secure the WAN connection to a redundant pair of FortiGate-310B appliances at the RWHC Information Technology Network datacenter in Sauk City, Wis. and to a redundant pair of FortiGate-310B appliance as well as FortiManager™ and FortiAnalyzer™ appliances located at the Madison, Wis. datacenter. The FortiManager and FortiAnalyzer appliances are helping the IT team to manage all deployed FortiGate appliances and analyze data traversing the network.

"We are extremely pleased with the Fortinet deployment. Our employees are much more productive with the reduction of spam thanks to the FortiMail appliance. Additionally, the deployment of FortiGate solution throughout the pilot program is allowing small rural hospitals the same amount of network security that their larger counterparts have access to -- something that would not have been previously available to them," said David Chitwood, Information Technology manager at Rural Wisconsin Healthcare Cooperative. "We are able to see these great benefits while also helping us meet compliance mandates."

"RWHC is a great example of a healthcare organization taking full advantage of Fortinet's breadth and depth of products because they realize that network security is more than just a firewall or a single functionality," said Pete Brant, vice president of enterprise sales at Fortinet. "The combination of FortiGate appliances and FortiMail makes a powerful security solution for an industry that is so tightly regulated by safeguards to protect data."

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the 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 2009 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.

Copyright © 2011 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, FortiDB 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. For clarity, Fortinet makes no contractual commitments, guarantees or assurances herein. This news release may contain forward-looking statements that involve uncertainties and assumptions. 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, including but not limited to, any statements related to expected trends in cybercriminal activity. These trends are difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contact:

Maeve Naughton

Fortinet, Inc.

(408) 486-7819

mnaughton@fortinet.com

Source: Fortinet

News Provided by Acquire Media